Diszkrét matematika 2.C szakirány

1. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼ nagy

Komputeralgebra Tanszék

2016. tavasz

Gráfok alapfogalmai

Definíció

A $G = (\varphi, E, V)$ hármast (irányítatlan) gráfnak nevezzük, ha E, V halmazok, $V \neq \emptyset$, $V \cap E = \emptyset$ és $\varphi \colon E \to \{\{v, v'\} \mid v, v' \in V\}$. E-t az élek halmazának, V-t a csúcsok (pontok) halmazának és φ-t az illeszkedési leképezésnek nevezzük. A φ leképezés E minden egyes eleméhez egy V-beli rendezetlen párt rendel.

Elnevezés

$v \in \varphi(e)$ esetén e illeszkedik v-re, illetve v végpontja e-nek.

Megjegyzés

Az illeszkedési leképezés meghatározza az $I \subset E \times V$ illeszkedési relációt: $(e, v) \in I \Leftrightarrow v \in \varphi(e)$.

Gráfok alapfogalmai

Definíció

Ha E és V is véges halmazok, akkor a gráfot véges gráfnak nevezzük, egyébként végtelen gráfnak.
$E = \emptyset$ esetén üres gráfról beszélünk.

Megjegyzés

Az informatikában elsősorban a véges gráfok játszanak szerepet, így a továbbiakban mi is véges gráfokkal foglalkozunk.

Definíció

Ha egy él egyetlen csúcsra illeszkedik, azt hurokélnek nevezzük.
Ha $e \neq e'$ esetén $\varphi(e) = \varphi(e')$, akkor e és e' párhuzamos élek.
Ha egy gráfban nincs sem hurokél, sem párhuzamos élek, akkor azt egyszerű gráfnak nevezzük.

Gráfok alapfogalmai

Definíció

Az $e \neq e'$ élek szomszédosak, ha van olyan $v \in V$, amelyre $v \in \varphi(e)$ és $v \in \varphi(e')$ egyszerre teljesül. A $v \neq v'$ csúcsok szomszédosak, ha van olyan $e \in E$, amelyre $v \in \varphi(e)$ és $v' \in \varphi(e)$ egyszerre teljesül.

Definíció

A v csúcs fokszámán (vagy fokán) a rá illeszkedő élek számát értjük, a hurokéleket kétszer számolva.
Jelölése: $d(v)$ vagy $deg(v)$.

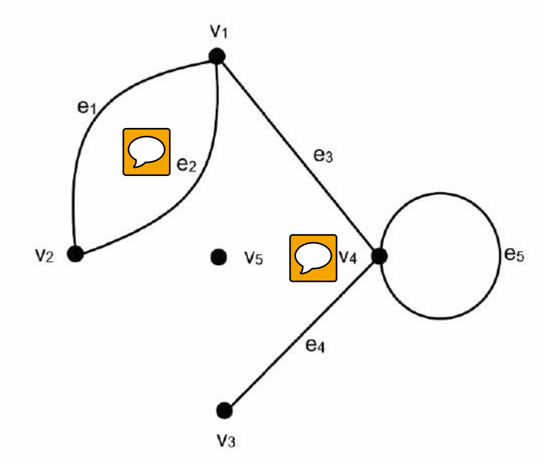
Definíció

Ha $d(v) = 0$, akkor v-t izolált csúcsnak nevezzük.

Definíció

Ha egy gráf minden csúcsának a foka n, akkor azt n-reguláris gráfnak hívjuk. Egy gráfot regulárisnak nevezünk, ha valamely n-re n-reguláris.

Példa



$V = \{v_1, v_2, v_3, v_4, v_5\}$
$E = \{e_1, e_2, e_3, e_4, e_5\}$
$\varphi = \{(e_1, \{v_1, v_2\}), (e_2, \{v_1, v_2\}), (e_3, \{v_1, v_4\}), (e_4, \{v_3, v_4\}), (e_5, \{v_4\})\}$

A fokszámösszeg

Állítás

A $G = (\varphi, E, V)$ gráfra

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

Bizonyítás

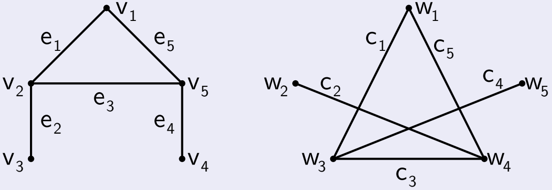
Élszám szerinti teljes indukció: $|E| = 0$ esetén mindkét oldal 0. Tfh. $|E| = n$ esetén igaz az állítás. Ha adott egy gráf, amelynek $n+1$ éle van, akkor annak egy élét elhagyva egy n élű gráfot kapunk. Erre teljesül az állítás az indukciós feltevés miatt. Az elhagyott élt újra hozzávéve a gráfhoz az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

Gráfok alapfogalmai

Definíció

A $G = (\varphi, E, V)$ és $G' = (\varphi', E', V')$ gráfok izomorfak, ha léteznek $f: E \to E'$ és $g: V \to V'$ bijektív leképezések, hogy minden $e \in E$-re és $v \in V$-re e pontosan akkor illeszkedik v-re, ha $f(e)$ illeszkedik $g(v)$-re.

Példa



Megfelelő f és g bijekciók:

$f = \{(e_1, c_5), (e_2, c_2), (e_3, c_3), (e_4, c_4), (e_5, c_1)\}$

$g = \{(v_1, w_1), (v_2, w_4), (v_3, w_2), (v_4, w_5), (v_5, w_3)\}$

Gráfok alapfogalmai

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

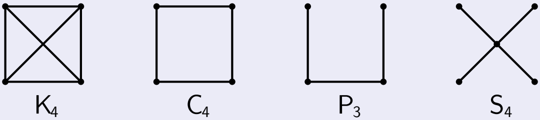
Az n csúcsú teljes gráfnak $\binom{n}{2} = n(n-1)/2$ éle van, és K_n-nel jelöljük.

További példák

Definíció

A C_n **ciklus** csúcsai egy szabályos n-szög csúcspontjai, és pontosan a szomszédos csúcspontoknak megfelelő csúcsok szomszédosak.
A P_n **ösvény** C_{n+1}-ből valamely él törlésével adódik.
Az S_n **csillagban** egy szabályos n-szög csúcspontjainak és középpontjának megfelelő csúcsok közül a középpontnak megfelelő csúcs szomszédos az összes többivel.

Példák



Gráfok alapfogalmai

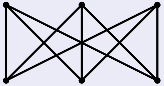
Definíció

A $G = (\varphi, E, V)$ gráfot páros gráfnak nevezzük, ha V-nek létezik V' és V'' diszjunkt halmazokra való felbontása úgy, hogy minden él egyik végpontja V'-nek, másik végpontja pedig V''-nek eleme.

Definíció

Azt az egyszerű páros gráfot, amelyben $|V'| = m$, $|V''| = n$ és minden V'-beli csúcs minden V''-beli csúccsal szomszédos, $K_{m,n}$-nel jelöljük.

Példa



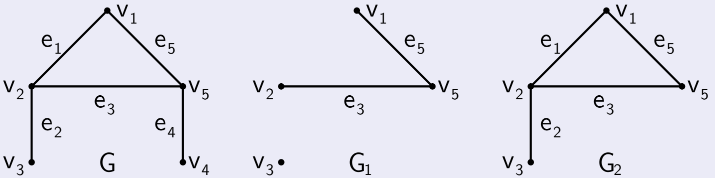
$K_{3,3}$

Gráfok alapfogalmai

Definíció

A $G' = (\varphi', E', V')$ gráfot a $G = (\varphi, E, V)$ gráf **részgráfjának** nevezzük, ha $E' \subset E$, $V' \subset V$ és $\varphi' \subset \varphi$. Ekkor G-t a G' **szupergráfjának** hívjuk. Ha a G' részgráf mindazokat az éleket tartalmazza, melyek végpontjai V'-ben vannak, akkor G'-t a V' által meghatározott **feszített (vagy telített) részgráf**nak nevezzük.

Példa



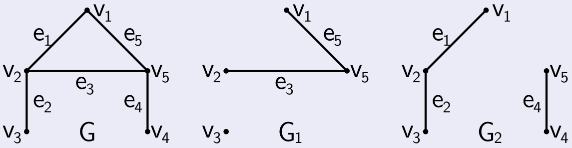
G-nek G_1 részgráfja, de nem feszített részgráfja, míg G_2 feszített részgráfja.

Gráfok alapfogalmai

Definíció

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

Példa



G_2 a G_1 gráf G-re vonatkozó komplementere.

Megjegyzés

Ha G' egyszerű gráf, és külön nem mondjuk, akkor a V'-beli csúcspontokkal rendelkező teljes gráfra vonatkozó komplementert értjük G' komplementere alatt.

Gráfok alapfogalmai

Definíció

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.

Definíció

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 $G' = (\varphi|_{E \setminus E'}, E \setminus E', V \setminus V')$ részgráfot értjük.

Gráfok alapfogalmai

Definíció

Legyen $G = (\varphi, E, V)$ egy gráf. A

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

sorozatot sétának nevezzük v_0-ból v_n-be, ha

- $v_j \in V \quad 0 \leq j \leq n$,
- $e_k \in E \quad 1 \leq k \leq n$,
- $\varphi(e_m) = \{v_{m-1}, v_m\} \quad 1 \leq m \leq n$.

A séta hossza a benne szereplő élek száma (n).
Ha $v_0 = v_n$, akkor zárt sétáról beszélünk, különben nyílt sétáról.

Definíció

Ha a sétában szereplő élek mind különbözőek, akkor vonalnak nevezzük.
Az előzőeknek megfelelően beszélhetünk zárt vagy nyílt vonalról.

Gráfok alapfogalmai

Definíció

Ha a sétában szereplő csúcsok mind különbözőek, akkor **útnak** nevezzük.

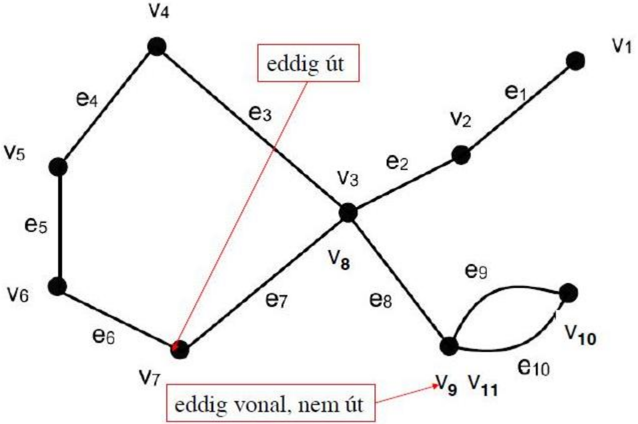
Megjegyzés

Egy út mindig vonal.
A nulla hosszú séták mind utak, és egyetlen csúcsból állnak.
Egy egy hosszú séta pontosan akkor út, ha a benne szereplő él nem hurokél.

Definíció

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

Példa



út: $v_1, e_1, v_2, e_2, v_3, \ldots, v_6, e_6, v_7$;
vonal, de nem út: $v_1, e_1, v_2, e_2, v_3, \ldots, v_8, e_8, v_9$;
kör: $v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_8 (= v_3)$.

Gráfok alapfogalmai

Állítás

Egy G gráfban a különböző v és v' csúcsokat összekötő sétából alkalmasan törölve éleket és csúcsokat a v-t v'-vel összekötő utat kapunk.

Bizonyítás

A 2. előadáson...

Gráfok alapfogalmai

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.

Megjegyzés

Bármely él két végpontja azonos osztályba tartozik (Miért?), így a gráf minden éle hozzátartozik egy komponenshez.

Megjegyzés

Egy gráf akkor és csak akkor összefüggő, ha minden csúcs ugyanabba az osztályba tartozik, azaz ha csak egyetlen komponense van.

Gráfok alapfogalmai

Definíció

Egy gráfot fának nevezünk, ha összefüggő és körmentes.

Diszkrét matematika 2.C szakirány

2. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. tavasz

Gráfok alapfogalmai

Állítás

Egy G gráfban a különböző v és v' csúcsokat összekötő sétából alkalmasan törölve éleket és csúcsokat a v-t v'-vel összekötő utat kapunk.

Bizonyítás

Legyen az állításban szereplő séta a következő:

$$v = v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n = v'.$$

Ha valamely $i < j$ esetén $v_i = v_j$, akkor töröljük az

$$e_{i+1}, v_{i+1}, e_{i+2}, v_{i+2}, \ldots, v_{j-1}, e_j, v_j$$

részt, és ismételjük ezt, amíg van csúcsismétlődés. Ha már nincs, akkor utat kaptunk, és mivel minden lépésben csökken a séta hossza, ezért az eljárás véges sok lépésben véget ér.

Fák

Definíció

Egy gráfot fának nevezünk, ha összefüggő és körmentes.

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

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

Fák

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

(2) $\Rightarrow$ (3)

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

Tfh. 2 út is létezik a különböző v és v' csúcsok között, legyenek ezek: $v, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v'$ és $v, e'_1, v'_1, e'_2, \ldots, v'_{m-1}, e'_m, v'$. 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 $v_{k-1}, e'_k, v'_k, \ldots, e'_m, v', e_n, v_{n-1}, e_{n-1}, v_{n-2}, \ldots, v_{k+1}, e_{k+1}, v_k$ sétával.

Fák

Bizonyítás

(3) $\Rightarrow$ (4)

Annak a bizonyítása, hogy nincs kör a gráfban indirekt:
tfh. létezik kör: $v, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v$. Ekkor v_1 és v között két különböző út is van: $v_1, e_2, \ldots, v_{n-1}, e_n, v$ 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:
$v, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v', e, v$.

(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?):
$v', e, v, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v'$. Ekkor $v, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v'$ út lesz v és v' között.

Fák

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: $v_0, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v_n$. 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 $v', e, v_0, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v_n$ út hossza nagyobb lenne, mint a maximális út hossza. Ha viszont e másik végpontja az út valamely v_k csúcsa, akkor $v_k, e, v_0, e_1, v_1, e_2, \ldots, v_{k-1}, e_k, v_k$ kör lenne, ami szintén ellentmondás.

