Bácsó Sándor

Diszkrét Matematika II.

mobiDIÁK könyvtár

Bácsó Sándor

Diszkrét Matematika II.

mobiDIÁK könyvtár

SOROZATSZERKESZTŐ

Fazekas István

Bácsó Sándor

Diszkrét Matematika II.

egyetemi jegyzet

mobiDIÁK könyvtár
Debreceni Egyetem Informatikai Intézet

Lektor

Fazekas István

mobiDIÁK könyvtár
Debreceni Egyetem
Informatikai Intézet
4010 Debrecen, Pf. 12
http://mobidiak.unideb.hu

A mű a *A mobiDIÁK önszervező mobil portál* (IKTA, OMFB-00373/2003) és a *GNU Iterátor, a legújabb generációs portál szoftver* (ITEM, 50/2003) projektek keretében készült.

Tartalomjegyzék

1. fejezet
Euklideszi és unitér terek

1. Lineáris, bilineáris és kvadratikus formák

1.1. Definíció. Legyen V egy n-dimenziós vektortér az $\mathbb{R}$ test felett. Az $L : V \to \mathbb{R}$ lineáris leképezést *lineáris formának* vagy *lineáris funkcionál*nak nevezzük.

1.2. Megjegyzés. Az $L : V \to \mathbb{R}$ leképezés lineáris forma, ha

1. additív: $\forall \underline{a}, \underline{b} \in V$ esetén $L(\underline{a} + \underline{b}) = L(\underline{a}) + L(\underline{b})$,
2. homogén: $\forall \underline{a} \in V$ és $\forall \lambda \in \mathbb{R}$ esetén $L(\lambda \underline{a}) = \lambda L(\underline{a})$.

1.3. Megjegyzés. A V vektortéren értelmezett lineáris formák halmaza vektorteret alkot, melyet V duális terének nevezünk. Jele: V^*.

1.4. Megjegyzés. Legyen $L : V \to \mathbb{R}$ lineáris forma, és $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ bázis V-ben. Ekkor egy tetszőleges $\underline{a} \in V$ vektor esetén ha $\underline{a} = \alpha_1 \underline{a}_1 + \cdots + \alpha_n \underline{a}_n$, akkor

$$L(\underline{a}) = L(\alpha_1 \underline{a}_1 + \cdots + \alpha_n \underline{a}_n) = \alpha_1 \underbrace{L(\underline{a}_1)}_{l_1} + \cdots + \alpha_n \underbrace{L(\underline{a}_n)}_{l_n} = \sum_{i=1}^{n} \alpha_i l_i.$$

Ez azt jelenti, hogy elegendő ismernünk L hatását a bázisvektorokon, mert az $l_i \quad (i = 1, \ldots, n)$ számok segítségével L tetszőleges vektoron felvett értékét meg tudjuk határozni.

1.5. Definíció. Az $L : V \to \mathbb{R}$ lineáris forma $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ bázisra vonatkozó *báziselőállítás*ának nevezzük az $l_1, \ldots, l_n$ skalárokat, ahol $l_i = L(\underline{a}_i) \quad (i = 1, \ldots, n)$.

1.6. Következmény. Ha az $L : V \to \mathbb{R}$ lineáris forma (a) bázisra vonatkozó báziselőállítása $l_1, \ldots, l_n$ és $\underline{a} = \alpha_1 \underline{a}_1 + \cdots + \alpha_n \underline{a}_n$, akkor

$$L(\underline{a}) = \sum_{i=1}^{n} \alpha_i l_i.$$

1.7. Tétel. *Legyen az* $L : V \to \mathbb{R}$ *lineáris forma* $(a) = (\underline{a}_1, \dots, \underline{a}_n)$ *bázisra vonatkozó előállítása* $l_1, \dots, l_n$, *a* $(b) = (\underline{b}_1, \dots, \underline{b}_n)$ *bázisra vonatkozó előállítása pedig* $k_1, \dots, k_n$ *és legyen a bázistranszformáció mátrixa* $S : (a) \overset{S}{\to} (b)$. *Ekkor*

$$\text{ha} \quad \underline{l} = \begin{pmatrix} l_1 \\ \vdots \\ l_n \end{pmatrix} \quad \text{és} \quad \underline{k} = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \quad \text{akkor} \quad \underline{k} = S\underline{l}.$$

Bizonyítás. Ha $(a) \overset{S}{\to} (b)$, akkor $\underline{b}_j = \sum_{i=1}^{n} s_{ij}\underline{a}_i$, így

$$k_j = L(\underline{b}_j) = L\left(\sum_{i=1}^{n} s_{ij}\underline{a}_i\right) = \sum_{i=1}^{n} s_{ij} \underbrace{L(\underline{a}_i)}_{l_i} = \sum_{i=1}^{n} s_{ij} l_i = (S\underline{l})_j.$$

□

1.8. Következmény. Ha megadunk egy $l_1, \dots, l_n$ szám n-est, akkor egy és csak egy olyan lineáris forma létezik, amelynek az (a) rögzített bázisra vonatkozó báziselőállítása $l_1, \dots, l_n$.

1.9. Tétel. *A* V *n-dimenziós vektortér* V^* *duális vektortere szintén n-dimenziós, és egy bázisát adják azok az* $M_i : V \to \mathbb{R}$ $(i = 1, \dots, n)$ *lineáris formák, amelyeknek az* $(a) = (\underline{a}_1, \dots, \underline{a}_n)$ *bázisra vonatkozó báziselőállításuk:* $M_i(\underline{a}_j) = \delta_{ij}$ $(j = 1, \dots, n)$.

Bizonyítás. 1. Lineárisan függetlenek: Ha

$$\alpha_1 M_1 + \dots + \alpha_n M_n = \mathcal{O},$$

ahol $\mathcal{O} : V \to \mathbb{R}$, $\mathcal{O}(\underline{a}) = 0$ az azonosan nulla lineáris forma, akkor

$$\alpha_1 \underbrace{M_1(\underline{a}_j)}_{0} + \dots + \alpha_j \underbrace{M_j(\underline{a}_j)}_{1} + \dots + \alpha_n \underbrace{M_n(\underline{a}_j)}_{0} = \mathcal{O}(\underline{a}_j) = 0,$$

tehát $\alpha_j = 0$ $j = (1, \dots, n)$.

2. Generátorrendszer: Megmutatjuk, hogy egy tetszőleges $L : V \to \mathbb{R}$ lineáris forma előáll az $M_1, \dots, M_n$ lineáris formák lineáris kombinációjaként. Legyen $\underline{a} \in V$ egy tetszőleges vektor, melynek felírása az (a) bázisban: $\underline{a} = \lambda_1\underline{a}_1 + \dots + \lambda_n\underline{a}_n$. Ekkor

$$\begin{aligned} M_i(\underline{a}) &= M_i(\lambda_1\underline{a}_1 + \dots + \lambda_n\underline{a}_n) \\ &= \lambda_1 \underbrace{M_i(\underline{a}_1)}_{0} + \dots + \lambda_i \underbrace{M_i(\underline{a}_i)}_{1} + \dots + \lambda_n \underbrace{M_i(\underline{a}_n)}_{0} = \lambda_i, \end{aligned}$$

és

$$\begin{aligned} L(\underline{a}) &= L(\lambda_1\underline{a}_1 + \cdots + \lambda_n\underline{a}_n) \\ &= \underbrace{\lambda_1}_{M_1(\underline{a})}\underbrace{L(\underline{a}_1)}_{l_1} + \cdots + \underbrace{\lambda_n}_{M_n(\underline{a})}\underbrace{L(\underline{a}_n)}_{l_n} = \sum_{i=1}^{n} l_i M_i(\underline{a}), \end{aligned}$$

tehát $L = \sum_{i=1}^{n} l_i M_i$.

□

1.10. Definíció. A $B : V \times V \to \mathbb{R}$ leképezést *bilineáris formának* nevezzük, ha mindkét változójában lineáris: $\forall \underline{x}, \underline{y}, \underline{z} \in V$ és $\forall \alpha, \beta \in \mathbb{R}$ esetén

1. $B(\alpha\underline{x} + \beta\underline{y}, \underline{z}) = \alpha B(\underline{x}, \underline{z}) + \beta B(\underline{y}, \underline{z})$,
2. $B(\underline{x}, \alpha\underline{y} + \beta\underline{z}) = \alpha B(\underline{x}, \underline{y}) + \beta B(\underline{x}, \underline{z})$.

1.11. Megjegyzés. A V vektortéren legyen $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ egy bázis, és $B : V \times V \to \mathbb{R}$ egy bilineáris forma. Ha az $\underline{x} \in V$ vektor felírása az (a) bázisban $\underline{x} = x_1\underline{a}_1 + \cdots + x_n\underline{a}_n$, az $\underline{y} \in V$ vektoré pedig $\underline{y} = y_1\underline{a}_1 + \cdots + y_n\underline{a}_n$, akkor

$$B(\underline{x}, \underline{y}) = B\left(\sum_{i=1}^{n} x_i\underline{a}_i, \sum_{j=1}^{n} y_j\underline{a}_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \underbrace{B(\underline{a}_i, \underline{a}_j)}_{c_{ij}}.$$

Tehát elegendő ismernünk a bilineáris forma hatását a bázisvektor párokon, mert a $c_{ij} = B(\underline{a}_i, \underline{a}_j) \in \mathbb{R}$ számok segítségével a B tetszőleges vektorpáron felvett értékét meghatározhatjuk.

1.12. Definíció. A $B : V \times V \to \mathbb{R}$ *bilineáris forma mátrixa* az $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ bázisra vonatkozóan a $C = (c_{ij})$ mátrix, ahol $c_{ij} = B(\underline{a}_i, \underline{a}_j)$.

1.13. Tétel. *Legyen a $B : V \times V \to \mathbb{R}$ bilineáris forma mátrixa az $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ bázisra vonatkozóan C és az $\underline{x}, \underline{y} \in V$ vektorok lineáris kombinációként való előállítása az (a) bázisban $\underline{x} = x_1\underline{a}_1 + \cdots + x_n\underline{a}_n$ illetve $\underline{y} = y_1\underline{a}_1 + \cdots + y_n\underline{a}_n$. Ha*

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{és} \quad Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

akkor

$$B(\underline{x}, \underline{y}) = X^T C Y.$$

Bizonyítás. Az 1.11. megjegyzés szerint

$$B(\underline{x},\underline{y}) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j c_{ij} = (x_1,\dots,x_n)\begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = X^T C Y.$$

□

1.14. Megjegyzés. Egy V n-dimenziós vektortéren értelmezett összes bilineáris formák halmaza vektorteret alkot az alábbi összeadásra és skalárszorzásra nézve:

1. $(B_1 + B_2)(\underline{x},\underline{y}) \doteq B_1(\underline{x},\underline{y}) + B_2(\underline{x},\underline{y})$,
2. $(\lambda B)(\underline{x},\underline{y}) \doteq \lambda B(\underline{x},\underline{y})$.

Mivel minden bilineáris forma azonosítható a mátrixával (minden bilineáris formát egyértelműen meghatároz a bázisvektor párokon felvett értéke, vagyis a c_{ij} számok, és minden $C \in M_{n\times n}$ mátrix esetén az $(\underline{x},\underline{y}) \longmapsto X^T C Y$ leképezés bilineáris forma), így ennek a vektortérnek a dimenziója megegyezik az $(n \times n)$-es mátrixok terének dimenziójával, n^2-tel.

1.15. Tétel. *Legyenek* $(a) = (\underline{a}_1,\dots,\underline{a}_n)$ *és* $(b) = (\underline{b}_1,\dots,\underline{b}_n)$ *bázisok* V*-ben, és a bázistranszformáció mátrixa* $S : (a) \overset{S}{\to} (b)$. *Ha a* $B : V \times V \to \mathbb{R}$ *bilineáris forma mátrixa az* (a) *bázisban* A, *a* (b) *bázisban* C, *akkor*

$$C = S^T A S.$$

Bizonyítás. Ha $(a) \overset{S}{\to} (b)$, akkor $\underline{b}_j = \sum_{i=1}^{n} s_{ij}\underline{a}_i$, így

$$C_{ij} = c_{ij} = B(\underline{b}_i,\underline{b}_j) = B(\sum_{k=1}^{n} s_{ki}\underline{a}_k, \sum_{l=1}^{n} s_{lj}\underline{a}_l) =$$

$$\sum_{k=1}^{n}\sum_{l=1}^{n} s_{ki}s_{lj}\underbrace{B(\underline{a}_k,\underline{a}_l)}_{A_{kl}} = \sum_{k=1}^{n} S^T_{ik}\underbrace{\sum_{l=1}^{n} A_{kl}S_{lj}}_{(AS)_{kj}} = (S^T A S)_{ij}.$$

□

1.16. Következmény. Egy bilineáris forma különböző bázisokban vett mátrixainak rangja megegyezik.

Bizonyítás. Mivel egy bázistarnszformáció S mátrixa és annak transzponáltja S^T is reguláris és egy reguláris mátrixszal való szorzás nem változtat egy mátrix rangján, így $rg(S^T A S) = rgA$. □

1.17. Definíció. Egy bilineáris forma valamely bázisban vett mátrixának a rangját a *bilineáris forma rangjának* nevezzük.

1.18. Definíció. Egy $B : V \times V \to \mathbb{R}$ bilineáris formát *szimmetrikus*nak nevezzük, ha bármely $\underline{x}, \underline{y} \in V$ esetén

$$B(\underline{x}, \underline{y}) = B(\underline{y}, \underline{x}).$$

1.19. Tétel. *Egy $B : V \times V \to \mathbb{R}$ bilineáris forma akkor és csak akkor szimmetrikus, ha tetszőleges bázisban vett mátrixa szimmetrikus.*

Bizonyítás. 1. Belátjuk, hogy ha B mátrixa valamely bázisban szimmetrikus, akkor minden bázisban az. Legyen B mátrixa az (a) bázisban A, a (b) bázisban C és $(a) \xrightarrow{S} (b)$. Ha A szimmetrikus, azaz $A^T = A$, akkor

$$C^T = (S^T A S)^T = S^T \underbrace{A^T}_{A} \underbrace{(S^T)^T}_{S} = S^T A S = C,$$

tehát C is szimmetrikus.

2. Ha B szimmetrikus bilineáris forma és mátrixa az (a) bázisban $C = (c_{ij})$, akkor

$$C_{ij} = c_{ij} = B(\underline{a}_i, \underline{a}_j) = B(\underline{a}_j, \underline{a}_i) = c_{ji} = C_{ji} = C_{ij}^T,$$

tehát $C = C^T$, vagyis C szimmetrikus mátrix.

3. Legyen B mátrixa az (a) bázisban szimmetrikus: $c_{ij} = c_{ji}$. Ekkor tetszőleges $\underline{x}, \underline{y} \in V$ vektorok esetén, ha $\underline{x} = \sum_{i=1}^{n} x_i \underline{a}_i$ és $\underline{y} = \sum_{j=1}^{n} y_j \underline{a}_j$, akkor

$$B(\underline{x}, \underline{y}) = B\left(\sum_{i=1}^{n} x_i \underline{a}_i, \sum_{j=1}^{n} y_j \underline{a}_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \underbrace{B(\underline{a}_i, \underline{a}_j)}_{c_{ij}=c_{ji}} =$$

$$\sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j B(\underline{a}_j, \underline{a}_i) = B\left(\sum_{j=1}^{n} y_j \underline{a}_j, \sum_{i=1}^{n} x_i \underline{a}_i\right) = B(\underline{y}, \underline{x}),$$

tehát B szimmetrikus.

□

1.20. Megjegyzés. A szimmetrikus bilineáris formák alteret alkotnak a bilineáris formák vektorterében. Ennek az altérnek a dimenziója $\dfrac{n(n+1)}{2}$, mivel a szimmetrikus mátrixok altere is ennyi dimenziós (a főátlóban és a főátló felett álló elemeket tetszőlegesen választhatjuk).

1.21. Definíció. A $B : V \times V \to \mathbb{R}$ szimmetrikus bilineáris formából származó *kvadratikus formának* nevezzük a $Q : V \to \mathbb{R}$ leképezést:

$$Q(\underline{x}) = B(\underline{x}, \underline{x}) \quad \forall \underline{x} \in V.$$

A $B(\underline{x}, \underline{y})$ bilineáris formát a $Q(\underline{x})$ kvadratikus forma *poláris formájának* nevezzük.

1.22. Tétel. *A $Q : V \to \mathbb{R}$ kvadratikus forma egyértelműen meghatározza poláris formáját:*

$$B(\underline{x}, \underline{y}) = \frac{1}{2}(Q(\underline{x} + \underline{y}) - Q(\underline{x}) - Q(\underline{y})).$$

Bizonyítás. A $B(\underline{x}, \underline{y})$ szimmetrikus bilineáris forma kifejezhező az alábbi egyenlőségből:

$$Q(\underline{x} + \underline{y}) = B(\underline{x} + \underline{y}, \underline{x} + \underline{y}) =$$
$$\underbrace{B(\underline{x}, \underline{x})}_{Q(\underline{x})} + B(\underline{x}, \underline{y}) + B(\underline{y}, \underline{x}) + \underbrace{B(\underline{y}, \underline{y})}_{Q(\underline{y})} = Q(\underline{x}) + 2B(\underline{x}, \underline{y}) + Q(\underline{y}),$$

tehát

$$B(\underline{x}, \underline{y}) = \frac{1}{2}(Q(\underline{x} + \underline{y}) - Q(\underline{x}) - Q(\underline{y})).$$

□

1.23. Definíció. A $Q(\underline{x})$ *kvadratikus forma mátrixa* alatt poláris formájának mátrixát értjük.

1.24. Következmény. A $B(\underline{x}, \underline{y})$ szimmetrikus bilineáris formából származó $Q(\underline{x})$ kvadratikus forma hatása az $\underline{x} \in V$ vektoron:

$$Q(\underline{x}) = X^T C X,$$

ahol C a kvadratikus forma mátrixa az (a) bázisban, X pedig az $\underline{x}$ vektor (a) bázisbeli koordinátáiból álló oszlopvektor.

1.25. Definíció. A $Q : V \to \mathbb{R}$ kvadratikus formát *kanonikus alak*únak nevezzük, ha valamely bázisban az előállítása

$$Q(\underline{x}) = \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$$

alakú. Ezt a bázist a $Q(\underline{x})$ kvadratikus forma *kanonikus bázis*ának nevezzük.

1.26. Következmény. Egy kvadratikus forma az (a) bázisban pontosan akkor kanonikus alakú, ha mátrixa ebben a bázisban diagonális, mert

$$Q(\underline{x}) = X^T C X = \sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij} x_i x_j$$

akkor lesz kanonikus alakú, ha $i \neq j$ esetén $c_{ij} = 0$.

1.27. Tétel. *Lagrange tétel. A V vektortéren értelmezett tetszőleges $Q(\underline{x})$ kvadratikus forma esetén létezik V-nek olyan bázisa, melyben $Q(\underline{x})$ kanonikus alakú.*

1.28. Következmény. Minden $C \in M_{n\times n}$ szimmetrikus mátrixhoz található olyan $S \in M_{n\times n}$ reguláris mátrix, hogy S^TCS diagonális alakú.

1.29. Következmény. Egy kvadratikus forma különböző bázisokban vett mátrixainak a rangja megegyezik.

1.30. Definíció. Egy *kvadratikus forma rangján* valamely bázisban vett mátrixának rangját értjük.

1.31. Definíció. Egy kvadratikus formát *normál alak*únak nevezünk, ha a kanonikus alakjában csak $+1, -1$ és 0 együtthatók szerepelnek.

1.32. Következmény. Minden kvadratikus formához létezik olyan bázis, amelyben normál alakú.

Bizonyítás. Legyen $(a) = (\underline{a}_1, \dots, \underline{a}_n)$ az a bázis, melyben a $Q(\underline{x})$ kvadratikus forma kanonikus alakú: $Q(\underline{x}) = \lambda_1 x_1^2 + \dots + \lambda_n x_n^2$. Ha tekintjük Q-t a

$$(b) = \left(\frac{\underline{a}_1}{\sqrt{|\lambda_1|}}, \dots, \frac{\underline{a}_n}{\sqrt{|\lambda_n|}} \right)$$

báziban, akkor $Q(\underline{x}) = \sum_{i=1}^{n} \varepsilon_i x_i^2$, ahol $\varepsilon_i \in \{1, -1, 0\}$. Ekkor az $(a) \to (b)$ bázistranszformáció mátrixa:

$$S = \begin{pmatrix} \frac{1}{\sqrt{|\lambda_1|}} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \frac{1}{\sqrt{|\lambda_n|}} \end{pmatrix},$$

és Q mátrixa a (b) bázisban:

$$S^TCS = \begin{pmatrix} \frac{1}{\sqrt{|\lambda_1|}} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \frac{1}{\sqrt{|\lambda_n|}} \end{pmatrix} \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{|\lambda_1|}} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \frac{1}{\sqrt{|\lambda_n|}} \end{pmatrix} =$$

$$\begin{pmatrix} \frac{\lambda_1}{|\lambda_1|} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \frac{\lambda_n}{|\lambda_n|} \end{pmatrix}.$$

□

1.33. Tétel (Sylvester-féle tehetetlenségi törvény vagy inercia tétel). *Egy kvadratikus forma normál alakjában szereplő* $+1, -1$ *és* 0 *együtthatók száma független a négyzetösszeg alakra hozás módjától.*

1.34. Következmény. Minden szimmetrikus $C \in M_{n\times n}$ mátrixhoz létezik olyan $S \in M_{n\times n}$ reguláris mátrix, hogy $S^T CS$ diagonális alakú, és a főátlóban csak $+1, -1$ és nulla szerepel.

1.35. Tétel. *Legyen a* V *vektortéren értelmezett* $Q(\underline{x})$ *kvadratikus forma mátrixa az* (a) *bázisban* $C \in M_{n\times n}$, *és jelölje* Δ_i *az* i*-edik főminor-determinánst:*

$$\Delta_i = \begin{vmatrix} c_{11} & \dots & c_{1i} \\ \vdots & \ddots & \vdots \\ c_{i1} & \dots & c_{ii} \end{vmatrix}.$$

Ekkor létezik V*-nek olyan* (b) *kanonikus bázisa, melyben*

$$Q(\underline{x}) = \lambda_1 x_1^2 + \dots + \lambda_n x_n^2,$$

ahol

$$\lambda_1 = \frac{1}{\Delta_1}, \quad \lambda_2 = \frac{\Delta_1}{\Delta_2}, \ \dots \ , \quad \lambda_n = \frac{\Delta_{n-1}}{\Delta_n}.$$

1.36. Definíció. A V vektortéren értelmezett $Q(\underline{x})$ kvadratikus forma

1. *pozitív definit*, ha $Q(\underline{x}) > 0 \quad \forall(\underline{x} \neq \underline{0}) \in V$,
2. *negatív definit*, ha $Q(\underline{x}) < 0 \quad \forall(\underline{x} \neq \underline{0}) \in V$,
3. *pozitív szemidefinit*, ha $Q(\underline{x}) \geq 0 \quad \forall \underline{x} \in V$, és létezik $\underline{x} \neq \underline{0}$ úgy, hogy $Q(\underline{x}) = 0$,
4. *negatív szemidefinit*, ha $Q(\underline{x}) \leq 0 \quad \forall \underline{x} \in V$, és létezik $\underline{x} \neq \underline{0}$ úgy, hogy $Q(\underline{x}) = 0$,
5. 5. *indefinit*, ha $Q(\underline{x})$ negatív és pozitív értékeket egyaránt felvesz.

