Diszkrét matematika II.

Mérai László előadásai alapján

Utolsó módosítás: 2024. január 19.

1. Beugró kérdések

1.1. Számelmélet

1. Mondja ki a maradékos osztás tételét! Ossza el maradékosan 18-at 7-tel!

1.1.1. Tétel. Maradékos osztás

$$\forall a, b \in \mathbb{Z},\ b \neq 0,\ \exists! q, r \in \mathbb{Z}\ :\ a = bq + r\ \wedge\ 0 \leq r < |b|$$

Jelölése: $r = \boxed{a \mod q}$ (kiejtése: „a modulo q”). Az operáció neve **modulo**.
A $\boxed{q}$ számot **hányados**nak nevezzük, az $\boxed{r}$ szám pedig az **osztási maradék**.

Bizonyítás. A tételt csak nemnegatív számok esetében bizonyítjuk.

(a) Létezés: a szerinti indukcióval.

Ha $a < b$, akkor $a = b \cdot 0 + a$ ($q = 0$, $r = a$).

Ha $a \geq b$, akkor tegyük fel, hogy a-nál kisebb számok már felírhatók ilyen alakban. Legyen $a - b = bq' + r'$. Ekkor $a = b(q' + 1) + r'$ és legyen $q = q' + 1, r = r'$.

(b) Egyértelműség: Legyen $a = bq + r = bq' + r'$. Ekkor $b(q - q') = r' - r$. Ez csak akkor lehet, ha $q = q'$ és $r = r'$.

Megoldás. $18 \mod 7 = 4$.

2. Definiálja a legnagyobb közös osztót! Mi lesz $(12, 18)$?

1.1.1. Definíció. Legnagyobb közös osztó

Legyenek $a, b \in \mathbb{Z}$ és $d \in \mathbb{N}$. A d **az** a **és** b **legnagyobb közös osztója**, ha

- $d|a\ \wedge\ d|b$
- $\forall k \in \mathbb{Z}\ :\ (k|a\ \wedge\ k|b) \implies k|d$

Jelölése: $d = (a, b) = \mathrm{lnko}(a, b) = \gcd(a, b)$. Definíció szerint $(0, 0) = 0$

Megoldás. Az euklideszi-algoritmussal megkapjuk, hogy $\mathrm{lnko}(12, 18) = 6$.

3. Mondja ki a lineáris diofantikus egyenletek megoldhatóságáról szóló tételt! Megoldható-e a $12x + 18y = 5$ egyenlet? Ha igen, adjon megoldást, ha nem, indokoljon!

1.1.2. Tétel. Bővített euklideszi algoritmus

Minden $a, b, c \in \mathbb{Z}$ esetén **pontosan** akkor léteznek $x, y \in \mathbb{Z}$, hogy $ax + by = c$, ha $(a, b)|c$.

$$\forall a, b, c \in \mathbb{Z},\ (a, b)|c,\ \exists x, y \in \mathbb{Z}\ :\ ax + by = c$$

Bizonyítás. Elég $c = (a, b)$ esetet vizsgálni.
Legyenek $q_i, r_i \in \mathbb{Z}$ az *euklideszi algoritmus*sal megkapott hányadosok, maradékok:

$$r_{i-2} = r_{i-1} \cdot q_i + r_i.$$

Legyen $x_{-1} := 1,\ x_0 := 0$ és

$$x_i = x_{i-2} - q_i \cdot x_{i-1} \quad (i \geq 1).$$

Hasonlóan legyen $y_{-1} := 0,\ y_0 := 1$ és

$$y_i = y_{i-2} - q_i \cdot y_{i-1} \quad (i \geq 1).$$

Ekkor $i \geq 1$ esetén: $x_i \cdot a + y_i \cdot b = r_i,$ ami speciálisan $x_n a + y_n b = r_n = (a, b)$:

- $i = -1, 0$ esetében: $r_{-1} = 1 \cdot a + 0 \cdot b,\ r_0 = 0 \cdot a + 1 \cdot b$
- más esetben:

$$\begin{aligned} r_{i-2} &= x_{i-2} \cdot a + y_{i-2} \cdot b \\ r_{i-1} &= x_{i-1} \cdot a + y_{i-1} \cdot b \\ r_i &= r_{i-2} - r_{i-1} \cdot q_i \end{aligned} \iff \begin{aligned} r_i &= (x_{i-2} \cdot a + y_{i-2} \cdot b) - (x_{i-1} \cdot a + y_{i-1} \cdot b) \cdot q_i \\ &= (x_{i-2} - q_i \cdot x_{i-1}) \cdot a + (y_{i-2} - q_i \cdot y_{i-1}) \cdot b \end{aligned}$$

Megoldás. Mivel $\text{lnko}(12, 18) = 6 \ \wedge\ 6 \nmid 5 \longrightarrow$ nincs megoldás.

