4. Számelmélet, gráfok, kódoláselmélet

Számelmélet

Relációk, rendezések

Alapfogalmak

- Az (x, y) ***rendezett pár***, ha $(x, y) = (u, v) \iff x = u \ \wedge \ y = v$.
  Ezt a tulajdonságot halmazokkal definiáljuk:
  $$(x, y) := \{\{x\}, \{x, y\}\}$$
- Az X, Y ***halmazok Descartes-szorzata*** vagy direkt szorzata:
  $$X \times Y := \{(x, y) : x \in X, y \in Y\}$$
- Ha X, Y halmazokra $R \subset X \times Y$, akkor R ***reláció*** X és Y között.
- Egy halmazt ***binér relációnak*** nevezünk, ha minden eleme rendezett pár.
  Ha R binér reláció és $(x, y) \in R$, akkor használható a következő jelölés: xRy
- Az R binér reláció ***értelmezési tartománya***: $\mathrm{dmn}(R) := \{x \mid \exists y : (x, y) \in R\}$
- Az R binér reláció ***értékkészlete***: $\mathrm{rng}(R) := \{y \mid \exists x : (x, y) \in R\}$
- Egy R binér reláció ***inverze***: $R^{-1} := \{(a, b) : (b, a) \in R\}$
- Legyen R binér reláció, és A halmaz. Az A ***halmaz képe***: $R(A) := \{y \mid \exists x \in A : (x, y) \in R\}$
- Az R és S binér relációk ***kompozíciója***:
  $$R \circ S := \{(x, y) \mid \exists z : (x, z) \in S \ \wedge \ (z, y) \in R \ \}$$

Tulajdonságok

Az R egy X-beli binér reláció (azaz $R \subset X \times X$), és $\forall x, y, z \in X$, ekkor a reláció

reflexív	$(x, x) \in R$
irreflexív	$(x, x) \notin R$
szimmetrikus	$(x, y) \in R \Longrightarrow (y, x) \in R$
antiszimmetrikus	$(x, y) \in R \ \wedge \ (y, x) \in R \Longrightarrow x = y$
szigorúan antiszimmetrikus	$(x, y) \in R \Longrightarrow (y, x) \notin R$
tranzitív	$(x, y) \in R \ \wedge \ (y, z) \in R \Longrightarrow (x, z) \in R$
trichotóm	Ha minden $x, y \in X$ esetén az alábbiak közül pontosan egy teljesül *a)* $x = y$ *b)* $(x, y) \in R$ *c)* $(y, x) \in R$
dichotóm	$(x, y) \in R \ \vee \ (y, x) \in R$

Rendezések

Legyen X halmaz, R,S relációk X-beliek.

- Az R binér reláció ***ekvivalenciareláció***, ha
  - Reflexív
  - Szimmetrikus
  - Tranzitív
- Az R binér reláció ***részbenrendezés***, ha
  - Reflexív
  - Antiszimmetrikus
  - Tranzitív
- Az R binér reláció ***(teljes) rendezés***, ha
  - Részbenrendezés, és
  - Dichotóm
- X részhalmazainak egy $\mathcal{O}$ rendszerét ***osztályozás***nak hívjuk, ha $\mathcal{O}$ páronként diszjunkt nemüres halmazokból álló halmazrendszer, melyre $\bigcup \mathcal{O} = X$.

  Tétel: Egy ekvivalenciareláció meghatároz egy osztályozást.
  Fordítva: $\mathcal{O}$ osztályozásra, az $R = \bigcup \left\{ Y \times Y : Y \in \mathcal{O} \right\}$ ekvivalenciareláció.

Korlátok

Legkisebb, legnagyobb, minimális, maximális elem

X halmazbeli *részbenrendezés* ($\preccurlyeq$) *legkisebb* (legelső) eleme egy olyan $x \in X$, hogy

$$\forall y \in X : x \preccurlyeq y$$

(Ilyen nem biztos, hogy létezik, de ha igen, akkor egyértelmű).
X halmazbeli *részbenrendezés* ($\preccurlyeq$) *legnagyobb* (utolsó) eleme egy olyan $x \in X$, hogy

$$\forall y \in X : y \preccurlyeq x$$

- x-et ***minimálisnak*** nevezzük, ha nincs nála kisebb elem,
- x-et ***maximálisnak*** nevezzük, ha nincs nála nagyobb elem.

(Szemben a legkisebb/legnagyobb elemekkel, minimális/maximális elemből több is lehet.
Ha viszont X rendezett, akkor legkisebb=minimális, legnagyobb=maximális.)

Alsó, felső korlát

X részbenrendezett halmaz, $Y \subset X$. Az $x \in X$ elem az Y

- *alsó korlátja*, ha $\forall y \in Y : x \preccurlyeq y$.
- *felső korlátja*, ha $\forall y \in Y : y \preccurlyeq x$.

Látható, hogy x nem feltétlenül eleme Y-nak, sőt az is lehet, hogy Y-nak nincs alsó/felső korlátja, vagy akár több is van. Ha azonban $x \in Y$, akkor egyértelmű és ez Y legkisebb eleme.

Infimum, szuprémum

Ha az alsó korlátok között van *legnagyobb elem*, azt Y alsó határának, ***infimum***ának nevezzük. (Jelölése: $\inf Y$)
Ha a felső korlátok között van *legkisebb elem*, azt Y felső határának, szuprémumának nevezzük. (Jelölése: $\sup Y$)

Alsó, felső határ tulajdonság

X részbenrendezett halmaz. Ha $\forall\ \emptyset \neq Y \subset X : Y$ felülről korlátos és van ***szuprémum***a, akkor felső határ tulajdonságú. Illetve ha $\forall\ \emptyset \neq Y \subset X : Y$ alulról korlátos és van infimuma, akkor alsó határ tulajdonságú.

Függvények és műveletek

Függvények

Egy f reláció ***függvény***, ha

$$(x, y) \in f\ \wedge (x, y')\ \in f \Longrightarrow y = y'$$

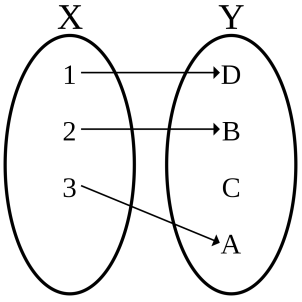
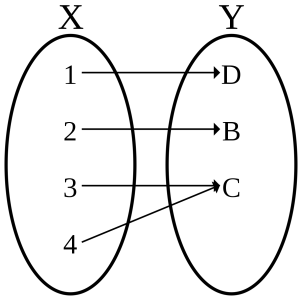
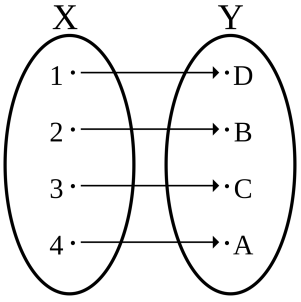
Más szóval minden x-hez legfeljebb egy olyan y létezik, hogy $(x, y) \in f$

Így minden $x \in \mathrm{dmn}(f)$-re az $f(x) = \{y\}$.
Jelölése: $f(x) = y$ vagy $f : x \mapsto y$ vagy $f_x = y$.

Értelmezési tartomány, értékkészlet

Az $f : X \to Y$ jelölést használjuk, ha $\mathrm{dmn}(f) = X$.
Az $f \in X \to Y$ jelölést használjuk, ha $\mathrm{dmn}(f) \subset X$ (amikor $\mathrm{dmn}(f) \subsetneq X$ is előfordulhat).
Mindkét esetben $\mathrm{rng}(f) \subset Y$.

Az f függvény

injektív kölcsönösen egyértelmű	***szürjektív***	***bijektív***
$f(x) = y\ \wedge\ f(x') = y\ \Longrightarrow\ x = x'$ Ez azzal ekvivalens, hogy f^{-1} reláció is függvény.	$\forall y \in Y : \exists x \in X : f(x) = y$ Azaz $rng(f) = Y$. Tehát az f függvény az egész Y-ra képez.	*injektív és szürjektív*
		

Indexelt család

Az x függvény i helyen felvett értékét x_i-vel is szoktuk jelölni.

Ilyenkor gyakran

- $\mathrm{dmn}(f) = I$ értelmezési tartományt ***indexhalmaz***nak, az
- elemeit ***index***eknek,
- $\mathrm{rng}(f)$-et ***indexelt halmaz***nak, és magát
- az x függvényt ***indexelt család***nak szoktuk nevezni.

