Diszkrét Matematika II. – Kidolgozott Vizsgatételek

1. Tétel: Számelméleti alapok

1. Oszthatóság az egész számok körében

Definíció: Azt mondjuk, hogy az a egész osztja a b egészet (jelölés: $a|b$), ha létezik olyan c egész, amellyel $a \cdot c = b$ (azaz b/a szintén egész).

- Példák: $1|13$, $6|12$, $-6|12$, $i|13$ (ez utóbbi a Gauss-egészekre vonatkozó kiterjesztés).
- **Tulajdonságok:**
  1. $a|b$ és $b|c \Rightarrow a|c$ (tranzitivitás).
  2. $a|b$ és $a|c \Rightarrow a|b+c$ és $a|b-c$.
  3. $a|b \Rightarrow a|bc$ tetszőleges c-re.
  4. $a|b$ és $b|a \iff |a| = |b|$ (az egész számok körében).

2. Egységek és asszociált számok

Egység: Azokat az elemeket, amelyek minden más elemet osztanak, *egységeknek* nevezzük. Az egész számok körében ($\mathbb{Z}$) az egységek az **1** és a **-1**. (Definíció szerint az egységek az 1 osztói).

Asszociáltak: Két szám, a és b *asszociáltak*, ha $a|b$ és $b|a$.

- Az egész számok körében ez azt jelenti, hogy $a = b$ vagy $a = -b$ (csak egységszorzóban térnek el).

3. Felbonthatatlan (irreducibilis) számok és prímszámok

Fontos különbséget tenni a két fogalom között, bár az egész számok körében egybeesnek.

- **Felbonthatatlan (irreducibilis):** Egy t nem nulla, nem egység elemet felbonthatatlannak nevezünk, ha csak triviális osztói vannak (az egységek és a saját asszociáltjai).
  - Formálisan: t felbonthatatlan, ha $t = ab \Rightarrow a$ vagy b egység.
- **Prímszám:** Egy p nem nulla, nem egység elemet prímnek nevezünk, ha rendelkezik a „prímtulajdonsággal”: ha p oszt egy szorzatot, akkor osztja legalább az egyik tényezőt.
  - Formálisan: p prím, ha $p|ab \Rightarrow p|a$ vagy $p|b$.

Kapcsolatuk (Azonosság és eltérés):

1. **Prím $\Rightarrow$ Felbonthatatlan:** Ez minden integritási tartományban (így az egészek körében is) igaz. (Bizonyítás vázlat a diáról: Ha p prím és $p = ab$, akkor $p|ab \Rightarrow p|a$ vagy $p|b$. Ha $p|a$, akkor $a = pk$, így $p = pkb \Rightarrow 1 = kb$, tehát b egység).
2. **Felbonthatatlan $\Rightarrow$ Prím:** Ez **az egész számok körében igaz** (a Számelmélet alaptétele miatt), de **„ravaszabb számkörökben” (általános gyűrűkben) nem**

feltétlenül.

- A diák példát nem hoznak konkrét „ravasz” számkörre (pl. $\mathbb{Z}[\sqrt{-5}]$), de hangsúlyozzák, hogy az egész számoknál a fordított irány bizonyításához szükség van a Bővített Euklideszi algoritmusra (vagy a számelmélet alaptételére).

4. Maradékos osztás tétele

Tétel: Tetszőleges a és $b \neq 0$ egész számokhoz egyértelműen léteznek q (hányados) és r (maradék) egész számok úgy, hogy:

$$a = bq + r, \quad \text{ahol } 0 \leq r < |b|.$$

- Ez biztosítja az euklideszi algoritmus működését.

5. Legnagyobb közös osztó (LNKO) és Legkisebb közös többszörös (LKKT)

- **LNKO** (a, b)**:** Az a d szám, amelyre $d|a$, $d|b$, és ha $c|a$ és $c|b$, akkor $c|d$.
- **LKKT** $[a, b]$**:** Az az m szám, amelyre $a|m$, $b|m$, és ha $a|c$ és $b|c$, akkor $m|c$.
- **Kapcsolatuk:** $|a \cdot b| = (a, b) \cdot [a, b]$.

6. Bővített Euklideszi algoritmus

Ez az eljárás nemcsak megadja két szám LNKO-ját, hanem elő is állítja azt a két szám lineáris kombinációjaként.

- **Algoritmus:** A maradékos osztásokat végezzük ismételten:
  1. $r_{n-2} = q_n r_{n-1} + r_n$
  2. Amikor a maradék 0 lesz, az utolsó nem nulla maradék az LNKO.
- **Lineáris kombináció:** Visszafelé helyettesítve kifejezhetjük az LNKO-t $d = ax + by$ alakban.
- **Jelentősége:** Ezzel bizonyítható, hogy ha p felbonthatatlan, akkor prím is (az egészek körében). Továbbá ezzel oldhatók meg a lineáris diofantikus egyenletek és kongruenciák (inverz keresés).

7. A számelmélet alaptétele

Tétel: Minden 1-nél nagyobb egész szám felírható prímszámok szorzataként, és ez a felírás a tényezők sorrendjétől eltekintve egyértelmű.

- **Kanonikus alak:** $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

8. Számelméleti függvények ($\tau(n)$ és $\phi(n)$)

A kanonikus alakból ($n = \prod p_i^{\alpha_i}$) számolhatóak:

- Osztók száma ($\tau(n)$ vagy $d(n)$): A kanonikus alak kitevőit használva:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\dots(\alpha_k + 1)$$

  Magyarázat: Minden prímhatványból 0-tól α_i-ig választhatunk kitevőt, ezek kombinációi adják az osztókat.
- Euler-féle ϕ függvény: Az n-hez relatív prím számok száma n-ig. Kiszámítása a kanonikus alakból:

$$\phi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$$

  Multiplikativitás: Ha $(a, b) = 1$, akkor $\phi(ab) = \phi(a)\phi(b)$.

9. Prímek száma és eloszlása

- **Euklidész tétele:** Végtelen sok prímszám van.
  - *Bizonyítás:* Tegyük fel indirekt, hogy véges sok van: $p_1, \dots, p_n$. Legyen $N = p_1 \dots p_n + 1$. N-nek van prímfelbontása, de egyik p_i sem osztja (mert 1 maradékot adnak). Tehát kell lennie egy új prímnek.
- **Dirichlet tétele:** A diák *említik*, de bizonyítás nincs.
  - *Tétel:* Minden $an + b$ számtani sorozatban végtelen sok prím van, ha $(a, b) = 1$. (Megjegyzés: A diákban konkrétan a $4k - 1$, $4k + 1$, $6k - 1$, $6k + 1$ alakú prímekről lehet szó speciális esetként, de a tétel neve szerepel a listádban).
- **Eratoszthenész szitája:** Algoritmus prímek keresésére N-ig.
  1. Felírjuk a számokat 2-től N-ig.
  2. A legelső (2) prím, kihúzzuk a többszöröseit.
  3. A következő nem kihúzott szám prím, kihúzzuk a többszöröseit.
  4. Ezt addig ismételjük, amíg a vizsgált szám négyzete nagyobb nem lesz N-nél.

10. Kongruenciák

Definíció: Legyen $m \geq 2$ egész (modulus). Azt mondjuk, hogy a kongruens b-vel modulo m (jelölés: $a \equiv b \pmod{m}$), ha $m | a - b$, azaz a és b ugyanazt a maradékot adja m-mel osztva.

Tulajdonságok (Ekvivalencia reláció):

1. **Reflexív:** $a \equiv a \pmod{m}$.
2. **Szimmetrikus:** $a \equiv b \Rightarrow b \equiv a \pmod{m}$.
3. **Tranzitív:** $a \equiv b, b \equiv c \Rightarrow a \equiv c \pmod{m}$.
4. **Műveleti tulajdonságok:**
   - Ha $a \equiv b$ és $c \equiv d$, akkor $a + c \equiv b + d$ és $a \cdot c \equiv b \cdot d$.
   - Következmény: $a \equiv b \Rightarrow a^k \equiv b^k$.

11. Lineáris kongruenciák és Diofantikus egyenletek

Lineáris kongruencia: $ax \equiv b \pmod{m}$.

- **Megoldhatóság feltétele:** Pontosan akkor oldható meg, ha $(a, m) | b$.
- **Megoldások száma:** Ha megoldható, akkor (a, m) darab megoldása van modulo m.
- **Megoldás módja:** Visszavezethető lineáris diofantikus egyenletre.

Lineáris diofantikus egyenlet: $ax + by = c$ (ahol x, y egészek).

- Ez ekvivalens az $ax \equiv c \pmod{b}$ (és $by \equiv c \pmod{a}$) kongruenciával.
- Megoldás a Bővített Euklideszi algoritmussal: Először megoldjuk az $ax' + by' = (a, b)$ egyenletet, majd beszorzunk $c/(a, b)$-vel.

12. Szimultán kongruenciák és a Kínai maradék-tétel

Probléma: Keressük az x-et, amely több kongruenciát egyszerre elégít ki:

$x \equiv c_1 \pmod{m_1}$

$x \equiv c_2 \pmod{m_2}$

...

Kínai maradék-tétel (KMT):

Legyenek $m_1, m_2, \ldots, m_n$ páronként relatív prím számok. Ekkor a fenti kongruencia-rendszer megoldható, és a megoldás egyértelmű modulo $M = m_1 m_2 \ldots m_n$.

- Bizonyítás/Konstrukció elve: Legyen $M_i = M/m_i$. Mivel $(M_i, m_i) = 1$, létezik y_i, hogy $M_i y_i \equiv 1 \pmod{m_i}$. A megoldás: $x = \sum_{i=1}^{n} c_i M_i y_i \pmod{M}$.