4. Definiálja a prímszámokat! Az alábbi számok közül melyek prímek: 1, 2, 3, 4, 5, 6?

1.1.2. Definíció. Prímszámok

Egy $p \neq 0, \pm 1$ szám **prímszám**, ha

$$p = a \cdot b \implies p = \pm a \ \vee\ p = \pm b$$

Megoldás. 2, 3, 5.

5. Mondja ki a számelmélet alaptételét! Írja fel az $n = 18$-at a tétel szerint!

1.1.3. Tétel. Számelmélet alaptétele

$\forall n \in \mathbb{Z} \backslash \{0, \pm 1\}$ sorrendtől és előjeltől eltekintve egyértelműen felírható prímszámok szorzataként:

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} = \pm \prod_{i=1}^{\ell} p_i^{\alpha_i}$$

ahol $p_1, p_2, \ldots, p_\ell$ pozitív prímek és $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ pozitív egészek.

Megoldás. $n = 18 = 2^1 \cdot 3^2$.

6. Definiálja a kongruencia relációt! Mondjon példát két különböző x egészre, mely teljesíti az $x \equiv 3 \mod 4$ relációt!

1.1.3. Definíció. Kongruencia

Adott $n \neq 0$ és $a, b \in \mathbb{Z}$ esetén, a **kongruens b-vel modulo** n;

$$a \equiv b \mod n, \quad \text{ha } n | (a - b).$$

Megoldás. $x_1 = 3,\ x_2 = 7$.

7. Mondja ki a lineáris kongruenciák megoldhatóságára vonatkozó tételt! Megoldható-e a $12x \equiv 2 \mod 10$ lineáris kongruencia? Ha igen, adja meg az összes megoldást, ha nem, indokoljon!

1.1.4. Tétel. Lineáris kongruenciák

Legyenek $a, b, n \in \mathbb{Z}$, $n > 1$. Azt mondjuk, hogy

$$ax \equiv b \mod n \text{ megoldható} \iff (a,n)|b$$

és pontosan (a,n) darab inkongruens megoldása van $\mod n$.

Bizonyítás. A bizonyítás algoritmikus.

$$ax \equiv b \mod n \iff ax + ny = b$$

I. Szükséges feltétel ($\Longrightarrow$): mivel (a,n) osztja a bal oldalt, osztja a jobb oldalt is, azaz

$$(a,n)|ax \implies (a,n)|ax + ny.$$

II. Elégséges feltétel ($\Longleftarrow$): a **bővített euklideszi algoritmus** szerint

$$\exists x_0, y_0 \in \mathbb{Z} \ : \ x_0 a + y_0 n = (a,b).$$

Beszorozva $\dfrac{b}{(a,n)}$ -nel megkapjuk a megoldást.

III. Megoldások száma: Legyen $a' := \dfrac{a}{(a,n)}$, $b' := \dfrac{b}{(a,n)}$, $n' := \dfrac{n}{(a,n)}$. Ekkor $(a', b') = 1$.

Ha (x_0, y_0) és (x_1, y_1) két megoldása az $a'x + n'y = b'$ egyenletnek, akkor

$$a'(x_0 - x_1) + n'(y_0 - y_1) = 0.$$

Ekkor $x_0 \equiv x_1 \mod n'$.

További megoldások: $\boxed{\dfrac{b}{(a,n)} \cdot x + k \cdot n' \quad (k = 0, \ldots, (a,n) - 1)}$.

