

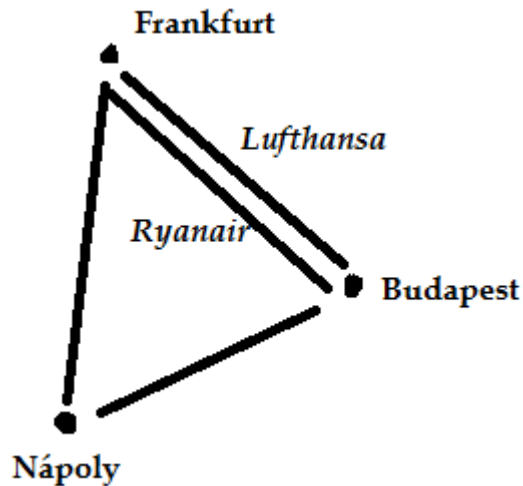
Javítások

- 3. oldal:** Véges gráf: VÉGES sok él és VÉGES sok csúcs alkotja
- 4. oldal:** e_i él a v_{i-1} és v_i csúcsokra illeszkedik
- 4. oldal:** Nyílt és zárt séta/vonal definíciója fel volt cserélve
- 17. oldal:** Illeszkedési mátrix ábráján a 4-es él 4-es címkéje hiányzott
- 22. oldal:** A homomorf képből is van semleges elem részben
- 26. oldal:** Polinomszorítás: $f_i * g_{k-i}$ a g_{k-1} helyett
- 27. oldal:** Polinom foka, polinom főegyütthatója és monom részben f_n (felső index) helyett f_0 (alsó index)
- 28. oldal:** Maradékos osztás bizonyítása: létezik olyan q és r eleme $R[x]$
- 40. oldal:** $\Psi: A^* \rightarrow B^*$ (A ábécé szavait alakítom át B ábécé szavaira)
- 41. oldal:** Például prefix kód: $\{01, 001, 000\}$
- 45. oldal:** Optimális kód(2): annak is legalább kettő a kifoka. és
(4): r nem kongruens n
- 48. oldal:** C hibajavító képessége: $d-1/2$
- 55. oldal:** Egyszerűbb példa: mind a két vonalon 0 van. 59. oldal: Algoritmusok hatékonysága $g = O(f)$

Gráfok

Gráfok: Tulajdonképpen pontok, éllel összekötve, rajtuk címkék vagy súlyok.

Pl.: Városok közötti repülőjáratok



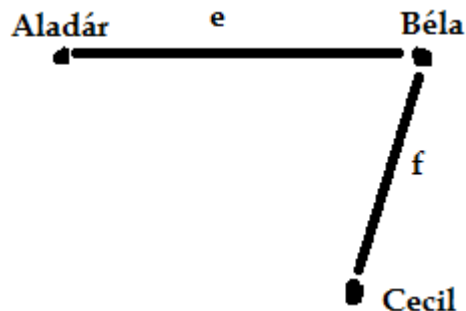
Irányítatlan gráf: $G = (\varphi, E, V)$ hármas

E: Élek halmaza [E – edge]

V: Csúcsok halmaza [V – vertex, vertices]

φ : Illeszkedési leképezés: $E \rightarrow V$ -beli **rendezetlen párok** halmazába képzi

Pl.: Emberek közötti ismeretségek



$E = \{e, f\}$

$V = \{\text{Aladár, Béla, Cecil}\}$

$\varphi = \{ (e, \{\text{Aladár, Béla}\}), (f, \{\text{Béla, Cecil}\}) \}$
rendezetlen párok

$\varphi = e \rightarrow \{\text{Aladár, Béla}\}$

$f \rightarrow \{\text{Béla, Cecil}\}$

Irányítatlan gráfok újra:

Ha $v \in \varphi(e)$ [v a $\varphi(e)$ egyik komponense], akkor **e illeszkedik v -re** vagy **v végpontja e -nek**.

Pl. előző ismeretséges példa

$\varphi(e) = \{\text{Aladár, Béla}\} \rightarrow \text{Aladár} \in \varphi(e)$

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



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



2 különböző él **párhuzamos él**, ha ugyanazokra a csúcsokra illeszkedik.

Formálisan: $\varphi(e_1) = \varphi(e_2)$, de $e_1 \neq e_2$



Ha egy él csak egy csúcsra illeszkedik, akkor **hurokél**.

Formálisan: $\varphi(e) = \{v, v\}$



$G = (\varphi, E, V)$ **véges gráf**, ha E és V is véges [azaz véges sok él és véges sok csúcs alkotja]. Az informatikában ilyenekkel foglalkozunk.

Ha egy csúcsra nem illeszkedik él, akkor azt **izolált csúcsnak** nevezzük.



Egyszerű gráf: Nincs se párhuzamos éle és nincs hurokéle sem.

Pl: Facebook-ban az emberek közötti ismertségek, hisz nem lehetünk valakinek kétszer az ismerősei (párhuzamos élek), és nem lehetünk saját magunk ismerősei sem (hurokél).

Fokszám: Az adott csúcsra illeszkedő élek száma, a hurokéleket duplán számolva.

Jele: $d(v)$ vagy $\deg(v)$ (degree – fok)

Pl.: Facebook-ban az ismerőseink száma.



$$d(v) = 6 \text{ (4 sima él + 1 hurokél)}$$

Tétel:

Egy gráf összes csúcsának fokszám-összege megegyezik a gráf éleinek kétszeresével.

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

Bizonyítás: Ha olyan élt adunk a gráfhoz, amely két különböző csúcsra illeszkedik, akkor mindkét csúcs fokszáma eggyel nő, azaz az össz. fokszám kettővel nő. Ha hurokélt adunk a gráfhoz, akkor az csak egy csúcsra illeszkedik, de mivel a hurokéleket kétszeresen számoljuk, ezért az össz. fokszám ugyancsak kettővel nő.

k-reguláris gráf: Olyan gráf, amelyben minden csúcs fokszáma k . ($k \in \mathbb{N}$)

Pl.: A négyzet 2-reguláris gráf

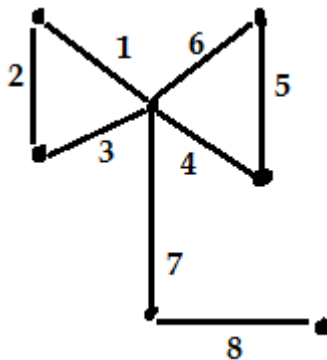


Séta: Egy n hosszú séta v_0 -ból v_n -be egy olyan **sorozat**:

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

ahol e_i él a v_{i-1} és v_i csúcsokra illeszkedik. ($i = 1..n$)

Pl.: 8 hosszú séta



Vonal: Olyan séta, ahol minden él különbözik.

Pl.: A fenti 8 hossz hosszú séta vonal is egyben.

Út: Olyan séta, ahol minden csúcs különbözik. Az út mindig nyílt.

Pl.: A fenti 8 hossz hosszú séta nem út, hiszen a középső csúcs kétszer is szerepel.

Nyílt séta/vonal: Ha a kezdő és a végpont különbözik. [$v_0 \neq v_n$]

Zárt séta/vonal: Ha a kezdő és a végpont megegyezik. [$v_0 = v_n$]

Kör: Legalább 1 hosszú zárt vonal, ha a csúcsok különbözőek, kivéve az elsőt és az utolsót [v_0 és v_n].

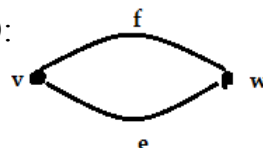
Példák körökre:

1 hosszú kör (**hurokél**):



v, e, v

2 hosszú kör (**párhuzamos élek**):



v, e, w, f, v

3 hosszú kör (**háromszög**)

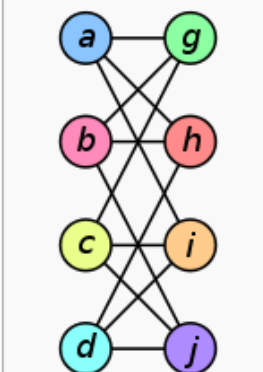
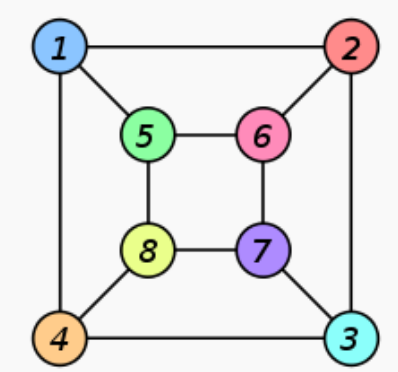
4 hosszú kör (**négyszög**)

Gráfok izomorfája: Legyen $G = (V, E)$ és $G' = (V', E')$ két gráf!

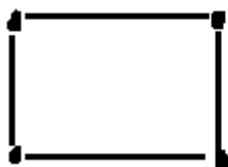
Ez a két gráf akkor izomorf egymással, ha van olyan E -t E' -re leképező f **bijekció** (kölsönösen egyértelmű leképezés), és V -t a V' -re leképező olyan g **bijekció**, hogy minden $e \in E$ -re és $v \in V$ -re e pontosan akkor illeszkedik v -re, ha $f(e)$ **illeszkedik** $g(v)$ -re.

Jele: $G \cong H$.

Pl.:

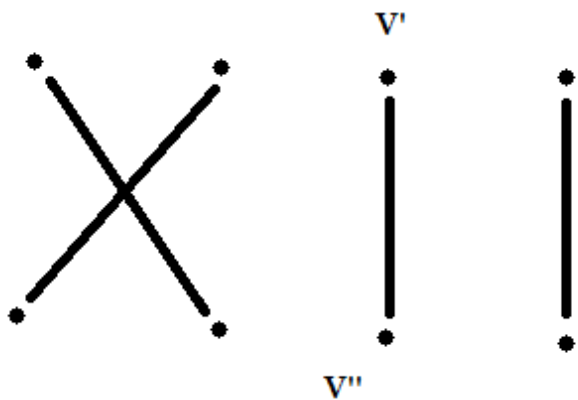
$G = (V, E)$	$G' = (V', E')$	$f : V \rightarrow V'$
		$f(a) = 1$ $f(b) = 6$ $f(c) = 8$ $f(d) = 3$ $f(g) = 5$ $f(h) = 2$ $f(i) = 4$ $f(j) = 7$

Illetve ezek is izomorfak.



Páros gráf: Egy gráf páros, ha a csúcsok V halmazának van olyan V' és V'' diszjunkt részhalmaza ($V' \cup V'' = V$ és $V' \cap V'' = \emptyset$), és minden él egyik végpontja V' -ben, a másik V'' -ben van.

Pl.: $V' = \text{tanárok}$, $V'' = \text{órák}$, a gráf pedig maga az órarend.

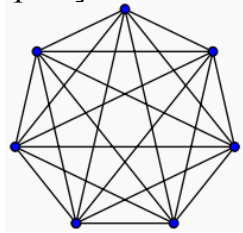


Speciális gráfok:

- K_n : n csúcspontú teljes gráf! (minden csúcs össze van kötve mindegyikkel)

[K – komplett]

Pl.: K_7



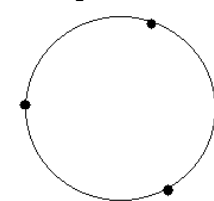
- P_n : n hosszú út [P – path]

Pl.: P_2



- C_n : n hosszú kör [C – circle]

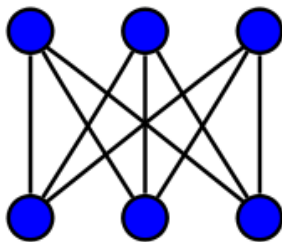
Pl.: C_3



- $K_{m,n}$: m illetve n csúcspontból álló teljes páros gráf

Pl.: $K_{3,3}$ vagyis a **három ház – három kút gráf**

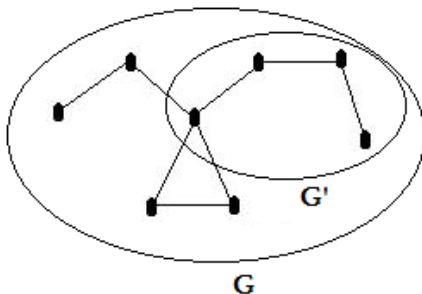
Házak



Kútak

Részgráf: Egy $G' = (\varphi', E', V')$ gráf részgráfja $G = (\varphi, E, V)$ -nek, ha $V' \subseteq V$, $E' \subseteq E$, és $\varphi' \subseteq \varphi$

Pl.:



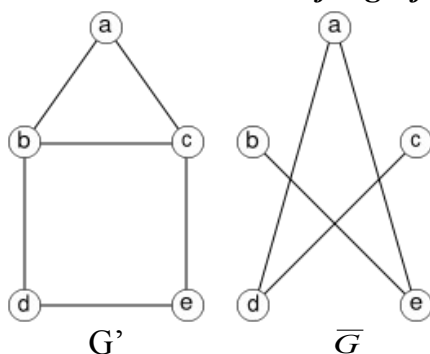
Komplementer: Ha G' részgráfja G -nek, akkor G' -nek a G -re vonatkozó komplementere:

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

($\varphi|_{E \setminus E'}$: leszűkítjük φ értelmezési tartományát $E \setminus E'$ -re)

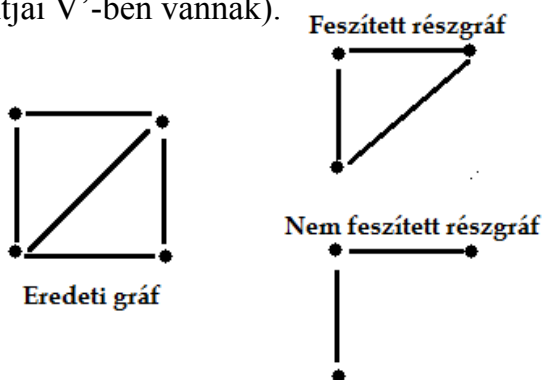
Ha G' egyszerű gráf, és csak simán komplementert említünk, akkor a G' **csúcshalmazán értelmezett teljes gráf komplementére** gondolunk.

Pl.:



Feszített (telített) részgráf: G' a G feszített részgráfja, ha a G' -beli csúcsok között levő összes G -beli élt tartalmazza (azaz G' mindazokat az éleket tartalmazza, amelyek végpontjai V' -ben vannak).

Pl.:



Tétel: Ha v -ből vezet séta v' -be, akkor út is vezet v -ből v' -be.

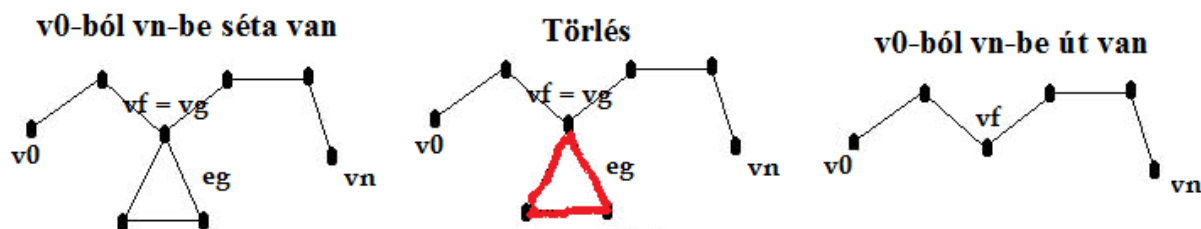
Bizonyítás: v -ből v' -be vezető séta így néz ki:

$v_0, \dots, v_f, v_f \dots v_g, v_g, \dots, v_n$

Legyen $f < g$, és $v_f = v_g$.

Ekkor ez a $v_f \dots v_g$ pazarlás, ezt egyszerűen ki lehet törölni a gráfból!

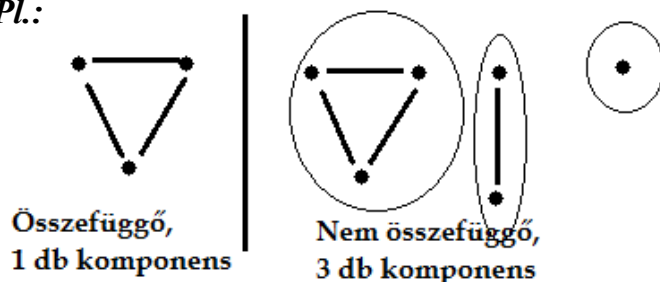
Így a séta hossza minden ilyen lépéssel csökken, és a végén már nem lesznek $v_f = v_g$ csúcsok, tehát egy utat kapunk (azaz minden csúcs különböző lesz).



Következtetés: A „ v -ből vezet út w -be” reláció **transzitiv** (hisz ha v -ből vezet út w -be, és w -ből is x -be, akkor v -ből is vezet út x -be), **szimmetrikus** (hisz ha v -ből vezet út w -be, akkor w -ből is vezet út v -be), és **reflexív** (hisz v -ből vezet út v -be, méghozzá a nulla hosszúságú út), tehát ez egy **ekvivalenciareláció**. Így ez meghatároz egy **osztályozást**. Az egy ilyen osztály által meghatározott feszített részgráf a gráf egy **komponense**.

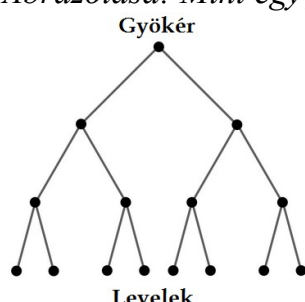
Összefüggő gráf: Ha bármely csúcsából el lehet jutni bármelyikbe (azaz bármely két csúcs összeköthető sétával). Ez azzal ekvivalens, hogy **csak 1 db komponense** van.

Pl.:



Fa: Egy gráf fa, ha összefüggő és nincs benne kör.

Ábrázolása: Mint egy fa fejjel lefelé.



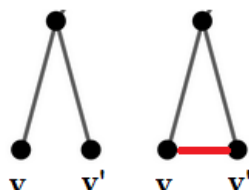
Tétel: Egy egyszerű G gráfra a következők ekvivalensek.

- 1.) G fa
- 2.) G összefüggő, de bármely él törlésével kapott részgráf már nem összefüggő.
- 3.) Minden v, v' csúcsra igaz, hogy pontosan egy út vezet v -ből v' -be
- 4.) G körmentes, de ha hozzáveszek egy új élt, akkor már nem lesz körmentes.

Bizonyítás: Azt kell bizonyítani, hogy 1-esből következik a 2-es, 2-esből a 3-as, 3-asból a 4-es, 4-esből pedig az 1-es! ($1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$)

- $1 \Rightarrow 2$: Ha G fa, akkor összefüggő is (lásd a fa definícióját).

Indirekt bizonyítás: Tegyük fel, hogyha a fából törölünk egy $v-v'$ élt, akkor továbbra is összefüggő marad, azaz létezik út v -ből v' -be. Ha viszont visszarájzolom ezt a kitörölt $v-v'$ élt, akkor kör keletkezik. De mivel a fában nem lehet kör, ez így ellentmondás. Mivel ez egy indirekt bizonyítás, így bizonyítottuk az állítást.

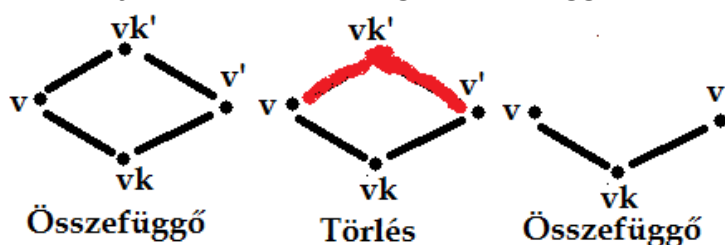


- $2 \Rightarrow 3$: *Indirekt bizonyítás:* Tegyük fel, v -ből v' -be két különböző út is vezet.

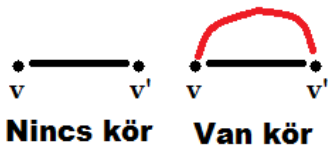
Legyen k az a legkisebb index, ahol már $v_k \neq v'_k$ (azaz szétvált az út).

Az egyik út: v, v_k, v' , a másik pedig $v, v_{k'}, v'$

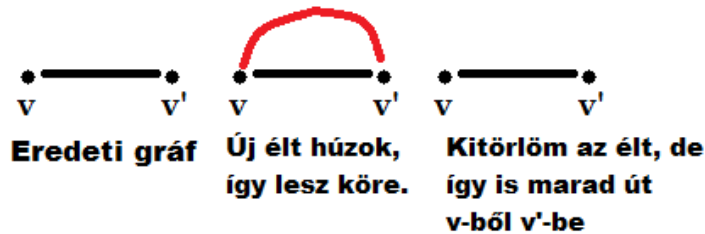
Bármely utat töröljük a kettő közül, a gráf összefüggő marad, ellentmondás!



3 \Rightarrow 4 : Ha pontosan egy út vezet v -ből v' -be, akkor biztos, hogy nincs kör a gráfban.
 Ha pontosan egy út vezet v -ből v' -be, és felveszek egy újabb élt, akkor biztosan kör keletkezik, azaz nem lesz körmentes a gráf.



4 \Rightarrow 1 : Ha G körmentes, akkor az már csak az összefüggőség tulajdonság kell a fához!
 Akkor lesz összefüggő, ha bármely v csúcsból vezet út bármely v' csúcsba.
 Tudjuk (4-es pont), hogyha egy új élt húzunk a gráfba, akkor már lesz köre. Ha viszont azt új élt töröljük, akkor még marad egy út v -ből v' -be, tehát teljesül az összefüggőség feltétele. Mivel G gráf összefüggő és körmentes, így biztosan fa is.

