

Diszkrét matematika 2.

Szóbelin várható tételbizonyítások

A kidolgozást dr. Nagy Gábor előadásdiái alapján Lanka Máté készítette.

1. Gráfok alapfogalmai

Mit mondhatunk irányítatlan gráfban a fokszámok összegéről?

Állítás

A $G = (\varphi, E, V)$ gráfra

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

Bizonyítás

Élszám szerinti teljes indukció: $|E| = 0$ esetén mindkét oldal 0. Tfh. $|E| = n$ esetén igaz az állítás. Ha adott egy gráf, amelynek $n + 1$ éle van, akkor annak egy élet elhagyva egy n élű gráfot kapunk. Erre teljesül az állítás az indukciós feltevés miatt. Az elhagyott élt újra hozzávéve a gráfhoz az egyenlőség mindkét oldala 2-vel nő.

Mit mondhatunk teljes gráf élszámáról?

Példa

Ha egy egyszerű gráfban bármely két különböző csúcs szomszédos, akkor **teljes gráfról** beszélünk.

Teljes gráfok esetén, ha a csúcsok halmazai között létezik bijektív leképezés, akkor a két teljes gráf a csúcsok és élek elnevezésétől eltekintve megegyezik. Ebben az értelemben beszélünk bármely $n \in \mathbb{Z}^+$ esetén az n csúcsú teljes gráfról.

Megjegyzés

Az n csúcsú teljes gráfnak $\binom{n}{2} = n(n-1)/2$ éle van, és K_n -nel jelöljük.

Mit állíthatunk séta és út kapcsolatáról?

Megjegyzés

Egy út mindig vonal.

A nulla hosszú séták mind utak, és egyetlen csúcsból állnak.

Az egy hosszú séták utak, ha a bennük szereplő él nem hurokél.

Legyen \sim a csúcsok halmazán értelmezett reláció, amelyre $v_1 \sim v_2$ pontosan akkor, ha

van v_1 kezdőpontú és v_2 végpontú séta a gráfban. Bizonyítsd be, hogy ez a reláció ekvivalenciareláció!

Definíció

Egy gráfot **összefüggőnek** nevezünk, ha bármely két csúcsa összeköthető sétával.

A $G = (\varphi, E, V)$ gráf esetén V elemeire vezessük be a \sim relációt: $v \sim v'$ pontosan akkor, ha G -ben vezet út v -ből v' -be.

A \sim ekvivalenciareláció (Miért?), így meghatároz egy osztályozást V -n.

A csúcsok egy adott ilyen osztálya által meghatározott feszített részgráf a gráf egy **komponense**.

2. Fák

Add meg 3 ekvivalens jellemzését a fa fogalmának!

Tétel

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 1 út van v -ből v' -be;
- (4) G -nek nincs köre, de bármilyen új él hozzávételével kapott gráf már tartalmaz kört.



A bizonyítás menete

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

Bizonyítás

$(1) \Rightarrow (2)$

G összefüggősége következik a fa definíciójából. Az állítás másik részét indirekten bizonyítjuk.

Tfh. létezik egy olyan e él (a végpontjai legyenek v és v') a gráfban, aminek a törlésével kapott gráf összefüggő. Ekkor létezne út v -ből v' -be, amit kiegészítve a törölt éllel és a megfelelő csúccsal egy kört kapnánk:

$v, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v', e, v$.

$(2) \Rightarrow (3)$

Legalább egy út létezik az összefüggőség miatt. Indirekten bizonyítjuk, hogy nem létezhet két különböző út:

Tfh. 2 út is létezik a különböző v és v' csúcsok között, legyenek ezek:

$v, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v'$ és $v, e'_1, v'_1, e'_2, \dots, v'_{m-1}, e'_m, v'$. Legyen k a legkisebb olyan index, amelyre $v_k \neq v'_k$. (Miért létezik ilyen?) Az e_k élt törölve összefüggő gráfot kapunk, mert a v_{k-1}, e_k, v_k séta helyettesíthető a $v_{k-1}, e'_k, v'_k, \dots, e'_m, v', e_n, v_{n-1}, e_{n-1}, v_{n-2}, \dots, v_{k+1}, e_{k+1}, v_k$ sétával.

Bizonyítás

(3) \Rightarrow (4)

Annak a bizonyítása, hogy nincs kör a gráfban indirekt:

tfh. létezik kör: $v, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v$. Ekkor v_1 és v között két különböző út is van: $v_1, e_2, \dots, v_{n-1}, e_n, v$ illetve v_1, e_1, v .

Ha a hozzávett e él hurokél, és a v csúcsra illeszkedik, akkor v, e, v kör lesz. Ha a hozzávett e él a különböző v és v' csúcsokra illeszkedik, akkor a köztük lévő utat megfelelően kiegészítve kapunk kört:

$v, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v', e, v$.

(4) \Rightarrow (1)

Az, hogy G -nek nincs köre triviálisan teljesül. Kell, hogy G összefüggő, vagyis tetszőleges v és v' csúcsa között van út. Vegyük a gráfhoz a v -re és v' -re illeszkedő e élet. Az így keletkező körben szerepel e (Miért?):

$v', e, v, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v'$. Ekkor $v, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v'$ út lesz v és v' között.



Mit mondhatunk körmentes gráfban az elsőfokú csúcsokról?

Lemma

Ha egy G véges gráfban nincs kör, de van él, akkor G -nek van legalább 2 elsőfokú csúcsa.

Bizonyítás

A G -beli utak között van maximális hosszúságú (hiszen G véges), és a hossza legalább 1, így a végpontjai különbözőek. Megmutatjuk, hogy ezek elsőfokúak. Legyen az említett út: $v_0, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v_n$. Ha lenne az e_1 -től különböző v_0 -ra illeszkedő e él, annak másik végpontja (v') nem lehet az útban szereplő csúcsoktól különböző, mert akkor $v', e, v_0, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v_n$ út hossza nagyobb lenne, mint a maximális út hossza. Ha viszont e másik végpontja az út valamely v_k csúcsa, akkor $v_k, e, v_0, e_1, v_1, e_2, \dots, v_{k-1}, e_k, v_k$ kör lenne, ami szintén ellentmondás.

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

Tétel

Egy G egyszerű gráfra, amelynek n csúcsa van ($n \in \mathbb{Z}^+$) 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.

Bizonyítás

$n = 1$ esetén az állítás triviális. (Miért?)

(1) \Rightarrow (2): n szerinti TI: tfh. $n = k$ -ra igaz az állítás. Tekintsünk egy $k + 1$ csúcsú G fát. Ennek legyen v egy olyan csúcsa, aminek a foka 1. (Miért van ilyen?) Hagyjuk el a gráfból v -t. Az így kapott gráf G'

nyilván körmentes. Összefüggő is lesz, hiszen v egy G -beli útnak csak kezdő- vagy végpontja lehet, így a G' tetszőleges v' és v'' csúcsa közti G -beli út nem tartalmazhatja sem v -t, sem a rá illeszkedő élt, így G' -beli út is lesz egyben. Tehát G' fa, ezért alkalmazva az indukciós feltevést $k - 1$ éle van, és így G -nek k éle van.

Bizonyítás

(2) \Rightarrow (3): n szerinti TI: tfh. $n = k$ -ra igaz az állítás. Tekintsünk egy $k + 1$ csúcsú körmentes G gráfot, aminek k éle van. Ennek legyen v egy olyan csúcsa, aminek a foka 1. (Miért van ilyen?) Hagyjuk el a gráfból v -t. Az így kapott G' gráf az indukciós feltevés miatt összefüggő, tehát tetszőleges v' és v'' csúcsa között vezet út G' -ben, ami tekinthető G -beli útnak is. G' tetszőleges csúcsa és v közötti utat úgy kaphatunk, hogy az adott csúcs és a v -vel szomszédos csúcs közötti utat kiegészítjük az elhagyott éllel és v -vel.