13. Maradékosztályok és rendszerek

- **Maradékosztály:** Az egymással kongruens elemek halmaza. Modulo m pontosan m darab maradékosztály van ($\overline{0}, \overline{1}, \ldots, \overline{m-1}$).
- **Teljes maradékrendszer (TMR):** Olyan halmaz, amely minden maradékosztályból pontosan egy elemet tartalmaz (pl. $0, 1, \ldots, m-1$). Elemeinek száma m.
- **Redukált maradékrendszer (RMR):** Azon maradékosztályok reprezentánsaiból áll, amelyek relatív prímek a modulushoz ($(a, m) = 1$).
  - Elemeinek száma: $\phi(m)$.
  - Tulajdonság: Ha $a_1, \ldots, a_{\phi(m)}$ egy RMR és $(c, m) = 1$, akkor $ca_1, \ldots, ca_{\phi(m)}$ is RMR.

Műveletek: A maradékosztályokkal végezhető összeadás és szorzás ($\mathbb{Z}_m$ gyűrű). Ha $m = p$ prím, akkor $\mathbb{Z}_p$ test (van osztás is, kivéve nullával).

14. Kis Fermat-tétel és Euler-Fermat tétel

- Euler-Fermat tétel: Ha $(a, m) = 1$, akkor

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Ez az általánosítás.

- **Kis Fermat-tétel:** Ha p prím.
    1. alak: Ha $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$. (Ez az Euler-Fermat speciális esete, mivel $\phi(p) = p-1$).
    2. alak: Minden a-ra: $a^p \equiv a \pmod{p}$.

15. Gyors hatványozás

Nagy kitevős hatványok maradékának kiszámítására szolgáló algoritmus (pl. $a^b \pmod{m}$).

- **Módszer:** A kitevőt (b) kettes számrendszerbe írjuk, vagy "négyzetre emelés és szorzás" (square and multiply) módszert alkalmazunk.
    - Lépések: $a, a^2, a^4, a^8 \dots \pmod{m}$ kiszámolása ismételt négyzetre emeléssel, majd azok összeszorzása, ahol a kitevő bináris alakjában 1-es áll.
    - *Haszna:* A műveletigény logaritmikus a kitevő méretére nézve.

16. Generátor, Primitív gyök, Diszkrét logaritmus

- **Elem rendje:** A legkisebb $k > 0$, amire $a^k \equiv 1 \pmod{m}$. (Jelölés: $o_m(a)$). A rend mindig osztója $\phi(m)$-nek (Lagrange/Euler-Fermat miatt).
- **Primitív gyök (Generátor):** Olyan g elem, amelynek a rendje pontosan $\phi(m)$.
    - Ez azt jelenti, hogy g hatványai előállítják az összes redukált maradékosztályt (ciklikus csoportot alkotnak).
    - *Létezés:* Prímszám modulusra (p) mindig létezik primitív gyök.
- **Diszkrét logaritmus:** Ha g egy primitív gyök, akkor bármely a (ahol $(a,p)=1$) felírható $g^k \equiv a \pmod{p}$ alakban. Ezt a k kitevőt nevezzük az a diszkrét logaritmusának ($ind_g(a)$).
    - A diszkrét logaritmus kiszámítása nehéz probléma (erre épül a kriptográfia).

17. Titkosítás (Kriptográfia alapok)

- **Caesar-kód:** Betűk eltolása az ábécében fix k értékkel ($x \mapsto x+k \pmod{26}$). Szimmetrikus kulcsú, könnyen törhető.
- **RSA-titkosítás (Aszimmetrikus):**
    - **Kulcsgenerálás:** Választunk két nagy prímet (p, q). Modulus: $n = pq$. Kiszámoljuk $\phi(n) = (p-1)(q-1)$.
    - Választunk egy e titkosítási kitevőt, melyre $(e, \phi(n)) = 1$.
    - Kiszámoljuk a titkos d kitevőt: $d \equiv e^{-1} \pmod{\phi(n)}$ (bővített euklideszivel).
    - **Nyilvános kulcs:** (n, e). **Titkos kulcs:** (d).
    - **Titkosítás:** $c \equiv m^e \pmod{n}$.
    - **Megfejtés:** $m \equiv c^d \pmod{n}$. (Az Euler-Fermat tétel miatt működik).
- **Diffie-Hellman kulcscsere:**

- Cél: Közös titkos kulcs létrehozása nem biztonságos csatornán.
- Adott egy nagy p prím és egy g primitív gyök (ezek nyilvánosak).
- Alice választ titkos a-t, küldi: $A = g^a \pmod{p}$.
- Bob választ titkos b-t, küldi: $B = g^b \pmod{p}$.
- Alice számol: $K = B^a \pmod{p} = (g^b)^a = g^{ab}$.
- Bob számol: $K = A^b \pmod{p} = (g^a)^b = g^{ab}$.
- A közös titok K, amit egy lehallgató az A és B ismeretében nem tud könnyen kiszámolni (diszkrét logaritmus probléma nehézsége).

2. Tétel: Algebrai alapok, polinomok – Kidolgozott vizsgaanyag (Javított formázás)

1. Algebrai struktúrák alapjai

Binér művelet: Adott egy H halmaz. A H-n értelmezett *binér (kétváltozós) művelet* egy $f : H \times H \to H$ függvény. (Jelölése általában infix módon: $a * b$).

Asszociativitás: Egy $*$ binér művelet asszociatív a H halmazon, ha minden $a, b, c \in H$ esetén $(a * b) * c = a * (b * c)$.

- *Példa nem asszociatív műveletre:* A valós számok kivonása. $(5 - 3) - 1 = 1$, de $5 - (3 - 1) = 3$.

Kommutativitás: Egy $*$ binér művelet kommutatív a H halmazon, ha minden $a, b \in H$ esetén $a * b = b * a$.

- *Példa nem kommutatív műveletre:* Mátrixszorzás, vagy szövegek összefűzése ("a"+"b" $\neq$ "b"+"a").

Algebrai struktúra: Egy $(H; M)$ rendezett pár, ahol H egy nem üres halmaz, M pedig a H-n értelmezett műveletek halmaza.

Grupoid: Olyan algebrai struktúra, amelynek egyetlen binér művelete van: $(G; *)$.

Félcsoport: Olyan grupoid, amelynek művelete *asszociatív*.

- *Példa grupoidra, ami nem félcsoport:* $(\mathbb{Z}; -)$, mert a kivonás nem asszociatív.

Semleges elem (Egységelem): A G struktúra $e \in G$ eleme semleges elem, ha minden $a \in G$-re $a * e = e * a = a$.

Monoid: Olyan félcsoport, amelynek van semleges eleme. (Tehát: asszociatív és van egységelem).

Inverz: Egy monoidban az $a \in G$ elem inverze az a $b \in G$ elem, amelyre $a * b = b * a = e$ (ahol e a semleges elem).

Csoport: Olyan monoid, amelyben *minden elemnek létezik inverze*. (Tulajdonságok: zárt, asszociatív, van egységelem, minden elem invertálható).

Abel-csoport: Olyan csoport, amelyben a művelet *kommutatív*.

2. Gyűrűk és Testek

Disztributivitás: A $\cdot$ művelet disztributív a $+$ műveletre nézve, ha minden a, b, c-re: $a \cdot (b + c) = a \cdot b + a \cdot c$ és $(b + c) \cdot a = b \cdot a + c \cdot a$.

Gyűrű: Az $(R; +, \cdot)$ struktúra gyűrű, ha:

1. $(R; +)$ *Abel-csoport* (összeadásra nézve kommutatív csoport).
2. $(R; \cdot)$ *Félcsoport* (szorzásra nézve asszociatív).
3. A szorzás *disztributív* az összeadásra nézve.

Nullelem és Egységelem gyűrűben:

- **Nullelem (0):** Az összeadásra vonatkozó semleges elem.
- **Egységelem (1):** A szorzásra vonatkozó semleges elem (ha létezik).

Speciális gyűrűtípusok:

- **Egységelemes gyűrű:** Van benne szorzásra vonatkozó egységelem ($1 \neq 0$).
- **Kommutatív gyűrű:** A szorzás művelete is kommutatív.
- **Nullosztómentes gyűrű:** Ha $ab = 0$, akkor $a = 0$ vagy $b = 0$.
- **Integritási tartomány:** Kommutatív, egységelemes, nullosztómentes gyűrű.

Karakterisztika: Az a legkisebb pozitív n egész, amelyre $\underbrace{1 + \cdots + 1}_{n} = 0$. Ha nincs ilyen, a karakterisztika 0.

Osztó és Egység:

- **Osztó:** $a|b$, ha létezik c, hogy $b = ac$.
- **Egység (Invertálható elem):** Az az elem, amely osztója az egységelemnek (van inverze).

Példák:

- *Gyűrű:* Egész számok ($\mathbb{Z}$), Maradékosztályok ($\mathbb{Z}_m$).
- *Véges test:* $\mathbb{Z}_p$ (ahol p prím).
- *Végtelen test:* Valós számok ($\mathbb{R}$), Racionális számok ($\mathbb{Q}$).

Bizonyítandó állítások gyűrűkben:

1. **Nullelemmel való szorzás:** Bármely gyűrűben $a \cdot 0 = 0$.
   - *Bizonyítás:* $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$. Kivonva mindkét oldalból $a \cdot 0$-t kapjuk, hogy $0 = a \cdot 0$.
2. **Test nullosztómentessége:** Minden test nullosztómentes.
   - *Bizonyítás:* Tegyük fel, hogy $ab = 0$ és $a \neq 0$. Mivel testben vagyunk, létezik a^{-1}. Szorozzuk be balról: $a^{-1}(ab) = a^{-1} \cdot 0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0$.

3. Polinomok alapfogalmai

Polinom: Egy R gyűrű feletti polinom egy $(a_0, a_1, \ldots)$ végtelen sorozat, ahol véges sok kivétellel minden $a_i = 0$. Jelölés: $f(x) = \sum a_i x^i$.