1.37. Példa. Ha az $\mathbb{R}^3$ vektortéren értelmezett kvadratikus forma normál alakja

1. $Q(\underline{x}) = x_1^2 + x_2^2 + x_3^2$, akkor Q pozitív definit,
2. $Q(\underline{x}) = -x_1^2 - x_2^2 - x_3^2$, akkor Q negatív definit,
3. $Q(\underline{x}) = x_1^2 + x_2^2$, akkor Q pozitív szemidefinit, mert például $Q((0,0,1)) = 0$,
4. $Q(\underline{x}) = -x_1^2 - x_2^2$, akkor Q negatív szemidefinit, mert például $Q((0,0,1)) = 0$,
5. $Q(\underline{x}) = x_1^2 - x_2^2 + x_3^2$, akkor Q indefinit, mert például $Q((1,0,0)) > 0$ de $Q((0,1,0)) < 0$.

1.38. Következmény. A $Q(\underline{x})$ kvadratikus forma akkor és csak akkor pozitív definit, ha kanonikus előállításában minden együtthatója pozitív.

1.39. Következmény. Egy véges dimenziós vektortéren értelmezett pozitív és negatív definit kvadratikus formák rangja megegyezik a vektortér dimenziójával.

Bizonyítás. Kvadratikus forma kanonikus bázisban felírt mátrixa diagonális alakú, és az átlóban a kanonikus alakban szereplő együtthatók állnak. Az 1.38. következmény miatt pozitív (negatív) definit kvadratikus forma esetén az átlóban nem szerepelhetnek nullák, így a mátrix determinánsa (az átlóban szereplő elemek szorzata) nem nulla. □

1.40. Következmény. A $Q(\underline{x})$ kvadratikus forma akkor és csak akkor pozitív definit, ha mátrixának $\Delta_1, \ldots, \Delta_n$ főminor-determinánsa pozitívak.

Bizonyítás. Az 1.35. tétel következménye. □

1.41. Megjegyzés. Lineáris, bilineáris és kvadratikus formákat a komplex számtest felett is lehet értelmezni, de a definíciójuk és a viselkedésük némileg eltér a valós esettől. A következőkben csak ezekre a különbségekre térünk ki, azokat a tulajdonságokat, amelyeket változtatás nélkül át lehet vinni $\mathbb{R}$-ről $\mathbb{C}$-re, nem soroljuk fel.

1.42. Definíció. 1. Legyen V vektortér a $\mathbb{C}$ test felett. Az $L_1 : V \to \mathbb{C}$ leképezést *elsőfajú lineáris formának* (vagy funkcionálnak) nevezzük, ha bármely $\underline{x}, \underline{y} \in V$ és $\lambda \in \mathbb{C}$ esetén teljesülnek az alábbiak:
   (a) $L_1(\underline{x} + \underline{y}) = L_1(\underline{x}) + L_1(\underline{y})$,
   (b) $L_1(\lambda \underline{x}) = \lambda L_1(\underline{x})$.
2. Az $L_2 : V \to \mathbb{C}$ leképezést *másodfajú lineáris formának* nevezzük, ha tetszőleges $\underline{x}, \underline{y} \in V$ és $\lambda \in \mathbb{C}$ esetén fennáll, hogy
   (a) $L_2(\underline{x} + \underline{y}) = L_2(\underline{x}) + L_2(\underline{y})$,
   (b) $L_2(\lambda \underline{x}) = \overline{\lambda} L_2(\underline{x})$.

1.43. Tétel. *Legyen $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ egy bázis a V vektortéren és $\underline{x} \in V$ egy tetszőleges vektor, melynek az (a) bázisbeli felírása: $\underline{x} = x_1\underline{a}_1 + \ldots x_n\underline{a}_n$.*

Ha $L_1 : V \to \mathbb{C}$ egy elsőfajú lineáris forma és $L_1(\underline{a}_i) = l_i \quad (i = 1, \ldots, n)$ az L_1 báziselőállítása az (a) bázisra vonatkozóan, akkor

$$L_1(\underline{x}) = \sum_{i=1}^{n} x_i l_i.$$

Ha $L_2 : V \to \mathbb{C}$ egy másodfajú lineáris forma és $L_2(\underline{a}_i) = k_i \ \ (i = 1, \dots, n)$ az L_2 báziselőállítása az (a) bázisra vonatkozóan, akkor

$$L_2(\underline{x}) = \sum_{i=1}^{n} \overline{x_i} k_i.$$

Bizonyítás. Az elsőfajú lineáris formára vonatkozó állítás megegyezik a valós esettel, a másodfajú lineáris formára pedig:

$$L_2(\underline{x}) = L_2(x_1\underline{a}_1 + \dots x_n\underline{a}_n) = \overline{x}_1 \underbrace{L_2(\underline{a}_1)}_{k_1} + \dots + \overline{x}_n \underbrace{L_2(\underline{a}_n)}_{k_n} = \sum_{i=1}^{n} \overline{x}_i k_i.$$

□

1.44. Definíció. Legyen V egy vektortér a $\mathbb{C}$ test felett. A $B : V \times V \to \mathbb{C}$ leképezést *bilineáris formának* nevezzük, ha rögzített $\underline{y} \in V$ vektor mellett $B(\underline{x}, \underline{y})$ elsőfajú lineáris forma és rögzített $\underline{x} \in V$ vektor mellett $B(\underline{x}, \underline{y})$ másodfajú lineáris forma. Másképpen $B(\underline{x}, \underline{y})$ első változójában lineáris, második változójában pedig másodfajú lineáris:

1. $B(\underline{x} + \underline{y}, \underline{z}) = B(\underline{x}, \underline{z}) + B(\underline{y}, \underline{z})$ $\quad \forall \underline{x}, \underline{y}, \underline{z} \in V,$
2. $B(\lambda\underline{x}, \underline{y}) = \lambda B(\underline{x}, \underline{y})$ $\quad \forall \underline{x}, \underline{y} \in V, \ \forall \lambda \in \mathbb{C},$
3. $B(\underline{x}, \underline{y} + \underline{z}) = B(\underline{x}, \underline{y}) + B(\underline{x}, \underline{z})$ $\quad \forall \underline{x}, \underline{y}, \underline{z} \in V,$
4. 4. $B(\underline{x}, \lambda\underline{y}) = \overline{\lambda} B(\underline{x}, \underline{y})$ $\quad \forall \underline{x}, \underline{y} \in V, \ \forall \lambda \in \mathbb{C}.$

1.45. Tétel. *Legyen $B : V \times V \to \mathbb{C}$ egy bilineáris forma, $\underline{x}, \underline{y} \in V$ tetszőleges vektorok melyeknek az $(a) = (\underline{a}_1, \dots, \underline{a}_n)$ bázisban a felírása $\underline{x} = x_1\underline{a}_1 + \dots + x_n\underline{a}_n$ illetve $\underline{y} = y_1\underline{a}_1 + \dots + y_n\underline{a}_n$. Ha a B bilineáris forma báziselőállítása (a)-ra vonatkozóan $B(\underline{a}_i, \underline{a}_j) = c_{ij} \ \ (i, j = 1, \dots, n)$, akkor*

$$B(\underline{x}, \underline{y}) = \sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij} x_i \overline{y_j}.$$

Másképpen, ha $C = (c_{ij}) \in M_{n\times n}$,

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \overline{Y} = \begin{pmatrix} \overline{y_1} \\ \vdots \\ \overline{y_n} \end{pmatrix} \quad \text{akkor} \quad B(\overline{x}, \overline{y}) = X^T C \overline{Y} \ .$$

Bizonyítás. Az állítás a bilineáris forma definíciójának következménye:

$$B(\underline{x}, \underline{y}) = B\left(\sum_{i=1}^{n} x_i\underline{a}_i, \sum_{j=1}^{n} y_j\underline{a}_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i \overline{y_j} \underbrace{B(\underline{a}_i, \underline{a}_j)}_{c_{ij}} = X^T C \overline{Y}.$$

□

1.46. Definíció. A $B : V \times V \to \mathbb{C}$ bilineáris formát *Hermite-szimmetrikus* vagy *Hermite-féle bilineáris formának* nevezzük, ha bármely $\underline{x}, \underline{y} \in V$ vektorok esetén

$$B(\underline{x}, \underline{y}) = \overline{B(\underline{y}, \underline{x})}.$$

1.47. Tétel. *Egy $B : V \times V \to \mathbb{C}$ bilineáris forma akkor és csak akkor Hermite-féle, ha mátrixa konjugált szimmetrikus: $C = \overline{C}^T$, vagyis $c_{ij} = \overline{c_{ji}}$.*

Bizonyítás. 1. Ha B Hermite-féle bilineáris forma, és mátrixa az (a) bázisban $C = (c_{ij})$, akkor

$$c_{ij} = B(\underline{a}_i, \underline{a}_j) = \overline{B(\underline{a}_j, \underline{a}_i)} = \overline{c_{ji}}.$$

2. Ha $c_{ij} = \overline{c_{ji}}$, akkor tetszőleges $\underline{x}, \underline{y} \in V$ esetén

$$B(\underline{x}, \underline{y}) = \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}x_i\overline{y_j} = \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{c_{ji}}x_i\overline{y_j} =$$

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \overline{c_{ji}\overline{x_i}y_j} = \overline{\sum_{i=1}^{n}\sum_{j=1}^{n} c_{ji}y_j\overline{x_i}} = \overline{B(\underline{y}, \underline{x})}.$$

□

1.48. Definíció. Egy $B : V \times V \to \mathbb{C}$ Hermite-féle bilineáris formából származó *Hermite-féle kvadratikus forma*: $Q : V \to \mathbb{C},\ Q(\underline{x}) = B(\underline{x}, \underline{x})$.

1.49. Tétel. *Egy $Q : V \to \mathbb{C}$ Hermite-féle kvadratikus forma értéke mindig valós szám.*

Bizonyítás. Mivel egy $z \in \mathbb{C}$ szám pontosan akkor valós szám ha $z = \overline{z}$ és B Hermite-szimmetrikus bilineáris forma volt, így

$$Q(\underline{x}) = B(\underline{x}, \underline{x}) = \overline{B(\underline{x}, \underline{x})} = \overline{Q(\underline{x})}$$

miatt $Q(\underline{x}) \in \mathbb{R}$. □

1.50. Tétel. *Egy $Q(\underline{x})$ Hermite-féle kvadratikus forma egyértelműen meghatározza azt az Hermite-szimmetrikus bilineáris formát, amelyből származik:*

$$B(\underline{x}, \underline{y}) = \frac{1}{2}\Big[Q(\underline{x} + \underline{y}) - Q(\underline{x}) - Q(\underline{y}) + i\big(Q(\underline{x} + i\underline{y}) - Q(\underline{x}) - Q(\underline{y})\big)\Big].$$

Bizonyítás. Először a bilineáris forma valós részét határozzuk meg:

$$Q(\underline{x}+\underline{y}) = B(\underline{x}+\underline{y},\underline{x}+\underline{y}) = \underbrace{B(\underline{x},\underline{x})}_{Q(\underline{x})} + B(\underline{x},\underline{y}) + \underbrace{B(\underline{y},\underline{x})}_{\overline{B(\underline{x},\underline{y})}} + \underbrace{B(\underline{y},\underline{y})}_{Q(\underline{y})} =$$

$$Q(\underline{x}) + Q(\underline{y}) + \underbrace{B(\underline{x},\underline{y}) + \overline{B(\underline{x},\underline{y})}}_{2ReB(\underline{x},\underline{y})},$$

ahonnan

$$\mathrm{Re}B(\underline{x},\underline{y}) = \frac{1}{2}(Q(\underline{x}+\underline{y}) - Q(\underline{x}) - Q(\underline{y})).$$

$B(\underline{x},\underline{y})$ képzetes része pedig:

$$Q(\underline{x}+i\underline{y}) = B(\underline{x}+i\underline{y},\underline{x}+i\underline{y}) = \underbrace{B(\underline{x},\underline{x})}_{Q(\underline{x})} + \underbrace{B(\underline{x},i\underline{y})}_{\bar{i}B(\underline{x},\underline{y})} + \underbrace{B(i\underline{y},\underline{x})}_{iB(\underline{y},\underline{x})} + \underbrace{B(i\underline{y},i\underline{y})}_{i\bar{i}B(\underline{y},\underline{y})} =$$

$$Q(\underline{x}) + Q(\underline{y}) - iB(\underline{x},\underline{y}) + i\overline{B(\underline{x},\underline{y})} = Q(\underline{x}) + Q(\underline{y}) - i\underbrace{(B(\underline{x},\underline{y}) - \overline{B(\underline{x},\underline{y})})}_{2iImB(\underline{x},\underline{y})} =$$

$$Q(\underline{x}) + Q(\underline{y}) + 2ImB(\underline{x},\underline{y}),$$

ahonnan

$$\mathrm{Im}B(\underline{x},\underline{y}) = \frac{1}{2}(Q(\underline{x}+i\underline{y}) - Q(\underline{x}) - Q(\underline{y})).$$

□

1.51. Következmény. Legyen (a) bázis a V vektortéren. Egy $Q : V \to \mathbb{R}$ Hermite-féle kvadratikus forma hatása egy tetszőleges vektoron:

$$Q(\underline{x}) = \sum_{i=1}^{n} c_{ij} x_i \overline{x_j} = X^T C \overline{X}.$$

1.52. Tétel. *Legyen V egy vektortér a $\mathbb{C}$ test felett. Tetszőleges V-n értelmezett $Q(\underline{x})$ Hermite-féle kvadratikus forma esetén létezik V-ben olyan bázis, melyben $Q(\underline{x})$ kanonikus alakú:*

$$Q(\underline{x}) = \lambda_1 x_1 \overline{x_1} + \cdots + \lambda_n x_n \overline{x_n}$$

és $\lambda_1, \ldots, \lambda_n$ valós számok.

2. Euklideszi terek

2.1. Definíció. Az $\mathbb{E}$ véges dimenziós valós vektorteret *Euklideszi tér*nek nevezzük, ha $\mathbb{E}$-n adott egy olyan szimmetrikus bilineáris forma, melyhez tartozó kvadratikus forma pozitív definit. Ekkor a bilineáris formát $\mathbb{E}$-n definiált *belső szorzás*nak vagy *skaláris szorzás*nak nevezzük. Jele: $(\underline{x}, \underline{y})$.

2.2. Definíció. Legyen $\underline{x} \in \mathbb{E}$, ekkor $\underline{x}$ *normáján* vagy *hosszán* az

$$\|\underline{x}\| = \sqrt{(\underline{x}, \underline{x})}$$

számot értjük.

2.3. Megjegyzés. Mivel a belső szorzathoz (mint bilineáris formához) tartozó kvadratikus forma pozitív definit, így $(\underline{x}, \underline{x}) \geq 0$ miden $\underline{x} \in \mathbb{E}$ esetén. Ez azt jelenti, hogy a norma definíciójában szereplő $\sqrt{(\underline{x}, \underline{x})}$ tetszőleges $\underline{x} \in \mathbb{E}$ esetén értelmezhető.

2.4. Tétel. *Az $\mathbb{E}$ Euklideszi téren a norma teljesíti az alábbi tulajdonságokat: bármely $\underline{x} \in \mathbb{E}$ vektor és $\lambda \in \mathbb{R}$ esetén:*

1. $\|\underline{x}\| \geq 0$; $\|\underline{x}\| = 0 \iff \underline{x} = \underline{0}$,
2. $\|\lambda \underline{x}\| = |\lambda| \|\underline{x}\|$.

Bizonyítás. 1. Következik abból, hogy $\|\underline{x}\|^2 = (\underline{x}, \underline{x})$ pozitív definit kvadratikus forma.

2. $\|\lambda \underline{x}\| = \sqrt{(\lambda \underline{x}, \lambda \underline{x})} = \sqrt{\lambda^2 (\underline{x}, \underline{x})} = |\lambda| \sqrt{(\underline{x}, \underline{x})} = |\lambda| \|\underline{x}\|$.

□

2.5. Példa. $\mathbb{R}^3$-ban, ha φ jelöli az $\underline{x}, \underline{y} \in \mathbb{R}^3$ vektorok szögét, akkor

$$(\underline{x}, \underline{y}) = |\underline{x}| |\underline{y}| \cos \varphi$$

belső szorzat, és a természetes báziban felírt $\underline{x} = (x_1, x_2, x_3)$, $\underline{y} = (y_1, y_2, y_3)$ vektorok esetén

$$(\underline{x}, \underline{y}) = x_1 y_1 + x_2 y_2 + x_3 y_3.$$

Ekkor egy $\underline{x} \in \mathbb{R}^3$ vektor normája $\sqrt{x_1^2 + x_2^2 + x_3^2} = |\underline{x}|$ lesz.

2.6. Definíció. Azokat az $\underline{e} \in \mathbb{E}$ vektorokat, melyekre , $\|\underline{e}\| = 1$ *normált vektor*oknak nevezzük.

2.7. Példa. Tetszőleges $(\underline{x} \neq 0) \in \mathbb{E}$ vektor esetén $\dfrac{\underline{x}}{\|\underline{x}\|}$ normált vektor.

2.8. Definíció. Legyen $\mathbb{E}$ Euklideszi tér. Az $\underline{x}, \underline{y} \in \mathbb{E}$ nemnulla vektorok φ *szög*én a következőt értjük:

$$\varphi = \arccos \frac{(\underline{x}, \underline{y})}{\|\underline{x}\| \|\underline{y}\|}.$$

2.9. Megjegyzés. Mivel a definíció szerint $\cos\varphi = \dfrac{(\underline{x},\underline{y})}{\|\underline{x}\|\|\underline{y}\|}$, így

$$-1 \le \frac{(\underline{x},\underline{y})}{\|\underline{x}\|\|\underline{y}\|} \le 1$$

fenn kell hogy álljon, de ez a következő, fontos tétel miatt mindig teljesül.

2.10. Tétel (Cauchy-Swarz-Bunyakowszky egyenlőtlenség). *Az $\mathbb{E}$ Euklideszi vektortér tetszőleges $\underline{x},\underline{y}$ vektoraira teljesül, hogy*

$$|(\underline{x},\underline{y})| \le \|\underline{x}\|\|\underline{y}\|.$$

Egyenlőség akkor és csak akkor áll fenn, ha $\underline{x} = \mu\underline{y}$ valamely $\mu \in \mathbb{R}$ esetén.

Bizonyítás. 1. Tekintsük a

$$\begin{aligned} 0 &\le \|\underline{x}+\lambda\underline{y}\|^2 = (\underline{x}+\lambda\underline{y},\underline{x}+\lambda\underline{y}) = (\underline{x},\underline{x}) + \lambda^2(\underline{y},\underline{y}) + 2\lambda(\underline{x},\underline{y}) \\ &= \|\underline{x}\|^2 + \lambda^2\|\underline{y}\|^2 + 2\lambda(\underline{x},\underline{y}) \end{aligned}$$

egyenlőtlenséget, amely minden $\underline{x},\underline{y} \in \mathbb{E}$ és $\lambda \in \mathbb{R}$ esetén teljesül. Ez λ-ban másodfokú, így akkor és csak akkor teljesülhet, ha a diszkrimináns kisebb vagy egyenlő mint nulla (ellenkező esetben a $0 = \|\underline{y}\|^2\lambda^2 + 2(\underline{x},\underline{y})\lambda + \|\underline{x}\|^2$ másodfokú egyenletnek két különböző valós gyöke van, és ezen két gyök által meghatározott nyílt intervallumban a jobboldal negatív értékeket vesz fel). Tehát

$$4(\underline{x},\underline{y})^2 - 4\|\underline{x}\|^2\|\underline{y}\|^2 \le 0,$$

$$(\underline{x},\underline{y})^2 \le \|\underline{x}\|^2\|\underline{y}\|^2,$$

$$|(\underline{x},\underline{y})| \le \|\underline{x}\|\|\underline{y}\|.$$

2. Egyenlőség pontosan akkor teljesül valamely $\underline{x},\underline{y}$ esetén, ha a diszkrimináns nulla. Ekkor a $0 = \|\underline{x}+\lambda\underline{y}\|^2$ másodfokú egyenletnek pontosan egy λ_1 megoldása van és erre $\underline{x}+\lambda_1\underline{y} = \underline{0}$, tehát $\underline{x}$ és $\underline{y}$ lineárisan függőek.

□

2.11. Tétel (Minkowski egyenlőtlenség vagy háromszög egyenlőtlenség). *Az $\mathbb{E}$ Euklideszi tér tetszőleges $\underline{x},\underline{y}$ vektoraira fennáll, hogy*

$$\|\underline{x}+\underline{y}\| \le \|\underline{x}\| + \|\underline{y}\|$$

és

$$\|\underline{x}+\underline{y}\| = \|\underline{x}\| + \|\underline{y}\| \quad \Longleftrightarrow \quad \text{ha létezik } \lambda \ge 0 : \quad \underline{x} = \lambda\underline{y}.$$

Bizonyítás. 1. A Cauchy-Swarz-Bunyakowszky egyenlőtlenséget használva

$$\begin{aligned}\|\underline{x}+\underline{y}\|^2 &= (\underline{x}+\underline{y},\underline{x}+\underline{y}) = \|\underline{x}\|^2+\|\underline{y}\|^2+2(\underline{x},\underline{y})\\ &\leq \|\underline{x}\|^2+\|\underline{y}\|^2+2\|\underline{x}\|\|\underline{y}\| = (\|\underline{x}\|+\|\underline{y}\|)^2.\end{aligned}$$

2. Egyenlőség akkor és csak akkor áll fenn, ha $(\underline{x},\underline{y}) = \|\underline{x}\|\|\underline{y}\|$, aminek szükséges feltétele, hogy $\underline{x}$ és $\underline{y}$ lineárisan függő legyen. Ha $\underline{x} = \lambda\underline{y}$, akkor
$$(\underline{x},\underline{y}) = (\lambda\underline{y},\underline{y}) = \lambda\|\underline{y}\|^2,$$
így $\lambda < 0$ esetén $(\underline{x},\underline{y}) < 0 \leq \|\underline{x}\|\|\underline{y}\|$ miatt nem teljesülhet az egyenlőség.