Megoldás. $12x \equiv 2 \mod 10$. Hozzáadunk 10-et a jobb oldalhoz, amíg osztahtó nem lesz.

$$\begin{aligned} 12x &\equiv 12 \mod 10 \quad /(12,10) = 2 \\ 6x &\equiv 6 \mod 5 \quad / : 6 \\ x &\equiv 1 \mod 5 \end{aligned}$$

8. Mondja ki a kínai maradéktételt! Megoldható-e az

$$\left.\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \end{aligned}\right\}$$

szimultán kongruenciarendszer? Ha igen, adja meg az összes megoldást, ha nem, indokoljon!

1.1.5. Tétel. Kínai maradék tétel

Legyenek $k \in \mathbb{N}^+$, $n_1, n_2, \ldots, n_k \in \mathbb{N}\backslash\{0,1\}$ páronként relatív prímszámok és $c_1, c_2, \ldots, c_k \in \mathbb{Z}$. Ekkor a

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}\right\}$$

kongruenciarendszer megoldható és bármely két megoldása kongruens egymással modulo $n_1 \cdot n_2 \cdots n_k$.

Bizonyítás. A bizonyítás algoritmikus.

I. Legyen $k := 2$:

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \end{aligned}\right\}$$

A **bővített euklideszi algoritmus**sal oldjuk meg az alábbi egyenletet:

$$n_1x_1 + n_2x_2 = 1.$$

Legyen $c_{1,2} := n_1x_1 \cdot c_2 + n_2x_2 \cdot c_1$. Ekkor[a]

$$c_{1,2} = n_1x_1 \cdot c_2 + n_2x_2 \cdot c_1 = c_2 \cdot \overbrace{(1 - n_2x_2)}^{n_1x_1+n_2x_2=1} + n_2x_2 \cdot c_1 = c_2 + (c_1 - c_2)n_2x_2$$

Ebből az következik, hogy

$$c_{1,2} \equiv c_1 \mod n_1 \tag{1}$$
$$c_{1,2} \equiv c_2 \mod n_2 \tag{2}$$

A (2) egyenletet megkapjuk a fentiekhez hasonló átalakításokkal. Összegezve,

$$c_{1,2} \equiv c_j \mod n_j \quad (j = 1, 2).$$

Ha $x \equiv c_{1,2} \mod n_1n_2$, akkor x megoldása a két kongruenciának. Megfordítva: ha x megoldása a két kongruenciának, akkor az $(x - c_{1,2})|n_1 \ \wedge \ (x - c_{1,2})|n_2$, így a szorzatukkal is: $x \equiv c_{1,2} \mod n_1n_2$ (ne feledjük, hogy $(n_1, n_2) = 1$).

II. Általános eset. Az alábbi

$$\left.\begin{aligned} x &\equiv c_1 \mod n_1 \\ x &\equiv c_2 \mod n_2 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}\right\}$$

szimultán kongruencia ekvivalens a

$$\left.\begin{aligned} x &\equiv c_{1,2} \mod n_1n_2 \\ x &\equiv c_3 \mod n_3 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}\right\}$$

rendszerrel. Iterálva az eljárást, megkapjuk az

$$x \equiv c_{1,\ldots,k} \mod n_1n_2\ldots n_k$$

kongruenciát.

[a]Forrás: `https://www.wikiwand.com/en/Chinese_remainder_theorem#Existence_(constructive_proof)`

Megoldás. $x \equiv \overbrace{1}^{c_1} \mod \overbrace{2}^{n_1}$ és $x \equiv \overbrace{2}^{c_2} \mod \overbrace{3}^{n_2}$.
$(2,3) = 1 \Longrightarrow$ megoldható a szimultán kongruencia. $2x_1 + 3x_2 = 1 \Longrightarrow x_1 = -1, x_2 = 1$.
Legyen $c_{1,2} := c_2 n_1 x_1 + c_1 n_2 x_2 = 2 \cdot 2 \cdot 1 + 1 \cdot 3 \cdot (-1) = -1$

$$\begin{aligned} x &\equiv c_{1,2} && \mod (n_1 n_2) \\ x &\equiv -1 && \mod 6 \\ x &\equiv 5 && \mod 6 \end{aligned}$$

9. Definiálja az Euler-féle φ függvényt! Mi lesz $\varphi(6)$? *Megoldás.* $\varphi(6) = 2$.

1.1.4. Definíció. Euler-függvény

Adott $n \in \mathbb{N}$ szám esetén legyen

$$\varphi(n) = |\{1 \le a < n \mid (a,n) = 1\}|$$

az **Euler-függvény** (vagy **Euler-féle φ-függvény**).