Műveletek

- **Binér művelet**: $f : \mathbf{X} \times \mathbf{X} \to X$ függvény az X halmazon.
- **Unér művelet**: $f : \mathbf{X} \to X$ függvény az X halmazon.
- **Nullér művelet**: $f : \{\emptyset\} \to X$ az X halmazon. (Gyakorlatilag elemkiválasztás)

Tulajdonságok

- Legyen $\boxplus, \circledcirc$ binér műveletek X-en. $\forall x, y, z \in X$.
  1. $\boxplus$ ***asszociatív***, ha
  $$(x \boxplus y) \boxplus z = x \boxplus (y \boxplus z)$$
  2. $\boxplus$ ***kommutatív***, ha
  $$x \boxplus y = y \boxplus x$$
  3. $\boxplus$ ***disztributív*** a $\circledcirc$-ra, ha
  $$x \boxplus (y \circledcirc z) = (x \boxplus y) \circledcirc (x \boxplus z) \quad \text{- baloldali}$$
  $$(y \circledcirc z) \boxplus x = (y \boxplus x) \circledcirc (z \boxplus x) \quad \text{- jobboldali}$$
- Legyen $\circledcirc$ binér művelet X-en és $\boxdot$ binér művelet Y-on $f : X \to Y$ ***művelettartó*** ha:
$$\forall x_1, x_2 \in X : f(x_1 \circledcirc x_2) = f(x_1) \boxdot f(x_2)$$

Számfogalom, komplex számok

Számfogalom

Algebrai struktúrák

Legyen G halmaz és $\star$ egy művelet

Semleges (egység) elem: $a \in G$ semleges elem, ha $\forall g \in G : a \star g = g \star a = g$.

Inverz elem: $g, g^{-1} \in G$ és $a \in G$ semleges elem, akkor a g^{-1} a g inverze, ha
$$g \star g^{-1} = a \text{ és } g^{-1} \star g = a$$

Nullosztó: x, y nullától különböző elemek, de $x \cdot y = 0$. (x bal oldali, y jobb oldali nullosztó)

- A G halmaz egy $\star$ művelettel, azaz a $(G, \star)$ párt ***grupoid***nak nevezzük.
- Ha egy grupoidban a $\star$ *művelet asszociatív*, akkor a grupoid ***félcsoport***.
- *Semleges elemes félcsoportot* ***monoid***nak nevezzük.
- Ha egy *monoidban minden elemnek van inverze*, akkor ***csoport***ról beszélünk.
- Ha egy *csoportban a művelet kommutatív*, akkor ***Abel-csoport***.
- Az $(R, +, \cdot)$ ***gyűrű***, ha
  - az összeadással Abel-csoport,
  - a szorzással félcsoport és
  - teljesül mindkét oldali disztributivitás.

  Ha a *szorzás kommutatív*, akkor ***kommutatív gyűrű***.

  Ha a *szorzásnak van egységeleme*, akkor ***egységelemes gyűrű***.
- A nullosztó mentes kommutatív gyűrűt ***integritási tartomány***nak nevezzük.
- Az R integritási tartomány ***rendezett integritási tartomány***, ha rendezett halmaz, továbbá az összeadás és szorzás monoton.
  - *Összeadás monoton:* $x, y, z \in R$ *és* $x \leq y \;\Rightarrow\; x + z \leq y + z$
  - *Szorzás monoton:* $x, y \in R$ *és* $x, y \geq 0 \;\Rightarrow\; x \cdot y \geq 0$
- Egy R gyűrűt, ha $R \setminus \{0\}$ *szorzással Abel-csoport*, akkor ***test***nek nevezzük.
- Ha egy test rendezett integritási tartomány, akkor ***rendezett test***.

Természetes számok

Legyen $^+ : \mathbb{N} \to \mathbb{N}$ unér művelet. Az alábbi feltételeket ***Peano-axiómák***nak nevezzük:

1. $0 \in \mathbb{N}$	(a 0 természetes szám)
2. $\forall n \in \mathbb{N}, \exists! n^+ \in \mathbb{N}$, *hogy* $n \neq n^+$	(n *rákövetkezője*)
3. $\nexists n \in \mathbb{N},$ hogy $n^+ = 0$	(nem létezik olyan természetes szám, aminek a 0 a rákövetkezője)
4. Ha $n,\ m\ \in \mathbb{N},$ és $m^+ = n^+,$ *akkor* $n = m$	(a $^+$ művelet injektív)
5. $A \subseteq \mathbb{N},\ 0 \in A,$ továbbá $\forall n \in A : n^+ \in A,$ akkor $A = \mathbb{N}$	(a matematikai indukció elve)

Tétel. Van olyan $\left(\mathbb{N}, (0, ^+)\right)$ pár, amely eleget tesz a Peano axiómáknak.

Műveletek

- Összeadás
  $k, m, n \in \mathbb{N}$, akkor:
  1. *Asszociatív*: $(k + m) + n = k + (m + n)$
  2. *Kommutatív*: $n + k = k + n$
  3. $n + 0 = 0 + n = n$ *(**0**: additív zéruselem)*
  4. *Egyszerűsítési szabály*: $n + k = m + k$ vagy $k + n = k + m$, akkor $m = n$
- Szorzás
  $k, m, n \in \mathbb{N}$, akkor:
  1. *Asszociatív*: $(k \cdot m) \cdot n = k \cdot (m \cdot n)$
  2. *Kommutatív*: $n \cdot k = k \cdot n$
  3. $0 \cdot n = n \cdot 0 = 0$ *(**0**: multiplikatív zéruselem)*
  4. $n \cdot 1 = 1 \cdot n = n$ *(**1**: a multiplikatív egységelem)*
  5. *Disztributív*: $k \cdot (m + n) = k \cdot m + \cdot n$, illetve $(m + n) \cdot k = m \cdot k + n \cdot k$
  6. *Egyszerűsítési szabály*: $k \neq 0$ esetén: $n \cdot k = m \cdot k$, akkor $m = n$

Egész számok

Természetes számok körében az összeadásra nézve csak a nullának van inverze, másként szólva, a kivonás általában nem végezhető el.

Tekintsük a $\sim \subset \mathbb{N} \times \mathbb{N}$ relációt. Értelmezzük ezeken a párokon a

- $(a, b) \sim (c, d)$ relációt, ha $a + d = c + b$ relációt, az
- $(a, b) + (c, d) = (a + c, b + d)$ összeadást, a
- $(a, b) \cdot (c + d) = (a \cdot c + b \cdot d, a \cdot d + c \cdot b)$ szorzást, valamint a
- $(a, b) \leq (c, d)$, relációt ha $a + d \leq c + b$

A $\sim$ ekvivalenciareláció. Az ekvivalenciaosztályok halmazát jelöljük $\mathbb{Z}$-vel. Az így nyert halmazt nevezzük az egész számok halmazának.

Mindegyik ekvivalenciaosztály reprezentálható az $(n, 0)$ vagy $(0, n)$ (vagy akár egyszerre mindkettő) alakú elemével. Az $n \in \mathbb{N}$ számot az $[(n, 0)]$ osztály azonosítja (más szóval a természetes számok beágyazhatók $\mathbb{Z}$-be), illetve a $[(0, n)]$ osztályt $-n$-nel jelöljük (így megkaptuk az összes ekvivalenciaosztályt, a $[(0, 0)]$ osztályt kétszer, hiszen $-0 = 0$).

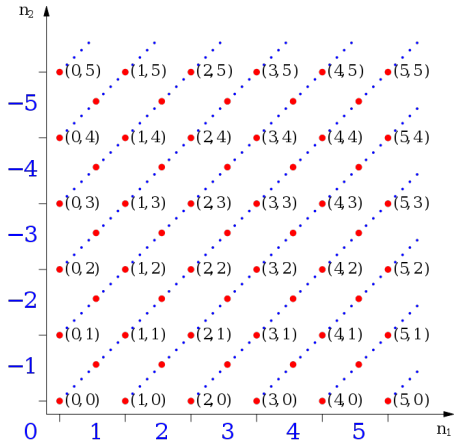
Így az $[(a, b)]$-t $\begin{cases} a - b, & \text{ha } a \geq b \\ -(b - a), & \text{ha } a < b \end{cases}$ módon jelölhetjük.

Ez a jelölés az egész számok megszokott reprezentációját adja: $\{...-3, -2, -1, 0, 1, 2, 3, ...\}$.

Például:

$$\begin{aligned}
0 = [(0,0)] &= [(1,1)] = \cdots &&= [(k,k)] \\
1 = [(1,0)] &= [(2,1)] = \cdots &&= [(k+1,k)] \\
-1 = [(0,1)] &= [(1,2)] = \cdots &&= [(k,k+1)] \\
2 = [(2,0)] &= [(3,1)] = \cdots &&= [(k+2,k)] \\
-2 = [(0,2)] &= [(1,3)] = \cdots &&= [(k,k+2)].
\end{aligned}$$

$\mathbb{Z}$ elemei a szokásos műveletekkel **gyűrű**t alkotnak. Az (a, b) pár additív inverze a (b, a) pár. A piros pontok a természetes számok rendezett párjait mutatják. Az összekötött piros pontok a vonal végén kékkel írt egész számot reprezentáló ekvivalenciaosztályok.



Racionális számok

Az egész számok körében a nem nulla elemek közül csak az 1-nek és a -1-nek van multiplikatív inverze, másként szólva az osztás általában nem végezhető el. Tekintsük a $\sim \subset \mathbb{Z} \times \mathbb{Z}$ relációt. A racionális számok precízen egész számok rendezett párjaként definiálhatók: (a, b) ahol b nem nulla. Az összeadást és szorzást ezeken a párokon a következőképp definiáljuk:

- $(a, b) + (c, d) = (ad + bc, bd)$ összeadást, a
- $(a, b) \cdot (c, d) = (ac, bd)$ szorzást.

