- $9/19 \ldots 21$:

$<$

A *logikai formulák* (vagy *mondat*ok) az adott elmélet predikátumaiból épülnek fel a $\neg$ („*nem*”), $\wedge$ („*és*”), $\vee$ („*vagy*”), $\Rightarrow$ („*ha* … *akkor* …”) és $\iff$ („*akkor és csak akkor*” vagy „*pontosan akkor*”) *logikai jel*ek, valamint a két kvantor, a $\exists$ („létezik” vagy „van

$>$

A *logikai formulák* (vagy *mondat*ok) az adott elmélet predikátumaiból épülnek fel a $\neg$ („*nem*”, idegen szóval *negáció*), $\wedge$ („*és*”, idegen szóval *konjukció*), $\vee$ (megengedő „*vagy*”, idegen szóval *diszjunkció*), $\Rightarrow$ („*ha* … *akkor* …”, *implikáció*) és $\iff$ („*akkor és csak akkor*” vagy „*pontosan akkor*”, *ekvivalencia*), $\oplus$ (kizáró „*vagy*”, gyakrabban „*vagy* … *vagy* …”: pontosan az egyik), $|$ („*sem* … *sem* …”), $\|$ (összeférhetetlen „*vagy*”, gyakrabban „*vagy* … *vagy* …”: legfeljebb az egyik, de lehet, hogy egyik se) *logikai jel*ek, valamint a két *kvantor*, a $\exists$ („létezik” vagy „van

- $9/-14$:

$<$

félreértést, akkor a formula felírásából elhagyhatunk zárójeleket.

$>$

félreértést, akkor a formula felírásából elhagyhatunk zárójeleket.

Néha kevesebb logikai jelet illetve kvantort használunk. Ekkor az adott logikai jellel/jelekkel illetve kvantorral/kvantorokkal felírható logikai formulákról beszélünk.

- $10/-10$:

$<$

dező nyelv használatakor predikátumokkal definiálnunk kell, amit kérdezni szeretnénk.

$>$

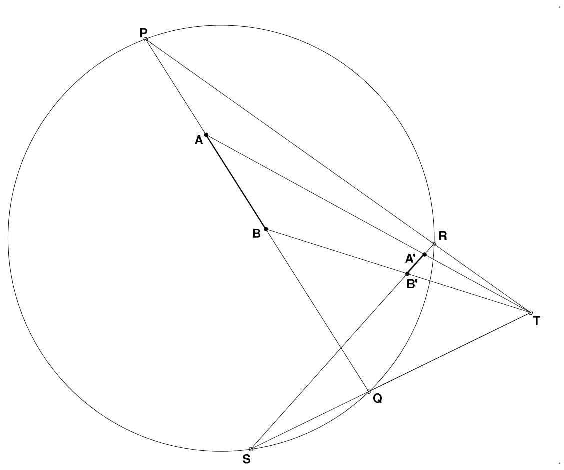
dező nyelv használatakor predikátumokkal definiálnunk kell, amit kérdezni szeretnénk.

Néha nem is olyan könnyű eldönteni, hogyan formalizáljunk valamit. Például a magyar nyelvű mondatok formalizálásánál gondot okozhat a vagy háromféle használata. Az „Átok reá, ki gyávaságból Vagy lustaságból elmarad” mondatban a vagy megengedő értelmű, a „Vagy bolondok vagyunk s elveszünk egy szálig, Vagy ez a mi hitünk valóságra válik” mondatban kizáró, a „vagy iszol, vagy vezetsz” mondatban pedig összeférhetetlen értelmű. Lásd Quine [68] könyvének részletes elemzéseit. A matematikában a vagy legtöbbször megengedő értelmű.

- $12/-13$:

$<$

Az axiomatikus alapfogalmakat nem definiáljuk. Ezeken azt érthetünk, amit akarunk, csak arra kell figyelnünk, hogy az axiómák a mi olvasatunkban is igazak maradjanak. A bizonyítások menetét az értelmezés nem befolyásolja, hiszen a fogalmak szemléletes jelentését amúgy sem használhatjuk fel a tárgyalás során. Ha például valaki a geometriai „tér”, „pont”, „egyenes”, „sík” stb. fogalma alatt ezeknek csak egy adott gömb belsejébe eső részeit érti, akkor a geometriai tételek nagy része igaz marad



0.1. Szakaszok egyenlősége a Cayley–Klein-modellben

vagy érdekesen módosul az axiomatikus alapfogalmak ügyes értelmezése esetén (Cayley–Klein-modell, lásd Hajós György [32], 130. oldal). Az 1.1. ábra a szakaszok egyenlőségét szemlélteti.

Talán még meglepőbb, hogy ha „pont" alatt egy függvényt, az f és g „pontokon" átmenő „egyenesen" a $\lambda \cdot f + (1-\lambda) \cdot g$ függvények halmazát értjük (ahol λ tetszőleges valós szám), akkor is értelmes matematikát kapunk, amely némiképp a geometriára emlékeztet, például a háromszög oldalaira tanult egyenlőtlenségek is érvényesek maradnak.

$>$

Ha például valaki a geometriai „pont" alatt (X, Y) párokat ért, ahol X és Y is a „páros" vagy „páratlan" fogalom lehet, rövidítve e, illetve e, egyenes alatt pedig $AX + BY = C$ alakú egyenleteket, ahol az A, B, C együtthatók mindegyike e vagy o lehet, de A és B nem lehet mindkettő e, illeszkedés alatt pedig azt érti hogy az (X, Y) pont koordinátái kielégítik az adott egyenletet, akkor olyan geometriához jut, amelyben 4 pont és 6 egyenes van, teljesül, hogy bármely két különböző pontra egy és csak egy egyenes illeszkedik, teljesül a párhuzamossági axióma, és még néhány más axióma is, például, hogy létezik három olyan pont, amely nem fekszik egy egyenesen. Ebben a geometriában is érvényes minden olyan tétel, amelynek bizonyításához csak ezeket az axiómákat használtuk fel. Ehhez hasonló véges geometriák szerepet játszanak a kódoláselméletben.

- $13/-6$:

$<$

Ezek helyett Bolyai Farkas azt az állítást vette axiómának, hogy „három pont vagy egy egyenesen, vagy egy körön van". (Ennek előnye, hogy teljes kört már mindenki látott — bár 3 millió fényév sugarú kört még egyikünk sem.)

Ha az előbbi állítások bármelyikét hozzávesszük Eukleidész többi axiómájához (az úgynevezett maradék axiómarendszerhez), ugyanazt a geometriát kapjuk: bármelyik rendszerben bizonyítható a többi tétel igazsága. Ezért aligha megalapozott egyiket vagy másikat egyszerűbbnek vagy bonyolultabbnak tartani a többinél — inkább arról van szó, hogy melyikhez szoktunk hozzá, hogy a kezdő még nem érzékeli egyik-másik állítás súlyát.

Bolyai János a maradék axiómarendszerből építette fel abszolút geometriáját. Az 1.1. ábra az euklideszi síkban fekszik, és egyúttal a hiperbolikus síkgeometria egy lehetséges modellje, tehát ha a Bolyai-geometriában van ellentmondás, akkor az euklideszben is van. A fordított irányú állítás is bizonyítható.

$>$

Ezek helyett Bolyai Farkas azt az állítást vette axiómának, hogy „három pont vagy egy egyenesen, vagy egy körön van”.

Ha az előbbi három állítás bármelyikét hozzávesszük Eukleidész többi axiómájához (az úgynevezett maradék axiómarendszerhez), ugyanazt a geometriát kapjuk: bármelyik rendszerben bebizonyítható a másik két állítás.

- $16/-7$:

$<$

mondjuk, hogy a halmazrendszer *diszjunkt*. Ha a halmazrendszer bármely két halma-

$>$

mondjuk, hogy a halmazrendszer *diszjunkt*. Ha a halmazrendszer bármely két különböző halma-

- $20/4$:

$<$

irányított él x-ből y-ba (azaz rajzoljunk egy x-ből y-ba vezető nyilat), ha $(x,y) \in R$.

$>$

irányított él x-ből y-ba (azaz rajzoljunk egy x-ből y-ba vezető nyilat), ha $(x,y) \in R$. Lásd az 1.3. ábrát.

- $20/16$:

$<$

relációt értjük.

$>$

relációt értjük. Lásd az 1.4. ábrát.

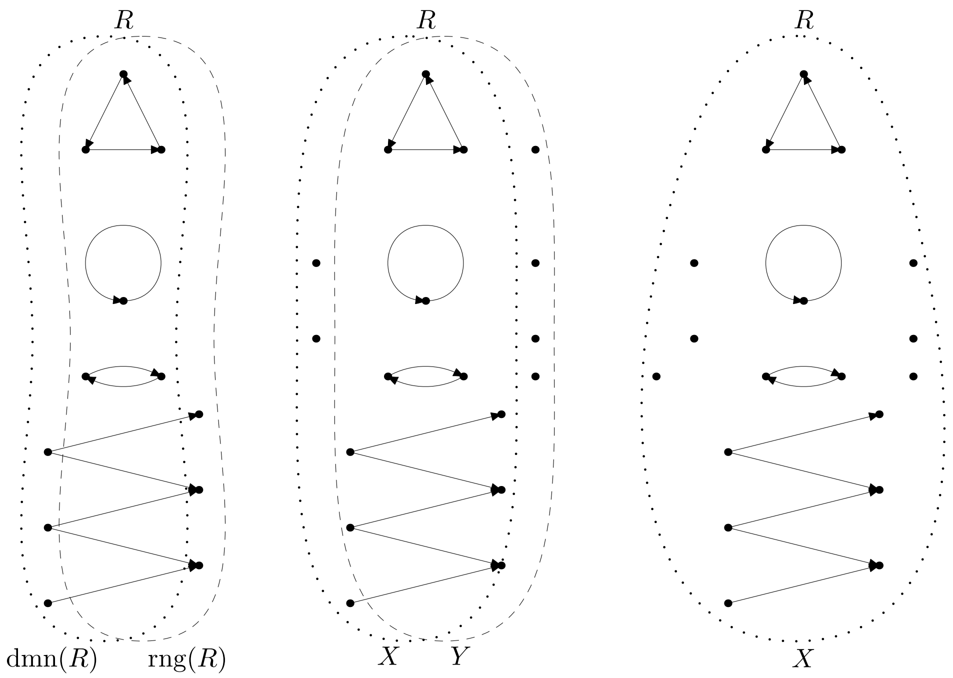
- $20/-1$:

$<$

relációt értjük. (Egyesek fordítva, $S \circ R$-et írnak; a fenti jelölés előnye, hogy ezzel bármely A halmazra $R\big(S(A)\big) = (R \circ S)(A)$.)

$>$

relációt értjük. Lásd az 1.5. ábrát. (Egyesek fordítva, $S \circ R$-et írnak; a fenti jelölés előnye, hogy ezzel bármely A halmazra $R\big(S(A)\big) = (R \circ S)(A)$.)



0.2. ábra: dmn és rng, reláció X és Y között, X-beli reláció.

- 21/12 :

  <

  Definíció. Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1) *tranzitív*, ha minden x, y, z-re $(x, y) \in R$ és $(y, z) \in R$ esetén $(x, z) \in R$;

(2) *intranzitív*, ha minden x, y, z-re $(x, y) \in R$ és $(y, z) \in R$ esetén $(x, z) \notin R$;

(3) *szimmetrikus*, ha minden x, y-ra $(x, y) \in R$ esetén $(y, x) \in R$;

(4) *antiszimmetrikus*, ha minden x, y-ra $(x, y) \in R$ és $(y, x) \in R$ esetén $x = y$;

(5) *szigorúan antiszimmetrikus*, ha minden x, y-ra $(x, y) \in R$ esetén $(y, x) \notin R$;

(6) *reflexív*, ha minden $x \in X$ esetén $(x, x) \in R$;

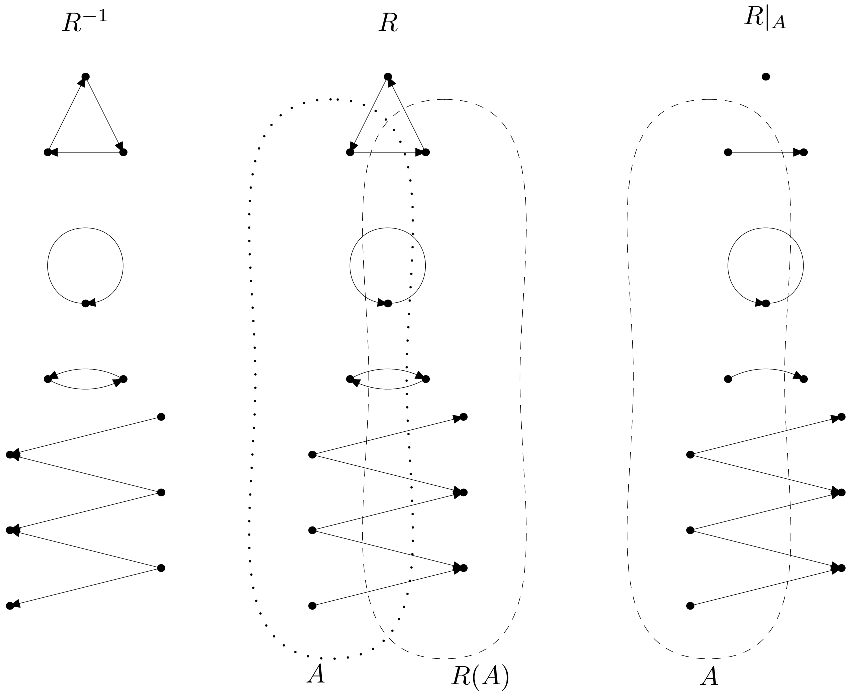
(7) *irreflexív*, ha minden $x \in X$ esetén $(x, x) \notin R$;

(8) *trichotom*, ha minden $x, y \in X$ esetén $x = y$, $(x, y) \in R$ és $(y, x) \in R$ közül pontosan egy teljesül;

(9) *dichotom*, ha minden $x, y \in X$ esetén $(x, y) \in R$ vagy $(y, x) \in R$ (esetleg mindkettő), azaz bármely két elem összehasonlítható.

Vegyük észre, hogy az első öt tulajdonság csak R-től, míg az utolsó négy R-től és X-től is függ, így ezek az (R, X) pár tulajdonságai.

A binér reláció definíciójánál említett példák között mindegyik feltétel teljesülésére és nem teljesülésére is találhatunk példát.



0.3. ábra: reláció inverze, halmaz képe, reláció megszorítása.

>

Definíció. Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1) *tranzitív*, ha minden x, y, z-re $(x, y) \in R$ és $(y, z) \in R$ esetén $(x, z) \in R$;

(2) *szimmetrikus*, ha minden x, y-ra $(x, y) \in R$ esetén $(y, x) \in R$;

(3) *antiszimmetrikus*, ha minden x, y-ra $(x, y) \in R$ és $(y, x) \in R$ esetén $x = y$;

(4) *szigorúan antiszimmetrikus*, ha minden x, y-ra $(x, y) \in R$ esetén $(y, x) \notin R$;

(5) *reflexív*, ha minden $x \in X$ esetén $(x, x) \in R$;

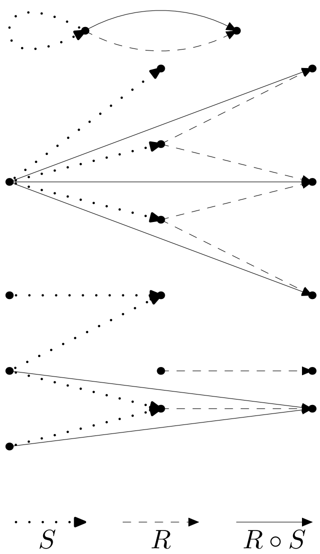
(6) *irreflexív*, ha minden $x \in X$ esetén $(x, x) \notin R$;

(7) *trichotom*, ha minden $x, y \in X$ esetén $x = y$, $(x, y) \in R$ és $(y, x) \in R$ közül pontosan egy teljesül;

(8) *dichotom*, ha minden $x, y \in X$ esetén $(x, y) \in R$ vagy $(y, x) \in R$ (esetleg mindkettő), azaz bármely két elem összehasonlítható.

Vegyük észre, hogy az első négy tulajdonság csak R-től, míg az utolsó négy R-től és X-től is függ, így ezek az (R, X) pár tulajdonságai.

A binér reláció definíciójánál mindegyik tulajdonság teljesülésére találunk példát, és a (2)–(8) tulajdonságok nem teljesülésére is találunk példát. Nem tranzitív a sík pontjai között az a reláció, hogy legfeljebb 1 távolságra vannak.



0.4. ábra: két reláció kompozíciója.

- 22/1 :

  <

  Tétel. *Valamely X halmazon értelmezett $\sim$ ekvivalenciareláció X-nek egy osztályfelbontását adja. Megfordítva, az X halmaz minden osztályfelbontása egy $\sim$ ekvivalenciarelációt hoz létre.*

Bizonyítás. Legyen $\sim$ egy X-beli ekvivalenciareláció, és legyen $\tilde{x} = \{y \in X : y \sim x\}$ az X halmaz x eleme segítségével definiált részhalmaza. Megmutatjuk, hogy az $\tilde{X} = \{\tilde{x} : x \in X\}$ halmaz az X egy osztályozása. Mivel $\sim$ reflexív, $x \in \tilde{x}$, vagyis az $\tilde{x}$ részhalmaz nem üres, és az X halmaz minden x eleme benne van a $\tilde{X}$ valamely elemében, például $\tilde{x}$-ban. Csak azt kell belátnunk, hogy a különböző részhalmazok metszete üres. Ha $\tilde{x} \cap \tilde{y} \neq \emptyset$, akkor legyen z a metszet egy eleme. Ekkor $z \sim x$ és $z \sim y$, amiből a szimmetria és a tranzitivitás miatt $x \sim y$. Ha most $w \in \tilde{x}$, akkor a tranzitivitás miatt $w \in \tilde{y}$. Hasonlóan, a szimmetria és a tranzitivitás miatt, ha $w \in \tilde{y}$, akkor $w \in \tilde{x}$. Azt kaptuk tehát, hogy $\tilde{x} = \tilde{y}$, azaz ha két részhalmaznak van közös eleme, akkor azonosak, vagyis a különböző $\tilde{x}$ részhalmazok diszjunktak, ezért valóban az X egy osztályfelbontását kaptuk, és $\tilde{x}$ az x-et tartalmazó osztály.

Megfordítva, legyen $\mathcal{O}$ az X egy osztályozása. Legyen

$$R = \big\{(x, y) \in X \times X : x \text{ és } y \text{ az } \mathcal{O} \text{ ugyanazon halmazának elemei}\big\}.$$

Ez az R nyilván reflexív, szimmetrikus és mivel az osztályok páronként diszjunktak, tranzitív is, tehát ekvivalenciareláció. $\square$

Vegyük észre, hogy ha egy ekvivalenciarelációból képezzük a fentiek szerint hozzá tartozó osztályozást, majd abból a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza. Hasonlóan, ha egy osztályozásból képezzük a hozzá tartozó ekvivalenciarelációt, majd ebből a megfelelő ekvivalenciaosztályokat, akkor az eredeti osztályozást kapjuk vissza.

>

Tétel. *Valamely X halmazon értelmezett $\sim$ ekvivalenciareláció esetén a $\tilde{x} = \{y \in X : y \sim x\}$, $x \in X$ ekvivalenciaosztályok X-nek egy $\tilde{X} = X/\sim$ osztályozását adják. Megfordítva, az X halmaz bármely $\mathcal{O}$ osztályozása esetén az $\cup\{Y \times Y : Y \in \mathcal{O}\}$ reláció ekvivalenciareláció, amelyhez tartozó ekvivalenciaosztályok halmaza $\mathcal{O}$. Hasonlóan, ha egy ekvivalenciarelációra képezzük az ekvivalenciaosztályokat, majd ebből a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza.*

Bizonyítás. Legyen $\sim$ egy X-beli ekvivalenciareláció, és legyen $\tilde{x} = \{y \in X : y \sim x\}$ az X halmaz x elemének ekvivalenciaosztálya. Azt kell megmutatnuk, hogy az $\tilde{X} = \{\tilde{x} : x \in X\}$ halmaz az X egy osztályozása. Mivel $\sim$ reflexív, $x \in \tilde{x}$, vagyis az $\tilde{x}$ részhalmaz nem üres, és az X halmaz minden x eleme benne van a $\tilde{X}$ valamely elemében, például $\tilde{x}$-ban. Már csak azt kell belátnunk, hogy a különböző ekvivalenciaosztályok metszete üres. Ha $\tilde{x} \cap \tilde{y} \neq \emptyset$, akkor legyen z a metszet egy eleme. Ekkor $z \sim x$ és $z \sim y$, amiből a szimmetria és a tranzitivitás miatt $x \sim y$. Ha most $w \in \tilde{x}$, akkor a tranzitivitás miatt $w \in \tilde{y}$. Hasonlóan, a szimmetria és a tranzitivitás miatt, ha $w \in \tilde{y}$, akkor $w \in \tilde{x}$. Azt kaptuk tehát, hogy $\tilde{x} = \tilde{y}$, azaz ha két részhalmaznak van közös eleme, akkor azonosak, vagyis a különböző $\tilde{x}$ részhalmazok diszjunktak, ezért valóban az X egy osztályozását kaptuk, és $\tilde{x}$ az x-et tartalmazó osztály.

Megfordítva, legyen $\mathcal{O}$ az X egy osztályozása, és legyen $R \cup \{Y \times Y : Y \in \mathcal{O}\}$. Nyilván $(x, y) \in \mathbb{R}$ pontosan akkor teljesül, ha x és y az $\mathcal{O}$ ugyanazon halmazának elemei. Ez az R nyilván reflexív, szimmetrikus és mivel az osztályok páronként diszjunktak, tranzitív is, tehát ekvivalenciareláció. Az is nyilvánvaló, hogy ha egy osztályozásból képezzük a hozzá tartozó ekvivalenciarelációt, majd ebből a megfelelő ekvivalenciaosztályokat, akkor az eredeti osztályozást kapjuk vissza, és fordítva, ha egy ekvivalenciarelációból képezzük a fentiek szerint hozzá tartozó osztályozást, majd abból a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza. $\square$

- 24/9 :

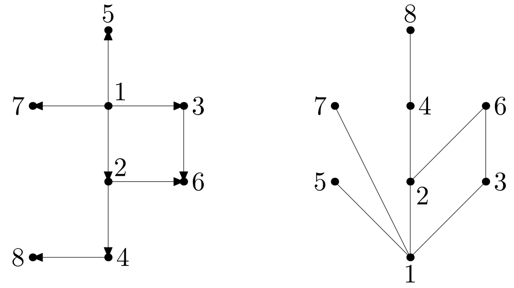
<

egyértelmű maximális eleme, akkor azt $\max X$-szel jelöljük.

>

egyértelmű maximális eleme, akkor azt $\max X$-szel jelöljük.

° **Példa.** Tekintsük az $\{1, 2, 3, 4, 5, 6, 7, 8\}$ halmazon az „osztója” részbenrendezést. A 1.6. ábrán ennek Hasse-diagrammja látható két alakban. Itt 1 legkisebb és minimális elem, 5, 6, 7 és 8 maximális elemek, de egyik sem legnagyobb; $\{1, 2, 4, 8\}$ lánc, de $\{1, 2, 3, 6\}$ nem; a 2 közvetlenül megelőzi 4-et, de 8-at nem.



0.5. ábra: *Hasse-diagramm* két alakban.

- 24/−16 :

  <

  Jólrendezés. Egy X részben rendezett halmazt *jólrendezett*nek, a rendezését pedig *jólrendezés*nek nevezzük, ha X bármely nem üres részhalmazának van legkisebb eleme. Jólrendezett halmaz mindig rendezett.

  >

  Jólrendezés. Egy X rendezett halmazt *jólrendezett*nek, a rendezését pedig *jólrendezés*nek nevezzük, ha X bármely nem üres részhalmazának van legkisebb eleme.

- 28/−10 :

  <

  zett függvényt) „szorzótáblával" is megadhatunk: az első oszlopba a baloldali operandus,

  >

  zett függvényt) *műveleti táblá*val is megadhatunk: az első oszlopba a baloldali operandus,

- 28/−8 :

  <

  ◦ **Descartes-szorzatok és relációk.** Az X_1 és X_2 halmazok Descartes-szorzatát mint az összes (x_1, x_2), $x_1 \in X_1$, $x_2 \in X_2$ rendezett párok halmazát definiáltuk. Létezik egy természetes, kölcsönösen egyértelmű megfeleltetés $X_1 \times X_2$ elemei és az $\{1, 2\}$-vel indexezett olyan családok között, amelyekre $x_1 \in X_1$ és $x_2 \in X_2$. Ennek megfelelően, ha az $(x_1, x_2, \ldots, x_n)$ elem n-eseket az $\{1, 2, \ldots, n\}$ halmaz, azaz $\mathbb{N}^+$-nak az $n \in \mathbb{N}^+$-nál nem nagyobb elemei által indexelt családokkal azonosítjuk, akkor az $X_1 \times X_2 \times \cdots \times X_n$ Descartes-szorzatot mint az összes olyan x_i, $i \in \{1, 2, \ldots, n\}$ családok halmazát definiálhatjuk, amelyekre $x_i \in X_i$, ha $i \in \{1, 2, \ldots, n\}$. Ilyen szorzathalmazok részhalmazait *n-változós reláció*knak nevezzük. Tetszőleges kapcsolatokat relációkkal írhatunk le, ezért a relációk fontos szerepet játszanak az adatbázis-kezelő rendszerekben. Egy Descartes-szorzaton értelmezett függvényt szokás egyébként *többváltozós függvény*nek is nevezni. Megjegyezzük, hogy egy f többváltozós függvénynek $(x_1, x_2, \ldots, x_n)$-hez rendelt értékét mindenki $f(x_1, x_2, \ldots, x_n)$-nel jelöli $f\big((x_1, x_2, \ldots, x_n)\big)$ helyett. Ha $X_1 = X_2 = \cdots = X_n = X$, akkor $X_1 \times X_2 \times \cdots \times X_n$ helyett X^n-et szokás írni. Ennek a halmaznak a részhalmazait X-beli *relációk*nak, esetleg homogén relációknak nevezzük. Többváltozós függvények esetén is előfordul, hogy a változókat alsó indexként írjuk. Például a *Kronecker-féle δ-függvény*t a $\delta_{x,y} = 1$, ha $x = y$ és $\delta_{x,y} = 0$, ha $x \neq y$ összefüggésekkel definiáljuk ($x, y \in X$).

Nincs szükségünk a természetes számokra, ha tovább általánosítjuk a halmazok szorzatának fogalmát.

Descartes-szorzat. Legyen X_i, $i \in I$ egy halmazcsalád. A halmazcsaládhoz tartozó *kiválasztási függvény*nek nevezzük azokat az $x : I \to \cup_{i\in I} X_i$ függvényeket, amelyekre $x_i \in X_i$ minden $i \in I$-re. Az X_i, $i \in I$ halmazcsalád $\times_{i\in I} X_i$ *Descartes-szorzat*a a halmazcsaládhoz tartozó összes kiválasztási függvények halmaza. Ha nem okozhat félreértést, csak $\times_i X_i$-t írunk. Világos, hogy ha van olyan $i \in I$, amelyre $X_i = \emptyset$, akkor nincs kiválasztási függvény, így $\times_i X_i = \emptyset$. Ha $I = \emptyset$, akkor viszont az üres függvény kiválasztási függvény, így $\times_i X_i = \{\emptyset\}$. Ha minden $i \in I$-re $X_i = X$, akkor X^I-t írunk $\times_{i\in I} X_i$ helyett. Így X^I az összes I-t X-be képező függvények halmaza. Ha $I = \emptyset$, akkor $X^I = \{\emptyset\}$, ha pedig $I = \{i\}$, akkor létezik egy természetes, kölcsönösen egyértelmű leképezése X^I-nek X-re, pontatlanul fogalmazva X^I azonosítható X-szel.

Ha $J \subset I$, akkor az $x \mapsto x|_J$ leképezést $\times_{i\in I} X_i$-nek $\times_{j\in J} X_j$-be való *projekció*jának nevezzük. Ha $J = \{j\}$, akkor ez az $x \mapsto x_j$ leképezéssel azonosítható, és *j-edik projekció*nak nevezzük.

>

Reláció és Descartes-szorzat általános esetben. Sokfajta kapcsolatot írhatunk le relációkkal, ezért az általános relációfogalom fontos szerepet játszik az adatbáziskezelő rendszerekben. Tekintsük bizonyos „jellemzők” vagy „nevek” („attributumok”) egy I halmazát. Például egy személyi törzsállomány esetén egy ember leírására az alábbi jellemzők halmazát használhatjuk:

$$I = \{\text{személyi\_szám}, \text{név}, \text{lakcím}, \text{végzettség}\}.$$

Minden $i \in I$-hez hozzárendeljük az adott attributumhoz rendelhető értékek X_i halmazát, például $X_{\text{személyi\_szám}}$ lehet a 11 jegyű decimális számok halmaza. Tekintsünk egy

$$x : I \mapsto \cup_{i\in I} X_i$$

függvényt, amelyre $x_i \in X_i$ minden $i \in I$-re. Egy ilyen függvényt az informatikában az X_i ($i \in I$) indexelt családhoz tartozó *rekord*nak nevezünk: I elemei a *mezőnev*ek, x_i pedig a rekordnak az i nevű *mező*je. Az X_i ($i \in I$) indexelt családhoz tartozó rekordoknak egy tetszőleges halmazát az adott X_i ($i \in I$) indexelt családhoz tartozó *adattáblá*nak nevezzük. A gyakorlatban a mezőneveket persze csak egyszer tároljuk le valamilyen sorrendben, és ugyanebben a sorrendben tároljuk az egyes rekordok mezőit. Az alábbi táblázat egy adattáblát mutat:

személyi_szám	név	lakcím	végzettség
`15106111888`	`Vass Oxid`	`Arad`	`egyetem`
`17806111888`	`Czink Szulfid`	`Budapest`	`egyetem`
`17809171888`	`Arany Klorid`	`Budapest`	`szakiskola`
`18809151888`	`Radon Fluorid`	`Debrecen`	`szakiskola`
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Általánosabban, a matematika nyelvén fogalmazva, legyen X_i, $i \in I$ egy tetszőleges indexelt halmazcsalád. A halmazcsaládhoz tartozó *kiválasztási függvény* minden olyan $x : I \to \cup_{i \in I} X_i$ függvény, amelyre $x_i \in X_i$ minden $i \in I$-re. Az X_i $(i \in I)$ halmazcsaládhoz tartozó *reláción* kiválasztási függvények egy tetszőleges halmazát értjük. Legyen a halmazcsalád *Descartes-szorzat*a a halmazcsaládhoz tartozó összes kiválasztási függvények halmaza. Ha nem okozhat félreértést, csak $\times_i X_i$-t írunk. Kételemű I esetén a binér reláció fogalmát, illetve két halmaz Descartes-szorzatát kapjuk vissza, ha az I egyik eleméhez rendelt értéket első koordinátának, a másikhoz rendelt értéket pedig második koordinátának tekintjük.

Világos, hogy ha van olyan $i \in I$, amelyre $X_i = \emptyset$, akkor nincs kiválasztási függvény, így $\times_i X_i = \emptyset$. Ha $I = \emptyset$, akkor viszont az üres függvény az egyetlen kiválasztási függvény, így $\times_i X_i = \{\emptyset\}$. Ha minden $i \in I$-re $X_i = X$, akkor -t írunk $\times_{i \in I} X_i$ helyett. Így X^I az összes I-t X-be képező függvények halmaza. (Ezt a jelölést tetszőleges X és I halmazok esetén használjuk a továbbiakban.) Ennek a halmaznak a részhalmazait X-beli *reláció*knak vagy *homogén reláció*knak nevezzük. Most is ha $I = \emptyset$, akkor $X^I = \{\emptyset\}$. Ha I egyelemű, $I = \{i\}$, akkor $\big\{(i, x)\big\} \mapsto x$ egy természetes, kölcsönösen egyértelmű leképezése X^I-nek X-re, pontatlanul fogalmazva X^I azonosítható X-szel.

Ha $J \subset I$, akkor az $x \in \times_i X_i$ kiválasztási függvényekre értelmezett $x \mapsto x|_J$ leképezést $\times_{i \in I} X_i$-nek $\times_{j \in J} X_j$-be való *vetítés*ének, idegen szóval *projekció*jának nevezzük. Ha J egyelemű, $J = \{j\}$, akkor ez a $p_j : x \mapsto x_j$ leképezéssel azonosítható, amit *j-edik projekció*nak nevezünk. Egy $\times_{i \in I} X_i$-be képező f függvényre $f_j = p_j \circ f$ az f függvény *j-edik koordinátafüggvény*e.

Ha $I = J \cup K$, akkor gyakran hasznos az x kiválasztási függvényt az $(x|_J, x|_K)$ rendezett párral azonosítani, mert ekkor tetszőleges relációból binér reláció lesz, és használhatjuk binér relációk kompozícióját (összetételét) tetszőleges relációk *kompozíció*jának (*összetétel*ének) képzésére. Ha egy $R \subset \times_{i \in I} X_i$ reláció esetén az $\big\{(x|_J, x|_K) : x \in R\big\}$ binér reláció függvény, akkor azt mondjuk, hogy $x|_J$ az x kiválasztási függvénynek az R relációban a J-beli indexekhex tartozó (illetve az x rekordnak az R adattáblában a J-beli mezőnevekhez tartozó) *kulcs*a. A kulcsok segítségével vett összetétel a halmazműveletek, a részhalmazképzés és a projekció mellett az egyik leggyakoribb művelet relációs adatbáziskezelőknél.

- $28/-8$:
  $<$
  Hasonlóan egy véges halmazon egy unér műveletet (vagy általánosabban, bármely,

$>$

$\oplus$	$\uparrow$	$\downarrow$
$\uparrow$	$\downarrow$	$\uparrow$
$\downarrow$	$\uparrow$	$\downarrow$

$\mid$	$\uparrow$	$\downarrow$
$\uparrow$	$\downarrow$	$\downarrow$
$\downarrow$	$\downarrow$	$\uparrow$

$\Vert$	$\uparrow$	$\downarrow$
$\uparrow$	$\downarrow$	$\uparrow$
$\downarrow$	$\uparrow$	$\uparrow$

Hasonlóan egy véges halmazon egy unér műveletet (vagy általánosabban, bármely,

- 29/8 :

$<$

azaz a $\{0, 1, \ldots, n-1\}$ halmazt a $\{\uparrow, \downarrow\}$ halmazba képező függvények halmazán.

$>$

azaz a $\{0, 1, \ldots, n-1\}$ halmazt a $\{\uparrow, \downarrow\}$ halmazba képező függvények halmazán. Az a szokás, hogy az $\uparrow$ értéket 1, a $\downarrow$ értéket pedig 0 reprezentálja. Áramkörökben $\uparrow$ reprezentációja magas feszültség- vagy áramérték (H, mint high), $\downarrow$ reprezentációja pedig alacsony feszültség- vagy áramérték (L, mint low), vagy pedig fordítva. Az első esetben *pozitív logiká*ról, a második esetben pedig *negatív logiká*ról beszélünk.