10. Mondja ki az Euler–Fermat-tételt! Mi lesz $3^4 \equiv ? \mod 8$? Válaszát indokolja!

1.1.6. Tétel. Euler–Fermat-tétel

Legyenek $a, n \in \mathbb{Z}$, $(a,n) = 1$. Ekkor

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

ahol φ az Euler-függvény.

Bizonyítás. Lineáris kongruenciákkal.
Tekintsük az

$$ax \equiv b \mod n$$

lineáris kongruenciát. Mivel $(a,n) = 1$, minden b-hez létezik egyértelmű (vagyis pontosan egy) x megoldás, azaz az

$$x \mapsto ax \mod n,$$

ami $\mathbb{Z}_n^*$ maradékosztálynak egy bijekciója. Így a

$$\mathbb{Z}_n^* \quad \text{és} \quad \{ax \mod n \mid x \in \mathbb{Z}_n^*\}$$

halmazok azonosak. Ekkor a halmazok elemeinek **szorzata** is megegyezik:

$$\prod_{x \in \mathbb{Z}_n^*} x \equiv \prod_{x \in \mathbb{Z}_n^*} ax \equiv a^{\varphi(n)} \cdot \prod_{x \in \mathbb{Z}_n^*} x \mod n.$$

Mivel

$$\left(n, \prod_{x \in \mathbb{Z}_n^*} x\right) = 1$$

így a szorzattal egyszerűsíthetünk: $1 \equiv a^{\varphi(n)} \mod n$.

Megoldás. $(3,8) = 1$ ✓. $\varphi(8) = 4$ ✓. Így $3^{\varphi(8)} = 3^4 \equiv 1 \mod 8$.

1.2. Polinomok

1. Definiálja a polinomok fokát! Mennyi lesz $\deg(x^3+x-1) = ?$

1.2.1. Definíció. Polinomok foka

Adott polinom $f := c_n x^n + \ldots + c_0$ **együtthatói** a $c_n, \ldots, c_0$ számok, míg $c_n \neq 0$ esetén f **foka** $\deg f = n$ és **főegyütthatója** c_n.

Megoldás. $\deg(x^3+x-1) = 3$.

2. Definiálja a maradékos osztást polinomok körében! Ossza el maradékosan az $f = x^3+3x+1 \in \mathbb{Q}[x]$ polinomot a $g = x+1 \in \mathbb{Q}[x]$ polinommal!

1.2.1. Tétel. Maradékos osztás polinomok körében

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$ és $f, g \in \mathbb{K}[x]$, $g \neq 0$. Ekkor

$$\exists q, r \in \mathbb{K}[x] : f = q \cdot g + r \ \wedge \ \deg r < \deg g.$$

Bizonyítás. A bizonyítás analóg az egész számok esetéhez, $\deg f$ szerinti teljes indukcióval bizonyítjuk. Ha $\deg f < \deg g$, akkor legyen $q = 0$, $r = f$.
Tegyük fel, hogy ha $\deg f < n$, akkor igaz az állítás. Legyen most

$$f := c_n x^n + \ldots + c_0 \quad \text{és} \quad g := d_m x^m + \ldots + d_0 \quad (c_n, d_m \neq 0,\ n \geq m).$$

Legyen $\tilde{f} := f - \frac{c_n}{d_m} x^{n-m} \cdot g$. Ekkor $\deg \tilde{f} < n$. Az indukció szerint legyen

$$\tilde{f} = f - \frac{c_n}{d_m} x^{n-m} \cdot g = \tilde{q} \cdot g + \tilde{r} \quad (\deg \tilde{r} < \deg g).$$

Ekkor

$$f = \left(\tilde{q} + \frac{c_n}{d_m} x^{n-m} \right) \cdot g + \tilde{r}.$$

Megoldás. $f : g = x^2 - x + 4$.

3. Mondja ki a gyöktényező kiemelhetőségére vonatkozó tételt! Mondjon példát két olyan g polinomra, melynek gyöke az $x = 1$ és $x = 2$ érték!

1.2.2. Tétel. A gyöktényező kiemelhetősége

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$. Legyenek $f \in \mathbb{K}[x]$ és $x_1 \in \mathbb{K}$ egy gyöke. Ekkor f felírható $f = (x - x_1) \cdot g$ formában valamely $g \in \mathbb{K}[x]$ polinommal.