Annak érdekében, hogy teljesüljön az elvárt $\frac{2}{4} = \frac{1}{2}$ tulajdonság, definiálni kell egy ekvivalenciarelációt is $(\sim)$ a következőképpen:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

Ez az ekvivalenciareláció kompatibilis a fent definiált összeadással és szorzással. Legyen ezután **Q** az ekvivalenciaosztályok halmaza, más szóval azonosnak tekintjük az (a, b) és a (c, d) párt, ha ekvivalensek.

Az így kapott számok halmazán a teljes rendezés is definiálható:

$$(a, b) \leq (c, d) \Leftrightarrow (bd > 0 \wedge ad \leq bc) \vee (bd < 0 \wedge ad \geq bc)$$

A $\sim$ reláció ekvivalenciareláció, az ekvivalenciaosztályok halmazát jelöljük $\mathbb{Q}$-val.
$\mathbb{Q}$ elemeit racionális számoknak nevezzük. $(\mathbb{Q}, +, \cdot)$ **rendezett test**.

Valós számok

Nincs olyan $a \in \mathbb{Q}$ szám, melynek négyzete 2. Tehát nem minden szám írható fel $\frac{m}{n}$ $(m, n \in \mathbb{N}^+)$ alakban.

Archimédeszi rendezettség: Egy F rendezett testet archimédeszien rendezett, ha

$$x, y \in F : \exists n \in \mathbb{N} : nx \geq y \quad (x > 0)$$

A racionális számok rendezett teste archimédeszien rendezett, de nem felső határ tulajdonságú. Egy felső határ tulajdonságú rendezett testet a valós számok testének nevezünk, és $\mathbb{R}$-rel jelöljük. $(\exists! \mathbb{R})$

Komplex számok

A komplex számok szükségét a harmadfokú egyenletek megoldására való Cardano-képlet szülte. Ugyanis abban az esetben, amikor az egyenletnek három különböző valós gyöke van, a képletben a gyökjel alá negatív szám kerül.
A komplex számok halmaza $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. $\mathbb{C}$ az

- $(x, y) + (x', y') = (x + x', y + y')$ összeadással és az
- $(x, y) \cdot (x', y') = (xx' - yy', y'x + yx')$ szorzással test.

A komplex számok halmaza *nem rendezett test*, mivel (tétel alapján) egy rendezett integritási tartományban $x \neq 0 \Rightarrow x^2 > 0$. (Ez azonban $(0, 1)^2 = i^2 = -1$-re nem teljesül).

A komplex számok körében

- (0,0) a nullelem,
- $(1, 0)$ egységelem,
- (x, y) additív inverze $(-x, -y)$, és
- $(0, 0) \neq (x, y)$ pár multiplikatív inverze az $(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2})$ pár.

Valós számok azonosítása

Mivel $(x, 0) + (x', 0) = (x + x', 0)$ és $(x, 0) \cdot (x', 0) = (xx', 0)$ így az összes $(x, 0), x \in \mathbb{R}$ komplex számot azonosíthatjuk $\mathbb{R}$-rel.

Komplex számok algebrai alakja

Mivel

$$(x, y) = (x, 0) + (y, 0) \cdot i = x + yi$$

így a komplex számokat $a + bi$ algebrai alakban is írhatjuk.

Ekkor az

- $\mathrm{Re}(z) = x$ valós számot a $z = (x, y)$ komplex szám ***valós rész***ének, az
- $\mathrm{Im}(z) = y$ valós számot pedig a ***képzetes rész***ének nevezzük.

Konjugált

$z = x + yi$ komplex szám konjugáltja: $\overline{z} = x - yi$

Tulajdonságai:

1. $\overline{z + w} = \overline{z} + \overline{w}$
2. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$
3. $\overline{\overline{z}} = z$
4. $z + \overline{z} = 2\mathrm{Re}(z)$
5. $z - \overline{z} = i \cdot 2\mathrm{Im}(z)$

Abszolút érték

A $z = (x, y)$ komplex szám abszolút értéke: $|z| = \sqrt{x^2 + y^2}$
Tulajdonságai:

1. $z \cdot \overline{z} = |z|^2$
2. $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$
3. $|z| = \overline{|z|}$
4. $|z \cdot w| = |z| \cdot |w|$
5. $|z + w| \leq |z| + |w|$

Trigonometrikus alak

- Argumentum
  $z \neq 0$ esetén az a z argumentuma $\forall t \in \mathbb{R}$, melyre $\mathrm{Re}(z) = |z|\cos(t)$, és $\mathrm{Im}(z) = |z|\sin(t)$. Más szóval a z argumentuma az origóból a z-be mutató vektor és a pozitív valós tengellyel bezárt szöge.

- Trigonometrikus alak
  A z komplex szám trigonometrikus alakja: $z = |z|(\cos(t)+i\cdot\sin(t)$

- Moivre-azonosságok
  Legyen $z = |z|(\cos(t)+i\cdot\sin(t))$, és $w = |w|(\cos(s)+i\cdot\sin(s))$. Ekkor

$$z \cdot w = |z||w|(\cos(t + s) + i \cdot \sin(t + s))$$

$$\frac{z}{w} = \frac{|z|}{|w|}(\cos(t - s) + i \cdot \sin(t - s)) \quad (w \neq 0)$$

$$z^n = |z|^n(\cos(nt) + i \cdot \sin(nt)) \quad (n \in \mathbb{Z})$$

- Gyökvonás
  Legyen $z^n = w$ ekkor:

$$\sqrt[n]{w} = \left\{ z_k = \sqrt[n]{|w|}\left(\cos\left(\frac{t + 2k\pi}{n}\right) + \sin\left(\frac{t + 2k\pi}{n}\right)\right), k = 0, ..., n - 1 \right\}$$

De mivel ez a jelöltés összetéveszthető a valósak között (egyértelművé tett) valós gyökvonással. így ezt a jelölést nem használjuk. Vezessük be helyette a n-edik komplex egységgyök fogalmát:

$$\varepsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i \cdot \sin\left(\frac{2k\pi}{n}\right), \quad k = 0, ..., n-1$$

Ezek után a w gyökeit a z és az n-edik komplex egységgyökök segítségével kaphatjuk meg:

$$z\varepsilon_0, \ldots, z\varepsilon_{n-1}$$

Leszámlálások véges halmazokon

Véges halmazok

- Halmazok ekvivalenciája
  X, Y *halmazok ekvivalensek*, ha létezik X-et Y-ra képező bijekció.
  Jele: $X \sim Y$
- Véges és végtelen halmazok
  X halmaz *véges*, ha $\exists n \in \mathbb{N} : X \sim \{1, 2, ..., n\}$, *egyébként végtelen.* Ha létezik n, akkor az egyértelmű, és ekkor a halmaz elemszámának/számosságának nevezzük. Jele: $\#(X)$

Skatulya elv

Ha X, Y véges halmazok és $\#(X) > \#(Y)$, akkor egy $f : X \to Y$ leképezés nem lehet kölcsönösen egyértelmű (azaz bijekció).

Leszámolások

Ha számít az elemek kiválasztásának a sorrendje, akkor csak permutáció vagy variáció lehet.

Permutáció

Az A halmaz egy permutációja az önmagára való kölcsönösen egyértelmű leképezése. Az A halmaz elemei különbözőek. Hányféleképpen lehet sorbarakni ismétlés nélkül sorbarakni A elemeit. Az A halmaz összes permutációjának száma:

$$P_n = \prod_{k=1}^{n} k \;=\; n!$$

Példa: a, b, c permutáció: abc, bac, acb, bca, cba

Variáció

Az A halmaz elemeiből készíthető, különböző tagokból álló $a_1, a_2, ..., a_k$ sorozatokat az A halmaz k-ad osztályú variációinak nevezzük. Ha A véges ($\#(A) = n$), akkor V_n^k ($k < n$) száma megegyezik az $\{1, 2, ..., k\}$-t $\{1, 2, ..., n\}$-be képező kölcsönösen egyértelmű leképezések számával:

$$V_n^k = \frac{n!}{(n-k)!}$$

Példa 1: a, b, c másod osztályú variációi: ab, ac, bc, ba, ca, cb
Példa 2: 12 csapatos bajnokságon hányféle sorrend alakulhat ki az első három (dobogós) helyen?

$$V_{12}^3 = \frac{12!}{(12-3)!} = 1320$$

Kombináció

Ha A halmaz $k \in \mathbb{N}$ elemű részhalmazait k-ad osztályú kombinációinak nevezzük. Ha A véges, akkor C_n^k száma megegyezik $\{1, 2, ..., n\}$ k elemű részhalmazainak számával.

$$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Ismétléses permutáció

$A = \{a_1, \ldots, a_r\}$ halmaz elemeinek ismétlődései $i_1, \ldots, i_r$. (Az elemek ismétléses permutációi olyan $i_1 + \cdots + i_r = n$ tagú sorozatok, melyben az a_j elem i_j-szer fordul elő.)

