Diszkrét matematika 2.

Fülöp Ágnes

ELTE IK Komputeralgebra Tanszék

2018. december 7.

Előadás:

1. előadás: 1-32 (szeptember 13.)
2. előadás: 33-53 (szeptember 27.)
3. előadás: 54-106 (október 4.)
4. előadás: 107-123 (október 11.)
5. előadás: 124-151 (október 18.)
6. előadás: 152-185 (október 25.)
7. előadás: 186-217 (november 8.)
8. előadás: 218-240 (november 15.)
9. előadás: 241-275 (november 22.)
10. előadás: 276-336 (november 29.)
11. előadás: 337-435 (december 6.)

Irányítatlan gráfok

Egy **irányítatlan gráf** vagy röviden **gráf** alatt egy

$$G = (\varphi, E, V)$$

hármast értünk, ahol
V a *csúcs*ok vagy *szögpont*ok halmaza,
E az *élek* halmaza,
a φ *illeszkedési leképezés* pedig egy E-t a V-beli elemekből álló rendezetlen párok halmazába képező leképezés.

Előfordulhat, hogy két pontot több különböző él is összeköt, sőt az is, hogy egy vagy több él egy pontot saját magával köt össze.

Illeszkedés

Ha valamely $e \in E$-re és $v \in V$-re $v \in \varphi(e)$, akkor azt mondjuk, hogy e *illeszkedik* v-re, vagy v *végpont*ja e-nek.

Megjegyezzük:
a jelölésből E elhagyható lenne, hiszen az $\mathrm{dmn}(\varphi)$, azonban V nem, mert nem biztos, hogy minden csúcsra illeszkedik él:

Izolált csúcs

azokat a csúcsokat, amelyekre nem illeszkedik él, *izolált csúcs*oknak nevezzük.

Üres gráf

Még az is előfordulhat, hogy az E halmaz üres; ilyen esetben *üres gráf*ról beszélünk.

Illeszkedési reláció

Az élek és csúcsok közötti illeszkedés egy reláció E és V között, amelyet *illeszkedési relációnak* nevezünk.

Szomszédos él

Két különböző *élt szomszédos*nak nevezünk, ha van olyan csúcs, amely mindkettőre illeszkedik.

Szomszédos csúcs

Két különböző *csúcsot* *szomszédos*-nak nevezünk, ha van olyan él, amelyre mindkettő illeszkedik.

Hurok él

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

Párhuzamos élek

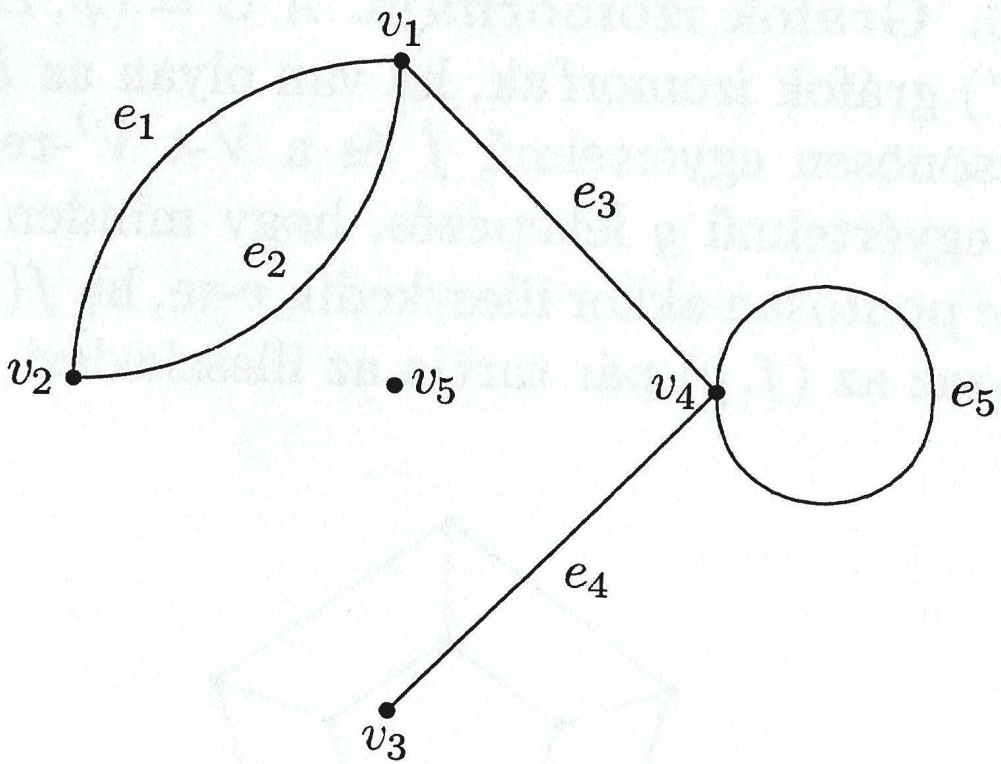
v_1, e_1, v_2, e_2, v_3 út is, vonal is;

$v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_3$ kör.

Ha az $e_1 \neq e_2$ élek ugyanazokra a csúcsokra illeszkednek, akkor *párhuzamos élek*ről vagy *többszörös élekről* beszélünk.

Egyszerű gráf

Ha egy gráf nem tartalmaz sem hurokélt, sem párhuzamos éleket, akkor *egyszerű gráfnak* nevezzük.



7.1. ábra

Ha $G = (\varphi, E, V)$ egy gráf és $S \subset V$, akkor jelölje $E(S)$ azon élek halmazát, amelyek egyik végpontja S-ben, a másik pedig $V \setminus S$-ben van.

Fokszám

Ha egy csúcsra csak véges sok él illeszkedik, akkor a csúcs *fokszám*án a rá illeszkedő élek számát értjük, a csúcsra illeszkedő hurokéleket kétszer számolva.

Egy $v \in V$ csúcs fokát rendszerint $\deg(v)$-vel vagy $d(v)$-vel jelöljük.

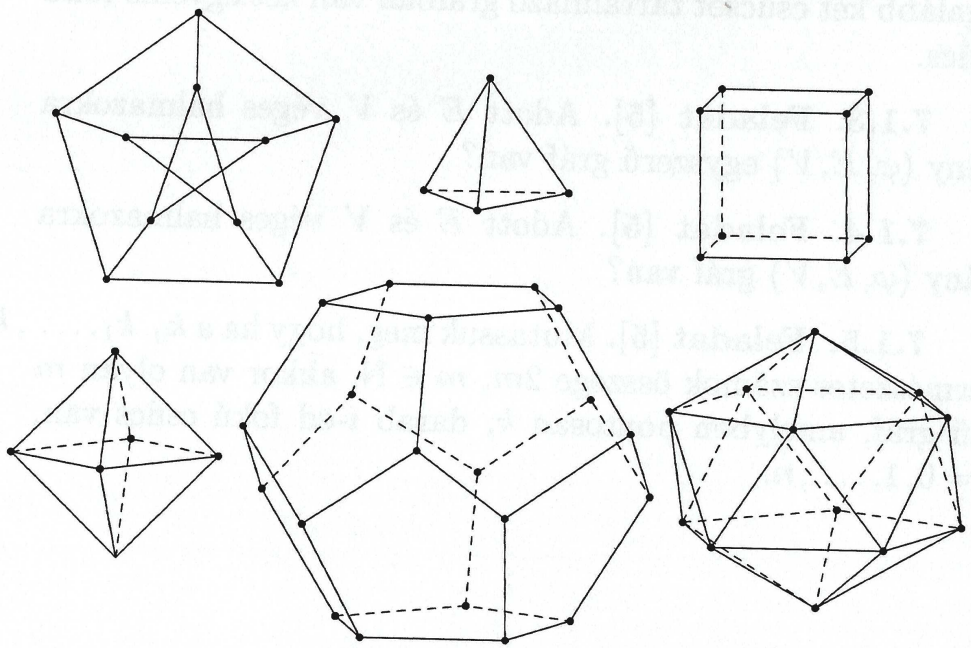
Reguláris gráf

Ha egy gráfban minden csúcs foka n, akkor *n-reguláris*nak nevezzük; *reguláris gráf* alatt olyan gráfot értünk, amely valamely $n \in \mathbb{N}$-re n-reguláris.

Példa:

Az n-reguláris gráfra a H_n n-dimenziós hiperkocka;
ennek csúcsai az n hosszú 0-1 sorozatok, és két csúcs akkor van összekötve, ha a két sorozat pontosan egy helyen különbözik.

További példák a *Petersen-gráf* és az öt szabályos test élei és csúcsai által alkotott gráfok.



7.2. ábra

Állítás

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

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

-Mivel minden újabb él a bal oldali összeget kettővel növeli.

Következmény

Ebből azonnal következik, hogy egy véges gráfban a páratlan fokszámú csúcsok száma páros.

Gráfok izomorfiája

A $G = (\varphi, E, V)$ és $G' = (\varphi', E', V')$ gráfok *izomorf*ak, ha van olyan az E-t E'-re képező kölcsönösen egyértelmű f és a V-t V'-re képező kölcsönösen egyértelmű g leképezés, hogy minden $e \in E$-re és $v \in V$-re e pontosan akkor illeszkedik v-re, ha $f(e)$ illeszkedik $g(v)$-re, azaz az (f, g) pár tartja az illeszkedési relációt.

Két gráf izomorfiáját általában nem könnyű bizonyítani,
néha nincs sokkal jobb módszer, mint az összes lehetséges (f, g) leképezés-párokat kipróbálni.

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

Egyszerű gráfok esetén:

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

Teljes gráfok

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

n szögpontú teljes gráf

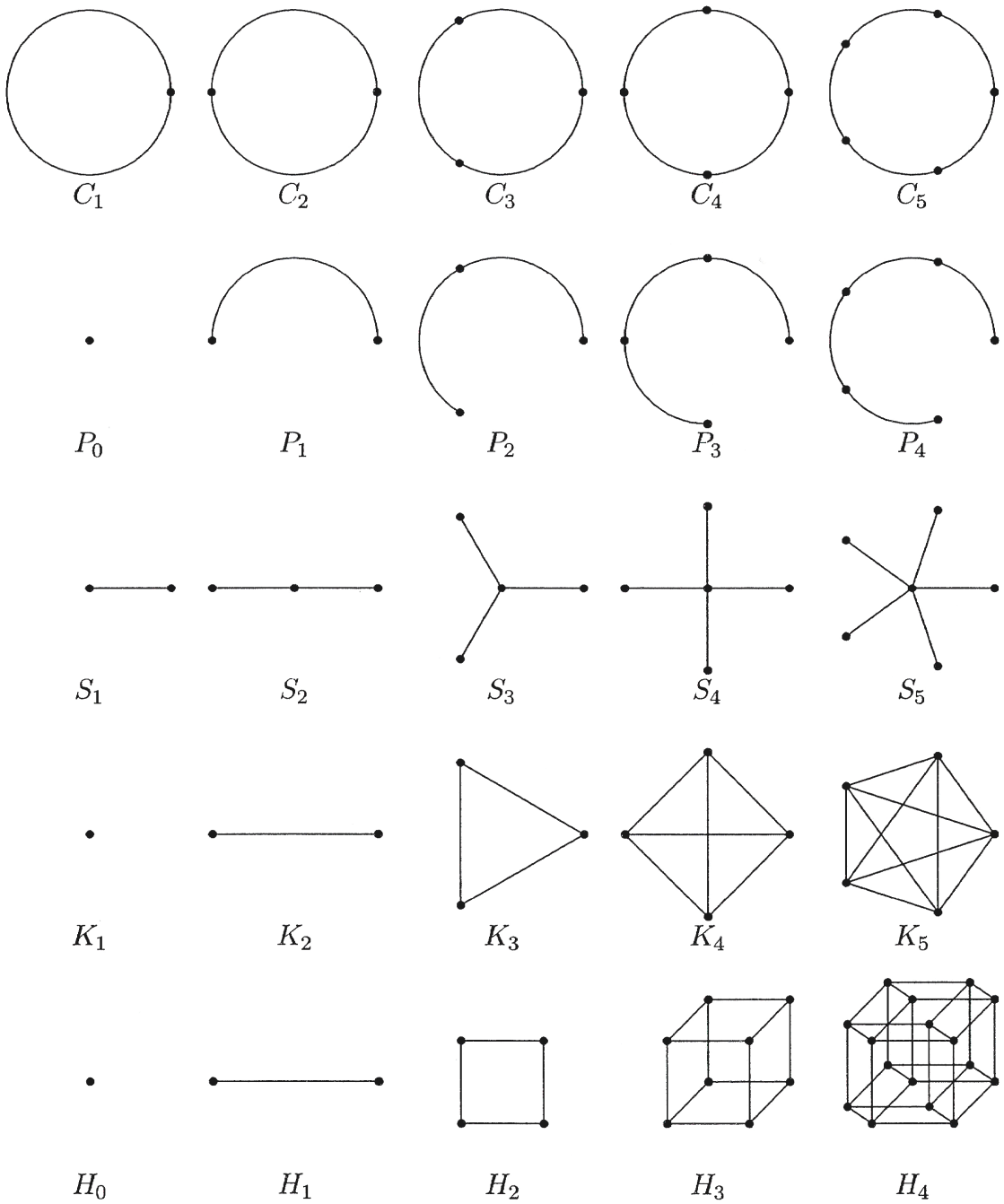
Teljes gráfok esetén, ha a csúcsok halmazai között létezik kölcsönösen egyértelmű leképezés (ekvivalens halmazok), akkor a két teljes gráf izomorf, azaz teljes gráfok a csúcsok és élek elnevezésétől eltekintve megegyeznek. Ebben az értelemben beszélünk bármely $n \in \mathbb{N}$ esetén n *szögpontú teljes gráf*ról.

Állítás

Az n szögpontú teljes gráfnak $n(n-1)/2$ éle van, és K_n-nel szokás jelölni.

Bizonyítás teljes indukcióval.

Példa:
-Öt szabályos test élgráfjáról, a Petersen-fráfról, a H_n hiperkockáról.
- C_n *ciklikus* csúcsai az n-edik egységgyökök, ahol él megy minden egységgyökből a következőbe (cikliksan).
-A P_n *ösvény* C_{n+1}-ből az 1-be vivő él törlésével adódik. A S_n *csillagban* az n-edik egységgyökök vannak összekkötve a nullával.


C_1
C_2
C_3
C_4
C_5
P_0
P_1
P_2
P_3
P_4
S_1
S_2
S_3
S_4
S_5
K_1
K_2
K_3
K_4
K_5
H_0
H_1
H_2
H_3
H_4

Gráfok Descartes-szorzata

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

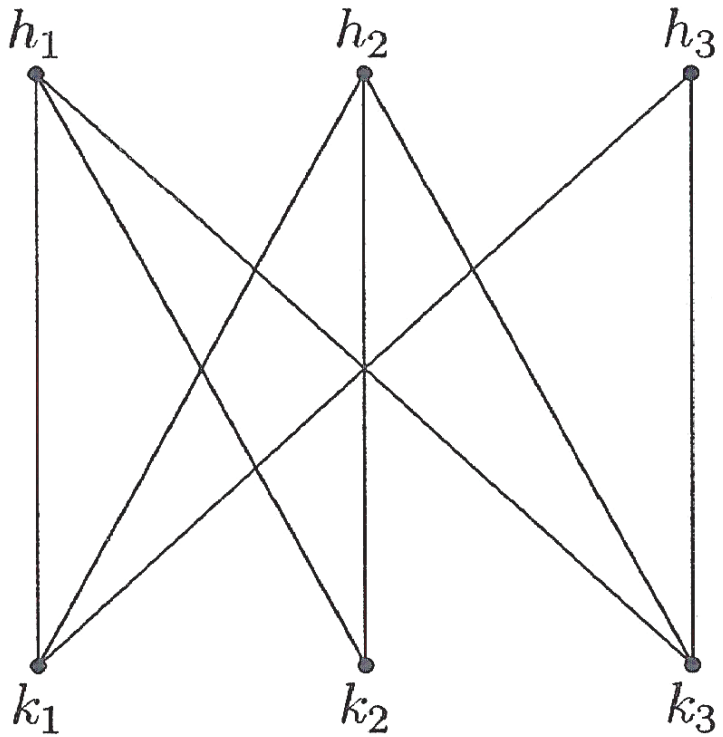
Páros gráfok

Egy *páros gráf* (vagy *kétrészes gráf*) egy olyan gráf, amelynél adott a csúcsok V halmazának egy V', V'' diszjunkt halmazokra való felbontása úgy, hogy minden él egyik végpontja az egyik, másik végpontja a másik halmazba esik.
Egy páros gráfot tehát egy (φ, E, V', V'') négyesként adhatunk meg.

Példa:

-A „három ház, három kút” gráf, amelynél V' három házból, V'' három kútból áll, és bármely ház és bármely kút között van egy él, de több él nincs.

Azt az egyszerű páros gráfot, amelyben $\natural(V') = m$, $\natural(V'') = n$ és minden V'-beli csúcs minden V''-beli csúccsal össze van kötve $K_{m,n}$-nel jelöljük. A $K_{3,3}$ ('három ház, három kút) páros gráf.



Részgráf

A $G' = (\varphi', E', V')$ gráfot a $G = (\varphi, E, V)$ gráf *részgráf*jának nevezzük, ha $E' \subset E$, $V' \subset V$ és $\varphi' \subset \varphi$. Néha azt mondjuk, hogy G a G' *szupergráf*ja.

Feszített részgráf

Ha a G' részgráf mindazokat az éleket tartalmazza, amelyek végpontjai V'-ben vannak,
azaz ha G' a legbővebb részgráf V'-beli csúcsokkal,
akkor G'-t a V' által meghatározott *feszített részgráf*nak vagy *telített részgráf*nak nevezzük.

Komplementer

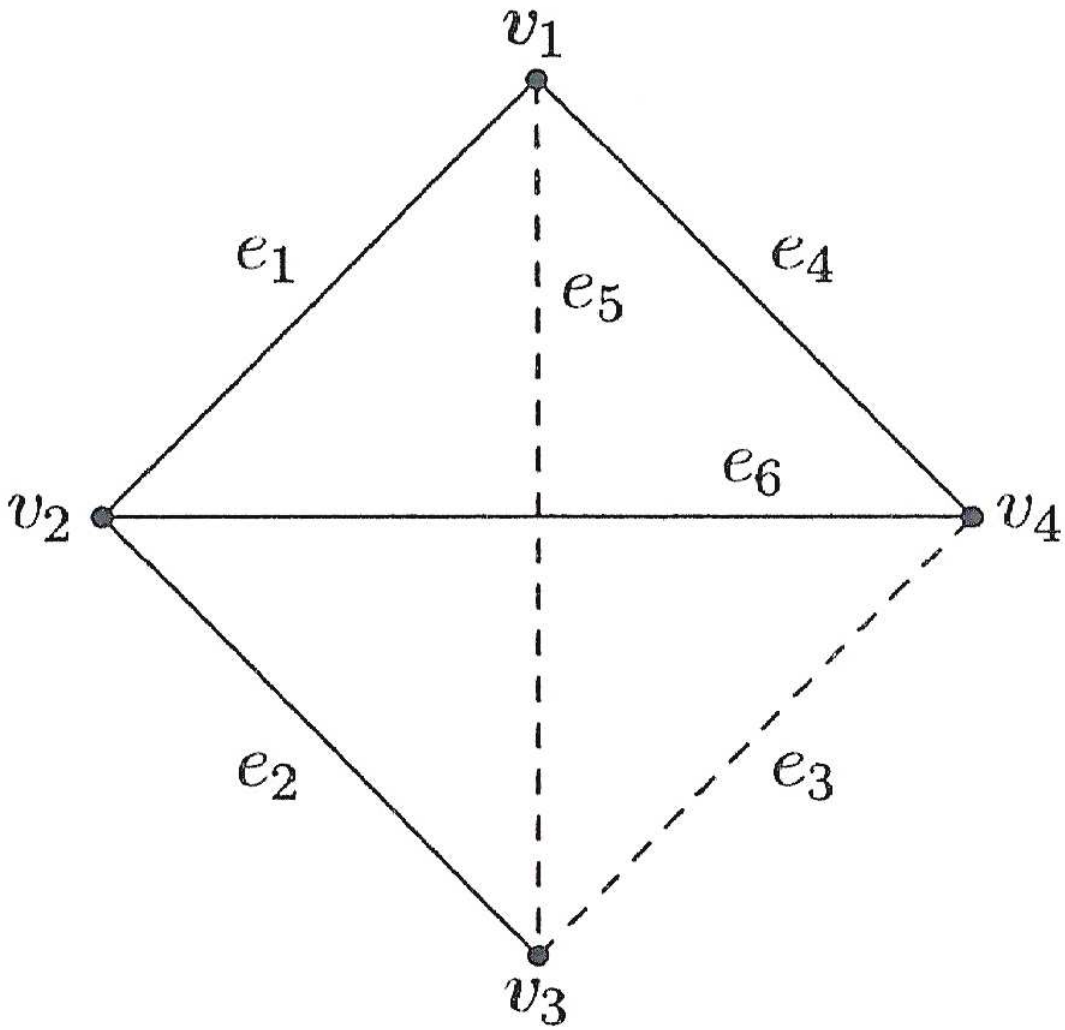
Ha $G' = (\varphi', E', V')$ részgráfja a $G = (\varphi, E, V)$ gráfnak, akkor a G'-nek G-re vonatkozó *komplementer*én a $(\varphi|_{E \setminus E'}, E \setminus E', V)$ gráfot értjük.

Teljes gráfra vonatkozó komplementer

-Ha G' egyszerű gráf, és nem mondjuk meg, hogy mely gráfra vonatkozó komplementeréről van szó, akkor a V'-beli csúcspontokkal rendelkező olyan egyszerű gráfra gondolunk, amelyben pontosan azok a csúcsok szomszédosak, amelyek G'-ben nem;
Ez a V'-beli csúcspontokkal rendelkező
teljes gráfra vonatkozó komplementer.

Megjegyzés: Az ilyen gráfok az élek elnevezésétől eltekintve azonosak, azaz izomorfak.

Szaggatott vonal mutatja a komplementer gráfot,
$(\{e_1, e_4, e_6\}, \{v_1, v_2, v_4\})$ feszített $(\{e_1, e_6\}, \{v_1, v_2, v_4\})$ nem feszített részgráf.



Élhalmaz- csúcshalmaz törlésével kapott részgráf

Ha $G = (\varphi, E, V)$ egy gráf és $E' \subset E$, akkor a G-ből az E' *élhalmaz törlésével kapott gráf*on a $G' = (\varphi|_{E \setminus E'}, E \setminus E', V)$ részgráfot értjük.

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

Séták, vonalak, utak és körök

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

-Egy G-beli n *hosszú séta* v-ből v'-be egy olyan

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

$n \geq 0$ véges sorozat, amelyre e_i a v_{i-1} és v_i csúcsokra illeszkedő él, ha $1 \leq i \leq n$ és $v_0 = v$, $v_n = v'$.

-Ha $v = v'$, a sétát *zárt sétá*nak nevezünk, egyébként *nyílt sétá*nak.

-Ha a sétában szereplő élek mind különbözőek, akkor *vonal*nak nevezzük.

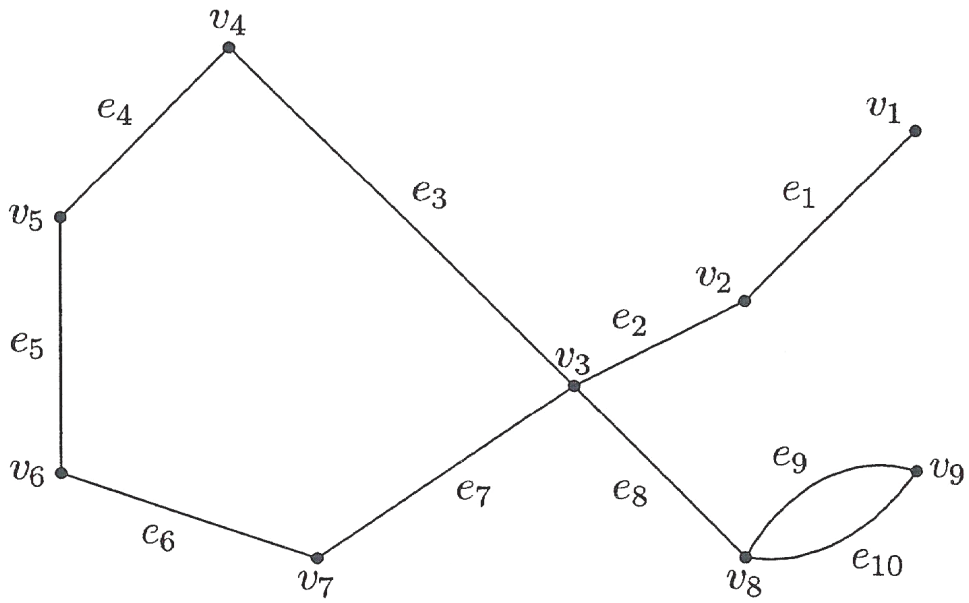
-Ha egy vonal zárt séta, akkor *zárt vonal*nak nevezzük, egyébként *nyílt vonal*nak.

-Egy sétát *út*nak fogunk nevezni, ha a $v_0, v_1, \ldots, v_n$ csúcsok mind különbözők.

-A nulla hosszú séták mind utak és egyetlen csúcsból állnak.
-Az egy hosszú séták utak, ha a bennük szereplő egyetlen él nem hurokél.
-Egy út nem tartalmazhat sem hurokélt, sem párhuzamos éleket, sem ugyanazt az élt kétszer.
-Speciálisan, egy út mindíg vonal.

Kör

-Egy legalább egy hosszú zárt vonalat *kör*nek nevezünk, ha a kezdő- és a végpont megegyeznek, de egyébként a vonal pontjai különbözőek.
-Az egy hosszú körök egyetlen hurokélt tartalmaznak.
-A kettő hosszú körök két különböző, de párhuzamos élt tartalmaznak.
-Ha egy kör 3, 4, ... hosszú, akkor néha *háromszög*nek, *négyszög*nek, ... nevezzük.



7.7. ábra

$v_3, e_8, v_8, e_9, v_9, e_{10}, v_8, e_8, v_3$ zárt séta, de nem út és nem vonal;

$v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_3, e_8, v_8$
vonal, de nem út;

v_1, e_1, v_2, e_2, v_3 út is, vonal is;

$v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_3$ kör.

Állítás

Az előző pont jelöléseivel, bármely G gráfban a különböző v és v' csúcsokat összekötő sétából alkalmasan törölve e_i, v_i párokat, a v-t v'vel összekötő utat kaphatunk.

Bizonyítás

Ha $v_i = v_j$, $i < j$, töröljük az

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

részt, és ismételjük ezt, amíg minden csúcs különböző lesz.
Mivel a séta hossza minden lépésben csökken, az eljárás véges sok lépésben véget ér.

Állítás

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

Bizonyítás

Ha nincs ismétlődő csúcs, kivéve, hogy az első és utolsó megegyezik, a vonal már kör, és készen vagyunk.
Egyébként az ismétlődő csúcs első előfordulásától a másodikig haladva,
egy rövidebb zárt vonalat kapunk, és ezt kihagyva,
az eredeti vonalból is egy rövidebb zárt vonal marad.
Ezek közül azokkal, amelyek nem körök, megismételjük az eljárást.
Minden lépésben, ha van még olyan zárt vonal, amely nem kör, abból két rövidebb vonalat kapunk.
Végül csupa kör marad.

Összefüggőség

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

-Ez azzal ekvivalens, hogy bármely két csúcsa összeköthető úttal.
-Nyilván egy adott gráf csúcsaira az a reláció, hogy két csúcs összeköthető úttal, ekvivalenciareláció a csúcsok halmazán, így meghatároz egy osztályozást.
-A csúcsok egy adott osztálya által meghatározott telített részgráf a gráf egy *komponens*e.
-Két különböző osztályba tartozó csúcs nem lehet szomszédos, így a gráf minden éle hozzátartozik egy komponenshez.
-Egy gráf akkor és csak akkor összefüggő,
ha minden csúcs ugyanabba az osztályba tartozik, azaz ha csak egyetlen komponense van.

Fák

Egy gráfot *fá*nak nevezünk, ha összefüggő és nincs köre.

Tétel

Egy G egyszerű gráfra a következő feltételek ekvivalensek:
(1)G fa;
(2)G összefüggő, de bármely él törlésével a kapott részgráf már nem összefüggő;
(3)ha v és v' a G különböző csúcsai, akkor pontosan egy út van v-ből v'-be;
(4)G-nek nincs köre, de bármilyen új él hozzávételével kapott gráf már tartalmaz kört.

Bizonyítás

-Ha egy, mondjuk v, v' végpontú élt törölve, a gráf összefüggő maradna,
akkor létezne út v-ből v'-be, amit kiegészítve a törölt éllel, egy kört kapnánk, így (1)-ből következik (2).

Bizonyítás folytatśa

-Ha most két különböző út lenne v-ből v'-be,
akkor az egyiken szereplő csúcsokat $v, v_1, v_2, \ldots$-vel,
a másikban szereplőket $v, v_1', v_2', \ldots$-vel jelölve,
legyen k a legkisebb olyan index, amelyre $v_k \neq v_k'$.
Törölve a v_{k-1}, v_k végpontú élt, a gráf összefüggő maradna,
mivel bármely sétában, amelyben ez az él szerepel,
helyettesíthetjük a $v_{k-1}, v_k', v_{k+1}', \ldots, v', \ldots, v_{k+1}, v_k$ csúcsokon át haladó sétával.
Ezzel beláttuk, hogy (2)-ből következik (3).

-Ha a gráfban van egy $v, v', \ldots, v$ kör,
akkor nyilván két út vezet v-ből v'-be, így (3)-ból következik (1).

-Végül, ha a gráf fa, akkor körmentes.
Ha egy új hurokélt veszünk hozzá, akkor már tartalmaz kört,
ha pedig az új él végpontjai $v \neq v'$, akkor a v-ből v'-be vezető utat ezzel kiegészítve, kört kapunk.

Bizonyítás folytatása

-Megfordítva, ha (4) teljesül,
akkor azt kell megmutatni, hogy
bármely $v \neq v'$-re vezet séta v-ből v'-be.
Vegyünk hozzá egy új élt a gráfhoz, amelynek végpontjai v és v'.
Az új gráfban van kör.
Ebben az új él kell, hogy szerepeljen.
Törölve a körből az új élt, egy utat kapunk v-ből v'-be.

Tétel

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

Bizonyítás

A G-beli utak között van maximális hosszúságú.
Válasszunk egy ilyet, ennek hossza legalább 1.
Vezessen v-ből v'-be.
Megmutatjuk, hogy v és v' is elsőfokúak.
Ha valamelyik nem lenne elsőfokú, akkor belőle még vezetne valahova él.
Ha egy olyan csúcsba, amely nincs az adott úton, akkor az út hossza nem maximális.
Ha egy olyan csúcsba, amely az úton van, akkor a gráfban van kör.

Tétel

Egy G egyszerű véges gráfra n csúccsal a következő feltételek ekvivalensek:
(1)G fa;
(2)G-ben nincs kör és $n-1$ éle van;
(3)G összefüggő és $n-1$ éle van.

Bizonyítás

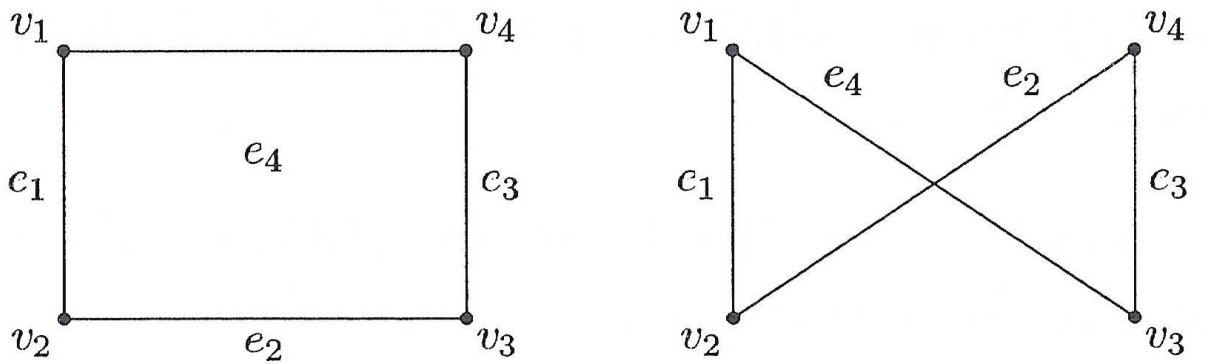
-Ha $n=1$, az állítás triviális.
Tegyük fel, hogy G fa, $n>1$, és legyen v_n egy olyan csúcsa G-nek, amelynek csak egy szomszédja van, v_{n-1}.
Töröljük a v_n csúcsot: a maradék G' gráf fa,
mivel bármely útnak v_n csak a kezdőpontja vagy a végpontja lehet.
Így n szerinti indukcióval kapjuk (1)-ből (2)-t.
-Hasonlóan kapjuk (2)-ből (3)-at:
a fenti jelölésekkel G összefüggő, mivel v_n-ből vezet út v_{n-1}-be és (teljes indukcióval) v_{n-1}-ből vezet út G'-ben minden más csúcsba.

Bizonyítás folytatása

-Végül tegyük fel, hogy (3) teljesül.
Ha G-nek van köre, akkor a kör bármely élét törölve,
egy olyan gráfot kapunk, amely még mindíg összefüggő.
Folytassuk az élek törlését addig, amíg végül már nem marad kör a gráfban.
Ha k lépést tettünk, akkor egy n csúcsú fát kapunk $n - k - 1$ éllel.
De mivel (1)-ből következik (2), csak $k = 0$ lehetséges.

Feszítőfa

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



7.8. ábra

Állítás

Minden véges összefüggő gráfnak létezik feszítőfája.

Bizonyítás

A bizonyítás konstruktív.
Amíg van a gráfban kör, hagyjuk el annak egyik élét.
A maradék gráf összefüggő marad.
Véges sok lépésben az eljárás megakad: ekkor a kapott gráf összefüggő és körmentes.

Állítás

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

Bizonyítás

Legyen F egy feszítőfája G-nek.
Ennek $\natural(V) - 1$ éle van.
Legyen E' a G azon éleinek halmaza, amelyek nem szerepelnek F-ben.
Ha $e \in E'$, akkor ezt az élt hozzáadva F-hez, a kapott gráf tartalmaz legalább egy K_e kört.
Az eredeti gráf is tartalmazza K_e-t.
A kapott K_e kör tartalmazza e-t,
de ha $e \neq e' \in E'$, akkor $K_{e'}$ nem tartalmazza e-t,
így a K_e, $e \in E'$ körök élhalmazai mind különbözőek.

Megjegyzés

-Az előző bizonyításban szereplő K_e kör élhalmazát az $e \in E'$ él egyértelműen meghatározza.
Ha ugyanis az F feszítőfához hozzáadva az e élt,
a kapott gráfban két különböző élhalmazú kör lenne,
mivel mindkettő tartalmazza e-t, az e egyik végpontjától a másikig két különböző úton is el lehetne jutni F-ben,
így F nem lenne fa.
-Az előző bizonyításban szereplő K_e, $e \in E'$ körrendszer élhalmazait tehát az F feszítőfa egyértelműen meghatározza.
Ezt a körrendszert az F feszítőfához tartozó *alapkörrendszer*nek nevezzük.
-Lehet, hogy a gráfban más élhalmazú körök is vannak,
de megmutatható, hogy egy alapkörrendszer segítségével megadható G valamennyi köre.
-A tételben szereplő szám csakalsó korlát, hiszen például a tetraéder élgráfjában több kör van, mint $\natural(E) - \natural(V) + 1$.

Vágás

Legyen $G = (\varphi, E, V)$ egy gráf.
-Ha v', v'' csúcsok,
$V' \subset V$,
és minden v'-ből v''-be vivő útban szerepel valamely $v \in V'$ csúcs,
akkor azt mondjuk, hogy V' *elvágja* a v' és v'' csúcsokat.
-Ha $E' \subset E$ és minden v'-ből v''-be vivő útban szerepel valamely $e \in E'$ él,
akkor azt mondjuk, hogy E' *elvágja* a v', v'' csúcsokat.
-Ha vannak olyan csúcsok, amelyeket az E' élhalmaz elvág,
akkor E'-t *elvágó élhalmaz*nak nevezzük.
-Ha egy elvágó halmaznak nincs olyan valódi részhalmaza,
amely ugyancsak elvágó halmaz, akkor *vágás*nak nevezzük.

Állítás

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

Bizonyítás

Legyen F egy feszítőfája G-nek, az F éleinek halmaza legyen E'.
Konstruálunk E_e, $e \in E'$ vágásokat úgy, hogy E_e tartalmazza az $e \in E'$ élt,
de semmilyen más $e' \in E'$ élt nem tartalmaz.
Az $E \setminus E'$ élhalmaz nem elvágó halmaz, hiszen F összefüggő.
Az $(E \setminus E') \cup \{e\}$, $e \in E'$ halmazok viszont elvágó halmazok.
Tehát minden il yen halmaz tartalmaz legalább egy vágást, legyen ez E_e.
Ez nyilván tartalmazza az e élt, de más $e' \in E'$ élt nem tartalmaz.
Egyébként az $(E \setminus E') \cup \{e\}$ élhalmaz pontosan egy vágást tartalmaz,
mivel e törlése E'-ből két komponensre vágja a fát.

Bizonyítás folytatása

A vágásban pontosan azok az élek vannak,
amelyeknek végpontjai különböző komponensekben vannak.

Erdő

Körmentes gráfot *erdő*nek nevezünk.
Egy erdő komponensei nyilván fák, a fák pedig összefüggő erdők.
Egy gráf olyan részgráfját, amely a gráf minden komponenséből egy feszítőfát tartalmaz,
a gráf *feszítő erdő*jének nevezünk.
Egy véges erdő éleinek száma nyilván a csúcsok számának és a komponensek számának különbsége.
A nem összefüggő gráfoknál az erdők ugyanazt a szerepet töltik be, mint az összefüggő gráfoknál a fák.

Euler-vonal

A legelső gráfelméleti problémával Eulernél találkozunk:

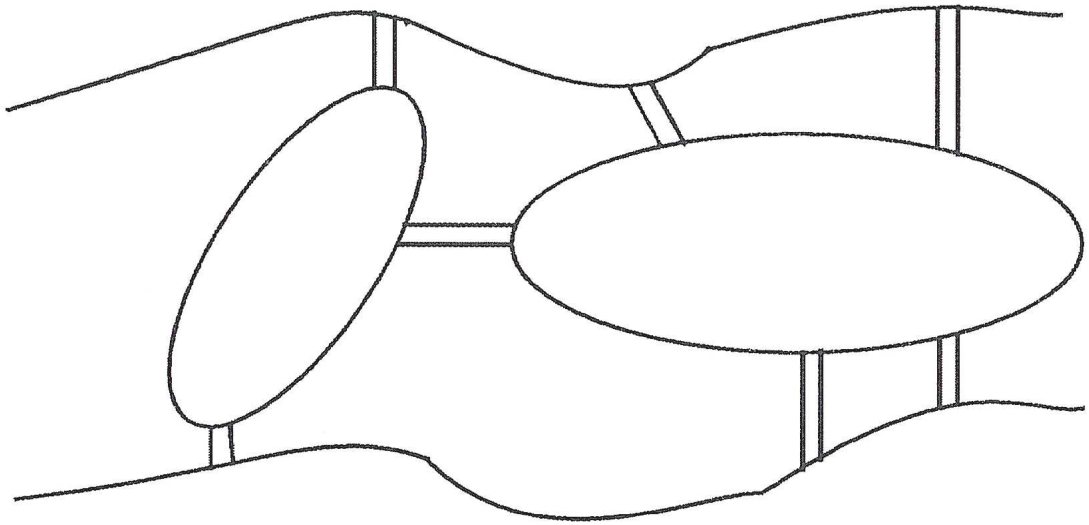
Egy folyón két sziget van, amelyeket híd köt össze.

Az egyik szigetet két-két, a másikat egy-egy híd köti össze mindkét parttal.

Be lehet-e járni egy pontból indulva a hét hidat úgy, hogy mindegyiken pontosan egyszer haladunk át, és ugyanoda érkezünk vissza?

Euler vonal

Általánosabban kérdezhetjük, hogy egy véges gráfban létezik-e olyan zárt vonal,
amelyben minden él szerepel,
illetve adott v, v' csúcsokhoz a v-ből v'-be vezető olyan vonal,
úgynevezett *Euler-vonal*, amelyben minden él szerepel.



7.9. ábra: Kőnigsbergi hidak

Ha $v \neq v'$, akkor v minden előfordulásánál az Euler-vonalban két él szerepel,
amely illeszkedik v-re, kivéve az elsőt, így v páratlan fokú.

Hasonlóan adódik, hogy v' is páratlan fokú, minden más csúcs pedig páros fokú,
és ha $v = v'$, akkor minden csúcs páros fokú.

Ez az egyszerű szükséges feltétel mutatja, hogy
Euler problémájára a válasz negatív.

Másrészt, ez a szükséges feltétel elégséges is, ha a (véges) gráf összefüggő.

A következő állítás egy általánosabb kérdést is megválaszol.

Állítás

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

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

Bizonyítás

A bizonyítás konstruktív.

Először tegyük fel, hogy $s = 0$.

Induljunk ki egy tetszőlegesen kiválasztott v csúcsból álló, élt nem tartalmazó zárt vonalból.

Ha az eddigi kapott zárt vonalban nem minden él szerepel, akkor az összefüggőség miatt van a vonalon olyan v' csúcs,
amelyre illeszkedő élek közül nem minden él van felhasználva.

Bizonyítás folytatása

Induljunk el ebből a csúcsból egy fel nem használt élen és haladjunk mindíg fel nem használt éleken.

Mivel minden csúcsra páros sok fel nem használt él illeszkedik, a továbbhaladás csak akkor lehetséges, ha visszaérünk v'-be.

Ha most az eredeti vonalon elmegyünk v-ből v'-be,
az új vonalon körbemegyünk, majd az eredeti vonalon haladunk tovább,
akkor az eredeti vonalnál hosszabb zárt vonalat kapunk.

Az általános eset bizonyításához kössük össze páronként a páratlan fokú csúcsokat egy-egy új éllel.

A kapott gráfban van zárt Euler-vonal.
Ebből törölve az s új élt, s nyílt vonalra esik szét.

Hasonlónak tűnő, mégis sokkal nehezebben megválaszolható kérdés.

Hamilton-út

Van-e egy gráfban olyan v-ből v'-be vezető út, amelyen a gráf minden pontja szerepel.

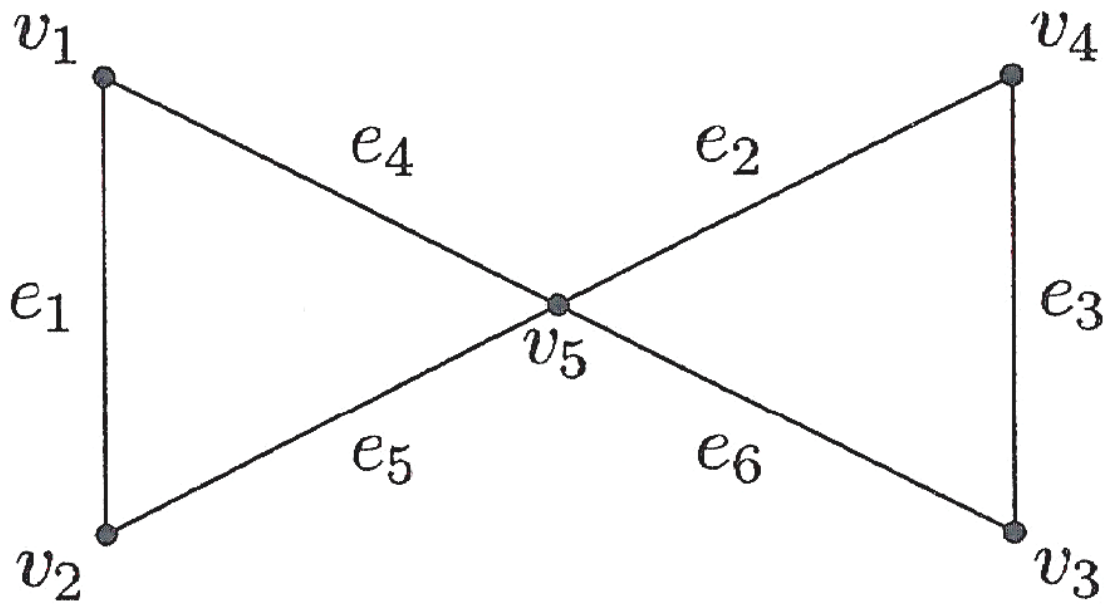
Egy ilyen utat *Hamilton-út*nak nevezünk.

*Hamilton-kör*nek egy olyan kört nevezünk, amelyben a gráf minden csúcsa szerepel.

-Hamilton-út vagy Hamilton kör létezéséhez a gráfnak végesnek és összefüggőnek kell lenni.

-Ha egy gráfban létezik Hamilton-kör, akkor nyilván létezik Hamilton-út is.

Bár vannak tételek, amelyek azt mutatják, hogy ha egy véges összefüggő gráf minden pontja „elég magas” fokú,
akkor létezik Hamilton-út illetve Hamilton-kör,
nem ismerünk igazán jó kritériumot Hamilton-út illetve Hamilton-kör létezésére.



7.10. ábra

A 7.10 ábrán egy olyan gráfot láthatunk, amelyben van zárt Euler-vonal és nincs Hamilton-kör.

Gyakorlati alkalmazásokban gyakran további adatokat csatolunk a gráf éleihez, illetve csúcsaihoz.

Címkézett és Súlyozott gráfok

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

Ha csak élcímkék és élcímkézés adott, akkor *élcímkézett gráfról*, ha pedig csak csúcscímkék és csúcscímkézés adott, akkor *csúcscímkézett gráfról* beszélünk.

-Gyakran színezett gráfról beszélünk címkézett gráf helyett.

-A címkéket felhasználhatjuk például arra, hogy az adott csúcsra illeszkedő éleket meszámozzuk, rendezzük, stb.

Élsúlyozott, csúcssúlyozott gráf

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

-Egy (φ, E, V, w) élsúlyozott gráfban egy $E' \subset E$ véges élhalmaz súlya $\sum_{e \in E'} w(e)$.

-Hasonlóan egy (φ, E, V, w) csúcssúlyozott gráfban egy $V' \subset V$ véges csúcshalmaz súlya $\sum_{v \in V'} w(v)$.

Nagyon sok gráfalgoritmus súlyozott gráfokkal foglalkozik.

Mohó algoritmus minimális összsúlyú feszítőerdő konstrukciójára

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

Egy (φ, E, V, w) súlyozott összefüggő véges gráfban az összes csúcsot tartalmazó üres részgráfból indulva, és a már kiválasztott részgráfhoz addig adva hozzá a minimális súlyú olyan élt, amellyel a kiválasztott részgráf még nem tartalmaz kört, egy minimális súlyú feszítőfát kapunk.

Az algoritmus általában Kruskál algoritmusa néven ismert.

Bizonyítás

Elég egy komponensre szorítkozni.

Világos, hogy a kiválasztott élek egy F feszítőfát adnak.

Tegyük fel, hogy a minimális súlyú F' feszítőfa súlya kisebb, mint F súlya; válasszuk olyan F'-t, amelynek a lehető legtöbb közös éle van F-el.

Legyen e' olyan éle F'-nek, amely nem éle F-nek.

Ha e'-t hozzávesszük F-hez, a kapott gráfban van egy K kör.

A kör minden e élére $w(e) \leq w(e')$, mert ha valamelyikre $w(e) > w(e')$ teljesülne, az algoritmus az e helyett e'-t választotta volna.

Ha F'-ből elhagyjuk e'-t, a kapott gráf nem összefüggő, hanem két komponense van.

A K körön szereplő élek egyike, e', összekötötte a két komponenst.

Bizonyítás folytatása

Kell hogy legyen a körön legalább még egy él, amely összeköti a két komponenst; jelöljük ezt e''-vel.

Az F' gráfból elhagyva e'-t és hozzávéve e''-t, a kapott F'' gráf is feszítőfa.

Tudjuk, hogy $w(e'') \leq w(e')$.

Ha $w(e'') < w(e')$ lenne, akkor ebből az következne, hogy F'' súlya kisebb, mint F' súlya, így F' súlya nem minimális.

Ha $w(e'') = w(e')$ teljesülne, akkor F'' olyan minimális súlyú feszítőfa lenne, amelynek több közös éle lenne F-el, mint F'-nek.

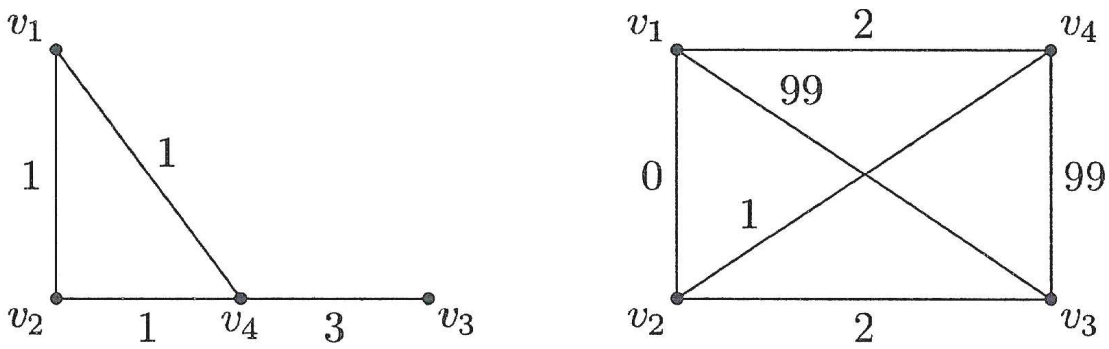
Mindkét eset ellentmondásra vezetett, így beláttuk, hogy az algoritmus működik.

A 7.11 ábra bal oldalán látható gráf mutatja, hogy nem mindíg tudunk a maradék élek közül minimális súlyú élt választani, különben a harmadik ilyen él behúzásakor kört kapnánk.

Megjegyzés.

Mohó algoritmus

Kruskal algoritmusa példa úgynevezett *mohó algoritmus*ra: minden lépésben a lehetséges lehetőségek közül az adott lépésben lehető legkedvezőbbet választjuk.



7.11. ábra

Mohó algoritmusok folytatás

Még a Hamilton-kör keresésénél is nehezebb probléma az *utazó ügynök problémája*: véges, összefüggő, élsúlyozott gráfban a minimális összsúlyú Hamilton-kör megtalálása (egyúttal azt is eldöntve, van-e Hamilton-kör).

-Nem meglepő tehát, hogy az a mohó algoritmus, amely a legkisebb súlyú élből indulva, a kapott vonalat mindíg, valamelyik végén egy minimális súlyú éllel hosszabbítja meg, már egy 4 csúcspontú teljes gráfban sem feltétlenül találja meg a minimális súlyú Hamilton-kört.

-A mohó algoritmusok nem mindíg optimálisak, például könnyű példát adni olyan 4 csúcspontú teljes gráfra, amelyben a mohó algoritmus nem adja meg a minimális súlyú Hamilton-kört.

Megjegyzés.
A gráfelmélet több mint 100 évig megoldatlan problémája volt a *négyszínsejtés*, mely szerint bármely síkba rajzolható egyszerű gráf csúcsaihoz hozzárendelhetünk négy színt úgy, hogy a szomszédos csúcsokhoz rendelt színek különbözőek. 1976-ban és amerikai matematikusok bizonyították be a sejtést.

Ez volt az első nevezetes matematikai probléma, amelynek bizonyításához számítógépet is használtak.

Irányított gráfok

Egy irányított gráfon szemléletesen pontoknak egy halmazát értjük, amelyek közül bizonyosakat irányított éleknek nevezett irányított ívekkel összekötünk.

A pontos definíció megértéséhez gondoljunk arra, hogy hogyan ábrázolnánk egy irányított gráfot számítógépben:

Definíció

Egy *irányított gráf* alatt egy $G = (\Psi, E, V)$ hármast értünk, ahol V a *csúcs*ok vagy *szögpont*ok halmaza, E az *él*ek halmaza, a Ψ *illeszkedési leképezés* pedig egy E-t $V \times V$-be képező leképezés.

Ha $\Psi(e) = (v, v')$, akkor azt mondjuk, hogy v az e *kezdőpont*ja, v' pedig a *végpont*ja.

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

Mindazokat a fogalmakat, amelyeket irányítatlan gráfokra definiáltunk, használni fogjuk irányított gráfokra is; ilyenkor mindíg a megfelelő irányítatlan gráfra gondolunk.

Definíció

Azt is mondjuk, hogy G a G' egy *irányítás*a.

Természetesen egy gráfnak általában több irányítása is van.

A $G = (\Psi, E, V)$ irányított gráf *megfordítás*án azt a $G' = (\Psi', E, V)$ irányított gráfot értjük, amelyre $\Psi(e) = (v, v')$ esetén $\Psi'(e) = (v', v)$. (Természetesen hurokél megfordítása saját maga.)

Irányított gráfoknál is gyakran szokás némileg pontatlanul az illeszkedési leképezést elhagyni a jelölésből és egy $G = (E, V)$ irányított gráfról beszélni.

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

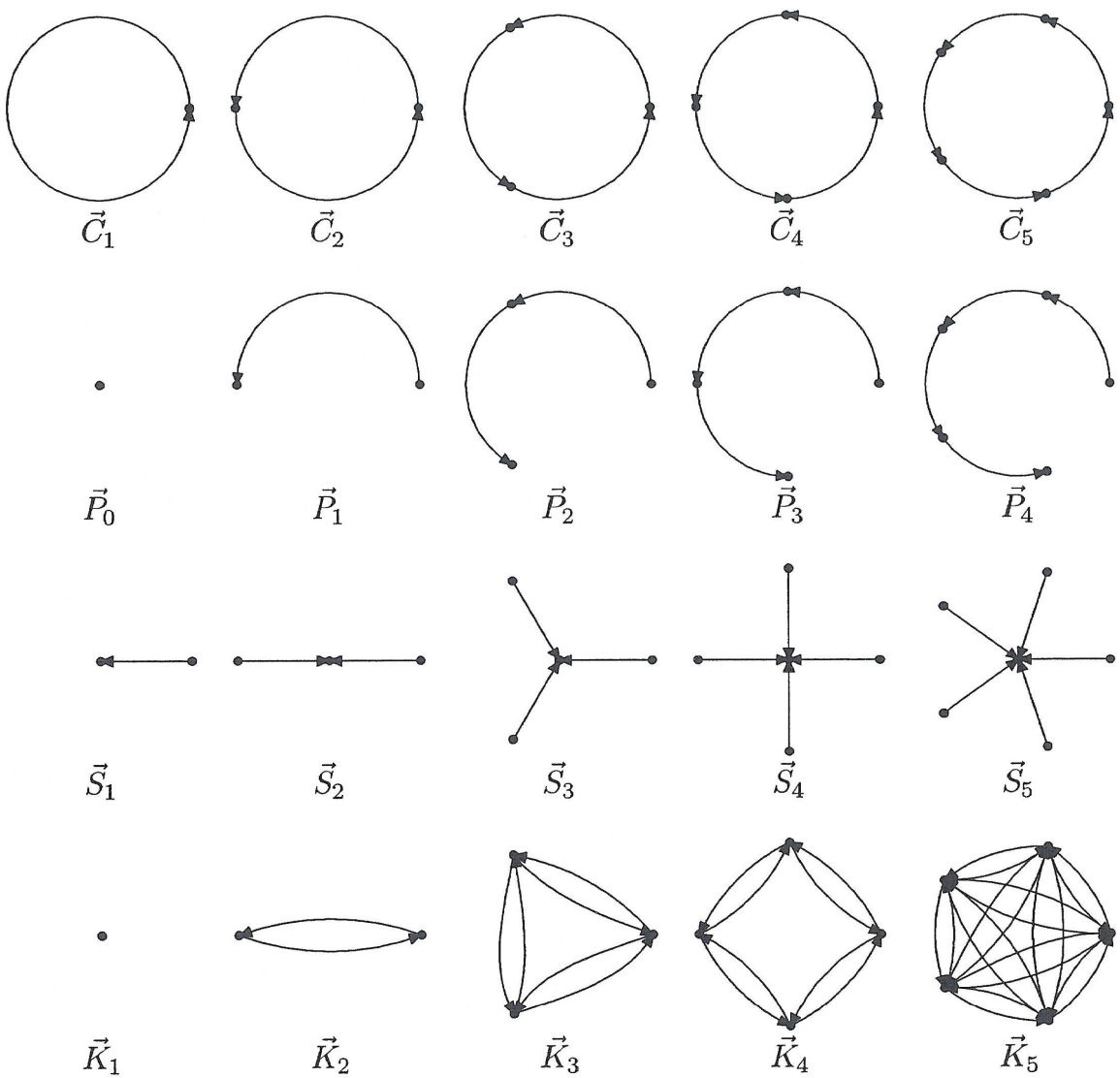
Gráf foka

Ha $G = (\Psi, E, V)$ egy irányított gráf és $S \subset V$, akkor jelölje $E^+(S)$ azon élek halmazát, amelyek kezdőpontja S-ben, végpontja pedig $V \setminus S$-ben van, és jelölje $E^-(S)$ azon élek halmazát, amelyek végpontja S-ben, kezdőpontja pedig $V \setminus S$-ben van.

Ha egy csúcs csak véges sok élnek kezdőpontja, akkor ezek számát a csúcs *kifok*ának nevezzük.

Hasonlóan, ha egy csúcs csak véges sok élnek végpontja, akkor ezek számát a csúcs *befok*ának nevezzük.

Ha egy csúcs kifoka nulla, akkor *nyelő*nek, ha pedig befoka nulla, akkor *forrás*nak nevezzük.