- 36/−21 :

$<$

$x * (y * z)$, akkor G-t (pontosabban a $(G, *)$ párt) *félcsoport*nak nevezzük. Ha a G

$>$

$x * (y * z)$, akkor G-t (pontosabban a $(G, *)$ párt) *félcsoport*nak nevezzük. Semleges elemes félcsoport neve *monoid*. Ha a G

- 36/−14 :

$<$

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

$>$

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

Egy G monoid azon elemeinek halmazát, amelyeknek van inverze, G^*-gal jelöljük. Bármely G monoidra $(G^*, *)$ csoport.

- 39/13 :

$<$

Ez a félcsoport általában nem kommutatív.

$>$

Ez a félcsoport nem kommutatív, ha X legalább kételemű.

Többváltozós függvények. Egy $X_1 \times X_2 \times \cdots \times X_n$ Descartes-szorzaton vagy annak egy részhalmazán értelmezett függvényt szokás *többváltozós függvény*nek is nevezni. Többváltozós függvények esetén is előfordul, hogy a változókat alsó indexként írjuk. Például a *Kronecker-féle δ-függvény*t a $\delta_{x,y} = 1$, ha $x = y$ és $\delta_{x,y} = 0$, ha $x \neq y$ összefüggésekkel definiáljuk ($x, y \in X$).

- $39/-15$:

$<$

rekurziótétel nem használható, mert a sorozat általános tagja nem csak az előzőtől függ. A

$>$

rekurziótétel nem használható, mert a sorozat általános tagja nem csak az előzőtől, hanem az előző kettőtől függ.

Másik példaként tekintsük azt a problémát, hogy az $n+1$ tényezős $x_0x_1\cdots x_n$ szorzatot hányféleképpen lehet zárójelezni, azaz a szorzások sorrendjét hányféleképpen lehet kijelölni. Jelölje c_n ezt a számot. (Ezek az úgynevezett *Catalan-számok*; számos informatikai problémánál előkerülnek.) Ha $n = 0$, akkor nyilván $c_n = 1$. Egyébként gyűjtsük össze azokat a zárójelezéseket, amelyekben a legkülső szorzás x_k után áll. Ezek száma $c_k c_{n-k-1}$, így azt kapjuk, hogy

$$c_n = c_0c_{n-1} + c_1c_{n-2} + \cdots + c_{n-1}c_0.$$

Ha a c_n számot ennek az összefüggésnek az alapján akarjuk kiszámítani, akkor az összes előző számra szükség van.

A rekurziótétel alábbi általánosabb változata lehetővé teszi, hogy egy sorozat egy tagját az összes előző tag függvényeként adjuk meg.

- $39/-15$:

$<$

A tétel és a bizonyítás érvényes marad akkor is, ha $\mathbb{N}$ helyett tetszőleges N jólrende-

$>$

A tétel szemléletesen fogalmazva azt mondja, hogy ha adott egy függvényünk, amely egy egydimenzió tömb esetén kiszámítja a tömb már feltöltött kezdetéből, hogy a következő helyre mit kell tennünk, akkor ennek segítségével a tömböt akármeddig feltölthetjük.

A tétel és a bizonyítás érvényes marad akkor is, ha $\mathbb{N}$ helyett tetszőleges N jólrende-

- $40/-1$:

$<$

jelöljük.

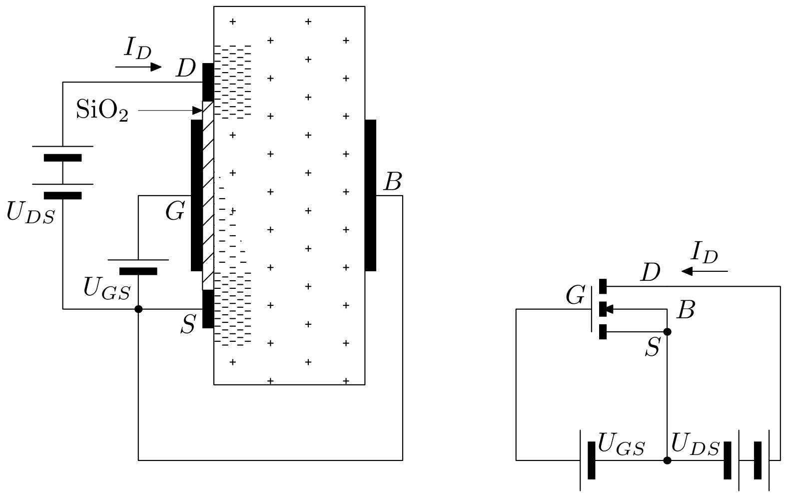
$>$

jelöljük.

Logikai függvények. *Logikai függvény* (vagy *Boole-függvény*) alatt az $\{\uparrow, \downarrow\}^n$ halmazt az $\{\uparrow, \downarrow\}^m$ halmazba leképező függvényt értünk, ahol $m, n \in \mathbb{N}$. A számítógép központi egysége, de a központi tár is lényegében logikai függvényeket megvalósító áramkörökből és (órajelvezérelt) tárolókból áll. A logikai jeleknek megfelelő logikai műveletek közül néhányat (hogy melyeket, az a használt technológiától függ, manapság például a ‚nem", angol rövidítése NOT, és az „összeférhetetlen vagy", angol rövidítése NAND) közvetlenül meg tudunk valósítani hardver alapelemként, a többi logikai függvényt ezek segítségével kell megvalósítani.

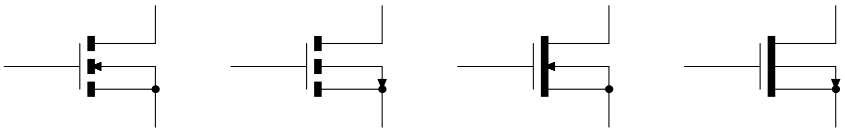
Tekintsünk $X_1, X_2, \ldots, X_n$ nullváltozós predikátumokat, amelyeknél az egyszerűség kedvéért nem írtuk ki a predikátum jele után az üres zárójelet. Minden, ezen predikátumokkal felírt formula, amely nem tartalmaz kvantort (ez itt most természetes feltevés, hiszen nincsenek változók), egy $\{\uparrow, \downarrow\}^n$-et $\{\uparrow, \downarrow\}$-ba képező logikai függvényt ad meg: minden $X_1, X_2, \ldots, X_n$ helyére az $\uparrow$ illetve $\downarrow$ jelek valamelyikét helyettesítve, majd a logikai jeleknek megfelelő logikai műveleteket elvégezve, $\uparrow$ vagy $\downarrow$ értéket kapunk. Például az $(X_1, X_2, X_3) \mapsto \neg(X_1 \wedge X_2) \vee X_3$ logikai függvény értéke $X_1 = X_2 = X_3 =\downarrow$ esetén $\uparrow$, míg $X_1 = X_2 =\uparrow$, $X_3 =\downarrow$ esetén $\downarrow$.

A következő tétel azt mutatja, hogy az $m = 1$ esetben minden logikai függvényt megkaphatunk így, már a $\neg$, $\wedge$ és $\vee$ felhasználásával is. Az $m > 1$ esetben a koordinátafüggvényeket állíthatjuk elő így. Természetesen a hardver tervezők egyrészt arra törekednek, hogy a szükséges logikai függvényeket minél kevesebb hardver logikai alapelem segítségével valósítsák meg, mert annál kisebb lesz az áramkör, másrészt, hogy minél kevesebb hardver logikai alapelem kapcsolódjon egymás után, mert annál kisebb lesz a késleltetés, így annál gyorsabb lesz az áramkör működése.



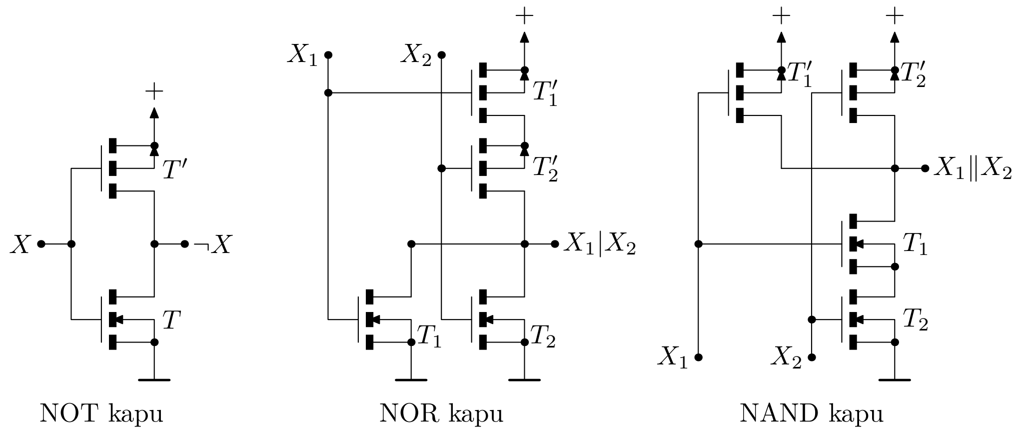
0.6. ábra: MOSFET működése és rajzjele.

A mai számítógépekben a *kapcsolóelem*ek rendszerint *térvezérlésű tranzisztor*ok, *FET*-ek (*field effect transistor*), amelyek számunkra elektromos térrel vezérelt kapcsolónak tekinthetők. A 2.1. ábrán egy ilyen eszköz szerkezetét és működését, valamint a kapcsolási rajzokon használt jelét mutatjuk be. Az elektródák jól vezető anyagból, rendszerint fémből készülnek (az ábrán fekete). A *p típusú* félvezető szilicium alaplemezben (amelyben tehát a vezetést a kristályrács elektronhiányos helyei, a pozitív töltésű „*lyuk*ak" biztosítják) diffúzióval az S *forrás* (*source*) és D *nyelő* (*drain*) elektródák alatt olyan szigeteket hoznak létre, amelyekben sok vezetésre képes elektron van. Az alaplemeztől szigetelő réteggel elválasztott G *kapu* (*gate*) elektródára pozitív U_{GS} feszültséget adva S-hez képest, az elektronok egy része beáramlik a szigetelő réteg alá, létrehozva az n típusú, elektronokat tartalmazó *csatornát*. Növelve a feszültséget, a csatorna végül elér a D elektróda alatti szigetig, és ekkor a D-re adott, S-hez képes pozitív U_{DS} feszültség hatására I_G áram indul meg, az eszköz vezet. Csökkentve az U_{GS} feszültséget, az eszköz lezár. (Az alaplemez kivezetését, a B bázis (base) elektródát mindig az S elektródához kötik.) Az eszközt *szigetelt kapu*s FET-nek, *IGFET*-nek (*insulated gate FET*), vagy — mivel legtöbbször a kapu fém, a szigetelő pedig sziliciumdioxid — *MOSFET*-nek (*MOS*: *metall-oxid-semiconductor*) nevezzük. A rajzon szereplő változat $U_{GS} = 0$ esetén zárva van, ezért *önzáró*nak vagy *növekményes*nek illetve *dúsításos*nak (*enhancement*) nevezzük. Készíthető olyan változat is, amelyben a gyártás során a szigetelő réteg alatt eleve létrehozunk egy n típusú csatornát, amely csak negatív U_{GS} feszültség hatására ürül ki, és zár le az eszköz, ezt *önvezető*nek vagy *kiürítéses*nek (*depletion*) nevezzük. Végül mindkét típus elkészíthető n típusú alaplemezen p típusú szigetekkel és csatornával is; ezt röviden *p csatornás MOSFET*-nek fogjuk nevezni (míg az előzőleg tárgyalt eszközt *n csatornás MOSFET*-nek); ennek működtetéséhez a telepfeszültségeket meg kell fordítani, és az áramirány is megfordul. A felsorolt típusok rajzjelét a 2.2. ábrán láthatjuk.



0.7. ábra: MOSFET típusok rajzjele.

A 2.3. ábra a legegyszerűbb, de gyakran használt *statikus CMOS* (*CMOS*: *complementer MOS*) kapuk kapcsolási rajzát mutatja. A bal oldali, komplementálást végző *nem kapu* (*NOT kapu*, *inverter*) működése a következő: Ha a bemenet alacsony feszültségen van, a T tranzisztor, amely n csatornás önzáró MOSFET, zárva van, a komplementer T' tranzisztor, amely p csatornás önzáró MOSFET, viszont kinyit, mert a kapuelektródája a pozitív tápfeszültséghez kötött S elektródához képest negatív feszültségen van. Így a kimenet össze van kötve a tápfeszültséggel, de nincs összekötve a földdel, tehát nagy feszültségű. Ha a bemenet nagy feszültségen van, a helyzet megfordul: T kinyit, T' lezár, és a kimenet alacsony feszültségű lesz.



0.8. ábra: Statikus CMOS kapuáramkörök.

Hasonlóan működik a középen látható *sem-sem kapu* (*not or*, *NOR*): ha valamelyik bemenet magas feszültségen van, akkor a neki megfelelő T tranzisztor kinyit, T' tranzisztor pedig lezár, így a kimenet alacsony feszültségű lesz, egyébként pedig magas feszültségű. A jobb oldalon álló *összeférhetetlen vagy* (*not and*, *NAND*) kapunál, ha mindkét bemenet magas feszültségen van, a T_1 és T_2 tranzisztorok kinyitnak, a T_1' és T_2' tranzisztorok pedig lezárnak, így a kimenet alacsony feszültségre kerül, minden más esetben pedig magas feszültségre. Mindkét kapufajta három bemenettel is készülhet (több bemenet növeli a szükséges tápfeszültséget).

Figyeljük meg, hogy mindhárom kapunál akármilyen bemenetnél a kimenet vagy a földdel, vagy a tápfeszültséggel van csak összekötve, így állandósult állapotban áram gyakorlatilag nem folyik, csak kapcsoláskor. Ez ennek az áramkörtípusnak a fő előnye: kis sebességnél igen keveset fogyaszt. Hátránya, hogy a kapcsolási idők nem elég kicsik. Nagy sebességű áramköröknél bonyolultabb kapcsolásokat használnak.

Logikai függvények diszjunktív normál alakja. *Az előző pont jelöléseivel, minden $f : \{\uparrow, \downarrow\}^n \to \{\uparrow, \downarrow\}$ logikai függvény felírható*

$$f(X_1, X_2, \ldots, X_n) = \mathcal{A}_1 \vee \mathcal{A}_2 \vee \ldots \vee \mathcal{A}_m$$

alakban, ahol $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$ különböző logikai formulák, de mindegyik

$$\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \ldots \wedge \mathcal{B}_{n_k}$$

alakú, ahol $\mathcal{B}_j$ vagy X_{i_j}, vagy $\neg X_{i_j}$ és $1 \leq i_1 < i_2 < \ldots < i_{n_k} \leq n$.

Emlékeztetünk rá, hogy $\wedge$ illetve $\vee$ asszociatív logikai műveletek a $\{\uparrow, \downarrow\}$ halmazon, így ha nulla tényezőre hajtjuk végre őket, akkor az eredmény az egységelemük, $\uparrow$ illetve $\downarrow$ lesz.

Bizonyítás. Direkt módon konstruáljuk meg a normálalakot: ha valamilyen

$$(x_1, x_2, \dots, x_n) \in \{\uparrow, \downarrow\}^n$$

sorozatra f igaz értéket vesz fel, akkor képezzünk egy $\mathcal{A}$ tagot, amelyben $\mathcal{B}_j = X_j$, ha a sorozatban x_j igaz, és $\mathcal{B}_j = \neg X_j$, ha a sorozatban x_j hamis. Az összes így adódó (legfeljebb 2^n) tagot kapcsoljuk össze diszjunkcióval. $\square$

Normálalakok. Az előző tétel bizonyításában adódó *normálalak*ot *teljes diszjunktív normál alak*nak nevezzük, mert benne $n_k = n$ minden k-ra. Egyes $\mathcal{A}$ logikai részformulák összevonásával, vagy bármilyen más módon kapható, a tétel állításában szereplő alakot *diszjunktív normál alak*nak nevezünk. (Részletesebben lásd Knuth [43], Vol. 4., Fas. 0.) Ha az $(x_{,}x_2, \dots, x_n) \mapsto \neg f(x_1, x_2, \dots, x_n)$ logikai függvény állítjuk elő diszjunktív normál alakban, majd mindkét oldalt negáljuk, akkor az f logikai függvény

$$f(X_1, X_2, \dots, X_n) = \mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \dots \wedge \mathcal{A}_m$$

alakban való felírását kapjuk, ahol $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m$ különböző logikai formulák, de mindegyik

$$\mathcal{B}_1 \vee \mathcal{B}_2 \vee \dots \vee \mathcal{B}_{n_k}$$

alakú, ahol $\mathcal{B}_j$ vagy X_{i_j}, vagy $\neg X_{i_j}$ és $1 \le i_1 < i_2 < \dots < i_{n_k} \le n$. Ezt az alakot *konjuktív normál alak*nak nevezzük, ha pedig $n_k = n$ minden k-ra, akkor *teljes konjuktív normál alak*nak.

Megjegyezzük, hogy készülnek olyan integrált áramkörök, úgynevezett *programozható logikai sík*ok (angolul *programmable logical array*, *PLA*), amelyek programozhatók bármely logikai függvény megvalósítására, ha annak koordinátafüggvényei normálalakban adottak.

• 41/−1 :

$<$

lunk.

$>$

lunk.

Természetes számok számítógépes ábrázolása. A mai számítógépek mindegyike alapvetően *kettes számrendszer*ben dolgozik: a *bináris jegy*, a *binary digit* angol kifejezésből *bit* 0 vagy 1 lehet. A természetes számokat (*előjel nélküli*, angolul *unsigned* számokat) a számítógép kettes számrendszerben ábrázolja. Történeti érdekesség, hogy készítettek *hármas számrendszer*ben működő *ternáris* gépet is. (Természetesen, ha rögzített hosszúságú, például 8, 16, 32 vagy 64 bites számábrázolást használunk, az eredmény *túlcsordul*hat, és csak az alacsonyabb helyiértékű bitjeit kapjuk meg.) Számunkra jóval kényelmesebb a biteket kettessével, hármassával vagy négyessével csoportosítva *négyes* (*kvadrális*), *nyolcas* (*oktális*) vagy *tizenhatos* (*hexadecimális*) számrendszert használni. A byteszervezésű gépek (IBM 360-as sorozat) elterjedése óta a memória legkisebb címezhető egysége rendszerint 8 bit, azaz 1 *bájt* (az angol *byte* elnevezést az IBM Stretch gép tervezői vezették be 1956-ban). Mivel egy fél bájt (angolul *nybble*) egy hexadecimális jegynek felel meg, leggyakrabban hexadecimális számrendszert használunk. Néhány üzleti alkalmazás tizes számrendszert kíván: ekkor a számjegyeket ASCII-kódjukkal ábrázoljuk, vagy *binárisan kódolt decimális* (angolul *binary coded decimal*, *BCD*) kódot használunk, melyben a tizes számrendszerbeli egy-egy jegy egy-egy félbájtot foglal el, binárisan kódolva.

$\circ$* **Hash-transzformáció.** A számrendszerek és a maradékos osztás felhasználható úgynevezett *hash-transzformáció*ra vagy *kulcs-cím transzformáció*ra: egy R rekord K kulcsát — például 256 alapú számrendszerben — számnak tekintjük, és egy adott M számmal (amelyet érdemes olyan prímnek választani, amely egyetlen kettőhatványhoz sem esik nagyon közel) maradékosan osztjuk. A kapott $0 \leq h(K) < M$ érték megmondja, hogy egy tömbben hol van az R rekord címe. Persze, több R_i rekord K_i kulcsára lehet $h(K_i)$ ugyanaz: ezeket a rekordokat egy listában helyezzük el. Ha a keresés jóval gyakoribb, mint új rekordok bejegyzése, a listákat tarthatjuk rendezetten is. Belső tárban a listák ne legyenek túl hosszúak: ha hosszuk jóval 1 fölé megy, érdemes új, nagyobb M-et választani, és az összes rekordot „újrahashelni”. Például ha semmit nem tudunk az elhelyezendő rekordok számáról, kezdhetünk $M = 5$-tel, és ha növelni kell M-et, az előző M kétszerese utáni első prímet választjuk a következő M-nek. A módszer mágneslemezen is használható, itt $h(K)$ egy szektor relatív címét adja, amelyben a rekord van. Ha egy újabb rekord esetleg már nem fér az adott szektorba, rakhatjuk egyszerűen a következő szektorba is.

• $43/1 \ldots -1$:
$<$

Tétel. *Tekintsük* $\mathbb{N} \times \mathbb{N}$*-en az* $(m, n) \sim (m', n')$*, ha* $m + n' = m' + n$ *relációt, az* $(m, n) + (m', n') = (m + m', n + n')$ *összeadást és az* $(m, n) \cdot (m', n') = (m \cdot m' + n \cdot n', m \cdot n' + m' \cdot n)$ *szorzást, valamint az* $(m, n) \leq (m', n')$*, ha* $m + n' \leq m' + n$ *relációt. A* $\sim$ *reláció ekvivalenciareláció. Az ekvivalenciosztályok halmazát* $\mathbb{Z}$*-vel fogjuk jelölni, és elemeit* egész számok*nak nevezzük. Az összeadás, a szorzás és a* $\leq$ *reláció kompatibilis az ekvivalenciával, így az egész számok között értelmezve van az összeadás, a szorzás és a* $\leq$ *reláció, amely rendezés, továbbá*

(1) $\mathbb{Z}$ *az összeadásra nézve Abel-csoport;*

(2) $\mathbb{Z}$ *a szorzással kommutatív egységelemes félcsoport;*

(3) *ha* $x, y \in \mathbb{Z}$ *és egyik sem nulla, akkor szorzatuk sem nulla;*

(4) *ha* $x, y, z \in \mathbb{Z}$*, akkor* $x \cdot (y + z) = x \cdot y + x \cdot z$ *(disztributivitás);*

(5) *ha* $x, y, z \in \mathbb{Z}$ *és* $x \leq y$*, akkor* $x + z \leq y + z$ *(az összeadás monoton);*

(6) *ha* $x, y \in \mathbb{Z}$ *és* $x, y \geq 0$*, akkor* $x \cdot y \geq 0$ *(a szorzás monoton).*

Bizonyítás. A $\sim$ reláció nyilván ekvivalenciareláció (az összeadás kommutativitását és asszociativitását és a természetes számok összeadásának egyszerűsítési szabályát használjuk fel a bizonyításhoz).

Megmutatjuk, hogy a párok összeadása kompatibilis az ekvivalenciarelációval. Mivel a párok összeadása kommutatív, elég azt megmutatni, hogy ha $(m, n) \sim (m', n')$, akkor

$(m,n)+(m'',n'') \sim (m',n')+(m'',n'')$. Az, hogy $(m,n) \sim (m',n')$, azt jelenti, hogy $m+n' = m'+n$. Ebből $m+m''+n'+n'' = n+n''+m'+m''$, ami viszont azt jelenti, hogy

$$(m,n)+(m'',n'') = (m+m'',n+n'') \sim (m'+m'',n'+n'') = (m',n')+(m'',n'').$$

Mivel a párok összeadása kommutatív és asszociatív, az ekvivalenciosztályoké is. A $(0,0)$ pár osztálya nullelem, ezt jelöljük nullával. Az (m,n) pár osztályának additív inverze az (n,m) pár osztálya. Így $\mathbb{Z}$ az összeadással Abel-csoport. $\square$

Megmutatjuk, hogy a párok szorzása is kompatibilis az ekvivalenciarelációval. Mivel a párok szorzása kommutatív, elég azt megmutatni, hogy ha $(m,n) \sim (m',n')$, akkor $(m,n)\cdot(m'',n'') \sim (m',n')\cdot(m'',n'')$. Az, hogy $(m,n) \sim (m',n')$, azt jelenti, hogy $m+n' = m'+n$. Mindkét oldalt szorozva m''-vel azt kapjuk, hogy $m\cdot m''+n'\cdot m'' = m'\cdot m''+n\cdot m''$. Ha előbb a két oldalt felcseréljük, majd mindkét oldalt szorozzuk n''-vel, azt kapjuk, hogy $m'\cdot n''+n\cdot n'' = m\cdot n''+n'\cdot n''$. Összeadva ezt a két egyenlőséget, azt kapjuk, hogy $m\cdot m''+n\cdot n''+m'\cdot n''+m''\cdot n' = m\cdot n''+m''\cdot n+m'\cdot m''+n'\cdot n''$. Ez azt jelenti, hogy

$$\begin{aligned}(m,n)\cdot(m'',n'') &= (m\cdot m''+n\cdot n'', m\cdot n''+m''\cdot n)\\ &\sim (m'\cdot m''+n'\cdot n'', m'\cdot n''+m''\cdot n') = (m',n')\cdot(m'',n'').\end{aligned}$$

Mivel a párok szorzása kommutatív, az osztályoké is. Egyszerű számolás mutatja, hogy a párok szorzása asszociatív, így az osztályoké is. Az $(1,0)$ pár egységelem a párok multiplikatív félcsoportjában, így az osztálya egységelem $\mathbb{Z}$-ben. A párok szorzása disztributív, amiből adódik, hogy az osztályoké is.

$>$

Tétel. *Tekintsük $\mathbb{N}\times\mathbb{N}$-en az $(m,n) \sim (m',n')$, ha $m+n' = m'+n$ relációt és az $(m,n)+(m',n') = (m+m',n+n')$ összeadást. A $\sim$ reláció ekvivalenciareláció. Az ekvivalenciosztályok halmazát $\mathbb{Z}$-vel fogjuk jelölni, és elemeit* egész számok*nak nevezzük. Az összeadás kompatibilis az ekvivalenciával, így az egész számok között értelmezve van az összeadás és $\mathbb{Z}$ az összeadásra nézve Abel-csoport.*

Bizonyítás. A $\sim$ reláció nyilván ekvivalenciareláció (az összeadás kommutativitását, asszociativitását és a természetes számok összeadásának egyszerűsítési szabályát használjuk fel a bizonyításhoz).

Megmutatjuk, hogy a párok összeadása kompatibilis az ekvivalenciarelációval. Mivel a párok összeadása kommutatív, elég azt megmutatni, hogy ha $(m,n) \sim (m',n')$, akkor $(m,n)+(m'',n'') \sim (m',n')+(m'',n'')$. Az, hogy $(m,n) \sim (m',n')$, azt jelenti, hogy $m+n' = m'+n$. Ebből $m+m''+n'+n'' = n+n''+m'+m''$, ami viszont azt jelenti, hogy

$$(m,n)+(m'',n'') = (m+m'',n+n'') \sim (m'+m'',n'+n'') = (m',n')+(m'',n'').$$

Mivel a párok összeadása kommutatív és asszociatív, az ekvivalenciosztályoké is. A $(0,0)$ pár osztálya nullelem, ezt jelöljük nullával. Az (m,n) pár osztályának additív inverze az (n,m) pár osztálya. Így $\mathbb{Z}$ az összeadással Abel-csoport.

- $44/1\ldots 20$:

<

Következő lépésként megmutatjuk, hogy ha $(m,n)\le(m'',n'')$ és $(m,n)\sim(m',n')$, akkor $(m',n')\le(m'',n'')$. Valóban, az $m+n''\le m''+n$ egyenlőtlenséghez „hozzáadva" az $m'+n=m+n'$ egyenlőséget, majd $m+n$-nel egyszerűsítve, kapjuk, hogy $m'+n''\le m''+n'$. Hasonlóan kapjuk, hogy ha $(m,n)\le(m'',n'')$ és $(m',n')\sim(m'',n'')$, akkor $(m,n)\le(m',n')$. Ezzel beláttuk, hogy a $\le$ reláció kompatibilis az osztályozással. A definíció alapján nem nehéz belátni, hogy $\le$ rendezés az osztályokon.

(5) egyszerű számolással adódik. (6) bizonyításához vegyük észre, hogy $(0,0)\le(m,n)$ pontosan akkor teljesül, ha $m\ge n$. Felírva m-et $n+k$ alakban valamely $k\in\mathbb{N}$-re, azt kapjuk, hogy $(m,n)\sim(k,0)$. Ezt alkalmazva (m',n')-re is, kapjuk (6)-ot. Végül (3) bizonyításához azt kell észrevennünk, hogy ha $(m,n)\not\sim(0,0)$, akkor vagy egy $(k,0)$, vagy egy $(0,k)$ alakú párral ekvivalens valamely $k\in\mathbb{N}^+$-ra. Ezt alkalmazva (m',n')-re is, négy eset van, amit meg kell vizsgálnunk, és kapjuk (3)-at. $\square$

Tétel: $\mathbb{N}$ beágyazása $\mathbb{Z}$-be. *Az előző tétel jelöléseivel, a $\varphi : n\mapsto\widetilde{(n,0)}$ leképezése $\mathbb{N}$-nek $\mathbb{Z}$-be kölcsönösen egyértelmű, összeadás- és szorzástartó, monoton növekedő, valamint $\varphi(n)=n\varphi(1)$ minden $n\in\mathbb{N}$-re. Így $\varphi(\mathbb{N})$-et azonosíthatjuk $\mathbb{N}$-el. Ezzel az azonosítással $\mathbb{N}\cup(-\mathbb{N})=\mathbb{Z}$ és $\mathbb{N}\cap(-\mathbb{N})=\{0\}$.*

Bizonyítás. Teljes indukcióval adódik, hogy $\varphi(n)=n\varphi(1)$ minden $n\in\mathbb{N}$-re. Az állítás többi része az előző tétel bizonyításában tett észrevételek segítségével könnyen belátható. $\square$

Hatványozás egész kitevővel. Ha G egy egységelemes félcsoport, $g\in G$, akkor az $n\mapsto g^n$ leképezést

>

Tétel: $\mathbb{N}$ beágyazása $\mathbb{Z}$-be. *Az előző tétel jelöléseivel, a $\varphi : n\mapsto\widetilde{(n,0)}$ leképezése $\mathbb{N}$-nek $\mathbb{Z}$-be kölcsönösen egyértelmű, összeadástartó, valamint $\varphi(n)=n\varphi(1)$ minden $n\in\mathbb{N}$-re. Így $\varphi(\mathbb{N})$-et azonosíthatjuk $\mathbb{N}$-el. Ezzel az azonosítással $\mathbb{N}\cup(-\mathbb{N})=\mathbb{Z}$ és $\mathbb{N}\cap(-\mathbb{N})=\{0\}$.*

Bizonyítás. Mivel megállapodás szerint, ha semmit sem adunk össze, az összeg a nullelem, $0\varphi(1)=\widetilde{(0,0)}=\varphi(0)$. Ugyancsak az összeg definíciója szerint $1\varphi(1)=\widetilde{(1,0)}=\varphi(1)$. Teljes indukcióval

$$\varphi(n^+)=n\varphi(1)+\varphi(1)=\widetilde{(n,0)}+\widetilde{(1,0)}=\widetilde{(n+1,0)}=\varphi(n^+)$$

minden $n\in\mathbb{N}$-re. Az állítás többi része adódik, ha belátjuk, hogy $\mathbb{Z}$ minden eleme, azaz minden ekvivalenciaosztály pontosan egyet tartalmaz a $(k,0)$ illetve $(0,k)$ alakú elemek közül, ahol $k\in\mathbb{N}$. Legyen $m,n\in\mathbb{N}$. Ha $n\ge m$, akkor van olyan $k\in\mathbb{N}$, amelyre $n=m+k$; ekkor $(m,n)\sim(k,0)$. Hasonlóan, ha $n\le m$, akkor van olyan $k\in\mathbb{N}$, hogy $n+k=m$; ekkor $(m,n)\sim(0,k)$. Másrészt, ha $(k,0)\sim(k',0)$, akkor $k=k'$; ha $(0,k)\sim(0,k')$, akkor is $k=k'$; végül ha $(k,0)\sim(0,k')$, akkor $k=k'=0$. $\square$

Az egész számok rendezése. Ha $m, n \in \mathbb{Z}$, akkor legyen $m \leq n$, ha van olyan $k \in \mathbb{N}$, amelyre $m + k = n$. Ez persze ugyanazt jelenti, mint hogy $n - m \in \mathbb{N}$. Ugyanúgy, mint a természetes számoknál, adódik, hogy így egy részbenrendezést kapunk. Az egész számok körében $-\mathbb{N}$ elemeit az jellemzi, hogy kisebb vagy egyenlőek, mint nulla: ha $n \in \mathbb{N}$, akkor $(-n) + n = 0$, így $-n \leq 0$, és ha $m \leq 0$, akkor valamely $n \in \mathbb{N}$-re $m + n = 0$, azaz $m = -n$. Innen következik, hogy $-\mathbb{N}$ bármely eleme kisebb vagy egyenlő, mint $\mathbb{N}$ bármely eleme. Mivel $m \leq n$ esetén $n - m \in \mathbb{N}$, azt kapjuk, hogy $(-n) + (n - m) = -m$, azaz $-\mathbb{N}$ elemei is összehasolíthatóak. Ezzel beláttuk, hogy $\mathbb{Z}$ rendezett. Megmutatjuk, hogy ha $k, m, n \in \mathbb{Z}$ és $m \leq n$, akkor $m + k \leq n + k$; valóban, $(n + k) - (m + k) = n - m \in \mathbb{N}$. Ezt a tulajdonságot úgy hívjuk, hogy az *összeadás monoton*.

Az egész számok szorzása. Ha $m, n \in \mathbb{Z}$, akkor az $m, n \in \mathbb{N}$ esetben legyen mn a természetes számokra definiált szorzat, ha $m, -n \in \mathbb{N}$, akkor legyen $mn = nm = -m(-n)$, és ha $-m, -n \in \mathbb{N}$, akkor legyen $mn = (-m)(-n)$. Esetszétválasztással azonnal adódik, hogy a szorzat pontosan akkor lesz nulla, ha valamelyik tényezője nulla, ezzel a szorzással $\mathbb{Z}$ kommutatív félcsoport az 1 egységelemmel, valamint ha $k, m, n \in \mathbb{Z}$, akkor $k \cdot (m + n) = k \cdot m + k \cdot n$, azaz a szorzás *disztributív* az összeadásra nézve. (Rövidesen belátjuk az úgynevezett előjelszabályt, amelyből következik, hogy a szorzást nem is definiálhattuk volna másként, ha azt akarjuk, hogy disztributív legyen az összeadásra nézve.)

Hatványozás egész kitevővel. Ha G egységelemes félcsoport, $g \in G$-nek van inverze, akkor az $n \mapsto g^n$ leképezést

- $44/22$:

$<$

és $(g^m)^n = g^{mn}$ minden $m, n \in \mathbb{Z}$-re, továbbá ha $g, h \in G$ felcserélhető elemek, akkor

$>$

és $(g^m)^n = g^{mn}$ minden $m, n \in \mathbb{Z}$-re, továbbá ha $g, h \in G$ felcserélhető elemek amelyeknek van inverze, akkor

- $48/-16$:

$<$

párok, így az osztályok szorzása asszociatív. Ezzel beláttuk, hogy $\mathbb{Q}$ kommutatív gyűrű.

$>$

párok, így az osztályok szorzása disztributív. Ezzel beláttuk, hogy $\mathbb{Q}$ kommutatív gyűrű.

- $49/-17 \ldots -16$:

$<$

egységelemmel. Ekkor egyértelműen létezik egy kölcsönösen egyértelmű és összeadástartó $\varphi : \mathbb{Q} \to F$ leképezés. Ez a leképezés monoton növekedő és szorzástartó is, és $\varphi(m/n) =$

$>$

egységelemmel. Ekkor egyértelműen létezik egy kölcsönösen egyértelmű, összeadás- és szorzástartó $\varphi : \mathbb{Q} \to F$ leképezés. Ez a leképezés monoton növekedő is, és $\varphi(m/n) =$

- $52/-11$:

  $<$

Nyilván, ha $y > 0$, akkor $0 \le x \bmod y < y$, ha pedig $y < 0$, akkor $y < x \bmod y \le 0$.