Megoldás. $g_1 := x(x-1) = x^2 - x$, $g_2 := x(x-2) = x^2 - 2x$.

4. Mondja ki a polinom foka és gyökeinek száma közötti összefüggést! Hány gyöke lehet az $f = x^5 + x + 1 \in \mathbb{Q}[x]$ polinomnak?

1.2.3. Tétel. Összefüggés polinom foka és gyökeinek száma között

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$. Egy $f \in \mathbb{K}[x]$ polinomnak legfeljebb $\deg f$ gyöke lehet.

Bizonyítás. A bizonyítás $\deg f$ szerinti teljes indukcióval.

I. $\boxed{\deg f = 0}$: azaz $f = c_0$, $c_0 \neq 0$, akkor f-nek nincs gyöke.

II. $\boxed{\deg f \geq 1}$: ha f-nek nincs gyöke, akkor igaz az állítás.
Ellenkező esetben legyen $x_1 \in \mathbb{K}$ egy gyöke. A **maradékos osztás tétele** szerint

$$f = q \cdot (x - x_1) + r, \ \deg r < 1, \ r \in \mathbb{K}.$$

Mivel $f(x_1) = 0 = q(x_1) \cdot (x_1 - x_1) + r$, így $r = 0$, tehát $f = q \cdot (x - x_1)$ és $\deg q = n - 1$.

Ha x_2 egy másik gyöke f-nek ($x_2 \neq x_1$), akkor

$$0 = f(x_2) = q(x_2) \cdot (x_2 - x_1) \implies q(x_2) = 0.$$

Mivel q-nak legfeljebb $\deg q = n - 1$ gyöke van, így f-nek lefeljebb $n - 1 + 1 = n$ gyöke lehet.

Megoldás. f-nek legfeljebb $\deg f = 5$ gyöke lehet.

5. Definiálja polinomok legnagyobb közös osztóját! Mi lesz az $f = (x - 1)(x + 1) \in \mathbb{Q}[x]$ és $g = x(x - 1)^2(x + 1) \in \mathbb{Q}[x]$ polinomok legnagyobb közös osztója?

1.2.2. Definíció. Legnagyobb közös osztó polinomokra

$f, g \in \mathbb{K}[x]$ polinomok legnagyobb közös osztója $h = (f, g) = \text{lnko}(f, g) \in \mathbb{K}[x]$, ha

- h közös osztó: $h|f \ \wedge \ h|g$;
- h a legnagyobb: $q|f \ \wedge \ q|g \implies q|h$;
- h főegyütthatója 1.

Megoldás. f gyökei $x_{f1} = 1$, $x_{f2} = -1$; g gyökei $x_{g1} = 0$, $x_{g2} = 1$ (kétszeresen) és $x_{g3} = -1$.
Közös gyökök: $1, -1$. Tehát $\text{lnko}(f, g) = (x - 1)(x + 1)$.

Alternatív módon az euklideszi algoritmussal vagy polinomosztással is kiszámolható.

6. Definiálja a formális deriváltat! Mi lesz az $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ polinom formális deriváltja?

1.2.3. Definíció. Formális derivált

Polinomokra definiáljuk az f' formális deriváltat a következő módon:

- $(x^n)' = n \cdot x^{n-1}$
- $(c \cdot f)' = c \cdot f'$
- $(f + g)' = f' + g'$

Megoldás. $f' = 2x + 1 \equiv 1 \mod 2$ (ugyanis $\mathbb{Z}_2$ felett vagyunk).

7. Definiálja az irreducibilis polinom fogalmát! Irreducibilis lesz-e az $f = (x+1)(x+2) \in \mathbb{R}[x]$ polinom?

1.2.4. Definíció. Irreducibilis polinom

Egy f polinom **irreducibilis**, ha nem bontható szorzatra nem-triviális módon, azaz

$$f = g \cdot h \Longrightarrow \deg g = \deg f \ \vee \ \deg h = \deg f.$$

Megoldás. Mivel a polinom felírható szorzatként, így nem irreducibilis.

8. Definiálja a kongruencia relációt polinomok körében! Mondjon példát két különböző $g \in \mathbb{Z}_2[x]$ polinomra, mely teljesíti a $g \equiv x+1 \mod x^2+x+1$ relációt!