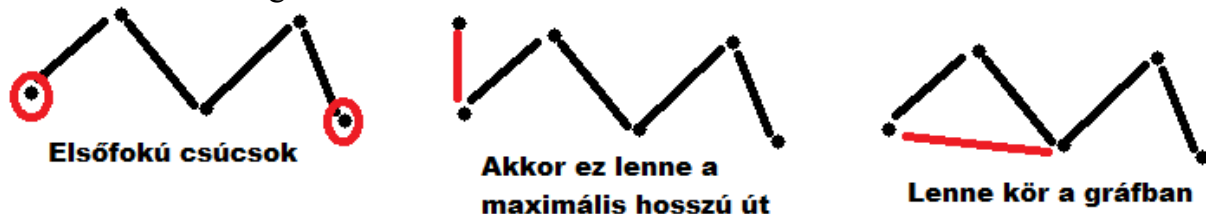


Tétel: G véges n csúcsú gráfra az alábbi állítások ekvivalensek.

- 1.) G fa
- 2.) G -ben nincs kör és $n-1$ éle van.
- 3.) G -ben összefüggő, és $n-1$ éle van.

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

Bizonyítás: Vegyük a gráfban a leghosszabb utat. Ennek az útnak a két végpontja biztosan elsőfokú csúcs. Ugyanis, ha nem lenne elsőfokú, akkor lenne még éle. Ha viszont ez a plusz él egy úton kívüli csúcshoz mutatna, akkor nem a maximális hosszúságú utat vettük volna, ha pedig egy úton belüli csúcshoz mutatna, akkor nem lenne körmentes a gráf.



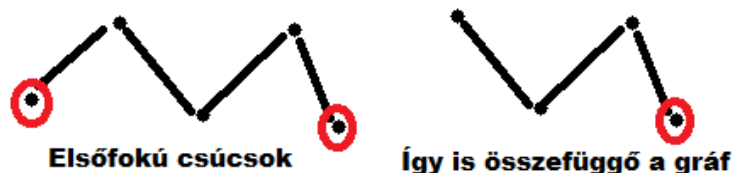
Tétel: Ehhez használjuk fel az előző segédteételt!

G véges n csúcsú gráfra az alábbi állítások ekvivalensek.

- 1.) G fa
- 2.) G -ben nincs kör és $n-1$ éle van.
- 3.) G -ben összefüggő, és $n-1$ éle van.

Bizonyítás: Azt kell bizonyítani, hogy $1 \Rightarrow 2$ -esből következik a 2-es, 2-esből a 3-as, a 3-asból pedig az 1-es! ($1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$)

- $1 \Rightarrow 2$: Mivel G fa, így a definíció szerint nincs benne kör.
Teljes indukció: $n=1$ -re igaz! (hisz ha a csúcsok száma n (1), akkor ahhoz $n-1$ (0) él fog tartozni, mert nem lehet a gráfban hurokél, hisz az már kört alkotna.
 $n>1$ élnél a fenti segédteétel miatt biztos van elsőfokú csúcs. Ha azt a hozzá tartozó éllel együtt eltávolítjuk a gráfból, akkor az így kapott gráf még mindig fa lesz, és $(n-1)$ csúcsa, valamint $(n-2)$ éle lesz (a teljes indukció miatt). Ha a törölt élt visszarajzoljuk, akkor pontosan $(n-1)$ él lesz a gráfban.
- $2 \Rightarrow 3$: *Teljes indukció:* $n=1$ -re igaz! (hisz ha a csúcsok száma n (1), $n-1$ (0) él van benne, és körmentes, akkor biztosan összefüggő is.
 $n>1$ élnél a fenti segédteétel miatt biztos van elsőfokú csúcs. Ha azt a hozzá tartozó éllel együtt eltávolítjuk a gráfból, akkor összefüggő gráfot kapunk (az indukciós feltétel miatt).



- $3 \Rightarrow 1$: Ha G összefüggő, akkor csak a körmentességet kell bizonyítani, és fa lesz.
 Ha nem lenne körmentes a gráf, akkor egyesével távolítsunk el a körökből egy-egy élet úgy, hogy a gráf összefüggő maradjon. Folytassuk ezt addig, amíg már nem marad kör. Így tehát k él törlése után egy fát kaptunk, aminek nyilván $(n-1)$ éle van (lásd $1 \Rightarrow 2$ pont). De abból indultunk ki (3.) pont), hogy alaphoz $n-1$ élünk van, ez pedig úgy lehetséges, ha $k=0$, azaz nem töröltünk ki egy élt sem, tehát eredetileg is fánk volt.

Feszítőfa: G gráfnak G' részgráf a feszítőfája, ha fa és az összes G -beli csúcsot tartalmazza.



Állítás: Minden összefüggő véges gráfnak van feszítőfája.

Bizonyítás: Ha van a gráfban kör, akkor töröljük ki az egyik élét. Ezt ismételve végül összefüggő körmentes gráfot, azaz feszítőfát kapunk.

Tétel: Ha egy G összefüggő véges gráfnak n csúcsa és e éle van, akkor van benne legalább $(e-n+1)$ olyan kör, amelyeknek az élhalmaza különböző.

Élhalmaza különböző: Ez azért kell a tételbe, hogy egy ilyen kört csak 1 db körnek nézzünk, és ne 6 különbözőnek! Mert alapesetben attól függően, hogy melyik csúcsból indulunk ki, és hogy merrefelé haladunk 6 különböző kört kaphatunk.



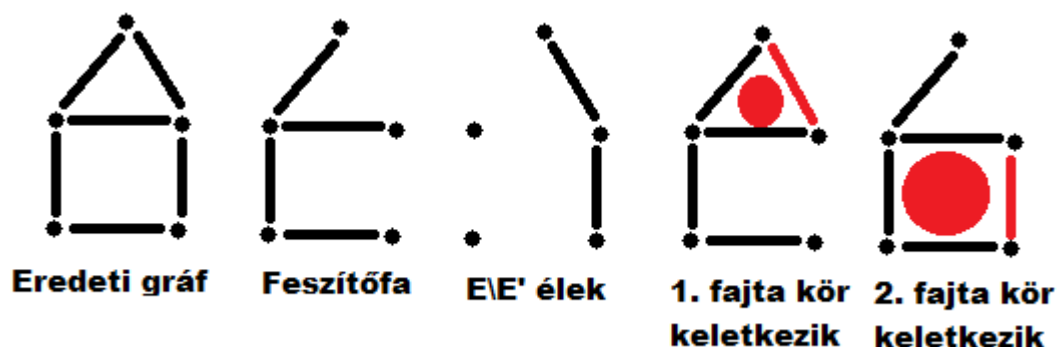
Bizonyítás: Vegyünk egy feszítőfát, ennek az éleit jelölje E' ($n-1$ éle van, hisz fa). A gráf éleinek halmazát jelöljük E -vel (e éle van).

Így $E \setminus E'$ elemszáma: $e - (n-1) = e - n + 1$

Egy $e \in E \setminus E'$ élt hozzávéve a feszítőfához kör keletkezik.

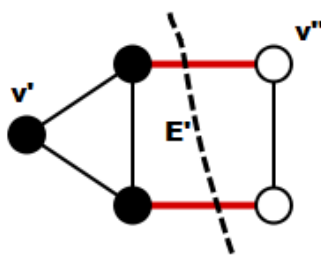
Ezek különböző e -re más és más körök, és mivel összesen $(e-n+1)$ különböző $e \in E \setminus E'$ él van, így legalább $(e-n+1)$ különböző kört kapunk.

Például: Itt $n=5$, $e=6$, és legalább $e-n+1=2$ különböző kör keletkezik.



Legyen $G = (\varphi, E, V)$ gráf, $v', v'' \in V$ pedig csúcsok!

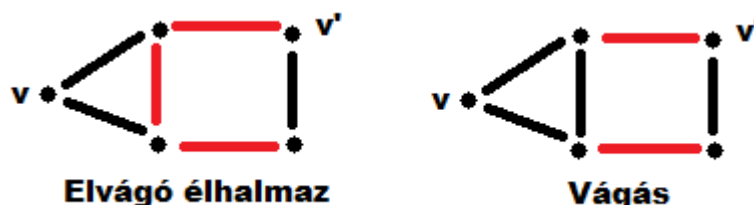
Egy $E' \subseteq E$ élhalmaz **elvága** v' -t és v'' -t, ha minden v' -ből v'' -be vezető úton szerepel valamelyik E' -beli él.



$V' \subseteq V$ csúcsalmaz **elvágó csúcsalmaz**, ha minden v' -t v'' -vel összekötő úton szerepel valamelyik V' -beli csúcs.

E' élhalmaz **elvágó élhalmaz**, ha van olyan v' és v'' csúcs, amiket elvág.

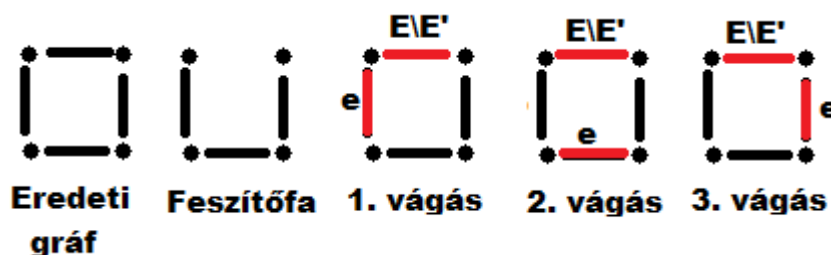
Egy elvágó élhalmaz **vágás**, ha nincs olyan valódi részhalmaza, ami elvágó halmaz.



Tétel: Egy n csúcsú véges összefüggő gráfban van legalább $n-1$ különböző vágás.

Bizonyítás: Legyen F a gráf fészítőfája, éleinek halmazát pedig jelöljük E' -vel. $e \in E'$ pedig legyen a gráf egyik éle. Készítsünk olyan vágást, ami F élei közül csak e -t tartalmazza. Ha ezt az e -t elhagyjuk F fészítőfából, akkor az két komponensre esik szét. A vágáshoz e -n kívül vegyük még hozzá az összes E' -n kívüli élt, ami ezt a két komponenst összeköti. Tehát így $e \in E'$ élenként egy darab különböző vágást kapunk. Mivel F fészítőfa, így $n-1$ éle van, tehát legalább $n-1$ darab különböző vágás lesz.

Például: $n=4$ csúcsú véges összefüggő gráfnál, legalább $n-1=3$ különböző vágás lesz.



Erdő: Körmentes gráf, de nem feltétlenül összefüggő. A fák erdők is egyben, hisz körmentesek.



Fészítőerdő: Egy erdő minden komponense fa. G gráf G' részgráfját G fészítőerdejének nevezzük, ha G' minden komponense G adott komponensének a fészítőfája.

Euler-vonal: Olyan vonal v csúcsból v' csúcsba, amely a gráf minden élt pontosan egyszer érinti. Nem minden gráfban van.

Pl.: Le tudod rajzolni a ceruza felemelése nélkül? = Van-e a gráfban Euler-vonal?

Ha pontosan két csúcs fokszáma páratlan, az összes többi pedig páros, akkor biztosan van a gráfban nyílt Euler-vonal.

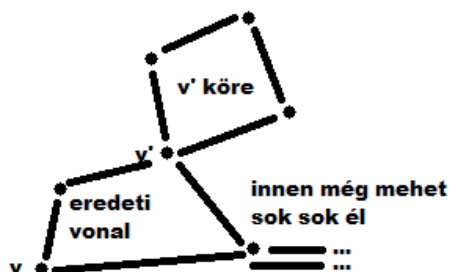
Tétel: Egy véges összefüggő gráfban pontosan akkor létezik zárt Euler-vonal, ha minden csúcs páros fokszámú. Ha a páratlan fokú csúcsok száma $2s$, akkor a gráf s darab páronként éldiszjunkt nyílt vonal (azaz nincs közös élük) egyesítése.

Bizonyítás:

1.) Ha a gráfban minden csúcs fokszáma páros, akkor van benne zárt Euler-vonal.

Induljunk ki abból az esetből, hogy egy 1 db csúcsunk (v) és 0 élünk van. Az egyetlen csúcsunk fokszáma 0 (ami páros), és bizony van is a gráfban zárt Euler-vonal (a nulla hosszúságú vonal).

Ha több mint 0 él van a gráfunkban, akkor a gráf összefüggősége miatt lesz olyan v' csúcs, ahova vezet még fel nem használt él. Induljunk el ebből a v' csúcsból és haladjunk folyamatosan a fel nem használt éleken. Mivel minden csúcs fokszáma páros, egy idő után visszaérkezünk v' -be. Ha most az eredeti vonalon elmegyünk v -ből v' -be, majd végigmegyünk a v' körén, majd az eredeti vonalon haladunk tovább, akkor az eredeti vonalnál hosszabb zárt vonalat kapunk. Ezt a módszert egészen addig alkalmazzuk, amíg van a gráfban fel nem használt él. Mivel minden csúcs fokszáma páros, egy idő után nem marad fel nem használt él, és megkapjuk a zárt Euler-vonalat.

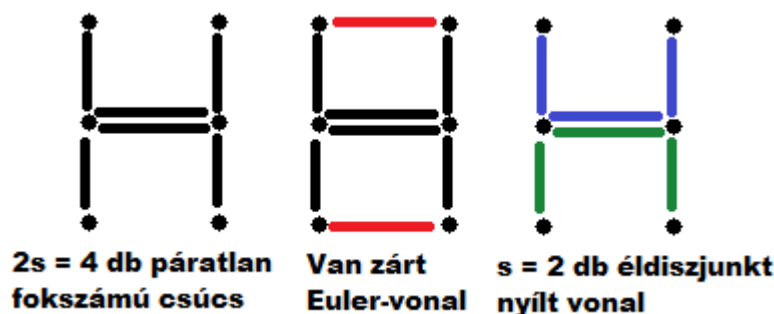


2.) Ha létezik zárt Euler-vonal, akkor minden csúcs fokszáma páros.

Mivel a zárt Euler-vonal a gráf minden csúcsát érinti, így minden csúcsnál kell lennie egy „bemenő élnek” és egy „kimenő élnek”. Így biztosan minden csúcshoz páros számú él tartozik, azaz minden csúcs fokszáma is páros.

3.) Ha a páratlan fokú csúcsok száma $2s$, akkor a gráf s darab páronként éldiszjunkt nyílt vonal (azaz nincs közös élük) egyesítése.

Kössük össze a páratlan fokszámú csúcsokat egymással. Így minden csúcs fokszáma páros lesz, és a gráfban lesz Euler-vonal. Ebből töröljük ki az s darab most behúzott élt, így a gráf s darab nyílt vonalra esik szét.



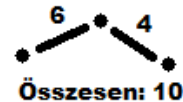
Hamilton út/kör: Olyan út/kör a gráfban, amelyben a gráf minden csúcsa pontosan egyszer szerepel. A megtalálására és a létezésére nincs tétel/kritérium.

Utazó ügynök problémája: Minimális súlyú Hamilton-kör megtalálása egy gráfban.

Címkézett gráfok: Ha adott egy $G(\varphi, E, V)$ gráf, a C_e és C_v halmazok (élcímkek illetve csúcscímkek halmaza), valamint a $c_e: E \rightarrow C_e$ és $c_v: V \rightarrow C_v$ leképezések (élcímkézés illetve csúcscímkézés), akkor a $(\varphi, E, V, c_e, C_e, c_v, C_v)$ hetest címkézett gráfnak nevezzük.

Súlyozott gráfok: Gyakori, hogy $C_e = \mathbf{R}$ és $C_v = \mathbf{R}$, ekkor élsúlyozásáról és élsúlyozott gráfról, illetve csúcssúlyozásról és csúcssúlyozott gráfról beszélünk, a jelölésből pedig elhagyjuk C_e -t és C_v -t.

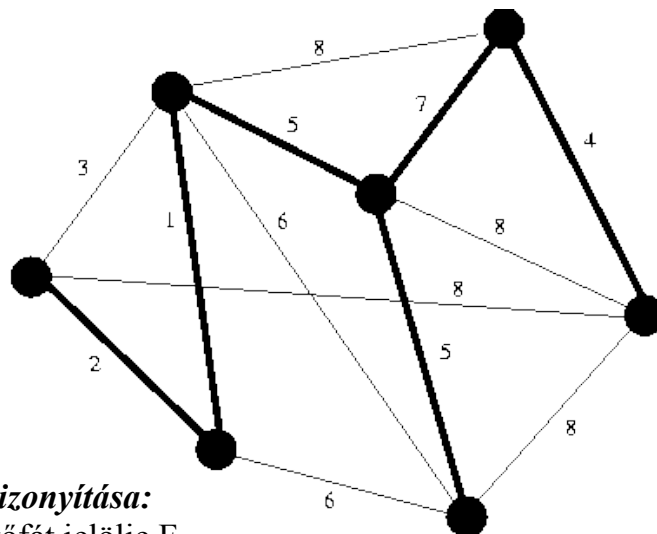
Véges élhalmaz súlya: Egy $G(\varphi, E, V, w)$ élsúlyozott gráfban egy $E' \subset E$ véges élhalmaz súlya: $w(E') = \sum_{e' \in E'} w(e')$ (az élek súlyának összege)



Véges csúcshalmaz súlya: Egy $G(\varphi, E, V, w)$ csúcssúlyozott gráfban egy $V' \subset V$ véges csúcshalmaz súlya: $w(V') = \sum_{v' \in V'} w(v')$ (a csúcsok súlyának összege)

Kruskal algoritmusa: Megtalálja az adott összefüggő és élsúlyozott gráfban (súlyok ≥ 0) a minimális összsúlyú feszítőfát. (pl. városok között kell megépíteni a legkisebb összköltségű villamos vezetékhálózatot).

Kiindulunk az összes csúcst tartalmazó üres gráfból (egy él sincs benne), és minden lépésben berajzoljuk azt a minimális súlyú élt, amellyel még nem keletkezik a gráfban kör. Ez véges sok lépés után kirajzolja a minimális összsúlyú feszítőfát.



Algoritmus helyességének bizonyítása:

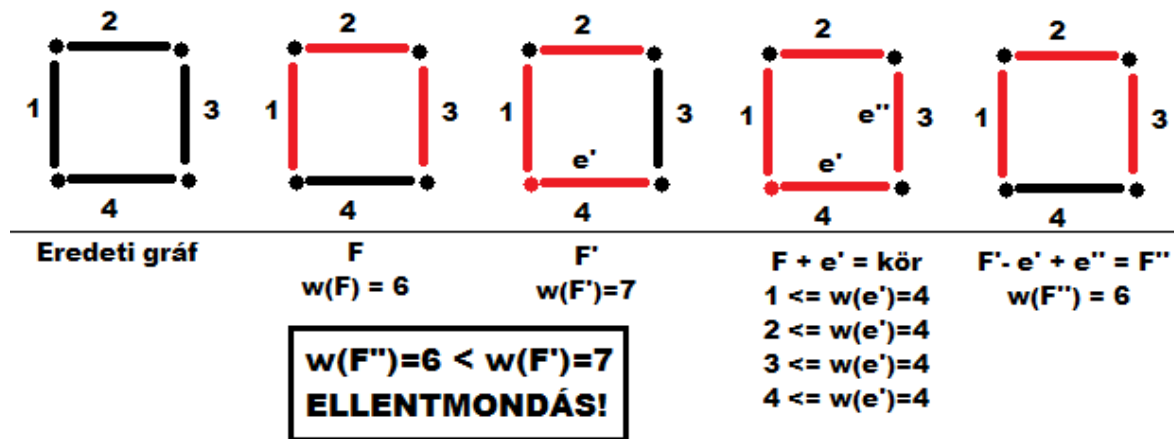
A minimális összsúlyú feszítőfát jelölje F .

Indirekt bizonyítás: Legyen F' F -nél is kisebb összsúlyú feszítőfa. Olyan F' -et válasszunk, amelyiknek a lehető legtöbb közös éle van F -el.

e' jelölje F' egy olyan élét, amely F -ben nem szerepel. Ha F -hez hozzávesszük e' -t is, akkor kört kapunk. A kör minden e élére igaz, hogy: $w(e) \leq w(e')$, hisz különben e' -t választotta volna az algoritmus.

Most F' -ből hagyjuk el e' -t, és adjuk hozzá a kör azon e'' élét, amivel $(F' - e' + e'')$ (jelölje F'') fa lesz. Így ellentmondást kapunk, hisz F'' súlya kisebb lesz, mint F' -é (pedig a feltevésünk szerint F' a legkisebb összsúlyú feszítőfa), vagy ugyanakkora súlyú, de több közös éle van F -el, mint F -nek (ez is ellentmondás).

Például:



Mohó algoritmus: Kruskal algoritmus is ilyen, ezek az adódó lehetőségek közül minden lépésben a legkedvezőbbet választják, nem gondolkodnak előre.

A mohó algoritmus nem minden esetben adja meg a helyes megoldást, például már egy 4 csúspontú teljes gráfban sem feltétlenül tudja megtalálni a minimális súlyú Hamilton-kört.

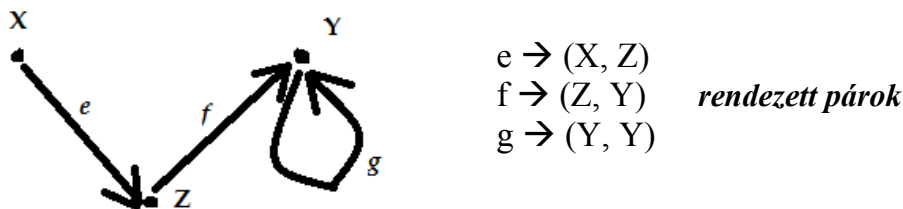
Irányított gráf: $G = (\psi, E, V)$ hármas

E: Élek halmaza [E – edge]

V: Csúcsok halmaza [V – vertex, vertices]

ψ : Illeszkedési leképezés: $E \rightarrow V \times V$ -be képi (Descartes-szorzat, azaz rendezett párok)

Pl.:



Ugyanúgy van, mint az irányítatlan gráfoknál: izomorfia, séta, út, vonal, kör, részgráf.