Műveletek:

- *Összeadás:* Együtthatónként ($(f+g)_k = a_k + b_k$).
- *Szorzás:* Konvolúcióval ($(fg)_k = \sum_{j=0}^{k} a_j b_{k-j}$).

Öröklődő tulajdonságok ($R \to R[x]$):

Ha R gyűrű/kommutatív/egységelemes/nullosztómentes $\Rightarrow$ $R[x]$ is az.

Fogalmak:

- **Együttható:** Az a_k elemek.
- **Konstans tag:** Az a_0 elem.
- **Fokszám ($\deg f$):** A legnagyobb index, ahol az együttható nem 0.
- **Főegyüttható:** A fokszámhoz tartozó együttható.
- **Főtag:** A főegyüttható és a legmagasabb kitevőjű hatvány szorzata.
- **Konstans polinom:** Foka ≤ 0 (vagy a nullpolinom).
- **Nullpolinom:** Minden együtthatója 0 (foka általában $-\infty$).
- **Lineáris polinom:** Elsőfokú ($ax+b$).
- **Monom:** Egyetlen tagból álló polinom.
- **Főpolinom:** A főegyüttható 1.

Fokszámtételek és bizonyításuk:

1. **Összeg foka:** $\deg(f+g) \leq \max(\deg f, \deg g)$.
   - *Bizonyítás:* Ha k nagyobb mindkét foknál, akkor $a_k = 0$ és $b_k = 0$, így összegük is 0.
   - *Szigorú egyenlőtlenség példa:* $f = x+1$, $g = -x+2$. $\deg(f)=1, \deg(g)=1$, de $f+g=3$, aminek foka 0.
2. **Szorzat foka:** Ha R nullosztómentes, akkor $\deg(fg) = \deg f + \deg g$.
   - *Bizonyítás:* A legnagyobb indexű tag az $a_n b_m$ lesz. Mivel R nullosztómentes és $a_n \neq 0, b_m \neq 0$, ezért szorzatuk sem 0.

R tulajdonságainak öröklődése (Bizonyítás):

- *Egységelem:* Ha $1 \in R$, akkor a konstans 1 polinom egységelem $R[x]$-ben. (Mert a szorzásnál $(f \cdot 1)_k = a_k \cdot 1 = a_k$).

Függvénytani vonatkozások:

- **Helyettesítési érték:** $f(c)$ az az elem, amit x helyére c-t írva kapunk.
- **Gyök:** Az a c elem, amire $f(c) = 0$.
- **Polinomfüggvény:** A helyettesítés által generált $R \to R$ leképezés.
- *Példa különböző polinomra, azonos függvénnyel:* $\mathbb{Z}_p$ test felett x^p és x polinomok különbözőek (fokszámuk eltér), de a Kis Fermat-tétel miatt ugyanazt a függvényt adják ($c^p \equiv c$).

3. Tétel: Polinomok maradékos osztása és következményei

1. A polinomok maradékos osztásának tétele

Tétel: Legyen R egységelemes integritási tartomány (olyan gyűrű, ahol nincs nullosztó, van 1-es elem). Legyenek $f, g \in R[x]$ polinomok, és tegyük fel, hogy g főegyütthatója egység R-ben (invertálható).

Ekkor egyértelműen léteznek olyan q (hányados) és r (maradék) polinomok $R[x]$-ben, amelyekre:

$$f = q \cdot g + r, \quad \text{ahol } \deg(r) < \deg(g) \text{ vagy } r = 0.$$

Bizonyítás:

- **Egzisztencia (Létezés):** Az f foka szerinti teljes indukcióval.
  - Ha $\deg(f) < \deg(g)$, akkor legyen $q = 0$ és $r = f$. A feltétel teljesül.
  - Ha $\deg(f) \geq \deg(g)$: Legyen f főtagja $a_n x^n$, g főtagja $b_m x^m$ ($n \geq m$). Mivel b_m egység, létezik inverze. Tekintsük a $h(x) = f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$ polinomot. Ezzel a lépéssel kiejtettük f főtagját, így $\deg(h) < \deg(f)$. Az indukciós feltevés miatt h-ra létezik felbontás: $h = q_1 g + r$. Visszahelyettesítve: $f = (a_n b_m^{-1} x^{n-m} + q_1)g + r$. Ez megadja a kívánt q és r polinomokat.
- **Unicitás (Egyértelműség):**
  - Tegyük fel, hogy két előállítás létezik: $f = qg + r = q'g + r'$.
  - Átrendezve: $(q - q')g = r' - r$.
  - Vizsgáljuk a fokszámokat!
    - A jobb oldal foka: $\deg(r' - r) < \deg(g)$ (mivel r és r' foka is kisebb g-énél).
    - A bal oldal foka: Ha $q \neq q'$, akkor $\deg((q - q')g) = \deg(q - q') + \deg(g) \geq \deg(g)$ (mivel R nullosztómentes).
  - Ez ellentmondás, kivéve, ha $q - q' = 0$, azaz $q = q'$. Ekkor pedig $r' - r = 0 \Rightarrow r = r'$.

2. Gyöktényező és leválasztása

Gyöktényező fogalma: Ha c gyöke az f polinomnak ($f(c) = 0$), akkor az $(x - c)$ elsőfokú polinomot az f **gyöktényezőjének** nevezzük.

Gyöktényező leválasztására vonatkozó tétel (Bézout-tétel polinomokra):

Az $c \in R$ elem pontosan akkor gyöke az $f \in R[x]$ polinomnak, ha $(x - c)$ osztója $f(x)$-nek.

$$f(c) = 0 \iff (x - c) \mid f(x)$$

Bizonyítás:

- Osszuk el maradékosan $f(x)$-et $(x-c)$-vel. Mivel $(x-c)$ főegyüttható ja 1 (egység), az osztás elvégezhető.

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

  Ahol $\deg(r) < \deg(x-c) = 1$, tehát r egy konstans polinom ($r \in R$).
- Helyettesítsünk x helyére c-t:

$$f(c) = q(c)(c-c) + r = q(c) \cdot 0 + r = r$$

  Tehát a maradék pontosan a helyettesítési érték ($f(c)$).
- **Következtetés:**
  - Ha $f(c) = 0$, akkor $r = 0$, tehát $f(x) = q(x)(x-c)$, azaz $(x-c) \mid f(x)$.
  - Ha $(x-c) \mid f(x)$, akkor a maradék $r = 0$, így $f(c) = 0$.

3. Gyökök száma

Tétel: Egy nullától különböző, n-edfokú polinomnak egy integritási tartomány felett **legfeljebb** n darab gyöke lehet.

Bizonyítás (Indukcióval):

- $n = 0$ esetén (nemnulla konstans) 0 gyök van. Állítás igaz.
- $n = 1$ esetén ($ax + b$) legfeljebb 1 gyök van ($-a^{-1}b$, ha létezik inverz).
- Tegyük fel, hogy $n-1$-re igaz. Legyen $\deg(f) = n$.
  - Ha f-nek nincs gyöke, akkor $0 \leq n$, igaz.
  - Ha van egy c gyöke, akkor leválaszthatjuk a gyöktényezőt: $f(x) = (x-c)g(x)$.
  - Itt $\deg(g) = n-1$.
  - Ha y egy tetszőleges gyöke f-nek ($f(y) = 0$), akkor $(y-c)g(y) = 0$.
  - Mivel R integritási tartomány (nincs nullosztó), ezért vagy $y - c = 0$ (azaz $y = c$), vagy $g(y) = 0$.
  - g-nek az indukciós feltevés miatt legfeljebb $n-1$ gyöke lehet. Ehhez jön még a c, tehát összesen legfeljebb $1 + (n-1) = n$ gyök.

Példa különböző gyökszámra:

Tekintsük az $f(x) = x^2 + 1$ polinomot.

- **Valós számok testén ($\mathbb{R}$):** Nincs gyöke (0 db).
- Komplex számok testén ($\mathbb{C}$): Két gyöke van (i és $-i$). (Megjegyzés: Ha nem integritási tartományt nézünk, pl. $\mathbb{Z}_8$, ott az $x^2 - 1$-nek 4 gyöke is lehet: 1, 3, 5, 7. De a tétel csak integritási tartományokra szólt.)

4. Horner-elrendezés

Ez egy algoritmus a polinom helyettesítési értékének gyors kiszámítására (és a gyöktényezővel való osztásra).

Legyen $f(x) = a_n x^n + \cdots + a_1 x + a_0$. A c helyen vett helyettesítési értéket a következő sorozattal számoljuk:

- $y_0 = a_n$
- $y_1 = y_0 \cdot c + a_{n-1}$
- ...
- $y_k = y_{k-1} \cdot c + a_{n-k}$
- A végeredmény $y_n = f(c)$. Ez kevesebb szorzást igényel, mint a hatványozásos behelyettesítés. A kapott $y_0, \ldots, y_{n-1}$ értékek adják az $(x - c)$-vel való osztás hányadosának együtthatóit.

5. Polinomok egyezése ($n + 1$ helyen)

Tétel: Ha f és g legfeljebb n-edfokú polinomok egy integritási tartomány felett, és $n + 1$ különböző helyen megegyeznek az értékeik, akkor $f = g$ (a polinomok egyenlőek).

Bizonyítás:

- Tekintsük a különbségi polinomot: $h(x) = f(x) - g(x)$.
- Mivel $\deg(f) \leq n$ és $\deg(g) \leq n$, ezért $\deg(h) \leq n$.
- A feltétel szerint $n + 1$ darab c_i helyen $f(c_i) = g(c_i)$, tehát $h(c_i) = 0$.
- Így h-nak $n + 1$ gyöke van.
- A "Gyökök száma" tétel miatt egy nemnulla, legfeljebb n-edfokú polinomnak nem lehet $n + 1$ gyöke.
- Tehát h csak a nullpolinom lehet: $h(x) = 0 \Rightarrow f(x) = g(x)$.