Fák

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.

Fák

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.

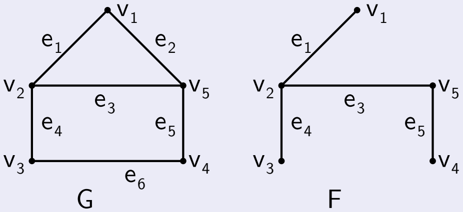
(3) $\Rightarrow$ (1): Ha a feltételnek eleget tevő gráfban van kör, akkor az abban szereplő tetszőleges él elhagyásával összefüggő gráfot kapunk. (Miért?) Folytassuk az élek törlését, amíg már nincs több kör a kapott gráfban, tehát fa lesz. Ha k élt hagytunk el, akkor a kapott gráfnak $n-1-k$ éle van,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

Feszítőfa

Definíció

A G gráf egy F részgráfját a feszítőfájának nevezzük, ha a csúcsainak halmaza megegyezik G csúcsainak halmazával, és fa.

Példa



Feszítőfa

Állítás

Minden összefüggő véges gráfnak létezik feszítőfája.

Bizonyítás

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

Feszítőfa

Állítás

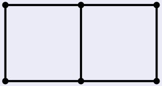
Egy $G = (\varphi, E, V)$ összefüggő véges gráfban létezik legalább $|E| - |V| + 1$ kör, amelyek élhalmaza különböző.

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.

Megjegyzés

Előfordulhat, hogy a becslés nem pontos ($3 > 7 - 6 + 1 = 2$).



Feszítőfa

Definíció

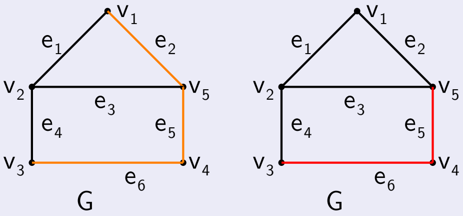
Legyen $G = (\varphi, E, V)$, $v, v' \in V$ és $E' \subset E$. Azt mondjuk, hogy E' elvágja a v és v' csúcsokat, ha minden v-ből v'-be menő út tartalmaz E'-beli élet.
Ha léteznek olyan csúcsok, amelyeket E' elvág, akkor E'-t elvágó élhalmaznak nevezzük.

Definíció

Ha egy elvágó élhalmaznak nincs olyan valódi részhalmaza, amely maga is elvágó élhalmaz, akkor vágásnak nevezzük.

Feszítőfa

Példa



$\{e_2, e_5, e_6\}$ elvágó élhalmaz, mert elvágja v_4-et és v_2-t, hiszen mindhárom v_4 kezdőpontú és v_2 végpontú útban van olyan él, ami eleme:

v_4, e_6, v_3, e_4, v_2,

v_4, e_5, v_5, e_3, v_2,

$v_4, e_5, v_5, e_2, v_1, e_1, v_2$.

Ugyanakkor nem vágás, mert $\{e_5, e_6\}$ olyan valódi részhalmaza, ami szintén elvágó.

Utóbbi vágás, hiszen sem $\{e_5\}$, sem $\{e_6\}$, sem $\emptyset$ nem elvágó élhalmaz.

Feszítőfa

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.

Megjegyzés

Ebben az esetben is előfordulhat, hogy a becslés nem pontos.

Erdő, feszítőerdő

Definíció

Egy körmentes gráfot **erdőnek** nevezünk.
Egy gráfnak olyan részgráfját, ami minden komponensből egy feszítőfát tartalmaz, **feszítőerdőnek** nevezzük.

Állítás

Tetszőleges gráfnak létezik feszítőerdeje.

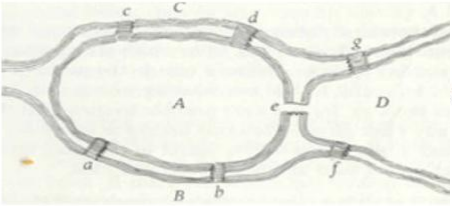
Állítás

Egy véges erdő éleinek száma a csúcsainak és komponenseinek számának különbsége.

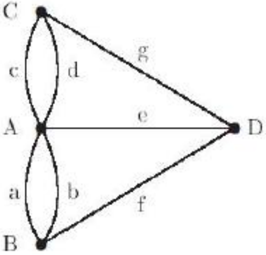
Megjegyzés

A nem összefüggő gráfoknál az erdők, illetve feszítőerdők azt a szerepet töltik be, mint összefüggő gráfok esetén a fák, illetve feszítőfák.

Euler-vonal



G:



Definíció

Egy gráfban az olyan vonalat, amelyben a gráf minden éle szerepel, **Euler-vonalnak** nevezzük.

Megjegyzés

Mivel vonalban nincs élismétlődés, ezért egy Euler-vonal a gráf minden élét pontosan egyszer tartalmazza.

Euler-vonal

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:
$v_0, e_1, v_1, e_2, \ldots, v_{n-1}, e_n, v_0$.
A vonal kezdő- és végpontját leszámítva egy csúcs minden előfordulása esetén a mellette lévő két különböző él 2-vel járul hozzá a fokszámához. A kezdő- és végpont ugyanaz, ezért ennek is páros lesz a foka.

Euler-vonal

Bizonyítás

$\Leftarrow$: a bizonyítás konstruktív. Induljunk ki egy élt nem tartalmazó zárt vonalból (v). Ha az eddig kapott 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.

Hamilton-út/kör

Definíció

Egy gráfban az olyan utat, amelyben a gráf minden csúcsa szerepel, Hamilton-útnak nevezzük.
Egy gráfban az olyan kört, amelyben a gráf minden csúcsa szerepel, Hamilton-körnek nevezzük.

Megjegyzés

Mivel útban nincs csúcsismétlődés, ezért egy Hamilton-út a gráf minden csúcsát pontosan egyszer tartalmazza.

Tétel (Dirac)

Ha a $G = (\varphi, E, V)$ gráfra $|V| > 2$, és minden csúcsának a foka legalább $|V|/2$, akkor van Hamilton-köre.

Bizonyítás

NB.

Diszkrét matematika 2.C szakirány

3. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. tavasz

Címkézett gráfok

Definíció

Legyen $G = (\varphi, E, V)$ egy gráf, C_e és C_v halmazok az élcímkék, illetve csúcscímkék halmaza, továbbá $c_e : E \to C_e$ és $c_v : V \to C_v$ leképezések az élcímkézés, illetve csúcscímkézés. Ekkor a $(\varphi, E, V, c_e, C_e, c_v, C_v)$ hetest címkézett gráfnak nevezzük.

Definíció

Élcímkézett, illetve csúcscímkézett gráfról beszélünk, ha csak élcímkék és élcímkézés, illetve csak csúcscímkék és csúcscímkézés adott.

Megjegyzés

Címkézett gráf helyett a színezett gráf elnevezés is használatos.

Címkézett gráfok

Definíció

$C_e = \mathbb{R}$, illetve $C_v = \mathbb{R}$ esetén élsúlyozásról és élsúlyozott gráfról, illetve csúcssúlyozásról és csúcssúlyozott gráfról beszélünk, és a jelölésből C_e-t, illetve C_v-t elhagyjuk.

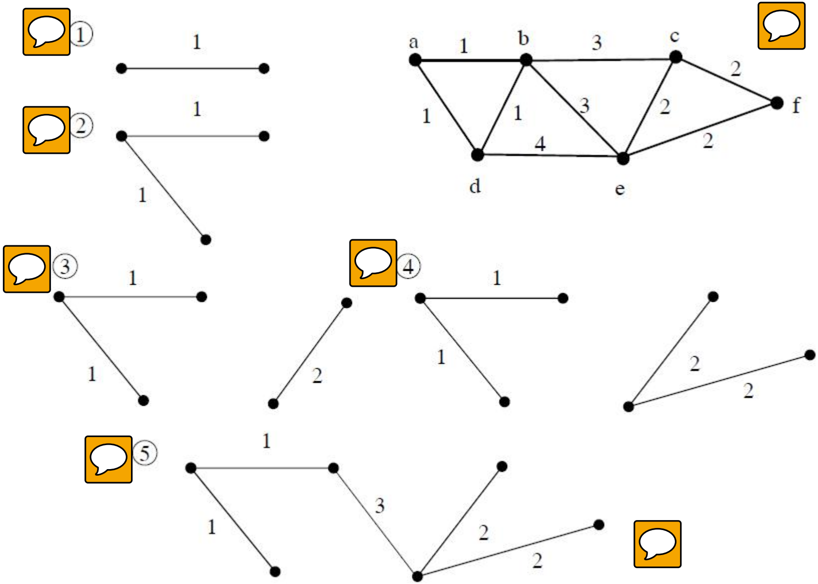
Definíció

Egy $G = (\varphi, E, V, w)$ élsúlyozott gráfban az $E' \subset E$ élhalmaz súlya $\sum_{e \in E'} w(e)$.

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.

Példa



Címkézett gráfok

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 feszítőfája a gráfnak. Ha több ilyen van, akkor F' legyen az a minimális súlyú, 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?).

Címkézett gráfok

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.

Definíció

Egy algoritmust **mohó algoritmusnak** nevezünk, ha minden lépésben az adódó lehetőségek közül az adott lépésben legkedvezőbbek egyikét választja.

Megjegyzés

A Kruskal-algoritmus egy mohó algoritmus.

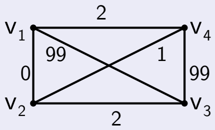
Címkézett gráfok

Megjegyzés

A mohó algoritmus nem mindig optimális.

Példa

Keressünk minimális összsúlyú Hamilton-kört a következő gráfban.



Irányított gráfok

Definíció

A $G = (\psi, E, V)$ hármast **irányított gráfnak** nevezzük, ha E, V halmazok, $V \neq \emptyset$, $V \cap E = \emptyset$ és $\psi \colon E \to V \times V$.
E-t az **élek halmazának**, V-t a **csúcsok (pontok) halmazának** és ψ-t az **illeszkedési leképezésnek** nevezzük. A ψ leképezés E minden egyes eleméhez egy V-beli rendezett párt rendel.

Elnevezés

$\psi(e) = (v, v')$ esetén azt mondjuk, hogy v **kezdőpontja**, v' pedig **végpontja** e-nek.

Definíció

Bármely $G = (\psi, E, V)$ irányított gráfból kapható egy $G' = (\varphi, E, V)$ irányítatlan gráf úgy, hogy $\psi(e) = (v, v')$ esetén $\varphi(e)$-t $\{v, v'\}$-nek definiáljuk.
Ekkor azt mondjuk, hogy G a G' egy **irányítása**.

Irányított gráfok

Megjegyzés

Az irányítatlan gráfokra definiált fogalmakat használni fogjuk irányított gráfok esetén is, mégpedig a megfelelő irányítatlan gráfra értve.

Definíció

Ha $e \neq e'$ esetén $\psi(e) = \psi(e')$, akkor e és e' szigorúan párhuzamos élek.

Definíció

Azon élek számát, amiknek a v csúcs kezdőpontja, v kifokának nevezzük, és $deg^+(v)$-vel vagy $d^+(v)$-vel jelöljük.
Azon élek számát, amiknek a v csúcs végpontja, v befokának nevezzük, és $deg^-(v)$-vel vagy $d^-(v)$-vel jelöljük.
Ha egy csúcs kifoka 0, akkor nyelőnek, ha a befoka 0, akkor forrásnak nevezzük.

Irányított gráfok

Állítás

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

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

Definíció

A $G = (\psi, E, V)$ és $G' = (\psi', E', V')$ irányított gráfok izomorfak, ha léteznek $f : E \to E'$ és $g : V \to V'$ bijektív leképezések, hogy minden $e \in E$-re és $v \in V$-re v pontosan akkor kezdőpontja e-nek, ha $g(v)$ kezdőpontja $f(e)$-nek, és v pontosan akkor végpontja e-nek, ha $g(v)$ végpontja $f(e)$-nek.

Irányított gráfok

Definíció

A $G' = (\psi', E', V')$ irányított gráfot a $G = (\psi, E, V)$ irányított gráf **irányított részgráfjának** nevezzük, ha $E' \subset E$, $V' \subset V$ és $\psi' \subset \psi$. Ekkor G-t a G' **irányított szupergráfjának** hívjuk.
Ha a G' irányított részgráf mindazokat az éleket tartalmazza, melyek kezdőpontjai és végpontjai V'-ben vannak, akkor G'-t a V' által meghatározott **feszített irányított** (vagy **telített irányított**) **részgráfnak** nevezzük.

Definíció

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.

Irányított gráfok

Definíció

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.

Definíció

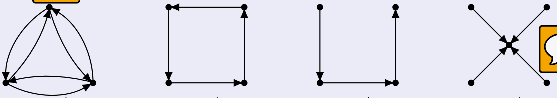
Ha $G = (\psi, E, V)$ egy irányított gráf, és $V' \subset V$, akkor legyen E' az összes olyan élek halmaza, amelyeknek kezdőpontja vagy végpontja valamely V'-beli csúcs. A G-ből a V' csúcshalmaz törlésével kapott irányított gráfon a $G' = (\psi|_{E \setminus E'}, E \setminus E', V \setminus V')$ irányított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

Irányított gráfok

Definíció

A $\overrightarrow{C_n}$ irányított ciklus a C_n ciklus olyan irányítása, melyben az élek irányítása azonos (minden csúcs befoka és kifoka is 1).
A $\overrightarrow{P_n}$ irányított ösvény $\overrightarrow{C_{n+1}}$-ból valamely él törlésével adódik.
Az $\overrightarrow{S_n}$ irányított csillag az S_n csillag olyan irányítása, melyben a középső csúcs nyelő, az összes többi pedig forrás.
Adott csúcshalmaznál az irányított teljes gráfban tetszőleges v és v' különböző csúcsokhoz található pontosan egy olyan él, aminek v a kezdőpontja és v' a végpontja. $\overrightarrow{K_n}$ nem K_n irányítása, sőt nem is egyszerű gráf, ha $n > 1$.