(3) \Rightarrow (1): Ha a feltételnek eleget tevő gráfban van kör, akkor az abban szereplő tetszőleges él elhagyásával összefüggő gráfot kapunk. (Miért?) Folytassuk az élek törlését, amíg már nincs több kör a kapott gráfban, tehát fa lesz. Ha k élt hagytunk el, akkor a kapott gráfnak $n - 1 - k$ éle van, ugyanakkor az (1) \Rightarrow (2) rész miatt a kapott fának $n - 1$ éle van, így $k = 0$, tehát a gráfunkban nem volt kör, így fa.

3. Feszítőfa, Euler-vonal, Hamilton-kör Mikor létezik feszítőfája egy gráfnak?

Állítás

Minden összefüggő véges gráfnak létezik feszítőfája.

Bizonyítás

Amíg van kör a gráfban, hagyjuk el annak egy élet. A kapott gráf összefüggő marad. Véges sok lépésben fát kapunk.

Mit mondhatunk összefüggő gráfban a körök számáról?

Állítás

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

Bizonyítás

Tekintsük G -nek egy F feszítőfáját. Ennek $|V| - 1$ éle van. Jelöljük E' -vel G azon éleinek halmazát, amelyek nem élei F -nek. $e \in E'$ -t hozzávéve F -hez keletkezik egy K_e kör (Miért?), ami kör G -ben. A K_e kör tartalmazza e -t (Miért?), és $e \neq e' \in E'$ esetén $K_{e'}$ nem tartalmazza e -t. Így kapunk $|E| - |V| + 1$ kört, amiknek az élhalmaza különbözik.

Mit mondhatunk összefüggő gráfban a vágások számáról?

Állítás

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

Bizonyítás

Tekintsük G -nek egy F feszítőfáját. Jelöljük E' -vel F éleinek halmazát, E'' -vel pedig G azon éleinek halmazát, amelyek nem élei F -nek. Ekkor E'' nem elvágó halmaz (Miért?), de tetszőleges $e \in E'$ esetén $E'' \cup \{e\}$ már az (Miért?). Legyen E_e az a vágás, amit $E'' \cup \{e\}$ tartalmaz (Miért van ilyen?). E_e tartalmazza e -t (Miért?), de $e \neq e' \in E'$ esetén nem tartalmazza e' -t, így kaptunk $|V| - 1$ különböző vágást.

Mit állíthatunk összefüggő gráfban zárt Euler-vonal létezésével kapcsolatban?

Állítás

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

Bizonyítás

\Rightarrow : Legyen a zárt Euler-vonal a következő:

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

A vonal kezdő- és végpontját leszámítva egy csúcs minden előfordulása esetén a mellette lévő két különböző él 2-vel járul hozzá a fokszámahoz. A kezdő- és végpont ugyanaz, ezért ennek is páros lesz a foka.

Bizonyítás

\Leftarrow : a bizonyítás konstruktív. Induljunk ki egy élt nem tartalmazó, zárt vonalból (v). Ha az aktuális zárt vonalban nem minden él szerepel, akkor az összefüggőség miatt van olyan csúcs (v'), amelyre illeszkedő élek közül

nem szerepel mindegyik. Induljunk el ebből a csúcsból egy fel nem használt élen, és haladjunk tovább mindig fel nem használt éleken. Mivel minden csúcsra páros sok fel nem használt él illeszkedik, a továbbhaladás csak akkor nem lehetséges, ha visszaértünk v' -be. Ha most az eredeti vonalon elmegyünk v -ből v' -be, az új vonalon körbemegyünk, majd az eredeti vonalon haladunk tovább, akkor az eredeti vonalnál hosszabb, zárt vonalat kapunk, így ezt az eljárást ismételve véges sok lépésben megkapunk egy Euler-vonalat.

4. Címkeztet gráfok

Ismertesd a Kruskal algoritmust és a rá vonatkozó tételt!

Algoritmus(Kruskal)

Egy élsúlyozott gráf esetén az összes csúcsot tartalmazó üres részgráfból kiindulva minden lépésben vegyük hozzá a minimális súlyú olyan élt, amivel nem keletkezik kör.

Tétel

A Kruskal-algoritmus egy minimális súlyú feszítőerdőt határoz meg. Összefüggő gráf esetén minimális súlyú feszítőfát kapunk.

Bizonyítás

Elég összefüggő gráfra bizonyítani (Miért?).

Összefüggő gráf esetén az algoritmus nyilván feszítőfát eredményez (Miért?).

Indirekt tfh. van az algoritmus által meghatározott F feszítőfánál kisebb súlyú F' feszítőfája a gráfnak. Ha több ilyen van, akkor válasszuk közülük azt, amelyiknek a legtöbb közös éle van F -fel. Legyen e' olyan éle F' -nek, ami nem éle F -nek. (Miért van ilyen?) Az F -hez e' hozzávételével kapott gráfban van egy K kör (Miért?). Ezen kör tetszőleges e élére $w(e) \leq w(e')$ (Miért?). Az F' -ből az e' törlésével kapott gráf nem összefüggő (Miért?), és pontosan 2 komponense van (Miért?). A K -nak van olyan éle (e''), aminek a végpontjai az F' -ből az e' törlésével kapott gráf különböző komponenseiben vannak (Miért?).

Biz.folyt.

Tekintsük azt a gráfot, amit F' -ből az e' törlésével és az e'' hozzávételével kapunk. Az így kapott gráf is feszítőfa (Miért?), és $w(e'') < w(e')$ esetén kisebb súlyú, mint F' , míg $w(e'') = w(e')$ esetén ugyanakkora súlyú, de több közös éle van F -fel. Mindkét esetben ellentmondásra jutottunk.

5. Síkba rajzolható gráfok, gráfok színezése, gráfok ábrázolása Hogy szól Euler tétele síkba rajzolható gráfokról?

Tétel (Euler-formula)

Egy $G = (\varphi, E, V)$ összefüggő síkgráf tetszőleges síkbeli reprezentációját tekintve, melyre t jelöli a tartományok számát, teljesül a következő összefüggés.

$$|E| + 2 = |V| + t$$

Bizonyítás (vázlat)

Ha a gráfban van kör, annak egy élét törölve az általa elválasztott két tartomány egyesül, így a tartományok és élek száma is (vagyis az egyenlet mindkét oldala) 1-gyel csökken. Az eljárás ismétlésével fát kapunk, amire teljesül az összefüggés (Miért?).

Mit mondhatunk síkgráf élszámáról?

Állítás

Ha a $G = (\varphi, E, V)$ egyszerű, összefüggő síkgráfra $|V| \geq 3$, akkor

$$|E| \leq 3|V| - 6.$$

Bizonyítás

$|V| = 3$ esetén 2 ilyen gráf van: P_2 és C_3 , amelyekre teljesül az állítás. $|V| > 3$ esetén legalább 3 éle van a gráfnak (Miért?). Mivel G egyszerű, ezért minden tartományát legalább 3 él határolja, ezért a tartományok határán végigszámolva az éleket az így kapott érték legalább $3t$. Mivel minden él legfeljebb két tartományt választ el, ezért $3t \leq 2|E|$. Az Euler-formulát használva $3(|E| + 2 - |V|) \leq 2|E|$, amiből kapjuk az állítást.

Mit mondhatunk síkgráfban a minimális foksámú csúcs fokáról?