6. Polinomok és Polinomfüggvények (Végtelen R esetén)

Kérdés: Mit mondhatunk a kapcsolatukról?

Válasz: Ha R végtelen integritási tartomány, akkor a polinomok gyűrűje ($R[x]$) és a polinomfüggvények gyűrűje izomorf. Azaz kölcsönösen egyértelmű megfeleltetés van közöttük: különböző polinomokhoz különböző függvények tartoznak.

Bizonyítás:

- Azt kell belátni, hogy ha két polinomhoz tartozó függvény ugyanaz ($\hat{f} = \hat{g}$), akkor a polinomok is egyenlőek ($f = g$).
- Ha $\hat{f}(c) = \hat{g}(c)$ minden $c \in R$-re, akkor a $h = f - g$ polinomnak minden $c \in R$ elem gyöke.
- Mivel R végtelen, így h-nak végtelen sok gyöke van.
- Egy nemnulla polinomnak csak véges sok gyöke lehet. Tehát h a nullpolinom.
- Így $f - g = 0 \Rightarrow f = g$.

7. Oszthatóság és LNKO polinomok körében

Oszthatóság: Az f polinom osztja g-t ($f \mid g$), ha létezik olyan $h \in R[x]$, hogy $g = f \cdot h$.

Kitüntetett közös osztó:

Két polinom (f, g) legnagyobb közös osztója (LNKO) az a d polinom, amelyre:

1. $d \mid f$ és $d \mid g$ (közös osztó).
2. Ha k egy tetszőleges közös osztó, akkor $k \mid d$.
3. **"Kitüntetett":** A d főegyütthatója 1 (főpolinom). Ez teszi egyértelművé, mivel az egységszorzótól eltekintve az LNKO egyértelmű.

Euklideszi algoritmus alkalmazhatósága:

- **Milyen polinomokra:** Test feletti polinomokra (pl. $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{Z}_p[x]$) biztosan alkalmazható bármely két polinomra (ahol az osztó nem 0).
- **Indoklás:** Az euklideszi algoritmus a maradékos osztáson alapul. A maradékos osztás tételében feltétel volt, hogy az osztó főegyütthatója **egység** (invertálható) legyen. Testben minden nemnulla elem egység, így a maradékos osztás (és az algoritmus) mindig elvégezhető. (Gyűrűben, pl. $\mathbb{Z}[x]$-ben nem mindig, mert pl. $2x$-szel nem tudunk maradékosan osztani, ha a 2-nek nincs inverze).

8. Bővített Euklideszi algoritmus

Ez az eljárás megadja két polinom LNKO-ját ($d(x)$), és előállítja azt a két polinom lineáris kombinációjaként:

$$d(x) = f(x)u(x) + g(x)v(x)$$

Működése és Helyessége:

Az algoritmus ugyanazt a sorozatot képezi, mint a számoknál ($r_{n-2} = q_n r_{n-1} + r_n$), polinomokkal végezve a maradékos osztást.

Helyesség bizonyítása:

- Jelölje (f, g) a két polinom közös osztóinak halmazát.
- Mivel $f = qg + r$, ezért ha egy d osztja f-et és g-t, akkor osztja $r = f - qg$-t is. Fordítva: ha osztja g-t és r-t, osztja f-et is.
- Tehát az LNKO a lépések során nem változik: $(r_{i-2}, r_{i-1}) = (r_{i-1}, r_i)$.
- Az utolsó nemnulla maradék az LNKO.
- A lineáris kombinációs előállítás ($u(x), v(x)$ keresése) visszafelé helyettesítéssel történik, ami a fenti egyenletek átrendezéséből ($r = f - qg$) matematikailag következik.

4. Tétel: Derivált, Interpoláció, Véges testek, Racionális gyökteszt

1. Polinomok algebrai deriváltja

Definíció:

Legyen R gyűrű, és $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Az f polinom algebrai deriváltjának nevezzük az

$$f'(x) = \sum_{i=1}^{n} i \cdot a_i x^{i-1}$$

polinomot. (Tehát formálisan: a_0 eltűnik, $a_1 x$-ből a_1 lesz, $a_2 x^2$-ből $2a_2 x$, stb., ahogy az analízisben megszoktuk, de itt határérték nélkül).

Tulajdonságok:

Minden $f, g \in R[x]$ és $c \in R$ esetén:

1. $(f+g)' = f' + g'$ (Additivitás)
2. $(c \cdot f)' = c \cdot f'$ (Homogenitás)
3. $(f \cdot g)' = f' \cdot g + f \cdot g'$ (Szorzatszabály / Leibniz-szabály)

Elsőfokú főpolinom n-edik hatványának deriváltja:

Állítás: Legyen $(x-c)$ egy elsőfokú főpolinom. Ekkor $((x-c)^n)' = n(x-c)^{n-1}$.

Bizonyítás (Indukcióval):

- $n = 1$ esetén: $(x-c)' = 1$, és $1 \cdot (x-c)^0 = 1$. Igaz.
- Tegyük fel, hogy $n-1$-re igaz. Vizsgáljuk n-re: $((x-c)^n)' = ((x-c)^{n-1} \cdot (x-c))'$ A szorzatszabályt alkalmazva: $= ((x-c)^{n-1})' \cdot (x-c) + (x-c)^{n-1} \cdot (x-c)'$ Az indukciós feltevés és $(x-c)' = 1$ miatt: $= ((n-1)(x-c)^{n-2}) \cdot (x-c) + (x-c)^{n-1} \cdot 1$
  $= (n-1)(x-c)^{n-1} + (x-c)^{n-1} = (n-1+1)(x-c)^{n-1} = n(x-c)^{n-1}$.

2. Többszörös gyök és a derivált kapcsolata

Definíció (Többszörös gyök, Multiplicitás):

A $c \in R$ elemet az $f \in R[x]$ polinom k-szoros gyökének nevezzük (vagy a gyök multiplicitása k), ha

$$(x-c)^k \mid f(x), \quad \text{de} \quad (x-c)^{k+1} \nmid f(x).$$

Kapcsolat a deriválttal (Tétel):

Legyen R nullosztómentes gyűrű. Ha c az f polinom k-szoros gyöke ($k \geq 1$), és R karakterisztikája nem osztója k-nak, akkor c a deriváltnak (f') pontosan $(k-1)$-szeres gyöke.

Bizonyítás:

- Írjuk fel f-et a k-szoros gyök segítségével: $f(x) = (x-c)^k \cdot g(x)$, ahol $g(c) \neq 0$ (mivel a gyök pontosan k-szoros).
- Deriváljuk f-et a szorzatszabály szerint: $f'(x) = ((x-c)^k)' \cdot g(x) + (x-c)^k \cdot g'(x)$
  $= k(x-c)^{k-1}g(x) + (x-c)^k g'(x)$ Emeljük ki $(x-c)^{k-1}$-et:
  $f'(x) = (x-c)^{k-1} \cdot \underbrace{[k \cdot g(x) + (x-c)g'(x)]}_{h(x)}$
- Látható, hogy $(x-c)^{k-1} \mid f'(x)$.
- Hogy pontosan $k-1$ a multiplicitás, be kell látni, hogy $h(c) \neq 0$.
  $h(c) = k \cdot g(c) + (c-c)g'(c) = k \cdot g(c)$.
- Mivel R nullosztómentes, $g(c) \neq 0$ és a feltétel szerint k nem 0 a gyűrűben (karakterisztika nem osztja), ezért $h(c) \neq 0$. Tehát f'-nek c pontosan $k-1$-szeres gyöke.

Példa, amikor a gyök multiplicitása nem csökken (vagy nő):

Ez csak akkor fordulhat elő, ha a gyűrű karakterisztikája osztja a multiplicitást (k-t).

- **Példa:** Legyen $R = \mathbb{Z}_p$ (ahol p prím), és $f(x) = x^p$.
- A gyök $c = 0$, multiplicitása p (mivel $x^p = (x-0)^p$).
- A derivált: $f'(x) = p \cdot x^{p-1}$. Mivel $\mathbb{Z}_p$-ben $p \equiv 0$, ezért $f'(x) = 0$ (a nullpolinom).
- A nullpolinomnak a 0 "végtelen sokszoros" gyöke (bármilyen hatvánnyal osztható), tehát a multiplicitás nem $p-1$ lett.

3. Lagrange-interpoláció

Feladat: Adott n darab különböző alappont ($x_1, \ldots, x_n$) és hozzájuk tartozó értékek ($y_1, \ldots, y_n$). Keresünk egy legfeljebb $n-1$-edfokú polinomot, amelyre $f(x_i) = y_i$.

Lagrange-alappolinom (l_i):

Olyan polinom, amely az x_i helyen 1-et, az összes többi x_j helyen 0-t vesz fel.

$$l_i(x) = \prod_{j=1, j \neq i}^{n} \frac{x - x_j}{x_i - x_j} = \frac{(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_n)}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)}$$

Ennek foka $n-1$.

Lagrange-interpolációs polinom:

$$L(x) = \sum_{i=1}^{n} y_i \cdot l_i(x)$$

Helyesség bizonyítása:

- Létezés: Behelyettesítve egy tetszőleges x_k alappontot: $L(x_k) = \sum y_i l_i(x_k)$. Mivel $l_i(x_k) = 1$, ha $i = k$, és 0, ha $i \neq k$, az összegből csak az $y_k \cdot 1$ marad. Tehát $L(x_k) = y_k$. A fokszám legfeljebb $n-1$, mert $n-1$-edfokú polinomok összege.
- Egyértelműség: Tegyük fel, hogy f és g két ilyen polinom. Ekkor $h = f - g$ foka legfeljebb $n-1$, és mind az n helyen 0 az értéke. A polinomok gyökszámára vonatkozó tétel miatt egy nemnulla, legfeljebb $n-1$-edfokú polinomnak nem lehet n gyöke. Tehát h a nullpolinom, azaz $f = g$.