Példák



$\overrightarrow{K_3}$ $\overrightarrow{C_4}$ $\overrightarrow{P_3}$ $\overrightarrow{S_4}$

Irányított gráfok

Definíció

Legyen $G = (\psi, E, V)$ egy irányított gráf. A

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

sorozatot irányított sétának nevezzük v_0-ból v_n-be, ha

- $v_j \in V \quad 0 \leq j \leq n$,
- $e_k \in E \quad 1 \leq k \leq n$,
- $\psi(e_m) = (v_{m-1}, v_m) \quad 1 \leq m \leq n$.

Ha $v_0 = v_n$, akkor zárt irányított sétáról beszélünk, különben nyílt irányított sétáról.

Definíció

Ha az irányított sétában szereplő élek mind különbözőek, akkor irányított vonalnak nevezzük.
Az előzőeknek megfelelően beszélhetünk zárt vagy nyílt irányított vonalról.

Irányított gráfok

Definíció

Ha az irányított sétában szereplő csúcsok mind különbözőek, akkor irányított útnak nevezzük.

Definíció

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

Definíció

Egy irányított gráfot erősen összefüggőnek nevezünk, ha bármely csúcsából bármely csúcsába vezet irányított út.

Irányított gráfok

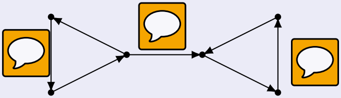
A $G = (\psi, E, V)$ irányított gráf esetén V elemeire vezessük be a $\sim$ relációt: $v \sim v'$ pontosan akkor, ha G-ben vezet irányított út v-ből v'-be, és v'-ből is vezet irányított út v-be.

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.

Megjegyzés

Az irányítatlan gráfokkal ellentétben nem feltétlenül tartozik az irányított gráf minden éle valamely erős komponenshez.



Megjegyzés

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

Irányított gráfok

Definíció

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

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.

Irányított gráfok

Definíció

A gyökérből egy adott csúcsba vezető út hosszát a csúcs szintjének hívjuk.
A csúcsok szintjeinek maximumát az irányított fa magasságának nevezzük.

Definíció

$\psi(e) = (v, v')$ esetén azt mondjuk, hogy v' a v gyereke, illetve v a v' szülője.
Ha két csúcsnak ugyanaz a szülője, akkor testvéreknek hívjuk őket.

Definíció

Bármely v csúcsra tekinthetjük azon csúcsok halmazát, amelyekhez vezet irányított út v-ből. Ezen csúcsok által meghatározott feszített irányított részgráfot (amely irányított fa, és v a gyökere) v-ben gyökerező irányított részfának nevezzük.

Irányított gráfok

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 $f(s) = 0$; minden más v csúcsra legyen $f(v) = \infty$

(2) Ha $T \subset S$ vagy $H = \emptyset$, akkor az algoritmus véget ér.

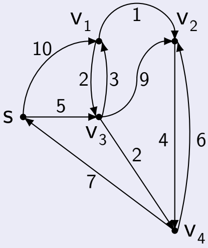
(3) Legyen $t \in H$ egy olyan csúcs, amelyre $f(t)$ minimális. Tegyük át t-t S-be, és minden e élre, amely t-ből $v \in V \setminus S$-be vezet, ha $f(t) + w(e) < f(v)$, akkor legyen $f(v) = f(t) + w(e)$, és ha $v \notin H$, tegyük át v-t H-ba. Menjünk (2)-re.

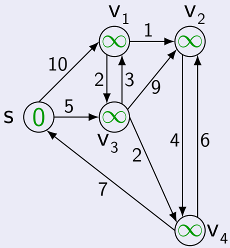
Tétel

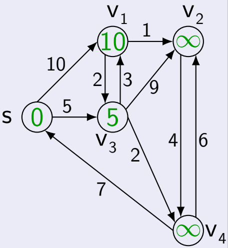
A Dijkstra-algoritmus a csúcshalmazon értelmez egy $f : V \to \overline{\mathbb{R}}$ függvényt, amely $t \in T$ esetén az adott s csúcsból a t csúcsba vezető irányított séták súlyainak a minimuma (∞, ha nincs ilyen séta).

Irányított gráfok

Példa



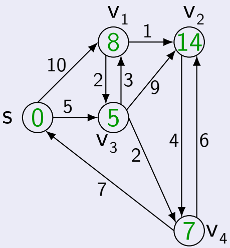




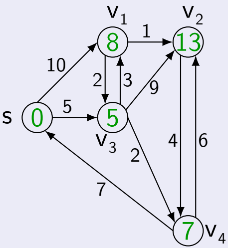
$S = \emptyset, H = \{s\}$ $\qquad$ $S = \{s\}, H = \{v_1, v_3\}$

Irányított gráfok

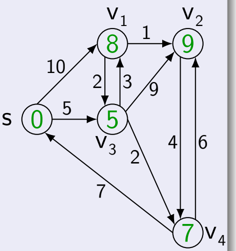
Példa



$S = \{s, v_3\}$
$H = \{v_1, v_2, v_4\}$



$S = \{s, v_3, v_4\}$
$H = \{v_1, v_2\}$



$S = \{s, v_3, v_4, v_1\}$
$H = \{v_2\}$

Diszkrét matematika 2.C szakirány

4. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. tavasz

Irányított gráfok

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 $f(s) = 0$; minden más v csúcsra legyen $f(v) = \infty$.

(2) Ha $T \subset S$ vagy $H = \emptyset$, akkor az algoritmus véget ér.

(3) Legyen $t \in H$ egy olyan csúcs, amelyre $f(t)$ minimális. Tegyük át t-t S-be, és minden e élre, amely t-ből $v \in V \setminus S$-be vezet, ha $f(t) + w(e) < f(v)$, akkor legyen $f(v) = f(t) + w(e)$, és ha $v \notin H$, tegyük át v-t H-ba. Menjünk (2)-re.

Tétel

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

Irányított gráfok

Bizonyítás

Az S elemszáma szerinti indukcióval megmutatjuk, hogy:

1. minden $t \in S$-re $f(t)$ az s csúcsból a t csúcsba vezető irányított séták súlyainak minimuma;
2. 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 $f(v)$.

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 $f(t') \leq W'$, és mivel t-t választottuk $f(t) \leq f(t')$, így $f(t) \leq W$, amivel az állítás első részét beláttuk.

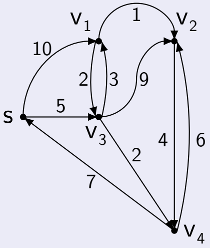
Irányított gráfok

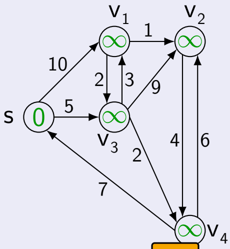
Biz.folyt.

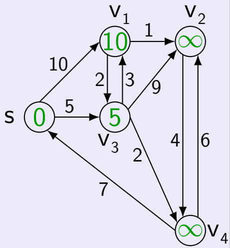
Miután (3)-ban az $f(v)$ értékeket megváltoztattuk, tekintsünk egy s-ből v-be vezető sétát, aminek csak az utolsó csúcsa nincs S-ben, legyen t' az utolsó előtti csúcsa, e pedig az utolsó éle. Mivel $t' \in S$, az s-től t'-ig vezető részséta súlya legalább $f(t')$, így a teljes séta súlya legalább $f(t')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

Irányított gráfok

Példa



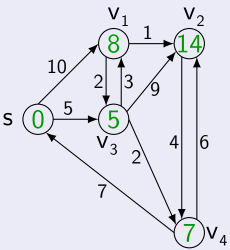




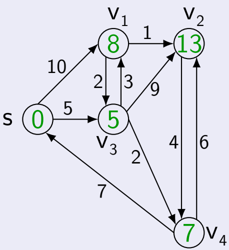
$S = \emptyset, H = \{s\}$ $S = \{s\}, H = \{v_1, v_3\}$

Irányított gráfok

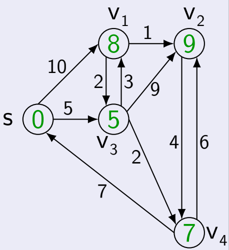
Példa



$S = \{s, v_3\}$
$H = \{v_1, v_2, v_4\}$



$S = \{s, v_3, v_4\}$
$H = \{v_1, v_2\}$



$S = \{s, v_3, v_4, v_1\}$
$H = \{v_2\}$

Síkgráfok

Definíció

Egy G gráfot **síkgráfnak** nevezünk, ha az felrajzolható a síkra anélkül, hogy az éleinek a csúcspontokon kívül lennének közös pontjai. Egy ilyen felrajzolását a G gráf **síkbeli reprezentációjának** is nevezzük.

Megjegyzés

Nem minden gráf ilyen, ellenben minden gráf $\mathbb{R}^3$-ben lerajzolható.

Definíció

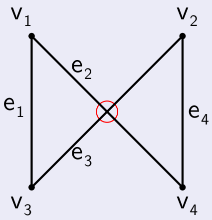
A G gráf egy síkbeli reprezentációja esetén **tartománynak** nevezzük az élek által határolt síkidomot. Ez nem feltétlenül korlátos, ilyenkor külső tartományról beszélünk, egyébként pedig belső tartományról.

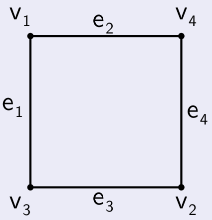
Megjegyzés

Egy belső tartomány valamely másik reprezentációban lehet külső tartomány is, de a tartományok száma nem függ a reprezentációtól.

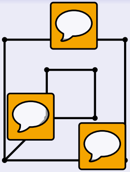
Síkgráfok

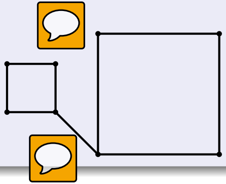
Példa





Példa





Síkgráfok

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, aminek 1 tartománya van, így teljesül rá az összefüggés (Miért?).

Síkgráfok

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.

Megjegyzés

A becslés nem összefüggő síkgráfok esetén is teljesül, hiszen élek hozzávételével összefüggő síkgráfot kaphatunk.

Síkgráfok

Állítás

Ha $G = (\varphi, E, V)$ egyszerű 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.

Síkgráfok

Állítás

$K_{3,3}$ nem síkgráf.

Bizonyítás

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

Állítás

K_5 nem síkgráf.

Bizonyítás

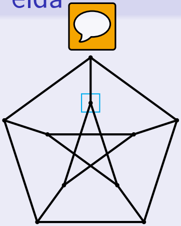
Indirekt tfh. K_5 síkgráf. $|E| = 10$ és $|V| = 5$, így az élszámra vonatkozó becslés alapján $10 \leq 3 \cdot 5 - 6 = 9$, ami ellentmondás.

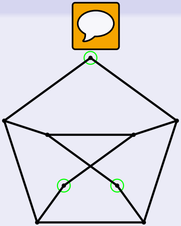
Síkgráfok

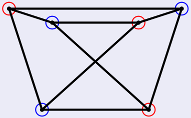
Definíció

A G és G' gráfokat topologikusan izomorfnak nevezzük, ha az alábbi lépést, illetve a fordítottját alkalmazva, véges sok lépésben az egyikből a másikkal izomorf gráfot kaphatunk: egy másodfokú csúcsot törlünk, és a szomszédjait összekötjük egy éllel.

Példa







Tétel (Kuratowski) (NB)

Egy egyszerű gráf pontosan akkor síkgráf, ha nincs olyan részgráfja, ami topologikusan izomorf K_5-tel vagy $K_{3,3}$-mal.

Gráfok színezése

Szeretnénk egy térképet kiszínezni úgy, hogy a szomszédos régiók különböző színűek legyenek.
A probléma megközelítése gráfokkal: a régióknak felelnek meg a csúcsok.
Két csúcs szomszédos, ha a megfelelő régióknak van közös határvonala.
A térképnek megfelelő gráf síkgráf lesz.

Tétel (Négyszíntétel) (NB)

Minden síkgráf 4 színnel színezhető.

Megjegyzés

1976-ban bizonyította Appel és Haken. Ez volt az első nevezetes sejtés, aminek a bizonyításához számítógépet is használtak. 1936 lehetséges ellenpéldát ellenőriztek, 1200 órán keresztül futott a program.

Gráfok színezése

Definíció

Egy gráf egy csúcsszínezését jólszínezésnek nevezzük, ha a szomszédos csúcsok színe különböző.

Definíció

Egy gráf kromatikus száma az a legkisebb n természetes szám, amelyre jólszínezhető n színnel.

Megjegyzés

A kromatikus szám pontosan akkor 1, ha nincs éle a gráfnak, és ha 2 a kromatikus szám, akkor a gráf páros. A síkgráfok kromatikus száma legfeljebb 4.

Gráfok mátrixai

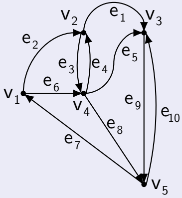
Definíció

Ha egy $G = (\psi, E, V)$ irányított gráf élei $e_1, e_2, \ldots, e_n$, csúcsai pedig $v_1, v_2, \ldots, v_m$, akkor az alábbi illeszkedési mátrix (vagy élmátrix) egyértelműen megadja a gráfot:

$$a_{ij} = \begin{cases} 1 & \text{, ha } e_j\text{-nek } v_i \text{ kezdőpontja;} \\ -1 & \text{, ha } e_j \text{ nem hurokél, és } v_i \text{ a végpontja;} \\ 0 & \text{, egyébként.} \end{cases}$$

A megfelelő irányítatlan gráf élmátrixa az $|a_{ij}|$ elemekből áll.

Példa



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

Gráfok mátrixai

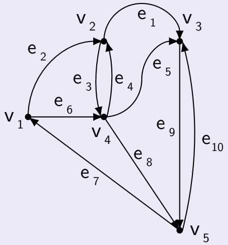
Definíció

A G irányított gráf csúcsmátrixában legyen b_{ij} a v_i kezdőpontú és v_j végpontú élek száma.