□

2.12. Következmény. Ha $x_i, y_i \in \mathbb{R}$ $(i = 1,\ldots,n)$, akkor

$$\left(\sum_{i=1}^n x_i y_i\right)^2 \leq \sum_{i=1}^n x_i^2 \sum_{i=1}^n y_i^2.$$

Bizonyítás. A 2.5. példában szereplő belső szorzatra felírva a Cauchy-Swarz-Bunyakowszky egyenlőtlenséget adódik az állítás. □

2.13. Megjegyzés. Egy V vektorteret *normált tér*nek nevezzük, ha adva van rajta egy $\|\ \| : V \to \mathbb{R}$ leképezés (norma), amely teljesíti az alábbi tulajdonságokat: bármely $\underline{x},\underline{y} \in V$ és $\lambda \in \mathbb{T}$ esetén

1. $\|\underline{x}\| \geq 0$ és $\|\underline{x}\| = 0 \iff$ ha $\underline{x} = \underline{0}$,
2. $\|\lambda\underline{x}\| = |\lambda|\|\underline{x}\|$.
3. $\|\underline{x}+\underline{y}\| \leq \|\underline{x}\| + \|\underline{y}\|$.

Az Euklideszi terek a belső szorzatból származó normával normált teret alkotnak a 2.4. tétel és a Minkowsky egyenlőtlenség szerint, de nem minden normált tér Euklideszi tér.

2.14. Definíció. Az $\mathbb{E}$ Euklideszi tér $\underline{x}$ és $\underline{y}$ vektorainak *távolság*a:

$$d(\underline{x},\underline{y}) = \|\underline{x}-\underline{y}\|$$

2.15. Következmény. Tetszőleges $\underline{x},\underline{y},\underline{z} \in \mathbb{E}$ vektorok esetén:

$$d(\underline{x},\underline{z}) \leq d(\underline{x},\underline{y}) + d(\underline{y},\underline{z}).$$

Bizonyítás. Az állítás a Minkowsky egyenlőtlenség felírva az $\underline{x}-\underline{y}$ és $\underline{z}-\underline{y}$ vektorokra:

$$d(\underline{x},\underline{z}) = \|\underline{x}-\underline{z}\| = \|(\underline{x}-\underline{y})-(\underline{z}-\underline{y})\| \leq \|\underline{x}-\underline{y}\|+\|\underline{z}-\underline{y}\| = d(\underline{x},\underline{y})+d(\underline{y},\underline{z}).$$

□

2.16. Megjegyzés. A V vektorteret *metrikus tér*nek nevezzük, ha adva van rajta egy $d : V \times V \to \mathbb{R}$ leképezés (*metrika*), amely teljesíti az alábbi tulajdonságokat: bármely $\underline{x}, \underline{y}, \underline{z} \in V$ esetén

1. $d(\underline{x}, \underline{y}) \geq 0$ és $d(\underline{x}, \underline{y}) = 0 \iff$ ha $\underline{x} = \underline{y}$,
2. $d(\underline{x}, \underline{y}) = d(\underline{y}, \underline{x})$,
3. $d(\underline{x}, \underline{z}) \leq d(\underline{x}, \underline{y}) + d(\underline{y}, \underline{z})$.

Minden normált tér metrikus tér a $d(\underline{x}, \underline{y}) \doteq \|\underline{x} - \underline{y}\|$ metrikával (természetesen az Euklideszi tereken a belső szorzatból származó norma segítségével definiált távolságfüggvény eleget tesz a metrika követelményeinek), de nem minden metrikus tér normált tér.

2.17. Definíció. Az $\mathbb{E}$ Euklideszi vektortér $\underline{x}$ és $\underline{y}$ vektorait *merőleges*nek vagy *ortogonális*nak nevezzük, ha $(\underline{x}, \underline{y}) = 0$. Jele: $\underline{x} \perp \underline{y}$.

2.18. Következmény. A nullvektor minden $\mathbb{E}$-beli vektorra merőleges.

2.19. Definíció. Az $(\underline{a}_1, \ldots, \underline{a}_k)$ $\mathbb{E}$-beli vektorrendszert ortogonálisnak nevezzük, ha vektorai páronként merőlegesek egymásra, azaz $\underline{a}_i \perp \underline{a}_j$, $(i, j = 1, \ldots, k)$ $i \neq j$.

2.20. Definíció. Az $(\underline{e}_1, \ldots, \underline{e}_k) \in \mathbb{E}$ vektorrendszer *ortonormált*, ha vektorai páronként merőlegesek és normáltak: $\underline{e}_i \perp \underline{e}_j$ $(i, j = 1, \ldots, k)$ $i \neq j$, $\|\underline{e}_i\| = 1$ $(i = 1, \ldots, k)$. Másképpen $(\underline{e}_i, \underline{e}_j) = \delta_{ij}$ $(i, j = 1, \ldots, k)$.

2.21. Tétel (Pythagoras tétel). *Legyen $\mathbb{E}$ Euklideszi vektortér. Az $\underline{x}, \underline{y} \in \mathbb{E}$ vektorok akkor és csak akkor merőlegesek egymásra, ha*

$$\|\underline{x} + \underline{y}\|^2 = \|\underline{x}\|^2 + \|\underline{y}\|^2.$$

Bizonyítás. Mivel $\|\underline{x} + \underline{y}\|^2 = (\underline{x} + \underline{y}, \underline{x} + \underline{y}) = \|\underline{x}\|^2 + \|\underline{y}\|^2 + 2(\underline{x}, \underline{y})$, így

1. ha $\underline{x} \perp \underline{y}$, akkor $(\underline{x}, \underline{y}) = 0$ miatt
$$\|\underline{x} + \underline{y}\|^2 = \|\underline{x}\|^2 + \|\underline{y}\|^2,$$
2. ha $\|\underline{x} + \underline{y}\|^2 = \|\underline{x}\|^2 + \|\underline{y}\|^2$, akkor $2(\underline{x}, \underline{y}) = 0$ miatt $\underline{x} \perp \underline{y}$.

□

2.22. Tétel. *Ha $(\underline{e}_1, \ldots, \underline{e}_k) \in \mathbb{E}$ ortonormált vektorrendszer, akkor lineárisan független vektorrendszer.*

Bizonyítás. Belátjuk, hogy a nullvektor csak triviális lineáris kombinációként állítható elő az $\underline{e}_1, \ldots, \underline{e}_k$ vektorokból. Ha $\underline{0} = \alpha_1 \underline{e}_1 + \cdots + \alpha_k \underline{e}_k$, akkor

$$0 = (\underline{0}, \underline{e}_i) = (\alpha_1 \underline{e}_1 + \cdots + \alpha_k \underline{e}_k, \underline{e}_i) =$$

$$\alpha_1 \underbrace{(\underline{e}_1, \underline{e}_i)}_{0} + \cdots + \alpha_i \underbrace{(\underline{e}_i, \underline{e}_i)}_{1} + \cdots + \alpha_k \underbrace{(\underline{e}_k, \underline{e}_i)}_{0} = \alpha_i$$

teljesül minden $i \in \{1, \ldots, k\}$ esetén. □

2.23. Definíció. Az $(\underline{e}_1, \ldots, \underline{e}_n) \in \mathbb{E}$ ortonormált vektorrendszert *ortonormált bázis*nak nevezzük, ha generátorrendszere $\mathbb{E}$-nek, azaz ha $\mathbb{E}$ egy n-dimenziós Euklideszi tér.

2.24. Tétel (Gram-Schmidt-féle ortogonalizációs eljárás). *Az $\mathbb{E}$ Euklideszi tér tetszőleges $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ bázisához létezik olyan $(e) = (\underline{e}_1, \ldots, \underline{e}_n)$ ortonormált bázisa $\mathbb{E}$-nek, hogy*

$$\mathcal{L}(\underline{a}_1, \ldots, \underline{a}_k) = \mathcal{L}(\underline{e}_1, \ldots, \underline{e}_k) \quad (k = 1, \ldots, n).$$

Bizonyítás. Adunk egy gyakorlatban is jól használható eljárást az (e) bázis megkonstruálására.

1. Legyen $\underline{e}_1 = \dfrac{\underline{a}_1}{\|\underline{a}_1\|}$, ekkor természetesen $\mathcal{L}(\underline{a}_1) = \mathcal{L}(\underline{e}_1)$, és $\underline{e}_1$ normált vektor.
2. Ha már létezik $\underline{e}_1, \ldots, \underline{e}_k$ ortonormált rendszer, melyre $\mathcal{L}(\underline{a}_1, \ldots, \underline{a}_k) = \mathcal{L}(\underline{e}_1, \ldots, \underline{e}_k)$, akkor legyen az $\underline{e}'_{k+1}$ vektor a következő:

   $$\underline{e}'_{k+1} = \underline{a}_{k+1} - (\underline{a}_{k+1}, \underline{e}_1)\underline{e}_1 - \cdots - (\underline{a}_{k+1}, \underline{e}_k)\underline{e}_k \ .$$

   Ekkor ennek a vektornak a normáltja megfelelő lesz: ha $\underline{e}_{k+1} = \dfrac{\underline{e}'_{k+1}}{\|\underline{e}'_{k+1}\|}$, akkor
   (a) $\underline{e}_1, \ldots, \underline{e}_k, \underline{e}_{k+1}$ ortonormált rendszer, mert

   $$(\underline{e}_{k+1}, \underline{e}_i) =$$

   $$\frac{1}{\|\underline{e}'_{k+1}\|}\Big((\underline{a}_{k+1}, \underline{e}_i) - (\underline{a}_{k+1}, \underline{e}_1) \underbrace{(\underline{e}_1, \underline{e}_i)}_{0} - \cdots - (\underline{a}_{k+1}, \underline{e}_i) \underbrace{(\underline{e}_i, \underline{e}_i)}_{1}$$

   $$- \cdots - (\underline{a}_{k+1}, \underline{e}_k) \underbrace{(\underline{e}_k, \underline{e}_i)}_{0} \Big) = \frac{1}{\|\underline{e}'_{k+1}\|}\big((\underline{a}_{k+1}, \underline{e}_i) - (\underline{a}_{k+1}, \underline{e}_i) \big) = 0,$$

   (b) $\mathcal{L}(\underline{a}_1, \ldots, \underline{a}_{k+1}) = \mathcal{L}(\underline{e}_1, \ldots, \underline{e}_{k+1})$, mert $\underline{e}_{k+1}$-et az $\underline{e}_1, \ldots, \underline{e}_k$, $\underline{a}_{k+1}$ vektorok lineáris kombinációjaként állítottuk elő.

□

2.25. Következmény. Minden ortonormált vektorrendszer kiegészíthető ortonormált bázissá.

2.26. Tétel. *Legyen az $\mathbb{E}$ Euklideszi téren $(e) = (\underline{e}_1, \dots, \underline{e}_n)$ ortonormált bázis és az $\underline{x}, \underline{y} \in \mathbb{E}$ vektorok felírása az (e) bázisban $\underline{x} = x_1\underline{e}_1 + \dots + x_n\underline{e}_n$ illetve $\underline{y} = y_1\underline{e}_1 + \dots + y_n\underline{e}_n$. Ekkor*

$$(\underline{x}, \underline{y}) = \sum_{i=1}^{n} x_i y_i.$$

Bizonyítás. A belső szorzat bilinearitása miatt

$$(\underline{x}, \underline{y}) = (x_1\underline{e}_1 + \dots + x_n\underline{e}_n, y_1\underline{e}_1 + \dots + y_n\underline{e}_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \underbrace{(\underline{e}_i, \underline{e}_j)}_{\delta_{ij}} = \sum_{i=1}^{n} x_i y_j.$$

□

2.27. Tétel. *Legyen $(e) = (\underline{e}_1, \dots, \underline{e}_n)$ ortonormált bázis az $\mathbb{E}$ Euklideszi vektortéren, és $\underline{x} \in \mathbb{E}$. Ekkor az $\underline{x}$ vektor úgynevezett Fourier előállítása:*

$$\underline{x} = \sum_{i=1}^{n} (\underline{x}, \underline{e}_i)\underline{e}_i.$$

Bizonyítás. Ha az $\underline{x}$ vektor felírása az (e) bázisban $\underline{x} = x_1\underline{e}_i + \dots + x_n\underline{e}_n$, akkor

$$(\underline{x}, \underline{e}_i) = (x_1\underline{e}_1 + \dots + x_n\underline{e}_n, \underline{e}_i) = \sum_{j=1}^{n} x_i \underbrace{(\underline{e}_j, \underline{e}_i)}_{\delta_{ij}} = x_i,$$

tehát $\underline{x} = \sum_{i=1}^{n} x_i\underline{e}_i = \sum_{i=1}^{n} (\underline{x}, \underline{e}_i)\underline{e}_i$. □

2.28. Tétel. *Ha $(e) = (\underline{e}_1, \dots, \underline{e}_n)$ ortonormált bázis az $\mathbb{E}$ Euklideszi téren és $\underline{x} \in \mathbb{E}$, akkor*

1. *Bessel egyenlőtlenség:*

$$\sum_{i=1}^{k} (\underline{x}, \underline{e}_i)^2 \le \|\underline{x}\|^2 \qquad 1 \le k \le n,$$

2. *Parseval egyenlőség:*

$$\sum_{i=1}^{n} (\underline{x}, \underline{e}_i)^2 = \|\underline{x}\|^2.$$

Bizonyítás. Felhasználva, hogy $(\underline{x}, \underline{e}_i) = x_i$ és a 2.26. tétel alapján

$$\begin{aligned} \|\underline{x}\|^2 &= (\underline{x}, \underline{x}) = \sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} (\underline{x}, \underline{e}_i)^2 = \sum_{i=1}^{k} (\underline{x}, \underline{e}_i)^2 + \sum_{i=k+1}^{n} (\underline{x}, \underline{e}_i)^2 \\ &\geq \sum_{i=1}^{k} (\underline{x}, \underline{e}_i)^2. \end{aligned}$$

□

2.29. Definíció. Azt mondjuk, hogy az $\mathbb{E}_1$ és az $\mathbb{E}_2$ Euklideszi vektorterek *izometrikusan izomorf*ak, ha létezik $\psi : \mathbb{E}_1 \to \mathbb{E}_2$ bijektív leképezés, amely megtartja a belső szorzatot, azaz

$$(\underline{x}, \underline{y})_1 = (\psi(\underline{x}), \psi(\underline{y}))_2 \qquad \forall \underline{x}, \underline{y} \in \mathbb{E}_1 \ ,$$

ahol $(\ ,\ )_1$ jelöli az $\mathbb{E}_1$-beli belső szorzást és $(\ ,\ )_2$ pedig az $\mathbb{E}_2$-belit.

2.30. Tétel. *Minden n-dimenziós Euklideszi vektortér izometrikusan izomorf a 2.5. példában szereplő belső szorzással ellátott $\mathbb{R}^n$-el.*

Bizonyítás. Már beláttuk, hogy minden n-dimenziós vektortér izomorf $\mathbb{R}^n$-el és az izomorfizmust a koordinátaleképezés valósítja meg (lásd Diszkrét Matematika 1. 5. fejezet). Belátjuk, hogy ez a leképezés megtartja a belső szorzatot. Legyen $\mathbb{E}$-ben $(a) = (\underline{a}_1, \ldots, \underline{a}_n)$ ortonormált bázis és az $\underline{x}, \underline{y} \in \mathbb{E}$ vektorok felírása (a)-ben $\underline{x} = x_1\underline{a}_1 + \cdots + x_n\underline{a}_n$ illetve $\underline{y} = y_1\underline{a}_1 + \cdots + y_n\underline{a}_n$. $\mathbb{R}^n$-ben legyen $(e) = (\underline{e}_1, \ldots, \underline{e}_n)$ a kanonikus bázis, a koordinátaleképezés pedig

$$\kappa(\underline{x}) = x_1\underline{e}_1 + \cdots + x_n\underline{e}_n = (x_1, \ldots, x_n).$$

Ha az $\mathbb{E}$-beli belső szorzást $(\ ,\ )_1$ jelöli és az $\mathbb{R}$-beli belső szorzást $(\ ,\ )$, akkor

$$(\underline{x}, \underline{y})_1 = \sum_{i=1}^{n} x_i y_i,$$

$$(\kappa(\underline{x}), \kappa(\underline{y})) = ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{i=1}^{n} x_i y_i.$$

□

2.31. Következmény. Két Euklideszi tér pontosan akkor izomorf, ha dimenziójuk megegyezik.

2.32. Tétel. *Legyen $\mathbb{E}$ Euklideszi tér és $\underline{x} \in \mathbb{E}$. Ekkor az $\underline{x}$ vektorra merőleges vektorok halmaza alteret alkot $\mathbb{E}$-ben.*

Bizonyítás. 1. Ha $\underline{a} \perp \underline{x}$ és $\underline{b} \perp \underline{x}$, azaz $(\underline{a}, \underline{x}) = 0$, $(\underline{b}, \underline{x}) = 0$, akkor

$$(\underline{a} + \underline{b}, \underline{x}) = (\underline{a}, \underline{x}) + (\underline{b}, \underline{x}) = 0 + 0 = 0,$$

tehá $\underline{a} + \underline{b} \perp \underline{x}$.

2. Ha $\underline{a} \perp \underline{x}$ vagyis $(\underline{a}, \underline{x}) = 0$ akkor $(\lambda \underline{a}, \underline{x}) = \lambda(\underline{a}, \underline{x}) = 0$, tehát $\lambda \underline{a} \perp \underline{x}$.

□

2.33. Példa. $\mathbb{R}^3$-ban az $\underline{e}_3 = (0, 0, 1)$ vektorra merőleges vektorok halmaza az $\{(x, y, 0) \mid x, y \in \mathbb{R}\}$ sík.

2.34. Definíció. Legyen H egy altér az $\mathbb{E}$ Euklideszi térben. A H altér *ortogonális komplementer*ének nevezzük azon vektorok halmazát, amelyek H minden vektorára merőlegesek. Jele $H^\perp$.

$$H^\perp = \{\underline{x} \in \mathbb{E} \mid \underline{x} \perp \underline{h} \ \ \forall \underline{h} \in H\}.$$

2.35. Tétel. *Legyen $\mathbb{E}$ Euklideszi tér és $H \subset \mathbb{E}$ altér. Ekkor $H^\perp$ is altér.*

Bizonyítás. 1. Ha $\underline{x}, \underline{y} \in H^\perp$ azaz $(\underline{x}, \underline{h}) = 0$, $(\underline{y}, \underline{h}) = 0 \quad \forall \underline{h} \in H$, akkor

$$(\underline{x} + \underline{y}, \underline{h}) = (\underline{x}, \underline{h}) + (\underline{y}, \underline{h}) = 0 + 0 = 0 \quad \forall \underline{h} \in H,$$

tehá $\underline{x} + \underline{y} \in H^\perp$.

2. Ha $\underline{x} \in H^\perp$ vagyis $(\underline{x}, \underline{h}) = 0 \quad \forall \underline{h} \in H$, akkor $(\lambda \underline{x}, \underline{h}) = \lambda(\underline{x}, \underline{h}) = 0 \quad \forall \underline{h} \in H$, tehát $\lambda \underline{x} \in H^\perp$.

□

2.36. Következmény. Legyen H altér az $\mathbb{E}$ Euklideszi térben. Ekkor

1. $\underline{x} \in H^\perp$ akkor és csak akkor, ha $\underline{x}$ merőleges H minden bázisvektorára.
2. H ortogonális komplementerének az ortogonális komplementere is altér.
3. $(H^\perp)^\perp = H$ és $H \oplus H^\perp = \mathbb{E}$.

Bizonyítás. 1. és 2. nyilvánvaló.

3. egyen $\underline{e}_1, \ldots, \underline{e}_k$ otonormált bázisa H-nak (ilyen a Gram-Schmidt ortogonalizációs eljárással megadható) és $(e) = (\underline{e}_1, \ldots, \underline{e}_k, \ldots, \underline{e}_n)$ ennek kiegészítése $\mathbb{E}$ ortonormált bázisává. Ekkor minden $\underline{x} \in \mathbb{E}$ egyértelműen felírható (e)-beli elemek lineáris kombinációjaként:

$$\underline{x} = \underbrace{x_1\underline{e}_1 + \cdots + x_k\underline{e}_k}_{\underline{x}' \in H} + \underbrace{x_{k+1}\underline{e}_{k+1} + \cdots + x_n\underline{e}_n}_{\underline{x}'' \in H^\perp},$$

tehát minden $\underline{x} \in \mathbb{E}$ egyértelműen felírható

$$\underline{x} = \underline{x}' + \underline{x}'' \quad \text{alakban, ahol} \quad \underline{x}' \in H, \ \underline{x}'' \in H^\perp.$$

Ez pontosan azt jelenti, hogy $\mathbb{E} = H \oplus H^\perp$. □

2.37. Definíció. Ha H altér az $\mathbb{E}$ Euklideszi vektortérben, és $\underline{x} = \underline{x}' + \underline{x}''$, ahol $\underline{x}' \in H$ és $\underline{x}'' \in H^\perp$, akkor az $\underline{x}$ vektornak a H altértől vett *távolság*án az $\|\underline{x}''\|$ számot értjük.

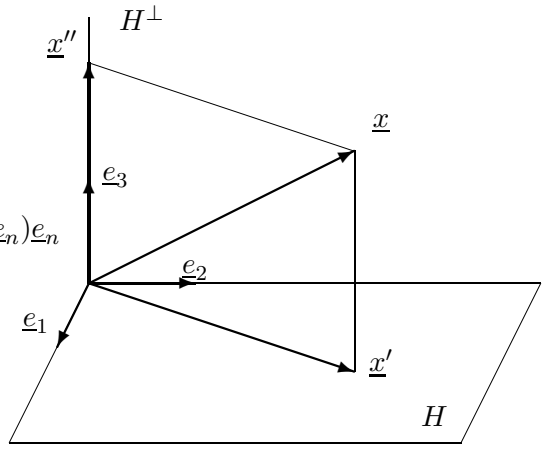
2.38. Megjegyzés. Legyen $\mathbb{E}$ Euklideszi tér és H egy altere. Az $\underline{x}$ vektor $\underline{x} = \underline{x}' + \underline{x}''$ $\underline{x}' \in H$, $\underline{x}'' \in H^\perp$ felbontásában az $\underline{x}'$ komponens nem más mint $\underline{x}$ merőleges vetülete a H altérre, $\underline{x}''$ pedig $\underline{x}$ merőleges vetülete a $H^\perp$ altérre. Ha $(e) = (\underline{e}_1, \ldots, \underline{e}_n)$ otronormált bázis és $H = \mathcal{L}(\underline{e}_1, \ldots, \underline{e}_k)$, akkor a Fourier előállítást használva a merőleges vetületek egyszerűen kiszámíthatók:

$\underline{x} = x_1\underline{e}_1 + \cdots + x_n\underline{e}_n =$

$(\underline{x}, \underline{e}_1)\underline{e}_1 + \cdots + (\underline{x}, \underline{e}_n)\underline{e}_n$

$\underline{x}' = (\underline{x}, \underline{e}_1)\underline{e}_1 + \cdots + (\underline{x}, \underline{e}_k)\underline{e}_k$

$\underline{x}'' = (\underline{x}, \underline{e}_{k+1})\underline{e}_{k+1} + \cdots + (\underline{x}, \underline{e}_n)\underline{e}_n$



3. Unitér terek

3.1. Megjegyzés. Mivel az Unitér terek és az Euklideszi terek között sok hasonlóság van, azokat a bizonyításokat amelyek változtatásnélkül vihetők át Unitér terekre, nem írjuk le.