Titokmegosztás (Shamir-féle):

- **Cél:** Egy S titkot osszunk szét n résztvevő között úgy, hogy bármely k résztvevő összeállva vissza tudja fejteni, de $k-1$ semmit ne tudjon meg róla.
- **Módszer:**
  1. Választunk egy p prímet ($p > S, n$).
  2. Készítünk egy $k-1$-edfokú véletlen $f(x)$ polinomot $\mathbb{Z}_p$ felett úgy, hogy a konstans tagja a titok ($f(0) = S$), a többi együttható véletlen.
  3. A résztvevőknek kiosztjuk az $(i, f(i))$ párokat ($i = 1 \dots n$).
- **Visszafejtés:** Ha k ember összejön, van k darab pontjuk. Erre a k pontra egyértelműen illeszthető egy legfeljebb $k-1$-edfokú polinom (Lagrange-interpolációval). Ennek a polinomnak a konstans tagja ($f(0)$) a titok.
- **Biztonság:** $k-1$ pont esetén a konstans tag bármi lehet (bármilyen S értékhez létezik polinom, ami illeszkedik a pontokra), így kevesebb ember semmit nem tud a titokról.

4. Véges testek

Elemszám:

Bármely véges test elemszáma egy prímszám pozitív egész kitevős hatványa ($q = p^n$).

- Itt p a test karakterisztikája.
- Minden p prímre és $n \geq 1$-re létezik p^n elemű test, és ez izomorfiától eltekintve egyértelmű. Jelölése: $\mathbb{F}_{p^n}$ vagy $GF(p^n)$.

Konstrukció (p^n elemű test):

1. Vegyük a $\mathbb{Z}_p$ testet (a modulo p maradékosztályok).
2. Tekintsük a $\mathbb{Z}_p[x]$ polinomgyűrűt.
3. Válasszunk egy n-edfokú **irreducibilis** (felbonthatatlan) $m(x)$ polinomot $\mathbb{Z}_p[x]$-ben.
4. A véges test a $\mathbb{Z}_p[x]$ gyűrűnek az $m(x)$ polinom által generált ideál szerinti faktorgyűrűje lesz:

   $$F = \mathbb{Z}_p[x] / (m(x))$$

   Ez a test azon polinomokból áll, melyek foka kisebb mint n. Számuk p^n. A műveletek (összeadás, szorzás) modulo $m(x)$ értendők.

5. Racionális gyökteszt (Schönemann-Eisenstein kritériumhoz kapcsolódó, de ez a "Racionális gyöktétel")

Tétel:

Legyen $f(x) = a_n x^n + \cdots + a_1 x + a_0$ egy egész együtthatós polinom ($a_i \in \mathbb{Z}$). Ha a p/q (ahol $(p, q) = 1$) racionális szám gyöke f-nek, akkor:

1. $p \mid a_0$ (a számláló osztja a konstans tagot)
2. $q \mid a_n$ (a nevező osztja a főegyütthatót).

Bizonyítás:

- Mivel p/q gyök: $a_n(p/q)^n + \cdots + a_1(p/q) + a_0 = 0$.
- Szorozzunk be q^n-nel:

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

- $p \mid a_0$ bizonyítása: Rendezzük az egyenletet: $p(a_n p^{n-1} + \cdots + a_1 q^{n-1}) = -a_0 q^n$. A bal oldal osztható p-vel, így a jobb oldal is: $p \mid a_0 q^n$. Mivel $(p, q) = 1$, ezért $(p, q^n) = 1$ is igaz, tehát p-nek osztania kell a_0-t.
- $q \mid a_n$ bizonyítása: Hasonlóan, emeljük ki q-t a tagokból (kivéve az elsőt): $a_n p^n = -q(a_{n-1} p^{n-1} + \cdots + a_0 q^{n-1})$. A jobb oldal osztható q-val $\Rightarrow q \mid a_n p^n$. Mivel $(q, p) = 1$, ezért $q \mid a_n$.

Alkalmazás: $\sqrt{2} \notin \mathbb{Q}$ bizonyítása:

- Tekintsük az $f(x) = x^2 - 2$ polinomot. Ennek gyökei $\pm\sqrt{2}$.
- Mivel f egész együtthatós, alkalmazhatjuk a racionális gyöktesztet.
- $a_n = 1$, $a_0 = -2$.
- Lehetséges racionális gyökök (p/q):
  - $q \mid 1 \Rightarrow q = 1$.
  - $p \mid -2 \Rightarrow p \in \{1, -1, 2, -2\}$.
- A lehetséges racionális gyökök: $\pm 1, \pm 2$.
- Helyettesítsünk be:
  - $1^2 - 2 \neq 0$
  - $(-1)^2 - 2 \neq 0$
  - $2^2 - 2 \neq 0$
  - $(-2)^2 - 2 \neq 0$
- Mivel egyik sem gyök, a polinomnak nincs racionális gyöke. Tehát $\sqrt{2}$ irracionális.

5. Tétel: Polinomok felbonthatósága

1. Egységek jellemzése test fölötti polinomgyűrűben

Állítás: Legyen F test. Az $F[x]$ polinomgyűrűben az egységek (invertálható elemek) pontosan a nullától különböző konstans polinomok (azaz a 0-adfokú polinomok).

Bizonyítás:

- Legyen $f, g \in F[x]$, és $f \cdot g = 1$ (az egységelem).
- A fokszámtétel szerint (mivel test nullosztómentes):

$$\deg(f \cdot g) = \deg(f) + \deg(g) = \deg(1) = 0$$

- Mivel a fokszámok nemnegatív egészek, $\deg(f) + \deg(g) = 0$ csak úgy lehetséges, ha $\deg(f) = 0$ és $\deg(g) = 0$.
- Tehát f nullától különböző konstans polinom.

2. Elsőfokú polinomok és gyökök kapcsolata (Testben)

Állítás: Test fölött minden elsőfokú polinomnak **pontosan egy** gyöke van.

Bizonyítás:

- Legyen $f(x) = ax + b$, ahol $a \neq 0$.
- A gyököt keressük: $ax + b = 0$.
- Mivel testben vagyunk és $a \neq 0$, létezik a^{-1} inverz.
- Rendezzük az egyenletet: $ax = -b \implies x = -ba^{-1}$.
- Ez az elem egyértelműen létezik a testben.

Példa olyan elsőfokú polinomra, amelynek nincs gyöke:

- Ez csak akkor lehetséges, ha **nem test** fölött vagyunk (hanem "csak" gyűrűben).
- **Példa:** $\mathbb{Z}[x]$-ben a $2x + 1$ polinomnak nincs gyöke az egész számok körében (a gyöke $-1/2$ lenne, ami nem egész).
- Vagy $\mathbb{Z}_4[x]$-ben a $2x + 1$-nek nincs gyöke (behelyettesítve: $0 \to 1, 1 \to 3, 2 \to 1, 3 \to 3$).

3. Lineáris (elsőfokú) polinomok felbonthatósága

Állítás: Test fölötti polinomgyűrűben minden elsőfokú polinom felbonthatatlan (irreducibilis).

Bizonyítás:

- Tegyük fel, hogy $f(x) = g(x)h(x)$, ahol $\deg(f) = 1$.
- A fokszámtétel miatt: $1 = \deg(g) + \deg(h)$.
- Mivel a fokszámok nemnegatív egészek, ez csak úgy lehet, ha az egyik fokszám 1, a másik 0.

- A 0-adfokú polinomok test fölött egységek. Tehát az egyik tényező szükségképpen egység.
- Mivel f-nek csak triviális felbontása van (egyik tényező egység), ezért felbonthatatlan.

4. Másod- és harmadfokú polinomok felbonthatósága

Tétel: Egy test fölötti másod- vagy harmadfokú polinom pontosan akkor felbontható (reducibilis), ha van gyöke az adott testben.

(Következésképpen: Pontosan akkor irreducibilis, ha nincs gyöke).

Bizonyítás:

- $\Rightarrow$ (Ha van gyöke, akkor felbontható): Ha c gyök, akkor a gyöktényező kiemelhető: $f(x) = (x - c)g(x)$. Mivel f foka legalább 2, ezért g foka legalább 1. Így sem $(x - c)$, sem $g(x)$ nem egység (fokuk > 0), tehát a felbontás valódi.
- $\Leftarrow$ (Ha felbontható, akkor van gyöke): Tegyük fel, hogy $f = g \cdot h$ valódi felbontás. Ekkor $\deg(g) \geq 1$ és $\deg(h) \geq 1$. Mivel $\deg(f) = \deg(g) + \deg(h)$ értéke 2 vagy 3, ez csak úgy lehetséges, ha legalább az egyik tényező elsőfokú. (Pl. $2 = 1 + 1$ vagy $3 = 1 + 2$). Ha van elsőfokú tényező (pl. g), akkor annak (az előző pont miatt) van gyöke a testben. Ez a gyök egyben f-nek is gyöke.

(Megjegyzés: Ez a tétel 4-ed foktól kezdve nem igaz, pl. $(x^2 + 1)(x^2 + 1)$ *felbontható* $\mathbb{R}$*-ben, de nincs valós gyöke.)*

5. Felbonthatatlan polinomok $\mathbb{C}$ és $\mathbb{R}$ fölött

- $\mathbb{C}$ (Komplex számok) fölött: Csak az elsőfokú polinomok felbonthatatlanok. (Indoklás: Az algebra alaptétele miatt minden legalább elsőfokú polinomnak van gyöke, így a másod- vagy magasabb fokúak gyöktényezők leválasztásával tovább bonthatók).
- $\mathbb{R}$ (Valós számok) fölött: A felbonthatatlan polinomok lehetnek:
  1. **Elsőfokúak.**
  2. Másodfokúak negatív diszkriminánssal ($D < 0$).

     (Minden másodfokúnál magasabb fokú polinom felbontható valós együtthatós tényezőkre).