Állítás

Ha $G = (\varphi, E, V)$ egyszerű, összefüggő síkgráf, akkor

$$\delta = \min_{v \in V} d(v) \leq 5.$$

Bizonyítás

Feltehető, hogy $|V| \geq 3$ (Miért?).

Indirekt tfh. $\delta \geq 6$. Ekkor $6|V| \leq 2|E|$ (Miért?), továbbá az előző állítást használva $2|E| \leq 6|V| - 12$, vagyis $6|V| \leq 6|V| - 12$, ami ellentmondás.

Bizonyítsd be, hogy K_5 és $K_{3,3}$ nem síkgráf!

Állítás

$K_{3,3}$ nem síkgráf.

Bizonyítás

Indirekt tfh. $K_{3,3}$ síkgráf, és jelöljük t -vel a síkbeli reprezentációjában a tartományok számát. Ekkor $|E| = 9$ és $|V| = 6$ miatt az Euler-formula alapján $t = 5$. Mivel páros gráf, így minden tartomány határa legalább 4 élt tartalmaz (Miért?), és minden él két tartomány határán van, ezért $4t \leq 2|E|$, amiből $20 \leq 18$ adódik, ami ellentmondás.



Állítás

K_5 nem síkgráf.

Bizonyítás

Indirekt tfh. K_5 síkgráf. $|E| = 10$ és $|V| = 5$, így az élszámra vonatkozó becslés alapján $10 \leq 3 \cdot 5 - 6 = 9$, ami ellentmondás.

6. Irányított gráfok

Mit mondhatunk a fokszámösszegekről irányított gráfban?

Állítás


A $G = (\psi, E, V)$ irányított gráfra

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



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

A $G = (\psi, E, V)$ irányított gráf esetén V elemeire vezessük be a \sim relációt: $v \sim v'$ pontosan akkor, ha G -ben vezet irányított út v -ből v' -be, és v' -ből is vezet irányított út v -be.

A \sim ekvivalenciareláció (Miért?), így meghatároz egy osztályozást V -n. 

A csúcsok egy adott ilyen osztálya által meghatározott feszített irányított részgráf az irányított gráf egy **erős komponense**.

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

Állítás

A gyökérből bármely adott csúcsba vezető egyetlen út egyben irányított út is.

Bizonyítás

Az út hossza szerinti TI: ha az út hossza $n = 1$, akkor azért lesz irányított út, mert a gyökér befoka 0. Tfh. $n = k$ -ra teljesül az állítás. Vegyünk egy olyan v csúcsot, amibe vezető út hossza $k + 1$. Az útból elhagyva v -t és a rá illeszkedő e élt egy k hosszú utat kapunk, amiről az indukciós feltevés értelmében tudjuk, hogy ir. út. v nem lehet e kezdőpontja, mert akkor az e -re illeszkedő másik csúcs befoka legalább 2 lenne.

Bizonyítsd be Dijkstra algoritmusának a helyességét!

Algoritmus (Dijkstra)

A $G = (\psi, E, V, w)$ élsúlyozott irányított gráfról tegyük fel, hogy az élsúlyok pozitívak, $s \in V$ és $T \subset V$.

- (1) Legyen $S = \emptyset$, $H = \{s\}$ és $d(s) = 0$; minden más v csúcsra legyen $d(v) = \infty$
- (2) Ha $T \subset S$ vagy $H = \emptyset$, akkor az algoritmus véget ér.
- (3) Legyen $t \in H$ egy olyan csúcs, amelyre $d(t)$ minimális. Tegyük át t -t S -be, és minden e élre, amely t -ből $v \in V \setminus S$ -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.

Tétel

A Dijkstra-algoritmus a csúcshalmazon értelmez egy $d: V \rightarrow \overline{\mathbb{R}}$ függvényt, amely $t \in T$ esetén az adott s csúcsból a t csúcsba vezető irányított séták minimuma (∞ , ha nincs ilyen séta).

Bizonyítás

Az S elemszáma szerinti indukcióval megmutatjuk, hogy:

- 1 minden $t \in S$ -re $d(t)$ az s csúcsból a t csúcsba vezető irányított séták súlyának minimuma;

- ha $v \in H$, akkor minden olyan s -ből v -be vezető irányított sétának, amelynek v -n kívül minden csúcsa S -ben van a súlya legalább $d(v)$.

Inicializálás után ezek nyilvánvalóak.

Tegyük fel, hogy (3)-ban $t \in H$ -t választottuk, és tekintsünk egy tetszőleges s -ből t -be vezető irányított sétát, aminek a súlya W , továbbá legyen t' a séta első olyan csúcsa, amely nincs S -ben. A séta s -ből t' -ig vivő részének W' súlyára $W' \leq W$ (Miért?), az indukciós feltevés második része szerint $d(t') \leq W'$, és mivel t -t választottuk $d(t) \leq d(t')$, így $d(t) \leq W$, amivel az állítás első részét beláttuk.

Biz.folyt.

Miután (3)-ban a $d(v)$ értékeket megváltoztattuk, ha egy séta s -ből v -be visz, és csak az utolsó csúcsa nincs S -ben, legyen t' az utolsó előtti csúcsa, e pedig az utolsó éle. Mivel $t' \in S$, az s -től t' -ig vezető részséta súlya legalább $d(t')$, így a teljes súlya legalább $d(t') + w(e)$, és amikor t' -t bevettük S -be legfeljebb ennyire állítottuk $d(v)$ értékét, azóta pedig csak csökkenhetett.

7. Algebrai alapok, polinomokkal kapcsolatos alapfogalmak Mi teljesül nullelemmel való szorzás esetén?

Állítás

Legyen $(R; *, \circ)$ gyűrű $0 \in R$ nullelemmel. Ekkor $\forall r \in R$ esetén $0 \circ r = r \circ 0 = 0$.

Bizonyítás

$$0 \circ r = (0 * 0) \circ r = (0 \circ r) * (0 \circ r) \implies 0 = 0 \circ r.$$

A másik állítás bizonyítása ugyanígy.

Mit mondhatunk testben a nullosztókról?

Állítás

Test nullosztómentes.

Bizonyítás

Legyen $(F; *, \circ)$ test $0 \in F$ nullelemmel, és $1 \in F$ egységelemmel.
Indirekt tfh. léteznek $a, b \in F$ nem-nulla elemek, amikre $a \circ b = 0$.
Ekkor $b = 1 \circ b = a^{-1} \circ a \circ b = a^{-1} \circ 0 = 0$, ami ellentmondás.



Mit mondhatunk polinomok összegének/szorzatának fokáról?

Állítás

Legyen $f, g \in R[x]$, $\deg(f) = n$, és $\deg(g) = k$. Ekkor:

- $\deg(f + g) \leq \max(n, k)$;
- $\deg(f \cdot g) \leq n + k$.

Bizonyítás

Legyen $h = f + g$. Ekkor $j > \max(n, k)$ esetén $h_j = 0 + 0 = 0$.

Legyen $h = f \cdot g$. Ekkor $j > n + k$ esetén

$$h_j = \sum_{i=0}^j f_i g_{j-i} = \sum_{i=0}^n f_i g_{j-i} + \sum_{i=n+1}^j f_i g_{j-i} = \sum_{i=0}^n f_i \cdot 0 + \sum_{i=n+1}^j 0 \cdot g_{j-i} = 0.$$

R milyen tulajdonságai öröklődnek $R[x]$ -re?

Állítás

Ha az R gyűrű kommutatív, akkor $R[x]$ is kommutatív.