$\vec{C}_1$
$\vec{C}_2$
$\vec{C}_3$
$\vec{C}_4$
$\vec{C}_5$
$\vec{P}_0$
$\vec{P}_1$
$\vec{P}_2$
$\vec{P}_3$
$\vec{P}_4$
$\vec{S}_1$
$\vec{S}_2$
$\vec{S}_3$
$\vec{S}_4$
$\vec{S}_5$
$\vec{K}_1$
$\vec{K}_2$
$\vec{K}_3$
$\vec{K}_4$
$\vec{K}_5$

7.12. ábra

Állítás

Egy $v \in V$ csúcs kifokát rendszerint $\deg^+(v)$-vel vagy $d^+(v)$-vel, befokát rendszerint $\deg^-(v)$-vel vagy $d^-(v)$-vel jelöljük.

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

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

Mivel minden újabb él mindkét összeget eggyel növeli.

Példa

Egy $\overrightarrow{C}_n$ *irányított ciklus* csúcsai az n-edik egységgyökök, ahol irányított él megy minden egységgyökből a következőbe (ciklikusan).

A $\overrightarrow{P}_n$ *irányított ösvény* $\overrightarrow{C}_{n+1}$-ből az 1-be vivő él adódik.

Az $\overrightarrow{S}_n$ *irányított csillagban* az n-edik egységgyökökből visz irányított él a nullába.

Irányított teljes gráf

Adott csúcshalmaznál az *irányított teljes gráfban* minden csúcsból minden tőle különböző csúcsba visz irányított él.

Az n-csúcsú irányított teljes gráfot $\overrightarrow{K}_n$ jelöli; ez nem K_n irányítása, ha $n > 1$.

Példa

Legyen E egy V-beli reláció és legyen $\Psi(e) = e$, ha $e \in E$, azaz egy csúcsot egy másikkal pontosan akkor kössünk össze, ha az első relációban áll a másodikkal.

Ekkor (Ψ, E, V) irányított gráf. így relációk irányított gráfokkal szemléltethetők.

Véges gráfok éllistás ábrázolása

Legyen (Ψ, E, V) egy irányított gráf. A csúcsok beolvasásakor minden csúcsnak adunk egy sorszámot és egy táblázatban eltároljuk ezt a sorszámozást.

Minden csúcshoz felépítjük azon élek listáját, amelyeknek ez a csúcs a kezdőpontja: a Ψ leképezés olvasásakor, ha az $(e, (v, v'))$ párt olvassuk, akkor az (n, n') párt hozzáfűzzük az n sorszámú csúcs listájához, ahol n a v, az n' pedig a v' csúcs sorszáma.

Egyéb információkat, például a csúcsok illetve élek nevét, címkéket, stb., is a csúcshoz illetve élhez fűzhetünk.

Sok gráfalgoritmus kényelmesen megvalósítható az éllistás ábrázolással.

Például a gráf megfordítását úgy kaphatjuk, hogy az éllistákat végigolvasva, felépítjük a megfordítás éllistás ábrázolást.

Irányítatlan gráfok éllistás ábrázolásánál minden élt mindegyik végpontjának az éllistájába beírunk.

Ez annak felel meg, hogy minden nem hurokélt egy oda-vissza menő irányított élpárnak tekintünk.

Számos irányított gráfokra kidolgozott algoritmus ezzel az ábrázolással irányítatlan gráfokra is működik.

Irányított gráfok izomorfiája

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

Irányított részgráf

A $G' = (\Psi', E', V')$ irányított gráfot a $G = (\Psi, E, V)$ irányított gráf *irányított részgráf*jának nevezzük, ha $E' \subset E$, $V' \subset V$ és $\Psi' \subset \Psi$.

Néha azt mondjuk, hogy G a G' *irányított szupergráf*ja.

Ha a G' irányított részgráf mindazokat az éleket tartalmazza, amelyek kezdőpontjai és végpontjai is V'-ben vannak, akkor G'-t a V' által meghatározott *feszített irányított részgráf*nak vagy *telített irányított részgráf*nak nevezzük.

Komplementer

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

Ha nem mondjuk meg, hogy melyik gráfra vonatkozó komplementerről van szó, akkor az irányított teljes gráfra vonatkozó komplementerre gondolunk.

Élhalmaz- csúcshalmaz törlésével kapott részgráf

Ha $G = (\Psi, E, V)$ egy irányított gráf és $E' \subset E$, akkor a G-ből az E' élhalmaz törlésével kapott irányított gráfon a $G' = (\Psi|_{E \setminus E'}, E \setminus E', V)$ irányított részgráfot értjük.

Ha $G = (\Psi, E, V)$ egy irányított gráf és $V' \subset V$, akkor legyen E' az összes olyan élek halmaza, amelyeknek kezdőpontja vagy végpontja valamely V'-beli csúcs.

A G-ből a V' *csúcshalmaz törlésével kapott irányított gráf*on a $G' = (\Psi_{E \setminus E'}, E \setminus E', V \setminus V')$ részgráfot értjük.

Irányított séták, vonalak, utak és körök

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

Egy G-beli n *hosszú* *irányított séta* v-ből v'-be egy olyan

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

$n \geq 0$ véges sorozat, amelyre e_i kezdőpontja v_{i-1} végpontja pedig v_i, ha $1 \leq i \leq n$ és $v_0 = v$, $v_n = v'$.

Elegendő az élek sorozatát megadni, mert azok meghatározzák a csúcsokat.

Ha $v = v'$, az irányított sétát *zárt irányított sétá*nak nevezünk, egyébként *nyílt irányított sétá*nak.

Ha az irányított sétában szereplő élek mind különbözőek, akkor *irányított vonal*nak nevezzük.

Ha egy irányított vonal zárt irányított séta, akkor *zárt irányított vonal*nak nevezzük, egyébként *nyílt irányított vonal*nak.

Egy irányított sétát *irányított út*nak fogunk nevezni, ha a $v_0, v_1, \ldots, v_n$ csúcsok mind különbözők.

Egy legalább egy hosszú zárt irányított vonalat *irányított kör*nek nevezünk, ha a kezdő- és a végpont megegyeznek, de egyébként az irányított vonal bármely más pontja ezektől és egymástól különbözik.

Az, hogy v-ből vezet irányított séta a v'-be, nyilván azzal ekvivalens, hogy v-ből v'-be vezet irányított út.

Ez a reláció nyílván tranzitív.

Ha a megfelelő szigorú reláció irreflexív is - ami azzal ekvivalens, hogy nincs irányított kör - akkor részben rendezés. Az alábbi algoritmus eldönti, hogy van-e irányított kör, és ha nincs, akkor ezt a részben rendezést kiterjeszti rendezéssé.

Topologikus rendezés

Az alábbi algoritmuss egy véges gráfra eldönti, hogy van-e benne irányított kör, és ha nincs, akkor megadja a csúcsok egy olyan sorrendjét, hogy csak akkor megy egy v csúcsból él egy v' csúcsba, ha ebben a sorrendben v előbb van mint v'.

(1)[Inicializálás] Beolvassuk a gráfot és felépítjük az éllistás ábrázolását, egyúttal minden csúcshoz meghatározva a befokát is.

A nulla befokú csúcsokat betesszük az eredmény sorba.

Legyen n a csúcsok száma, m az eredmény sorba tett csúcsok száma és $i \leftarrow 1$.

(2) [Vége?] Ha $i > n$, a sorrend az eredmény sorban.

Egyébként, ha $i > m$, akkor van irányított kör a maradék $n - m$ csúcsú gráfban.

(3) [éltörlések] Az eredmény sor i-edik eleméből kiinduló éleket egyenként töröljük, az él végpontjának befokát mindíg eggyel csökkentve.

Topologikus rendezés folytatśa

Ha valamelyik csúcs befoka nulla lesz, akkor a sor végére tesszük, eggyel növelve m-t.

Végül legyen $i \leftarrow i + 1$ és menjünk a (2)-re.

Bizonyítás

Ha egy csúcs bekerül az eredmény sorba, akkor már minden olyan él amelyből hozzá vezet él, a sorban van.

Ha nem minden csúcs kerül be az eredmény sorba, akkor a maradék gráf csúcsain nem lehet részben rendezés az a reláció, hogy vezet él az egyikből a másikba, mert nincs legkisebb elem.

Igy a megfelelő szigorú reláció nem irreflexiv, tehát van irányított kör.

Erős összefüggőség

Egy irányított gráfot *erősen összefüggő*nek nevezünk, ha bármely (v, v') csúcspár esetén vezet irányított séta v-ből v'-be.

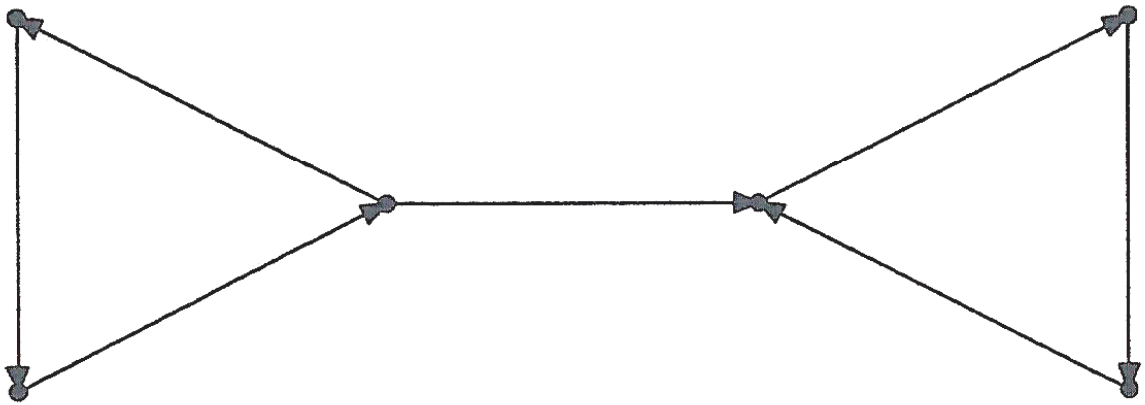
Ez azzal ekvivalens, hogy bármely (v, v') csúcspár esetén vezet irányított út v-ből v'-be.

Nyilván egy adott gráf csúcsaira az a reláció, hogy az egyikből a másikba és a másikból az egyikbe is vezett irányított út, ekvivalencia reláció a csúcsok halmazán, így meghatároz egy osztályozást.

A csúcsok egy adott osztálya által meghatározott telített irányított részgráf az irányított gráf egy *erős komponens*e.

Vegyük észre, -az irányítatlan gráfokkal ellentétben- nem feltétlenül tartozik az irányított gráf minden éle valamely erős komponenshez.

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



7.13. ábra

Irányított fák

Egy irányított gráfot *irányított fa*nak nevezünk, ha fa, és van egy olyan csúcsa, melynek a befoka 0, az összes többi csúcs befoka 1.

Azt a csúcsot, melynek a befoka 0 csúcs nyilván egyértelműen meghatározott, ez az irányított fa *gyökér*e.

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

A csúcsok szintjeinek maximumát (amely véges irányított fa esetén létezik) a fa magasságának nevezzük.

Ha van olyan él, amelynek v a kezdőponja, v' pedig a végpontja, akkor azt mondjuk, hogy v' a v gyermeke, illetve hogy a v a v' szülője.

Ha két csúcsnak ugyanaz a szülője, akkor *testvér*-nek nevezzük őket.

irányított fa (folytatás)

Bármely v csúcsra tekinthetjük azon csúcsok halmazát, amelyekhez vezet irányított út v-ből.

Ezek a csúcsok meghatároznak egy feszített irányított részgráfot, amely nyilván irányított fe és v a gyökere; ezt a v-ben gyökerező *irányított részfának* nevezzük.

Irányított fának azokat a csúcsait, amelyek kifoka nulla, *levél*nek nevezzük.

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

Gyökeres fának egy és csak egy irányítása van, amellyel irányított fa lesz úgy, hogy a kijelölt csúcs a gyökér: a kijelölt csúcsból egy másik adott csúcsba vezető egyetlen utolsó éle legyen az adott csúcshoz tartozó egyetlen bemenő él.

Igy a gyökér ekvivalens az irányítás megadásával.

irányított fa (folytatás)

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

Legfontosabbak a *bináris fák*: itt 0 vagy 1 helyett bal illetve jobb kimenő élről , stb. beszélünk.

Megjegyezzük, hogy két q-ad rendű fát akkor is különözőnek tekintünk, ha csak a cimkézésben különböznek, például, ha egy bináris fában csak egyetlen él van, akkor sem mindegy, hogy az bal vagy jobb él.

Az irányított fákat úgy szoktuk lerajzolni, hogy a gyökér van felül.

Ez nem felel meg a szóhasználatnak, de megfelel a gondolkodásunknak: gyökér alatt vannak a gyermekei, stb,

-Kupac

-Kupac rendezés

-B-fa

Dijkstra módszere

A (Ψ, E, V, w) véges súlyozott irányított tegyük fel, hogy az élsúlyok pozitívak, $s \in V$ és $T \subset V$.

Az alábbi algoritmus a csúcshalmazon értelmez egy $d : V \to R$ függvényt, amely $t \in T$ esetén az adott s csúcsból a t csúcsba vezető irányított séták súlyának minimuma ($+\infty$, ha nincs ilyen séta):

(1) [Inicializálás] Legyen $S = \emptyset, H = \{s\}$ és $d(s) = 0$; minden más v csúcsra legyen $d(v) = +\infty$.

(2)[Kész?] Ha $T \subset S$, vagy $H = \emptyset$, akkor az algoritmus véget ért.

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

Bizonyítás

Indukcióval megmutatjuk, hogy minden $t \in S$-re $d(t)$ az s csúcsból a t csúcsba vezető irányított séták súlyának minimuma, ha pedig $v \in H$, akkor minden olyan s-ből v-be vezető irányítottsétának, amelynek minden csúcsa S-ben van, kivéve az utolsót, a súlya legalább $d(v)$.

Inicializálás után ez nyilvánvaló.

Tegyük fel, hogy (3)-ban t-t választottuk és tekintsünk egy tetszőleges s-ből t-be vezető irányított sétát.

Legyen ennek súlya W. Legyen t' a séta első olyan csúcsa, amely nincs S-ben.

A séta s-ből t'-ig vivő részének W' súlyára $W' \leq W$ és az indukciós feltevés szerint $W' \geq d(t')$, így $W > d(t)$.

Miután (3)-ban a $d(v)$ értékeket megváltoztattuk, ha egy séta s-ből v-be visz és csak az utolsó csúcsa nincs S-ben, legyen t' az utolsó elötti csúcsa, e pedig az utolsó éle.

Bizonyítás folytatása

Mivel $t' \in S$ az s-től t'-ig vezető részséta súlya legalább $d(t')$, így a teljes séta súlya legalább $d(t') + w(e)$ és amikor t'-t bevettül S-be, legfeljebb ennyire állítottuk $d(v)$ értékét, azóta pedig csak csökkenhetett.

Megjegyzés

Az előző algoritmus könnyen módosítható úgy, hogy egy az s-ből t-be vezető minimális összsúlyú sétát is megkapjuk: amikor $d(v)$ étrékét módosítjuk, jegyezzük fel a v csúcshoz az e élt, felülírva az előző feljegyzést, ha volt olyan.

A feljegyzések segítségével visszafelé követhetünk egy minimális összsúlyú sétát. Ha minden ilyen sétára szükségünk van, akkor minden csúcsnál éleknek egy listáját kell nyilvántartanunk: amíg $v \notin H$, a lista üres, egyébként ha (3)-ban $d(t) + w(t) \leq d(v)$, akkor e-vel bővítjük a listát, ha pedig $d(t) + w(e) < d(v)$, akkor töröljük, és beletesszük e-t.

Mivel minden ilyen séta út, mert az élek súlya pozitív.

Dinamikus programozás

Néha olyan feladattal találkozunk, amely számos egymást átfedő részfeladatra vezet.

Ilyenkor célszerűbb lehet az összes részfeladatot megoldani.

Például, ha csak az s-ből t-be vezető minimális összsúlyú séta súlya érdekel bennünket, akkor is célszerűbb - mint azt Dijkstra algoritmusában tesszük - minden csúcsra elkezdeni megoldani a feladatot.

Ezt a megoldási módszert nevezik *dinamikus programozásnak*.

-Szélességi bejárás
-Mélységi bejárás
-Dinic-Dinic módszere
-PERT
-Folyamprobléma

Gráfok rajzolhatósága

Legyen $X \subset \mathbb{R}^n$.

Egy X-beli *görbe* egy, a $[0,1]$ valós intervallumot X-be képező Γ folytonos függvény.

Azt mondjuk, hogy $\gamma(0)$ a γ *görbe kezdőpontja*, $\gamma(1)$ pedig az *görbe végpontja*.

Ha legfeljebb a kezdő és végpontok egyeznek meg, akkor azt mondjk, hogy γ *egyszerű görbe*.

Egy $G = (\Psi, E, V)$ irányított gráf egy X-beli *lerajzolás*án azt értjük, hogy a gráf csúcsaihoz X különböző pontjait, éleihez pedig X-beli egyszerű görbéket rendelünk, amelyek egymást nem metszik;

pontosan fogalmazva a G gráf X-beli lerajzolásán egy (f, g) függvénypárt értünk, ahol $f : V \to X$ kölcsönösen egyértelmű, g pedig minden $e \in E$-hez egy olyan X-beli g_e egyszerű görbét rendel.

Gráfok rajzolhatósága

Kezdőpontja e kezdőpontjának f általi képe, végpontja e végpontjának f általi képe, és a $g_e(]0,1[)$, $e \in E$ halmazok egymástól és $\mathrm{rng}(f)$-től diszjunktak.

Egy irányítatlan gráf egy X-beli *lerajzolás*án bármelyik irányításának az X-beli lerajzolását értjük.

Ha a G (irányított vagy irányítatlan) gráfnak létezik egy $X \subset \mathrm{R}^n$-beli lerajzolása, akkor azt mondjuk, hogy G az X-be *rajzolható*.

Nem minden gráf rajzolható, mert például lehet, hogy olyan sok csúcs van, hogy eleve nem létezik $f : V \to X$ kölcsönösen egyértelmű leképezés.

Ezért csak véges gráfokkal foglalkozunk.

A rajzolhatóságra vonatkozó állításaink átvihetőek tetszőleges véges gráfokra is.

Csak a síkba, gömbfelületre és a (három dimenziós) térbe rajzolhatósággal foglalkozunk.

Állítás

Tetszőleges véges egyszerű gráf $\mathbb{R}^3$-ba rajzolható.

Bizonyítás

Ha legfeljebb három csúcs van, az állítás nyilvánvaló.

Egyébként a csúcsok száma szerinti indukcióval haladunk: Kiválasztva egy v csúcsot, a többi csúcs által feszített részgráf $\mathbb{R}^3$-ba rajzolható.

A többi csúcs $\mathbb{R}^3$-beli képei közül bármely három meghatároz egy síkot.

Válasszuk v képét úgy, hogy ezen síkok egyikén se legyen rajta.

Legyenek azon élek képei, amelyeknek végpontja v, lineáris függvények.

Segédtétel

Legyen $X \subset \mathbb{R}^3$ egy gömbfelület és (f, g) a $G = (\Psi, E, V)$ egyszerű véges gráf egy X-beli lerajzolása.
Ekkor van olyan $x \in X$ pont, amely sem f, sem a g_e, $e \in E$ egyszerű görbék értékkészletében nincs benne.

Tétel

Egy $G = (\Psi, E, V)$ egyszerű véges gráf pontosan akkor rajzolható egy $X \subset \mathbb{R}^3$ egy gömbfelületre, ha síkba rajzolható.

Bizonyítás

Ha a gráf síkba rajzolható, válasszunk egy, a síkot érintő gömbfelületet, és a gömbnek érintési ponttal ("déli sarok") átellenes pontjából ("északi sarok") vetítsük a gráf síkba rajzolását a gömbfelületre.
A megfordítás az előző segédtételen múlik: válasszuk ki a segédtételben leírt x pontot, legyen ez az "északi sarok" és vegyünk fel olyan síkot,

Bizonyítás folytatása

amely az ezzel átellenes pontban ("déli sarok") érinti a gömbfelületet, majd az x pontból vetítsük a gráf gömbfelületre rajzolását a síkra.

Tartományok

Az $\mathbb{R}^n$ egy X nyílt részhalmazát *tartomány*nak nevezzük, ha bármely két különböző pontjához van olyan X-beli egyszerű görbe, amelynek az egyik pont a kezdőpontja, a másik pedig a végpontja.

Euler tétele

Legyen (f, g) a $G = (\Psi, E, V)$ egyszerű véges összefüggő gráf egy síkba rajzolása.

Ekkor a $G' = \cup_{e \in E} \mathrm{rng}(g_e)$ halmaz komplementere $2 + \natural(E) - \natural(V)$ páronként diszjunkt tartomány egyesítése.

Gráfok topologikus ekvivalenciája

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

Kuratowski tétele

Egy egyszerű véges gráf akkor és csak akkor síkba rajzolható, ha nincs olyan részgráfja, amely topologikusan izomorf a K_5 öt szögpontú teljes gráffal vagy a $K_{3,3}$ „három ház, három kút" gráffal.

-A Petersen-gráf nem síkba rajzolható, mivel tartalmaz a $K_{3,3}$-mal topologikusan izomorf részgráfot.
(Töröljük bármelyik csúcsot, majd redukáljuk a kapott gráfot a másodfokú csúcsok kiküszöbölésével.)

Gráfok mátrixai

Ha $n, m \in \mathbb{N}$ természetes számok, egy m-szer n-es *a mátrix* egy $(i,j) \mapsto a_{i,j}$, $i,j \in \mathbb{N}$, $1 \leq i \leq m$, $1 \leq j \leq n$ leképezés.

Egy mátrixot rendszerint téglalap alakban rendezett táblázatként képzelünk el, ahol az i-edik sor j-edik eleme (másként a j-edik oszlop i-edik eleme) $a_{i,j}$.

Ezért az első indexet *sorindex*nek, a második indexet *oszlopindex*nek nevezzük.

(Néha egy mátrix sorait és oszlopait nullától kezdve indexeljük.)

Ha egy $G = (\Psi, E, V)$ irányított gráf élei $e_1, e_2, \ldots, e_n$ csúcsai pedig $v_1, v_2, \ldots, v_m$, akkor az alábbi *élmátrix* vagy *illeszkedési mátrix* egyértelműen megadja a gráfot:
$1 \leq i \leq m$ és $1 \leq j \leq n$ esetén $a_{i,j} = 1$, ha e_j-nek v_i kezdőpontja és $a_{i,j} = -1$, ha e_j nem hurokél, és e_j-nek v_i végpontja.

A megfelelő irányítatlan gráf élmátrixán az $|a_{i,j}|$ mátrixot értjük.

Gráfok mátrixai

A G irányított véges gráf b csúcsmátrixában legyen $b_{i,j}$ a v_i kezdőpontú, v_j végpontú élek száma, ha $1 \leq i, j \leq m$.

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

Megjegyezük, hogy bár több más módon is rendelhetünk gráfokhoz mátrixokat és a mátrixok felhasználhatók gráf számítógépes ábrázolására, bár erre a célra más adatszerkezetek, például láncolt listák gyakran gazdaságosabban használhatók.

Algebrai struktúrák

Algebrai struktúrák

Az algebrai struktúrákat $(H;\Omega)$ párral jelöljük, ahol H tetszőleges halmaz (tartóhalmaz), Ω H-n értelmezett műveletek halmaza.

Ha Ω az n_0 nullaváltozós, n_1 egyváltozós és rendre n_i i-változós műveletekből áll, akkor azt mondjuk, hogy az $(n_0, n_1, \ldots, n_i, \ldots)$ sorozat az $(H;\Omega)$.

Félcsoport, csoport, kommutativitás

Grupoid

Legyen $*$ egy binér művelet a G halmazon.

A $(G,*)$ párt szokás *grupoid*nak is nevezni.

Semleges elem

A G egy s elemét *bal* illetve *jobb oldali* semleges elemnek nevezzük, ha $s * g = g$ illetve $g * s = g$ minden $g \in G$-re.

Ha s bal és jobb oldali semleges elem is, akkor *semleges elemnek* nevezzük.

A G-ben létezhet akárhány bal oldali semleges elem.

Például
a $(g, h) \mapsto h$ műveletnél minden elem bal oldali semleges elem, a $(g, h) \mapsto g$ műveletnél pedig minden elem jobb oldali semleges elem.

Ha azonban van egy bal oldali s_b és egy jobb oldali s_j semleges elem, akkor $s_b = s_b * s_j = s_j$,
így bármely bal oldali semleges elem megegyezik bármely jobb oldali semleges elemmel,
azaz csak egy bal és jobb oldali semleges elem van.

Félcsoport

Ha a $*$ binér művelet a G halmazon *asszociatív*,
azaz $x, y, z \in X$ esetén $(x * y) * z = x * (y * z)$,
akkor G-t (pontosabban a $(G, *)$ párt) *félcsoport*nak nevezzük.

Inverz elem

Ha a G félcsoportban s semleges elem, és $g, g^* \in G$-re
$g * g^* = s$,
akkor azt mondjuk, hogy g a g^* *balinverz*e, g^* pedig a g *jobbinverz*e.
Ha g^* a g bal- és jobbinverze is, akkor azt mondjuk, hogy a g *inverz*e.

Ekkor nyilván g meg a $g*$ inverze.

Ha g^* a g egy balinverze, g^{**} pedig a g egy jobbinverze, akkor $g^* = g^* * (g * g^{**}) = (g^* * g) * g^{**} = g^{**}$.

Speciálisan, ha g-nek van inverze, az egyértelmű.

Az inverzképzést unér műveletnek is tekinthetjük.

Vegyük észre, hogy ha h-nak h^* az inverze, akkor $g * h$ inverze $h^* * g^*$.

Csoport

Ha egy egységelemes félcsoport minden elemének van inverze, akkor *csoport*nak nevezzük.

Kommutatív művelet

Ha a $*$ binér művelet a G halmazon, $g, h \in G$ és $g * h = h * g$,
akkor azt mondjuk,
hogy g és h *felcserélhető*ek.
Ha G bármely két eleme felcserélhető,
akkor a $*$ műveletet *kommutatív*nak nevezzük.

Kommutatív esetben a műveletet gyakran $+$-szal jelöljük (additív jelölés),
a semleges elemet *nullelem*nek nevezzük,
és n-el vagy 0-val (ha nagyon precízek vagyunk, n_G-vel vagy 0_G-vel) jelöljük,
a g inverzét pedig $-g$-vel jelöljük és g *ellentett*jének nevezzük.
A kommutatív csoportokat *Abel-csoport*nak szokás nevezni,
Gyakran $h + (-g)$ helyett $h - g$-t írunk.

Nem kommutatív esetben a műveletet rendszerint $\cdot$-al jelöljük (multiplikatív jelölés),
a semleges elemet *egységelemnek* nevezzük, és e-vel vagy 1-gyel (ha nagyon precízek vagyunk, akkor e_G-vel vagy 1_G-vel) jelöljük.

A g inverzét általában g^{-1}-el jelöljük, néha $1/g$-vel.

Ha kommutatív esetben multiplikatív jelölést használunk, akkor $h \cdot g^{-1}$ helyett gyakran h/g- írunk.

A nem kommutatív esetben ez nem célszerű,
mert $h \cdot g^{-1}$ nem feltétlenül egyenlő $g^{-1} \cdot h$-val.

Megjegyzés

Az előző két tétel mutatja, hogy $(\mathbb{N}, +)$ kommutatív félcsoport a 0 nullelemmel (belátható, hogy csak a 0-nak van additív inverze, a 0), és $(\mathbb{N}, \cdot)$ is kommutatív félcsoport az 1 egységelemmel (belátható, hogy csak az 1-nek van multiplikatív inverze, az 1).

Példák

(1) Ha X tetszőleges halmaz, akkor $\left(\wp(X), \cap\right)$ és $\left(\wp(X), \cup\right)$ kommutatív egységelemes félcsoportok,

(2) Ha X egy halmaz, akkor az X-beli binér relációk a $\circ$ összetétellel egységelemes félcsoportot alkotnak,
amely általában nem kommutatív és nem is csoport, bár vannak invertálható elemei.

(3) Ha X egy halmaz, akkor az X-et önmagába képező függvények a $\circ$ összetétellel egységelemes félcsoportot alkotnak.

Ha csak az összes injektív illetve az összes szürjektív leképezéseket tekintjük,
akkor is egységelemes félcsoportot kapunk.

Az összes bijektív leképezések csoportot alkotnak.

Ha az összes nem injektív leképezéseket illetve az összes nem szürjektív leképezéseket tekintjük,
akkor is félcsoportot kapunk, de ez már nem lesz egységelemes.

Ezekben az esetekben a művelet általában nem kommutatív.

Példák

Ha $X = \{\uparrow, \downarrow\}$, akkor $(X, \wedge)$ és $(X, \vee)$ kommutatív egységelemes félcsoportok,
$(X, \iff)$ Abel-csoport, míg $(X, \rightarrow)$-ben nincs egységelem,
a művelet nem asszociatív és nem is kommutatív.

Homomorfizmusok

Legyen adott a G és G' halmazokon egy-egy binér művelet;

Homomorfizmus

Egy $\varphi : G \to G'$ művelettartó leképezést *homomorfizmus*nak fogunk nevezni, és azt mondjuk, hogy $\varphi(G)$ a G homomorf képe.

Monomorfizmus

Ha a φ homomorfizmus kölcsönösen egyértelmű (injektív), akkor *monomorfizmus*nak,

Epimorfizmus

Ha φ G'-re képez (szürjektív), akkor egy G'-re való *epimorfizmus*nak nevezzük.

Izomorfizmus

Ha φ kölcsönösen egyértelmű és G'-re képez (bijektív), akkor azt mondjuk, hogy φ *izomorfizmus* G és G' között.

Ha G és G' között létezik izomorfizmus,
akkor azt mondjuk, hogy izomorfak;
ilyenkor algebrai szempontból nem lehet különbséget tenni közöttük.

Endomorfizmus

Ha $G' = G$ ugyanazzal a művelettel, akkor a homomorfizmusokat *endomorfizmus*-nak.

Automorfizmus

Ha $G' = G$ ugyanazzal a műveletttel, akkor az izomorfizmusokat *automorfizmus*oknak nevezzük.

Homomorfizmusok összetétele is homomorfizmus:
$\varphi' : G' \to G''$ is homomorfizmus, akkor

$$\begin{aligned}(\varphi' \circ \varphi)(xy) &= \varphi'\big(\varphi(xy)\big) \\ &= \varphi'\big(\varphi(x)\varphi(y)\big) \\ &= \varphi'\big(\varphi(x)\big)\varphi'\big(\varphi(y)\big) \\ &= (\varphi' \circ \varphi)(x)(\varphi' \circ \varphi)(y).\end{aligned}$$

Izomorfizmusok összetétele izomorfizmus.
Izomorfizmus inverze is izomorfizmus:

$$\varphi^{-1}\big((\varphi(x)\varphi(y)\big) = \varphi^{-1}\big(\varphi(xy)\big) = xy = \varphi^{-1}\big(\varphi(x)\big)\varphi^{-1}\big(\varphi(y)\big).$$

Az $\mathbb{I}_G$ automorfizmus.

Példák

(1) Ha $a > 1$, akkor az $x \mapsto a^x$ leképezés $(\mathbb{R}, +)$-nak a pozitív valós számok szorzással tekintett csoportjára izomorfizmus.

(2) Az $(\mathbb{R}, +)$ és $\big(\mathbb{R} \setminus \{0\}, \cdot\big)$ nem izomorfak, mert az másodikban két olyan elem is van, amelynek a négyzete az egységelem.

Reprezentációk

Fontos példánk egységelemes félcsoportra
egy tetszőleges X halmaz önmagába való leképezéseinek halmaza a függvényösszetétellel, mint művelettel.

Ha egy félcsoportnak egy ilyen leképezés-félcsoportba való homomorfizmusát tekintjük,
akkor a félcsoport *reprezentációjáról*, magyarul *ábrázolásról* beszélünk.

Ha a reprezentáció izomorfizmus, akkor *hű reprezentációról* beszélünk.

Bármely G egységelemes félcsoportnak könnyen megadhatjuk egy hű reprezentációját:

legyen $X = G$, és ha $g \in G$, legyen $\varphi_g(x) = gx$ minden $x \in X$-re, azaz φ_g a g-vel való balszorzás.

A $g \to \varphi_g$ leképezés homomorfizmus, mert

$$\varphi_{gh}(x) = ghx = \varphi_g(hx) = (\varphi_g \circ \varphi_h)(x), \quad \text{ha} \quad x \in X.$$

Ha $g \neq h$, akkor $\varphi_g \neq \varphi_h$, mert ha e az egységelem, akkor

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

így a reprezentáció hű.

Ezt a reprezentációt *G reguláris reprezentációnak* nevezzük.

Tétel

Az előző definíció jelöléseivel,
(1)ha G félcsoport, akkor a homomorf képe is félcsoport;

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

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

(4)ha G-ben g és h felcserélhetőek, akkor a homomorf képben g és h képei felcserélhetőek.

Bizonyítás

Jelölje x képét x'.
Ha G félcsoport, akkor a homomorf kép tetszőleges három elemét felírhatjuk a', b', c' alakban, ahol $a, b, c \in G$.

Bizonyítás folytatása

Ekkor a művelettartás miatt, ha G félcsoport, akkor
$(a'b')c' = (ab)'c' = (abc)' = a'(bc)' = a'(b'c')$.
Hasonlóan, ha e jobboldali egységeleme G-nek, mivel a homomorf kép egy tetszőleges eleme g' alakban írható, $g'e' = (ge)' = g'$, stb.
Ha g^* a g jobb oldali inverze, akkor $g'g^{*\prime} = (gg^*)' = e'$, stb.

Végül, ha g és h felcserélhetőek, akkor
$g'h' = (gh)' = (hg)' = h'g'$.

Következmény

-Csoport homomorf képe is csoport.

.Kommutatív félcsoport homomorf képe is kommutatív félcsoport.

-Abel-csoport homomorf képe is Abel-csoport.

Tétel

Ha G egy félcsoport, akkor az alábbi feltételek ekvivalensek:

(1)G csoport;

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

(3)$G \neq \emptyset$ és minden $a, b \in G$ esetén létezik olyan $x \in G$ illetve $y \in G$, amelyre $ax = b$ illetve
$ya = b$(a művelet invertálható);

Bizonyítás

-(1)-ből következik (2), mert az első egyenletben balról, a másodikban jobbról szorozva a^{-1}-el $x = a^{-1}b$, illetve $y = ba^{-1}$ következik,
és ezek megoldások is.

-(2)-ből következik a (3).

Bizonyítás folytatása

Belátjuk, hogy (3)-ból következik (1).
Legyen $a \in G$ rögzített.
Az $ax = a$ egyenlet megoldható, megoldását jelölje e.
Legyen $b \in G$ és y olyan eleme G-nek, amelyre $ya = b$.
Ekkor

$$be = (ya)e = y(ae) = ya = b,$$

így e jobb oldali egységelem.
Minden $b \in G$-hez létezik olyan b^*,
amelyre $bb^* = e$, mert a $bx = e$ egyenlet megoldható.

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

Vannak, akik ezt a tulajdonságot *regularitás*nak nevezik.

Megjegyezzük, hogy ha egy egységelemes félcsoportban teljesül az egyszerűsítési szabály, abból még nem következik, hogy csoport.

Példa: $(\mathbb{N}^+, \cdot)$.

Bizonyítás

A (3)-beli egyértelműségből következik.

Megjegyzés.

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

$\cdot$	α	β	γ
α	β	α	γ
β	α	γ	β
γ	γ	β	α

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

Példák

(1) Ha $n \in \mathbb{N}^+$, az n-edik komplex egységgyökök a szorzással Abel-csoportot alkotnak.

(2) Legyen p prímszám.
Az összes p^n-edik egységgyökök halmaza, ahol $n = 1, 2, \ldots$ a szorzással szintén Abel-csoport, ez a $Z(p^\infty)$ *Prüfer-csoport*.
(3) Az összes egységgyökök halmaza a szorzással (tehát az első példában szereplő csoportok egyesítése) szintén Abel-csoport.
(4) Az egységnyi abszolút értékű komplex számok a szorzással Abel-csoport.
(5) A $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ kvaterniók a kvaterniószorzással nem kommutatív csoportot alkotnak.
(6) A *Klein-féle csoport*ot a szorzótáblájával definiáljuk:

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

Mivel a szorzótábla szimmetrikus, ezért a a művelet kommutatív.

Geometriai példák.

(1) Az n oldalú szabályos sokszöget önmagába vivő egybevágóságok az egymás utáni végrehajtással alkotják a D_n *diéder csoport*ot.

Ha ε jelöli a középpont körüli $2\pi/n$ szöggel (pozitív irányba) történő forgatást, az összes forgatások az ε^k, $(k = 1, 2, \ldots, n)$ leképezések, $\varepsilon^n = e$, az egységelem, az identikus leképezés.

Van még n tükrözés is a csoportban:
ha n páratlan, akkor ezek a csúcsokon átmenő szimmetriatengelyekre való tükrözések,
ha pedig n páros, akkor $n/2$ darab csúcson átmenő szimmetriatengelyre és $n/2$ darab oldalfelező merőlegesre való tükrözés van.

Jelöljön τ egy rögzített, csúcson átmenő szimmetriatengelyre való tükrözést.

Erre nyilván $\tau^2 = e$, és a tükrözések $\tau, \tau\varepsilon, \ldots, \tau\varepsilon^{n-1}$ alakúak, továbbá $\varepsilon^k\tau = \tau\varepsilon^{-k}$ minden k-ra, mert ezek különbözőek és megfordítják a körüljárási irányt.

Tehát a diédercsoport

$$D_n = \left\{e, \varepsilon, \ldots, \varepsilon^{n-1}, \tau, \tau\varepsilon, \ldots, \tau\varepsilon^{n-1}\right\},$$

a számoláshoz pedig elég tudni, hogy $\varepsilon^n = \tau^2 = e$ és $\varepsilon\tau = \tau\varepsilon^{-1}$, amiből már indukcióval következik, hogy $\varepsilon^k\tau = \tau\varepsilon^{-k}$.

A diédercsoport név onnan ered, hogy egy ilyen sokszöget „kétlapnak" tekinthetünk, és a csoport elemeit azokkal a térbeli forgatásokkal azonosíthatjuk, amelyek ezt a „kétlapot" önmagába viszik. A diédercsoport $n = 2$ esetének a Klein-féle csoport felel meg.

(2) Számos további geometriai példa adható: eltolások, forgatások, egybevágóságok, hasonlóságok, stb.

További példák: geometriai alakzatok, kristályok, kristályrácsok, molekulák összes szimmetriáinak halmaza.

A csoportelmélet számos alkalmazásában a szimmetriacsoportok igen fontos szerepet játszanak.

Például molekulák szimmetriacsoportjának ismerete sokat segít az elektronszerkezet meghatározásában (azaz a Schrödinger-egyenlet megoldásában), sőt, Wigner Jenő alapvető felismerése szerint a fizikai törvények jó része szimmetriaelvek segítségével származtatható.

Részcsoport

Egy G grupoid egy H részhalmazát *részgrupoid*nak nevezzük, ha maga is grupoid a G-beli műveletet csak H elemei között tekintve. Ha H a G-beli műveletet csak H elemei között tekintve félcsoport, csoport, stb.,
akkor *részfélcsoportnak*, *részcsoportnak*, stb. nevezzük.

Számunkra legfontosabb az az eset lesz,
amikor H részcsoportja G csoportnak.

(Szokás ennek kifejezésére a $H \leq G$ jelölést használni.)

Ha G csoport, akkor az egész G és a csak az egységelemet tartalmazó egyelemű részhalmaz részcsoportok,
ezek a *triviális részcsoportok*.

A G-től különböző részcsoportokat *valódi részcsoportnak* nevezzük.

Emlékeztetünk rá, hogy a műveletet a részhalmazok között is értelmeztük, elemenként.

Ugyanígy értelmeztük részhalmazokra az inverzképzést is, elemenként.

(Szokás a részhalmazokat *komplexus*oknak is nevezni és *komplexusműveletek*ről beszélni.)

Állítás

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

(1)H részcsoport;

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

(3)$H \neq \emptyset$, $HH \subset H$ és $H^{-1} \subset H$;

(4)$H \neq \emptyset$ és $H^{-1}H \subset H$.

Bizonyítás

Ha (1) teljesül, akkor a szorzást H elemei között végezve, az művelet, így az eredménye H-ban van,
azaz $H \times H$-t H-ba képező leképezés.

Mivel H részcsoport, tartalmaz egy mondjuk f egységelemet.

Mivel bármely $h \in H$-ra $hf = h$ és $he = h$, a G-beli egyszerűsítési szabály miatt $f = e$.

Bizonyítás folytatása

Végül mivel minden $h \in H$-nak van inverze H-ban, de G-ben is, az inverz egyértelműsége miatt $h^{-1} \in H$ minden $h \in H$-ra.

Nyilván (2)-ből következik (3). Ha (3) fennáll, akkor $H^{-1} \subset H$ miatt $H^{-1}H \subset HH \subset H$, tehát a (3)-ból kapjuk (4)-t.

Végül, ha (4) fennáll, akkor bármely $h \in H$-ra $h^{-1}h = e \in H$, így G egységeleme H-ban is az.
Minden $h \in H$-ra $h^{-1}e \in H^{-1}H \subset H$, azaz minden elemnek van inverze a G-beli,
továbbá $(h_1^{-1})^{-1} = h_1$ miatt $h_1 \in H^{-1}$ és így minden $h_1, h_2 \in H$-ra $h_1 h_2 \in H^{-1}H \subset H$, tehát (1) teljesül.

Megjegyzés

Ha H részcsoport, akkor (3)-ban és (4)-ben a tartalmazások nem valódiak,
hiszen $e \in H$ miatt $H = eH \subset HH$, $H = eH \subset H^{-1}H$ és
ha $h \in H$, akkor $h = (h^{-1})^{-1} \in H^{-1}$, azaz $H \subset H^{-1}$.

Következmény

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

Bizonyítás

Mivel $e \in H_\gamma$ minden $\gamma \in \Gamma$-ra, H nem üres.

Mivel $H^{-1} \subset H_\gamma^{-1}$, kapjuk, hogy $H^{-1}H \subset H_\gamma^{-1}H_\gamma \subset H_\gamma$ minden $\gamma \in \Gamma$-ra.

Innen viszont $H^{-1}H \subset \cap_{\gamma\in\Gamma} H_\gamma = H$,
tehát H részcsoport G-ben.

Megjegyzés

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

Generátum

Legyen G egy csoport és $K \subset G$.
A K halmaz $< K >$ *generátuma* a G összes, K-t tartalmazó részcsoportjának metszete.

Az előző következmény szerint $< K >$ részcsoport, így $< K >$ a legszűkebb, K-t tartalmazó részcsoport.

Generátorrendszere

Ha $G =< K >$, akkor azt mondjuk, hogy K a G csoport *generátorrendszere*.

Ciklikus csoport

Ha egy csoportnak létezik egyelemű generátorrendszere, akkor *ciklikus*nak nevezzük, az elemet pedig egy *generátor*ának.

Állítás

Az előző definíció jelöléseivel,

$$< K >= \{g_1 g_2 \dots g_n : n \in \mathbb{N},\ g_i \in K \cup K^{-1},\ ha\ 1 \leq i \leq n\}.$$

Emlékeztetünk rá, hogy az üres szorzat az egységelem.
Az állításból nyilván $< K >=< K^{-1} >$.

Bizonyítás

Egyrész a jobb oldalon álló halmaz részcsoport,
mert tartalmazza az egységelemet, zárt a szorzásra és az inverzképzésre, továbbá tartalmazza K elemeit,
így tartalmazza K generátumát.

Másrészt minden elemének benne kell lennie K generátumában.

Példa

Lineáris transzformációk csoportjai.

Következmény

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

Bizonyítás

Az első állítás nyilvánvaló az előző állítás alapján.

Tegyük fel, hogy g a G ciklikus csoport egy generátora, φ pedig egy homomorfizmusa G-nek.

Ekkor indukcióval $\varphi(g^n) = \varphi(g)^n$ minden $n \in \mathbb{N}$-re és így $\varphi(h^{-1}) = \varphi(h)^{-1}$ miatt minden $n \in \mathbb{Z}$-re is,
így $\varphi(< g >) =< \varphi(g) >$.

Rend

Egy G véges csoport *rend*jén az elemeinek számát értjük, egyébként azt mondjuk, hogy a *csoport rendje végtelen*.

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

Tétel

Végtelen ciklikus csoport izomorf az egész számok additív csoportjával,

míg n elemű ciklikus csoport a modulo n maradékosztályok $\mathbb{Z}_n$ additív csoportjával izomorf.

Speciálisan, ciklikus csoportok kommutatívak.

Bizonyítás

Legyen g egy generátor, és tekintsük az $n \mapsto g^n$, $n \in \mathbb{Z}$ homomorfizmust.

Bizonyítás folytatása

Ha ez kölcsönösen egyértelmű, akkor izomorfizmusa $\mathbb{Z}$-nek G-re.

Ha ez a leképezés nem kölcsönösen egyértelmű, akkor vannak olyan $i > j$ kitevők, hogy $g^i = g^j$.

Ekkor $g^{i-j} = e$, tehát van olyan pozitív egész szám, amelyre hatványozva g-t az egységelemet kapjuk.

Jelölje n a legkisebb ilyen pozitív egész kitevőt, azaz g rendjét.

Ha $0 \leq r < n$ és $g^r = e$, akkor $r = 0$.

Az $e, g, g^2, \ldots, g^{n-1}$ elemek mind különbözőek, mert ha $0 \leq j < i < n$ esetén $g^i = g^j$ teljesülne,
akkor abból $g^{i-j} = e$ következne, ami lehetetlen.

Másrészt ha $i > j$ és $i \equiv j \pmod{n}$, akkor $i = j + kn$ valamely $k \in \mathbb{N}$-re,
így $g^i = g^{j+kn} = g^j (g^n)^k = g^j e^k = g^j$.

Bizonyítás folytatása

Így G-nek n eleme van, a $\varphi : i \mapsto g^i$ leképezés $\mathbb{Z}$-t G-re képezi, műveletartó és minden modulo n maradékosztályon konstans.

Legyen $\tilde{\varphi}$ az a leképezés, amely $\mathbb{Z}_n$ egy maradékosztályához G-nek azt az elemét rendeli,
amelyet φ rendel a maradékosztály elemeihez.

$\tilde{\varphi}$ a $\mathbb{Z}_n$ additív csoportját G-re képezi,
mivel mindkettőnek n eleme van, kölcsönösen egyértelmű,
és mivel φ műveletartó volt, homomorfizmus is:

ha $\tilde{x}, \tilde{y} \in \mathbb{Z}_n$, akkor $\tilde{\varphi}(\tilde{x} + \tilde{y}) = \tilde{\varphi}(\widetilde{x + y}) =$
$= \varphi(x + y) = \varphi(x)\varphi(y) = \tilde{\varphi}(\tilde{x})\tilde{\varphi}(\tilde{y})$,
tehát $\tilde{\varphi}$ izomorfizmus.

Megjegyzés.
Az előző bizonyítás azt is mutatja, hogy véges rendű elem rendje megegyezik az általa generált ciklikus csoport rendjével.

Tétel

Ciklikus csoport minden részcsoportja is ciklikus.

Bizonyítás

Legyen $G =< g >$ és H a részcsoport.

Ha $H = \{e\}$, készen vagyunk.

Egyébként van olyan nullától különböző $k \in \mathbb{Z}$, amelyre $g^k \in H$.

Feltehető, hogy $k > 0$, mert egyébként k helyett $-k$-t vehetünk.

Legyen d az a legkisebb pozitív kitevő, amelyre $g^d \in H$.

Megmutatjuk, hogy $H =< g^d >$.
Azt kell bizonyítani, hogy H-nak tetszőleges g^m eleme g^d hatványa.
Legyen $q = \lfloor m/d \rfloor$, $r = m \bmod d$.
Ekkor $g^r = g^{m-qd} = g^m (g^d)^{-q} \in H$, ahonnan d definíciója miatt $r = 0$, és így $g^m = (g^d)^q$.

Tétel

Legyen G egy n rendű véges ciklikus csoport,
g pedig egy generátoreleme G-nek.

Ha $a \in \mathbb{Z}$ és $d = lnko(a, n)$,
akkor g^a az egyetlen m-ed rendű $H = \{g^d g^{2d}, \ldots g^{md} = e\}$ ciklikus részcsoportot genrálja, ahol $n = md$.

A G minden részcsoportja előáll így valamely $d|n$-re.
G-nek $\varphi(n)$ generátora van.

Bizonyítás

Az előző tétel bizonyítása szerint minden H részcsoport g^d hatványaiból áll,
ahol d a legkisebb pozitív kitevő,
amelyre $g^d \in H$ és $j = n$ választással azt is kapjuk,
hogy $n \mod d = 0$, azaz $d|n$, $n = md$,
amiből $H = \{g^d g^{2d}, \ldots g^{md} = e\}$,
tehát H rendje egyértelműen meghatározza d-t és igy H-t.

Bizonyítás folytatása

Mivel g^a a g^d hatványa, így az általa generált részcsoport része H-nak.
Mivel alkalmas $x, y \in \mathbb{Z}$-re $d = ax + ny$,
azt kapjuk, hogy $g^d = g^{ax+ny} = g^{ax} g^{ny} = g^{ax} e^y = g^{ax} = (g^a)^x$ és így g^a generálja is H-t.

Az utolsó állítás abból következik,
hogy $\varphi(n)$ darab olyan $0 \leq a < n$ természetes szám van, amelyre a és n relatív prímek.
$\triangle$

Egy halmaz elemeit egy műveleti tulajdonság szerint osztályokba soroljuk és a továbbiakban ezeket osztályokat vizsgáljuk.

Például az egész számokat az n-nel való osztási maradékuk szerint n osztályba sorolhatjuk, így ha két egész szám összeadásánál az osztási maradék moduló n érdekel minket, akkor elég ebben az n elemű halmazban számolni.

Algebrai struktúra osztályokra bontását általánosabban fogjuk tárgyalni.

Mellékosztályok

Legyen G egy csoport és legyen H a G egy részcsoportja.
Vezessük be az $a \sim b$, ha $ab^{-1} \in H$ relációt.

Ez ekvivalenciareláció.

Vizsgáljuk meg az ekvivalenciaosztályokat.

Azt állítjuk, hogy $a \in G$ ekvivalenciaosztálya a Ha halmaz.

Ha $b \in Ha$, akkor $b = ha$ valamely $h \in H$-ra.

Innen $ba^{-1} = h$, azaz $ab^{-1} = h^{-1} \in H$.
Megfordítva, ha $a \sim b$, akkor $ab^{-1} = h \in H$, ahonnan
$b = h^{-1}a \in H^{-1}a \subset Ha$.

Ha most az $a \sim b$, ha $b^{-1}a \in H$ ekvivalenciarelációt vezetjük be, akkor hasonlóan számolva kapjuk, hogy az a ekvivalenciaosztálya az aH halmaz.

Mellékosztályok

Az előző ekvivalenciaosztályokat a G csoport H szerinti *jobb oldali mellékosztályainak*,
az utóbbiakat pedig *bal oldali mellékosztályainak* nevezzük.

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

Index

Ha véges sok jobb oldali mellékosztály van,
akkor azok száma a H *indexe*,
egyébként azt mondjuk, hogy H *indexe* végtelen.

A H részcsoport G beli indexét $[G : H]$-val jelöljük.

Lagrange tétele

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

Bizonyítás

Dolgozhatunk jobb oldali mellékosztályokkal.
Akármelyik a elem mellékosztálya és
H között a $h \mapsto ha$,
$h \in H$ leképezés az egyszerűsítési szabály miatt bijektív,
így a mellékosztályoknak mindnek ugyanannyi eleme van, mint H-nak.
Mivel páronként diszjunktak és uniójuk G, készen vagyunk.

Következmény

Véges csoportban elem rendje osztja a csoport rendjét.

Bizonyítás

Az elem rendje az általa generált részcsoport rendje.

Következmény

Prímszámrendű csoport ciklikus.

Bizonyítás

Bármely az egységelemtől különböző eleme kell, hogy generálja.

Tétel

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

Bizonyítás

Az, hogy prímszámrendű csoportnak csak triviális részcsoportja vannak,
azonnal következik Lagrange tételéből.
Ha csak triviális részcsoportok vannak,
akkor bármely, az egységelemtől különböző g eleme a csoportnak generálja a csoportot, így az ciklikus.

Bizonyítás folytatása

A ciklikus csoportok közül pedig csak a prímszámrendűeknek nincs valódi részcsoportjuk:
ha a csoport végtelen rendű, akkor $< g^2 >$ valódi részcsoport,
ha pedig a csoport rendje $n = n_1 n_2$, $n_1, n_2 > 1$,
akkor $< g^{n_1} >$ egy valódi részcsoport.

Normálosztó.

Egy G csoport egy N részcsoportja szerint mellékosztályok között a (komplexus) szorzás nem feltétlenül kompatibilis az osztályozással: $NaNb$ nem biztos hogy egyenlő Nab-vel vagy egyáltalán egy jobb oldali mellékosztállyal.

Normálosztó

Ha N részcsoportja G-nek és minden $a \in G$-re $aN = Na$, akkor N-et *normálosztó*nak vagy *normális részcsoport*nak vagy *invariáns részcsoport*nak nevezzük.

(Szokásos az $N \lhd G$ jelölés.)

Ha N normálosztó, akkor nyilván a jobb és bal oldali mellékosztályok megegyeznek és

fordítva, ha egy N részcsoportra a jobb és bal oldali mellékosztályok megegyeznek, akkor - felhasználva, hogy aN és Na is tartalmazza a-t - kapjuk, hogy $aN = Na$ minden $a \in G$-re.

-Meg fogjuk mutatni, hogy normálosztóknál a művelet kompatibilis az osztályozással.

Abel-csoportban minden részcsoport normálosztó.

Az egész G és a csak az egységelemet tartalmazó egyelemű részhalmaz normálosztók, ezek a *triviális normálosztók*.

A G-től különböző normálosztókat *valódi normálosztóknak* nevezzük.

Egy 2 indexű N részcsoport mindíg normálosztó, mert csak két bal és két jobb oldali mellékosztálya van, N és $G \setminus N$.

Tétel

Legyen N a G csoport részcsoportja. A következő feltételek ekvivalensek:
(1)N normálosztó;
(2)$a^{-1}Na = N$ minden $a \in G$-re;
(3)$a^{-1}Na \subset N$ minden $a \in G$-re;

Bizonyítás

(1)-ből következik (2), mert $a^{-1}Na = Na^{-1}a = N$.
(2)-ből következik (1), mivel $Na = a(a^{-1}Na) = aN$.
(2)-ből következik (3).
Ha (3) fennáll, akkor $a^{-1}Na \subset N$, és a helyére a^{-1}-et írva $aNa^{-1} \subset N$, amiből

$$N = a^{-1}(aNa^{-1})a \subset a^{-1}Na$$

így (2)-t kaptuk.

Következmény

Normálosztók metszete is normálosztó.

Következik (3)-ból; a bizonyítás hasonló annak bizonyításához, hogy részcsoportok metszete részcsoport.

Példa.

A D_3 diédercsoportban egy adott τ tükrözés által generált $H = \{e, \tau\}$ részcsoport nem normálosztó,
mert $H\varepsilon = \{\varepsilon, \tau\varepsilon\}$ de $\varepsilon H = \{\varepsilon, \varepsilon\tau\} = \{\varepsilon, \tau\varepsilon^2\}$.
A forgatások által alkotott $\{e, \varepsilon, \varepsilon^2\}$ részcsoport normálosztó, mert 2 az indexe.

Belső automorfizmusok

Ha G csoport és $a \in G$ rögzített, akkor a G-én értelmezett $x \mapsto a^{-1}xa$, leképezés automorfizmusa G-nek, mert xy-hoz az $a^{-1}(xy)a$ elemet rendeli, ami $a^{-1}xa$ és $a^{-1}ya$ szorzata, tehát homomorfizmus, az egyszerűsítési szabály miatt kölcsönösen egyértelmű és minden elem előáll képként, mert x az axa^{-1} képe.

-Altalában nem minden automorfizmus belső automorfizmus: például kommutatív esetben csak az identikus leképezés belső automorfizmus, de az inverzképzés is automorfizmus.

-Ha az x elemhez van olyan belső automorfízmus, amely y-ba viszi át, akkor azt mondjuk, hogy x és y *konjugáltak*.

-Ez ekvivalenciareláció, az ekvivalenciaosztályok a *konjugált elemosztályok*.

-Egy automorfizmusnál egy részcsoport képe részcsoport.

-Az előző tétel (2) pontja szerint a normálosztók pontosan azok a részcsoportok, amelyeknek a képe minden belső automorfizmusnál saját maga, azaz olyan részcsoportok, amelyek minden elemükhöz az azzal konjugáltakat is tartalmazzák.

Ez az oka az invariáns részcsoport elnevezésnek.

Centralizátor és centrum*

Egy G csoport egy adott x elemével felcserélhető elemek G-nek egy részcsoportját alkotják, ez az x *centralizátora*, jelölése $C(x)$.

A $C = \cap_{x \in G} C(x)$ részcsoport normálosztó is, hiszen G minden elemmel felcserélhető elemeit tartalmazza,
ezeket pedig minden belső automorfizmus az egységelembe viszi;
C a G csoport *centruma*.

Osztályegyenlet*

Egy G csoportban az $x \in G$ elem *konjugált elemosztályának annyi eleme van, amennyi* $C(x)$ *szerinti mellékosztály.*

Ha G véges csoport, akkor $\sum [G : C(x)]$ a G rendje, ahol az összegzés a különböző elemosztályokból választott egy-egy x-re értendő; ez az osztályegyenlet.

Bizonyítás*

Az x konjugáltja, $g^{-1}xg$ és $h^{-1}xh$ pontosan akkor egyenlő, ha $(hg^{-1})x = x(hg^{-1})^{-1}$, azaz ha $hg^{-1} \in C(x)$.
Ez azzal ekvivalens, hogy g és h ugyanazon $C(x)$ szerinti jobboldali mellékosztákyba tartoznak.
Ezzel az első állítást beláttuk.
A konjugált elemosztályok elemszámának összege G rendje.