1.2.5. Definíció. Kongruenciareláció polinomokra

Legyen $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p\}$ és legyen $h \in \mathbb{K}[x]$ úgy, hogy $h \neq 0$. Ekkor

$$\forall f, g \in \mathbb{K}[x] : h|(f-g) \Longrightarrow f \equiv g \mod h.$$

Megoldás. $g := x+1$ vagy $g := x^2$.

9. Mondja ki a Lagrange interpolációról szóló tételt! Hány olyan legfeljebb harmadfokú polinom van, mely a 3 helyen a 2-t, az 1 helyen a 0-t, a 6 helyen a -9-t és a 0 helyen a -1-t veszi fel?

1.2.4. Tétel. Lagrange-interpoláció

Legyenek $x_0, x_1, \ldots, x_n \in \mathbb{C}$ páronként különböző **alappontok** és $y_0, y_1, \ldots, y_n \in \mathbb{C}$ tetszőleges értékek. Ekkor

$$\exists! f \in \mathbb{C}[x] : \deg f \leq n \ \wedge \ f(x_i) = y_i \quad (i \in [0..n]).$$

Bizonyítás.

I. Létezés: volt, Lagrange-alappolinomokkal.

$$L_i := \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - x_i}{x_j - x_i}, \qquad f := \sum_{i=0}^{n} y_i L_i$$

II. A polinom fokszáma: mivel $\deg L_i = 0$, így $\deg f = \deg \sum_i y_i L_i \leq n$.

III. Egyértelműség: ha $f(x_i) = g(x_i) = y_i$ $(i \in [0..n])$ és $\deg f, \deg g \leq n$, akkor legyen $F := f - g$. Ekkor $\deg F \leq n$. Ekkor $F(x_i) = 0$, így F-nek $n+1$ gyöke van, ellentmondás.

Megoldás. A tétel szerint pontosan egy ilyen létezik, ami legfeljebb harmadfokú.

1.3. Kódelmélet

1. Definiálja a betűnkénti kódolás fogalmát! Betűnkénti kódolás lesz-e a $\varphi(a) = 01$, $\varphi(b) = 11$, $\varphi(c) = 01$ függvény?

1.3.1. Definíció. Betűnkénti kódolás / Kódolás

Legyen $\mathcal{X} := \{x_1, x_2, \ldots, x_n\}$ halmaz a **forrásábécé** és $\mathcal{Y} := \{y_1, y_2, \ldots, y_k\}$ a **kódábécé**. Ekkor egy $\varphi : \mathcal{X} \to \mathcal{Y}^*$ **injektív** függvényt **(betűnkénti) kódolás**nak hívunk.

- $\mathcal{Y}^*$ jelöli az $\mathcal{Y}$ elemeiből álló véges szavak halmazát.
- A φ függvényt kiterjesztjük az $\mathcal{X}^*$ halmazra betűnként:

$$\varphi(u_1 u_2 \ldots u_r) = \varphi(u_1)\varphi(u_2)\ldots\varphi(u_r).$$

Megoldás. Nem, ugyanis $\varphi(a) = \varphi(c) = 01$, azaz φ nem injektív.

2. Definiálja a felbontható kódolás fogalmát! Felbontható kódolás lesz-e a $\varphi(a) = 01$, $\varphi(b) = 11$, $\varphi(c) = 10$ függvény?

1.3.2. Definíció. Felbontható kódolás

Egy $\varphi : \mathcal{X} \to \mathcal{Y}^*$ kódolás **felbontható** (vagy **egyértelműen dekódolható**), ha

$$\forall \mathbf{u}, \mathbf{v} \in \mathcal{X}^*, \mathbf{u} \neq \mathbf{v} : \varphi(u_1)\varphi(u_2)\ldots\varphi(u_r) \neq \varphi(v_1)\varphi(v_2)\ldots\varphi(v_s),$$

ahol $\mathbf{u} := u_1 u_2 \ldots u_r$ és $\mathbf{v} = v_1 v_2 \ldots v_s$.

Megoldás. Igen, felbontható – nincs olyan eset, hogy két kódszó ugyanaz lenne.