$$P_n^{i_1,\ldots,i_r} = \frac{n!}{i_1! i_2! \cdots i_r!}$$

Példa 1: a, l, m, a ismétléses permutációi:

$$P_4^{2_a,1_l,1_m} = \frac{4!}{2!1!1!} = 12$$

Ismétléses variáció

Az A véges halmaz elemeiből készíthető (nem feltétlenül különböző) $a_1, \cdots, a_k$ sorozatokat, az A halmaz k-ad osztályú ismétléses variációinak nevezzük.

$${}^iV_n^k = n^k$$

Példa 1: 2, 3 4, 5 felhasználásával hány három jegyű számot lehet képezni, ha egy számjegy többször is szerepelhet?

$${}^iV_4^3 = 4^3 = 64$$

Példa 2: TOTÓ kitöltése. Lehetséges értékek 1,2,X. Három érték, és 14 hely.

$${}^iV_3^{14} = 3^14 = 4.782.969$$

Ismétléses kombináció

Az A véges halmaz. A halmazból k elemet kiválasztva, ismétléseket megengedve, de a sorrend figyelmen kívül hagyva, az A halmaz k-ad osztályú ismétléses kombinációit kapjuk.

$${}^iC_n^k = \binom{n+k-1}{k}$$

Tételek

- **Binomiális tétel**
  Két tagú kifejezések n-edik hatványának kiszámításához ad egy formulát.
  $x, y \in R$ (kommutatív egységelemes gyűrű), $n \in \mathbb{N}$. Ekkor

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

- **Polinomiális tétel**
  $r, n \in \mathbb{N}$ és $x_1, x_2, \cdots, x_r \in R$ (kommutatív egységelemes gyűrű), ekkor

$$(x_1 + \cdots + x_r)^n = \sum_{i_1+\cdots+i_r=n} P_n^{i_1,\cdots,i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} =$$
$$\sum_{i_1+\cdots+i_r=n} \frac{n!}{i_1! i_2! \cdots i_r!} \cdot x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} \qquad (i_1, \cdots, i_r \in \mathbb{N})$$

- **Szita formula**
  $X_1, \cdots, X_k \subset X$ (véges halmaz). f az X-en értelmezett, egy Abel-csoportba képző függvény. Legyen:
$$S = \sum_{x \in X} f(x)$$
$$S_r = \sum_{1 \le i_1 \le \cdots \le i_r \le k} \left(\sum_{x \in X_{i_1} \cap \cdots \cap X_{i_r}} f(x) \right)$$
  és
$$S_0 = \sum_{x \in X \setminus \bigcup_{i=1}^{k} Xi} f(x)$$
  Ekkor
$$S_0 = S - S_1 + S_2 - S_3 + \cdots + (-1)^k S_k$$

Számelméleti alapfogalmak, lineáris kongruencia-egyenletek

Számelméleti alapfogalmak

Oszthatóság egységelemes integritási tartományban

R egységelemes integritási tartomány, $a, b \in R$.
Ha $\exists c \in R : a = bc$, akkor b osztója a-nak (a a b többszöröse). Jele: $b \big| a$

A $b = 0$-t kivéve legfeljebb egy ilyen c létezik.

Az oszthatóság tulajdonságai egységelemes integritási tartományban.

- Ha $b \big| a$ és $b' \big| a'$, akkor $bb' \big| aa'$
- $\forall a \in R : a \big| 0$ (a nullának minden elem osztója)
- $0 \big| a \Leftrightarrow a = 0$ (a null csak saját magának osztója)
- $\forall a \in R : 1 \big| a$ (az egységelem minden elem osztója)
- $b \big| a \Rightarrow \forall c \in R : bc \big| ac$
- $bc \big| ac$ és $c \neq 0 \Rightarrow b \big| a$
- $b \big| a_i$ és $c_i \in R,\ (i = 1, \cdots, j) \ \Rightarrow\ b \big| \sum_{i=1}^{j} a_i c_i$
- az $\big|$ reláció reflexív és tranzitív

Felbonthatatlan elem és prímelem

$0, 1 \neq a \in R$ *felbonthatatlan* (irreducibilis), ha $a = bc$ esetén b vagy c egység ($b, c \in R$).
$0, 1 \neq p \in R$ *prím*, ha $\forall a, b \in R : p \big| ab$ esetén $p \big| a$ vagy $p \big| b$

Legnagyobb közös osztó, legkisebb közös többszörös, relatív prím

R egységelemes integritási tartomány. $a_1, \cdots, a_n \in R$ elemeknek $b \in R$

- *legnagyobb közös osztója*, ha $b \big| a_i$ és $b' \big| a_i$ esetén $b' \big| b$.

  Ha b egység, akkor $a_1, \cdots, a_n$ *relatív prímek.*

- *legkisebb közös többszöröse* $b \in R$, ha $a_i \big| b$ és $a_i \big| b'$ esetén $b \big| b'$.

Bővített euklideszi algoritmus

Az eljárás meghatározza az $a, b \in \mathbb{Z}$ számok legnagyobb közös osztóját ($d \in \mathbb{Z}$), valamint $x, y \in \mathbb{Z}$ számokat úgy, hogy

$$d = ax + by$$

A számelmélet alaptétele

Minden pozitív természetes szám (sorrendtől eltekintve) egyértelműen felbontható prímszámok szorzataként.

Eratoszthenész szitája

- Írjuk fel a számokat 1-től n-ig, (itt például 100-ig) egyesével.
- Keressük meg az első olyan 1-től nagyobbat, amelyik még nincs sem kihúzva (next), sem megjelölve. Elsőként ez a 2.
- Ezután húzzuk ki ennek többszöröseit, és (next)-et jelöljük meg.
- Ismételjük meg a második lépéstől újra az eljárást. Természetesen egy összetett szám többször is kihúzásra kerülhet.
- Az algoritmus akkor álljon le, ha a második lépésnél talált szám négyzete már nagyobb, mint n.

Lineáris kongruencia egyenletek

Kongruencia

Ha $a, b, m \in \mathbb{Z}$ azt mondjuk, hogy a kongruens b-vel modulo m, azaz hogy a és b egészek m-mel vett osztási maradéka egyenlő, ha .

$$m \big| a - b$$

azaz

$$\exists k \in \mathbb{Z} : a = km + b$$

Jelölése:

$$a \equiv b \ (mod\ m)$$

Ha a nem kongruens b-vel modulo m, azt mondjuk, ***inkongruens*** vele.
Jelölése: $a \not\equiv b \pmod m$.

Maradékosztályok

A kongruencia ekvivalenciareláció, tehát osztályoz. Egy $m \in \mathbb{Z}$ modulus szerinti kongruencia ekvivalencia-osztályait m szerinti maradékosztályoknak nevezzük.
Az a elem által reprezentált maradékosztályt $\widetilde{a} \mod m$ vagy $[a]$ jelöli.
Általában egy maradékosztályt a legkisebb nemnegatív eleme reprezentál.

Ha egy maradékosztály valamely eleme relatív prím a modulushoz, akkor mindegyik az, és a maradékosztályt *redukált maradékosztály*nak nevezzük.

Páronként inkongruens egészek egy rendszerét *maradékrendszernek* nevezzük.

Ha egy maradékrendszer minden maradékosztályból tartalmaz elemet, akkor *teljes maradékrendszer*.

Ha maradékrendszer pontosan a redukált maradékosztályokból tartalmaz elemet, akkor *redukált maradékrendszer*.

Euler-féle φ függvény

$m > 0$ egész szám. Az Euler-féle $\varphi(m)$ függvény a modulo m redukált maradékosztályok számát adja meg. Ez nyilván megegyezik a $0, 1, \cdots, m-1$ számok közötti, m-hez relatív prímek számával.

Euler-Fermat tétel: Legyen $m > 1$ egész, a relatív prím m-hez, ekkor:

$$a^{\varphi(m)} \equiv 1 \ \ (mod\ m)$$

Fermat tétel: Legyen p prím, és $a \in \mathbb{Z} : p \nmid a$, ekkor

$$a^{p-1} \equiv 1 \ \ (mod\ p)$$

Lineáris kongruencia megoldása

Keressük az $ax \equiv b \mod m$ kongruencia megoldásait ($a, b, m \in \mathbb{Z}$ ismert).
Ez ekvivalens azzal, hogy keressünk olyan x-et, melyre (valamely y-nal) $ax + my = b$.

Legyen $d = \text{lnko}(a, m)$. Mivel d osztója $ax + my$-nak, b-t is osztania kell, különben nincs megoldás. Így

$$\frac{a}{d}x + \frac{m}{d}y = \frac{b}{d}, \text{ ekkor } a'x + m'y = 1.$$

A bővített euklideszi algoritmus segítségével olyan u, v számokat kapunk, melyekkel

$$a'u + m'v = 1 \text{ (ui.: } a', m' \text{ relatív prímek)}$$

Az egyenletet b'-vel beszorozva

$$a'ub' + m'vb' = b' \Rightarrow x \equiv ub' \mod m'$$

Lineáris kongruenciarendszer megoldása

Két lineáris kongruencia esetén a megoldások

$$x \equiv a \ \ (mod\ m) \text{ és } x \equiv b \ \ (mod\ n)$$

A közös megoldáshoz az

$$x = a + my = b + nz \Leftrightarrow my - nz = b - a$$

egyenletet kell megoldani. Akkor és csak akkor van megoldás, ha $d = \text{lnko}(m, n)$ osztója $b - a$-nak. Ekkor a megoldás valamely x_1 egésszel $x \equiv x_1 \mod \text{lkkt}(m, n)$ alakban írható. (Több kongruencia esetén az eljárás folytatható.)