Tétel

Legyen G csoport. Ekkor
(1) egy N normálosztó szerinti mellékosztályok a csoportnak a művelettel kompatibilis osztályozását alkotják.

(2) egy N normálosztó szerinti mellékosztályok közötti művelet megegyezik az osztályok mint halmazok komplexusszorzásával.

(3) minden, a művelettel kompatibilis osztályozás esetén az egységelem osztálya normálosztó és az osztályozás ezen normálosztó szerinti mellékosztályokból áll.

Bizonyítás

Ha N normálosztó, $a' \in Na$ és $b' \in Nb$, akkor a részcsoportok szerinti mellékosztályokról tanultakat felhasználva $Na' = Na$ és $Nb' = Nb$, tehát

$$a'b' \in (Na')(Nb') = (Na)(Nb) = N(aN)b = N(Na)b = N^2ab =$$

$$= Nab,$$

azaz az osztályozás kompatibilis a művelettel, amivel beláttuk az (1)-t.
Másrészt

$$\{a'b' : a' \in Na, b' \in Nb\} = (Na)(Nb) = Nab,$$

tehát az osztályok szorzása megegyezik a komplexusszorzással, amivel beláttuk a (2)-t.

Bizonyítás folytatása

A (3)-as bizonyításához tegyük fel, hogy adott egy, a szorzással kompatibilis ekvivalenciareláció, és jelölje N az e egységelem osztályát.

Mivel $a \in N$ esetén $e = a^{-1}a \sim a^{-1}e = a^{-1}$, kapjuk hogy $N^{-1} \subset N$.

Ha $a, b \in N$ fennáll, akkor $ab \sim ee = e$, így $NN \subset N$, tehát N részcsoport.

Ha most $x \in N$ és g tetszőleges, akkor $g^{-1}xg \sim g^{-1}eg = e$, így $g^{-1}Ng \subset N$, tehát N normálosztó.

Ha a és b ekvivalensek, akkor $a^{-1}ab^{-1}$ és $a^{-1}bb^{-1}$ is, azaz $a^{-1} \sim b^{-1}$.

Innen viszont $e = aa^{-1} \sim ab^{-1}$, azaz $ab^{-1} \in N$.

Megfordítva, ha $ab^{-1} \in N$, azaz $ab^{-1} \sim e$, akkor $a = ab^{-1}b \sim eb = b$, és így az ekvivalenciarelációhoz tartozó osztályozás pontosan az N szerinti mellékosztályokból áll.

Következmény

Egy G csoportnak egy N normálosztó szerinti mellékosztályai a (komplexus)szorzásra nézve csoportot alkotnak.

Bizonyítás

A G-nek a mellékosztályok (a komplexusszorzással mint művelettel tekintett) halmazára való $a \mapsto Na$ leképezése művelettartó, így a homomorf képre tanultakból következik az állítás.

Faktorcsoport

Az előző következményben szereplő csoportot a G csoport N normálosztó szerinti *faktorcsoport*jának (vagy *hányadoscsoport*jának) nevezzük és G/N-el jelöljük. Ha G rendje véges, akkor G/N rendje $[G : N]$.

Altalában a faktor struktúrák azért fontosak, mert ha számos esetben lehetőség van arra, hogy ezekben vizsgáljuk az eredeti struktúra bizonyos tulajdonságait.

Példák.

(1) Ha $N = G$, akkor G/N egyelemű. Ha $N = \{e\}$, akkor az osztályok egyeleműek, így G/N izomorf G-vel.

(2) A $\mathbb{Z}$ additív csoportban bármely $m \in \mathbb{Z}$-re az $m\mathbb{Z}$ normálosztó szerint faktorcsoport $\mathbb{Z}_m$ additív csoportja.

(3) A kvaterniócsoportban a kételemű $< -1 >$ részcsoport szerinti faktorcsoport izomorf a Klein-féle csoporttal.

Homomorfizmus magja

Egy G csoportnak egy G' csoportba való φ homomorfizmusánál a *homomorfizmus magja*-n a G' csoport e' egységelemének a teljes inverz képét értjük.

A φ magját $\ker(\varphi)$-vel jelöljük.

Homomorfizmustétel

Egy G csoport egy φ homomorfizmusánál a homomorfizmus magja normálosztó.

és a $G/\ker(\varphi)$ faktorcsoport izomorf $G' = \varphi(G)$-vel.

A G bármely N normálosztója magja valamely homomorfizmusnak: a G-nek G/N-re való kanonikus leképezése homomorfizmus, amelynek magja N.

Bizonyítás

A $\varphi^{-1}(a')$, $a' \in G'$ halmazrendszer a G egy osztályozása.

Megmutatjuk, hogy kompatibilis a szorzással.

Valóban, bármely $a \in \varphi^{-1}(a')$-re és $b \in \varphi^{-1}(b')$-re $\varphi(ab) = \varphi(a)\varphi(b) = a'b'$, azaz $ab \in \varphi^{-1}(a'b')$, függetlenül az a és b választásától.

Bizonyítás folytatása

Igy $e \in \varphi^{-1}(e')$ osztálya, ami $\ker(\varphi)$, normálosztó, és a szerinte vett osztályozás éppen a megadott osztályozás.

Az $a' \mapsto \varphi^{-1}(a')$ bijeleképktív leképezés homomorfizmus és így G' izomorfizmusa $G/\ker(\varphi)$-re.

A tétel második fele az előző tétel következményének bizonyítása alapján nyilvánvaló.

Konkrét példa:

G az egész számok halmaza a $+$ művelettel, G' a $\{\uparrow, \uparrow\}$ halmaz a kizáró vagy művelettel a φ függvény pedig az $n \longrightarrow 2|n$ logikai értékű leképezés, így

$\ker(\varphi) = 2\mathbb{Z}$.

A kanonikus leképezés G-ből $G/\ker(\varphi)$-re κ, az izomorfizmus pedig ψ.

Direkt szorzat

Legyen G_i, $i \in I$ egy-egy binér művelettel ellátott halmazok egy családja.

Az egyszerűség kedvéért mindegyik halmazon a műveletet jelöljük szorzással. Ekkor a

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

Descartes-szorzatot ellátva az $(ab)_i = a_i b_i$, ha $i \in I$ összefüggéssel definiált művelettel a G-t a G_i, $i \in I$ család *direkt szorzat*ának nevezzük.

-A legfontosabb speciális eset, amikor $I = \{1, 2, \ldots, n\}$, ekkor a direkt szorzat elemei $a = (a_1, a_2, \ldots, a_n)$, $a_i \in G_i$, ha $i \in I$ alakú n-esek.

-Mivel a szorzás definíció szerint koordinátánként történik, ha $b = (b_1, b_2, \ldots, b_n)$ egy másik eleme a direkt szorzatnak, akkor $ab = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$.

-Ha minden G_i félcsoport, akkor G is, ha minden G_i kommutatív, akkor G is, ha minden G_i egységelemes, akkor G is, és ha minden G_i csoport, akkor G is.

-Ez utóbbi esetben ha $J \subset I$, akkor az $a \mapsto a|_J$ projekció homomorfizmus, képe $\times_{i \in J} G_i$, magja pedig izomorf $\times_{i \in I \setminus J} G_i$-vel.

A direkt szorzás segítségével a véges Abel-csoportok szerkezete teljesen leírható:

Végesen generált Abel-csoportok alaptétele

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

Cayley tétele

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

A halmaz választható G-nek.

Bizonyítás

Tekintsük G reguláris reprezentációját, azaz
legyen $a \in G$ és a-hoz rendelt p_a-ra legyen $p_a(x) = ax$, ha $x \in G$.

Tudjuk, hogy az $a \mapsto p_a$ hozzárendelés monomorfizmus.
A p_a leképezések az egyszerüsítési szabály miatt kölcsönösen egyértelműek és a G-re képeznek, mivel $a^{-1}x$ képe p_a-nál x.

Permutációcsoportok.

Tetszőleges A halmaz összes permutációnak a $\circ$ művelettel tekintett csoportját, az A halmaz *szimmetrikus csoport*jának nevezzük míg annak részcsoportjait, a *permutációcsoport*ok.
A szimmetrikus csoport szerkezete csak az alaphalmaz elemeinek számától függ:

Ha φ az A halmaznak a B halmazra való kölcsönösen egyértelmű leképezése, akkor tudjuk, hogy $f \mapsto \varphi \circ f \circ \varphi^{-1}$ megfeleltetés kölcsönösen egyértelmű leképezése (bijekciója) A összes permutációinak B összes permutációira.
Mivel a permutációk összetételére ez a megfeleltetés művelettartó is, hiszen

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

így A és B permutációinak csoportjai izomorfak.
Mivel minket elsősorban a véges csoportok érdekelnek, az $\{1, 2, \ldots, n\}$, $n \in \mathbb{N}$ alakú halmazok permutációinak vizsgálatára szorítkozhatunk.
Az $\{1, 2, \ldots, n\}$ halmaz összes permutációinak csoportját S_n-el fogjuk jelölni és n-ed fokú *szimmetrikus csoport*nak nevezzük. Rendje $n!$.

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

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

azaz minden elem alá odaírjuk a képét.
Bármilyen más sorrendben is felírhatjuk az elemeket és alájuk a képüket, például ha $q \in S_n$,

$$q = \begin{pmatrix} 1 & 2 & \ldots & n \\ q_1 & q_2 & \ldots & q_n \end{pmatrix}$$

egy tetszőleges másik permutáció, akkor p írható

$$p = \begin{pmatrix} q_1 & q_2 & \ldots & q_n \\ p_{q_1} & p_{q_2} & \ldots & p_{q_n} \end{pmatrix}$$

alakban is. A két permutáció szorzata

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

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

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

Egy

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

alakban írt permutációra legyen k az inverziók száma az alsó sorban, azaz az összes olyan $1 \leq i < j \leq n$ párok száma, amelyekre $p_i > p_j$.

A permutációt *páros permutáció*nak illetve *páratlan permutáció*nak nevezzük a szerint, hogy k páros vagy páratlan, ez a permutáció *paritása*.

Permutációkat egy másik alakban is felírhatunk.

Ha $1 \leq i_1, i_2, \ldots, i_k \leq n$ különböző természetes számok,
jelölje $(i_1, i_2, \ldots, i_k)$ azt a permutációt, amely i_1-et i_2-be, i_2-t i_3-ba, stb., i_k-t i_1-be viszi, minden más számot pedig fixen hagy.

Egy ilyen permutációt k hosszúságú *ciklus*nak nevezünk.
(A ciklus jelölés nem teljesen pontos, mert nem derül ki belőle, hogy mely S_n elemeiről van szó.)

Egy ciklus többféleképpen is felírható, bármelyik i_j-vel kezdhetünk.

Diszjunkt ciklusok nyilván felcserélhetőek.

Minden permutáció felírható páronként diszjunkt ciklusok szorzataként,
és ez az előállítás egyértelmű is,
ha a sorrendtől és a felírásból nyilván elhagyható egy (vagy nulla) hosszúságú ciklusoktól eltekintünk.

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

Mivel

$$(i_1, i_2, i_3, i_4, \ldots, i_k) = (i_1, i_3, i_4, \ldots, i_k)(i_1, i_2),$$

minden permutáció felírható transzpozíciók szorzataként.
Bár ez az előállítás nem egyértelmű, az alábbi állítás igaz:

Tétel*

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

Bizonyítás

MIvel az identikus permutáció páros, csak azt kell megmutatnunk, hogy ha egy permutációt jobbról szorzunk egy transzpozícióval, akkor megváltozik a permutáció paritása. Ha a

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

permutációt szorozzuk az (i,j), $i < j$ transzpozícióval jobbról,

akkor az eredmény a

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ p_1 & p_2 & \dots & p_j & \dots & p_i & \dots & p_n \end{pmatrix}$$

permutáció. Ha $k < i$ vagy $k > j$, akor azon inverziók száma, amelyekben p_k résztvesz, nem változik.

Ugyanez a helyzet, ha $i < k < j$, de p_k vagy nagyobb, mint $\max\{p_i, p_j\}$ vagy kisebb mint $\min\{p_i, p_j\}$.

Ha $i < k < j$ és $\min\{p_i, p_j\} < p_k < \max\{p_i, p_j\}$, akkor azon inverziók száma, amelyekben p_k résztvesz, kettővel változik.

Mivel $p_i > p_j$ esetén egy inverzió megszűnik, $p_i < p_j$ esetén pedig egy új keletkezik, az állítást beláttuk.

Következmény

Az S_n csoportbanszorzásnál a paritások "mod 2 összeadódnak": egy páros és egy páratlan permutáció szorzata páratlan. Két páros vagy két páratlan permutáció szorzata páros.

A páros permutációk részcsoportot alkotnak S_n-ben.

Példa.

Az S_4-ben

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1,3,2,4) = (1,3)(1,2)(1,4)$$

páratlan, míg

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = () = (1,2)(2,1) = (1,3)(3,1)$$

páros.

Definíció

Egy G csoport egy *normálláncán* részcsoportoknak egy olyan

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

véges sorozatát értjük, amelyben G_i normálosztó G_{i-1}-ben, ha $i = 1, 2, \ldots, n$.

A G csoportot *feloldhatónak* nevezzük, ha van olyan normállánca, amelynek a G_{i-1}/G_i *faktorai* Abel-csoportok.

A normállánc faktorai némi tájékoztatást nyújtanak a csoportról.

Mivel a véges Abel-csoportok szerkezetét ismerjük, a feloldható véges csoportokról elég sok információnk van.

Vannak azonban olyan csoportok, amelyeknek egyáltalán nincs nem triviális normálosztója, ezeket *egyszerű csoport*nak nevezzük.

Egy előző tételből tudjuk, hogy az egyszerű véges Abel-csoportok az egyelemű csoport és a prímrendű ciklikus csoportok.

A nemkommutatív véges egyszerű csoportok is ismertek (ez a csoportelmélet egyik legnagyobb diadala), ezeknek azonban már a felsorolása is olyan bonyolult, hogy itt nem lehet tárgyalni, annak bizonyítása pedig hogy valóban ezek és csak ezek a véges egyszerű csoportok, több tízezer oldal több száz cikkben szétszórva.

Legyen $n > 1$ természetes szám.
Az előző következmény szerint $S_n \supset A_n \supset \{e\}$ egy normállánca S_n-nek.
Megmutatható, hogy $n \geq 5$ esetén A_n nem kommutatív egyszerű csoport, így ez a normállánc nem is bővíthető tovább.
Ennek felhasználásával az is belátható, hogy S_n nem felodható, ha $n \geq 5$.

Példa

Megmutatható, hogy S_4-ben

$$\{()\} \subsetneq \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subsetneq A_4, \subsetneq S_4$$

a normálosztók, ahol () az identikus permutáció, így A_4 nem egyszerű csoport.

Gyűrűk testek

Gyűrűk

Egy R halmazt egy $(+, \cdot)$ binér műveletekből álló párral *gyűrű*nek nevezünk, ha az összeadással Abel-csoport (a nullelemet 0 fogja jelölni), a szorzással félcsoport, és teljesül mindkét oldali disztributivitás, azaz ha $x, y, z \in R$, akkor

$$x(y+z) = xy + xz \quad \text{és} \quad (y+z)x = yx + zx.$$

-Ha a szorzás kommutatív, akkor a gyűrűt *kommutatív gyűrű*nek nevezzük.

-Ha a szorzásnak van egységeleme, akkor a gyűrűt *egységelemes gyűrű*nek nevezzük.

-Tetszőleges gyűrűben $x0 = x(0+0) = x0 + x0$.

Mindkét oldalhoz hozzáadva $-x0$-t, kapjuk, hogy $x0 = 0$.

Hasonlóan adódik, hogy $0x = 0$. érvényes az úgynevezett „előjelszabály” is: $(-x)y = x(-y) = -xy$ és $(-x)(-y) = xy$ minden x, y elemre.

Például

$xy + (-x)y = \big(x + (-x)\big)y = 0y = 0$, amiből az inverz egyértelműsége miatt $(-x)y = -xy$;
a többi összefüggés hasonlóan adódik.

Az is teljesül, hogy $n(xy) = (nx)y = x(ny)$ minden x, y gyűrűbeli elemre és $n \in \mathbb{Z}$-re.

(Figyelem, $(n, x) \mapsto nx$ nem a gyűrűbeli szorzás, hanem ismételt összeadással van definiálva!).

Ha $n \in \mathbb{N}$, ekkor ez az összefüggés teljes indukcióval adódik, felhasználva a disztributivitást; innen az általános esetet az előjelszabály felhasználásával kapjuk.

Nullgyűrű

A legegyszerűbb példa a *nullgyűrű*, amely csak egy elemet tartalmaz, ez nyilván a 0.

Zérógyűrű

additív Abel-csoport, amelyben bármely két elem szorzatát nullának értelmezzük;
ezeket a gyűrűket *zérógyűrű*nek nevezzük.

Fontosabb példa $\mathbb{Z}$.

Ezek a gyűrűk mind kommutatív gyűrűk, a nullgyűrű és $\mathbb{Z}$ egységelemesek.

Példák

Példák gyűrűkre a racionális és a valós számok,
a páros egész számok, a racionális együtthatós polinomok, a valós együtthatós polinomok,

Nullosztók, integritási tartomány, rendezett integritási tartomány

Mint a zérógyűrűk példája mutatja, két nem nulla elem szorzata lehet nulla egy gyűrűben.

Nullosztó

Ha x, y egy R gyűrű nullától különböző elemei, és $xy = 0$, akkor azt mondjuk, hogy x és y egy *nullosztópár*, x *bal oldali nullosztó*, y pedig jobb oldali nullosztó.

A nullgyűrűben nincsenek ilyenek, de ez a gyűrű érdektelen.

Ezért egy legalább kételemű gyűrűt *nullosztómentes*nek nevezünk, ha nincsenek benne nullosztópárok.

Ez azzal ekvivalens, hogy $R \setminus \{0\}$ egy nem üres félcsoport a szorzással.

- Nullosztómentes gyűrűben nem nulla elemmel való szorzásnál lehet balról is, jobbról is egyszerűsíteni, mert ha $xy = xz$ vagy $yx = zx$, akkor $x(y - z) = 0$ vagy $(y - z)x = 0$, így $y - z = 0$.

-A megfordítás:
ha van nullosztópár, akkor a bal oldali nullosztóval balról,
a jobb oldali nullosztóval pedig jobbról nem lehet egyszerűsíteni.

-Ha a gyűrűben van a nullától különböző egységelem, és x-nek van multiplikatív inverze,
akkor x nem lehet sem bal, sem jobb oldali nullosztó, hiszen
$xy = 0$-ból vagy $yx = 0$-ból $x^{-1}xy = y = 0$ illetve $yxx^{-1} = y = 0$ következik.

Integritási tartomány

Kommutatív nullosztómentes gyűrűt *integritási tartomány*nak nevezünk.

Nyilván $\mathbb{Z}$ egységelemes integritási tartomány.

Rendezett integritási tartomány

Az R-et *rendezett integritási tartomány*nak nevezzük, ha rendezett halmaz, integritási tartomány, és
(1)ha $x, y, z \in R$ és $x \leq y$, akkor $x + z \leq y + z$ (az *összeadás monoton*);
(2)ha $x, y \in R$ és $x, y \geq 0$, akkor $xy \geq 0$ (a *szorzás monoton*).

-A $\mathbb{Z}$ tulajdonságait felsoroló tétel úgy is fogalmazható, hogy $\mathbb{Z}$ rendezett integritási tartomány.

Tétel

Egy rendezett halmaz, amely integritási tartomány, akkor és csak akkor rendezett integritási tartomány, ha az alábbi feltételek fennállnak:
(1')ha $x, y, z \in R$ és $x < y$, akkor $x + z < y + z$ (az összeadás szigorúan monoton);
(2')ha $x, y \in R$ és $x, y > 0$, akkor $xy > 0$ (a szorzás szigorúan monoton).

Bizonyítás

Ha a definícióból (1) teljesül, $x < y$, akkor $x \leq y$ és így $x + z \leq y + z$.
Egyenlőség nem teljesülhet,
mert akkor $x = x + z - z = y + z - z = y$ következne, így kapjuk (1')-t.
(1')-ből nyilván következik (1), mert az egyenlőség esete triviális.

Ha a definícióból (2) teljesül és $x, y > 0$, akkor $x, y \geq 0$, így $xy \geq 0$.
Ha $xy = 0$ lenne,
akkor x és y egy nullosztópár lenne, ami lehetetlen, így kapjuk (2')-t.
(2')-ből nyilván következik (2), mert gyűrűben $x0 = 0y = 0$.

Ferdetest, test, rendezett test

Ferdetest

Egy F gyűrűt *ferdetest*nek nevezünk, ha a nullelemet 0-val jelölve $F \setminus \{0\}$ a szorzással csoport.

A szorzás egységelemét rendszerint 1-el jelöljük.

Test

Ha a szorzás kommutatív, akkor a ferdetestet testnek nevezzük.

-Minden test egységelemes integritási tartomány.

-A legegyszerűbb példa testre a *kételemű test*: $\{0, 1\}$. Egy másik példa $\mathbb{Q}$.

Rendezett test

Egy testet *rendezett test*nek nevezünk, ha test és rendezett integritási tartomány.

Az előző tétel szerint $\mathbb{Q}$ rendezett test.

Megjegyezzük, hogy a kételemű testen nincs olyan rendezés, amellyel rendezett test,
mert rendezett testben $1 > 0$ és $-1 < 0$, de a kételemű testben $-1 = 1$.

Példák

További példák testre a valós illetve a komplex számok, a modulo p maradékosztályok, ha p prímszám,
ferdetestre pedig a kvaterniók, mint azt később látni fogjuk.
Ezek közül a valós számok rendezett testet alkotnak.

(1) Egy tetszőleges X halmazt egy R gyűrűbe képező összes függvények R^X halmaza a pontonkénti összeadással és szorzással gyűrű.

Ha R kommutatív, akkor ez a gyűrű is kommutatív, ha R egységelemes, akkor az R^X gyűrű is egységelemes,
de ha R is és X is legalább kételemű, akkor R^X nem test, és nem nullosztómentes,
még akkor sem, ha R test illetve ha R nullosztómentes.

(2) Egy tetszőleges A Abel-csoport endomorfizmusai gyűrűt alkotnak a pontonkénti összeadással és a függvények kompozíciójával, mint szorzással.
Ezt a gyűrűt A *endomorfizmusgyűrű*jének nevezzük.

Homomorfizmusok

Homomorfizmus

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

Monomorfizmus

Ha a φ homomorfizmus kölcsönösen egyértelmű *injektív*, akkor *monomorfizmus*nak,

Epimorfizmus

ha pedig R'-re képez *szürjektív*, akkor egy R'-re való *epimorfizmus*nak nevezzük.

Izomorfizmus

Ha φ kölcsönösen egyértelmű és R'-re képez *bijektív*, akkor azt mondjuk, hogy φ *izomorfizmus* R és R' között.
Ha R és R' között létezik *izomorfizmus*, akkor azt mondjuk, hogy *izomorfak*;
ilyenkor algebrai szempontból nem lehet különbséget tenni közöttük.

Endomorfizmus, automorfizmus

Ha $R' = R$ ugyanazokkal a műveletekkel,
akkor a *homomorfizmusokat* *endomorfizmus*oknak,
az *izomorfizmusokat* pedig *automorfizmus*oknak is nevezzük.

Hasonlóan, mint a csoportoknál, adódik, hogy

Állítás

-homomorfizmusok összetétele is homomorfizmus,
-izomorfizmusok összetétele izomorfizmus,
-izomorfizmus inverze is izomorfizmus és
-$\mathbb{I}_R$ automorfizmus.

Példa

A komplex konjugálás a komplex számok testének automorfizmusa.

Tétel

Gyűrű homomorf képe is gyűrű.

Bizonyítás

A csoportoknál tanultak alapján csak a disztributivitást kell belátni.
Jelölje x képét x'.
A homomorf kép tetszőleges három elemét felírhatjuk a', b', c' alakban.
így $a'(b'+c') = a'(b+c)' = \big(a(b+c)\big)' = (ab+bc)'$

Bizonyítás folytatása

$= (ab)' + (ac)' = a'b' + a'c'$ és hasonlóan
$(b' + c')a' = b'a' + c'a'$.

Reprezentációk

Reprezentáció

Egy R gyűrűnek egy A Abel-csoport endomorfizmusgyűrűjébe való homomorfizmusát R *reprezentációjának* nevezzük.

Hű reprezentáció

Ha a leképezés monomorfizmus, akkor *hű reprezentációról* beszélünk.

Egy egységelemes gyűrűnek mint egységelemes félcsoportnak a reguláris reprezentációja a gyűrű
reguláris reprezentációja;
mint tudjuk ez hű reprezentáció.

Ugy a gyűrűknél, mint a testeknél fontos jellemző az elemek additív rendje,
amely megfelelő feltétel teljesülése esetén minden nem nulla elemre megegyezik.

Tétel

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

Bizonyítás

Ha egy nullosztómentes R gyűrűben egy nem nulla a elem addítív rendje $n \in \mathbb{N}^+$, és b tetszőleges nem nulla elem,
akkor $n(ab) = (na)b = 0b = 0$, másrészt pedig
$n(ab) = a(nb)$, így $nb = 0$ kell legyen,
azaz b rendje is véges, és legfejebb annyi, mint a rendje.
Mivel a és b szerepe felcserélhető, minden nem nulla elemnek ugyanannyi az additív rendje.
Megmutatjuk, hogy ez a közös rend ha nem végtelen, akkor csak prímszám lehet.

Bizonyítás folytatása

Ugyanis, ha n a nem nulla a elem additív rendje, akkor $n > 1$ és ha $n = km$, akkor $0 = na = k(ma)$.
Ha $m < n$, akkor $ma \neq 0$, tehát $k = n$, mert egyébként ma additív rendje kisebb lenne, mint n.

Gyűrű karakterisztikája

Az előző tétel szerint nulloszómentes gyűrűben a nem nulla elemek additív rendje megegyezik.

Ha ez a közös érték *végtelen*, akkor azt mondjuk, hogy a *gyűrű karakterisztikája nulla*,
ha pedig egy *véges n érték*, akkor azt mondjuk, hogy a *gyűrű karakterisztikája n.*
Jelölése: $\mathrm{chara}(R)$.

Hasznos észrevétel, hogy ha $n = \text{char}(R) > 0$, akkor bármely $a, b \in R$ esetén

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = a^n + b^n$$

mert, n prím és $0 < k < n$ esetén a binomiális együttható osztható n-nel.
Igy $x \longrightarrow x^n$ és innen indukcióval minden $k \in \mathbb{N}^+$-ra $x \longrightarrow x^{n^k}$ is automorfizmus.

Részgyűrű, ideál

Legyen R egy halmaz a $(+, \cdot)$ binér művelettel.

Egy R gyűrű egy S részhalmazát *részgyűrű*nek, illetve *résztestnek* nevezzük,
ha maga is gyűrű, illetve test az adott műveletekkel.

Részgyűrű

Vizsgáljuk azt az esetet, amikor R maga is gyűrű.

A részcsoportoknál tanultak szerint egy $S \neq \emptyset$ részhalmaza R-nek pontosan akkor részgyűrű, ha
$a, b \in R$ esetén $a - b \in S$ és $ab \in S$.

Ezek a feltételek úgy is írhatók, hogy $S - S \subset S$ illetve $SS \subset S$.

A részgyűrű fogalma a részcsoport fogalmával analóg: olyan additív részcsoport amelyből a szorzás nem vezet ki.

Azt a szerepet, amelyet csoportoknál a normálosztók játszottak, a gyűrűk esetében az ideálok játszák.

Ideál

Az I részgyűrűt *jobbideál*nak illetve *balideál*nak nevezzük, ha $a \in I$ és $r \in R$ esetén $ar \in I$ illetve $ra \in I$. Ha I egyszerre balideál és jobbideál is, akkor *ideál*nak nevezzük.

Ideál folytatśa

Az I jobbideál illetve balideál, azzal ekvivalens hogy $I - I \subset I$ és $IR \subset I$ illetve hogy $I - I \subset I$ és $RI \subset I$.
Igy az hogy I ideál, azzal ekvivalens, hogy $I - I \subset I$, $IR \subset I$ és $RI \subset I$.

-Innen azonnal következik, hogy akárhány jobbideál, balideál illetve ideál metszete ismét jobbideál, balideál illetve ideál.

Triviális ideálok

Az egész R és a csak a nullelemet tartalmazó egyelemű részhalmaz ideálok, ezek a *triviális ideál*ok.

Egyszerű gyűrű

Ha egy gyűrűben ezeken kívül nincs más ideál,
akkor *egyszerű gyűrű*nek nevezzük.

Valódi ideál

Az R-től különböző idálokat *valódi ideál*nak nevezzük.

Kommutatív gyűrűben a jobbideál és a balideál fogalma egybeesik az ideál fogalmával.

Generált ideál

Egy $A \subset R$ részhalmaz által *generált ideál*on az összes, az A-t tartalmazó ideálok metszetét érjük.
Jelölése: (A).

Tudjuk, hogy (A) ideál; ez a legszűkebb ideál, amely tartalmazza A-t.

Főideál

Ha egy I ideált egyetlen $a \in R$ generál, azaz $I = (a)$, akkor *főideál*nak nevezzük.

(Hasonlóan definiálható az A által generált jobbideál illetve balideál is.)

Példák

(1) Az $\mathbb{R}^{\mathbb{R}}$ függvénygyűrűben részgyűrűt alkotnak például a korlátos függvények, a folytonos függvények, a korlátos folytonos függvények, a polinomfüggvények, stb.

(2) Egy X lineáris tér önmagába való lineáris leképezései a pontonkénti összeadással és a függvényösszetétellel mint szorzással X (mint Abel-csoport) endomorfizmusgyűrűjének egy részgyűrűjét alkotják.

(3) Ha az előző pontban szereplő X lineáris tér n dimenziós, akkor az önmagába való lineáris leképezéseinek az előző pontban megadott gyűrűje izomorf az $n \times n$-es mátrixoknak a mátrixok összeadásával és szorzásával tekintett gyűrűjével.

(4) Az egész számok gyűrűjében egy m egész szám többszörösei ideált alkotnak. Ez nyilván főideál, m generálja.

(5) A $\mathbb{Q} \times \{0\}$ halmaz ideál $\mathbb{Q} \times \mathbb{Q}$-ban.

Következmény

Egy R gyűrűnek egy I ideál szerinti mellékosztályai a összeadásra és a szorzásra nézve gyűrűt alkotnak.

Bizonyítás

Ha $\sim$ a megfelelő ekvivalenciareláció, akkor $x \longrightarrow \tilde{x}$ mindkét műveletre nézve művelettartó.

Faktorgyűrű

Az előző következményben szereplő gyűrűt az R gyűrű I ideál szerinti *maradékosztálygyűrű*jének (vagy *faktorgyűrű*jének illetve *hányadosgyűrű*jének) nevezzük és R/I-vel jelöljük.

Példa

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

Megjegyzés

Az előző tétel (1) öszefüggésében egyenlőség általában nem teljesül, tehát a maradékosztályok szorzása nem biztos, hogy megegyezik a komplexusszorzással.

Például

ha $R = \mathbb{Z}$, $I = 8\mathbb{Z}$, $a = b = 4$, akkor

$(I + a)(I + b) = (8\mathbb{Z} + 4)(8\mathbb{Z} + 4) = 64\mathbb{Z} + 32\mathbb{Z} + 32\mathbb{Z} + 16 =$

$64\mathbb{Z} + 32\mathbb{Z} + 16 \subset 16\mathbb{Z}$,

ami csupa 16-tal osztható számot tartalmaz,

viszont $8\mathbb{Z} + 16$ minden 8-cal oszthatót, tehát kapjuk, hogy

$$(8\mathbb{Z} + 4)(8\mathbb{Z} + 4) \subset 16\mathbb{Z} \subset 8\mathbb{Z} + 16 \quad (\neq 8\mathbb{Z} + 16).$$

Homomorfizmus magja

Egy R gyűrűnek egy R' gyűrűbe való φ homomorfizmusánál a *homomorfizmus magján* az R' gyűrű nullelemének a teljes inverz képét értjük.

A φ magját $\ker(\varphi)$-vel jelöljük.

Homomorfizmustétel

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

Bizonyítás

Azt, hogy a $\varphi^{-1}(a')$, $a' \in R'$ halmazrendszer az R egy, az összedással kompatibilis osztályozása, tudjuk a csoportelméletből.
Ha $a', b' \in R'$, akkor a $\varphi^{-1}(a')$ bármely a elemére és a $\varphi^{-1}(b')$ bármely b elemére
$\varphi(ab) = \varphi(a)\varphi(b) = a'b'$, azaz $ab \in \varphi^{-1}(a'b')$, így az osztályozás a szorzással is kompatibilis.
Tehát ez az osztályozás egy I ideál szerinti osztályozás.
Az ideál a nulla teljes inverz képe.

Bizonyítás folytatása

Az $a' \mapsto \varphi^{-1}(a')$ leképezés izomorfizmusa R'-nek $R/\ker(\varphi)$-re. A tétel második fele az előző tétel következményének bizonyítása alapján nyilvánvaló.

Példa

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

Tetszőleges R gyűrűre $R/\{0\}$ izomorf R-el, R/R pedig nullgyűrű.

Direkt szorzat

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

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

Descartes-szorzat folytatása

Descartes-szorzatot ellátva az $(a+b)_i = a_i + b_i$, ha $i \in I$ és $(ab)_i = a_i b_i$, ha $i \in I$ összefüggéssel definiált műveletekkel a G-t a G_i, $i \in I$ család *direkt szorzat*ának nevezzük.

A direkt szorzat a hatványozás általánosítása.

A legfontosabb speciális eset, amikor $I = \{1, 2, \ldots, n\}$, ekkor a direkt szorzat elemei $a = (a_1, a_2, \ldots, a_n)$, $a_i \in G_i$, ha $i \in I$ alakú n-esek.

Mivel az összeadás és a szorzás definíció szerint koordinátánként történik,
ha $b = (b_1, b_2, \ldots, b_n)$ egy másik eleme a direkt szorzatnak, akkor
$a + b = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ és
$ab = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$.

-Ha minden G_i gyűrű, akkor G is,
-ha minden G_i kommutatív, akkor G is,
-ha minden G_i egységelemes, akkor G is,
de sohasem test, még csak nem is nullosztómentes, ha I legalább két elemű.

Ha $J \subset I$, akkor az $a \longrightarrow a|_J$ projekció homomorfizmus,
képe $\times_{i \in J} G_i$, magja pedig izomorf $\times_{i \in I \setminus J} G_i$-vel.

Példa

Ha az $n, m \in \mathbb{N}^+$ számok relatív prímek,
akkor a kínai maradéktételből kapjuk, hogy
$\mathbb{Z}_m \times \mathbb{Z}_n$ gyűrű izomorf a $\mathbb{Z}_{mn}$ gyűrűvel.

Speciálisan a modulo n redukált maradékosztályok multiplikatív csoportját $\mathbb{Z}_n^*$-nel jelölve,
$\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ izomorf $\mathbb{Z}_{nm}^*$-nel.

Egyébként mivel $\mathbb{Z}_n^*$ rendje $\varphi(n)$,
minden elemének rendje osztja $\varphi(n)$-et,
azaz bármely $a \in \mathbb{Z}_n^*$-re $a^{\varphi(n)}$ a $\mathbb{Z}_n^*$ egységeleme;ez Euler tétele.

Tétel

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

Bizonyítás

A jobb oldalon álló halmaz tartalmazza a-t és
elemei közül nyilván nem vezet ki a kivonás és az R elemeivel való szorzás, így (a) része a jobb oldali halmaznak.

Másrészt, ha a benne van egy I ideálban, akkor minden $ar = ra$, $r \in R$ alakú eleme is.

Következmény

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

Gauss-gyűrűk

-Központi szerepet játszik az egyértelmű faktorizáció irreducibilis elemekre.

Gauss-gyűrű

Egy R egységelemes integritási tartományt *Gauss-gyűrű*nek (vagy *egyértelmű faktorizációs tartomány*nak) nevezünk,
ha minden nullától és egységtől különböző elem sorrendtől és egységektől eltekintve egyértelműen felírható irreducibilis elemek (véges) szorzataként.

Azaz ha a nem nulla és nem egység,
akkor felírható $a = p_1 p_2 \cdots p_n$ alakban, ahol $p_1, p_2, \ldots, p_n$ (nem feltétlenül különböző) irreducibilis elemek,
és ha $a = q_1 q_2 \cdots q_m$ egy másik előállítás irreducibilis elemek szorzataként,
akkor $m = n$ és van olyan $\sigma \in S_n$ permutáció, hogy q_{σ_i} és p_i asszociáltak, ha $i = 1, 2, \ldots, n$.

Az előállítás felírható

$$a = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

alakban is,
ahol ε egység,
$p_1, p_2, \ldots, p_k$ páronként nem asszociált irreducibilis elemek,
a kitevők pedig $\mathbb{N}^+$ (vagy $\mathbb{N}$) elemei.

(Ebbe az alakba az egységek is beleférnek, ha $k = 0$.)

A felbontásból leolvashatók a osztói, ezek

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

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

Ha több elemünk van, és mindnek adott az irreducibilis tényezőkre való felbontása,
akkor közös osztóik, valamint hasonlóan közös többszöröseik is leolvashatók,
és látjuk, hogy létezik legnagyobb közös osztó és legkisebb közös többszörös.

Állítás

Egy Gauss-gyűrűben minden irreducibilis elem prím,

Bizonyítás

Ha a nullától és egységtől különböző p irreducibilis elemre $p|ab$,
akkor vagy $ab = 0$, amiből valamelyik nulla, vagy pedig $ab = pd$
valamely $d \neq 0$ elemre,
amiből d-t felírva (1) alakban, az ab egy olyan előállítását kapjuk irreducibilis elemek szorzataként, amelyben szerepel p.
Ha most felírjuk az a és a b felbontását (1) alakban,
valamelyikben szerepelnie kell p-nek,
mert egyébként ab faktorizációja nem lenne egyértelmű.

Példa

Vannak olyan egységelemes integritási tartományok, amelyek nem Gauss-gyűrűk.

Könnyű látni, hogy az $R = \mathbb{Z} + i\sqrt{5}\mathbb{Z} \subset \mathbb{C}$ halmaz részgyűrűje $\mathbb{C}$-nek.

Minden $c = a + i\sqrt{5}b \in R$, $a, b \in \mathbb{Z}$-re $|c|^2 = a^2 + 5b^2$ természetes szám, és kongruens $0, 1, 4 \pmod 5$.

Mivel $d|c$ esetén az abszolút érték multiplikativitása miatt nyilván $|d|^2 \big| |c|^2$, és az 1 egységelemre $|1|^2 = 1$, az egységek ± 1.

A $9 = 3 \cdot 3 = (2 + \sqrt{5}i)(2 - \sqrt{5}i)$ felbontásokban $|3|^2 = 9$, aminek nincs olyan nem triviális osztója, amelyre 5-tel osztva $0, 1, 4$ maradékot ad.

Hasonlóan $|2 \pm \sqrt{5}i|^2 = 9$, így 3, $2 + \sqrt{5}i$ és $2 - \sqrt{5}i$ irreducibilisek R-ben és nem prímek, valamnt az irreducibilis elemekre bontás nem egyérttelmű.

Euklideszi gyűrűk

A legegyszerűbb gyűrűk, amelyekről be fogjuk látni, hogy -Gauss-gyűrűk, az euklideszi gyűrűk.

Euklideszi gyűrű

Egy R egységelemes integritási tartományt *euklideszi gyűrű*nek nevezünk, ha a nem nulla elemein értelmezve van egy $\mathbb{N}$-beli értékű φ függvény úgy, hogy
(1)ha $a, b \in R$, $b \neq 0$, akkor van olyan $q, r \in R$, hogy $a = bq + r$ és $r = 0$ vagy $r \neq 0$ és $\varphi(r) < \varphi(b)$;
(2)$\max\{\varphi(a), \varphi(b)\} \leq \varphi(ab)$ minden $a, b \in R$, $a \neq 0$, $b \neq 0$ esetén.

(Tulajdonképpen az (R, φ) párt kellene euklideszi gyűrűnek neveznünk.)

Megfigyelhetjük, hogy φ az egész számok esetén az abszolút érték által játszott szerepet általánosítja:
$\mathbb{Z}$ az $n \to |n|$ függvénnyel nyilván euklideszi gyűrű.

Mint ez a példa is mutatja, hogy
a definícióban szereplő r általában nem egyértelmű:
itt például lehet a legkisebb nemnegatív maradék, a legkisebb abszolut értékű maradék, stb.

A legfontosabb a test feletti egyhatározatlanú polinomok gyűrűje, ezzel részletesen foglalkozni fogunk.

Állítás

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

Az nem igaz, hogy ha $\varphi(b) = \varphi(a)$, akkor a és b asszociáltak.

Bizonyítás

Ha $\varphi(\varepsilon)$ minimális, akkor az e egységelemet osztva ε-nal, az r maradék csak nulla lehet, így ε egység.
Ha $b|a$, akkor a (2) tulajdonság miatt $\varphi(b) \leq \varphi(a)$.

Bizonyítás folytatása

Ha ε egység, $a \in R$ pedig olyan elem, amelyre $\varphi(a)$ minimális, akkor $\varepsilon | a$ miatt $\varphi(\varepsilon)$ is minimális.

Ha a és b asszociáltak,
akkor $\varphi(a) \leq \varphi(b)$ és fordítva is.

Végül tegyük fel, hogy $b|a$ és $\varphi(a) = \varphi(b)$.

Felírva a-t $bq + r$ alakban, meg kell mutatnunk, hogy $r \neq 0$ lehetetlen.

Mivel $r = b - aq = b + bc(-q) = b(e - cq)$, azt kapnánk, hogy $\varphi(r) \geq \varphi(b)$, ami ellentmondás.

Példa: *Gauss-egészek*
A komplex síkbeli egységnégyzetrács elemei, azaz a
$G = \mathbb{Z} + i\mathbb{Z} = \{n + im : n, m \in m\mathbb{Z}\} \subset \mathbb{C}$
úgynevezett *Gauss-egészek* euklideszi gyűrűt alkotnak a
$\varphi(n + im) = |n + im|^2 = n^2 + m^2$ függvénnyel.

Az, hogy (2) fennáll, következik a komplex abszolút érték multiplikativitásából.

A másik tulajdonság belátásához jelölje q a G halmaz a/b-hez legközelebbi (egyik) elemét.

Ekkor $\left|a/b - q\right|^2 < 1$, mivel az abszolút érték legfeljebb $\sqrt{1/2}$.

Innen $|b|^2|a/b - q|^2 < |b|^2$, azaz $|a - bq|^2 < |b|^2$, tehát (1) teljesül.

Az egységek nyilván ± 1 és $\pm i$.

Bővített euklidesz algoritmus

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

(1)[Inicializálás.] Legyen $x_0 \leftarrow e$, a gyűrű egységeleme,
$y_0 \leftarrow 0$, $r_0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow e$, $r_1 \leftarrow b$, $n \leftarrow 0$.

(2)[Vége?] Ha $r_{n+1} = 0$,
akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ért.

(3)[Ciklus.] Legyen $r_n = q_{n+1} r_{n+1} + r_{n+2}$,
ahol $r_{n+2} = 0$ vagy $\varphi(r_{n+2}) < \varphi(r_{n+1})$,
legyen $x_{n+2} \leftarrow x_n - q_{n+1} x_{n+1}$,
$y_{n+2} \leftarrow y_n - q_{n+1} y_{n+1}$, $n \leftarrow n + 1$ *és menjünk (2)-re.*

Bizonyítás

Mivel a $\varphi(r_1), \varphi(r_2), \ldots$ természetes számok szigorúan monoton csökkenő sorozata,
az eljárás véget ér, mert egyébként $\mathbb{N}$ nem lenne jólrendezett.

Teljes indukcióval $ax_n + by_n = r_n$, így $d = ax + by$.

Innen a és b közös osztói mind osztói d-nek.

Mivel $r_{n+1} = 0$, vagy $n = 0$,
ekkor $d = a$ és $b = 0$, vagy pedig $n > 0$, és
$r_0, r_1, \ldots, r_{n-1}$ mind többszörösei r_n-nek,
mert $r_{n-1} = q_n r_n$, $r_{n-2} = q_{n-1} r_{n-1} + r_n$, és így tovább,

speciálisan $a = r_0$ és $b = r_1$ többszörösei d-nek,
tehát d legnagyobb közös osztó.

Tétel

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

Bizonyítás

Az egyik irányt már láttuk.

Tegyük fel, hogy p felbonthatatlan, és legyen $p|ab$.

Tegyük fel, hogy $p \not| a$.

Ekkor p és a legnagyobb közös osztói az egységek.

A bővített euklideszi algoritmussal kaphatunk olyan x, y elemeket, hogy $px + ay = \varepsilon$, egy egység.

Szorozva b-vel és ε multiplikatív inverzével,
$pbx\varepsilon^{-1} + aby\varepsilon^{-1} = b$.

Mivel p osztója a bal oldalnak, a jobb oldalnak is.

Tétel

Euklideszi gyűrűben minden nem nulla és nem egység elem sorrendtől és asszociáltságtól eltekintve egyértelműen felírható prímelemek szorzataként.
Azaz euklideszi gyűrű Gauss-gyűrű.

Bizonyítás

Először a felbontás létezését bizonyítjuk.

Ha az adott a elem nem irreducibilis, akkor felírható két olyan, mondjuk b és c elem szorzataként, amelyekre $\max\{\varphi(b), \varphi(c)\} < \varphi(a)$.

Indukcióval folytatjuk ezt az eljárást:
ha a kapott szorzatnak van nem irreducibilis tényezője, akkor a nem irreducibilis tényezők közül kiválasztva egy olyat, amelyre φ maximális, azt helyettesítsük két tényező szorzatával.

Minden lépésben vagy a maximális φ érték csökken, vagy azon tényezők száma, amelyekre a maximális φ érték vétetik fel, ha több ilyen volt.

Bizonyítás folytatása

Az eljárás a természetes számok jólrendezettsége miatt véges sok lépésben
csupa irreducibilis tényezőből álló felbontáshoz vezet.

A felbontás egyértelműségének bizonyításához,
tegyük fel, hogy van olyan a, amely két lényegesen különböző módon bontható fel,
és legyen a olyan ezek közül, amelyre $\varphi(a)$ minimális:

$$a = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k .$$

Mivel $p_1 | a$, azaz $p_1 | q_1 q_2 \cdots q_k$, van olyan i, hogy $p_1 | q_i$.
Ekkor viszont p_1 és q_i asszociáltak,
mert q_i irreducibilis.

Egyszerűsítve a közös tényezővel egy olyan a' elemet kapunk,
amelyre $\varphi(a') < \varphi(a)$ és felbontása nem egyértelmű.

Tétel

Euklideszi gyűrűben minden ideál főideál.

Bizonyítás*

Legyen R euklideszi gyűrű I pedig egy ideálja.

Ha $I = \{0\}$, akkor $I = (0)$.

Egyébként legyen a az I egy olyan eleme, amelyre $\varphi(a)$ minimális.

Mivel nyilván $(a) \subset I$,
csak a fordított tartalmazást kell megmutatni.

Ha valamely $b \in I$ nem lenne többszöröse a-nak, akkor maradékos osztással egy olyan $r \in I$ elemet kapnánk, amelyre $\varphi(r) < \varphi(a)$.

Definíció

Egy R gyűrű egy I valódi ideálját *maximális ideál*nak nevezzük, ha nincs nála bővebb valódi ideál, amely tartalmazza, azaz ha a valódi ideálok között a tartalmazásra nézve maximális.

Következmény

Egy euklideszi gyűrű egy nem triviális ideálja pontosan akkor maximális,
ha egy irreducibilis elem generálja.

Bizonyítás*

Ha $I = (a)$ maximális, akkor a nem nulla és nem egység,
valamint nem lehet egy b nem triviális osztója,
mert erre $(a) \subsetneq (b) \subsetneq R$ teljesülne.

Megfordítva, ha a irreducibilis,
akkor $(0) \subsetneq (a) \subsetneq R$ és ha egy I ideálra $(a) \subsetneq I \subsetneq R$,
akkor annak b generátorára $b|a$, de b nem egység és nem is asszociáltja a-nak, ami lehetetlen.

Tétel

Legyen R kommutatív egységelemes gyűrű, I az R egy ideálja.
Az R/I faktorgyűrű akkor és csak akkor test, ha I maximális ideál.

Bizonyítás*

Először tegyük fel, hogy I maximális ideál, és
tekintsük R/I egy nem nulla $I + a$ elemét.

Az $S = \{x + ay : x \in I, y \in R\}$ halmaz nyilván ideál.

Mivel I valódi része S-nek, $S = R$,
így alkalmas $x \in I$-re és $y \in R$-re $e = x + ay$.

Ez azt jelenti, hogy
$\tilde{e} = I + e = I + x + ay = I + ay \supset (I + a)(I + y)$, azaz y osztálya R/I-ben a osztályának inverze.

Megfordítva, tegyük fel, hogy R/I test, S pedig olyan ideál, amely valódi módon tartalmazza I-t, azaz létezik olyan a, amelyre $a \in S$ de $a \notin I$.

Bizonyítás folytatása*

Mivel R/I test, az $\tilde{a}\tilde{x} = \tilde{b}$ egyenlet bármely $b \in R$-re megoldható, azaz van olyan $x \in R$, hogy $I + ax = I + b$.

De $I + ax \subset S$, így $b \in S$.

Mivel b tetszőleges, $S = R$.

Definíció

Egy R gyűrű egy I ideálját *prímideál*nak nevezzük, ha $ab \in I$ esetén $a \in I$ vagy $b \in I$.
Euklideszi gyűrűben ez azt jelenti, hogy az ideál generátorai prímelemek.

Tétel

Legyen R kommutatív egységelemes gyűrű, I az R egy ideálja. Az R/I faktorgyűrű akkor és csak akkor integritási tartomány, ha I az R egy valódi prímideálja.

Bizonyítás*

Maradékosztályokra áttérve, az hogy I prímideál, azzal ekvivalens, hogy
$\tilde{a}\tilde{b} = \tilde{0}$ esetén $\tilde{a} = \tilde{0}$ vagy $\tilde{b} = \tilde{0}$, amiből következik az állítás;

az $I \neq R$ feltétel azt zárja ki, hogy R/I zérógyűrű legyen.

Következmény

Kommutatív egységelemes gyűrűben minden maximális ideál prímideál.

Bizonyítás*

Test integritási tartomány is.

Tétel

Egy kommutatív egységelemes egyszerű gyűrű akkor és csak akkor test, ha nem nullgyűrű.

Bizonyítás

Ha van olyan $a \neq 0$ elem, amely nem invertálható,
akkor az $(a) = aR$ főideál nem tartalmazza az egységelemet,
így R-nek van nem triviális ideálja.

Megfordítva, ha R test, $I \neq \{0\}$ egy ideál, $a \in I$, $a \neq 0$,
akkor bármely $b \in R$-re $b = aa^{-1}b \in I$, tehát $I = R$.

Hányadostest

Legyen R a nullgyűrűtől különböző integritási tartomány.

Az $R \times R \setminus \{0\}$ halmazon vezessük be az $(a, b) \sim (a', b')$,
ha $ab' = a'b$ ekvivalenciarelációt,
az $(a, b) + (a', b') = (ab' + a'b, bb')$ összeadást
és az $(a, b)(a', b') = (aa', bb')$ szorzást.

Belátható, hogy a műveletek kompatibilisek az
ekvivalenciarelációval és
az ekvivalenciaosztályok testet alkotnak,
amelyet az R *hányadostest*ének nevezünk.

Bizonyítás

$\sim$ reflexív és szimmetrikus.

Ha $(a, b) \sim (a', b')$ és $(a', b') \sim (a'', b'')$,
akkor $ab' = ba'$ és $a'b'' = b'a''$.

A két összefüggést összeszorozva $aa'b'b'' = ba'b'a''$.

Ha $a' \neq 0$, akkor $a'b' \neq 0$, így egyszerüsítve azt kapjuk,
hogy $ab'' = ba''$, azaz $(a, b) \sim (a'', b'')$.

Ha $a' = 0$, akkor $b' \neq 0$ miatt $a = 0$ és $a'' = 0$,
és ekkor is $(a, b) \sim (a'', b'')$.

Az összeadás kompatibilis az ekvivalenciarelációval,
mert ha $(a, b) \sim (a', b')$,
akkor $ab' = ba'$, amiből $ab'b''b'' = ba'b''b''$,
innen viszont

$$(ab'' + ba'')b'b'' = ab'b''b'' + bb'a''b'' = ba'b''b'' + bb'a''b'' =$$

$$= (a'b'' + b'a'')bb''$$

Bizonyítás folytatása

tehát

$$(a,b)+(a'',b'')=(ab''+ba'',bb')\sim(a'b''+b'a'',b'b'')=$$

$$=(a',b')+(a'',b'')$$

és a párok összeadása triviálisan kommutatív, így elég ezt belátni.

Mivel a párok összeadása könnyen kiszámolhatóan aszszociatív is, az ekvivalenciaosztályok összeadása is kommutatív és asszociatív.

A $(0,b)$ alakú párok halmaza nullelem, ezt jelöljük nullával.

Az (a,b) párosztályának additív inverze a $(-a,b)$ pár osztálya.

Igy $R\times(R\setminus\{0\})$ ekvivalenciaosztályainak halmaza az összeadással Abel-csoport.

A szorzás is kompatibilis az osztályozással, mert ha $(a,b)\sim(a',b')$, akkor $ab'=ba'$, amiből $aa''b'b''=ba'a''b''$, így

$$(a,b)(a'',b'')=(aa'',bb'')\sim(a'a'',b'b'')=(a',b')(a'',b'').$$

Bizonyítás folytatása

Mivel a párok szorzása láthatóan kommutatív, beláttuk a szorzás kompatibilitását az osztályozással.

Mivel a párok szorzása asszociatív is, az osztályoké is asszociatív.

Egyszerű számolás mutatja, hogy
$(a, b)((a'b') + (a''b''))$ és $(a, b)(a'b') + (a, b)(a''b'')$ ekvivalens párok, így az osztályok szorzása disztributív.

Ezzel beláttuk, hogy $R \times (R \setminus \{0\})$ ekvivalenciaosztályainak halmaza kommutatív gyűrű.

A (b, b) alakú párok halmaza a multiplikatív egységelem az osztályok halmazában.

Ha $(a, b) \not\sim (0, b')$, akkor $a \neq 0$,
ekkor viszont az (a, b) pár osztályának multiplikatív inverze a (b, a) pár osztálya.

Ezzel a bizonyítást befejeztük.

Következmény

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

Algebrai struktúrák

Nem csak egy vagy két műveletet tekinthetünk egy halmazon, hanem tetszőlegesen sokat, és ezek nem csak nullér, unér és binér műveletek lehetnek,
hanem akárhány változósak.
Igy az algebrai struktúra általános fogalmához jutunk.
Számos fogalom és konstrukció (részstruktúra, faktorstruktúra, direkt szorzat, stb.)
átvihető tetszőleges algebrai struktúrákra is,
de ezzel itt nem foglalkozunk.

Polinomok

Legyen R gyűrű.

Az *(egyhatározatlanú) polinomokról* eddigi ismereteink szerint $\sum_{i=0}^{n} f_i x^i$ alakú véges összegek, ahol x a „*határozatlan*”, $n \in \mathbb{N}$, $f_i \in R$, ha $0 \leq i \leq n$, az összeadás és szorzás pedig tagonként történik.

Definíció pontossá tehető:

Ha $f = (f_0, f_1, \dots)$ és $g = (g_0, g_1, \dots)$ is R-beli sorozatok végtelen sorozatok, azaz $R^{\mathbb{N}}$ elemei,

akkor összegüket az $f + g = (f_0 + g_0, f_1 + g_1, \dots)$ sorozatként, szorzatukat pedig azon $h = (h_0, h_1, \dots)$ sorozatként definiálva, amelyre

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

egy gyűrűt kapunk.

-Ha R kommutatív, akkor ez a gyűrű is kommutatív.
-Ha R egységelemes 1 egységelemmel, akkor a sorozatok gyűrűje is az, benne az $(1, 0, 0, \dots)$ sorozat egységelem.

-Ha az R gyűrű nullosztómentes, akkor a sorozatok gyűrűje is, mivel ha m illetve n a legkisebb index, amelyre $f_m \neq 0$ illetve $g_n \neq 0$, akkor $h_{m+n} = f_m g_n \neq 0$.

Egyhatározatlanú polinomok

Az R feletti *egyhatározatlanú polinomokon* olyan R-beli $f = (f_0, f_1, \dots)$ sorozatokat értünk,
amelyeknek csak véges sok tagja nem nulla, a fenti műveletekkel.

Ha $i > m$ esetén $f_i = 0$ és $j > n$ esetén $g_j = 0$,
akkor $k > m + n$ esetén a $h_k = \sum_{i+j=k} f_i g_j$ összegnek minden tagja nulla,
így polinomok szorzata polinom és polinomok összege is polinom,
azaz a polinomok a fenti gyűrűnek részgyűrűjét alkotják.

Konstans polinomok

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

A $f = (f_0, f_1, \dots, f_n, 0, 0, \dots)$ polinom jelölésére a
$f = f_0 x^0 + f_1 x^1 + f_2 x^2 + \cdots + f_n x^n$ alakot fogjuk használni.

Ez a jelölés emlékeztet arra, hogy a műveleteket hogyan kell elvégezni.

Általában x^0-at nem írjuk ki, x^1 helyett pedig x-et írunk,
így az $f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n$ alakot kapjuk.

Az f_i neve az *i-ed fokú tag együtthatója*.

A nullad fokú tag együtthatója a polinom *konstans tagja*.

Az $f = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n$ felírásból a nulla együtthatójú tagokat szokás elhagyni
illetve a felíráshoz további nulla együtthatójú tagok adhatók hozzá,
így a felírás nem egyértelmű.