3. Definiálja a prefix kódok fogalmát! Adjon meg az $\{a, b, c\}$ forrásábécén egy prefixkódolását!

1.3.3. Definíció. Prefixkód

Egy φ kódolás **prefixkód** (vagy **prefixmentes kód**), ha

$$\nexists \mathbf{u}, \mathbf{v} \in \mathcal{X}^*, \mathbf{u} \neq \mathbf{v} : \mathbf{u} \text{ prefixe } \mathbf{v}\text{-nek}.$$

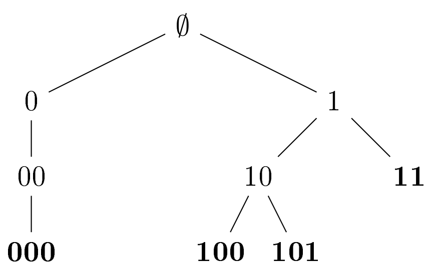
Megoldás. Legyen $\mathcal{Y} := \{0, 1\}$ a kódábécé. $\varphi(a) := 00$, $\varphi(b) := 01$, $\varphi(c) := 10$.

4. Definiálja a kódfa fogalmát! Rajzolja fel a $\{100, 101, 11, 000\}$ kód kódfáját!

1.3.4. Definíció. Kódfa

Egy φ kód **kódfája** egy olyan fa, melynek csúcsai a **kódszavak** és azok **prefixei**, valamint az $y_1 y_2 \ldots y_s$ és $y_1 y_2 \ldots y_{s+1}$ csúcsok vannak összekötve.

Megoldás.



5. Definiálja a Hamming-távolságot! Mennyi lesz $d(010, 110) = ?$, $d(0000, 0009) = ?$

1.3.5. Definíció. Hamming-távolság

Legyen $\mathbf{u}, \mathbf{v} \in \Sigma^n$ két szó. A szavak **Hamming-távolsága**:

$$d(\mathbf{u}, \mathbf{v}) := |\{i \in [1..n] \mid u_i \neq v_i\}|.$$

Megoldás. $d(010, 110) = 1$. $d(0000, 0009) = 1$.

6. Mondja ki a kód kódtávolsága és a hibajelző, hibajavító képesség közötti összefüggést! Hány hibát jelez ill. javít a $\mathcal{C}$ kód, ha $d(\mathcal{C}) = 8$?

1.3.1. Tétel. Összefüggés a kódtávolság és a hibajelző és -javító képesség közt

Egy $\mathcal{C}$ kód $d = d(\mathcal{C})$ kódtávolsággal:

- $d - 1$ hibát tud **jelezni**;
- $t = \left\lfloor \dfrac{d-1}{2} \right\rfloor$ hibát tud **javítani**.

Megoldás. A $\mathcal{C}$ kód 7 hibát tud jelezni és 3 hibát tud javítani.

7. Definiálja a lineáris kódok fogalmát! Lineáris lesz-e a $\mathcal{C} = \{110, 101, 111\} \subset \mathbb{Z}_2^3$ kód?

1.3.6. Definíció. Lineáris kód

Egy $\mathcal{C} \subset \mathbb{F}_q^n$ kód **lineáris**, ha $\mathcal{C}$ egy lineáris altér $\mathbb{F}_q^n$-ben. Ekkor $k = \dim \mathcal{C}$ a kód **dimenziója**. Speciálisan, ha $|\mathcal{C}| = q^k$, akkor $\mathcal{C}$ egy (n, k) kód.

Megoldás. $\mathbb{Z}_2^3$: 3 hosszú és $\mathbb{Z}_2$ felett. $|\mathcal{C}| = 3$, $q = 2 \longrightarrow 2^k \neq 3 \Longrightarrow \forall k \in \mathbb{Z}$-re nem lineáris.

8. Definiálja lineáris kódok generátormátrixát! Mi lesz a $(b_1, b_2) \mapsto (b_1, b_2, b_1 + b_2)$ bináris lineáris kód generátormátrixa?

1.3.7. Definíció. Generátormátrix

Legyen $\mathcal{C}$ egy lineários (n, k) kód $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k$ generátorokkal. Ekkor a $\mathcal{C}$ egy **generátormátrixa** $G = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k) \in \mathbb{F}_q^{n \times k}$.