A megfelelő irányítatlan gráf csúcsmátrixának elemeire:

$$b_{ij} = \begin{cases} \text{a } v_i\text{-re illeszkedő hurokélek száma} & \text{, ha } i = j; \\ \text{a } v_i\text{-re és } v_j\text{-re is illeszkedő élek száma} & \text{, egyébként.} \end{cases}$$

Példa



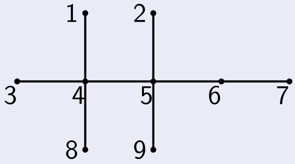
$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Prüfer-kód

Definíció

Legyen adott egy $F = (\varphi, E, V, w)$ csúcscímkézett fa, az egyes csúcsok címkéi 1 és n közötti különböző egész számok, ahol $n = |V|$. Töröljük az elsőfokú csúcsok közül a legkisebb sorszámút, és írjuk fel ennek szomszédjának a számát. A kapott fára (Miért fa?) folytassuk az eljárást, amíg már csak egy csúcs marad, mégpedig az n címkéjű (Miért?). A sorozat $n-1$-edig tagja szükségképpen n, ezért ez elhagyható.
A kapott $n-2$ hosszú sorozat az F fa **Prüfer-kódja**.

Példa



A Prüfer-kód: 4546545(9).

Prüfer-kód

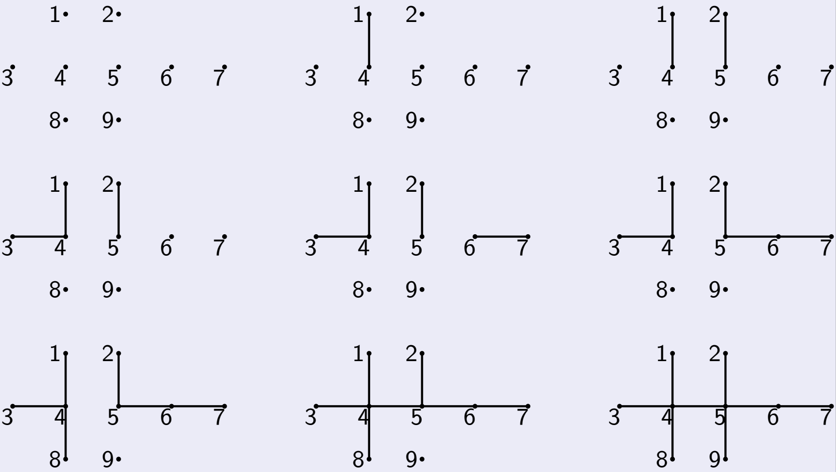
Algoritmus (Prüfer-kódból fa készítése)

Legyen a Prüfer-kód $p_1, p_2, \dots, p_{n-2}, p_{n-1} = n$. Legyen a kódban nem szereplő legkisebb sorszám s_1. Ha s_i-t már meghatároztuk, akkor legyen s_{i+1} az a legkisebb sorszám, amely különbözik az alábbiaktól: $s_1, s_2, \dots, s_i; p_{i+1}, p_{i+2}, \dots, p_{n-2}, p_{n-1} = n$. Ilyennek mindig lennie kell, mert n lehetőségből legfeljebb $n-1$ számút nem engedünk meg. Az n csúcsot tartalmazó üres gráfból kiindulva minden i-re $(1 \leq i \leq n-1)$ megrajzoljuk az s_i és p_i csúcsokra illeszkedő élt.

Prüfer-kód

45465459 1;5465459 12;465459 123;65459 1237;5459 12376;459 123768;59 1237684;9

Példa



Műveletek

Definíció

Egy X halmazon értelmezett művelet alatt egy $*: X^n \to X$ függvényt értünk.
Egy X halmazon értelmezett binér (kétváltozós) művelet egy $*: X \times X \to X$ függvény. Gyakran $*(x, y)$ helyett $x * y$-t írunk.

Példa

- $\mathbb{C}$ halmazon az $+$, $\cdot$ binér művelet.
- $\mathbb{C}$ halmazon az $\div$ (osztás) nem művelet, mert $\mathrm{dmn}(\div) \neq \mathbb{C} \times \mathbb{C}$.
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ halmazon az $\div$ binér művelet.

Műveleti tulajdonságok

Definíció

A $* : X \times X \to X$ művelet
asszociatív, ha $\forall a, b, c \in X : (a * b) * c = a * (b * c)$;
kommutatív, ha $\forall a, b \in X : a * b = b * a$.

Példa

- $\mathbb{C}$-n az $+$ ill. a $\cdot$ műveletek asszociatívak, kommutatívak.
- A függvények halmazán a kompozíció művelete asszociatív: $(f \circ g) \circ h = f \circ (g \circ h)$.
- A függvények halmazán a kompozíció művelete nem kommutatív: $f(x) = x + 1$, $g(x) = x^2$: $x^2 + 1 = (f \circ g)(x) \neq (g \circ f)(x) = (x + 1)^2$.
- A kivonás az egész számok halmazán nem asszociatív: $-1 = (1 - 1) - 1 \neq 1 - (1 - 1) = 1$.

Algebrai struktúrák

Definíció

A $(H; M)$ pár algebrai struktúra, ha H egy halmaz, M pedig H-n értelmezett műveletek halmaza.
Az egy binér műveletes struktúrát grupoidnak nevezzük.

Példa

- $(\mathbb{N}; +)$ algebrai struktúra, mert természetes számok összege természetes szám (ld. Diszkrét matematika 1.), és grupoid is.
- $(\mathbb{N}; -)$ nem algebrai struktúra, mert például $0 - 1 = -1 \notin \mathbb{N}$.
- $(\mathbb{Z}; +, \cdot)$ algebrai struktúra, mert egész számok összege és szorzata egész szám (ld. Diszkrét matematika 1.), de nem grupoid.
- $(\mathbb{Z}_m; +, \cdot)$ algebrai struktúra (ld. Diszkrét matematika 1.), nem grupoid.

Félcsoportok

Definíció

A $(G;*)$ grupoid félcsoport, ha $*$ asszociatív G-n.
Ha létezik $s \in G$: $\forall g \in G : s * g = g * s = g$,
akkor az s semleges elem (egységelem), $(G;*)$ pedig semleges elemes félcsoport (egységelemes félcsoport, monoid).

Példa

- $\mathbb{N}$ az $+$ művelettel egységelemes félcsoport $n = 0$ egységelemmel.
- $\mathbb{Q}$ a $\cdot$ művelettel egységelemes félcsoport $n = 1$ egységelemmel.
- $\mathbb{C}^{k \times k}$ a mátrixszorzással egységelemes félcsoport az egységmátrixszal mint egységelemmel.

Csoportok

Definíció

Legyen $(G;*)$ egy egységelemes félcsoport e egységelemmel. A $g \in G$ elem inverze a $g^{-1} \in G$ elem, melyre $g * g^{-1} = g^{-1} * g = e$.
Ha minden $g \in G$ elemnek létezik inverze, akkor $(G;*)$ csoport.
Ha ezen felül $*$ kommutatív is, akkor $(G;*)$ Abel-csoport.

Példa

- $\mathbb{Q}$ az $+$ művelettel, a 0 egységelemmel.
- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ a $\cdot$ művelettel, az 1 egységelemmel.
- $\{M \in \mathbb{C}^{k \times k} : \det M \neq 0\}$ a mátrixszorzással, és az egységmátrixszal mint egységelemmel.
- $X \to X$ bijektív függvények a kompozícióval, és az $id_X : x \mapsto x$ identikus leképzéssel mint egységelemmel.

Diszkrét matematika 2. C szakirány

5-6. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. tavasz

Gyűrűk

Definíció

Legyen $(R;*,\circ)$ algebrai struktúra, ahol $*$ és $\circ$ binér műveletek. Azt mondjuk, hogy teljesül a $\circ$-nek a $*$-ra vonatkozó bal oldali disztributivitása, illetve jobb oldali disztributivitása, ha
$\forall k,l,m \in R$-re: $\quad k\circ(l*m)=(k\circ l)*(k\circ m)$, illetve
$\forall k,l,m \in R$-re: $\quad (l*m)\circ k=(l\circ k)*(m\circ k)$.

Példa

$(\mathbb{Z};+,\cdot)$ esetén teljesül a szorzás összeadásra vonatkozó mindkét oldali disztributivitása.

Elnevezés

$(R;*,\circ)$ két binér műveletes algebrai struktúra esetén a $*$-ra vonatkozó semleges elemet nullelemnek, a $\circ$-re vonatkozó semleges elemet egységelemnek nevezzük. A nullelem szokásos jelölése 0, az egységelemé 1, esetleg e.

Gyűrűk

Definíció

Az $(R; *, \circ)$ két binér műveletes algebrai struktúra gyűrű, ha

- $(R; *)$ Abel-csoport;
- $(R; \circ)$ félcsoport;
- teljesül a $\circ$-nek a $*$-ra vonatkozó mindkét oldali disztributivitása.

Az $(R; *, \circ)$ gyűrű egységelemes gyűrű, ha R-en a $\circ$ műveletre nézve van egységelem.
Az $(R; *, \circ)$ gyűrű kommutatív gyűrű, ha a $\circ$ művelet (is) kommutatív.

Példa

- $(\mathbb{Z}; +, \cdot)$ egységelemes kommutatív gyűrű.
- $(2\mathbb{Z}; +, \cdot)$ gyűrű, de nem egységelemes.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a szokásos műveletekkel egységelemes kommutatív gyűrűk.
- $\mathbb{C}^{k \times k}$ a szokásos műveletekkel egységelemes gyűrű, de nem kommutatív, ha $k > 1$.

Nullosztómentes gyűrűk

Definíció

Ha egy $(R, *, \circ)$ gyűrűben $\forall r, s \in R$, $r, s \neq 0$ esetén $r \circ s \neq 0$, akkor R nullosztómentes gyűrű.

Példa

Nem nullosztómentes gyűrű

- $(\mathbb{R}^{2\times 2}; +, \cdot)$: $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Állítás

Nullosztómentes gyűrűben a nem-nulla elemek additív rendje megegyezik, és vagy egy p prímszám vagy végtelen.

Definíció

Ha az előző állításban szereplő közös rend p, akkor a gyűrű karakterisztikája p, ha a közös rend végtelen, akkor pedig 0. Jelölése: $char(R)$.

Nullosztómentes gyűrűk

Definíció

A kommutatív, nullosztómentes gyűrűt integritási tartománynak nevezzük.

Példa

- $(\mathbb{Z}; +, \cdot)$

Definíció

Az $(R; *, \circ)$ egységelemes integritási tartományban az $a, b \in R$ elemekre azt mondjuk, hogy a osztója b-nek, ha van olyan $c \in R$, amire $b = a \circ c$. Jelölése: $a|b$.

Definíció

Az egységelem osztóját egységnek nevezzük.

Testek

Definíció

Az $(R; *, \circ)$ gyűrű ferdetest, ha $(R \setminus \{0\}; \circ)$ csoport. A kommutatív ferdetestet testnek nevezzük.

Példa

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a szokásos műveletekkel,
- $\mathbb{Z}_p$ a szokásos műveletekkel, ha p prím.

Alapfogalmak

Definíció

Legyen $(R;+,\cdot)$ gyűrű. A gyűrű elemeiből képzett $f=(f_0,f_1,f_2,\dots)$ $(f_j\in R)$ végtelen sorozatot R fölötti polinomnak nevezzük, ha csak véges sok eleme nem-nulla.
Az R fölötti polinomok halmazát $R[x]$-szel jelöljük.
$R[x]$ elemein definiáljuk az összeadást és a szorzást.
$f=(f_0,f_1,f_2,\dots)$, $g=(g_0,g_1,g_2,\dots)$ és $h=(h_0,h_1,h_2,\dots)$ esetén $f+g=(f_0+g_0,f_1+g_1,f_2+g_2,\dots)$ és $f\cdot g=h$, ahol

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

Megjegyzés

Könnyen látható, hogy polinomok összege és szorzata is polinom.

Alapfogalmak

Állítás (NB)

Ha $(R;+,\cdot)$ gyűrű, akkor $(R[x];+,\cdot)$ is gyűrű, és R fölötti polinomgyűrűnek nevezzük.

Megjegyzés

Gyakran az $(R;+,\cdot)$ gyűrűre szimplán R-ként, az $(R[x];+,\cdot)$ gyűrűre $R[x]$-ként hivatkozunk.

Állítás

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

Állítás

$1 \in R$ egységelem esetén $e = (1, 0, 0 \dots)$ egységeleme lesz $R[x]$-nek.

Alapfogalmak

Állítás

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

Bizonyítás

Legyen n, illetve m a legkisebb olyan index, amire $f_n \neq 0$, illetve $g_m \neq 0$.

$$(f \cdot g)_{n+m} = \sum_{j=0}^{n+m} f_j g_{n+m-j} = \sum_{j=0}^{n-1} f_j g_{n+m-j} + f_n g_m + \sum_{j=n+1}^{n+m} f_j g_{n+m-j} =$$

$$= 0 + f_n g_m + 0 = f_n g_m \neq 0$$

Alapfogalmak

Jelölés

Az $f = (f_0, f_1, f_2, \ldots, f_n, 0, 0, \ldots)$, $f_n \neq 0$ polinomot $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$, $f_n \neq 0$ alakba írjuk.

Definíció

Az előző pontban szereplő polinom esetén f_i-t az i-ed fokú tag együtthatójának nevezzük, f_0 a polinom konstans tagja, f_n a főegyütthatója, $f_n x^n$ a főtagja, n pedig a foka. f fokának jelölésére $deg(f)$ használatos.

Alapfogalmak

Megjegyzés

A főegyüttható tehát a legnagyobb indexű nem-nulla együttható, a fok pedig ennek indexe.
A $0 = (0, 0, \dots)$ nullpolinomnak nincs legnagyobb indexű nem-nulla együtthatója, így a fokát külön definiáljuk, mégpedig $deg(0) = -\infty$.

Definíció

A konstans polinomok a legfeljebb nulladfokú polinomok, a lineáris polinomok pedig a legfeljebb elsőfokú polinomok. Az $f_i x^i$ alakba írható polinomok a monomok. Ha $f \in R[x]$ polinom főegyütthatója R egységeleme, akkor f-et főpolinomnak nevezzük.