Kínai maradéktétel

Legyenek $m_1, \cdots, m_n \in \mathbb{N}$ egynél nagyobb páronként relatív prímek, és $c_1, \cdots, c_n \in \mathbb{Z}$. Az

$$x \equiv c_j \ \ (mod\ m_j) \qquad (j = 1,\ \ldots,\ n)$$

kongruenciarendszer megoldható ($1 \leq j \leq n$), és a megoldása egyetlen maradékosztálya lesz modulo M, ahol $M = m_1 m_2 \cdots m_n$.

Gráfok

Általános és síkgráfok

- Egy ***irányítatlan gráf*** a $G = (V, E, \varphi)$ rendezett 3-as, ahol:
  - V - a csúcsok halmaza
  - E - élek halmaza
  - φ - illeszkedési reláció ($\varphi \in E \times V$)

  Ha $v \in \varphi(e)$, akkor v illeszkedik az e élre. ($v \in V, e \in E$). Egy élnek mindig két vége van.
- Él-, és csúcstípusok
  - $v \in V$ ***izolált csúcs***, ha $\nexists e \in E : v \in \varphi(e)$
  - $e, e' \in E$ élek ***párhuzamos élek***, ha $\varphi(e) = \varphi(e')$
  - $e \in E$ ***hurokél***, ha $\left|\varphi(e)\right| = 1$
- Egy ***irányítatott gráf*** a $G = (V, E, \psi)$ rendezett 3-as, ahol:
  - V - a csúcsok halmaza
  - E - élek halmaza
  - ψ - illeszkedési reláció ($\psi \in E \to V \times V$)

  $\psi(e) = (v, v')$, ahol v az e él kezdőpontja, v' a végpontja.

Véges, egyszerű gráfok - alapfogalmak

- G gráf ***egyszerű gráf***, ha nem tartalmaz párhuzamos vagy hurokéleket.
- $G = (V, E, \varphi)$ gráf ***véges gráf***, ha V, E véges halmazok.
- Szomszédság, fok
  Két él szomszédos, ha van közös pontjuk.
  Két csúcs szomszédos, ha van közös élük.
  $v \in V$ szomszédjainak száma a v ***foka***. [Jele: $\deg(v) = \mathrm{d}(v)$]
- G **r-*reguláris gráf***, ha minden pont foka r
- G ***teljes gráf***, ha minden él be van húzva, más szóval $(\left|V\right| - 1)$-reguláris. (Jele: $K_{\left|V\right|}$)
- G ***páros gráf***, ha $V = V' \cup V''$ és $V' \cap V'' = \emptyset$ (diszjunkt), valamint él csak V' és V'' között fut. Ha viszont így V' és V'' között minden él be húzva, akkor teljes páros gráf. (Jele: $K_{n,m}$, ahol $n = \left|V'\right|, m = \left|V''\right|$)
- $G = (V, E, \varphi)$ ***részgráfja*** $G' = (V', G', \varphi')$-nek, ha $V \subset V' \ \wedge \ E \subset E' \ \wedge \ \varphi \subset \varphi'$
- G gráfban egy n hosszú ***séta*** v-ből v'-be egy olyan

  $$\boldsymbol{v_0},\ e_1,\ \boldsymbol{v_1},\ \cdots\ ,\ \boldsymbol{v_{n-1}},\ e_n,\ \boldsymbol{v_n}$$

  sorozat, melyre $v = v_1,\ v' = v_n$ és $v_{i-1},\ v_i \in \varphi(e_i)$

  Egy *séta* ***vonal***, ha *minden él legfeljebb egyszer* szerepel a sorozatban.

  Egy *vonal* ***út***, ha *minden csúcs legfeljebb egyszer* szerepel a sorozatban.

  Egy séta/vonal/út ***zárt***, ha *kezdő és végpontja* megegyezik, egyébként ***nyílt***.
- Egy gráf ***összefüggő***, ha bármely két csúcs közt van út.

  Ez a reláció ekvivalenciareláció, melynek ekvivalenciaosztályait *komponensek*nek nevezzük.
- $G = \big(V, E, \varphi, C_e, c_e, C_v, c_v\big)$ rendezett 7-es ***címkézett gráf***ot jelöl, ahol C_e, C_v tetszőleges halmazok, és

  $$c_e : E \to C_e$$
  $$c_v : E \to C_v$$

  Ha $C_e = C_v = \mathbb{R}^+$, akkor a gráfot ***súlyozott gráf***nak nevezzük, és w a csúcs/él súlya. $\big(w(e) = c_e(e),\ w(v) = c_v(v)\big)$

Síkba rajzolhatóság

- Egy gráf ***síkba rajzolható***, ha lerajzolható úgy, hogy az élei nem keresztezik egymást.
- Két gráf ***topologikusan izomorf***, ha a következő lépést illetve fordítottját véges sok ismétlésével egyikből a másikat kapjuk: Egy másodfokú csúcsot elhagyunk, és a szomszédjait összekötjük.
- Ha G gráf síkba rajzolható, akkor a ***tartományok*** az élek által határolt síkidomok.
  (A nem korlátolt síkidom is tartomány.)

Tételek

1. Minden véges gráf $\mathbb{R}^3$-ban lerajzolható.
2. Ha egy véges gráf síkba rajzolható $\iff$ gömbre rajzolható
3. ***Euler-tétel***: Ha a G véges gráf összefüggő, síkba rajzolható gráf, akkor:
$$\big|E\big| + 2 = \big|V\big| + \big|T\big|$$
4. ***Kuratowsky-tétel***: Egy véges gráf pontosan akkor síkba rajzolható, ha nem tartalmaz K_5-tel, vagy $K_{3,3}$-mal topologikusan izomorf részgráfot.

Fák

- Egy G gráf ***fa***, ha *összefüggő* és *körmentes*.
- Legyen F részgráfja G-nek. Ha F fa és csúcsainak halmaza megegyezik G csúcsainak halmazával, akkor F-et a G feszítőfájának nevezzük.
  - Ha G ***egyszerű gráf***, akkor a következő feltételek ekvivalensek:
    1. G fa
    2. G összefüggő, de bármely él törlésével már nem az
    3. Két különböző csúcs között csak egy út van
    4. G körmentes, de egy él hozzáadásával már nem az
  - Ha G ***egyszerű véges gráf***, akkor a következő feltételek ekvivalensek:
    1. G fa
    2. G-ben nincs kör és $n-1$ éle van
    3. G összefüggő és $n-1$ éle van
- Az ***irányított fa*** olyan fa, melyre:
$$\exists v \in V : d^-(v) = 0 \text{ és } \forall v' \neq v : d^-(v') = 1 \quad \text{(Egy csúcs befoka } \textit{0}\text{, a többié } \textit{1}\text{)}$$
  További fogalmak:
  - $r \in V, d^-(r) = 0$ csúcsot ***gyökér csúcs***nak nevezzük
  - v' ***csúcs szintje*** az r, v' út hossza
  - $(v, v') \in \psi(e)$, a v szülője v'-nek, v' gyereke, v-nek.
  - v levél, ha $d^+(v) = 0$

Euler- és Hamilton-gráfok

Euler-gráf

Az ***Euler-vonal*** olyan vonal v-ből v'-be a gráfban, amelyben minden él szerepel.
Ha $v = v'$ akkor ezt a vonalat Euler-körvonalnak is szokás nevezni.
Euler-vonallal rendelkező gráfot ***Euler-gráf***nak nevezik.

Tétel: Egy összefüggő véges gráfban pontosan akkor létezik Euler-körvonal, ha minden csúcs páros fokú.

Hamilton-gráf

A ***Hamilton-út*** egy olyan út v-ből v'-be a gráfban, mely minden csúcsot tartalmaz.
Ha $v = v'$ akkor ezt az utat ***Hamilton-kör***nek is szokás nevezni.
Hamilton-úttal rendelkező gráfot ***Hamilton-gráf***nak nevezik.

Gráfok adatszerkezetei

Gráfok számítógépes reprezentációjához legtöbbször láncolt listákat, vagy mátrixokat szoktak használni. A láncolt listák inkább ritka gráfokra, míg a mátrixok sűrű gráfok esetén gazdaságosak.

Illeszkedési mátrix

$G = (V, E, \psi)$ irányított gráf esetén a gráfot egy $A = \{0, 1, -1\}^{n \times m}$ mátrix segítségével tudjuk reprezentálni, ahol $V = \{v_1, \cdots, v_n\}$, és $E = \{e_1, \cdots, e_m\}$.