Egyértelművé válik azonban,
ha kikötjük, hogy $f_n \neq 0$ legyen és
minden n-nél alacsonyabb fokú tag is szerepeljen.

Ekkor f_n a polinom *főegyütthatója*, n pedig a polinom*foka*,
jelölése: $\deg(f)$.

(Egy másik lehetőség a felírás egyértelművé tételére, hogy
minden nulla együtthatójú tagot elhagyunk.)

A nulla polinom egyértelmű felírása az üres összeg,
nincs főegyütthatója és fokát $-\infty$-nek definiáljuk.

A konstans polinomok a legfeljebb nulladfokú polinomok.

A legfeljebb elsőfokú polinomok a *lineáris polinom*ok.

Monom

Azokat a polinomokat, amelyek $f_i x^i$ alakba írhatók, *monom*oknak nevezzük.

Az R feletti egyhatározatlanú polinomok gyűrűjét $R[x]$-el jelöljük.

Néha egy $f \in R[x]$ polinomra inkább az $f(x)$ jelölést fogjuk használni.

Ha R egységelemes 1 egységelemmel, akkor az $f_i x^i$ tag helyett $f_i = 1$ esetén x^i-t szokás írni.

Speciálisan, $x = (0, 1, 0, 0, \dots)$ és indukcióval kapjuk hogy ha $n \in \mathbb{N}$,
akkor x^n olyan sorozat, amelyben az n indexű tag az 1 egységelem, az összes többi tag pedig nulla.

Főpolinom

Ha egy polinom főegyütthatója R egységeleme,
akkor *főpolinom*nak (vagy *normált polinom*nak) nevezzük.

-Ha az R gyűrű nullosztómentes, akkor két nem nulla polinom szorzatának a főegyütthatója a főegyütthatók szorzata, foka pedig a fokok összege:
ha $f = \sum_{i=0}^{m} f_i x^i$, $f_m \neq 0$, $g = \sum_{i=0}^{n} g_i x^i$, $g_n \neq 0$, $h = fg$,
akkor a $h_k = \sum_{i+j=k} f_i g_j$ összegnek $k = m + n$ esetén egyetlen nem nulla tagja van, $f_m g_n$.

-Tehát h nem nulla polinom, így $R[x]$ is nullosztómentes.
(Egyébként mivel a nulla polinom fokát $-\infty$-nek választottuk,
$\deg(fg) = \deg(f) + \deg(g)$ mindíg teljesül.)

Mivel R izomorf a konstans polinomok részgyűrűjével,
$\mathrm{char}(R) = \mathrm{char}(R[x])$.

Formális hatványsorok

Ha R egy gyűrű, akkor az R-beli végtelen sorozatok gyűrűjét az előző definícióban definiált műveletekkel $R[[x]]$-el jelöljük, elemeit *formális hatványsor*oknak nevezzük, és az $f = (f_0, f_1, \dots)$ elemet $\sum_{i=0}^{\infty} f_i x^i$ alakban írjuk.

Polinomfüggvények

A polinomok definíciójánál használt jelölésekkel, egy $f = f_0 + f_1 x + \cdots + f_n x^n$ polinomnak az $r \in R$ helyen felvett helyettesítési értékén az $f(r) = f_0 + f_1 r + \cdots + f_n r^n \in R$ elemet értjük. Az $r \to f(r)$ leképezést az f polinomhoz tartozó *polinomfüggvény*nek hívjuk.

Polinom gyöke

Ha f helyettesítési értéke az r helyen nulla,
akkor azt mondjuk, hogy r az f *gyök*e.

A polinomokat nem R-en értelmezett függvényként definiáltuk, tehát a polinomok nem R-en értelmezett függvények.

(Szokás megkülönböztetésként az f polinomhoz tartozó polinomfüggvényt például $\hat{f}$-vel jelölni.)

-Előfordulhat, hogy két különböző polinomhoz ugyanaz a polinomfüggvény tartozik.

Például ha az R gyűrű véges, de nem a nullgyűrű, akkor végtelen sok polinom van $R[x]$-ben, míg csak véges sok R-et R-be képező függvény létezik.

Ha p prímszám, $R = \mathbb{Z}_p$, akkor bármely $n \in \mathbb{Z}$-re $n^p \equiv n \bmod p$, azaz minden $r \in \mathbb{Z}_p$-re $r^p = r$, így a $\mathbb{Z}_p$ feletti x^p és az x polinomokhoz ugyanaz a polinomfüggvény tartozik.

-A fentiek alapján általánosabban az is belátható, hogy minden $\mathbb{Z}_p$ feletti polinomhoz van egy p-nél alacsonyabb fokú (vagy nulla) $\mathbb{Z}_p$ feletti polinom, amihez ugyanaz a polinomfüggvény tartozik.

-A később bizonyítandó tételekből azonban az következni fog, hogy ha R végtelen egységelemes integritási tartomány,
akkor $R[x]$ két különböző eleméhez nem tartozik ugyanaz a polinomfüggvény.

Ekkor a polinomokat azonosíthatjuk a polinomfüggvényekkel.

-Ha R kommutatív egységelemes gyűrű,
akkor bármely $c \in R$-re a $\vartheta_c : f \mapsto f(c)$ leképezése $R[x]$-nek R-re epimorfizmus.

Maradékos osztás tétele polinomokra

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

Bizonyítás

Először q és r létezését bizonyítjuk a fokszám szerinti indukcióval.

Ha $\deg(f) < \deg(g)$, akkor $q = 0$ és $r = f$ választható.

Indukcióval, ha f főegyütthatója f_n, a g főgyütthatója pedig g_k, legyen $f^* = f - f_n g_k^{-1} g x^{n-k}$.

Mivel $\deg(f^*) < \deg(f)$, az indukciós feltevés szerint $f^* = gq^* + r^*$, ahonnan $r = r^*$, $q = f_n g_k^{-1} x^{n-k} + q^*$ választással kapjuk az előállítást.

Az egyértelműség onnan következik, hogy $gq + r = gq^* + r^*$ esetén $g(q - q^*) = r^* - r$;
innen, ha valamelyik oldal nem nulla, akkor a másik sem, de a bal oldal fokszáma legalább $k = \deg(g)$,
a jobb oldal fokszáma pedig ennél kisebb.

Következmény

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

Bizonyítás

Testben minden nem nulla elem egység, így minden nem nulla g-re alkalmazható az előző tétel,
továbbá ha f, g nem nulla polinomok, akkor
$\deg(fg) = \deg(f) + \deg(g) \geq \max\{\deg(f), \deg(g)\}$.

Következmény: gyöktényező leválasztása

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

Bizonyítás

A maradékos osztás tételét alkalmazva $g = x - c$ választással $f = (x - c)q + r$.
Ha $r \neq 0$ lenne, akkor $\deg(r) = 0$ miatt a c helyen az egyik oldal helyettesítési értéke nulla, a másiké nem nulla lenne.

Következmény

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

Bizonyítás

A fokszám szerinti indukcióval dolgozunk.
Ha $\deg(f) = 0$, igaz az állítás.

Ha $\deg(f) > 0$, és c egy gyök, akkor $f = (x - c)g$, ahol $1 + \deg(g) = \deg(f)$.

Ha d az f egy gyöke, akkor vagy $d - c = 0$, azaz $d = c$, vagy d gyöke g-nek, ahonnan következik az állítás.

Következmény

Ha két legfeljebb n-ed fokú polinom (a nulla polinomot is ide értve) $n+1$ különböző helyen ugyanazt az értéket veszi fel, akkor megegyeznek.

Bizonyítás

Egyébként a különbségpolinom olyan legfeljebb n-ed fokú nem nulla polinom lenne, amelynek $n+1$ gyöke van.

Következmény

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

Bizonyítás

Egyébként a különbségpolinomnak végtelen sok gyöke lenne.

Megjegyzés

A maradékos osztás tétele algoritmust ad a maradékos osztás elvégzésére.

Ez az algoritmus annak eldöntésére is alkalmazható, hogy g osztója-e f-nek.

Ha ugyanis $f = gh$, akkor h főegyütthatója az az egyetlen R-beli h_{n-k} elem, amelyre $f_n = g_k h_{n-k}$ és az $f^* = f - h_{n-k}x^{n-k}g$, $h^* = h - h_{n-k}x^{n-k}$ jelölésekkel $f^* = gh^*$.

Ha tehát az osztás során a
a k-nál nem alacsonyabb fokú közbülső maradék főegyüthatója nem osztható g főegyütthatójával,
vagy az algoritmus végén a maradék nem nulla,
akkor $g \not| f$, egyébként pedig megkapjuk h-t.

Megjegyzés:

Horner-elrendezés

A maradékos osztás tételét alkalmazva az f és a $g = x - c$ polinomra azt kapjuk, hogy $f = (x - c)q + r$, ahol r konstans, értéke $f(c)$.

Így $n - 1$ szorzással és ugyanannyi összeadással megkaphatjuk $f(c)$-t.

Megjegyzés

Az hogy egy polinomnak hány gyöke van, függ attól, hogy milyen gyűrű felett tekintjük.

Például az $1 + x^2$ polinomot $\mathbb{Z}$, $\mathbb{Q}$, illetve $\mathbb{R}$ felett tekintve, nincs gyöke,
$\mathbb{C}$ felett két gyöke van, i és $-i$,
ha $\mathbb{Z}_p$ felett tekintjük, ahol p prímszám, akkor $p = 2$ esetén egy gyöke van,
$p = 3$ esetén nincs gyöke és $p = 5$ esetén két gyöke van.

Megjegyezzük, hogy minden $q = bi + cj + dk$, $b, c, d \in \mathbb{R}$ kvaternióra, amelyre $b^2 + c^2 + d^2 = 1$,
teljesül, hogy $1 + q^2 = 0$, és ilyen kvaternió végtelen sok van.

A kvaterniók szorzása azonban nem kommutatív.

Körosztási polinomok*

Ha $n \in \mathbb{N}^+$, legyen $\varepsilon_0, \varepsilon_1 \ldots, \varepsilon_{n-1}$ az n-edik egységgyökök.

Az ε_k pontosan akkor primitív n-edik egységgyök, ha n és k relatív prímek:
valóban, $\varepsilon_k^x = \varepsilon_1^{kx} = \varepsilon_j$ pontosan akkor teljesül valamely $x \in \mathbb{Z}$-re, ha $kx \equiv k \bmod n = j$;
ha k és n relatív prímek, akkor ez az egyenlet megoldható minden $j \in \mathbb{Z}$-re,
ha pedig nem relatív prímek, akkor például $j = 1$-re nem megoldható.

Legyen

$$\Phi_n(x) = \prod_{0 \le k < n, \text{lnko}(k,n)=1} (x - \varepsilon_k),$$

az n-edik körosztási polinom;
ennek foka $\varphi(n)$.

Mivel bármely ε_k egységgyök m rendjére $m \mid n$, és erre az m-re (de csak erre) ε_k primitív m-edik egységgyök,

$$\prod_{m|n} \Phi_m(x) = \prod_{0 \le k < n} (x - \varepsilon_k) = x^n - 1.$$

Innen egyébként $\sum_{m|n} \varphi(m) = n$.

Teljes indukcióval megmutatjuk, hogy Φ_n egész együtthatós:
$\Phi_1(x) = x - 1$ egész együtthatós, és ha minden $m < n$-re Φ_n egész együtthatós, akkor $x^n - 1 = \Phi_n(x) p_n(x)$ miatt, ahol

$$p_n(x) = \prod_{m|n, m<n} \Phi_m(x)$$

egész együtthatós főpolinom, n-re is.

Mivel $m \mid n$ esetén $x^m - 1 \mid p_m(x)$, az is adódik, hogy

$$\Phi_n \mid \frac{x^n - 1}{x^m - 1} = \left(\sum_{j=0}^{n/m-1} x^{mj} \right).$$

Wilson tétele

Ha p prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.

Bizonyítás

A $p = 2$ eset triviális.

Ha $p > 2$, akkor a $\mathbb{Z}_p$ feletti
$x^{p-1} - 1 - \prod_{i=1}^{p-1}(x - i)$ polinom nulla kell legyen, mert
$1, 2, \ldots, p-1$ gyökei,
foka pedig legfeljebb $p - 2$.

Igy speciálisan a konstans tag is nulla kell legyen $\mathbb{Z}_p$-ben.

Polinom algebrai deriváltja

Legyen R gyűrű.
Egy $f = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n \in R[x]$ polinom *algebrai deriváltján* vagy röviden *deriváltján* az $f' = f_1 + 2f_2 x + 3f_3 x^2 + \cdots + n f_n x^{n-1} \in R[x]$ polinomot értjük.

-Egységelemes integritási tartomány felett az $f \mapsto f'$ algebrai deriválás rendelkezik az alábbi tulajdonságokkal:
(1)konstans polinom deriváltja a nulla polinom;
(2)az x polinom deriváltja az egységelem;
(3)$(f+g)' = f' + g'$, ha $f, g \in \mathbb{R}[x]$(additivitás);
(4)$(fg)' = f'g + fg'$, ha $f, g \in \mathbb{R}[x]$(szorzat differenciálási szabálya);
ez utóbbi tulajdonság belátásához az additivitás és a disztributivitás miatt csak azt kell észrevenni,
hogy monomok szorzatára igaz az összefüggés.

Megjegyzés

Megfordítva, ha R egységelemes integritási tartományra egy $f \mapsto f'$ leképezése $R[x]$-nek önmagába rendelkezik ezzel a négy tulajdonsággal,
akkor i szerinti indukcióval az $f_i x^i$ monom deriváltja
$(f_i x^{i-1} \cdot x)' = (i-1) f_i x^{i-2} x + f_i x^{i-1} = i f_i x^{i-1}$,
amiből az $f' = f_1 + 2f_2 x + 3f_3 x^2 + \cdots + n f_n x^{n-1}$ formula következik tetszőleges polinomra.

Tétel

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

Bizonyítás

Ha $f = g^n h$, ha akkor differenciálással

$$f' = n g^{n-1} h + g^n h' = g^{n-1}(nh + h').$$

Következmény

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

Bizonyítás

Ha $g^n \mid f$, de $g^{n+1} \nmid f$, akkor $g^{n-1} \mid f'$, így $g^{n-1} \mid d$. Innen $g^2 \mid q$ nem lehetséges, mert abból $g^{n+1} \mid f$ következne.

Többszörös gyökök

n-szeres gyök

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

Azt mondjuk, hogy $c \in R$ az f egy n-szeres gyöke, ha $(x-c)^n | f$ de $(x-c)^{n+1} \not| f$.

(Szokásos az $(x-c)^n \| f$ jelölés is.) Ez azzal ekvivalens, hogy $f = (x-c)^n g$, ahol g-nek c nem gyöke.

Tétel

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $n \in \mathbb{N}^+$ és $c \in R$ az f egy n-szeres gyöke.
Ekkor c az f'-nek legalább $(n-1)$-szeres gyöke, és ha $\mathrm{char}(R) \nmid n$ (például ha $\mathrm{char}(R) = 0$), akkor pontosan $(n-1)$-szeres gyöke.

Bizonyítás

Ha $f = (x-c)^n g$, akkor $f' = (x-c)^{n-1}\big((x-c)g' + ng\big)$.

Innen látszik, hogy c legalább $(n-1)$-szeres gyöke f'-nek.

A zárójelben álló kifejezés értéke a c helyen $ng(c)$, ami $g(c) \neq 0$ miatt nem nulla, ha $\mathrm{char}R \nmid n$.

Megjegyzés

A derivált gyöke nyilván nem feltétlenül gyöke a polinomnak.

(például x^2+1-nek 0 nem gyöke, de a deriváltjának igen)

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

Irreducibilis polinomok és testbővítések

-A test feletti egyhatározatlanú polinomok euklideszi gyűrűt alkotnak,
így bennük a prímelem és az irreducibilis elem fogalma egybeesik és minden nem nulla polinom irreducibilis polinomok szorzatára bomlik,
lényegében egyértelműen.

-Az egységek a nem nulla konstans polinomok.

-Bármely test felett az elsőfokú polinomok irreducibilisek.

Legyen F test, és $f \in F[x]$ egy n-ed fokú ($n \in \mathbb{N}^n$) irreducibilis főpolinom.

Ekkor $\tilde{F} = F[x]/(f)$ test;
ez következik abból, hogy az (f) főideál maximális ideál, de közvetlenül is belátható:
ha $g \notin (f)$, azaz f nem osztja g-t,
akkor alkalmazva a bővített euklideszi algoritmust, olyan u és v polinomokat kapunk, amelyekre
$d = fu + gv$,
ahol d az f és g egyik legnagyobb közösosztója, egy nullad fokú polinom.

Innen d osztálya az egységelem $\tilde{F}$-ban, v osztály pedig g osztályának az inverze.

Minden mellékosztályban a legalacsonyabb fokú polinom fokszáma kisebb, mint n és csak egy n-nél alacsonyabb fokú polinom van;

Ez meghatározó úgy, hogy a mellékosztály tetszőleges g elemére vesszük
az f-fel való osztásánál adódó r maradékot:
mivel $g = qf + r$, $g - r \in (f)$.

A műveleteket végezhetjük ezekkel a reprezentánsokkal:
ha a szorzat foka nem kisebb, mint n,
akkor osztunk f-fel, és vesszük a maradékot.

Jelölje $\tilde{x}$ az $x \in F[x]$ polinom osztályát $F[x]/(f)$-ben.

A $\tilde{F}$ test elemei egyértelműen felírhatók
$a_0 + a_1\tilde{x} + \cdots + a_{n-1}\tilde{x}^{n-1}$ alakban, ahol $a_0, a_1, , \ldots a_{n-1} \in F$.

Igy F részteste $\tilde{F}$-nak.
(A $\tilde{F}[x]$-belinek is tekinthető f polinom $\tilde{F}[x]$-ben már nem irreducibilis, $\tilde{x}$ egy gyöke.)

Legyen p egy prímszám.

A fenti konstrukciót alkalmazva a $\mathbb{Z}_p$ véges testre és egy f irreducibilis főpolinomra,
egy p^n elemű véges testet kapunk.

Azt, hogy az n-ed fokú $f \in \mathbb{Z}_p[x]$ polinom irreducibilis-e, például úgy is megvizsgálhatjuk, hogy minden, legfeljebb $\lfloor n/2 \rfloor$ fokszámú polinommal megpróbáljuk elosztani.

(Ennél sokkal hatékonyabb eljárást is fogunk tanulni.)

Példák

(1) Tekintsük az $\mathbb{R}[x]$ polinomgyűrűben az R felett irreducibilis x^2+1 polinom által generált (x^2+1) főideált.
Minden mellékosztályban a legalacsonyabb fokú polinom lineáris és a mellékosztályban pontosan egy lineáris polinom van.
A faktorgyűrű szorzásával a mellékosztályok $\mathbb{C}$-vel izomorf testet alkotnak.

(2) Tekintsük a $\mathbb{Z}_2[x]$ polinomgyűrűben az x^2+x+1 irreducibilis polinom által generált (x^2+x+1) főideál.
Minden mellékosztályban a legalacsonyabb fokú polinom lineáris, és a mellékosztályban pontosan egy lineáris polinom van.

A faktorgyűrű szorzásával a mellékosztályok egy négyelemű testet alkotnak.

Véges testek elemszáma

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

Bizonyítás

Ha p az F véges test karakterisztikája és e az egységeleme, akkor a $\mathbb{Z}$-t F-be képező $n \to ne$ homomorfizmus magja $p\mathbb{Z}$.

Azonosítva $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$-t a leképezés értékkészletével, $\mathbb{Z}_p$ az F részteste.

Nyilván F vektortér $\mathbb{Z}_p$ felett és ha n dimenziós, akkor F-nek p^n eleme van.

Megjegyzések

(1) Abból, hogy egy test karaktetisztikája egy p prímszám, nem kövtkezik, hogy a test véges.

Például $\mathbb{Z}_p[x]$ hányadostestének karakterisztikája p.

(2) Ha $n > 1$, akkor egy p^n elemű véges test nem izomorf $\mathbb{Z}_{p^n}$-el, sem $\mathbb{Z}_p^n$-el,
bár mindegyiknek ugyanannyi eleme van, mert az utóbbiak nem nullosztómentes gyűrűk
(de nem izomorfak, mert $\mathbb{Z}_{p^n}$ additív csoportja ciklikus,
míg $\mathbb{Z}_p^n$-ben minden nem nulla elem additív rendje p).

Alkalmazás: A Rijndael és AES blokkrejtjelzők

Tétel

Véges test nem nulla elemeinek multiplikatív csoportja ciklikus.

Ha a véges testnek q eleme van, akkor bármely c elemére $c^q = c$.

Az állítás a Fermat-tétel általánosítása.

Bizonyítás

Legyen a nem nulla elemek multiplikatív csoportja G és legyen a G rendje n.

Ha $d \mid n$ és van olyan $g \in G$, amelynek a rendje d, akkor ez egy $H = \{1, g, g^2, \ldots g^{d-1}\}$ ciklikus részcsoportot generál.

Bizonyítás folytatása

Mivel testben az $x^d = 1$ egyenletnek legfeljebb d megoldása van, azok mind a H részcsoportban vannak.

Speciálisan, minden d rendű eleme G-nek genrátora H-nak és $\varphi(d)$ ilyen van.

Igy d rendű eleme G-nek 0 vagy $\varphi(d)$ darab van.

Ha valamilyen $d \mid n$-re nulla lenne, az ellentmondana annak, hogy $\sum_{d|n} \varphi(d) = n$.

Igy van n rendű elem is -éppen $\varphi(n)$ számú - tehát G ciklikus.

Tétel

Legyen F egy q elemű véges test.

Egy F feletti d-ed fokú irreducibilis főpolinom, akkor és csakis akkor osztja $x^{q^n} - x$-et, ha $d \mid n$.

Bizonyítás

Legyen f egy d-ed fokú irreducibilis főpolinom és tekintsük az $\tilde{F} = F[x]/(f)$ véges testet, amelynek q^d eleme van.

Ennek bármely y elemére $y^{q^d} = y$. Innen k szerinti teljes indukcióval

$$y^{q^{dk}} = y^{(q^{d(k-1)}q^d)} = \left(y^{q^{d(k-1)}}\right)^{q^d} = y^{q^d} = y$$

minden $y \in \tilde{F}$-ra. Igy $d \mid n$ esetén $y^{q^n} = y$ az $\tilde{F}$-ban, ami speciálisan $y = \tilde{x}$ választással azt is jelenti, hogy az F feletti $x^{q^n} - x$ polinom osztható f-fel.

Fordítva, legyen ξ a $\tilde{F}$ nem nulla elemei multiplikatív csoportjának egy generátora.

Legyen p az $\tilde{F}$ karakterisztikája.

Azok az $\eta \in \tilde{F}$ elemek, amelyekre $\eta^{q^n} = \eta$ az összeadásra nézve zárt halmazt alkotnak, mert $(\eta_1 + \eta_2)^{p^k} = \eta_1^{p^k} + \eta_2^{p^k}$ és q^n is p-hatvány.

Bizonyítás folytatása

Nyilván az ilyen η elemek halmaza a szorzásra is zárt.

Igy ha f osztja az $x^{q^n} - x$ polinomot $F[x]$-ben, akkor $\tilde{F}$-ben $\tilde{x}^{q^n} = \tilde{x}$,

amiből mivel ξ az $\tilde{x}$ polinomja, $\xi^{q^n} = \xi$ is teljesül.

De ha $n = kd + r$, $0 \leq r < d$, akkor

$$\xi = \xi^{q^n} = \xi^{(q^{dk} q^r)} = \left(\xi^{q^{dk}}\right)^{q^r} = \xi^{q^r},$$

ami $r > 0$ esetén ellentmond annak, hogy ξ generátorelem.

Következmény

Az F feletti n-ed fokú irreducibilis polinomok száma legalább $(q^n - q^{\lfloor n/2 \rfloor} \lfloor \lg n \rfloor)/n > 0$.

Bizonyítás

Mivel $x^{q^n} - x$ deriváltja a -1 polinom, bármely irreducibilis főpolinomnak legfeljebb az első hatványa osztja $x^{q^n} - x$-t.

Bármely d valódi osztójára n-nek d osztója n/p_i-nek valamely p_i prímtényezőjére n-nek.

Igy azon irreducibilis főpolinomok, amelyek osztói $x^{q^n} - x$-nek, de fokuk kisebb, mint n, mind osztói valamely $x^{q^{n/p_i}} - x$ polinomnak, amelynek foka legfeljebb $q^{\lfloor n/2 \rfloor}$.

Mivel az n különböző prímosztóinak száma legfejebb $\lfloor \lg n \rfloor$, azon irreducibilis főpolinomok,
amelyek osztói $x^{q^n} - x$-nek, de fokuk kisebb mint n,
szorzatának a foka legfeljebb $q^{\lfloor n/2 \rfloor} \lfloor \lg n \rfloor$.

Igy a pontosan n-ed fokú irreducibilis főpolinomok szorzatának a foka legalább $q^n - q^{\lfloor n/2 \rfloor} \lfloor \lg n \rfloor$.

Hátra van még annak bizonyítása, hogy ez a szám pozitív.

Felhasználva, hogy $q \geq 2$, ez könnyen ellenőrizhető
$n = 1, 2, 3, 4, 5, 6, 7, 8$ esetén.

Megmutatjuk, hogy $n \geq 8$ esetén a $q^n > q^{n/2} \lg n$ egyenlőtlenség is teljesül.

Ha $n = 8$, a két egyenlőtlenség ekvivalens, egyébként pedig teljes indukcióval

$$q^{n+1} = qq^n > qq^{n/2} \lg n = q^{(n+1)/2} \lg(n+1)\sqrt{q}\frac{\lg n}{\lg(n+1)}$$

$$> q^{(n+1)/2} \lg(n+1),$$

mert

$$\sqrt{q}\frac{\lg n}{\lg(n+1)} > \sqrt{2}\frac{\lg n}{\lg(2n)} \geq \sqrt{2}\frac{\lg n}{1+\lg n} = \sqrt{2}\frac{1}{1+1/\lg n}$$

$$\geq \sqrt{2}\frac{1}{1+1/3} = \frac{3\sqrt{2}}{4} > 1.$$

Következmény

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

Bizonyítás

Alkalmazzuk az előző következményt $\mathbb{Z}_p$-re.

Testbővítések

Ha F a K részteste, akkor azt is mondjuk, hogy K az F test *bővítése*.

Nyilván K vektortér F felett.

Bővítés foka

Ennek a vektortérnek a dimenzióját a *bővítés fokának* nevezzük és $[K : F]$-fel jelöljük;
ha véges, akkor véges *bővítésről* beszélünk.

Legyen $\alpha \in K$. A K összes, F-et és α-t tartalmazó résztestének a metszete maga is részteste K-nak: ez az

$$F(\alpha) = \{p(\alpha)/q(\alpha) : p, q \in F[x], q(\alpha) \neq 0\}$$

részhalmaza K-nak.

Ha van olyan $0 \neq p \in F[x]$ polinom, amelynek α gyöke, akkor azt mondjuk,
hogy α *algebrai* F felett.
Az α *minimálpolinomja* F felett egy minimális fokú ilyen oplinom.
Egy minimálpolinom minden olyan $F[x]$-beli polinomnak osztója, amelynek α gyöke,
mert egyébként a két polinom legnagyobb közös osztója egy,
a minimálpolinomnál alacsonyabb fokú polinom lenne, amelynek α gyöke.
Igy a minimálpolinomok egymás asszociáltjai.
A minimálpolinomok nyilván irreducipilisek.
Fokszámuk az α foka F felett.

Tétel

Legyen K az F test bővítése.
Ha $\alpha \in K$ algebrai F felett, a foka n és f egy minimálpolinomja, akkor $F(\alpha)$ izomorf $F[x]/(f)$-fel, és
$F(\alpha)$ minden eleme egyértelműen írható fel $\sum_{j=0}^{n-1} r_j \alpha^j$ alakban, ahol $r_0, r_1, \ldots, r_{n-1} \in F$.

Bizonyítás

A $g \to g(\alpha)$ leképezés olyan homomorfizmusa az $F[x]$ gyűrűnek K-ba,
amelynek magja (f), így értékkészlete egy $F[x]/(f)$-el izomorf test.
Az értékkészlete tartalmazza F-et és α-t, így $F(\alpha)$-t is.
Mivel $F(\alpha)$ nyílván tartalmazza $\sum_{j=0}^{n-1} r_j \alpha^j$ alakú összeget,
csak azt kell megmutatnunk, hogy az értékkészlet minden eleme ebben a halmazban van.
Legyen $g \in F[x]$ tetszőleges és írjuk fel $g = qf + r$ alakban; nyilván $g(\alpha) = r(\alpha)$.

Véges testek alaptétele

Bármely $q = p^n$ (p prím, $n \in \mathbb{N}^+$) prímhatványra a q elemű véges testek izomorfak.
Már láttuk, hogy bármely q prímhatványra van q elemű véges test.
Mivel a tétel szerint lényegében csak egy q elemű véges test van,
beszélhetünk a q elemű véges testről.
Ezt $\mathbb{F}_q$-val jelöljük.

Bizonyítás

Legyen F egy tetszőleges q elemű véges test, p pedig az F karakterisztikája, és $q = p^n$.
Ekkor, mint tudjuk az egységelem többszörösei egy $\mathbb{Z}_p$-vel izomorf résztestet alkotnak.
Ezt $\mathbb{Z}_p$-vel azonosítva, $\mathbb{Z}_p$ a K részteste.
Legyen f egy n-ed fokú irreducibilis főpolinom.
Ez osztója $\mathbb{Z}_p$ felett a $g(x) = x^q - x$ polinomnak.
A g polinom F felett elsőfokú polinomok szorzatára bomlik, mert minden $y \in F$ gyöke, így q különböző gyöke van.
De akkor az irreducibilis tényezőkre való felbontás egyértelműsége miatt
f is elsőfokú tényezők szorzatára bomlik F felett.
Jelölje α az f egyik gyökét F felett.
Mivel $\mathbb{Z}_p(\alpha)$-nak $q = p^n$ eleme van, $\mathbb{Z}_p(\alpha) = F$.
Mivel $\mathbb{Z}_p(\alpha)$ izomorf $\mathbb{Z}_p[x]/(f)$-fel
az F izomorf $\mathbb{Z}_p[x]/(f)$-fel.

Wedderburn tétele

Véges ferdetest kommutatív.

Bizonyítás

Legyen K véges ferdetest és ha $x \in K$,
legyen $C_K(x) = \{y \in K : xy = yx\}$, valamint
$C_k = \cap_{x \in K} C_K(x)$.
Minden $C_K(x)$ és így C_K is ferdetest, de C_K kommutatív is.
Legyen q a C_K elemeinek száma.
Mivel minden $C_K(x)$ vektortér C_K felett, elemszámuk q^{n_x} valamely $n_x \in \mathbb{N}^+$-ra.
Speciálisan $K = C_K(0)$ elemszáma is q-hatvány, mondjuk q^n.
Mivel K vektortér a $C_K(x)$ ferdetest felett is,
$n_x \mid n$ minden $x \in K$-ra.
Tekintsük most a $G = K \setminus \{0\}$ multiplikatív csoport.
A $C(x)$ konjugált elemosztály $x \neq 0$ esetén $C_K(x) \setminus \{0\}$ és így a C centrum $C_K \setminus \{0\}$.

Az osztályegyenelet szerint

$$q^n - 1 = q - 1 + \sum [G : C(x)] = q - 1 + \sum \frac{q^n - 1}{q^{n_x} - 1};$$

az összegzés a nem egyelemű konjugált elemosztályok egy-egy x reprezentánsára értendő $q - 1$ pedig az egyelemű konjugált elemosztályok száma, amely C elemszáma.
A Ψ_n körosztási polinom q helyen felvett értéke osztja a bal oldalt és a jobb oldali összeg minden tagját, így $q - 1$-et is.
Ha azonban $n > 1$, akkor ez ellentmondás, mert
$\Psi_n(x) = \prod(x - \varepsilon_k)$, ahol a szorzat az összes primitív n-edik ε_k egységgyökre értendő, így $\mid \Psi_n(q) \mid = \prod \mid q - \varepsilon_k \mid$ és a jobb oldalon minden tényező abszolut értéke nagyobb, mint $q - 1$.
Tehát $n = 1$ és $K = C_K$.

Polinom faktorizálás véges testek felett

Első lépésként az $\mathbb{F}_q$ feletti f polinomot ($q = p^n$, p prím, $n \in \mathbb{N}^+$) a korábbi tétel következményben megadott lépés ismétlésével négyzetmentes tényezők szorzatára bontjuk;
gondot okozhat, hogy az f és f' polinomok d legnagyobb közös osztója f is lehet, ha $f' = 0$.

Ez akkor fordulhat elő, ha $f_0 + f_1 x^p + f_2 x^{2p} + \cdots + f_m x^{mp}$ alakú az f,
azaz csak olyan monomokban lép fel nem nulla együttható, amelyekre a kitevő p többszöröse.

Ekkor $g_j = f_j^{q/p}$ választással $g_j^p = f_j^q = f_j$, és a $g = g_0 + g_1 x + \cdots + g_m x^m$ polinomra

$$g(x)^p = g_0^p + (g_1 x)^p + \cdots + (g_m x^m)^p = f(x)$$

így elég g-t faktorizálni.

Második lépésként egy már négyzetmentes f polinomra $d = 1, 2 \ldots$-re számoljuk ki
$f(x)$ és $x^{q^d} - x$ legnagyobb közös osztóját, az $f_d(x)$ polinomot.

Az f_1 az f elsőfokú, az f_2 az f másodfokú, stb., irreducibilis tényezőinek szorzata.
Természetesen ha f_1 nem konstans, akkor f_2 kiszámítása előtt f-et célszerű helyettesíteni f/f_1-el, stb.
Ha így teszünk, akkor megállhatunk, ha d nagyobb nem lesz, mint $\lfloor \deg(f)/2 \rfloor$; ekkor f már irreducubilis.
Harmadik lépésként az f_d polinomokat "hasítjuk" szét.
Ha f_d fokszáma d, akor nyilván irreducibilis, megállhatunk.
Ha valamelyik f_d fokszáma nagyobb, mint d, akkor egy valószínűségi módszert használhatunk a "széthasításra".
Ez azon alapul, hogy tetszőleges $t(x)$ "tesztpolinomra" $t(x)^{q^d} - t(x)$ többszöröse $x^{q^d} - x$-nek; valóban, mivel F karakterisztikája p és q a p hatványa,

$$t(x)^{q^d} = \left(\sum_{j=0}^{k} t_j x^j\right)^{q^d} = \sum_{j=0}^{k} t_j^{q^d} (x^j)^{q^d} = \sum_{j=0}^{k} t_j \left(x^{q^d}\right)^j,$$

ahonnan $F[x]/(x^{q^d} - x)$-ben számolva

$$\tilde{t}^{q^d} = \sum_{j=0}^{k} t_j \left(\tilde{x}^{q^d}\right)^j = \sum_{j=0}^{k} t_j \tilde{x}^j = \tilde{t}.$$

Ha most a $t(x)^{q^d} - t(x)$ polinomnak vesszük egy faktorizációját, akkor valószínű, hogy f_d irreducibilis osztói nem mind ugyanabban a tényezőben lesznek,
és legnagyobb közös osztó képzéssel kinyerhetők.

Páratlan q esetén a nyilvánvaló

$$t(x)^{n^d} - t(x) = \left(t(x)^{(q^d-1)/2} - 1\right)\left(t(x)^{(q^d-1)/2} + 1\right) t(x)$$

faktorizálás használható;
megmutatható, hogy ha a t tesztpolinomot véletlenszerűen választjuk az összes $2d$-nél alacsonyabb fokú polinomok közül, akkor f_d és $t(x)^{(q^d-1)/2} - 1$ legnagyobb közös osztója legalább $1/2 - 1/(2q^d)$ eséllyel nem triviális.

(A gyakorlatban sokszor már azzal is célt érünk,
ha t-t véletlen elsőfokú főpolinomnak választjuk.)

Páros q esetén a

$$t(x)^{n^d} - t(x) = \prod_{c \in \mathbb{F}_q} \left(T\left(t(x)\right) - c \right)$$

faktorizálás használható, ahol

$$T(x) = x + x^q + x^{q^2} + \cdots + x^{q^{(d-1)}};$$

ez úgy adódik, hogy a nyilvánvaló $x^q - x = \prod_{c \in \mathbb{F}_q} (x - c)$ faktorizálásba x helyére $T(x)$-t írunk és felhasználjuk, hogy $T(x)^q - T(x) = x^{q^d} - x$, mivel $T(x)^q = T(x^q)$, majd x helyére $t(x)$-t helyettesítünk.

Magasabb fokú kongruenciák

Az

$$f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n \equiv 0 \bmod (m)$$

kongruencia megoldásait keressük, ahol $f_0, f_1, \ldots f_n \in \mathbb{Z}$ és $m \in \mathbb{N}$, $m > 1$.

A kínai maradéktétel segítségével a kongruencia minden megoldását megkaphatjuk, ha m kanonikus felbontásában szereplő prímhatvány tényezőket véve modulusnak, meghatározzuk a megoldásokat.

Hasznos észrevétel, hogy ha p prímszám, $\alpha \in \mathbb{N}^+$, akkor minden $x \in \mathbb{Z}$-re

$$x^{j+\varphi(p^\alpha)} \equiv x^j \bmod x^\alpha, \text{ ha } j \geq \alpha;$$

ennek a segítségével redukáljuk a kungruencia fokát.
Az $\alpha = 1$ eset elintézhető az előző pont alapján,
hiszen ekkor egy $\mathbb{Z}_p$ feletti polinom gyöktényezőit kell meghatároznunk.
Végük az $\alpha > 1$ eset az alábbi lemma alpján indukcióval visszavezethető az $\alpha = 1$ esetre.

Hensel-lemma

Legyen p prímszám, $\alpha \in \mathbb{N}^+$, $f, g_\alpha, h_\alpha, u, v \in \mathbb{Z}[x]$,
$deg(u) < deg(h_\alpha)$, $deg(v) < deg(g_\alpha)$
és tegyük fel, hogy g_α főpolinom,
$deg(f) = deg(g_\alpha) + deg(h_\alpha)$ valamint teljesülnek az

$$f(x) \equiv g_\alpha(x)h_\alpha(x) \ mod \ p^\alpha,$$

$$u(x)g_\alpha(x) + v(x)h_\alpha(x) \equiv 1 \ mod \ p$$

kongruenciák.

Ekkor léteznek olyan $g_{\alpha+1}, h_{\alpha+1} \in \mathbb{Z}[x]$ polinomok, amelyre

$$g_{\alpha+1}(x) \equiv g_\alpha(x) \ mod \ p^\alpha$$

és

$$h_{\alpha+1}(x) \equiv h_\alpha(x) \ mod \ p^\alpha$$

továbbá a fenti feltételek mind teljesülnek $\alpha + 1$-el α helyett.

A $g_{\alpha+1}$ és $h_{\alpha+1}$ polinomok egyértelműek modulo $p^{\alpha+1}$.

A bizonyítás konstruktív, algoritmust ad $g_{\alpha+1}$és $h_{\alpha+1}$ meghatározására.

Bizonyítás

Ha létezik $g_{\alpha+1}$ és $h_{\alpha+1}$, akkor $g_{\alpha+1} = g_\alpha + p^\alpha \overline{g}$ illetve $h_{\alpha+1} = h_\alpha + p^\alpha \overline{h}$ alakú,
ahol $\overline{g}, \overline{h} \in \mathbb{Z}[x]$, $\deg(\overline{g}) < \deg(g_\alpha)$, $\deg(\overline{h}) \leq \deg(h_\alpha)$.

Az

$$u(x)g_{\alpha+1}(x) + v(x)h_{\alpha+1}(x) \equiv 1 \bmod p$$

feltétel ekkor nyilván teljesül, az

$$f(x) \equiv g_{\alpha+1}(x)h_{\alpha+1}(x)$$

$$= (g_\alpha(x) + p^\alpha \overline{g}(x))(h_\alpha(x) + p^\alpha \overline{h}(x)) \bmod p^{\alpha+1}$$

feltétel pedig azzal ekvivalens, hogy

$$\overline{h}(x)g_\alpha(x) + \overline{g}(x)h_\alpha(x) \equiv w(x) \bmod p$$

ahol

$$w(x) = \frac{f(x) - g_\alpha(x)h_\alpha(x)}{p^\alpha}$$

Tetszőleges $q(x) \in \mathbb{Z}[x]$-re

$$(u(x)w(x) + q(x)h_\alpha(x))\, g_\alpha(x)$$

$$+ (v(x)w(x) - q(x)g_\alpha(x))\, h_\alpha(x) \equiv w(x) \bmod p.$$

Legyen q a vw polinomnak a g_α polinommal $\mathbb{Z}_p$ felett való osztásánál fellépő hányados, $\overline{g} = vw - qg_\alpha$ és $\overline{h} = vw - qh_\alpha$, mindkettő $\mathbb{Z}_p$ felett kiszámolva.

Mivel $\overline{g}$ a vw polinomnak g_α-val való osztásnál fellépő maradék, $\deg(w) \leq \deg(f) = \deg(g_\alpha) + \deg(h_\alpha)$ azt kapjuk, hogy $\deg(\overline{h}) \leq \deg(h_\alpha)$,
mivel egyébként az előző kongruencia nem teljesülne.

Ha $\overline{\overline{g}}$ és $\overline{\overline{h}}$ másik megoldás, akkor

$$(\overline{h} - \overline{\overline{h}}(x))g_\alpha(x) \equiv (\overline{\overline{g}} - \overline{g}(x))h_\alpha(x) \bmod p.$$

Mivel $\mathbb{Z}_p$ felett g_α és h_α relatív prímek, g_α osztja $\overline{\overline{g}} - \overline{g}$-t.

Mivel ennek fokszáma kisebb, mint g_α fokszáma, csak nulla lehet.

Innen a másik oldal is nulla.

Irreducibilis polinomok $\mathbb{C}, R, Q$ és $\mathbb{Z}$ felett

A *komplex számtest* felett az algebra alaptétele szerint minden $\mathbb{C}[x]$-beli nem konstans polinomnak van gyöke,
Igy a gyöktényező leválasztására vonatkozó állítás szerint pontosan az elsőfokú polinomok az irreducibilisek és
egy n-ed fokú $f_0 + f_1 x + \cdots + f_n x^n$ polinomot a tényezők sorrendjétől eltekintve egyértelműen felírhatunk

$$f_n (x - c_1)^{\alpha_1} (x - c_2)^{\alpha_2} \cdots (x - c_k)^{\alpha_k}$$

*gyöktényezős alak*ban, ahol a különböző $c_1, c_2, \ldots, c_k$ komplex számok a különböző gyökök,
az $\alpha_1, \alpha_2, \ldots, \alpha_k$ pozitív természetes számok pedig az egyes gyökök multiplicitásai,
$\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$.

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

Megmutatjuk, hogy más irreducibilis polinom nincs.

Egy a valós számtest feletti, azaz valós együtthatós $f = f_0 + f_1 x + \cdots + f_n x^n$ polinom tekinthető komplex együtthatósnak is,
így az algebra alaptétele szerint $n \geq 1$ esetén van olyan $c \in \mathbb{C}$, hogy $f_0 + f_1 c + \cdots + f_n c^n = 0$.

Ha c valós, akkor f nem irreducibilis.

Ha $c \notin \mathbb{R}$, akkor konjugálással $f_0 + f_1 \overline{c} + \cdots + f_n \overline{c}^n = 0$, tehát c konjugáltja is gyök.

A $g_c = (x - c)(x - c) = x^2 - 2\Re(c)x + |c|^2$ valós együtthatós polinommal $\mathbb{R}$ felett maradékosan osztva, $f = g_c q + r$.

Az r csak nulla lehet, mert egyébként legfeljebb elsőfokú lenne és nem lehetne nem valós komplex gyöke.

Tehát a valós számtest felett minden $f_0 + f_1 x + \cdots + f_n x^n$ polinom legfeljebb másodfokú irreducibilis polinomok szorzatára bontható lényegében egyértelműen.

A racionális számtest felett bonyolultabb a helyzet.
Vannak polinomok, például $x^2 - 2$, amelyek $\mathbb{Q}$ felett irreducibilisek, bár $\mathbb{R}$ felett nem.
Meg fogjuk mutatni, hogy $\mathbb{Q}[x]$-ben minden $n \in \mathbb{N}^+$-ra van olyan n-ed fokú polinom, amely irreducibilis.
A $\mathbb{Z}[x]$ gyűrű nem tehető euklideszi gyűrűvé.
Ha ugyanis euklideszi gyűrűvé tudnánk tenni, akkor a 2 és x polinomok legnagyobb közös osztója, amely létezik és 1, előállítható lenne $1 = 2u + xv$ alakban valamely $u, v \in \mathbb{Z}[x]$ polinomokkal, ami nem lehetséges, mert a jobb oldal konstans tagja páros.
A $\mathbb{Q}[x]$-beli és $\mathbb{Z}[x]$-beli faktorok között kapcsolat van, bár nem ugyanazok.

Például a $6x^2 + 12x + 12$ polinom $\mathbb{Z}[x]$-ben nem felbonthatalan, felírható $2 \cdot 3 \cdot (x^2 + 2x + 2)$ alakban, míg $\mathbb{Q}[x]$-ben felbonthatatlan, itt ugyanis 2 és 3 egységek, így $6x^2 + 12x + 12$ asszociáltja az $x^2 + 2x + 2$ polinomnak, amelynek nincs racionális gyöke, mert még valós sincs.

-Általánosabban,
legyen R egy Gauss-gyűrű, K pedig a hányadosteste.

Minden $R[x]$-beli polinom tekinthető $K[x]$-belinek is.

Egy $K[x]$-beli polinom együtthatói nevezőinek szorzatával beszorozva a polinomot,
egy vele $K[x]$-ben asszociált polinomot kapunk, ami már $R[x]$-beli.

Ugyancsak asszociált főpolinomot kapunk $K[x]$-ben,
ha a főegyütthatóval végigosztjuk a polinomot.

Az $R[x]$-ben általában nem tudjuk a főegyütthatóval végigosztani a polinomot.

Az R irreducibilis elemei irreducibilisek $R[x]$-ben is, míg $K[x]$-ben egységek.

Ettől eltekintve, az $R[x]$-beli és $K[x]$-beli felbonthatóság lényegében ekvivalens:
ha egy $R[x]$-beli polinom előáll $R[x]$-ben két nem konstans, tehát alacsonyabb fokú polinom szorzataként, akkor nyilván $K[x]$-ben is.

A megfordítást, azt, hogy a két reducibilitás egybeesik, Gauss tétele adja.

Az így kapott kapcsolat $R[x]$ és $K[x]$ között nagyon fontos: néha azt használjuk ki, hogy $K[x]$ euklideszi gyűrű, tehát Gauss-gyűrű, máskor meg az R-beli oszthatóságot.

(A K-beli oszthatóság triviális.)

Primitív polinomok

Legyen R egy Gauss-gyűrű. Ekkor $R[x]$ egy polinomját *primitív polinom*nak nevezzük,
ha együtthatóinak az egységelem legnagyobb közös osztója.

(Test felett minden nem nulla polinom ilyen.)

Az $R[x]$-beli irreducubilis polinomok nyilván primitívek.
Minden $0 \neq f \in R[x]$ polinom előállítható $f = df^*$ alakban, ahol f^* primitív polinom és $0 \neq d \in R$; az előállításhoz emeljük ki f együtthatóinak legnagyobb közös osztóját.
Az előállítás nyilván lényegében egyértelmű, d és f^* egység faktorok erejéig egyértelműen meghatározottak.

Gauss lemmája

Legyen R egy Gauss-gyűrű, $f, g \in R[x]$ pedig nullától különböző primitív polinomok.

Ekkor fg is primitív polinom.

Bizonyítás

Tegyük fel, hogy fg nem primitív polinom.

Ekkor van olyan $p \in R$ prímelem, amely osztja fg minden együtthatóját.

Legyen i illetve j a legkisebb olyan index, amelyre $p \nmid f_i$ illetve $p \nmid g_j$.

Mivel az fg polinom $i+j$-edik együtthatója

$$f_0 g_{i+j} + \cdots + f_i g_j + \cdots + f_{i+j} g_0,$$

és ebben az összegben p minden más tagot oszt, osztania kell $f_i g_j$-t is, tehát $p \mid f_i$ vagy $p \mid g_j$, ami ellentmondás.

Segédtétel

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

Minden $0 \neq f \in K[x]$ polinom felírható $f = af^*$ alakban, ahol $0 \neq a \in K$ és $f^* \in R[x]$ egy primitív polinom.

A felírás lényegében egyértelmű, a és f^* egy R-beli egység szorzó illetve reciproka erejéig egyértelműen meghatározott.

Bizonyítás

Irjuk fel f együtthatóit R-beli elemek hányadosaiként.

Végigszorozva f-et az együtthatói nevezőinek c szorzatával, majd kiemelve a kapott $R[x]$-beli polinom együtthatóinak d legnagyobb közös osztóját, kapjuk az előállítást $a = d/c$-vel.

Ha $f = bg^*$ egy másik előállítás, akkor b-t felírva d'/c', $c', d' \in R$ alakban,
azt kapjuk, hogy $dc'f^* = d'cg^*$, amiből az $R[x]$-beli polinomok lényegében egyértelmű előállítása miatt következik az egység szorzó erejéig való egyértelműség.

Gauss tétele

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

Bizonyítás

Tegyük fel, hogy $f = gh$, ahol $g, h \in K[x]$ nem konstans polinomok.
Irjuk fel f-et df^* alakban, ahol $f^* \in R[x]$ primitív polinom, $d \in R$.
Felírva g-t ag^{**}, a h-t pedig bh^{**} alakban,
ahol $g^{**}, h^{**} \in R[x]$ primitív polinomok,
$df^* = f = gh = abg^{**}h^{**}$.
Mivel Gauss lemmája szerint $g^{**}h^{**}$ primitív polinom és az előző lemma szerint pedig f előállítása primitív polinom segítségével lényegében egyértelmű, valamely R-beli ε egységgel $f^* = \varepsilon g^{**}h^{**}$ és $\varepsilon d = ab$, ahol $a, b \in K$.

így azt kapjuk, hogy $f = df^* = d\varepsilon g^{**} h^{**}$, így
például $g^* = d\varepsilon g^{**}$, $h^* = h^{**}$ választással kapjuk f kívánt felbontását.
Figyeljük meg, hogy ha f primitív polinom volt, akkor g^* és h^* is azok.
A (2) rész bizonyításához vegyük észre, hogy egy konstans
pontosan akkor egység R-ben,
ha mint konstans polinom egység $R[x]$-ben és
pontosan akkor irreducibilis R-ben,
ha mint konstans polinom irreducibilis $R[x]$-ben,
továbbá $R[x]$ nem konstans irreducibilis polinomjai primitívek.

Legyen $0 \neq f \in R[x]$ és írjuk fel f-et df^* alakban, ahol $d \in R$, $f^* \in R[x]$ primitív polinom.

Az (1) bizonyításának utolsó mondata szerint, indukcióval,
f-et előállíthatjuk $f_1 f_2 \cdots f_n$ alakban, ahol $f_1, f_2, \ldots, f_n$ primitív irreducibilis polinomok,
d-t pedig $\varepsilon p_1 \cdots p_m$ alakban,
ahol $p_1, \ldots, p_m$ irreducibilis elemek R-ben, ε pedig egység R-ben.

Az egyértelműség bizonyításához, tegyük fel, hogy

$$\varepsilon p_1 \cdots p_m f_1 \cdots f_n = f = \varepsilon' q_1 \cdots q_r g_1 \cdots g_s,$$

ahol ε, ε' egységek, $p_1, \ldots, p_m$ és $q_1, \ldots, q_r$ irreducibilis R-beli elemek,
$f_1, \ldots, f_n$ és $g_1, \ldots, g_s$ pedig legalább elsőfokú R felett irreducibilis polinomok,
így primitívek és az első lépés szerint irreducibilisek K felett is.

Igy a fellépő polinomok f-nek egy K feletti irreducibilis faktorizációját is megadják, $s = n$, és
(megfelelő átindexelés után) alkalmas $0 \neq \varepsilon_i \in K$ elemekkel
$f_i = \varepsilon_i g_i$.

Az előző segédtétel szerint minden ε_i egység R-ben.

Igy

$$\varepsilon p_1 \cdots p_m = \varepsilon'' q_1 \cdots q_r$$

valamely $\varepsilon'' \in R$ egységgel. Mivel R Gauss-gyűrű, kapjuk az állítást.

Schönemann–Eisenstein tétel

Ha az R Gauss-gyűrű feletti legalább elsőfokú f primitív polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a főegyütthatónak de osztója minden más együtthatónak, p^2 viszont nem osztója a konstans tagnak, akkor f irreducibilis.
Hasonlóan, ha az R Gauss-gyűrű feletti legalább elsőfokú f polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a konstans tagnak de osztója minden más együtthatónak, p^2 viszont nem osztója a főgyütthatónak, akkor f irreducibilis.

Bizonyítás

Az első esetre végezzük el a bizonyítást, a másik eset bizonyítása hasonló.

Tegyük fel, hogy $f = gh$.
Mivel p nem osztja az f főegyütthatóját,
sem a g, sem a h főgyütthatóját nem osztja.

Bizonyítás folytatása

Legyen m a legkisebb olyan index, amelyre $p \nmid g_m$ és legyen n a legkisebb olyan index, amelyre $p \nmid h_n$. Ha $k = m + n$, akkor

$$p \nmid f_k = \sum_{i+j=k} h_i g_j,$$

mivel p osztja a jobb oldalon álló összeg minden tagját, kivéve azt a tagot, amelyben $i = m$ és $j = n$.
Igy $m + n = \deg(f)$, ahonnan $m = \deg(g)$ és $n = \deg(h)$.
Viszont az m és a n nem lehetnek egyszerre pozitívak,
mert különben $p^2 \mid f_0 = h_0 g_0$ teljesülne.
Igy az egyik polinom konstans.
Ha nem lenne egység, akkor f nem lenne primitív.

Következmény

Ha p prímelem, $n \in \mathbb{N}^+$, akkor $f = x^n + p$ irreducibilis R és (a Gauss-tétel miatt) a hányadosteste felett.

Speciálisan, ha p prímszám, akkor $x^n + p$ irreducubilis $\mathbb{Z}$ és $\mathbb{Q}$ felett.

Megjegyzés

(1) Ha R test, a Schönemann-Eisentein-tétel nyilván nem alkalmazható irreducibilis polinomok konstruálására, hiszen ekkor R-ben nincs olyan elem, amely nem nulla és nem egység, így nincsenek prímek.

Néha az irreducibilitás bizonyításához a Schönemann–Eisenstein tétel nem alkalmazható közvetlenül, csak némi kerülővel. Például a

$$\sum_{j=0}^{n-1} x^j = \frac{x^n - 1}{x - 1} \in \mathbb{Z}[x]$$

polinomok nem irreducibilisek, ha n összetett szám, mert ha $n = km$, akkor

$$\sum_{j=0}^{n-1} x^j = \left(\sum_{j=0}^{k-1} x^{mj}\right)\left(\sum_{j=0}^{m-1} x^j\right).$$

Ha viszont n prímszám, akkor a fenti polinom irreducibilis.

Ennek bizonyításához vegyük észre, hogy ha a polinom felbontható lenne, akkor x helyére $x+1$-et írva, az így kapott polinom is az lenne, de ez

$$\frac{\sum_{j=0}^{n}\binom{n}{j}x^j - 1}{x} = \sum_{j=0}^{n-1}\binom{n}{j+1}x^j$$

amire már alkalmazható a Schönemann–Eisenstein tétel, mert ha n prím, akkor

$$\binom{n}{j+1}$$

többszöröse, n-nek, ha $n-1 > j \geq 0$, egyenlő n-nel, ha $j = 0$, és 1, ha $j = n-1$.

Lagrange-interpoláció

A polinomok osztására vonatkozó tétel következményei között láttuk, hogy ha R egy egységelemes integritási tartománynak $c_0, c_1, \ldots, c_n$ különböző elemei, $d_0, d_1, \ldots, d_n$ pedig tetszőleges elemei R-nek,
akkor legfeljebb egy olyan legfeljebb n-ed fokú f polinom (ideértve a nulla polinomot is) létezik, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \ldots, n$.

Ha R test, akkor mindíg létezik is ilyen polinom, és az alábbi *Lagrange interpolációs eljárás*sal megkapható.
Legyen

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

a j-edik *Lagrange interpolációs alappolinom* és legyen $f = \sum_{j=0}^{n} d_j l_j$.

Titokmegosztás

A Lagrange-interpoláció titokmegosztásra is felhasználható.
Tegyük fel, hogy egy $t \in \mathbb{N}$ titkot n részre akarunk osztani úgy, hogy bármelyik m részből a titok visszaállítható legyen, de kevesebből semmi információt ne lehessen kapni a titokról.

Válasszunk egy, a t maximális lehetséges értéknél (és n-nél is) nagyobb p prímet és véletlen $a_1, a_2, \dots a_{m-1} \in \mathbb{Z}_p$ együtthatókat, majd számítsuk ki a $\mathbb{Z}_p$ feletti $t + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1}$ polinom $y_1, y_2, \dots y_n$ értékeit az $1, 2, \dots n$ helyeken.
Ezek a titokrészek: bármelyik m titokrészből a polinom megkapható Lagrange-interpolációval, így a titok adódik, de kevesebb részből nem.

Kronecker-eljárás

Ha R egy (végtelen) Gauss-gyűrű, amelyben rendelkezésünkre áll egy eljárás,
amellyel akármelyik elem osztóit meg tudjuk határozni,
valamint vannak eljárások a műveletek végzésére (például, ha $R = \mathbb{Z}$),
akkor egy $f \in R[x]$ polinomnak meghatározhatjuk az irreducibilis faktorait.

Ha $f = gh$, akkor bármely $c \in R$-re $f(c) = g(c)h(c)$, így $g(c)|f(c)$.

Legyen K az R hányadosteste.