3.2. Definíció. Legyen $\mathbb{U}$ vektortér $\mathbb{C}$ felett és $(\ ,\ ) : \mathbb{U} \times \mathbb{U} \to \mathbb{C}$ leképezés olyan, hogy bármely $\underline{x}, \underline{y}, \underline{z} \in \mathbb{U}$ és $\lambda \in \mathbb{C}$ esetén

1. $(\underline{x}, \underline{y}) = \overline{(\underline{y}, \underline{x})}$, azaz Hermite-szimmetrikus,
2. $(\lambda\underline{x}, \underline{y}) = \overline{\lambda}(\underline{x}, \underline{y})$, azaz első változójában homogén,
3. $(\underline{x} + \underline{y}, \underline{z}) = (\underline{x}, \underline{z}) + (\underline{y}, \underline{z})$, azaz első változójában additív,
4. $(\underline{x}, \underline{x}) \geq 0$ és $(\underline{x}, \underline{x}) = 0 \iff \underline{x} = \underline{0}$.

Ekkor azt mondjuk, hogy $\mathbb{U}$ *unitér* tér az $(\underline{x}, \underline{y})$ belső szorzással ellátva.

3.3. Következmény. Ha $\mathbb{U}$ unitér tér az $(\underline{x},\underline{y})$ belső szorzással, akkor minden $\underline{x},\underline{y},\underline{z}\in\mathbb{U}$ és $\lambda\in\mathbb{C}$ esetén

1. $(\underline{x},\lambda\underline{y})=\overline{\lambda}(\underline{x},\underline{y})$,
2. $(\underline{x},\underline{y}+\underline{z})=(\underline{x},\underline{y})+(\underline{x},\underline{z})$,
3. $(\underline{x},\underline{x})$ valós szám.

Bizonyítás. 1. $(\underline{x},\lambda\underline{y})=\overline{(\lambda\underline{y},\underline{x})}=\overline{\lambda(\underline{y},\underline{x})}=\overline{\lambda}\overline{(\underline{y},\underline{x})}=\overline{\lambda}(\underline{x},\underline{y})$,

2. $(\underline{x},\underline{y}+\underline{z})=\overline{(\underline{y}+\underline{z},\underline{x})}=\overline{(\underline{y},\underline{x})+(\underline{z},\underline{x})}=\overline{(\underline{y},\underline{x})}+\overline{(\underline{z},\underline{x})}=(\underline{x},\underline{y})+(\underline{x},\underline{z})$,

3. Az $\overline{(\underline{x},\underline{y})}=(\underline{y},\underline{x})$ egyenlőségbe $\underline{y}$ helyébe is $\underline{x}$-et írva $\overline{(\underline{x},\underline{x})}=(\underline{x},\underline{x})$, tehát $(\underline{x},\underline{x})$ egyenlő a konjugáltjával, így valós szám.

□

3.4. Következmény. Ha az $\mathbb{U}$ komplex számtest felett értelmezett vektortéren megadunk egy Hermite-féle bilineáris formát, melyből származó kvadratikus forma pozitív definit, akkor ezáltal egy belső szorzást definiáltunk, és minden Unitér téren adott belső szorzás Hermite-szimmetrikus bilineáris forma, amelyhez tartozó kvadratikus forma pozitív definit.

3.5. Definíció. Egy $\mathbb{U}$ Unitér tér tetszőleges $\underline{x}$ elemének hossza vagy normája az

$$\|\underline{x}\|=\sqrt{(\underline{x},\underline{x})}$$

valós szám.

3.6. Definíció. Az $\mathbb{U}$ Unitér tér $\underline{x}$ és $\underline{y}$ vektorait merőlegesnek vagy ortogonálisnak nevezzük, ha $(\underline{x},\underline{y})=0$.

3.7. Definíció. Az $(e)=(\underline{e}_1,\dots,\underline{e}_n)\in\mathbb{U}$ vektorrendszert ortonormáltnak nevezzük, ha páronként merőleges egységvektorok: $(\underline{e}_i,\underline{e}_j)=\delta_{ij}\quad(i,j=1,\dots,n)$.

3.8. Tétel. *Egy $\mathbb{U}$ Unitér tér ortonormált vektorrendszerének tagjai lineárisan függetlenek.*

3.9. Megjegyzés. A Gram-Schmidt-féle ortogonalizációs eljárás Unitér tereken ugyanúgy végrehajtható, mint Euklidesz tereken.

3.10. Tétel. *Legyen az $\mathbb{U}$ Unitér téren $(e)=(\underline{e}_1,\dots,\underline{e}_n)$ ortonormált bázis és az $\underline{x},\underline{y}\in\mathbb{U}$ vektorok felírása az (e) bázisban $\underline{x}=x_1\underline{e}_1+\dots+x_n\underline{e}_n$ illetve $\underline{y}=y_1\underline{e}_1+\dots+y_n\underline{e}_n$. Ekkor*

$$(\underline{x},\underline{y})=\sum_{i=1}^{n}x_i\overline{y_i}.$$

Bizonyítás. A belső szorzat bilinearitása miatt

$$(\underline{x},\underline{y}) = (x_1\underline{e}_1+\cdots+x_n\underline{e}_n, y_1\underline{e}_1+\cdots+y_n\underline{e}_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i\overline{y_j}\underbrace{(\underline{e}_i,\underline{e}_j)}_{\delta_{ij}} = \sum_{i=1}^{n} x_i\overline{y_j}.$$

□

3.11. Tétel. *Legyen* $(e) = (\underline{e}_1,\ldots,\underline{e}_n)$ *ortonormált bázis az* $\mathbb{U}$ *Unitér vektortéren, és* $\underline{x}\in\mathbb{U}$. *Ekkor az* $\underline{x}$ *vektor úgynevezett Fourier előállítása:*

$$\underline{x} = \sum_{i=1}^{n}(\underline{x},\underline{e}_i)\underline{e}_i.$$

3.12. Tétel. *Ha* $(e) = (\underline{e}_1,\ldots,\underline{e}_n)$ *ortonormált bázis az* $\mathbb{U}$ *Unitér téren és* $\underline{x},\underline{y}\in\mathbb{U}$, *akkor*

1. *Bessel egyenlőtlenség:*

$$\sum_{i=1}^{k}|(\underline{x},\underline{e}_i)|^2 \le \|\underline{x}\|^2 \qquad 1\le k\le n,$$

2. *Parseval egyenlőség:*

$$\sum_{i=1}^{n}|(\underline{x},\underline{e}_i)|^2 = \|\underline{x}\|^2.$$

3. *Cauchy-Swarz-Bunyakowszky egyenlőtlenség:*

$$|(\underline{x},\underline{y})| \le \|\underline{x}\|\|\underline{y}\|.$$

Bizonyítás. Felhasználva, hogy $(\underline{x},\underline{e}_i) = x_i$ és a 3.10. tétel alapján

$$\begin{aligned}\|\underline{x}\|^2 &= (\underline{x},\underline{x}) = \sum_{i=1}^{n}\underbrace{x_i\overline{x_i}}_{|x_i|} = \sum_{i=1}^{n}|(\underline{x},\underline{e}_i)|^2 = \sum_{i=1}^{k}|(\underline{x},\underline{e}_i)|^2 + \sum_{i=k+1}^{n}|(\underline{x},\underline{e}_i)|^2\\ &\ge \sum_{i=1}^{k}|(\underline{x},\underline{e}_i)|^2.\end{aligned}$$

□

3.13. Tétel. *Ha* H *altér az* $\mathbb{U}$ *Unitér téren és* $H^\perp$ *jelöli az ortogonális komplementerét, akkor*

$$H\oplus H^\perp = \mathbb{U} \quad \text{és} \quad (H^\perp)^\perp = H.$$

4. Euklideszi terek lineáris operátorai

4.1. Tétel. *Legyen $\mathbb{E}$ egy véges dimenziós Euklideszi tér és $\varphi : \mathbb{E} \to \mathbb{E}$ egy lineáris operátor. Ekkor φ-nek létezik egy- vagy két-dimenziós invariáns altere.*

Bizonyítás. Legyen φ mátrixa valamely bázisban A, és tekintsük a φ lineáris leképezés karakterisztikus egyenletének (amely független a bázis megválasztásától) egy λ gyökét, azaz

$$|A - \lambda E| = 0.$$

1. Ha λ valós gyök, akkor λ sajátérték és létezik $\underline{x} \in \mathbb{E}$ úgy, hogy $\varphi(\underline{x}) = \lambda\underline{x}$. Ekkor a $\underline{x}$ sajátvektor által generált $\mathcal{L}(\underline{x})$ egy dimenziós altér invariáns.
2. Ha $\lambda = \alpha + \beta i \quad \beta \neq 0$ komplex gyök, akkor tekintsük $\mathbb{E}$-t egy időre $\mathbb{C}$-feletti vektortérként, és φ-t pedig mint ezen a vektortéren értelmezett lineáris transzformációt (az eredeti bázisra vonatkozó A mátrixszal). A skalártartománynak ezen kibővítése természetesen csak egy absztrakció amire azért van szükségünk, mert a komplex esetben λ sajátértéke φ-nek, így létezik hozzá $\underline{a}$ sajátvektor, és ennek segítségével fogjuk megkonstruálni $\mathbb{E}$-nek egy két dimenziós invariáns alterét.

   Legyen $\underline{x}$ az a vektor melynek koordinátái az $\underline{a}$ vektor koordinátáinak valós részei, és $\underline{y}$ koordinátái legyenek az $\underline{a}$ koordinátáinak képzetes részei. Ekkor $\underline{a} = \underline{x} + i\underline{y}$, ahol $\underline{x}, \underline{y} \in \mathbb{E}$ valós vektorok. Mivel

$$\varphi(\underline{a}) = \lambda(\underline{a}) = \lambda(\underline{x} + i\underline{y}) = (\alpha + i\beta)(\underline{x} + i\underline{y}) = \alpha\underline{x} - \beta\underline{y} + i(\beta\underline{x} + \alpha\underline{y})$$

   illetve

$$\varphi(\underline{a}) = \varphi(\underline{x} + i\underline{y}) = \varphi(\underline{x}) + i\varphi(\underline{y}),$$

   így

$$\varphi(\underline{x}) = \alpha\underline{x} - \beta\underline{y}, \tag{4.1}$$

$$\varphi(\underline{y}) = \beta\underline{x} + \alpha\underline{y}. \tag{4.2}$$

   Belátjuk, hogy $\underline{x}, \underline{y}$ nem nullvektorok és lineárisan függetlenek.

   (a) Ha $\underline{x} = \underline{0}$ lenne, akkor $\varphi(\underline{x}) = \underline{0}$, amiből (4.1) miatt $\underline{y} = \underline{0}$ következik. Ekkor $\underline{a} = \underline{0}$, ami ellentmond annak, hogy $\underline{a}$ sajátvektor volt.

   (b) Ha $\underline{y} = \underline{0}$, akkor $\varphi(\underline{y}) = \underline{0}$, amiből (4.2) miatt $\underline{x} = \underline{0}$, igy $\underline{a}$ nullvektor lenne, ami ellentmondás.

(c) Indirekt tegyük fel, hogy $\underline{x}, \underline{y}$ lineárisan függő vektorok, azaz létezik olyan $\sigma \neq 0$ szám, amire $\underline{y} = \sigma\underline{x}$. Ekkor (4.2)-ből és (4.1)-ből

$$\varphi(\sigma\underline{x}) = \beta\underline{x} + \alpha\sigma\underline{x},$$

$$\varphi(\underline{x}) = \alpha\underline{x} - \beta\sigma\underline{x}.$$

Kivonva az első egyenlet σ-szorosát a másodikból $(1+\sigma^2)\varphi(\underline{x}) = \alpha\underbrace{(1+\sigma^2)}_{\neq 0}\underline{x}$, tehát $\varphi(\underline{x}) = \alpha\underline{x}$, ami (4.1) miatt azt jelenti, hogy $\beta\underline{y} = \underline{0}$, és ez ellentmond annak, hogy sem β sem $\underline{y}$ nem nulla.

Ezzel beláttuk, hogy az $\mathcal{L}(\underline{x}, \underline{y})$ két-dimenziós, és (4.1),(4.2) szerint ez invariáns altér $\mathbb{E}$-ben.

□

4.2. Tétel. *Legyen $\mathbb{E}$ egy Euklideszi vektortér és $\varphi, \psi : \mathbb{E} \to \mathbb{E}$ lineáris operátorok. Ha bármely $\underline{x}, \underline{y} \in \mathbb{E}$ esetén*

$$(\underline{x}, \varphi(\underline{y})) = (\underline{x}, \psi(\underline{y})),$$

akkor $\varphi \equiv \psi$.

Bizonyítás. Ha teljesülnek a tétel feltételei, akkor

$$0 = (\underline{x}, \varphi(\underline{y})) - (\underline{x}, \psi(\underline{y})) = (\underline{x}, \varphi(\underline{y}) - \psi(\underline{y})) = (\underline{x}, (\varphi - \psi)(\underline{y})),$$

ami $\underline{x} := (\varphi - \psi)(\underline{y})$ esetén azt jelenti, hogy

$$0 = ((\varphi - \psi)(\underline{y}), (\varphi - \psi)(\underline{y})) = \|(\varphi - \psi)(\underline{y})\|^2.$$

Ekkor $(\varphi - \psi)(\underline{y}) = \underline{0}$ vagyis $\varphi(\underline{y}) = \psi(\underline{y})$. Mivel $\underline{y}$ tetszőleges volt, így $\varphi \equiv \psi$. □

4.3. Definíció. Legyen $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris operátor az $\mathbb{E}$ Euklideszi téren. A $\varphi^* : \mathbb{E} \to \mathbb{E}$ lineáris operátort a φ *adjungált*jának nevezzük, ha bármely $\underline{x}, \underline{y} \in \mathbb{E}$ esetén

$$(\varphi(\underline{x}), \underline{y}) = (\underline{x}, \varphi^*(\underline{y})).$$

4.4. Tétel. *Az $\mathbb{E}$ Euklideszi tér tetszőleges $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris operátorának egyértelműen létezik φ^* adjungált operátora. Ha az $\mathbb{E}$ egy ortonormált bázisában φ mátrixa A, akkor ebben a bázisban φ^* mátrixa A^T.*

Bizonyítás. Legyen az $\mathbb{E}$ Euklideszi térnek $(e) = (\underline{e}_1, \ldots, \underline{e}_n)$ egy ortonormált bázisa és ebben a bázisban φ mátrixa $A = (a_{ij})$ és φ^* mátrixa $A^* =$

(a^*_{ij}). Ekkor $\varphi(\underline{e}_i) = \sum_{k=1}^{n} a_{ik}\underline{e}_k$, így

$$(\varphi(\underline{e}_i), \underline{e}_j) = \left(\sum_{k=1}^{n} a_{ik}\underline{e}_k, \underline{e}_j\right) = \sum_{k=1}^{n} a_{ik}\underbrace{(\underline{e}_k, \underline{e}_j)}_{\delta_{kj}} = a_{ij},$$

$$(\underline{e}_i, \varphi^*(\underline{e}_j)) = \left(\underline{e}_i, \sum_{k=1}^{n} a^*_{jk}\underline{e}_k\right) = \sum_{k=1}^{n} a^*_{jk}\underbrace{(\underline{e}_i, \underline{e}_k)}_{\delta_{ki}} = a^*_{ji}.$$

Innen $a_{ij} = a^*_{ji}$, tehát $A^* = A^T$ szükséges. A belső szorzat bilinearitása és φ linearitása miatt ha a bázisvektorokra teljesül, hogy $(\varphi(\underline{e}_i), e_j) = (\underline{e}_i, \overline{\varphi}(\underline{e}_j))$, akkor ez tetszőleges $\underline{x}, \underline{y} \in \mathbb{E}$ vektorokra is teljesül. Ekkor az a lineáris transzformáció melynek mátrixa az (e) bázisban A^T, eleget tesz az adjungált operátor definíciójában szereplő követelményeknek.

Ha két adjungált operátor is létezne, akkor bármely $\underline{x}, \underline{y} \in \mathbb{E}$ esetén

$$(\varphi(\underline{x}), \underline{y}) = (\underline{x}, \varphi^*(\underline{y})) = (\underline{x}, \overline{\varphi}(\underline{y}))$$

teljesülne, ami a 4.2. tétel miatt csak akkor lehetséges, ha $\varphi^* \equiv \overline{\varphi}$. Tehát adjugált oprátor minden φ lineáris transzformáció esetén létezik, egyértelmű és ortonormált bázis esetén mátrixa a φ mátrixának transzponáltja. □

4.5. Tétel. *Legyenek φ és ψ lineáris operátorok az $\mathbb{E}$ Euklideszi téren, Id pedig legyen az identikus transzformáció. Ekkor*

1. $Id = Id^*$,
2. $(\varphi^*)^* = \varphi$,
3. $(\varphi + \psi)^* = \varphi^* + \psi^*$,
4. $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$,
5. *ha φ invertálható, akkor* $(\varphi^{-1})^* = (\varphi^*)^{-1}$.

Bizonyítás. Legyen $\underline{x}, \underline{y} \in \mathbb{E}$ tetszőleges. Ekkor

2. $(\underline{x}, (\varphi^*)^*(\underline{y})) = (\varphi^*(\underline{x}), \underline{y}) = (\underline{y}, \varphi^*(\underline{x})) = (\varphi(\underline{y}), \underline{x}) = (\underline{x}, \varphi(\underline{y}))$,
3. $(\underline{x}, (\varphi + \psi)^*(\underline{y})) = ((\varphi + \psi)(\underline{x}), \underline{y}) = (\varphi(\underline{x}) + \psi(\underline{x}), \underline{y})$
   $= (\varphi(\underline{x}), \underline{y}) + (\psi(\underline{x}), \underline{y}) = (\underline{x}, \varphi^*(\underline{y})) + (\underline{x}, \psi^*(\underline{y})) = (\underline{x}, \varphi^*(\underline{y}) + \psi^*(\underline{y}))$
   $= (\underline{x}, (\varphi^* + \psi^*)(\underline{y}))$,
4. $(\underline{x}, (\varphi \circ \psi)^*(\underline{y})) = ((\varphi \circ \psi)(\underline{x}), \underline{y}) = (\varphi(\psi(\underline{x})), \underline{y}) = (\psi(\underline{x}), \varphi^*(\underline{y}))$
   $= (\underline{x}, \psi^*(\varphi^*(\underline{y}))) = (\underline{x}, (\psi^* \circ \varphi^*)(\underline{y}))$,
5. a 3. tulajdonság miatt
   $$\varphi^* \circ (\varphi^{-1})^* = (\varphi^{-1} \circ \varphi)^* = \mathrm{Id}^* = \mathrm{Id}.$$

Megjegyezzük, hogy a tétel következménye a mátrixok transzponáltjára vonatkozó tulajdonságoknak is, hiszen az adjungált operátorok azonosíthatóak a mátrixukkal, ami éppen az eredeti operátor mátrixának transzponáltja. □

4.6. Definíció. Az $\mathbb{E}$ Euklideszi tér $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris operátorát *önadjungált* vagy *szimmetrikus* operátornak nevezzük, ha $\varphi = \varphi^*$, azaz az operátor adjungáltja saját maga.

4.7. Következmény. Legyen a $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris operátor mátrixa az $\mathbb{E}$ Euklideszi tér egy ortonormált bázisában A. φ akkor és csak akkor lesz önadjungált operátor, ha $A = A^T$, azaz φ mátrixa tetszőleges ortonormált bázisban szimmetrikus.

4.8. Tétel. *Legyenek $\varphi, \psi : \mathbb{E} \to \mathbb{E}$ önadjungált operátorok, Id pedig az identikus leképezés az $\mathbb{E}$ Euklideszi téren. Ekkor*

1. *$Id = Id^*$, tehát Id önadjungált,*
2. *$(\varphi + \psi)^* = \varphi + \psi$, önadjungált operátorok összege is az,*
3. *$(\varphi \circ \psi)^* = \varphi \circ \psi$ akkor és csak akkor teljesül, ha φ és ψ felcserélhető, azaz ha $\varphi \circ \psi = \psi \circ \varphi$.*

Bizonyítás. Az állítások a 4.5. tétel következményei. □

4.9. Példa. 1. Egy $\lambda \neq 0$ skalárral való nyújtás önadjungált operátor: $\varphi(\underline{x}) = \lambda \underline{x}$ $\forall \underline{x} \in \mathbb{E}$ (lásd 2.38. megjegyzés) esetén

$$(\varphi(\underline{x}), \underline{y}) = (\lambda \underline{x}, \underline{y}) = \lambda(\underline{x}, \underline{y}) = (\underline{x}, \lambda \underline{y}) = (\underline{x}, \varphi(\underline{y})).$$

2. Egy $H \subset \mathbb{E}$ altérre történő merőleges vetítés önadjungált operátor: $\varphi(\underline{x}) = \underline{x}'$, ahol $\underline{x}' \in H$ és $\underline{x}'' = \underline{x} - \underline{x}' \in H^\perp$ esetén

$$(\varphi(\underline{x}), \underline{y}) = (\underline{x}', \underline{y}) = (\underbrace{\underline{x}'}_{\in H}, \underbrace{\underline{y}'}_{\in H} + \underbrace{\underline{y}''}_{\in H^\perp}) = (\underline{x}', \underline{y}') + \underbrace{(\underline{x}', \underline{y}'')}_{0} = (\underline{x}', \underline{y}')$$

$$(\underline{x}, \varphi(\underline{y})) = (\underline{x}, \underline{y}') = (\underline{x}' + \underline{x}'', \underline{y}') = (\underline{x}', \underline{y}') + \underbrace{(\underline{x}'', \underline{y}')}_{0} = (\underline{x}', \underline{y}') \ ,$$

tehát $(\varphi(\underline{x}), \underline{y}) = (\underline{x}, \varphi(\underline{y}))$, azaz φ valóban önadjungált.