  $>$

Nyilván, ha $y > 0$, akkor $0 \le x \bmod y < y$, ha pedig $y < 0$, akkor $y < x \bmod y \le 0$. Az $x \bmod 1 = x - \lfloor x \rfloor$ értéket x *törtrész*ének nevezzük.

Bővített valós számok. Néha szükségünk lesz a *bővített valós szám*ok $\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$ halmazára. A valós számok rendezését úgy terjesztjük ki $\overline{\mathbb{R}}$-ra, hogy $-\infty < x < +\infty$ teljesüljön minden $x \in \mathbb{R}$-re. A bővített valós számok körében bármely részhalmaznak van szuprémuma és infimuma (de $\sup \emptyset = -\infty$ és $\inf \emptyset = +\infty$). Az ellentettképzésnél $-(+\infty) = -\infty$ és $-(-\infty) = +\infty$. Az összeadást is értelmezzük, ha nem is mindenütt: $x + (+\infty) = (+\infty) + x = +\infty$, ha $x \in \overline{\mathbb{R}}$, $x > -\infty$ és $x + (-\infty) = (-\infty) + x = -\infty$, ha $x \in \overline{\mathbb{R}}$, $x < +\infty$, de $(+\infty) + (-\infty)$ és $(-\infty) + (+\infty)$ nincs értelmezve.

Valós számok kerekítése és fixpontos ábrázolása számítógépben. Valós számok pontosan nem ábrázolhatók számítógépben, de közelítőlek igen. Egyik mód erre a *fixpontos ábrázolás*. Kettes számrendszert használva, rögzítünk egy N egész számot, a törtrész hosszát. Az $n/2^N$, $n \in \mathbb{Z}$ alakú valós számok pontosan ábrázolhatók, ha n-et tároljuk. Egy tetszőleges x valós szám helyett a hozzá legközelebb eső pontosan ábrázolható számot tároljuk; ha két ilyen van, akkor azt, amelyben n páros (ez kiküszöböli, hogy ebben az esetben mindig egyirányban történjen a kerekítés); ez a *szabályos kerekítés*. Más *kerekítés* mellett is dönthetünk: $-\infty$ felé való kerekítés esetén az x-nél nem nagyobb pontosan ábrázolható számok közül választjuk ki az x-hez legközelebbit; ha $+\infty$ felé kerekítünk, akkor az x-nél nem kisebb pontosan ábrázolható számok közül választjuk ki az x-hez legközelebbit (ezek a kerekítési módon az intervallumaritmetikánál fontosak); végül *csonkítás* esetén az $|x|$-nél kisebb abszolút értékű pontosan ábrázolható számok közül választjuk ki az x-hez legközelebbit. Az ábrázolásnál *kerekítési hiba* lép fel. Műveletek után is ezeket a *kerekítési szabály*okat alkalmazhatjuk a (pontos) eredményre, és természetesen általában a műveleteknél is kerekítési hiba lép fel. Ha n bitjeinek száma korlátozott, akkor csak egy intervallum elemei ábrázolhatók aránylag kis (szabályos kerekítésnél 2^{-N-1}, a többi kerekítésnél 2^{-N}) hibával, ezen kívüli számoknál *túlcsordulás* lép fel.

Valós számok lebegőpontos ábrázolása számítógépben. Fixpontos számábrázoláskor a hiba a szám abszolút értékéhez képes nagy lehet, ha a szám abszolút értéke kicsi. A *lebegőpontos számábrázolás* ezt küszüböli ki, a hiba és a szám értéke hányadosának abszolút értéke, a *relatív hiba* nagyon sok nagyságrenden keresztül kicsi marad. Csak bináris ábrázolással, azon belül is csak az *IEEE 754* szabvány által leírt, ma szinte kizárólagosan használt ábrázolással foglalkozunk. Ennél a pontosan ábrázolható számok $n \cdot 2^{k-N}$ alakúak, ahol $n, k \in \mathbb{Z}$ és $1 - 2^K < k < 2^K$, $-2^{N+1} < n < 2^{N+1}$; a K és N

konstansoknak a szabvány által megengedett értékeit az alábbi táblázat tartalmazza.

pontosság	bájtok száma	$K+1$	N
egyszeres	4	8	23
kétszeres	8	11	52
kiterjesztett kétszeres	≥ 10	≥ 15	≥ 63
négyszeres	16	15	112

Az egyszeres pontosság használatos például képfeldolgozásnál. A kétszeres pontosság az általános a legtöbb más esetben. A négyszeres pontosság tulajdonképpen nem szerepel a szabványban, de egyre terjed. A kisebb pontosságról nagyobbra való konverzió csak nullákkal való kiegészítéssel jár, míg fordított irányban kerekítés történik.

Az $n \cdot 2^{k-N}$ alakban való felírás általában nem egyértelmű, mert ha n páros, akkor $(n/2) \cdot 2^{k+1-N}$ ugyanannak a számnak egy másik felírása. Úgy tesszük egyértelművé, hogy k-t a lehető legkisebbnek választjuk. Ha ekkor $|n| \geq 2^N$, akkor $n \cdot 2^{k-N} = \pm 2^k \cdot (1+f)$, ahol $f = (|n| - 2^N)/2^N < 1$ a szám *törtrésze*; ha $|n| < 2^N$, akkor csak $k = 2 - 2^K$ lehet, ekkor $n \cdot 2^{k-N} = \pm 2^k \cdot (0+f)$, ahol $f = |n|/2^N < 1$ a szám *törtrésze*; ez utóbbi esetben ha $n \neq 0$, akkor a szám *szubnormális lebegőpontos szám*, minden más esetben *normális lebegőpontos szám*. A pontosan ábrázolható lebegőpontos számok esetén az ábrázolás a következő: a legfelső bit az előjelbit (0 pozitív, 1 negatív), ezután jön a $K+1$ bites exponens, ami $|n| \geq 2^N$ esetén $k + 2^K - 1$, azaz k értéke $2^K - 1$-többletes kódban, egyébként pedig 0, ezután pedig a törtrész N biten. Két nulla is van, ± 0, de a hardver (általában) egyenlőnek tekinti őket. A speciális $2^{K+1} - 1$ exponens érték 0 törtrésszel $\pm\infty$ ábrázolására szolgál (ha az exponens túl nagy lenne, akkor is ez az ábrázolás); ha a törtrész nem nulla akkor a tartalom nem szám (*NaN*, Not any Number), mégpedig ha a törtrész legfelső bitje 0, akkor jelző nem szám (*SNaN*, Signaling Not any Number), ami megszakítást is okoz. A további részleteket lásd a [38] cikkben. Az egyes eseteket az alábbi táblázat foglalja össze.

szám típus	előjel bit	exponens	implicit bit	törtrész
$\pm\infty$	$\pm$	$111\ldots111_2$	1	$000\ldots000_2$
NaN	?	$111\ldots111_2$	1	$1??\ldots???_2$
SNaN	?	$111\ldots111_2$	1	$0??\ldots???_2$
normális	$\pm$	$k + 2^K - 1$	1	$\|n\| - 2^N$
szubnormális	$\pm$	0	0	$\|n\|$
nulla	$\pm$	0	0	0

- $54/-1$:

$<$

felépítésnek a részletes tárgyalását lásd a Hewitt–Stromberg [36] könyvben.

$>$

felépítésnek a részletes tárgyalását lásd a Hewitt–Stromberg [36] könyvben.

Tétel: gyökvonás. *Minden $x \geq 0$ valós számhoz és $n \in \mathbb{N}^+$ természetes számhoz pontosan egy olyan $y \geq 0$ valós szám található, amelyre $y^n = x$.*

Az y számot az x szám n-edik *gyökének* nevezzük és $\sqrt[n]{x}$-el ($n = 2$ esetén $\sqrt{x}$-el is) vagy $x^{1/n}$-el jelöljük.

Bizonyítás. Világos, hogy legfeljebb egy ilyen y létezik, hiszen $y_1 < y_2$ esetén $y_1^n < y_2^n$. Ha $x = 0$, akkor $y = 0$. Legyen E azoknak a t pozitív valós számoknak a halmaza, amelyekre $t^n < x$. Ha $t = x/(1+x)$, akkor $0 < t < 1$, így $t^n \leq t < x$, így E nem üres. Ha $t > 1 + x$, akkor $t^n \geq t > 1 + x$, így $1 + x$ az E felső korlátja. Legyen $y = \sup E$. Meg fogjuk mutatni, hogy $y^n = x$. A bizonyítás indirekt: megmutatjuk, hogy az $y^n < x$ és $y^n > x$ egyenlőtlenségek mindegyike ellentmondásra vezet.

A

$$b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \cdots + a^{n-1})$$

azonosság alapján $b^n - a^n \leq (b-a)nb^{n-1}$, ha $0 < a < b$.

Tegyük fel, hogy $y^n < x$. Válasszunk olyan h számot, amelyre $0 < h < 1$ és

$$h < \frac{x - y^n}{n(y+1)^{n-1}}.$$

Legyen $a = y$, $b = y + h$. Ekkor

$$(y+h)^n - y^n \leq hn(y+h)^{n-1} \leq hn(y+1)^{n-1} < x - y^n,$$

így $(y+h)^n < x$, és ezért $y + h \in E$. Ez ellentmond y felső határ voltának.

Tegyük fel, hogy $y^n > x$. Legyen

$$k = \frac{y^n - x}{ny^{n-1}}.$$

Ekkor $0 < k < y$. Ha $t \geq y - k$, akkor

$$y^n - t^n \leq y^n - (y-k)^n \leq kny^{n-1} = y^n = x,$$

így $t^n \geq x$, és $t \notin E$. Így $y - k$ az E egy felső korlátja. Ez ellentmond y felső határ voltának. $\square$

Következmény. *Ha a és b nemnegatív valós számok és $n \in \mathbb{N}^+$, akkor $\sqrt[n]{ab} = \sqrt[n]{a}\,\sqrt[n]{b}$.*

Bizonyítás. Legyen $\alpha = \sqrt[n]{a}$ és $\beta = \sqrt[n]{b}$. Ekkor $(\alpha\beta)^n = ab$, így az egyértelműségből következik az állítás. $\square$

* **A természetes, az egész és a racionális számok bevezetése a valós számok segítségével.** Az $x^+ := x + 1$, ha $x \in \mathbb{R}$ jelöléssel, jelölje $\mathbb{N}$ az $\mathbb{R}$ mindazon N részhalmainak a metszetét, amelyek rendelkeznek az alábbi két tulajdonsággal:

(1) $0 \in N$;

(2) ha $n \in N$, akkor $n^+ \in N$.

Az $\mathbb{N}$ halmaz elemeit *természetes szám*oknak nevezzük. (Vannak, akik a természetes számokat 1-el kezdik.)

Megmutatjuk, hogy $\mathbb{N}$ rendelkezik az alábbi tulajdonságokkal, amelyeket történeti okokból *Peano-axiómák*nak nevezzük:

(1) $0 \in \mathbb{N}$;

(2) ha $n \in \mathbb{N}$, akkor $n^+ \in \mathbb{N}$;

(3) ha $n \in \mathbb{N}$, akkor $n^+ \neq 0$;

(4) ha $n, m \in \mathbb{N}$ és $n^+ = m^+$, akkor $n = m$;

(5) ha $S \subset \mathbb{N}$, $0 \in S$ és ha $n \in S$ akkor $n^+ \in S$, akkor $S = \mathbb{N}$.

Mivel $\mathbb{N}$ olyan halmazok metszete, amelyek rendelkeznek az (1) és (2) tulajdonságokkal, $\mathbb{N}$ is rendelkezik ezekkel a tulajdonságokkal, így (P1) és (P2) teljesül. (P5) a *matematikai indukció elve* vagy röviden az *indukció elve* (a *teljes indukció elve* elnevezés is használatos, de mi ezt szűkebb értelemben fogjuk használni); abból következik, hogy az S halmaz rendelkezik az (1) és (2) tulajdonságokkal, így $\mathbb{N} \subset S$. (P4) következik az egyszerűsítési szabályból. Végül (P3) fennállását (P5) segítségével bizonyítjuk. (Az ilyen bizonyításokat *matematikai indukció*val vagy röviden *indukció*val való bizonyításoknak szokás nevezni, és nagyon gyakran szerepelnek természetes számokra vonatkozó állítások bizonyításánál.) Legyen $S = \{n \in \mathbb{N} : n^+ > 0\}$. Nyilván $0 \in S$, és ha $n \in S$, akkor $(n^+)^+ > 0 + 1 > 0$, így $n^+ \in S$. Innen (P5) miatt $S = \mathbb{N}$, azaz teljesül (P3).

Megjegyezzük, hogy ha $m, n \in \mathbb{N}$, akkor (n szerinti indukcióval) $m + n \in \mathbb{N}$. Hasonlóan, mivel $mn^+ = mn + m$, az n szerinti indukcióval kapjuk, hogy $mn \in \mathbb{N}$, ha $m, n \in \mathbb{N}$. Ugyancsak n szerinti indukcióval, ha $m, n \in \mathbb{N}$ és $m \leq n$, akkor $n - m \in \mathbb{N}$.

A természetes számok körében az összeadásra nézve csak a 0-nak van inverze, másként szólva, a kivonás általában nem végezhető el. Ez indokolta az egész számok bevezetését. A $\mathbb{Z} = -\mathbb{N} \cup \mathbb{N} \subset \mathbb{R}$ halmaz elemeit oknak nevezzük. A definíció alapján adódik, hogy $\mathbb{Z}$-ből nem vezet ki az összeadás és az additív inverz képzése, az előjelszabály alapján pedig, hogy a szorzás sem.

Az egész számok körében a nem nulla elemek közül csak 1-nek és -1-nek van multiplikatív inverze, másként szólva, az osztás általában nem végezhető el. Ez indokolta a racionális számok bevezetését. A $\mathbb{Q} = \{m/n \in \mathbb{R} : m, n \in \mathbb{Z}, n \neq 0\}$ halmaz elemeit *racionális szám*oknak nevezzük; $\mathbb{R} \setminus \mathbb{Q}$ elemeit *irracionális szám*oknak szokás nevezni. A racionális számok rendezett testet alkotnak: $0 = 0/1 \in \mathbb{Q}$, $1 = 1/1 \in \mathbb{Q}$, ha $m/n \in \mathbb{Q}$ és $m'/n' \in \mathbb{Q}$, akkor $(-m)/n = -m/n \in \mathbb{Q}$, $m/n + m'/n' = (mn' + m'n)/(nn') \in \mathbb{Q}$ és $(m/n)(m'/n') = (mm')/(nn') \in \mathbb{Q}$, valamint ha $0 \neq m/n$, akkor $m \neq 0$, így $1/(m/n) = n/m \in \mathbb{Q}$.

- 60/5 :

<

Könnyen ellenőrizhető, hogy $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$. Ezek

>

Könnyen ellenőrizhető, hogy $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$. A számolási szabályok legegyszerűbben a 3.3. ábra alapján jegyezhetők meg: a nyilak mentén haladva ciklikusan körbe, a két kvaternió szorzata a harmadik, míg ellenkező irányba haladva az ellentettje. Ezek

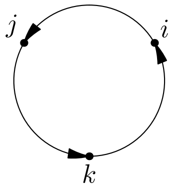
- 60/8 :

$<$

számok felcserélhetők i, j, k-val, számolni velük.

$>$

számok felcserélhetők i, j, k-val, számolni velük.



0.9. ábra: kvaterniók szorzása.

- 60/17 ... 27 :

$<$

Kvaterniók és a háromdimenziós euklideszi tér. A kvaterniók $\mathbb{R}^4$ pontjainak is tekinthetők. A kvaterniók összeadása megfelel a vektorok szokásos összeadásának. A tisztán képzetes kvaterniók $\mathbb{R}^3$ pontjaival azonosíthatók. A $p = xi + yj + zk$ és $p' = x'i + y'j + z'k$ tisztán képzetes kvaterniók szorzatának valós része $-\langle p, p' \rangle$, ahol $\langle p, p' \rangle = xx' + yy' + zz'$, képzetes része pedig $p \times p' = (yz' - zy')i + (zx' - xz')j + (xy' - x'y)k$. A $(p, p') \mapsto \langle p, p' \rangle$ leképezést *belső szorzás*nak nevezzük (nem művelet!). A $(p, p') \mapsto p \times p'$ leképezés nem kommutatív művelet, amely mindkét oldalról disztributív az összeadásra nézve, és *vektori szorzás*nak vagy *külső szorzás*nak szokás nevezni. Végül, ha p'' is egy tisztán képzetes kvaternió, akkor a $(p, p', p'') \mapsto \langle p, p' \times p'' \rangle$ leképezést *vegyes szorzás*nak szokás nevezni. A kvaterniókat a háromdimenziós mozgásokkal való szoros kapcsolatuk miatt felhasználják robotok vezérlésénél.

$>$

* **Vektoriális szorzás.** A kvaternószorzás eltérését a kommutativitástól a $p \times q = \frac{1}{2}(pq - qp)$ mennyiséggel mérhetjük. Ez egy új szorzás a kvaterniók között, amelyet *vektoriális szorzás*nak nevezünk, mert a könnyen ellenőrizhető $\Re(pq) = \Re(qp)$ egyenlőség miatt a valós része mindig nulla. A vektoriális szorzás mindkét oldalról disztributív az összeadásra nézve és valós szám bármelyik tényezőjéből kiemelhető. Nyilván $p \times p = 0$ bármely $p \in \mathbb{H}$-ra, ahonnan

$$\begin{aligned} 0 &= (p + q) \times (p + q) = p \times p + p \times q + q \times p + q \times q \\ &= p \times q + q \times p, \end{aligned}$$

tehát tetszőleges $p, q \in \mathbb{H}$-ra $p \times q = -q \times p$, azaz a vektoriális szorzás nem kommutatív, hanem *antikommutatív*. A definícióból könnyen adódik, hogy teljesül a *Jacobi-identitás*: tetszőleges $p, q, r \in \mathbb{H}$-ra

$$(p \times q) \times r + (q \times r) \times p + (r \times p) \times q = 0.$$

A vektoriális szorzás nem asszociatív, például $i \times (i \times j) = i \times k = -j$, míg $(i \times i) \times j = 0$.

* **Kvaterniók és a háromdimenziós euklidészi tér.** A kvaterniók a fentiek alapján $\mathbb{R}^4$ (azaz a négydimenziós *téridő*) pontjainak is tekinthetők. A kvaterniók összeadása megfelel az $\mathbb{R}^4$-beli összeadásnak. A tisztán képzetes kvaterniók $\mathbb{R}^3$-mal, és így a három dimenziós tér pontjaival azonosíthatók: egy derékszögű koordinátarendszerben $(x, y, z) \in \mathbb{R}^3$ koordinátákkal rendelkező pontnak az $xi+yj+zk$ tisztán képzetes kvaternió felel meg. Ily módon i, j és k rendre a koordinátarendszer három tengelyén vett egységvektoroknak felelnek meg. Ha mást nem mondunk, akkor a koordinátarendszert úgy választjuk, hogy *jobbsodrású* legyen, azaz egy jobbmenetes csavart az i vektor irányából a j vektor irányába forgatva, a k vektor irányába haladjon. A tisztán képzetes kvaterniók összeadása megfelel a térbeli vektorok szokásos (paralelogramma-szabály) összeadásának. A $v = xi + yj + zk$ és $v' = x'i + y'j + z'k$ tisztán képzetes kvaterniók szorzatának valós része $-\langle v, v' \rangle$, ahol $\langle v, v' \rangle = xx' + yy' + zz'$, képzetes része pedig

$$\begin{aligned}\Im(vv') &= \frac{1}{2}(vv' - \overline{vv'}) = \frac{1}{2}(vv' - \overline{v'}\,\overline{v}) = \frac{1}{2}\big(vv' - (-v')(-v)\big) = \frac{1}{2}(vv' - v'v) \\ &= v \times v' = (yz' - zy')i + (zx' - xz')j + (xy' - x'y)k.\end{aligned}$$

A $(v, v') \mapsto \langle v, v' \rangle$ leképezést *belső szorzás*nak vagy *skaláris szorzás*nak nevezzük (bár nem művelet, de „kommutatív” és „mindkét oldalról disztributív az összeadásra nézve”). Nyilván $\langle v, v \rangle = |v|^2$. Egy kvaternió pontosan akkor vektor, ha a négyzete valós és kisebb vagy egyenlő nulla: ha s skalár, v vektor, akkor

$$(s + v)^2 = s^2 + v^2 + 2sv = s^2 - \langle v, v \rangle + v \times v + 2sv = s^2 - \langle v, v \rangle + 2sv;$$

ez az $s = 0$ esetben valós és kisebb, vagy egyenlő nulla, és ha valós, akkor $v = 0$ vagy $s = 0$, de a $v = 0$, $s \neq 0$ esetben nagyobb mint nulla. Ha v'' is egy vektor, akkor, mint könnyen kiszámolható, $v \times (v' \times v'') = \langle v, v'' \rangle v' - \langle v, v' \rangle v''$. Végül a $(v, v', v'') \mapsto \langle v, v' \times v'' \rangle$ leképezést *vegyes szorzás*nak szokás nevezni.

- $60/-10 \ldots -8$:

$<$

(mert mindkét oldal négyzete $p\overline{p}q\overline{q}$), $\big|\Re(p)\big| \leq |p|$, $\big|\Im(p)\big| \leq |p|$ és $|p| \leq \big|\Re(p)\big| + \big|\Im(p)\big|$. Ugyanúgy, mint a komplex számok esetében, belátható, hogy teljesül a $|p + q| \leq |p| + |q|$ *háromszög-egyenlőtlenség* és a $\big||p| - |q|\big| \leq |p - q|$ egyenlőtlenség.

$>$

(mert mindkét oldal négyzete $p\overline{p}q\overline{q}$). Teljesül a $|p+q| \leq |p|+|q|$ *háromszög-egyenlőtlenség* és a belőle kapható $\big||p| - |q|\big| \leq |p-q|$ egyenlőtlenség; mindkettő ugyanúgy kapható, mint a komplex számoknál.

* **A szorzások geometriai jelentése.** Ha egy vektort valós számmal (skalárral) szorzunk, az a vektor nyújtásának illetve összehúzásának felel meg, negatív valós szám esetén pedig az irányítás is változik. Az előző pont szerint ha v és v' tisztán képzetes kvaterniók, azaz vektorok, akkor

$$\langle v, v'\rangle^2 + |v \times v'|^2 = |v|^2|v'|^2. \tag{1}$$

Innen $\big|\langle v, v'\rangle\big| \le |v||v'|$ és $|v \times v'| \le |v||v'|$.

A koszinusz-tételből, ha a v és v' vektorok által bezárt szög φ, akkor

$$\begin{aligned} 2|v||v'|\cos\varphi &= |v|^2 + |v'|^2 - |v - v'|^2 \\ &= \langle v, v\rangle + \langle v', v'\rangle - \big(\langle v, v\rangle + \langle v', v'\rangle - \langle v, v'\rangle - \langle v', v\rangle\big) \\ &= 2\langle v, v'\rangle, \end{aligned}$$

tehát $\langle v, v'\rangle = |v||v'|\cos\varphi$. Ha v egységvektor és $v' \ne 0$, akkor $\langle v, v'\rangle$ abszolút értéke a v' vektor v irányú vetületének hossza, előjele pedig pozitív, ha a két vektor hegyesszöget zár be, negatív, ha a két vektor tompaszöget zár be, és nulla, ha merőlegesek.

Ebből az eredményből (1) felhasználásával $|v \times v'| = |v||v'||\sin\varphi|$, a v és v' által kifeszített paralelogramma területe. Tehát ha v és v' párhuzamosak, akkor vektori szorzatuk nulla lesz. Egyszerű számolással adódik, hogy $\langle v, v \times v'\rangle = 0$ és $\langle v', v \times v'\rangle = 0$, azaz $v \times v'$ merőleges a v és v' vektorokra. Az irányítás meghatározásához vegyük észre, hogy ha a v vektort az i irányba, a v' vektort pedig az i és j által adott síkba forgatjuk, de úgy, hogy második koordinátája ne legyen negatív, akkor vektori szorzatuk k irányú. Ez azt jelent, hogy v, v' és $v \times v'$ ugyanolyan irányítású vektorrendszert alkotnak, mint i, j és k.

Végül a vegyes szorzat geometriai jelentése a v, v' és v'' vektorok által kifeszített paralelepipedon előjeles térfogata, hiszen ennek alapterülete $|v' \times v''|$, magassága pedig $|v|\cos\varphi$, ahol φ a v és $v' \times v''$ által bezárt szög.

* **Forgatások.** A kvaterniókat a háromdimenziós forgatásokkal való szoros kapcsolatuk miatt felhasználják robotok vezérlésénél. Legyen p egy *egységvektor*, azaz egységnyi abszolút értékű vektor, v pedig egy tetszőleges p-re merőleges vektor. Megmutatjuk, hogy a $v \mapsto qv$ leképezés, ahol q az egységnyi abszolút értékű $q = \cos\varphi + p\sin\varphi$ kvaternió, a v vektornak a φ szöggel való elforgatása a p tengely körül, éspedig a p vektor vége felől nézve olyan irányba, mint a k vektor vége felől i-nek j-be való forgatása. Mivel $\langle v, p\rangle = 0$,

$$qv = (\cos\varphi + p\sin\varphi)v = v\cos\varphi + pv\sin\varphi = v\cos\varphi + p \times v\sin\varphi,$$

amiből adódik az állítás.

Most tekintsük a $v \mapsto qvq^{-1}$ leképezést. Megmutatjuk, hogy ez tetszőleges v vektorra a p tengely körüli 2φ szöggel való elforgatás. Először tegyük fel, hogy v merőleges p-re. Mivel $q^{-1} = \cos\varphi - p\sin\varphi$, a $\tilde{v} = qv$ jelöléssel, mivel $\tilde{v}$ merőleges p-re,

$$\tilde{v}q^{-1} = \tilde{v}(cos\varphi - p\sin\varphi) = \tilde{v}\cos\varphi - \tilde{v} \times p\sin\varphi = \tilde{v}\cos\varphi + p \times \tilde{v}\sin\varphi,$$

azaz $\tilde{v}q^{-1}$ a $\tilde{v}$ vektor φ szöggel történő továbbforgatásával kapható. Most legyen v tetszőleges, és írjuk fel $v = v' + v''$ alakban, ahol $v' = \alpha p$, $\alpha = \langle v, p\rangle$ és $v'' = v - v'$. Mivel v'' merőleges p-re, $qv''q^{-1}$ a v''-nek 2φ szöggel való elforgatásával adódik. Másrészt

$$qv'q^{-1} = (\cos\varphi + p\sin\varphi)\alpha p(\cos\varphi - p\sin\varphi) = \alpha p(\cos^2\varphi + \langle p, p\rangle \sin^2\alpha) = \alpha p = v',$$

azaz v' a transzformációnál nem változik. Ezzel az állítást beláttuk.

Az állításból azonnal adódik, hogy két forgatás egymásutánja is forgatás, és ennek tengelye és szöge is meghatározható, mert a $v \mapsto q'vq'^{-1}$ és $v \mapsto q''vq''^{-1}$ leképezések összetétele a $v \mapsto qvq^{-1}$ leképezés, ahol $q = q''q'$ egységnyi abszolút értékű kvaternió. Vegyük figyelembe, hogy φ és $\varphi + \pi$ ugyanazt a forgatást adják, de a $\cos\varphi + p\sin\varphi$ és a $\cos(\varphi+\pi) + p\sin(\varphi+\pi) = -\cos\varphi - p\sin\varphi$ kvaterniók egymás ellentettjei. Általánosabban, bármely $q \neq 0$ kvaternióra és $\alpha \neq 0$ valós számra a $v \mapsto qvq^{-1}$ és a $v \mapsto q'vq'^{-1}$ leképezések megegyeznek, ha $q' = \alpha q$.

* **Egyéb geometriai alkalmazások.** A háromdimenziós térben p_0 és p_1 által megadott pontok *távolsága* $|p_1 - p_0|$. Ha $p_0 \neq p_1$, akkor a két ponton átmenő egyenesnek a $v = p_1 - p_0$ vektor egy *irányvektora*; az egyenes bármely p pontjára $p - p_0$ a v vektor egy skalárszorosa, azaz valamely $t \in \mathbb{R}$-re $p = p_0 + tv$. Ez az *egyenes paraméteres egyenlete*. Ha p_0, p_1 és p_2 három pont, amelyek nem esnek egy egyenesbe, akkor a három ponton átmenő sík tetszőleges p pontjához léteznek olyan t_1 és t_2 valós számok, amelyekkel a $p - p_0 = v$ irányvektorra $v = t_1v_1 + t_2v_2$, ahol v_1 illetve v_2 a $p_1 - p_0$ illetve $p_2 - p_0$ irányvektorok. Innen $p = p_0 + t_1v_1 + t_2v_2$, ez a *sík paraméteres egyenlete*. A koordinátákat kiírva, ez három összefüggést jelent. Kettőből kifejezve a t_1 és t_2 paramétereket, és beírva a harmadikba, egy egyenletet kapunk, ez a *sík egyenlete*. Ugyanezt úgy is megkaphatjuk, hogy választunk egy, a v_1-re és a v_2-re is merőleges n *normálvektor*t, például $v_1 \times v_2$-t, és észrevesszük, hogy a v vektorokat az jellemzi, hogy merőlegesek n-re, azaz $\langle p, n\rangle = \langle p_0, n\rangle$. Hasonló módon, a sík paraméteres egyenletéből két sík egyenletét kaphatjuk (az egyenes ezek metszete), ez az *egyenes egyenletrendszere*.

A p pont és a p_0 ponton átmenő, n normálvektorú sík távolságát különösen egyszerű számolni, ha n-et egységvektornak választjuk, mivel ez a $p - p_0$ vektor n irányú vetületének hossza, azaz $\langle p - p_0, n\rangle$ abszolút értéke. Egy p pont távolságát a p_0 ponton átmenő, v irányvektorú egyenestől ugyancsak akkor a legegyszerűbb akkor számolni, ha v egységvektor: ez $(p - p_0) \times v$ hossza. A p_1 illetve p_2 pontokon átmenő, v_1 illetve v_2 irányvektorú egyenesek távolsága, ha n egységvektor, amely merőleges v_1-re és v_2-re is, $\langle p_2 - p_1, n\rangle$ abszolút értéke. Ezen két egyenes hajlásszöge a v_1 és v_2 vektorok által bezárt szög, amelynek koszinusza $\langle v_1, v_2\rangle$ abszolút értéke, ha v_1 és v_2 egységvektorok. Végül a v irányvektorú egyenes és az n normálvektorú sík hajlásszögének színusza, ha n és v is egységvektor, $\langle v, n\rangle$ abszolút értéke.

- 61/1 . . . 3 :

<

$\Re(u) = \Re(p)$, *képzetes része* $\Im(u) = \big(\Im(p), q\big)$. Egyszerű számolás mutatja, hogy $\mathbb{O}$ Abel-csoport a fenti összeadással: a nullelem a $(0, 0)$ pár, a (p, q) pár additív inverze a

$(-p,-q)$ pár. Teljesül mindkét oldali disztributivitás is. Vegyük észre, hogy ha $p, p' \in \mathbb{H}$, akkor

>

$\Re(u) = \Re(p)$, *képzetes része* $\Im(u) = \big(\Im(p), q\big)$. (A jelölés eltér a komplex számoknál szokásostól!) A definíció alapján könnyen belátható, hogy ha $u, v \in \mathbb{O}$, akkor $\overline{\overline{u}} = u$, $u + \overline{u} = 2\Re(u)$, $u - \overline{u} = 2\Im(u)$, $\overline{u+v} = \overline{u} + \overline{v}$, $\Re(uv) = \Re(vu)$ és $\overline{uv} = \overline{v}\,\overline{u}$ (sic!). Egyszerű számolás mutatja, hogy $\mathbb{O}$ Abel-csoport a fenti összeadással: a nullelem a $(0,0)$ pár, a (p,q) pár additív inverze a $(-p,-q)$ pár. A szorzásra nézve az $(1,0)$ pár egységelem. Teljesül mindkét oldali disztributivitás is. Vegyük észre, hogy ha $p, p' \in \mathbb{H}$, akkor

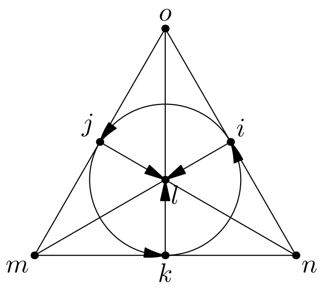
- 61/12...16 :

<

felírható $a + bi + cj + dk + el + fm + gn + ho$ alakban, ahol $a, b, c, d, e, f, g, h \in \mathbb{R}$. A szorzás nem asszociatív, mert például $(ij)l = kl \neq -kl = i(jl)$. Az $u\overline{u}$ szám itt is nem negatív valós szám, amely akkor és csak akkor nulla, ha $u = 0$, és segítségével bármely adott $u, v \in \mathbb{O}$, $u \neq 0$ oktávokhoz találhatók olyan oktávok, amelyekkel u-t balról, illetve jobbról szorozva v-t kapjuk, nevezetesen $\big(1/(u\overline{u})\big)(v\overline{u})$, illetve $\big(1/(u\overline{u})\big)(\overline{u}v)$.

>

felírható $a + bi + cj + dk + el + fm + gn + ho$ alakban, ahol $a, b, c, d, e, f, g, h \in \mathbb{R}$. Ilyen alakban $\Re(u) = a$, $\Im(u) = u - \Re(u)$ és $\overline{u} = \Re(u) - \Im(u)$, azaz $\overline{u}$-at úgy kapjuk, hogy i, j, k, l, m, n és o együtthatóját az ellentettjével helyettesítjük. Az i, j, k, l, m, n, o elemek mindegyikének a négyzete -1, egyébként a szorzataikra vonatkozó — a definícióból adódó — számolási szabályok a 3.4. ábráról olvashatók le: a körön, illetve az egyeneseken a megjelölt irányban haladva (ciklikusan) az egyik elemtől a másikig az eredmény a harmadik elem lesz, míg ellenkező irányban haladva az ellentettje.



0.10. ábra: oktávok szorzása.

A szorzás nem asszociatív, mert például

$$(ij)l = kl = o \neq -o = in = i(jl).$$

Az u, v, w elemek szorzásának asszociativitástól való eltérését az

$$[u, v, w] = (uv)w - u(vw)$$

mennyiséggel, az úgynevezett *asszociátor*ral mérhetjük. Az asszociátor az u, v, w elemek közül kettőt felcserélve ellenkezőjére változik, ezt *alternatív* tulajdonságnak nevezzük; bár az alternatív tulajdonság közvetlenül is kiszámolható, megmutatjuk, hogy következik a disztributivitásokból és a könnyebben kiszámolható

$$(uu)v = u(uv) \quad \text{és} \quad v(uu) = (vu)u,$$

azaz $[u, u, v] = 0$ és $[v, u, u] = 0$ speciális eseteiből. Valóban, ezekből

$$0 = [u, u+v, u+v] = [u, u, u] + [u, u, v] + [u, v, u] + [u, v, v] = [u, v, u],$$

azaz az asszociativitás mindig teljesül, ha két tényező egyenlő. Innen

$$0 = [u, v+w, v+w] = [u, v, v] + [u, v, w] + [u, w, v] + [u, w, w],$$

azaz $[u, v, w] = -[u, w, v]$. Hasonlóan adódik a többi eset.