Bizonyítás

$$\begin{aligned}(f \cdot g)_k &= f_0 g_k + f_1 g_{k-1} + \dots + f_{k-1} g_1 + f_k g_0 = \\ &= g_k f_0 + g_{k-1} f_1 + \dots + g_1 f_{k-1} + g_0 f_k = \\ &= g_0 f_k + g_1 f_{k-1} + \dots + g_{k-1} f_1 + g_k f_0 = (g \cdot f)_k\end{aligned}$$

8. Polinomok maradékos osztásának tétele és következményei

Hogyan szól a polinomok maradékos osztásának tétele?

Tétel (polinomok maradékos osztása)

Legyen R egységelemes integritási tartomány, $f, g \in R[x]$, és tegyük fel, hogy g főegyütthatója egység R -ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = qg + r$, ahol $\deg(r) < \deg(g)$.

Bizonyítás

Létezés: f foka szerinti TI: ha $\deg(f) < \deg(g)$, akkor $q = 0$ és $r = f$ esetén megfelelő előállításunk.

Legyen f főegyütthatója f_n , g főegyütthatója g_k . $n \geq k$ esetén legyen

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

$\deg(f^*) < \deg(f)$ (Miért?) miatt f^* -ra használhatjuk az indukciós

feltevést, vagyis léteznek $q^*, r^* \in R[x]$ polinomok, amikre $f^* = q^*g + r^*$.

$$f(x) = f^*(x) + f_n g_k^{-1} g(x) x^{n-k} = q^*(x)g(x) + r^*(x) + f_n g_k^{-1} g(x) x^{n-k} = (q^*(x) + f_n g_k^{-1} x^{n-k})g(x) + r^*(x),$$

így $q(x) = q^*(x) + f_n g_k^{-1} x^{n-k}$ és $r(x) = r^*(x)$ jó választás.

Bizonyítás folyt.

Egyértelműség: Tekintsük f két megfelelő előállítását:

$$f = qg + r = q^*g + r^*, \text{ amiből:}$$

$$g(q - q^*) = r^* - r.$$

Ha a bal oldal nem 0, akkor a foka legalább k , de a jobb oldal foka legfeljebb $k - 1$, tehát

$$0 = g(q - q^*) = r^* - r, \text{ és így}$$

$$q = q^* \text{ és } r = r^*.$$

Hogy szól a gyöktényező leválasztására vonatkozó tétel?

Következmény (gyöktényező leválasztása)

Ha $0 \neq f \in R[x]$, és $c \in R$ gyöke f -nek, akkor létezik olyan $q \in R[x]$, amire $f(x) = (x - c)q(x)$.

Bizonyítás

Osszuk el maradékosan f -et $(x - c)$ -vel (Miért lehet?):

$$f(x) = q(x)(x - c) + r(x).$$

Mivel $\deg(r(x)) < \deg(x - c) = 1$, ezért r konstans polinom.

Helyettesítsünk be c -t, így azt kapjuk, hogy

$$0 = f(c) = q(c)(c - c) + r(c) = r(c),$$

amiből $r = 0$.

Hány gyöke lehet egy polinomnak?

Következmény

Az $f \neq 0$ polinomnak legfeljebb $\deg(f)$ gyöke van.

Bizonyítás

f foka szerinti TI:

$\deg(f) = 0$ -ra igaz az állítás (Miért?).

Ha $\deg(f) > 0$, és $f(c) = 0$, akkor $f(x) = (x - c)g(x)$ (Miért?), ahol $\deg(g) + 1 = \deg(f)$ (Miért?). Ha d gyöke f -nek, akkor $d - c = 0$, amiből $d = c$, vagy d gyöke g -nek (Miért?). Innen következik az állítás.

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

Következmény

Ha két, legfeljebb n -ed fokú polinomnak $n + 1$ különböző helyen ugyanaz a helyettesítési értéke, akkor egyenlők.

Bizonyítás

A két polinom különbsége legfeljebb n -ed fokú, és $n + 1$ gyöke van (Miért?), ezért nullpolinom (Miért?), vagyis a polinomok egyenlők.

Mit mondhatunk végtelen R esetén a polinomfüggvényekről?

Következmény

Ha R végtelen, akkor két különböző $R[x]$ -beli polinomhoz nem tartozik ugyanaz a polinomfüggvény.

Bizonyítás

Ellenkező esetben a polinomok különbségének végtelen sok gyöke lenne (Miért?).

Bizonyítsd be a bővített euklideszi algoritmus helyességét test fölötti polinomok esetén!

Algoritmus

Legyen R test, $f, g \in R[x]$. Ha $g = 0$, akkor $(f, g) = f = 1 \cdot f + 0 \cdot g$, különben végezzük el a következő maradékos osztásokat:

$$\begin{aligned}f &= q_1 g + r_1; \\g &= q_2 r_1 + r_2; \\r_1 &= q_3 r_2 + r_3; \\&\vdots \\r_{n-2} &= q_n r_{n-1} + r_n; \\r_{n-1} &= q_{n+1} r_n.\end{aligned}$$

Ekkor $d = r_n$ jó lesz kitüntetett közös osztónak.

Az $u_{-1} = 1$, $u_0 = 0$, $v_{-1} = 0$, $v_0 = 1$ kezdőértékekkel, továbbá az $u_k = u_{k-2} - q_k \cdot u_{k-1}$ és $v_k = v_{k-2} - q_k \cdot v_{k-1}$ rekurziókkal megkapható $u = u_n$ és $v = v_n$ polinomok olyanok, amelyekre teljesül $d = u \cdot f + v \cdot g$.

Bizonyítás

A maradékok foka természetes számok szigorúan monoton csökkenő sorozata, ezért az eljárás véges sok lépésben véget ér.

Indukcióval belátjuk, hogy $r_{-1} = f$ és $r_0 = g$ jelöléssel $r_k = u_k \cdot f + v_k \cdot g$ teljesül minden $-1 \leq k \leq n$ esetén:

$k = -1$ -re $f = 1 \cdot f + 0 \cdot g$, $k = 0$ -ra $g = 0 \cdot f + 1 \cdot g$.

Mivel $r_{k+1} = r_{k-1} - q_{k+1} \cdot r_k$, így az indukciós feltevést használva:

$$\begin{aligned}r_{k+1} &= u_{k-1} \cdot f + v_{k-1} \cdot g - q_{k+1} \cdot (u_k \cdot f + v_k \cdot g) = \\&= (u_{k-1} - q_{k+1} \cdot u_k) \cdot f + (v_{k-1} - q_{k+1} \cdot v_k) \cdot g = u_{k+1} \cdot f + v_{k+1} \cdot g.\end{aligned}$$

Tehát $r_n = u_n \cdot f + v_n \cdot g$, és így f és g közös osztói r_n -nek is osztói.

Kell még, hogy r_n osztója f -nek és g -nek.

Indukcióval belátjuk, hogy $r_n | r_{n-k}$ teljesül minden $0 \leq k \leq n+1$ esetén:

$k = 0$ -ra $r_n | r_n$ nyilvánvaló, $k = 1$ -re $r_{n-1} = q_{n+1} r_n$ miatt $r_n | r_{n-1}$.

$r_{n-(k+1)} = q_{n-(k-1)} r_{n-k} + r_{n-(k-1)}$ miatt az indukciós feltevést használva kapjuk az állítást, és így $k = n$, illetve $k = n+1$ helyettesítéssel

$r_n | r_0 = g$, illetve $r_n | r_{-1} = f$.

9. Polinomok algebrai deriváltja, véges testek, racionális gyökteszt, Lagrangeinterpoláció

Mivel egyenlő elsőfokú főpolinom n -edik hatványának deriváltja?

Állítás

Ha R egységelemes integritási tartomány, $c \in R$ és $n \in \mathbb{N}^+$, akkor $((x - c)^n)' = n(x - c)^{n-1}$.

Bizonyítás

n szerinti TI:

$n = 1$ esetén $(x - c)' = 1 = 1 \cdot (x - c)^0$.