Csúcs kifoka: Azon élek száma, amelyeknek a csúcs a kezdőpontja. Jele: $d^+(v)$

Csúcs befoka: Azon élek száma, amelyeknek a csúcs a végpontja. Jele: $d^-(v)$

Állítás: Egy véges irányított gráfban a csúcsok befokának és kifokának összege megegyezik egymással, illetve az élek számával.

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

(Minden újabb él megrajzolása a gráfba mindhárom összeget eggyel növeli).

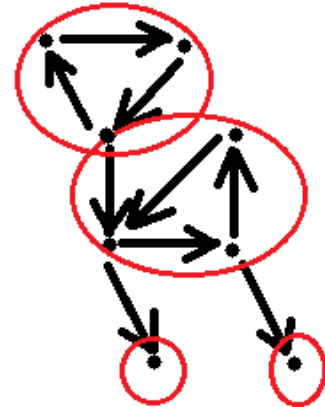
Összefüggőség irányított gráfoknál:

Az „ u csúcsból vezet út v csúcsba, és v csúcsból is vezet út u -ba” reláció ekvivalenciareláció, hisz reflexív, szimmetrikus és tranzitív (indoklás lásd az irányítatlan gráfok összefüggősége). Így meghatároz egy osztályozást is.

Egy ilyen osztály által feszített részgráf a gráf **erős komponense** (azaz az erősen komponensen belüli csúcsok kölcsönösen elérhetők egymásból).

Ha csak egy darab erős komponense van a gráfnak, akkor a gráf **erősen összefüggő** (azaz bármely két csúcs kölcsönösen elérhető egymásból).

Például ebben a gráfban 4 darab erős komponens van.



Irányított fa:

Az irányított fákban minden él egy irányba vezet.

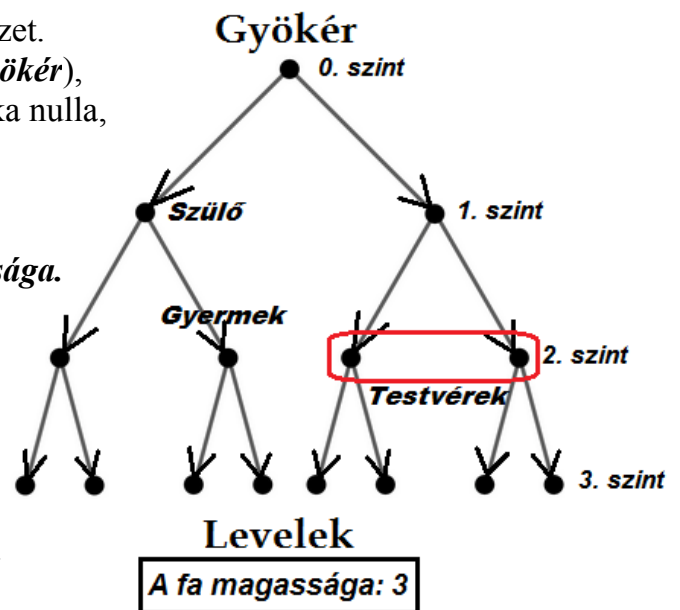
Van egy csúcs, aminek a befoka nulla (ez a **gyökér**), a többié egy. Azok a csúcsok, amiknek a kifoka nulla, azok a fa **levelei**.

Minden csúcsba pontosan egy darab út vezet a gyökértől, ezek hossza a **csúcs szintje**.

A csúcsok szintjeinek maximuma a **fa magassága**.

Ha v -ből vezet irányított út v' -be, akkor v a v' **szülője**, v pedig a v' (egyik) **gyereke**.

Ha v' és v'' szülője is v , és $v' \neq v''$, akkor v' és v'' testvérek.

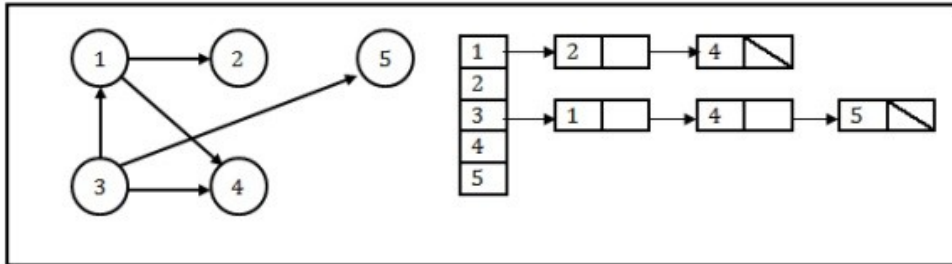


Bináris fa: Minden csúcs kifoka legfeljebb 2 (azaz maximum 2 gyereke lehet egy csúcsnak).

q -áris fa: Minden csúcs kifoka legfeljebb q (azaz maximum q gyereke lehet egy csúcsnak).

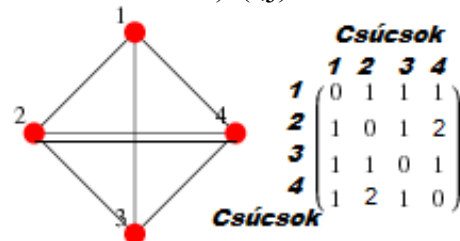
Gráfok tárolása:

- 1.) **Él-listás ábrázolás:** A csúcsok beolvasásakor minden csúcsnak adunk egy sorszámot, és egy táblázatban eltároljuk a sorszámozást. Minden csúcshoz felépítjük azon élek listáját, amelyeknek ez a csúcs a kezdőpontja.

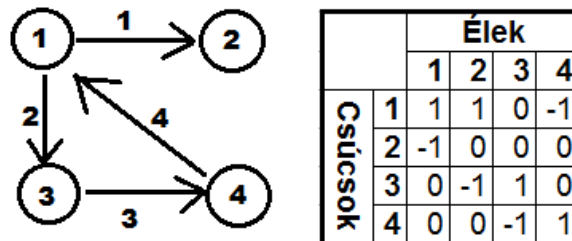


2.) Mátrixos ábrázolás:

- **Szomszédsági (adjacencia) mátrix:** A gráf csúcsait megszámozzuk, majd a mátrix (aminek mindkét oldalán a csúcsszámok vannak) (i,j) -dik elemében azt tároljuk el, hogy az i -dik és a j -dik csúcs között hány él van.

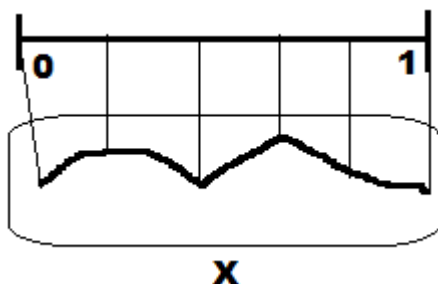


- **Illeszkedési (incidencia) mátrix:** A gráf éleit és csúcsait is megszámozzuk, majd a mátrix (aminek vízszintes oldalán az élszámok, függőleges oldalán pedig a csúcsszámok vannak) (i,j) -dik elemébe $(+1)$ -t írunk, ha az i -dik élnek a j -dik csúcs a kezdőpontja, és (-1) -t, ha az i -dik élnek a j -dik csúcs a végpontja. Irányítatlan gráfoknál a (-1) -ek helyére is $(+1)$ -ek kerülnek.



Gráfok lerajzolhatósága:

$X \subseteq \mathbb{R}^n$ (n dimenziós tér egy részhalmaza) esetén egy X -beli **görbe** egy $\gamma: [0,1] \rightarrow X$ folytonos függvény. (Azaz egy olyan görbe vonal, ami sehol sem szakad meg.)



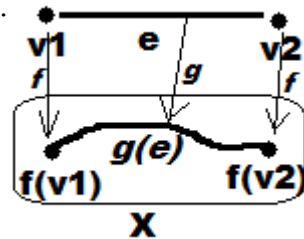
Egyszerű görbe: Olyan $\gamma:[0,1] \rightarrow X$ folytonos függvény, amelynek legfeljebb a kezdő és végpontja egyezik meg (azaz sehol sem metszi önmagát).

Egy $G = (\psi, E, V)$ irányított **gráf lerajzolása** X -ben egy (f,g) rendezett pár, ahol:

f: $V \rightarrow X$ injektív függvény (csúcsok pozíciója a síkon)

g: $E \rightarrow \{\text{görbék halmaza}\}$ (e él $\rightarrow g_e$ egyszerű görbe)

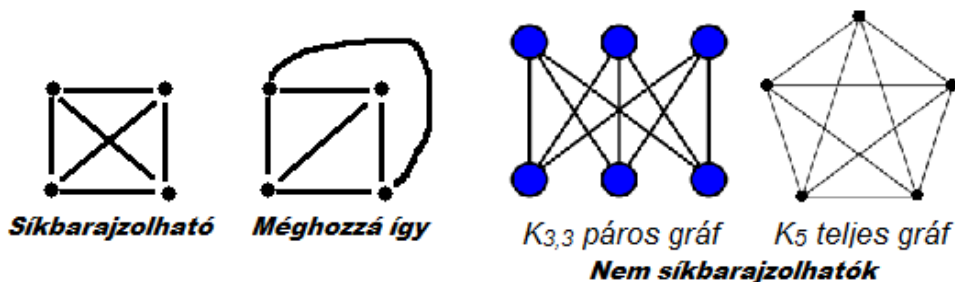
és a $g_e \subset]0, [1$ görbék egymástól és az $\text{rng}(f)$ -től is diszjunktak (azaz nem metszhetik se önmagukat, se egymást).



Például: Mi szabályos lerajolás és mi nem?



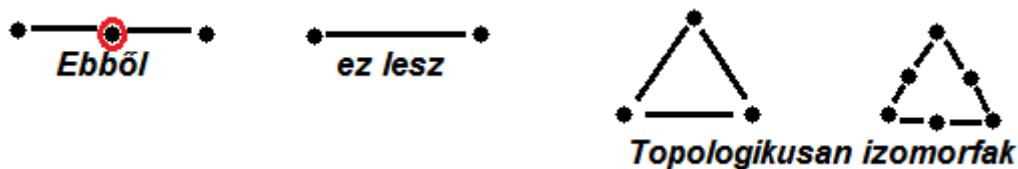
Ha G gráfnak van \mathbb{R}^2 -be (síkba $[x,y]$ koordináta) rajzolása, akkor G **síkbarajzolható**.



G_1 és G_2 gráfok **topologikusan izomorfak**, ha az alábbi lépést vagy a fordítottját véges sokszor elvégezve egyik gráfot át lehet alakítani a másikká.

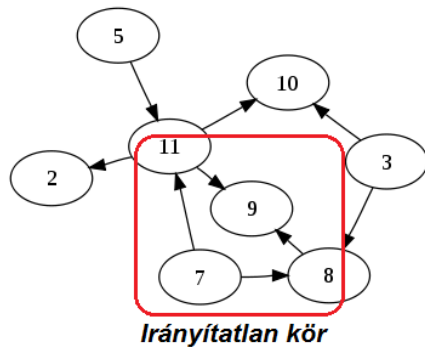
Lépés: Egy másodfokú csúcsot letörlök, és a szomszédjait egy új éllel összekötöm.

Fordítottja: Egy élt kettéválasztok, és berakok közé egy másodfokú csúcsot.

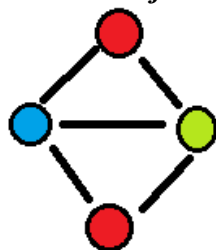


Kuratowski tétele: Egy gráf pontosan akkor síkba rajzolható, ha nem tartalmaz se a $K_{3,3}$ páros gráffal, se a K_5 teljes gráffal topologikusan izomorf részgráfot.

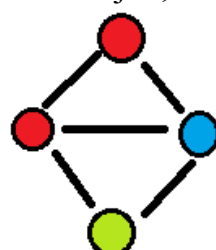
Irányított körmentes gráf (DAG Directed acyclic graph): Olyan irányított gráf, amely nem tartalmaz kört. (Nem egyenlő a fával, mert irányítatlan kör lehet benne.)



Egy gráf csúcsainak színezését **jólszínezésnek** hívjuk, ha a szomszédos csúcsok színe mindig különböző.



Jólszínezés



Nem jólszínezés

Egy gráf **k színnel színezhető**, ha van olyan jólszínezése, ami legfeljebb k színt használ. Azt a legkisebb $k \in \mathbb{N}$ számot, melyre a gráf k színnel színezhető, a gráf

kromatikus számának nevezzük. Jelölése: $\chi^{(G)}$ (khi betű)

Állítás: G páros gráf $\Leftrightarrow \chi^{(G)} = 2$

Négyszíntétel

Minden síkbarajzolható gráf $\chi^{(G)} \leq 4$ (azaz legfeljebb 4 színnel jólszínezhető).

[Ez az első számítógéppel bizonyított matematikai tétel. Azt kellett bizonyítani, hogy minden térkép kiszínezhető legfeljebb 4 színnel. Be is lett bizonyítva]

Csoportok

Csoport: $(G, *)$ pár csoport, ha:

- $*$ binér (kétváltozós) művelet G -n (két G -beli elemhez egy G -beli elemet rendel)
- $*$ asszociatív (szabadon zárójelezhető)
- van semleges eleme ($s * g = g$ illetve $g * s = g$)
- minden elemnek van inverze ($g * g^{-1} = s$ illetve $g^{-1} * g = s$)

Abel-csoport: Ha $(G, *)$ pár csoport és $*$ kommutatív művelet G -n.

Példák Abel-csoportokra:

$(\mathbb{Z}, +)$

- két egész szám összege egész szám
- $a + (b + c) = (a + b) + c$
- semleges elem a 0: $a + 0 = a$
- inverz az ellentett: $a + (-a) = 0$
- kommutatív: $a + b = b + a$

$(\mathbb{R}^+, *)$

- két \mathbb{R}^+ szám szorzata is \mathbb{R}^+ szám
- $(a * b) * c = a * (b * c)$
- semleges elem az 1: $a * 1 = a$
- inverze a reciproka: $a * (1/a) = 1$
- kommutatív: $a * b = b * a$

Részcsoporthoz: $(G, *)$ csoportnak H a részcsoporthoz, ha $H \subseteq G$ és a $*$ művelet csak H elemein értelmezve (leszűkítve H -ra) is csoportot alkot. Jele: $H \leq G$

Például: $(\text{Páros számok}, +) \leq (\text{Egész számok}, +)$

[Hisz a páros számok az egész számok részhalmaza, és a páros számok az összeadással csoportot alkotnak (páros számok összege páros szám, az összeadás asszociatív, semleges elem a 0 (páros szám), inverz az ellentett (páros szám ellentettje páros)).]

Művelettartó leképezés: Legyen X és X' két halmaz. Legyen $*$ binér művelet X -en, $'$ pedig binér művelet X' -en. Egy $f: X \rightarrow X'$ leképezést művelettartónak nevezünk, ha $f(x * y) = f(x) *' f(y)$ minden $x, y \in X$ -re.

Legyen adott $(G_1, *)$ és $(G_2, ')$ csoportok. Egy $f: G_1 \rightarrow G_2$ művelettartó leképezést **homomorfizmusnak** nevezünk, és $f(G_1)$ -et pedig G_1 **homomorf képének** nevezzük.

Ha f homomorfizmus bijektív, akkor **izomorfizmus**. Jele: $G_1 \cong G_2$

Ha $f: G \rightarrow G$ alakú az izomorfizmus (azaz ugyanonnan képez ugyanoda), akkor **automorfizmus**.

Példa izomorfizmusra:

$G_1 = (\{0, 1\}, + \text{ mod } 2)$

+	0	1
0	0	1
1	1	0

$G_2 = (\{-1, 1\}, *)$

*	1	-1
1	1	-1
-1	-1	1

$f: G_1 \rightarrow G_2$ izomorfizmus! $f(0) = 1$ $f(1) = -1$

f művelettartó leképezés, hisz pl. $f(0 + 1) = f(0) * f(1)$

$f(0 + 1) = f(1) = (-1)$ és $f(0) * f(1) = 1 * (-1) = (-1)$

f injektív, hisz nem rendeli ugyanazt az értéket két különböző számhoz a függvény, és szürjektív is (hisz az 1-et és a (-1)-et is előállítja), így tehát f bijektív.

Példa homomorfizmusra (ami nem izomorfizmus):

$$G_1 = (\mathbb{Z}, +) \quad G_2 = (\mathbb{Z}_2 = \{0, 1\}, +_{\text{mod } 2})$$

f: $G_1 \rightarrow G_2$ homomorfizmus! $f(n) = \{0, \text{ha } n \text{ páros és } 1, \text{ha } n \text{ páratlan}\}$

f művelettartó leképezés, hisz pl. $f(3+6)=f(3)+_{\text{mod } 2} f(6)$

$$f(3+6)=f(9)=1 \text{ és } f(3)+_{\text{mod } 2} f(6)=1+_{\text{mod } 2} 0=1$$

f nem bijektív, hisz nem is injektív, mert pl. 2-höz, 4-hez stb. is ugyanúgy 0-t rendel.

Generátum:

1. fajta definíció:

Legyen $(G, +)$ csoport, és legyen $K \subseteq G$ (K halmaz G részhalmaza).

K generátuma: $\langle K \rangle = \{g_1 g_2 g_3 \dots g_n : n \in \mathbb{N}, g_i \in K \cup K^{-1}, i=1 \dots n\}$

Szavakkal: $\langle K \rangle$ mindazokat az elemeket tartalmazza, amelyeket K -beli elemekből elő lehet állítani az inverzképzés és G csoport művelete (jelen esetben $+$) segítségével.

Például: $G = (\mathbb{Z}, +)$

$$K = \{6, 9\} \quad K^{-1}(\text{K-beli elemek inverzei}) = \{-6, -9\}$$

$$\langle K \rangle = \{6+(-6) = 0, 9+(-6) = 3, 6=6, 9=9, 9+6+(-3) = 12, 6+(-9) = -3, 6+(-6)+(-6) = -6 \dots\}$$

$$\langle K \rangle = \{\dots -6, -3, 0, 3, 6, 9 \dots\} \text{ (azaz a 3-al osztható egész számok)}$$

2. fajta definíció:

K generátuma ($\langle K \rangle$) G -nek az a legszűkebb részcsoportja, amelynek részhalmaza K .

3. fajta definíció:

K generátuma ($\langle K \rangle$) a G összes K -t tartalmazó részcsoportjának a metszete.

Előző példa: $G = (\mathbb{Z}, +)$ és $K = \{6, 9\}$

G K -t tartalmazó részcsoportjai: $H_1 = \mathbb{Z}$ és $H_2 = \{3\text{-al osztható egész számok}\}$

$$H_1 \cap H_2 = H_1 = \{3\text{-al osztható számok}\} = \{\dots -6, -3, 0, 3, 6, 9 \dots\}$$

Tétel: Részcsoportok tetszőleges metszete is részcsoport.

(Formálisan: Ha $H_\gamma, \gamma \in \Gamma \leq G$, akkor $\bigcap_{\gamma \in \Gamma} H_\gamma \leq G$)

(Γ egy indexhalmaz, pl. $1, 2, \dots, n$)

$$\bigcap_{\gamma \in \Gamma}$$

Bizonyítás:

Legyen $H = \bigcap_{\gamma \in \Gamma} H_\gamma$ és $(G, *)$ pedig a csoport.

1.) H zárt a $*$ binér műveletre:

Legyen $g_1, g_2 \in H$ tetszőleges elemek. Mivel H a H_γ -k metszete, így g_1 és g_2 eleme minden H_γ halmaznak. Mivel H_γ részcsoport (és így zárt a $*$ műveletre), ezért $(g_1 * g_2) \in H_\gamma$. Ám mivel H a H_γ -k metszete, így $(g_1 * g_2) \in H$, tehát H is zárt a $*$ műveletre.

2.) H -ban van egységelem:

e egységelem \in minden H_γ halmaznak, mivel minden H_γ halmaz csoport. Ám mivel H a H_γ -k metszete, így e egységelem $\in H$.

3.) *H-ban minden elemnek van inverze:*

Legyen $g \in H$ tetszőleges elem. Mivel H a H_γ -k metszete, így g eleme minden H_γ halmaznak. Mivel H_γ részcsoport (és így minden elemnek van inverze), ezért létezik olyan $g^{-1} \in H_\gamma$, hogy $g * g^{-1} = e$. Ám mivel H a H_γ -k metszete, így $g^{-1} \in H$, és $g * g^{-1} = e$ H -ban is.

Például: $G = (\mathbb{Z}, +)$ és $H_1 = \{3\text{-al osztható egészek}\}$, $H_2 = \{4\text{-el osztható egészek}\}$

H_1 és H_2 részcsoportok metszete $H = \{12\text{-vel osztható egészek}\}$

$H_1 = \{\dots -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, \dots\}$

$H_2 = \{\dots -12, -8, -4, 0, 4, 8, 12, 16, 20, 24, 27, 30, 33, 36, \dots\}$

$H = \{\dots -12, 0, 12, 24, 36\}$

Legyen $g_1 = 12, g_2 = 24 \in H$. $12, 24 \in H_1$ és $12, 24 \in H_2$. $g_1 * g_2 = 12 + 24 = 36$.

$36 \in H_1$ és $36 \in H_2$, így $36 \in H$.

$e = 0$ az egységelem. $0 \in H_1$ és $0 \in H_2$, $0 \in H$.

$g = 12$ és $g^{-1} = -12$. $-12 \in H_1$ és $-12 \in H_2$, így $-12 \in H$. $12 + (-12) = 0 = e$

Ciklikus csoport:

Ha $\langle K \rangle = G$ (azaz K a teljes G -t generálja), akkor K a G csoport **generátorrendszere**.

Ha G csoportnak létezik egyelemű generátorrendszere ($K = \{g\}$ és $\langle g \rangle = G$), akkor G csoportot **ciklikusnak** nevezzük, g -t pedig G **generátorának** hívjuk.

(Jelölések: Ha $K = \{g\}$, akkor $\langle K \rangle$ helyett $\langle g \rangle$ is írható.)