Bármely $n \in \mathbb{N}$-re választva különböző $c_0, c_1, \ldots, c_n$ elemeket R-ben,
bármely $d_j|f(c_j)$, $j = 0, 1, \ldots, n$ értékekhez
Lagrange-interpolációval meghatározhatjuk azt az egyetlen $g \in K[x]$ polinomot,

amelyre $\deg(g) \leq n$ és $g(c_j) = d_j$,
azaz $g(c_j)|f(c_j)$ $j = 0, 1, \ldots, n$.

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

(Néha érdemes az osztás előtt ellenőrizni még néhány $c \in R$-re, hogy $g(c)|f(c)$ teljesül-e.

Azt is megnézhetjük, hogy g főegyütthatója osztja-e f főegyötthatóját,
bár ezt az osztási algoritmus az első lépésben ellenőrzi.)

Ha $n = 0$-val indulunk és egyesével növeljük n-et, akkor csak irreducibilis polinomosztókat fogunk találni
(mert egy reducibilis, legalább elsőfokú osztó irreducibilis tényezőit előbb megtaláljuk).

Ha $n \leq \lfloor \deg(f)/2 \rfloor$-ig nem találtunk osztót, akkor f irreducibilis.

Az elsőfokú faktorok megadják az K-beli és
ezáltal R-beli gyököket.

(Sok gyűrűben a faktorizálásra, mind az irreducibilitás bizonyítására sokkal hatékonyabb eljárások is léteznek.)

Cardano-képlet

Keressünk gyökképletet kettőnél magasabb fokú komplex együtthatós polinomok gyökeinek meghatározására.

A főegyütthatóval végigosztva, feltehetjük, hogy az 1.

Ha $y^n + f_1 y^{n-1} + f_2 y^{n-2} + \cdots + f_n = 0$,
akkor $y = x - f/n$ (invertálható) helyettesítéssel az egyenlet
$x^n + g_2 x^{n-2} + g_3 x^{n-3} + \cdots + g_n = 0$ alakú lesz,
így elég azt az esetet vizsgálni, amikor a második legmagasabb fokú tag nulla.

A másodfokú esetben a helyettesítés után a megoldás triviális.

A harmadfokú esetben az $x^3 + px + q = 0$ egyenlet megoldásait keressük $x = u + v$ alakban.

Mivel $x^3 = (u+v)^3 = u^3 + v^3 + 3uv(u+v)$,
azaz $x^3 - 3uvx - (u^3 + v^3) = 0$,

ha sikerül u-t és v-t úgy választani, hogy $uv = -p/3$ és $u^3 + v^3 = -q$ teljesüljön, akkor készen vagyunk.

Az első egyenletből $u^3 v^3 = -p^3/27$, így u^3 és v^3 a $z^2 + qz - p^3/27$ másodfokú egyenlet, az úgynevezett *karakterisztikus egyenlet* gyökei, például

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Így végül is a megoldásokat a

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Cardano-képlet adja, ahol a kilenc lehetséges köbgyök párból azt a hármat kell választani, amelyeknek szorzata $-p/3$.

Egyszerű számolás mutatja, hogy ezek valóban megadják $x^3 + px + q$ gyöktényezős felbontását.

A negyedfokú esetben az $x^4 + px^2 + qx + r = 0$ egyenlet bal oldalát az $\alpha \in \mathbb{C}$ paraméter bevezetésével átalakítva az egyenletet

$$\left(x^2 + \frac{p}{2} + \alpha\right)^2$$

$$-\left(2\alpha x^2 - qx + \left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right)\right) = 0$$

alakra hozhatjuk.
Ha sikerül az α paramétert úgy választani,
hogy a legnagyobb zárójelben álló másodfokú polinom x-nek teljes négyzet legyen,
akkor az egyenlet két másodfokú egyenletre esik szét, így megoldható.

Ehhez az kell, hogy a zárójelben álló másodfokú polinomnak egyetlen kétszeres gyöke legyen, azaz fenn kell állnia a

$$q^2 - 8\alpha\left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right) = 0$$

összefüggésnek.

Ezt a harmadfokú egyenletet megoldva, három alkalmas α értéket kapunk.

Magasabb fokú egyenletre nem adható hasonló gyökképlet.

Ha $n \geq 5$, akkor még olyan egész együtthatós n-ed fokú polinom is létezik,
amelynek gyökei nem írhatók fel racionális számok, a négy alapművelet és gyökvonások segítségével, azaz még "saját gyökképlete" sincs, ilyen például $x^5 - 4x + 2$.

Az első ilyen jellegű eredmény Abeltől származik,
aki ezzel a problémával kapcsolatban kezdte el vizsgálni csoportok kommutativitását.

A kérdéskört Galois tisztázta teljesen, aki megmutatta,
hogy az egyenlet négy alapművelettel és gyökjelekkel való megoldhatósága attól függ,
hogy a gyökök bizonyos permutációiból alkotott csoport, az egyenlet Galois-csoportja feloldható-e.

Speciális esetekben tehát sikerülhet meghatározni a gyököket, például sokszor segít egy új változó bevezetése $y = h(x)$ alakban, ahol h polinom; ez *Tschirnhaus-transzformáció*.

Racionális törtfüggvények

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

Parciális törtekre bontás

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

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

polinomok, amelyekkel

Állítás folytatása

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

A tételt az integrálásnál használjuk $\mathbb{R}$ illetve $\mathbb{C}$ feletti polinomokra.

Bizonyítás

Teljes indukcióval bizonyítunk.

Ha $n = 1$, az állítás nyilvánvaló.

Ha $n = 2$, akkor a kiterjesztett euklideszi algoritmussal kaphatunk olyan f_1, f_2 polinomokat,
amelyekre $f_1 g_2 + f_2 g_1 = 1$, amit $g_1 g_2$-vel osztva kapjuk az állítást.

Végül az általános eset úgy következik, hogy
a $g_1, g_2, \ldots, g_{n-2}, g_{n-1} g_n$ polinomokra alkalmazva az indukciós feltevést, kapunk egy

$$\frac{1}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \cdots + \frac{f_{n-2}}{g_{n-2}} + \frac{f^*}{g_{n-1}g_n}$$

előállítást, majd a $n = 2$ speciális esetből kapott

$$\frac{1}{g_{n-1}g_n} = \frac{f^*_{n-1}}{g_{n-1}} + \frac{f^*_n}{g_n}$$

előállítás mindkét oldalát szorozzuk f^*-al, és ezt írjuk az utolsó tag helyére.

Következmény

Ha $h \in K[x]$, akkor léteznek olan $h_j \in K[x]$

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

Bizonyítás

Szorozzuk a tételben kapott előállítás mindkét oldalát h-el.

Következmény

Az előző következményben kapott előállítás felírható

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

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

Bizonyítás

Minden tagban osszuk maradékosan a számlálót a nevezővel.

Megjegyzés

Ha a $g_1, g_2, \ldots, g_n$ polinomokat a g-nek irreducibilis polinomok szorzataként történő előállításával kaptuk,
akkor az előző következményben szereplő törtek u/v^k alakúak és $\deg(u) < \deg(v^k)$.

Ezek a törtek felírhatók

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

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

Ez $k = 1$ esetén nyilvánvaló,
egyébként pedig indukcióval következik, ha u-t maradékosan osztjuk v-vel,
majd mindkét oldalt végigosztjuk v^k-val.

Többhatározatlanú polinomok

Legyen R gyűrű, $n \in \mathbb{N}$. Az R feletti n határozatlanú *polinom*ok gyűrűjét n szerinti indukcióval definiáljuk:
ha $n = 0$, legyen $R[x_1, x_2, \ldots, x_n] = R$, az egy határozatlanú polinomok gyűrűjét már definiáltuk,
ha pedig $n > 1$, akkor legyen

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

azaz az n határozatlanú polinomok olyan polinomjai x_n-nek, amelynek együtthatói az $x_1, x_2, \ldots x_{n-1}$ határozatlanok polinomjai.

Az $x_1, x_2, \ldots, x_n$ helyett bármilyen más betűk is szerepelhetnek.

Néha egy $f \in R[x_1, x_2, \ldots, x_n]$ polinomra inkább az $f(x_1, x_2, \ldots, x_n)$ jelölést fogjuk használni.

A rekurziv definíció miatt, azok a tulajdonságok, amelyek öröklődnek a gyűrűről a polinomgyűrűre, többhatározatlanú polinomok gyűrűjére is öröklődnek.

Az *n határozatlanú polinomok*

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

alakú véges összegek, ahol $x_1, x_2, \ldots, x_n$ a „*határozatlan*ok” és $f_{i_1,i_2,\ldots,i_n} \in R$.
Az $a \in R$ elemhez hozzárendelve azt a polinomot,
amelyre $f_{0,0,\ldots 0} = a$ és $f_{i_1,i_2,\ldots i_n} = 0$ egyébként az R egy olyan leképezését kapjuk a polinomok gyűrűjébe,
amely monomorfizmus, értékkészletének elemei a *konstans polinomok*, ezeket R elemeivel azonosíthatjuk. Az

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

tagot *monomok*nak nevezzük,

$$f_{i_1,i_2,\ldots i_n}$$

az *együtthatója*, $(i_1, i_2, \ldots i_n)$ a *multifoka*, $i_1 + i_2 + \cdots + i_n$ pedig a *foka*.

Az n-határozatlanú polinomok jelölésére a hagyományos

$$f = \sum_{i_1+\cdots+i_n \le m} f_i x^i = \sum_{i_1+i_2+\cdots+i_n \le m} f_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

felírást fogjuk használni.

Gyakran az x_j^0 alakú tényezőket nem írjuk ki, x_j^1 helyett pedig x_j-t írunk.

Az (egyetlen) nulladfokú tag együtthatója a polinom *konstans* tagja.

Mivel ebből a felírásból a nulla együtthatójú tagokat szokás elhagyni,
illetve a felíráshoz további nulla együtthatójú tagok adhatók hozzá, a felírás nem egyértelmű.

Egyértelművé válik azonban, ha kikötjük, hogy m minimális legyen, és
minden m-nél nem magasabb fokú tag -egyszer- szerepeljen.

Ez a minmimális m a polinom *foka*, jelölése $\deg(f)$.

(Egy másik lehetőség a felírás egyértelművé tételére, hogy minden nulla együtthatójú tagot elhagyunk.)

A nulla polinom egyértelmű felírása az üres összeg és fokát $-\infty$-nek definiáljuk.

A konstans polinomok a legfeljebb nulladfokú polinomok.

A legfeljebb elsőfokú polinomok a *lineáris polinom*ok.

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

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

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

egy másik polinom, akkor összegük az

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

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

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

- f legfeljebb m-ed fokú, g legfeljebb l-ed fokú, akkor h legfeljebb $m+l$-edfokú.

Ha az R gyűrű nullosztómentes, akkor az $R[x_1, x_2, \ldots x_n]$ gyűrű is nullosztómentes és két polinom szorzatának a foka a fokok összege.

Ha R egységelemes 1 egységelemmel, akkor $R[x_1, \ldots, x_n]$ is egységelemes, benne az $f_{0,0,\ldots,0} = 1$ és egyébként $f_{i_1,i_2,\ldots,i_n} = 0$ összefüggéssel definiált polinom egységelem.

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

tag szokásos írásmódja $f_{i_1,i_2,\ldots,i_n} = 1$ esetén

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Számítógépen vagy az m fokszámot és az együtthatók $f_{i_1,i_2,\ldots,i_n}$, $i_j \leq m$, ha $j = 1, 2, \ldots, n$ tömbjét tároljuk, vagy a nem nulla együtthatókra az

$$((i_1, i_2 \dots i_n), f_{i_1,i_2,\dots i_n})$$

párok egy láncolt listáját.

Multiindexek

Többhatározatlanú polinomok felírása tömörebbé tehető az alábbi módon:

az $\mathbb{N}^n$ elemeit általában *multiindexek*nek fogjuk nevezni.

Multiindexek összegét koordinátánként definiáljuk.

Ha $i = (i_1, i_2, \dots i_n)$, akkor legyen $|i| = i_1 + i_2 + \dots + i_n$ és $x^i = x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$.

Ezzel a jelöléssel az f polinom $\sum_{|i| \leq m} f_i x^i$ véges összegként írható.

(Tulajdonképpen f egy olyan $\mathbb{N}^n$-et R-be képező függvénnyel azonosítható, amely véges sok helyen vesz fel nem nulla értéket.)

Az $f_i x^i$ monom multifoka i, foka $|i|$.

Ha $f = \sum_i f_i x^i$ és $g = \sum_i g_i x^i$ polinomok, akkor összegük a $\sum_i (f_i + g_i) x^i$ polinom, szorzatuk pedig az a $h = fg$ polinom, amelyre $h_k = \sum_{i,j \in \mathbb{N}^n, i+j=k} f_i g_j$, ha $k \in \mathbb{N}^n$.

Formális hatványsorok

Ha R egy gyűrű, akkor az R feletti n határozatlanú *formális hatványsorok* $R[\![x_1, x_2, \ldots, x_n]\!]$ gyűrűjét mint $R[\![x_1, x_2, \ldots, x_{n-1}]\!][\![x_n]\!]$-et definiáljuk (az $n = 0$ esetben legyen $R[\![x_1, x_2, \ldots, x_n]\!] = R$), elemeit $\sum_{i \in \mathbb{N}^n} f_i x^i$ alakban írjuk.

Tétel

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

Bizonyítás

Gauss tételének felhasználásával teljes indukcióval következik, mivel

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

Megjegyzés

Ha $n > 1$, akkor $R[x_1, x_2, \dots x_n]$ nem tehető euklideszi gyűrűvé, még akkor sem, ha R test, mert 1 az x_1 és x_2 polinomok legnagyobb közös osztója, de semilyen $p_1(x_1, x_2)$, $p_2(x_1, x_2)$ polinomokkal nem áll elő $x_1 p_1(x_1, x_2) + x_2 p_2(x_1, x_2)$ alakban, mert mindkét szorzat konstans tagja nulla.

Szimmetrikus polinomok

Legyen R egységelemes integritási tartomány. Az $f \in R[x_1, x_2, \dots, x_n]$ polinomot *szimmetrikus polinom*nak nevezzük, ha a határozatlanok tetszőleges permutációjára ugyanaz marad, azaz ha bármely $\sigma \in S_n$-re

$$f(x_{\sigma_1}, x_{\sigma_2}, \dots, x_{\sigma_n}) = f(x_1, x_2, \dots, x_n).$$

Tekintsük az

$$f = (z - x_1)(z - x_2) \cdots (z - x_n) \in R[x_1, x_2, \dots, x_n, z]$$

polinomot.

Ezt $z^n - s_1 z^{n-1} + s_2 z^{n-2} - \cdots + (-1)^n s_n$ alakba írva,
$s_1, s_2, \ldots, s_n$ az $x_1, x_2, \ldots, x_n$ változóknak nyilván szimmetrikus polinomjai,

$$s_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

alakba írhatók; ezek elemei *elemi szimmetrikus polinom*ok.
Az s_k egy k-ad fokú homogén polinom.
Más szimmetrikus polinomok például a

$$\sigma_k = \sum_{i=1}^{n} x_i^k \quad k = 0, 1, \ldots$$

*hatványösszeg*ek.
Egy $f_i x^i \in R[x_1, x_2, \ldots, x_n]$ nem nulla monom *súly*án az $i_1 + 2i_2 + 3i_3 + \cdots + ni_n$ természetes számot értjük,
ez függ a határozatlanok sorrendjétől is.

Az $f \neq 0$ polinom *súly*án a benne nem nulla együtthatóval fellépő $f_i x^i$ monomok súlyainak maximumát értjük;
a nulla polinom súlya $-\infty$.

Szimmetrikus polinomok alaptétele

Az R egységelemes integritási tartomány feletti minden $f \in R[x_1, x_2, \ldots, x_n]$ szimmetrikus polinomhoz található olyan egyértelműen meghatározott $F \in R[y_1, y_2, \ldots, y_n]$ polinom, amelyre

$$f(x_1, \ldots, x_n) = F\big(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)\big),$$

ahol $s_1, s_2, \ldots, s_n$ az $x_1, x_2, \ldots, x_n$ határozatlanok elemi szimmetrikus polinomjai. Ha f fokszáma d, akkor F súlya is d.

Bizonyítás

Az előállítás létezését n szerinti teljes indukcióval bizonyítjuk.

Ha $n = 1$, az előállítás nyilván teljesül.

Ha $n - 1$-re teljesül az előállítás, akkor n-re ugyanezt d szerinti teljes indukcióval bizonyítjuk.

Ha f konstans polinom azaz $d \leq 0$, akkor ez triviális.

Tegyük fel, hogy az előállítás minden d-nél alacsonyabb fokú polinomra létezik.

Legyen $f(x_1, \ldots, x_n)$ foka d.

Ekkor van olyan $F^*(y_1, \ldots, y_{n-1})$ polinom,
amelynek súlya nem nagyobb mint d, és amelyre

$$f(x_1, \ldots, x_{n-1}, 0) = F^*(s_1^*, s_2^*, \ldots, s_{n-1}^*),$$

ahol $s_1^*, s_2^*, \ldots, s_{n-1}^*$ az $x_1, x_2, \ldots, x_{n-1}$ határozatlanok elemi szimmetrikus polinomjai.

Mivel definíció szerint

$$(z - x_1) \cdots (z - x_{n-1}) = z^{n-1} - s_1^* z^{n-2} + \cdots + (-1)^{n-1} s_{n-1}^*,$$

az összefüggést z-vel szorozva

$$(z - x_1) \cdots (z - x_{n-1}) z = z^n - s_1^* z^{n-1} + \cdots + (-1)^{n-1} s_{n-1}^* z,$$

azaz az s_j^* polinomok úgy állnak elő a megfelelő
$s_j \in R[x_1, \ldots, x_n]$ elemi szimmetrikus polinomokból,
hogy x_n helyére nullát írunk.

Megmutatjuk, hogy $F^*(s_1, \ldots, s_{n-1})$ foka $x_1, \ldots, x_n$-ben legfeljebb d.

Ugyanis $F^*(y_1, \ldots, y_{n-1})$-ben csak olyan $F^*_{i_1,\ldots,i_{n-1}} y_1^{i_1} \cdots y_{n-1}^{i_{n-1}}$ monomok léphetnek fel, amelyekre $i_1 + 2i_2 + \cdots + (n-1)i_{n-1} \leq d$.

Az $y_i \leftarrow s_i$ helyettesítés során ez a monom az

$$F^*_{i_1,\ldots,i_{n-1}} s_1^{i_1} s_2^{i_2} \cdots s_{n-1}^{i_{n-1}}$$

polinomba megy át, ami, figyelembe véve, hogy s_j foka j, az $x_1, \ldots, x_n$ határozatlanoknak legfeljebb d-ed fokú polinomja.

Tekintsük most az

$$f^*(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - F^*(s_1, \ldots, s_{n-1})$$

legfeljebb d-ed fokú polinomot.

Ez az $x_1, \ldots, x_n$ határozatlanok szimmetrikus polinomja, mert a különbség első tagja szimmetrikus polinom, a második tagja pedig szimmetrikus polinomok polinomja, így szintén szimmetrikus polinom.

Fennáll továbbá, hogy $f^*(x_1, \ldots, x_{n-1}, 0) = 0$, így x_n osztója $f^*(x_1, \ldots, x_n)$-nek, azaz f^*-nak nincsenek olyan tagjai, amelyekben x_n a nulladik hatványon szerepel.
Az f^* szimmetrikussága miatt tetszőleges j-re $f^*(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n) = 0$ is fennáll.

Innen az következik, hogy f^* minden tagjában x_j legalább az első hatványon szerepel.

Tehát $s_n = x_1 \cdots x_n$ osztója az f^* polinomnak:

$$f^*(x_1, \ldots, x_n) = s_n f^{**}(x_1, \ldots, x_n),$$

ahol f^{**} szimmetrikus polinom és foka legfeljebb $d - n < d$.

Indukciós feltevésünk szerint van olyan legfeljebb $d - n$ súlyú $F^{**}(y_1, \ldots, y_n)$ polinom, amelyre

$$f^{**}(x_1, \ldots, x_n) = F^{**}(s_1, \ldots, s_n).$$

tehát

$$f^*(x_1, \ldots, x_n) = s_n F^{**}(x_1, \ldots, x_n),$$

Innen

$$f(x_1, \ldots, x_n) = F^*(s_1, \ldots, s_n) + s_n F^{**}(s_1, \ldots, s_n),$$

és a jobb oldalon álló mindkét tag, tehát összegük is,
legfeljebb d súlyú $x_1, \ldots, x_n$-ben. Igy

$$F(x_1, \ldots, x_n) = F^*(s_1, \ldots, s_n) + s_n F^{**}(s_1, \ldots, s_n)$$

választható.

Indukcióval megmutatjuk, hogy az elemi szimmetrikus polinomok algebrailag függetlenek R felett,
ami azt jelenti, hogy tetszőleges $F(y_1, \ldots, y_n)$ nem nulla polinomra $F(s_1, \ldots, s_n) \in R[x_1, \ldots, x_n]$ nem nulla polinom.

Ha két előállítás különbségére alkalmazzuk,
akkor ebből azonnal következik a tételben szereplő előállítás egyértelműsége.

Ha $s_1, \ldots, s_n$ nem lennének algebrailag függetlenek,
akkor létezne egy minimális fokszámú $F(y_1, y_2, \ldots, y_n)$ polinom,
amelyre

$$F(s_1, \ldots, s_n) = 0.$$

Tekinsük F-et mind $R[y_1, \ldots, y_{n-1}][y_n]$ elemét, legyen

$$F(y_1, \ldots, y_n) = F_0(y_1, \ldots, y_{n-1}) + F_1(y_1, \ldots, y_{n-1})y_n +$$
$$\cdots + F_d(y_1, \ldots, y_{n-1})y_n^d.$$

Itt $F_0 \neq 0$, mert egyébként y_n osztója lenne F-nek, mondjuk

$$F(y_1, \ldots, y_n) = y_n G(y_1, \ldots, y_n)$$

következne, amiből viszont

$$F(s_1, \ldots, s_n) = s_n G(s_1, \ldots, s_n)$$

és így $G(s_1, \ldots, s_n) = 0$ következne.

Mivel $G(y_1, \ldots y_n)$ foka kisebb $F(y_1, \ldots y_n)$ fokánál,
ez ellentmond F minimalitásának.

Az $y_j \leftarrow s_j$ helyettesítés után

$$F(s_1, \ldots, s_n) = F_0(s_1, \ldots, s_{n-1}) + F_1(s_1, \ldots, s_{n-1})s_n + \cdots$$
$$+F_d(s_1, \ldots, s_{n-1})s_n^d.$$

Tekintsük ezt, mint $x_1, \ldots, x_n$ polinomját, és vegyük az $x_n = 0$ helyen.

Mivel ekkor $s_n = 0$, azt kapjuk, hogy

$$0 = F_0(s_1^*, \ldots, s_{n-1}^*).$$

Mivel $F_0 \neq 0$ nem triviális összefüggést találtunk $x_1, x_2, \ldots, x_{n-1}$ elemi szimmetrikus polinomjai, azaz $s_1^*, \ldots, s_{n-1}^*$ között, ami ellentmond indukciós feltevésünknek.

Newton képletei

Ha az R egyységelemes integritási tartomány felett az $x_1, x_2, \ldots, x_n$ határozatlanok elemi szimmetrikus polinomjai $s_1, s_2, \ldots, s_n$ és σ_i, $i = 1, 2, \ldots$ a megfelelő hatványösszegek, akkor fennállnak a

$$\begin{aligned}
\sigma_1 - s_1 &= 0, \\
\sigma_2 - s_1\sigma_1 + 2s_2 &= 0, \\
&\vdots \\
\sigma_{n-1} - s_1\sigma_{n-2} + \cdots & \\
+(-1)^{n-2}s_{n-2}\sigma_1 + (-1)^{n-1}(n-1)s_{n-1} &= 0,
\end{aligned}$$

és

$$\sigma_{k+n} - s_1\sigma_{k+n-1} + \cdots + (-1)^n s_n \sigma_k = 0 \quad (k = 0, 1, \dots)$$

egyenletek.

Bizonyítás

Tekintsük az

$$f(z) \quad = (z - x_1)\cdots(z - x_n) = z^n + a_1 z^{n-1} + \cdots + a_n,$$
$$a_k = (-1)^k s_k$$

polinomot. Mivel $f(x_i) = 0$ $(i = 1, 2, \dots, n)$,

$$\sum_{i=1}^{n} x_i^k f(x_i) = 0, \quad \text{ha} \quad k \geq 0.$$

Ez azt jelenti, hogy

$$\sum_{i=1}^{n} \left(x_i^{k+n} + a_1 x_i^{k+n-1} + \cdots + a_n x_i^k \right) =$$

$$= \sigma_{k+n} + a_1\sigma_{k+n-1} + \cdots + a_n\sigma_k = 0,$$

tehát a tételben az utolsó egyenletek $(k = 0, 1, 2 \dots)$ fennállnak.

Legyen $h_i(z) = \prod_{j \neq i}(z - x_j)$. Ekkor

$$f(z) = (z - x_i)h_i(z).$$

Másrész, felhasználva hogy

$$z^j - x_i^j = (z - x_i)\left(z^{j-1} + z^{j-2}x_i + \cdots + zx_i^{j-2} + x_i^{j-1}\right),$$

és hogy $f(x_i) = 0$, ha a_0 a gyűrű egységeleme, azt kapjuk hogy

$$\begin{aligned} f(z) &= f(z) - f(x_i) \\ &= (a_n - a_n) + a_{n-1}(z - x_i) + \cdots + a_0(z^n - x_i^n) \\ &= (z - x_i)\sum_{k=0}^{n-1} a_k \sum_{j=0}^{n-k-1} x_i^j z^{n-k-j-1}. \end{aligned}$$

Innen $h_i(z)$ a jobb oldalon $z - x_i$ utáni részre.
Ezt, valamint a szorzat differenciálási szabályából adódó $f'(z) = \sum_{i=1}^{n} h_i(z)$ összefüggést felhasználva

$$f'(z) = \sum_{i=1}^{n} h_i(z) = \sum_{i=1}^{n}\sum_{k=0}^{n-1} a_k \sum_{j=0}^{n-k-1} x_i^j z^{n-k-j-1}$$

$$= \sum_{k=0}^{n-1} \sum_{j=0}^{n-k-1} \sum_{i=1}^{n} a_k x_i^j z^{n-k-j-1}$$

$$= \sum_{t=0}^{n-1} z^{n-t-1} \sum_{j+k=t} a_k \sum_{i=1}^{n} x_i^j$$

$$= \sum_{t=0}^{n-1} \left(\sum_{k+j=t} a_k \sigma_j \right) z^{n-i-1},$$

ahol $\sigma_0 = na_0$.

Mivel másrészt $f'(z) = \sum_{t=0}^{n-1} (n-t) a_t z^{n-t-1}$, az együtthatók összehasonlításával

$$(n-t)a_t = \sum_{k+j=t} a_k \sigma_j, \quad i = 1, \ldots, n-1.$$

Ez a tételben szereplő első $n-1$ egyenlet.

Kommunikáció és kódolás

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

Az információ átvitele térben történik.

Valójában minden információátvitel térben és időben történik, és egyes esetekben az egyik, míg más esetekben a másik dimenzió domináns.

Ha telefonálunk, akkor a távolság a fontosabb, ugyanakkor az információ adathordozókra való rögzítése és egy későbbi időpontban való visszaolvasása esetén a helyváltozás kevésbé fontos.

A továbbiakban általában úgy beszélünk az adatátvitelről, mintha az térben történne, de ebbe mindíg beleértjük az időbeliséget is.

A modellel kapcsolatban felmerül néhány kérdés:

(1) mi az információ és hogyan mérhető az információ;
(2) hogyan történik az információ átvitele;
(3) milyen kapcsolat van az elküldött és a vett adat között.

Információ, bit, entrópia

Az információról mindenkinek van valamilyen intuitív fogalma.

A nagyszámú definíció közül itt azt említjük meg, amely szerint az *információ* új ismeret.

Az információt Shannon nyomán az általa megszüntetett bizonytalansággal mérjük.

Gyakoriság, relatív gyakoriság, eloszlás

Tegyük fel, hogy egy információforrás nagy számú, összesen n üzenetet bocsát ki.
Az összes ténylegesen előforduló különböző üzenet legyen $a_1, a_2, \dots a_m$ $(m \in \mathbb{N}^+)$.
Ha az a_i üzenet k_i-szer fordul elő, akkor azt mondjuk, hogy *gyakorisága* k_i, *relatív gyakorisága* pedig $p_i = k_i/n > 0$.
A $p_1, p_2, \dots p_m$ szám-m-est az üzenetek *eloszlásának* nevezzük.
Nyilván $\sum_{i=1}^{m} p_i = 1$.

Üzenet információtartalma

Az a_i üzenet egyedi *információtartalmának* célszerű definíciója $I_i = -\log_r p_i$, ahol r egy 1-nél nagyobb valós szám.
A logaritmus alapja az információ egységét határozza meg.
Amennyiben az alap 2, akkor az információ egysége a *bit*, és ilyenkor $\log_r p_i$ helyett egyszerűen $\log p_i$-t írunk.

Többnyire nem az egyes üzenetek egyedi információtartalma, hanem az üzenetforrás által kibocsátott üzenetek

Entrópia

$H_r(p_1 \dots p_m) = -\sum_{i=1}^{m} p_i \log_r p_i$ *átlagos információ tartalma*
érdekes, ez a *forrás entrópiája*,
amely csak az üzenetek eloszlásától függ, de tartalmuktól nem.
Általánosabban, egy m tagú *eloszlás* egy pozitív valós számokból álló $p_1, p_2, \dots p_m$ sorozat, amekyre $\sum_{i=1}^{m} p_i = 1$.
Az *eloszlás entrópiáját* a

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

összefüggéssel értelmezzük.

A fogalom nem csak a kódolásnál hasznos, hanem például bináris kereséseknél is.

(Van összefüggés a fizikai értelemben vett entrópiával is.)

Segédtétel

Legyen $p_1, \dots p_m$ egy eloszlás. Egy $I \subset \mathbb{R}$ intervallumon szigorúan konvex $f : I \to \mathbb{R}$ függvényre az

$$f\left(\sum_{i=1}^{m} p_i q_i\right) \leq \sum_{i=1}^{m} p_i f(q_i), \quad \text{ha} \quad q_1 \dots q_m \in I$$

Jensen-egyenlőtlenség teljesül és egyenlőség pontosan akkor áll fenn, ha $q_1 = q_2 = \dots = q_m$.

Bizonyítás

Ha $m = 1$, akkor nincs mit bizonyítani.

Az $m = 2$ esetben az állítás a szigorú konvexitás definíciója.

Indukcióval, legyen $p = \sum_{i=1}^{m} p_i$.
Ekkor $p + p_{m+1} = 1$ és így

$$\sum_{i=1}^{m+1} p_i f(q_i) = p \sum_{i=1}^{m} \frac{p_i}{p} f(q_i) + p_{m+1} f(q_{m+1})$$

$$\geq pf\left(\sum_{i=1}^{m} p_i q_i/p\right) + p_{m+1} f(q_{m+1})$$

$$\geq f\left(\sum_{i=1}^{m+1} p_i q_i\right),$$

valamint az egyenlőségek pontosan akkor teljesülnek, ha $q_1 = q_2 = \cdots = q_m$ és $q_{m+1} = \sum_{i=1}^{m} p_i q_i/p = q_m$.

Tétel

Bármilyen eloszláshoz tartozó entrópiára

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

és egyenlőség pontosan akkor teljesül,
ha $p_1 = p_2 = \cdots = p_m = 1/m$.
Az m elemű eloszlás átlagos információtartalmának maximuma tehát $\log m$ bit.

Bizonyítás

Mivel $-\log_r$ szigorúan konvex függvény,

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

$$\geq -\log_r \left(\sum_{i=1}^{m} p_i / p_i \right) = -\log_r m.$$

Kódolás

A következő két kérdést együtt tárgyaljuk. Ahhoz, hogy az adatot továbbítani tudjuk, először is olyan alakra kell hozni, hogy képesek legyünk a céljainknak megfelelően kezelni.

A *kódolás* a legáltalánosabb értelemben az üzenetek halmazának egy másik halmazba való *leképezését* jelenti.

Ha a leképezés injektív, akkor azt mondjuk, hogy a kódolás *felbontható* vagy *egyértelműen dekódolható*, egyébként *veszteséges*, mert információvesztéssel jár.

Gyakran az üzenetet valamilyen karakterkészlet elemeiből alkotott sorozattal adjuk meg.

Ez az eljárás is egy kódolás, ilyen például az írás.

Kódolás tehát a kínai írás, a japán írás az óegyiptomi írás és hasonlóan kódolás a latin betűs írás is.

Minden esetben arról van szó, hogy egy kódolandó üzenetet meghatározott módon felbontunk egymáshoz csatlakozó, előre rögzített olyan elemi részekre
- nem teljesen pontosan fogalmazva rendre "szavakra", "szótagokra", "fogalmakra", "hangokra" -,
hogy minden üzenet előálljon ilyen elemi részek egymás után fűzésével, de egyetlen üzenetet se lehessen kétféleképpen felbontani ezekre az elemi résszekre, "betűkre".

Az ilyen részeknek megadjuk a kódját és a teljes üzenetet úgy kódoljuk, hogy az elöbbi részek kódját egymás után írjuk.

A kódoláshoz tehát megadjuk az elemi részek kódját, amelyet egy szótár tartalmaz és ezek segítségével kódoljuk az üzeneteket.

Az ilyen kódolást *betűnkénti kódolásnak* nevezzük (léteznek más kódok is).

A betűket gyakran számokká kódoljuk: jelenleg elterjedt az úgynevezett ASCII-kód, amellyel 128 különböző jel kódolható, illetve ennek a kódnak a kiterjesztései, amelyekkel 256 vagy 65536 jelet lehet kódolni.

Néha számokat akarunk betűkké kódolni (például ASCII fájlként küldhessük el):
egy módszer, hogy a 32....63 számokat változatlanul hagyjuk, a 0...31 számokhoz pedig hozzáadunk 64-et, majd az ASCII-kód szerinti betűt tekintjük.

A valóságban az egyes üzenetek különböző gyakorisággal fordulnak elő.

Ez a felismerés vezetett ahhoz a gondolathoz, hogy célszerű a gyakrabban előforduló üzeneteket rövidebb kóddal megadni.

Egy ilyen kódolás *tömörítést* végez, amelynek során csökkentjük az eredeti jelsorozatban meglévő *redundanciát*.

A redundancia, vagy más néven a terjengősség azt jelenti, hogy a mondandónkat lényegesen hosszabban fejezzük ki, mint amennyire az szükséges lenne.

Például a $\mathrm{nyilvánosság}$ szó 12 betűből áll, holott legfeljebb öt betű $(26^6 - 1)/25 = 12,356,631$ lehetőséget biztosít, így az összes magyar szó kódolására elég lenne.

Például a szót már a $\mathrm{nylvnssg}$ mássalhangzókból is kitalálhatjuk.

Elsőként említett kódolást nevezzük *üzenetkódolásnak*, míg a másodikat *gazdaságos kódolásnak*.

A két lépést együttesen *forráskódolásnak* nevezik.

A csatornán áthaladó jel torzulást szenved, így a vétel helyére nem pontosan az a jelsorozat érkezik, mint amit a csatorna bemenetére betápláltak.

Amennyiben bármilyen jelsorozat egy lehetséges üzenet, akkor a módosulást nem vesszük észre,
a vétel helyén semilyen módon nem tudjuk eldönteni egy vett jelsorozatról, hogy az megegyezik-e az eredetileg elküldött üzenettel,
vagy egy másik üzenet változott meg és így kaptuk a vett jelsorozatot.

A biztonságosabb átvitel érdekében úgynevezett *hibakorlátozó kódolást* végzünk a csatorna bementetén.

Ezzel a kódolással szándékosan viszünk redundanciát a kódolt üzenetbe.

Gondoljuk meg, hogy az élő nyelvek redundanciájának köszönhetően zajban is megértjük, amit egy előadó mond, jóllehet az általunk hallott hang nem azonos azzal, ami eredetileg elhangzott.

A megfelelő hibakorlátozó kód kiválasztása függ a csatornától is, ezért ezt a kódolást *csatornakódolásnak* nevezik.

Végezetül a kódolt üzenetet ténylegesen, fizikailag is át kell vinni a csatornán.

Az átvitelhez olyan alakra kell transzformálni az üzenetet, amely forma fizikailag alkalmas a nagy távolságra történő továbbításra.

Ilyen pédául, ha leírjuk az üzenetet és levél formájában küldjük el, vagy ha elektromos jellé alakítjuk át és például telefonvonalon keresztül továbbítjuk.

Ezt a berendezést most -kissé pontatlanul -*modemnek* fogjuk nevezni.

Bár a közvetlen témához nem szorosan kapcsolódik, ám mindenképpen a kommunikációval kapcsolatos a titkosság és a hitelesség kérdése,
vagyis az adatátvitel során, amennyiben szükséges gondoskodni kell az üzenet titkosításáról és hitelességéről is.

Az utóbbit például digitális aláírással lehet megvalósítani.

A titkosítást és hitelesítést a tömörítés után kell végezni, mert titkosított üzenet már nem tömöríthető.

Forráskódolás

Betűnkénti kódolás

Mint már említettük a betűnkénti kódolás során az eredeti üzenetet meghatározott módon egymáshoz átfedés nélkül csatlakozó részekre bontjuk,
egy-egy ilyen részt egy szótár alapján kódolunk és az így kapott kódokat az eredeti sorrendnek megfelelően egymáshoz láncoljuk.

(Feltesszük, hogy az üzenet véges és a végét érzékeljük.)

Az általánosság csorbítása nélkül feltehetjük, hogy a szótár alapján kódolandó elemi üzenetek egy *A abc* (*a kódolandó abc*) *betűi* és egy-egy ilyen betű kódja egy másik (az előbbitől nem feltétlenül különböző) *B abc*, a *kódoló abc* vagy *kódabc* betűivel felírt szó, vagyis ezen *abc*ből vett betűk véges hosszúságú sorozata a sorozat elemeit egyszerűen egymás mellé írva.

A továbbiakban mindkét *abc*ről feltesszük, hogy nem üres és véges.

Ha a B *abc* egyelemű, kételemű, háromelemű stb., akkor rendre unáris, bináris, ternáris, stb., kódról beszélünk.

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

Az előbbiek alapján a betűnkénti kódolást egy
$\varphi : A \to B^*$ leképezés határozza meg, amelyet természetes módon terjesztünk ki egy $\psi : A^* \to B^*$ leképezéssé:
ha $a_1, a_2, \ldots a_n = \alpha \in A^*$ (tehát $n \in \mathbb{N}$, és $a_i \in A$,
ha $1 \leq i \leq n$), akkor α kódja $\psi(\alpha) = \varphi(a_1)\varphi(a_2)\ldots\varphi(a_n)$;
$\mathrm{rng}(\psi)$ elemei a *kódszavak*.

Nyilván, ha φ nem injektív, vagy az üres szó benne van az értékkészletében,
akkor a kapott ψ kódolás nem injektív, azaz nem felbontható, ezért betűnkénti kódolásnál mindíg fel fogjuk tenni, hogy φ injektív és B^+-ba képez.

Példa

Tipikus példa betűnkénti kódolásra a *Morse-kód*.

Itt az angol *abc* (csak nagybetűkkel) a kódolandó *abc*, míg a kódoló *abc* két betűt tartalmaz, a pontot és a vonást (hang esetén "ti" és "tá")
és például az sms szó kódja "...- -...".

Az így adódó kódokat nem tudnánk dekódolni, mert nem injektív a megfeleltetés.

Például a vb szó kódja megegyezik az előbbi kóddal.

A valóságban természetesen az egyes jelek, továbbá az egyes betűk adása között meghatározott szünetet tartanak, és
így már a kódolás egyértelmű lesz:
konkrétan egy vonás háromszor olyan hosszú, mint egy pont,
és minden jel után egy egységnyi szünet következik,
majd a betű kódja végén még további két egységnyi szünet van
(egy pont átviteléhez szükséges időt tekintve egységnek).

Ha egy egységnyi hosszúságú jelet egy 1-es, és egy egységnyi hosszúságú szünetet egy 0 jelöl,
akkor pédául a B kódja, amely az eredeti ponttal és vonással megadott rendszerben "-...",
most 111010101000 lesz.

Ezzel a kiegészítéssel már egyértelműen dekódolható a vett üzenet, hiszen minden betű kódja három nullára végződik, és nincs olyan betű, amelynél a kódszó belsejében, vagy az elején lenne három nulla.

Ennél a kódnál a három nullának önmagában is van jelentése, ez a szóköz kódja, vagyis ez választja el egymástól az egymás után következő szavak kódját (így egy szó kódjának a végén hat darab nulla áll).

Ekkor sms kódja 10101000111011100010101000000
míg vb kódja 10101011100011101010100000
így a két kód jól megkülönböztethető és a kódolás egyértelműen megfejthető.

Prefix, szuffix, infix

Legyen α, β és γ az A abcvel felírt három szó.

Ekkor α *prefixe* (vagy *előtagja*) és

γ *szuffixe* (vagy utótagja) az $\alpha\gamma$ szónak,

β pedig *infixe* (vagy *belső tagja*) $\alpha\beta\gamma$-nak.

Szavak egy halmaza *prefixmentes* halmaz,
ha nincs benne két olyan különböző szó, hogy egyik a másik prefixe.

Ha α egy szó, akkor az üres szó és α mind prefixe, mind szuffixe, mind infixe α-nak.

Ezek az α *triviális prefixei*, *triviális szuffixei* és *triviális infixei*.

A prefix, szuffix, illetve infix *valódi prefix*, *valódi szuffix*, ill. *valódi infix*, ha nem egyezik meg α-val.

Kódfa

A betűnkénti kódolás szemléletesen és egyértelműen adható meg egy irányított fa segítségével.

$\varphi : A \to B^+$ egy betűnkénti kódolás.

Tetszőleges szóhalmaz, így a φ értékkészletében levő kódszavak összes prefixeinek halmaza is részbenrendezett a "prefixe" relációra.

Készítsük el ennek a relációnak a Hasse-diagrammját.

Nyilván egy irányított fát kapunk, amelynek gyökere az üres szó, és minden szó a hosszának megfelelő szinten van.

A fa éleit színezzük úgy B elemeivel, hogy ha $\beta = \alpha b$ valamely $b \in B$-re, akkor az α-ból β-ba vezető él színe legyen b.

Nyilván bármely csúcs esetén a csúcsból kivezető élek mind különböző színűek.

A kódfa valamely csúcsát, amely nem levél, *teljes csúcsnak*, illetve *csonka csúcsnak* nevezzük, attól függően, hogy tartozik-e minden színhez a csúcsból kiinduló, az adott színnel színezett él.

A kódfa csúcsait is kiszínezhetjük: az $a \in A$ kódjának megfelelő csúcs színe legyen a, azon csúcsok színe, amelyek nincsenek φ értékkészletében, legyen "üres".

A levél színe nem lehet "üres".

Az előbbi konstrukciót meg is fordíthatjuk.

Tekintsünk egy véges élszínezett irányított fát,
ahol a színek halmaza B és az egy csúcsból kiinduló élek mind különböző színűek az A véges abc-nek a fa csúcsaira való kölcsönösen egyértelműleképezéssel együtt, amelynél minden levél fellép képként.

Az $a \in A$ betű kódja legyen az a szó, amelyet úgy kapunk, hogy a gyökértől az a-nak megfelelő csúcsig haladó irányított úton összeolvassuk az élek színeit.

Prefix kód, egyenletes kód és vesszős kód

Tegyük fel, hogy a $\varphi : A \to B^+$ injektív leképezés $\mathrm{rng}(\varphi)$ értékkészlete B^+ prefixmentes részhalmaza.

Ekkor a φ által meghatározott $\psi : A^* \to B^*$ betünkénti kódolás nyilván könnyen dekódolható,
mert ha egymás után érkeznek a kódabc betűi, és nézzük az addig beérkezett szimbólumokból összeálló szót,
akkor amint ez kiadja a kódolandó *abc* valamely betüjének kódját, azonnal dekódolható is,
hiszen a folytatásával kapott jelsorozat már egyetlen betűnek sem lehet a kódja.

Ezen dekódolási módszer miatt szokás az ilyen kódot *prefix kódnak* nevezni.

(A *prefixmentes kód* elnevezés is használatos, mivel a dekódolás $\mathrm{rng}(\varphi)$ prefixmentességén múlik.)

Prefix kód nyilván felbontható.

Egy betünkénti kód *egyenletes kód* vagy *fix hosszúságú kód*, ha a betűk kódjainak hossza azonos.

Mivel egy ilyen kód nyilván prefix, ezért felbontható, így mindíg van felbontható kód.

Egy betünkénti kód *vesszős kód*,
ha van olyan η szó, a *vessző*, hogy η minden kódszónak szuffixe,
de egyetlen kód sem áll elő $\alpha\eta\beta$ alakban nem üres β szóval.

Egy vesszős kód prefix kód, mert a vessző egyértelműen jelzi a beérkezett jelsorozatban egy-egy kódszó végét
és ha ezt folytatjuk, akkor már biztosan nem kapunk kódszót,
hiszen ebben a meghosszabbított sorozatban a vessző infixe lenne.

Ha egy betűnkénti kódban nincs vessző, akkor a kód *vesszőmentes*.

A Morse-kódnál láttuk, hogy az eredeti, csak ponttal és vonással megadott betűnkénti kód nem felbontható,
míg az 1-gyel és 0-val való átírás után kapott szabály szerinti kód vesszős, ahol a 000 jelsorozat a vessző.

Egy betűnkénti kód ponntosan akkor prefix kód, ha a kódfájának csak a levelei kódszavak.

Példák

A fenti jelölésekkel legyen $A = \{a, b, c\}$, $B = \{0, 1\}$, és ψ a φ-ből képezett leképezés.

(1) Legyen $\varphi(a) = 00$, $\varphi(b) = 1$ és $\varphi(c) = 01$.

A kódszavak halmaza prefixmentes, így ez egy prefix kód, tehát egyértelműen dekódolható.

(2) Legyen $\varphi(a) = 10$, $\varphi(b) = 11$ és $\varphi(c) = 01$.

Ez egynletes kód, így egyben prefix kód.

(3) Legyen $\varphi(a) = 0010$, $\varphi(b) = 10$ és $\varphi(c) = 010$.

Ennél a kódnál minden kódszó 10-ra végződik,
vagyis 10 mindegyiknek szuffixe, de az 10 egyetlen kódszónak sem valódi prefixe és nem is valódi infixe.

Ez a kód tehát vesszős kód, így prefix kód.

(4) Legyen $\varphi(a) = 10$, $\varphi(b) = 1$ és $\varphi(c) = 01$.

Ekkor $\psi(ab) = \varphi(a)\varphi(b) = 101 = \varphi(b)\varphi(c) = \psi(bc)$, tehát ez a kód nem dekódolható: bár φ injektív, ψ nem.

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

Ez a kód egyértelműen megfejthető, tehát ψ injektív.

Tegyük ugyanis fel, hogy valameddig már dekódoltuk a beérkezett kódolt üzenetet és most érkezik egy újabb jel.

Ha ez a jel 0, akkor utána csak egy 0 következhet és ez a 00 csupán a c kódja lehet.

Ha viszont ez a jel 1, akkor ezt még nem tudjuk dekódolni.

Amennyiben ez után az 1 után ismét 1 következik, akkor már tudjuk,
hogy az első 1 egy b kódja, de a második 1-et még nem tudjuk dekódolni.

Mindaddig, amíg csak 1-ek követik egymást,
az utolsóként beérkező 1 kivételével valamennyit
egyértelműen dekódoljuk b-ként.

Abban az esetben, ha az 1 után vége van az adásnak,
akkor ezt az utolsóként maradt 1-et szintén egyértelműen b-ként dekódoljuk.

Ha viszont az 1 után 0 következik,
akkor mindaddig, amíg vagy egy 1 nem érkezik, vagy vége nincs az adásnak, nem tudunk dekódolni.

Amikor viszont vagy egy 1 érkezik, vagy vége van az adásnak,
akkor hátulról visszafelé végrehajtható a dekódolás:
minden két-két 0-t c-nek dekódolunk és
a végén vagy egy egyedül álló 1 marad, ami a b kódja, vagy 10 lesz a maradék, ami viszont az a kódja.

Könnyen ellenőrizhető, hogy másként az előbbi jelsorozat nem dekódolható.

Ez tehát egy felbontható, de nem prefix kód.

Tétel-McMillian-egyenlőtlenség

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

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

Fordítva, ha $l_1, \dots l_n$ *olyan pozitív egész számok, hogy*

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

akkor van az A-nak a B elemeivel való olyan felbontható, sőt prefix kódolása, hogy az a_j *betű kódjának hossza* l_j.

△

A fenti tételben szereplő egyenlőtlenség a *McMillian-egyenlőtlenség*, amely lényegében véve azt fejezi ki, hogy
egy felbontható betűnkénti kódban az átlagos szóhosszúság nem lehet túlságosan kicsi
(mert ha a szóhosszúság kicsi, akkor r megfelelő negatív kitevős hatványa nagy, viszont az összeg értéke nem haladhatja meg az 1-et).

A tétel második része azt mutatja, hogy
egy felbontható, de nem prefix kódnak nincs nagy jelentősége, hiszen ugyanolyan hosszakkal készíthető prefix kód is, amely "online" dekódolást tesz lehetővé.

A második rész bizonyítása konstruktív: algoritmust ad a kód megkonstruálására.

Bizonyítás

Tekintsük a $\varphi : A \to B^+$ injektív leképezés által meghatározott felbontható kódot.
Jelöljük C-vel $\mathrm{rng}(\varphi) \subset B^+$-t és legyen $M = \sum_{j=1}^{n} r^{-l_j}$ a tételbeli összeg.
Indukcióval i-re megmutatjuk, hogy $\sum_{\alpha \in C^i} r^{-|\alpha|} = M^i$.
Ha $\alpha \in C^{i+1} = C^i \times C$, akkor α megadható $\alpha = \alpha_1 \alpha_2$ alakban, ahol $\alpha_1 \in C^i$ és $\alpha_2 \in C$
és ha a kód felbontható, akkor ez a felbontás egyértelmű és

$$\sum_{\alpha \in C^{i+1}} r^{-|\alpha|} = \sum_{\alpha_1 \in C^i} \sum_{\alpha_2 \in C} r^{-|\alpha_1 \alpha_2|}$$

$$= \sum_{\alpha_1 \in C^i} \sum_{\alpha_2 \in C} r^{-(|\alpha_1| + |\alpha_2|)}$$

$$= \sum_{\alpha_1 \in C^i} \sum_{\alpha_2 \in C} r^{-|\alpha_1|} r^{-|\alpha_2|}$$

Bizonyítás folytatása

$$= \sum_{\alpha_1 \in C^i} r^{-|\alpha_1|} \sum_{\alpha_2 \in C} r^{-|\alpha_2|}$$

$$= M^i M = M^{i+1},$$

ahol az első egyenlőségnél használtuk ki, hogy a kód felbontható. Ezt az összeget másképp is ki tudjuk számítani, ha az összegben szereplő tagokat a kitevőkben szereplő hosszak növekvő sorrendben írjuk és az azonos kitevőkhöz tartozó tagokat összevonjuk.
Legyen $w_k^{(i)}$ a C^i-beli k hosszúságú szavak száma és L a C-beli szavak hosszának maximuma.
Ekkor a C^i-beli szavak hosszának maximuma iL, és

$$M^i = \sum_{\alpha \in C^i} r^{-|\alpha|} = \sum_{k=1}^{iL} w_k^{(i)} r^{-k} \leq \sum_{k=1}^{iL} r^k r^{-k} = iL,$$

mert r szimbólummal maximum r^k különböző k hosszúságú szó

Bizonyítás folytatása

írható fel.

A fentiek szerint minden pozitív egész i-re $M^i \leq iL$, vagyis $M^i/i \leq L$.

Ha $M > 1$ lenne, akkor $M^i/i \to \infty$ miatt, vagy közvetlenül az $i \geq 2$ esetén érvényes

$$L \geq \frac{M^i}{i} = \frac{(1+(M-1))^i}{i} = \frac{1}{i}\sum_{j=0}^{i}\binom{i}{j}(M-1)^j$$

$$> \frac{1}{i}\binom{i}{2}(M-1)^2 = (i-1)\frac{(M-1)^2}{2}$$

egyenlőtlenségből az arkhimédészi rendezettlenség miatt ellentmondást kapnánk.

A tétel második állításának bizonyításához feltehetjük, hogy $l_1 \leq l_2 \leq \cdots \leq l_n$ és legyen $1 \leq k \leq n$-re $c_k = \sum_{j=1}^{k-1} r^{-l_j}$.

Ez a sorozat szigorúan monoton nő, az első eleme 0 és

Bizonyítás folytatása

a $\sum_{j=1}^{n} r^{-l_j} \leq 1$ feltétel alapján az utolsó is, így minden tagja kisebb 1-nél.
Igy minden k-ra $r^{l_k} c_k = \sum_{j=1}^{k-1} r^{l_k - l_j} < r^{l_k}$ és a bal oldalon egy nem negatív egész szám áll,
hiszen a hosszak rendezése következtében az összeg tagjainak kitevője nem negatív egész szám,
$r^{l_k} c_k$ felírható az r alapú számrendszerben pontosan l_k hosszon (a felírás kezdődhet nullával is).
Ez lesz az a_k kódja, a számjegyeket kicserélve B betűire.
(Másként az 1-nél kisebb c_k nem negatív valós szám r-alapú számrendszerben pontosan felírható törtrészében l_k jeggyel és ezek a jegyek az a_k kódját adják.)
Amennyiben $1 \leq i < k \leq n$, akkor

$$r^{l_k}(c_k - c_i) = \sum_{j=1}^{k-1} r^{l_k - l_j} - \sum_{j=1}^{i-1} r^{l_k - l_j} = \sum_{j=i}^{k-1} r^{l_k - l_j} \geq r^{l_k - l_i}$$

Bizonyítás folytatása

ezért a megfelelő kódok első l_i számjegye közül legalább egy különböző, tehát a megadott kód prefix kód.

Atlagos szóhosszúság, optimális kód

Átlagos szóhosszúság

Legyen $A = \{a_1, \dots a_n\}$ a kódolandó *abc*, $p_1, \dots p_n$ a betűk eloszlása,
$\varphi : A \to B^+$ egy betűnkénti kódolás l_i az a_i kódjának hossza.
Ekkor $\bar{l} = \sum_{i=1}^{n} p_i l_i$ a *kód átlagos szóhosszúsága*.

Optimális kód

Ha adott elemszámú *abc*-vel és eloszlással egy felbontható betűnkénti kód átlagos szóhosszúsága minimális,
akkor *optimális* kódnak nevezzük.

Van-e optimális kód, mivel valós számok egy részhalmazában nem feltétlenül van minimális elem.

Válasszunk azonban egy tetszőleges felbontható kódot és legyen ennek átlagos szóhosszúsága l.
Mivel $p_i l_i > l$ esetén a kód nem lehet optimális,
elég azon kódokat tekintenünk, amelyekre $l_i \leq l/p_i$, ha $i = 1, \ldots n$.
Ilyen kód csak véges sok van, így van köztük minimális átlagos hosszúságú.
Mint az előző tételből tudjuk, ez választható prefix kódnak is.
Algoritmust fogunk adni az optimális kód megkonstruálására.

Shannon tétele zajmentes csatornára

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

Bizonyítás

A McMillian-egyenlőtlenséget, $-\log_r$ szigorú konvexitását és a segédtételt használva,

Bizonyítás folytatása

$$\bar{l} - H_r(p_1, \dots p_n) = \sum_{i=1}^{n} p_i l_i + \sum_{i=1}^{n} p_i \log_r p_i$$

$$= -\sum_{i=1}^{n} p_i \log_r r^{-l_i} - \sum_{i=1}^{n} p_i \log_r \frac{1}{p_i}$$

$$= -\sum_{i=1}^{n} p_i \log_r \frac{r^{-l_i}}{p_i} \geq -\log_r \left(\sum_{i=1}^{n} r^{-l_i} \right)$$

$$\geq -\log_r 1 = 0.$$

Tétel: Shannon-kód létezése

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

Az korábbi tétellel együtt ez azt jelenti, hogy van olyan kód, amelynek átlagos szóhossza kevesebb mint 1-el haladja meg

az elméleti alsó határt.
A bizonyítás konstruktív, algoritmust is ad a korábbi tételek segítségével együtt a kód meghatározására.

Bizonyítás

Válasszunk olyan $l_1, \dots l_n$ természetes számokat, amelyekre $r^{-l_i} \leq p_i < r^{-l_i+1}$, ha $i = 1, \dots n$.

Ekkor $\sum_{i=1}^{n} r^{-l_i} \leq \sum_{i=1}^{n} p_i = 1$,
így a korábbi tétel alapján van prefix kód az adott l_i hosszakkal.

Mivel $l_i < 1 - \log_r p_i$, erre

$$\bar{l} = \sum_{i=1}^{n} p_i l_i < \sum_{i=1}^{n} p_i (1 - \log_r p_i) = 1 + H_r(p_1, \dots p_n).$$

Tétel: *optimális kód konstrukciója*

Az előző tétel jelöléseivel legyen $n > 1$.
Tekintsünk egy optimális prefix kódot és a kódfáját és legyen a kódszavak hosszának maximuma L.

Tétel folytatása

Ekkor (1) ha $p_i > p_j$, *akkor* $l_i \leq l_j$;
(2) a kódfában csak az $L-1$*-edik szinten lehet csonka csúcs és még a csonka csúcsokból is legalább két él indul ki.*
Továbbá
(3) van olyan optimális prefix kód, amelynek kódfájában legfeljebb egy csonka csúcs van;
(4) egy optimális prefix kód kódfájában pontosan akkor nincs csonka csúcs,
ha $r \equiv n \bmod (r-1)$, *azaz*

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

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

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

Tétel folytatása

(5) ha $n \leq r$, akkor egybetűs kódszavakat választva optimális prefix kódot kapunk;
(6) legyen $\beta_1, \dots \beta_n$ az r-elemű kódabc-vel megadott, a $p_1, \dots p_n$ eloszláshoz tartozó optimális prefix kód, amelynek a kódfájában nincs csonka csúcs.
Ha $2 \leq m \leq r$ és valamely $1 \leq k \leq n$-re a $p_{n+1}, \dots p_{n+m}$ pozitív valós számokra $\sum_{i=1}^{m} p_{n+i} = p_k$ továbbá

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

akkor

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

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

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

"finomított" eloszláshoz tartozó optimális prefix kód.