Tfh. $n = k$ -ra teljesül az állítás, vagyis $((x - c)^k)' = k(x - c)^{k-1}$.

Ekkor

$$\begin{aligned} ((x - c)^{k+1})' &= ((x - c)^k(x - c))' = ((x - c)^k)'(x - c) + (x - c)^k(x - c)' = \\ &= k(x - c)^{k-1}(x - c) + (x - c)^k \cdot 1 = (x - c)^k(k + 1). \end{aligned}$$

Ezzel az állítást beláttuk.

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

Tétel

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

Bizonyítás

Ha $f(x) = (x - c)^n g(x)$, ahol c nem gyöke g -nek, akkor

$$\begin{aligned} f'(x) &= ((x - c)^n)'g(x) + (x - c)^n g'(x) = \\ &= n(x - c)^{n-1}g(x) + (x - c)^n g'(x) = (x - c)^{n-1}(ng(x) + (x - c)g'(x)). \end{aligned}$$

Tehát c tényleg legalább $(n - 1)$ -szeres gyöke f' -nek, és akkor lesz

$(n - 1)$ -szeres gyöke, ha c nem gyöke $ng(x) + (x - c)g'(x)$ -nek, vagyis $0 \neq ng(c) + (c - c)g'(c) = ng(c) + 0 \cdot g'(c) = ng(c)$. Ez pedig teljesül, ha $\text{char}(R) \nmid n$.

Hogyan adható meg olyan polinom, amely adott helyeken adott helyettesítési értékkel rendelkezik?

Tétel

Legyen R test, $c_0, c_1, \dots, c_n \in R$ különbözőek, továbbá $d_0, d_1, \dots, d_n \in R$ tetszőlegesen. Ekkor létezik egy olyan legfeljebb n -ed fokú polinom, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \dots, n$.

Bizonyítás

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

$$f(x) = \sum_{j=0}^n d_j l_j(x).$$

$l_j(c_i) = 0$, ha $i \neq j$, és $l_j(c_j) = 1$ -ből következik az állítás.

Mik lehetnek egy primitív egészegyütthatós polinom racionális gyökei?

Tétel

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ primitív polinom. Ha $f\left(\frac{p}{q}\right) = 0$, $p, q \in \mathbb{Z}$, $(p, q) = 1$, akkor $p|f_0$ és $q|f_n$.

Bizonyítás

$$0 = f\left(\frac{p}{q}\right) = f_n \left(\frac{p}{q}\right)^n + f_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + f_1 \left(\frac{p}{q}\right) + f_0 \quad / \cdot q^n$$

$$0 = f_n p^n + f_{n-1} q p^{n-1} + \dots + f_1 q^{n-1} p + f_0 q^n$$

$p|f_0 q^n$, mivel az összes többi tagnak osztója p , és így $(p, q) = 1$ miatt $p|f_0$.

$q|f_n p^n$, mivel az összes többi tagnak osztója q , és így $(p, q) = 1$ miatt $q|f_n$.

Bizonyítsd be, hogy $\sqrt{2} \notin \mathbb{Q}$!

Állítás

$\sqrt{2} \notin \mathbb{Q}$.

Bizonyítás

Tekintsük az $x^2 - 2 \in \mathbb{Z}[x]$ polinomot.

Ennek a $\frac{p}{q}$ alakú gyökeire $(p, q \in \mathbb{Z}, (p, q) = 1)$ teljesül, hogy $p|2$ és $q|1$, így a lehetséges racionális gyökei ± 1 és ± 2 .



10. Polinomok felbonthatósága

Hogyan jellemezhetőek test fölötti polinomgyűrűben az egységek?

Állítás

Legyen $(F; +, \cdot)$ test. Ekkor $f \in F[x]$ pontosan akkor egység, ha $\deg(f) = 0$.

Bizonyítás

\Leftarrow

Ha $\deg(f) = 0$, akkor f nem-nulla konstans polinom: $f(x) = f_0$. Mivel F test, ezért létezik $f_0^{-1} \in F$, amire $f_0 \cdot f_0^{-1} = 1$, így f tényleg egység.

\Rightarrow

Ha f egység, akkor létezik $g \in F[x]$, amire $f \cdot g = 1$, és így $\deg(f) + \deg(g) = \deg(1) = 0$ (Miért?), ami csak $\deg(f) = \deg(g) = 0$ esetén lehetséges.

Mit mondhatunk test fölötti elsőfokú polinomokról a gyökökkel kapcsolatban?

Állítás

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $\deg(f) = 1$, akkor f -nek van gyöke.

Bizonyítás

Ha $\deg(f) = 1$, akkor felírható $f(x) = f_1x + f_0$ alakban, ahol $f_1 \neq 0$. Azt szeretnénk, hogy létezzen $c \in F$, amire $f(c) = 0$, vagyis $f_1c + f_0 = 0$. Ekkor $f_1c = -f_0$ (Miért?), és mivel létezik $f_1^{-1} \in F$, amire $f_1 \cdot f_1^{-1} = 1$ (Miért?), ezért $c = -f_0 \cdot f_1^{-1} \left(= -\frac{f_0}{f_1} \right)$ gyök lesz.

Mit mondhatunk a lineáris polinomokról test fölötti polinomgyűrűben felbonthatóság szempontjából?

Állítás

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $\deg(f) = 1$, akkor f felbonthatatlan.

Bizonyítás

Legyen $f = g \cdot h$. Ekkor $\deg(g) + \deg(h) = \deg(f) = 1$ (Miért?) miatt $\deg(g) = 0 \wedge \deg(h) = 1$ vagy $\deg(g) = 1 \wedge \deg(h) = 0$. Előbbi esetben g , utóbbiban h egység a korábbi állítás értelmében.

Hogyan jellemezhetők a test fölötti másod-, illetve harmadfokú polinomok felbonthatóság szempontjából?

Állítás

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $2 \leq \deg(f) \leq 3$, akkor f pontosan akkor felbontható, ha van gyöke.

Bizonyítás

\Leftarrow

Ha c gyöke f -nek, akkor az $f(x) = (x - c)g(x)$ egy nemtriviális felbontás (Miért?).

\Rightarrow

Mivel $2 = 0 + 2 = 1 + 1$, illetve $3 = 0 + 3 = 1 + 2$, és más összegként nem állnak elő, ezért amennyiben f -nek van nemtriviális felbontása, akkor van elsőfokú osztója. A korábbi állítás alapján ennek van gyöke, és ez nyilván f gyöke is lesz.

Hogyan jellemezhetők a \mathbb{C} fölötti felbonthatatlan polinomok?

Tétel

$f \in \mathbb{C}[x]$ pontosan akkor felbonthatatlan, ha $\deg(f) = 1$.

Bizonyítás

←

Mivel \mathbb{C} a szokásos műveletekkel test, ezért korábbi állítás alapján teljesül.

⇒

Indirekt tfh. $\deg(f) \neq 1$. Ha $\deg(f) < 1$, akkor $f = 0$ vagy f egység, tehát nem felbonthatatlan, ellentmondásra jutottunk.

$\deg(f) > 1$ esetén az algebra alaptétele értelmében van gyöke f -nek. A gyöktényezőt kiemelve az $f(x) = (x - c)g(x)$ alakot kapjuk, ahol $\deg(g) \geq 1$ (Miért?), vagyis egy nemtriviális szorzat-előállítást, így f nem felbonthatatlan, ellentmondásra jutottunk.

Hogyan jellemezhetők az \mathbb{R} fölötti felbonthatatlan polinomok?

Tétel

$f \in \mathbb{R}[x]$ pontosan akkor felbonthatatlan, ha

- $\deg(f) = 1$, vagy
- $\deg(f) = 2$, és f -nek nincs (valós) gyöke.