4.10. Tétel. *Ha H a φ önadjungált operátor invariáns altere, akkor $H^\perp$ is invariáns altér.*

Bizonyítás. Legyen $\underline{x} \in H^\perp$ és belátjuk, hogy $\varphi(\underline{x})$ is $H^\perp$ eleme, azaz $(\varphi(\underline{x}), \underline{h}) = 0$ minden $\underline{h} \in H$ esetén. Mivel φ önadjungált és H invariáns altér, így

$$(\varphi(\underline{x}), \underline{h}) = (\underbrace{\underline{x}}_{\in H^\perp}, \underbrace{\varphi(\underline{h})}_{\in H}) = 0.$$

□

4.11. Tétel. *Egy $\varphi : \mathbb{E} \to \mathbb{E}$ önadjungált lineáris operátor karakterisztikus egyenletének minden gyöke valós.*

Bizonyítás. Indirekt tegyük fel, hogy létezik $\lambda = \alpha + i\beta$ $(\beta \neq 0)$ nem valós gyök. Ekkor a 4.1. tétel bizonyításában leírtak alapján léteznek $\underline{x}, \underline{y} \in \mathbb{E}$ nem nulla vektorok úgy, hogy

$$\varphi(\underline{x}) = \alpha\underline{x} - \beta\underline{y}$$
$$\varphi(\underline{y}) = \beta\underline{x} + \alpha\underline{y},$$

így

$$(\varphi(\underline{x}), \underline{y}) = (\alpha\underline{x} - \beta\underline{y}, \underline{y}) = \alpha(\underline{x}, \underline{y}) - \beta(\underline{y}, \underline{y})$$
$$(\underline{x}, \varphi(\underline{y})) = (\underline{x}, \beta\underline{x} + \alpha\underline{y}) = \beta(\underline{x}, \underline{x}) + \alpha(\underline{x}, \underline{y}).$$

Mivel φ önadjungált, ezért az egyenletek baloldalai megegyeznek, és a jobboldalakat egyenlővé téve

$$\underbrace{\beta}_{\neq 0}(\underbrace{(\underline{x}, \underline{x})}_{\neq 0} + \underbrace{(\underline{y}, \underline{y})}_{\neq 0}) = 0$$

adódik, ami ellentmondás. □

4.12. Következmény. Önadjungált lineáris operátor spektruma teljes.

4.13. Tétel (Struktúratétel). *Ha $\varphi : \mathbb{E} \to \mathbb{E}$ önadjungált lineáris operáror az $\mathbb{E}$ véges dimenziós Euklideszi téren, akkor $\mathbb{E}$-ben létezik φ sajátvektoraiból álló ortonormált bázis.*

Bizonyítás. $\mathbb{E}$ dimenziója szerinti teljes indukciót alkalmazunk.

Ha $\dim \mathbb{E} = 1$, akkor az állítás nyilvánvaló. Tegyük fel, hogy a tétel igaz minden n-nél kisebb dimenziós Euklideszi tér esetén, és legyen most $\mathbb{E}$ n-dimenziós.

Tekintsük egy $\underline{x} \in \mathbb{E}$ sajátvektorát a φ önadjungált operátornak (ilyen létezik a 4.12. következmény miatt). Ekkor a $H := \mathcal{L}(\underline{x})$ altér φ invariáns, és a 4.10. tétel szerint $H^\perp$ szintén invariáns altér. Mivel H 1-dimenziós altér, ezért $H^\perp$ $(n-1)$-dimenziós Euklideszi tér, így az indukciós feltevés szerint létezik olyan $(\underline{e}_1, \ldots, \underline{e}_{n-1})$ ortonormált bázisa amely φ sajátvektoraiból áll. Az $\underline{x}$ sajátvektor merőleges a $H^\perp$ altér miden vektorára, így $\left(\underline{e}_1, \ldots, \underline{e}_{n-1}, \frac{\underline{x}}{\|\underline{x}\|}\right)$ ortonormált bázis lesz $\mathbb{E}$-ben. □

4.14. Megjegyzés. Mivel sajátvektorokból álló bázisban a lineáris transzformációk mátrixai diagonális alakúak, így a Struktúratétel szerint minden önadjungált operátor mátrixa diagonalizálható.

4.15. Tétel (Főtengelytranszformációs tétel). *Egy véges dimenziós Euklideszi téren adott $Q(\underline{x})$ kvadratikus formához létezik olyan ortonormált bázis, amelyben a kvadratikus forma kanonikus alakú, és az ebben szereplő együtthatók a kvadratikus forma tetszőleges bázisra vonatkozó mátrixának sajátértékei.*

Bizonyítás. Legyen (b) ortonormált bázis $\mathbb{E}$-ben, és tegyük fel, hogy $Q(\underline{x})$ mátrixa (b)-ben A. Legyen φ az a lineáris transzformáció, amelynek mátrixa (b)-ben A. Mivel A szimmetrikus mátrix, így φ önadjungált leképezés, tehát létezik φ sajátvektoraiból álló $(e) = (\underline{e}_1, \dots, \underline{e}_n)$ ortonormált bázis. Ha a sajátvektorokhoz tartozó sajátértékek $\lambda_1, \dots, \lambda_n$, akkor

$$Q(\underline{x}) = X^T \underbrace{AX}_{\varphi(\underline{x})} = (\underline{x}, \varphi(\underline{x})) = \left(\underline{x}, \varphi\left(\sum_{i=1}^{n} x_i \underline{e}_i\right)\right) =$$

$$\sum_{i=1}^{n} x_i (\underline{x}, \underbrace{\varphi(\underline{e}_i)}_{\lambda_i \underline{e}_i}) = \sum_{i=1}^{n} \lambda_i x_i \underbrace{(\underline{x}, \underline{e}_i,)}_{x_i} = \sum_{i=1}^{n} \lambda_i x_i^2,$$

azaz $Q(\underline{x})$ az (e) bázisban kanonikus alakú, és a kanonikus alakban szereplő együtthatók a kvadratikus forma mátrixának sajátértékei. □

4.16. Következmény. Minden szimmetrikus mátrix diagonalizálható, azaz hasonló egy diagonális mátrixhoz. A hasonlóságot egy olyan S mátrix valósítja meg, amelynek oszlopaiban egymásra merőleges egységhosszú vektorok koordinátái szerepelnek, az ilyen mátrixot a későbbiekben ortogonális mátrixnak fogjuk nevezni.

4.17. Definíció. Az $\mathbb{E}$ Euklideszi téren adott $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris transzformációt ortogonálisnak nevezzük, ha bármely $\underline{x}, \underline{y} \in \mathbb{E}$ esetén

$$(\underline{x}, \underline{y}) = (\varphi(\underline{x}), \varphi(\underline{y})).$$

4.18. Következmény. Mivel az ortogonális transzformációk megtartják a belső szorzatot, így megőrzik a vektorok normáját és szögét is.

4.19. Tétel. *Ha egy $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris transzformáció megtartja a vektorok normáját (azaz tetszőleges $\underline{x} \in \mathbb{E}$ esetén $\|\varphi(\underline{x})\| = \|\underline{x}\|$), akkor ortogonális transzformáció.*

Bizonyítás. Ha φ normatartó, akkor $\|\varphi(\underline{x} + \underline{y})\| = \|\underline{x} + \underline{y}\|$ teljesül minden $\underline{x}, \underline{y} \in \mathbb{E}$ esetén, így

$$\|\varphi(\underline{x}+\underline{y})\|^2 = (\varphi(\underline{x}+\underline{y}), \varphi(\underline{x}+\underline{y})) = \underbrace{(\varphi(\underline{x}), \varphi(\underline{x}))}_{\|\varphi(\underline{x})\|^2} + 2(\varphi(\underline{x}), \varphi(\underline{y})) + \underbrace{(\varphi(\underline{y}), \varphi(\underline{y}))}_{\|\varphi(\underline{y})\|^2}$$

$$= \|\varphi(\underline{x})\|^2 + 2(\varphi(\underline{x}), \varphi(\underline{y})) + \|\varphi(\underline{y})\|^2 = \|\underline{x}\|^2 + 2(\varphi(\underline{x}), \varphi(\underline{y})) + \|\underline{y}\|^2$$

és

$$\|\varphi(\underline{x}+\underline{y})\|^2 = \|\underline{x}+\underline{y}\|^2 = (\underline{x}+\underline{y}, \underline{x}+\underline{y}) = \|\underline{x}\|^2 + 2(\underline{x}, \underline{y}) + \|\underline{y}\|^2$$

alapján $2(\varphi(\underline{x}), \varphi(\underline{y})) = 2(\underline{x}, \underline{y})$ adódik, így φ ortogonális. □

4.20. Tétel. *A $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris operátor akkor és csak akkor ortogonális transzformáció, ha ortonormált bázist ortonormált bázisba visz át.*

Bizonyítás. 1. Ha φ ortogonális transzformáció, akkor szögtartó és normatartó, tehát merőleges vektorokat merőleges vektorokba visz és normált vektorokat normált vektorokba.

2. Ha φ az $(e) = (\underline{e}_1, \ldots, \underline{e}_n)$ ortonormált bázist ortonormált bázisba viszi, akkor

$$(\underline{x}, \underline{y}) = \left(\sum_{i=1}^{n} x_i \underline{e}_i, \sum_{j=1}^{n} y_j \underline{e}_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \underbrace{(\underline{e}_i, \underline{e}_j)}_{\delta_{ij}} = \sum_{i=1}^{n} x_i y_i$$

és

$$\begin{aligned} (\varphi(\underline{x}), \varphi(\underline{y})) &= \left(\sum_{i=1}^{n} x_i \varphi(\underline{e}_i), \sum_{j=1}^{n} y_j \varphi(\underline{e}_j) \right) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \underbrace{(\varphi(\underline{e}_i), \varphi(\underline{e}_j))}_{\delta_{ij}} = \sum_{i=1}^{n} x_i y_i, \end{aligned}$$

tehát φ belsőszorzat-tartó, így ortogonális.

□

4.21. Következmény. A $\varphi : \mathbb{E} \to \mathbb{E}$ ortogonális lineáris operátor mátrixa reguláris.

Bizonyítás. Mivel ortogonális operátor bázist bázisba visz, így a $\varphi(\mathbb{E})$ képtér n-dimenziós lesz, tehát φ szürjektív. Ez ekvivalens azzal, hogy φ automorfizmus, és ekkor φ mátrixa reguláris. □

4.22. Tétel. *A $\varphi : \mathbb{E} \to \mathbb{E}$ lineáris operátor akkor és csak akkor ortogonális, ha $\varphi^* = \varphi^{-1}$.*

Bizonyítás. 1. Ha φ ortogonális transzformáció, akkor

$$(\underline{x}, \underline{y}) = (\varphi(\underline{x}), \varphi(\underline{y})) = (\underline{x}, \varphi^* \varphi(\underline{y}))$$

miatt $\mathrm{Id} = \varphi^* \varphi$, tehát $\varphi^* = \varphi^{-1}$.

2. Ha $\varphi^* = \varphi^{-1}$ teljesül, akkor

$$(\varphi(\underline{x}), \varphi(\underline{y})) = (\underline{x}, \underbrace{\varphi^*\varphi}_{\varphi^{-1}\varphi=\mathrm{Id}}(\underline{y})) = (\underline{x}, \underline{y}).$$

□

4.23. Következmény. Ha $\varphi : \mathbb{E} \to \mathbb{E}$ ortogonális operátor, akkor φ mátrixa az $\mathbb{E}$ egy tetszőleges ortonormált bázisában olyan, hogy $A^T = A^{-1}$. Az ilyen mátrixokat ortogonális mátrixoknak nevezzük. Ha φ mátrixa valamely ortonormált bázisban ortogonális, akkor φ ortogonális transzformáció.

4.24. Következmény. Ha a $\varphi : \mathbb{E} \to \mathbb{E}$ ortogonális operátor mátrixa valamely bázisban A, akkor $|\det A| = 1$.

Bizonyítás. Mivel hasonló mátrixok determinánsa megegyezik, így elegendő ortonormált bázis esetén bizonyítani az állítást. Ekkor $A^T = A^{-1}$ miatt $AA^T = E$, és

$$1 = \det E = \det(AA^T) = \det A \underbrace{\det A^T}_{\det A} = (\det A)^2.$$

□

4.25. Következmény. Ortogonális mátrix sor illetve oszlopvektorai ortonormált bázist alkotnak $\mathbb{R}^n$-ben.

Bizonyítás. Mivel $AA^T = E$, ezért $\sum_{k=1}^{n} a_{ik}a_{kj}^T = (\underline{a}_i, \underline{a}_j) = \delta_{ij}$, tehát az A mátrix sorvektorai egymásra merőleges egységhosszú vektorok. □

4.26. Példa. $\mathbb{R}^2$-ben az origó körüli α szögű forgatás mátrixa egy ortogonális mátrix:

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

4.27. Következmény. Ortogonális operátor inverze is ortogonális.

Bizonyítás. Legyen a φ ortogonális operátor mátrixa valamely ortonormált bázisban A. Ekkor $A^T = A^{-1}$, ezért $(A^T)^{-1} = (A^{-1})^{-1}$, tehát $(A^{-1})^T = (A^{-1})^{-1}$. Mivel φ^{-1} mátrixa ortogonális mátrix, így φ^{-1} ortogonális operátor. □

4.28. Következmény. Ha a $H \subset \mathbb{E}$ altér invariáns altere a $\varphi : \mathbb{E} \to \mathbb{E}$ ortogonális operátornak, akkor $H^\perp$ is invariáns altér.

Bizonyítás. Legyen $\underline{y} \in H^\perp$. Ekkor $\underline{h} \perp \underline{y}$ teljesül vagyis $(\underline{y}, \underline{h}) = (\varphi(\underline{y}), \varphi(\underline{h})) = 0$ minden $\underline{h} \in H$ esetén. Mivel H invariáns altér volt és φ automorfizmus, így $\varphi(H) = H$, tehát $\varphi(\underline{y})$ merőleges a H altér minden vektorára, azaz $\varphi(\underline{y}) \in H^\perp$. □

4.29. Tétel. *Legyen $\varphi : \mathbb{E} \to \mathbb{E}$ az n-dimenziós $\mathbb{E}$ Euklideszi tér ortognális operátora. Ekkor $\mathbb{E}$-ben létezik olyan ortonormált bázis, amelyben φ mátrixának szerkezete az alábbi:*

$$\begin{pmatrix}
1 & \dots & 0 & & & & & & & \\
\vdots & \ddots & \vdots & & & & & & & \\
0 & \dots & 1 & & & & & & & \\
 & & & -1 & \dots & 0 & & & & \\
 & & & \vdots & \ddots & \vdots & & & & \\
 & & & 0 & \dots & -1 & & & & \\
 & & & & & & \cos\alpha_1 & -\sin\alpha_1 & & \\
 & & & & & & \sin\alpha_1 & \cos\alpha_1 & & \\
 & & & & & & & & \ddots & \\
 & & & & & & & & \cos\alpha_k & -\sin\alpha_k \\
 & & & & & & & & \sin\alpha_k & \cos\alpha_k
\end{pmatrix}.$$

4.30. Megjegyzés. Az ortogonális transzformációk mátrixának fenti alakja azt jelenti, hogy $\mathbb{E}$ 1 illetve 2-dimenziós invariáns alterek direkt összegére bomlik, és φ az 1-dimenziós alterekben (+1)-el vagy (-1)-el való szorzásként hat, a 2-dimenziós alterekben pedig origó körüli forgatásként.

4.31. Példa. 1. Ha $\mathbb{E}$ 1-dimenziós Euklideszi tér, $\underline{e} \in \mathbb{E}$ egy normált vektor és φ ortogonális transzformáció $\mathbb{E}$-n, akkor $1 = \|\underline{e}\| = \|\varphi(\underline{e})\|$ miatt $\varphi(\underline{e}) = \pm\underline{e}$. Ekkor

$$\varphi(\underline{x}) = \varphi(x\underline{e}) = x\varphi(\underline{e}) = \pm x\underline{e} = \pm\underline{x},$$

tehát φ vagy (+1)-el vagy (-1)-el való szorzás.

2. Ha $\mathbb{E}$ 2-dimenziós Euklideszi tér és a $\varphi : \mathbb{E} \to \mathbb{E}$ ortogonális operátor mátrixa egy ortonormált bázisban A, akkor $AA^T = E$ miatt

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

vagyis

$$a_{11}^2 + a_{12}^2 = 1 \quad a_{21}^2 + a_{22}^2 = 1$$

$$a_{11}a_{21} + a_{12}a_{22} = 0 \quad a_{21}a_{11} + a_{22}a_{12} = 0$$

adódik. Ennel az egyenletrendszernek kétféle mátrix tesz eleget:

$$A_1 = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \qquad A_2 = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}.$$

Az első esetben origó körüli α szögű forgatást kapunk, de a második esetben A_2 szimmetrikus mátrix, tehát φ önadjungált leképezés. Ekkor A_2 diagonalizálható és a főátlóban a sajátértékek fognak szerepelni, ezek ebben az esetben (+1)-ek vagy (-1)-ek lehetnek:

$$A_2 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \quad \text{ahol} \quad \lambda_1 = \pm 1 \ \ , \lambda_2 = \pm 1 \ .$$

5. Unitér terek lineáris operátorai

5.1. Megjegyzés. Mivel az Unitér terek lineáris operátorainak elmélete sok szempontból hasonló az Euklideszi tereken adott lineáris transzformációk elméletével, így ebben a fejezetben csak néhány eltérésre hívjuk fel a figyelmet.

5.2. Tétel. *Ha az $\mathbb{U}$ unitér téren adott $\varphi : \mathbb{U} \to \mathbb{U}$ lineáris operátor mátrixa egy ortonormált bázisban A, akkor φ^* mátrixa: $A^* = \overline{A^T}$.*

Bizonyítás. Legyen az $\mathbb{U}$ Euklideszi térnek $(e) = (\underline{e}_1, \ldots, \underline{e}_n)$ egy ortonormált bázisa és ebben a bázisban φ mátrixa $A = (a_{ij})$ és φ^* mátrixa $A^* = (a^*_{ij})$. Ekkor $\varphi(\underline{e}_i) = \sum_{k=1}^{n} a_{ik}\underline{e}_k$, így

$$(\varphi(\underline{e}_i), \underline{e}_j) = \left(\sum_{k=1}^{n} a_{ik}\underline{e}_k, \underline{e}_j \right) = \sum_{k=1}^{n} a_{ik} \underbrace{(\underline{e}_k, \underline{e}_j)}_{\delta_{kj}} = a_{ij},$$

$$(\underline{e}_i, \varphi^*(\underline{e}_j)) = \left(\underline{e}_i, \sum_{k=1}^{n} a^*_{jk}\underline{e}_k \right) = \sum_{k=1}^{n} \overline{a^*_{jk}} \underbrace{(\underline{e}_i, \underline{e}_k)}_{\delta_{ki}} = \overline{a^*_{ji}}.$$

Innen $a_{ij} = \overline{a^*_{ji}}$, tehát $A^* = \overline{A^T}$ szükséges. □

5.3. Definíció. A $\varphi : \mathbb{U} \to \mathbb{U}$ lineáris operátort *önadjungált*nak vagy *Hermite-félének* nevezzük, ha $\varphi = \varphi^*$.

5.4. Tétel. *A $\varphi : \mathbb{U} \to \mathbb{U}$ önadjungált operátor sajátértékei valósak.*

Bizonyítás. Legyen λ sajátértéke φ-nek, és $\underline{x}$ egy λ-hoz tartozó sajátvektor. Ekkor

$$\lambda(\underline{x},\underline{x}) = (\lambda\underline{x},\underline{x}) = (\varphi(\underline{x}),\underline{x}) = (\underline{x},\varphi^*(\underline{x})) =$$
$$(\underline{x},\varphi(\underline{x})) = (\underline{x},\lambda\underline{x}) = \overline{\lambda}(\underline{x},\underline{x}),$$

ahonnan $(\underline{x},\underline{x}) \neq 0$ miatt $\lambda = \overline{\lambda}$ következik, tehát λ valós szám. □

5.5. Következmény. Minden Unitér téren értelmezett önadjungált operátor esetén létezik olyan ortonormált bázis, amelyben az operátor mátrixa diagonális alakú, és a főátlóban valós számok szerepelnek.

5.6. Definíció. A $\varphi : \mathbb{U} \to \mathbb{U}$ lineáris operátort *unitér*nek nevezük, ha $\varphi^* = \varphi^{-1}$.

5.7. Definíció. A $\varphi : \mathbb{U} \to \mathbb{U}$ lineáris operátort *normális*nak nevezzük, ha $\varphi^* \circ \varphi = \varphi \circ \varphi^*$, azaz ha φ és φ^* felcserélhető.

5.8. Következmény. Ha egy operátor önadjungált, akkor normális. Ha egy operátor unitér, akkor normális. Megfordítva nem igaz.

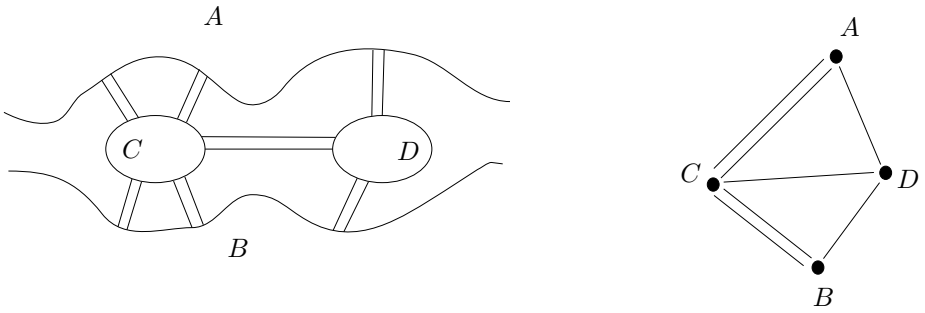
5.9. Tétel. *Minden $\varphi : \mathbb{U} \to \mathbb{U}$ normális operátor esetén létezik $\mathbb{E}$-nek olyan ortonormált bázisa, amelyben φ mátrixa diagonális.*

5.10. Megjegyzés. Unitér téren értelmezett normális operátor esetén létezik ortonormált bázis, amelyben a transzformáció mátrixa diagonális alakú. Ha az operátor önadjungált is, akkor a főátlóban valós számok szerepelnek, ha pedig unitér, akkor a főátlóban szereplő sajátértékek abszolút értéke 1.

2. fejezet
Gráfelmélet

1. Gráfelméleti alapfogalmak

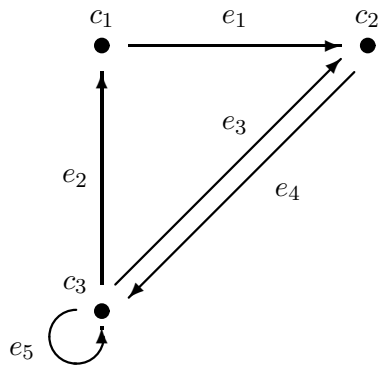
1.1. Megjegyzés. A gráfelmélet megszületése Euler nevéhez köthetô, aki 1736-ban vetette fel illetve oldotta meg a königsbergi hidak problémáját. A kérdés az volt, hogy be lehet-e járni a königsbergi Pregel folyóban lévő két szigetet a partokkal és egymással összekötő hidakat úgy, hogy mindegyikre csak egyszer lépünk rá és visszatérünk a kiindulási pontra.



1.2. Definíció. Legyenek E és $C \neq \emptyset$ diszjunkt halmazok, és legyen $\varphi : E \to C \times C$ leképezés. Ekkor a $G = (E, \varphi, C)$ hármast *irányított gráf*nak nevezzük. E-t a *gráf éle*inek nevezzük, C-t a *gráf csúcsa*inak. A $G = (E, \varphi, C)$ gráfot *véges*nek nevezzük, ha $|E|$ és $|C|$ véges ($|E|$ az E halmaz számosságát jelöli).