Bizonyítás

Ha (1) nem teljesülne, akkor

$$0 < (p_i - p_j)(l_i - l_j) = (p_i l_i + p_j l_j) - (p_i l_j + p_j l_i),$$

és innen $p_i l_j + p_j l_i < p_i l_i + p_j l_j$, azaz a két betű, a_i és a_j kódját felcserélve csökken az átlagos szóhosszúság.

Ha (2) nem teljesül és a j-edik szinten van csonka csúcs, ahol $j < L - 1$,
akkor egy L-edik szinten lévő levelet a hozzá vezető éllel áthelyezve erre a csonka csúcsra,
és esetleg az áthelyezett élt átszínezve, a levélhez tartozó betű kódjának hossza L-ről $j + 1$-re változik,
vagyis csökken az átlagos szóhosszúság.

Ha valamely csonka csúcsot csak egy él hagy el,
akkor elhagyva ezt az élt és az ennek az élnek a másik végén levő csúcsból kiinduló részfát áthelyezve az elöbbi csúcsba,
az áthelyezett részfa leveleihez tartozó kódszavak hossza eggyel csökken, és így az átlagos szóhosszúság is csökken.

(3)-hoz legyen egy optimális kód kódfájában két különböző csonka csúcs.

Az elöbbiek szerint ezek azonos szinten vannak,
így egyikükről az egyik élhez tartozó levelet az éllel együtt áthelyezve a másik csonka csúcsra és esetleg ezt az élt átszínezve az átlagos szóhosszúság nem változik.

Ilyen áthelyezések sorozatával viszont vagy a fogadó csúcs telítődik, tahát a csonka csúcsok száma csökken,
vagy a másik csonka csúcson legfeljebb egy él maradna, ami az előbbi pont alapján optimális kód kódfáján lehetetlen.

Hogy belássuk (4)-et, tekintsünk egy n levelet tartalmazó kódfát.

Töröljük ebben a fában az egyik csúcshoz tartozó összes levelet, a csonka csúcshoz tartozó levelekkel kezdve, ha van csonka csúcs.

Ha m számú levelet töröltünk, akkor az új fában $m-1$-gyel kevesebb levél lesz.

Folytassuk az eljárást mindaddig amíg a végén csak a gyökér marad meg.

Ha összesen s lépést hajtottunk végre,
akkor $m-1+(s-1)(r-1)=n-1$,
vagyis $n=(s-1)(r-1)+m$ és $2 \leq m \leq r$.

Az (5)-ben megadott kód nyilván optimális prefix kód.
(6)-ban az a_k betű kódját helyettesítjük m kódszóval, úgy hogy a prefix tulajdonság megmarad.

(Ezzel a kódolandó abc méretét $m-1$ betűvel növeljük, az átlagos kódhossz pedig p_k-val nő.)

Jelölje a kapott kódot φ.

Tegyük fel, hogy az állítás nem igaz és legyen φ^* a

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

eloszláshoz tartozó valamely optimális prefix kód.

Ekkor φ^* átlagos hossza kisebb, mint φ átlagos hossza.

Az általánosság csorbítása nélkül feltehetjük,
hogy φ^* kódfájában is legfeljebb csak egy csonka csúcs van.

A φ kód konstrukciójából, illetve (4)-ből mindkét kódban egyszerre van csonka csúcs és ha van,
akkor a kifoka ugyanannyi, m, ha pedig nincs, akkor $m = r$.

Mivel φ^* optimális kód, ezért (1) és (2) szerint az m darab legkisebb valószínűséghez tartozó kódszó a legmagasabb szinten van a kódfában
és ugyanezen a lemagasabb szinten vannak azok a kódszavak; amelyek az esetleges csonka csúcs gyermekeihez tartoznak.

Mivel kódszavak cseréje, ha azok azonos szinten vannak, nem változtatja meg a kód átlagos hosszát,
ezért feltehetjük, hogy mindkét kódban az m legkisebb valószínűségű kódszóhoz tartozó levél ugyanahhoz a csúcshoz tartozik.

Ezeket törölve, mindkét kód átlagos hossza ugyanannyival változik.
Igy a φ^*-ból kapott kód átlagos hossza kisebb lesz,
mint a φ-ből kapott kódé, ami lehetlen,
hiszen feltettük, hogy a φ-ből kapott kód optimális kód.

Huffman-kód

Optimális kódot ad az úgynevezett *Huffman-kód*,
amelyet az előző tétel (4)-(6) pontjai alapján tudunk megszerkezteni.

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

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

(Célszerű kupac struktúrát használni.)

Ezek után ismételjük meg az előző redukciót, de most már minden lépésben r betűvel csökkentve a kódolandó halmazt, mígnem már csak r betű marad (feltehetjük, hogy induláskor több, mint r betű volt, ellenkező esetben a redukció elmarad.)

Most a redukált *abc* legfeljebb r betűt tartalmaz és ha volt redukció,
akkor pontosan r betűt.

Ezeket a kódoló *abc* elemeivel kódoljuk, majd a redukciónak megfelelően visszafelé haladva,
az ott összevont betűk kódját az összevonásként kapott betű már meglévő kódjának a kódoló *abc* különböző betűivel való kiegészítésével kapjuk.

Példa

Mutatunk egy példát a Huffman- és a Shannon kódra.
Mindkét esetben ugyanazon forrást fogjuk kódolni,
így összehasonlítható a két kód hatékonysága.

Legyen a kódolandó *abc* 10-elemű
(mondjuk az angol *abc* első 10 betűjével jelölve),
az egyes betűk relatív gyakorisága rendre 0.17, 0.02, 0.13, 0.02, 0.01, 0.31, 0.02, 0.17, 0.06, 0.09, és a kódoló *abc* $\{0, 1, 2\}$.

Mivel 10-2=4(3-1)+0, az első lépésben 0+2=2 betűt kell összefogni,
majd a további lépésekben hármat-hármat (az "új betűket" párokkal, illetve hármasokkal jelöljük).

Amikor már csak 3 betűből áll az *abc*,
akkor ezt a három betűt rendre 0-val, 1-gyel és 2-vel kódoljuk,
majd visszafelé haladva előállítjuk a kívánt kódot.

A kód átlagos szóhosszúsága ≈ 1.79, míg az entrópia értéke ≈ 1.73
így a kód átlagos szóhosszúsága igen jól megközelíti az elméletileg elérhető legkisebb értéket.

Ugyanezen *abc*-t fogjuk most a Shannon-kóddal kódolni.

Most is sorba kell rendezni az *abc*-t a relatív gyakoriságok csökkenő sorrendjében.

Meghatározzuk a szükséges szóhosszúságokat.

Mivel 0.31, 0.17, 0.13 kisebbek, mint 1/3, de nem kisebbek, mint 1/9, f,a,h és c kódhossza 2.

Hasonlóan *j* és *i* kódhossza 3, míg b, d és g kódhossza 4, végül e kódhossza 5.

Az f kódja 00, az a kódja 01, a h kódja 02
és ez utóbbihoz hármas alapú számrendszerben 1-et adva kapjuk c kódját, amely így 10.

Ehhez 1-et adva 11-et kapunk, de j kódjának hossza 3,
ezért ezt még jobbról ki kell egészíteni egy darab 0-val, tehát j kódja 110.

Hasonlóan haladva megkapjuk a teljes kódot.

Most a kód átlagos szóhosszúsága 2.30,
mely nagyobb, mint a Huffman-kódnál volt (1.79), de kisebb, mint 2.73, az entrópia plusz 1.

Megadjuk az ékezet nélküli latin betűk magyar nyelvben való előfordulásának relatív gyakoriságaihoz tartozó bináris Huffman- és Shannon-kódot

(a Shannon-kódnál a Q betű kódjának hosszát az egyébként előforduló hosszak maximumának vettük,
általában is a nagyon kis gyakoriságokat kicsit megnövelve,
korlátozhatjuk a kódszavak hosszát, nem sokat rontva a kódon.)

Az adott eloszláshoz tartozó entrópia értéke ≈ 4.1289,
míg a Huffman-kód átlagos szóhosszúsága ≈ 4.1528,
a Shannon-kódé pedig ≈ 4.5989.

Ugyanakkor a Morse-kód 0-val 1-gyel való kódolásánál az átlagos szóhosszúság ugyanezekkel a gyakoriságokkal ≈ 12.299.

Látható, hogy mekkora javulás érhető el.

Ennek egyik oka, hogy a vessző határozottan növeli az átlagos szóhosszúságot.

A kódolandó *abc* kiterjesztése

Egyszerű módon el tudjuk érni,
hogy egy felbontható kódban az egy betűre jutó átlagos szóhosszúság tetszőlegesen megközelítse az entrópia értékét, azaz az elméleti alsó határt.

Ehhez az eredeti *abc*-ből elkészítjük az összes kétbetűs, hárombetűs, stb. szót,
és egy-egy ilyen szót tekintünk egy új *abc* egy-egy betűjének, ahol egy-egy ilyen új betűhöz a benne szereplő betűk relatív gyakoriságainak szorzatát rendelve
kapjuk a megfelelő eloszlást.

Az így kapott kód az eredeti kód *kétszeres, háromszoros stb. kiterjesztése*.

Ha m betű egybefogásából áll a kiterjesztett abc,
akkor van olyan kód, amelynek egy betűre jutó átlagos szóhosszúsága

$$\bar{l} < -\sum_{i=1}^{n} p_i \log_r p_i + \frac{1}{m}$$

(azaz 1 helyett csak 1/m-mel van az elméleti alsó határ felett),
ahol n az eredeti abc betűinek száma és a p_i-k az eredeti abc betűinek relatív gyakoriságai.

A módszer szépséghibája,
hogy például a kétszeres kiterjesztésnél azonos számot rendel
ty-hoz és yt-hez,
holott a magyar nyelvben a két betűkombináció még megközelítőleg sem azonos gyakorisággal fordul elő.

Ha a párok valódi gyakoriságait tekintjük, még jobb kódot kapunk.

A kiterjesztésnek határt szab, hogy a kódolandó abc,
igy a kódtábla is nagyon nagy lesz, ezért a gyakorlatban nem használják.

Szótárkódok

A betünkénti kódolás nem képes kihasználni,
ha az egymás után következő betűk egymástól nem függetlenek,
vagyis egy betű mejelenése nem független attól, hogy előtte milyen betűket bocsátott ki az adó.

Egy élő nyelvű szöveg általában ilyen:
a magyar nyelvben a t után sokkal gyakoribb az y, mint például az r után.

A korábban említett kiterjesztés sem megoldás erre a problémára.

Egy másik probléma, hogy amennyiben egy üzenet nem tipikus,
várhatóan benne a betűk előfordulásának relatív gyakorisága eltér a szokásostól,
akkor egy rögzített kódtábla, amely a tipikus szövegek betűgyakorisága alapján épül fel,
nem ad jó kódot még a Huffman-kód esetén sem.

Ha viszont egy ilyen esetben a konkrét szöveg statisztikája alapján hozzuk létre a kódtáblát, akkor ezt is továbbítani kell.

Vannak rövid szövegek esetén hasznos "ad hoc" megoldások.

Például 256 elemű bővített ASCII kód esetén egy "escape" karaktert fenntartva, azzal átléphetünk egy másik kódtáblába, amiben csak a 32-94 kódú ASCII karakterek szerepelnek, de a felső bit le van vágva.

Igy egy 6 bites kódot kapunk, ami négyesével összecsomagolható három bájtra.

Itt a 95-ös ASCII kód megfelelője az "escape", ami visszalép a 256 elemű kódba.

Egy másik megoldásban 40 kódszó van:
a 26 nagy betű, a 10 számjegy, 1 "escape" karakter és 3 "táblaváltó",
amelyekkel egy-egy karakter erejéig 3 másik 40-es tábla valamelyikére válthatunk.

40 alapú számrendszerben három ilyen kód egy 64000-nél kisebb számmá áll össze, ami két bájton elfér.

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

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

A alábbiakban ilyen kódokat mutatunk be.

Futamkódolás

Bizonyos szövegállományokban gyakran fordulnak elő (egymás utáni) ismétlődő karakterek (például ismétlődő szóközök).

Ilyenkor célszerű lehet úgy tömöríteni,
hogy a karaktert csak egyszer adjuk meg, majd megadjuk az ismétlések számát.

A gondot az okozza, hogy az ilyen számokat el kell választani a szöveg karaktereitől.

Egyik lehetőség, hogy például a legalább háromszor ismétlődő karaktert háromszor leírjuk, majd utána írunk egy decimális számjegyet, amely megadja, hogy még hányszor ismétlődik.

Például a 40 karakter hosszú

␣␣␣␣␣␣␣␣␣*gugogogogol*␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣

sor igy tömörítve

␣␣␣5*gugogogogol*␣␣␣9␣␣␣6

lesz; a második szóköz sorozatot csak "két részletben" tudtuk leírni, mert nincs 9-nél nagyobb decimális számjegy.

(Persze a decimális számjegy helyett egy egész bájt is jelezhetné az ismétlődést,
de az elv és a korlát létezése nem változtana.)

Ha van olyan betű az *abc*ben, amely biztosan nem fordulhat elő a szövegben, például a @,
akkor azt használhatjuk "escape" karakternek,
jelezve, hogy az utána következő számjegy nem része a szövegnek, hanem az "escape" elötti betű legalább egyszer ismétlődik (0 számjegy 1 ismétlés stb.).

Ezzel a szöveg

$$\sqcup @6gugogogogogol \sqcup @9 \sqcup @8$$

lesz.

Ha # egy másik "escape" karakter,
akkor azt például felhasználhatjuk annak jelzésére,
hogy utána 1 helyett 2 számjegy írja le az eddig még nem kódolható számú ismétlődéseket
(00 jelentése 11 ismétlés stb.).

Igy a szöveg

$$\sqcup @6gugogogogogol \sqcup \#09$$

lesz.

Egy másik lehetőség, hogy ismert szöveghossz esetén
az egyik "escape" azt jelzi, hogy a szöveg végéig már csak a "triviális" karakter - jelen esetben a szóköz - ismétlődik.

Példánkban így a tömörített szöveg

$$\sqcup @6gugogogogogol\#$$

lesz.

Látszólag gondot okoz "escape" karakterek hiánya.

Ha azonban a futamkódolás eredményére egy prefix kódolást alkalmazunk,
akkor annyi "escape" karaktert képezhetünk,
amennyit akarunk.

Sőt az "escape" karaktert és az utána következő számot egybefoghatjuk és
ezekhez a párokhoz rendelhetünk egy prefix kódszót, vagy akár a betűt, az "escape" karaktert és az utána következő számot fogjuk össze, és
ehhez a hármashoz rendelünk prefix kódszót.

Fax üzenetek kódolására elterjedt ez a fajta kód.

Csak fekete és fehér képelemek vannak, egy sor általában 1664 képelem, soronként olvassunk.

A futamhosszakat kvázi "64 alapú" számrendszerben adjuk meg: $1, 2, \ldots, 63$ és $64, 128, 192, 256, \ldots 2560$.

Külön kód van a fehér és a fekete képelemsorozatok számára.

Ha a képelemek száma legalább 64, akkor először a magasabb helyiértékű számjegyet küldjük át.

Minden sor fehér képelemsorozattal képződik és "soe vége" karakter zárja le.

Ennek kódja (mindkét kódtáblában) 000000000001.

Semmilyen más kód nem kezdődik 7-nél több nullával, így ha a vevő 8 nullát talál, akkor a következő egyesig olvas.

Ez biztosítja, hogy egy átviteli hiba esetén legfeljebb egy sor megy tönkre.

Kódhosszak alapján a megfelelő Huffmann-kód már algoritmmussal felépíthető, bár itt nincs minden kódhossz kihasználva.

LZ77

gzip parancs

LZW-kódok

Példa LZW-kódra

compress parancs

Digitalizálás

Egy valós értékű függvényt (fizikai vagyis *analóg jelet*) számítógépen közvetlenül nem tudunk reprezentálni, ezért mintavételezéssel sorozattá alakítjuk, majd a kapott valós számokat egész számokká alakítva kvantáljuk.

A két lépés együtt a *digitalizálás*.

Egy $t \to F(t)$ függvényt (ami legtöbbször az idő függvényének gondolunk, bár ez nem szükségszerű) *mintavételezéssel* alakíthatunk (mindkét irányban végtelen) sorozattá:

legyen $f_k = F(\tau_0 + k\tau)$, ha $k \in \mathbb{Z}$, ahol $\tau_0 \in \mathbb{R}$ és $0 < \tau \in \mathbb{R}$ rögzítettek.

A mintavételezés *periódusideje* τ,
ennek reciproka, $1/\tau$ a *mintavételi frekvencia*, azaz az időegységre eső minták száma.

Természetesen, ha a F jel csak egy véges intervallumon van értelmezve, akkor a minta is véges sorozat lesz.

Tekintsük példaként a $t \longrightarrow \sin(2\pi(t-\tau_0)/T)$ periódikus jelet, amelynek periódusa T (azaz $F(t+T) = F(t)$ minden $t \in \mathbb{R}$-re), frekvenciája így $1/T$.

Ennek τ mintavételi periódusidővel való mintavételezésével az $f_k = \sin(2\pi k\tau/T)$, $k \in \mathbb{Z}$ sorozatot kapjuk.

észrevehetjük, hogy ha egy ilyen szinuszos jel frekvenciája a mintavételi frekvencia fele,
azaz ha $2/T = 1/\tau$, akkor $f_k = \sin(\pi k) = 0$,
ami megegyezik az azonosan nulla jel mintavételezésével kapott sorozattal.

Ez azt mutatja, hogy a mintavételi frekvencia felénél nem kisebb frekvenciájú jelösszetevők a mintavételnél elveszhetnek.

Ezért a mintavételi frekvencia az átvinni kívánt jel legmagasabb frekvenciájú összetevője frekvenciájának több mint kétszerese kell legyen:
ez *Shannon mintavételi törvénye*.
Kétdimenziós $(x, y) \to F(x, y)$ jelnél, például képnél kétdimenziós mintavételezést alkalmazhatunk:

$$f_{i,j} = F(\xi_0 + i\xi, \eta_0 + j\eta).$$

Háromdimenziós $(x, y, t) \to F(x, y, t)$ jelnél, például mozgóképnél a mintavételezés is háromdimenziós:

$$f_{i,j,k} = F(\xi_0 + i\xi, \eta_0 + j\eta, \tau_0 + k\tau).$$

A mintavétlezéssel kapott jel még nem tárolható a számítógépben: kerekítéssel digitalizálni kell.
Általában egészre kerekítünk valamilyen szabály szerint.
A kerekítés előtt rendszerint egy szigorúan monoton $v \to q(v)$ *kvantálsi függvény*t alkalmazzunk a mintavételezéssel kapott értékekre,
majd kerekítünk ez a tulajdonképpeni *kvantálás*.

A kvantálási függvény gyakran lineáris, $q(v) = av + b$ alakú.

Minél nagyobb a, annál kisebb változás elég v-ben, hogy másik egész számot kapjunk a kerekítés után,
tehát annál finomabb a kvantálás, azaz annál közelebbi jelszinteket tudunk megkülönböztetni.

A b konstanssal például elérhetjük, hogy a kvantált értékek nemnegatívak legyenek,
b tehát szinteltolást jelent.

A kvantálás sajnos azt is jelenti, hogy "zajt" viszünk be a jelbe.

A hang (egységnyi felületre eső) teljesítménye a hangnyomás négyzetével arányos.

A mikrofon a hangnyomással arányos feszültséget hoz létre,
villamos teljesítmény ennek a négyzetével arányos,
tehát arányos a hangteljesítménnyel.
Fülünk érékenysége logaritmikus jellegű:
bármely két hang között akkor érzünk ugyanolyan hangosságkülönbséget, ha teljesítményük aránya ugyanaz az érték.

Ezért hangjel kvantálásnál logaritmikus jellegű kvantálási függvényt érdemes alkalmazni,
mert ekkor ugyan hangosabb jelnél a kvantálási zaj is hangosabb lesz,
de a teljesítményük aránya ugyanaz marad,
így egyformán érezzük zajosnak a különböző intenzitású részeket.

Például a telefontársaságok az észak-Amerikában és Japánban a

$$v \longrightarrow \operatorname{sgn}(v)\frac{\log(1+\mu|v|)}{\log(1+\mu)}$$

függvényt használják rendszerint $\mu = 255$ választással, míg a világ többi részén a

$$v \longrightarrow \begin{cases} \operatorname{sgn}(v)\frac{A|x|}{(1+\ln A)}, & \text{ha } 0 \le |x| < 1/A \\ \operatorname{sgn}(v)\frac{1+\ln|Ax|}{(1+\ln A)}, & \text{ha } 1/A \le |x| \le 1 \end{cases}$$

rendszerint $A = 87.6$ választással; ez mindkét esetben úgy értendő, hogy a fenti függvényeket mint $[-1,1]$-et önmagába képező függvényeket kell tekinteni és alkalmazásuk előtt és után is konstanssal való szorzást alkalmazunk.

(Az első függvény valamivel kisebb alapzajt, a második valamivel jobb dinamikát biztosít.)
Az is lehet, hogy egy már (lineárisan, finoman) kvantált jelet kvantálunk újra nemlineáris kvantálással. (Például digitális telefonnál a fenti függvényekkel tulajdonképpen 14 bites lineárisan kvantált értéket kvantálnak újra, hogy 8 bites értéket kapjanak, valamivel növelve a zajt, de csökkentve az átviendő bitek számát.)
Amikor a digitalizált jelet visszaalakítjuk analóg jellé,
a kvantálási függvény inverzét kell alkalmazunk.
általában a digitalizálás mindkét lépésben
- a mintavételezésnél és a kvantálásnál is
- elvész az információ egy része,
így általában minden digitalizálást használó kódolás eleve veszteséges.
Néhány tömörítő eljárás *vektorkvantálást* használ:

összetartozó mennyiségeket (például egy színes képpont színkoordinátáit) együtt vektoroknak tekintünk, és egy vektorokat tartalmazó kódtáblából keressük ki a hozzá legközelebbi vektort.

DFT és IDFT

Tekintsünk egy $T > 0$ periódus szerint periódikus valósváltózós komplex értékű F függvényt
(azaz $F(t+T) = F(t)$ minden $t \in \mathbb{R}$-re),
legyen a mintavételi frekvencia az $1/T$ "alapfrekvencia" n-szerese,
ahol $n \in \mathbb{N}^+$, azaz legyen $\tau = T/n$ és legyen (kényelmi okokból)
$\tau_0 = 0$.

A mintavételezéssel kapott $f_j = F(\tau_0 + j\tau)$ $(j \in \mathbb{Z})$ sorozat n szerint periódikus,
azaz $f_{j+n} = f_j$ minden $j \in \mathbb{Z}$-re,
így egy $\mathbb{Z}_n$-en értelmezett f függvénynek is tekinthető,
vagyis az $f_0, f_1, \ldots f_{n-1}$ értékek egyértelműen jellemzik;
a $\tau_0 + j\tau, j = 0, 1, \ldots n-1$ pontok *alappontok*
(elég lenne az is, hogy a j mod n teljes maradékrendszer legyen).

Ezt a függvényt szeretnénk "eltolt szinuszos" jelek lineáris kombinációjaként előállítani:

Tekintsük a
$H_k(t) = \cos(2\pi kt/T) + i\sin(2\pi kt/T),\ k \in \mathbb{Z}$
ugyancsak T szerint periódikus komplex értékű függvényeket.

A H_k függvénynek a fenti módon való mintavételezésével az $\omega_n^{jk}; j \in \mathbb{Z}$ sorozatot kapjuk,
ahol $\omega_n = \cos(2\pi/n) + i\sin(2\pi/n)$ az első n-edik egységgyök.

Legyen $\hat{f}_k = \sum_{j=0}^{n-1} f_j \omega_n^{-jk}$ (azaz az

$$(f_0, f_1, \ldots f_{n-1})$$

és az

$$\left(\omega_n^0, \omega_n^k, \ldots \omega_n^{(n-1)k}\right)$$

$\mathbb{C}^n$-beli vektorok belső szorzata), ha $k \in \mathbb{Z}$.

A $\hat{f}_k,\ k \in \mathbb{Z}$ sorozat is n szerint periódikus,
hiszen $\omega_n^n = 1$, így

$$\hat{f}_{k+n} = \sum_{j=0}^{n-1} f_j \omega_n^{-j(k+n)} = \sum_{j=0}^{n-1} f_j \omega_n^{-jk} = \hat{f}_k.$$

Tehát az f sorozathoz az $\hat{f}$ sorozatot rendelő leképezés a $\mathbb{Z}_n$-en értelmezett komplex értékű függvények n-dimenziós komplex (azaz $\mathbb{C}$ feletti) vektorterét önmagába képezi le.

Ezt a leképezést nevezzük *diszkrét Fourier-transzformációnak*, DFT-nek.

A diszkrét Fourier-transzformáció olyan fontos leképezés, hogy gyors végrehaktására integrált áramköröket gyártanak, számos műszaki alkalmazással (jelanalízis, digitális szűrés, stb.), és szoros kapcsolatban áll az analízisben tanulmányozott Fourier-sorokkal és Fourier-transzformációval.

A DFT nyilván lineáris.

Vegyük észre, hogy

$$\sum_{j=0}^{n-1} (\omega_n^k)^j = \frac{(\omega_n^k)^n - 1}{\omega_n^k - 1}$$

0, ha $\omega_n^k \neq 1$ és a szumma nyilván n, ha $\omega_n^k = 1$.

Ebből következik,hogy a

$$H_0, H_1, \ldots H_{n-1}$$

függvények mintavételezésével kapott
$h_k : \mathbb{Z}_k \to \mathbb{C}$ vektorok páronként ortogonálisak és
mindegyiknek az önmagával vett belső szorzata n, hiszen

$$< h_{k'}, h_{k''} >= \sum_{j=0}^{n-1} h_{k'}(j)\overline{h_{k''}(j)} = \sum_{j=0}^{n-1} \omega_n^{jk'} \omega_n^{-jk''} = \sum_{j=0}^{n-1} \omega_n^{j(k'-k'')}.$$

Innen a

$$t \to \frac{1}{n} \sum_{k=0}^{n-1} \hat{f}_k H_k(t)$$

függvény a mintavételezés $t = j\tau$ pontjaiban megegyezik a
kiindulási F függvénnyel,
azaz az F periódikus függvényt közelítettük a H_k periódikus
függvények segítségével.

(Egyébként ugyanez igaz, ha a k indexek bármely
mod n vett teljes maradékrendszert futnak be.)

Speciálisan, a DFT invertálható, és "majdnem" (az $1/n$ szorzótól és az origóra való tükrözéstől eltekintve) saját maga az inverze: $t = j\tau$ helyettesítéssel

$$f_j = \frac{1}{n}\sum_{k=0}^{n-1} \hat{f}_k \omega_n^{jk} = \frac{1}{n}\sum_{k=0}^{n-1} \hat{f}_k \omega_n^{-(-j)k} = \frac{1}{n}\hat{f}_{-j}.$$

A DFT inverzét *inverz Fourier-transzformációnak*, IDFT-nek nevezzük.
További hasznos észrevétel, hogy

$$\hat{\hat{f}}_k = \sum_{j=0}^{n-1} \overline{f}_j \omega_n^{-jk} = \overline{\sum_{j=0}^{n-1} f_j \omega_n^{jk}} = \overline{\hat{f}_{-k}}.$$

Igy, ha az f_j sorozat valós, akkor $\hat{f}_k = \hat{\hat{f}}_k = \overline{\hat{f}_{-k}}$.
Ennek az észrevételnek a segítségével megvizsgálhatjuk a

$$\frac{1}{n}\sum_{k=0}^{n-1} \hat{f}_k H_k(t)$$

összegben az egyes tagok jelentését.

Az $f_0 H_0(t)$ tag konstans, az átlag n-szerese.

Valós f_j sorozat esetén, ha $0 < k \leq n/2$,
$f_k = r_k(\cos\varphi_k + i\sin\varphi_k)$, akkor

$$\hat{f}_k H_k(t) + \hat{f}_{-k} H_{-k}(t) = r_k(\cos\varphi_k + i\sin\varphi_k)(\cos(2\pi kt/T) + i\sin(2\pi kt/T))$$
$$+ r_k(\cos\varphi_k - i\sin\varphi_k)(\cos(2\pi kt/T) - i\sin(2\pi kt/T))$$
$$= 2r_k\cos(2\pi kt/T + \varphi_k),$$

azaz $2r_k$-szor egy koszinuszos jel φ_k fáziseltolással,
tehát az eredeti jelet lényegében koszinuszos ("harmonikus") jelek összegére bontottuk,
amelyek frekvenciája az $1/T$ alapfrekvencia k-szorosa,
$0 \leq k \leq n/2$.

A $2r_k/n = 2|\hat{f}_k|/n = 2|\hat{f}_{-k}|/n$ mennyiség úgy tekinthető,
mint a $\cos(2\pi kt/T + \varphi_k)$ harmonikus jelnek az amplitudója az F jelben, ha $0 < k < n/2$;
ha $k = n/2$, akkor $\hat{f}_k = \hat{f}_{-k}$ valós és $H_k = \overline{H_{-k}}$,
így $k = n/2$ esetén a $\cos(2\pi kt/T + \varphi_k)$ harmonikus jel
amplitudója az eredeti F jelben $r_k/n = |\hat{f}_k|/n = |\hat{f}_{-k}|/n$.

A φ_k eltolási érték a "fáziseltolás".

Végül vegyük még észre, hogy ha az f_j $(j \in \mathbb{Z})$ sorozat páros, akkor

$$f_j = f_{-j} = \frac{1}{n}\hat{\hat{f}}_{-(-j)} = \frac{1}{n}\hat{\hat{f}}_j,$$

ahonnan

$$\hat{f}_k = \frac{1}{n}\hat{\hat{\hat{f}}}_k = \hat{f}_{-k},$$

azaz az $\hat{f}_k$ sorozat is páros.

Ha az f_j sorozat valós és páros, akkor a $\hat{f}_k$ sorozat páros és $\overline{\hat{f}_k} = \hat{\overline{f}}_k = \hat{f}_{-k} = \hat{f}_k$ azaz valós is.

Hasonlóan, ha az f_j sorozat páratlan, akkor

$$-f_j = f_{-j} = \frac{1}{n}\hat{\hat{f}}_j$$

ahonnan

$$-\hat{f}_k = \frac{1}{n}\hat{\hat{\hat{f}}}_k = \hat{f}_{-k},$$

azaz $\hat{f}$ is páratlan.

Ha az f_j sorozat valós és páratlan, akkor a $\hat{f}_k$ sorozat páratlan és $\overline{\hat{f}_k} = \hat{\overline{f}}_k = \hat{f}_{-k} = -\hat{f}_k$, azaz képzetes.

FFT

A gyors Fourier-transzformáció (Fast Fourier Transform, FFT) a diszkrét Fourier-transzformált gyors kiszámítására szolgál.

Legyen $n \in \mathbb{N}^+$ rögzített és az egyszerűség kedvéért vezessük be az $\omega = \overline{\omega_n} = \omega_n^{-1}$ jelölést.

Vegyük észre, hogy az előző pontban használt jelölésekkel $\hat{f}_k$ nem más, mint az $f^{(0)}(x) = \sum_{j=0}^{n-1} f_j x^j$ polinom $x_k = \omega^k$ helyen felvett értéke:

$$f^{(0)}(\omega^k) = \sum_{j=0}^{n-1} f_j (\omega^k)^j = \sum_{j=0}^{n-1} f_j \omega_n^{-kj} = \hat{f}_k.$$

Az $\hat{f}_k$ értékek gyors kiszámításához vezető trükk:

ha $n = n_1 n_2$. akkor $y = x^{n_1}$ jelöléssel

$$f^{(0)}(x^{n_1 j_2 + k_1}) = \sum_{k_1=0}^{n_1-1} x^{k_1} f_{k_1}^{(1)}(y),$$

ahol

$$f_{k_1}^{(1)}(y) = \sum_{j_2=0}^{n_2-1} f_{n_1 j_2 + k_1} y^{j_2}, \quad k_1 = 0, 1, \dots n_1 - 1.$$

Ha $x = \omega^{k_1}, \omega^{k_1+n_2}, \dots \omega^{k_1+(n_1-1)n_2}$, akkor a hozzá tartozó y ugyanaz,
így minden kiszámított $f_{k_1}^{(1)}(y)$ érték többször is felhasználható.
Például,
ha $n_1 = 2$, $n = 2n_2$, akkor az $f^{(0)}$ polinom ω^k és $\omega^{k+n/2}$ helyen felvett értékeit egyszerre számolhatjuk ki (azt is felhasználva, hogy $\omega^{n/2} = -1$) az alábbi "pillangó művelettel":

$$f^{(0)}(\omega^j) = f_0^{(1)}(\omega^{2k}) + \omega^k f_1^{(1)}(\omega^{2k}),$$

$$f^{(0)} = \omega^{k+n/2}) = f_0^{(1)}(\omega^{2k}) - \omega^k f_1^{(1)}(\omega^{2k}).$$

Például,
ha $n = 8$, $n_1 = 2$, akkor $x = \omega^k$ és $x = \omega^{k+4}$ esetén y értéke ω^{2k}, így az

$$f_0 + f_2 y + f_4 y^2 + f_6 y^3$$

és

$$f_1 + f_3 y + f_5 y^2 + f_7 y^3$$

értékeket kétszer is tudjuk használni, így a munkát nagyjából megfelezzük.

Természetesen rekurzívan is alkalmazhatjuk ezt a trükköt.

Az együtthatóikkal adott polinomok értékeit kell kiszámolnunk a megadott helyeken.

Az elöbbiek alapján rekurzív programot írhatunk a diszkrét Fourier-transzformáció elvégzésére,
ha n "kis tényezők szorzatára" bontható.

A gyakorlatban legtöbbször használt $n = 2^m$ esetben célszerűbb azonban a rekurziót ciklussá átalakítani.

Vezessük be az $[d_s, d_{s-1}, \ldots, d_2, d_1] = \sum_{j=1}^{s} d_j 2^{j-1}$ jelölést.

Definiáljuk az

$$f^{(s)}_{j_1,j_2\dots j_s} = \sum_{j=0}^{2^{m-s}-1} f_{[j_s,j_{s-1}\dots j_2 j_1]} x^j \quad \text{ha} \quad 0 \le s \le m, \quad j_1,\dots j_s \in \{0,1\}$$

"közbülső polinomokat".

Az $f^{(m)}_{jj_1j_2\dots j_m}$ polinomok konstansok, értékük $f_{[j_m j_{m-1}\dots j_2 j_1]}$. Az

$$f^{(s)}_{j_1j_2\dots j_s}(\omega^{k2^s}) = f^{(s+1)}_{j_1j_2\dots j_s,0}(\omega^{k2^{s+1}}) + \omega^{k2^s} f^{(s+1)}_{j_1j_2\dots j_s,1}(\omega^{k2^{s+1}})$$

$$f^{(s)}_{j_1j_2\dots j_s}(\omega^{k2^s+n/2}) = f^{(s+1)}_{j_1j_2\dots j_s,0}(\omega^{k2^{s+1}}) - \omega^{k2^s} f^{(s+1)}_{j_1j_2\dots j_s,1}(\omega^{k2^{s+1}})$$

pillangóművelet segítségével rendre az $s = m-1, m-2, \dots, 1, 0$ értékekre számítjuk ki a függvényértékeket. Egyetlen n elemű A tömböt használunk,

$$f^{(s)}_{j_1j_2\dots j_s}(\omega^{[k_{m-s}k_{m-s-1}\dots k_2k_1]2^s})$$

értéke $A[k_1, k_2, \dots k_{m-s}, j_1, \dots j_s]$-be kerül, ahol

$$k_1, k_2, \dots, k_{m-s}, j_1, \dots j_s \in \{0,1\}.$$

Igy az alábbi algoritmust kapjuk.

FFT algoritmus

Az előző pont jelöléseivel az algoritmus az A tömbben lévő

$$A[j_m j_{m-1} \dots j_2 j_1] = f_{[j_m j_{m-1} \dots j_2 j_1]}, \quad j_1, \dots j_m \in \{0, 1\}$$

sorozat Fourier-transzformáltját számolja ki.

Az egész számítás "helyben" az A tömbben zajlik,
a részeredmények és végeredmény is az A tömbben keletkezik,
de $\hat{f}_{[k_m, k_{m-1}, \dots k_2, k_1]}$ nem az A tömb $[k_m, k_{m-1}, \dots k_2, k_1]$ indexű elemében foglal helyet,
hanem az ebből a bitsorozatból "bitfordítással" kapott indexű helyen:

$$\hat{f}_{[k_m, k_{m-1}, \dots k_2, k_1]} = A[k_1, k_2, \dots k_{m-1}, k_m] \text{ ha } k_1 \dots k_m \in \{0, 1\}.$$

A számítás használ egy T segédtáblázatot, amely az ω hatványait tartalmazza, "bitfordított" sorrendben:

$$T[j_{m-1}, \dots j_2 j_1] \leftarrow \omega^{[j_1 j_2 \dots j_{m-1}]}, \text{ ha } j_1 \dots j_m \in \{0, 1\}$$

Az algoritmus:

(1) [Inicializálás.]
Legyen $l \leftarrow 2^{m-1}$.

(2) [Menet kezdete.]
Legyen $j \leftarrow 0$ és $t \leftarrow 0$.

(3) [Pillangósorozat kezdete.]
Legyen $k \leftarrow j + l$ és $w \leftarrow T[t]$.

(4) [Pillangó művelet.]
Legyen $x \leftarrow A[j]$ és $y \leftarrow wA[j + l]$, majd
legyen $A[j] \leftarrow x + y$ és $A[j + l] \leftarrow x - y$,
végül legyen $j \leftarrow j + 1$.

(5) [Pillangósorozat vége?]
Ha $j < k$, menjünk vissza (4)-re.

(6) [Menet vége?]
Ha $k + l < n$, legyen $j \leftarrow k + l$, $t \leftarrow t + 1$,
és menjünk vissza (3)-ra.

(Most $A[k_1 k_2 \dots k_{m-s} j_1 j_2 \dots j_s] = f^{(s)}_{j_1 j_2 \dots j_s}(\omega^{[k_{m-s} k_{m-s-1} \dots k_2 k_1]2^s})$, lásd az előző pontot.)

(7) [Vége?]
Legyen $l \leftarrow \lfloor l/2 \rfloor$. Ha $l > 0$, menjünk vissza (2)-re, egyébként az algoritmus véget ért.

Az eredmény kiolvasásához, illetve a T tábla feltöltéséhez szükséges "bitfordítás" eltolásokkal történhet:
a számot balra tolva, egyenként megkapjuk bitjeit és
azokat jobbra tolással összerakjuk fordított sorrendben.

Még egyszerűbb
a következő természetes szám bitfordítottját az előző természetes szám bitfordítottjából számítani,
a legnagyobb helyiértékű bithez 1-et hozzáadva és
az átvitelt az alacsonyabb helyiértékek felé végezve.

Vegyük észre, hogy ugyanaz a T táblázat különböző m értékekre is megfelel, ha a maximális m értékre számoljuk ki, és csak egy kezdőszeletét használjuk.

Könnyű összeszámolni, hogy az algoritmus $5n \log n$ valós lebegőpontos műveletet használ,
míg a polinomértékek Horner-elrendezéssel való kiszámítása $\approx 2n^2$ lebegőpontos műveletet használna.

IFFT algoritmus

Az előzőpontban megadott algoritmus megfordítható
és megfordításával a DFT inverzére kapunk gyors algoritmust:

ha a meneteket fordított sorrendben hajtjuk végre,
$l = 1, 2, \ldots 2^{m-1}$-re és a (4) pillangóműveletet invertáljuk,
akkor a transzformáció inverzét kapjuk:

(4') [Inverz pillangó.]
Legyen $x \leftarrow A[j]$, $y \leftarrow A[j+l]$, majd $A[j] \leftarrow (x+y)/2$,
$A[j+l] \leftarrow (x-y)/(2w)$, végül $j \leftarrow j+1$.
A felhasznált T táblázat ugyanaz.
(4')-ben a kettővel való osztásokat elhagyhatjuk, ha az egész algoritmus elején vagy végén az A tömb minden elemét osztjuk 2^m-mel.

Vegyük észre azt is, hogy $1/w = \overline{w}$,
így itt sincs szükség osztásra, szorzással is dolgozhatunk.

Gyors szorzás FFT-vel

Legyen $f = \sum_{j=0}^{n-1} f_j x^j$, $g = \sum_{j=0}^{n-1} g_j x^j$ és
h az f és g polinomok szorzata.

Tegyük fel, hogy $\deg(h) = \deg(f) + \deg(g) < n$.

Mivel $\hat{f}_k = f(\omega_n^{-k})$, $\hat{g}_k = g(\omega_n^{-k})$, azt kapjuk, hogy
$h(\omega_n^{-k}) = \hat{f}_k \hat{g}_k$, vagyis, ha h fokszáma kisebb, mint n, azaz
$h = \sum_{j=0}^{n-1} h_j x^j$, akkor $\hat{h}_k = \hat{f}_k \hat{g}_k \quad (0 \leq k < n)$.

Innen h meghatározható IFFT-vel.

Így gyors algoritmust kaptunk polinomszorzásra, amely $\approx 15n \log n$
valós lebegőpontos műveletet használ.

A q alapú számrendszerben felírt $f(q) = \sum_{j=0}^{n-1} f_j q^j$ és
$g(q) = \sum_{j=0}^{n-1} g_j q^j$ számok szorzata $h(q) = \sum_{j=0}^{n-1} h_j q^j$,
ha a megfelelő f és g polinomok szorzata az n-nél alacsonyabb fokú
$h = \sum_{j=0}^{n-1} h_j x^j$ polinom.

(A q nem lehet túl nagy, mert kerekítési hibák lépnek fel.)

Igy számok szorzására kapunk gyors algoritmust.

Más gyors algoritmusok is vannak.

DCT és IDCT

A mérnöki gyakorlatban jobban szeretnek valós számsorozathoz valós transzformált sorozatot rendelni.

Tekintsünk egy valós változós valós értékű $2T$ szerint periódikus páros F függvényt
(most célszerűbb lesz T helyett $2T$-t használni.)

Legyen a mintavételi frekvencia az $1/(2T)$ "alapfrekvencia" $2n$-szerese, ahol $n > 2$ egy természetes szám, azaz legyen $\tau = T/n$ és legyen $\tau_0 = \tau/2$.

A mintavételezéssel kapott $f_j = F(\tau_0 + j\tau)$, $j \in \mathbb{Z}$ sorozatot az $f_0, f_1, \ldots f_{n-1}$ értékek egyértelműen jellemzik, mert a sorozat $2n$-szerint periódikus, azaz $f_{j+2n} = f_j \ \ (j \in \mathbb{Z})$ és a párosság valamint $\tau_0 = \tau/2$ miatt $f_{-j-1} = f_j$, ha $0 \leq j < n$.

A F függvényt szeretnénk "koszinuszos" jelek lineáris kombinációjaként előállítani.

Tekintsük a $H_k(t) = \cos(\pi k t/T)$, $k \in \mathbb{Z}$ ugyancsak $2T$ szerint periódikus páros függvényeket.

A H_k függvény mintavételezésével a

$$\cos \frac{\pi k(j+1/2)}{n}, \quad j \in \mathbb{Z}$$

sorozatot kapjuk.

Legyen

$$c_k = \sum_{j=0}^{n-1} f_j \cos \frac{\pi k(j+1/2)}{n}, \quad \text{ha} \quad k \in \mathbb{Z},$$

azaz c_k az $(f_0, f_1, \ldots f_{n-1})$ és a

$$\left(\cos \frac{\pi k}{2n}, \cos \frac{3\pi k}{2n} \ldots \cos \frac{(2n-1)\pi k)}{2n} \right)$$

$\mathbb{R}^n$-beli vektorok belső szorzata.

Az

$$(f_0, f_1 \dots f_{n-1}) \to (c_0, c_1, \dots c_{n-1})$$

leképezés $\mathbb{R}^n$-et önmagába képezi le.

Ezt a leképezést nevezzük
diszkrét koszinusz-transzfomációnak, DCT-nek.

A DCT nyilván lineáris.

Vegyük észre, hogy

$$\sum_{j=0}^{2n-1} (\omega_{4n}^k)^{2j+1} = \omega_{4n}^k \frac{(\omega_{4n}^{2k})^{2n} - 1}{\omega_{4n}^{2k} - 1} = 0,$$

ha $-2n < k < 2n$, $k \neq 0$.

Mivel a koszinusz páros és periódikus,

$$\sum_{j=0}^{n-1} \cos \frac{\pi k(j+1/2)}{n} = \frac{1}{2} \sum_{j=-n}^{n-1} \cos \frac{\pi k(j+1/2)}{n}$$

$$= \frac{1}{2} \sum_{j=0}^{2n-1} \cos \frac{\pi k(j+1/2)}{n}$$

$$= \sum_{j=0}^{2n-1} \left(\omega_{4n}^{k(2j+1)} + \omega_{4n}^{-k(2j+1)} \right) = 0.$$

ha $-2n < k < 2n$ és $k \neq 0$.
Ebből következik, hogy a H_k, $0 \leq k < n$ függvények mintavételezésével kapott $h_k \in \mathbb{R}^n$ vektorok belső szorzata

$$< h_{k_1}, h_{k_2} >= \sum_{j=0}^{n-1} \cos \frac{\pi k_1(j+1/2)}{n} \cos \frac{\pi k_2(j+1/2)}{n}$$

$$= \frac{1}{2} \sum_{j=0}^{n-1} \left(\cos \frac{\pi(k_1+k_2)(j+1/2)}{n} + \cos \frac{\pi(k_1-k_2)(j+1/2)}{n} \right),$$

azaz az előző kiefejezés szerint, ha $0 \leq k_1, k_2 < n$, $k_1 \neq k_2$, akkor 0, ha $0 = k_1 = k_2$, akkor n, ha pedig $0 \neq k_1 = k_2 < n$, akkor $n/2$.

Innen a

$$t \to \frac{c_0}{n} + \frac{2}{n} \sum_{k=0}^{n-1} c_k H_k(t)$$

függvény a mintavételezésnél $t = \tau/2 + j\tau$ pontjaiban megegyezik a kiindulási F függvénnyel.
Speciálisan a DCT invertálható:
$t = \tau/2 + j\tau$ helyettesítéssel

$$f_j = \frac{c_0}{n} + \frac{2}{n} \sum_{k=0}^{n-1} c_k \cos \frac{\pi k(j + 1/2)}{n}.$$

A DCT inverzét inverz diszkrét koszinusz-transzformációnak
IDCT-nek nevezzük.
További hasznos észrevétel, hogy
kapcsolat van a diszkrét koszinusz-transzformáció és a diszkrét Fourier-transzformáció között,
a DCT kifejezhető a DFT-vel:
legyen $g_{2j+1} = f_j$ és $g_{2j} = 0$, ha $j \in \mathbb{Z}$.
Ekkor a g sorozat valós, páros és $4n$ szerinti periodikus.

A diszkrét Fourier-transzformáltja így valós és páros, tehát

$$\hat{g}_k = \frac{\hat{g}_k + \hat{g}_{-k}}{2} = \frac{1}{2}\sum_{j=0}^{4n-1} g_j(\omega_{4n}^{-jk} + \omega_{4n}^{jk})$$

$$= \sum_{j=0}^{2n-1} f_j \frac{\omega_{4n}^{-(2j+1)k} + \omega_{4n}^{(2j+1)k}}{2}$$

$$= \sum_{j=0}^{2n-1} f_j \cos\frac{\pi k(j+1/2)}{n} = \sum_{j=-n}^{n-1} f_j \cos\frac{\pi k(j+1/2)}{n}$$

$$= 2\sum_{j=0}^{n-1} f_j \cos\frac{\pi k(j+1/2)}{n} = 2c_k.$$

Kétdimenziós DFT és DCT

A kétdimenziós DFT egy $(f_{j_1,j_2})_{j_1=0\,j_2=0}^{n_1-1\,n_2-1}$ mátrixhoz $(\hat{f}_{k_1,k_2})_{k_1=0k_2=0}^{n_1-1n_2-1}$ mátrixot rendel.

Definíciója:

$$\hat{f}_{k_1,k_2} = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} \omega_{n_1}^{-j_1 k_1} \omega_{n_2}^{-j_2 k_2} f_{j_1,j_2},$$

$$\text{ha} \quad 0 \le k_1 < n_1, \quad 0 \le k_2 < n_2.$$

A definícióból

$$\hat{f}_{k_1,k_2} = \sum_{j_1=0}^{n_1-1} \omega_{n_1}^{-j_2 k_1} \left(\sum_{j_2=0}^{n_2-1} \omega_{n_2}^{-j_2 k_2} f_{j_1,j_2} \right)$$

$$= \sum_{j_2=0}^{n_2-1} \omega_{n_2}^{-j_2 k_2} \left(\sum_{j_1=0}^{n_1-1} \omega_{n_1}^{-j_1 k_1} f_{j_1,j_2} \right),$$

azaz a kétdimenziós DFT kiszámolható úgy, hogy előbb a mátrix soraira, majd oszlopaira (vagy fordítva) alkalmazunk egydimenziós DFT-t.

A kétdimenziós DCT definíciója

$$c_{k_1,k_2} = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} \cos \frac{\pi k_1 (j_1 + 1/2)}{n_1} \cos \frac{\pi k_2 (j_2 + 1/2)}{n_2} f_{j_1,j_2}$$

$$\text{ha } \; 0 \leq k_1 < n_1, \;\; 0 \leq k_2 < n_2.$$

Ez is kiszámolható úgy, hogy
a mátrix soraira, majd az oszlopaira (vagy fordítva) alkalmazunk egy dimenziós DCT-t.

Tremészetesen mindkét transzformáció általánosítható magasabb dimenziós tömbökre is.

Hangtömörítés
Képtömörítés
PNG
JPEG
DJVu
MPEG

Hibakorlátozó kódolás

A *hibakorlátozó kódokat* két csoportba sorolhatjuk:

hibajelző kódok és hibajavító kódok.

Mindkét típussal foglalkozunk.

Mindkét esetben az üzenethalmaz elemeihez kódszavakat rendelünk és
a kódszavak segítségével próbáljuk a hibákat jelezni, illetve javítani.

Ha az üzenet könnyen megismételhető,
akkor a hangsúly általában a hibajelzésben van,
ha azonban az ismétlés nehéz vagy lehetetlen, akkor a hibajavításra tolódik át.
A hibakorlázozó kódokkal kapcsolatban mindíg feltesszük, hogy
az egyes kódszavak hossza azonos,
a kódszó betűi egy adott véges *abc*, a *kódabc* elemei és
az átvitel során nincs *szinkronhiba*,
vagyis a vétel helyére a kódabcnek ugyanannyi betűje érkezik meg, mint amennyit elküldtünk.

Hibajelző kódok feladata

A hibajelző kódok feladata, hogy a vétel helyén észrevegyük, ha az átvitel során az adat megváltozott.

Minden hibát természetesen nem lehet felderíteni, hiszen abban az esetben, ha egy elküldött kódszó úgy változik, hogy a vétel helyére egy másik kódszó érkezik, akkor a vevőnek semmi oka nincs kételkedni abban, hogy az elküldött kódszó az volt, mint ami megérkezett.

Minden olyan esetben azonban, amikor az érkező jelsorozat különbözik valamennyi lehetséges kódszótól, a vevő biztos lehet benne, hogy az átvitel során sérült a jelsorozat.

Példa

Legyen $d_1, d_2 \dots d_n$ decimális számjegyek egy sorozata, $n \leq 10$.

Egészítsük ki a sorozatot egy $n+1$-edik "számjeggyel", amelynek értéke

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

ha $b_{n+1} = 10$, akkor az X "római számjegy".

Ha valamelyik számjegyet elírjuk,
akkor az összefüggés nyilván nem teljesülhet:

ha d_j helyett d_j'-t írunk,
akkor az összeg $j(d_j' - d_j)$-vel nőtt, ami nem lehet 11-gyel osztható.

Ugyanez a helyzet, ha $1 \leq j < n$-re d_j-t és d_{j+1}-et felcseréljük:

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

Ez az ellenőrző "számjegy" tehát véd az egyszeres tévesztések és a felcserélések ellen.

Ezt használják könyvek ISBN-számának és a magyar személyi számoknak gépelési hibák elleni védelmére.

Példa: paritásbites kód

A legegyszerűbb hibajelző kód a *paritásbites kód*.

Legyen például az üzenethalmaz az n-bites bináris jelsorozatok halmaza és
egészítsük ki ezeket a jelsorozatokat egy $n+1$-edik bittel,
az úgynevezett *paritásbittel*:

amennyiben egy üzenetben az 1-esek száma páratlan,
akkor írjunk a bitsorozat végére egy 0-t,
míg az ellenkező esetben egy 1-et
(vagy fordítva, de egy adott kódban mindíg ugyanazon szabály szerint).

Az így kiegészített $n+1$-bites szavak mindegyikében páratlan sok 1-es van.

Ha most egy ilyen kódszót elküldünk és a vevőhöz olyan szó érkezik, amelyben az egyesek száma páros,
akkor biztos, hogy hiba történt az átvitel során.

Ha viszont az egyesek száma páratlan,
akkor úgy kell tekintenünk (de nem állíthtjuk), hogy nem történt hiba.

Könnyen beláthatjuk, hogy az előbbi eset akkor következik be,
ha az átvitel során páratlan sok helyen sérül a kódszó,
míg az utóbbi akkor, ha páros sok helyen történik változás.

Ez azt jelenti, hogy minden olyan esetben észrevesszük a hibát,
ha egy hiba történik,
de van olyan eset, amikor két hiba történik és ezt nem vesszük észre
(sőt a konkrét esetben páros sok hiba esetén mindíg ez a helyzet).

Ez indokolja az alábbi definíciót.

Hibajelző kód

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

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

Könnyű olyan feltételt adni, amely jellemzi a t-hibajelző, illetve a pontosan t-hibajelző kódokat:

Kódok távolsága és súlya.

A kódabc két egyforma hosszú szavának u-nak és v-nek a *Hamming-távolsága* $d(u,v)$
az azonos pozícióban lévő különböző jegyek száma és
a *kód távolsága* $d(C)$ a különböző kódszópárok távolságainak minimuma.

A kód távolsága csak akkor van értelmezve, ha legalább két kódszó van.

Ha a kódabc egy A additív Abel-csoport,
akkor a kódabc egy u szavának a $w(u)$ *Hamming-súlya* a nullától különböző jegyeinek száma,
míg a *kód* $w(C)$ súlya a nem nulla kódszavak súlyainak minimuma
(ha van nem nulla kódszó, azaz a csoport nem egyelemű).

A Hamming-távolság rendelkezik a távolság szokásos tulajdonságaival, vagyis bármely u, v, z-re.

(1) $d(u, v) \geq 0$;

(2) $d(u, v) = 0$ *akkor és csak akkor, ha* $u = v$;

(3) $d(u, v) = d(v, u)$ *(szimmetria);*

(4) $d(u, z) \leq d(u, v) + d(v, z)$ *(háromszög-egyenlőtlenség)*

Azt is könnyű belátni, hogy
$d(u, v) = w(u - v)$ és $w(u) = d(u, 0)$.

Ha még az is igaz, hogy a kódszavak maguk is Abel-csoportot alkotnak a koordinátánkénti művelettel,
azaz a kódszavak C halmaza az A^n egy részcsoportja,
akkor *csoportkódról* beszélünk.

Ekkor $d(C) = w(C)$.

A továbbiakban egy kód távolságát d és súlyát w jelöli.

(A megadott jelölések kissé pontatlanok,
hiszen ugyanaz a betű jelöli a függvényt, mint két kódszó,
valamint a kód távolságát és hasonló igaz a súlyra is,
de a környezet alapján mindíg világos lesz, hogy éppen minek a jelöléséről van szó).

Mivel két kódszó legalább d helyen különbözik,
így ha egy elküldött kódszó az adatávitel legalább egy, de d-nél kevesebb helyen sérül,
akkor az így kapott szó biztosan nem kódszó.

Ugyanakkor van a kódban két oyan kódszó,
amelynek pontosan d helyen különböznek és
ha az egyiket küldik és ez úgy változik, hogy éppen a másik érkezik meg,
akkor d hiba történt,
de ezt a vétel helyén nem vesszük észre, nem tudunk jelezni.

Ebből következik, hogy a bevezetett távolságfogalommal egy kód akkor és csak akkor t-hibajelző, ha $t < d$ és
akkor és csak akkor pontosan t-hibajelző, ha
$t = d - 1$, tehát nagyobb távolság nagyobb hibajelző képességet jelent.

A paritásbites kód esetén a kód távolsága 2.

Az eredeti üzenethalmaz elemei közötti távolság ugyanis legalább 1 és vannak olyan n-bites sorozatok, amelyek éppen egy helyen különböznek.

Ekkor az egyik üzenetben az 1-esek száma páros a másikban páratlan, vagyis a kiegészítő bit különbözni fog a két kódszóban és a két kódszó éppen 2 helyen különbözik egymástól, ezen kódszavak távolsága 2.

Ugyanakkor azok a kiegészített bitsorozatok, amelyek eredetileg legalább két helyen tértek el egymástól, a kiegészítés után is legalább két helyen fognak különbözni, vagyis ezek távolsága ismét minimum 2 és így a kód távolsága valóban pontosan 2.

Ez azt jelenti, hogy ez a kód pontosan 1-hibajelző, ahogy azt fentebb már megállapítottuk.

A paritásbites kóddal a hibát csak érzékelni, jelezni tudjuk, de a hibás jelsorozatot nem tudjuk kijavítani.