Példa

- $x^3 + 1 \in \mathbb{Z}[x]$
- $\frac{2}{3} \in \mathbb{Q}[x]$
- $\pi x + (i + \sqrt{2}) \in \mathbb{C}[x]$

Alapfogalmak

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

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

Alapfogalmak

Megjegyzés

Nullosztómentes gyűrű esetén egyenlőség teljesül a 2. egyenlőtlenségben, hiszen

$$h_{n+k} = \sum_{i=0}^{n+k} f_i g_{n+k-i} = \sum_{i=0}^{n-1} f_i g_{n+k-i} + f_n g_k + \sum_{i=n+1}^{n+k} f_i g_{n+k-i} = f_n g_k \neq 0.$$

Alapfogalmak

Definíció

Az $f(x) = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n \in R[x]$ polinom $r \in R$ helyen felvett helyettesítési értékén az $f(r) = f_0 + f_1r + f_2r^2 + \ldots + f_nr^n \in R$ elemet értjük.
$f(r) = 0$ esetén r-et a polinom gyökének nevezzük.
Az $\hat{f} : r \mapsto f(r)$ leképezés az f polinomhoz tartozó polinomfüggvény.

Megjegyzés

Ha R véges, akkor csak véges sok $R \to R$ függvény van, míg végtelen sok $R[x]$-beli polinom, így vannak olyan polinomok, amikhez ugyanaz a polinomfüggvény tartozik, például $x, x^2 \in \mathbb{Z}_2[x]$.

Példa

$f(x) = x^2 + x - 2 \in \mathbb{Z}[x]$-nek a -2 helyen felvett helyettesítési értéke $(-2)^2 + (-2) - 2 = 0$, ezért -2 gyöke f-nek.

Horner-elrendezés

Legyen $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0$, ahol $f_n \neq 0$. Ekkor átrendezéssel a következő alakot kapjuk:
$f(x) = (\cdots((f_n \cdot x + f_{n-1}) \cdot x + f_{n-2}) \cdot x + \ldots + f_1) \cdot x + f_0$, és így
$f(c) = (\ldots((f_n \cdot c + f_{n-1}) \cdot c + f_{n-2}) \cdot c + \ldots + f_1) \cdot c + f_0$.
Vagyis $f(c)$ kiszámítható n db szorzás és n db összeadás segítségével.

	f_n	f_{n-1}	f_{n-2}	$\ldots$	f_0	
c	$\times$	$c_1 = f_n$	$c_2 = c_1 c + f_{n-1}$	$\ldots$	$c_n = c_{n-1}c + f_1$	$f(c) = c_n c + f_0$

Általánosan: $c_k = c_{k-1}c + f_{n-k+1}$, ha $1 < k \leq n$.

Példa

Határozzuk meg az $f(x) = x^4 - 3x^3 + x + 6$ polinom -2 helyen vett helyettesítési értékét!

	1	-3	0	1	6	
-2	$\times$	1	-5	10	-19	44

A maradékos osztás tétele és következményei

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 előállítást kapunk.
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.

A maradékos osztás tétele és következményei

Bizonyítás folyt.

Egyértelműség: Tekintsük f két megfelelő előállítását:
$f = qg + r = q^*g + r^*$, 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
$0 = g(q - q^*) = r^* - r$, és így
$q = q^*$ és $r = r^*$.

Definíció

Ha $c \in R$ az $f \in R[x]$ polinom gyöke, akkor $(x - c) \in R[x]$ a c-hez tartozó gyöktényező.

A maradékos osztás tétele és következményei

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 $r = 0$.

A maradékos osztás tétele és következményei

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.

A maradékos osztás tétele és következményei

Következmény

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

Bizonyítás

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

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?).

Bővített euklideszi algoritmus

Definíció

Azt mondjuk, hogy $f, g \in R[x]$ polinomok esetén f osztója g-nek (g többszöröse f-nek), ha létezik $h \in R[x]$, amire $g = f \cdot h$.

Definíció

Az $f, g \in R[x]$ polinomok kitüntetett közös osztója (legnagyobb közös osztója) az a $d \in R[x]$ polinom, amelyre $d|f$, $d|g$, és tetszőleges $c \in R[x]$ esetén $(c|f \wedge c|g) \Rightarrow c|d$.

Test fölötti polinomgyűrűben tetszőleges nem-nulla polinommal tudunk maradékosan osztani, ezért működik a bővített euklideszi-algoritmus.

Ez $f, g \in R[x]$ esetén (R test) meghatározza f és g kitüntetett közös osztóját, a $d \in R[x]$ polinomot, továbbá $u, v \in R[x]$ polinomokat, amelyekre $d = u \cdot f + v \cdot g$.

Bővített euklideszi algoritmus

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 $d = u \cdot f + v \cdot g$.

Bővített euklideszi algoritmus

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:
$r_{k+1} = u_{k-1} \cdot f + v_{k-1} \cdot g - q_{k+1} \cdot (u_k \cdot f + v_k \cdot g) =$
$= (u_{k-1} - q_{k+1} \cdot u_k) \cdot f + (v_{k-1} - q_{k+1} \cdot v_k) \cdot g = u_{k+1} \cdot f + v_{k+1} \cdot g$.
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 $r_n | r_{-1} = f$.

Polinomok algebrai deriváltja

Definíció

Legyen R gyűrű. Az
$f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_2 x^2 + f_1 x + f_0 \in R[x]$ $(f_n \neq 0)$ polinom **algebrai deriváltja** az
$f'(x) = nf_n x^{n-1} + (n-1)f_{n-1}x^{n-2} + \ldots + 2f_2 x + f_1 \in R[x]$ polinom.

Megjegyzés

Itt $kf_k = \underbrace{f_k + f_k + \ldots + f_k}_{k \text{ db}}$.

Állítás

Legyen R gyűrű, $a, b \in R$ és $n \in \mathbb{N}^+$. Ekkor $(na)b = n(ab) = a(nb)$.

Bizonyítás

$$(\underbrace{a + a + \ldots + a}_{n \text{ db}})b = (\underbrace{ab + ab + \ldots + ab}_{n \text{ db}}) = a(\underbrace{b + b + \ldots + b}_{n \text{ db}})$$

Polinomok algebrai deriváltja

Állítás

Ha R egységelemes integritási tartomány, akkor az $f \mapsto f'$ algebrai deriválás rendelkezik a következő tulajdonságokkal:

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

Megjegyzés

Megfordítva, ha egy R egységelemes integritási tartomány esetén egy $f \mapsto f'$, $R[x]$-et önmagába képező leképzés rendelkezik az előző 4 tulajdonsággal, akkor az az algebrai deriválás.

Polinomok algebrai 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
$((x-c)^{k+1})' = ((x-c)^k(x-c))' = ((x-c)^k)'(x-c) + (x-c)^k(x-c)' =$
$= k(x-c)^{k-1}(x-c) + (x-c)^k \cdot 1 = (x-c)^k(k+1)$.
Ezzel az állítást beláttuk.

Állítás (NB)

Ha R integritási tartomány, $char(R) = p$, és $0 \neq r \in R$, akkor $n \cdot r = 0 \iff p|n$.

Polinomok algebrai deriváltja

Definíció

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

Megjegyzés

A definíció azzal ekvivalens, hogy $f(x) = (x-c)^n g(x)$, ahol c nem gyöke g-nek. (Miért?)

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 $char(R) \nmid n$, akkor pontosan $(n-1)$-szeres gyöke.

Polinomok algebrai deriváltja

Bizonyítás

Ha $f(x) = (x-c)^n g(x)$, ahol c nem gyöke g-nek, akkor
$f'(x) = ((x-c)^n)' g(x) + (x-c)^n g'(x) =$
$= n(x-c)^{n-1} g(x) + (x-c)^n g'(x) = (x-c)^{n-1}(ng(x) + (x-c)g'(x))$.
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 $char(R) \not| n$.

Példa

Legyen $f(x) = x^4 - x \in \mathbb{Z}_3[x]$. Ekkor 1 3-szoros gyöke f-nek, mert

$$f(x) = x(x^3 - 1) \overset{\mathbb{Z}_3}{=} x(x^3 - 3x^2 + 3x - 1) = x(x-1)^3.$$

$$f'(x) = 4x^3 - 1 \overset{\mathbb{Z}_3}{=} x^3 - 3x^2 + 3x - 1 = (x-1)^3,$$

tehát 1 3-szoros gyöke f'-nek is.

Lagrange-interpoláció

Tétel

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

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.

Lagrange-interpoláció

Példa

Adjunk meg olyan $f \in \mathbb{R}[x]$ polinomot, amelyre $f(0) = 3$, $f(1) = 3$, $f(4) = 7$ és $f(-1) = 0$!

A feladat szövege alapján $c_0 = 0$, $c_1 = 1$, $c_2 = 4$, $c_3 = -1$, $d_0 = 3$, $d_1 = 3$, $d_2 = 7$ és $d_3 = 0$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$$l_0(x) = \frac{(x-1)(x-4)(x+1)}{(0-1)(0-4)(0+1)} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$$

$$l_1(x) = \frac{(x-0)(x-4)(x+1)}{(1-0)(1-4)(1+1)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$$

$$l_2(x) = \frac{(x-0)(x-1)(x+1)}{(4-0)(4-1)(4+1)} = \frac{1}{60}x^3 - \frac{1}{60}x$$

$$l_3(x) = \frac{(x-0)(x-1)(x-4)}{(-1-0)(-1-1)(-1-4)} = -\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$$

$$f(x) = 3l_0(x) + 3l_1(x) + 7l_2(x) + 0l_3(x) = \frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$$

	$\frac{22}{60}$	$-\frac{3}{2}$	$\frac{68}{60}$	3	
1	$\times$	$\frac{22}{60}$	$-\frac{68}{60}$	0	3
4	$\times$	$\frac{22}{60}$	$-\frac{2}{60}$	1	7
-1	$\times$	$\frac{22}{60}$	$-\frac{112}{60}$	3	0

Polinomok felbonthatósága

Definíció

Legyen R egységelemes integritási tartomány.
Ha a $0 \neq f \in R[x]$ polinom nem egység, akkor felbonthatatlannak (irreducibilisnek) nevezzük, ha $\forall a, b \in R[x]$-re

$$f = a \cdot b \Longrightarrow (a \text{ egység} \vee b \text{ egység}) .$$

Ha a $0 \neq f \in R[x]$ polinom nem egység, és nem felbonthatatlan, akkor felbonthatónak (reducibilisnek) nevezzük.

Megjegyzés

Utóbbi azt jelenti, hogy f-nek van nemtriviális szorzat-előállítása (olyan, amiben egyik tényező sem egység).

Polinomok felbonthatósága

Állítás

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

Állítás

Test nullosztómentes.

Állítás

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

Bizonyítás

Később.

Polinomok felbonthatósága

Állítás

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

Bizonyítás

Később.

Megjegyzés

Ha $(R;+,\cdot)$ nem test, akkor egy R fölötti elsőfokú polinomnak nem feltétlenül van gyöke, pl. $2x-1 \in \mathbb{Z}[x]$.

Polinomok felbonthatósága

Állítás

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

Bizonyítás

Később.

Megjegyzés

Tehát nem igaz, hogy egy felbonthatatlan polinomnak nem lehet gyöke.

Polinomok felbonthatósága

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

Később.

Polinomok felbonthatósága

Tétel

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

Bizonyítás

Később.

Tétel

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

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

Bizonyítás

Később.

Polinomok felbonthatósága

Definíció

$f \in \mathbb{Z}[x]$-et primitív polinomnak nevezzük, ha az együtthatóinak a legnagyobb közös osztója 1.

Tétel (Schönemann-Eisenstein)

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

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

akkor f felbonthatatlan $\mathbb{Z}$ fölött.

Bizonyítás

NB. (Lehet, hogy később igen.)

Polinomok felbonthatósága

Megjegyzés

A feltételben f_n és f_0 szerepe felcserélhető.

Megjegyzés

A tétel nem használható test fölötti polinom irreducibilitásának bizonyítására, mert testben nem léteznek prímek, hiszen minden nem-nulla elem egység.

Diszkrét matematika 2. C szakirány

7. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. tavasz

Polinomok felbonthatósága

Definíció

Legyen R egységelemes integritási tartomány.
Ha a $0 \neq f \in R[x]$ polinom nem egység, akkor felbonthatatlannak (irreducibilisnek) nevezzük, ha $\forall a, b \in R[x]$-re

$$f = a \cdot b \Longrightarrow (a \text{ egység} \vee b \text{ egység}) .$$

Ha a $0 \neq f \in R[x]$ polinom nem egység, és nem felbonthatatlan, akkor felbonthatónak (reducibilisnek) nevezzük.

Megjegyzés

Utóbbi azt jelenti, hogy f-nek van nemtriviális szorzat-előállítása (olyan, amiben egyik tényező sem egység).

Emlékeztető

Test nullosztómentes, így F test és $f, g \in F[x]$ esetén:
$\deg(fg) = \deg(f) + \deg(g)$.

Polinomok felbonthatósága

Állítás

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

Bizonyítás

$\Longleftarrow$

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.

$\Longrightarrow$

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.

Polinomok felbonthatósága

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.

Megjegyzés

Ha $(R;+,\cdot)$ nem test, akkor egy R fölötti elsőfokú polinomnak nem feltétlenül van gyöke, pl. $2x-1 \in \mathbb{Z}[x]$.

Polinomok felbonthatósága

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.

Megjegyzés

Tehát nem igaz, hogy egy felbonthatatlan polinomnak nem lehet gyöke.

Polinomok felbonthatósága

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

$\Longleftarrow$

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

$\Longrightarrow$

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.

Polinomok felbonthatósága

Tétel

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

Bizonyítás

$\Longleftarrow$

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

$\Longrightarrow$

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.

Polinomok felbonthatósága

Tétel

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

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

Bizonyítás

$\Longleftarrow$

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.

$\Longrightarrow$

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.

Polinomok felbonthatósága

Bizonyítás folyt.