Ha $u = a + bi + cj + dk + el + fm + gn + ho$, ahol $a, b, c, d, e, f, g, h \in \mathbb{R}$, akkor legyen

$$|u| = \sqrt{a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2}.$$

A kvaterniókra a szokásos abszolút értéket kapjuk vissza. Ha $u, v \in \mathbb{O}$, akkor $u\overline{u} = \overline{u}u = |u|^2$, $|0| = 0$, $u \neq 0$ esetén $|u| > 0$, $|u| = |\overline{u}|$, $\bigl|\Re(u)\bigr| \le |u|$, $\bigl|\Im(u)\bigr| \le |u|$, és $|uv| = |u||v|$ (mert mindkét oldal négyzete $(u\overline{u})(v\overline{v})$). Teljesül az $|u + v| \le |u| + |v|$ *háromszög-egyenlőtlenség* és a belőle kapható $\bigl||u| - |v|\bigr| \le |u - v|$ egyenlőtlenség; mindkettő ugyanúgy kapható, mint a komplex számoknál.

Figyeljük meg, hogy bármely $u, v \in \mathbb{O}$, $u \neq 0$ oktávokhoz pontosan egy olyan w oktáv van, amelyre $uw = v$, nevezetesen $w = \bigl(1/|u|^2\bigr)(\overline{u}v)$; az egyértelműség onnan következik, hogy ha $uw = v = uw'$, akkor $u(w - w') = 0$, ahonnan $|w - w'| = 0$. Hasonlóan egyértelműen oldható meg w-re a $wu = v$ egyenlet is, ha $u \neq 0$, nevezetesen $w = \bigl(1/(u\overline{u})\bigr)(v\overline{u})$.

- 66/2 :

  <

kek összege k; ezek az A halmaz *ismétléses kombinációi*. Ha A véges halmaz, akkor ezek

  >

kek összege k; ezek az A halmaz k-ad osztályú *ismétléses kombinációi*. Ha A véges halmaz, akkor ezek

- 69/4 :

  <

  Kiválasztási axióma. *Nem üres halmazok bármely családjához létezik*

  >

  * **Kiválasztási axióma.** *Nem üres halmazok bármely családjához létezik*

- 69/12 :

  <

  Zorn-lemma. *Ha egy részbenrendezett halmaz minden lánca felülről kor-*

  * **Bizonyítás.** A Zorn-lemma következik az úgynevezett Hausdorff-féle maximum-

  >

  * **Zorn-lemma.** *Ha egy részbenrendezett halmaz minden lánca felülről kor-*

  Bizonyítás. A Zorn-lemma következik az úgynevezett Hausdorff-féle maximum-

- 71/4 :

  <

  Jólrendezési tétel. *Minden halmaz jólrendezhető.*

  * **Bizonyítás.** Legyen X egy halmaz, és tekintsük $X \times X$ azon részhalmazait, amelyek

  >

  * **Jólrendezési tétel.** *Minden halmaz jólrendezhető.*

  Bizonyítás. Legyen X egy halmaz, és tekintsük $X \times X$ azon részhalmazait, amelyek

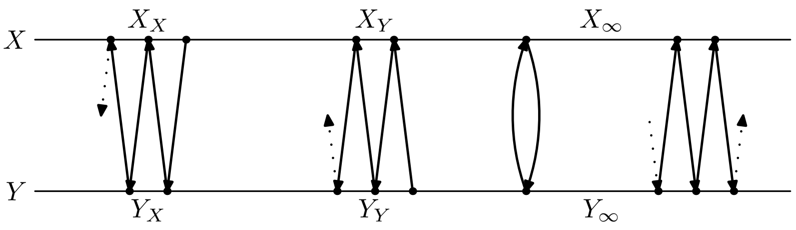
- 72/9 :

  <

Y-t is az Y_X, Y_Y és Y_∞ halmazra.

  >

Y-t is az Y_X, Y_Y és Y_∞ halmazra. (Lásd az 5.1. ábrát.)



0.11. ábra

- 74/12 :

  <

Az f kölcsönösen egyértelmű és $\mathbb{N}$-re képez. $\square$

  >

Az f kölcsönösen egyértelmű és $\mathbb{N}$-re képez, mert a $(0,k),(1,k-1),\ldots,(k,0)$ párokat rendre a

$$\frac{k(k+1)}{2}, \frac{k(k+1)}{2}+1, \ldots, \frac{k(k+1)}{2}+k = \frac{k^+(k^++1)}{2}-1$$

számokba viszi át. $\square$

- 78/−1 :

$<$

Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

$>$

Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

Egy elemnek az asszociáltjaitól különböző osztóit az elem *valódi osztó*inak nevezzük. Egy nem nulla elemnek az asszociáltak és az egységek a *triviális osztó*i.

- 82/8 :

$<$

$$\lim_{x\to\infty} \frac{\natural\{p : p \le x,\, p \text{ prímszám}\}}{\frac{x}{\ln x}} = 1.$$

$>$

$$\lim_{x\to\infty} \frac{\natural\{p : p \le x,\, p \text{ prímszám}\}}{\frac{x}{\ln x}} = 1.$$

Illusztrációként lásd a 6.1. ábrát.

- 83/6 :

$<$

és futásideje nem hosszabb, mint egy konstansszor az n hosszának a 13-dik hatványa.

$>$

és futásideje nem hosszabb, mint egy konstansszor az n hosszának a 13-adik hatványa.

- 84/3 . . . 4 :

$<$

reprezentáljuk. Az a elem által reprezentált maradékosztályt $\overline{a} \bmod m$ vagy rövidebben $\overline{a}$ jelöli. Természetesen a maradékosztály bármely eleme választható reprezentánsnak.

$>$

reprezentáljuk. Az a elem által reprezentált maradékosztályt $\tilde{a} \bmod m$ vagy rövidebben $\tilde{a}$ jelöli. Természetesen a maradékosztály bármely eleme választható reprezentánsnak.

- 84/−12 :

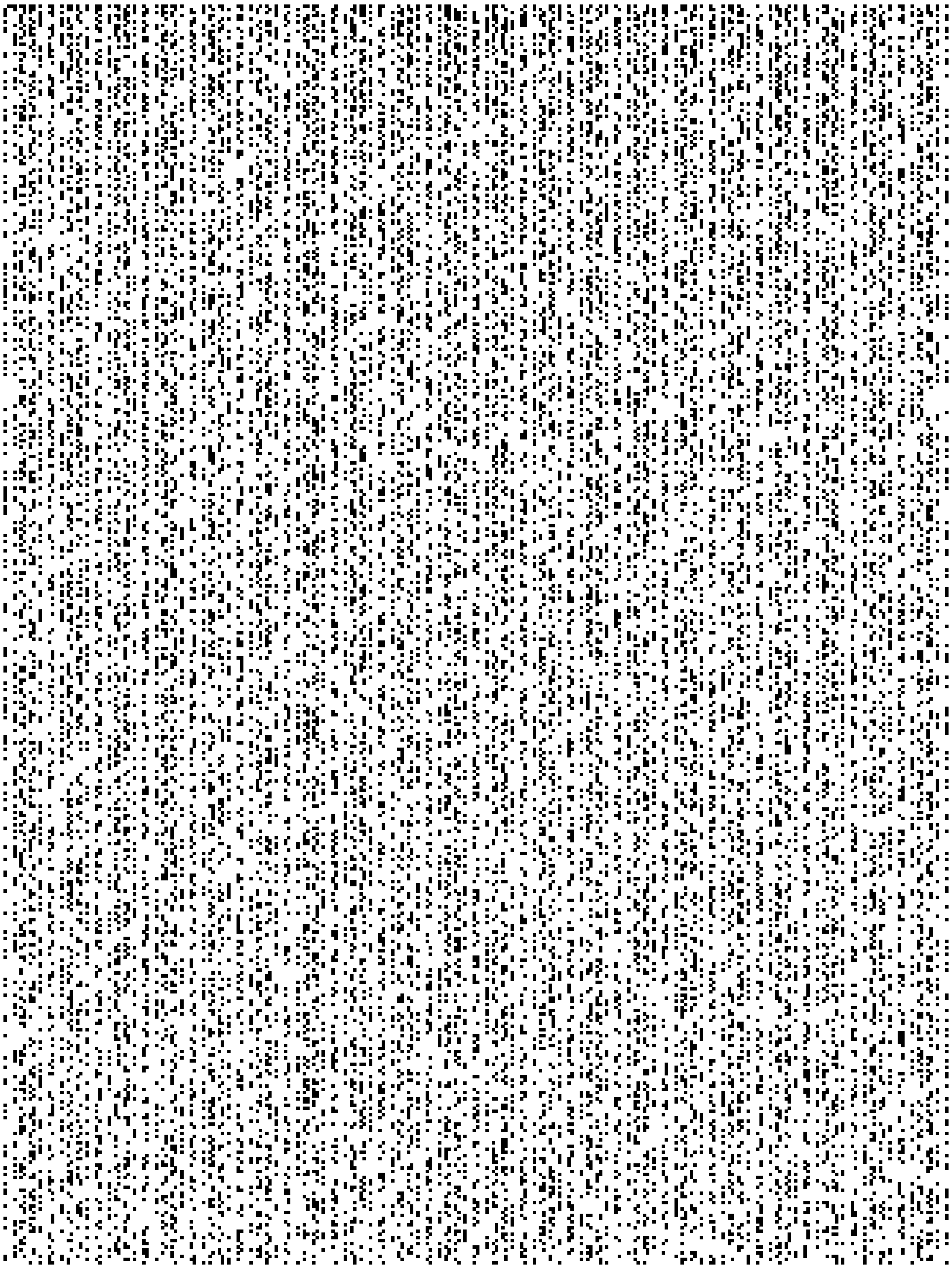
$<$

érdektelen. Ha $m = \pm 1$, akkor $\mathbb{Z}_m$ egyelemű, a zérógyűrű, így ez az eset is érdektelen.

$>$

érdektelen. Ha $m = \pm 1$, akkor $\mathbb{Z}_m$ egyelemű, a zérógyűrű, így ez az eset is érdektelen.

* **Komplemens számábrázolás.** Negatív számok számítógépes ábrázolására elterjedt a *komplemens ábrázolás*. Csak a bináris gépek esetével foglalkozunk. Egy n-bites gépen az egyik, régebben használt lehetőség $0 \le k < 2^{n-1}$ esetén $-k$ ábrázolására, hogy $-k \bmod (2^n - 1)$ kettes számrendszerbeli alakját tároljuk. Ezt úgy kapjuk, hogy k kettes számrendszerbeli alakját levonjuk $2^n - 1$ kettes számrendszerbeli alakjából. Mivel ez utóbbi csupa egyesből áll, a kivonás során nincs átvitel, k kettes számrendszerbeli



0.12. ábra: a 240 000-nél kisebb páratlan prímek, sorfolytonosan, 400 sor

alakját csak bitenként komplementáljuk. Innen ered az ábrázolás neve: *egyesekre komp-*

lemens ábrázolás. A negatív számok legfelső bitje 1, de a nullának két ábrázolása van: $000\dots000$ és $111\dots111$. Az ellentett képzése gyors, az ábrázolható számok intervalluma szimmetrikus a nullára, de az előjeles számok összeadását modulo (2^n-1) kell végezni. Mára kiszorította a *kettes komplemens ábrázolás*: $0<k\le 2^{n-1}$ esetén $-k$ ábrázolására $-k \bmod 2^n$ kettes számrendszerbeli alakját tároljuk. Ezt úgy kapjuk, hogy k kettes számrendszerbeli alakjának vesszük a bitenkénti komplementerét, majd hozzáadunk 1-et. Ennél pontosan a negatív számok legfelső bitje 1, és a nullának csak egy ábrázolása van. Az ellentett képzése lassabb, és az ábrázolható számok intervalluma nem szimmetrikus a nullára, de az előjeles számok összeadását is modulo 2^n kell végezni, ugyanúgy, mint az előjel nélküliekét. Természetesen mindkét ábrázolásnál előfordulhat túlcsordulás, ha az eredmény nincs az ábrázolható intervallumban.

- $84/-5\dots-4$:

<

Bizonyítás. Legyen $d=\text{lnko}(a,m)$. Ha $1<d<m$, akkor $a\cdot(m/d)=(a/d)\cdot m\equiv 0 \pmod m$, ahonnan $x=m/d$ jelöléssel $\overline{a}\cdot\overline{x}=\overline{0}$, azaz $\overline{a}$ nullosztó $\mathbb{Z}_m$-ben. Ha $d=1$,

>

Bizonyítás. Legyen $d=\text{lnko}(a,m)$. Ha $1<d<m$, akkor $a\cdot(m/d)=(a/d)\cdot m\equiv 0 \pmod m$, ahonnan $x=m/d$ jelöléssel $\tilde{a}\cdot\tilde{x}=\tilde{0}$, azaz $\tilde{a}$ nullosztó $\mathbb{Z}_m$-ben. Ha $d=1$,

- $84/-2$:

<

$ax+my=1$. Innen $ax\equiv 1 \pmod m$ azaz $\overline{a}\cdot\overline{x}=\overline{1}$ miatt $\overline{x}$ az $\overline{a}$ inverze $\mathbb{Z}_m$-ben.

>

$ax+my=1$. Innen $ax\equiv 1 \pmod m$ azaz $\tilde{a}\cdot\tilde{x}=\tilde{1}$ miatt $\tilde{x}$ az $\tilde{a}$ inverze $\mathbb{Z}_m$-ben.

- $85/1$:

<

Az Euler-féle φ függvény. Legyen $m>0$ egész szám, és jelölje $\varphi(m)$ a

>

Diszkrét logaritmus probléma. A következő pont mutatja, hogy Z_m-ben nem nehéz hatványozni. Azonban a tapasztalat szerint még ha m prím is, Z_m invertálható elemeinek multiplikatív csoportjában egy a alap és egy a^k hatvány ismeretében nehéz meghatározni a k kitevőt, legalábbis ha $m-1$-nek vannak nagy prímtényezői: ez a *diszkrét logaritmus probléma*. A probléma számos más csoport esetén is nehéznek tűnik.

* **Gyors hatványozás.** Az alábbi algoritmus akármilyen G (multiplikatív) félcsoportban hatékonyan kiszámolja egy $g\in G$ elem n-edik hatványát, ahol $n\in\mathbb{N}^+$. (Célszerű n-et kettes számrendszerben felírni, mert akkor a mellékszámítások triviálisak.) Válasszunk olyan $k\in\mathbb{N}$-et, amelyre $2^k\le n<2^{k+1}$. Minden $0\le j\le k$-ra sorban kiszámítjuk $x_j=g^{n_j}$-t, ahol $n_j=\lfloor n/2^{k-j}\rfloor$, azaz n_j az n bináris felírásának első $j+1$ jegye által megadott természetes szám. Nyilván $n_0=1$, így $x_0=g$. Ha n_j páros, akkor $n_j=2n_{j-1}$, így $x_j=x_{j-1}^2$, ha pedig n_j páratlan, akkor $n_j=2n_{j-1}+1$, így $x_j=gx_{j-1}^2$. Az eredmény $x_k=g^n$. Például ha $n=23$, akkor n kettes számrendszerben 10111, így n_j,

$j = 0, 1, 2, 3, 4$-re kettes számrendszerben 1, 10, 101, 1011 és 10111, tehát $x_0 = g^{n_0} = g$, $x_1 = g^{n_1} = x_0^2$, $x_2 = g^{n_2} = gx_1^2$, $x_3 = g^{n_3} = gx_2^2$ és $x_4 = g^n = g^{n_4} = gx_3^2$.

Diffie–Hellmann–Merkle-kulcscsere. A felhasználók megállapodnak egy nagy (több száz jegyű) Sophie Germain prímben, azaz olyan p prímben, amelyre $q = 2p + 1$ is prím, valamint egy $1 < g < p - 1$ alapban. (Bár nem tudjuk, hogy van-e végtelen sok Sophie Germain prím, a tapasztalat szerint elég sűrűn vannak, az n jegyűek közötti távolság nagyságrendben n^2.) Ha két felhasználó, Aliz és Bob valamely szokásos rejtjelzési rendszer, például az AES (lásd 8.3.55.) felhasználásával titkosított üzenetet akar váltani, akkor szükségük van egy véletlenszerű közös kulcsra. Választanak egy $1 < a < p$ illetve $1 < b < p$ véletlen kitevőt, kiszámolják és felteszik a honlapukra a $g^a \bmod q$ illetve $g^b \bmod q$ értékeket. Mindketten ki tudják számolni $g^{ab} \bmod q$ értékét, ez lesz a közös titkos kulcs. Az eljárás biztonsága azon múlik, hogy g, $g^a \bmod q$ és $g^b \bmod q$ ismeretében sem látszik jobb megoldás $g^{ab} \bmod q$ meghatározására, mint a vagy b megkeresése, ez viszont a nehéz diszkrét logaritmus probléma. Ezt a kulcscsere módszert használja az ssh (secure shell) és az SSL (Secure Socket Layer), illetve annak a továbbfejlesztése, a TLS (Transport Layer Security) protokoll is. Az üzenetek manipulálására képes „közbeékelődő” támadó úgynevezett „nagymester sakk támadásával” szemben védtelen, ezért nem biztonságos hálózaton inkább egy módosított formában használják: digitálisan aláírva (lásd 6.2.39., 6.2.42.) küldik át a $g^a \bmod q$ illetve $g^b \bmod q$ értékeket.

Hasonlóan használható más csoport is, amelyben könnyű a hatványozás, de nehéz a diszkrét logaritmus probléma megoldása.

Feladat [5]. Készítsünk 3 alapú logaritmustáblát $\mathbb{Z}_{17}$-ben.

Az Euler-féle φ függvény. Legyen $m > 0$ egész szám, és jelölje $\varphi(m)$ a

- 87/−7 :

<

Az RSA-eljárás. Az alábbi rejtjelzési sémát Rivest, Shamir és Adleman találták. Keressünk két „nagy” p, q prímet, $p \neq q$ (például 140–160 jegyűeket), és legyen $n = pq$. Válasszunk egy véletlen $1 < e < (p-1)(q-1)$ exponenst, és a bővített euklideszi algoritmussal oldjuk meg az

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

kongruenciát. (Ha azt találjuk, hogy

$$\text{lnko}\big(e, (p-1)(q-1)\big) > 1,$$

kezdjünk mindent elölről.) Ha $1 < m < n$ egy üzenet, akkor $c = m^e \bmod n$ használható, mint az üzenet rejtjelzett formája. Ebből az üzenet visszakapható:

$$(m^e)^d = m^{k(p-1)(q-1)+1} = \left(m^{(p-1)}\right)^{k(q-1)} \cdot m \equiv m \pmod{p},$$

mert ha $p|m$, akkor mindkét oldal nullával kongruens, ha viszont $p\nmid m$, akkor a Fermat-tétel szerint $m^{p-1} \equiv 1 \pmod p$. Hasonlóan $(m^e)^d \equiv m \pmod q$. Innen a kínai maradéktétel szerint $m = c^d \bmod n$. Az n és e értékek nyilvánosságra is hozhatók. Az eljárás biztonsága azon múlik, hogy n prímtényezőinek meghatározása a mai módszerekkel évmilliárdokig tartana.

A séma felhasználható digitális aláírásra is: Aliz (esetleg Bob kulcsával rejtjelezve) az

$$m, m^{d_A} \bmod n_A$$

párt küldi el Bobnak (a második szám az aláírás).

Az eljárás bizonyítványok kiállítására is felhasználható. Egy hitelt érdemlő szervezettől, aminek nyilvános kulcsát mindenki ismeri, aláírt levélben kaphatjuk meg Aliz nyilvános kulcsát, így ha Aliztól levelet kapunk, biztosak lehetünk benne, hogy nem csalóval állunk szemben, aki Aliznak adja ki magát.

Az RSA-eljárás egy alkalmazása gyorsabb, nem nyilvános kulcsú rejtjelző eljárások kulcsainak cseréje.

Az eljáráshoz szükséges „nagy" prímeket például a Miller–Rabin-féle valószínűségi teszttel találhatjuk meg. A hatványozás hatékonyan egy gyors hatványozási eljárással végezhető.

$>$

Az RSA-eljárás. Az alábbi rejtjelezési sémát Rivest, Shamir és Adleman találták. Keressünk két „nagy" (például 150–160 jegyű) p, q, $p \neq q$ prímet, és legyen $n = pq$. Válasszunk egy $1 < e < (p-1)(q-1)$ kitevőt, és a bővített euklideszi algoritmussal oldjuk meg az

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

kongruenciát. (Ha azt találjuk, hogy

$$\operatorname{lnko}\big(e, (p-1)(q-1)\big) > 1,$$

kezdjük elölről az eljárást.) Ha $1 < m < n$ egy üzenet, akkor $c = m^e \bmod n$ használható, mint az üzenet rejtjelezett formája. Ebből az üzenet újabb hatványozással visszakapható:

$$(m^e)^d = m^{k(p-1)(q-1)+1} = \left(m^{(p-1)}\right)^{k(q-1)} \cdot m \equiv m \pmod p,$$

mert ha $p|m$, akkor mindkét oldal nullával kongruens, ha viszont $p\nmid m$, akkor a Fermat-tétel szerint $m^{p-1} \equiv 1 \pmod p$. Hasonlóan $(m^e)^d \equiv m \pmod q$. Innen a kínai maradéktétel szerint, mivel $p \neq q$ prímek, $m = c^d \bmod n$. Az n és e értékek nyilvánosságra is hozhatók, ekkor bárki tud nekünk rejtjelzett üzenetet küldeni: az eljárás úgynevezett *nyilvános kulcsú kódolás*. Biztonsága azon múlik, hogy d, p és q értékét más nem ismeri: az n prímtényezőinek meghatározása a mai módszerekkel nagyon sokáig tartana, mert nagy prímtényezők meghatározására nincs hatékony módszerünk.

Az RSA eljárás felhasználható digitális aláírásra is: Aliz (Bob kulcsával rejtjelezve) nemcsak az m üzenetet, hanem

$$m^{d_A} \bmod n_A$$

értékét is elküldi Bobnak: ez az aláírás, mert csak Aliz volt képes kiszámítani. Ha az m üzenet hosszú, célszerű egy $h(m)$ véletlenszerűnek látszó „lenyomatát" használni az aláírásnál m helyett. Rejtjelezési célra kifejlesztett, jelenleg gyakran használt lenyomatképző „hash"-függvények a 160 bites lenyomatot adó SHA-1 (Secure Hash Algorithm) illetve a szabadalommal nem védett RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest). Újabb változataik nagyobb biztonságot adó hosszabb lenyomatot adnak: lásd a Wikipedia-t.

Az eljárás bizonyítványok kiállítására is felhasználható. Egy hitelt érdemlő szervezettől, aminek nyilvános kulcsát mindenki ismeri, aláírt levélben kaphatjuk meg Aliz nyilvános kulcsát, így ha Aliztól levelet kapunk, biztosak lehetünk benne, hogy nem csalótól kaptunk üzenetet, aki Aliznak adja ki magát.

Az RSA-eljárás egy alkalmazása nála gyorsabb, nem nyilvános, hanem szimmetrikus kulcsú „klasszikus" rejtjelező eljárások (például AES, lásd 8.3.55.) kulcsainak cseréje. Így működik például az e-mail-ek védelmére szolgáló PGP (Pretty Good Privacy) rendszer, amely először egy véletlen kulcsot generál, azt átküldi RSA-rejtjelezéssel, majd az aláírt üzenetet küldi el a véletlen kulccsal rejtjelezve. Ezt a módszert „digitális borítéknak" nevezik.

Az RSA kódolás használatánál néhány biztonsági szabály be kell tartani. Másmás n-et használjunk rejtjelezésre és digitális aláírásra. Az n bitjeinek száma legfeljebb néggyel legyen rövidebb, mint a névleges bitszám, ami ma szokásosan 1024. A prímeket úgy nyerjük, hogy véletlenszerűen választott számoktól kezdve keressük meg az első prímet, ezzel biztosítható a magas (minimum 128 bit) entrópia (lásd 9.1.1.). A nagyobb és a kisebb prím hányadosa legalább $\sqrt{2}$, de legfeljebb 2^{30} legyen. Véletlen hexadecimális jegyeket nyerhetünk például egy karaktersorozat visszagépelésénél mérve az időket modulo 16 ms. Az e exponenst nem ajánlatos túl kicsinek választani, szokásos legkisebb értéke 65537. Az üzenet egy nulla bájttal kezdődik, majd ezután egy legalább 8 nem nulla bájtot tartalmazó (véletlen, minden üzenetnél más) „sózás" következik, amelyet egy újabb nulla bájt határol, és ezután következnek a szöveg bájtjai; a teljes hossz 128 bájt. A kezdő nulla bájt biztosítja, hogy $m < n$. A „sózás" szerepe az, hogy ne lehessen kitalálni az üzenetet, és rejtjelezve ellenőrizni, hogy tényleg az-e. Hosszabb üzenetet részekre bontunk. A dekódolás gyorsítható, ha a

$$c^{d \bmod (p-1)} \bmod p \quad \text{és} \quad c^{d \bmod (q-1)} \bmod q$$

értékeket számítjuk ki, és ezekből a kínai maradéktétel alapján állítjuk vissza m-et. Az RSA áltánosítható arra az esetre, amikor n kettőnél több „nagy" prím szorzata. A 2048 névleges bitszám valószínűleg legalább 10-15 évre biztosítja a titkosságot, 3072 bit jóval tovább. További részletek: RFC 3447.

Az eljáráshoz szükséges „nagy" prímeket például a Miller–Rabin-féle valószínűségi teszttel találhatjuk meg.

- $88/-3$:

  $<$

Ismételt alkalmazásával tetszőlegesen kis valószínűséget elérhetünk.

A valószínűségi teszt nagyon ritkán hibázik: $25 \cdot 10^9$-ig csak 13 olyan összetett szám van, amely átmegy a teszten az $a = 2, 3, 5$ alapokkal.

* **Gyors hatványozás.** Az alábbi algoritmus akármilyen G (multiplikatív) félcsoportban kiszámolja egy $g \in G$ elem n-edik hatványát, ahol $n \in \mathbb{N}^+$. (Célszerű n-et kettes számrendszerben felírni, mert akkor a mellékszámítások triviálisak.) Válasszunk olyan $k \in \mathbb{N}$-et, amelyre $2^k \le n < 2^{k+1}$. Minden $0 \le j \le k$-ra kiszámítjuk $x_j = g^{n_j}$-t, ahol $n_j = \lfloor n/2^{k-j} \rfloor$. Nyilván $n_0 = 1$, így $x_0 = g$. Ha n_j páros, akkor $n_j = 2n_{j-1}$, így $x_j = x_{j-1}^2$, ha pedig n_j páratlan, akkor $n_j = 2n_{j-1} + 1$, így $x_j = gx_{j-1}^2$. Az eredmény $x_k = g^n$. Például ha $n = 23$, akkor n kettes számrendszerben 10111, így n_j, $j = 0, 1, 2, 3, 4$ kettes számrendszerben 1, 10, 101, 1011 és 10111, tehát $x_0 = g^{n_0} = g$, $x_1 = g^{n_1} = x_0^2$, $x_2 = g^{n_2} = gx_1^2$, $x_3 = g^{n_3} = gx_2^2$ és $x_4 = g^n = g^{n_4} = gx_3^2$.

>

Ismételt alkalmazásával tetszőlegesen kis hibavalószínűséget elérhetünk. Például kriptográfiai célra 2^{-60}-nál kisebb hibavalószínűséget szokás előírni, amit 30 véletlen alappal elérhetünk.

A valószínűségi teszt nagyon ritkán hibázik. Az első összetett szám, amely a 2 alappal átmegy a teszten 2 047, amely még a 3 alappal is 1 373 653, amely még az 5 alappal is 25 326 001, amely még a 7 alappal is 118 670 087 467, amely még a 11 alappal is 2 152 302 898 747, amely még a 13 alappal is 3 474 789 660 383, és amely még a 17 alappal is 341 550 071 728 321.

* **Digital Signature Standard.** A DSS szabvány az alábbi DSA (Digital Signature Algorithm) eljárást használja digitális aláírásra: Válasszunk egy h kriptográfiai „hash”-függvényt, amely az m üzenetből 160 bites „lenyomatot” készít (lásd a 6.2.39. pontot). Keressünk egy 160 bites q prímet, majd egy olyan 1024 bites p prímet, amelyre $p - 1$ többszöröse q-nak, és válasszunk egy olyan a alapot, amelyre $g = a^{(p-1)/q} \bmod p > 1$. Minden felhasználó a h függvényt és a g, p, q értékeket fogja használni. Minden felhasználó választ magának egy véletlen titkos $1 < x < q$ értéket, kiszámolja $y = g^x \bmod p$ értékét, és az nyilvánosságra hozza. Egy-egy üzenet aláírásának a menete a következő: Választunk egy $1 < k < q$ véletlen értéket. Kiszámoljuk az

$$r = (g^k \bmod p) \bmod q$$

és

$$s = k^{-1}\big(h(m) + xr\big) \bmod q$$

értékét. Abban a ritka esetben, amikor $r = 0$ vagy $s = 0$, új k értéket választunk, egyébként az aláírás az (r, s) pár. Az aláírás ellenőrzésére a címzett kiszámolja az $w = s^{-1} \bmod q$, $u_1 = h(m)w \bmod q$, $u_2 = rw \bmod q$ és $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$ értékeket. Ha $v = r$, akkor az aláírást helyesnek fogadja el. Valóban, mivel a Fermat-tétel szerint $g^q \equiv a^{p-1} \equiv 1 \pmod p$, továbbá $k \equiv h(m)s^{-1} + xrs^{-1} \pmod q$, azt kapjuk, hogy

$$g^k \equiv g^{h(m)w} g^{xrw} \equiv g^{h(m)w} y^{rw} \equiv g^{u_1} y^{u_2} \pmod p,$$

ahonnan $r = v$.

Az eljárás hosszabb, például 224 vagy 256 bites lenyomatot adó hash-függvénnyel és ugyanennyi bites q-val, valamint 2048 illetve 3072 bites p-vel is használható.

• 90/13 :

$<$

$2\nu(2) = 2.$

$>$

$2\nu(2) = 2.$

Legyen $\kappa(n)$ az n szám prímtényezőinek, $\nu(n)$ pedig az n különböző prímosztóinak száma. Például $\kappa(1) = 0$, $\kappa(2) = 1$, $\kappa(3) = 1$, $\kappa(4) = 2$, $\kappa(5) = 1$, $\kappa(6) = 1$ és $\nu(1) = 0$, $\nu(2) = 1$, $\nu(3) = 1$, $\nu(4) = 1$, $\nu(5) = 1$, $\nu(6) = 2$. Könnyen végiggondolható, hogy κ teljesen additív számelméletifüggvény, míg ν additív, de nyilván nem teljesen additív, például $1 = \nu(4) \neq 2\nu(2) = 2$.

Ha r tetszőleges valós szám, legyen $\sigma_r(n) = \sum_{0<d|n} d^r$, és legyen $\tau = \sigma_0$, $\sigma = \sigma_1$, azaz τ az osztók száma, σ pedig az osztók összege. Például $\tau(1) = 1$, $\tau(2) = 2$, $\tau(3) = 2$, $\tau(4) = 3$, $\tau(5) = 2$, $\tau(6) = 4$ és $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$, $\sigma(5) = 6$, $\sigma(6) = 12$. Mivel ha m és n relatív prímek, akkor mn minden pozitív osztója egyértelműen írható fel cd alakban, ahol c az m, d pedig az n pozitív osztója,

$$\begin{aligned}\sigma_r(mn) &= \sum_{0<cd|mn} (cd)^r = \sum_{0<c|m} \sum_{0<d|n} c^r d^r = \sum_{0<c|m} c^r \sum_{0<d|n} d^r \\ &= \sum_{0<c|m} c^r \sigma_r(n) = \sigma_r(m)\sigma_r(n),\end{aligned}$$

azaz σ_r multiplikatív minden r-re. Mivel p^α osztói $1, p, p^2, \dots, p^\alpha$, kapjuk, hogy $\tau(p^\alpha) = \alpha + 1$ és $\sigma_r(p^\alpha) = (p^{r(\alpha+1)} - 1)/(p^r - 1)$, ha $r \neq 0$. Innen, ha $n = p_1^{\alpha_1} \cdots p_t^{\alpha_k}$ az n kanonikus alakja, akkor

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$$

és

$$\sigma_r(n) = \prod_{j=1}^{k} \frac{p_j^{r(\alpha_j+1)} - 1}{p_j^r - 1}, \quad \text{ha} \quad r \neq 0.$$

A számelméleti függvények értékének számítása általában nem egyszerű, ismernünk kell hozzá a szám kanonikus alakját.

• 90/13 :

$<$

$\circ *$ **Definíció.** Ha k tetszőleges valós szám, legyen $\sigma_k(n) = \sum_{d|n} d^k$, és legyen $\tau = \sigma_0$, $\sigma = \sigma_1$. Mivel σ_k az $n \mapsto n^k$ (teljesen) multiplikatív számelméleti függvény összegzési függvénye, multiplikatív. Továbbá, ha $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ az n kanonikus alakja, akkor

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$$

és

$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1},$$

ugyanis $\tau(p^\alpha) = \alpha + 1$ és $\sigma(p^\alpha) = (p^{\alpha+1} - 1)/(p-1)$, hiszen p^α osztói $1, p, p^2, \dots, p^\alpha$.
>
°* **Példa.** Tetszőleges k valós számra a σ_k számelméleti függvény multiplikativitása következik abból, hogy az $n \mapsto n^k$ (teljesen) multiplikatív számelméleti függvény összegzési függvénye.

• 93/1 :
<
Lánctörtek. Valós számok q_1, $q_1 + 1/q_2$, $q_1 + 1/(q_2 + 1/q_3)$, $\dots$ alakú kö-
>
* **Lánctörtek.** Valós számok q_1, $q_1 + 1/q_2$, $q_1 + 1/(q_2 + 1/q_3)$, $\dots$ alakú kö-

• 93/−4 :
<
° **Példák.** (1) Határozzuk meg 172/62 lánctörtközelítéseit. A számítás:
>
°* **Példák.** (1) Határozzuk meg 172/62 lánctörtközelítéseit. A számítás:

• 94/7 :
<
Lánctörtközelítések zárt alakja. *Az előző definíció jelöléseivel, ha*
>
* **Lánctörtközelítések zárt alakja.** *Az előző definíció jelöléseivel, ha*

• 95/1 :
<
Példa. Számítsuk ki $172/62 = //2, 1, 3, 2, 3//$ lánctörtközelítéseit zárt alak-
>
* **Példa.** Számítsuk ki $172/62 = //2, 1, 3, 2, 3//$ lánctörtközelítéseit zárt alak-

• 95/5 :
<
° **Megjegyzés.** Egy valós szám lánctörtközelítései meglehetősen gyorsan kon-
>
°* **Megjegyzés.** Egy valós szám lánctörtközelítései meglehetősen gyorsan kon-

• 95/9 :
<
Megjegyzés. Történeti érdekesség, hogy a görögök a lánctörteket használták
>
* **Megjegyzés.** Történeti érdekesség, hogy a görögök a lánctörteket használták

- 95/−7 :

  $<$

  Tétel. *Legyen α egy irracionális szám. Az előző tétel jelöléseivel, ha $p \in \mathbb{Z}$,*

  $>$

  * **Tétel.** *Legyen α egy irracionális szám. Az előző tétel jelöléseivel, ha $p \in \mathbb{Z}$,*

- 95/−1 :

  $<$

  * **Bizonyítás.** Lásd Niven és Zuckerman [66] könyvét, 140. oldal. $\square$

  $>$

  Bizonyítás. Lásd Niven és Zuckerman [66] könyvét, 140. oldal. $\square$

- 96/1 :

  $<$

  ° **Példa.** Közelítsük a π számot lánctörtek segítségével. Mivel

  $>$

  °* **Példa.** Közelítsük a π számot lánctörtek segítségével. Mivel

- 97/2 :

  $<$

Ebben a fejezetben a gráfelmélet alapjaival foglalkozunk. A gráfelmélet jelentőségét informatikai alkalmazásai adják.