Ciklikus csoport jelölése: $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$

g^n : azt jelenti, hogy a G csoport műveltét (pl. $+$ vagy $*$) n -szer elvégezzük a g elemen.

Például: $G = (\mathbb{Z}, +)$ csoport, $K = \{g\} = \langle 1 \rangle$ vagy $K = \{g\} = \langle -1 \rangle$.

Így az **1** és a **-1** is G csoport generátorai, hisz

$\langle 1 \rangle = \{1 + (-1) = 0, 1 = 1, 1 + 1 = 2, 1 + 1 + 1 = 3, \dots\}$ ill. $(-1) = -1, (-1) + (-1) = -2, \dots\}$

$\langle 1 \rangle = \{\text{az összes egész szám}\} = \mathbb{Z}$

$\langle -1 \rangle = \{(-1) + 1 = 0, (-1) = -1, (-1) + (-1) = -2, \dots\}$ ill. $1 = 1$ és $1 + 1 = 2, 1 + 1 + 1 = 3, \dots\}$

$\langle -1 \rangle = \{\text{az összes egész szám}\} = \mathbb{Z}$

Tétel: Csoport homomorf képe is csoport.

Bizonyítás: Legyen $(G_1, *)$ és $(G_2, *)$ csoportok között homomorfizmus (f függvény).

1.) *Asszociativitás teljesül a művelettartás miatt:*

$f((a+b)+c) = f(a+b)+f(c) = f(a)+f(b)+f(c)$

$f(a+(b+c)) = f(a)+f(b+c) = f(a)+f(b)+f(c)$

2.) *A homomorf képben is van semleges elem:*

Legyen g tetszőleges elem G_1 -ben, s_1 pedig a semleges elem G_1 -ben.

$f(g * s_1) = f(g)$

$f(g * s_1) = f(g) * f(s_1) = f(g) * s_2 = f(g)$

Ebből következik, hogy $s_2 = f(g) * s_2$, így s_2 semleges elem G_2 -ben.

3.) *A homomorf képben minden elemnek van inverze:*

Legyen g tetszőleges elem G_1 -ben, g^{-1} pedig g elem inverze G_1 -ben.

$f(g * g^{-1}) = f(s_1) = s_2$

$f(g * g^{-1}) = f(g) * f(g^{-1})$

Ebből következik, hogy $s_2 = f(g) * f(g^{-1})$, így $f(g)$ inverze $f(g^{-1})$ G_2 -ben.

Tétel: Ciklikus csoport homomorf képe is ciklikus csoport.

Bizonyítás: Legyen $(G_1, *)$ és $(G_2, *)$ csoportok között homomorfizmus (f függvény).

g jelölje G_1 csoport generátumát, azaz $G = \langle g \rangle = \{g^n, n \in \mathbb{Z}\}$

Legyen $g_2 \in G_2$ tetszőleges elem. Biztosan létezik olyan $g_2 \in G_2$, hogy $f(g_1) = g_2$.

Mivel g a teljes G_1 halmazt generálja, így $g_1 \in \langle g \rangle = \{g^n, n \in \mathbb{Z}\}$

Például legyen $g_1 = g^n$.

$f(g_1) = f(g^n) = f(g)^n$ a művelettartás miatt

(Magyarázat pl. $n=2$ -re: $f(g^2) = f(g * g) = f(g) * f(g) = f(g)^2$)

Így $g_2 \in f(g)^n$, az előzőek miatt pedig $g_2 \in \langle f(g) \rangle$, tehát a homomorf kép is ciklikus.

Következtetés: A generátor (g) képe ($f(g)$) generálja a homomorf képet.

Például: $G_1 = (\mathbb{Z}^+, +)$ és $G_2 = (\mathbb{Z}^+, *)$ a két csoport, f függvény pedig $f(x) = 2^x$

G_1 csoport generátuma $\langle 1 \rangle = G_1$.

Legyen például $g_2 = 16$, $f(g_1) = 16$. $2^{g_1} = 16$, így $g_1 = 4$.

$4 \in \langle 1 \rangle = \{1+1+1+1=4, \text{ azaz } n=4\}$

$f(4) = f(1+1+1+1) = f(1)*f(1)*f(1)*f(1) = 2^1*2^1*2^1*2^1 = 2^4 = 16$.

$16 \in 2^n$ ($n \in \mathbb{Z}$), azaz G_2 csoport generátuma $\langle 2 \rangle = G_2$.

A következtetés is igaz, hisz G_2 csoport generátuma valóban $\langle f(1) \rangle = \langle 2^1 \rangle = \langle 2 \rangle$

Tétel: Végtelen ciklikus csoport izomorf $(\mathbb{Z}, +)$ -al.

n elemű ciklikus csoport pedig izomorf $(\mathbb{Z}_n, +)$ -al.

Bizonyítás: Legyen $(\mathbb{Z}, +)$ és $(G, *)$ csoportok között homomorfizmus ($f(x) = g^x$).

g a G csoport generátora, azaz $\langle g \rangle = G$.

Ha belátjuk, hogy ez a homomorfizmus bijektív, akkor biztosan izomorfizmus is.

Indirekten bizonyítjuk, tegyük fel, hogy nem bijektív (nem kölcsönösen egyértelmű).

Ekkor biztosan lesznek olyan $i > j$ elemek, amikhez ugyanazt az értéket rendeli a függvény, azaz $g^i = g^j$. Jelölje e G egységelemét.

$g^i = e * g^j$. Ebből következik, hogy $e = g^{i-j}$.

Legyen r (G rendje) a legkisebb olyan pozitív egész kitevő, hogy $g^r = e$.

Ekkor igaz, hogy $G = \{g^0=e, g^1, g^2, \dots, g^j, \dots, g^i \dots g^{n-1}\}$ véges sok elem, és mind különböző.

Mivel $g^0 = e = g^r$, ezért $r = 0$. Egyrészt különböző mind, mert $0 \leq j < i \leq n-1$ esetén

$g^i \neq g^j$, hisz különben $g^{i-j} = e$ lenne, ami lehetetlen, mert akkor $i-j = r = 0$ lenne, de $i > j$. Mivel indirekt volt a bizonyítás, és láttuk, hogy $g^i \neq g^j$, bizonyított, hogy a homomorfizmus bijektív, azaz izomorfizmus.

Másrészt minden $i \in \mathbb{Z}$ szám felírható $i = k*n + j$ alakban ($i > j$ és $i \equiv j \pmod{n}$).

Tehát $g^i = g^{k*n+j} = (g^n)^k * g^j = e^k * g^j = e * g^j = g^j$.

Mivel $k*n + j < (k+1)*n$

$k*n + j < k*n + n$

$j < n$, ezért j értéke $0, 1 \dots n-1$ lehet.

Így G -nek n eleme van még hozzá: $G = \{g^0=e, g^1, g^2 \dots g^{n-1}\}$, ez pedig izomorf $(\mathbb{Z}_n, +)$ -al.

Például: $G(\{i, -i, 1, -1\} \in \mathbb{C}, *)$ ciklikus csoport izomorf $(\mathbb{Z}_4, +)$ -al f függvénnyel.

G generátuma $\langle g \rangle = \langle i \rangle$, (hisz: $i=i$, $i*i=-1$, $i*i*i=-i$, $i*i*i*i=1$)

$G = \{g^0=1, g^1=i, g^2=-1, g^3=-i\}$

(végtelenségig folytatódik ciklikusan: $g^4=1, g^5=i, g^6=-1, g^7=-i \dots$)

$f(1)=0$

$f(i)=1$

$f(-1)=2$

$f(-i)=3$

G				
*	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

\mathbb{Z}_4				
+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Izomorfizmus, hisz f bijektív (minden G elemhez más \mathbb{Z}_4 elemet rendel, és \mathbb{Z}_4 minden elemére képez).

Tétel: Ciklikus csoport minden részcsoportja is ciklikus csoport.

Bizonyítás:

Legyen $G = \langle g \rangle$ ciklikus csoport, $H \leq G$ pedig részcsoport.

Ha $H = \{e\}$, akkor már kész is vagyunk, hisz az egységelem generálja önmagát.

Egyébként pedig léteznie kell olyan $k \neq 0$, $k \in \mathbb{Z}$ -nek, hogy $g^k \in H$.

Tegyük fel, hogy $k > 0$, hisz $g^k \in H$ és $g^{-k} \in H$ ekvivalensek.

Legyen $d > 0$ az a legkisebb pozitív kivető, amire teljesül, hogy $g^d \in H$.

Ezt kell bebizonyítani: $\langle g^d \rangle = H$.

Azt tudjuk, hogyha $g^d \in H$, akkor $\langle g^d \rangle \in H$, hisz H részcsoport, tehát csoport, és így zárt az adott binér műveletre.

Azt kell belátni, hogy minden j -re igaz, hogyha: $g^j \in H$, akkor $g^j \in \langle g^d \rangle$

j számot felbonthatjuk maradékos osztásos alakban: $j = q*d + r$ ($0 \leq r < d$)

Így tudjuk, hogy: $g^j = g^{q*d+r} \in H$,

illetve, hogy mivel $g^d \in H$, így $(g^d)^q \in H$, azaz $g^{q*d} \in H$

Ha elosztom a kettőt egymással, akkor kiderül, hogy: $g^{(q*d+r) - q*d} = g^r \in H$

Ám mivel tudjuk, hogy d az a legkisebb pozitív kivető, amire teljesül, hogy $g^d \in H$ és $0 \leq r$, így biztos, hogy $r = 0$.

Így pedig $g^j = g^{q*d} = (g^d)^q \in H$

Például:

$G = (\mathbb{Z}, +) = \langle 1 \rangle$ H lehet például maga az egységeleme, azaz $H = \{e\} = 0$.

De például lehet $d = g^2 = 1+1 = 2$, azaz $H = \{\text{páros egész számok}\}$ részcsoport.

Ami igaz, hisz benne van a 0, és minden páros szám inverze az ellentettje ($-2+2=0$).

Igaz az is, hogy pl. $j = 6 = g^6$ is $\in H$.

$j = q*d + r$, azaz ebben az esetben $6 = q*2 + r$, így $q = 3$, és $r = 0$ teljesül.

Így pedig $g^j = g^6 = 6$ és $(g^d)^q = (g^2)^3 = (1+1)+(1+1)+(1+1) = 6$ szintén.

Gyűrűk

Gyűrű:

Jele: R (*ring*). Olyan $(R, +, *)$, amire igaz, hogy:

- $(R, +)$ Abel-csoport
- $(R, *)$ félcsoport
- van disztributivitás $[a(b+c) = a*b + a*c$ illetve $(b+c)a = b*a + b*c]$

Integritási tartomány:

Olyan gyűrű, ami kommutatív és nullosztómentes [*ha $a*b=0$, akkor $a=0$ vagy $b=0$*].
 $|R| \geq 2$, azaz legalább két eleme van (*kizárja a nullgyűrűt, aminek csak 1 eleme van*).

Egységelemes gyűrű:

Olyan gyűrű, amiben a szorzásnak van egységeleme.

Például: $(\mathbb{Z}, +, *)$ gyűrű és integritási tartomány is.

Polinomok

Például:

- $1+x+3x^2$ (**egyhatározatlanú polinom**, azaz csak egy ismeretlen van: x)
- $3x+8y^3+z^2$ (**többhatározatlanú polinom**, több ismeretlen is van: x, y és z)

Polinom:

Legyen R egy gyűrű. Ekkor egy R -beli együtthatós egyhatározatlanú f polinom egy olyan $f = (f_0, f_1, f_2 \dots f_n \dots)$ **R -beli végtelen hosszú sorozat**, melynek csak véges sok eleme nem nulla.

Jelölje $R[x]$ az R feletti egyhatározatlanú polinomok gyűrűjét.

Például:

$$\begin{aligned} 5+2x-7x^2 & (5, 2, -7, 0, 0, 0, 0, 0, 0 \dots 0) \\ 5y^7-2y^2+4 & (4, 0, -2, 0, 0, 0, 5, 0, 0 \dots 0) \end{aligned}$$

Műveletek polinomokkal:

• Összeadás:

Legyen $f = (f_0, f_1, f_2 \dots)$ és $g = (g_0, g_1, g_2 \dots)$ polinom.

Ekkor a két polinom összege $f+g = (f_0 + g_0, f_1 + g_1, f_2 + g_2 \dots)$

Például: $(x^2+3x+4) + (2x^2-x+8) = 3x^2+2x+12$

• Szorzás:

Legyen $f = (f_0, f_1, f_2 \dots)$ és $g = (g_0, g_1, g_2 \dots)$ polinom.

Ekkor a két polinom szorzata $f \cdot g = (h_0, h_1, h_2 \dots)$, ahol

$$h_k = \sum_{i=0}^k f_i \cdot g_{k-i}$$

Például: $(2+3x+5x^2) \cdot (1-2x+3x^2)$

*	1	-2x	3x ²
2	2	-4x	6x ²
3x	3x	-6x ²	9x ³
5x ²	5x ²	-10x ³	15x ⁴

$$15x^4 - x^3 + 5x^2 - x + 2$$

Átlónként kell összevonni őket	
x ⁰ :	2
x ¹ :	-4x + 3x = -x
x ² :	6x ² - 6x ² + 5x ² = 5x ²
x ³ :	9x ³ - 10x ³ = -x ³
x ⁴ :	15x ⁴

Állítás: Polinom összege és szorzata is gyűrű.

Konstans polinom: $(a, 0, 0, 0 \dots 0)$ alakú polinom. Például: 5

Legyen $f = (f_0, f_1, f_2 \dots f_i \dots)$ egy polinom.

f_i : Az i -ed fokú tag **együtthatója**.

f₀ : Konstans tag (például 5)

Egyszerűsített jelölés:

$x^1 = (0, 1, 0, 0, 0 \dots 0)$, $x^2 = (0, 0, 1, 0, 0 \dots 0)$, $x^3 = (0, 0, 0, 1, 0 \dots 0)$

Ekkor $f = (f_0, f_1, f_2 \dots f_i \dots)$ polinom így is felírható:

$$f = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n$$

Polinom foka: A legnagyobb olyan $n \in \mathbb{N}$, amire $f_n \neq 0$.

Jelölése: $\deg(f)$ (*degree*)

Polinom főegyütthatója: Az az f_n , amire igaz, hogy $f_n \neq 0$.

Például: $7x^3 - 4x + 3$ (foka: 3, főegyütthatója: 7, konstans tagja: 3)

Főpolinom: Olyan polinom, aminek a főegyütthatója R gyűrű egységeleme.

Például: $x^3 + 2x$

Nullpolinom: A $0 = (0, 0, 0 \dots 0)$ alakú polinom.

A nullpolinom foka a definíció szerint: $-\infty$ (*mínusz végtelen*).

Lineáris polinom: Legfeljebb elsőfokú polinomok.

Például: $5x$ vagy 3

Monom: Pontosan egy darab nem nulla tagú polinom $(0, 0, 0 \dots (f_n \neq 0), \dots 0)$

Például: $10x^3, 3x^2, 5x$ vagy 8

Állítás: Ha R nullosztómentes, akkor $R[x]$ is az, és

$$\deg(f * g) = \deg(f) + \deg(g),$$

valamint $f * g$ főegyütthatója pedig f és g főegyütthatóinak a szorzata.

Például: $f = (x^3 + 2x)$, $g = (x^2 + 3)$, és $\deg(f) = 3$, $\deg(g) = 2$

$$f * g = (x^5 + 5x^3 + 6x), \deg(f * g) = 5$$

Különleges eset: $f = 0$, $g = (x^2 + 3)$, és $\deg(f) = -\infty$, $\deg(g) = 2$

$$f * g = 0, \deg(f * g) = -\infty, \text{ de } \deg(f) + \deg(g) = -\infty + 2 = -\infty$$

(Ezért kellett a nullpolinom fokszámát $-\infty$ -nak definiálni).

Állítás: Minden R gyűrűre igaz, függetlenül attól, hogy nullosztómentes-e:

$$\deg(f * g) \leq \deg(f) + \deg(g),$$

$$\deg(f + g) = \max\{\deg(f), \deg(g)\}$$

Például: $R = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ Nem nullosztómentes, mert $2 * 2 = 4 = 0$.

Legyen $f = x^2$, $g = x^3$, így $f * g = x^5 = x^1$

$$\deg(f * g) = \deg(x^1) = 1$$

$$\deg(f) + \deg(g) = 2 + 3 = 5$$

Így $1 \leq 5$ teljesül.

Formális hatványsor:

Olyan $f = (f_0, f_1, f_2 \dots f_n \dots)$ sorozatok, amelyekben akárhány nem nulla elem lehet.

Például: $(1, 1, 1 \dots 1) = \sum_{i=0}^{\infty} x^i = x^0 + x^1 + x^2 + \dots$

Helyettesítési érték:

Legyen R egy gyűrű, és $r \in R$.

$f = f_0 + f_1 * x + f_2 * x^2 + \dots + f_n * x^n$ polinom r helyen vett helyettesítési értékén az

$f(r) = f_0 + f_1 * r + f_2 * r^2 + \dots + f_n * r^n \in R$ összeget értjük.

Ha f helyettesítési értéke r helyen 0, akkor r az f polinom **gyöke**.

Polinomfüggvény:

Az $r \rightarrow f(r)$ függvényt az f polinomhoz tartozó polinomfüggvénynek nevezzük.

Megjegyzés: Különböző polinomokhoz is tartozhat ugyanaz a polinomfüggvény.

Például: Legyen $\mathbb{Z}_2 = \{0, 1\}$, és legyenek $f(x) = x$ és $g(x) = x^2$ függvények.

Ekkor $f(0) = 0$, és $f(1) = 1$, valamint

$g(0) = 0^2 = 0$, és $g(1) = 1^2 = 1$

Maradékos osztás:

Polinomokat összeadhatunk, szorozhatunk és maradékos osztást is végezhetünk rajtuk.

Legyen R egységelemes integritási tartomány (pl. \mathbb{Z}), $f, g \in R[x]$, g főegyütthatója pedig legyen egység R -ben.

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

$f = g * q + r$, valamint tudjuk, hogy $\deg(r) < \deg(g)$.

Például:

Egész számoknál: $31 = 7 * 4 + 3$

Polinomoknál: $(x^2 + x + 2) = (x-1) * (x+2) + 4$ [$\deg(r=4) = 0 < \deg(g = x-1) = 1$]

Bizonyítás:

1.) Létezik olyan q és $r \in R[x]$, hogy $f = g * q + r$ és $\deg(r) < \deg(g)$.

Fokszám szerinti teljes indukcióval bizonyítunk.

Tegyük fel, hogy $\deg(f) < \deg(g)$. Így biztos, hogy $q = 0$ és $r = f$, azaz léteznek.

(Pl.: $(x+1) = (x^2+1) * q + r$ csak úgy megoldható, ha $q = 0$ és $r = (x+1)$)

Indukcióval tegyük fel, hogy $n-1$ fokszámra igaz, bizonyítsuk n fokszámra.

Legyen $f = f_0 + f_1 x^1 + f_2 x^2 + \dots + f_n x^n$ és $g = g_0 + g_1 x^1 + g_2 x^2 + \dots + g_k x^k$ két polinom.

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

$f^* = (f_0 + \dots + f_n x^n) - f_n * (g_k^{-1} * x^{n-k} * (g_0 + \dots + g_k x^k))$

$f^* = (\dots + f_n x^n) - f_n * (g_k^{-1} * x^{n-k} * (\dots + g_k x^k))$

$f^* = (\dots + f_n x^n) - f_n * (\dots + (g_k^{-1} * x^{n-k}) * (g_k x^k))$

$f^* = (\dots + f_n x^n) - f_n * (\dots + x_n)$

$f^* = f - (\dots + f_n x^n)$, így biztos, hogy $\deg(f^*) < \deg(f)$

Indukciós feltétel szerint: $f^* = g * q^* + r^*$

Innen látszik, hogy $r = r^*$, és $q = f_n * g_k^{-1} * x^{n-k} + q^*$

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

2.) Egyértelműen létezik, azaz csak egy ilyen van.

Indirekt bizonyítás, tegyük fel, hogy nem egyértelmű, azaz két különböző is létezik.

$$f = g * q + r = g * q' + r'$$

$$g * (q - q') = r' - r$$

$$// \text{Alkalmazzuk: } \deg(f * g) = \deg(f) + \deg(g)$$

$$\deg(g) + \deg(q - q') = \deg(r' - r) \quad // \text{Alkalmazzuk: } \deg(f + g) = \max\{\deg(f), \deg(g)\}$$

$$\deg(r' - r) = \max\{\deg(r), \deg(r')\} \quad // \text{Alkalmazzuk: } \deg(r) < \deg(g)$$

$$\max\{\deg(r), \deg(r')\} < \deg(g)$$

Így tehát:

$$\deg(g) + \deg(q - q') = \deg(r' - r) = \max\{\deg(r), \deg(r')\} < \deg(g)$$

$$\deg(g) + \deg(q - q') < \deg(g)$$

Ez csak akkor lehet, ha $\deg(q - q') = -\infty$, azaz $q - q' = 0$, tehát $q = q'$.

Azaz $f = g * q + r = g * q + r'$, tehát $r = r'$.

Így a két különböző maradékosztás ugyanaz, tehát csak egy van, azaz egyértelmű.