Ekkor a mátrix egyes elemei:

$$a_{ij} = \begin{cases} 1 & \text{ha } v_i \text{ kezdőpontja } e_j\text{-nek} \\ -1 & \text{ha } v_i \text{ végpontja } e_j\text{-nek} \\ 0 & \text{különben} \end{cases}$$

Ha G nem irányított, akkor $a_{ij} = \left|a_{i,j}\right|$

Csúcsmátrix

A fenti jelölésekkel irányított esetben $B \in \mathbb{Z}^{n \times n}$, ahol b_{ij} a v_i-ből v_j-be menő élek számát jelöli. Ha G irányítatlan, akkor b_{ii} v_i hurokéleinek száma, egyébként b_{ij} a v_i és v_j csúcsok közötti élek száma.

Kódoláselmélet

Polinomok és műveleteik

Legyen R gyűrű. Egy polinomot egy

$$\sum_{i=0}^{n} f_i x^i \quad (n \in \mathbb{N}, f_i \in R)$$

alakú véges összegnek tekintünk.

Az f_n tagot a polinom ***főegyüttható***jának nevezzük.

Műveletek

Legyen $R[x]$ az $f = (f_0, f_1, \cdots)$ végtelen sorozatok feletti gyűrű (polinomok gyűrűje), ahol $f_i \in R$.
Ekkor az $R[x]$-beli műveletek:

- Összeadás:
$$f + g = (f_0 + g_0, f_1 + g_1, \cdots) \qquad (f, g \in R[x])$$
- Szorzás:
$$f \cdot g = h = (h_0, h_1, \cdots) \qquad (f, g, h \in R[x]), \text{ ahol}$$
$$h_k = \sum_{i+j=k} f_i g_j$$

Megjegyzés:

- Ha R kommutatív, akkor $R[x]$ is az.
- Ha R egységelemes az 1 egységelemmel, akkor
  - R[x] is egységelemes az (1,0,0, $\cdots$) egységelemmel.

Maradékos osztás

Legyen R egységelemes integritási tartomány, $f, g \in R[x], g \neq 0$ és tegyük fel, hogy g főegütthatója egység R-ben. Ekkor

$$\exists! q, r \in R[x] : f = g \cdot q + r \qquad \big(\deg(r) < \deg(g)\big)$$

Horner-séma

A Horner-módszer egy polinom helyettesítési értékének kiszámítására alkalmas. (Ezzel együtt természetesen az is eldönthető, hogy adott c érték a polinom gyöke-e vagy nem. 4-ed fok felett erre még analitikus megoldás sincs.)

A módszer lényege, hogy az egyébként $f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$ polinom helyettesítési értékének kiszámolásához rendkívül sok szorzásra és összeadásra lenne szükség. A polinom átalakításával azonban a műveletek számát lecsökkenthetjük. A maradékos osztást alkalmazva:

$$f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0 = \big(f_n x^{n-1} + f_{n-1} x^{n-2} + \cdots\big)\, x + f_0$$

Ezt rekurzívan folytatva a következő alakra jutunk:

$$\Big(\big((f_n x + f_n - 1)x + f_n - 2\big)x + \cdots\Big)x + f_0$$

A helyettesítési érték kiszámítását egy táblázatban könnyebben elvégezhetjük.

	f_n	f_{n-1}	f_{n-2}	$\cdots$	f_0
c	f_n	$f_n c + f_{n-1}$	$(f_n c + f_{n-1})c + f_{n-2}$	$\cdots$	$f(c)$

A táblázat kitöltése a következőképp zajlik:

1. Az első sorba felírjuk a polinom együtthatóit

2. A második sor első cellájába beírjuk az argumentum értékét.
3. A főegyüttható alá beírjuk önmagát.
4. A második sor celláinak kitöltésével folytatjuk
5. Az előző cella elemét megszorozzuk az argumentummal
6. A szorzathoz adjuk hozzá az aktuális együtthatót
7. Az összeget írjuk be az aktuális cellába
8. Folytassuk az 5. ponttal, míg el nem jutunk az utolsó celláig

Az utolsó cellába a polinom helyettesítési értéke kerül.
(Ha ez nulla, akkor az argumentum a polinom gyöke.)

Betűnkénti kódolás

A kódolás a legáltalánosabb értelemben az üzentek halmazának egy másik halmazba való leképzését jelenti. Gyakran az üzenetet valamilyen karakterkészlet elemeiből alkotott sorozattal adjuk meg. Ekkor az üzenetet felbontjuk előre rögzített olyan elemi részekre, hogy minden üzenet egyértelműen előálljon ilyen elemi részek sorozataként. A kódoláshoz megadjuk az elemi részek kódját, amelyet egy szótár tartalmaz. Az ilyen kódolást ***betűnkénti kódolás***nak nevezzük.

A kódolandó üzenetek egy A ábécé betűi, és egy-egy betű kódja egy másik, B ábécé (kódábécé) betűinek felel meg. Tegyük fel, hogy mindkét ábécé nem üres és véges.

Egy A ábécé betűiből felírható szavak halmazát A^+-szal jelöljük, míg az üres szóval kiterjesztettet A^*-gal.

Ez alapján a betűnkénti kódolást egy $\varphi : A \to B^*$ leképezés határozza meg, amelyet kiterjeszthetünk egy $\psi : A^* \to B^*$ leképezéssé az alábbi módon:

Ha $\alpha_1\alpha_2...\alpha_n = \alpha \in A$, akkor α kódja $\psi(\alpha) = \varphi(\alpha_1)\varphi(\alpha_2)...\varphi(\alpha_3)$. Nyilván ha φ nem injektív (vagy az üres szó benne van az értékkészletében), akkor a ψ kódolás sem injektív, azaz nem egyértelműen dekódolható. Emiatt feltehetjük, hogy φ injektív, és B^+-ba képez.

Shannon- és Huffman-kód

Alapfogalmak

Az információforrás n üzenetet bocsájt ki. A különböző üzeneteket jelöljük $a_1, \cdots, a_m$-mel.

- Az a_i üzenet k_i-szer fordul elő, melyet ***gyakoriság***nak nevezzük.
- Az a_i ***relatív gyakorisága*** a $p_i = \frac{k_i}{n}$.
- A $p_1, \cdots, p_m$ szám m-est az üzentek ***eloszlás***ának nevezzük. $(\sum_{i=1}^{m} p_i = 1)$

Az a_i *üzenet* ***egyedi információtartalma***

- $I_i = -\log_r p_i$, ahol $r > 1$ (az információ egysége).

- $I_i = -\log_2 p_i$, ahol $r = 2$ (bitenkénti kódolás esetén).

Az üzenetforrás által kibocsátott átlagos információtartalom az ***entrópia***:

$$H_r(p_1, \cdots, p_m) = -\sum_{i=1}^{m} p_i \log_r p_i$$

Legyen $\alpha, \beta, \gamma \in A$ szavak. Ekkor az $\alpha\beta\gamma$ szónak

- α *prefixe*
- β *infixe*
- γ *szuffixe*

A betűnkénti kódoláshoz egyértelműen megadható egy szemléletes irányított, élcímkézett fa.

Legyen $\varphi : A \to B^*$ a betűnkénti kódolás.

- Készítsünk el egy olyan fát, melynek a gyökere az üres szó és ha $\beta = \alpha b \quad (b \in B)$-re, akkor α-ból húzódjon olyan él β-ba, melynek b címkéje van.
- Ekkor minden azonos hosszú szó egy szinten lesz.
- Azokat a csúcsokat, melyekből minden $b \in B$ címkével vezet ki él *teljes csúcs*nak nevezzük, különben *csonka csúcs*ok.

A $\varphi : A \to B^+$ injektív leképezés által meghatározott $\psi : A^* \to B^*$ betűnkénti kódolás

1. *felbontható* (egyértelműen dekódolható), ha ψ injektív
2. ***prefix kód***, ha φ értékkészlete prefixmentes.
3. ***egyenletes kód*** (fix hosszúságú), ha ψ értékkészletében minden elem megegyező hosszú
4. ***vesszős kód***, ha $\exists \vartheta \in B^+$ vessző, hogy ϑ szuffixe minden kódszónak, de sem prefixe, sem infixe semelyik kódszónak.

Legyen $A = \{a_1, \cdots, a_n\}$ a kódolandó ábécé. Az a_i kódjának hossza l_i.
Ekkor a kód átlagos szóhosszúsága:

$$\bar{l} = \sum_{i=1}^{n} p_i l_i$$

Ha egy adott elemszámú ábécével és adott eloszlással egy felbontható betűnkénti kód átlagos szóhoszúsága minimális, akkor ***optimális kód***nak nevezzük.

Shannon-kód

Shannon kód egy optimális kód (r elemszámú ábécével és p_i gyakoriságokkal).

Shannon kód előállítás

1. Az üzenetekben előforduló szimbólumok előfordulási gyakoriságának meghatározása.
2. A szimbólumok gyakoriság szerinti csökkenő sorrendbe rendezése.
3. A lista két részre osztása úgy, hogy a két részben lévő szimbólumok összesített gyakorisága (közel) egyenlő legyen.
4. A lista felső részéhez 0-át, az alsó részéhez 1-et rendelünk (vagy fordítva).
5. A 3.-ik és 4.-ik eljárást addig ismételjük, amíg a kettéosztott lista mindkét részében csak 1-1 szimbólum található.