Tfh. $deg(f) \geq 3$. Az algebra alaptétele értelmében f-nek mint $\mathbb{C}$ fölötti polinomnak van $c \in \mathbb{C}$ gyöke. Ha $c \in \mathbb{R}$ is teljesül, akkor a gyöktényező kiemelésével f egy nemtriviális felbontását kapjuk (Miért?), ami ellentmondás.
Mivel $f \in \mathbb{R}[x]$, ezért $\overline{c}$ is gyöke, hiszen

$$f(\overline{c}) = \sum_{j=0}^{deg(f)} f_j(\overline{c})^j = \sum_{j=0}^{deg(f)} \overline{f_j} \cdot \overline{c^j} = \sum_{j=0}^{deg(f)} \overline{f_j c^j} = \overline{\left(\sum_{j=0}^{deg(f)} f_j c^j \right)} = \overline{f(c)} = \overline{0} = 0.$$

Legyen $g(x) = (x - c)(x - \overline{c}) = x^2 - 2\,\mathrm{Re}(c)x + |c|^2 \in \mathbb{R}[x]$.
f-et g-vel maradékosan osztva létezik $q, r \in \mathbb{R}[x]$, hogy $f = qg + r$.
$r = 0$, mert $deg(r) < 2$, és r-nek gyöke $c \in \mathbb{C} \setminus \mathbb{R}$.
Vagyis $f = qg$, ami egy nemtriviális felbontás, ez pedig ellentmondás.

Polinomok felbonthatósága

Definíció

$f \in \mathbb{Z}[x]$-et primitív polinomnak nevezzük, ha az együtthatóinak a legnagyobb közös osztója 1.

Tétel (Schönemann-Eisenstein)

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

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

akkor f felbonthatatlan $\mathbb{Z}$ fölött.

Bizonyítás

NB. (Lehet, hogy később igen.)

Polinomok felbonthatósága

Megjegyzés

A feltételben f_n és f_0 szerepe felcserélhető.

Megjegyzés

A tétel nem használható test fölötti polinom irreducibilitásának bizonyítására, mert testben nem léteznek prímek, hiszen minden nem-nulla elem egység.

Racionális gyökteszt

Tétel

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \ldots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ 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

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

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

$p | f_0 q^n$, 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 $q | f_n$.

A racionális gyökteszt alkalmazása

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.

Véges testek

Tekintsük valamely p prímre a $\mathbb{Z}_p$ testet, továbbá egy $f(x) \in \mathbb{Z}_p[x]$ felbonthatatlan főpolinomot. Vezessük be a $g(x) \equiv h(x) \pmod{f(x)}$, ha $f(x) | g(x) - h(x)$ relációt.
Ez ekvivalenciareláció, ezért meghatároz egy osztályozást $\mathbb{Z}_p[x]$-en.

Minden osztálynak van $deg(f)$-nél alacsonyabb fokú reprezentánsa (Miért?), és ha $deg(g), deg(h) < deg(f)$, továbbá g és h ugyanabban az osztályban van, akkor egyenlőek (Miért?). Tehát $deg(f) = n$ esetén bijekciót létesíthetünk az n-nél kisebb fokú polinomok és az osztályok között, így p^n darab osztály van.

Az osztályok között értelmezhetjük a természetes módon a műveleteket. Ezeket végezhetjük az n-nél alacsonyabb fokú reprezentánsokkal: ha a szorzat foka nem kisebb, mint n, akkor az $f(x)$-szel vett osztási maradékot vesszük.

Véges testek

$f \not| g$ esetén a bővített euklideszi algoritmus alapján
$d(x) = u(x)f(x) + v(x)g(x)$.
Mivel $f(x)$ felbonthatatlan, ezért $d(x) = d$ konstans polinom, így $\frac{v(x)}{d}$ multiplikatív inverze lesz $g(x)$-nek.

Tétel (NB)

Az ekvivalenciaosztályok halmaza a rajta értelmezett összeadással és szorzással testet alkot.

Megjegyzés

Tetszőleges p prím és n pozitív egész esetén létezik p^n elemű test, mert létezik n-ed fokú felbonthatatlan polinom $\mathbb{Z}_p$-ben.

Megjegyzés

Véges test elemszáma prímhatvány, továbbá az azonos elemszámú testek izomorfak.

Véges testek

Példa

Tekintsük az $x^2 + 1 \in \mathbb{Z}_3[x]$ felbonthatatlan polinomot (Miért az?). A legfeljebb elsőfokú polinomok: $0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2$.
Az összeadás műveleti táblája:

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

Például:

$$2x + 2 + 2x + 1 = 4x + 3 \overset{\mathbb{Z}_3}{=} x$$

Véges testek

Példa folyt.

·	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

Például:

$$(2x+2)(2x+1) = 4x^2 + 6x + 2 \overset{\mathbb{Z}_3}{=} x^2 + 2 = (x^2+1) + 1$$

Feladat: Legyen $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$. Mik lesznek a $z^2 + 1 \in \mathbb{F}_9[z]$ polinom gyökei?

A kommunikáció során információt hordozó adatokat viszünk át egy csatornán keresztül az információforrástól, az adótól az információ címzettjéhez, a vevőhöz.

Adó $\rightarrow$ Csatorna $\rightarrow$ Vevő

A kommunikáció vázlatos ábrája

Megjegyzés

Az információ átvitele térben és időben történik. Egyes esetekben az egyik, más esetekben a másik dimenzió a domináns (pl. telefonálás; információ rögzítése adathordozóra, majd későbbi visszaolvasása).

Definíció

Az **információ** új ismeret. Shannon nyomán az általa megszüntetett bizonytalansággal mérjük.

Definíció

Tegyük fel, hogy egy információforrás nagy számú, összesen n üzenetet bocsát ki. Az összes ténylegesen előforduló különböző üzenet legyen $a_1, a_2, \ldots, a_k$.

Ha az a_j üzenet m_j-szer fordul elő, akkor azt mondjuk, hogy a gyakorisága m_j, relatív gyakorisága pedig $p_j = \frac{m_j}{n} > 0$.

A $p_1, p_2, \ldots, p_k$ szám k-ast az üzenetek eloszlásának nevezzük ($\sum_{j=1}^{k} p_j = 1$).

Az a_j üzenet egyedi információtartalma $I_j = -\log_r p_j$, ahol r egy 1-nél nagyobb valós szám, ami az információ egységét határozza meg. Ha $r = 2$, akkor az információ egysége a bit.

Az üzenetforrás által kibocsátott üzenetek átlagos információtartalma, vagyis $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$ a forrás entrópiája. Ez csak az üzenetek eloszlásától függ, a tartalmuktól nem.

Egy k tagú eloszlásnak olyan pozitív valós számokból álló $p_1, p_2, \ldots, p_k$ sorozatot nevezünk, amelyre $\sum_{j=1}^{k} p_j = 1$. Ennek az eloszlásnak az entrópiája $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$.

Diszkrét matematika 2.C szakirány

8. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu

Komputeralgebra Tanszék

2016. tavasz

Definíció

Legyen $I \subset \mathbb{R}$. Az $f : I \to \mathbb{R}$ függvényt konvexnek nevezzük, ha bármely $x_1, x_2 \in I$ és $0 \leq t \leq 1$ esetén

$$f\left(tx_1 + (1-t)x_2\right) \leq tf(x_1) + (1-t)f(x_2).$$

f szigorúan konvex, ha egyenlőség csak $t = 0$ vagy $t = 1$ esetén lehetséges.

Lemma (Jensen-egyenlőtlenség, NB)

Legyen $p_1, p_2, \ldots, p_k$ egy eloszlás, $f : I \to \mathbb{R}$ pedig egy szigorúan konvex függvény az $I \subset \mathbb{R}$ intervallumon. Ekkor $q_1, q_2, \ldots, q_k \in I$ esetén

$$f\left(\sum_{j=1}^{k} p_j q_j\right) \leq \sum_{j=1}^{k} p_j f(q_j),$$

és egyenlőség pontosan akkor áll fenn, ha $q_1 = q_2 = \ldots = q_k$.

Tétel

Bármilyen eloszláshoz tartozó entrópiára

$$H_r(p_1, p_2, \ldots, p_k) \le \log_r k,$$

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

Bizonyítás

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

$$-H_r(p_1, p_2, \ldots, p_k) = \sum_{j=1}^{k} p_j \log_r p_j =$$

$$= \sum_{j=1}^{k} p_j \left(-\log_r \frac{1}{p_j}\right) \ge -\log_r \left(\sum_{j=1}^{k} p_j \frac{1}{p_j}\right) = -\log_r k.$$

Definíció

A kódolás alatt a legáltalánosabb értelemben az üzenetek halmazának egy másik halmazba való leképezését értjük.
Ha a leképezés injektív, akkor azt mondjuk, hogy a kódolás felbontható, egyértelműen dekódolható, vagy veszteségmentes, egyébként veszteségesnek nevezzük, mert információvesztéssel jár.

Betűnkénti kódolás

A betűnkénti kódolás során az 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 (kódoló ábécé vagy kódábécé) betűivel felírt szó, vagyis ezen ábécéből vett betűk véges sorozata, a sorozat elemeit egyszerűen egymás mellé írva. Az ábécékről feltesszük, hogy nem-üresek és végesek.

Definíció

Az A ábécé betűivel felírható összes (legalább egy betűt tartalmazó) szó halmazát A^+ jelöli, míg az egyetlen betűt sem tartalmazó üres szóval (jele: $\emptyset$ vagy λ) kibővített halmazt A^*.

Betűnkénti kódolás

Definíció

A betűnkénti kódolást egy $\varphi : A \to B^*$ leképezés határozza meg, amelyet természetes módon terjesztünk ki egy $\psi : A^* \to B^*$ leképezéssé:
$a_1 a_2 \dots a_n = \alpha \in A^*$ esetén $\psi(\alpha) = \varphi(a_1)\varphi(a_2)\dots\varphi(a_n)$.
$\mathrm{rng}(\psi)$-t kódnak nevezzük, elemei a kódszavak.

Megjegyzés

Ha φ nem injektív, vagy az üres szó benne van az értékkészletében, akkor a kapott ψ kódolás nem injektív (Miért?), tehát nem felbontható, ezért betűnkénti kódolásnál feltesszük, hogy φ injektív, és B^+-ba képez.

Betűnkénti kódolás

Definíció

Tekintsünk egy A ábécét, és legyen $\alpha, \beta, \gamma \in A^*$. Ekkor α prefixe (előtagja), míg γ szuffixe (utótagja) $\alpha\gamma$-nak, β pedig infixe (belső tagja) $\alpha\beta\gamma$-nak.

Definíció

Prefixmentes halmaznak nevezzük szavak egy halmazát, ha nincs benne két különböző szó, hogy egyik a másik prefixe.

Definíció

Az üres szó és α prefixe, szuffixe és infixe is α-nak, ezeket α triviális prefixeinek, triviális szuffixeinek és triviális infixeinek nevezzük.

Definíció

α egy prefixét, szuffixét, illetve infixét valódi prefixnek, valódi szuffixnek, illetve valódi infixnek nevezzük, ha nem egyezik meg α-val.

Betűnkénti kódolás

Definíció

Tekintsük az injektív $\varphi : A \to B^+$ leképezést, illetve az általa meghatározott ψ betűnkénti kódolást.
Ha $\operatorname{rng}(\varphi)$ prefixmentes halmaz, akkor prefix kódról beszélünk.
Ha $\operatorname{rng}(\varphi)$ elemei azonos hosszúságúak, akkor egyenletes kódról, fix hosszúságú kódról, esetleg blokk-kódról beszélünk.
Vesszős kódról beszélünk, ha van egy olyan $\vartheta \in B^+$ szó (a vessző), amely minden kódszónak szuffixe, de egyetlen kódszó sem áll elő $\alpha\vartheta\beta$ alakban nem üres β szóval.

Állítás

Prefix kód felbontható.

Bizonyítás

Konstruktív: nézzük az eddig beérkezett betűkből összeálló szót. Amint ez kiadja a kódolandó ábécé valamely betűjéhez tartozó kódszót, azonnal dekódolhatunk a megfelelő betűre, mert a folytatásával kapott jelsorozat egyetlen betűhöz rendelt kódszó sem lehet.

Betűnkénti kódolás

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.

Betűnkénti kódolás

Példák

Legyen $A = \{a,b,c\}$, $B = \{0,1\}$, $\varphi : A \to B^+$ pedig az alábbi módon definiált.

	1.	2.	3.	4.	5.	6.
$\varphi(a)$	01	1	01	0	00	01
$\varphi(b)$	1101	01	011	10	10	001
$\varphi(c)$	01	10	11	11	11	0001

1. $\varphi(a) = \varphi(c) \implies \varphi$ nem injektív
2. $\psi(ab) =101= \psi(ca) \implies$ nem felbontható
3. nem prefix, de felbontható
4. prefix
5. egyenletes
6. vesszős

Betűnkénti kódolás

Tétel (McMillan-egyenlőtlenség, NB)

Legyen $A = \{a_1, a_2, \ldots, a_n\}$ 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

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

Tétel (McMillan-egyenlőtlenség megfordítása, NB)

Az előző tétel jelöléseit használva, ha $l_1, l_2, \ldots, l_n$ olyan pozitív egész számok, hogy $\sum_{j=1}^{n} r^{-l_j} \leq 1$, akkor van az A-nak a B elemeivel való olyan felbontható (sőt prefix) kódolása, hogy az a_j betűhöz rendelt kódszó hossza l_j.

Betűnkénti kódolás

Definíció

Legyen $A = \{a_1, a_2, \dots, a_n\}$ a kódolandó ábécé, $p_1, p_2, \dots, p_n$ a betűk eloszlása, $\varphi : A \to B^+$ injektív leképezés, továbbá $l_j = |\varphi(a_j)|$.
Ekkor $\bar{l} = \sum_{j=1}^{n} p_j l_j$ a kód átlagos szóhossza.
Ha adott elemszámú ábécével és eloszlással egy felbontható betűnkénti kód átlagos szóhosszúsága minimális, akkor optimális kódnak nevezzük.