Bizonyítás

←

Ha $\deg(f) = 1$, akkor korábbi állítás alapján f felbonthatatlan.

Ha $\deg(f) = 2$, és f -nek nincs gyöke, akkor f nem áll elő két elsőfokú polinom szorzataként (Miért?), vagyis csak olyan kéttényezős szorzat-előállítása lehet, melyben az egyik tényező foka 0, tehát egység.

⇒

Ha f felbonthatatlan, akkor nem lehet $\deg(f) < 1$. (Miért?)

Ha f felbonthatatlan, és $\deg(f) = 2$, akkor tfh. van gyöke. Ekkor az ehhez tartozó gyöktényező kiemelésével egy nemtriviális felbontását kapjuk f -nek (Miért?), ami ellentmondás.

Bizonyítsd be Gauss lemmáját!

Lemma (Gauss)

Ha $f, g \in \mathbb{Z}[x]$ primitív polinomok, akkor fg is primitív polinom.

Bizonyítás

Indirekt tfh. fg nem primitív polinom. Ekkor van olyan $p \in \mathbb{Z}$ prím, ami osztja fg minden együtthatóját. Legyen i , illetve j a legkisebb olyan index, amire $p \nmid f_i$, illetve $p \nmid g_j$ (Miért vannak ilyenek?). Ekkor fg -nek az $(i+j)$ indexű együtthatója $f_0g_{i+j} + \dots + f_i g_j + \dots + f_{i+j}g_0$, és ebben az összegben p nem osztója $f_i g_j$ -nek, de osztója az összes többi tagnak (Miért?), de akkor nem osztója az összegnek, ami ellentmondás.

Bizonyítsd be Gauss tételét egész együtthatós polinomokkal kapcsolatosan!

Tétel (Gauss tétele $\mathbb{Z}[x]$ -re)

Ha egy $f \in \mathbb{Z}[x]$ előállítható két nem konstans $g, h \in \mathbb{Q}[x]$ polinom szorzataként, akkor előállítható két nem konstans $g^*, h^* \in \mathbb{Z}[x]$ polinom szorzataként is.

Bizonyítás

Tfh. $f = gh$, ahol $g, h \in \mathbb{Q}[x]$ nem konstans polinomok. Legyen $f = df^*$, ahol $d \in \mathbb{Z}$, és $f^* \in \mathbb{Z}[x]$ primitív polinom, aminek a főegyütthatója pozitív. Ha felírjuk g -t ag^{**} , h -t pedig bh^{**} alakban, ahol $g^{**}, h^{**} \in \mathbb{Z}[x]$ primitív polinomok, amiknek a főegyütthatója pozitív, akkor azt kapjuk, hogy $df^* = f = gh = abg^{**} \cdot h^{**}$. Mivel Gauss lemmája szerint $g^{**} \cdot h^{**}$ is primitív polinom, továbbá f előállítása primitív polinom segítségével lényegében egyértelmű, ezért $f^* = g^{**}h^{**}$, és $d = ab$, vagyis $f = dg^{**}h^{**}$, és például $g^* = dg^{**}$, $h^* = h^{**}$ választással kapjuk f kívánt felbontását.

Bizonyítsd be a Schönemann-Eisenstein tételt egész együtthatós polinomokkal kapcsolatosan!

Tétel (Schönemann-Eisenstein)

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ legalább elsőfokú primitív polinom. Ha található olyan $p \in \mathbb{Z}$ prím, melyre

- $p \nmid f_n$,
- $p \mid f_j$, ha $0 \leq j < n$,
- $p^2 \nmid f_0$,

akkor f felbonthatatlan \mathbb{Z} fölött.

Bizonyítás

Tfh. $f = gh$. Mivel p nem osztja f főegyütthatóját, ezért sem a g , sem a h főegyütthatóját nem osztja (Miért?). Legyen m a legkisebb olyan index, amelyre $p \nmid g_m$, és o a legkisebb olyan index, amelyre $p \nmid h_o$. Ha $k = m + o$, akkor

$$p \nmid f_k = \sum_{i+j=k} g_i h_j,$$

mivel p osztja az összeg minden tagját, kivéve azt, amelyben $i = m$ és $j = o$.

Bizonyítás folyt.

Így $m + o = \deg(f)$, ahonnan $m = \deg(g)$ és $o = \deg(h)$. Viszont m és o nem lehet egyszerre pozitív, mert akkor $p^2 \mid f_0 = g_0 h_0$ teljesülne. Így az egyik polinom konstans, és ha nem lenne egység, akkor f nem lenne primitív.

11. Kódolás

Milyen felső korlát adható az entrópiára?

Tétel

Bármilyen eloszláshoz tartozó entrópiára

$$H_r(p_1, p_2, \dots, p_k) \leq \log_r k,$$

és egyenlőség pontosan akkor teljesül, ha $p_1 = p_2 = \dots = p_k = \frac{1}{k}$.

Bizonyítás

$r > 1$ esetén a $-\log_r(x)$ függvény szigorúan konvex, ezért használhatjuk a lemmát $q_j = \frac{1}{p_j}$ választással:

$$\begin{aligned} -H_r(p_1, p_2, \dots, p_k) &= \sum_{j=1}^k p_j \log_r p_j = \\ &= \sum_{j=1}^k p_j \left(-\log_r \frac{1}{p_j} \right) \geq -\log_r \left(\sum_{j=1}^k p_j \frac{1}{p_j} \right) = -\log_r k. \end{aligned}$$

Bizonyítsd be, hogy a prefix, az egyenletes, és a vesszős kódok is felbonthatóak!

Állítás

Prefix kód felbontható.

Bizonyítás

Konstruktív: nézzük az eddig beérkezett szimbólumokból összeálló szót. Amint ez kiadja a kódolandó ábécé valamely betűjének a kódját, azonnal dekódolhatunk a megfelelő betűre, mert a folytatásával kapott jelsorozat egyetlen betűnek sem lehet a kódja.

Állítás

Egyenletes kód prefix (így nyilván felbontható is).

Bizonyítás

Mivel a kódszavak hossza azonos, ezért csak úgy lehet egy kódszó prefixe egy másiknak, ha megegyeznek.

Állítás

Vesszős kód prefix (így nyilván felbontható is).

Bizonyítás

A vessző egyértelműen jelzi egy kódszó végét, hiszen ha folytatva kódszót kapnánk, abban a vessző tiltott módon szerepelne.

Mit mondhatunk optimális kód létezésével kapcsolatban?

Állítás

Adott ábécé és eloszlás esetén létezik optimális kód.

Bizonyítás

Válasszunk egy tetszőleges felbontható kódot (Miért van ilyen?), ennek átlagos szóhosszúsága legyen \bar{l} . Mivel $p_j l_j > \bar{l}$ esetén a kód nem lehet optimális (Miért?), ezért elég azokat a kódokat tekinteni, amelyekre $l_j \leq \frac{\bar{l}}{p_j}$, ha $j = 1, 2, \dots, n$. Ilyen kód csak véges sok van, így van köztük minimális átlagos hosszúságú.

Hogyan szól Shannon tétele zajmentes csatornára?

Tétel (Shannon tétele zajmentes csatornára)

Legyen $A = \{a_1, a_2, \dots, a_n\}$ a kódolandó ábécé, p_1, p_2, \dots, p_n a betűk eloszlása, $\varphi: A \rightarrow B^+$ injektív leképezés, B elemeinek a száma $r \geq 2$, továbbá $l_j = |\varphi(a_j)|$.

Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $H_r(p_1, p_2, \dots, p_n) \leq \bar{l}$.