Gyöktényező leválasztása:

Ha $f \neq 0$ és c az f gyöke (azaz $f(c) = 0$), akkor létezik olyan $q \neq 0$ polinom, hogy

$$f = q * (x - c)$$

Például: \mathbb{Z} -ben vagyunk.

$$f = x^3 - 2x^2 + 3x - 6 \quad c = 2, \text{ hisz } f(2) = 0.$$

Ekkor leválasztható a gyöktényező a következőképpen:

$$f = x^3 - 2x^2 + 3x - 6 = (x - 2) * (x^2 + 3)$$

Bizonyítás:

Végezzünk el f -en $(x - c)$ -vel maradékosztást.

$$f = (x - c) * q + r, \text{ ahol } \deg(r) < \deg(x - c)$$

De $\deg(x - c) = 1$, így $\deg(r) = 0$, azaz r egy konstans szám.

$$f(c) = (c - c) * q + r$$

$$f(c) = 0 = 0 * q + r$$

Tehát $r = 0$, azaz el lehet osztani maradék nélkül f -et $(x - c)$ -vel.

$$\text{Így } f = (x - c) * q$$

Polinom gyökeinek száma:

Egységelemes integritási tartományban $f \neq 0$ polinomnak legfeljebb $\deg(f)$ gyöke lehet.

Bizonyítás:

A fokszám szerinti teljes indukcióval bizonyítunk.

Nullfokú polinomnak (konstans szám) nulla gyöke lehet.

Elsőfokú polinomnak egy gyöke lehet.

Másodfokú polinomnak legfeljebb két gyöke lehet.

Tegyük fel, hogy n fokú polinomnak legfeljebb n gyöke lehet, bizonyítsuk $(n+1)$ -re!

Legyen f egy $(n+1)$ fokú polinom, válasszuk le belőle a gyöktényezőt.

$$f = (x - c) * q$$

$$\text{Ebből következik, hogy } \deg(f) = 1 + \deg(q)$$

$$\text{Mivel } \deg(f) = n+1, \text{ így } \deg(q) = n.$$

Abból indultunk ki, hogy egy n fokú polinomnak legfeljebb n gyöke lehet, és ha beszorozzuk ezt $(x - c)$ -vel, akkor pedig $(f\text{-nek})$ legfeljebb $(n+1)$ gyöke lehet.

Fontos, hogy egységelemes integritási tartományban legyünk, különben nem teljesül az állítás.

Például: $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ $f = x^2 - 1$ $\deg(f) = 2$
 f -nek viszont 4 gyöke is lehet, méghozzá: 1, 3, 5, 7
 $1^2 - 1 = 0$ $3^2 - 1 = 8 = 0$ $5^2 - 1 = 24 = 0$ $7^2 - 1 = 48 = 0$

Polinomok hasonlósága:

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

Bizonyítás:

Legyen $f = (f_0, f_1, f_2 \dots f_n \ 0 \dots 0)$ és $g = (g_0, g_1, g_2 \dots g_n \ 0 \dots 0)$ polinomok

Vegyük a két polinom különbségét:

$$f - g = (f_0 - g_0, f_1 - g_1, f_2 - g_2 \dots f_n - g_n \ 0 \dots 0)$$

Ha megegyezik a kettő, akkor a különbségnek $(0, 0 \dots 0)$ nullpolinomnak kell lennie.

Tehát $f_0 - g_0 = 0$ és $f_1 - g_1 = 0$ és $f_2 - g_2 = 0$ és $\dots f_n - g_n = 0$.

Ez pedig így $n+1$ hely (mert 0-tól számolunk n -ig).

Különböző polinomfüggvények:

Ha R gyűrű végtelen, akkor két különböző polinomhoz biztosan különböző polinomfüggvény tartozik.

Horner-elrendezés:

Legyen $f(x) = 3 + 2x + 5x^2 + 7x^3 - 4x^4 + 2x^5$ polinom

Helyettesítsük be az $f(x)$ -be x helyére mondjuk 4-et.

Ennek eredményét nagyon hosszas lenne kiszámolni.

A Horner-elrendezéssel viszont eltüntethetjük a hatványokat a polinomból:

$$\begin{aligned} &3 + x(2 + 5x + 7x^2 + 4x^3 + 2x^4) \\ &3 + x(2 + x(5 + 7x + 4x^2 + 2x^3)) \\ &3 + x(2 + x(5 + x(7 + 4x + 2x^2))) \\ &3 + x(2 + x(5 + x(7 + x(4 + 2x)))) \\ &\mathbf{3 + x * (2 + x *(5 + x *(7 + x *(4 + 2*x))))} \end{aligned}$$

Látható, hogy így mindössze $(n-1)$ szorzást és $(n-1)$ összeadást kellett elvégeznünk.

Polinom algebrai deriváltja:

Legyen R egy gyűrű és $f = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n \in R[x]$ polinom.

f polinom algebrai deriváltja a $f' = f_1 + 2f_2 x + 3f_3 x^2 \dots + n f_n x^{n-1} \in R[x]$ polinom.

Oka: $(f+g)' = f' + g'$ illetve $(x^n)' = n * x^{n-1}$

Deriválási tételek:

- 1.) Konstans polinom deriváltja a nullpolinom.
- 2.) x polinom deriváltja az egységelem (1) . $[(x^1)]' = 1 * x^0 = 1 * 1 = 1$
- 3.) Összeg deriváltja: $(f+g)' = f' + g'$
- 4.) Szorzat deriváltja: $(f * g)' = f' * g + f * g'$

Többszörös gyök:

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $f \neq 0$, $n \in \mathbb{N}^+$.

Ekkor $c \in R$ az f polinom n -szeres gyöke, ha:

$$f = (x-c)^n * q, \text{ de } (x-c) \nmid q \quad (\nmid: \text{nem osztója})$$

Például: $f = x^3 - x^2 - x + 1$ polinomnak az 1 kétszeres gyöke, hisz:

$$x^3 - x^2 - x + 1 = (x-1)^2 * (x+1)$$

Deriváltak többszörös gyökei:

Előzőből.

Ekkor c az f' -nek legalább $(n-1)$ -szeres gyöke.

(Ha $R = \mathbb{Z}, \mathbb{Q}$ vagy \mathbb{R} , akkor pedig pontosan $(n-1)$ -szeres gyöke.)

Bizonyítás:

Legalább $(n-1)$ -szeres gyök:

A többszörös (n) -szeres gyök definíciójából kiindulva.

$$f = (x-c)^n * q \quad // \text{Deriváljuk le, szorzatként kell! } (f * g)' = f' * g + f * g'$$

$$f' = ((x-c)^n * q)' = ((x-c)^n)' * q + (x-c)^n * q' = n * (x-c)^{n-1} * q + (x-c)^n * q'$$

Kiemelünk $(x-c)^{n-1}$ -t.

$$(x-c)^{n-1} * (n * q + (x-c) * q')$$

$(x-c)^{n-1}$ -ből már biztosan tudjuk, hogy $(n-1)$ -szeres gyök c , de mivel még szorozzuk $(n * q + (x-c) * q')$ -vel, ezért lehet még többszörös is, szóval így legalább $(n-1)$ -szeres.

Ha $R = \mathbb{Z}, \mathbb{Q}$ vagy \mathbb{R} , akkor pedig pontosan $(n-1)$ -szeres gyök:

Ezt kell még belátni hozzá: $(x-c) \nmid q$.

Ez ebben az esetben így néz ki: $(x-c) \nmid (n * q + (x-c) * q')$

Az oszthatóság miatt $(x-c)$ eltűnik a jobb oldalról

(*Például:* $(7 \nmid n * 10 + 7 * q)$ ugyanúgy igaz, minthogy $(7 \nmid n * 10)$, hisz $7 \mid 7 * q$)

Szóval: $(x-c) \nmid n * q$

De n -t is eltüntetjük a jobb oldalról.

(*Például:* $(7 \nmid n * 10)$ ugyanúgy igaz, minthogy $(7 \nmid 10)$, hisz $10 \mid n * 10$)

Így pedig: $(x-c) \nmid q$, és pont ezt akartunk bizonyítani.

Irreducibilis (felbonthatatlan) polinomok:

Előzmény: Az irreducibilis szám olyan $(n > 1) \in \mathbb{N}$ szám, amely csak $1 * n$ vagy $n * 1$ alakban írható fel természetes számok szorzataként. *Például:* 2, 3, 5, 7, 11, 13, 17 stb.

Legyen R egy egységelemes integritási tartomány, $f \in R[x]$ pedig egy polinom ($f \neq 0$ és f nem egység (azaz nem konstans polinom)). Ekkor f irreducibilis polinom, ha bármely $f = g * h$ felírásban g vagy h az $R[x]$ -ben **egység** (olyan elem, aminek a szorzásra nézve van inverze (reciproka)).

Például: $(x^2 + 1) \in R[x]$ polinom irreducibilis, hisz csak így lehet felbontani:

$$(x^2 + 1) = [c * (x^2 + 1)] * (1/c), \text{ ahol } c \text{ egy konstans (polinom), így van inverze.}$$

Irreducibilis polinomok \mathbb{C} (komplex számok halmaza) felett:

Előzmény: Az algebra alaptétele kimondja, hogy minden legalább elsőfokú polinomnak van gyöke.

Így az, ha $f \in \mathbb{C}[x]$ komplex polinom elsőfokú $\Leftrightarrow f$ irreducibilis polinom (azaz az elsőfokú komplex polinomok az irreducibilis polinomok \mathbb{C} -ben).

Bizonyítás:

Egyik irány: Ha elsőfokú a komplex polinom, akkor irreducibilis is.

A polinom felbontható $f = g * h$ alakban. // $\deg(f * g) = \deg(f) + \deg(g)$ szabály

$$\deg(f) = \deg(g) + \deg(h)$$

$$// \text{Mivel } f \text{ elsőfokú, így } \deg(f) = 1$$

$$\deg(f) = 1 = \deg(g) + \deg(h)$$

Azaz $\deg(g) = 1$ és $\deg(h) = 0$ lesz, vagy fordítva.

Így vagy f vagy g foka nulla lesz, azaz f vagy g konstans, és így egység is.

Tehát $f = \text{egység} * g$, azaz f irreducibilis polinom.

Másik irány: Ha a komplex polinom irreducibilis, akkor elsőfokú is.

Ha f polinom irreducibilis, akkor $\deg(f) \geq 1$, különben f nullpolinom vagy egység (konstans polinom) lenne, ami az irreducibilis polinom definíciója miatt nem lehet.

Így tehát az algebra alaptétele miatt biztosan van gyöke, legyen ez $c \in \mathbb{C}$.

Kiemelem f -ből a gyöktényezőt:

$$f = (x - c) * q \quad // \text{alkalmazom a } \deg(f * g) = \deg(f) + \deg(g) \text{ szabályt}$$

$$\deg(f) = 1 + \deg(q)$$

$$\deg(q) = \deg(f) - 1$$

Akkor lesz f irreducibilis, ha q egy konstans (hisz $(x - c)$ elsőfokú), azaz $\deg(q) = 0$.

$\deg(q) = 0$, azaz $(\deg(f) - 1) = 0$, ebből pedig következik, hogy:

$\deg(f) = 1$, azaz f polinom elsőfokú.

Irreducibilis polinomok \mathbb{R} (valós számok halmaza) felett:

Ha $\deg(f) = 1 \Rightarrow f$ irreducibilis.

Ha $\deg(f) = 2$: f irreducibilis $\Leftrightarrow f$ -nek nincs valós gyöke.

Ha $\deg(f) \geq 3 \Rightarrow f$ nem irreducibilis.

Bizonyítás:

$f \in \mathbb{R}[x]$ valós polinomot tekintünk \mathbb{C} feletti polinomnak, és úgy bontsuk fel elsőfokú tényezők szorzatára.

Például: $x^2 + 1$ valós polinomként irreducibilis, de ha komplex polinomnak tekintjük, akkor már nem, hisz: $x^2 + 1 = (x - i) * (x + i) = x^2 + x * i - i * x - i^2 = x^2 - (-1) = x^2 + 1$

Lemma: Ha $c \in \mathbb{C} \setminus \mathbb{R}$ (azaz komplex, de nem valós) gyöke $f \in \mathbb{R}[x]$ -nek, akkor c konjugáltja (jele: \bar{c}) is gyöke f -nek (i konjugáltja pl. $-i$, lásd előző példa), így $(x - c)$ és $(x - \bar{c})$ is szerepel gyöktényezőként.

Tehát $f = (x - c) * (x - \bar{c}) * g$, így

$$(x - c) * (x - \bar{c}) \mid f \quad // \text{elvégezem a szorzást}$$

$$x^2 - (c + \bar{c})x + c * \bar{c} \mid f \quad // \text{minden } c \in \mathbb{C} \text{-re ez egy valós polinom lesz}$$

$$x^2 - 2 * \text{Re}(c)x + |c|^2 \mid f$$

Tehát f -nek van egy **másodfokú osztója**

(Azaz harmadfoktól kezdve már nem lehet irreducibilis, hisz ott a másodfokú osztó.)

Ha pedig $c \in \mathbb{R}$, akkor $c = \bar{c}$, tehát $(x - c) \mid f$.

(Azaz ha van valós gyöke, akkor az kiemelhető, és így nem lesz irreducibilis.)

Irreducibilis polinomok \mathbb{Q} (racióális számok halmaza) és \mathbb{Z} felett:

Minden $n \in \mathbb{N}$ -re létezik olyan f polinom, hogy $\deg(f) = n$, és f irreducibilis.

Például: $f = x^n + 2$ (magyarázat majd a Schönemann-Eisenstein kritériumnál)

Gauss-gyűrű (az egyértelmű prímfelbontásnak felel meg):

Olyan R egységelemes integritási tartomány, amelyben minden nem nulla elem egységektől és sorrendtől eltekintve egyértelműen felírható irreducibilis elemek szorzataként.

Például:

\mathbb{Z} Gauss-gyűrű (számelmélet alaptétele mondja ki):

$$\text{Pl.: } 21 = 3 \cdot 7 = 7 \cdot 3 = (-7) \cdot (-3) = (-3) \cdot (-7)$$

$\mathbb{R}[x]$ -ben (valós polinomok gyűrűje)

$$\text{Pl.: } x^3 - x^2 + x - 1 = (x^2 + 1) \cdot (x - 1), \text{ ahol } (x^2 + 1) \text{ és } (x - 1) \text{ irreducibilis polinomok.}$$

$$\text{Sorrendtől eltekintve: } x^3 - x^2 + x - 1 = (x^2 + 1) \cdot (x - 1) = (x - 1) \cdot (x^2 + 1)$$

$$\text{Egységektől eltekintve: } x^3 - x^2 + x - 1 = (x^2 + 1) \cdot (x - 1) = [3 \cdot (x^2 + 1)] \cdot [1/3 \cdot (x - 1)]$$

Euklideszi gyűrű (a maradékos osztásnak felel meg):

Olyan R egységelemes integritási tartomány, melyen értelmezve van egy

$\varphi: R \setminus \{0\} \rightarrow \mathbb{N}$ függvény úgy, hogy:

- (1) $\forall a, b \in R$ -hez ($b \neq 0$) $\exists q, r \in R$, hogy:
 $a = b \cdot q + r$, és $r = 0$, vagy $r \neq 0$, de $\varphi(r) < \varphi(b)$
- (2) $\forall a, b \in R$ -re ($a \neq 0$ és $b \neq 0$) igaz, hogy:
 $\varphi(a) \leq \varphi(a \cdot b)$ és $\varphi(b) \leq \varphi(a \cdot b)$

Példa euklideszi gyűrűkre:

• **\mathbb{Z}** euklideszi gyűrű, ahol $\varphi(n) = |n|$.

Maradékos osztás az egész számok között: $a = b \cdot q + r$.

$$\text{Pl.: } 15 = 7 \cdot 2 + 1$$

- (1) $r = 1 \neq 0$, és $\varphi(r) < \varphi(b)$, azaz $\varphi(1) < \varphi(7)$, azaz $|1| < |7|$
- (2) $\varphi(a) = \varphi(15) = |15|$, $\varphi(b) = \varphi(7) = |7|$, és $\varphi(a \cdot b) = \varphi(15 \cdot 7) = \varphi(105) = |105|$
 $\varphi(15) \leq \varphi(105)$, mert $|15| \leq |105|$, és $\varphi(7) \leq \varphi(105)$, mert $|7| \leq |105|$,

• Minden test euklideszi gyűrű is.

• Polinomok gyűrűje bármely test (pl. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) felett, ahol $\varphi(f) = \deg(f)$.

Maradékos osztás a polinomok között: $f = g \cdot q + r$, és teljesül: $\deg(r) < \deg(g)$.

- (1) Mivel $f = a$, és $g = b$, így $\deg(r) < \deg(g) = \deg(r) < \deg(b) = \varphi(r) < \varphi(b)$
- (2) $\deg(f) \leq \deg(f \cdot g)$, és $\deg(g) \leq \deg(f \cdot g)$, így az is teljesül, hogy:
 $\varphi(a) \leq \varphi(a \cdot b)$ és $\varphi(b) \leq \varphi(a \cdot b)$

Tétel: Minden euklideszi gyűrű Gauss-gyűrű is.

(„Azaz ha van maradékos osztás, akkor van egyértelmű prímfelbontás is.”)

Primitív polinom:

Legyen R egy Gauss-gyűrű, $f \in R[x]$ pedig egy polinom.

f primitív polinom, ha az együtthatóinak a legnagyobb közös osztója az egységelem.

(Azaz nem lehet kiemelni konstanszt a polinomból.)

Például: **$\mathbb{Z}[x]$** -ben vagyunk, ahol 1 az egységelem.

$$\text{Nem primitív polinom: } 3x^2 + 15x + 9 = 3 \cdot (x^2 + 5x + 3)$$

Azaz a 3 konstanszt kiemelhetjük a polinomból, hisz $3 \mid 3$, $3 \mid 15$ és $3 \mid 9$.

Primitív polinom: $10x^2 + 15x + 6$ (nem lehet kiemelni semmilyen konstanszt)

Mivel a 10-nek, a 15-nek és a 6-nak az 1-en kívül nincs közös osztója.

Gauss lemma:

Legyen R egy Gauss-gyűrű, f és $g \in R[x]$ ($f \neq 0$ és $g \neq 0$) pedig primitív polinomok. Ekkor a szorzatuk ($f \cdot g$) is primitív polinom.

Gauss tétele:

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

(Hányadostest: pl.: \mathbb{Z} -nek a \mathbb{Q} a hányadosteste, mert \mathbb{Q} -ban z_1/z_2 alakú törtek vannak)

(1) Ha $f \in R[x]$ polinom felbontható $f = g \cdot h$ alakra $K[x]$ -ben, akkor létezik olyan $g^* \in R[x]$ polinom, hogy $f = g^* \cdot h^*$.

Valamint $g^* = \text{konstans} \cdot g$, illetve $h^* = \text{konstans} \cdot h$ a $K[x]$ -ben.

(2) $R[x]$ is Gauss-gyűrű.

Következménye:

Mivel \mathbb{Z} egy Gauss-gyűrű, \mathbb{Q} pedig a hányadosteste, ezért:

$f \in \mathbb{Z}[x]$ polinomra igaz, hogyha $\mathbb{Q}[x]$ -ben felbontható $\Leftrightarrow \mathbb{Z}[x]$ -ben is felbontható.

Táblázat az alapgyűrű és a polinomgyűrű kapcsolatáról:

Ha az alapgyűrű (R),	akkor a polinomgyűrű ($R[x]$)
gyűrű	gyűrű
kommutatív gyűrű	kommutatív gyűrű
integritási tartomány	integritási tartomány
egységelemes integritási tartomány	egységelemes integritási tartomány
Gauss-gyűrű	Gauss-gyűrű
Euklideszi gyűrű	Gauss-gyűrű
Test	Euklideszi gyűrű

Modulo egy polinom számolások (kongruencia-számolások):

Előzmény: \mathbb{Z} -ben az egész számok között így működik a kongruencia.

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$$

Pl.: $10 \equiv 4 \pmod{6}$ igaz, hisz $6 \mid (10-4=6)$

Ekkor $\mathbb{Z} \rightarrow \mathbb{Z}_m$ gyűrű lesz, melynek az elemei:

$\{0, \dots, m-1\}$ (azaz a lehetséges maradékok halmaza)

Pl.: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5\}$ is gyűrű lesz!

Ha p prím, akkor \mathbb{Z}_p test lesz.

Polinomok között $K[x]$ -ben:

$$a \equiv b \pmod{f} \Leftrightarrow f \mid (a-b)$$

Tehát: $a = f \cdot q + r$, és $b = f \cdot q' + r$.

Ekkor $K[x] \rightarrow K[x]/(f)$ gyűrű lesz, melynek az elemei:

$\{g \mid \deg(g) < \deg(f)\}$ (azaz a lehetséges maradékok halmaza)

Ha f irreducibilis polinom, akkor $K[x]/(f)$ test lesz.

Testbővítések irreducibilis polinommal:

Legyen K egy test, $f \in K[x]$ pedig egy irreducibilis polinom.

Tekintsük az összes legfeljebb $\deg(f) - 1$ fokú polinomot $K[x]$ -ben a következő műveletekkel:

Összeadás: $g+h$ a $K[x]$ -ben

Szorítás: $(g \cdot h) \bmod f$

Reciprok számítás: $1/g = ?$

$\text{Inko}(f,g) = 1$, mert f irreducibilis, így $\exists u$ és v , hogy: $f \cdot u + g \cdot v = 1$
 $1/g = v$

Az így kapott struktúra egy test.

Például:

\mathbf{R} (valós számok teste) teste bővítve az (x^2+1) polinommal megadja \mathbf{C} -t (komplex számok teste).

A testbővítés alkalmazása:

Legyen K test $= \mathbf{Z}_p$, ahol p egy prímszám.

Legyen f egy n -edfokú irreducibilis polinom $\mathbf{Z}_p[x]$ -ben.

Ekkor \mathbf{Z}_p -t f -vel bővítve egy p^n elemű test kapunk.

Például: Legyen $p=3$ prímszám, és $f = x^2+1$ ($n=2$) fokú irreducibilis polinom.

Mivel $\deg(f) = 2$, így a bővített testben csak $(\deg(f) - 1 = 1)$ fokú polinomok lehetnek.

Így nézhetnek ki: $\{a \cdot x + b \mid a, b \in \mathbf{Z}_p = \{0, 1, 2\}\}$.