A hiba javításához tudni kellene, hogy a beérkezett jelsorozat melyik pozíción sérült
(és ha a kód nem lenne bináris, akkor azt is, hogy a sérült helyen mi volt eredetileg).

Abból, hogy az egyesek száma páros, tehát tudjuk, hogy történt hiba,
még nem tudjuk megállapítani, hogy melyik bit hibásodott meg, ugyanis bármelyik
(egyetlen vagy páratlan számú)
bit meghibásodása ugyanúgy azt eredményezi, hogy az egyesek száma páros lesz.

Minimális távolságú dekódolás

Említettük, hogy csupán a vett adatból nem mindíg tudjuk megállapítani,
történt-e hiba,
hiszen bármely elküldött kódszó megváltozhat úgy az átvitel során, hogy
bármely másik szó, például akármelyik kódszó érkezzen meg a vétel helyére.

A hibajavításhoz meg kell adni egy úgynevezett
döntés függvényt,
amely bármely lehetséges jelsorozathoz hozzárendel egy és csak egy kódszót.

(Az is lehetséges, hogy nem minden szó esetén akarunk dönteni.)

Ezt a döntési függvényt kell úgy meghatározni, hogy
a *döntési hiba*, tehát az a hiba, hogy
egy beérkezett jelsorozathoz nem a ténylegesen elküldött kódot rendeljük, a lehető legkisebb legyen.

Az előbbi feltételnek megfelelő legjobb függvény nem csupán az átviteli csatornától függ,
hanem az üzenetek eloszlásától is,
ezért helyette általában egy másik döntési függvényt alkalmazunk.

Elég természetesnek tűnik azt feltenni
(bár ez nem mindíg teljesül),
hogy egy vett szóban előforduló kevesebb hiba valószínűbb, mint a több hiba,
vagyis nagyobb valószínűséggel volt az üzenet egy olyan kódszó, amely a vett szótól kevesebb helyen tér el, mint amely több helyen különbözik tőle.

Másként szólva, egy vett szó esetén azt a kódszót választjuk,
amely tőle a lehető legkevesebb helyen tér el,
azaz a távolsága a vett szótól minimális.

Az ilyen döntési függvény által meghatározott dekódolást
minimális távolságú dekódolásnak mondjuk.

Ilyenkor előfordulhat, hogy egy adott szóhoz egynél több minimális távolságra levő kódszó van.

Ekkor vagy kiválasztunk ezek közül egyet, és az lesz a döntés eredménye
(de egy adott döntési függvény esetén az ilyen vett szó esetén mindíg ugyanarra a kiválasztott, minimális távolságra lévő kódszó mellett döntünk!),
vagy az ilyen szó esetén nem döntünk, csupán jelezzük a hibát.
Legyen például $\{0010, 0100, 1111\}$ egy bináris kód.
Ekkor az egyes négybites szavaktól minimális távolságra levő kódszavakat a 9.10 táblázat mutatja.
Látható, hogy négy esetben nem egyértelmű a helyzet.
Egy lehetőség, hogy ezekben az esetekben is dekódolunk és például az elöl álló kódszavakra döntünk.
A másik lehetőség, hogy amennyiben a vett szó az előbbi négy szó valamelyike, akkor nem döntünk, csak jelezzük a hibát.
Ha például a három kódszó három színt, mondjuk a fehéret, feketét és pirosat kódolja a példában megadott sorrendben és mondjuk a kódolt üzenet a fekete volt míg a vétel helyén a 0000 szót kell dekódolni, akkor a táblázat alkalmazásával a fehérre dekódolunk, ami adott esetben igen rossz döntés lehet.

Ebben az esetben célszerűbb nem dönteni,
hanem jelezni a hibát és ha lehet,
akkor megismételtetni ezt az üzenetet, vagy valamilyen más módon,
például a környező pontok színe alapján dönteni.

Azt azért megismételjük, hogy a döntési függvényt a rendszer tervezésekor rögzítettük,
és a továbbiakban mindíg ugyanúgy kell eljárnunk az adott rendszer keretein belül.

A döntési függvény táblázattal való megadása egyszerű,
de rendkívül helyigényes, ezért jobb módszereket fogunk keresni.

Megfigyelhetjük, hogy a dekódolás két részre bontható:
a hibajavításnál megpróbáljuk meghatározni, hogy mi volt az elküldött kódszó (ez a nehezebb),
majd visszaállítjuk az üzenetet.

Hibajavító kód

Egy kód *t-hibajavító*, ha minden olyan esetben helyesen javít,
amikor egy elküldött kódszó legfeljebb t helyen változik meg.

A kód *pontosan t-hibajavító*,
ha t-hibajavító, de nem $t+1$-hibajavító,
azaz van olyan $t+1$ hibával érkező üzenet,
amelyet a kód helytelenül javít, vagy nem javít.

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

Viszont $t \geq d/2$ esetén nincs olyan döntési függvény, amely
t-hibajavító,
mert a kódban van két olyan kódszó, mondjuk u és w, amelyek
pontosan d helyen különböznek.

Irjuk u-ban ebből a d számú pozícióból t helyre a w adott
pozícióján található jegyet, és
jelöljük az így kapott szót v-vel.

A v az u-tól t helyen különbözik, míg w-től
$d - t \leq d/2 \leq t$ helyen.

Ha a dekódolás t-hibajavító lenne,
akkor v-t egyrészt u-ra, másrészt w-re kellene javítani.

Tehát egy d-távolságú kód minimális távolságú dekódolással minden $t < d/2$-re t-hibajavító és pontosan $\lfloor (d-1)/2 \rfloor$-hibajavító.

Általánosabban, tegyük fel, hogy $s \geq t$ természetes számok.

Egy kód t-hibajavító és s-hibajelző,
ha minden legfeljebb t-hibát kijavít és minden legfeljebb s-hibát jelez (ideértve a kijavított legfeljebb t-hibákat is).

Megmutatjuk, hogy ha $t + s < d$,
akkor minimális távolságú dekódolással minden t-hiba kijavítható úgy, hogy minden s-hiba jelezhető.

Ha legfeljebb t-hibát javítunk a minimális távolságú dekódolással, akkor $t < r \leq s$ hiba esetén, ha u volt az eredeti kódszó és v a vett kódszó, akkor bármely u-tól különböző w kódszóra $d(v, w) \leq t$ lehetetlen, mert ebből
$d(u, w) \leq d(u, v) + d(v, w) \leq r + t \leq s + t < d$ következne.

Másrészt, ha egy kód $t + s < d$,
akkor minimális távolságú dekódolással minden t-hiba kijavítható úgy, hogy minden s-hiba jelezhető.

Másrészt, ha egy kód t-hibajavító és s-hibajelző, akkor $t + s < d$.

Valóban, ha u és w két kódszó, amelyek távolsága d és $t + s \geq d$,
akkor az u kódszót t helyen megváltoztatva úgy, hogy ott különbözzön u-tól és megegyezzen w-vel,
akkor ha a v szót vesszük, azt u-ra kell javítanunk, de lehet, hogy w-ből keletkezett legfeljebb s hibával.

Hibajavítás ismert hibahelyekkel

Tegyük fel, hogy egy kód távolsága d és az átvitel során $t + r$ hiba lépett fel,
ahol r hibának ismerjük a helyét
(például, mert a kódbetűket paritásellenőrzéssel viszszük át).

Ha $2t + r < d$, akkor a hibákat ki tudjuk javítani:
Legyen u az eredeti kódszó, v a vett szó, w egy tetszőleges kódszó.

Jelölje $\tilde{u}$,$\tilde{v}$ és $\tilde{w}$ azokat a szavakat, amelyeket úgy kapunk, hogy az adott r helyen álló betűket elhagytuk.

Válasszuk ki ezen "rövidített" kódszavak közül azt, amelyik legfeljebb t helyen tér el $\tilde{v}$-től:
ilyen egyetlen van, $\tilde{u}$, mert $u \neq w$ esetén
$d \leq d(u,w) \leq d(\tilde{u},\tilde{w})+r \leq d(\tilde{u},\tilde{v})+d(\tilde{v},\tilde{w})+r \leq t+r+d(\tilde{v},\tilde{w})$,
ahonnan $d(\tilde{v},\tilde{w}) > t$.

Az $\tilde{u}$ ismeretében u egyértelműen adódik,
mert $u \neq w$ esetén $\tilde{u} \neq \tilde{w}$, hiszen $r < d$.

Másrészt, ha egy kód bármely ismert r helyen és ismeretlen t helyen fellépő hibáját ki tudjuk javítani,
akkor $2t + r < d$.

Ha u és w két kódszó, amelyek távolsága d és $2t + r \geq d$,
akkor az u kódszót $t + r$ helyen megváltoztatva úgy, hogy ott különbözzön u-tól és megegyezzen w-vel,
akkor ha a v szót vesszük, azt u-ra kell javítanunk,
de lehet, hogy w-ből keletkezett legfeljebb t ismeretlen helyű hibával.

Ismétléses kód

Legyen egy binárisan kódolt üzenethalmazunk és küldjük el az üzenetet úgy, hogy minden egyes bitet megháromszorozzunk, azaz ugyanazt a bitet háromszor egymás után küldjük.

A vétel helyén a három összetartozó bit közül legalább kettő azonos lesz, így a minimális távolságú dekódolás esetén a vett három bithez a többségi döntés alapján rendelünk egy bitet.

A döntési hiba még jelentősen csökkenthető, ha az eredeti egy bit helyett nem három, hanem $5, 7, 9, \ldots, 2n+1$ stb., az eredeti bittel azonos jegyet küldünk.

Meghatározott feltételek esetén igazolható, hogy n növekedésével a döntési hiba valószínűsége 0-hoz tart.

Ebből azonban hiba lenne arra következtetni, hogy megtaláltuk a szinte biztosan hibátlan adatátvitel módját.

Egyrészt, mint említettük az előbbi eredmény csak bizonyos feltételek esetén teljesül.

Másrészt nézzük meg, hogy mi ennek az ára.

Az egyes bitek átviteléhez adott, 0-nál hosszabb időre van szükség, így n növekedésével az üzenet egy-egy bitjének átviteléhez szükséges idő is nő és tart a végtelenhez,
vagyis az 1 valószínűséggel hibátlan átvitel esetén egyetlen bitnyi üzenetet sem tudunk továbbítani.

Az átviteli idő növekedése egyben az átviteli költséget is növeli, az is tart a végtelenhez.

Szerencsére a helyzet nem ennyire rossz.

Shannon egy tétele szerint bizonyos feltételek teljesülése esetén lehet az üzeneteket úgy kódolni, hogy az átvitel sebessége egy - csak a csatornától függő -értéket,
a *csatornakapacitást* tetszőlegesen megközelítsen,
miközben a dekódolás hibája tetszőlegesen érték alá szorítható.

A tétel elméleti jelentőségű, ugyanis ilyen kódot nem sikerült konstruálni és még ha sikerülne is, akkor is használhatatlan lenne a gyakorlatban, olyan nagy lenne a kódszavak hossza és olyan nagy lenne a kódszavak száma.

A tétel fontossága mégis felbecsülhetetlen, ugyanis azt igazolja, hogy lehetséges olyan kódot konstruálni,
amelynél mind a sebesség, mind a döntési hiba kielégít egy reális elvárást.

Kétdimenziós paritásellenőrzés

A korább tárgyalt paritáselemes kód segítségével könnyen tudunk egy minimális távolságú dekódolással 1-hibajavító kódot konstruálni.

Legyenek az üzenetek n-bites szavak, és tegyük fel, hogy m üzenetünk van.

Egészítsünk ki minden kódszót egy paritásbittel például páratlan paritásúvá,
majd m ilyen kódszóból alkossunk egy blokkot.

Irjuk egymás alá a blokk $n+1$-bites kódszavait és
most az egy-egy oszlopban álló m-bites sorozatokat egészítsük ki egy-egy paritásbittel, például páros paritásúvá.

Az így kapott $n+1$-bites szóval kiegészítve a blokkot kapjuk az eredeti m üzenet kódját.

A gyakorlatban ezt a kódolási sémát például mágnesszalagon alkalmazzák és ott az egyes szavak nyolc bitből álló bájtok, vagyis $n = 8$.

Ilyenkor szokás az egyes bájtok ellenőrzésére szolgáló paritásbiteket VRC-nek nevezni,
ami a Vertical Redundancy Check (keresztirányú ellenőrzés) kezdőbetűiből álló rövidítés,
míg az ellenőrző bájt az LRC, azaz Longitudinal Redundancy Check (hosszirányú ellenőrzés.)

Ez a rendszer bárhol fellépő egyetlen hiba esetén képes azt javítani.

Ha ugyanis $b_{i,j}$ és csak ez a bit hibás,
akkor pontosan egy hiba van az i-edik szóban,
tehát ennek ellenőrzése során hibajelzést kapunk.

Az összes többi szó ellenőrzése azt adja, hogy azokban nincs hiba, és hasonlóan, a j-edik és csak a j-edik oszlop ellenőrzésénél hibajelzésre kerül sor, vagyis a két eredményből azt kapjuk, hogy az i-edik szó j-edik bitje és csak ez a bit hibás, amit ennek a bitnek a komplementálásával kijavíthatunk.

Eszerint azonban minden olyan esetben, amikor az i-edik és csak az i-edik szóban, valamint a j-edik és csak a j-edik oszlopban kapunk hibajelzést, azt gondoljuk, hogy ez a bit hibásodott meg, és ezt "javítjuk", vagyis az ellenkezőjére változtatjuk.
Pedig könnyen beláthatjuk, hogy ellenőrzésekor ugyanerre az eredményre jutunk akkor is, ha minden oszlopban és minden szóban, kivéve a j-edik oszlopot és i-edik szót, páros számú hiba lép fel (ebben beleértve a hibátlan esetet is 0 hibával), míg a kitünetett i-edik szóban és j-edik oszlopban is a hibák száma páratlan.
Ilyen például, ha az i-edik szóban a $j+1$-edik bit, valamint az $i+1$-edik szó j-edik és $j+1$-edik bitje, tehát összesen három bit hibásodik meg.
A vétel helyén semmilyen módszerrel nem tudjuk eldönteni, hogy valóban egy hiba történt-e, és így helyesen javítunk, vagy a megfigyelt hibajelzés több hiba együttes hatása, aminek következtében vagy egy addig helyes bitet "javítunk" helytelenre, vagy egy tényleg hibás bitet javítunk, de még további, felderítetlen hiba is van a vett üzenetben.

Hasonlóan előfordulhat, hogy volt hiba, de észre sem vesszük, nevezetesen, ha minden szóban és minden oszlopban a hibák száma páros.

Ennek tipikus példája, amikor négy hiba egy téglalap négy sarkában lép fel,
ahol a téglalap két éle egy-egy szóban van.

Végül előfordulhat, hogy egynél több szóban, illetve egynél több oszlopban kapunk hibajelzést,
amikor biztosan tudjuk, hogy volt hiba, de a hibák száma egynél nagyobb,
így javításra ebben a rendszerben nincs lehetőségünk.

Ennek legegyszerűbb példája, amikor pontosan két hiba lép fel.

A most ismertetett rendszert nevezhetjük
kétdimenziós paritásellenőrzésnek.

Ilyet használnak nagy mágnesszalagos tárolóknál
(egy bizonyos rögzítési mód esetén, mert többféle is létezik),
ahol egymás mellé írják ki egy kiegészített bájt 9 bitjét és az adatokat mindíg blokkosan tárolják.

Ebben az esetben keresztirányban páratlanra, míg hosszirányban párosra egészítenek ki.

Hamming-korlát

Ha egy q elemű *abc* n hosszú szavaiból álló C kód t-hiba javító, akkor bármely két kódszóra a tőlük legfeljebb t távolságra lévő szavak halmazai diszjunktak.

Mivel egy kódszótól j távolságra pontosan $\binom{n}{j}(q-1)^j$ szó van, azt kapjuk, hogy

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

Ez a *Hamming-korlát* a kódszavak számára.

Ha az egyenlőség teljesül, akkor a kódot *tökéletesnek* nevezzük.

Mivel kevés tökéletes kód van, a gyakorlatban az alábbi korlát fontosabb.

Singleton-korlát

Ha egy q elemű *abc* n hosszú szavaiból álló C kód távolsága d, akkor minden kódszóból elhagyva $d-1$ betűit (ugyanarról a $d-1$ helyről)
még mindíg különböznek a kódszavak, de csak $n-d+1$ hosszúak.

Innen a kódszavak számára azt kapjuk, hogy
$\natural(C) \leq q^{n-d+1}$, ez a *Singleton-korlát*.

Ha egyenlőség áll, a kódot
maximális távolságú szeparábilis kódnak, MDS-kódnak nevezzük.

Ekkor $\natural(C) = q^k$, ahol $k = n-d+1$.
A szeparábilis (elválasztható) kód elnevezést az indokolja, hogy (bármely) rögzített $d-1 = n-k$ helyen álló betűket elhagyva a kódszavakból, q^k különböző szó marad,
ezért a kódolást végezhetjük úgy, hogy az üzeneteket leképezzük ezekre a szavakra,
majd kiegészítjük ellenörző betűkkel,
így az ellenőrző betűk elválaszthatók a kódoló betűktől.

Lineáris kód

Ahhoz, hogy a kódolás és a dekódolás minél egyszerűbb legyen, a kódoláshoz olyan rendszereket célszerű alkalmazni, amelyek rendelkeznek valamilyen belső struktúrával.

Jó kódok konstruálhatóak algebrai rendszerek segítségével.

A gyakorlatban alkalmazott kódok jelentős része lineáris kód:

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

Ennek a térnek bármely altere egy *lineáris kód*.

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

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

Itt a Singleton-korlát $k \leq n - d + 1$.

Lineáris kódnál mindíg feltesszük, hogy a kódolandó üzenetek K^k elemei, azaz a kódabc elemeiből képzett k-asok.

A paritásbites kód általában nem lineáris, de ha páros sok egyesre egészítünk ki, akkor már lineáris F_2 felett.

Generátormátrix, ellenőrző mátrix, szindróma

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

Ezt a mátrixával jellemezhetjük, ez a kódolás *generátormátrixa*.

Egy a szokásos bázisban vett mátrix pontosan akkor generátormátrix, ha az oszlopai bázist alkotnak a kódszavak terében.

A hibajavításra használható egy (tetszőleges) $H : K^n \to K^{n-k}$ szürjektív lineáris leképezés, amelynek a magja C; egy ilyen leképezést *ellenőrző leképezésnek*, mátrixát egy a kód *ellenőrző mátrixának* nevezzük.

Ha $v \in K^n$, akkor a v-hez tartozó *szindróma* (jellemző), az $s = Hv$ vektor pontosan akkor nulla, ha v kódszó.
A két leképezés csak az köti össze, hogy G képtere H magja: mindkettő a kódszavak halmaza.
Ezért a kódszavak halmazát bármelyik leképezés megadja.
A hibajavítás nem függ G-től, csak a kódszavak halmazától.
Az ellenőrző mátrix segítségével is meghatározható a kód súlya: az ellenőrző mátrixnak pontosan akkor van m oszlopa, amelynek megfelelő vektorok lineárisan függőek, ha van olyan kódszó, amelynek súlya legfeljebb m.
A kódoló leképezést célszerű úgy megválasztani, hogy a kódszavak meghatározott helyein az üzenet betűi álljanak, mert ekkor a hibajavítás után nincs más dolgunk, mint az "ellenőrző" betűket elhagyni.
Ilyenkor *szisztematikus kódolásról* beszélünk.
Lineáris kódolásnál ez elérhető például úgy, hogy elemi oszlopműveletek használatával, hasonlóan, mint a Gauss-eliminációnál.

Átalakítjuk a generátormátrixot. Az elemi oszlopműveletek nem változtatják meg a transzformáció értékkészletét.

A kódszavak betűit alkalmasan permutálva, azt is elérhetjük, hogy az üzenet betűi a kódszónak az előre megadott k helyén állnak:

a permutáció nem változtatja meg a linearitást és a súlyt.

A szindróma felhasználható a hiba javítására.

Szindrómadekódolás

Az előző pont jelöléseivel, ha $s \in K^{n-k}$, legyen $e(s)$ a $H^{-1}(s)$ halmaz egy olyan rögzített vektora, amelynek súlya az adott mellékosztályban minimális.

Ezeket az $e(s)$ vektorokat *mellékosztály-vezetőnek* fogjuk nevezni.

Ha $c \in K^n$ egy kódszó, $v \in K^n$ a vett szó, $e = v - c$ a hiba és ha $w(e) < d/2$, tehát ha a hiba javítható,
akkor $He(s) = s = Hv = He$, így $w(e(s)) \leq w(e)$, ahonnan $w(e - e(s)) < d$.

De $H(e - e(s)) = 0$, így a különbség kódszó,
tehát $e = e(s)$, így $c = v - e(s)$, a hibát kijavítottuk.

A szindrómadekódolás tárigénye sokkal kisebb, mint a táblázattal való dekódolásé,
mert itt csak a mellékosztályvezetőket kell tárolni, de még mindíg nagyon nagy lehet.

Példa:Fano-kód

A 3.4 ábrán látható a *Fano-sík* felhasználható hibajavító kód konstruálására.
Megszámozva a pontokat 1-től 7-ig, a kódszavak az egyenesekhez tartoznak:
olyan bitsorozatok, amelyekben az adott egyenesre illeszkedő pontoknak megfelelő bitek egyesek, a többi nulla, illetve ezek egyes komplemensei.
Kódszó még a csupa nulla illetve csupa egy bitsorozat.
Igy egy $[7, 4, 3]_2$ lineáris kódot kapunk.
Ez a kód tökéletes kód, de nem MDS-kód.

Olyan mátrix, amiből oszlopműveletekkel
(az első oszlopot hozzáadva minden továbbihoz,
majd a kapott második oszlopot hozzáadva az elsőhöz és a harmadikhoz,
ezután a kapott harmadik oszlopot hozzáadva a másodikhoz,
végül a negyedik oszlopot hozzáadva a másodikhoz és a harmadikhoz) a

Generátor mátrixot kapjuk, amely szisztematikus kódot ad, a kódolandó szó a kódszó elejére kerül.

Jelölje b_1, b_2, b_3 és b_4 ezen mátrix oszlopainak megfelelő vektorait $\mathbb{F}_2^7$-nek, $e_1, e_2, \dots e_7$ illetve f_1, f_2, f_3 az $\mathbb{F}_2^7$ illetve $\mathbb{F}_2^3$ szokásos bázisát.

A H leképezést definiáljuk azzal, hogy a

$$b_1, b_2, b_3, b_4, e_5, e_6, e_7$$

bázis első négy vektorát nullába, az utolsó hármat pedig rendre f_1, f_2, f_3-ba viszi.

Mivel $e_1 = b_1 - e_6 - e_7$, $e_2 = b_2 - e_5 - e_7$, $e_3 = b_3 - e_5 - e_6$ és $e_4 = b_4 - e_5 - e_6 - e_7$ a szokásos bázisban a

ellenőrző mátrixot kapjuk.

A Fano-kód pontosan 1-hibajavító-kód.

Példa: Reed-Müller-kódok

$\mathbb{F}_2^t$ pontjait számozzuk meg 1-től 2^t-ig és
legyen $0 < r < t$ rögzített.

A kódszavakat úgy kapjuk, hogy
minden egyes r-dimenziós affin sokasághoz hozzárendelünk egy nulla-egy sorozatot:

az adott affin sokaságra illeszkedő pontoknak megfelelő helyre egyest, a többi helyre nullát írunk,
valamint tekintjük még a csupa nulla és a csupa egyes bitsorozat.

Ez egy bináris $[n, k, d]_2$, ahol $n = 2^t$, $d = 2^r$ és
$k = \sum_{j=0}^{r} \binom{t}{j}$.

A $t = 5$, $r = 4$ paraméterekkel adódó $[36, 6, 16]_2$ kódot használták a Mariner 9 Mars-szonda képeinek Földre küldésére:
egy pixel 64 lehetséges árnyalatot tartalmazott.

Hamming-kód

Az úgynevezett *Hamming-kód* egyetlen hiba javítására alkalmas lineáris kód.

Legyen $m > 1$.

Az ellenőrző mátrix oszlopai (a szokásos bázisban) azok $\mathbb{F}_q^m$ vektorok, amelynek az első nem nulla komponense 1.

A mátrix oszloprangja nyilván m, így a megfelelő lineáris leképezés képtere $\mathbb{F}_q^m$.

Az oszlopok száma
$n = 1 + q + q^2 + \cdots + q^{m-1} = (q^m - 1)/(q - 1)$ és a kódszavak $k = n - m$ dimenziós alteret alkotnak.

Mivel az ellenörző mátrix bármely két oszlopa lineárisan független, a kód távolsága legalább 3.

Több nem lehet, mivel a kód tökéletes 1-hibajavító:
$q^k(1 + n(q-1)) = q^k(1 + q^m - 1) = q^m + k = q^n$.

A hibajavítás a szindróma segítségével könnyen elvégezhető:

ha csak egy hibája van, akkor az e hibavektornak egyetlen nem nulla koordinátája van, legyen ez α.

Az $s = He$ szindróma a H mátrixa valamelyik oszlopának az α-szorosa.

Mivel minden oszlop legelső nem nulla eleme 1, a szindróma legelső nem nulla eleme α.

Ennek ismeretében, a szindrómát osztva α-val, megkereshető, hogy melyik oszlopot kapjuk;
ez a koordinátája volt hibás az üzenetnek.

Polinomkódok

Lineáris kódnál a szavak k hosszú kódolandó szavak tekinthetők $\mathbb{F}_q$ feletti k-nál alacsonyabb fokú polinomoknak is, a betűket nullától indexelve.

Ha a kódolást úgy végezzük, hogy ezt a p polinomot beszorozzuk egy rögzített m-ed fokú g polinommal
($m \in \mathbb{N}^+$),
akkor lineáris kódot és kódolást kapunk, $n = m + k$ hosszú kódszavakkal, mivel a $p \longrightarrow pg$ leképezés kölcsönösen egyértelmű.

Az ilyen típusú lineáris kódolást *polinomkódolásnak* nevezzük, a g a kód *generátorpolinomja*.

A generátorpolinomról feltehetjük (és a továbbiakban is feltesszük), hogy főpolinom,
hiszen osztva a főegyütthatóval, a kódszavak halmaza nem változik.

A generátorpolinomot nem célszerű úgy választani, hogy konstans tagja nulla legyen,
hiszen ekkor minden kódpolinom konstans tagja is nulla,
így a kódszavak nulla indexű betűje nem hordoz információt.

A továbbiakban ezért mindíg feltesszük, hogy a generátorpolinom konstans tagja nem nulla.

Mivel a generátorpolinom is kódszó, a kód súlya nem lehet nagyobb, mint a generátorpolinom súlya és
mivel a k (és így n) növelésével a kódszavak halmaza bővül, a kód súlya csak csökkenhet.

A korábbi tétel szerint elég nagy j-re $g(x)|x^{q^j} - x$, így
$g(x)|x^{q^{j-1}} - 1$,
azaz $n \geq q^j$ esetén a kód súlya már csak kettő.

Egyébként, ha $g(x)|x^l - 1$, akkor $n = l$ esetén a kód *ciklikus kód*:
ha $a_0 a_1 \dots a_{n-2} a_{n-1}$ egy kódszó, akkor $a_{n-1} a_0 a_1 \dots a_{n-2}$ is kódszó:

$$a_{n-1} + a_0 x + a_1 x^2 + \dots a_{n-2} x^{n-1}$$
$$= x(a_0 + a_1 x + \dots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1})$$
$$-a_{n-1}(x^n - 1),$$

így osztható $g(x)$-el.

Polinomkódolás esetén könnyen készíthetünk szisztematikus kódot is:
ha p az üzenetpolinom, akkor $p(x)x^m$-et maradékosan osztva $g(x)$-el $p(x)x^m = q(x)g(x) + r(x)$;

a kódszó legyen $p(x)x^m - r(x)$:
a végén az eredeti üzenet betűi állnak.

Mivel az x^m-mel való szorzás és a maradékképzés lineáris, ez lineáris kódolás.

Az üzenet ellenőrzése is egyszerű:
megnézzük, hogy osztható-e $g(x)$-szel.

CRC-kódok

Egyszerű, csak hibajelzés szolgáló $\mathbb{F}_2$ feletti polinomkódok az úgynevezett CRC,
vagyis Cyclic Redundancy Check, "ciklikus ellenőrzés" kódok.
A kódolás a fent leírt.
Megjegyezzük, hogy $\mathbb{F}_2$ felett
(sőt minden $\mathbb{F}_q$ felett, ahol q kettőhatvány) $r(x) = -r(x)$.

A CRC-kódok hibajelző képessége

A paritásbites ellenőrzéssel már foglalkoztunk.

A többi CRC-polinom a fenti táblában mind vagy irreducibilis, vagy $x+1 = x-1$-szeresei egy irreducibilis polinomnak.

A kód súlya legalább 2, mert x-hatványa nem lehet kódpolinomok között.

A kód súlya mindaddig nagyobb, mint kettő,
ameddig meg nem jelenik a kódpolinomok között egy
$x^{j+l} + x^j = x^j(x^l - 1)$ alakú polinom.

Mivel a konstans tag nem nulla, ez csak akkor lehet, ha $g(x)|x^l - 1$.

Ekkor viszont $x^{il} - 1 = (x^l - 1)(x^{(i-1)l} + x^{(i-2)l} + \cdots + 1)$ is és így $x^{il+j} - x^j$ is többszöröse g-nek.

Ha g egy m-ed fokú $(m > 1)$ irreducibilis polinom, akkor a korábbi tétel szerint $g(x)|x^{2^m} - x$-nek,
azaz $g(x)|x^{2^m-1} - 1$.

Legyen l a legkisebb olyan érték, amelyre $g(x)|x^l - 1$.

Mivel $2^m - 1 = il + j$ esetén $x^j - 1 = x^{2^m-1} - 1 - (x^{il+j} - x^j)$ is osztható $g(x)$-szel, $l|2^m - 1$.

Ellenőrizve a lehetséges értékeket számítógéppel,
l meghatározható.

Ha a kódhossz nem nagyobb, mint l, a kód súlya legalább 3.

Ha a CRC-polinom $x - 1$-szer egy m-ed fokú $g(x)$ irreducibilis polinom,
akkor minden kódszó is $x - 1$ többszöröse, így csak páros lehet a súlya.

A fenti gondolatmenet itt is érvényes a legkisebb l kitevőre,
amelyre $x^l - 1$ többszöröse a kódpolinomnak, $l|2^m - 1$,
aminek alapján l meghatározható.

Itt a kód súlya legalább négy, hiszen nagyobb, mint 2 és páros.

Megjegyezzük, hogy a kód súlya nem lehet túl nagy, ha n nagy.

Például 32 bites CRC polinomnál, ha $n = 84$,
akkor a kód nem lehet 7-hibajavító,
mert $\binom{84}{7} > 2^{32}$, tehát a Hamming-egyenlőtlenség nem teljesülne,
igy távolsága kisebb, mint 15;
ha $n = 124$, akkor a kód lehet 6-hibajavító,
mert $\binom{124}{6} > 2^{32}$,
tehát a Hamming-egyenlőtlenség nem teljesülne, így távolsága kisebb, mint 15 stb.

Végül megjegyezzük, hogy minden CRC-kód jelez minden olyan hibát,
amelynél a hibás bitek egyetlen olyan intervallumba, "hibacsomóba" esnek, amelynek hossza legfeljebb a CRC-polinom foka:
ekkor ugyanis a hibapolinom $e(x)x^j$ alakú, ahol $e(x)$ foka kisebb, mint a CRC-polinom foka, így nem lehet osztható az utóbbival.

Golay-kódok

A $[23, 12, 7]_2$ Golay-kódot az $x^1 1 + x^1 0 + x^6 + x^5 + x^4 + x^2 + 1$ polinom generálja és tökéletes kód.

Ezzel a kóddal védik a műholdas műsorszórás szolgáltatásazonosítását.

A $[24, 12, 8]_2$ Golay-kódot ebből úgy kapjuk, hogy minden kódszót kiegészítünk páros paritásúra.

Ezt a kódot használták a Voyager űrszondák színes képek továbbítására.

A $[11, 6, 5]_3$ Golay-kódot az $x^5 + x^4 + 2x^3 + x^2 + 2$ polinom generálja és tökéletes kód.

A $[12, 6, 6]_3$ Golay-kódot úgy kapjuk, hogy minden kódszót kiegészítünk
úgy, hogy a jegyek összege modulo három nulla legyen.

A kódok szoros kapcsolatban állnak egyszerű csoportokkal:

például S_{23} illetve S_{24} azon permutációi, amelyek a megfelelő bináris kódot önmagába viszik,
egy 10200960, illetve 244823040 elemű egyszerű csoportot alkotnak.

Vandermonde-determináns

Ha

$$x_1, x_2 \dots x_m$$

egy K test elemei, akkor

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & \dots & x_m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{m-1} & x_2^{m-1} & x_3^{m-1} & \dots & x_m^{m-1} \end{pmatrix}$$

mátrix determinánsa

$$\prod_{1 \le i < j \le m} (x_j - x_i)$$

Bizonyítás

Az m szerinti teljes indukcióval:

vonjuk ki a másodiktól kezdve minden sorból a felette álló x_1-szeresét.

Reed-Solomon-kódok

Legyen most K egy tetszőleges véges test, alkossák az abc-t ennek elemei, a K elemszámát jelölje q.

Legyen a K egy nem nulla α elemének multiplikatív rendje n.

Ekkor az α^i, $0 \leq i < n$ elemek páronként különböznek és mindegyik gyöke az $z^n - 1 \in K[z]$ polinomnak,
ezért megadják ezen polinom összes gyökét.

Igy $z^n - 1 = \prod_{i=0}^{n-1}(z - \alpha^i)$.

Legyen $0 < k < n$, $\quad m = n - k$ és $g = \prod_{i=1}^{m}(z - \alpha^i)$.

Ez a polinom egy K fölötti, m-edfokú főpolinom és nyilván osztója a $z^n - 1$ polinomnak.
A g mint generátorpolinom által megadott $[n, k]_q$ polinomkód a g (vagy az α) által generált *Reed-Solomon-kód*.

Most tekintsük a polinomok C halmazának egy c elemét.

Mivel g osztója c-nek, g minden gyöke gyöke c-nek is, vagyis $c(\alpha^i) = 0$, ha $0 \leq i \leq m$.

Fordítva, ha $u \in K^n$ és minden $1 \leq i \leq m$-re $u(\alpha^i) = 0$,
akkor valamennyi i-re $z - \alpha^i$ osztója u-nak,
de akkor ezek legkisebb közös többszöröse,
azaz a szorzatuk, tehát g is osztója u-nak,
vagyis ez esetben u a kódhoz tartozik.

Ez azt jelenti, hogy $u \in K^n$ akkor és csak akkor eleme a kódnak,
ha g valamennyi gyöke egyben u-nak is gyöke,
vagyis ha minden $1 \leq i \leq m$-re $\sum_{j=0}^{n-1} (\alpha^i)^j u_j = 0$.

Igy a $h_{i,j} = \alpha^{ij}$ $(1 \leq i \leq m, 0 \leq j < n)$ mátrix egy ellenőrző mátrix:
a hozzá tartozó H lineáris leképezésre $Hu = 0$,
akkor és csak akkor, ha $u \in C$.

A kód súlyának meghatározásához megmutatjuk, hogy H mátrixának bármely m oszlopa lineárisan független.

Legyen $0 \leq j_1 < \cdots < j_m < n$ és nézzük a mátrix j_1 indexű oszlopait.

Ezek a mátrix egy m-edrendű kvadratikus részmátrixát adják, amelynek l-edik oszlopában az i-edik elem
$h_{i,j_1} = (\alpha^i)^{j_1} = (\alpha^{j_1})^i$.
Most nézzük ezen részmátrix determinánsát.

A determináns l-edik oszlopában minden elemből kiemelhető α^{j_1}.

Mivel a kiemelt elem nem nulla, ezért az eredeti determináns akkor és csak akkor 0,
ha a kiemelés után kapott determináns értéke 0.

A kapott determináns l-edik oszlopában α^{j_1} egymás után következő hatványai állnak, a 0 kitevős hatvánnyal kezdve,
vagyis ez egy Vandermonde-determináns.

Igy az előző állítás szerint a determináns értéke
$\prod_{0 \leq s < t < m} (\alpha^{j_s} - \alpha^{j_t}) \neq 0$,
ami azt jelenti, hogy a mátrix bármely m oszlopa lineárisan független.

Ebből a kód d távolsága nagyobb, mint m
és igy (mivel nagyobb nem lehet) $d = n - k + 1$ azaz a kód MDS-kód,
tehát elég nagy m esetén több hiba is javítható.

Reed-Solomon-kód dekódolása

A Reed-Solomon-kód lineáris, tehát a hiba javítható például a szindrómadekódolással,
de mutatunk egy ennél lényegesen praktikusabb hibajavítást.
Legyen adott egy $[n, k, d]_q$ Reed-Solomon-kód,
$m = n - k$, $d = n - k + 1 = m + 1$, $g = \prod_{i=1}^{m}(z - \alpha^i)$ a kód generátorpolinomja, e a hibavektor és
$L(z) = \prod_{\{j:e_j \neq 0\}}(1 - \alpha^j z)$ az úgynevezett *hibahelypolinom*.
Ennek ismeretében a hibák helye meghatározható:
megkeressük, hogy mely α^{-j}-k gyökei $L(z)$-nek és ezen j-k megadják a hibák helyét.
Legyen $E(z) = \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z)$ az úgynevezett *hibaértékpolinom*, ahol $L_j(z) = L(z)/(1 - \alpha^j z)$, ha $e_j \neq 0$.

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

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

A következő tétel lehetővé teszi a két polinom gyors és igen kis tárigényű kiszámítását a szindróma segítségével.

Tétel

Legyen $s(z)$ a szindrómához tartozó polinom.

Az előző pont jelöléseivel tegyük fel, hogy a hibahelyek száma, azaz $L(z)$ fokszáma legfeljebb $m/2$
(ami azzal ekvivalens, hogy kisebb, mint $d/2$,
azaz hibajavítás egyáltalán végezhető).

Alkalmazzuk a bővített euklideszi algoritmust az $a(z) = z^m$ és $b(z) = s(z)$ polinomokra.

Az ottani jelölésekkel legyen l a legkisebb index, amelyre $\deg(r_i) < m/2$ és legyen $r_l = ax_l + by_l$.

Ekkor $y_l(0) \neq 0$ és $L(z) = y_l(z)/y_l(0)$, $E(z) = r_l(z)/y_l(0)$.

Bizonyítás

Először megmutatjuk, hogy z^m osztja az $E(z) - L(z)s(z)$ polinomot,
ahol $s(z) = s_0 + s_1 z + \cdots + s_{m-1} z^{m-1}$ a szindrómához tartozó polinom.

Valóban

$$E(z) - L(z)s(z) = \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z) - L(z) \sum_{i=0}^{m-1} s_i z^i$$

$$= \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z) - \sum_{i=0}^{m-1} L(z) \left(\sum_{j=0}^{n-1} (\alpha^{i+1})^j e_j \right) z^i$$

$$= \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z) - \sum_{j=0}^{n-1} e_j L(z) \sum_{i=0}^{m-1} (\alpha^{i+1})^j z^i$$

$$= \sum_{\{j:e_j \neq 0\}} \left(\alpha^j e_j L_j(z) - \alpha^j e_j L(z) \sum_{i=0}^{m-1} (\alpha^j)^i z^i \right)$$

$$= \sum_{\{j:e_j \neq 0\}} \left(\alpha^j e_j L_j(z) - \alpha^j e_j L(z) \frac{1 - (\alpha^j z)^m}{1 - \alpha^j z} \right)$$

$$= \sum_{\{j:e_j \neq 0\}} \left(\alpha^j e_j L_j(z) - \alpha^j e_j L(z)(1 - (\alpha^j z)^m) \right)$$

$$= z^m \sum_{\{j:e_j \neq 0\}} \alpha^{j(m+1)} e_j L_j(z).$$

Ez azt jelenti, hogy alkalmas $f(z)$ polinommal
$E(z) = f(z)z^m + L(z)s(z)$.

Igy z^m és $s(z)$ legnagyobb közös osztója $E(z)$-nek és fokszáma legfeljebb annyi, mint $E(z)$ fokszáma, ami kisebb, mint $m/2$.

Igy van olyan maradék az euklideszi algoritmus alkalmazása során, amelynek fokszáma kisebb, mint $m/2$.

Az $E(z) = f(z)z^m + L(z)s(z)$ egyenlet $y_l(z)$-szereséből kivonva az

$$r_l(z) = a(z)x_l(z) + b(z)y_l(z) = z^m x_l(z) + s(z)y_l(z)$$

egyenlet $L(z)$-szeresét azt kapjuk, hogy (1)

$$E(z)y_l(z) - L(z)r_l(z) = (f(z)y_l(z) - L(z)x_l(z))z^m.$$

Azt akarjuk megmutatni, hogy a zárójelben álló polinom nulla.
A bővített euklideszi algoritmus az
$r_0 = a, r_1 = b, x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1$ kezdĂľértékkel indul.
Megmutatjuk, hogy (2)

$$\deg(y_j) = \deg(a) - \deg(r_{j-1})$$

és

$$x_{j-1}y_j - x_j y_{j-1} = (-1)^{j-1}, \quad \text{ha } j > 0.$$

Mindkét állítás teljesül $j = 1$-re.

Indukcióval

$$\deg(y_{j+1})\deg(y_{j-1} - q_j y_j) = \deg(q_j y_j) = \deg(q_j) + \deg(y_j)$$

$$= \deg(r_{j-1}) - \deg(r_j) + \deg(a) - \deg(r_{j-1})$$

$$\deg(a) - \deg(r_j)$$

és

$$x_j y_{j+1} - x_{j+1} y_j = x_j(y_{j-1} - g_j y_j) - (x_{j-1} - q_j x_j) y_j = (-1)^j.$$

Térjünk vissza (1)-hez.
Mivel l választása és (2) miatt

$$\deg(y_l) = \deg(a) - \deg(r_{j-1}) \leq m - m/2 = m/2.$$

$\deg(E) < m/2$, $\deg(r_l) < m/2$, $\deg(L) \leq m/2$, a bal oldal foka kisebb, mint m,
így (1)-ben a zárójelben csak nulla állhat.

Innen $Ey_l = Lr_l$ és $fy_l = Lx_k$.

Mivel definíciójuk szerint E és L relatív prímek, valamint (3) szerint x_l és y_l is, innen az következik, hogy
L osztója y_l-nek és y_l osztója L-nek, tehát asszociáltak,
azaz $L = cy_l$ valamely nem nulla konstassal.

Innen $E = cr_l$ ugyanazzal a konstanssal.

Mivel L konstans tagja 1, kapjuk az állítást.

Kódrövidítés

Néhány kód, például a Reed-Solomon-kód csak meghatároztott hosszakban konstruálható.

Ilyenkor segít a kódrövidítés.

Tetszőleges kódra gyűjtsük össze mindazokat a kódszavakat, amelyekben egy adott helyen egy adott betű áll.

Csak ezeket fogjuk használni és a kódolás után az adott helyen álló adott betűt kihagyjuk,
a dekódolás előtt pedig újra beírjuk.

A kódrövidítés nem csökkenti a távolságot
(ha a rövidített kódnak egyáltalán még van távolságra).

Lineáris kódnál azokat a kódszavakat érdemes felhasználni a rövidített kódban,
amelyekben az adott helyen nulla áll,
mert ekkor a rövidített kód is lineáris lesz.

Ha egy $[n, k, d]_q$ lineáris kódot igy röviditünk,
akkor azon kódszavak C' altere,
amelyekben az adott helyen nulla áll az eredeti kódszavak C alterének egy alterét,
így a C Abel-csoportnak egy részcsoportját alkotja,
továbbá bármely két C-beli kódszó különbsége,
amelyekben az adott helyen ugyanaz a betű áll, a C''-ben van,
igy C' indexe C-ben legfeljebb q, ahonnan C'-nek legalább q^{k-1} eleme van.

Igy k vagy nem változik, vagy eggyel csökken.

Ha az eredeti kód MDS-kód volt és $k > 1$, akkor a rövidített is az marad,
mert a $d = n - k + 1$ egyenlőségben a bal oldalon d csak nőhet,
a jobb oldalon n eggyel csökken, k viszont legfeljebb eggyel csökkenhet,
így a Singleton-korlát miatt egyik oldal sem változhat.

Kódok direkt szorzata

úgy mint a kétdimenziós paritásellenőrzésnél, két kód felhasználásával készíthetünk egy harmadik kódot:
előbb keresztirányban kódolunk az első kóddal, majd hosszirányban a másodikkal, vagy fordítva.

Az így kapott kód a kódok direkt szorzata.

Ha az egyes kódok távolsága d_1 és d_2, akkor a direktszorzatuk távolsága legalább $d_1 d_2$; valóban, két különböző kódszó, ha valamely sorban különbözik, akkor ott legalább d_1 helyen különbözik és legalább d_2 ilyen sornak kell lennie, mert egyébként nem lehetne olyan oszlop, amelyben a két kódban legalább d_2 helyen különbözik.

Például a DVD-n az adatokat (egyebek közt) egy $[208, 192]_{256}$ és egy $[182, 172]_{256}$ rividített Ree-Solomon-kód direkt szorzata védi.

Kaszkád kódok

Egy további kódötvöző eljárás a *kaszkád kód*.

Tegyük fel, hogy egy kód betűi megfeleltethetők egy másik kód adott hosszúságú szavainak.

Kódoljuk először az első kóddal, majd a kapott kódszó betűit kódoljuk második kóddal.

Ha az első kód távolsága $d_1 d_2$, hiszen két különböző kódszó az első kódolás után legalább d_1 betűben
és ezek mindegyikének a kódja a második kódolá után legalább d_2 helyen különbözik.

A legegyszerűbb példa kaszkád kódra,
amikor egy $[n, k]_{256}$ Reed-Solomon-kód után bájtonként paritásbitet képezünk.

Adatátszövés

Az átvitel során a hibák gyakran *hibacsomókban*, idegen szóval *burstökben* jelentkeznek.

Bár például a Reed-Solomon-kódok alkalmasak rövidebb hibacsomók javitására is,
a hosszabb hibacsomók túlterhelik a kódot.

Ez ellen úgy védekezhetünk, hogy a kódolás után az egyes blokkok adatait szétszórjuk:
ez az *adatátszövés*.

A legegyszerűbb esetben valahány adott hosszúságú blokkot sorfolytonosan helyezünk el egy mátrixban,
majd az adatokat oszlopfolytonosan olvassuk ki onnan,
dekódolás elött pedig forditva végrehajtva ezt, visszaállitjuk az eredeti sorrendet.

Algoritmusok

Számítási modellek

Számítási eljárás

Egy *számítási eljárás* alatt egy $C = (Q, Q_b, Q_k, f)$ négyest értünk, ahol Q az állapotok halmaza a $Q_b \subset Q$ és $Q_k \subset Q$ részhalmazai a bemeneti allapotok, ill. kimeneti állapotok halmazai, az $f : Q \to Q$ átmeneti függvény pedig egy olyan függvény, amely Q_k elemeit pontonként fixen hagyja, azaz amelyre $f(q) = q$, ha $q \in Q_k$. Minden $x \in Q_b$ bemeneti állapot definiál egy $q_0, q_{1,2} \ldots$ számítási sorozatot a

$$q_0 = x \quad \text{és} \quad q_{n+1} = f(q_n), \quad \text{ha} \quad n \geq 0$$

összefüggéssel.

Azt mondjuk, hogy az x bemenetre a számítási sorozat n lépésben véget ér, ha n a legkisebb olyan egész, amelyre $q_n \in Q_k$; ekkor $q_n = q_{n+1} = q_{n+2} = \ldots$ a számítás eredménye.
Előfordulhat, hogy egy számítási sorozat nem ér véget.
PL. Euklideszi algoritmus

Szimulálás

Azt mondjuk, hogy a

$$C' = (Q', Q'_b, Q'_k, f')$$

számítási eljárás a

$$C = (Q, Q_b, Q_k, f)$$

számítási eljárást *szimulálja*, ha van olyan $g : Q_b \longrightarrow Q'_b$ függvény, a bemeneti kódolás, olyan $h : Q' \longrightarrow Q$ függvény, az állapotdekódolás és olyan $k : Q' \longrightarrow \mathbb{N}^+$ függvény, hogy
(1) ha $x \in Q$, akkor a C számítás pontosan akkor adja az y eredményt, ha van olyan $y' \in Q'_k$, hogy $g(x)$ bemenettel a C' számítás az y' eredményt adja, és $h(y') = y$;

(2) ha $q' \in Q'$, akkor $f(h(q')) = h(f'^{k(q')}(q'))$, ahol $f'^{k(q')}$ azt jelenti, hogy az f' leképezést $k(q')$-ször ismételjük.
Bármely számítási eljárást szimulálja saját magát.
Ha a C' számítási eljárás szimulálja a C számítási eljárást, a C'' számítási eljárás pedig szimulálja a C'-t, akkor C'' szimulálja C-t.
Például: bővített Euklideszi algoritmus

Szimulációs sebességének összehasonlítása

A szimuláció definíciójában szereplő k függvény megadja, hogy a szimulált eljárás egy lépését (a q állapottól függően) a szimuláló eljárás hány lépésben szimulálja.
Ha a k azonosan 1, akkor azt mondjuk, hogy a szimuláció valós idejű.
Ha a k függvény korlátos, akkor úgy tekintjük, hogy a sebességkülönbség nem lényeges.
Az alábbi definíció, amelybe a "konstans elhanyagolása" be van építve, az ilyen típusú sebesség összehasonlításokat teszi egyszerűen

Ordó Legyen $f : \mathbb{N} \to \mathbb{R}$ egy számsorozat.
Jelölje $O(f)$ (nagy ordó f, vagy $O(f(n))$ mindazon $g : \mathbb{N} \to \mathbb{R}$ számsorozatok halmazát, amelyekre van olyan (g-től függő) $C \in \mathbb{R}^+$ konstans és $N \in \mathbb{N}$ index, hogy $|g(n)| \leq C|f(n)|$, ha $n \geq N$.
Ha f és f^*, ill. g és g^* véges sok tag kivételével megegyeznek, akkor $g \in O(f)$ pontosan akkor teljesül, ha $g^* \in O(f^*)$ teljesül.
Ezért a jelölést akkor is használni fogjuk, ha f vagy g (vagy mind kettő) véges sok indexre nincs értelmezve.
Gyakran pontatlanul $g \in O(f)$ helyett azt írják, hogy $g = O(f)$.
Ha g egy legfeljebb k-ad fokú polinom, akkor $g(n) \in O(n^k)$, vagy pontatlanabbul $g(n) = O(n^k)$.

Algoritmus

Több pédát láttunk már algoritmusra, de az algoritmus fogalmát nem definiáltuk. Ez nem okoz problémát minaddig, amíg olyan problémákkal nem kerülünk szembe, amelyeknek a megoldására nem találunk algoritmust.

Ha ilyen problémára akadunk, felmerül, hogy van-e egyáltalán algoritmus az adott problémára.
Ha meg akarjuk mutatni, hogy nincs, akkor definiálnunk kell, mit is értünk algoritmuson.
Mivel több gyakorlati problémára nincs algoritmus, az ilyen negatív eredmények nagyon fontosak.
Olyan számítási eljárások érdekelnek bennünket, amelyek számítógépen szimulálhatók.
Bizonyos számítási eljárások biztosan nem szimulálhatók a számítógépen.
Például valós számok lánctörtközelítéseinek meghatározása az euklideszi algoritmushoz nagyon hasonló számítási eljárás adható, azonban számítógépen nem tudjuk szimulálni, hiszen valós számokat kellene ábrázolnunk, ami lehettlen teljes pontossággal számítógépen ábrázolni.
Már két valós szám összehasonlítása is gondot okozna: hiába olvassuk sorba a számok tizedes jegyeit, bár az előbb-utóbb kiderül, ha a két szám nem egyenlő, az egyetlen lépésben sem derül ki, hogy a számok egyenlőek.

Ha átgondoljuk, hogy mit is kell algoritmus alatt értenünk, amit mechanikusan végre tudunk hajtani, papírokra ceruzával jelet írhatunk, azok közül egyeseket kiradírozva felülírhatunk, vagy a jelsorozat elejére vagy végére újabb jeleket írhatunk.
Mivel a jeleket sorfolytonosan olvassuk és írjuk, feltehetjük, hogy adott számú papírszalaggal dolgozunk, amelyek azonban akármennyire meghosszabbíthatók mindkét végükön, de mindíg csak egy véges rész az amin jelek vannak.
Eközben véges sok dolgot fejben tarthatunk, így nem lényeges megszorítás, ha feltesszük, hogy egyszerre csak egy jelet olvasunk és írunk minden szalagon.
Látszólag szükségünk lenne még beszúrásokra is, ez azonban radírozás és arrébb írás segítségével megoldható.
Úgy tűnhet, hogy növelné lehetőségeinket, ha két dimenzióban használnánk a papírt; ez megfelene annak, hogy végtelen sok papírszalagunk van, de persze minden időpontban csak véges sok szalagra van írva valami.
Azonban egy papírlapot csigavonalban haladva egy szalaggá vághatjuk fel (csak egyik irányban végtelen!).

Így arra a következtetésre juthatunk, hogy algoritmus formájában azok a számítási eljárások adhatók meg, amelyek úgynevezett Turin-gépen szimulálhatók.

Turin-gépek

Egy Turin-gép $k \geq 1$ darab szalagból és egy vezérlőegységből áll.
A szalagok mindkét irányban végtelen sok mezőre vannak osztva.
Minden mezőn egy-egy betű van egy véges abc-ből, úgy, hogy véges sok mező kivételével minden mezőn a szóköz (üres jel) $\sqcup$ áll:
Az egyszerűség kedvéért a továbbiakban a szalag jobb és bal szélén álló végtelen sok üres mezőt nem jelezzük.
A vezérlőegység véges sok, úgynevezett belső állapotban lehet.
Az állapotok között van egy a s start állapot és egy h halt állapot.
Minden szalaghoz tartozik egy író-olvasó fej.
Az alábbi példában két szalag van és a vezérlőegység a b belső állapotban van.

Kezdetben a vezérlőegység az s start állapotban van.
Minden lépésben minden fej elolvassa azt a jelet, amely éppen a fej alatt van, majd három dolog történik, a leolvasott jelektől és a vezérlőegység belső állapotától függően: minden fej felülírja az olvasott jelet (lehet, hogy ugyanarra, amibe volt), minden fej egymástól függetlenül elmozdul egy mezővel jobbra vagy balra, vagy helyben marad és a vezérlőegység átmegy másik állapotba.
Ha a gép a h halt (vagy befejező) állapotba jut, a gép megáll (mielőtt bármit is tenne a szalagokkal).
Matematikailag egy T Turin-gép egy $(T = B, A, \varphi)$ hármas, ahol az A, B véges halmazok a szalagábécé, ill. a belső állapotok halmaza, $\sqcup \in A$, $s, h \in B$ és

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

egy tetszőleges leképezés.
A $<, >$, ill. $=$ jelek azt jelentik, hogy az adott szalagon a fej balra lép, jobbra lép, ill. helyben marad.
Ha nagyon precizek akarunk lenni, akkor a $k \in \mathbb{N}^+$ számot (szalagok számát), a $\sqcup$ szóköz jelet és az s, h start és halt

állapotokat is feltüntethetjük a jelölésben: $T = (k, B, A, \sqcup, s, h, \varphi)$.
Az, hogy

$$\varphi : (h, a_1, \dots a_k) \to (b', a_1' \dots a_k', c_1 \dots c_k)$$

ahol $b, b' \in B$ és, ha $1 \leq i \leq k$, akkor $a_i, a_i' \in A$, $c_i \in \{<, =, >\}$,
azt jelenti, hogy a gép egy lépése a következő:
ha a t időpontban b a belső állapota és az egyes szalagokról az $a_1 \dots a_k$ betüket olvassa, akkor a $t+1$ időpontra a b' belső állapotba megy át, az olvasott betűk helyére az $a_1' \dots a_k'$ betűket írja és az i-edik szalagon a fej balra lép, jobbra lép, ill. helyben marad, attól függően, hogy c_i a $<$, a $>$, vagy az $=$ jel.
Mivel a Turing-gép a h halt állapotban úgysem csinál semmit megállapodhatunk abban, hogy

$$\varphi : (h, a_1 \dots a_k) \to (h, a_1 \dots a_k, =, \dots, =).$$

Turing-gép mint számítási eljárás; bemenet és kimenet

Az előző definíció jelöléseivel egy Turing-gép aktuális állapotát egy

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

sorozat írja le, ahol $\alpha_i \in A^*$ szó az i-edik szalagon balról jobbra olvasott betűk az első nem üres jellel kezdve és a fej alatti betűvel végezve, a $\beta_i \in A^*$ szó pedig az i-edik szalagon jobbról balra olvasott betűk az első nem üres jellel kezdve, és a fejtől jobbra álló betűvel végezve, mindkettő lehet üres.
A bemeneti állapotok azok az állapotok, amelyekre $b = s$, a kimeneti állapotok pedig azok az állapotok, amelyekre $b = h$.
Könnyű megadni az állapotok halmazán a Turing-gép működésének megfelelő leképezést három függvény segítségével: az egyik egy szó utolsó betüjét adja vissza, a másik a szó többi részét, a harmadik pedig a szó végére ír egy adott betűt.
Mindig feltesszük, hogy az induláskor minden β_i az üres szó, tehát az α_i-k a bemeneti szavak, a fejek a bemenet jobb szélén állnak.