$>$

Ebben a fejezetben a gráfelmélet alapjaival foglalkozunk. Számos problémában csak bizonyos dolgok közötti kapcsolatok létezése vagy nem létezése fontos, ilyenkor rendszerint gráfelméleti problémához jutunk. Például bejárható-e a sakktábla huszárral úgy, hogy ugyanoda érjünk vissza, ahonnan elindultunk? Írhatunk-e 0-kat és 1-eket egy kör mellé úgy, hogy adott irányban körbemenve minden lehetséges módon leolvasva a négy egymás utáni számjegyet, minden négy hosszú 0–1-sorozatot pontosan egyszer kapjunk meg? Legfeljebb hány összeköttetés (vagy hány gép) eshet ki egy adott számítógépes hálózatból úgy, hogy még legyen bármely két gép között összeköttetés? Mennyi egy számítógépes hálózat „átviteli kapacitása”? Hogyan térképezhetők fel az emberek közötti ismeretségek? Legalább hány rétegű nyomtatott áramköri lap kell egy adott áramkör legyártásához? Melyik a legrövidebb villamos hálózat? Hányféleképpen kapcsolódhatnak össze adott atomok? Milyen lehetséges „reakcióutak” vannak egy részecskefizikai folyamatnál? A problémák különböző területekről jönnek, szerteágazóak és változó nehézségűek, de talán a legfontosabb alkalmazásokat az informatika adja.

- 98/5 :

  $<$

véges gráfok vizsgálatával foglalkozunk.

$>$

véges gráfok vizsgálatával foglalkozunk.

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 pedig $V \setminus S$-ben van.

- 98/-15 :

$<$

valamely $n \in \mathbb{N}$-re n-reguláris.

$>$

valamely $n \in \mathbb{N}$-re n-reguláris. Példa n-reguláris gráfra az n-dimenziós H_n *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: lásd a ábrát.

- 98/-6 :

$<$

Két gráf izomorfiáját általában nem könnyű bizonyítani, lényegében nincs sokkal jobb módszer, mint az összes lehetséges f, g leképezéseket kipróbálni. Persze, ha a két

$>$

Két gráf izomorfiáját általában nem könnyű bizonyítani, néha nincs lényegesen jobb módszer, mint az összes lehetséges f, g leképezéseket kipróbálni. Például a ábrán szereplő gráfra nem nyilvánvaló, hogy nem izomorf a Petersen-gráffal. Persze, ha a két

- 99/3 :

$<$

$g(v)$ és $g(w)$ szomszédosak, akkor G és G' nyilván izomorfak.

$>$

$g(v)$ és $g(w)$ szomszédosak, akkor G és G' nyilván izomorfak.

A gráelmélet elsősorban *gráftulajdonság*okkal foglalkozik; ezek olyan tulajdonságok, amelyekkel izomorf gráfok egyszerre rendelkeznek.

- 99/4 :

$<$

Teljes gráfok. Ha egy egyszerű gráfban bármely két különböző csúcsot él köt össze, akkor a gráfot *teljes gráf* nak nevezzük. Teljes gráfok esetén, ha a csúcsok halmazai között létezik kölcsönösen egyértelmű leképezés, 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. Az n szögpontú teljes gráfnak $n(n-1)/2$ éle van.

$>$

Példák. Ha egy egyszerű gráfban bármely két különböző csúcsot él köt össze, akkor a gráfot *teljes gráf* nak vagy *klikk*nek nevezzük. Teljes gráfok esetén, ha a csúcsok halmazai között létezik kölcsönösen egyértelmű leképezés, 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 gráfról. Az n szögpontú teljes gráfnak $n(n-1)/2$ éle van, és K_n-nel szokás jelölni. Ugyanebben az értelemben beszélünk az öt szbályos test élgráfjáról, a Petersen-gráfról, a H_n hiperkockáról. Néhány további példa: a C_n *ciklus* csúcsai az n-edik egységgyökök, ahol él megy minden egységgyökből a következőbe (ciklikusan). A P_n *ösvény* C_{n+1}-ből az 1-be vivő él törlésével adódik. Az S_n *csillag*ban az n-edik egységgyökök vannak összekötve a nullával. Lásd a ábrát.

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-szorzat*uk 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. Például ha H_1-ből n példány Descartes-szorzatát vesszük, H_n-et kapjuk. Ilyen Descartes-szorzatot használnak összeköttetési gráfnak masszív paralel számítógépekben: H_n mellett P_m két vagy három példányának Descartes-szorzata (síkrács illetve térrács), valamint C_m két vagy három példányának Descartes-szorzata (két- illetve háromdimenziós tórusz) fordul elő gyakran; rendszerint m kettőhatvány.

- $99/-13\ldots-12$:

$<$

és bármely kút között van egy él, de több él nincs. A 7.2. ábrán balra látható K_5 az öt szögpontú teljes gráf, míg jobbra $K_{3,3}$ („három ház, három kút” gráf) páros gráf.

$>$

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 7.2. ábrán balra látható K_5, az öt szögpontú teljes gráf, míg jobbra a $K_{3,3}$ („három ház, három kút”) páros gráf.

- $104/3$:

$<$

vannak olyan csúcsok, amelyeket az E' élhalmaz elvág, akkor E'-t *elvágó élhalmaz*nak

$>$

vannak olyan csúcsok, amelyeket az E' élhalmaz elvág, akkor E'-t *elvágó halmaz*nak

- $105/10$:

$<$

Bizonyítás. Először tegyük fel, hogy $s = 1$. Legyenek v és v' a páratlan fokú csúcsok. Tekintsük a v-ből v'-be vezető, különböző vonalak közül a maximális hosszúságút. Ha ebben nem minden él szerepelne, akkor az összefüggőség miatt lenne a vonalon olyan v'' csúcs, amelyre illeszkedő élek közül nem minden él van felhasználva. Induljunk el ebből a csúcsból egy fel nem használt élen, és haladjunk mindig fel nem használt éleken. Mivel minden csúcsra páros sok fel nem használt él illeszkedik, a továbbhaladás csak akkor nem 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 vonalat kapnánk v-ből v'-be.

Teljesen hasonlóan adódik az $s = 0$ eset. Ha $v = v'$ esetén van v-ből v'-be vezető zárt Euler-vonal, akkor a gráf minden csúcsa páros fokú, és ha a gráf összefüggő, akkor ez a szükséges feltétel elégséges is.

Az általános eset hasonlóan bizonyítható. Kiválasztva két különböző páratlan fokú csúcsot és egy, az egyikből a másikba vezető utat, a felhasznált éleket törölve, a gráf minden csúcsának fokszáma páros számmal csökken, kivéve a kezdőpontot és a végpontot. A gráf ugyan nem biztos, hogy összefüggő marad, de ha egy komponensben marad páratlan fokú csúcs, akkor nem marad egyedül, mert a páratlan fokú csúcsból elindulva, és csupa különböző éleken sétálva, csak egy páratlan fokú csúcsban akadhatunk el. Végül, azokat a legalább egy élt tartalmazó komponenseket, amelyekben nem maradt páratlan fokú csúcs, bejárhatjuk egy zárt vonallal, és ezt hozzávehetjük valamelyik vonalhoz, amivel van közös pontja. □

>

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 eddig 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. Induljunk el ebből a csúcsból egy fel nem használt élen, és haladjunk mindig fel nem használt éleken. Mivel minden csúcsra páros sok fel nem használt él illeszkedik, a továbbhaladás csak akkor nem 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 kapnunk.

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. □

- 107/1 :

<

Kruskal algoritmusa. *Egy (φ, E, V, w) élsúlyozott 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.*

Bizonyítás. Világos, hogy a kiválasztott élek egy F feszítőfát adnak. Tegyük fel,

>

Mohó algoritmus minimális feszítőerdő konstrukciójára. *Egy élsúlyozott véges (φ, E, V, w) gráfban az összes csúcsot tartalmazó üres részgráfból indulva, és a már kiválasztott részgráfhoz amíg lehet hozzáadva egy minimális súlyú olyan élt, amellyel a kiválasztott részgráf még nem tartalmaz kört, egy minimális súlyú feszítőerdőt kapunk.*

Az algoritmus általában Kruskal algoritmusa néven ismeretes, bár Borůvka egy jóval előbb felfedezett és a moráviai villamoshálózat megtervezésére használt általánosabb de bonyolultabb algoritmusának a speciális esete. Felhasználható adatok csoportosítására, úgynevezett klaszterezésre is, ha egy adott súlyhatár feletti éleket nem használunk fel.

Bizonyítás. Elég egy komponensre szorítkozni. Világos, hogy a kiválasztott élek egy F feszítőfát adnak. Tegyük fel,

- 107/$-7 \ldots -1$:

<

Megjegyzés. Kruskal algoritmusa példa úgynevezett *mohó algoritmus*ra: minden lépésben a lehetséges lehetőségek közül az adott lépésben lehető legkedvezőbbet választjuk. A mohó algoritmusok nem mindig optimálisak, például könnyű példát adni olyan 4 csúcspontú teljes gráfra, amelyben a mohó algoritmus nem adja meg a minimális súlyú Hamilton-kört, ahogy az a ábrán látható.

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 Appel és Haken amerikai matematikusok bizonyították be a sejtést. Ez volt az első nevezetes matematikai probléma, amelynek bizonyításához számítógépet is használtak.

$>$

Mohó algoritmusok. Kruskal algoritmusa példa úgynevezett *mohó algoritmus*ra: minden lépésben a lehetséges lehetőségek közül az adott lépésben lehető legkedvezőbbet választjuk. A mohó algoritmusok nem mindig optimálisak. Még a Hamilton-kör keresésénél is nehezebb probléma az *utazó ügynök problémája*: véges, összefüggő, élsúlyozott gráfban a minimális összsúlyú Hamilton-kör megtalálására (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 mindig valamelyik végén egy minimális súlyú éllel hosszabbítja meg, már egy 4 csúcspontú teljes gráfban sem feltétlenül találja meg a minimális súlyú Hamilton-kört, ahogy az a ábrán látható.

- 108/12 :

$<$

niálva. Mindazokat a fogalmakat, amelyeket irányítatlan gráfokra definiáltunk, használni

$>$

niálva. Mindazokat a fogalmakat, amelyeket irányítatlan gráfokra definiáltunk — ideértve a címkézést, súlyozást, stb. is — használni

- 108/−13 :

$<$

*huzamos élek*ről beszélünk.

$>$

*huzamos élek*ről beszélünk.

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.

- 108/−5 :

$<$

hiszen minden újabb él mindhárom összeget eggyel növeli.

$>$

hiszen minden újabb él mindhárom összeget eggyel növeli.

Példák. Egy $\vec{C}_n$ *irányított ciklus* csúcsai az n-edik egységgyökök, ahol irányított él megy minden egységgyökből a következőbe (ciklikusan). A $\vec{P}_n$ *irányított ösvény* $\vec{C}_{n+1}$-ből az 1-be vivő él törlésével adódik. Az $\vec{S}_n$ *irányított csillag*ban az n-edik egységgyökökből visz irányított él a nullába. A $\vec{K}_n$ gráfban minden csúcsból minden tőle különböző csúcsba visz irányított él (ez nem K_n irányítása, ha $n > 1$). Lásd a ábrát.

- $108/-1$:

$<$

Ezt már használtuk is a relációknál.

$>$

Ezt már használtuk is a relációknál.

Véges gráfok éllistás ábrázolása. Legyen (ψ, E, V) egy irányított gráf. A csúcsok beolvasásakor minden csúcsnak adunk egy sorszámot, és egy táblázatban (célszerűen egy hashtáblában) eltároljuk ezt a sorszámozást. Minden csúcshoz felépítjük azon élek listáját, amelyeknek ez a csúcs a kezdőpontja: a ψ leképezés olvasásakor, ha az $\big(e, (v, v')\big)$ 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 járulékos információkat, például a csúcsok illetve élek nevét, cimkéket, stb. is a csúcshoz illetve az élhez fűzhetünk. Sok gráfalgoritmus kényelmesen megvalósítható az éllistás ábrázolással. Például a gráf megfordítását úgy kaphatjuk, hogy az éllistákat végigolvasva, felépítjük a megfordítás éllistás ábrázolását.

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.

- $109/-11$:

$<$

egymástól különbözik.

Erős összefüggőség. Egy irányított gráfot *erősen összefüggő*nek nevezünk, ha bármely (v, v') csúcspár esetén vezet irányított séta v-ből v'-be. Ez nyilván azzal ekvivalens, hogy bármely (v, v') csúcspár esetén vezet irányított út v-ből v'-be. Nyilván

$>$

egymástól különbözik.

Az, hogy v-ből vezet irányított séta v'-be, nyilván azzal ekvivalens, hogy v-ből v'-be vezet irányított út. Ez a reláció nyilván 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 algoritmus 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 mindig eggyel csökkentve. Ha valamelyik csúcs befoka nulla lesz, akkor a sor végére tesszük, eggyel növelve m-et. végül legyen $i \leftarrow i + 1$, és menjünk (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. Így a megfelelő szigorú reláció nem irreflexív, tehát van irányított kör. $\square$

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

- 110/1 :

<

Irányított fák. Egy irányított gráfot *irányított fá*nak nevezünk, ha fa, és van olyan csúcsa, amelyből minden csúcshoz vezet irányított út. Ez a csúcs nyilván egyértelműen meghatározott, ez az irányított fa *gyöke*re. (Vannak, akik irányított fán az általunk definiált irányított fa megfordítását értik: ilyenkor a gyökérhez vezet minden csúcsból irányított út.) Irányított fában a gyökértől nyilván csak egy út vezet minden csúcshoz. Ebből következik, hogy minden, a gyökértől különböző csúcs befoka egy. Azok a csúcsok, amelyekhez n hosszú út vezet a gyökértől, alkotják az n-edik *szint*et.

>

Irányított fák. Az *irányított fa* olyan irányított gráf, amely fa, és van egy csúcsa, amelynek a befoka 0, az összes többi csúcs befoka 1. Azt a csúcsot, amelynek befoka 0, *gyökér*nek nevezzük. (Vannak, akik irányított fán az általunk definiált irányított fa megfordítását értik: ilyenkor a gyökér kifoka 0, minden más csúcs kifoka 1.) Az út hossza szerinti indukcióval adódik, hogy a gyökérből bármely adott csúcsba vezető egyetlen út egyben irányított út is; ennek hossza az adott csúcs *szint*je.

- 110/1 :

<

amelyek kifoka nulla, *levél*nek nevezzük.

>

amelyek kifoka nulla, *levél*nek nevezzük.

Ha egy irányítatlan fában kijelölünk egy csúcsot, akkor *gyökeres fá*ról beszélünk. Gyökeres fának egy és csak egy irányítása van, amellyel irányított fa lesz úgy, hogy a kijelölt csúcs a a gyökér: a kijelölt csúcsból egy másik adott csúcsba vezető egyetlen út utolsó éle legyen az adott csúcshoz tartozó egyetlen bemenő él. Így a gyökér kijelölése ekvivalens az irányítás megadásával.

Egy *q-ad rendű fa* egy olyan élcímkézett irányított fa, amelyben minden él címkéje egy q-nál kisebb természetes szám, és minden csúcsra a kimenő élek címkéi különböznek. Legfontosabbak a *bináris fák*: itt 0 vagy 1 helyett bal illetve jobb kimenő élről, bal illetve jobb gyerekről, stb. beszélünk. Megjegyezzük, hogy két q-ad rendű fát akkor is különbözőnek tekintünk, ha csak a címkézésben 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: a gyökér alatt vannak a gyermekei, stb.

* **Kupac.** Legyen $q \in \mathbb{N}$, $q \geq 2$. Egy q-alapú *q-alapú kupac* rendezett halmazból vett rekordoknak egy $R_0, R_1, \ldots, R_{n-1}$ sorozata, amelyre teljesül a *kupac tulajdonság*: ha $0 \leq i < j < n$ és $i = \lfloor (j-1)/q \rfloor$, akkor $R_i \leq R_j$. A kupac úgy is felfogható, mint egy irányított fa, amelyben az R_i csúcsnak legfeljebb q gyermeke van: az R_j rekordok, ahol $j = qi+1, qi+2, \ldots, qi+q$ és $j < n$; a kupac tulajdonság azt jelenti, hogy a szülő sohasem nagyobb, mint a gyermeke. Így a kupacban a R_0 gyökérnél nincs kisebb rekord. Ezért alkalmas a kupac úgynevezett *elsőbbségi sorok* kezelésére, amelyekben mindig a legkisebb elemre van szükségünk, mint soron következőre.

Ha $R_0, R_1, \ldots, R_{n-2}$ már kupac, és új rekordot akarunk a kupachoz adni, akkor azt a sorozat végére tesszük, majd ha kisebb, mint a szülője, megcseréljük vele, és ezt folytatjuk, míg a kupac tulajdonság helyreáll. Néha elsőbbségi soroknál egy rekord megváltozik, és kisebb lesz, mint volt: ekkor is a fent leírt lépés ismétlésével állíthatjuk helyre a kupac tulajdonságot.

A legfontosabb kupac művelet a „süllyesztés". Ezt alkalmazzuk például, ha egy rekord megváltozik, nagyobb lesz. Tegyük fel, hogy az R_i rekord gyermekeihez tartozó részfákra teljesül a kupac tulajdonság, és azt akarjuk elérni, hogy az R_i-hez tartozó részfára is teljesüljön. Legyen R_j az R_i gyermekei közül a legkisebb. Ha ez nem kisebb, mint R_i, akkor készen vagyunk. Ha kisebb, akkor cseréljük meg R_i-t és R_j-t: az R_i „egy szinttel lesüllyedt". Folytassuk a süllyesztést az új R_j-vel.

A süllyesztés segítségével könnyű az R_0 rekordot kicserélni egy új rekordra: R_0 helyére tesszük az új rekordot, majd süllyesztjük. Hasonlóan, ha az $R_0, R_1, \ldots, R_n$ kupacból el akarjuk venni R_0-at, akkor R_n-et a helyére tesszük, majd „süllyesztjük". Ha tetszőleges másik rekordot akarjuk elvenni, akkor úgy tekintjük, mintha lecsökkent volna minden más rekordnál kisebbre, így R_0 helyére kerül, és el tudjuk venni. Egy $R_0, R_1, \ldots, R_{n-1}$ sorozatból úgy építhetünk kupacot, hogy az utolsóval kezdve a rekordokat sorra „süllyesztjük".

Leggyakrabban a $q = 2$ esetet használjuk, ekkor *bináris kupac*ról beszélünk. A $q > 2$ esetnek csak akkor van jelentősége, ha a rekordok gyakran csökkennek, mert ha q nagy, ez a művelet olcsó. Bináris kupacnál célszerű a sorozatot 1-től indexelni, mert $i' = i+1$, $j' = j+1$ jelöléssel a $i = \lfloor (j-1)/q \rfloor$ összefüggés megfelelője $i' = i+1 = 1 + \lfloor (j-1)/q \rfloor =$

$\lfloor j'/2 \rfloor$. Az alábbi példa a kupacépítést mutatja bináris kupacra, betűkkel.

```
      ↓     ↓
 buildingheap

     ↓    ↓↓
 buildingheap

    ↓   ↓↓
 builainghedp

   ↓  ↓↓
 buigainlhedp

  ↓ ↓↓
 buigainlhedp

     ↓    ↓↓
 baiguinlhedp

 ↓↓↓
 baigdinlheup

  ↓ ↓↓
 abigdinlheup

↓
 abigdinlheup
```

* **Kupacrendezés.** A kupacstruktúra felhasználható rendezett halmazból vett rekordok egy sorozatának a rendezésére. Először építsünk kupacot. Ezután a legkisebb rekordot elvéve, csökkentsük eggyel a kupacot, és tegyük a legkisebb rekordot a felszabaduló helyre, a többi mögé. Ezt a lépés ismételve mindaddig, amíg a kupac el nem fogy, a kapott rekordsorozat monoton csökkenő. Ha monoton növekvő sorozatot akarunk, akkor megfordítjuk az egyenlőtlenségeket.

A kupacrendezés felhasználható külső tárban lévő rekordsorozat rendezésére is. Az első fázisban megtöltjük a belső tárat rekordokkal, kupacot építünk, majd kivisszük a legkisebb rekordot, és beolvasunk egy új rekordot. Ha az új rekord nem kisebb, mint a kivitt rekord, akkor a kupacba kerül, ha kisebb, akkor a kupac eggyel csökken, és az új rekord a kupac mögé kerül. Amikor a kupac elfogyott, elkészült egy „menet". A bent lévő rekordokból kupacot építve, új menetet kezdünk, egészen addig, amíg a bemenet el nem fogy.

A második fázis a menetek „összefésülésével" növeli azok méretét. Jónéhány menetet megnyitva, mindegyikből beolvassuk az első rekordot és kupacot építünk. A legkisebb rekord kivitele után ugyanabból a menetből, amiből ez származott, olvasunk a helyére egy másikat, mindaddig, amíg minden megnyitott menet elfogy. A menetek számát — mindíg a rövidebb menetek összefésülésével — egyre csökkentjük: ez a rendezett kimenet.

Gyakran a rekordok nagyok, mozgatásuk időigényes (vagy bonyolult, mert nem egyforma hosszúak). Ekkor a kupacot csak a kulcsaikból építjük, a kulcshoz hozzátéve a rekord címét, de lehet csak a címekből épiteni a kupacot.

* **B-fa.** Rekordok rendezett halmazból vett kulcsainak mágneslemezen való tárolására szolgáló struktúra. Egy *q-ad rendű B-fa* egy adattábla rekordjainak kulcsaiból épített q-adrendű irányított fa ($q \geq 3$), amelyben a gyökér és a levelek kivételével minden csúcsnak legalább $q/2$ gyermeke van, és a levelek mind ugyanazon a szinten vannak. Ha egy csúcsnak $k+1$ gyermeke van, akkor k kulcsot is tartalmaz, a következő elrendezésben:

$$P_0, K_1, P_1, K_2, \ldots, P_{k-1}, K_k, P_k.$$

Itt $K_1 < K_2 < \ldots < K_k$ kulcsok, P_i pedig egy mutató (pointer) azaz egy abszolút vagy relatív cím, amely egy olyan részfára mutat, amelyben szereplő kulcsok szigorúan K_i és K_{i+1} közé esnek. A levelekben nincs információ, így azokra mindre a NULL mutató fog mutatni. Ugyancsak NULL mutató van a további mutatók helyén. Célszerűen minden csúcs egy szektort foglal el a lemezen, így egyben olvasható vagy írható. (A „kulcs" tartalmazhat egy további mutatót is, amely a hozzá tartozó rekordra mutat.) Lásd a ábrát.

A keresés nyilvánvaló. Új kulcs beszúrásához megkeressük a „helyét" a legalsó szinten, és oda szúrjuk be; probléma csak akkor van, ha az adott szektorban ez lenne a q-adik kulcs. Ekkor a szektort „kettévágjuk", a „középső" kulcsot egy szinttel feljebb szúrjuk be, a maradékot pedig két szektorba tesszük, a „középső" kulcsnál kisebb kulcsokat az egyikbe, a nagyobbakat a másikba. A törlés sem sokkal bonyolultabb.

* **Oszd meg és uralkodj.** Az előző két példa, a kupacrendezés és a B-fa tipikus példa az „oszd meg és uralkodj" elv alkalmazására: a feladatot kisebb részekre bontjuk, majd még kisebbekre, stb., amelyek úgy épülnek egymásra mint egy irányított fa szintjei.

Dijkstra módszere. *A (ψ, E, V, w) véges súlyozott irányított gráfra tegyük fel, hogy az élsúlyok pozitívak, $s \in V$ és $T \subset V$. Az alábbi algoritmus a csúcshalmazon értelmez egy $d : V \to \overline{\mathbb{R}}$ függvényt, amely $t \in T$ esetén az adott s csúcsból 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 irányított sétának, 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 $W \geq d(t)$. 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 előtti csúcsa, e pedig az utolsó éle. Mivel $t' \in S$, az s-től t'-ig vezető részséta súlya legalább $d(t')$, így a teljes séta súlya legalább $d(t') + w(e)$, és amikor t'-t bevettük S-be, legfeljebb ennyire állítottuk $d(v)$ értékét, azóta pedig csak csökkenhetett. $\square$

Megjegyzés. Az előző algoritmus könnyen módosítható úgy, hogy egy, az s-ből t-be vezető minimális összsúlyú sétát is megkapjunk: amikor $d(v)$ értékét 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 $d(t) + w(e) \leq d(v)$, akkor e-vel bővítjük a listát, ha pedig $d(t) + w(e) < d(v)$, akkor töröljük, és beletesszük e-t. Természetesen 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 — az előző pont jelöléseivel — 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 felladatot. Ezt a megoldási módszert nevezik *dinamikus programozás*nak.

* **Feladat [7].** Bináris kupac és éllistás ábrázolás segítségével írjunk hatékony algoritmust Dijsktra módszerére.

* **Szélességi bejárás.** Dijkstra módszere arra is felhasználható, hogy egy véges irányított gráfban keressünk egy irányított fákból álló erdőt, amelyben minden fában a gyökérből az eredeti gráfban az adott csúcsba vezető legrövidebb irányított út szerepel: Minden él súlyát tekintsük 1-nek. Választva egy tetszőleges csúcsot, alkalmazzuk Dijkstra módszerét. Ha maradt még csúcs, a maradék csúcsokra újra alkalmazzuk a módszert, stb.

Észrevehetjük, hogy most a Dijkstra módszerénél szereplő H halmazban lévő csúcsok súlya legfeljebb kétféle lehet, a csúcsok súlya soha nem csökken, és az újonnan bekerülő csúcsok súlya a nagyobbik súly. Ez azt jelenti, hogy a H halmaz elemeit tarthatjuk egy sorban, amelynek a végére tesszük az új belépőket, és az elejéről léptetünk át az S halmazba.

Azt is észrevehetjük, hogy ha irányítatlan gráf éllistás ábrázolására alkalmazzuk a módszert, a feszítő erdő fái az eredeti gráf egy feszítő erdejét adják.

* **Mélységi bejárás.** A szélességi bejárást módosítsuk úgy, hogy amikor kiveszünk egy csúcsot a H sorból, a szomszédait betesszük a sorba, de az újonnan belépő csúcsokat nem a sor végére tesszük, hanem az elejére (a már bentlévőket kihagyjuk). Itt a csúcsok nem súlyt kapnak, hanem két sorszámot. Az első a *bejárási szám*, ez azt mondja meg, hogy az adott csúcs hanyadikként került be a H halmazba, a második a *befejezési szám*, ez azt mondja meg, hogy az adott csúcs hanyadikként került át az S halmazba. Induláskor minden csúcsnak mindkét száma nulla. A bejárási és befejezési számok egyrészt mutatják, hogy egy csúcs melyik halmazban van, másrész más algoritmusok használják őket.

* **PERT.** Egy nagy feladat részekre bontásának és a részfeladatok ütemezésének módszere a PERT (Program Evaluation and Review Technique). A részfeladatok egy irányított gráf éleinek felelnek meg, amelyek súlya a részfeladat elvégzésének ideje. A csúcsok állapotoknak felelnek meg: a csúcsba befutó éleknek megfelelő részmunkáknak be kell fejeződnie, mielőtt a csúcsból kifutó éleknek megfelelő részmunkák megkezdődhetnek. Az egész munka az s start állapotból indul, és a t terminál állapotban fejeződik be. A gráf nem tartalmazhat irányított kört, s befoka és t kifoka nulla, és minden v csúcsba rajta van valamely s-ből t-be vezető irányított úton. A minimális befejezési időtartamot a maximális összsúlyú s-ből t-be vezető irányított út összsúlya adja. Ezt az utat (vagy az ilyen utakat) *kritikus út*nak nevezzük, a kritikus utakon fekvő csúcsok illetve élek pedig a *kritikus csúcs*ok illetve *kritikus él*ek: ezek késlekedése az egész munka befejezésének késlekedését jelenti. Bár a hasonló feladatok általában nehezek, segít az, hogy a gráf nem tartalmaz irányított kört. Az egyes csúcsok elérésének legkorábbi időpontjai meghatározhatók, ha a csúcsokat megszámozzuk egy topologikus rendezésnek megfelelő sorrendben. Legyen $d(s) = d(1) = 0$ és $i = 2, 3, \ldots, n$-re legyen

$$d(i) = \min\big\{d(j) + w(e) : e \in E^+(i), \psi(e) = (j, i)\big\}.$$

Ugyanúgy, mint Dijkstra módszerénél, nyomonkövethetjük a kritikus utakat is.

* **Folyamprobléma.** Egy $G = (\psi, E, V)$ véges irányított gráfot két kijelölt pontjával, az s *start*al és a t *cél*lal (terminál), $s \neq t$, valamint egy $c : E \to \mathbb{R}^+$ élsúlyozással *hálózat*nak nevezünk. A c függvény jelentése az egyes élek szállítási *kapacitás*a (időegység alatt).

Tetszőleges $S \subset V$ esetén jelölje $E(S)$ azokat az éleket, amelyek S és $V \setminus S$ között futnak. Ezek közül jelölje $E^+(S)$ azon élek halmazát, amelyek kezdőpontja S-ben van, $E^-(S)$ pedig azon élek halmazát, amelyeknek a végpontja van S-ben.

Egy hálózatot egy újabb $f : E \to \mathbb{R}$ élsúlyozással *folyam*nak nevezünk, ha minden $s \neq v \neq t$ pont esetén teljesül az $\sum_{e \in E^+(v)} f(e) = \sum_{e \in E^-(v)} f(e)$ *megmaradási feltétel* és tetszőleges e él esetén teljesül a $0 \leq f(e) \leq c(e)$ *kapacitásfeltétel*. Az f függvény jelentése az egyes éleken (időegység alatt) szállított mennyiség. A folyam *érték*e $\|f\| = \sum_{e \in E^-(t)} f(e) - \sum_{e \in E^+(t)} f(e)$, a t-be (időegység alatt) beérkező mennyiség. Tetszőleges hálózat esetén az azonosan nulla f egy folyam. Célunk maximális értékű folyam keresése. Ha egy folyamban egy élre $f(e) = c(e)$, akkor az élt *telített él*nek nevezzük. ha egy folyamban minden s-ből t-be vezető úton van telített él, akkor azt mondjuk, hogy a folyam *blokkoló folyam*. Az alábbi ábra példát ad blokkoló folyamra, amely nem maximális folyam.

Ha (G, s, t, c, f) egy folyam, ahol $G = (\psi, E, V)$, definiáljuk a folyamhoz tartozó *javító hálózat*ot: a csúcsok halmaza ugyancsak V, és minden $e \in E$-hez az új G_f gráfban két él tartozhat: ha $f(e) < c(e)$, akkor a G_f-ben szerepel egy e^+ él, amelyek kezdőpontja és végpontja ugyanaz, mint e-nek, de kapacitása $c_f(e^+) = c(e) - f(e)$, ha pedig $f(e) > 0$, akkor szerepel egy e^- él, amelynek kezdőpontja e végpontja, végpontja e kezdőpontja, és $c_f(e^-) = f(e)$. Vegyük észre, hogy ha a javító hálózaton van egy pozitív értékű $g : E_f \to \mathbb{R}$ folyam, akkor $h(e) = f(e) + g(e^+) - g(e^-)$ egy olyan folyam a (G, s, t, c) hálózaton, amelynek értéke $\|h\| = \|f\| + \|g\| > \|f\|$. Javító folyamot már akkor tudunk konstruálni, ha találunk egy *javító utat*, ami egyszerűen egy irányított út G_f-ben s-ből t-be: legyen az irányított út minden e^* élére $g(e^*) = c$, ahol c a $c(e^*)$ értékek minimuma az útban szereplő e^* élekre, minden más $e^* \in E_f$-re pedig legyen $g(e^*) = 0$.

A következő lemma mutatja, hogy a folyam értéke $E(S)$ alakú elvágó élhalmazok segítségével számolható, és ezek segítségével a folyam értékére könnyen kiszámolható felső becslést kaphatunk. A következő tétel pedig azt muatja, hogy ez a felső becslés éles.

* **Lemma.** *Az előző definíció jelöléseivel, minden $S \subset V$ halmazra, amelyre $s \in S$ és $t \notin S$, teljesül, hogy $\|f\| = \sum_{e \in E^+(S)} f(e) - \sum_{e \in E^-(S)} f(e)$, és így $\|f\| \le c\big(E^+(S)\big)$.*

Bizonyítás. Az egyenlőség a definícióból következik, ha $S = V \setminus \{t\}$, és ha teljesül S-re, akkor bármely $v \in S$, $v \neq s$ esetén $S \setminus \{v\}$-re is, mert v eltávolításakor az összeg $\sum_{e \in E^+(v)} f(e)$-vel csökken, és $\sum_{e \in E^-(v)} f(e)$-vel nő, de a megmaradási feltétel szerint a két mennyiség ugyanaz. Az egyenlőségből a felső becslés nyilvánvaló:

$$\|f\| = \sum_{e \in E^+(S)} f(e) - \sum_{e \in E^-(S)} f(e) \le \sum_{e \in E^+(S)} f(e) \le c\big(E^+(S)\big).$$

* **Ford–Fulkerson-tétel.** *Az előző definíció jelöléseivel az alábbiak ekvivalensek:*

(1) *f maximális értékű folyam;*

(2) *f-hez nem létezik javító út;*

(3) *létezik olyan $S \subset V$, amelyre $s \in S$, $t \notin S$, és $c\big(E^+(S)\big) = \|f\|$.*

Bizonyítás. Az nyilvánvaló, hogy (1)-ből következik (2). Ha (2) teljesül, akkor legyen S azon pontok halmaza, amelyekek irányított üton elérhetők G_f-ben. Nyilván $s \in S$, és mivel nincs javító út, $t \notin S$. Minden $e \in E^+(S)$-re $f(e) = c(e)$ és minden $e \in E^-(S)$-re $f(e) = 0$, hiszen egyébként $V \setminus S$ egy pontja is elérhető lenne G_f-ben irányított úton. Ekkor viszont az előző lemmából $\|f\| \le c\big(E^+(S)\big)$. Végül az előző lemma szerint bármely folyam értéke legfeljebb $c\big(E^+(S)\big)$ lehet, így ha (3) teljesül, akkor $\|f\|$ maximális.

* **Edmonds–Karp-heurisztika.** Az előző tétel alapján még nem világos, hogyan érdemes a javító utakat választnai, sőt, még azt sem láttuk be, hogy létezik maximális folyam. Az is előfordulhat, hogy „gondatlanul” választva a javító utakat, a növekvő folyamérték konvergál egy értékhez, de ez kisebb, mint a maximális folyam értéke. Megmutatható, hogy ha mindig a legkevesebb élből álló javító utak közül választunk, akkor a javító utak élszámai monoton növekedő sorozatot alkotnak, és egy élszám legfeljebb $\natural(E)$-szer fordulhat elő. Mivel a javító út élszáma maximum $\natural(V) - 1$ lehet, az eljárás véges sok lépésben véget ér. Ez az *Edmonds–Karp-heurisztika*.