Megoldás. A lineáris kód egy paritásbit, ahol $k = 2$.

$$G = \begin{pmatrix} \mathbf{I}_k \\ \mathbf{1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{(2+1) \times 2}$$

9. Definiálja lineáris kódok ellenőrzőmátrixát! Mi lesz a $(b_1, b_2) \mapsto (b_1, b_2, b_1 + b_2)$ bináris lineáris kód ellenőrző mátrixa?

1.3.8. Definíció. Ellenőrzőmátrix

Legyen $\mathcal{C}$ egy (n, k) kód. Ekkor $\mathcal{C}$ **ellenőrzőmátrixa** az a $H \in \mathbb{F}_q^{(n-k) \times n}$ mátrix, melyre $H\mathbf{c} = 0$ pontosan akkor, ha $\mathbf{c} \in \mathcal{C}$.

Megoldás. A lineáris kód egy paritásbit, ahol $k = 2$. $H = \mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_q^{(n-1) \times n}$

2. Fogalmak

Ezen a listán csak azokat dolgoztam ki, amelyek nem szerepelnek explicite a beugró kérdéssorban.

1. Mondja ki a kongruencia és az alapműveletek közötti összefüggésre vonatkozó tételt!

2.0.1. Tétel. A kongruencia és az alapműveletek közti összefüggés

Legyenek $a, b, c, d, n \in \mathbb{Z}, n \neq 0$. Ekkor:

- $a \equiv b \mod n \ \wedge \ c \equiv d \mod n$ esetén $a + c \equiv b + d \mod n$
- $a \equiv b \mod n \ \wedge \ c \equiv d \mod n$ esetén $a \cdot c \equiv b \cdot d \mod n$

2. Mondja ki a Singleton-korlátot tetszőleges (nem feltétlen lináris) kódokra!

2.0.2. Tétel. Singleton-korlát

Egy $\mathcal{C} \subset \Sigma^n$ kód $d = d(\mathcal{C})$ minimális távolság esetén: $|\mathcal{C}| \leq (|\Sigma|)^{n-d+1}$.

Bizonyítás. Legyen $\mathcal{C}' \subset (|\Sigma|)^{n-d+1}$, amit $\mathcal{C}$ kódszavaiból kapunk az utolsó $d-1$ koordináta eltörlésével. Ha $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ $(\mathbf{u} \neq \mathbf{v})$, akkor $d(\mathbf{u}, \mathbf{v}) \geq d$, azaz legalább d pozíciıóban különböznek. Speciálisan, $\mathbf{u}, \mathbf{v}$ kódok $d-1$ koordináta eltörlése után is különböznek. Tehát $|\mathcal{C}| = |\mathcal{C}'| \leq (|\Sigma|)^{n-d+1}$.

3. Definiálja a szisztematikus kódolás fogalmát!

2.0.1. Definíció. Szisztematikus kódolás

Egy $\mathbf{u} \mapsto G\mathbf{u}$ kódolás **szisztematikus**, ha a kódszavak utolsó $n-k$ elemét elhagyva a kódolandó szót kapjuk, azaz az alábbi alakkal rendelkezik:

$$G = \begin{pmatrix} \mathbf{I}_k \\ B \end{pmatrix} \in \mathbb{F}_q^{n \times k}, \quad B \in \mathbb{F}_q^{(n-k) \times k}.$$

3. Tételek bizonyítása

Ezen a listán csak azokat dolgoztam ki, amelyek nem szerepelnek explicite a beugró kérdéssorban.

1. Bizonyítsa be, hogy a prefix kódok felbonthatóak! (10 pont)

3.0.1. Tétel. Prefixkódok felbonthatósága

Minden prefixkód felbontható.

Bizonyítás. Legyen $\mathbf{v} := v_1 v_2 \dots v_s \in \mathcal{Y}^*$ egy üzenet **kódolása** – azaz $\exists \mathbf{u} \in \mathcal{X}^* : \varphi(\mathbf{u}) = \mathbf{v}$.
Vizsgáljuk meg a prefixeit: $v_1,\ v_1v_2,\ v_1v_2v_3,\ \dots$
Ha találunk egy $v_1 v_2 \dots v_i$ $(i \in [1..s])$ szót, ami egy betű kódszavak, azt dekódolhatjuk.
Mivel a kód **prefix**, ez nem lehet más betű kódjának prefixe.
Az eljárást folytatjuk a $v_{i+1} v_{i+2} \dots v_s$ kóddal.