Példa 2:

Szimbólumok	**Gyakoriság**	**Relatív gyakoriság**	**Információ tartalom**	**Bitek száma**
A	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
B	7	$\frac{7}{39} \simeq 0.17$	$-log_2(\frac{7}{39}) = 2.47$	$-log_2(\frac{7}{39}) * 7 = 17.34$
C	15	$\frac{15}{39} \simeq 0.38$	$-log_2(\frac{15}{39}) = 1.37$	$-log_2(\frac{15}{39}) * 15 = 20.67$
D	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
E	5	$\frac{5}{39} \simeq 0.13$	$-log_2(\frac{5}{39}) = 2.96$	$-log_2(\frac{5}{39}) * 5 = 14.81$

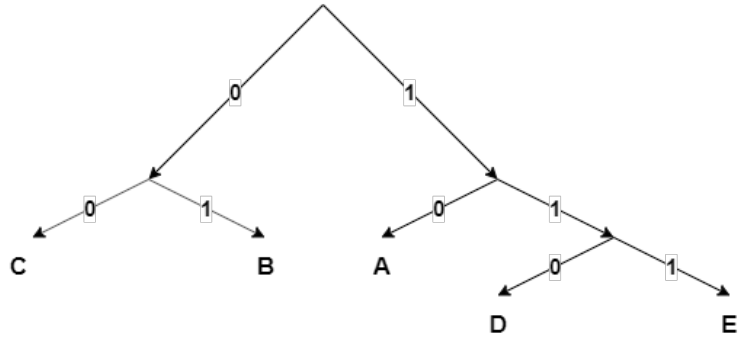
Rendezzük a szimbólumokat gyakoriság szerint csökkenő sorrendben:

Szimbólumok	**Gyakoriság**	**Relatív gyakoriság**	**Információ tartalom**	**Bitek száma**
C	15	$\frac{15}{39} \simeq 0.38$	$-log_2(\frac{15}{39}) = 1.37$	$-log_2(\frac{15}{39}) * 15 = 20.67$
B	7	$\frac{7}{39} \simeq 0.17$	$-log_2(\frac{7}{39}) = 2.47$	$-log_2(\frac{7}{39}) * 7 = 17.34$
A	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
D	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
E	5	$\frac{5}{39} \simeq 0.13$	$-log_2(\frac{5}{39}) = 2.96$	$-log_2(\frac{5}{39}) * 5 = 14.81$

Szimbólumok									
C	15	***22***	**0**	C	15	***15***	**0**		
B	7			B	7	***7***	**1**		
A	6			A	6	***6***	**0**		
D	6	***17***	**1**	D	6	***11***	**1**	D	**0**
E	5			E	5			E	**1**

C	**B**	**A**	**D**	**E**
00	**01**	**10**	**110**	**111**

A kódfát 1. ábrán láthatjuk.



1. ábra. Shannon-kód példa 2. kódfája

Huffman kód előállítás:

1. Az üzenetekben előforduló szimbólumok előfordulási gyakoriságának meghatározása.
2. A szimbólumok gyakoriság szerinti csökkenő sorrendbe rendezése.
3. A két legkevésbé gyakori szimbólumot összevonjuk és beírjuk a szimbólumok közé a gyakorisági sorba.
4. A 3.-ik pontot addig ismételjük, amíg 2 elemű lesz a lista. Ekkor az egyik elemhez 0-át a másikhoz 1-et rendelünk.
5. Visszalépünk az előző összevont szimbólumhoz, és az előbbivel azonos sorrendben a két szimbólumhoz 0-át és 1-et rendelünk, mindaddig, míg vissza nem jutunk az egyes szimbólumokhoz.

Példa 2:

Szimbólumok	**Gyakoriság**	**Relatív gyakoriság**	**Információ tartalom**	**Bitek száma**
A	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
B	7	$\frac{7}{39} \simeq 0.17$	$-log_2(\frac{7}{39}) = 2.47$	$-log_2(\frac{7}{39}) * 7 = 17.34$
C	15	$\frac{15}{39} \simeq 0.38$	$-log_2(\frac{15}{39}) = 1.37$	$-log_2(\frac{15}{39}) * 15 = 20.67$
D	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
E	5	$\frac{5}{39} \simeq 0.13$	$-log_2(\frac{5}{39}) = 2.96$	$-log_2(\frac{5}{39}) * 5 = 14.81$

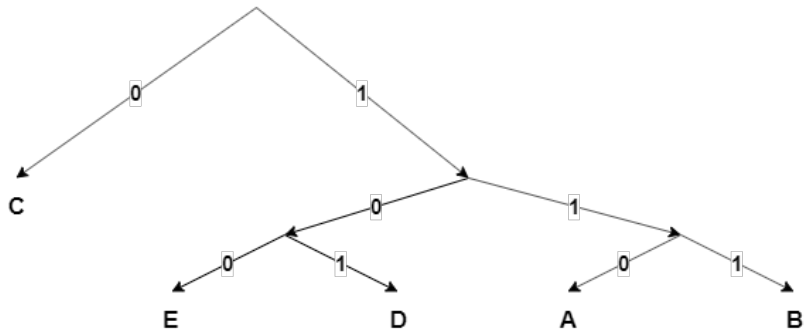
Rendezzük a szimbólumokat gyakoriság szerint csökkenő sorrendben:

Szimbólumok	**Gyakoriság**	**Relatív gyakoriság**	**Információ tartalom**	**Bitek száma**
C	15	$\frac{15}{39} \simeq 0.38$	$-log_2(\frac{15}{39}) = 1.37$	$-log_2(\frac{15}{39}) * 15 = 20.67$
B	7	$\frac{7}{39} \simeq 0.17$	$-log_2(\frac{7}{39}) = 2.47$	$-log_2(\frac{7}{39}) * 7 = 17.34$
A	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
D	6	$\frac{6}{39} \simeq 0.15$	$-log_2(\frac{6}{39}) = 2.70$	$-log_2(\frac{6}{39}) * 6 = 16.20$
E	5	$\frac{5}{39} \simeq 0.13$	$-log_2(\frac{5}{39}) = 2.96$	$-log_2(\frac{5}{39}) * 5 = 14.81$

Szimbólumok												
C	15		C	15		C	15		***ABDE***	24	**1**
B	7		***DE***	**11**		**AB**	**13**	**1**	C	15	**0**
A	6		B	**7**	**1**	DE	11	**0**			
D	6	**1**	A	6	**0**						
E	5	**0**									

C	**B**	**A**	**D**	**E**
0	**111**	**110**	**101**	**100**
	ABDE → AB → B	ABDE → AB → A	ABDE → DE → D	ABDE → DE → E

A kódfát 2. ábrán láthatjuk.



2. ábra. Huffman-kód példa 2. kódfája

Hibajavító kódok, kódtávolság

Hibakorlátozó kódolás

A hibakorlátozó kódokat két csoportba sorolhatjuk: *hibajelző* és *hibajavító* kódok.
Mindkét esetben az üzenetekhez kódszavakat rendelünk, amik alapján az átvitel során keletkező hibákat kezelni tudjuk.

Amennyiben az üzenet

- *könnyen ismételhető* $\Longrightarrow$ ***hibajelző***,
- *nehezen ismételhető* $\Longrightarrow$ ***hibajavító*** kódot alkalmazunk.

Kódok távolsága, súlya

A kódábécé u és v szavának ***Hamming-távolsága*** $d(u, v)$ az azonos pozícióban levő, eltérő jegyek száma.

A Hamming-távolság rendelkezik a távolság szokásos tulajdonságaival, vagyis $\forall u, v, z$:

- $d(u, v) \geq 0$
- $d(u, v) = 0 \iff u = v$
- $d(u, v) = d(v, u)$ (szimmetria)
- $d(u, z) \leq d(u, v) + d(v, z)$ (háromszög egyenlőtlenség)

A kód távolsága

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

Amennyiben az A kódábécé Abel-csoport a 0 nullelemmel, ekkor egy u szó ***Hamming-súlya*** $w(u)$ a szóban szereplő nem nulla elemek száma.
Ekkor a kód súlya

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

Hibajavító kód

Amikor egy olyan szót kapunk, ami nem kódszó, a hozzá legkisebb Hamming-távolságú kódszóra javítjuk.

- A K kód ***t-hibajavító***, ha egy legfeljebb t helyen megváltozott kódot helyesen javít.
- A K kód ***pontosan t-hibajavító***, ha t-hibajavító, de nem $t + 1$-hibajavító.

Megjegyzés: d minimális távolságú kód esetén $\frac{d}{2}$-nél kevesebb hibát biztosan egyértelműen tudunk javítani.

Hamming-korlát

Egy q elemű ábécé n hosszú szavaiból álló C kód t-hibajavító.
Ekkor bármely két kódszóra a tőlünk legfeljebb t távolságra lévő szavak halmazai diszjunktak.

Mivel egy kódszótól j távolságra pontosan $\binom{n}{j}(q-1)^j$ szó van, így a ***Hamming-korlát*** a kódszavak számára adott t-nél:

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

Amennyiben egyenlőség áll fent *tökéletes kód*ról beszélünk.