* **Dinicódszere.** Az előző pontban leírtnál is jobb taktika egy lépésben nem csak javító utat, hanem blokkoló folyamot keresni a javító hálózatban, pontosabban egy részében. Nevezzük egy v csúcs szintjének a javító hálózatban az s-ből a v csúcsba vezető legrövidebb út élszámát. A szintek az s-ből kiinduló mélységi kereséssel könnyen meghatározhatók. Ha t-be nem vezet a javító hálózatban irányított út, akkor készen vagyunk,

nincs javító út. Egyébként legyen t szintja k. Dobjunk ki a javító hálózatból minden olyan élt, amely nem „előre megy”, azaz amely nem egy magasabb (nyilván csak eggyel magasabb) szinten lévő csúcsba visz. A megmaradó H hálózat nem tartalmaz irányított kört. Ha ebben a hálózatban sikerül egy g blokkoló folyamot találni, akkor azt hozzáadva f-hez, az $f+g$-hez tartozó javító hálózatban k-nál magasabb szinten lesz a t, mert minden s-ből t-be vezető k hosszúságú úton legalább egy él kritikussá válik, így törlődik a javító hálózatból; keletkeznek ugyan új élek, de ezek mind visszafelé, alacsonyabb szinten lévő csúcsokba visznek. Mivel t legfeljebb az $\natural(V)-1$-edik szinten lehet, véges sok lépésben véget ér az eljárás, egyúttal azt is bizonyítva, hogy van maximális folyam.

A H hálózatban az azonosan nulla g folyamból kiindulva a következő három lépés felhasználásával keresünk blokkoló folyamot:

(1) „Nyomulás”: egy s-ből t-be vezető irányított utat építünk. Az út utolsó pontjából kimenő valamelyik élen tovább haladunk egy még be nem járt pontba, addíg, amíg t-be nem érünk, vagy el nem akadunk. Ha már el sem tudunk indulni s-ből, akkor készen vagyunk.

(2) „Növelés”: ha t-be értünk, akkor találtunk egy növelő utat. A g folyamot az út mentén megnöveljük a növelő út legkisebb kapacitású élének kapacitásával, az út mentén a kapacitásokat ennyivel csökkentjük, és a kritikussá vált éleket töröljük, majd a „nyomulással” folytatjuk.

(3) „Takarítás”: erre akkor kerül sor, ha a „nyomulás” egy v csúcsnál elakadt. Ekkor töröljük a v-be menő éleket, eggyel visszalépünk, és onnan próbálkozunk a ..nyomulással”.

Az algoritmus véget ér, mert minden „növelés” illetve „takarítás” elfogyaszt egy élt, így ezek száma O'sszesen legfeljebb $\natural(E)$ lehet. Ugyanennyi lehet a ‚nyomulások” száma is, mert mindegyik után „növelés” vagy „takarítás” következik. Nyilvánvaló, hogy az algoritmus egy blokkoló folyamot talál H-ban.

- 112/3 :

<

°* **Megjegyzés.** Az előző „bizonyítás” kihagyott részeinek pontos igazolása

>

°* **Megjegyzés.** Euler tételéből levezethető, hogy az öt szögpontú teljes gráf nem síkba rajzolható: 7 tartományt 10 él határolna, így mivel minden él két tartomány közös határa, tartományonként $20/7<3$ él jutna, ami egyszerű gráfban lehetetlen. Hasonlóan adódik, hogy a „három ház, három kút” gráf sem síkba rajzolható: 5 tartományt 9 él határolna, de a gráf páros, így a tartományoknak legalább 4 oldala van.

Az előző „bizonyítások” és az előző tétel „bizonyítása” kihagyott részeinek pontos igazolása

- 112/14 :

<

* **Gráfok topologikus ekvivalenciája.** A G és G' véges gráfokat *topologi-*

>

Kromatikus szám. 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 Appel és Haken amerikai matematikusok bizonyították be a sejtést. Ez volt az első nevezetes matematikai sejtés, amelynek bizonyításához számítógépet is használtak. Általánosan, egy gráf egy csúcsszínezését *jólszínezés*nek nevezzük, ha a szomszédos csúcsok színe különböző. A gráf *kromatikus szám*a a legkisebb olyan n természetes szám, amelyre a gráf jólszínezhető n színnel; ha nincs ilyen, akkor ∞. Már annak eldöntése is nehéz probléma, hogy egy gráf kromatikus száma három, vagy nem.

* **Gráfok topologikus izomorfizmusa.** A G és G' véges gráfokat *topologi-*

- 114/2 . . . 8 :

  <

  Eddigi tanulmányaink során már számos olyan fogalommal találkoztunk, amely az algebra körébe tartozik. Gondolhatunk például a természetes, illetve egész számok halmazára, amelyeken a szorzás és az összeadás tulajdonságait vizsgáltuk. A számoknál megismert fogalmak jelentős része értelmezhető olyan halmazokon is, amelyek elemei nem számok. Ennek a fejezetnek a fő feladata az, hogy az eddigiekben már értelmezett, a műveletekkel kapcsolatos fogalmakat minél általánosabb körre terjesszük ki, elősegítve azok algebrai módszerekkel történő vizsgálatát.

  >

  Az eddigiekben már számos algebrai fogalommal találkozhattunk: félcsoport, csoport, gyűrű, test, stb. Eddig elsősorban mint egy vagy két művelet tulajdonságait röviden leíró elnevezést használtuk ezeket. Megfigyelhetjük, hogy $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ illetve $\mathbb{H}$ elemeit elsősorban „koordinátázásra” használjuk: míg a természetes számokkal egy megszámlálható halmaz elemeit, a komplex számokkal már a sík pontjait vagy a villamosságtanban impedanciákat, a kvaterniókkal pedig a téridő pontjait vagy robotkarok háromdimenziós forgatásait — az azokon végzett műveletekkel együtt — koordinátázhatjuk. Más tárgyakban is tanulunk hasonló „koordinátázó” matematikai fogalmakat, például lineáris algebrában a lineáris egyenletrendszerek és leképezések jellemzésére alkalmas mátrixokat, analízisben függvényeket, de már középiskolában is görbéket algebrai egyenletek segítségével jellemeztünk.

  Az algebra célja ilyen „koordinátázó” matematikai struktúrák — egy vagy több művelettel ellátott halmazok — általános vizsgálata. Ezek egy művelet esetén rendszerint csoportok, vagy legalábbis félcsoportok, két művelet esetén pedig gyűrűk. Fontos szerepet játszanak a művelettartó leképezések, elsősorban a reprezentációk: ezek értékkészlete valamely függvényhalmaz, például permutációk vagy lineáris leképezések. A vizsgált struktúra képe művelettartó leképezésnél úgy tekinthető, mint az eredeti struktúra egy közelítése, és csoportoknál megfelel egy faktorcsoportnak, gyűrűknél pedig egy faktorgyűrűnek; ezek a maradékosztályok általánosításai. „Elég sok” ilyen közelítést ismerve, az eredeti struktúrát megismerhetjük vagy dolgozhatunk benne. Ez a gondolat számos algoritmus alapja is. A tárgyalás elvezet bennünket a véges testek megismeréséhez, amelyek polinomokkal koordinátázhatók, és fontos alkalmazásaik vannak a rejtjelzésben és a kódoláselméletben.

- 115/$-5\ldots-2$:

$<$

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

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

$>$

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

- $116/{-18}$:

$<$

A következő állításból láthatjuk, hogy a csoport fogalmának négy különböző definí-

$>$

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 *reprezentáció*járól, magyarul *ábrázolás*áról beszélünk. Ha a reprezentáció izomorfizmus, akkor *hű reprezentáció*ról beszélünk. (Ha X véges halmaz, akkor elemeit megfeleltetve egy lineáris tér bázisának, X önmagába való leképezéseinek egy lineáris tér transzformációi felelnek meg, így véges halmaz feletti reprezentációból könnyen kaphatunk lineáris leképezésekkel való reprezentációt.)

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

$$\varphi(gh)(x) = ghx = \varphi(g)(hx) = \big(\varphi(g) \circ \varphi(h)\big)(x), \quad \text{ha} \quad x \in X.$$

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 reprezentáció*jának nevezzük.

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

A következő állításból láthatjuk, hogy a csoport fogalmának több különböző definí-

- $116/{-16} \ldots -1$:

$<$

Tétel. *Ha G egy félcsoport, akkor az alábbi feltételek ekvivalensek:*

(1) *létezik G-ben egy e jobb oldali egységelem, és minden $a \in G$ elemhez létezik olyan a^* elem, amelyre $aa^* = e$;*

(2) *G csoport;*

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

(4) *$G \neq \emptyset$ 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. Megmutatjuk, hogy (1)-ből következik (2). Legyen a tetszőleges eleme G-nek, a^* pedig olyan, amelyre $aa^* = e$, és legyen b olyan, amelyre $a^*b = e$. Ekkor egyrészt

$$a^*aa^*b = a^*a(a^*b) = a^*ae = a^*a,$$

másrészt

$$a^*aa^*b = a^*(aa^*)b = a^*eb = a^*b = e.$$

Ezzel beláttuk, hogy $a^*a = aa^* = e$. Mivel egyrészt $aa^*a = a(a^*a) = ae = a$, másrészt $aa^*a = (aa^*)a = ea$, azt kapjuk, hogy $ea = a$, azaz e egységelem is, és így a^* az a inverze.

$>$

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 könnyen 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. Nyilván (2)-ből következik (3).

- 117/1 ... 9 :

$<$

(2)-ből könnyen következik (3), 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. Nyilván (3)-ból következik (4).

Belátjuk, hogy (4)-ből 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. Nyilván minden $b \in G$-hez létezik olyan b^*, amelyre $bb^* = e$, mert a $bx = e$ egyenlet megoldható. $\square$

$>$

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. Hasonlóan következik bal oldali egységelem létezése is, így van egységelem. Nyilván minden $b \in G$-hez létezik olyan b^*, amelyre $bb^* = e$, mert a $bx = e$ egyenlet megoldható. Hasonlóan, van balinverz is. $\square$

- $117/15$:

  $<$

  Bizonyítás. A (3)-beli egyértelműségből következik. $\square$

  $>$

  Bizonyítás. A (2)-beli egyértelműségből következik. $\square$

- $117/-12$:

  $<$

táblázattal megadott művelet invertálható, mégsem kapunk csoportot, mert a művelet

  $>$

táblázattal megadott műveletre elvégezhető az osztás, mégsem kapunk csoportot, mert a művelet

- $117/-18\ldots-14$:

  $<$

Részcsoport. Egy G csoport egy H részhalmazát *részcsoport*nak nevezzük, ha maga is csoport a G-beli műveletet csak H elemei között tekintve. (Szokás ennek kifejezésére a $H \leq G$ jelölést használni.) Nyilván az egész G és a csak az egységelemet tartalmazó egyelemű részhalmaz részcsoportok, ezek a *triviális részcsoport*ok. A G-től különböző részcsoportokat *valódi részcsoport*nak nevezzük.

  $>$

Részfélcsoport, 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 *részfélcsoport*nak, *részcsoport*nak, stb. nevezzük. Számunkra legfontosabb az az eset lesz, amikor H récscsoportja a G csoportnak. (Szokás ennek kifejezésére a $H \leq G$ jelölést használni.) Nyilván ha G csoport, akkor az egész G és a csak az egységelemet tartalmazó egyelemű részhalmaz részcsoportok, ezek a *triviális részcsoport*ok. A G-től különböző részcsoportokat *valódi részcsoport*nak nevezzük.

- $119/-14$:

  $<$

tor***á***nak.

  $>$

torának.

$^{\circ *}$ **Példa: lineáris transzformációk csoportjai.** Egy F testre F^n invertálható lineáris transzformációinak csoportját $\mathbb{GL}(F^n)$ fogja jelölni, ez az *általános lineáris csoport*. A lineáris algebrában bizonyítják, hogy ennek elemeit az jellemzi, hogy determinánsuk nem nulla, és hogy $\mathbb{GL}(F^n)$ izomorf az F-beli elemű $n \times n$-es nem nulla determinánsú mátrixok multiplikatív csoportjával. Az 1 determinánsú lineáris transzformációk $\mathbb{GL}(F^n)$ egy részcsoportját alkotják, ez az $\mathbb{SL}(F^n)$ *speciális lineáris csoport*.

Az $F = \mathbb{C}$ esetben tekinthetjük $\mathbb{GL}(\mathbb{C}^n)$ azon lineáris transzformációinak részcsoportját, amelyek megtartják $\mathbb{C}^n$ elemeinek szokásos hosszát, ez az $\mathbb{U}(n)$ *unitér csoport*.

Elemeinek determinánsa 1 abszolút értékű. Mátrixukat ortonormált bázisban az jellemzi, hogy az inverze megegyezik a konjugált transzponáltjával. Az unitér csoportok fontos szerepet játszanak a fizikában. Az $\mathbb{U}(1)$ csoport lényegében $\mathbb{C}$ egységnyi abszolút értékű elemeinek multiplikatív csoportja. További részcsoport $\mathbb{SU}(n) = \mathbb{U}(n) \cap \mathbb{SL}(\mathbb{C}^n)$, a *speciális unitér csoport*.

Hasonlóan, az $F = \mathbb{R}$ esetben tekinthetjük $\mathbb{GL}(\mathbb{R}^n)$ azon lineáris transzformációinak részcsoportját, amelyek megtartják $\mathbb{R}^n$ elemeinek szokásos hosszát, ez az $\mathbb{O}(n)$ *ortogonális csoport*. Elemeinek determinánsa 1 abszolút értékű. Mátrixukat ortonormált bázisban az jellemzi, hogy az inverze megegyezik a transzponáltjával. További részcsoport $\mathbb{SO}(n) = \mathbb{O}(n) \cap \mathbb{SL}(\mathbb{R}^n)$, a *speciális ortogonális csoport*. Elemei $\mathbb{R}^n$ origó körüli forgatásainak felelnek meg: annak, hogy a determináns 1, az a szerepe, hogy a transzformáció nem változtatja meg a bázisok irányítását.

Az egységnyi abszolút értékű kvaterniók a nem nulla kvaterniók multiplikatív csoportjának egy részcsoportját alkotják. Ugyanez a helyzet, ha a kvaterniószorzás helyett a $(q, q') \mapsto q'q$ „fordított szorzást" tekintjük. Egy egységnyi abszolút értékű q kvaternióra tekintsük a $\varphi_q : p \mapsto pq$ leképezését $\mathbb{H} = \mathbb{C}^2$-nek önmagába. Ha $q = (z, w) \in \mathbb{C}^2$, akkor (az $1, j$ bázisban) φ mátrixa

$$\begin{pmatrix} z & -\overline{w} \\ w & \overline{z} \end{pmatrix},$$

ami könnyen láthatóan 1 determinánsú, és inverze megegyezik a konjugált transzponáltjával, így φ_q egy unitér transzformáció. Az $\mathbb{SU}(2)$ csoport minden eleme előáll így: ha mátrixa (az $1, j$ bázisban)

$$\begin{pmatrix} z & u \\ w & v \end{pmatrix},$$

akkor az inverze — felhasználva, hogy determinánsa 1 —

$$\begin{pmatrix} v & -u \\ -w & z \end{pmatrix},$$

amit összehasonlítva a konjugált transzponáltjával, azt kapjuk, hogy $u = -\overline{w}$ és $v = \overline{z}$, valamint — mivel a determináns 1 —, $|z|^2 + |w|^2 = 1$. A $q \mapsto \varphi_q$ leképezés izomorfizmus a fordított szorzással tekintett egységnyi abszolút értékű kvaterniók és $\mathbb{SU}(2)$ között.

Tekintsük most egy egységnyi abszolút értékű q kvaternióra a háromdimenziós vektorokon értelmezett $\psi_q(v) = qvq^-1$ forgatást: lásd a 3.4.34. pontot. Ez homomorfizmusa a fordított szorzással tekintett egységnyi abszolút értékű kvaterniók csoportjának $\mathbb{SO}(3)$-ra, amely a q és $-q$ kvaterniókat (de csak ezeket) ugyanabba a forgatásba viszi. Összerakva az előbbi izomorfizmus inverzével, egy $\varphi_q \mapsto \psi_q$ homomorfizmust kapunk, amely az $\mathbb{SU}(2)$-beli φ_q és $\varphi_{-q} = -\varphi_q$ leképezéseket (de csak ezeket) ugyanabba a forgatásba viszi.

Az $F = \mathbb{R}$ esetben, ha $p + q = n$, tekinthetjük $\mathbb{GL}(\mathbb{R}^n)$ azon lineáris transzformációinak $\mathbb{O}(p, q)$ részcsoportját, amelyek megtartják az

$$(x_1, x_2, \ldots, x_n) \mapsto x_1^2 + x_2^2 + \cdots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \cdots x_{p+q}^2$$

kvadratikus forma értékét; ez a csoport az $\mathbb{O}(n)$ ortogonális csoport általánosítása: a $p = n$, $q = 0$, illetve a $p = 0$, $q = n$ esetben $\mathbb{O}(n)$-et kapjuk vissza. Ennek részcsoportja az $\mathbb{SO}(p,q) = \mathbb{O}(p,q) \cap \mathbb{SL}(\mathbb{R}^n)$ csoport.

A fizikában a relativitáselmélet miatt fontos szerepet játszik az $\mathbb{O}(1,3)$ *Lorentz-csoport*. Mivel a kvaterniók megfelelnek az ($\mathbb{R}$ felett) négydimenziós téridő pontjainak, elemeit olyan $\mathbb{R}$-lineáris invertálható $L : \mathbb{H} \to \mathbb{H}$ leképezéseknek is tekinthetjük, amelyekre $\Re(p^2) = \Re\big(L(p)^2\big)$ minden $p \in \mathbb{H}$-ra. Az $\mathbb{SO}(1,3)$ *speciális Lorentz-csoport* részcsoportját alkotja az $\mathbb{SO}^+(1,3)$ *valódi Lorentz-csoport*: ebben $\mathbb{SO}(1,3)$ azon elemei vannak, amelyek minden $p \in \mathbb{H}$-ra, amelyre $\Re(p^2) > 0$, a p időszerű részének előjelét is megőrzik. Például p konjugálása, a tértükrözés a Lorentz-csoportban van, de nincs benne a speciális Lorentz-csoportban, a $p \mapsto -p$ téridő-tükrözés a speciális Lorentz-csoportban van, de nincs benne a valódi Lorentz-csoportban.

Legyen $p = p_0 + p_1 i + p_2 j + p_3 k$ és $q = q_0 + q_1 i + q_2 j + q_3 k$. Megmutatható, hogy a valódi Lorentz-csoportot generálják a

$$\begin{pmatrix} q_r \\ q_s \end{pmatrix} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} p_r \\ p_s \end{pmatrix}$$

alakba írható $p \mapsto q$ térbeli forgatások (itt $1 \le r, s \le 3$, a többi koordináta nem változik, φ valós paraméter; a forgatás inverze a $-\varphi$-hez tartozó forgatás), valamint a

$$\begin{pmatrix} q_0 \\ q_s \end{pmatrix} = \begin{pmatrix} \cosh\varphi & \sinh\varphi \\ \sinh\varphi & \cosh\varphi \end{pmatrix} \begin{pmatrix} p_0 \\ p_s \end{pmatrix}$$

alakba írható $p \mapsto q$ mozgások (itt $1 \le s \le 3$, a többi koordináta nem változik, φ valós paraméter; a mozgás inverze a $-\varphi$-hez tartozó mozgás).

A $p = p_0 + p_1 i + p_2 j + p_3 k$ kvaterniót azonosítva az $1, j$ bázisban

$$p_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p_1 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + p_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + p_3 \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

mátrixú $\mathbb{C}$-lineáris $\mathbb{C}^2$-t önmagába képező A önadjungált transzformációval, $\Re(p^2) = \det(A)$. Egy $C \in \mathbb{SL}(\mathbb{C}^2)$ transzformációhoz hozzárendelve az $A \mapsto CAC^*$ leképezést, az $\mathbb{SL}(\mathbb{C}^2)$ csoportnak az $\mathbb{O}(1,3)$ csoportba való homomorfizmusát kapjuk. Nyilván C-hez és $-C$-hez ugyanaz a leképezés tartozik, de könnyen megmutatható, hogy csak $\mathbb{C}^2$ identikus leképezéséhez és az ellentettjéhez tartozik $\mathbb{H}$ identikus leképezése. Az is megmutatható, hogy ezen homomorfizmus értékkészlete a valódi Lorentz-csoport. Például az $1, j$ bázisban

$$\begin{pmatrix} e^{\varphi/2} & 0 \\ 0 & e^{-\varphi/2} \end{pmatrix}$$

mátrixú $C \in \mathbb{SL}(\mathbb{C}^2)$ lineáris leképezéshez a

$$\begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} \cosh\varphi & \sinh\varphi \\ \sinh\varphi & \cosh\varphi \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$$

mozgás tartozik.

Az összes $p \mapsto Lp + c$ alakú leképezései $\mathbb{H}$-nak $\mathbb{H}$-ra alkotják a *Poincaré-csoport*ot, ahol L a valódi Lorentz-csoport tetszőleges eleme, c pedig tetszőleges kvaternió.

- $122/-15$:

  $<$

tókat *valódi normálosztó*nak nevezzük.

  $>$

tókat *valódi normálosztó*nak nevezzük. Egy 2 indexű N részcsoport mindig normálosztó, mert csak két bal és jobb oldali mellékosztály van, N és $G \setminus N$.

- $123/1$:

  $<$

  Belső automorfizmusok. Ha G csoport és $a \in G$ rögzített, akkor a G-

  $>$

  * **Belső automorfizmusok.** Ha G csoport és $a \in G$ rögzített, akkor a G-

- $123/1$:

  $<$

képe. Az ilyen alakú automorfizmusokat *belső automorfizmus*oknak nevezzük. Nyilván 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. Ez az oka az invariáns részcsoport elnevezésnek.

  $>$

képe. Az ilyen alakú automorfizmusokat *belső automorfizmus*oknak nevezzük. Ha az x elemhez van olyan belső automorfizmus, amely y-ba viszi át, akkor azt mondjuk, hogy x és y *konjugált*ak. Ez nyilván ekvivalenciareláció, az ekvivalenciaosztályok a *konjugált elemosztály*ok. Nyilván 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 *centralizátor*a, 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 *centrum*a.

* **Osztályegyenlet.** *Egy G csoportban az $x \in G$ elem konjugált elemosztályának annyi eleme van, amennyi $C(x)$ szerinti mellékosztály. Ha G véges csoport, akkor $\sum \big[G : C(x)\big]$ a G rendje, ahol az összegzés a különböző elemosztályokból választott egy-egy x-re értendő; ez az osztályegyenlet.*

Bizonyítás. Az x két 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 mellékosztályba tartoznak. Ezzel az első állítást beláttuk. A konjugált elemosztályok elemszámának összege nyilván G rendje.

* **Példák.** (1) A Q kvaterniócsoportban a konjugált elemosztályok $\{1\}$, $\{-1\}$, $\{i,-i\}$, $\{j,-j\}$, $\{k,-k\}$ és $C(1)=C(-1)=Q$, $C(i)=C(-i)=\{1,-1,i,-i\}$, $C(j)=C(-j)=\{1,-1,j,-j\}$, $C(k)=C(-k)=\{1,-1,k,-k\}$, így $C=\{1,-1\}$.

(2) A D_3 diédercsoportban a konjugált elemosztályok $\{e\}$, $\{\varepsilon,\varepsilon^2\}$, $\{\tau,\tau\varepsilon,\tau\varepsilon^2\}$, és $C(e)=D_3$, $C(\varepsilon)=C(\varepsilon^2)=\{e,\varepsilon,\varepsilon^2\}$, $C(\tau)=\{e,\tau\}$, $C(\tau\varepsilon)=\{e,\tau\varepsilon\}$, $C(\tau\varepsilon^2)=\{e,\tau\varepsilon^2\}$, így $C=\{e\}$.

- 125/2 :

<

Véges Abel-csoportok alaptétele. *Egy véges Abel-csoport prímhatványrendű ciklikus csoportok direkt szorzatával izomorf. A prímhatványrendek egyértelműen meghatározottak.*

* **Bizonyítás.** Megtalálható például Fuchs [20] jegyzetében, 60. oldal. □

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

Bizonyítás. Legyen $a\in G$, és legyen $p_a(x)=ax$, ha $x\in G$. A p_a leképezések az egyszerűsítési szabály miatt kölcsönösen egyértelműek és G-re képeznek, mivel $a^{-1}x$ képe p_a-nál x. Megmutatjuk, hogy az $a\mapsto p_a$ hozzárendelés monomorfizmus. Nyilván $p_a\neq p_b$, ha $a\neq b$, mivel $p_a(e)=a\neq b=p_b(e)$. Továbbá $(p_a\circ p_b)(x)=p_a(bx)=abx=p_{ab}(x)$ minden $x\in G$-re, így a hozzárendelés művelettartó. □

>

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.*

A tétel természetesen alkalmazható minden véges Abel-csoportra.

* **Bizonyítás.** Megtalálható például Safarevics [73] könyvében, 47.–48. oldal. □

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 legyen $p_a(x)=ax$, ha $x\in G$. Tudjuk, hogy az $a\mapsto p_a$ hozzárendelés monomorfizmus. A p_a leképezések az egyszerűsítési szabály miatt kölcsönösen egyértelműek és G-re képeznek, mivel $a^{-1}x$ képe p_a-nál x. □

- 127/−6 :

<

permutációk részcsoportot alkotnak S_n-ben. □

>

permutációk normálosztót alkotnak S_n-ben.

S_n páros permutációinak csoportját A_n-nel jelölünk, és n-edfokú *alternáló csoport*nak nevezünk.

Bizonyítás. A_n a tétel szerint részcsoport. Ha $n > 1$, akkor S_n-nek az A_n szerinti (akár bal, akár jobb oldali mellékosztályai) A_n és $S_n \setminus A_n$, így a jobb és bal oldali mellékosztályok egybeesnek, azaz A_n normálosztó S_n-ben. $\square$

- 128/1 :

  $<$

  Definíció. Egy G csoport egy *normállánc*án részcsoportoknak egy olyan

  $>$

  * **Definíció.** Egy G csoport egy *normállánc*án részcsoportoknak egy olyan

- $128/15\ldots19$:

  $<$

  Legyen $n > 1$ természetes szám. Az előző következmény szerint S_n-ben a páros permutációik egy részcsoportot alkotnak, amelyet A_n-nel jelölünk, és n-edfokú *alternáló csoport*nak nevezünk. Az előző következmény szerint S_n-nek az A_n szerinti (akár bal, akár jobb oldali mellékosztályai) A_n és $S_n \setminus A_n$, így a jobb és bal oldali mellékosztályok egybeesnek, azaz A_n normálosztó S_n-ben. Így $S_n \supset A_n \supset \{e\}$ egy normállánca S_n-

  $>$

  Legyen $n > 1$ természetes szám. Az előző következmény szerint $S_n \supset A_n \supset \{e\}$ egy normállánca S_n-

- $128/-15$:

  $<$

  Példa. Megmutatható, hogy S_4-ben

  $>$

  * **Példa.** Megmutatható, hogy S_4-ben

- $129/-5\ldots-2$:

  $<$

  (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.

  $>$

  (2) Megmutatjuk, hogy egy tetszőleges A Abel-csoport összes endomorfizmusai egységelemes gyűrűt alkotnak a pontonkénti összeadással és a függvények kompozíciójával, mint szorzással; ezt a gyűrűt A *endomorfizmusgyűrű*jének nevezzük. Valóban, ha $f, g : A \to A$ endomorfizmusok, akkor $g \circ f$ nyilván endomorfizmus, és $f + g$ is endomorfizmus, mivel

$$(f+g)(x+y) = f(x+y)+g(x+y) = f(x)+f(y)+g(x)+g(y) = (f+g)(x)+(f+g)(y).$$

Az összeadás nyilván kommutatív, asszociatív, az azonosan nulla lekézés nullelem, és az f additív inverze $-f$. Ha még $h : A \to A$ is endomorfizmus, akkor

$$\begin{aligned}\big((f+g)\circ h\big)(x) &= (f+g)\big(h(x)\big) = f\big(h(x)\big) + g\big(h(x)\big) \\ &= (f\circ h)(x) + (g\circ h)(x) = (f\circ h + g\circ h)(x),\end{aligned}$$

azaz teljesül a jobb oldali disztributivitás. A bal oldali disztributivitás hasonlóan adódik. Végül vegyük észre, hogy az identikus leképezés egységelem.

- 130/14 :

<

mondjuk, hogy a *gyűrű karakterisztikája* n. Jelölése: $\mathrm{char}(R)$.

>

mondjuk, hogy a *gyűrű karakterisztikája* n. Jelölése: $\mathrm{char}(R)$.

Hasznos észervétel, hogy ha $n = \mathrm{char}(R) > 0$, 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. Így $x \mapsto x^n$ — és innen indukcióval minden $k \in \mathbb{N}^+$-ra $x \mapsto x^{n^k}$ is — automorfizmus.

- 130/−1 :

<

hasonlóan $(b'+c')a' = b'a' + c'a'$. $\square$

>

hasonlóan $(b'+c')a' = b'a' + c'a'$. $\square$

Reprezentációk. Egy R gyűrűnek egy A Abel-csoport endomorfizmusgyűrűjébe való homomorfizmusát R *reprezentáció*jának nevezzük. Ha a leképezés monomorfizmus, akkor *hű reprezentáció*ról beszélünk. Egy egységelemes gyűrűnek mint egységelemes félcsoportnak a reguláris reprezentációja a gyűrű *reguláris reprezentáció*ja; mint tudjuk, ez hű reprezentáció.

- 131/5 . . . 7 :

<

Ha X tetszőleges halmaz, akkor $\wp(X)$ példa Boole-gyűrűre a $(\triangle, \cap)$ műveletekkel. Egy halmazhoz a karakterisztikus függvényét rendelve látjuk, hogy ez a gyűrű a $\{0,1\}^X$ függvénygyűrűvel izomorf.

>

A nullgyűrűtől különböző legegyszerűbb példa Boole-gyűrűre $\{\uparrow, \downarrow\}$ a $(\oplus, \wedge)$ műveletekkel. Ha X tetszőleges halmaz, akkor $\wp(X)$ példa Boole-gyűrűre a $(\triangle, \cap)$ műveletekkel. (Figyeljük meg a nagyfokú hasonlóságot a logikai műveletek és a halmazműveletek között: nem véletlen, hiszen mindkét esetben Boole-gyűrűben vagyunk.) Egy halmazhoz a karakterisztikus függvényét rendelve látjuk, hogy ez a gyűrű a $\{0,1\}^X$ függvénygyűrűvel izomorf. Természetesen egy Boole-gyűrű minden részgyűrűje is Boole-gyűrű. Megmutatható, hogy minden Boole-gyűrű izomorf valamely halmaz részhalmazai Boole-gyűrűjének egy részgyűrűjével.

- $131/8\ldots 9$:

$<$

Részgyűrű, ideál. Egy R gyűrű egy $S \neq \emptyset$ részhalmazát *részgyűrű*nek nevezzük, ha $a, b \in S$ esetén $a - b \in S$ és $ab \in S$. Ezek a feltételek nyilván úgy is írhatók,

$>$

Részgyűrű, résztest, ideál. Legyen R egy halmaz a $(+.\cdot)$ binér műveletekkel. Az R gyűrű egy S részhalmazát *részgyűrű*nek, illetve *résztest*nek nevezzük, ha maga is gyűrű, illetve test az adott műveletekkel. A számunkra legfontosabb eset az lesz, amikor R maga is gyűrű. A részcsoportoknál tanultak szerint egy $S \neq \emptyset$ részhalmaza R-nek pontosan akkor részgyűrű, ha $a, b \in S$ esetén $a - b \in S$ és $ab \in S$. Ezek a feltételek nyilván úgy is írhatók,

- $132/-4$:

$<$

Megjegyzés. Az előző tétel (1) öszefüggésében az egyenlőség

$>$

* **Megjegyzés.** Az előző tétel (1) öszefüggésében az egyenlőség

- $135/17$:

$<$

$\mathbb{Z}$ az $n \mapsto |n|$ függvénnyel nyilván euklideszi gyűrű.

$>$

$\mathbb{Z}$ az $n \mapsto |n|$ függvénnyel nyilván euklideszi gyűrű. Mint ez a példa is mutatja, a definícióban szereplő r általában nem egyértelmű: itt például lehet a legkisebb nemnegatív maradék, a legkisebb abszolút értékű maradék, stb.

- $135/20$:

$<$

Állítás. Euklideszi gyűrűben pontosan azok az elemek az egységek, ame-

$>$

* **Állítás.** Euklideszi gyűrűben pontosan azok az elemek az egységek, ame-

- $136/-6$:

$<$

Tétel. *Euklideszi gyűrűben minden ideál főideál.*

$>$

* **Tétel.** *Euklideszi gyűrűben minden ideál főideál.*

- 137/1 :

  $<$

  Definíció. Egy R gyűrű egy I valódi ideálját *maximális ideál*nak nevezzük,

  $>$

  * **Definíció.** Egy R gyűrű egy I valódi ideálját *maximális ideál*nak nevezzük,

- 137/4 :

  $<$

  Következmény. *Egy euklideszi gyűrű egy nem triviális ideálja pontosan*

  $>$

  * **Következmény.** *Egy euklideszi gyűrű egy nem triviális ideálja pontosan*

- 137/10 :

  $<$

  Tétel. *Legyen R kommutatív egységelemes gyűrű, I az R egy ideálja. Az*

  $>$

  * **Tétel.** *Legyen R kommutatív egységelemes gyűrű, I az R egy ideálja. Az*

- 138/1 :

  $<$

  Hányadostest. *Legyen R integritási tartomány. Az $R \times \big(R \setminus \{0\}\big)$ halma-*

  $>$

  Hányadostest. *Legyen R a nullgyűrűtől különböző integritási tartomány. Az $R \times \big(R \setminus \{0\}\big)$ halma-*

- 139/−19 :

  $<$

nullosztómentes.

  $>$

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

- 140/2 . . . 5 :

  $<$

re $r^p = r$, így a $\mathbb{Z}_p$ feletti x^p és 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 $\mathbb{Z}_p$ feletti polinom, amihez ugyanaz a polinomfüggvény tartozik.

  $>$

re $r^p = r$, így a $\mathbb{Z}_p$ feletti x^p és x polinomokhoz ugyanaz a polinomfüggvény tartozik.

- $141/-19\ldots-21$:

$<$

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.

$>$

Megjegyezzük, hogy minden $x=bi+cj+dk$, $b,c,d\in\mathbb{R}$ kvaternióra, amelyre $b^2+c^2+d^2=1$, teljesül, hogy $1+x^2=0$, és ilyen kvaternió végtelen sok van. A kvaterniók szorzása azonban nem kommutatív. A nem nullosztómentes $\mathbb{Z}_{65}$-ben 8, 18, 47, 57 mind gyökei $1+x^2$-nek.