1.3. Példa. Legyen a $G = (E, \varphi, C)$ gráf esetén $E = \{e_1, e_2, e_3, e_4, e_5\}$, $C = \{c_1, c_2, c_3\}$ és φ az élekhez rendelje az alábbi csúcspárokat:

$$\varphi(e_1) = (c_1, c_2),$$
$$\varphi(e_2) = (c_3, c_1),$$
$$\varphi(e_3) = (c_3, c_2),$$
$$\varphi(e_4) = (c_2, c_3),$$
$$\varphi(e_5) = (c_3, c_3).$$



1.4. Definíció. A $G' = (E', \varphi', C')$ gráfot a $G = (E, \varphi, C)$ gráf *részgráf*jának nevezzük, ha

1. $E' \subset E$ és $C' \subset C$,
2. minden $e \in E'$ esetén $\varphi'(e) = \varphi(e)$.

1.5. Definíció. Ha a $G = (E, \varphi, C)$ gráfban $\varphi(e) = (c, c)$, akkor e-t it hurokélnek nevezzük.

1.6. Definíció. Ha a $G = (E, \varphi, C)$ gráfban $\varphi(e_1) = (c_1, c_2)$ és $\varphi(e_2) = (c_1, c_2)$, akkor azt mondjuk, hogy e_1 és e_2 *szigorúan párhuzamos élek*.

1.7. Definíció. Ha a $G = (E, \varphi, C)$ gráfban $\varphi(e_1) = (c_1, c_2)$, és $\varphi(e_2) = (c_2, c_1)$, akkor e_1 és e_2 párhuzamos élek.

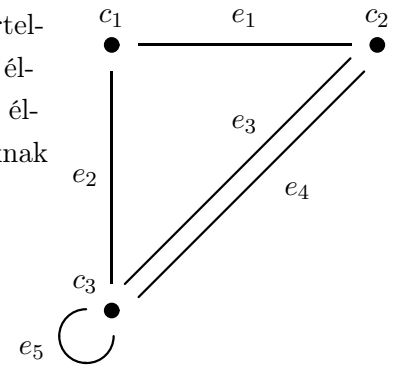
1.8. Példa. Az 1.3. példában szereplő gráf esetén e_5 egy hurokél, e_3 és e_4 pedig párhuzamos élek, de nem szigorúan párhuzamosak.

1.9. Definíció. Jelölje $C * C$ a C-beli elemekből álló rendezetlen párok halmazát:

$$C * C = \{(c_1, c_2) \mid c_1, c_2 \in C \text{ és a sorrend nem számít}\} .$$

Ha E egy halmaz, C egy nem üres halmaz és $\varphi : E \to C * C$, akkor a $G = (E, \varphi, C)$ hármast *irányítatlan gráf*nak nevezzük.

1.10. Megjegyzés. A hurokél definíciója irányítatlan gráfoknál ugyanaz, mint irányított gráfoknál, de a párhuzamosság és a szigorú párhuzamosság között nincs értelme különbséget tenni. Ilyenkor többszörös élről vagy multiélről beszélünk, a többszörös éleket tartalmazó gráfokat pedig multigráfoknak nevezzük:



$$\varphi(e_1) = (c_1, c_2), \qquad \varphi(e_2) = (c_1, c_3),$$
$$\varphi(e_3) = (c_2, c_3), \qquad \varphi(e_4) = (c_2, c_3),$$
$$\varphi(e_5) = (c_3, c_3).$$

1.11. Definíció. A $G = (E, \varphi, C)$ gráfot *egyszerű gráf*nak nevezzük, ha sem párhuzamos éleket, sem hurokéleket nem tartalmaz.

1.12. Definíció. Ha egy gráf nem tartalmaz egyetlen élt sem, akkor *üres-gráf*nak nevezzük.

1.13. Definíció. A $G = (E, \varphi, C)$ gráf $c \in C$ *csúcsának a fokán* a csúcsra illeszkedő élek számát értjük, jele: $\delta(c)$. (A hurokéleket kétszeresen számoljuk.)

1.14. Tétel. *Kézfogási tétel. Egy $G = (E, \varphi, C)$ véges gráf esetén a csúcsok fokszámainak összege egyenlő az élek számának kétszeresével:*

$$\sum_{c \in C} \delta(c) = 2|E|.$$

Bizonyítás. Mivel minden él pontosan két csúcsra illeszkedik, így a fokszámok összegzésénél minden élt kétszer számolunk. □

1.15. Következmény. A $G = (E, \varphi, C)$ véges gráf páratlan fokszámú csúcsainak a száma páros.

Bizonyítás. A kézfogási tétel szerint

$$\underbrace{2|E|}_{\text{páros}} = \sum_{c \in C} \delta(c) = \underbrace{\sum_{\substack{c \in C \\ \delta(c) \text{ páros}}} \delta(c)}_{\text{páros}} + \sum_{\substack{c \in C \\ \delta(c) \text{ páratlan}}} \delta(c),$$

így a páratlan fokú csúcsok fokszámainak összege is páros. Ez csak akkor lehetséges, ha páros sok ilyen csúcs van. □

1.16. Definíció. Egy $G = (E, \varphi, C)$ gráf $e_1, \ldots, e_n \in E$ élsorozatát *törött-vonal*nak nevezzük, ha

$$\varphi(e_1) = (c_0, c_1),\ \varphi(e_2) = (c_1, c_2), \ldots,\ \varphi(e_n) = (c_{n-1}, c_n).$$

1.17. Definíció. Ha a $G = (E, \varphi, C)$ gráf egy töröttvonalában a csúcsok mind különbözőek, akkor ezt a töröttvonalat *út*nak nevezzük. Irányított gráf esetén irányított útról beszélünk.

1.18. Definíció. Legyen a $G = (E, \varphi, C)$ gráfban $e_1, \ldots, e_n \in E$ egy töröttvonal, ahol $\varphi(e_1) = (c_0, c_1), \ldots\ \varphi(e_n) = (c_{n-1}, c_n)$. Ezt a töröttvonalat *kör*nek nevezzük, ha $c_1, \ldots, c_{n-1}, c_n$ mind különbözőek, de $c_0 = c_n$.

1.19. Definíció. Egy $G = (E, \varphi, C)$ gráf útjának a *hossz*a alatt az útban szereplő élek számát értjük.

1.20. Definíció. A c_i, c_j csúcsok *távolság*án az őket összekötő utak hosszainak minimumát értjük. Jele: $d(c_i, c_j)$.

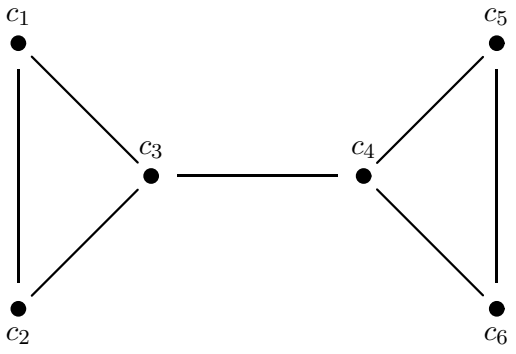
Ha két csúcsot nem köt össze út, akkor azt mondjuk, hogy a távolságuk végtelen.

1.21. Definíció. Egy $G = (E, \varphi, C)$ *gráf átmérője* a csúcsok távolságának maximuma:

$$\operatorname{diam}(G) = \max_{c_i, c_j \in C} d(c_i, c_j).$$

1.22. Példa. Az alábbi gráf átmérője:

$$\operatorname{diam}(G) = \max_{c_i, c_j \in C} d(c_i, c_j) =$$
$$d(c_1, c_6) = d(c_1, c_5) =$$
$$d(c_2, c_5) = d(c_2, c_6) = 3.$$



1.23. Definíció. A $G = (E, \varphi, C)$ gráfot *összefüggő*nek nevezzük, ha minden csúcsából minden csúcsába vezet út.

1.24. Tétel. *Egy $G = (E, \varphi, C)$ összefüggő gráf esetén C metrikus tér a d távolságfogalommal.*

1.25. Definíció. A $G = (E, \varphi, C)$ gráf $G' = (E', \varphi', C')$ részgráfját *komponens*nek nevezzük, ha

1. G' összefüggő,
2. G-ben nem létezik olyan G'' összfüggő részgráf, amelynek valódi részgráfja G',

tehát a maximális összefüggő részgráfok a komponensek.

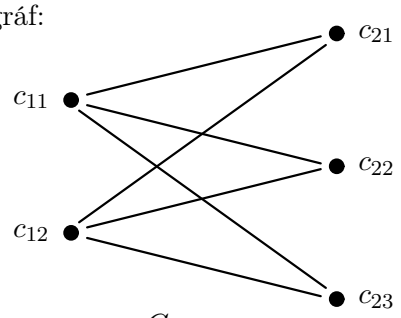
1.26. Definíció. Egy $G = (E, \varphi, C)$ egyszerű, összefüggő gráfot *fának* nevezünk, ha nem tartalmaz kört.

1.27. Definíció. Egy $G = (E, \varphi, C)$ gráfot *erdő*nek nevezünk, ha komponensei fák.

1.28. Tétel. *Minden fagráf tartalmaz legalább két elsőfokú csúcsot.*

1.29. Definíció. Egy $G = (E, \varphi, C)$ gráf *páros*, ha csúcsainak halmaza felbontható két olyan C_1, C_2 halmazra, amelyek diszjunktak, $C_1 \cup C_2 = C$ és minden $e \in E$ él esetén ha $\varphi(e) = (c_1, c_2)$, akkor $c_1 \in C_1$ és $c_2 \in C_2$.

1.30. Példa. Páros gráf:



ahol c_{11}, $c_{12} \in C_1$, c_{21}, c_{22}, $c_{23} \in C_2$.

1.31. Tétel. *Egy $G = (E, \varphi, C)$ gráf akkor és csak akkor páros, ha nem tartalmaz páratlan hosszúságú kört.*

1.32. Tétel. *Ha a $G = (E, \varphi, C)$ gráf fa, akkor*

$$|C| - 1 = |E|.$$

1.33. Következmény. Ha a $G = (E, \varphi, C)$ gráf erdő, és k darab komponensből áll, akkor

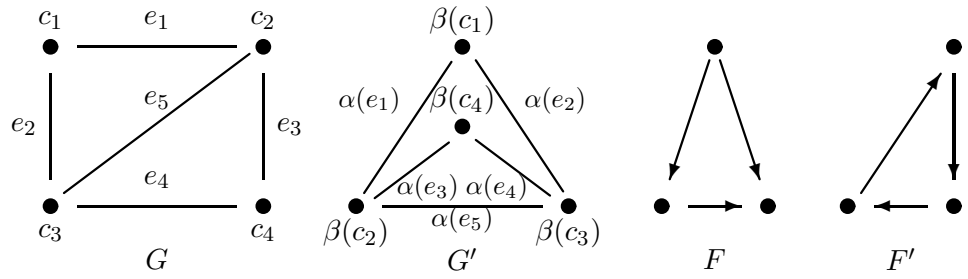
$$|C| - k = |E|.$$

1.34. Definíció. A $G = (E, \varphi, C)$ és a $G' = (E', \varphi', C')$ gráfok *izomorf*ak egymással, ha

1. létezik $\alpha : E \to E'$ bijektív leképezés,
2. létezik $\beta : C \to C'$ bijektív leképezés,

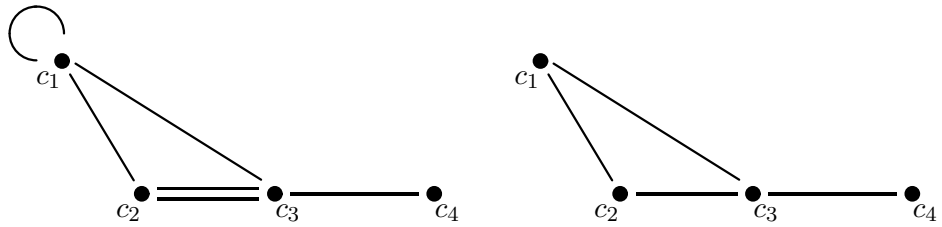
3. minden $e \in E$, $\varphi(e) = (c_1, c_2)$ esetén $\varphi'(\alpha(e)) = (\beta(c_1), \beta(c_2))$.

1.35. Példa. A G és a G' gráf izomorf, de az F és az F' gráfok nem izomorfak:



1.36. Definíció. A $G = (E, \varphi, C)$ gráfnak a G' fagráf a *feszítőfája*, ha G' részgráfja G-nek, és G minden csúcsa G'-nek is csúcsa.

1.37. Példa. Gráf és feszítőfája:



1.38. Tétel. *Egy G gráfnak akkor és csak akkor létezik feszítőfája, ha összefüggő.*

1.39. Definíció. Egy $G = (E, \varphi, C)$ irányított gráfnak a $c \in C$ csúcs a *gyökere*, ha c-ből G minden csúcsába el lehet jutni irányított út mentén.

1.40. Definíció. A G irányított gráfot *irányított fá*nak nevezzük, ha G fa és van egy gyökere.

1.41. Definíció. Egy $G = (E, \varphi, C)$ egyszerű gráfot *n-szögpontú teljes gráf*nak nevezünk, ha bármely két különböző csúcsát él köti össze, és $|C| = n$. Jele: T^n vagy K^n.

1.42. Tétel. *A T^n n-szögpontú teljes gráf éleinek száma* $\dfrac{n(n-1)}{2}$.

1.43. Definíció. A $G = (E, \varphi, C)$ egyszerű gráf *komplementergráf*ja az a gráf, amely G-t teljes gráffá egészíti ki.

Tehát ha $|C| = n$, és tekintjük azt a T^n teljes gráfot amelynek részgráfja G, akkor T^n-ből törölve G éleit megkapjuk a G komplementetgráfját.

1.44. Definíció. Legyen $G = (E, \varphi, C)$ gráf és $\{G_1, \ldots, G_n\}$ a G részgráfjainak egy halmaza. Azt mondjuk, hogy $\{G_1, \ldots, G_n\}$ a G-nek egy *fedés*e, ha a G valamennyi csúcsa és éle szerepel a $G_1, .., G_n$ részgráfok valamelyikében.

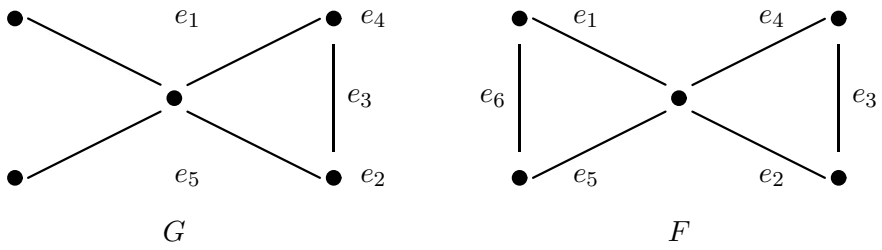
1.45. Definíció. Ha a $G = (E, \varphi, C)$ gráf $\{G_1, \ldots, G_n\}$ fedésének egyetlen részhalmaza sem fedés, akkor *minimális fedés*nek nevezzük.

2. Euler-kör, Euler-vonal, Hamilton-kör

2.1. Definíció. Egy $G = (E, \varphi, C)$ gráf $e_1, \ldots, e_n$ élsorozatát *Euler-vonal*nak nevezzük, ha E minden élét pontosan egyszer tartalmazza.

Ha $\varphi(e_1) = (c_0, c_1), \ldots, \varphi(e_n) = (c_{n-1}, c_n)$ esetén $c_0 = c_1$, akkor zárt Euler-vonalról beszélünk, ellenkező esetben nyílt Euler-vonalról.

2.2. Példa. A G gráfban $\{e_1, e_2, e_3, e_4, e_5\}$ egy nyílt Euler-vonal, míg az F gráfban $\{e_1, e_2, e_3, e_4, e_5, e_6\}$ egy zárt Euler-vonal:



2.3. Definíció. Egy G gráf *Euler-gráf*, ha van zárt Euler-vonala.

2.4. Tétel. *Egy G gráf akkor és csak akkor Euler-gráf, ha összefüggő, és minden csúcsának a foka páros.*

2.5. Definíció. Legyen $G = (E, \varphi, C)$ gráf. Ennek egy $H = \Big(\varphi(e_1) = (c_0, c_1), \ldots, \varphi(e_n) = (c_{n-1}, c_n)\Big)$ útja *Hamilton-út*, ha a $c_0, \ldots, c_n$ csúcsok mind különbözőek, és G-nek nincs más csúcspontja ezeken kívül.

2.6. Definíció. A $G = (E, \varphi, C)$ gráf K körét *Hamilton-kör*nek nevezzük, ha K tartalmazza G minden csúcsát.

2.7. Tétel. *Ha egy G egyszerű gráfban minden csúcspont foka legalá'bb $k \geq 2$, akkor van a gráfban egy legalább $k + 1$ hosszúságú kör.*

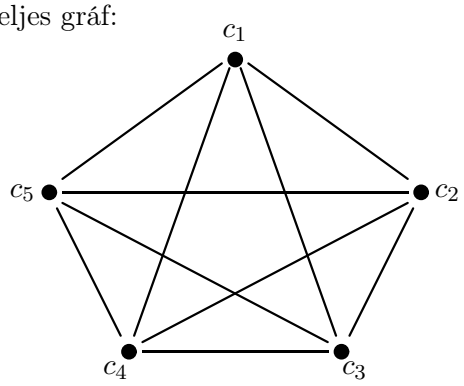
2.8. Tétel. *Ha a $G = (E, \varphi, C)$ egyszerű gráf minden $c \in C$ csúcsára fennáll, hogy $\delta(c) \geq \dfrac{|C|}{2}$, akkor a gráf összefüggő.*

2.9. Definíció. Egy $G = (E, \varphi, C)$ gráf esetén az élek halmazának $|E|$ számosságát a G méretének nevezzük, a csúcsok $|C|$ számosságát pedig a G gráf rendjének nevezzük.

2.10. Definíció. Egy élen fekvő két csúcsot *szomszédos csúcs*nak nevezünk, tehát ha $\varphi(e) = (c_1, c_2)$, akkor c_1 és c_2 szomszédos csúcsok.

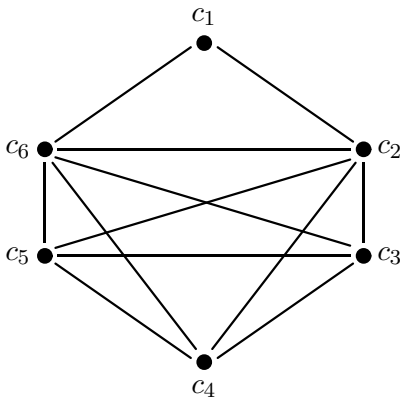
2.11. Definíció. Egy egyszerű gráf *teljes gráf*, ha bármely két csúcsa szomszédos.

2.12. Példa. Teljes gráf:



2.13. Tétel (Ore tétel). *Ha egy $G = (E, \varphi, C)$ gráf rendje nagyobb mint 2 és bármely két nem szomszédos c_i, c_j csúcspont fokának az összege nagyobb vagy egyenlő mint G rendje, akkor G-nek van Hamilton köre.*

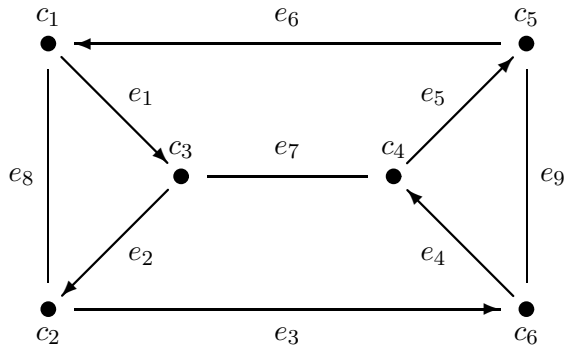
2.14. Példa. Az alábbi gráf nem teljesíti Ore tételét:



2.15. Tétel (Dirac tétel). *Ha az $n = 2k$ csúcspontú egyszerű gráf bármely csúcsának a foka legalább k, akkor G-nek van Hamilton köre.*

2.16. Megjegyzés. A Hamilton-körök megkeresésének problémájával rokon területe a kombinatórikus optimalizálásnak az úgynevezett utazó ügynök problémája. Itt egy ügynöknek minimális költséggel kell bejárnia bizonyos városokat. Ha a városokat csúcsoknak tekintjük, a városokat összekötő utak lesznek a gráf élei, és minden élhez hozzárendeljük az adott út megtételének a költségét, akkor a feladat egy olyan Hamilton-kör keresése, amely mentén a költségek összege minimális.

2.17. Példa. Az alábbi gráf rendje 6, és minden csúcsának a foka 3, ezért Dirac tétele szerint van Hamilton-köre:



Például a $H = (e_1, e_2, e_3, e_4, e_5, e_6)$ kör egy Hamilton kör, hiszen minden csúcs pontosan egyszer szerepel benne: $\varphi(e_1) = (c_1, c_3)$, $\varphi(e_2) = (c_3, c_2)$, $\varphi(e_3) = (c_2, c_6)$, $\varphi(e_4) = (c_6, c_4)$, $\varphi(e_5) = (c_4, c_5)$, $\varphi(e_6) = (c_5, c_1)$.

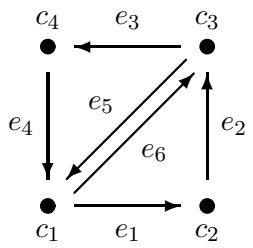
3. Gráfok csúcsmátrixa

3.1. Definíció. Legyen $G = (E, \varphi, C)$ irányított gráf és $|C| = n$. A G *csúcsmátrix*a az az $A = (a_{ij}) \in M_{n\times n}$ mátrix, melynek a_{ij} általános eleme egyenlő a c_i csúcsból a c_j csúcsba vezető élek számával.

3.2. Tétel. *Legyen $A \in M_{n\times n}$ a G gráf csúcsmátrixa. Az A mátrix l-edik hatványának $(A^l)_{ij}$ általános eleme megadja a c_i csúcsból a c_j csúcsba vezető l hosszúságú töröttvonalak számát.*

3.3. Példa.

A következő gráf csúcsmátrixnak harmadik hatványa megadja, hogy egyik csúcsból a másikba hányféleképpen lehet eljutni 3 élen végighaladva:



$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad A^2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad A^3 = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Például c_3 csúcsból c_3 csúcsba vezető 3 hosszúságú töröttvonalak: (e_3, e_4, e_6) és (e_5, e_1, e_2).

3.4. Lemma. *Egy $G = (E, \varphi, C)$ irányított, véges gráf pontosan akkor tartalmaz legalább $|C|$ hosszúságú irányított töröttvonalat, ha G-ben van irányított kör.*

3.5. Következmény. Egy $G = (E, \varphi, C)$ véges, irányított gráf pontosan akkor tartalmaz kört, ha G csúcsmátrixának $|C| = n$-edik hatványa nem azonosan nulla.