Ha azonban semmit sem tudunk a bemeneti szavakról, akkor például azt a feladatot sem tudjuk Turing-géppel megoldani, hogy töröljük le a szalagokat, hiszen akármeddig lépkedünk balra, nem tudjuk, van-e még valami ettől is balra, így soha nem állhatunk meg.
Valamit tehát még tudnunk kell a bemenetről.
Legegyszerűbb feltenni, hogy $\alpha_i \in A_0^*$, ahol $A_0 = A \setminus \{\sqcup\}$, azaz, hogy a bementi szavak nem tartalmaznak üres jelet.
Ha mást nem mondunk, ezzel a feltevéssel élünk, bár kevesebb is elég, például hogy legfeljebb adott számú $\sqcup$ jel van a bemenetben egymás mellett, vagy a bemenet bal szélét valamely speciális sorozat jelzi.
Fontos, hogy csak a bemenetnél élünk ilyen erős megszorítással, a számítás közben nem.
A kimenetre hasonló megállapítások érvényesek, mint a bemenetre: a megálláskor az α_i szavakat tekintjük kimenetnek a β_i szavakat pedig szemétnek, sőt, ha mást nem mondunk, csak az α_i szavak végét, az utolsó üres jel utáni betűket tekintjük kimenetnek, a többi része α_i-nek szemét.

Ha Turing-gépeket össze akarunk kapcsolni a szemét zavaró lehet.
Meg fogjuk mutatni, hogyan lehet tőle megszabadulni.
Ha csak $m < k$ bemeneti szóról beszélünk, akkor feltesszük, hogy az első m szalagra vannak felírva, a többi szalag az induláskor üres.
Speciálisan, ha csak egy szó a bemenet az az első szalagon van ez a standard input.
A bemenet hosszán a bemeneti szavak hosszának összegét értjük.
Hasonlóan, ha $n < k$ kimeneti szóról beszélünk, akkor feltesszük, hogy az utolsó n szalagra vannak felírva a kimenetkor, a többi szalag tartalma szemét.
Speciálisan, ha csak egy kimeneti szóról beszélünk, akkor az az utolsó szalagon van, ez a standard output.
Néha az utolsó elötti szalagot másik kimeneti szalagként, mint szabványos hiba szalagot használjuk.
A kimenet hosszán a kimeneti szavak hosszának összegét értjük.
A Turing-gépeket A_0 elemeinek száma szerint szokás elnevezni: ha A_0 egyelemű, akkor unáris, ha kételemű, akkor bináris stb. gépről beszélünk.

Mejegyzés

A Turing-gépeknek nagyon sok, minden lényeges szempontból ekvivalens definíciója van.

Turing-gép szimulálása csökkentett jelkészlettel

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

Bizonyítás

Az A elemeit alakalmas n-re A' elemeiből alkotott n-esekkel kódolljuk úgy, hogy A üres jelének kódja az A' üres jeléből alkotott n-es legyen.
Ha A'-nek legalább három eleme van, akkor a kódolást lehet úgy is választani, hogy más A-beli jel kódja ne tartalmazza az üres jelet, csak az üres jelé.

A T' konstrukcióját az $A = \{0, 1, 2, 3\}$ és $A' = \{\sqcup, I\}$ esetben fogjuk részletesen bemutatni, de ebből világos lesz az általános eset is.
Feltéve, hogy A-ban a 0 az üres jel, legyen $n = 2$ és válasszuk a $0 \to \sqcup\sqcup$, $1 \to \sqcup I$, $2 \to I\sqcup$, $3 \to II$ kódolást.
Minden $h \neq b \in B$ belső állapotához T-nek a T' gépnek a $b, b_\sqcup, b_I$ a b_i $i \in A$, valamint a $b_{i,c}$ $i \in A$ és $c \in \{<, >\}$ belső állapotai tartoznak; ezért többszörözzük meg minden $b \neq h$ esetén a belső állapotokat, hogy ezek segítségével emlékezzünk dolgokra.
Ha a T' a gép a b belső állapotban van, akkor mindíg egy kódszó jobb szélén áll. Elolvassa egy kód jobb oldali betűjét, attól függően, hogy mit olvasott a $b_\sqcup$ vagy b_I állapotba megy át és balra lép.
Most attól függően, hogy itt mit olvasott, a b_i állapotok valamelyikébe megy át, ezzel megjegyezve, hogy milyen betű kódját olvasta a két lépésben, a szalagra i^* kódjának bal oldali betűjét írja és jobbra lép, itt i=0, ha a $b_\sqcup$ állapotban voltunk és $\sqcup$ betűt olvastunk, i=1, ha b_I állapotban voltunk és $\sqcup$ betűt olvastunk stb., és $\varphi(b, i) = (b^*, i^*, c)$.
A b_i állapotban, ha a c az $=$ jel, akkor a szalagra i^* kódjának második betűjét írjuk, átmegyünk a b^* állapotba és helyben

maradunk.
Egyébként a szalagra i^* kódjának második betűjét írjuk, az i és c értékének megfelelő $b_{i,c}$ állapotba megyünk át, és c értékének megfelelően balra vagy jobbra mozgunk.
A $b_{i,c}$ állapotban azt írjuk a szalagra, amit olvastunk a c értékének megfelelően balra vagy jobbra mozgunk, és a b^* állapotba megyünk át.
A T gép bármely lépését T' legfeljebb 4 lépésben szimulálja.
Általános esetben, amikor A betűit A' betűiből képzett n hosszú szavaknak feleltetjük meg, minden lépést legfeljebb $2n$ lépésben tudunk szimulálni.
$\triangle$

Szavak kódolása számmá és vissza

Sokszor szükség van arra, hogy egy Turing-gép bemeneti szavait számnak tekintsük. Ilyenkor mindíg feltesszük, hogy a gép A ábécéje a $\{0, 1, \ldots r-1\}$ számjegyekből áll, és 0 az üres jel.
Egy A^*-beli $\alpha = a_n a_{n-1} \ldots a_0$ bemeneti szó vagy üres szó, vagy nem 0-val kezdődik és r alapú számrendszerben az $|\alpha|_r = \sum_{i=0}^{n} a_i r^i$

számot reprezentálja.
Az $\alpha \to |\alpha|_r$ leképezés kölcsönösen egyértelmű képezi le A^* nem 0-val kezdődő szavait $\mathbb{N}$-re.
Ha csak A_0^*-beli szavakat akarunk számmá kódolni, akkor az $\alpha \to |\alpha|_{r-1}$ leképezést használhatjuk, ahol természetesen $\alpha = a_n a_{n-1} \dots a_0$ esetén $|\alpha|_{r-1} = \sum_{i=0}^{n} a_i (r-1)^i$, de itt a jegyek között már r-1 is szerepel annnak ellenére, hogy $r-1$ alapú számrendszert használunk.
Az $\alpha \to |\alpha|_{r-1}$ leképezés kölcsönösen egyértelműen képezi le A_0^*-ot $\mathbb{N}$-re, ami teljes indukcióval könnyen belátható.
Például egy n darab egyesekből álló α szóra $|\alpha|_1 = |\alpha| = n$, ezért egy ilyen szót az n szám unáris kódjának nevezzük.
Egy unáris kódban felírt szám Turing-gép általi konvertálása egy $\alpha \in A_0^*$ szóvá, amire $|\alpha|_{r-1} = n$, vagy fordítva hasonlóan végezhető, mint a példák között leírt unáris-bináris konverzió.
Ugyancsak hasonlóan végezhető egy unáris kódban felírt szám konvertálása egy $\alpha \in A^*$ szóvá, ha tudunk annyit a szóról, hogy nem okoz gondot a bal, ill a jobb szélének a megtalálása.

Turing-gép szimulálása egy szalaggal

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

Bizonyítás

Az S gép mezőit 2k darab mezőből álló csoportokra osztjuk.
Az induláskor a fej egy ilyen mezőcsoportba jobb szélén áll.
Ezen mezőcsoportba írt

$$a_1 a_2 \dots a_k f_1 f_2 \dots f_k$$

betűkből $a_1 a_2 \dots a_k$ rendre azon mezők tartalma, amelyeken induláskor a T gép első, második stb szalagján a fejek állnak.
Az ettől balra álló mezőcsoport első k betűje a T gép szalagjain a fejtől balra álló betűket tartalmazza. stb.
Szükség van azonban annak jelzésére is, hogy a szimuláció során hol állnak T szalagjain a fejek.

Az S szalagján egy-egy mezőcsoport $f_1 f_2 \dots f_k$ betűi ezt adják meg: ha a T gép i-edik szalagján a mezőcsoportban szereplő a_i betűn áll a fej, akkor f_i nem az üres jel, egyébként az üres jel.
Kezdetben tehát az S gép szalagján azon mezőcsoport $f_1, f_2, \dots f_k$ mezői, amelyiknek a bal szélén a fej áll, mind nem üresek, az összes többi mezőcsoport $f_1, f_2 \dots f_n$ mezői pedig mind üresek.
A T gép egy lépésének szimulálása annak a 2k hosszú mezőcsoportnak a jobb szélér
Hol indul, amelyben a leginkább jobbra lévő fej van.
A szimuláció során S emlékszik arra, hogy T milyen állapotban van, és arra is, hogy egy mezőcsoport melyik mezőjén áll.
Balra lépkedve megkeresi minden szalaghoz a fejet és megjegyzi a megfelelő szalagjelet is.
Mikor minden fejet megtalál, tudja mit kell tenni:
mit írjon a megfelelő mezőkre, merre mozdítsa a fejeket és melyik állapotba menjen át.
Jobbra visszafelé haladva a megfelelő helyeken ír a szalagra, és megfelelően mozgatja a fejeket.
Hogy eközben ne kelljen fejnek balra visszalépni, célszerűen,

miközben balra mozog, minden fejnek megelőlegzi, hogy balra fog lépni, és balra mozdítja el.
Ha mégsem balra mozdul a fej, jobbra haladva korrigál.
Ha pedig a T gép n lépését szimuláltuk, akkor a fejek legfeljebb n mezőcsoporttal mozdultak el balra vagy jobbra.
Igy a következő lépés szimulálása során legfeljebb 2n+1 mezőcsoportot kell balra haladva végigolvasnunk, hogy begyűjtsük a jelenlegi helyzetre vonatkozó információkat.
Ezután legfeljebb még egy mezőcsoportot haladunk balra, majd visszafelé legfeljebb 2n+3 mezőcsoporton kell végiglépegetnünk.
Igy az n+1-edik lépés szimulálása legfeljebb 2k(4n+5) lépést igényel.
Innen a szimuláció teljes lépésszámára legfeljebb
$\sum_{n=0}^{t-1} 2k(4n+5) = 2kt(2t+3)$.
$\triangle$

Megjegyzés:
Ha az előző tételben szereplő S gép kétszalagos, akkor $O(t \log t)$ lépésben is elvégezhető a szimulálás.

Szemétgyűjtés

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

Bizonyítás:
Az S konstrukciója könnyű, ha az ábécéje tartalmaz egy olyan jelet, amelyet A nem.
Ha például $* \notin A$, akkor a * jelet második üres jelként használhatjuk: ha T üres jelet írna, akkor ezt a jelet írjuk, ha pedig ezt a jelet olvassuk, akkor úgy viselkedünk, mint T, ha ugyanezen szalagon az üres jelet olvas.
Mielőtt megállnánk, végezzünk minden szalagon szemétgyűjtést: minden szalagon először jobbra haladva irjunk egy * jelet, majd

jobbra lépve töröljük mindent az első ⊔ jelig.
Ezután balra haladva keressük meg a * jelet, törüljük és lépünk balra, majd balra lépkedve, keressük meg az első * jelet és ettől balra töröljük mindent az első ⊔ jelig.
Ezután jobbra haladva keressük meg a * jelet,töröljük és menjünk a kimeneti szó jobb szélére.
Eközben legfeljebb O(t) lépést teszünk.
Ha ugyanazt az ábécét akarjuk használni, akkor kódolást kell alkalmazni.
Ha $a \in A$, akkor kódja legyen $\sqcup a$ míg * kódja legyen egy olyan pár, amelynek első betűje nem ⊔.
A szimuláció azzal kezdődik, hogy a bemeneti szavakat széthúzzuk, ⊔ jeleket írva közéjük.
Mivel T olvassa a bemenetet, a bemeneti szavak hossza legfeljebb t+1, így ez $O(t^2)$ lépést igényel.
A szemétgyűjtés után a kimeneti szavakat összenyomjuk, törölve a betűjeik közé írt ⊔ jeleket;
ez szintén legfeljebb $O(t^2)$ lépést igényel.
△

Eddig minden feladatra új Turing-gépet készítettünk.
A valódi számítógépnél viszont minden új feladathoz programot írunk és ugyanazt a gépet használjuk. Ez megtehető a Turing-gépnél is.

Univerzális Turing-gépek

Legyen A egy (legalább két elemű)ábécé, $k \geq 1$.
Van olyan k+1 szalagos U Turing-gép A ábécével, hogy bármely k szalagos $T = (B, A, \varphi)$ Turing-gépre a T bemenetét felírva az U első k szalagjára a k+1-edik szalagra pedig egy, csak a φ-től függő $\omega \in A^*$ programot írva U szimulálja T működését (az első k szalagján).
Ha A-nak legalább három eleme van, akkor U-t úgy is választhatjuk, hogy a programok ne tartalmazzanak üres jelet.
Ha T egy bemeneten t lépést tesz, akkor U a szimulálást O(t) lépésben végzi.
Biz. (könyv)

Egyszalagos univerzális Turing-gép

Legyen A egy (legalább kételemű) ábécé. Van olyan egyszalagos U Tring-gép A ábécével, hogy bármely egyszalagos $T = (B, A, \varphi)$ Turing-gépre a T bemenetét és egy, csak a φ-től függő $\omega \in A^*$ programot felírva az U szalagjára, U szimulálja T működését.
Ha A-nak legalább három eleme van, akkor U-t úgy is választhatjuk, hogy a programok ne tartalmazzanak üres jelet.
Ha T szemétgyűjtéssel dolgozott, akkor U is.
Ha T egy bemeneten t lépést tesz, akkor U a szimulálást O(t) lépésben végzi.

RAM-gép

A valódi számítógépekhez közelebb álló gépmodell.
Az M memória minden $M[k], k \in \mathbb{Z}$ rekesze tetszőleges egész számot tárolhat, de egyszerre mindig csak véges sok nem nulla értéket tárol.
A gépeknek három regisztere van: az A akkumlátor, a B regiszter és a I indexregiszter, ezek tartalma is egész szám.

Van még egy programmemória, ennek rekeszei természetes számokkal vannak indexelve, és utasításokat tartalmaznak.
Az utasításkészlet (könyv)
A programvégrehajtás a nullás sorszámú sorral indul és minden sorban végrehajtódik, ha nincs ugrás. A gép akkor áll meg, ha a vezérlés olyan sorra kerül, amely nem tartalmaz utasítást.
Minden RAM-gép tekinthető számítási eljárásnak, az állapotot a regiszterek tartalma, a memória tartalma és az aktuális programsor sorszáma adja meg.
A memória és a regiszterek vagy azok egyike tekinthető bemenetnek ill. kimenetnek.

A RAM-gép végrehajtási ideje

Egy RAM-gép lépésszáma nem a legjobb mérőszáma annak, hogy mennyi munkát végez, mert tetszőleges hosszúságú számokkal végzett műveleteket szimulálhatunk.
Ezért szokásosabb RAM-gépek lépésszáma helyett a futásidejükről beszélni.
Ezt úgy kapjuk, hogy egy lépés idejét nem egységnyinek vesszük,

hanem annyinak, amennyi a benne fellépő összes egész szám bitjei számának összege, ahol minden számnál egy bitet számolunk az előjelre.
Igy a 0 egybites, a $0 \neq n \in \mathbb{Z}$ szám bitjeinek száma pedig $2 + \lfloor \log_2 |n| \rfloor$.
Emiatt szokás logaritmikus költségű RAM-gépről is beszélni.

Turing-gép szimulálása RAM-gépen

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

Bizonyítás

Feltehetjük, hogy a $T = (B, A, \varphi)$ Turing-gép ábécéje $A = \{0, 1, \ldots r\}$, ahol 0 az üres jel, belső állapotait pedig $B = \{0, 1, \ldots m\}$, ahol 0 a start, m pedig a halt.
Legyenek φ koordinátái β, α és γ, azaz $\alpha(j, i) \in A$, $\beta(j, i) \in B$ és $\gamma(j, i) \in \{<, =, >\}$, ha $i \in A$ és $j \in B$.

A szimuláció során a memóriatartalom megfelel a szalagon álló betűknek, I pedig a fej helyzetét tartalmazza.
A program a $P_j, 0 \leq j \leq m$ és Q_{ji}, $0 \leq i \leq r, 0 \leq j < m$ részekből áll.
A P_j programrész azt utánozza, hogy a Turing-gép a j állapotban van, kiolvassa, hogy mi áll a szalagon, majd ettől függően más-más $Q_{j,i}$-re ugrik:
A P_m programrész álljon egyszerűen egyetlen üres programsorból.
A $Q_{j,i}$ programrész átírja a szalag tartalmát, módosítja I-t a fej mozgásának megfelelően, majd az úl j' állapotnak megfelelő $P_{j'}$ programrésze ugrik,
ahol a $Q_{j,i}$-hez tartozó $\gamma(j,i)$-nek megfelelő módosítást egy DEC utasítás, ill. egy INC utasítás hajtja végre, vagy pedig teljesen kimarad ez a sor, attól függően, hogy $\gamma(j,i)$ értéke $<$, $>$ vagy $=$.
Maga a program: konyv
A futási időre vonatkozó becslés onnan következik, hogy a Turing-gép egy lépése a RAM-gép korlátos számú lépésének felel meg és a Turing-gép n lépésben legfeljebb n rekeszekbe ír bármit is, így ezek címe legfeljebb $O(\log n)$ hosszú.

RAM-gép szimulálása Turing-gépen

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

Bizonyítás

A Turing-gép ábécéje legyen $\{\sqcup, 0, 1, -, ;\}$.
Az első, második és harmadik szalagon rendre A, B és I tartalma szerepel kettes számrendszerben, előjellel.
Ha a negyedik szalagon minden rekesz tartalmát sorra feltüntetnénk, akkor gondot jelentene, hogy a RAM-gép képes akár a 2^m sorszámú rekeszbe is írni O(m) idő alatt, így a szalag teleírt része nagyon hosszú lesz, és nagyon hosszú időbe telik, amíg a fej végigléptet rajta.
Ezért ST utasításakor a negyedig szalagra, az eddig felírtaktól jobbra egy ; M[I];I sorozatot írunk, ahol M[I] és I tartalmát kettes számrendszerben írjuk fel előjellel.
A RAM-gép bemenetét ugyanezzel a kóddal írjuk erre a szalagra.

Erről a szalagról sohasem törlünk semmit.
Ha LD utasítást kell végrehajtani, jobbról balra végiglépegetnünk a szalagon és megkeressük adott I-vel a legkésőbbi feljegyzést; ha nincs feljegyzés, az olvasás eredménye 0.
Az ugyanarra a címre való újabb írások mintegy eltakarják a régieket.
A többi utasítást könnyű szimulálni Turing-géppel.
Turing-gépünk egy olyan szupergép lesz, amelyben a RAM-gép minden programsorának megfelel belső állapotok egy halmaza; ezek egy olyan Turing-gépet alkotnak, amely végrehajtja az adott utasítást, majd a fejeket mind a négy szalagon a feljegyzések jobb szélére viszi.
Minden ilyen Turing-gép halt állapota megegyezik a következő utasításhoz tartozó Turing-gép start állapotával; feltételes ugrás esetén, ha a feltétel teljesül, az adott sornak megfelelő gép start állapotába megy át a szupergép.
A nulladik programsornak megfelelő Turing-gép start állapotba lesz a szupergép start állapota, míg az üres soroknak a szupergép halt állapota felel meg.

A legtöbb utasítás szimulálása a RAM-gép végrehajtási idejével arányos számú lépéssel történik.
Kivétel az olvasás, de ha a RAM-gép futásideje n, akkor ehhez sem kell O(n)-nél több lépés, így a teljes lépésszám $O(n^2)$.
$\triangle$

Megjegyzés
Az előző tétel bizonyításából világos, hogy ha jelentősen kibővítjük a RAM-gép utasításkészletét a fenti tétel akkor is érvényben marad. Ha a regiszterek számát megnöveljük, akkor is csak a szalagok számát kell megnövelni.

Kiszámíthatóság

Kiszámítható függvények

Legyen A egy legalább kételemű ábécé, amely tartalamzza a $\sqcup$ jelet, és legyen $A_0 = A \setminus \{\sqcup\}$.
Egy $f : A_0^{*m} \to A_0^{*n}$ függvényt Turing-kiszámíthatónak vagy röviden csak kiszámíthatónak nevezzük, ha van olyan Turing-gép, amely bármely $(\alpha_1, \alpha_2, \ldots \alpha_m) \in A_0{*}^m$ bemenettel megáll és az utolsó

szalagjára rendre

$$f(\alpha_1, \alpha_2 \dots \alpha_m)$$

koordinátai vannak írva.
Altlánosabban, egy $f \in A_0^{*m} \to A_0^{*n}$ parciális függvényt parciálisan Turing-kiszámíthatónak vagy röviden csak parciálisan kiszámíthatónak nevezzük, ha van olyan Turing-gép, amely egy

$$(\alpha_1, \alpha_2, \dots \alpha_m) \in A_0^{*m}$$

bemenettel, pontosan akkor áll meg, ha

$$(\alpha_1, \alpha_2 \dots \alpha_m) \in dmn(f)$$

és ekkor az utolsó n szalagjára rendre $f(\alpha_1, \alpha_2 \dots \alpha_m)$ koordinátái vannak írva.
Ha egy Turing-gépet egy függvény kiszámítására akarunk felhasználni, akkor általában kényelmesebb néhány írásjellel kibővíteni az ábécét és egy szalagon adni be a bemenetet.
Ugyanez érvényes a kimenetre is.
Például ha egy egyváltozós egész együtthatós polinom a bemenet, akkor választhatunk $A = \{\sqcup, 0, 1, -\}$ ábécét, minden együtthatót

más szalagra írva fel kettes számrendszerben, de kényelmesebb az ábécéhez hozzávenni a ; pontosvessző jelet is, és az együtthatókat egy szalagra felírni, pontosvesszővel választva el azokat.
Ha egy többváltozós egész együtthatós $\sum a_{i_1,\dots i_l} x_1^{i_1} x_2^{i_2} \dots x_l^{i_l}$ polinom a bemenet, akkor az ábécéhez a , vessző jelet is hozzávéve, az $a_{i_1 \dots i_l}$, $i_1 \dots i_l$ szavakat, ahol $a_{i_1 \dots i_l} \neq 0$, tetszés szerint egymás után írva adhatjuk meg a polinomot.
Ezen megoldások alapján alsősorban az $f : A_1^* \to A_0^*$ kiszámítható függvények és az $f \in A_0^* \to A_0^*$ parciálisan kiszámítható függvények érdekelnek bennünket.

Nyelvek

Gyakran csak igen-nem problémák érdekelnek bennünket és a Turing-gépet ilyen problémák megoldására használjuk.
Például, ha csak az érdekel bennünket, hogy egy

$$p(x_1 \dots x_l) = \sum a_{i_1 \dots i_l} x_1^{i_1} x_2^{i_2} \dots x_l^{i_l}$$

egész együtthatós polinomra a $p(x_1 \dots x_l) = 0$ egyenletnek van-e egész számokból álló megoldása, akkor olyan Turing-gépet

szeretnék készíteni, mely azt megmondja.
Azok a bemenetek, amelyekre van megoldás, az összes lehetséges bemenetek egy részhalmazát alkotják és az érdekel bennünket, hogy egy adott bemenet benne van-e ebben a részhalmazban.
Nem világos, hogy van-e olyan Turing-gép, mely azt megmondja, bár olyan Turing-gépet tudunk készíteni, amely megáll, ha van megoldás és azt ki is írja.
A fenti meggondolások alapján, az előző definíció jelöléseivel egy $\mathcal{L} \subset A_0^*$ halmazt nyelvnek fogunk nevezni.
Bár az előző bekezdés meggondolásai szerint elsősorban a nyelvek érdekelnek bennünket, az alábbi két fogalmat mégis célszerű lesz általánosabban definiálni.

Eldönthető nyelvek

Egy $\mathcal{L} \subset A_0^*$ nyelvet, vagy általánosabban egy $\mathcal{L} \subset A_0^{*m}$ halmazt Turing-eldönthetőnek vagy röviden csak eldönthetőnek nevezzük, ha van olyan Turing-gép, amely bármely A_0^{*m}-beli bemenetre megáll, és jelzi ha a bemenet benne van $\mathcal{L}$-ben: ha benne van, akkor az A_0^*-beli kimeneti szó nem üres, ha pedig nincs benne, akkor üres.

Az $\mathcal{L} \subset A_0^{*m}$ halmaz nyilván pontosan akkor eldönthető, ha az $A_0^{*m} \setminus \mathcal{L}$ komplementere eldönthető.
Minden véges halmaz eldönthető, mivel megadható olyan Turing-gép, amely emlékszik a halmazra.
Mivel kontinuum sok ilyen nyelv van, de csak megszámlálható sok Turing-gép, kell lennie nem eldönthető nyelvnek.

Kiszámítható parciális függvények

Egy $f \in A_0^* \to A_0^*$ parciális függvényt Turing-kiszámíthatónak vagy röviden csak kiszámíthatónak nevezzük, ha értelmezési tartománya eldönthető, ő maga pedig parciálisan kiszámítható.
Ilyen függvények esetén előbb el tudjuk dönteni, hogy az értelmezési tartományban vannak-e és ha igen, csak akkor kezdhetjük kiszámítani a függvényt, így gépünk biztos, hogy megáll.
Ha jelezni kívánjuk, hogy a bemenet nincs az értelmezési tartományban, egyik lehetőségünk, hogy az utolsó előtti szalagot standard error szalagnak tekintjük, és ha a bemenet nincs az értelmezési tartományban, ide üres jelet írunk, egyébként pedig nem üres jelet.

A másik lehetőség, hogy az eredményt mindig valamilyen írásjellel zárjuk le, és az output csak akkor lesz üres, ha a bemenet nincs az értelmezési tartományban.
Altalánosabban, az $f \in A_0^{*m} \to A_0^{*n}$ parciális függvényt Turing-kiszámíthatónak vagy röviden csak kiszámíthatónak nevezzük, ha értelmezési tartománya eldönthető, ő maga pedig parciálisan kiszámítható.
A fenti két módszer segítségével itt is megadhatjuk, hogya bemenet nincs az értelmezési tartományban.

Felsorolható nyelvek

Egy $\mathcal{L} \subset A_0^*$ nyelvet, vagy áltlánosabban egy $\mathcal{L} \subset A_0^{*n}$ halmazt Turing-felsorolhatónak vagy röviden csak felsorolhatónak nevezünk, ha vagy üres, vagy van olyan Turing-gép, amellyel egy adott $I \in A_0$ jelre $\{I\}^*$ szavait írva a bemenetre, $\mathcal{L}$ elemeit kapjuk meg kimenetként.
Lényegtelen, hogy A_0 melyik betűjét választjuk I-nek, hiszen a Turing-gép kezdheti azzal a működését, hogy végigmely a bemeneten és annak minden betűjét kicseréli I-re.

Mivel kontinuum sok nyelv van, megszámlálhatóan sok Turing-gép kell lennie nem felsorolható nyelvnek.

Tétel

Az előző definíció jelöléseivel, egy nem üres $\mathcal{L} \subset A_0^*$ nyelv akkor és csak akkor felsorolható, ha van olyan kiszámítható $f : A_0^* \to A_0^*$ függvény, amelynek $\mathcal{L}$ az értékkészlete.
Altalánosabban, rögzített n-re és bármilyen m-re, nem üres $L \subset A_0^{*n}$ halmaz pontosan akkor felsorolható, ha valamely kiszámítható $f : A_0^{*m} \to A_0^{*n}$ függvény értékkészlete.

Bizonyítás

Feltehetjük, hogy $A = \{0, 1, \ldots r\}$ és 0 az üres jel.
Az első állítás bizonyításához vegyük észre, hogy először egy Turing-géppel az $|\alpha|_r$ szám unáris felírásává konvertálva egy $\alpha \in A_0^*$ bemeneti szót, majd működtetve az $\mathcal{L}$-et felsoroló Turing-gépet, olyan Turing-gépet kapunk, amely egy $f : A_0^* \to A_0^*$ függvényt számít ki, melynek értékkészlete $\mathcal{L}$.

Megfordítva, $\{1\}^*$ egy l hosszú szavát Turing-géppel előbb olyan $\alpha \in A_0^*$ szóvá konvertálnva, amelyre $l = |\alpha|_r$ majd működtetve az f-et kiszámító Turing-gépet, $\mathcal{L}$ egy felsorolását kapjuk.
Általános esetben is hasonlóan járunk el, de miután az $\alpha_i \in A_0^*$ $1 \leq i \leq m$ bemeneti szót minden szalagon átkonvertáltuk $|\alpha_i|_r$ unáris alakjává, ezeket valahogyan egyetlen szám unáris alakjává kell konvertálni.
Tanultuk, hogy a $\varphi(u, v) = w(w+1)/2 + u,\ w = u + v$ összefüggésekkel definiált függvény kölcsönösen egyértelműen képezi le $\mathbb{N} \times \mathbb{N}$-et $\mathbb{N}$-re és nyilván könnyen számítható még unáris Turing-gépen is.
Igy a

$$(j_1, j_2, \ldots j_m) \to \varphi(j_1, \varphi(j_2, \varphi(j_3 \ldots \varphi(j_{m-1}, j_m) \ldots)))$$

leképezés kölcsönösen egyértelműen képezi le $\mathbb{N}^m$-et $\mathbb{N}$-re és nyilván könnyen számítható még unáris Turing-gépen is.
A megfordításhoz φ inverzét kell kiszámítani.
Azon $u, v \in \mathbb{N}$ természetes számok megkereséséhez, amelykere $\varphi(u, v)$ egy adott $z \in \mathbb{N}$, meg kell keresni azt az egyetlen w

természetes számot, melyre w=u+v és z=w(w+1)/2+u.
Sorban próbálkozva a $w = 0, 1, \ldots$ értékekkel, keressük meg azt az egyetlen w-t, amelyre $0 \leq z - w(w+1)/2 = u \leq w$.
$\triangle$

Church-tézis

Az előző fejezet eredményei alátámasztják az úgynevezett Church-tézist, mely szerint algoritmussal pontosan az számítható ki, ami Turing-géppel.
Szokás Church Turing-tézisről is beszélni, mert Church eredetileg a λ-kalkulusra fogalmazta meg hipotézisét.
A tézis természetesen nem bizonyítható, hiszen az algoritmus fogalmát nem definiáltuk, de a tapasztalatok alátámasztják.
Kicsit pontosabb formában a tézis azt mondja ki, hogy az algoritmussal parciálisan kiszámítható parciális függvények éppen a parciálisan Turing-kiszámítható parciális függvények.

Tétel

Az előző definíció jelöléseivel, egy $\mathcal{L} \subset A_0^*$ nyelv akkor és csak akkor felsorolható, ha van olyan Turing-gép, amelynek első szalagjára $\alpha \in A_0^*$-ot írva, akkor és csak akkor áll le, ha $\alpha \in \mathcal{L}$, azaz ha $\mathcal{L}$ egy $f \in A_0^* \to A_0^*$ parciálisan kiszámítható parciális függvény értelmezési tartománya.
Altalánosabban, rögzített m-re és bármilyen n-re, egy nem üres $\mathcal{L} \subset A_0^{*m}$ halmaz pontosan akkor felsorolható, ha valamely $f \in A_0^{*m} \to A_0^{*n}$ parciálisan kiszámítható parciális függvény értelmezési tartománya.

Bizonyítás

Az egyik irány könnyű: legyen $\mathcal{L} \subset A_0^{*m}$ felsorolható; feltehetjük, hogy nem üres.
Vegyünk egy T Tuting-gépet, amely felsorolja $\mathcal{L}$-et és egészítsük ki egy olyan T' Turing-géppé, amely sorra előállítja T-nek a $0, 1, 2, \ldots$ unáris kódját az $m+1$-edik szalagra bemenetnek, futtatja T-t, majd megnézi, hogy T kimenete az az első m szalagra írt adott

$(\alpha_1 \dots \alpha_m) \in A_0^{*m}$-e és megáll, ha igen.
A másik irányt először arra a speciális esetre bizonyítjuk, amikor $\mathcal{L}$ nyelv.
Feltehetjük, hogy $A = \{0, 1, \dots r\}$ ahol 0 az üres jel és hogy $\mathcal{L}$ nem üres.
Legyen $\alpha \in \mathcal{L}$ tetszőleges szó, de rögzített szó, melynek csak az a szerepe, hogy ezt fogjuk a kimenetre írni, ha jobbat nem tudunk.
Legyen T az a Turing-gép, mely pontosan akkor áll meg, ha a bemenete egy $\xi \in \mathcal{L}$ szó.
Csináljuk egy T' Turing-gépet, amelynek alső szalagjára egy $i \in \mathbb{N}$ természetes számot írva, a T első szalagjára a $j = i - \lfloor \sqrt{i} \rfloor^2$ számot írja, azt átkonvertálja azzá a $\xi \in A_0^*$ szóvá, amelyre $|\xi|_r = j$ majd i lépésen keresztül próbálja működtetni T-t.
Igy minden ξ bementtel egyre több lépésen át futtatjuk T-t.
Ha ezalatt a T gép leáll, akkor T' az utolsó szalagjára ξ-t ír és leáll.
Ha ezalatt T nem áll le, akkor T' az utolsó szalagjára az α szót írja.
A T' gép az $\mathcal{L}$ nyelvet sorolja fel.
Az általános esetben $m > 1$ csak annyit kell módosítanunk, hogy az előző tétel bizonyításában látott módon a j számot szétkódoljuk

egy $(j_1, j_2, \ldots j_m) \in \mathbb{N}^m$ szám m-essé és ezt írjuk T bemenő szalagjaira, ezt szalagonként konvertáljuk egy $(\xi_1, \ldots \xi_m) \in A_0^{*m}$ bemenetté, majd i lépésen kerül próbáljuk működtetni T-t.
Ha ezalatt a T gép leáll, akkor T' utolsó szalagjaira $(\xi_1 \ldots \xi_m)$ keresztül, egyébként egy rögzített $(\alpha_1 \ldots \alpha_m) \in \mathcal{L}$.
$\triangle$

Lemma
Eldönthető nyelvek felsorolhatóak.
Altalánosabban, ha egy $\mathcal{L} \subset A_0^{*m}$ halmaz eldönthető, akkor felsorolható is.

Bizonyítás
Tegyük fel, hogy $\mathcal{L} \subset A_0{*}^m$ eldönthető.
Ha $\mathcal{L} = \emptyset$, akkor készen vagyunk, egyébként legyen $(\alpha_1 \ldots \alpha_m) \in \mathcal{L}$ tetszőleges, de rögzített.
Bármely $(\xi_1 \ldots \xi_m) \in A_0^{*m}$ bemenetre, ha az $\mathcal{L}$-beli, másoljuk a kimenetre, egyébként pedig legyen a kimenet $(\alpha_1 \ldots \alpha_m)$.
$\triangle$

Tétel

Egy nyelv pontosan akkor eldönthető, ha ő is és a komplementere is felsorolható.
Altalánosabban, $\mathcal{L} \subset A_0^{*n}$ pontosan akkor eldönthető, ha $\mathcal{L}$ és $A_0^{*m} \setminus \mathcal{L}$ is felsorolható.

Bizonyítás

Ha $\mathcal{L}$ eldönthető, akkor a komplementere is, így az előző lemma szerint mindkettő felsorolható.
Megfordítva, tegyük fel, hogy $\mathcal{L}$ és a komplementere is felsorolható. Készítsünk két Turing-gépet, az egyik $\mathcal{L}$-et a másik a komplementerét sorolja fel és egy harmadik gépet, amely ellátja őket bemenettel futtatja és figyeli, hogy melyik adja ki $(\alpha_1 \dots \alpha_m)$-et.
Ez előbb-utóbb bekövetkezik és akkor eldöntöttük, benne van-e $(\alpha_1 \dots \alpha_m)$ bemenet az $\mathcal{L}$-ben.
Könnyű a három gépet egyetlen géppé kapcsolni.
$\triangle$

A megállási feladat

Példát akarunk mutatni arra, hogy van algoritmikusan megoldhatatlan probléma.
Az ugynevezett megállási feladatról fogjuk megmutatni, hogy Turing-géppel nem megoldható: adott egy Turing-gép és a bemenete.
Döntsük el, hogy a Turing-gép az adott bemeneten megáll-e?
A potos megfogalmazáshoz legyen egy $T = (B, A, \varphi)$ Turin-gép $\mathcal{L}_T$ nyelvre azon $\alpha \in A_0^*$ szavak halmaza, melyekre a gép minden szalagjára az α szót írva, ezzel a bemenettel T megáll.

Tétel

Bármely T Turing-gépre $\mathcal{L}_T$ felsorolható.
Bármely ábécére van olyan kétszalagos T Turing-gép, amelyre $\mathcal{L}_T$ nem eldönthető.

Bizonyítás

Az $\mathcal{L}_T$ nyel a korábi tétel szerint felsorolható, mert az a T' gép, amely egyetlen α bemenetét lemásolja minden szalagjára, mindegyiken visszamegy α jobb szélére, majd úgy működik, mint T pontosan $\mathcal{L}$ szavaira áll le.
A másik állítás bizonyításának lényege az átlós eljárás. Lényegében egy U kétszalagos univerzális Turing-gépet fogunk felhasználni, amelynek ábécéje tetszőleges, de kicsit átalakítjuk, hogy az inputja A_0^*-beli legyen.
Nyilván feltehetjük, hogy

$$A = \{0, 1, \ldots r\}$$

A T gép második szalagjára egy egyszalagos gép programját unáris kódban írjuk fel.
A T a működését azzal kezdi, hogy a második szalagon az unáris kódot konvertálja a szokásos A^*-beli programmá, majd úgy működik, mint U.
A korábbi tétel szerint azt kell megmutatnunk, hogy $A_0^* \setminus \mathcal{L}_T$ nem felsorolható.

Tegyük fel indirekt, hogy $\mathcal{L}_T$ komplementere felsirolható.
Ekkor létezik olyan k szalagos Turing-gép, mely pontosan akkor áll le az $\alpha \in A_0^*$ bemenettel, ha $\alpha \notin \mathcal{L}_T$.
Készítünk egy egyszalagos T^* gépet, amely a következőképpen működik; először szétzúzza az α bemeneti szót, hogy szomszédos betűi között 2k-1 üres jel álljon, majd visszamegy a jobb szélére és T_k működését szimulálja egy szalagon.
A T^* nyilván pontosan akkor áll le, ha $\alpha \notin \mathcal{L}_T$.
Legyen T^* programja ω.
Irjuk a T mindkét szalagjára az ω szót.
A szimuláció miatt T potosan akkor áll le, ha $\omega \notin \mathcal{L}_T$, ami ellentmond $\mathcal{L}_T$ definíciójának.
$\triangle$

Tétel

Bármely ábécére van olyan egyszalagos S Turingép, amelyre $\mathcal{L}_S$ nem eldönthető, azaz nem eldönthető, hogy adott bemenetre S megáll-e.

Bizonyítás

Készítsünk olyan S egyszalagos Turing-gépet, amely azzal kezdi működését, hogy az α bemenet minden betűjét megduplázza, majd a kapott szó betűit széthúzza egy-egy $\sqcup$ jelet írva közéjük, visszhamegy a jobb szélre és az előző tételben szereplő T kétszalagos gép működését szimulálja 1 szalagon. Ekkor $\mathcal{L}_S = \mathcal{L}_T$.
$\triangle$

Tétel

Eldönthetetlen, hogy egy egyszalagos Turing-gép az üres bemeneten megáll-e.
Pontosabban, legyen $A = \{0, 1, \ldots r\}$ az ábécé és álljon $\mathcal{L} \subset \{1\}^*$ azon A abecejű egyszalagos Turing-gépek unáris kódban felírt proramjaiból, amelyek üres bemenettel megállnak.
Ekkor $\mathcal{L}$ nem eldönthető.

Bizonyítás

Az előző tételben szereplő S gépet módosítjuk úgy, hogy először az adott $\alpha \in A_0^*$ szót írja ki a szalagra, menjen a jobb szélére, majd működjön úgy, mint S.
Az így kapott T_α gép persze függ az α szótól.
Az α szóból és S programjából kiszámíthatjuk T_α univerzális Turing-gépnek szóló programját egy P Turing-géppel.
Ha a Turing-gépek programjainak unáris kódjaiból el tudnánk dönteni, hogy üres bemenettel megállnak-e, akkor ezt a gépet működtetve a P gép után, olyan Turing-gépet kapnánk, amely eldöntené, hogy S az α bemenettel megáll-e, ami az előző tétel szerint lehetetlen.
$\triangle$

Tétel

Eldönthetetlen, hogy egy T Turing-gépre az $\mathcal{L}_T$ nyelv üres-e.
Pontosabban legyen $A = \{0, 1, \ldots r\}$ az ábécé és álljon $\mathcal{L}' \subset \{1\}^*$ azon T' egyszalagos Turing-gépek unáris kódban felírt programjaiból, amelyekre a $\mathcal{L}_{T'}$ nyelv üres.

Ekkor $\mathcal{L}'$ nem eldönthető.

Bizonyítás

Adott egyszalagos T Turing-géphez konstruáljunk egy egyszalagos T' gépet, amely a következőt csinálja: először letörli a szalagot, majd úgy működik, mint a T gép.
Ha T az üres bemeneten véges sok lépésben megáll, akkor T' minden bemeneten véges sok lépésben megáll, igy $\mathcal{L}_{T'}$ nem üres.
Ha T az üres bemeneten nem áll meg, akkot T' semillyen bemeneten sem áll meg.
A T programjából a T' programja Turing-géppel megkonstruálható.
Ha lenne olyan Turing-gép, amely a $\mathcal{L}'$ nyelvet eldönti, akkor ezt a T programjából T' programját kiszámító gép kimenetével mint bemenettel működtetve olyan gépet kapnánk, mely az előző tételben szereplő $\mathcal{L}$ nyelvet eldönti, ami lehetetlen.
$\triangle$

Irodalom

-Járai Antal, Bevezetés a matematikába

Vizsga

A vizsga két részből áll írásbeli és szóbeli.
Az írásbeli beugrón 8 kérdésre kell válaszolni, 5 helyes válasz esetén lehet szóbelizni.
A szóbelin mindenki 2 tételt húz, melyeket ki kell dolgozni, az első részből legalább 1 állítást részletesen be kell tudni bizonyítani, a második részben a fogalmak, módszerek, állítások ill bizonyításainak összefoglalását kell elmondani.

I. Első rész

1. Irányítatlan gráfok, illeszkedés, izolált csúcs, üres gráf, illeszkedési relálió, szomszédos él, szomszédos csúcs, hurok él, párhuzamos él, egyszerű gráf, fokszám, reguláris gráf, vertexpontok fokai és az élek száma közti összefüggés, izomorfia, teljes gráf, n szögpontú teljes gráf éleinek a száma, gráfok Descartes-szorzata, páros gráfok, részgráf, feszített részgráf, komplementer, élhalmaz-csúcshalmaz törlésével kapott részgráf

2. Séták, vonalak, utak, körök, G gráfban v-t v'-vel összeköthető út megkonstruálása, zárt vonal és az éldiszjunkt körök kapcsolata,

összefüggőség, fa, fa és összefüggőség kapcsolata, nincs kör létezik elsőfokú csúcs, n csúcsú fa

3. Feszítőfa, összefüggőség és a feszítőfa kapcsolata, véges összefüggő gráfban az éldiszjunkt körök száma, alapkörrendszer, vágás, vágások száma véges összefüggő gráfban, erdő, Euler-vonal, Euler-vonal létezése, Hamilton-út, címkézett, súlyozott gráfok, élsúlyozás, csúcssúlyozás, mohó algoritmus, Kruskál algoritmus

4. Irányított gráf, szigorúan párhuzamos élek, gráf foka, vertexponrok fokai és az élek száma közti összefüggés, irányított teljes gráf, éllistás ábrázolás, irányított gráfok izomorfiája, irányított részgráf, komplementer, élhalmaz, csúcshalmaz törlésével kapott irányított részgráf, irányított séták, vonalak, utak, körök, topologikus rendezés, erős összefüggőség, irányított fák, Dijkstra módszere, dinamikus programozás, gráfok mátrixai

5. Homomorfizmus, monomorfizmus, epimorfizmus, izomorfizmus, endomorfizmus, automorfizmus, félcsoport homomorf képe is félcsoport, félcsoport ekvivalens megfogalmazásai, részcsoport, G csoport és H részhalamza G-nek ekvivalens megfogalamzások, generátum, generátorrendszer, ciklikus csoport, K által generált csoport, ciklikus csoport homomorf képe

6. Rend, ciklikus csoportok izomorfiája, ciklikus csoportok részcsoportjai, mellékosztályok, index, Lagrange tétel, normálosztó, normálosztó ekvivalens állítások, faktorcsoport, homomorfizmusmagja, homomorfizmus tétel, Direkt szorzat, végesen generált Abel-csoportok alaptétele, Cayley tétel

7. Gyűrű, nullgyűrű, zérógyűrű, nullosztó, integritási tartomány, rendezett integritási tartomány, ferdetest, test, rendezett test, gyűrű homomorf képe is gyűrű, mullosztómentes gyűrűben a nem nulla elemek additív rendje, gyűrű karakterisztika, részgyűrű, ideál, főideál, faktorgyűrű, homomorfizmus magja, homomorfizmus tétel

8. Direkt szorzat, Gauss-gyűrű, Gauss-gyűrű és az irreducibilitás ill. prím kapcsolata, Euklideszi gyűrű, egységek és asszociáltak, bővített euklideszi algoritmus, felbonthatatlan és prím viszonya az Euklideszi gyűrűben, Euklideszi gyűrű és Gauss-gyűrű kapcsolata, test és a nullgyűrű kapcsolata, hányadostest

9. Egyhatározatlanú polinomok, konstans polinomok, polinom foka, nullpolinom, monom, főpolinom, polinomfüggvények, polinom gyöke, maradékos osztás tétele, gyökténező leválasztása, polinom gyökeinek a száma, Wilson tétele, derivált polinom, többszörös gyök

10. Véges testek elemszáma, véges test nem nulla eleminek multiplikatív csoportja ciklikus, testbővítés, véges testek alaptétele, Weddernburn tétel, Schönemann-Eisenstein tétel, többhatározatlanú polinomok, multifoka, multiindexe, irreducibilis polinomok $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ felett

Második rész

1. Információ, gyakoriság, relatív gyakoriság, bit, entrópia, entrópia felső becslése, kódolás, felbontható, egyértelműen dekódolható, betűnkénti kódolás, tömörítés, üzenetkódolás, gazdaságos kódolás, forráskódolás, hibakorlátozó kódolás, csatornakódolás, kódabc, kódszó, prefix, szuffix, infix, kódfa, prefix kód, egyenletes kód, vesszős kód

2. McMillian-egyenlőtlenség, átlagos szóhosszúság, optimális kód, Shannon tétele zajmentes csatornára, Shannon-kód létezése, optimális kód konstrukciója, kódolandó abc kiterjesztése, szótárkódok

3. Hibakorlátozó kódolás, hibajelző kódok, paritásbites kód, t-hibajelző, pontosan t-hibajelző kód, kód távolság, kód súlya, csoportkód, minimális távolságú dekódolás, döntés függvény, döntési hiba

4. A t-hibajavító kód, pontosan t-hibajavító kód, hibajavítás ismert hibahelyekkel, ismétléses kód, kétdimenziós paritásellenőrzés,

Hamming-korlát, Singleton-korlát, MDS-kód

5. Lineáris kód, generátor és ellenőrző mátrix, szindróma, szisztematikus kódolás, szindrómadekódolás, mellékosztál-vezető, Hamming-kód, Polinomkód, generátorpolinom, Reed-Solomon-kódok, hibahelypolinom, hibaértékpolinom, kódrövidítés, kódok direkt szorzata, kaszkád kódok adatátszövés

6. Algoritmusok, ordó, Turin-gép, Turin-gép mint számítási eljárás, Univerzális Turin-gépek

Irásbeli kérdések

Definiálja a gráf, csúcsok, élek illeszkedési leképezés fogalmát.
Definiálja az "illeszkedik", "véggpontja" és izolált "csúcs" fogalmakat.
Definiálja az üres gráf és az illeszkedési reláió fogalmát.
Definiálja csúsok, illetve élek szomszédosságát.
Definiálja a hurokél és a páhuzamos élek fogalmát.
Definiája az egyszerű gráf és a véges gráf fogalmát.
Definiálja gráfban a fokszám és a reguláris gráf fogalmát.

Mit mondhatunk a gráfban a fokszámok összegéről?
Definiálja gráfok izomorfiáját.
Definiálja a teljes gráf fogalmát.
Hány éle van egy teljes gráfnak?
Definiálja a páros gráf fogalmát.
Adja meg a "három ház három kút" gráfot.
Definiálja a részgráf és a feszített részgráf fogalmát.
Definiálja részgráf komplementerét.
Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott gráfot.
Definiálja a séta és a séta hossza fogalmát.
Definiálja a nyílt és a zárt sétát.
Definiálja az út fogalmát.
Definiálja a vonal fogalmát.
Definiálja a kör fogalmát.
Hogyan kaphatunk sétából utat? Fogalmazza meg az állítást.
Definiálja az összefüggőség és a komponens fogalmát.
Mi a kapcsolat a komponensek és az összefüggőség között?
Definiálja a fa fogalmát.
Fogalmazzon meg két szükséges és elégséges feltételt arra, hogy egy egyszerű gráf fa legyen.
Egy véges gráfban nincs kör, de van él. Mit állíthatunk fokszámokkal

kapcsolatban?
Egy egyszerű véges gráfnak n csúsa van. Fogalmazzon meg két olyan szükséges és elégséges feltételt amelyben szerepel az élek száma, arra, hogy a gráf fa.
Definiálja a feszítőfa fogalmát.
Mit állíthatunk feszítőfa létezéséről?
Mikor mondjuk, hogy egy csúcs halmaz illetve élhalmaz elvág két csúcsot?
Definiálja az elvágó élhalmaz és a vágás fogalmát.
Mit állíthatunk véges összefüggő gráfban a vágások számáról?
Definiálja az erdő fogalmát. Mi az összefüggés a fákkal?
Definiálja a feszítőőerdő fogalmát. Hány éle van egy véges gráf feszítő erdőjének?
Definiálja az Euler-vonal fogalmát.
Fogalmazza meg a véges összefüggő gráfok vonalak egyesítéseként való előállításra vonatkozó tételt.
Definiálja a Hamilton-út illetve Hamilton-kör fogalmát.
Definiálja a címkézett gráf fogalmát.
Definiálja a súlyozott gráf fogalmát.
Fogalmazza meg a Kruskal algoritmust és a rá vonatkozó tételt.
Mit értünk mohó algoritmuson?
Definiálja az irányított gráf, csúsok, élek és illeszkedési leképezés

fogalmát.
Definiálja irányított gráfban a kezdőpont és a végpont fogalmát.
Definiálja a gráf irányítása illetve megfordítása fogalmát.
Definiálja a szigorúan párhuzamos élek fogalmát.
Definiálja az egyszerű gráf és a véges gráf fogalmát.
Definiálja csúcs befokát és kifokát.
Mit mondhatunk irányított gráfokra a fokszámok összegéről?
Definiálja irányított gráfok izomoráját.
Definiálja az irányított részgráf és a feszített irányított részgráf fogalmát.
Definiálja irányított részgráf komplementerét.
Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott irányított gráfot.
Definiálja a irányított séta és az irányított séta hossza fogalmát.
Definiálja a nyílt és a zárt irányított sétát.
Definiálja az irányított út fogalmát.
Definiálja az irányított kör fogalmát.
Definiálja az erős összefüggőség és az erős komponens fogalmát.
Mi a kapcsolat az erős komponensek és az erős összefüggőség között?
Definiálja az irányított fa és gyökere fogalmát.
Definiálja irányított fában a leveleket.
Definiálja egy művelet esetén a homomorfizmus és a homomorf kép

fogalmát.
Definiálja egy művelet esetén a monomorfizmus, az epimorfizmus és az izomorfizmus fogalmát.
Definiálja egy művelet esetén az endomorfizmus és az automorfizmus fogalmát.
Mit mondhatunk homomorfizmusnál félcsoport, egységelem, inverz és felcserélhető elemek esetén?
Mi mondhatunk homomorfizmusnál csoport, kommutatív félcsoport és Abel-csoport esetén?
Adjon meg szükséges és elégséges feltételeket arra, hogy egy félcsoport csoport legyen.
Fogalmazza meg csoportban az egyszerüsítési szabályt.
Adjon meg szükséges és elégséges feltételeket arra, hogy egy csoport egy részhalmaza részcsoport legyen.
Mit mondhatunk részcsoportok metszetéről?
Definiálja a generátum és a generátorrendszer fogalmát.
Definiálja a ciklikus csoport és generátora fogalmát.
Fogalmazza meg a generátumot leíró állítást.
Mit mondhatunk ciklikus csoport homomorf képéről?
Definiálja csoport és elem rendjét.
Fogalmazza meg a ciklikus csoportok szerkezetét leíró tételt.

Mi a kapcsolat elem és részcsoport rendje között?
Mit mondhatunk ciklikus csoport részcsoportjairól?
Mit mondhatunk véges ciklikus csoport részcsoportjai generátorainak számáról?
Definiálja a bal- és jobboldali mellékosztályokat.
Mi a kapcsolat a bal- és a jobboldali mellékosztályok között?
Definiálja részcsoport indexét.
Fogalmazza meg Lagrange tételét.
Mi a kapcsolat elem rendje és a csoport rendje között?
Definiálja a normálosztó fogalmát.
Adjon meg szükséges és elégséges feltételeket arra, hogy egy részcsoport normálosztó legyen.
Mit mondhatunk normálosztók metszetéről?
Fogalmazza meg kompatibilis osztályozások és a normálosztók közötti kapcsolatot leíró tételt.
Definiálja a faktorcsoport fogalmát és fogalmazza meg a definícióban felhasznált tételt.
Fogalmazza meg a homomorfizmus-tételt csoportokra.
Definiálja csoportok direkt szorzatát.
Fogalmazza meg a véges Abel-csoportok alaptételét.
Fogalmazza meg Cayley tételét.

Definiálja két művelet esetén a homomorfizmus és a homomorf kép fogalmát.
Definiálja két művelet esetén a monomorfizmus, az epimorfizmus és az izomorfizmus fogalmát.
Definiálja két művelet esetén az endomorfizmus és az automorfizmus fogalmát.
Mit mondhatunk homomorfizmusnál gyűrű képéről?
Definiálja gyűrű karakterisztikáját.
Definiálja a részgyűrű fogalmát.
Definiálja a jobbideál, balideál és ideál fogalmát.
Definiálja a triviális ideál és a valódi ideál fogalmát.
Definiálja az egyszerű gyűrű fogalmát.
Definiálja a generált ideál és a főideál fogalmát.
Definiálja gyűrűben a mellékosztályokat.
Definiálja a faktorgyűrű fogalmát és fogalmazza meg a definícióban felhasznált tételt.
Fogalmazza meg a homomorfizmus-tételt gyűrűkre.
Definiálja a Gauss-gyűrű fogalmát.
Igaz-e hogy Gauss-gyűrűben minden irreducibilis elem prím?
Definiálja az euklideszi gyűrű fogalmát.
Fogalmazza meg az euklideszi gyűrűben az egységeket és az

asszociáltakat leíró tételt.
Fogalmazza meg a bővített euklideszi algoritmust euklideszi gyűrűben.
Mi a kapcsolat euklideszi gyűrűben a prímelemek és az irreducibilis elemek között?
Definiálja az egyhatározatlanú polinom fogalmát.
Definiálja egyhatározatlanú polinomok összeadását és szorzását.
Definiálja polinom együtthatóit, főegyütthatóit és fokszámát.
Definiálja a lineáris polinomokat.
Definiálja a monom fogalmát egy határozatlan esetén.
Definiálja a főpolinom fogalmát.
Mit mondhatunk polinomok szorzatának főegyütthatóiról?
Mit mondhatunk polinomok szorzatának fokáról?
Definiálja polinom helyettesítési értékét és gyökét.
Definiálja a polinomhoz tartozó polinomfüggvényt. Tartozhat-e különböző polinomokhoz ugyanaz a polinomfüggvény?
Fogalmazza meg a maradékos osztás tételét polinomokra.
Fogalmazza meg a gyöktényező leválasztására vonatkozóállítást.
Legfeljebb hány gyöke van egy polinomnak? Fogalmazza meg az állítást.
Milyen esetben kölcsönösen egyértelmű a megfeleltetés a polinomok és a polinomfüggvények között? Fogalmazza meg az állítást.
Definiálja polinom algebrai deriváltját.

Az f, g polinomokra $g^n | f$. Mit állíthatunk f'ről? Fogalmazza meg az állítást.
Hogyan kaphatunk egy polinomból négyzetmentes polinomot?
Fogalmazza meg az állítást.
Definiálja polinom többszörös gyökét.
Mi a kapcsolat a polinom gyökei és a deriváltjának a gyökei között?
Fogalmazza meg az állítást.
Lehet-e egy polinom n-szeres gyöke a deriváltnak is legalább n-szeres gyöke?
Fogalmazza meg a véges testek elemszámát leíró tételt.
Van-e minden prímhatványnak megfelelő elemszámú véges test?
Fogalmazza meg a véges testek alaptételét.
Definiálja a többhatározatlanú polinom fogalmát.
Definiálja többhatározatlanú polinom együtthatóit, tagjainak multifokát és fokát.
Definiálja a többhatározatlanú monom fogalmát.
Definiálja többhatározatlanú polinom fokát. Milyen megállapodások mellett egyértelmű egy többhatározatlanú polinom felírása?
Definiálja a többhatározatlanú lineáris polinomokat.
Hogyan írhatjuk fel két többhatározatlanú polinom összegének, illetve szorzatának az együtthatóit?

Milyen esetben lesz a többhatározatlanú polinomok gyűrűje nullosztómentes?
Mit mondhatunk két tőbbhatározatlanú polinom szorzatának a fokáról?
Milyen esetben lesz a többhatározatlanú polinomok gyűrűje Gauss-gyűrű?
Fogalmazza meg az állítást.