Lineáris kódok

A véges test és A^n lineáris tér. Minden $K \leq A^n$ alteret ***lineáris kód***nak nevezzük.
Ha az altér

- k dimenziós,
- a kód távolsága d és
- $\#(A) = q$ (*Hamming-korlát*)

akkor az ilyen kódot $[n, k, d]_q$ kódnak nevezzük.

Egy lineáris kódnál feltesszük, hogy kódolandó üzenetek K^k elemei, azaz a kódábécé elemeiből képzett k-asok.

Generátormátrix

K véges test feletti $[n, k, d]_q$ lineáris kódolást válasszuk egy (kölcsönösen egyértelmű) lineáris leképezésnek:

$$G : K^k \to K^n$$

Ezt egy mátrixszal, az úgy nevezett generátormátrixszal jellemezhetjük.

Polinomkódok

Egy lineáris kód esetén az üzeneteket megfeleltethetjük $\mathbb{F}_q$ (q elemű véges test) feletti k-nál alacsonyabb fokú polinomoknak.

$$(a_0, a_1, \cdots, a_{k-1}) \to a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$$

Legyen $G(x)$ rögzített m-edfokú polinom. A $p(x)$ polinomot (üzenet) $G(x)$-szel szorozva lineáris kódolást kapunk (mivel a $p \to pG$ kölcsönösen egyértelmű).

Ekkor a kódszavak hossza: $n = k + m$.

Az ilyen típusú lineáris kódolást ***polinomkódolás***nak nevezzük.

Megjegyzés: Feltehetjük, hogy $G(x)$ főpolinom (együtthatója egység), illetve a konstans tag nem nulla (ha nulla lenne, a szorzatban kiesne a konstans tag, így a kódban a nulla indexű betű soha nem hordozna információt)

CRC - Cyclic Redundancy Check

Ha egy polinomkódban $G(x) \big| x^n - 1$, akkor ***ciklikus kód***ról beszélünk.

Ekkor, ha $a_0 a_1 \cdots a_{\mathbf{n-1}}$ kódszó, akkor $a_{\mathbf{n-1}} a_0 \cdots a_{n-2}$ is az, mivel:

$$a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1} \;=\; x \cdot (a_0 + a_1 x + \cdots a_{n-1} x^{n-1}) - a_{n-1}(x^n - 1)$$

osztható $G(x)$-szel.

A *CRC* az $\mathbb{F}_2$ feletti ciklikus kódokat foglalja magába, és *kizárólag hibajelzésre alkalmas.*

A kódolás menete következő:

1. Vegyük $p(x)x^m = (0,\ 0,\ \cdots,\ 0,\ a_m,\ a_{m+1},\ \cdots,\ a_{n-1})$
2. Ezt osszuk el $G(x)$-el maradékosan

$$p(x)x^m = q(x)G(x) + r(x)$$

Ekkor a kódszó legyen:

$$p(x)x^m - r(x) = q(x)G(x)$$

Ez osztható $G(x)$-szel és magas fokszámokon az eredeti üzenet betűi helyezkednek el.

A fogadott szó ellenőrzése: Megnézzük, hogy osztható-e $G(x)$-szel. Ha nem oszható, akkor hiba történt.

Kiegészítés

Shannon-kód

A következő módon állítjuk elő:

1. Rendezzük a betűket relatív gyakoriságaik alapján csökkenő sorrendbe.
2. Határozzuk meg az $l_1, \cdots, l_n$ szóhosszúságokat a következő módon:

$$r^{-l_i} \leq p_i < r^{-l_i+1}$$

3. Osszuk el az ábécé elemeit az egyes helyiértékeken.

Példa 1:

Legyen a kódábécé a $0, 1, 2$ halmaz, az kódolandó betűk és gyakoriságaik pedig a következők:

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

A relatív gyakoriságok rendezése után:

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

Határozzuk meg szóhosszúságokat. Az f, a, h és c esetében: $3^{-2} = r^{-l_i} \leq p_i < r^{-l_i+1} = 3^{-1}$ Tehát azok szóhosszúsága 2. A többi esetben is így járunk el:

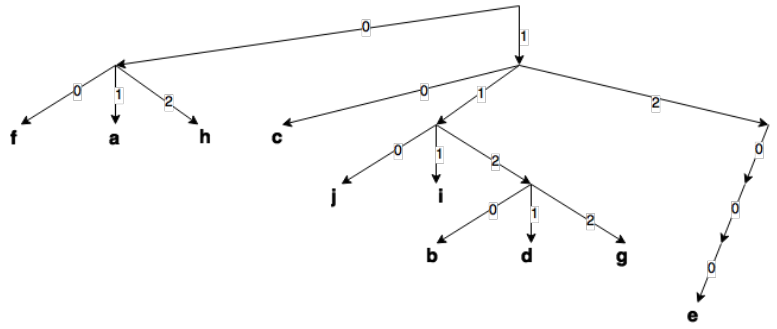
f	a	h	c	j	i	b	d	g	e
0,31	0,17	0,17	0,13	0,09	0,06	0,02	0,02	0,02	0,01
2	2	2	2	3	3	4	4	4	5

Ezek alapján f kódszava a 00, a kódszava a 01, h-hoz a 02 tartozik, míg c-hez 10. A j-hez ezek után 11 tartozna, de mivel az 3 hosszú, így 110.

A kódszavak tehát a következőképp alakulnak:

f	a	h	c	j	i	b	d	g	e
0,31	0,17	0,17	0,13	0,09	0,06	0,02	0,02	0,02	0,01
2	2	2	2	3	3	4	4	4	5
00	01	02	10	110	111	1120	1121	1122	12000

Az elkészült kódfa 3. ábrán látható.



3. ábra. Shannon-kód példa 1. kódfája

Hufmann-kód

A Huffman-kód is optimális kód (r elemszámú ábécével és p_i gyakoriságokkal), melyet a következő módon állítunk elő.

1. Rendezzük a betűket relatív gyakoriságaik alapján csökkenő sorrendbe.

2. Annak érdekében, hogy csak egy csonka csúcs keletkezzen

$$m \equiv n \mod r-1$$

kongruenciának teljesülnie kell, ahol m az egyetlen csonka csúcs kifoka. Ami ekvivalens azzal, hogy $m = 2 + ((n-2) \mod r-1)$. Tehát osszuk el $n-2$-t $r-1$-gyel, és így m a maradék+2 lesz.

3. Az első lépésben a sorozat m utolsó betűjét összevonjuk (új jelölést/betűt adunk neki), és ennek a relatív gyakorisága a tagok relatív gyakoriságának összege lesz. Rendezzük a sorozatot. Ezen lépés után már a betűk száma kongruens $r-1$-gyel, így a következő redukciós lépésekben mindig teljes csúcsokat tudunk készíteni.

4. Az utolsó r betűt vonjunk össze, helyettesítsük egy új betűvel és relatív gyakoriság legyen a relatív gyakoriságok összege.

5. A 4-es redukciós lépést addig ismételjük míg r db betű nem marad. Ekkor rendre minden betűhöz a kódábécé egy-egy betűjét rendeljük.

6. Ha redukált elemmel találkozunk szétbontjuk, majd az ő elemeihez is a kódábécé betűit rendeljük, de konkatenáljuk az előzővel.

7. A 6-os lépést addig ismételjük míg marad redukált elem.

Példa 1:

A Shannon-kódnál látott forrást kódoljuk be ugyanúgy $\{0, 1, 2\}$ kódábécével.

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

Rendezzük relatív gyakoriság szerint:

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

Osszuk el $n-2$-t $r-1$-gyel: $10-2=4*(3-1)+0$. Így m a maradék+2, azaz $m=2$. Az utolsó m betűt összevonjuk, és rendezzük a sorozatot:

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

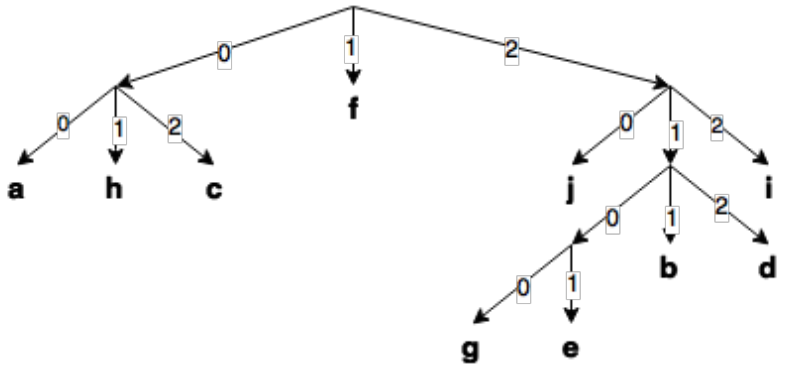
Innentől kezdve minden redukciós lépésben az utolsó r db azaz 3 betűt vonjuk össze:

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

Ezt addig ismételjük, míg r darab betű marad:

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

A szétbontás alapján a 4. ábrán látható fát tudjuk összeállítani.



4. ábra. Huffman-kód példa 1. kódfája

Ezek alapján a kódtábla:

betű	gyakoriság	kód
f	0,31	1
a	0,17	00
h	0,17	01
c	0,13	02
j	0,09	20
i	0,06	22
b	0,02	211
d	0,02	212
g	0,02	2100
e	0,01	2101