6. Primitív polinom és Gauss-lemma

Primitív polinom: Egy egész együtthatós polinom ($f \in \mathbb{Z}[x]$) primitív, ha együtthatóinak legnagyobb közös osztója 1.

- $f(x) = a_n x^n + \cdots + a_0$, primitív, ha $(a_n, \ldots, a_0) = 1$.

Gauss-lemma:

Két primitív polinom szorzata is primitív.

Bizonyítás (Indirekt):

- Legyen $f, g \in \mathbb{Z}[x]$ primitív, és tegyük fel, hogy $h = f \cdot g$ nem primitív.
- Ekkor h együtthatóinak lnko-ja $d > 1$, tehát van egy p prímosztója, ami h minden együtthatóját osztja.
- Tekintsük a polinomokat modulo p (az együtthatókat $\mathbb{Z}_p$ testben nézzük). Mivel p osztja h minden együtthatóját, ezért $\overline{h} = \overline{0}$ (a nullpolinom) $\mathbb{Z}_p[x]$-ben.
- Tehát $\overline{f} \cdot \overline{g} = \overline{0}$.
- Mivel f primitív, nem minden együtthatója osztható p-vel, így $\overline{f} \neq \overline{0}$. Hasonlóan $\overline{g} \neq \overline{0}$.
- $\mathbb{Z}_p$ test, így $\mathbb{Z}_p[x]$ integritási tartomány (nincs nullosztó). Két nemnulla polinom szorzata nem lehet nulla.
- Ellentmondás.

7. Polinomok előállítása primitív polinomokkal

- Egész együtthatós ($f \in \mathbb{Z}[x]$): Minden nemnulla f egyértelműen felírható $f = c(f) \cdot f^*$ alakban, ahol:
  - $c(f)$ egy pozitív egész szám (az együtthatók lnko-ja, a polinom *tartalma*),
  - f^* egy primitív polinom.
- Racionális együtthatós ($f \in \mathbb{Q}[x]$): Minden nemnulla f egyértelműen felírható $f = r \cdot f^*$ alakban, ahol:
  - r egy pozitív racionális szám,
  - f^* egy primitív egész együtthatós polinom.

8. Gauss-tétel (Reláció $\mathbb{Z}[x]$ és $\mathbb{Q}[x]$ között)

Tétel: Egy legalább elsőfokú egész együtthatós polinom pontosan akkor felbonthatatlan $\mathbb{Z}[x]$ -ben, ha felbonthatatlan $\mathbb{Q}[x]$-ben is.

(Másképp: Ha felbontható racionálisok felett, akkor felbontható egészek felett is).

Bizonyítás:

- Az egyik irány triviális: Ha f felbontható $\mathbb{Z}$-ben ($f = gh$), akkor ez a felbontás jó $\mathbb{Q}$-ban is.
- **Visszafelé:** Tegyük fel, hogy $f \in \mathbb{Z}[x]$ felbontható $\mathbb{Q}$ felett: $f = g \cdot h$, ahol $g, h \in \mathbb{Q}[x]$.
- Írjuk fel g és h polinomokat a primitív alakjukkal: $g = r_g \cdot g^*$ és $h = r_h \cdot h^*$ (ahol $r_g, r_h \in \mathbb{Q}$, g^*, h^* primitívek).
- Ekkor $f = (r_g r_h) \cdot g^* h^*$.
- Mivel f egész együtthatós, írjuk fel az ő primitív alakját is: $f = c(f) \cdot f^*$.
- A Gauss-lemma miatt $g^* h^*$ is primitív polinom.
- A racionális együtthatós felírás egyértelműsége miatt ($f = r \cdot f^*_{\text{prim}}$) következik, hogy f^* és $g^* h^*$ asszociáltak (itt ± 1 szorzó), és $c(f) = \pm r_g r_h$.
- Tehát $f = (\pm c(f) g^*) \cdot h^*$ egy felbontás $\mathbb{Z}[x]$-ben is (hiszen $c(f)$ egész, g^* egész együtthatós).

9. Schönemann-Eisenstein kritérium

Tétel: Legyen $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám, amelyre:

1. $p \nmid a_n$ (nem osztja a főegyütthatót),
2. $p \mid a_{n-1}, \ldots, a_0$ (osztja az összes többi együtthatót),
3. $p^2 \nmid a_0$ (négyzete nem osztja a konstans tagot),

akkor f felbonthatatlan $\mathbb{Q}[x]$-ben (és így $\mathbb{Z}[x]$-ben is).

Bizonyítás (Indirekt):

- Tegyük fel, hogy f felbontható: $f = g \cdot h$, ahol $g, h \in \mathbb{Z}[x]$ nem konstans polinomok. $g(x) = b_k x^k + \cdots + b_0$ $h(x) = c_m x^m + \cdots + c_0$ ($k + m = n$).
- Vizsgáljuk az egyenlőséget modulo p. Mivel $p \mid a_i$ minden $i < n$-re, ezért $\overline{f}(x) = \overline{a_n} x^n$. Tehát $\overline{g} \cdot \overline{h} = \overline{a_n} x^n$ a $\mathbb{Z}_p[x]$ gyűrűben.
- Mivel $\mathbb{Z}_p[x]$-ben az egyetlen irreducibilis tényező az x (és asszociáltjai), ezért $\overline{g}$ és $\overline{h}$ is csak x hatványa lehet (konstans szorzóval). $\overline{g}(x) \sim x^k \implies \overline{b_0} = 0 \implies p \mid b_0$. $\overline{h}(x) \sim x^m \implies \overline{c_0} = 0 \implies p \mid c_0$.
- A konstans tagok szorzata: $a_0 = b_0 \cdot c_0$.
- Mivel $p \mid b_0$ és $p \mid c_0$, ezért $p^2 \mid b_0 c_0 = a_0$.
- Ez ellentmond a 3. feltételnek ($p^2 \nmid a_0$).

6. Tétel: Entrópia és Forráskódolás – Kidolgozott vizsgaanyag

1. Kommunikáció és Információ alapjai

Kommunikáció vázlatos ábrája:

Adó $\rightarrow$ Csatorna $\rightarrow$ Vevő

(A folyamat: Információforrás $\rightarrow$ Kódoló $\rightarrow$ Csatorna $\rightarrow$ Dekódoló $\rightarrow$ Címzett)

Információ fogalma és mérése:

- **Definíció:** Az információ új ismeret. Shannon nyomán az általa megszüntetett bizonytalansággal mérjük.
- **Mérése:** A bekövetkezési valószínűség reciprokának logaritmusával. (Minél kisebb a valószínűség, annál nagyobb a meglepetés/információ).

Gyakoriság és Relatív gyakoriság:

Tegyük fel, hogy az információforrás N üzenetet bocsát ki.

- **Gyakoriság (k_i):** Hányszor fordult elő az i-edik üzenettípus (x_i).
- **Relatív gyakoriság (p_i):** $p_i = \frac{k_i}{N}$. (Nagy N esetén ez a valószínűség közelítése).

Üzenetek eloszlása:

A $P = \{p_1, p_2, \dots, p_n\}$ szám-n-est az üzenetek eloszlásának nevezzük, ahol $p_i \geq 0$ és $\sum p_i = 1$.

Egyedi információtartalom ($I(x_i)$):

Egy p_i valószínűséggel bekövetkező x_i esemény egyedi információtartalma:

$$I(x_i) = \log \frac{1}{p_i} = -\log p_i$$

(A logaritmus alapja általában 2, ekkor a mértékegység bit).

Átlagos információtartalom (Entrópia):

Az üzenetek egyedi információtartalmának várható értéke.

$$H(P) = \sum_{i=1}^{n} p_i I(x_i) = -\sum_{i=1}^{n} p_i \log p_i$$

(Megállapodás: $0 \cdot \log 0 = 0$).

Eloszlás definíciója:

Egy $P = (p_1, \ldots, p_n)$ szám-n-es eloszlás, ha $p_i \geq 0$ minden i-re, és $\sum_{i=1}^{n} p_i = 1$.

2. Entrópia tulajdonságai

Konvex és szigorúan konvex függvény:

Egy $f : (a, b) \to \mathbb{R}$ függvény (szigorúan) konvex, ha tetszőleges $x_1, x_2 \in (a, b)$ és $0 < \lambda < 1$ esetén:

$$f(\lambda x_1 + (1 - \lambda)x_2) \leq \lambda f(x_1) + (1 - \lambda) f(x_2)$$

(Szigorúan konvex: egyenlőség csak $x_1 = x_2$ esetén).

Geometriailag: a függvénygörbe a húr alatt helyezkedik el.

Jensen-egyenlőtlenség:

Ha f konvex függvény és $p_1, \ldots, p_n$ eloszlás, akkor:

$$f\left(\sum_{i=1}^{n} p_i x_i\right) \leq \sum_{i=1}^{n} p_i f(x_i)$$

(Konkáv függvényre, mint a $\log x$, az egyenlőtlenség iránya megfordul).

Felső korlát az entrópiára:

Állítás: Tetszőleges n elemű P eloszlásra $H(P) \leq \log n$. Egyenlőség pontosan akkor, ha $p_i = 1/n$ (egyenletes eloszlás).

Bizonyítás:

- A $g(x) = x \log x$ függvény szigorúan konvex a $(0, \infty)$ intervallumon.
- Alkalmazzuk a Jensen-egyenlőtlenséget $x_i = p_i$ értékekre és $1/n$ súlyokra:

$$g\left(\sum_{i=1}^{n} \frac{1}{n} p_i\right) \leq \sum_{i=1}^{n} \frac{1}{n} g(p_i)$$

- Bal oldal: $g(1/n) = \frac{1}{n} \log \frac{1}{n} = -\frac{1}{n} \log n$.
- Jobb oldal: $\frac{1}{n} \sum p_i \log p_i = -\frac{1}{n} H(P)$.
- Tehát: $-\frac{1}{n} \log n \leq -\frac{1}{n} H(P) \implies H(P) \leq \log n$.