Megjegyzés

Az átlagos kódhossz valós szám, és valós számok halmazában nem feltétlenül van minimális elem (ld. $\{\frac{1}{n} | n \in \mathbb{N}\}$), ezért optimális kód létezése nem triviális.

Betűnkénti kódolás

Állítás

Adott ábécé és eloszlás esetén létezik optimális kód.

Bizonyítás

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

Betűnkénti kódolás

Tétel (Shannon tétele zajmentes csatornára)

Legyen $A = \{a_1, a_2, \ldots, a_n\}$ a kódolandó ábécé, $p_1, p_2, \ldots, p_n$ a betűk eloszlása, $\varphi : A \to B^+$ injektív leképezés, B elemeinek a száma $r \geq 2$, továbbá $l_j = |\varphi(a_j)|$.
Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $H_r(p_1, p_2, \ldots, p_n) \leq \bar{l}$.

Bizonyítás

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

$$= -\sum_{j=1}^{n} p_j \log_r r^{-l_j} - \sum_{j=1}^{n} p_j \log_r \frac{1}{p_j} = -\sum_{j=1}^{n} p_j \log_r \frac{r^{-l_j}}{p_j} \geq$$

$$\geq -\log_r \left(\sum_{j=1}^{n} r^{-l_j} \right) \geq -\log_r 1 = 0$$

Betűnkénti kódolás

Tétel (Shannon kód létezése)

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

Bizonyítás

Válasszunk olyan $l_1, l_2, \ldots, l_n$ természetes számokat, amelyekre $r^{-l_j} \leq p_j < r^{-l_j+1}$, ha $j = 1, 2, \ldots, n$ (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

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

Optimális kódkonstrukció: Huffman-kód

Legyen $\{a_1, a_2, \ldots, a_n\}$ az üzenetek halmaza, a hozzájuk tartozó eloszlás pedig $p_1, p_2, \ldots, p_n$, a kódábécé elemszáma r.
Rendezzük relatív gyakoriság szerint csökkenő sorrendbe a betűket.
Osszuk el maradékosan $n-2$-t $r-1$-gyel:
$n-2 = q(r-1)+m \quad 0 \leq m < r-1$, és legyen $t = m+2$.
Helyettesítsük az utolsó t betűt egy új betűvel, amihez az elhagyott betűk relatív gyakoriságainak 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-et.
Ezeket a kódoló ábécé elemeivel kódoljuk, majd a redukciónak megfelelően visszafelé haladva, az összevont betűk kódját az összevonásként kapott betű már meglévő kódjának a kódoló ábécé különböző betűivel való kiegészítésével kapjuk.

Példa Huffman-kódra

Legyen $A = \{a, b, \ldots, j\}$, a relatív gyakoriságok $0,17; 0,02; 0,13; 0,02; 0,01; 0,31; 0,02; 0,17; 0,06; 0,09$, a kódoló ábécé pedig $\{0, 1, 2\}$. $10 - 2 = 4 \cdot (3 - 1) + 0$, így $t = 0 + 2 = 2$.

f	0,31	
a	0,17	
h	0,17	
c	0,13	
j	0,09	
i	0,06	
b	0,02	
d	0,02	
g	0,02	$\}$ 0, 03
e	0,01	

f	0,31	
a	0,17	
h	0,17	
c	0,13	
j	0,09	
i	0,06	
(g,e)	0,03	
b	0,02	$\}$ 0, 07
d	0,02	

f	0,31	
a	0,17	
h	0,17	
c	0,13	
j	0,09	
((g,e),b,d)	0,07	$\}$ 0, 22
i	0,06	

f	0,31	
(j,((g,e),b,d),i)	0,22	
a	0,17	
h	0,17	$\}$ 0, 47
c	0,13	

(a,h,c)	0,47
f	0,31
(j,((g,e),b,d),i)	0,22

Példa Huffman-kódra folyt.

(a,h,c)	0,47
f	0,31
(j,((g,e),b,d),i)	0,22

Kódolás:

(a,h,c)$\mapsto$0
- a$\mapsto$00
- h$\mapsto$01
- c$\mapsto$02

f$\mapsto$1

(j,((g,e),b,d),i)$\mapsto$2
- j$\mapsto$20
- ((g,e),b,d)$\mapsto$21
  - (g,e)$\mapsto$210
    - g$\mapsto$2100
    - e$\mapsto$2101
  - b$\mapsto$211
  - d$\mapsto$212
- i$\mapsto$22

Entrópia: $\approx 1,73$.

Átlagos szóhossz: $1,79$.

Betűnkénti kódolás

Tétel (NB)

A Huffman-kód optimális.

Példa Shannon-kódra

Az előző példában használt ábécét és eloszlást fogjuk használni. Rendezzük sorba az ábécét relatív gyakoriságok szerinti csökkenő sorrendben:

f	0,31
a	0,17
h	0,17
c	0,13
j	0,09
i	0,06
b	0,02
d	0,02
g	0,02
e	0,01

Példa Shannon-kódra folyt.

Határozzuk meg a szükséges szóhosszúságokat:
$\frac{1}{9} \leq 0,31; 0,17; 0,13 < \frac{1}{3}$, ezért f, a, h és c kódhossza 2.
$\frac{1}{27} \leq 0,09; 0,06 < \frac{1}{9}$, ezért j és i kódhossza 3.
$\frac{1}{81} \leq 0,02 < \frac{1}{27}$, ezért b, d és g kódhossza 4.
$\frac{1}{243} \leq 0,01 < \frac{1}{81}$, ezért e kódhossza 5.
Az f kódja 00, az a kódja 01, a h kódja 02, és ez utóbbihoz 1-et adva hármas alapú számrendszerben kapjuk c kódját, ami 10. Ehhez 1-et adva 11-et kapunk, de j kódjának hossza 3, ezért ezt még ki kell egészíteni jobbról egy 0-val, tehát j kódja 110. Hasonlóan folytatva megkapjuk a teljes kódot:

f	00
a	01
h	02
c	10
j	110
i	111
b	1120
d	1121
g	1122
e	12000

Átlagos szóhossz: $2,3 < 1,73 + 1$.

Diszkrét matematika 2.C szakirány

9. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu

Komputeralgebra Tanszék

2016. tavasz

Betűnkénti kódolás

Kódfa

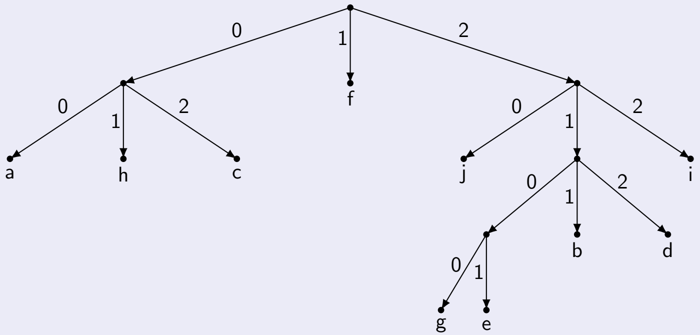
A betűnkénti kódolás szemléltethető egy címkézett irányított fával.
Legyen $\varphi : A \to B^*$ egy betűnkénti kódolás, és tekintsük $\mathrm{rng}(\varphi)$ prefixeinek halmazát. Ez a halmaz részbenrendezett a ,,prefixe'' relációra. (Miért?)
Vegyük ennek a Hasse-diagramját. Így egy irányított fát kapunk, aminek a gyökere az üres szó, és minden szó a hosszának megfelelő szinten van.
A fa éleit címkézzük úgy B elemeivel, hogy ha $\beta = \alpha b$ valamely $b \in B$-re, akkor az α-ból β-ba vezető él címkéje legyen b.
A kódfa csúcsait is megcímkézhetjük: az $a \in A$ kódjának megfelelő csúcs címkéje legyen $a \in A$; azon csúcs címkéje, amely nincsen $\mathrm{rng}(\varphi)$-ben, legyen ,,üres''.

Megjegyzés

Az előbbi konstrukció meg is fordítható. Tekintsünk egy véges, élcímkézett irányított fát, ahol az élcímkék halmaza B, az egy csúcsból kiinduló élek mind különböző címkéjűek, továbbá az A véges ábécének a csúcsokra való leképezését, amelynél minden levél előáll képként.
Az $a \in A$ betű kódja legyen az a szó, amelyet úgy kapunk, hogy a gyökértől az a-nak megfelelő csúcsig haladó irányított út mentén összeolvassuk az élek címkéit.

Kódfa

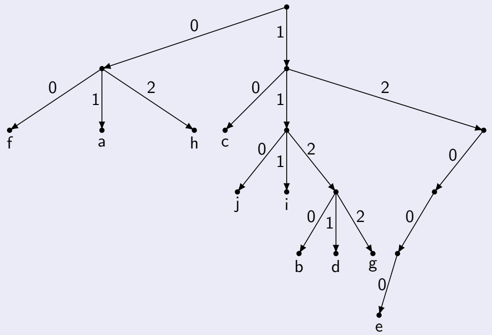
Példa



A Huffman-kódos példában szereplő kódhoz tartozó kódfa.
$\varphi(a) =$00, $\varphi(b) =$211, $\varphi(c) =$02, $\varphi(d) =$212, $\varphi(e) =$2101, $\varphi(f) =$1, $\varphi(g) =$2100, $\varphi(h) =$01, $\varphi(i) =$22, $\varphi(j) =$20.
A kódszavak prefixeinek halmaza:
$\{00, 0, \lambda, 211, 21, 2, 02, 212, 2101, 210, 1, 2100, 01, 22, 20\}$

Kódfa

Példa



A Shannon-kódos példában szereplő kódhoz tartozó kódfa.
$\varphi(a) = 01$, $\varphi(b) = 1120$, $\varphi(c) = 10$, $\varphi(d) = 1121$, $\varphi(e) = 12000$, $\varphi(f) = 00$, $\varphi(g) = 1122$, $\varphi(h) = 02$, $\varphi(i) = 111$, $\varphi(j) = 110$.
A kódszavak prefixeinek halmaza:
$\{01, 0, \lambda, 1120, 112, 11, 1, 10, 1121, 12000, 1200, 120, 12, 00, 1122, 02, 111, 110\}$

Hibakorlátozó kódolás

Példa (ISBN (International Standard Book Number) kódolása)

Legyen $d_1, d_2, \ldots, d_n$ 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 észrevesszük, ha $j < n$ esetén d_j-t és d_{j+1}-et felcseréljük:
az összeg $jd_{j+1} + (j+1)d_j - jd_j - (j+1)d_{j+1} = d_j - d_{j+1}$-gyel nő, ami csak akkor lehet 11-gyel osztható, ha $d_j = d_{j+1}$.

Megjegyzés

2007 óta 13 jegyű.
A személyi számnál is használják.

Hibakorlátozó kódolás

Példa (Paritásbites kód)

Egy n hosszú 0-1 sorozatot egészítsünk ki egy $n+1$-edik bittel, ami legyen 1, ha a sorozatban páratlan sok 1-es van, különben pedig legyen 0. Ha egy bit megváltozik, akkor észleljük a hibát.

Példa (Kétdimenziós paritásellenőrzés)

$$
\begin{array}{ccccc|c}
b_{0,0} & \cdots & b_{0,j} & \cdots & b_{0,n-1} & b_{0,n} \\
\vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\
b_{i,0} & \cdots & b_{i,j} & \cdots & b_{i,n-1} & b_{i,n} \\
\vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\
b_{m-1,0} & \cdots & b_{m-1,j} & \cdots & b_{m-1,n-1} & b_{m-1,n} \\
\hline
b_{m,0} & \cdots & b_{m,j} & \cdots & b_{m,n-1} & b_{m,n}
\end{array}
$$

Oszlopok és sorok végén paritásbit. Ha megváltozik egy bit, akkor a sor és az oszlop végén jelez az ellenőrző bit, ez alapján tudjuk javítani a hibát. Ha két bit változik meg, akkor észleljük a hibát, de nem tudjuk javítani.

Hibakorlátozó kódolás

Definíció

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

Példa

- ISBN - 1-hibajelző
- paritásbites kód - 1-hibajelző
- kétdimenziós paritásellenőrzés - 2-hibajelző

Hiba javításának módjai

ARQ (Automatic Retransmission Request) - újraküldés,
FEC (Forward Error Correction) - javítható, pl.: kétdimenziós paritásell.

Hibakorlátozó kódolás

Definíció

Legyen A véges ábécé, továbbá $u, v \in A^n$. Ekkor u és v Hamming-távolsága alatt az azonos pozícióban lévő különböző betűk számát értjük:

$$d(u, v) = |\{i : 1 \leq i \leq n \wedge u_i \neq v_i\}|.$$

Példa

0	1	1	1	0
1	0	1	0	1
$\neq$	$\neq$	$=$	$\neq$	$\neq$

d(01110,10101)=4

A	L	M	A
A	N	N	A
$=$	$\neq$	$\neq$	$=$

d(ALMA,ANNA)=2

Hibakorlátozó kódolás

Állítás

A Hamming-távolság rendelkezik a távolság szokásos tulajdonságaival, vagyis tetszőleges u, v, w-re

1) $d(u, v) \geq 0$;
2) $d(u, v) = 0 \iff u = v$;
3) $d(u, v) = d(v, u)$ (szimmetria);
4) $d(u, v) \leq d(u, w) + d(w, v)$ (háromszög-egyenlőtlenség).

Bizonyítás

1), 2) és 3) nyilvánvaló.
4) Ha u és v eltér valamelyik pozicióban, akkor ott u és w, illetve w és v közül legalább az egyik pár különbözik.

Hibakorlátozó kódolás

Definíció

A K **kód távolsága** ($d(K)$) a különböző kódszópárok távolságainak a minimuma.

Példa (*)

$$\begin{array}{lccccc}
(0,0) \mapsto (0,0,0,0,0) & & & & & \\
 & 3 & & & & \\
(0,1) \mapsto (0,1,1,1,0) & & 3 & & & \\
 & 4 & & & & 4 \\
(1,0) \mapsto (1,0,1,0,1) & & & & 3 & \\
 & 3 & & & & \\
(1,1) \mapsto (1,1,0,1,1) & & & & &
\end{array}$$

A kód távolsága 3.