* **Körosztási polinomok.** Ha $n\in\mathbb{N}^+$, legyenek $\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{n-1}$ 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 $kx \bmod n=j$; 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

$$\Phi_n(x)=\prod_{0\le k<n,\mathrm{lnko}(k,n)=1}(x-\varepsilon_k),$$

az n-edik *körosztási polinom*; ennek foka $\varphi(n)$. Mivel bármely ε_k egységgyök m rendjére $m|n$, 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 $m|n$ esetén $x^m-1|p_n(x)$, az is adódik, hogy

$$\Phi_n(x)\Big|\frac{x^n-1}{x^m-1}=\left(\sum_{j=0}^{n/m-1}x^{mj}\right).$$

- $141/-2\ldots-1$:

$<$

monomok szorzatára igaz az összefüggés. Megfordítva, ha egy $f\mapsto f'$ leképezése $R[x]$-nek önmagába rendelkezik ezzel a négy tulajdonsággal, akkor i szerinti indukcióval az

$>$

monomok szorzatára igaz az összefüggés. Megfordítva, ha egy $f\mapsto f'$ leképezése $R[x]$-nek önmagába rendelkezik ezzel a négy tulajdonsággal, akkor i szerinti indukcióval az

* **Megjegyzés.** Megfordítva, ha R egységelemes integritási tartományra egy $f \mapsto f'$ leképezése $R[x]$-nek önmagába rendelkezik az előző definícióban szereplő (1)–(4) tulajdonságokkal, 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 $f' = f_1 + 2f_2x + 3f_3x^2 + \cdots + nf_nx^{n-1}$ formula következik tetszőleges polinomra.

• 142/1 . . . 2 :

<

$f_i x^i$ 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 $f' = f_1 + 2f_2x + 3f_3x^2 + \cdots + nf_nx^{n-1}$ formula következik tetszőleges polinomra.

>

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

Bizonyítás. Ha $f = g^n h$, akkor differenciálással

$$f' = ng^{n-1}h + g^n h' = g^{n-1}(nh + h'). \quad \square$$

Következmény. *Ha R test, $f \neq 0$, és d az f és az f' legnagyobb közös osztója, akkor $q = f/d$ négyzetmentes, azaz egyetlen legalább elsőfokú g polinomnak a négyzetével sem osztható.*

Bizonyítás. Ha $g^n | f$ de $g^{n+1} \not| f$, akkor $g^{n-1} | f'$, így $g^{n-1} | d$. Innen $g^2 | q$ nem lehetséges, mert abból $g^{n+1} | f$ következne. $\square$

• 142/−21 . . . − 7 :

<

Legyen K test, és $f \in K[x]$ egy n-ed fokú ($n > 1$) irreducibilis főpolinom. Ekkor az (f) főideál maximális ideál, így $\bar{K} = K[x]/(f)$ test. Minden mellékosztályban a legalacsonyabb fokú polinom fokszáma kisebb, mint n, és csak egy ilyen polinom van; ez meghatározható úgy, hogy a mellékosztály tetszőleges elemére vesszük az f-fel való osztásánál adódó maradékot. A műveleteket ezekkel a reprezentánsokkal végezhetjük; ha a szorzat foka nem kisebb, mint n, akkor osztunk f-fel, és vesszük a maradékot. Jelölje α az $x \in K[x]$ polinom osztályát $K[x]/(f)$-ben. A $\bar{K}$ test elemei egyértelműen felírhatók $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ alakban, ahol $a_0, a_1, \ldots, a_{n-1} \in K$. Így K részteste $\bar{K}$-nak. A $\bar{K}[x]$-belinek is tekinthető f polinom $\bar{K}[x]$-ben már nem irreducibilis, α egy gyöke.

Legyen p egy prímszám. A fenti konstrukciót alkalmazva a $\mathbb{Z}_p$ véges testre, egy p^n elemű véges testet kapunk. (Megmutatható, hogy $\mathbb{Z}_p$ felett $\sum_{d|n} \mu(n/d)p^d/n \neq 0$ irreducibilis n-ed fokú főpolinom van; lásd Knuth [43], 4.6.2.(4) feladat.) Azt, hogy az n-ed fokú $f \in \mathbb{Z}_p[x]$ polinom irreducibilis, például úgy is megmutathatjuk, hogy minden, legfeljebb $\lfloor n/2 \rfloor$ fokszámú polinommal megpróbáljuk elosztani. (Ennél sokkal hatékonyabb eljárások is léteznek.)

>

Legyen F test, és $f \in F[x]$ egy n-ed fokú ($n \in \mathbb{N}^+$) 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 közös osztója, egy nullad fokú polinom. Innen d osztálya az egységelem $\tilde{F}$-ban, v osztálya pedig g osztályának az inverze. Minden mellékosztályban a legalacsonyabb fokú polinom fokszáma kisebb, mint n, és csak egy ilyen polinom van; ez meghatározható úgy, hogy a mellékosztály tetszőleges elemére vesszük az f-fel való osztásánál adódó maradékot. A műveleteket ezekkel a reprezentánsokkal végezhetjük; ha a szorzat foka nem kisebb, mint n, akkor osztunk f-fel, és vesszük a maradékot. Jelölje α az $x \in F[x]$ polinom osztályát $F[x]/(f)$-ben. A $\tilde{F}$ test elemei egyértelműen felírhatók $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ alakban, ahol $a_0, a_1, \ldots, a_{n-1} \in F$. Így F résztestе $\tilde{F}$-nak. (A $\tilde{F}[x]$-belinek is tekinthető f polinom $\tilde{F}[x]$-ben már nem irreducibilis, α egy gyöke.)

Legyen p egy prímszám. A fenti konstrukciót alkalmazva a $\mathbb{Z}_p$ véges testre, 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.)

• $142/-6\ldots-1:$

<

* **Példák.** (1) Tekintsük az $\mathbb{R}[x]$ polinomgyűrűben az (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 gyűrűt alkotnak. (Természetesen x^2+1 irreducibilis, és (x^2+1) maximális ideál.)

(2) Tekintsük a $\mathbb{Z}_2[x]$ polinomgyűrűben az (x^2+x+1) főideált. Minden mellékosztályban a legalacsonyabb fokú polinom lineáris, és a mellékosztályban pontosan egy

>

Példák. (1) Tekintsük az $\mathbb{R}[x]$ polinomgyűrűben az x^2+1 irreducibilis 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) főideált. Minden mellékosztályban a legalacsonyabb fokú polinom lineáris, és a mellékosztályban pontosan egy

• $143/1\ldots15:$

<

lineáris polinom van. A faktorgyűrű szorzásával a mellékosztályok egy négyelemű testet alkotnak. (Természetesen x^2+x+1 irreducibilis, és (x^2+x+1) maximális ideál.)

Véges testek alaptétele.

(1) *Bármely véges test elemeinek száma prímhatvány, ahol a prím a test karakterisztikája.*

(2) *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 (2) szerint lényegében csak egy q elemű véges test van, beszélhetünk a q elemű véges testről. Ezt $\mathbb{F}_q$-val jelöljük.

* **Bizonyítás.** (1) bizonyítása nem nehéz: ha p a K véges test karakterisztikája és e az egységeleme, akkor a $\mathbb{Z}$-t K-ba képező $n \mapsto ne$ homomorfizmusra csak $n \bmod p$-től függ n képe, így tekinthetjük $\mathbb{Z}_p \to K$ homomorfizmusnak is. Ez utóbbi homomorfizmus monomorfizmus is, így $\mathbb{Z}_p$-t azonosítva a leképezés értékkészletével $\mathbb{Z}_p$ a K részteste. Nyilván K vektortér $\mathbb{Z}_p$ felett, és ha n-dimenziós, akkor K-nak p^n eleme van.

(2) bizonyítása jóval nehezebb: lásd gondajanosGonda JánosGonda jegyzetét. $\square$

$>$

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 $n \mapsto ne$ 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. $\square$

- 143/−20 :

$<$

Tétel. *Véges test nem nulla elemeinek multiplikatív csoportja ciklikus.*

* **Bizonyítás** Egy n rendű G ciklikus csoportban minden $d|n$ esetén pontosan egy d rendű részcsoport van. Ez ciklikus és $\varphi(d)$ generátora van. Mivel G minden eleme generál egy részcsoportot, $\sum_{d|n} \varphi(d) = n$.

Legyen most a nem nulla elemek multiplikatív csoportja G, és legyen a G rendje n. Ha $d|n$ és van olyan $g \in G$, amelynek rendje d, akkor ez egy $H = \{1, g, g^2, \ldots, g^{d-1}\}$ ciklikus részcsoportot generál. Mivel testben az $x^d = 1$ egyenletnek legfeljebb d megoldása van, azok mind a H részcsoportban vannak. Speciálisan, minden d rendű eleme G-nek generátora H-nak, és $\varphi(d)$ ilyen van. Így d rendű eleme G-nek 0 vagy $\varphi(d)$ darab van. Ha valamely $d|n$-re nulla lenne, az ellentmondana annak, hogy $\sum_{d|n} \varphi(d) = n$. Így van n rendű elem is, tehát G ciklikus. $\square$

$>$

◦ **Alkalmazás: A Rijndael és AES blokkrejtjelzők.** A $Z^8 + Z^4 + Z^3 + Z + 1$ polinom irreducibilis $\mathbb{Z}_2$ felett. A 256 elemű $\mathbb{Z}_2[Z]/(Z^8+Z^4+Z^3+Z+1)$ testet Rijndael-testnek is nevezik: ezt a testet használja a Joan Daemen és Vincent Rijmen belga kriptográfusok által tervezett Rijndael-rendszer. A test elemei mellékosztályok, a mellékosztályokat a bennük szereplő egyetlen 8-nál alacsonyabb fokú polinommal reprezentáljuk. A rendszer titkos kulcsú, gyors a rejtjelezés és a fejtés, és a klasszikus, Shannon-tól származó elveken alapul: a kulcstól is függő helyettesítéseket és keveréseket alkalmaz a rejtjelzendő blokkra számos menetben egymás után. Alapvetően 32 bites szavakat használ. A rejtjelzendő blokk b és a kulcs k (szavakban megadott) mérete is 4, 5, 6, 7 vagy 8 szó lehet, egymástól függetlenül. Ha r menetet használunk, akkor először a k szavas kulcsot kiterjesztjük egy $r+1$ darab b szavas segédkulcs-sorozattá (lásd később). Egy W szót tekinthetünk egy (B_0, B_1, B_2, B_3) bájtnégyesnek, ahol a bájtok a memóriacímeik növekvő sorrendjében következnek. A teljes blokkot tekinthetjük egy bájtmátrixnak, amelynek egyes oszlopait a szavak bájtjai alkotják, a sorindexek $0, 1, 2, 3$. Egy tetszőleges B bájtot tekinthetünk egy $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)$ bitsorozatnak, egy $b_0 + b_1 2 + b_2 2^2 + \cdots + b_7 2^7$ számnak, illetve a Rijndael-test egy, a $b_0 + b_1 Z + \cdots + b_7 Z^7$ polinommal reprezentált elemének.

A rejtjelzés r menetből áll, ahol $r \geq 10$, ha $b = k = 4$, egyébként ha $b, k \leq 6$, akkor $r \geq 12$, és minden más esetben $r \geq 14$. A menetek előtt bitenkénti kizáró vagy műveletet végzünk a blokk és az első segédkulcs között. Az egyes menetek az alábbi négy lépésből állnak:

(1) Bájtonkénti S helyettesítés: A blokkra bájtonkénti elvégezzük az S helyettesítést, ahol $S(x) = Bx^{-1} + b$; itt x^{-1} azt jelenti, hogy az x bájtot a Rijndael-test egy elemével azonosítva, kiszámítjuk a multiplikatív inverzét (a nulla bájt inverzét nullának tekintjük). Az eredményül kapott x' bájtra kiszámítjuk az

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = C \begin{pmatrix} x'_0 \\ x'_1 \\ x'_2 \\ x'_3 \\ x'_4 \\ x\text{‘}_5 \\ x'_6 \\ x'_7 \end{pmatrix} + c$$

összefüggéssel adott y bájtot $\mathbb{Z}_2$ feletti mátrixszorzással és vektorösszeadással, ahol

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{és} \quad c = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

és $S(x) = y$. A helyettesítés inverze $x = S^{-1}(y) = \left(C^{-1}(y - c)\right)^{-1}$; a C mátrix modulo 2 inverze

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

(2) Sorkeverés: A blokknak megfelelő bájtmátrix sorait ciklikusan balra léptetjük, minden sort annyi bájttal, amennyi az indexe. Ha $b > 6$, akkor a 2, illetve 3 indexű sort 3-mal, illetve 4-gyel léptetjük. A transzformáció invertálása nyilvánvaló.

(3) Oszlopkeverés: A bájtmátrixban minden oszlopot egy polinomnak tekintünk a z változóban a Rijndael-test felett. Az együtthatókat az oszlop bájtjai adják, a 0 indexű sorban van a konstans tag. Ezt a polinomot szorozzuk a Rijndael-test feletti $(Z^2 + Z)z^3 + z^2 + z + Z$ polinommal, és az eredményt redukáljuk modulo $z^4 + 1$, ennek a (Rijndael-testbeli) együtthatói adják a keverés eredményét. Az invertálás azon alapul, hogy az előző polinomnak modulo $z^4 + 1$ van inverze: $(Z^3 + Z + 1)z^3 + (Z^3 + Z^2 + 1)z^2 + (Z^3 + 1)z + Z^3 + Z^2 + Z$.

(4) Segédkulcs hozzáadása: bitenként kizáró vagy műveletet végzünk a kapott szavak és a következő segédkulcs szavai között. Az invertálás ugyanez.

Az utolsó, r-edik menetben az oszlopkeverési lépés kimarad. A dekódolás nyilván a rejtjelzési lépések inverzeinek fordított sorrendben történő elvégzésével történik.

Le kell még írnunk a segédkulcsok képzését. A segédkulcsok tömbje $(r + 1)b$ szóból áll, ezt a szósorozatot olvassuk az elejétől kezdve, mindig b szót, ezek a segédkulcsok. A tömböt a következőképpen töltjük fel: az első k helyre kerülnek az eredeti kulcs szavai. A további W_i, $i = 0, 1, \ldots, (r+1)b-k-1$ szavakat a következőképpen képezzük: általában W_i az előtte álló, és a k-val előtte álló szóra alkalmazott bitenkénti kizáró vagy művelettel adódik. A $k \leq 6$ esetben ettől csak akkor térünk el, ha $i \equiv 0 \pmod k$; ekkor a két szó közötti kizáró vagy művelet előtt az előző szó bájtjait ciklikusan eggyel léptetjük (a 0 indexű bájt a 3 indexű bájt helyére kerül), bájtonként alkalmazzuk az S helyettesítést, majd a 0 indexű bájthoz bitenkénti kizáró vagy művelettel hozzáadjuk a Rijndael-test $Z^{\lfloor i/k \rfloor}$ által reprezentált eleme bitjeit. Ha $k > 6$, akkor még egy eltérés van: ha $i \equiv 4 \pmod k$, akkor a két szó közötti kizáró vagy művelet előtt az előző szóra bájtonként alkalmazzuk az S helyettesítést.

Az AES (Advanced Encryption Standard) USA-szabvány rejtjelző a Rijndael speciális esete: $b = 4$ és $k = 4$, $r = 10$ vagy $k = 6$, $r = 12$ vagy $k = 8$, $r = 14$.

Tétel. *Véges test nem nulla elemeinek multiplikatív csoportja ciklikus. Ha a véges testnek q eleme van, akkor bármely c elemére $c^q = c$.*

* **Bizonyítás** Legyen a nem nulla elemek multiplikatív csoportja G, és legyen G rendje n. Ha $d|n$ és van olyan $g \in G$, amelynek rendje d, akkor ez egy $H = \{1, g, g^2, \ldots, g^{d-1}\}$ ciklikus részcsoportot generál. Mivel testben az $x^d = 1$ egyenletnek legfeljebb d megoldása van, azok mind a H részcsoportban vannak. Speciálisan, minden d rendű eleme G-nek generátora H-nak, és $\varphi(d)$ ilyen van. Így d rendű eleme G-nek 0 vagy $\varphi(d)$ darab van. Ha valamely $d|n$-re nulla lenne, az ellentmondana annak, hogy $\sum_{d|n} \varphi(d) = n$ (lás például a 8.3.25. pontot). Így van n rendű elem is, tehát G ciklikus. □

- 143/−9 :

  <

  Irreducibilis polinomok. A komplex számtest felett az algebra alaptétele

$>$

* **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 $d|n$.*

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

$$y^{q^{dk}} = y^{(q^{d(k-1)} \cdot q^d)} = \left(y^{q^{d(k-1)}}\right)^{q^d} = y^{q^d} = y$$

minden $y \in \tilde{F}$-ra. Így $d|n$ 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-el.

Megfordítva, 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. Nyilván az ilyen η elemek halmaza a szorzásra is zárt. Így ha f osztja az $x^{q^n} - x$ polinomot $F[x]$-ben, akkor $\tilde{F}$-ban $\tilde{x}^{q^n} = \tilde{x}$, amiből, mivel ξ az $\tilde{x}$ polinomja, $\xi^{q^n} = \xi$ is teljesül. De ha $n = kd + r$, $0 \leq r < d$, akkor

$$\xi = \xi^{q^n} = \xi^{(q^{dk} \cdot q^r)} = \left(\xi^{q^{dk}}\right)^{q^r} = \xi^{q^r},$$

ami $r > 0$ esetén ellentmond annak, hogy ξ generátorelem. $\square$

Következmény. *Az F feletti n-ed fokú irreducibilis polinomok száma legalább $\left(q^n - q^{\lfloor n/2 \rfloor} \lfloor \lg n \rfloor\right)/n > 0$.*

* **Bizonyítás.** Mivel $x^{q^n} - x$ deriváltja a -1 polinom, bármely irreducibilis főpolinomnak legfeljebb az első hatványa osztja $x^{q^n} - x$-et. Bármely d valódi osztójára n-nek d osztója n/p_i-nek valamely p_i prímtényezőjére n-nek. Így azon irreduciblis 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 legfeljebb $\lfloor \lg n \rfloor$, azon irreduciblis főpolinomok, amelyek osztói $x^{q^n} - x$-nek, de fokuk kisebb mint n, szorzatának a foka legfeljebb $q^{\lfloor n/2 \rfloor} \lfloor \lg n \rfloor$. Így a pontosan n-ed fokú irreducibilis főpolinomok szorzatának a foka legalább $q^n - q^{\lfloor n/2 \rfloor} \lfloor \lg n \rfloor$. Hátravan 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 még a $q^n > q^{n/2} \lg n$ egyenlőtlenség is teljesül. Ha $n = 8$, a két egyenlőtlenség ekvivalens, egyébként pedig teljes indukcióval

$$q^{n+1} = q \cdot q^n > q \cdot q^{n/2} \lg n = q^{(n+1)/2} \lg(n+1) \sqrt{q} \frac{\lg n}{\lg(n+1)} > q^{(n+1)/2} \lg(n+1),$$

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. *Bármely $q = p^n$ (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 *bővítés*e. Nyilván K vektortér F felett. Ennek a vektortérnek a dimenzióját a *bővítés fok*ának nevezzük és $[K : F]$-fel jelöljük; ha véges, akkor *véges bővítés*ről 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 *minimálpolinom*ja F felett egy minimális fokú ilyen polinom. 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. Így a minimálpolinomok egymás asszociáltjai. A minimálpolinomok nyilván irreducibilisek. 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 $g \mapsto g(\alpha)$ 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 $F(\alpha)$ nyilván tartalmazza a $\sum_{j=0}^{n-1} r_j \alpha^j$ alakú összegeket, 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. $\square$

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, $n_x|n$ minden $x \in K$-ra. Tekintsük most a $G = K \setminus \{0\}$ multiplikatív csoportot. A $C(x)$ konjugált elemosztály $x \neq 0$ esetén $C_K(x) \setminus \{0\}$, és így a C centrum $C_K \setminus \{0\}$. Az osztályegyenlet szerint

$$q^n - 1 = q - 1 + \sum \big[G : C(x)\big] = q - 1 + \sum \frac{q^n - 1}{q^{n_x} - 1};$$

az összegzés a nem egyelemű konjugált elemosztályok egy-egy x reprezentánsára értendő, $q-1$ pedig az egyelemű konjugált elemosztályok száma, amely C elemszáma. A Φ_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 $\Phi_n(x) = \prod(x-\varepsilon_k)$, ahol a szorzat az összes primitív n-edik ε_k egységgyökre értendő, így $\big|\Phi_n(q)\big| = \prod |q - \varepsilon_k|$, és a jobb oldalon minden tényező abszolút értéke nagyobb, mint $q-1$. Tehát $n = 1$ és $K = C_K$.

* **Polinomfaktorizálás véges testek felett.** Első lépésként az $\mathbb{F}_q$ feletti f polinomot ($q = p^n$, p prím, $n \in \mathbb{N}^+$) a 8.3.30. 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 $f_0 + f_1x^p + f_2x^{2p} + \cdots + f_mx^{mp}$ 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 $g = g_0 + g_1x + \cdots + g_mx^m$ polinomra

$$g(x)^p = g_0^p + (g_1x)^p + \cdots + (g_mx^m)^p = f(x),$$

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 irreducibilis.

Harmadik lépésként az f_d polinomokat „hasítjuk” szét. Ha f_d fokszáma d, akkor nyilván irreducibilis, megállhatunk. Ha valamelyik f_d fokszáma nagyobb, mint d, akkor egy valószínűségi módszert használhatunk a „széthasítására”. 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,

$$t(x)^{q^d} = \big(\textstyle\sum_{j=0}^k t_jx^j\big)^{q^d} = \displaystyle\sum_{j=0}^k t_j^{q^d}(x^j)^{q^d} = \sum_{j=0}^k t_j\big(x^{q^d}\big)^j,$$

ahonnan $F[x]/(x^{q^d}-x)$-ben számolva

$$\tilde{t}^{q^d}=\sum_{j=0}^{k} t_j\big(\tilde{x}^{q^d}\big)^j=\sum_{j=0}^{k} t_j\tilde{x}^j=\tilde{t}.$$

Ha most a $t(x)^{q^d}-t(x)$ polinomnak vesszük egy faktorizálását, akkor valószínű, hogy f_d irreducibilis osztói nem mind ugyanabban a tényezőben lesznek, és legnagyobb közös osztó képzéssel kinyerhetők. Páratlan q esetén a nyilvánvaló

$$t(x)^{n^d}-t(x)=\big(t(x)^{(q^d-1)/2)}-1\big)\big(t(x)^{(q^d-1)/2)}+1\big)t(x)$$

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

$$t(x)^{n^d}-t(x)=\prod_{c\in\mathbb{F}_q}\Big(T\big(t(x)\big)-c\Big)$$

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 $T(x)$-et írunk, és felhasználjuk, hogy $T(x)^q-T(x)=x^{q^d}-x$, mivel $T(x)^q=T(x^q)$, majd x helyére $t(x)$-et helyettesítünk.

* **Magasabb fokú kongruenciák.** Az

$$f_0+f_1x+f_2x^2+\cdots+f_nx^n\equiv 0 \pmod{m}$$

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

$$x^{j+\varphi(p^\alpha)}\equiv x^j \pmod{x^\alpha},\quad \text{ha}\quad j\ge\alpha;$$

ennek a segítségével redukálhatjuk a kongruencia fokát. Az $\alpha=1$ eset elintézhető az előző pont alapján, hiszen ekkor egy $\mathbb{Z}_p$ feletti polinom gyöktényezőit kell meghatároznunk. Végül az $\alpha>1$ eset az alábbi lemma alapján 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*

$$f(x) \equiv g_\alpha(x)h_\alpha(x) \pmod{p^\alpha}, \quad u(x)g_\alpha(x) + v(x)h_\alpha(x) \equiv 1 \pmod{p}$$

kongruenciák. Ekkor léteznek olyan $g_{\alpha+1}, h_{\alpha+1} \in \mathbb{Z}[x]$ polinomok, amelyre

$$g_{\alpha+1}(x) \equiv g_\alpha(x) \pmod{p^\alpha} \quad \text{és} \quad h_{\alpha+1}(x) \equiv h_\alpha(x) \pmod{p^\alpha},$$

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 $g_{\alpha+1} = g_\alpha + p^\alpha \bar{g}$ illetve $h_{\alpha+1} = h_\alpha + p^\alpha \bar{h}$ alakú, ahol $\bar{g}, \bar{h} \in \mathbb{Z}[x]$, $\deg(\bar{g}) < \deg(g_\alpha)$, $\deg(\bar{h}) \le \deg(h_\alpha)$. Az

$$u(x)g_{\alpha+1}(x) + v(x)h_{\alpha+1}(x) \equiv 1 \pmod{p}$$

feltétel ekkor nyilván teljesül, az

$$f(x) \equiv g_{\alpha+1}(x)h_{\alpha+1}(x) = \big(g_\alpha(x) + p^\alpha \bar{g}(x)\big)\big(h_\alpha(x) + p^\alpha \bar{h}(x)\big) \pmod{p^{\alpha+1}}$$

feltétel pedig azzal ekvivalens, hogy

$$\bar{h}(x)g_\alpha(x) + \bar{g}(x)h_\alpha(x) \equiv w(x) \pmod{p},$$

ahol

$$w(x) = \frac{f(x) - g_\alpha(x)h_\alpha(x)}{p^\alpha}.$$

Tetszőleges $q(x) \in \mathbb{Z}[x]$-re

$$(1) \quad \big(u(x)w(x) + q(x)h_\alpha(x)\big)g_\alpha(x) + \big(v(x)w(x) - q(x)g_\alpha(x)\big)h_\alpha(x) \equiv w(x) \pmod{p}.$$

Legyen q a vw polinomnak a g_α polinommal $\mathbb{Z}_p$ felett való osztásánál fellépő hányados, $\bar{g} = vw - qg_\alpha$ és $\bar{h} = vw - qh_\alpha$, mindkettő $\mathbb{Z}_p$ felett kiszámolva. Mivel $\bar{g}$ a vw polinomnak g_α-val való osztásánál fellépő maradék, $\deg(\bar{g}) < \deg(g_\alpha)$. Mivel $\deg(w) \le \deg(f) = \deg(g_\alpha) + \deg(h_\alpha)$, azt kapjuk, hogy $\deg(\bar{h}) \le \deg(h_\alpha)$, mivel egyébként az (1) kongruencia nem teljesülhetne.

Ha $\bar{\bar{g}}$ és $\bar{\bar{h}}$ másik megoldás, akkor

$$\big(\bar{h}(x) - \bar{\bar{h}}(x)\big)g_\alpha(x) \equiv \big(\bar{\bar{g}}(x) - \bar{g}(x)\big)h_\alpha(x) \pmod{p}.$$

Mivel $\mathbb{Z}_p$ felett g_α és h_α relatív prímek, g_α osztja $\bar{\bar{g}} - \bar{g}$-t. Mivel ennek fokszáma kisebb, mint g_α fokszáma, csak nulla lehet. Innen a másik oldal is nulla.

Irreducibilis polinomok $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ és $\mathbb{Z}$ felett. A komplex számtest felett az algebra alaptétele

- 147/14 :

  <

  Megjegyzések. (1) Ha R test, a Schönemann–Eisenstein-tétel nyilván nem alkal-

  >

  8.3.30. Megjegyzések. (1) Ha R test, a Schönemann–Eisenstein-tétel nyilván nem alkal-

- 148/4 :

  <

  Megjegyzések. (1) Ha R test, a Schönemann–Eisenstein-tétel nyilván nem alkal-

  >

  8.3.30. Megjegyzések. (1) Ha R test, a Schönemann–Eisenstein-tétel nyilván nem alkal-

- 149/13 :

  <

a j-edik *Lagrange interpolációs alappolinom*, és legyen $f = \sum_{j=0}^{n} d_j l_j$.

  >

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 értékénél (és n-nél is) nagyobb p prímet és véletlen $a_1, a_2, \ldots a_{m-1} \in \mathbb{Z}_p$ együtthatókat, majd számítsuk ki a $\mathbb{Z}_p$ feletti $t + a_1x^1 + a_2x^2 + \cdots + a_{m-1}x^{m-1}$ polinom $y_1, y_2, \ldots, y_n$ értékeit az $1, 2, \ldots, n$ helyeken. Ezek a titokrészek: bármelyik m titokrészből a polinom megkapható Lagrange-interpolációval, így a titok adódik, de kevesebb részből nem.

- 149/13 :

  <

feloldható-e.

  >

feloldható-e. Speciális esetekben tehát sikerülhet meghatározni a gyököket, például sokszor segít egy új változó bevezetése $y = h(x)$ alakban, ahol h polinom; ez a *Tschirnhaus-transzformáció*.

- 152/16 :

  <

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]. \quad \square$$

  >

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]. \quad \square$$

Megjegyzés. Ha $n > 1$, akkor $R[x_1, x_2, \ldots, x_n]$ nem tehető euklidészi gyűrűvé, még akkor sem, ha R test, mert 1 az x_1 és x_2 polinomok legnagyobb közös osztója, de semmilyen p_1, $p-2$ polinomokkal nem áll előnem áll elő $p_1x_1 + p_2x_2$ alakban, mert mindkét szorzat konstans tagja nulla.

- $162/-17$:

$<$

múlik.) Pefix kód nyilván felbontható.

$>$

múlik.) Prefix kód nyilván felbontható.

- $173/-4$:

$<$

adva meg. Ebből az információból a 9.2.7. tétel bizonyításánál megadott algoritmussal

$>$

adva meg. Ebből az információból

- $193/-15..-1$:

$<$

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 $t+1$ hiba, 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 v, amelyek pontosan d helyen különböznek. Írjuk u-ban ebből a d számú pozícióból t helyre a v adott pozícióján található jegyet, és jelöljük az így kapott szót z-vel. A z az u-tól t helyen különbözik, míg v-től $d - t \leq d/2 \leq t$ helyen. Ha a dekódolás t-hibajavító lenne, akkor z-t egyrészt u-ra, másrészt v-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.

A továbbiakban feltesszük, hogy minimális távolságú dekódolás esetén a döntési függvény teljes, vagyis minden vett szóhoz hozzárendel egy kódszót.

$>$

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. Írjuk 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. Valóban, 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 visszük 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 egy 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 $2t + r < d$. Valóban, 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.

- 195/−12..1199/−10 :
  <

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 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 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. Lineáris kódnál a szavak tekinthetők polinomoknak is, a betűket nullától indexelve.

A paritásellenőrző kód általában nem lineáris, de ha párosra egészítünk ki, akkor már lineáris. További egyszerű lineáris kódok az úgynevezett *CRC*, vagyis *Cyclic Redundancy Check*, ciklikus ellenőrzés kódok. A test a kételemű test. A k bites kódolandó szó elejére írunk $m=n-k$ darab nullát, majd a megfelelő polinomot osztjuk egy adott m-ed fokú polinommal, a *kódpolinom*mal. Végül a kapott maradékkal kicseréljük a nullákat. Mivel a kételemű test felett minden polinom megegyezik az ellentettjével, a kódszavakat az jellemzi, hogy oszthatók a kódpolinommal. Néhány gyakran használt CRC-kódpolinom:

CRC-1 (paritásbit)	$x+1$
CRC-5-USB	x^5+x^2+1
CRC-8	x^8+x^2+x+1
CRC-16-IBM	$x^{16}+x^{15}+x^2+1$
CRC-16-CCITT	$x^{16}+x^{12}+x^5+1$
CRC-32 (Ethernet, FDDI, gzip, PNG)	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}$ $+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$
CRC-64-ISO	$x^{64}+x^4+x^3++x+1$

Generátormátrix, ellenőrző mátrix. A K véges test feletti $[n,k]$ lineáris kódnál célszerű a kódolási eljárást egy K^k-t $C\subset K^n$-re képező lineáris leképezésnek választani, ahol C a kódszavak altere. Ezt a mátrixával jellemezhetjük, ez a kódolás *generátormátrix*a. A dekódolásra használható egy $H: K^n \to K^k$ szürjektív lineáris leképezés, amelynek a magja C. Egy ilyen leképezés mátrixát a kód *ellenőrző mátrix*ának nevezzük. Ha $v\in K^n$, akkor az $s=Hv$ *szindróma* pontosan akkor nulla, ha v kódszó.

Szindrómadekódolás. Az előző pont jelöléseivel, ha $s\in K^{n-k}$, legyen $e(s)$ a $\{v : Hv=s\}$ halmaz egy olyan vektora, amelynek súlya minimális. Ezt *mellékosztály-vezető*nek fogjuk nevezni. Ha $c\in K^n$ egy kódszó, $v\in K^n$ a vett szó, $e=v-c$ a hiba, és $w(e)<d/2$, akkor $He(s)=s=Hv=He$, így $w\big(e(s)\big)\le w(e)$, ahonnan $w\big(e-e(s)\big)<d$. De $H\big(e-e(s)\big)=0$, így a különbség kódszó, tehát $e=e(s)$, a hiba javítható. A szindrómadekódolás tárigénye sokkal kisebb, mint a táblázattal való dekódolásé, de még mindig nagyon nagy lehet.

Singleton-korlát. Ha adott egy q elemű ábécé betűiből álló n hosszú kódszavakat tartalmazó C kód, amelynek távolsága d, akkor minden kódszóból elhagyva $d-1$ betűt (ugyanarról a $d-1$ helyről) még mindig különböznek a kódszavak, de csak $n-d+1$ hosszúak. Innen a kódszavak számára azt kapjuk, hogy $\natural(C)\le q^{n-d+1}$, ez a *Singleton-korlát*. Mindkét oldal logaritmusát véve $d+\log_q \natural(C)\le n+1$. Egy lineáris $[n,k,d]_q$-kódnál azt kapjuk, hogy $d+k\le n+1$. Ha egyenlőség áll, a lineáris kódot *maximális távolságú szeparábilis kód*nak, *MDS-kód*nak nevezzük. 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 lineáris kódolást választhatjuk úgy, hogy bármely adott k helyen a kódolandó szó betűi álljanak, így az ellenőrző betűk elválaszthatók a kódolandó betűktől.

* **Hamming-kód.** Az úgynevezett *Hamming-kód* egy hiba javítására alkalmas lineáris kód. Csak a bináris, azaz a kételemű test feletti speciális esettel foglalkozunk. Legyen $r \geq 2$ egész szám, $n = 2^r - 1$, és $k = n - r$. Készítsünk egy $r \times n$ méretű mátrixot, amelyben az $0 < j \leq n$ indexre a j-edik oszlopban a j szám kettes számrendszerbeli felírásának jegyei találhatóak, vagyis a mátrix i-edik sorának j-edik oszlopában $h_{i,j}$ áll ($0 \leq i < r$, $0 < j \leq n$), ahol $j = \sum_{i=0}^{r-1} h_{i,j} 2^i$. (Mivel $1 \leq j \leq n < 2^r$, ezért j biztosan felírható r jeggyel a bináris számrendszerben). Legyen például $r = 3$, akkor $n = 7$ és $k = 4$, továbbá

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

Mivel $r > t \in \mathbb{N}$ esetén 2^t kettes számrendszerben való felírása olyan, amelyben a 0-tól kezdődő indexelés mellett a t-edik és csak a t-edik jegy 1, az összes többi 0, ezért a mátrix r darab oszlopa, amelyek a 2^t indexhez tartoznak, egy egységmátrixot adnak (az előbbi példában az 1., a 2. és 4.), így a mátrix rangja r, tehát a megfelelő H lineáris leképezés szürjektív. Legyen C azon n-dimenziós bináris vektorok halmaza, amelyekre $Hc = 0$. Az ilyen vektorokban k komponens szabadon választható. (Persze nem bármelyik k, csak azok, amelyekkel a kimaradt komponensekhez tartozó indexek a mátrix reguláris részmátrixát határozzák meg, például a fenti példában nem jó választás az utolsó négy komponens, mert a mátrix első három oszlopa lineárisan összefüggő.) Legyenek ezért a kódolandó üzenetek k bitesek, és egy-egy ilyen üzenetet egészítsünk ki r bittel úgy, hogy a kapott n-bites vektor eleme legyen a C halmaznak. Tegyük fel, hogy egy ilyen n-bites üzenet az átvitel során megsérül. Ez azt jelenti, hogy bizonyos bitek az ellenkezőjükre változnak, amit úgy is megkaphatunk, ha ezekhez az eredeti bitekhez 1-et adunk modulo 2, vagyis tegyük fel, hogy c az eredeti n-bites vektor, $e = e_1 \ldots e_n$ a hibavektor, és a vétel helyére $v = c + e$ érkezik. Ha a H mátrix j-edik oszlopát h_j-vel jelöljük, akkor

$$Hv = H(c + e) = Hc + He = He = \sum_{e_j = 1} h_j,$$

hiszen e_i értéke csak 0 és 1 lehet. Ha pontosan egy hiba lépett fel, akkor egy és csak egy indexre, mondjuk s-re lesz e_j nullától különböző, és ekkor $Hv = h_s$. De H konstrukciója következtében h_s éppen s kettes számrendszerbeli felírása, vagyis Hv pontosan a hiba helyét adja.