Bizonyítás

$$\begin{aligned}\bar{l} - H_r(p_1, p_2, \dots, p_n) &= \sum_{j=1}^n p_j l_j + \sum_{j=1}^n p_j \log_r p_j = \\ &= - \sum_{j=1}^n p_j \log_r r^{-l_j} - \sum_{j=1}^n p_j \log_r \frac{1}{p_j} = - \sum_{j=1}^n p_j \log_r \frac{r^{-l_j}}{p_j} \geq \\ &\geq - \log_r \left(\sum_{j=1}^n r^{-l_j} \right) \geq - \log_r 1 = 0\end{aligned}$$

Mit mondhatunk Shannon-kód átlagos szóhosszáról?

Tétel (Shannon kód létezése)

Az előző tétel jelöléseivel, ha $n > 1$, akkor van olyan prefix kód, amire $\bar{l} < H_r(p_1, p_2, \dots, p_n) + 1$.

Bizonyítás

Válasszunk olyan l_1, l_2, \dots, l_n természetes számokat, amelyekre $r^{-l_j} \leq p_j < r^{-l_j+1}$, ha $j = 1, 2, \dots, n$ (Miért tudunk ilyeneket választani?). Ekkor $\sum_{j=1}^n r^{-l_j} \leq \sum_{j=1}^n p_j = 1$, így a McMillan-egyenlőtlenség megfordítása miatt létezik prefix kód az adott l_j hosszakkal. Mivel $l_j < 1 - \log_r p_j$ (Miért?), ezért

$$\bar{l} = \sum_{j=1}^n p_j l_j < \sum_{j=1}^n p_j (1 - \log_r p_j) = 1 + H_r(p_1, p_2, \dots, p_n).$$

12. Hibakorlátozó kódolás

Az ISBN kódolása milyen hibák esetén jelez?

Példa (ISBN (International Standard Book Number) kódolása)

Legyen d_1, d_2, \dots, d_n decimális számjegyek egy sorozata ($n \leq 10$). Egészítsük ki a sorozatot egy $n+1$ -edik számjeggyel, amelynek értéke

$$d_{n+1} = \sum_{j=1}^n j \cdot d_j \mod 11,$$

ha az nem 10, különben d_{n+1} legyen X.

Ha valamelyik számjegyet elírjuk, akkor az összefüggés nem teljesülhet: d_{n+1} elírása esetén ez nyilvánvaló, $j \leq n$ -re d_j helyett d'_j -t írva pedig az összeg $j(d'_j - d_j)$ -vel nőtt, ami nem lehet 11-gyel osztható (Miért?).

Azt is észrevevesszük, ha $j < n$ esetén d_j -t és d_{j+1} -et felcseréljük:

az összeg $j d_{j+1} + (j+1) d_j - j d_j - (j+1) d_{j+1} = d_j - d_{j+1}$ -gyel nő, ami csak akkor lehet 11-gyel osztható, ha $d_j = d_{j+1}$.

Példa

- ISBN - 1-hibajelző

Fogalmazd meg a Singleton-korlátra vonatkozó állítást!

Tétel (Singleton-korlát)

Ha $K \subset A^n$, $|A| = q$ és $d(K) = d$, akkor $|K| \leq q^{n-d+1}$.

Bizonyítás

Ha minden kódszóból elhagyunk $d - 1$ betűt (ugyanazokból a pozíciókból), akkor az így kapott szavak még mindig különbözőek, és $n - d + 1$ hosszúak. Az ilyen hosszú szavak száma szerepel az egyenlőtlenség jobb oldalán.

Fogalmazd meg a Hamming-korlátra vonatkozó állítást!

Tétel (Hamming-korlát)

Ha $K \subset A^n$, $|A| = q$ és K t -hibajavító, akkor

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

Bizonyítás

Mivel a kód t -hibajavító, ezért bármely két kódszóra a tőlük legfeljebb t távolságra lévő szavak halmazai diszjunktak (Miért?). Egy kódszótól pontosan j távolságra lévő szavak száma $\binom{n}{j} (q-1)^j$ (Miért?), így egy kódszótól legfeljebb t távolságra lévő szavak száma $\sum_{j=0}^t \binom{n}{j} (q-1)^j$. A jobb oldalon az n hosszú szavak száma szerepel (Miért?).

Mi a kapcsolat kód távolsága és hibajelző képessége között?

Tekintsünk egy kódot, aminek a távolsága d .

Ha egy elküldött kódszó legalább 1, de d -nél kevesebb helyen sérül, akkor az így kapott szó biztosan nem kódszó, mivel két kódszó legalább d helyen különbözik. Tehát legfeljebb $d - 1$ hiba esetén a kód jelez.

A kódban van két olyan kódszó, amelyek távolsága d , és ha az egyiket küldik, és ez úgy változik meg, hogy éppen a másik érkezik meg, akkor d hiba történt, de nem vesszük észre. Tehát van olyan d hiba, amit a kód nem tud jelezni.

Ezáltal a kód pontosan $d - 1$ -hibajelző.

Mi a kapcsolat kód távolsága és hibajavító képessége között?

Legyen a kód távolsága továbbra is d , és tegyük fel, hogy minimális távolságú dekódolást használunk.

$t < \frac{d}{2}$ hiba esetén biztosan jól javítunk, hiszen a háromszög-egyenlőtlenség miatt az eredetileg elküldött kódszótól különböző bármely kódszó biztosan $\frac{d}{2}$ -nél több helyen tér el a vett szótól (Miért?).

Másrészt legyenek u és w olyan kódszavak, amelyek távolsága d , és legyen v az a szó, amit úgy kapunk u -ból, hogy a d pozícióból $t \geq \frac{d}{2}$ helyre a w megfelelő pozíciójában lévő betűt írjuk.

Ekkor v az u -tól t helyen, míg w -tól $d - t \leq \frac{d}{2} \leq t$ helyen különbözik. Ha a kód t -hibajavító lenne, akkor v -t egyrészt u -ra, másrészt w -re kellene javítania.

Ezáltal a kód pontosan $\lfloor \frac{d-1}{2} \rfloor$ -hibajavító.

13. Lineáris kódolás

Bizonyítsd be, hogy F^n megfelelő műveletekkel lineáris teret alkot!

Mi az elégséges feltétele a kód linearitásának?

Definíció

Legyen F véges test. Ekkor az F elemeiből képzett rendezett n -esek a komponensenkénti összeadással, valamint az n -es minden elemének ugyanazzal az F -beli elemmel való szorzásával egy F feletti n -dimenziós F^n lineáris teret alkotnak. Ennek a térnek egy tetszőleges altere egy **lineáris kód**.

Megjegyzés

Itt F elemei a betűk, és F^n elemei a szavak, az alter elemei a kódszavak.

Milyen összefüggés van lineáris kód súlya és távolsága között?

Állítás

Ha K lineáris kód, akkor $d(K) = w(K)$.

Bizonyítás

$d(u, v) = w(u - v)$, és mivel K linearitása miatt $u, v \in K$ esetén $u - v \in K$, ezért a minimumok is megegyeznek (Miért?).

Mi a kapcsolat a generátormátrix és ellenőrző mátrix között?

Megjegyzés

A G mátrixhoz tartozó kódolásnak H pontosan akkor ellenőrző mátrixa, ha $\text{Ker}(H) = \text{Im}(G)$

Példa

1) A $(*)$ kód egy ellenőrző mátrixa:

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

Példa folyt.

2) A háromszori ismétlés kódjának egy ellenőrző mátrixa:

$$H = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

3) A paritásbites kód egy ellenőrző mátrixa:

$$H = (1 \ 1 \ \dots \ 1)$$

Mi a kapcsolat szisztematikus kód generátormátrixa és ellenőrző mátrixa között?