Felmerül a kérdés, hogy vajon mi lehetett a kódszó, ha a (0,1,0,0,0) szót kapjuk.

Hibakorlátozó kódolás

Definíció

Minimális távolságú dekódolás esetén egy adott szóhoz azt a kódszót rendeljük, amelyik hozzá a legközelebb van. Több ilyen szó esetén kiválasztunk ezek közül egyet, és az adott szóhoz mindig azt rendeljük.

Megjegyzés

A dekódolás két részre bontható: a hibajavításnál megpróbáljuk meghatározni, hogy mi volt az elküldött kódszó, majd visszaállítjuk az üzenetet. Mivel az utóbbi egyértelmű, ezért hibajavító kódok dekódolásán legtöbbször csak a hibajavítást értjük.

Definíció

Egy kód t-hibajavító, ha minden olyan esetben helyesen javít, amikor egy elküldött szó legfeljebb t helyen változik meg.
Egy kód pontosan t-hibajavító, ha t-hibajavító, de van olyan $t+1$ hibával érkező szó, amit helytelenül javít, vagy nem javít.

Hibakorlátozó kódolás

Megjegyzés

Ha a kód távolsága d, akkor minimális távolságú dekódolással $t < \frac{d}{2}$ esetén t-hibajavító.

Példa

A (*) kód pontosan 1-hibajavító.
$(0,0,0,0,0) \rightsquigarrow (1,0,0,0,1) \longrightarrow (1,0,1,0,1)$

Példa (ismétléses kód)

$a \longmapsto (a,a,a) \quad d = 3 \quad 1$-hibajavító,
$a \longmapsto (a,a,a,a,a) \quad d = 5 \quad 2$-hibajavító.

Hibakorlátozó kódolás

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.

Definíció

Ha egy kódra a Singleton-korlát egyenlőséggel teljesül, akkor azt maximális távolságú szeparábilis kódnak (MDS-kód) nevezzük.

Példa

Az n-szeri ismétlés kódja. Ekkor $d = n$, és $|K| = q$.

Hibakorlátozó kódolás

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?).

Hibakorlátozó kódolás

Definíció

Ha egy kódra a Hamming-korlát egyenlőséggel teljesül, akkor azt perfekt kódnak nevezzük.

Példa

A (*) kód esetén $|K| = 4$, $n = 5$, $q = 2$ és $t = 1$.
B.O.$= 4\left(\binom{5}{0}(2-1)^0 + \binom{5}{1}(2-1)^1\right) = 4(1+5) = 24$,
J.O.$= 2^5 = 32$.
Nem perfekt kód.

A kód távolságának és hibajelző képességének kapcsolata

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 különböző 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.

A kód távolságának és hibajavító képességének kapcsolata

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-től $d - t \leq \frac{d}{2} \leq t$ 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.

Lineáris kódok

Definíció

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

Megjegyzés

Itt $\mathbb{F}$ elemei a betűk, és $\mathbb{F}^n$ elemei a szavak, az altér elemei a kódszavak.

Jelölés

Ha az altér k-dimenziós, a kód távolsága d, a test elemeinek a száma pedig q, akkor $[n, k, d]_q$ kódról beszélünk.
Ha nem lényeges d és q értéke, akkor elhagyjuk őket a jelölésből, és $[n, k]$-t írunk.

Lineáris kódok

Megjegyzés

Egy $[n, k, d]_q$ kód esetén a Singleton-korlát alakja egyszerűsödik:

$$q^k \leq q^{n-d+1} \iff k \leq n - d + 1.$$

Példa

1) A (*) kód egy $[5, 2, 3]_2$ kód:

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

Lineáris kódok

Példa folyt.

2) $\mathbb{F}_q$ felett az ismétléses kód:
pl. a háromszori ismétlés kódja: $a \mapsto (a, a, a)$.
Ez egy $[3, 1, 3]_q$ kód.

3) Paritásbites kód (ha páros sok egyesre egészítünk ki):
$(b_1, b_2, \ldots, b_k) \mapsto (b_1, b_2, \ldots, b_k, \sum_{j=1}^{k} b_j)$.
Ez egy $[n, n-1, 2]_2$ kód.

Definíció

Az $\mathbb{F}$ véges test mint ábécé feletti n hosszú $u \in \mathbb{F}^n$ szó súlya alatt a nem-nulla koordinátáinak a számát értjük, és $w(u)$-val jelöljük.
Egy K kód súlya a nem-nulla kódszavak súlyainak a minimuma:

$$w(K) = \min_{u \neq 0} w(u).$$

Lineáris kódok

Megjegyzés

Egy szó súlya megegyezik a 0-tól vett távolságával:
$w(u) = d(u, (0, 0, \ldots, 0))$.

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?).

Diszkrét matematika 2.C szakirány

10. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu

Komputeralgebra Tanszék

2016. tavasz

Lineáris kódok

Megjegyzés

Egy szó súlya megegyezik a 0-tól vett távolságával:
$w(u) = d(u, (0, 0, \ldots, 0))$.

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?).

Lineáris kódok

Lineáris kód esetén a kódolás elvégezhető mátrixszorzással.

Definíció

Legyen $G : \mathbb{F}_q^k \to \mathbb{F}_q^n$ egy teljes rangú lineáris leképzés, illetve $\mathbf{G} \in \mathbb{F}_q^{n\times k}$ a hozzá tartozó mátrix. $K = \mathrm{Im}(G)$ esetén $\mathbf{G}$-t a K kód **generátormátrixának** nevezzük.

$$\begin{array}{cc} & \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} \\ \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nk} \end{pmatrix} & \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \end{array}$$

Lineáris kódok

Példa

1) A (*) kód egy generátormátrixa:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2) A háromszori ismétlés kódjának egy generátormátrixa:

$$\mathbf{G} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Lineáris kódok

Példa folyt.

3) A paritásbites kód egy generátormátrixa:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

Lineáris kódok

Definíció

Egy $[n, k, d]_q$ kódnak $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ mátrix az ellenőrző mátrixa, ha $\mathbf{H}v = 0 \iff v$ kódszó.

Megjegyzés

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

Példa

1) A (*) kód egy ellenőrző mátrixa:

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

Lineáris kódok

Példa folyt.

2) A háromszori ismétlés kódjának egy ellenőrző mátrixa:

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

3) A paritásbites kód egy ellenőrző mátrixa:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$$

Lineáris kódok

Definíció

Ha a kódszavak első k betűje megfelel az eredeti kódolandó szónak, akkor szisztematikus kódolásról beszélünk.
Ekkor az első k karakter az üzenetszegmens, az utolsó $n-k$ pedig a paritásszegmens.

Példa

1) A háromszori ismétlés kódja:

$$(\underbrace{a}_{\text{üz.sz.}}, \underbrace{a, a}_{\text{par.sz.}})$$

2) A paritásbites kód:

$$(\underbrace{b_1, b_2, \ldots, b_{n-1}}_{\text{üz.sz.}}, \underbrace{\sum_{j=1}^{n-1} b_j}_{\text{par.sz.}})$$

Lineáris kódok

Megjegyzés

Szisztematikus kódolás esetén könnyen tudunk dekódolni: a paritásszegmens elhagyásával megkapjuk a kódolandó szót.

Megjegyzés

Egy szisztematikus kód generátormátrixa speciális alakú:

$$\mathbf{G} = \begin{pmatrix} \mathbf{I}_k \\ \mathbf{P} \end{pmatrix},$$

ahol $\mathbf{I}_k \in \mathbb{F}_q^{k \times k}$ az egységmátrix, továbbá $\mathbf{P} \in \mathbb{F}_q^{(n-k) \times k}$.

Lineáris kódok

Állítás

Legyen $\mathbf{G} \in \mathbb{F}_q^{n\times k}$ egy szisztematikus kód generátormátrixa:
$\mathbf{G} = \begin{pmatrix} \mathbf{I}_k \\ \mathbf{P} \end{pmatrix}$. Ekkor $\mathbf{H} = \begin{pmatrix} -\mathbf{P} & \mathbf{I}_{n-k} \end{pmatrix}$ 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 $\mathbf{H}(\mathbf{G}u) = (\mathbf{HG})u = \mathbf{0}u = \underline{0}$,
vagyis $\mathrm{Im}(\mathbf{G}) \subset \mathrm{Ker}(\mathbf{H})$, amiből $\dim(\mathrm{Im}(\mathbf{G})) \leq \dim(\mathrm{Ker}(\mathbf{H}))$.
$\dim(\mathrm{Im}(\mathbf{G})) = k$ és $\dim(\mathrm{Ker}(\mathbf{H})) \leq k$ miatt viszont
$\dim(\mathrm{Im}(\mathbf{G})) \geq \dim(\mathrm{Ker}(\mathbf{H}))$ is teljesül, így $\mathrm{Im}(\mathbf{G}) = \mathrm{Ker}(\mathbf{H})$.

Példa

Ld. korábban.

Lineáris kódok

A kód távolsága leolvasható az ellenőrző mátrixból.

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 $\mathbf{H} = \begin{pmatrix} \underline{h_1} & \underline{h_2} & \cdots & \underline{h_n} \end{pmatrix}$.

$\Longrightarrow$

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.

$\Longleftarrow$

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

Lineáris kódok

Következmény

A kód távolsága a legkisebb pozitív egész l, amire létezik az ellenőrző mátrixnak l darab lineárisan összefüggő oszlopa.

Példa

A (*) kód esetén:

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

Egyik oszlopvektor sem a nullvektor, így nincs 1 darab lineárisan összefüggő oszlop.
Egyik oszlopvektor sem többszöröse egy másiknak, így nincs 2 darab lineárisan összefüggő oszlop.
Az 1., 3. és 5. oszlopok lineárisan összefüggőek, így a kód távolsága 3.

Lineáris kódok

A $\mathbf{H}$ ellenőrző mátrix segítségével dekódolni is lehet.

Definíció

Adott $\underline{v} \in \mathbb{F}_q^n$ esetén az $\underline{s} = \mathbf{H}\underline{v} \in \mathbb{F}_q^{n-k}$ vektort szindrómának nevezzük.

Megjegyzés

A $\underline{v}$ pontosan akkor kódszó, ha $\underline{s} = \underline{0}$.

Definíció

Legyen $\underline{c}$ a kódszó, $\underline{v}$ a vett szó. Az $\underline{e} = \underline{v} - \underline{c}$ a hibavektor.

Állítás

$\mathbf{H}\underline{v} = \mathbf{H}\underline{e}$.

Bizonyítás

$\mathbf{H}\underline{v} = \mathbf{H}(\underline{c} + \underline{e}) = \mathbf{H}\underline{c} + \mathbf{H}\underline{e} = \underline{0} + \mathbf{H}\underline{e} = \mathbf{H}\underline{e}$

Lineáris kódok

A dekódolás elve: $\underline{v}$-ből kiszámítjuk a $\mathbf{H}\underline{v}$ szindrómát, ami alapján megbecsüljük az $\underline{e}$ hibavektort, majd meghatározzuk $\underline{c}$-t a $\underline{c} = \underline{v} - \underline{e}$ képlet segítségével.

Definíció

Valamely $\underline{e}$ hibavektorhoz tartozó mellékosztály az $\{\underline{e} + \underline{c} : c \text{ kódszó}\}$ halmaz.

Megjegyzés

Az $\underline{e} = \underline{0}$-hoz tartozó mellékosztály a kód.

Állítás

Az azonos mellékosztályban lévő szavak szindrómája megegyezik.

Lineáris kódok

Definíció

Minden $\underline{s}$ szindróma esetén legyen $\underline{e}_{\underline{s}}$ az a minimális súlyú szó, melynek $\underline{s}$ a szindrómája. Ez az $\underline{s}$ szindrómához tartozó mellékosztály-vezető, a mellékosztály elemei $\underline{e}_{\underline{s}} + \underline{c}$ alakúak, ahol $\underline{c} \in K$ kódszó.

Szindrómadekódolás

Adott $\underline{v}$ esetén tekintsük az $\underline{s} = \mathbf{H}\underline{v}$ szindrómát, és az $\underline{e}_{\underline{s}}$ mellékosztály-vezetőt. Dekódoljuk $\underline{v}$-t $\underline{c} = \underline{v} - \underline{e}_{\underline{s}}$-nek.

Állítás

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

Lineáris kódok

Bizonyítás

Egyrészt a korábbi állítás alapján $\underline{s} = \mathbf{H}\underline{v} = \mathbf{H}\underline{e}$, másrészt $\underline{e_s}$ definíciója miatt $\underline{s} = \mathbf{H}\underline{e_s}$. Ezért $\underline{e}$ és $\underline{e_s}$ ugyanabban a mellékosztályban van, továbbá $w(\underline{e_s}) \leq w(\underline{e})$.

$w(\underline{e} - \underline{e_s}) = d(\underline{e}, \underline{e_s}) \leq d(\underline{e}, \underline{0}) + d(\underline{0}, \underline{e_s}) = w(\underline{e}) + w(\underline{e_s}) < d$.

De $\mathbf{H}(\underline{e} - \underline{e_s}) = \underline{0}$ miatt $\underline{e} - \underline{e_s}$ kódszó (Miért?), így $\underline{e} = \underline{e_s}$.

Példa

Tekintsük a (*) kódot.

$\underline{v} = (1, 1, 0, 1, 1)^T$ esetén $\mathbf{H}\underline{v} = \underline{0}$, így $\underline{v}$ kódszó.

$\underline{v} = (1, 1, 0, 0, 1)^T$ esetén $\mathbf{H}\underline{v} = (0, 1, 0)^T = \underline{s}$.

Mi az $\underline{s}$-hez tartozó mellékosztály-vezető?

A $(0, 0, 0, 1, 0)^T$ súlya 1, és a szindrómája a keresett $(0, 1, 0)^T$, így ez lesz a mellékosztály-vezető.

$\underline{c} = \underline{v} - \underline{e_s} = (1, 1, 0, 0, 1)^T - (0, 0, 0, 1, 0)^T = (1, 1, 0, 1, 1)^T$