Legyen például az előbbi 3×7-es mátrixhoz $c = 0100101$, akkor ellenőrizhető, hogy $Hc = 0$, vagyis c kódszó, és tegyük fel, hogy $e = 0000100$, vagyis az 5. bit és csak ez a bit az üzenet átvitele során megsérül. Ekkor a vétel helyén a $v = 0100001$ bitsorozatot kapjuk, és $s = Hv = 101$, ami mint bináris szám éppen 5, a hiba helye. Megváltoztatva a vett üzenetben az 5. bitet, a 0100101 bitsorozatot kapjuk, egyezésben az elküldött bitsorozattal. Amennyiben $e = 0000101$, akkor $s = 010$, és „javítás” után a 0000000 bitsorozatot kapjuk, ami nem egyezik az eredeti sorozattal, vagyis rosszul javítottunk. A Hamming-kód pontosan 1-hibajavító kód. Érdemes megnézni, hogy mi a helyzet, ha a hibavektor $e = 1110000$.

Reed–Solomon-kódok. Legyen K egy véges test, a test egy nem nulla α elemének multiplikatív rendje n és $0 < k < n$. Ekkor az α^i, $0 \le i < n$ elemek páronként különböznek, és mindegyik gyöke az $x^n - 1 \in K[x]$ polinomnak, ezért megadják ezen polinom összes gyökét. Így $x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i)$.

Legyen $m = n - k$ és $g = \prod_{i=1}^{m}(x - \alpha^i)$. Ez a polinom egy K fölötti, m-edfokú főpolinom, és osztója az $x^n - 1$ polinomnak. A $C = \{ag : a \in K[x], \deg(a) < k)\}$ halmaz a g (vagy az α) által generált *Reed–Solomon-kód*, és g a kód *generátorpolinom*ja. A C elemei n-nél alacsonyabb fokú polinomok. A $\varphi : a \mapsto ag$ leképezés K^k injektív lineáris leképezése C-re, amiből az is következik, hogy C a K^n egy k-dimenziós altere.

Most tekintsük a C egy c elemét. Ekkor g osztója c-nek, tehát g minden gyöke gyöke c-nek, vagyis $c(\alpha^i) = 0$, ha $1 \le i \le m$. Fordítva, ha $u \in K^n$, és minden $1 \le i \le m$-re $u(\alpha^i) = 0$, akkor valamennyi i-re $x - \alpha^i$ 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 $1 \le i \le m$-re $\sum_{j=0}^{n-1}(\alpha^i)^j u_j = 0$. Így a $h_{i,j} = \alpha^{ij}$, $1 \le i \le m$, $0 \le j < n$ mátrix egy ellenőrző mátrix, a hozzá tartozó H lineáris leképezésre $Hu = 0$ akkor és csak akkor, ha $u \in C$. Legyen $0 \le j_1 < \ldots j_m < n$, és nézzük a mátrix j_l indexű oszlopait. Ezek a mátrix egy m-edrendű kvadratikus részmátrixát adják, amelynek l-edik oszlopában az i-edik elem $h_{i,j_l} = (\alpha^i)^{j_l} = (\alpha^{j_l})^i$. Most nézzük ezen részmátrix determinánsát. A determináns l-edik oszlopában minden elemből kiemelhető α^{j_l}. 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_l} egymás után következő hatványai állnak, a 0 kitevős hatvánnyal kezdve, vagyis ez egy úgynevezett Vandermonde-típusú determináns. A méret szerinti indukcióval nem nehéz látni, hogy a determináns értéke $\prod_{0 \le s < t < m}\left(\alpha^{j_s} - \alpha^{j_t}\right) \ne 0$ (vonjuk ki minden sorból az felette álló α^{j_1}-szeresét). Ez viszont azt jelenti, hogy a mátrix bármely m oszlopa lineárisan független. Ebből egyrészt az következik, hogy rangja $m = n - k$, tehát a kód egy ellenőrző mátrixát kaptuk, másrészt, hogy egy legfeljebb $m = n - k$ súlyú e vektorra $He \ne 0$, tehát a kód távolsága $d = n - k + 1$, azaz a kód maximális távolságú. Ez mutatja, hogy megfelelő kóddal egynél több hiba is javítható.

A 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 $[n, k]_q$ Reed–Solomon-kód, $m = n - k$, $g = \prod_{i=1}^{m}(x - \alpha^i)$ a kód generátorpolinomja, e a hibavektor, és $L = \prod_{e_j \ne 0}(1 - \alpha^j z)$ az úgynevezett *hibahelypolinom*. Ennek ismeretében a hibák helye meghatározható: megkeressük, hogy mely α^{-j}-k gyökei L-nek, és a j-k megadják a hibák helyét. Legyen $E = \sum_{e_j \ne 0} \alpha^j e_j L_j$ az úgynevezett *hibaérték-polinom*, ahol $L_j = L/(1 - \alpha^j z)$, ha $e_j \ne 0$. Ha még ezt is ismerjük, akkor a hiba javítható, mert rögzített j esetén $L_i(\alpha^{-j})$ akkor és csak akkor nem nulla, ha $i = j$, ezért

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

A következő tétel lehetővé teszi a két polinom meghatározását.

Tétel. *Az előző pont jelöléseivel legyen s a szindrómához tartozó polinom. Tegyük fel, hogy a hibahelyek száma, azaz L fokszáma legfeljebb $m/2$. Végezzünk bővített euklideszi algoritmust az $a = z^r$ és $b = s$ polinomokkal. Az ottani jelölésekkel legyen l a legkisebb index, amelyre $\deg(r_k) < m/2$, és legyen $r_l = ax_l + by_l$. Ekkor $y_l(0) \neq 0$ és $L = y_l/y_l(0)$, $E = r_l/y_l(0)$.*

* **Bizonyítás.** Először megmutatjuk, hogy x^m osztja az $E - Ls$ polinomot. Valóban,

$$\begin{aligned}
E - Ls &= \sum_{e_j \neq 0} \alpha^j e_j L_j - L \sum_{i=0}^{m-1} s_i z^i = \sum_{e_j \neq 0} \alpha^j e_j L_j - \sum_{i=0}^{m-1} L\Big(\sum_{j=0}^{n-1} \left(\alpha^{i+1}\right)^j e_j\Big) z^i \\
&= \sum_{e_j \neq 0} \alpha^j e_j h_j - \sum_{j=0}^{n-1} e_j L \sum_{i=0}^{m-1} \left(\alpha^{i+1}\right)^j z^i = \sum_{e_j \neq 0} \Big(\alpha^j e_j L_j - \alpha^j e_j L \sum_{i=0}^{m-1} \left(\alpha^j\right)^i z^i\Big) \\
&= \sum_{e_j \neq 0} \Big(\alpha^j e_j L_j - \alpha^j e_j L \frac{1 - (\alpha^j z)^m}{1 - \alpha^j z}\Big) \\
&= \sum_{e_j \neq 0} \Big(\alpha^j e_j L_j - \alpha^j e_j L_j \big(1 - \alpha^j z\big) \frac{1 - (\alpha^j z)^m}{1 - \alpha^j z}\Big) \\
&= z^m \sum_{e_j \neq 0} \alpha^{j(m+1)} e_j L_j .
\end{aligned}$$

Ez azt jelenti, hogy alkalmas f polinommal $E = fz^m + Ls$. Így z^m és s legnagyobb közös osztója osztója E-nek, és fokszáma legfeljebb annyi, mint E fokszáma, ami kisebb, mint $m/2$. Így van olyan maradék az euklideszi algoritmus alkalmazása során, amelynek fokszáma kisebb, mint $m/2$. Az $E = fz^m + Ls$ egyenlet y_l-szereséből kivonva az

$$r_l = ax_l + by_l = z^m x_l + sy_l$$

egyenlet L-szeresét, azt kapjuk, hogy

(1) $$Ey_l - Lr_l = (fy_l - Lx_l)z^m.$$

>

Hamming-korlát. Ha egy q elemű ábécé 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

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

Ez a *Hamming-korlát* a kódszavak számára. Ha egyenlőség teljesül, akkor a kódot *tökéletes*nek nevezzük. Mivel kevés tökéletes kód van, a gyakorlatban az alábbi korlát fontosabb.

Singleton-korlát. Ha egy q elemű ábécé n hosszú szavaiból álló C kód távolsága d, akkor minden kódszóból elhagyva $d-1$ betűt (ugyanarról a $d-1$ helyről) még mindig különböznek a kódszavak, de csak $n-d+1$ hosszúak. Innen a kódszavak számára azt kapjuk, hogy $\natural(C) \leq q^{n-d+1}$, ez a *Singleton-korlát*. Ha egyenlőség áll, a kódot *maximális távolságú szeparábilis kód*nak, *MDS-kód*nak 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 ellenőrző 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 mindig feltesszük, hogy a kódolandó üzenetek K^k elemei, azaz a kódábécé elemeiből képzett k-asok

A paritásbites kód általában nem lineáris, de ha páros sok egyesre egészítünk ki, akkor már lineáris $\mathbb{F}_2$ 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 *generátormátrix*a. 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 leképez'ést *ellenőrző leképezés*nek, mátrixát Egy a kód egy *ellenőrző mátrix*ának 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, amelyeknek 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 kódolás*ról 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 álljanak: 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-vezető*nek 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 $w\big(e(s)\big) \leq w(e)$, ahonnan $w\big(e - e(s)\big) < d$. De $H\big(e - e(s)\big) = 0$, így a különbség kódszó, tehát $e = e(s)$, így $c = v - e(s)$, a hiba kijavítottuk. A szindrómadekódolás tárigénye sokkal kisebb, mint a táblázattal való dekódolásé, mert itt csak a melléosztályvezetőket kell tárolni, de még mindig nagyon nagy lehet.

Példa: Fano-kód. A 3.4. ábrán látható *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. Így egy $[7, 4, 3]_2$ lineáris kódot kapunk, a kódszavak: `1110000`, `1001100`, `0101010`, `0011001`, `1000011`, `0100101`, `0100110`, `0000000`, `0001111`, `0110011`, `1010101`, `1100110`, `0111100`, `1011010`, `1011001`, `1111111`. Ez a kód tökéletes kód, de nem MDS-kód. Egy generátormátrixa (a szokásos bázisban) például a

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

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

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

generátormátrixot 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, $e_1, e_2, \ldots, e_7$ 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

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

ellenőrző mátrixot kapjuk. A `000`, `100`, `010`, `001`, `110`, `101`, `011`, `111` szindrómákhoz tartozó mellékosztályvezetők rendre `0000000`, `0000100`, `0000010`, `0000001`, `0010000`, `0100000`, `1000000`, `0001000`. Legyen például a kód $c = 0100101$, akkor ellenőrizhető, hogy $Hc = 0$, vagyis c kódszó. Ha a hibavektor $e = 0000100$, vagyis az 5. bit és csak ez a bit az üzenet átvitele során megsérül, akkor a vétel helyén a $v = 0100001$ bitsorozatot kapjuk, és $s = Hv = 100$, amihez az e hibavektor tartozik. Megváltoztatva a vett üzenetben az 5. bitet, a 0100101 bitsorozatot kapjuk, egyezésben az elküldött bitsorozattal. Amennyiben két hiba van, például $e = 0000101$, akkor $s = 101$, és „javítás” után a 0110001 bitsorozatot kapjuk, ami nem egyezik az eredeti sorozattal, vagyis rosszul javítottunk. A Fano-kód pontosan 1-hibajavító kód. Ha a hibavektor $e = 1110000$, akkor észre sem vesszük a hibát.

* **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 $[n, k, d]_2$ kód, ahol $n = 2^t$, $d = 2^r$, és $k = \sum_{j=0}^{r} \binom{t}{j}$. A $t = 5$, $r = 4$ paraméterekkel adódó $[32, 6, 16]_2$ 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 az $\mathbb{F}_q^m$ vektorok, amelyeknek 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 ellenőrző mátrix bármely két oszlopa lineárisan független, a kód távolsága legalább 3. Több nem lehet, mivel a kód tökéletes 1-hibajavító: $q^k\bigl(1 + n(q-1)\bigr) = q^k(1 + q^m - 1) = q^m + k = q^n$. A hibajavítás a szindróma segítségével könnyen elvégezhető: ha csak egy hiba 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.

* **Feladat [7].** Készítsünk egy olyan Hamming-kódot a háromelemű test felett, amelynek hossza 13, dimenziója pedig 10. Mutassuk meg ennek segítségével, hogy a TOTÓ-n elegendő $3^{11} = 59049$ hasábot megjátszani, hogy biztosan legyen legalább 12 találatunk.

Polinomkódok. Lineáris kódnál a szavak k hosszú kódolandó szavak tekinthetők $\mathbb{F}_q$ feletti k-nál alacsonyabb fokú polinomnak is, a betűket nullától indexelve. Ha a kódolást úgy végezzük, hogy ezt a p 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 $p \mapsto pg$ leképezés kölcsönösen egyértelmű. Az ilyen típusú lineáris kódolás *polinomkódolás*nak nevezzük, g a kód *generátorpolinom*ja. A generátorpolinomról feltehetjük (és a továbbiakban fel is tesszük), 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 mindig 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 8.3.57. 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 $g(x)|x^\ell - 1$, akkor $n = \ell$ esetén a kód *ciklikus kód*: ha $a_0a_1 \dots a_{n-2}a_{n-1}$ egy kódszó, akkor $a_{n-1}a_0a_1 \dots a_{n-2}$ is kódszó:

$$\begin{aligned} &a_{n-1} + a_0x + a_1x^2 + \cdots a_{n-2}x^{n-1} \\ &\quad = x(a_0 + a_1x + \cdots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}) - a_{n-1}(x^n - 1), \end{aligned}$$

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 a az eredeti üzenet betűi állnak. Mivel az x^m-vel 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) $r(x) = -r(x)$. Néhány gyakran használt CRC-generátorpolinom:

Név	Generátorpolinom	Távolság	Maximális kódhossz
CRC-1 (paritásbit)	$x+1$	2	–
CRC-5-USB	x^5+x^2+1	3	2^5-1
CRC-8	x^8+x^2+x+1	4	2^7-1
CRC-16-IBM	$x^{16}+x^{15}+x^2+1$	4	$2^{15}-1$
CRC-16-CCITT	$x^{16}+x^{12}+x^5+1$	4	32767
CRC-32 (Ethernet, FDDI, gzip, PNG)	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}$ $+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$	3	$2^{32}-1$
CRC-64-ISO	$x^{64}+x^4+x^3+x+1$	3	2^64-1

* **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-hatvány nem

lehet a kódpolinomok között. A kód súlya mindaddig nagyobb, mint kettő, ameddig meg nem jelenik a kódpolinomok között egy $x^{j+l} + x^j = x^j(x^\ell - 1)$ alakú polinom. Mivel a konstans tag nem nulla, ez csak akkor lehet, ha $g(x)|x^\ell - 1$. Ekkor viszont $x^{i\ell} - 1 = (x^\ell - 1)(x^{(i-1)\ell} + x^{(i-2)\ell} + \cdots + 1)$ is, és így $x^{i\ell+j} - x^j$ is többszöröse g-nek. Ha g egy m-ed fokú ($m > 1$) irreducibilis polinom, akkor a 8.3.57. tétel szerint $g(x)|x^{2^m} - x$-nek, azaz $g(x)|x^{2^m-1} - 1$. Legyen ℓ a legkisebb olyan érték, amelyre $g(x)|x^\ell - 1$. Mivel $2^m - 1 = i\ell + j$ esetén $x^j - 1 = x^{2^m-1} - 1 - (x^{i\ell+j} - x^j)$ is osztható $g(x)$-szel, $\ell|2^m - 1$. 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 A fenti gondolatmenet itt is érvényes, a legkisebb ℓ kitevőre, amelyre $x^\ell - 1$ többszöröse a kódpolinomnak, $\ell|2^m - 1$, aminek alapján ℓ meghatározható. Itt a kód súlya legalább négy, hiszen nagyobb, mint 2, és páros. Megjegyezzük, hogya 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, így távolsága kisebb, mint 15; ha $n = 124$, akkor a kód nem 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 $x^11 + x^10 + x^6 + x^5 + x^4 + x^2 + 1$ 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 $x_1, x_2, \ldots, x_m$ egy K test elemei, akkor az*

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_m \\ x_1^2 & x_2^2 & x_3^2 & \ldots & x_m^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{m-1} & x_2^{m-1} & x_3^{m-1} & \ldots & x_m^{m-1} \end{pmatrix}$$

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. $\square$

Reed–Solomon-kódok. Legyen most K egy tetszőleges véges test, alkossák az ábécét ennek elemei, a K elemszámát jelo"lje 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 a $z^n - 1 \in K[z]$ polinomnak, ezért megadják ezen polinom összes gyökét. Így $z^n - 1 = \prod_{i=0}^{n-1} (z - \alpha^i)$.

Legyen $0 < k < n$, $m = n - k$ és $g = \prod_{i=1}^{m} (z - \alpha^i)$. Ez a polinom egy K fölötti, m-edfokú főpolinom, és nyilván osztója 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 kódpolinomok C halmazának egy c elemét. Mivel g osztója c-nek, g minden gyöke gyöke c-nek is, vagyis $c(\alpha^i) = 0$, ha $1 \leq i \leq m$. 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 $\sum_{j=0}^{n-1} (\alpha^i)^j u_j = 0$. Így 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 $0 \leq j_1 < \ldots j_m < n$, és nézzük a mátrix j_l indexű oszlopait. Ezek a mátrix egy m-edrendű kvadratikus részmátrixát adják, amelynek l-edik oszlopában az i-edik elem $h_{i,j_l} = (\alpha^i)^{j_l} = (\alpha^{j_l})^i$. Most nézzük ezen részmátrix determinánsát. A determináns l-edik oszlopában minden elemből kiemelhető α^{j_l}. 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_l} egymás után következő hatványai állnak, a 0 kitevős hatvánnyal kezdve, vagyis ez egy Vandermonde-determináns. Így az előző állítás szerint a determináns értéke $\prod_{0 \leq s < t < m} \left(\alpha^{j_s} - \alpha^{j_t}\right) \neq 0$, ami azt jelenti, hogy a mátrix bármely m oszlopa lineárisan független. Ebből a kód d távolsága nagyobb, mint m, és így (mivel nagyobb nem lehet) $d = n - k + 1$, azaz a kód MDS-kód, tehát elég nagy m esetén to"bb hiba is javítható.

A 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 *hibaérték-polinom*, 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 $\deg(r_l) < m/2$, 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,

$$\begin{aligned}
E(z) - L(z)s(z) &= \sum_{\{j:e_j\neq 0\}} \alpha^j e_j L_j(z) - L(z)\sum_{i=0}^{m-1} s_i z^i \\
&= \sum_{\{j:e_j\neq 0\}} \alpha^j e_j L_j(z) - \sum_{i=0}^{m-1} L(z)\Big(\sum_{j=0}^{n-1} \left(\alpha^{i+1}\right)^j e_j\Big) z^i \\
&= \sum_{\{j:e_j\neq 0\}} \alpha^j e_j L_j(z) - \sum_{j=0}^{n-1} e_j L(z) \sum_{i=0}^{m-1} \left(\alpha^{i+1}\right)^j z^i \\
&= \sum_{\{j:e_j\neq 0\}} \Big(\alpha^j e_j L_j(z) - \alpha^j e_j L(z) \sum_{i=0}^{m-1} \left(\alpha^j\right)^i z^i\Big) \\
&= \sum_{\{j:e_j\neq 0\}} \Big(\alpha^j e_j L_j(z) - \alpha^j e_j L(z) \frac{1-(\alpha^j z)^m}{1-\alpha^j z}\Big) \\
&= \sum_{\{j:e_j\neq 0\}} \Big(\alpha^j e_j L_j(z) - \alpha^j e_j L_j(z)\big(1-(\alpha^j z)^m\big)\Big) \\
&= z^m \sum_{\{j:e_j\neq 0\}} \alpha^{j(m+1)} e_j L_j(z).
\end{aligned}$$

Ez azt jelenti, hogy alkalmas $f(z)$ polinommal $E(z) = f(z0z^m + L(z)s(z)$. Így z^m és $s(z)$ legnagyobb közös osztója osztója $E(z)$-nek, és fokszáma legfeljebb annyi, mint $E(z)$ fokszáma, ami kisebb, mint $m/2$. Így 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

$$E(z)y_l(z) - L(z)r_l(z) = \big(f(z)y_l(z) - L(z)x_l(z)\big)z^m. \tag{1}$$

- 200/9 :

$<$

konstanssal. Innnen $E = cr_l$ ugyanazzal a konstanssal. Mivel L főpolinom, kapjuk az

$>$

konstanssal. Innnen $E = cr_l$ ugyanazzal a konstanssal. Mivel L konstans tagja 1, kapjuk az

- 204/−10 :

$<$

ha f vagy g (vagy mindkettő) véges sok indexre nincs értelmezve. Gyakran pontatlanul

$>$

ha f vagy g (vagy mindkettő) véges sok indexre nincs értelmezve. (Ugyanezt a kapcsolatot úgy is szokás jelölni, hogy $g \preccurlyeq f$ vagy $f \succcurlyeq g$, illetve hogy $f \in \Omega(g)$, azaz $\Omega(g)$ az összes olyan f függvények halmaza, amelyekhez van olyan C és N, hogy ha $n \ge N$, akkor $C\big|f(n)\big| \ge \big|g(n)\big|$. Az $O(g)$ és $\Omega(g)$ halmazok metszetét $\Theta(g)$ jelöli; $f \in \Theta(g)$ helyett azt is szokás írni, hogy $f \asymp g$.) Gyakran pontatlanul

- 211/9...10 :

$<$

mozdítsa a fejeket, és melyik állapotba menjen át. Ha kell, balra lép egy mezőcsoportot, majd jobbra visszafelé haladva a megfelelő helyeken ír a szalagra, és megfelelően moz-

$>$

mozdítsa a fejeket, és melyik állapotba menjen át. Jobbra visszafelé haladva a megfelelő helyeken ír a szalagra, és megfelelően moz-

- 211/12...13 :

$<$

mozog, minden fejnek „megelőlegezi”, hogy balra fog lépni, és balra mozdítja el, kivéve a bal szélső mezőcsoportban talált fejeket. Ha mégsem balra mozdul a fej, jobbra haladva

$>$

mozog, minden fejnek „megelőlegezi”, hogy balra fog lépni, és balra mozdítja el. Ha mégsem balra mozdul a fej, jobbra haladva

- 211/18 :

$<$

legfeljebb még egy mezőcsoportot haladunk balra, majd visszafelé legfeljebb $2n+3$ mező-

$>$

még egy mezőcsoportot haladunk balra, majd visszafelé legfeljebb $2n+3$ mező-

- 214/2 :

  $<$

lepjünk rajta balra.

  $>$

lépjünk rajta balra.

- 214/17 . . . 19 :

  $<$

s_1: Ha $a_1 = a_2$, akkor a második és harmadik szalagon lépjünk balra, a harmadik szalagon lépjünk jobbra a bal szélső nem üres mezőre, és menjünk a v_1 állapotba. Ha $a_1 \neq a_2$, akkor 2-n lépjünk balra, és menjünk a t_1 állapotba.

  $>$

s_1: Ha $a_1 = a_2$, akkor a második szalagon lépjünk balra, a harmadik szalagon lépjünk jobbra a bal szélső nem üres mezőre, és menjünk a v_0 állapotba. Ha $a_1 \neq a_2$, akkor a második szalagon lépjünk balra, a harmadikon jobbra, és menjünk a t_1 állapotba.

- 214/$-16 \ldots -15$:

  $<$

e_0: Ha $a_3 \neq \sqcup$, akkor írjuk a_3-at a második szalagra, és a második és harmadik szalagon lépjünk balra; egyébként menjünk az e_1 állapotba.

  $>$

e_0: Ha $a_3 \neq \sqcup$, akkor írjuk a_2-t a harmadik szalagra, és a második és harmadik szalagon lépjünk balra; egyébként menjünk az e_1 állapotba.

- 214/$-12 \ldots -11$:

  $<$

e_2: Az első szalagon lépjünk az a_2 által megadott módon, a harmadik szalagon pedig lépjünk jobbra, és menjünk a v_1 állapotba.

  $>$

e_2: Az első szalagon lépjünk az a_2 által megadott módon, a második és harmadik szalagon pedig lépjünk jobbra, és menjünk a v_1 állapotba.

- 214/$-2 \ldots -1$:

  $<$

v_4: Ha $a_2 \neq \sqcup$, akkor a második szalagon lépjünk balra, egyébként menjünk a v_6 állapotba.

  $>$

v_4: Ha $a_2 = \sqcup$, akkor a második szalagon lépjünk balra, egyébként menjünk a v_5 állapotba.

- 215/2 :

  $<$

  harmadik szalagon is lépjünk balra, és menjünk az s állapotba.

  $>$

  harmadik szalagon lépjünk balra, és menjünk az s állapotba.

- 222/−13 :

  <

  * **Markov-automaták.** Egy *Markov-automata* egy

Post-gép. Ez a gépmodell adattárolóként sort (first in first out vagy FIFO adattárat) használ. Ez egy, a gép véges, legalább két elemű A ábécéjéből képzett $\gamma \in A^*$ szó. A gép képes érzékelni, ha $\gamma = \emptyset$, azaz γ az üres szó. Ha $\gamma \in A^+$, akkor legyen $\mathrm{head}(\gamma)$ a γ első betűje, $\mathrm{tail}(\gamma)$ pedig a γ maradék részéből álló szó; legyen $\mathrm{tail}(\emptyset) = \emptyset$. Az A ábécének itt is van egy kitüntetett betűje, amit most $\sharp$ fog jelölni, a maradék ábécé $A_0 = A \setminus \{\sharp\}$. Maga a gép egy véges irányított címkézett gráf, amely négy különböző típusú csúcsot tartalmaz: van pontosan egy „start" címkéjű csúcs, ennek befoka nulla, kifoka egy, innen indul a gép. Vannak „halt" címkéjű csúcsok, ezek kifoka nulla, ha a gép ilyenbe jut, akkor megáll. A gép bemenete, illetve kimenete γ értéke a számítás kezdetén, illetve végén. A „$\gamma \leftarrow \gamma a$" címkéjű csúcsok értékadás írnak le, egy a kifokuk; ezeknél a az A ábécé bármely konkrét betűje lehet. Végül a „$\gamma \leftarrow \mathrm{tail}(\gamma)$" címkéjű vizsgáló csúcsok kifoka $\natural(A)+1$, és a kimenő élek címkéje $\emptyset$, illetve az A ábécé betűi; ezekből a csúcsokból a gép a $\emptyset$ címkéjű élen megy tovább, ha a γ üres szó volt, és a $\mathrm{head}(\gamma)$ címkéjű élen egyébként.

Tétel: Post-gép szimulálása Turing-gépen. *Bármely Post-gép szimulálható egyszalagos Turing-gépen ugyanazzal az ábécével.*

Bizonyítás. Először feltesszük, hogy a Turing-gép ábécéje $A \cup \{\llcorner\!\lrcorner\}$, ahol A a Post-gép ábécéje és $\llcorner\!\lrcorner \notin A$. A Turing-gép belső állapotai alapvetően a Post-gép csúcsainak felelnek meg, a szalagra pedig a γ szó van írva. A „$\gamma \leftarrow \gamma a$" típusú csúcsoknál a Turing-gép az γ szótól jobbra lévő első $\llcorner\!\lrcorner$ jelen áll, ide az $a \in A$ betűt írja, és ha a következő csúcs is ilyen típusú, akkor az annak megfelelő b' belső állapotba megy át. Ha a csúcs „$\gamma \leftarrow \mathrm{tail}(\gamma)$" típusú, akkor a Turing-gép a γ szó bal szélső betűjén áll, azt $\llcorner\!\lrcorner$ üres jellel írja felül, az olvasott betűnek megfelelően megy tovább ($\llcorner\!\lrcorner$ olvasása üres γ szót jelent), és ha a következő csúcs is ilyen típusú, akkor az annak megfelelő b' belső állapotba megy át. Különböző típusú csúcsok esetén egy $b'_<$ illetve $b'_>$ belső állapotot iktatunk közbe, amelyben a gép megkeresi az α szó megfelelő végét. A „halt" állapotba lépés előtt az α jobb szélső betűjére állunk. Az új $\llcorner\!\lrcorner$ betű bevezetését nyilván elkerülhetjük betűpárok használatával.

Tétel: Turing-gép szimulálása Post-gépen. *Bármely egyszalagos Turing-gép szimulálható Post-gépen ugyanazzal az ábécével.*

Bizonyítás. Először feltesszük, hogy a Post-gép ábécéje $A \cup \{\sharp\}$, ahol A a Turing-gép ábécéje a $\llcorner\!\lrcorner$ üres jellel és $\sharp \notin A$. A Turing-gép belső állapotainak a Post-gép bizonyos „$\alpha \leftarrow \mathrm{tail}(\alpha)$" típusú csúcsai felelnek meg, és a Post-gép a $\gamma \in A \cup \{\sharp\}$ szóval dolgozik, amely $\beta\sharp\alpha$ alakú, ahol β a Turing gép feje alatt és attól jobbra álló betűkből álló szó, α pedig a fejtől balra álló betűkből álló szó, természetesen mindkettő az utána illetve előtte álló végtelen $\llcorner\!\lrcorner$-sorozat nélkül, a $\sharp$ jel pedig a „töréspontot" jelzi.

Miután a Post-gép „elolvassa a fej alatt álló betűt", ha a Turing-gépnek jobbra kell lépnie, akkor látszólag egyszerű dolga van: a szalagra írandó betűt hozzáírja γ végéhez.

Ha azonban β egyetlen betűből állt, akkor a következő lépésben $\llcorner\!\lrcorner$ jelet kellene olvasnia. Ezért mindig egyszer „körbeléptetjük” a γ szót: először elolvassuk a következő betűt: ha ez $\sharp$, akkor előbb egy $\sharp$, majd egy $\llcorner\!\lrcorner$, aztán még egy $\sharp$ jelet írunk γ végére, ha pedig ez nem $\sharp$, akkor egy $\sharp$ jelet, majd az olvasott betűt írjuk γ végére, és folytatjuk, amíg végül egy $\sharp$ jelet olvasunk és írunk. A „körbeléptetés” befejezéséhez egy újabb $\sharp$ jel olvasásáig folytatjuk az olvasás és írást, de ezt a $\sharp$ jelet már nem írjuk ki.

Ha az aktuális betű elolvasása után a Turing-gépnek helyben kell maradnia, akkor az eljárás valamivel egyszerűbb: először egy $\sharp$ jelet írunk γ végére, majd az írandó betűt, és „körbeléptetjük” a γ szót.

Végül ha az aktuális betű elolvasása után a Turing-gépnek balra kell lépnie, akkor két „körbeléptetést” alkalmazunk: Először egy $\sharp$ jelet írunk γ végére, majd az írandó betűt, és körbeléptetünk, de az első $\sharp$ jel elérése után „késleltetéssel”, azaz csak két betű kiolvasása után írjuk vissza az elsőt, majd egy újabb betű kiolvasása után a másodikat, stb. Mikor $\sharp$ jelet olvasunk, akkor egy $\sharp$ jelet viszünk ki, és csak aztán visszük ki az előzőleg olvasott betűt, ami eredetileg α utolsó betűje volt. Azt az esetet is kezelni tudjuk, amikor α üres volt. Újabb körbeléptetéssel előállíthatjuk az új $\gamma' = \beta'\sharp\alpha'$ szót, és a b' belső állapotnak megfelelő csúcsba mehetünk.

* **Markov-automaták.** Egy *Markov-automata* egy

>

• 225/−6 . . . − 5 :

<

egy közelítésének) definiálja, amelyre $s(x) = x - x^3/6 + x^5/120$. A λ-kalkulus vázlatos ismertetése magyar nyelven Penrose [67] könyvében található meg. A λ-kalkulus is ek-

>

egy közelítésének) definiálja, amelyre $s(x) = x - x^3/6 + x^5/120$. A λ-kalkulus részletes ismertetése magyar nyelven Csörnyei [8] könyvében található meg. A λ-kalkulus is ek-

• 225/−1 :

<

rendszer is tartalmaz függvényabsztrakciót műveletként.

>

rendszer is tartalmaz függvényabsztrakciót műveletként.

Korlátozott gépmodellek. Egy *véges automata* lényegében egy olyan Turing-gép, amely működése során nem léphet jobbra. Hogy az outputot a szokásos módon kapjuk, inkább azt kötjük ki, hogy ha a gép (bármelyik szalagján) jobbra lép, akkor többé már nem írhat semmelyik szalagra.

Egy m *veremtáras gép* lényegében egy olyan Turing-gép $k > m$ szalaggal, amelynek az input és output szalagok kívül van m darab szalagja, a *vermek*, amelyeken jobbra is léphet, de akkor törölnie kell, amit olvasott, a többi szalagon pedig nem léphet jobbra. Hogy az outputot a szokásos módon kapjuk, itt is inkább azt kötjük ki, hogy ha a gép (bármelyik nem verem szalagján) jobbra lép, akkor többé már nem írhat semmelyik szalagra. Nem nehéz belátni, hogy $m > 1$ esetén a gép szimulálhat Turing-gépet, $m = 1$

esetén azonban megmutatható, hogy a gép „többet tud”, mint egy véges automata, de „kevesebbet tud”, mint egy Turing-gép. A korlátozott gépmodellek fontos szerepet játszanak az informatikában, más tárgyakból lesz róluk szó.

- $233/-14\ldots-13$:

$<$

(7) A $q(n,m)$ „hányados” függvény rekurzív definíciója: $q(0,m)=0$ és $q(n^+,m)=q(n,m)+\big[(n \bmod m)=m^-\big]$.

$>$

(7) A $\mathrm{quo}(n,m)$ „hányados” függvény rekurzív definíciója: $\mathrm{quo}(0,m)=0$ és

$$\mathrm{quo}(n^+,m)=\mathrm{quo}(n,m)+\big[(n \bmod m)=m^-\big].$$

- $240/14$:

$<$

[7] Csákány B.: *Algebra. Kézirat.* Tankönyvkiadó, Budapest, 1980.

$>$

[7] Csákány B.: *Algebra. Kézirat.* Tankönyvkiadó, Budapest, 1980.

[8] Csörnyei Z.: *Lambda-kalkulus. A funkcionális programozás alapjai.* TypoTeX, Budapest, 2007.