3. Kódolás alapfogalmai

Kódolás és Kód:

- **Kódolás:** Egy invertálható hozzárendelés, amely az üzenetek halmazának elemeihez véges hosszú jelsorozatokat (kódszavakat) rendel.
- **Kód:** A hozzárendelés értékkészlete (a kódszavak halmaza).

- **Betűnkénti kódolás:** Ha az üzenet elemi egységekből (betűkből) áll, és minden betűhöz egy rögzített kódszót rendelünk. Jele: $\varphi : A \to B^*$.

Kódolási típusok:

- **Felbontható (egyértelműen dekódolható):** Bármely üzenet kódolt alakja egyértelműen visszafejthető az eredeti üzenetté. Formálisan: a kiterjesztett φ^* leképezés injektív.
- **Veszteségmentes:** Ugyanaz, mint a felbontható.
- **Nem felbontható példa:** $A = \{a, b, c\}$, kódok: $0, 1, 01$. A "01" kód jelenthet "a, b"-t vagy "c "-t.

Ábécé, Szó, Halmazok:

- **Ábécé (A):** Véges, nem üres halmaz, elemei a betűk.
- **Szó:** Betűk véges sorozata.
- A^n**:** Az n hosszúságú szavak halmaza.
- A^***:** Az összes véges szó halmaza (beleértve az üres szót: ε).
- A^+**:** Az összes nem üres véges szó halmaza ($A^* \setminus \{\varepsilon\}$).

Leképezés feltétele:

A $\varphi : A \to B^*$ leképezésről feltesszük, hogy injektív (különböző betűknek különböző kódja van) és $\mathrm{rng}(\varphi) \subseteq B^+$ (nincs üres kódszó).

Prefix, Infix, Szuffix:

Legyen $u, v \in A^*$.

- **Prefix (előtag):** u prefixe v-nek ($u \sqsubseteq v$), ha létezik w, hogy $v = uw$.
- **Szuffix (utótag):** u szuffixe v-nek, ha létezik w, hogy $v = wu$.
- **Infix:** u infixe v-nek, ha léteznek w_1, w_2, hogy $v = w_1 u w_2$.
- **Triviális:** Minden szó önmagának és az üres szónak triviális prefixe/szuffixe.
- **Valódi:** Ha $u \sqsubseteq v$ és $u \neq v, u \neq \varepsilon$, akkor valódi prefix.

4. Kódtípusok és kapcsolataik

Prefixmentes kód (Prefix kód):

Egy $K \subseteq B^*$ kód prefixmentes, ha a kód egyik szava sem prefixe egy másik kódszónak. (Ezek azonnal dekódolhatók balról jobbra olvasva).

Egyenletes / Blokk kód:

Minden kódszó hossza azonos ($l_i = L$ minden i-re).

Vesszős kód:

Olyan kód, ahol egy speciális szimbólum (vessző) választja el a kódszavakat, amely a szavak belsejében nem fordul elő. (A gyakorlatban ez prefix kódnak tekinthető, ha a szeparátor a szó végén van).

Kapcsolat a kódok között:

$$\text{Egyenletes} \subset \text{Prefix} \subset \text{Felbontható}$$

$$\text{Vesszős} \subset \text{Prefix}$$

- **Bizonyítás (Vázlat):**
  - *Prefix $\Rightarrow$ Felbontható:* Mivel egyik szó sem kezdete a másiknak, az üzenet elején álló kódszót egyértelműen felismerjük, levágjuk, és folytatjuk.
  - *Egyenletes $\Rightarrow$ Prefix:* Ha minden szó hossza L, és különböznek, akkor egyik sem lehet a másik (ugyanolyan hosszú) valódi prefixe.
- Példa nem prefix, de felbontható kódra: $K = \{0, 01\}$ NEM jó példa, mert nem egyértelműen dekódolható (01 lehet $0, 1$?? Nem, ha 1 nincs a kódban. De $0, 0, 1 \to 001$ és $0, 01 \to 001$. Ez nem felbontható). Helyes példa: $\{0, 10\}$. (Szuffix kód). Üzenet: 10010. Visszafelé olvasva egyértelmű, vagy várva a következő bitre eldönthető. 0 önmagában áll, 1 után kötelező 0.

McMillan-egyenlőtlenség:

- Tétel: Ha létezik q elemű kódábécével $l_1, \ldots, l_n$ szóhosszakkal rendelkező felbontható kód, akkor:

$$\sum_{i=1}^{n} q^{-l_i} \leq 1$$

- **Megfordítása:** Ha az l_i egészekre teljesül az egyenlőtlenség, akkor létezik ilyen szóhosszakkal rendelkező prefix kód (tehát felbontható is).

5. Optimális kódolás

Kód átlagos szóhossza ($L(P, \varphi)$):

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

Ahol p_i az i-edik üzenet valószínűsége, l_i a hozzá tartozó kódszó hossza.

Optimális kód:

Adott P eloszláshoz és q elemű kódábécéhez tartozó felbontható kódok közül az, amelyikre az átlagos szóhossz minimális.

Optimális kód létezése (Bizonyítás):

- A McMillan-egyenlőtlenség miatt $\sum q^{-l_i} \leq 1$. Ez korlátozza a szóhosszakat.

- Belátható, hogy az optimális kódnál $l_i < n$ (vagy hasonló korlát), így csak véges sok szóhossz-kombináció jöhet szóba. Ezek közül kiválasztható a minimális átlagos szóhosszat adó.

Shannon tétele zajmentes csatornára:

Az átlagos szóhosszra alsó korlát az entrópia:

$$L \geq \frac{H(P)}{\log q}$$

- **Bizonyítás:** A $H(P) - L \log q$ mennyiséget vizsgálva (Kullback-Leibler divergenciához hasonló levezetéssel) és a $\ln x \leq x - 1$ egyenlőtlenséget használva adódik, kihasználva a Kraft/McMillan egyenlőtlenséget ($\sum q^{-l_i} \leq 1$).

Shannon-kód:

- Konstrukció: Legyen $l_i = \lceil -\log_q p_i \rceil$. Erre teljesül a Kraft-egyenlőtlenség ($\sum q^{-\lceil -\log_q p_i \rceil} \leq \sum q^{\log_q p_i} = \sum p_i = 1$), tehát létezik ilyen prefix kód.
- Átlagos szóhosszára vonatkozó tétel:

$$\frac{H(P)}{\log q} \leq L < \frac{H(P)}{\log q} + 1$$

- Bizonyítás: A kerekítés miatt: $-\log_q p_i \leq l_i < -\log_q p_i + 1$. Átlagolva ($p_i$-vel súlyozva): $\sum -p_i \log_q p_i \leq \sum p_i l_i < \sum -p_i \log_q p_i + \sum p_i$. $\frac{H(P)}{\log q} \leq L < \frac{H(P)}{\log q} + 1$.

Huffman-kód konstruálása:

Algoritmus optimális prefix kód készítésére:

1. Vegyük a két legkisebb valószínűségű üzenetet.
2. Vonjuk össze őket egy új üzenetté, melynek valószínűsége a kettő összege.
3. Az összevont üzenethez rendeljünk a fában egy közös csúcsot, a két eredetit gyerekként (élcímkék: 0 és 1).
4. Ismételjük, amíg egyetlen üzenet (a gyökér) marad.
5. A kódok a gyökértől a levelekig vezető út címkéi.

Kódfa:

A prefix kódok ábrázolására szolgáló gyökeres fa, ahol a gyökérből induló élek a kódábécé elemeivel vannak címkézve. A levelek felelnek meg a kódszavaknak (üzeneteknek).

7. Tétel: Hibakorlátozó és lineáris kódolás

1. Alapfogalmak és Hibajelzés

Paritásbites kód:

A legegyszerűbb hibajelző kód. Az üzenet bitjeihez hozzáveszünk egy extra bitet (paritásbit), úgy, hogy az 1-esek száma páros (vagy páratlan) legyen.

- Tulajdonsága: Képes jelezni, ha **páratlan** sok hiba történt. (Páros számú hibát nem vesz észre).

Kétdimenziós paritásellenőrzés:

Az üzenet bitjeit mátrixba rendezzük. Minden sor végére és minden oszlop aljára kiszámoljuk a paritásbitet (és a jobb alsó sarokba is).

- Képes javítani bármely 1 bites hibát (a hibás sor és oszlop metszete kijelöli a hibás bitet).
- Képes jelezni a 2 vagy 3 bites hibákat.

Hibajelző kódok fogalma:

- **t-hibajelző kód:** Olyan kód, amely képes észlelni, ha az átvitel során legfeljebb t hiba történt (azaz a vett szó nem kódszó).
- **Pontosan t-hibajelző:** Olyan kód, amely t-hibajelző, de $(t+1)$-hibajelző már nem.

2. Távolság fogalma

Hamming-távolság:

Két azonos hosszúságú szó ($u, v \in A^n$) Hamming-távolsága azon pozíciók száma, ahol a két szó eltér egymástól. Jele: $d(u, v)$.

$$d(u, v) = |\{i : u_i \neq v_i\}|$$

Tulajdonságai (Metrika):

1. **Nemnegativitás:** $d(u, v) \geq 0$, és $d(u, v) = 0 \iff u = v$.
2. **Szimmetria:** $d(u, v) = d(v, u)$.
3. **Háromszög-egyenlőtlenség:** $d(u, v) \leq d(u, w) + d(w, v)$ tetszőleges w-re.

Kód távolsága (d_{min}):

Egy C kód távolsága a kódban szereplő különböző kódszavak közötti Hamming-távolságok minimuma.

$$d(C) = \min\{d(u, v) : u, v \in C, u \neq v\}$$

Minimális távolságú dekódolás:

Olyan dekódolási eljárás, amely a vett y szóhoz azt a $c \in C$ kódszót rendeli, amelyre $d(y, c)$ minimális (azaz a "legközelebbi" kódszót választja). Ez a legvalószínűbb kódszó elve szimmetrikus csatorna esetén.