Állítás

Legyen $G \in \mathbb{F}_q^{n \times k}$ egy szisztematikus kód generátormátrixa:

$G = \begin{pmatrix} I_k \\ P \end{pmatrix}$. Ekkor $H = \begin{pmatrix} -P & I_{n-k} \end{pmatrix}$ ellenőrző mátrixa a kódnak.

Bizonyítás

$$\mathbf{H} \cdot \mathbf{G} = \begin{pmatrix} -\mathbf{P} & \mathbf{I}_{n-k} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{I}_k \\ \mathbf{P} \end{pmatrix} = -\mathbf{P} + \mathbf{P} = \mathbf{0} \in \mathbb{F}_q^{(n-k) \times k}$$

$$(\mathbf{H} \cdot \mathbf{G})_{ij} = \sum_{l=1}^k (-\mathbf{P})_{il} \cdot (\mathbf{I}_k)_{lj} + \sum_{l=1}^{n-k} (\mathbf{I}_{n-k})_{il} \cdot (\mathbf{P})_{lj} = -p_{ij} + p_{ij} = 0.$$

Tehát bármely u kódolandó szóra $\mathbf{H}(\mathbf{G}u) = (\mathbf{H}\mathbf{G})u = \mathbf{0}u = \mathbf{0}$,

vagyis $\text{Im}(\mathbf{G}) \subset \text{Ker}(\mathbf{H})$, amiből $\dim(\text{Im}(\mathbf{G})) \leq \dim(\text{Ker}(\mathbf{H}))$.

$\dim(\text{Im}(\mathbf{G})) = k$ és $\dim(\text{Ker}(\mathbf{H})) \leq k$ miatt viszont

$\dim(\text{Im}(\mathbf{G})) \geq \dim(\text{Ker}(\mathbf{H}))$ is teljesül, így $\text{Im}(\mathbf{G}) = \text{Ker}(\mathbf{H})$.

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

Állítás

Legyen \mathbf{H} egy $[n, k]$ kód ellenőrző mátrixa. A \mathbf{H} -nak pontosan akkor van l darab lineárisan összefüggő oszlopa, ha van olyan kódszó, aminek a súlya legfeljebb l .

Bizonyítás

Legyen $\mathbf{H} = \begin{pmatrix} \underline{h}_1 & \underline{h}_2 & \cdots & \underline{h}_n \end{pmatrix}$.

\Rightarrow

Ekkor $\sum_{j=1}^l u_j \cdot \underline{h}_{l_j} = \underline{0}$. Tekintsük azt a vektort, aminek az l_j -edik koordinátája u_j , a többi pedig 0 . Ez egyrészt kódszó lesz (Miért?), másrészt a súlya legfeljebb l .

\Leftarrow

Legyen $\underline{u} = (u_1, u_2, \dots, u_n)^T$ az a kódszó, aminek a súlya l . Ekkor \mathbf{H} -nak az \underline{u} nem-nulla koordinátáinak megfelelő oszlopai lineárisan összefüggők.

Bizonyítsd be, hogy a szindrómadekódolás megegyezik a minimális távolságú dekódolással, ha a hiba nem túl nagy!

Állítás

Legyen c a kódszó, $v = c + e$ a vett szó, ahol e a hiba, és $w(e) < d/2$. Ekkor a szindrómadekódolás a minimális távolságú dekódolásnak felel meg.

Bizonyítás

Egyrészt a korábbi állítás alapján $s = Hv = He$, másrészt e_s definíciója miatt $s = He_s$. Ezért e és e_s ugyanabban a mellékosztályban van, továbbá $w(e_s) \leq w(e)$.

$$w(e - e_s) \leq w(e) + w(-e_s) = w(e) + w(e_s) < d.$$

De $H(e - e_s) = 0$ miatt $e - e_s$ kódszó (Miért?), így $e = e_s$.

14. Polinomkódolás

Mit mondhatunk a lineáris ciklikus kódok és a polinomkódolás kapcsolatáról?

Tétel

Legyen K egy $[n, k]_q$ paraméterű lineáris ciklikus kód, és $g(x) \in K$ egy minimális fokszerű főpolinom. Ekkor

- 1) $g(x)$ egyértelmű, $\deg(g) = n - k$;
- 2) ha $f(x) \in \mathbb{F}_q[x]$, $\deg(f) < n$, akkor: $f(x) \in K \iff g(x) | f(x)$.

Bizonyítás

Legyen $h(x) \in K$ egy minimális fokú polinom:

$$h(x) = c_0 + c_1x + \dots + c_rx^r, \quad c_r \neq 0.$$

Mivel K lineáris, ezért $\frac{1}{c_r}h(x) \in K$ főpolinom.

Ha létezne $g_1(x), g_2(x) \in K$ minimális fokszerű (r) főpolinom, akkor $g_1(x) - g_2(x) \in K$ egy kisebb fokú polinom, ami ellentmondás, így $g(x) = \frac{1}{c_r}h(x)$.

Bizonyítás folyt.

Mivel K ciklikus, így $g(x), xg(x), \dots, x^{n-r-1}g(x) \in K$ (Miért?).

A linearitás miatt $\forall u_0, u_1, \dots, u_{n-r-1} \in \mathbb{F}_q$ -ra

$(u_0 + u_1x + \dots + u_{n-r-1}x^{n-r-1})g(x) = u(x)g(x) \in K$, így $g(x)$ legfeljebb n -ed fokú többszörösei kódszavak.

Legyen most $f(x) \in K$ tetszőleges. Kellene, hogy $g(x) | f(x)$.

Osszuk el maradékosan $f(x)$ -et $g(x)$ -szel:

$$f(x) = q(x)g(x) + r(x), \quad \deg(r(x)) < \deg(g(x)), \quad \deg(q(x)) \leq n - r - 1.$$

$$r(x) = f(x) - q(x)g(x) \in K \implies r(x) = 0 \quad (\text{Miért?})$$

Tehát minden kódszó előáll $(u_0 + u_1x + \dots + u_{n-r-1}x^{n-r-1})g(x)$ alakban. Ezek alapján $q^{n-r} = q^k$, és így $r = n - k$.

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

Tétel

Ha $g(x)$ egy $[n, k]_q$ paraméterű lineáris ciklikus kód generátorpolinomja, akkor $g(x) \mid x^n - 1$.

Bizonyítás

$x^{k-1}g(x) \in K$ főpolinom. Legyen $c_1(x) = x^k g(x) - (x^n - 1)$.

K ciklikussága miatt $c_1(x)$ is kódszó, és így:

$$g(x) \mid c_1(x) = x^k g(x) - (x^n - 1) \implies g(x) \mid x^n - 1.$$

Hogyan jellemezhetőek a kódszavak a paritásellenőrző polinom segítségével!

Tétel

Egy $c(x) \in \mathbb{F}_q[x]$ pontosan akkor kódszó, ha $c(x)h(x) \equiv 0 \pmod{x^n - 1}$ és $\deg(c(x)) < n$.

Bizonyítás

Az nyilvánvaló, hogy $\deg(c(x)) < n$.

\implies

$$c(x) \in K \Rightarrow c(x) = u(x)g(x) \Rightarrow c(x)h(x) = u(x)g(x)h(x) = u(x)(x^n - 1),$$

és így $c(x)h(x) \equiv 0 \pmod{x^n - 1}$.

\Longleftarrow

$$c(x)h(x) \equiv 0 \pmod{x^n - 1} \Rightarrow c(x)h(x) = a(x)(x^n - 1) \Rightarrow$$
$$\Rightarrow c(x) = a(x) \frac{x^n - 1}{h(x)} = a(x)g(x).$$