A bővített test elemei ezért a következők lehetnek:

$\{0 \cdot x + 0 = 0, 0 \cdot x + 1 = 1, 0 \cdot x + 2 = 2, 1 \cdot x + 0 = x, 1 \cdot x + 1 = x+1, 1 \cdot x + 2 = x+2, 2 \cdot x + 0 = 2x, 2x+1, 2x+2\}$

Ez így összesen $p^n = 3^2 = 9$ elem.

Egy szorzás ebben a bővített testben:

$(x+2) \cdot (x+2) = x^2 + 4x + 4$

Ám mivel \mathbf{Z}_3 -ban $4 = 4 \bmod 3 = 1$, ezért:

$x^2 + 4x + 4 = x^2 + 1x + 1$

De venni kell még ennek a $(\bmod f)$ -jét is:

$x^2 + 1x + 1 \pmod{f} = x^2 + 1x + 1 \pmod{x^2+1}$

$x^2 + 1x + 1 = (x^2+1) \cdot 1 + x$, azaz

$x^2 + 1x + 1 \pmod{x^2+1} = x$

Tehát a szorzás eredménye ebben a bővített testben:

$(x+2) \cdot (x+2) = x$

Véges testek alaptétele:

(1) Minden véges test p^n elemszámú valamilyen p prímszámra, és $n \geq 1$ egészre.

(Ezért nem lehet például 10 elemű véges test).

(2) Minden p prímszámra és $n \geq 1$ egészre létezik p^n elemszámú véges test, és ez egyértelmű az izomorf változatoktól eltekintve.

Tétel: Ha K egy véges test, akkor $(K \setminus \{0\}, \cdot)$ ciklikus csoportot alkot.

Például: $K = \mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$, és $\mathbf{Z}_5 \setminus \{0\} = \{1, 2, 3, 4\}$

Ekkor $\mathbf{Z}_5 \setminus \{0\}$ a szorzásra nézve ciklikus részcsoporthoz tartozik, generátora pedig a 2.

$2 \bmod 5 = 2$

$2 \cdot 2 = 4 \bmod 5 = 4$

$2 \cdot 2 \cdot 2 = 8 \bmod 5 = 3$

$2 \cdot 2 \cdot 2 \cdot 2 = 16 \bmod 5 = 1$

Ciklikus részcsoporthoz tartozik, hisz a 2-ből és a szorzásból minden $\mathbf{Z}_5 \setminus \{0\}$ -beli elem létrejött.

Schönemann-Eisenstein kritérium:

Legyen R egy Gauss-gyűrű, $f \in R[x]$ pedig egy legalább elsőfokú polinom.

$$f = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n$$

Legyen $p \in R$ egy prímelem (irreducibilis elem).

Ha $p \nmid f_n$, de $(p \mid f_0, p \mid f_1 \dots p \mid f_{n-1})$, és $p^2 \nmid f_0$, akkor f irreducibilis.

Ezzel a módszerrel könnyen létre tudunk hozni irreducibilis polinomokat.

Például: Legyen $R = \mathbb{Z}$, és $p = 2$ prímszám.

Mivel $2 \nmid 3$, de $(2 \mid 6, 2 \mid 14, 2 \mid 10)$, és $2^2 = 4 \nmid 10$, így a

$3x^5 + 6x^3 - 14x^2 + 10$ polinom biztosan irreducibilis polinom.

A módszer bizonyítja, hogy $x^n + 2 \in \mathbb{Z}[x]$ polinom minden $n \in \mathbb{N}$ esetén irreducibilis.

(mert $p=2$ prím nem osztója 1-nek, és $p \mid 2$ és $p^2 \nmid 2$ teljesül)

Lagrange-interpoláció:

Legyen R egy egységelemes integritási tartomány.

Legyenek $c_0, c_1 \dots c_n \in R$ alappontok, és $d_0, d_1 \dots d_n \in R$ függvényértékek.

Ekkor a Lagrange-interpolációval előállíthatunk egy olyan $f \in R[x]$ polinomot, hogy:

$$f(c_i) = d_i \quad \forall i = 0..n\text{-re}$$

Ha $\deg(f) \leq n$, akkor pontosan egy ilyen f polinom van csak.

j-dik Lagrange-alappolinom előállítás:

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

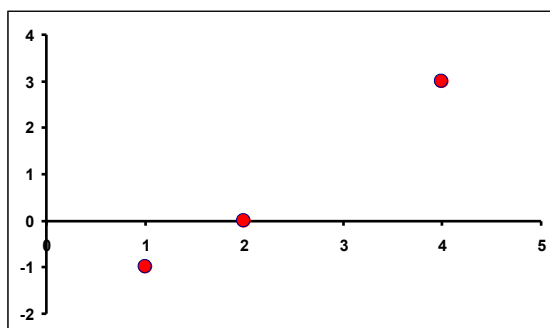
f(x) Lagrange-interpolációs polinom előállítás:

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

Például:

A módszer előállítja a megadott függvénykoordinátákon átmenő függvényt.

Legyenek $c_0=1$, $c_1=2$ és $c_2=4$ alappontok, és $d_0 = -1$, $d_2=0$ és $d_3=3$ függvényértékek.



Lagrange-alappolinomok előállítása:

$$l_0(x) = \frac{x-c_1}{c_0-c_1} * \frac{x-c_2}{c_0-c_2} = \frac{x-2}{1-2} * \frac{x-4}{1-4} = \frac{x^2-6x+8}{3}$$

$$l_1(x) = \frac{x-c_0}{c_1-c_0} * \frac{x-c_2}{c_1-c_2} = \frac{x-1}{2-1} * \frac{x-4}{2-4} = \frac{-x^2-5x+4}{2}$$

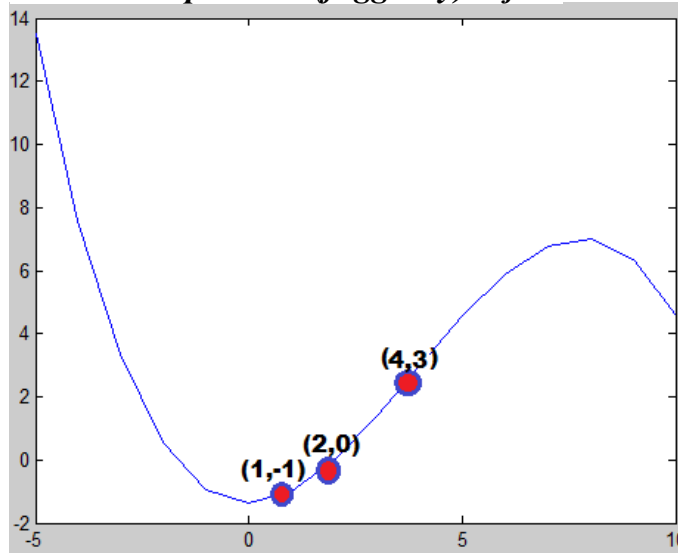
$$l_2(x) = \frac{x-c_0}{c_2-c_0} * \frac{x-c_1}{c_2-c_1} = \frac{x-1}{4-1} * \frac{x-2}{4-2} = \frac{x^2-3x+2}{6}$$

$f(x)$ Lagrange-interpolációs polinom előállítása:

$$d_0 * l_0(x) + d_1 * l_1(x) + d_2 * l_2(x) = -1 * l_0(x) + 0 * l_1(x) + 3 * l_2(x)$$

$$\frac{-2x^2 + 12x - 16 + 3x^2 - 9x + 6}{6} = \frac{1}{6}(x^2 + 3x - 10)$$

Az elkészült polinom (függvény) rajza:



Titokmegosztás Lagrange-interpolációval:

Legyen a titok egy $t \in \mathbb{N}$ szám. Az a célunk, hogy n ember között úgy osszuk szét számokat, hogy bármelyik m ember ($m < n$), ha összegyűlik, akkor meg tudja kapni a titkot, de $m-1$ ember már semmi információt ne tudhasson meg a titokról.

- 1.) Keressünk egy t -nél nagyobb p prímszámot.
- 2.) Készítsünk el $a_1, a_2 \dots a_m \in \mathbb{Z}_p$ véletlenszámokat.
- 3.) Készítsük el a $f = t + a_1 x + a_2 x^2 + \dots + a_m x^m \in \mathbb{Z}_p[x]$ polinomot.
- 4.) Adjuk oda az $i = 1 \dots n$ embernek a polinom $f(i)$ értékét.

A polinom megkapható Lagrange interpolációval, de csak akkor, ha m darab helyen tudjuk az $f(i)$ értékét.

Parciális törtekre bontás:

Legyen K egy test (pl. \mathbb{R} , \mathbb{Q} vagy \mathbb{C}).

Legyenek $g_1, g_2 \dots g_n \in K[x]$ páronként relatív prím polinomok (azaz a legnagyobb közös osztójuk egy konstans polinom).

Jelöljük g -vel a szorzatuk: $g = g_1 * g_2 * \dots * g_n$

Ekkor biztosan léteznek olyan $f_1, f_2 \dots f_n \in K[x]$ polinomok, amelyekre igaz, hogy:

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

Például:

$$g_1 = x-1, g_2 = x+1, g = g_1 * g_2 = x^2-1,$$

$$\frac{1}{x^2-1} = \frac{A}{x-1} + \frac{B}{x+1}$$

$$A(x+1) + B(x-1) = 1$$

$$Ax + A + Bx - B = 1$$

$$(A+B)x = 0 \text{ és } A - B = 1$$

$$\text{Tehát: } A = -B, \text{ és } -2B = 1$$

$$B = -1/2, \text{ azaz } f_2 = -1/2$$

$$A = +1/2, \text{ azaz } f_1 = +1/2$$

Bizonyítás:

Teljes indukcióval bizonyítjuk.

$$n=1 \text{ esetben: } g = g_1, \text{ azaz } \frac{1}{g} = \frac{1}{g_1}$$

$$n=2 \text{ esetben: } g = g_1 * g_2, \text{ azaz } \frac{1}{g_1 * g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$$

Mivel g_1 és g_2 relatív prímek, ezért az euklideszi algoritmus miatt létezik olyan f_1 és f_2 , hogy:

$$f_1 * g_2 + f_2 * g_1 = 1 \quad / \text{ szorzás } 1/(g_1 * g_2) \text{-vel}$$

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{1}{g_1 * g_2}$$

$n > 2$ esetben: Tegyük fel, hogy $(n-1)$ -re igaz, bizonyítsuk n -re!

$g = g_1 * g_2 \dots * g_{n-2} * (g_{n-1} * g_n)$, így ez csak $n-1$ tagból fog állni. Így:

$$\frac{1}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \dots + \frac{f^*}{g_{n-1} * g_n}$$

Az utolsó (f^*) tag visszavezethető az $n=2$ esetre, és ezt így tovább folytatva bebizonyosodik az állítás $n=n$ esetre is.

A többhatározatlanú polinomok világa:

Legyen R egy gyűrű és $n \geq 0$ egészek.

Rekurzívan definiáljuk az R feletti n határozatlanú polinomok gyűrűjét:

$$R[x_1, x_2, \dots, x_n] = R[x_1, x_2, \dots, x_{n-1}][x_n]$$

Például:

$$x^2 + 3xy + y^2 + y + 5 = 1 * y^2 + (3x+1) * y + (x^2+5) * 1$$

(Azaz y változós polinomként kezeljük, de az együttthatók nem konstansok, hanem maguk is polinomok).

Ábrázolva: $(x^2+5, 3x+1, 1, 0, \dots, 0)$

Minden n határozatlanú polinom egy olyan véges összeg, hogy:

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

Például:

$$x^2 + 3xy + 7x^4y^{10}$$

$$f_{2,0} = 1 \quad (x^2y^0)$$

$$f_{1,1} = 3 \quad (x^1y^1)$$

$$f_{4,10} = 7 \quad (x^4y^{10})$$

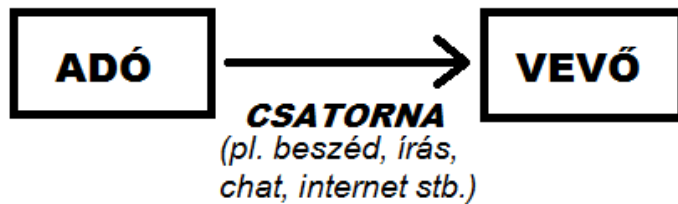
Multifok: $(i_1, i_2 \dots i_n)$, jelen esetben ez $(4, 10)$.

Fok: $(i_1+i_2+\dots+i_n)$, jelen esetben ez $4+10 = 14$.

A Gauss-tétel miatt minden test illetve \mathbf{Z} felett *minden többhatározatlanú polinom, azaz $R[x_1, x_2, \dots x_n]$ Gauss-gyűrű!*

A kódolás alapjai

A kommunikáció sémája:



Gazdaságos kódolás (adattömörítés) esetén:

A csatorna (pl. sávszélesség) **drága**.

Hibajavító kódolás (hibajavítás) esetén):

A csatorna **zajos**. Az a cél, hogy a zaj ne zavarja a kommunikációt.

Gazdaságos kódolás

Forráskódolás:

Van egy forrás (adó), ami egy véges ábécé betűit sugározza. Ezeket az üzeneteket szeretnénk átírni egy másik ábécé betűit használva **gazdaságos módon**.

Például: Morse-kód

Eredeti üzenet ábécéje: {A, B, C, ..., Z és az írásjelek}

Kódolt üzenet ábécéje: {ti, tá, szünet}

Gazdaságos kódolás, mert a gyakran használt betűk kódja rövid (pl.: E = ti), még a ritkán használtaké hosszú (pl.: V = ti-ti-ti-tá).

A kódolás matematikai leírása:

A kódolandó ábécé egy véges halmaz (A).

A kódoló ábécé is egy véges halmaz (B).

A és B véges halmazok elemei a **betűk** (tágabban értelmezve, lehetnek pl. számok is).

λ = Az üres szó

A^* = A betűiből alkotható **szavak** halmaza

A^+ = Az A betűiből alkotható szavak halmaza, kivéve az üres szó. ($A^* \setminus \{\lambda\}$)

Maga a kódolás a következő függvénnyel írható le:

$\varphi: A \rightarrow B^*$ (A ábécé betűit alakítom át B ábécé szavaira)

A kódolás fogalma kiterjeszthető:

$\Psi: A^* \rightarrow B^*$ (A ábécé szavait alakítom át B ábécé szavaira)

Például:

Legyen $A = \{a, b, c\}$ és $B = \{0, 1\}$.

$\varphi: a \rightarrow 00$ $\Psi: abc \rightarrow 00011$

$b \rightarrow 01$

$c \rightarrow 1$

Felbontható kód:

Ha φ injektív, azaz minden szónak más a kódja.

Egyenletes kód:

Ha φ injektív, és minden $a_1, a_2 \in A$ esetén: $|\varphi(a_1)| = |\varphi(a_2)|$
(Azaz minden betűnek egyforma hosszú a kódja.)

Egy egyenletes kód felbontható kód és prefix kód is.

Vesszős kód:

Minden betű kódja ugyanazzal a betűvel végződik (ezt a betűt hívják vesszőnek), és a vessző a betűk kódjában sehol máshol nem fordulhat elő.

Formálisan: v (vessző) szó minden szónak a szuffixe, de egyenlet szó sem állhat elő $\alpha v \beta$ alakban, hacsak nem β az üres szó.

Egy vesszős kód felbontható kód és prefix kód is.

Például: A Morse-kód is vesszős kód, hisz minden szó végén szünet (vessző) van.

Prefix, infix, szuffix:

Legyen A egy véges ábécé, és $\alpha, \beta, \gamma \in A^*$ szavak.

Ekkor $\alpha\beta\gamma$ szónak α a prefixe, β az infixe, γ pedig a szuffixe.

Prefix (másnéven prefixmentes) kód:

$H \subseteq B^*$ prefix kód, ha $h_1, h_2 \in H$ ($h_1 \neq h_2$) esetén h_1 nem prefixe h_2 -nek.

(Azaz egyik szó sem lehet egy másik szó prefixe.)

Például prefix kód: $\{01, 001, 000\}$

Például nem prefix kód: $\{01, 011, 001\}$

Egy prefix kód nem biztos, hogy egyenletes kód vagy vesszős kód.

Tétel: Egy prefix kód biztosan felbontható kód is.

Bizonyítás: A kapott lekódolt szót mohó módon bontjuk fel, azaz amint a betűsorozat megfelel egy betűnek a kódolt ábécében arra dekódoljuk.

Például: $\varphi: a \rightarrow 10, b \rightarrow 01, c \rightarrow 00$, a lekódolt szó pedig a 1000

Beolvassuk a karaktereket:

1 (ilyen kód nincs, tovább olvassuk a karaktereket)

10 (ez megfelel a kódjának, így ezt a-ra dekódoljuk)

0 (ilyen kód nincs)

00 (ez megfelel c kódjának, így ezt c-re dekódoljuk)

Kódok ábrázolása kódfával:

Az éleket B ábécé betűivel címkézzük.

Egy szó a gyökértől egy csúcscímkeig vezető utak címkesorozata.

A kódszavakat A betűivel címkézzük.

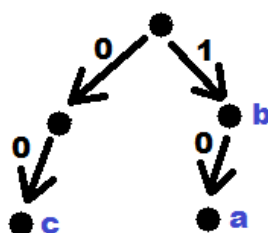
Például:

$A = \{a, b, c\}$ és $B = \{0, 1\}$

$\varphi: a \rightarrow 10$

$b \rightarrow 01$

$c \rightarrow 00$



Állítás: Egy kód prefix kód \Leftrightarrow Csak a levelekben vannak csúcscímkék.

McMillan-egyenlőtlenség:

Legyen A egy n elemű ábécé: $A = \{a_1, a_2, \dots, a_n\}$

Legyen B egy r elemű ábécé: $B = \{b_1, b_2, \dots, b_r\}$ ($r \geq 2$)

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

Legyen $l_j = |\varphi(a_j)|$ (azaz a j-edik betű kódjának a hossza)

Egyrészt ha a kód felbontható kód, akkor:

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

Másrészt ha l_1, l_2, \dots, l_n olyan, hogy:

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

akkor $A \rightarrow B$ felbontható kód, sőt prefix kód is, és $|\varphi(a_j)| = l_j$.

Következmény: Minden felbontható kódhoz van vele azonos szóhosszakkal bíró prefix kód is.

Példa a McMillan-egyenlőtlenség használatára:

Kérdés: Hány elemű A ábécét tudunk lekódolni 7 biten?

Egy bit 0 vagy 1 lehet, így 2 lehetőség van, tehát a válasz: $2^7 = 128$.

De ezt a kérdést megválaszolhatjuk a McMillan-egyenlőtlenség segítségével is.

$B = \{0, 1\}$, $r=2$, és minden j-re: $l_j=7$. Így:

$$\sum_{j=1}^n \frac{1}{2^7} = \frac{n}{2^7} \leq 1$$

Ezért $n \leq 2^7 = 128$, tehát a maximum **128** elemű ábécét tudunk lekódolni.

Gyakori és ritka betűk a kódolásban:

Legyen A egy n elemű ábécé: $A = \{a_1, a_2, \dots, a_n\}$

Legyen p_1, p_2, \dots, p_n számok az A ábécé eloszlása (betűk előfordulásának százalékos valószínűsége), úgy hogy $p_1 + p_2 + \dots + p_n = 1$.

Ha egy $\varphi: A \rightarrow B^+$ kód l_1, l_2, \dots, l_n szóhosszakkal rendelkezik, akkor

$\bar{l} = \sum_{j=1}^n p_j * l_j$ összeget a kód átlagos szóhosszúságának nevezzük.

Például:

$\varphi: \begin{array}{lll} a \rightarrow 10 & l_1 = 2 & p_1 = 0.4 \text{ (40\% a valószínűsége, hogy a betű van egy szövegben)} \\ b \rightarrow 1 & l_2 = 1 & p_2 = 0.35 \text{ (35\% a valószínűsége, hogy b betű van egy szövegben)} \\ c \rightarrow 00 & l_3 = 2 & p_3 = 0.25 \text{ (25\% a valószínűsége, hogy c betű van egy szövegben)} \end{array}$

$$\bar{l} = 0.4 * 2 + 0.35 * 1 + 0.25 * 2 = 1,65$$

(Azaz egy 100 hosszú random szöveget valószínűleg $100 * 1,65 = 165$ karakter hosszú szövegre tudunk lekódolni ezzel a módszerrel.)

Cél: \bar{l} minimalizálása!

A fenti példa esetében például 1,65-ről 1,6-ra javítható az átlagos kódhossz, ha a leggyakoribb betűhöz (a) rendeljük a legrövidebb kódot (1).

Optimális kód:

Olyan felbontható betűnkénti kód, melynek adott elemszámú ábécével és eloszlással az átlagos szóhosszúsága minimális.

A **Huffman-kód** például optimális:

$$H \leq \bar{l} < H+1$$

ahol H az entrópia.

Entrópia:

Legyen a kódoló ábécé r elemű, ekkor (p_1, p_2, \dots, p_n) .eloszlású forrás entrópiája:

$$H_r(p_1, p_2, \dots, p_n) = \sum_{j=1}^n -p_j \cdot \log_r(p_j)$$

Előre nem megjósolható dolgok (pl. *fejet vagy írást dobok: 50%-50%*) entrópiája **1**.
Nagyon valószínűsíthető dolgok (pl. *holnap nem találkozom Britney Spears-sel: 99,9%-0,1%*) entrópiája pedig nagyon alacsony: **1/100**.

Shannon-tétele zajmentes csatornára:

Létezik olyan felbontható kód, amelyre a kódoló ábécé r elemű, és

$$\bar{l} < H_r(p_1, p_2, \dots, p_n) + 1$$

Másrészt minden felbontható kódra igaz, hogy:

$$\bar{l} \geq H_r(p_1, p_2, \dots, p_n)$$

A tételt kimondja, hogy a tömörítésnek van korlátja, hisz az átlagos szóhosszúságnak mindig kisebbnek kell lennie, mint az entrópia + 1.