3. Hibajavítás és Korlátok

Hibajavító kódok fogalma:

- **t-hibajavító kód:** Olyan kód, amely esetén, ha legfeljebb t hiba történik, a minimális távolságú dekódolás visszaadja az eredeti kódszót.
- **Pontosan t-hibajavító:** t-hibajavító, de nem $(t+1)$-hibajavító.

Ismétléses kód:

Olyan kód, ahol az üzenetet egyszerűen n-szer megismételjük. (Pl. $0 \to 000, 1 \to 111$). Ez nagyon redundáns, de növeli a hibajavító képességet.

Kapcsolat a távolság és a hibajelző/javító képesség között:

- **Hibajelzés:** Egy kód pontosan akkor t-hibajelző, ha $d(C) \geq t+1$.
  - *Bizonyítás:* Ha t hiba történik, a vett szó távolsága a küldöttől t. Ha $d(C) > t$, akkor a vett szó nem lehet másik kódszó, tehát észleljük a hibát. Ha viszont $d(C) \leq t$, akkor létezik két kódszó t vagy kisebb távolságra, így az egyik átmehet a másikba t hibával, amit nem veszünk észre.
- **Hibajavítás:** Egy kód pontosan akkor t-hibajavító, ha $d(C) \geq 2t+1$.
  - *Bizonyítás:* A kódszavak köré írt t sugarú "gömböknek" diszjunktnak kell lenniük. Ha $d(C) \geq 2t+1$, akkor bármely két kódszó távolsága legalább $2t+1$. A háromszög-egyenlőtlenség miatt nem létezhet olyan y szó, ami mindkettőtől $\leq t$ távolságra lenne (mert akkor a két kódszó távolsága $\leq 2t$ lenne). Így a dekódolás egyértelmű.

Singleton-korlát:

Állítás: Ha C egy n hosszúságú, q elemű ábécé feletti kód, melynek távolsága d, akkor a kódszavak számára ($|C|$) teljesül:

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

- *Bizonyítás:* Hagyjuk el a kódszavak utolsó $d-1$ koordinátáját. A maradék szavak hossza $n-(d-1) = n-d+1$. Mivel az eredeti kód távolsága d volt, bármely két kódszó legalább d helyen különbözött, így ha $d-1$ helyet elhagyunk, még mindig különbözniük kell legalább 1 helyen. Tehát a "csonkolt" szavak mind különbözőek. Az ilyen hosszúságú szavakból összesen q^{n-d+1} van, tehát ennyi lehet maximum az eredeti kódszavak száma is.

MDS-kód: (Maximum Distance Separable) Olyan kód, amelyre a Singleton-korlát egyenlőséggel teljesül.

Hamming-korlát:

Állítás: Egy n hosszúságú, q elemű ábécé feletti t-hibajavító kód elemszámára teljesül:

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

(Ahol a szumma a t sugarú Hamming-gömb térfogata).

- *Bizonyítás:* A t-hibajavító tulajdonság miatt a kódszavak körüli t sugarú gömbök diszjunktak. Ezen gömbök összesített térfogata ($|C| \times V_{gömb}$) nem haladhatja meg a teljes tér méretét (q^n).

Perfekt kód: Olyan kód, amelyre a Hamming-korlát egyenlőséggel teljesül (a gömbök teljesen kitöltik a teret).

---

4. Lineáris kódok

Lineáris tér és kód:

- F^n **lineáris tér:** Ha F egy test (pl. $\mathbb{Z}_2$), akkor F^n (az n hosszú vektorok halmaza) vektorteret alkot a komponensenkénti összeadásra és skalárral szorzásra nézve.
- **Lineáris kód:** Az F^n vektortér egy C altere lineáris kód.
- **Paraméterek ($[n, k, d]$):**
  - n: kódhossz (vektorok dimenziója).
  - k: dimenzió (az altér dimenziója, azaz az információs bitek száma). A kódszavak száma q^k.
  - d: minimális távolság.

Singleton-korlát lineáris kódra:

Mivel $|C| = q^k$, a korlát ($q^k \leq q^{n-d+1}$) logaritmusát véve:

$$k \leq n - d + 1 \quad \text{vagy} \quad k + d \leq n + 1$$

Példa: Ismétléses kód lineáris. Paritásbites kód lineáris.

Súly fogalma:

- **Kódszó súlya ($w(c)$):** A nemnulla koordináták száma a szóban. (Ez megegyezik a $d(c, 0)$ távolsággal).
- **Kód súlya ($w(C)$):** A kódbeli nemnulla szavak súlyának minimuma.

Összefüggés a súly és távolság között:

Lineáris kód esetén a kód távolsága megegyezik a kód súlyával.

$$d(C) = w(C)$$

- *Bizonyítás:*
  - $d(C) = \min_{u \neq v} d(u, v)$.
  - Lineáris kódban $u, v \in C \Rightarrow u - v \in C$.
  - $d(u, v)$ definíció szerint az eltérő helyek száma, ami pont az $u - v$ vektor nemnulla elemeinek száma, azaz $w(u - v)$.
  - Mivel $u - v$ befutja az összes nemnulla kódszót (ha v-t rögzítjük és u fut, vagy fordítva), ezért a minimumuk megegyezik a minimális súllyal.

5. Mátrixok és Dekódolás

Mátrixok:

- **Generátormátrix (G):** Egy $k \times n$-es mátrix, amelynek sorai a kód (mint altér) bázisát alkotják.
  - Kódolás: $c = x \cdot G$ (ahol x a k hosszú üzenetvektor).
- **Ellenőrző mátrix (H):** Egy $(n - k) \times n$-es mátrix, amelyre a kód a mátrix magtere (nulltere).
  - $C = \{c \in F^n : c \cdot H^T = 0\}$.
  - Azaz a kódszavakra teljesül, hogy a H soraival vett skaláris szorzatuk 0.
- **Kapcsolat:** $G \cdot H^T = 0$ (a generátormátrix sorai merőlegesek az ellenőrző mátrix soraira).

Szisztematikus kódolás:

Olyan kódolás, ahol a kódszó első k bitje megegyezik az eredeti üzenettel (üzenetszegmens), a maradék $n - k$ bit pedig az ellenőrző bitek (paritásszegmens).

- **Alakja:**
  - $G = (I_k | P)$, ahol I_k a $k \times k$ egységmátrix, P egy $k \times (n - k)$ mátrix.
  - $H = (-P^T | I_{n-k})$.
- Bizonyítás a kapcsolatra ($GH^T = 0$):
  $G \cdot H^T = (I_k | P) \cdot \binom{-P}{I_{n-k}} = I_k(-P) + P \cdot I_{n-k} = -P + P = 0$.
- **Dekódolás:** Egyszerűen levágjuk a szó végéről a paritásszegmenst (ha nincs hiba).

Ellenőrző mátrix és a távolság kapcsolata:

A kód távolsága (d) az a legkisebb szám, ahány oszlopa H-nak lineárisan összefüggő. (Vagy másképp: $d - 1$ oszlop még bárhogy választva lineárisan független).

- *Bizonyítás:* A $H \cdot c^T = 0$ egyenlet azt jelenti, hogy a c nemnulla koordinátáinak megfelelő H-oszlopok lineáris kombinációja a nullvektor. Ha van w súlyú kódszó, akkor van w

darab lineárisan összefüggő oszlop. A minimális súly (ami $= d$) tehát a legkisebb számú összefüggő oszlophalmaz mérete.

6. Szindrómadekódolás

Fogalmak:

- **Szindróma (s):** A vett y szóra számolt $s = y \cdot H^T$ vektor. Ha $s = 0$, akkor y kódszó (vagy nem észlelt hiba).
- **Hibavektor (e):** $y = c + e$, ahol c a küldött kódszó, e a hiba.
  - A szindróma csak a hibától függ:
    $yH^T = (c + e)H^T = cH^T + eH^T = 0 + eH^T = eH^T$.
- **Mellékosztály:** Az F^n tér C szerinti mellékosztályai ($y + C$). Azonos szindrómájú szavak egy mellékosztályba tartoznak.
- **Mellékosztály-vezető:** A mellékosztály legkisebb súlyú (legkevesebb 1-est tartalmazó) eleme. Ez felel meg a legvalószínűbb hibavektornak.

Szindrómadekódolás menete:

1. Kiszámoljuk a vett y szó szindrómáját: $s = yH^T$.
2. Megkeressük az s szindrómához tartozó mellékosztály-vezetőt (legyen ez e_{vez}). (Ezt előre kiszámolt táblázatból nézzük).
3. A becsült kódszó: $\hat{c} = y - e_{vez}$.

Kapcsolat a minimális távolságú dekódolással:

A szindrómadekódolás ekvivalens a minimális távolságú dekódolással (lineáris kód esetén).

- *Bizonyítás:* A minimális távolságú dekódolás azt a c-t keresi, amire $d(y, c)$ minimális. Mivel $y - c = e$, ez azt jelenti, hogy olyan hibavektort keresünk, aminek a súlya ($w(e)$) minimális, és $y - e$ kódszó. Mivel $y - e \in C \iff y$ és e ugyanabban a mellékosztályban van, ezért a keresett e pont a mellékosztály legkisebb súlyú eleme (a vezető).

Hamming-kód:

Olyan bináris lineáris kód, amelynek ellenőrző mátrixában (H) az oszlopok az összes lehetséges nemnulla r bites vektort tartalmazzák.

- Paraméterek: $n = 2^r - 1$, $n - k = r$ (tehát $k = 2^r - 1 - r$).
- Távolsága: 3 (mert bármely 2 oszlop független, de van 3 összefüggő). Így 1 hibát javít.
- Példa ($r = 3$): $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ (Az oszlopok az 1-től 7-ig tartó számok binárisan).