3.6. Tétel. *A $G = (E, \varphi, C)$ gráf $c_i, c_j \in C$ csúcsainak $l = d(c_i, c_j)$ távolsága az a legkisebb l szám, amelyre $(A^l)_{ij} \neq 0$.*

3.7. Definíció. Ha $G(E, \varphi, C)$ gráfhoz adott egy olyan f leképezés, amely minden élhez egy valós számot rendel, akkor a $G(E, \varphi, C, f)$ egy *súlyozott gráf*, és $f(e)$ az e él súlya.

3.8. Megjegyzés (A legrövidebb út problémája). Legyen adott a $G(E, \varphi, C, f)$ súlyozott egyszerű gráf, ahol valamennyi $e \in E$-re $f(e) > 0$. A gráf két különböző c_i és c_j csúcsai közötti legrövidebb utat keressük, vagyis azt a c_i-ből c_j-be vezető utat, amelyre az élek súlyának összege minimális. Abban az esetben ha az élek súlya s, akkor a két csúcs közötti legrövidebb utat, ha az létezik, a csúcsmátrixból kiszámíthatjuk.

Legyenek a G gráf csúcsai $c_1, c_2, \ldots, c_n$ és a csúcsmátrix az $A = (a_{ij})$.

3.9. Tétel. *A c_i csúcsból a c_j $(i \neq j)$ csúcsba akkor vezet egy k hosszúságú legrövidebb út, ha $a_{ij}^k \neq 0$ és $a_{ij}^l = 0$, ahol $l = 0, 1, 2, \ldots, k-1$.*

A 3.3. példa esetén láthatjuk, hogy c_1-ből c_4-be van 2 hosszúságú legrövidebb út.

3. fejezet
Kódelmélet

1. Kombinatórikus valószínűség

1.1. Megjegyzés. A természetben előforduló jelenségeket két csoportba soroljuk: a determinisztikus jelenségek kimenetele kikövetkeztethető, míg a sztochasztikus jelenségek kimenetele nem. A szochasztikus jelenségek közül az egyedi jelenségek csak egyszer fordulnak elő, a tömegjelenségek pedig akárhányszor bekövetkezhetnek. A valószínűségszámítás a véletlentől függő tömegjelenségek tudománya.

1.2. Definíció. Egy véletlen tömegjelenség megfigyelését *kísérlet*nek nevezzük, egy kísérlet lehetséges kimeneteleit pedig *esemény*eknek. Azokat az eseményeket amelyek mindig csak egyféleképpen következhetnek be, akárhányszor is végezzük el a kísérletet, *elemi esemény*eknek nevezzük.

1.3. Példa. Egy szabályos kockával való dobás esetén például esemény az, hogy páros számot dobunk, vagy, hogy 3-nál kisebbet dobunk. Elemi esemény például az, hogy 6-ost dobunk.

1.4. Megjegyzés. Tekintsük egy véletlen tömegjelenséggel kapcsolatban szóbajöhető események halmazát. Ezen halmaz elemeivel különböző műveleteket végezhetünk. A halmaz elemeit $A, B, C, \cdots$ −vel jelöljük.

1.5. Definíció. Az A és a B *események egyenlőek*, ha akárhányszor is végezzük el a kísérletet, vagy egyszerre következnek be, vagy egyszerre nem következnek be. Jele: $A = B$.

1.6. Definíció. Az események halmazának van két kitüntetett eseménye: a *lehetetlen esemény* olyan esemény amelyik sohasem következik be, jele: $\emptyset$, a *biztos esemény* olyan esemény amelyik mindig bekövetkezik, jele: I.

1.7. Definíció. Az A esemény *ellentett* vagy másképpen *komplementer esemény*e pontosan akkor következik be, ha A nem következik be. Jele: $\overline{A}$.

1.8. Definíció. Az A és a B események *összeg*én azt az eseményt értjük, amelyik pontosan akkor következik be, ha A és B közül legalább az egyik bekövetkezik. Jele: $A + B$.

1.9. Definíció. Az A és a B események *szorzat*án azt az eseményt értjük, amelyik pontosan akkor következik be, ha A és B együttesen következik be. Jele: $A \cdot B$.

1.10. Tétel. *Az események közötti műveletek rendelkeznek a következő tulajdonságokkal:*

1. $A + A = A,\ A \cdot A = A$,
2. $A + B = B + A,\ A \cdot B = B \cdot A$,
3. $A + (B + C) = (A + B) + C,\ A \cdot (B \cdot C) = (A \cdot B) \cdot C$,
4. $A + \emptyset = A,\ A \cdot \emptyset = \emptyset$,
5. $A + I = I,\ A \cdot I = A$,
6. $A + \overline{A} = I,\ A \cdot \overline{A} = \emptyset$,
7. $(A + B) \cdot C = A \cdot C + B \cdot C,\ A \cdot B + C = (A + C) \cdot (B + C)$,
8. $\overline{A + B} = \overline{A} \cdot \overline{B},\ \overline{A \cdot B} = \overline{A} + \overline{B}$.

Bizonyítás. Csak az 7. állítás második részét igazoljuk:

$$(A+C)\cdot(B+C) = (A+C)\cdot B+(A+C)\cdot C = A\cdot B+C\cdot B+A\cdot C+C\cdot C =$$
$$A\cdot B+C\cdot B+A\cdot C+C = A\cdot B+C\cdot B+C\cdot A+C\cdot I = A\cdot B+C\cdot B+C\cdot(A+I) =$$
$$A \cdot B + C \cdot B + C \cdot I = A \cdot B + C \cdot (B + I) = A \cdot B + C \cdot I = A \cdot B + C.$$

□

1.11. Definíció. Tekintsünk egy H nem üres halmazt, amelyet *eseménytér*nek nevezünk, elemeit pedig *elemi esemény*eknek. Tekintsük a H részhalmazainak egy olyan $\mathcal{A}$ rendszerét (az $\mathcal{A}$ elemeit eseményeknek nevezzük), amelyre teljesülnek a következők:

1. Ha $A \in \mathcal{A}$, akkor $\overline{A} \in \mathcal{A}$,
2. ha $A, B \in \mathcal{A}$, akkor $A \cdot B \in \mathcal{A}$ és $A + B \in A$,
3. $H \in \mathcal{A},\ \emptyset \in \mathcal{A}$.

Ekkor $\mathcal{A}$-t *eseményalgebrának* nevezzük.

1.12. Példa. A kockadobás kísérlete esetén legyen az eseménytér a $H = \{1, 2, 3, 4, 5, 6\}$ halmaz, ennek elemei az elemi események. Legyen $\mathcal{A} = P(H)$, tehát H összes részhalmazai az események. Például jelentse az A esemény azt, hogy páros számot dobunk, B pedig, hogy 3-nál kisebbet. Ezek az események azonosíthatóak az $A = \{2, 4, 6\}$ illetve $B = \{1, 2\}$ halmazokkal, tehát pontosan akkor fog az A esemény bekövetkezni, ha a kísérlet kimenetelének megfelelő elemi esemény (például 2-est dobunk) mint

halmazelem szerepel az A halmazban. Ekkor az $A+B$ esemény megfelel az $A \cup B = \{1,2,4,6\}$ halmaznak, az AB szorzatesemény pedig az $A \cap B = \{2\}$ metszethalmaznak. Az I biztos esemény megfelelője maga a H halmaz.

Az események és a halmazok közötti megfeleltés miatt a halmazelméleti alapfogalmaknál leírtak a megfelelő változtatásokkal átvihetők eseményalgebrákra is.

1.13. Tétel. *Egy véges eseményalgebrában (azaz a H eseménytér véges) bármely esemény a sorrendtől eltekintve egyértelműen állítható elő elemi események összegeként. Tehát ha $E_1, \dots, E_n$ az elemi események, akkor $E_i \cdot E_j = \emptyset$ ha $i \neq j$ és $E_1 + \dots + E_n = I$. Ekkor minden $A \in \mathcal{A}$ esetén az $A = E_{i_1} + \dots + E_{i_k}$ felírás a sorrendtől eltekintve egyértelmű.*

1.14. Definíció. Az $A_1, \dots, A_n \in \mathcal{A}$ események *teljes eseményrendszer*t alkotnak, ha páronként kizárják egymást (azaz bármely két különböző esemény szorzata a lehetetlen esemény) és összegük a biztos esemény, vagyis $A_1 + \dots + A_n = I$.

1.15. Definíció. Legyen $\mathcal{A}$ egy eseményalgebra és A egy esemény $\mathcal{A}$-ból. Végezzük el a kísérletet n-szer és számoljuk össze, hogy ebből hányszor következett be az A esemény. Ezt a k számot az A esemény *gyakoriság*ának nevezzük az adott kísérletre vonatkozóan, a $\dfrac{k}{n}$ hányadost pedig az A *relatív gyakoriság*ának.

1.16. Megjegyzés. Ha a kísérletek számát minden határon túl növelve azt tapasztaljuk, hogy a relatív gyakoriság értékei egy jól meghatározott számérték körül ingadoznak, akkor ezt a 0 és 1 közé eső számot fogjuk az esemény valószínűségének nevezni, ez a valószínűség tapasztalati megfogalmazása. A következő, matematikai definíció Kolmogorovtól származik.

1.17. Definíció. Legyen $\mathcal{A}$ egy eseményalgebra. Ezen eseményalgebra minden egyes A eseményéhez hozzárendelünk egy $P(A)$-val jelölt valós számot amely rendelkezik a következő tulajdonságokkal:

1. $0 \leq P(A) \leq 1$,
2. $P(H) = 1$,
3. ha $A_1, A_2 \dots \in \mathcal{A}$ és $A_i \cdot A_j = \emptyset$ $i \neq j$ esetén, akkor $\displaystyle\sum_{i=1}^{\infty} A_i \in \mathcal{A}$ és

$$P\left(\sum_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i).$$

Ekkor $P(A)$-t az A esemény *valószínűség*ének nevezzük. Egy olyan eseményalgebrát, amelynek minden A eleméhez hozzá van rendelve egy $P(A)$ szám a fenti tulajdonságokkal, *valószínűségi algebrának* nevezzük. Ha az eseményalgebra véges, akkor a valószínűségi algebrát is *véges*nek nevezzük.

1.18. Definíció. Az olyan véges valószínűségi algebrát, amelyben az elemi események egyenlő valószínűséggel bírnak *klasszikus* valószínűségi algebrának nevezzük.

1.19. Tétel. *Klasszikus valószínűségi algebrában egy esemény valószínűségét úgy számíthatjuk ki, hogy az esemény szempontjából kedvező elemi események számát osztjuk az összes elemi esemény számával:*

$$P(A) = \frac{\textit{kedvező elemi események száma}}{\textit{összes elemi esemény száma}}.$$

Bizonyítás. Véges eseményalgebrában véges sok esemény van, amelyek teljes eseményrendszert alkotnak, azaz páronként kizárják egymást és összegük a biztos esemény.

Legyen A egy tetszőleges esemény, amely a valószínűségszámítás alaptételének értelmében előállítható elemi események összegeként:

$$A = E_{i_1} + \cdots + E_{i_k}.$$

Ekkor

$$P(A) = P(E_{i_1} + \cdots + E_{i_k}) = P(E_{i_1}) + \cdots + P(E_{i_k}).$$

Mivel $E_1 + \cdots + E_n = I$, így

$$1 = P(I) = P(E_1 + \cdots + E_n)$$

és a $P(E_i)$ valószínűségek egymással egyenlőek, ezért $P(E_i) = \dfrac{1}{n}$ minden $i \in \{1, \ldots, n\}$ esetén. Tehát

$$P(A) = P(E_{i_1}) + \cdots + P(E_{i_k}) = \frac{1}{n} + \cdots + \frac{1}{n} = \frac{k}{n}.$$

□

1.20. Példa. A fenti képletben szereplő számokat általában kombinatórikus úton határozzuk meg. Ha egy magyar kártyából három lapot húzunk, akkor az elemi események száma a lehetséges kártyalap-hármasok száma, tehát $\binom{32}{3}$, és minden elemi esemény valószínűsége $\dfrac{1}{\binom{32}{3}}$, tehát ez egy klasszikus

valószínűségi algebra. Ekkor annak az eseménynek a valószínűsége, hogy a három lap közül legalább egy zöld:

$$P = \frac{\text{kedvező esetek száma}}{\text{összes esetek száma}} = \frac{\binom{8}{1}\binom{24}{2} + \binom{8}{2}\binom{24}{1} + \binom{8}{3}\binom{24}{0}}{\binom{32}{3}} = 0,59.$$

1.21. Definíció. Legyen B egy pozitív valószínűségű esemény, továbbá A egy tetszőleges esemény. Ekkor az A eseménynek B-re mint feltételre vonatkozó *feltételes valószínűség*en a

$$P(A|B) \doteq \frac{P(A \cdot B)}{P(B)}$$

valószínűséget értjük.

1.22. Tétel (Valószínűségek szorzástétele). *Legyen B egy pozitív valószínűségű esemény és A egy tetszőleges esemény. Ekkor*

$$P(A \cdot B) = P(A|B)P(B).$$

1.23. Definíció. Az A és B eseményeket *független*nek nevezzük, ha

$$P(A \cdot B) = P(A)P(B).$$

1.24. Tétel (Teljes valószínűség tétele). *Alkossanak az $A_1, \ldots, A_n$ események egy teljes eseményrendszert, azaz $A_i \cdot A_j = \emptyset$ ha $i \neq j$ és $\sum_{i=1}^{n} A_i = I$. Legyen B egy tetszőleges esemény. Ekkor*

$$P(B) = \sum_{i=1}^{n} P(B|A_i)P(A_i).$$

1.25. Tétel (Bayes tétele). *A teljes valószínűség tételének feltételei mellett:*

$$P(A_i|B) = \frac{P(B|A_i)P(A_i)}{\sum_{j=1}^{n} P(B|A_j)P(A_j)}.$$

1.26. Tétel (Nagy számok Bernoulli-féle törvénye). *(Kapcsolat a relatív gyakoriság és a valószínűség között) Annak a valószínűsége, hogy a relatív gyakoriságnak az esemény valószínűségétől vett eltérése egy tetszőlegesen kicsiny $\varepsilon > 0$ számnál nagyobb legyen, a nullához fog tartani, ha a*

kísérletek száma tart a végtelenhez:

$$P\left(\left|\frac{k}{n} - P(A)\right| > \varepsilon\right) \to 0, \qquad ha \quad n \to \infty.$$

1.27. Definíció. Ha egy H eseménytér elemi eseményeihez egy-egy valós számot rendelünk, így egy függvényt értelmezünk, amelyet *valószínűségi változó*nak nevezünk és ξ-vel jelölünk.

Ha a ξ valószínűségi változó megszámlalhatóan végtelen sok értéket vesz fel, akkor *diszkrét* valószínűségi változóról beszélünk. (Pl. a kockadobás esetén az elemi eseményeken a ξ valószínűségi változó az $1, 2, 3, 4, 5, 6$ értékeket veheti fel.)

A ξ valószínűségi változó *folytonos*, ha annak értékei az egész számegyeneshez, vagy annak egy részinterrvallumához tartoznak. (Egy folytonos valószínűségi változót a következő példában mutatunk be.)

1.28. Definíció. Legyen $\xi : H \to \mathbb{R}$ egy tetszőleges valószínűségi változó. Ekkor az $F : \mathbb{R} \to [0, 1]$ függvényt a ξ *eloszlásfüggvény*ének nevezzük, ahol

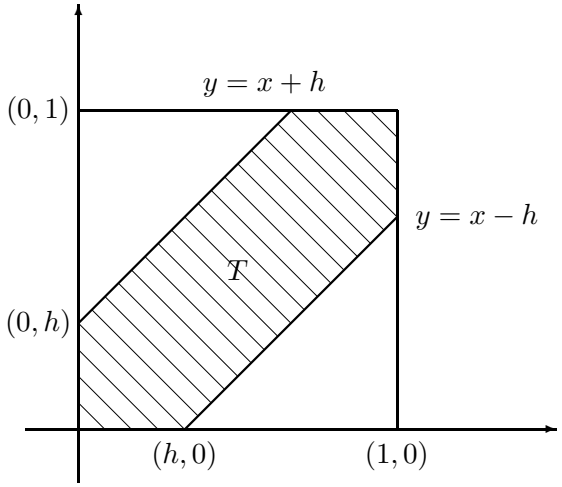
$$F(x) = P(\xi < x),$$

azaz F-nek az $x \in \mathbb{R}$ helyen felvett értéke megegyezik annak a valószínűségével, hogy a ξ valószínűségi változó x-nél kisebb értéket vesz fel.

1.29. Definíció. Ha egy kisérlethez tartozó események egy geometriai alakzat részhalmazainak feleltethetők meg úgy, hogy az egyes események valószínűsége az eseményhez rendelt részhalmaz geometriai mértékével arányos, akkor *geometriai valószínűség*ekről beszélünk.

1.30. Példa. Egy egységnyi hosszúságú szakaszon találomra kijelölünk két pontot. Mekkora a valószínűsége annak, hogy a köztük lévő távolság kisebb, mint egy adott h hossz, ahol $0 < h < 1$?

Jelölje a két pont távolságát a szakasz kezdőpontjától x és y. Ekkor az eseménytér teszőleges elemét azonosíthatjuk az egységnégyzet (x, y) koordinátájú pontjával. Annak valószínűségét keressük, hogy $|x - y| < h$, vagyis $y < x + h$ és $y > x - h$.



Ha az (x, y) koordinátájú pont a vonalazott részbe esik akkor teljesül, hogy $|x-y| < h$, ellenkező esetben pedig nem teljesül. így a keresett valószínűség a vonalazott rész területének és a négyzet teületének aránya:

$$P = \frac{T}{1} = \frac{1 - 2\dfrac{(1-h)^2}{2}}{1} = 1 - (1-h)^2 = 2h - h^2.$$

Legyen továbbá a ξ valószínűségi változó a két pont közötti távolság. Ekkor ξ eloszlásfüggvénye:

$$F_\xi(x) = P(\xi < x) = \begin{cases} 0 & \text{ha } x < 0 \\ 2x - x^2 & \text{ha } 0 \le x \le 1 \\ 1 & \text{ha } 1 < x \end{cases}.$$

Annak a valószínűsége, hogy a két pont távolsága legalább $\dfrac{3}{4}$:

$$P\left(\xi \ge \frac{3}{4}\right) = 1 - P\left(\xi < \frac{3}{4}\right) = 1 - \left(2 \cdot \frac{3}{4} - \left(\frac{3}{4}\right)^2\right) = \frac{1}{16}.$$

Az alábbiakban felsoroljuk a lefontosabb nevezetes diszkrét valószínűségi változókat.

1.31. Definíció. A ξ valószínűségi változó *binomiális eloszlás*ú, ha lehetséges értékei a $0, 1, \ldots, n$ számok és ezek közül a k-t a

$$P_k = \binom{n}{k} p^k (1-p)^{n-k}$$

valószínűséggel veszi fel, ahol $0 < p < 1$ az eloszlás paramétere.

1.32. Példa. Legyen $1 - p = 0,15$ annak a valószínűsége, hogy egy kosár almából hibásat választunk ki. Visszatevéssel egyenként véletlenszerűen válasszunk ki 20 darabot. Jelölje ξ a hibátlan almák számát, tehát ξ lehetséges értékei: $0, 1, \ldots, 20$, és ξ binomiális eloszlású lesz $p = 0,85$ paraméterrel. Ekkor annak a valószínűsége, hogy mind a 20 alma hibátlan lesz:

$$P(\xi = 20) = \binom{20}{20} \cdot 0,85^{20} \cdot 0,15^{0}.$$

1.33. Definíció. A ξ valószínűségi változó *hipergeometrikus eloszlás*ú, ha lehetséges értékei a $0, 1, \ldots, n$ számok és ezek közül a k-t a

$$P(\xi = k) = \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}}$$

valószínűséggel veszi fel.

1.34. Példa. $N = 100$-darab almából $M = 20$-darab férges. Visszatevés nélkül válasszunk ki $n = 10$-darabot. Ha ξ jelöli ezek közül a férges almák számát, akkor ξ hipergeometrikus eloszlású lesz, és annak a valószínűsége, hogy 5-darab férges alma lesz:

$$P(\xi = 5) = \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}} = \frac{\binom{20}{5}\binom{80}{5}}{\binom{100}{10}}.$$

1.35. Példa. Annak a valószínűsége, hogy egy lottószelvényen k-találatunk lesz:

$$P(\xi = k) = \frac{\binom{5}{k}\binom{85}{5-k}}{\binom{90}{5}}.$$

1.36. Definíció. A ξ valószínűségi változót λ paraméterű *Poisson eloszlás*únak nevezzük, ha lehetséges értékei a $0, 1, 2, \ldots$ számok, és ezek közül a k-val jelölt értéket a

$$P(\xi = k) = \frac{\lambda^k}{k!} \cdot e^{-\lambda}$$

valószínűséggel vesz fel.

2. Betű szerinti kódolás

Ebben a fejezetben röviden összefoglaljuk az információtovábbítás elméleti alapjait. Az első kódelméleti munkák az elmúlt század közepén jelentek meg (Claud Shannon (1948), Marcel Golay (1949), Richard Hamming (1950)).

Az információtovábbítás három fő eszközét különböztetjük meg: az adóberendezést, az információs csatornát és a vevőberendezést.

Mindenekelőtt tekintsünk egy úgynevezett kimeneti ábécét, amely lehet a magyar ábécé betűinek halmaza is. Jelölése: $A = \{a_1, \ldots, a_n\}$.

2.1. Definíció. Az $A = \{a_1, \ldots, a_n\}$ kimeneti ábécé jeleiből alkotott $a_{i_1}, \ldots, a_{i_k}$ sorozatokat *elsődleges közlés*nek nevezzük.

2.2. Megjegyzés. Az információs csatorna általában csak két különböző jeltipus továbbítását teszi lehetővé, és ezekhez a jelekhez a 0 és 1 számokat (az úgynevezett bináris kódokat) rendeljük hozzá. Az információtovábbítás folyamatában a következő lépéseket különböztetjük meg:

1. kódolás, vagyis az elsődleges közlés átalakítása bináris sorozattá,
2. modulálás, azaz a bináris sorozat átalakítása fizikai jelekké,
3. a fizikai jelek kiküldése az információs csatornára,
4. a fizikai jelek felfogása a vevőberendezésen,
5. demodulálás, vagyis a fizikai jelek visszaformálása bináris sorozattá,
6. dekódolás, azaz az elsődleges közlés előállítása a bináris sorozatból.

2.3. Definíció. Legyen $A = \{a_1, \ldots, a_n\}$ tetszőleges kimeneti ábécé, és legyen $K = \{\alpha_1, \ldots, \alpha_n\}$ véges hosszúságú bináris sorozatoknak valamilyen n-elmű halmaza. A kódolásnak azt a formáját, amelynél a kimeneti ábécé minden a_i betűjének egy $\alpha_i \in K$ bináris sorozatot feleltetünk meg, *betű szerinti kódolás*nak nevezzük.