A Huffman-kód:

Bemenet: Egy ábécé betűi eloszlásokkal (előfordulási valószínűségek). Pl.: A: 17%

Kimenet: Olyan prefix kód, ahol az átlagos szóhossz minimális.

Huffman-kód konstruálása:

Legyenek adottak az ábécé következő betűi a következő eloszlásokkal.

A: 17%, B: 31%, C: 17%, D: 13%, E: 7%, F: 9%, G: 6%.

1.) Rendezzük csökkenő sorrendbe a valószínűségeket!

B: 31%

A: 17%

C: 17%

D: 13%

F: 9%

E: 7%

G: 6%

2.) Vonjuk össze a két legkisebb valószínűségű betűt egy szóvá!

B: 31%

A: 17%

C: 17%

EG: 13%

D: 13%

F: 9%

3.) Folytassuk ezt addig, amíg már csak két valószínűség marad!

(figyelni a zárójelekre!)

B: 31%

B: 31%

(DF)A: 39%

B(C(EG)): 61%

DF: 22%

C(EG): 30%

B: 31%

(DF)A: 39%

A: 17%

DF: 22%

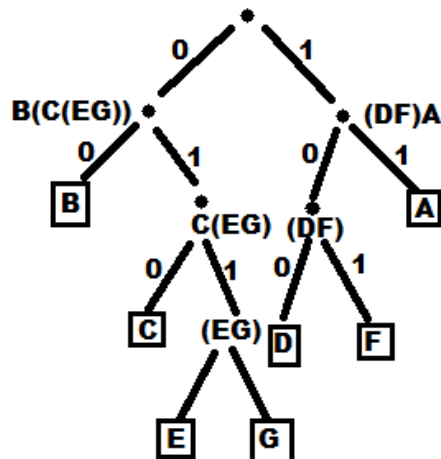
C(EG): 30%

C: 17%

A: 17%

EG: 13%

4.) Ez alapján alkossuk meg a kódfát (a zárójelek mentén szedjük szét a szavakat!)



5.) A kódfából (fentről lefelé) leolvashatók a betűk Huffman-kód szerinti kódjai:

A: 11

E: 0110

B: 00

F: 101

C: 010

G: 0111

D: 100

Látható, hogy a gyakori betűk (A, B) kódja rövid, a ritka betűké (E, G) pedig hosszú!

Mi a helyzet, ha a kódoló ábécénk nem kétbetűs $\{0, 1\}$, hanem három $\{0, 1, 2\}$?
 Ilyenkor nem a kettő, hanem a három legkisebb valószínű betűt vonjuk össze.

Az optimális kód tulajdonságai:

Legyen B ábécé szavainak száma r .

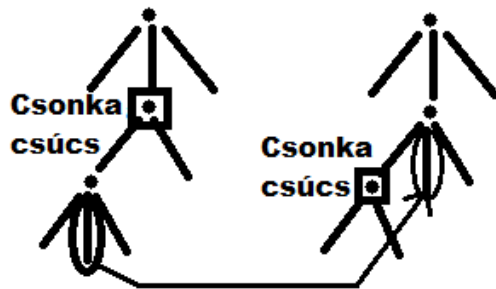
(0) A kód prefix kód.

(1) $p_m > p_n \Rightarrow l_m \leq l_n$ (A gyakori betű kódjának minél rövidebbnek kell lennie)

(2) Csak az utolsó előtti szinten lehet a kódfában csonka (r -nél kisebb kifokú) csúcs, de annak is legalább kettő a kifoka.

Bizonyítás:

A nem az utolsó előtti szinten lévő csonka csúcs teljessé tehető egy utolsó előtti szintből induló él áthelyezésével, így az utolsó előtti szinten lévő csúcs lesz csonka.



(3) Van olyan optimális kód, amelynek a kódfájában csak egy csonka csúcs van.

(4) Ha a kódfa r -felé ágazik, akkor:

van csonka csúcs a kódfában $\Leftrightarrow r \nmid n \pmod{r-1}$ (nem kongruens)

A csonka csúcs fokszáma: $m = 2 + (n-2) \pmod{r-1}$

Tétel:

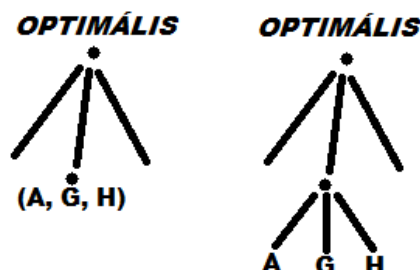
Ha a fenti 4 feltétel teljesül, és az összevonásokat (pl.: $E+G = EG$) a Huffman-kód szerint végezzük el, akkor optimális kódot kapunk.

Bizonyítás:

Teljes indukcióval bizonyítunk.

Kezdőlépés: Ha a kódolt ábécé $\leq r$, akkor a csupa 1 betűs szót tartalmazó kódolás az ideális. (pl.: kódoló ábécé: $\{0,1,2\}$, kódolandó betűk: $\{A, B\}$)

Indukció: Ha az összevont ábécére a kódfánk optimális, akkor az összevont csúcsoknak a gyerekként való beillesztése is optimális lesz. (Nem bizonyítjuk!)



Így a Huffman-kód optimális, de csak a betűnkénti kódolásra. A betűk viszont nem függetlenek egymástól (pl. a GY sokkal gyakrabban fordul elő a magyar nyelvben, mint az YG), így a Huffman-kód csak egy része a bonyolultabb kódolási eljárásoknak (például az MP3-formátumnak).

Hibakorlátozó kódolás

Ez már *szó* \rightarrow *szó* kódolás!

Cél: *Biztonságosan* tudjuk továbbítani az információt!

(A kommunikációs csatorna hibája esetén is tudja értelmezni a címzett az üzenetet.)

Példa: Személyi szám, könyvek ISBN-kódja, áruk vonalkódja stb.

(Személyi számoknál az utolsó számjegy az ellenőrzésre való, megállapítható belőle, hogyha valamelyik előző számjegy hibás, például elírták.)

Tulajdonképpen **n** hosszú szavakhoz **m** ($n \leq m$) hosszú kódszavakat rendelünk.

Például: $n=3$, $m=7$

$000 \rightarrow 0001000$

$001 \rightarrow 0010001$

Ennek a kódnak a logikája a következő: $abc \rightarrow abc[(1+a+b+c) \bmod 2]abc$

Így ha például 1000111 üzenetet kapjuk, akkor tudjuk, hogy biztosan hibás.

Hibas szám:

Megsérült karakterek száma a kódszóban.

Egy kód t-hibajelző:

Minden olyan esetben jelzi a hibát, ha legfeljebb t helyen volt hiba.

(A fenti kód például 2-hibajelző.)

Egy kód pontosan t-hibajelző:

t hibát biztosan jelez, de $(t+1)$ -et már nem mindig.

Egy kód t-hibajavító:

A t hibát ki is tudja javítani.

Egy kód pontosan t-hibajavító:

t hibát biztosan ki tud javítani, de $(t+1)$ -et már nem mindig.

A cél minél nagyobb t -s hibajavító kód létrehozása!

Hamming-távolság:

u és v n hosszú szavak Hamming-távolsága: (d -distance)

$d(u,v)$ = azon párok száma, ahol u és v eltérő betűket tartalmaz.

Például:

$u = 001010$

$v = 010110$

$d(u,v) = 3$

A Hamming-távolság tulajdonságai:

- (1) $d(u,v) \geq 0 \quad \forall u, v$ szóra
- (2) $d(u,v) = 0 \iff u = v$
- (3) $d(u,v) = d(v,u) \quad \forall u, v$ szóra (*szimmetria*)
- (4) $d(u,z) \leq d(u,v) + d(v,z) \quad \forall u, v, z$ szóra (*háromszög egyenlőtlenség*)

Gyakran előfordul, hogy egy kódábécé betűi Abel-csoportot adnak a mod-os összeadással (pl.: $\{0,1\}$, $+(\text{mod } 2)$).

Ilyenkor beszélhetünk egy **kódszó súlyáról** is. (*w-weight*)

$w(u)$ = A kódszó nullától különböző karaktereinek száma

Például:

$u = 001010$

$w(u) = 2$

A súly tulajdonságai:

- (1) $w(00\dots 0) = 0$
- (2) $w(\text{bármilyen más szó}) > 0$
- (3) $w(u) = d(u, (00\dots 0))$ (*u szó súlya a csupa nullát tartalmazó szótól való távolsága*)
- (4) $d(u,v) = w(u-v)$

Például:

$u = (32201223)$

$v = (21201212) \quad d(u,v) = 4$

$u-v = (11000011) \quad w(u-v) = 4$

Kód:

Kódszavak halmaza, jele: C (*c-code*)

Kód távolsága:

C kód távolsága:

$$d(C) = \min_{u \neq v} d(u,v)$$

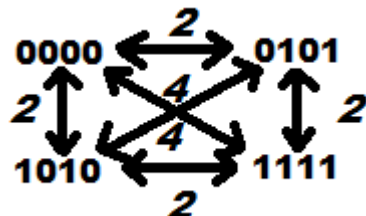
$$u \neq v$$

$$u, v \in C$$

Például:

$C = \{0000, 0101, 1010, 1111\}$

Kódszavak távolságjai felrajzolva egy diagramban:



A kód távolsága: $d(C) = 2$

Kód súlya:

Ha C kód Abel-csoport, akkor:

$$w(C) = \min w(u)$$

$$u \neq 00\dots 0$$

$$u, v \in C$$

Például:

$$C = \{0000, 0101, 1010, 1111\} \quad (\text{Ez egy Abel-csoport})$$

$$\emptyset \quad 2 \quad 2 \quad 4$$

Így tehát $w(C) = 2$

Állítás:

Ha C additív (összeadásra nézve) Abel-csoport, akkor $d(C) = w(C)$.

Bizonyítás:

(1) Minden súly távolság is egyben, méghozzá a $(00\dots 0)$ szótól való távolság, ami mindenképp benne van a kódban, hisz a kód Abel-csoport.

(2) Minden távolság súly is egyben, hisz $w(u-v) = d(u, v)$.

Megjegyzés:

A gyakorlatban C tényleg nagyon sokszor Abel-csoport (pl. bináris kódok esetén).

Ha N a kódszavak száma, akkor súlyból $N-1$ db, távolságból viszont $\binom{N}{2}$ van.

Tehát súlyból sokkal kevesebb van, így célszerű azokat számolni!

Állítás:

Legyen C egy kód, a távolsága pedig legyen d .

Ekkor C hibajelző képessége pontosan: $(d-1)$

Ekkor C hibajavító képessége pontosan: $\left\lfloor \frac{d-1}{2} \right\rfloor$ (alsó egész rész)

Bizonyítás:

Tegyük fel, hogy u szót akarjuk küldeni, de v szó érkezik meg t hibával.

Ekkor $d(u, v) = t$.

Hibajelzés:

Ha $t \leq d-1$, akkor v nem lehet kódszó, mert u kódszó, és $t < d \leq \min d(u, z) \forall u \neq z$ szóra. Ilyenkor biztos, hogy v nem kódszó, azaz biztosan észleljük a hibát.

Ha $t=d$, akkor létezik olyan v szó, hogy $d(u, v) = d$.

Ekkor pedig v -t egy helyes kódszónak észleljük, azaz nem látjuk, hogy hibás, pedig valójában az, csak $t=d$ hibával.

Hibajavítás:

Ha $t \leq \frac{d-1}{2}$, akkor $2t < d$.

Viszont lehetnek olyan $u_1, u_2 \in C$ kódszavak, hogy $d(u_1, v) \leq t$ és $d(v, u_2) \leq t$.

Ekkor a Hamming-távolság negyedik tulajdonsága (háromszög-egyenlőtlenség) miatt:

$$d(u_1, u_2) \leq d(u_1, v) + d(v, u_2) \leq 2t < d, \text{ ami ellentmondás hisz:}$$

$$d(u_1, u_2) < d, \text{ de } d\text{-nél nem lehet kisebb távolság (kód távolsága definíció).}$$

Cél: Minél nagyobb távolságú kódot csinálni, de olcsón!

Azaz ne legyen se túl hosszú a kódszó, se túl bonyolult a kiszámítása.

Konkrét kódok:

A kódolandó szavak legyenek $\{0,1\}^m$ (m hosszú 0-ból és 1-ből álló szavak)

1.) Ismétléses kódok:

$u \rightarrow uu$ (pl. 010 \rightarrow 010010) 1-es hibajelző, nem hibajavító, $w = d = 2$.
 3-szori ismétlődéssel: $u \rightarrow uuu$ 2-es hibajelző, 1 hibajavító, $d = w = 3$.
 k-szori ismétlődéssel: $u \rightarrow k*u$ k-1 hibajelző, $d = w = k$.

2.) Paritásbit:

$u_1 u_2 u_3 \dots u_m \rightarrow u_1 u_2 u_3 \dots u_m ((u_1 + u_2 + \dots + u_m) \bmod 2)$

Például: 010 \rightarrow 0101 és 0101 \rightarrow 01010

Az utolsó ellenőrzőszámjegy a paritásbit.

$d = 2$. A kód 1-es hibajelző, de nem hibajavító.

3.) Kétdimenziós paritásbit

Készítünk egy $m = m_1 * m_2$ táblázatot (100 hosszú kód esetén pl. egy 10x10-est)

				m_1
0	1	...	1	<i>paritásbit (első sor paritásbitje)</i>
0	1	...	0	<i>pb</i>
...	<i>pb</i>
1	0	...	1	<i>pb</i>
m_2	<i>pb</i>	<i>pb</i>	<i>pb</i>	<i>pb</i>
				<i>PB (a paritásbitek paritásbitje)</i>
				<i>első oszlop paritásbitje</i>

$m_1 * m_2 \rightarrow m_1 * m_2 + (m_1 + m_2 + 1)$

Abból, hogy melyik sor és melyik oszlop paritásbitje hibás, meg lehet mondani, hogy konkrétan a táblázat melyik értéke volt hibás.

3-hibajelző, 1-hibajavító a kód, és $d = 4$ ($2*2$).

Hamming-korlát:

Legyen C egy q elemű ábécé feletti n hosszú szavakból álló t -hibajavító kód.

Ekkor:

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

Magyarázat:

q^n egy fix szám, a q elemű ábécé betűiből kirakható összes n hosszú szavak száma.

Látható, hogy $|C|$ és t nem lehet egyszerre nagy, azaz minél több kódszóból áll a kód, annál kisebb a hibajavító képessége.

Például:

Tudunk-e 5 hosszú kódszavakból 8 elemű kódot 1-es hibajavító képességgel?

Ábécé: $\{0,1\}$, $q = |\{0,1\}| = 2$, $|C| = 8$, $t=1$, $n=5$

$$8 * \sum_{j=0}^1 \binom{5}{j} * (2-1)^j \leq 2^5 = 32$$

$$8 * (1 + 5) = 48 \leq 32$$

Ez nem igaz, tehát nem a válasz a kérdésre.

Bizonyítás:

Ha a kód t -hibajavító, akkor bármilyen n hosszú szó legfeljebb 1 kódszótól van $\leq t$ távolságra.

Geometriailag ezt körökkel lehet jól ábrázolni, ahol c kódszó a kör középpontja, t pedig a kör sugara.

Kör: $\{u \in C \text{ kódszavak, ahol } d(c,u) \leq t\}$

A körök mind diszjunktak, ez pedig bizonyítja az állítást.

Egy kódszótól j távolságra pontosan ennyi szó van:

$$\binom{n}{j} * (q-1)^j$$

Hol Hol
tér el? tér el?

Egy kódszótól legfeljebb t távolságra pontosan ennyi szó van:

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

Mivel a körök diszjunktak, és q^n az összes n hosszú lehetséges szó (q elemű abc):

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

Körök **Körök mérete**
Száma



Singleton-korlát:

Ha egy q elemű ábécé feletti n hosszú szavakból álló C kód távolsága d , akkor:

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

Bizonyítás:

Mivel az összes kódszó távolsága $\geq d$, akkor bármely két kódszóból az utolsó $d-1$ betűt eltávolítva a maradék $n-(d-1) = n-d+1$ hosszú szavak még mindig különböznek.
 q elemű ábécéből képzett $n-d+1$ hosszú szavakból pedig q^{n-d+1} lehet.

Például: $C = \{0000, 0101, 1010, 1111\}$ kód esetén:

$$q = |\{0,1\}| = 2, n=4, d(C)=2$$

Ha minden kódszóból eltávolítjuk az utolsó $d-1$ ($2-1=1$) betűt, akkor is különböző lesz mindegyik kódszó: $C' = \{000, 010, 101, 111\}$

A Singleton-korlát is stimmel, hisz:

$$4 \leq 2^{4-2+1} = 2^3 = 8$$

Maximális távolságú szeparábilis kód (MDS-kód):

Olyan kód, melynél a Singleton-korlátban egyenlőség van.

$$|C| = q^{n-d+1}$$

Az ilyen kód szétválasztható üzenetre és ellenőrző bitekre.

Lineáris kód:

Legyen K egy véges test. A kódunk lineáris kód, ha a kódszavak K^n n -dimenziós vektortér egy *alterét* alkotják.

(A kódszavak összege és skalárral való szorzás is kódszó lesz.)

Generátormátrix:

Bármely C lineáris kódhoz létezik (akár több is) olyan G generátormátrix, amire:

$C = \{G * v \mid v \in K^m \text{ eredeti szó}\}$, ahol C egy n -dimenziós altér.

Ellenőrzőmátrix:

Minden k -dimenziós altérhez létezik (akár több is) $((n-k) \times n)$ -es H ellenőrzőmátrix:

$$w \in C \iff H * w = 0$$

Így lehet leellenőrizni, hogy adott w szó kódszó-e C kódban. Ha igen, akkor $H * w = 0$.

Megjegyzés:

G és H nem egyértelmű. G -nek az oszlopain, H -nek a sorain végezhetünk elemi transzformációkat (pl. *skalárral való szorzás, kivonás egymásból*), és úgyis generátormátrix illetve ellenőrzőmátrix marad.

Állítás:

Egy H ellenőrző mátrixú kód távolsága a legkisebb d szám, melyre igaz, hogy H -nak bármelyik $d-1$ oszlopa lineárisan független, de van d olyan oszlop, amelyik lineárisan összefüggő.

Egy H ellenőrző mátrixú kód súlya H azon oszlopainak száma, amelyek lineáris kombinációja 0.

Létezik j súlyú kódszó \iff Létezik j db olyan oszlop, amely összefüggő.

Például:

Vegyünk $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ testet.

Efelett az $(a, b, c) \rightarrow (a, b, c, a+b+c, a+2b+3c)$ kód lineáris kód.

$C = \{a, b, c, (a+b+c), (a+2b+3c)\}$ egy 3 dimenziós altér az 5 dimenziós térben.

Generátormátrixa:

$$\mathbf{G}_{5 \times 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} \text{ mert } \begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} * = \begin{pmatrix} a \\ b \\ c \\ a+b+c \\ a+2b+3c \end{pmatrix}$$

Ellenőrzőmátrixa:

$$\mathbf{H}_{2 \times 5} = \begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 1 & 2 & 3 & 0 & -1 \end{pmatrix} \text{ mert } \begin{pmatrix} a \\ b \\ c \\ a+b+c \\ a+2b+3c \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 1 & 2 & 3 & 0 & -1 \end{pmatrix} * = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ szindróma}$$

Szindróma:

Ha H egy ellenőrző mátrix, és $v \in K^m$, akkor a $H*v$ vektor a szindróma (hibajellemző).

Ha a szindróma nulla, akkor $w \in C$, azaz w szó kódszó C -ben.

Ha a szindróma nem nulla, akkor w nem kódszó C -ben, vagyis w hibás.

Vannak módszerek, melyekkel a szindrómából visszafejthető, hogy a küldött üzenet melyik része volt hibás (pl. Fano-kód).

Hamming-kód (tökéletes/perfekt kód):

Olyan kód, amelyre a Hamming-korlát éles.

Polinom kódok:

Vegyünk egy g generátorphinomot, például $g = 2x^2 + 3x + 7$.

Ekkor a kódolás a következő lesz: $\mathbf{f} \rightarrow \mathbf{f} * \mathbf{g}$

Vektorokra átfogalmazva:

$$\mathbf{f} = f_0 + f_1x + f_2x^2 + \dots + f_{k-1}x^{k-1}$$

$$\mathbf{f} * \mathbf{g} = 7f_0 + (7f_1 + 3f_0)x + (7f_2 + 3f_1 + 2f_0)x^2 + (7f_3 + 3f_2 + 2f_1)x^3 + \dots$$

Kódolandó polinom: k -nál kisebb fokú polinomok:

Generátorphinom: m fokú polinom.

Kódszavak: $(k+m)$ hosszú szavakból álló k -dimenziós altér.

Generátormátrixa:

$$\mathbf{G} = \begin{pmatrix} 7 & 0 & \dots & \dots & \dots & \dots & 0 \\ 3 & 7 & 0 & \dots & \dots & \dots & 0 \\ 2 & 3 & 7 & 0 & \dots & \dots & 0 \\ 0 & 2 & 3 & 7 & 0 & \dots & 0 \\ 0 & 0 & 2 & 3 & 7 & 0 & 0 \end{pmatrix}$$

Mi felel meg itt H-nak (az ellenőrzőmátrixnak)?

Az adott polinom akkor van benne a kódban, ha maradékosan elosztva g-vel, a maradék nulla lesz. Tehát maga a maradék a szindróma.

Polinomkód például a **CRC-kódcsalád**.

Tipikusan d nem nagyon nagy, de minden olyan hibasorozatot észrevesz, amelynek a foka < g foka.