2.4. Megjegyzés. Betű szerinti kódolásnál tetszőleges $a_{i_1}a_{i_2}\ldots a_{i_k}$ elsődleges közléshez egy $\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$ bináris sorozatot tudunk hozzárendelni.

2.5. Definíció. A K halmazt *kód*nak, az $\alpha_1, \ldots, \alpha_n$ elemeket *kódszavak*nak, a kódszavak tetszőleges sorozatát pedig *kódolt közlés*nek nevezzük.

A kódelméleti alapfogalmak és alaptételek tárgyalásánál alapvető munkaként használjuk az Irodalomjegyzék **[3]** könyvet.

2.6. Példa. Legyen $A = \{a, b, c, d\}$ a kimeneti ábécé, $K = \{00, 01, 100, 101\}$ pedig a kód. Ekkor a *dac* szó (elsődleges közlés) betű szerinti kódolása a 10100100 bináris sorozat.

2.7. Megjegyzés. összefoglalva elmondhatjuk, hogy a kódolási eljárás egy függvény: $H : A^* \to \{0,1\}^*$. (Itt *-al jelöltük a megfelelő halmazbeli elemek összes véges sorozatából álló halmazt.) A dekódoláshoz képezni kell a $H^{-1} : \{0,1\}^* \to A^*$ inverz függvényt. A H^{-1} függvény akkor és csak akkor létezik, ha H egy-egy értelmű, azaz különböző A^*-beli szavakhoz különböző kódolt közléseket rendel.

2.8. Példa. Az $A = \{a, b, c, d\}$ kimeneti ábécé esetén a $K = \{00, 01, 11, 0001\}$ kód nem egy-egy értelmű kódolást valósít meg, mivel az ab-hez és a d-hez ugyanaz a bináris sorozat tartozik.

3. Felbontható kódok

3.1. Definíció. A $K = \{\alpha_1, \ldots, \alpha_n\}$ kódot *felbontható*nak nevezzük, ha tetszőleges bináris sorozat legfeljebb egyféleképpen bontható kódszavak sorozatára.

3.2. Megjegyzés. Ha a K-beli kódszavak hossza mind egyenlő, akkor a K kód felbontható. (Egy kódszó hossza alatt a benne szereplő 0 és 1 számok számát értjük.)

3.3. Definíció. A K kódot *prefix kód*nak nevezzük, ha egyetlen kódszó sem valódi kezdőszelete egy másik kódszónak.

3.4. Példa. Azok a kódok amelyek egyenlő hosszúságú kódszavakból állnak prefix kódok. Prefix kód az $A = \{a, b, c, d\}$ kimeneti ábécéhez tartozó $K_1 = \{00, 01, 100, 101\}$ kód is, de nem prefix kód a $K = \{00, 10, 100, 101\}$.

3.5. Tétel. *Minden prefix kód felbontható.*

3.6. Tétel. *McMillan-egyenlőtlenség. Jelölje $l_1, \ldots, l_n$ rendre az $\alpha_1, \ldots, \alpha_n$ K-beli kódszavak hosszát. Ha a $K = \{\alpha_1, \ldots, \alpha_n\}$ kód felbontható, akkor*

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1.$$

3.7. Megjegyzés. Ez a McMillan egyenlőtlenség csak szükséges feltétele a felbonthatóságnak. Meg lehet adni olyan nem felbontható kódot, amely eleget tesz a fenti egyenlőtlenségnek, például az $A = \{a, b, c, d\}$ és $K = \{00, 01, 11, 0001\}$ pár is ilyen. Igaz viszont a következő:

3.8. Tétel. *Ha $\sum_{i=1}^{n} 2^{-l_i} \leq 1$, akkor létezik olyan $K = \{\alpha_1, \ldots, \alpha_n\}$ prefix kód, melyben a kódszavak hossza $l_1, \ldots, l_n$.*

3.9. Definíció. Két kódot ekvivalensnek nevezünk, ha ugyanannyi kódszót tartalmaznak, és kódszavaik megfeleltethetők úgy egymásnak, hogy a hosszuk páronként megegyezik.

3.10. Következmény. Tetszőleges felbontható kódhoz találhatunk vele ekvivalens prefix kódot.

4. Optimális kódok

Egy adott kimeneti ábécé esetén vannak olyan jelek, amelyek gyakrabban fordulnak elő az információtovábbításban, így ezekhez célszerű rövid kódszavakat hozzárendelni, míg a ritkábban előfordulókhoz hosszabb kódszavak is tartozhatnak.

Legyen F egy jelforrás, amely az $A = \{a_1, \ldots, a_n\}$ ábécé betűit véletlenszerűen bocsájtja ki, az egymás utáni jeleket egymástól függetlenül. Legyen p_i annak a valószínűsége, hogy az F által kibocsájtott jel a_i. A valószínűségekre teljesülnek a következők: $p_i \geq 0$, $(i = 1, \ldots, n)$ és $\sum_{i=1}^{n} p_i = 1$. Így a p_i azt mutatja meg, hogy egy M számú jelből álló jelsorozatot véve, a benne előforduló a_i jelek száma közelítőleg $p_i \cdot M$.

Adjunk meg egy $A = \{a_1, \ldots, a_n\}$ ábécét és egy hozzá tartozó $K = \{\alpha_1, \ldots, \alpha_n\}$ felbontható kódot. K-ban az $\alpha_1, \ldots, \alpha_n$ kódszavak hossza legyen $l_1, \ldots, l_n$. így az

$$l_1 p_1 M + \cdots + l_n p_n M = M \sum_{i=1}^{n} p_i l_i$$

képlet egy $\alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_M}$ kódolt közlés átlagos hosszát adja.

4.1. Definíció. Az $L(K) = \sum_{i=1}^{n} p_i l_i$ számot a K kód F forrás melletti *költség*ének nevezzük.

4.2. Megjegyzés. Látható, hogy a költség és a kódszavak hossza összefügg.

4.3. Definíció. A K_0 felbontható kódot az F jelforrásra nézve *optimális*nak nevezzük, ha tetszőleges K felbontható kód esetén az F mellett $L(K_0) \leq L(K)$.

4.4. Megjegyzés. Ez azt jelenti, hogy az optimális kódok a kódolt közlések átlagos hosszának csökkentésében játszanak szerepet. Igaz a következő:

4.5. Tétel. *Tetszőleges F forráshoz létezik optimális prefix kód.*

4.6. Definíció. Az F forrás *entrópiájának* nevezzük a

$$H(F) = \sum_{i=1}^{n} p_i log_2 \frac{1}{p_i}$$

számot.

A költség és az entrópia kapcsolatát adja meg a következő két tétel:

4.7. Tétel (Claud Shannon tétele). *Egy F jelforráshoz tartozó tetszőleges K felbontható kódra teljesül, hogy:*

$$H(F) \leq L(K).$$

4.8. Tétel. *Az F jelforráshoz tartozó K_0 optimális kód költségére teljesül, hogy*

$$L(K_0) \leq H(F) + 1.$$

4.9. Következmény. Az F jelforráshoz tartozó K_0 optimális kódra igaz a következő becslés:

$$H(F) \leq L(K_0) \leq H(F) + 1.$$

5. Optimális kód konstrukciója

D. Huffmann amerikai matematikus 1951-ben adta meg az alábbi két tétel segítségével az optimális kódok egy lehetséges konstrukcióját.

Ismeretes az előző fejezetből, hogy tetszőleges jelforráshoz létezik optimális kód. A következő eljárásnál tegyük fel, hogy egy F jelforrás $A = \{a_1, \ldots, a_n\}$ kimeneti ábécéjének betűihez rendre a $p_1 \geq \cdots \geq p_n$ valószínűségek tartoznak. Optimális kódok meghatározásának *Huffmann-féle algoritmus*a a következő két tételen alapszik:

5.1. Tétel. *Egy F jelforráshoz létezik legalább egy $K = \{\alpha_1, \ldots, \alpha_n\}$ optimális prefix kód, amelyre $l_1 \leq \cdots \leq l_{n-1} = l_n$ és az utóbbi két kódszó $\alpha 0$ és $\alpha 1$ alakú (tehát csak az utolsó jegyben térnek el).*

5.2. Tétel. *Legyen F jelforrás egy $A = \{a_1, \ldots, a_n\}$ kimenő ábécével, és az A elemeihez tartozó $p_1 \geq \cdots \geq p_n$ valószínűségekkel, és legyen $K = \{\alpha_1, \ldots, \alpha_n\}$ az előző tétel alapján létező optimális prefix kód F-hez. Tegyük fel, hogy*

$$p_i = q_1 + q_2 \quad \text{és} \quad p_1 \geq \cdots \geq p_{i-1} \geq p_{i+1} \geq \cdots \geq p_n \geq q_1 \geq q_2.$$

Ekkor a

$$K' = \{\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n, \alpha_i 0, \alpha_i 1\}$$

kód optimális prefix kód lesz arra az F' jelforrásra nézve, melynek kimenő ábécéje $A' = \{a_1, \ldots, a_n, a_{n+1}\}$ és a hozzátartozó valószínűségek $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n, q_1, q_2$.

5.3. Megjegyzés. Ezen utóbbi két tétel segítségével minden $n+1$ betű kibocsájtó jelforráshoz tartozó optimális kód meghatározását visszavezethetjük egy n-betűs jelforrás esetére. A módszer a következő: Induljunk ki egy F jelforráshoz tartozó $A = \{a_1, \ldots, a_n, a_{n+1}\}$ ábécéből, a betűkhöz tartozó valószínűségek pedig legyenek $p_1 \geq \cdots \geq p_n \geq p_{n+1}$. Legyen továbbá F' egy másik jelforrás, a hozzá tartozó kimenő ábécé $B = \{b_1, \ldots, b_n\}$, a valószínűségek pedig $p_1 \geq \cdots \geq p_{i-1} \geq p_n + p_{n+1} \geq p_{i+1} \geq \cdots \geq p_{n-1}$. így ha $K' = \{\alpha_1, \ldots, \alpha_n\}$ optimális az F'-re nézve, akkor a $K = \{\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n, \alpha_i 0, \alpha_i 1\}$ optimális lesz az F jelforrás esetén. Az algoritmus bemutatására alkalmazzuk a következő példát:

5.4. Példa. Legyen $A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$, a valószínűségek pedig $\{0,2; 0,2; 0,19; 0,12; 0,11; 0,09; 0,09\}$. Ekkor az ábécé és a kódok redukálásának útja a következő:

0,20	0,20	0,23	0,37	0,40	0,60
0,20	0,20	0,20	0,23	0,37 +	0,40
0,19	0,19	0,20	0,20 +	0,23	
0,12	0,18	0,19 +	0,20		
0,11	0,12 +	0,18			
0,09 +	0,11				
0,09					

10	10	01	00	1	0
11	11	10	01	00	1
000	000	11	10	01	
010	001	000	11		
011	010	001			
0010	011				
0011					

így az ábécé betűszámának csökkentésével eljutottunk egy kételemű ábécéhez, amelyhez tartozó $\{0,1\}$ kód optimális. Visszafelé alkalmazva az eljárást növekvő elemszámú ábécéhez nyerhetünk optimális kódot.

6. Hibajavító kódok zajos csatorna esetén

Ha az információs csatorna zajos, akkor a demodulátorból kapot kódolt közlés hibákat tartalmazhat. Ebben a fejezetben olyan eljárásokat ismertetünk, amelyek lehetővé teszik a hibák felismerését, és annak a javítását.

Feltételezzük, hogy azonos hosszúságú kódszavakból álló bináris kódokkal történik az információközlés.

6.1. Definíció. A kódszavakat *blokk*oknak, a kódszavak hosszát *blokkméret*nek nevezzük.

6.2. Megjegyzés. Ezek a kódok felbonthatóak lesznek, mivel a blokkméretek egyenlők és a kódszavak különbözőek.

6.3. Definíció. Legyen a $K = \{\alpha_1, \ldots, \alpha_m\}$ kódhoz tartozó blokkméret n, és $t(\in \mathbb{N}) \leq n$. Azt mondjuk, hogy a (zajos) információs csatorna legfeljebb t hibát okoz, ha tetszőleges blokkban legfeljebb t jel értéke változik meg az információtovábbítás során.

6.4. Példa. Hibafelismerő kód egy hiba esetén:
Legyen minden kódszó olyan, hogy az első fele és a második fele megegyezik. Ekkor az 1 hibát okozó zaj a kódszó egyik felét tudja megváltoztatni. Tehát ahol a két "félkódszó" különbözik, ott hiba van.

6.5. Példa. Hibafelismerő és hibajavító kód egy hiba esetén:
Legyen adva olyen kódolás, amelynél a kódszó első, második és harmadik

harmada megegyezik. Ekkor 1 hibát ki is tudunk javítani, mivel jó harmadoknak azokat tudjuk elfogadni, amelyek legalább kétszer szerepelnek egy kódszóban.

6.6. Definíció. Az n blokkméretű bináris kódok halmazát jelöljük B^n-nel. Ekkor az $\alpha_1, \alpha_2 \in B^n$ kódszavak (vektorok) $\rho(\alpha_1, \alpha_2)$ *Hamming távolság*án azoknak a pozícióknak a számát értjük, amelyeken a kódszavak eltérnek egymástól.

6.7. Megjegyzés. A $\rho(\alpha_1, \alpha_2)$ távolság metrikát ad meg B^n-en, mivel teljesülnek a metrika tulajdonságai (lásd első fejezet 2.16. megjegyzés):

1. $\rho(\alpha_1, \alpha_2) \geq 0$, és $\rho(\alpha_1, \alpha_2) = 0 \iff \alpha_1 = \alpha_2$,
2. $\rho(\alpha_1, \alpha_2) = \rho(\alpha_2, \alpha_1)$,
3. $\rho(\alpha_1, \alpha_2) \leq \rho(\alpha_1, \alpha_3) + \rho(\alpha_3, \alpha_2)$.

6.8. Definíció. Egy $K \subset B^n$ kód esetén a

$$d(K) = min\{\rho(\alpha_1, \alpha_2) \mid \alpha_i, \alpha_j \in K\}$$

számot a K kód *kódtávolság*ának nevezzük.

6.9. Megjegyzés. A 6.4. példában a kódtávolság 2, a 6.5. példában pedig 3.

6.10. Példa. Paritásellenőrző kód:
Legyen B^n olyan kód, amely olyan n hosszúságú kódszavakból áll, amelyekben páros számú egyes szerepel. Ekkor $d(B^n) = 2$. A hiba felismerése egyszerű, meg kell számolni a beérkező 1-esek számát blokkonként. Ha ez páratlan, akkor hibás a kódszó.

6.11. Tétel. *Tetszőleges K kód akkor és csak akkor alkalmas t számú hiba felismerésére, ha* $d(K) \geq t + 1$.

6.12. Tétel. *Egy K kóddal akkor és csak akkor lehet t számú hibát javítani, ha* $d(K) \geq 2t + 1$.

7. Lineáris kódok és Hamming kódok

7.1. Definíció. Legyenek $\alpha = (a_1, \ldots, a_n)$ és $\beta = (b_1, \ldots, b_n) \in B^n$ bináris szám n-esek. Az α és β vektorok $\alpha + \beta$ *összeg*e alatt az $\alpha + \beta = (a_1 + b_1, \ldots, a_n + b_n)$ szám n-est értjük, ahol az $a_i + b_i$ összegnél a 2-vel való osztás maradékát értjük, azaz az összeget "modulo 2" kell venni.

7.2. Definíció. Ha λ bináris konstans (azaz 0 vagy 1), akkor az $\alpha = (a_1, \ldots, a_n)$ vektornak a λ *skalárral való szorzata* $\lambda\alpha = (\lambda a_1, \ldots, \lambda a_n)$, így $1\alpha = \alpha$ és $0\alpha = 0$.

7.3. Definíció. Azt mondjuk, hogy a K kód *lineáris*, ha bármely $\alpha, \beta \in K$ esetén $\alpha + \beta \in K$ és bármely $\lambda \in \{0, 1\}$ és $\alpha \in K$ esetén $\lambda\alpha \in K$ teljesül.

7.4. Definíció. Az $\alpha = (a_1, \ldots, a_n)$ vektor $w(\alpha)$ *súlya* alatt az α vektorban lévő nem nulla elemek számát értjük.

7.5. Tétel. *Egy K lineáris kód esetén*

$$\rho(\alpha, \beta) = w(\alpha + \beta).$$

7.6. Definíció. Egy K kód $w(K)$ súlya alatt a K-beli nem nulla szavak súlyának minimumát értjük.

7.7. Tétel. *Ha K lineáris kód, akkor*

$$d(K) = w(K).$$

7.8. Megjegyzés. Látható, hogy egy K lineáris kód altere B^n-nek egy kételemű test felett, így a vektorterek elméletéből adódik a következő.

7.9. Tétel. *Ha $K \subset B^n$ bináris kód, akkor létezik egy olyan $k \leq n$ természetes szám, hogy tetszőleges K-beli α kódszó egyértelműen megadható, mint az α_i $(i = 1, \ldots, k)$ vektorok lineáris kombinációja, azaz*

$$\alpha = \lambda_1\alpha_1 + \cdots + \lambda_k\alpha_k$$

valamilyen λ_i bináris konstansokkal.

7.10. Következmény. Az $\alpha_1, \ldots, \alpha_k$ vektorok a K egy bázisát alkotják, k pedig a K kód dimenziója.

7.11. Definíció. Legyen a K kód bázisa $\alpha_1, \ldots, \alpha_k$, és legyenek a bázisvektorok koordinátái $\alpha_i = (a_{i1}, \ldots, a_{in})$, $(i = 1, \ldots, k)$. Ekkor a

$$G = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{k1} & \ldots & a_{kn} \end{pmatrix}$$

mátrixot a kód *generátormátrix*ának nevezzük.

7.12. Következmény. Egy adott kód egy tetszőleges kódszava előáll a kód generátormátrixa sorainak lineáris kombinációjaként.

7.13. Definíció. Az α és β vektorok (α, β) *skaláris szorzat*a alatt az

$$(\alpha, \beta) = (a_1 b_1 + \cdots + a_n b_n)$$

összeget értjük, az összeget "modulo 2" kell venni.

7.14. Definíció. Az α és β vektorok *merőleges*ek egymásra, ha $(\alpha, \beta) = 0$.

Egy altér ortogonális komplementerének tulajdonságai miatt igaz a következő:

7.15. Tétel. *Legyen K egy m-dimenziós kód. Ekkor léteznek $\beta_1, \ldots, \beta_{n-m}$ független vektorok úgy, hogy egy $\alpha \in B^n$ vektor akkor és csak akkor eleme K-nak, ha $(\alpha, \beta_i) = 0$, $(i = 1, \ldots, n-m)$.*

7.16. Definíció. A $\beta_1, \ldots, \beta_{n-m}$ bázisú $K^\perp$ kódot a K kód *duális*ának nevezzük.

7.17. Következmény. A $K^\perp$ kód független a bázis megválasztásától.

7.18. Definíció. A K kód ellenőrző mátrixának nevezzük az alábbi mátrixot:

$$H = \big(\beta_1, \ldots, \beta_{n-m}\big) = \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n-m,1} & \ldots & b_{n-m,n} \end{pmatrix}.$$

7.19. Következmény. Legyen a K kód ellenőrző mátrixa H. Ekkor $\alpha \in K$ akkor és csak akkor, ha $H\alpha^T = 0$.

7.20. Megjegyzés. Mindezek alapján látható, hogy ha az $\alpha \in K$, $\alpha \neq 0$ kódszó súlya t, akkor a H mátrixban van t számú lineárisan függő oszlopvektor. Fordítva, ha a H-ban van t számú lineárisan függő oszlopvektor, akkor létezik $\alpha \in K$ kódszó, amelyre $w(\alpha) = t$. Tehát $d(K) > t$ akkor és csak akkor teljesül, ha a K kód ellenőrző mátrixából tetszőleges t számú oszlopot kiválasztva lineárisan független oszlopvektorokat kapunk. így az előző fejezet két utolsó tétele alapján igaz a következő:

7.21. Tétel. *Egy K lineáris kóddal akkor és csak akkor lehet t számú hibát javítani, ha a K ellenőrző H mátrixában tetszőlegesen kiválasztva $2t$ számú oszlopot lineárisan független oszlopvektorokat kapunk.*

7.22. Megjegyzés. Ezen tétel alapján az 1 hibát javító, úgynevezett Hamming kódokat a következőképpen adhatjuk meg:

Legyen a blokkméret $n = 2^l - 1$ alakú. Ha a H oszlopaiként az összes l hosszúságú nem nulla vektort tekintjük, akkor a H tetszőleges két oszlopa lineárisan független. Tehát az így megadott kód kódtávolsága legalább három, azaz egy hibát tudunk vele javítani.

7.23. Példa. Legyen $l = 3$, ekkor a blokkméret $2^l - 1 = 2^3 - 1 = 7$. Ellenőrző mátrixként tekinthetjük a következőt:

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

Legyen α eleme a K Hamming kódnak. Ekkor $H\alpha^T = 0$. Legyen továbbá β a kimenő jel, amelyet α-ból úgy kapunk, hogy egy helyen megváltoztatjuk, például

$$\alpha = (0,0,0,1,1,1,1) \quad ; \quad \beta = (0,0,0,0,1,1,1).$$

Ekkor $\beta = \alpha + \varepsilon$, ahol $\varepsilon = (0,0,0,1,0,0,0)$. így

$$H\beta^T = H(\alpha^T + \varepsilon^T) = H\alpha^T + H\varepsilon^T = H\varepsilon^T,$$

azaz

$$H\beta^T = H \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + H \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

azaz a β hibás kód, a negyedik helyen javítandó, mivel $H\beta^T$ a H negyedik oszlopával megegyező oszlopvektor.

Irodalomjegyzék

[1] Andrásfalvi Béla: Gráfelmélet, folyamatok, mátrixok, *Budapest, Akadémiai kiadó* (1983).

[2] Bélteky Károly: Analitikus geometria és lineáris algebra : I. éves nappali tanárszakos, matematikus és matematikus levelező hallgatók részére, *Budapest, Tankönyvkiadó* (1989).

[3] Demetrovics János, Denev Jordan, Pavlov Padiszlav: A számítástudomány matematikai alapjai, *Budapest, Tankönyvkiadó* (1985).

[4] Fazekas István: Valószinűségszámítás, *Debrecen, Kossuth Egyetemi K.* (2003).

[5] Gaál István, Kozma László: Lineáris algebra, *Debrecen, Kossuth Egyetemi K.* (2002).

[6] Halmos Pál: Véges dimenziós vektorterek, *Budapest, Müszaki Könyvkiadó* (1984).

[7] Kovács Zoltán: Geometria : az euklidészi geometria metrikus megalapozása, *Debrecen, Kossuth Egyetemi K.* (2002).

[8] Szendrei Ágnes: Diszkrét matematika : logika, algebra, kombinatorika, *Szeged, Polygon* (1994).

Tárgymutató