Vandermonde-mátrix:

Például:

$$\mathbf{V}_{m \times m} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_m \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_m^2 \\ \dots & \dots & \dots & \dots & \dots \\ x_1^{m-1} & x_2^{m-1} & x_3^{m-1} & \dots & x_m^{m-1} \end{pmatrix} \quad \mathbf{V}_{4 \times 4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 9 & 16 \\ 1 & 8 & 27 & 64 \end{pmatrix}$$

$$\det(\mathbf{V}) = \prod_{j>i} (x_j - x_i)$$

$$\det(\mathbf{V}) = (2-1) \cdot (3-1) \cdot (4-1) \cdot (3-2) \cdot (4-2) \cdot (4-3)$$

Következmény:

Az oszlopok lineárisan függetlenek, ha $x_i \neq x_j$

Reed-Solomon kódok:

(CD-n, DVD-n ezek védik az adatokat a karcolódástól)

Legyen \mathbf{K} egy véges test, $|\mathbf{K}| = q$.

Legyen k a kódolandó szavak hossza.

$\mathbf{K}^* = \mathbf{K} \setminus \{0\}$ egyik eleme legyen α .

α rendje legyen n . (azaz $\alpha^1 \neq 1, \alpha^2 \neq 1, \dots, \alpha^{n-1} \neq 1$, de $\alpha^n = 1$)

Legyen $m = n - k$.

Ekkor g generátorpolinom $= (x - \alpha) \cdot (x - \alpha^2) \cdot \dots \cdot (x - \alpha^m)$

Így ezzel a generátorpolinommal létrehozhatunk egy $[\mathbf{n}, \mathbf{k}]_q$ – kódot.

Kiszámolható, hogy a H-mátrix h_{ij} eleme:

$$h_{ij} = \alpha^{ij}$$

H bármely m oszlopa egymás után téve egy **Vandermonde-mátrixot** ad lineárisan független oszlopokkal.

$d = m + 1 = n - k + 1$, azaz ez a **maximális távolságú kód a Singleton-korlát szerint**.

Algoritmusok

Számítási eljárás:

$C = (Q, Q_b, Q_k, f)$ rendezett négyes, ahol:

Q : állapotok halmaza

$Q_b \subseteq Q$: bemeneti állapotok halmaza

$Q_k \subseteq Q$: kimeneti állapotok halmaza

$f: Q \rightarrow Q$ átmeneti függvény, ahol

$f(q) = q$, ha $q \in Q_k$ (a kimeneti állapotok nem változhatnak meg)

Ha $x \in Q_b$, akkor x definiál egy **számítási sorozatot**:

$q_0, q_1, q_2 \dots q_n$
 $q_0 = x$ és $q_{i+1} = f(q_i) \quad \forall i$ -re

A számítás **n lépésben véget ér**, ha n a legkisebb olyan egész szám, amelyre:

$q_n \in Q_k$
 onnantól pedig $q_n = q_{n+1} = q_{n+2} = \dots$
 q_n -t nevezik **a számítás eredményének** is.

Például: **Euklideszi algoritmus**

Bemenet = $Q_b = \mathbf{Z} \times \mathbf{Z}$ (egy számpár)

Kimenet = $Q_k = \mathbf{Z}$ (legnagyobb közös osztó)

Állapotok = $Q = Q_b \cup Q_k \cup (\mathbf{Z} \times \mathbf{Z} \times \{2,3\})$

(közbülső állapotok: 2 és 3 címkék, hogy épp a programkód melyik részén tartunk).

Átmeneti függvény:

Q_b : $f(a,b) = (a,b,2)$

Q_k : $f(a) = (a)$

$f(a,b,2) = \begin{cases} a, & \text{ha } b = 0 \\ (a,b,3), & \text{ha } b \neq 0 \end{cases}$

$f(a,b,3) = (b, a \bmod b, 2)$

2-es címke: $\text{if}(b==0) \{ \text{RETURN } a \}$

3-as címke: $a=b; b = a \bmod b; \text{GOTO } 2$

Bemenet: (18, 7)

$f: 18 = 7 \cdot 2 + 4 \quad (a=18, b=7)$

$7 = 4 \cdot 1 + 3 \quad (a=7, b=4)$

$4 = 3 \cdot 1 + 1 \quad (a=4, b=3)$

$3 = 1 \cdot 3 + 0 \quad (a=3, b=1)$

$1 = 1 \cdot 0 + 0 \quad (a=1, b=0)$

Kimenet: 1

Algoritmusosan:

$(18,7) \rightarrow (18,7,2) \xrightarrow{7 \neq 0} (18,7,3) \rightarrow (7,4,2) \xrightarrow{4 \neq 0} (7,4,3) \rightarrow (4,3,2) \xrightarrow{3 \neq 0} (4,3,3) \rightarrow (3,1,2) \xrightarrow{1 \neq 0} (3,1,3) \xrightarrow{0=0} (1,0,2) \rightarrow (1) \rightarrow (1) \rightarrow \dots$

Szimulálás:

Legyenek $C = (Q, Q_b, Q_k, f)$ és $C' = (Q', Q_b', Q_k', f')$ számítási eljárások.

Azt mondjuk, hogy **C' szimulálja C -t**, ha van szimuláló kódolás, azaz létezik:

h: $Q' \rightarrow Q$ állapotdekódolás

g: $Q_b \rightarrow Q_b'$ bemeneti kódolás

k: $Q' \rightarrow N^+$ szimuláló lépések száma

Valamint teljesülnek az alábbi feltételek:

(1): $x \in Q_b$ -re C számítási eljárás akkor adja $y \in Q_k$ eredményt, ha C' számítási eljárás a $g(x)$ bemenettel olyan $y' \in Q_k'$ eredményt ad, hogy $h(y') = y$.

(2): $\forall q' \in Q'$ állaptra igaz, hogy:

$$f(h(q)) = h(f' \circ f' \circ f' \circ f' \dots \circ f'(q')) \quad (k(q') \text{ db } f' \text{ van a}$$

kompozícióban)

Két számítási eljárást „ugyanannak” tekintünk, ha szimulálják egymást.

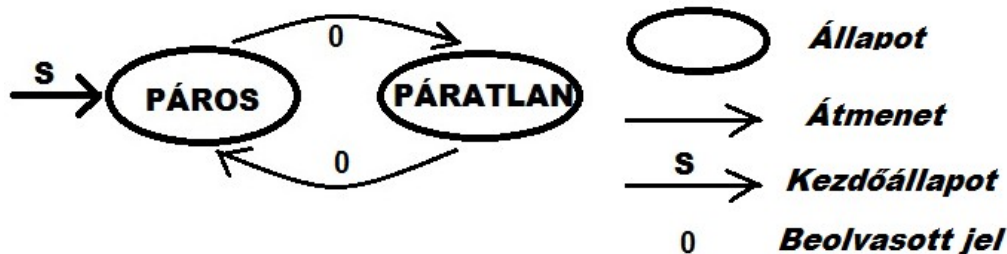
Például: C++-ban lehet írni Java virtuális gépet, Java-ban pedig lehet írni C++ fordítót, így a C++ szimulálja a Java-t, és a Java is szimulálja a C++-t.

Cél: A bonyolult algoritmusok legyenek szimulálhatóak a legalapvetőbbekkel, így elég csak azokat vizsgálni.

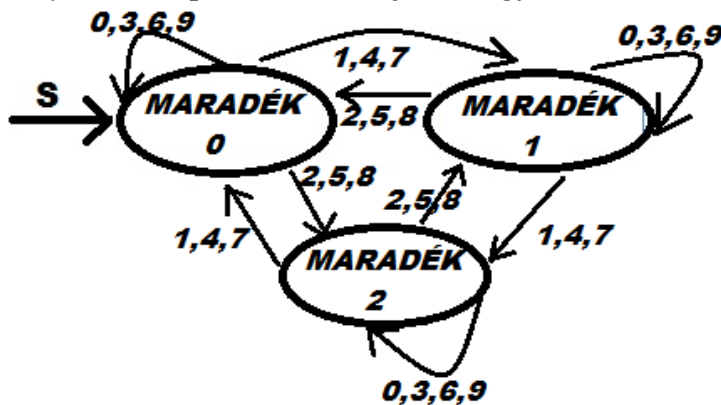
Véges automata:

Állapotokból áll, az átmenet az állapotok között pedig a beolvasott jelek hatására történik.

Egyszerűbb példa: Számoljuk meg, hogy egy csupa 0-ból álló szóban páros vagy páratlan számú 0 van-e. Például 0000 \rightarrow páros, 00000 \rightarrow páratlan.



Bonyolultabb példa: Számoljuk ki egy szám 3-mal való maradékát.



Pl: 223 \rightarrow Maradék 0 \rightarrow 2 \rightarrow Maradék 2 \rightarrow 2 \rightarrow Maradék 1 \rightarrow 3 \rightarrow Maradék 1

Turing-gép:

Tulajdonképpen egy véges automata memóriával (szalagokkal).

Elv: Van végtelen sok papírunk, de egy adott pillanatban a sok papír közül mindig csak egy apró részt figyelhetünk meg, csak ezen az apró részen dolgozhatunk.

Nagyon egyszerű szabályok alapján módosítjuk a papír tartalmát, pár dolgot pedig fejben tartunk.

Formális definíció:

Alkatrészek:

- **vezérlőegység:** véges sok lehetséges belső állapota van.

- **k db mindkét irányban végtelen szalag:** mezőkre vannak osztva ($k \geq 1$)

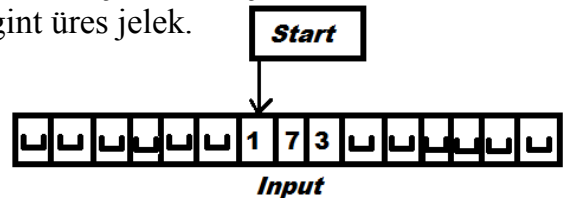
- **egy véges ábécé:** a szalag minden mezőjén pontosan egy betű állhat.

Van egy speciális jel: \square (üres jel)

A szavaknak csak véges sok pozíciójában lehet nem üres jel.

Működése:

- **Bemenet:** A vezérlőegység start állapotban van a szalag egy mezőjén.
A szalagon a vezérlőegységtől balra üres jelek, tőle jobbra az első üres jelig a bemenet (input), utána megint üres jelek.



- **Állapotfüggvény:** A változás attól függ, hogy a vezérlőegység melyik állapotban van, és hogy mit olvas a szalag azon mezőjéből, ahol éppen áll. Ennek hatására **új állapotba kerül** (lehet az is, ami eddig volt), **jelet ír a szalagra** (írhatja ugyanazt is, ami előtte volt rajta), és **jobbra, balra, vagy semerre mozdul egy mezőt**.
- **Kimenet:** Ha a vezérlőegység elfogadó állapotba jut, akkor megáll.
A kimenet az, ami ebben a pillanatban a szalagon van.

Az állapotfüggvény megadása:

Legyen **A** a szalagábécé, **B** pedig a belső állapotok halmaza. Ekkor az állapotfüggvény

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

(mozgás iránya)

Példa Turing-gépre:

Bemenet: Egy nullákból és egyekből álló string.

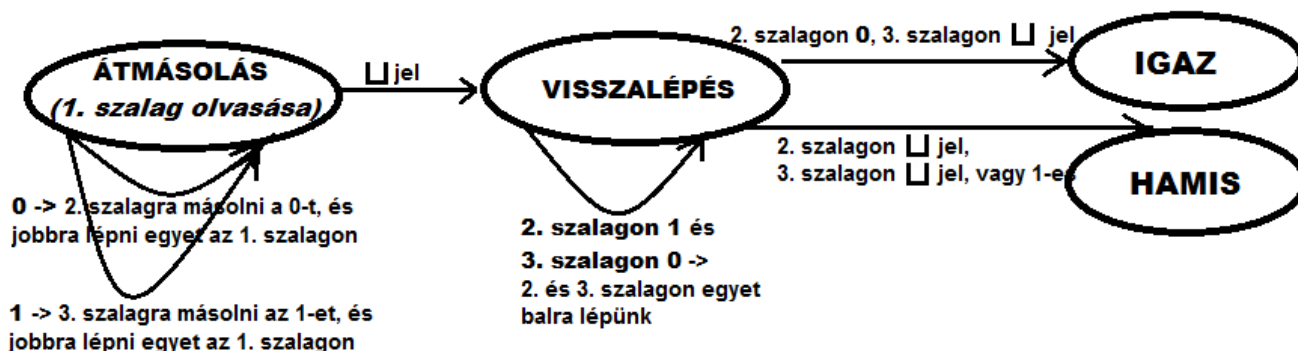
Feladat: Eldönteni, hogy 0-ból több van-e, mint 1-esből, vagy sem.

3 db szalagos Turing gépet kell csinálni.

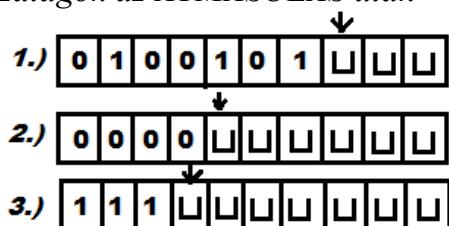
Első szalag: Bemenet

Második szalag: Kezdetben üres, ide írjuk majd a nullákat

Harmadik szalag: Kezdetben üres, ide írjuk majd az egyeket.



Szalagok az ÁTMÁSOLÁS után



Nagyon egyszerű és látszólag gyenge a Turing-gép, de mindent meg lehet vele oldani vele, amit például Java-ban meg lehet oldani.

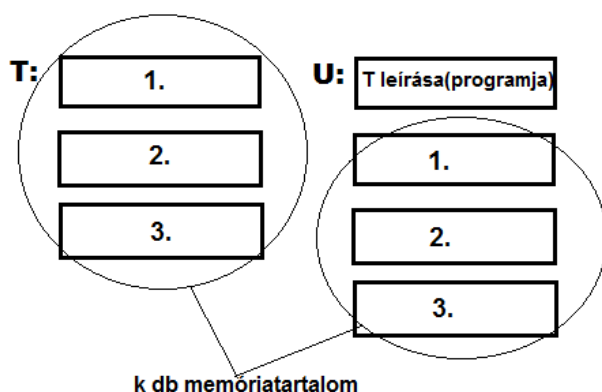
Állítás: Egy k szalagos T Turing-gép szimulálható S egyszalagos Turing-géppel. Ha T t lépésben számol, akkor S $2kt * (2t+3)$ (*kb. konstans * t^2*) lépésben számol.

Állítás: Minden Turing-gép leírható véges sok adattal (állapotok és állapotátmeneti szabályok). Mindez kódolható 0-k és 1-ek sorozataként.

Így létezik ***univerzális Turing-gép*** ($k+1$ szalagos).

Bármely k szalagos T Turing-gép esetében az U első szalagjára T kódját írva, a többi k szalagon U a T működését szimulálja, azaz bármely Turing-gép szimulálható U -val.

Tulajdonképpen U egy programozható Turing-gép.



Vannak algoritmikusan megoldhatatlan problémák:

Például:

- Egy egyenletrendszernek van-e egész megoldása?
- Egy Turing-gép még nem állt meg, vagy sosem fog megállni (végtelen ciklus)?
- Adott Turing-gép adott bemenetet elfogad, elutasít vagy végtelen ciklusba kerül?

Ezeket még Turing-géppel sem lehet megoldani, mert olyan sokfajta különböző eset van, hogy nincs rájuk általános algoritmus.

RAM-gép:

Véletlen elérésű memóriával rendelkező gép, azaz a memória cellákat indexeléssel el lehet érni, például $M[0]$, $M[1]$, stb.

Részei:

- *Végtelen nagy memória véletlen eléréssel.*
Memóriacellák elérése: $M[0]$, $M[-1]$, $M[1]$, $M[-2]$, $M[2]$ stb.
Ebben egész számokat tárolunk, de csak véges sok nem nulla szám lehet benne.
- *3 regiszter: A, B és I*
- *Program, ami soronként hajtódik végre.*

Utasításkészlete:

- **CLR** (clear): $A \leftarrow 0$, azaz A regisztert kinullázza ($A=0$)
- **INC** (increase): $A \leftarrow A+1$ ($A=A+1$)
- **DEC** (decrease): $A \leftarrow A-1$ ($A=A-1$)
- **GETB**: $A \leftarrow B$ ($A=B$)
- **GETI**: $A \leftarrow I$ ($A=I$)
- **PUTB**: $B \leftarrow A$ ($B=A$)
- **PUTI**: $I \leftarrow A$ ($I=A$)
- **ADD**: $A \leftarrow B$ ($A=A+B$)
- **LD** (load): $A \leftarrow M[i]$, i-dik memóriacella tartalma A-ba
- **ST** (store): $M[i] \leftarrow A$, A tartalma i-dik memóriacellába
- **JNP címke** (jump non positive):
Ha $A \leq 0$, akkor a vezérlés a címke programsorra ugrik. (*GOTO*)

Minden Turing-gép szimulálható RAM-géppel, és minden RAM-gép szimulálható Turing-géppel.

Rekurzív függvények:

Képzeljünk el egy primitív programozási nyelvet, mely a következőkből épül fel.

Függvények: $\text{zeros}(n_1, n_2, \dots, n_k) \rightarrow 0$ (mindenre nullát ad)
 $\text{proj}_i(n_1, n_2, \dots, n_k) \rightarrow n_i$ (i-dik elemet adja vissza)
 $\text{succ}(n) \rightarrow n+1$ (a paraméter értéket eggyel megnöveli)

Működés: **kompozíció:** Ha f és g definiált, akkor $f \circ g$ is definiált.
(meghívhatunk a függvényen belül egy másik függvényt)

rekurzió: A függvényeket rekurzívan is használhatjuk.

minimalizáció: Megállapítja, hogy egy függvény mikor lesz először 0.

```
n=0;  
while(f(n) != 0) {n++;}  
return n;
```

Minden Turing-gép szimulálható rekurzív függvényekkel, és a rekurzív függvények is szimulálhatóak Turing-géppel.

Következtetés:

Szimulálható egymással a Turing-gép, a RAM-gép, a rekurzív függvények, a lambda-kalkulus, a C, a Java, a C++ templatek, stb.

Church-tézis:

Algoritmussal pontosan az számolható ki, ami Turing-géppel szimulálható.

Algoritmusok hatékonysága:

Legyenek f és $g: \mathbb{N} \rightarrow \mathbb{R}$ függvények.

$g \in O(f)$ (nagy ordó) vagy másféleképpen $g = O(f)$ egy olyan függvényhalmaz:

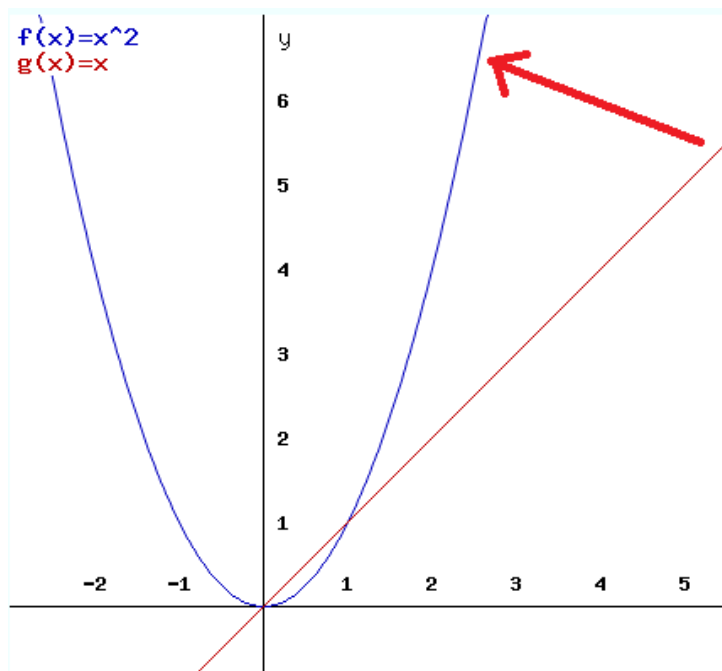
$$\exists c \in \mathbb{R}^+, n_0 \in \mathbb{N} : |g(n)| \leq c * |f(n)|, \text{ ha } n \geq n_0$$

(f hosszútávon – nagyon nagy n-eknél– nagyobb, mint g)

Például:

Legyenek $g(n) = n$ és $f(n) = n^2$ függvények.

Ekkor $g(n) \in O(f(n))$.



Lehet két függvény kölcsönösen nagy ordó egymásra:

Legyenek $f(n) = 5n^2$ és $g(n) = 6n^2$ függvények.

Ekkor $g(n) \in O(f(n))$, hisz ha $c = 2$, akkor $|6n^2| \leq 2 * |5n^2|$

És $f(n) \in O(g(n))$, hisz ha $c = 1$, akkor $|5n^2| \leq 1 * |6n^2|$

Fő felhasználási módjuk:

Egy algoritmus műveletigényét hasonlítjuk össze más algoritmusokkal.

Pl.: Két n jegyszámjegyű szám összeadása papíron: $n+1$ lépés = $O(n)$

Pl.: Két n jegyszámjegyű szám összeszorozása papíron: $n*n$ lépés = $O(n^2)$

Tételek:

- Ha egy Turing-gép minden bemenetre megáll (azaz sosem kerül végtelen ciklusba), akkor a futási ideje az a **t(n)** (t-time) függvény, amely az összes n hosszú bemeneten végzett lépésszámok maximuma (azaz a legrosszabb/leghosszabb eset lépésszáma).
- Egy Turing-gép tárigénye az a **s(n)** (s-storage) függvény, amely az összes n hosszú bemenetre felhasznált szalagok számának maximuma (azaz a legrosszabb/leghosszabb eset tárigénye).

Állítsuk sorba nagy ordó sebesség szerint a függvényeket!

$$\log n \leq \sqrt{n} \leq n / \log n \leq n \leq n^2 < n^3 < \dots < 2^n < 3^n < \dots < n! < \dots < n^n$$