1 Ortogonalne matrice

Ortonormiranih baza u euklidskom vektorskom prostoru ima mnogo: one čine podskup $\mathcal{B}_o \subset \mathcal{B}$ skupa svih baza. Postavlja se pitanje koja svojstva (osim regularnosti) mora da ima matrica prelaza koja povezuje dve ortonormirane baze.

Lema. Ako je $e \in \mathcal{B}_o$ ortonormirana baza i $e' = e \cdot C$ nova baza, pri čemu je $C \in GL(n)$, tada je $e' \in \mathcal{B}_o \Leftrightarrow$ kolone matrice C čine ortonormiran skup u $\mathbb{R}^n$.

Dokaz. Kolone matrice $C = (c_{ij})$ su koordinate vektora e'_i u bazi e. Pošto je e ortonormirana, skalarni proizvod (e'_i, e'_j) se lako izračunava preko tih koordinata: $(e'_i, e'_j) = c_{1i} \cdot c_{1j} + \ldots + c_{ni} \cdot c_{nj}$. Odavde tvrdjenje sledi neposredno. ∎

Definicija. Kvadratna matrica $C = (c_{ij}) \in \mathcal{M}(n, \mathbb{R})$ je *ortogonalna*, ako njene kolone čine ortonormiran skup vektora u prostoru kolona $\mathbb{R}^n$, tj. ako je

$$c_{1i} \cdot c_{1j} + \ldots + c_{ni} \cdot c_{nj} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases} .$$

Skup svih ortogonalnih matrica tipa n se obeležava sa $O(n, \mathbb{R}) = O(n)$.

Jasno je da svaka ortogonalna matrica mora da bude regularna: kolone su ortonormirane, dakle i linearno nezavisne. Opišimo još neke karakterizacije ortogonalnih matrica.

Tvrdjenje. Neka je $C \in \mathcal{M}(n, \mathbb{R})$. Sledeća tvrdjenja su ekvivalnentna:
(1) Matrica C je ortogonalna, tj. njene kolone čine ortonormiran skup u $\mathbb{R}^n$;
(2) njene vrste čine ortonormiran skup vektora u $\mathbb{R}^n$;
(3) $C^T \cdot C = E$;
(4) $C \cdot C^T = E$;
(5) $C \in GL(n)$ i $C^{-1} = C^T$.

Dokaz ide po shemi (1) $\Leftrightarrow$ (3) $\Leftrightarrow$ (5) $\Leftrightarrow$ (4) $\Leftrightarrow$ (2), čija je svaka karika očigledna na osnovu definicija. ∎

Iz ovog tvrdjenja vidimo da se može govoriti o ortogonalnim matricama nad proizvoljnim poljem $\mathbb{F}$, a ne samo nad poljem $\mathbb{R}$ jer se svojstva (3), (4) i (5) mogu formulisati nezavisno od polja.

Definicija. Matrica $C \in \mathcal{M}(n, \mathbb{F})$ je *ortogonalna matrica* nad poljem $\mathbb{F}$, ako važi jedno od (ekvivalentnih) svojstava: $C^T \cdot C = E$, $C \cdot C^T = E$, $C^{-1} = C^T$. Skup svih takvih matrica obeležavamo sa $O(n, \mathbb{F})$.

Tvrdjenje-definicija. Skup $O(n, \mathbb{F})$ za svako n je grupa u odnosu na množenje matrica. To je podgrupa grupe $GL(n, \mathbb{F})$ koja se naziva grupa ortogonalnih matrica tipa n nad $\mathbb{F}$ ili, prosto, *ortogonalna grupa*.

Dokaz. $E \in O(n, \mathbb{F})$, pa je $O(n) \neq \emptyset$. Na osnovu ranije primedbe, $O(n, \mathbb{F}) \subset GL(n, \mathbb{F})$. Ostaje da se proveri da, ukoliko su $A, B \in O(n, \mathbb{F})$, onda je i AB^{-1} ortogonalna. Ali invertovanje i transponovanje su nezavisne operacije, pa je

$$(AB^{-1})(AB^{-1})^T = AB^{-1}(B^{-1})^T A^T = AB^{-1}(B^T)^{-1} A^T = AB^{-1} B A^{-1} = E. \blacksquare$$

Primedba. Za $C \in O(n, \mathbb{F})$ determinanta $\det C = \pm 1$.

Tvrdjenje-definicija. Grupa $SO(n, \mathbb{F}) = O(n, \mathbb{F}) \cap SL(n, \mathbb{F})$ je podgrupa u $GL(n, \mathbb{F})$, tzv. *specijalna ortogonalna grupa*. To je podgrupa indeksa 2 u

$O(n,\mathbb{F})$. U slučaju $\mathbb{F}=\mathbb{R}$ je $SO(n)=O(n)\cap GL(n)^+$ gde je $GL(n)^+=\{A\in GL(n)|\det A>0\}$.

Dokaz. To je podgrupa kao presek dve podgrupe u $GL(n,\mathbb{F})$. Preslikavanje $\det : O(n,\mathbb{F})\rightarrow\{1,-1\}$ je epimorfizam multiplikativnih grupa čije je jezgro upravo $\mathrm{Ker}(\det)=SO(n,\mathbb{F})$, odakle sledi tvrdjenje. ∎

Opišimo sad grupe $SO(1)$, $O(1)$, $SO(2)$ i $O(2)$.

Tvrdjenje. (1) $SO(1)=\{1\}$, $O(1)=\{1,-1\}\subset GL(1)=\mathbb{R}^*$.

(2) $SO(2)=\left\{\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}\middle|\,\varphi\in[0,2\pi)\right\}$, $O(2)=SO(2)\cup\left\{\begin{pmatrix}\cos\varphi & \sin\varphi\\ \sin\varphi & -\cos\varphi\end{pmatrix}\middle|\,\varphi\in[0,2\pi)\right\}$.

Dokaz. Tvrdjenje (1) je očigledno. (2) Uslov $\begin{pmatrix}a & c\\ b & d\end{pmatrix}\in SO(2)$ može se zapisati u obliku sistema

$$\begin{aligned}a^2+b^2 &= 1\\ c^2+d^2 &= 1\\ ac+bd &= 0\\ ad-bc &= 1\end{aligned}$$

iz kojeg se dobija traženi oblik matrice. Drugi skup rešenja se dobija kada se u poslednjoj jednačini 1 zameni sa -1. Time smo opisali celo $O(2)$. ∎

Pokušaj takvog opisivanja grupe $O(3)$ osudjen je na neuspeh. Medjutim, kasnije ćemo imati novu interpretaciju pojma ortogonalne matrice nad $\mathbb{R}$, na osnovu koje ćemo moći geometrijskim sredstvima da opišemo klase sličnosti u $O(3)$.

Na osnovu svega rečenog možemo formulisati zaključak.

Neka je V euklidski vektorski prostor, e jedna ortonormirana baza i $e'=e\cdot C$ nova baza ($C\in GL(n)$). Tada je e' ortonormirana $\Leftrightarrow C\in O(n)$. Pri tom, e' je isto orijentisana kao $e\Leftrightarrow C\in SO(n)$.

2 Ortogonalni komplement. Ortogonalizacija

Definicija. Vektor v je *ortogonalan* na skup $S\subset V$ ako je, za svako $w\in S$, $v\perp w$. Skupovi S i S' su *ortogonalni* ako je, za sve vektore $v\in S$ i $v'\in S'$, $v\perp v'$. Ako je $S\subset V$, skup $S^\perp:=\{v\in V|v\perp S\}$ naziva se *ortogonalnim komplementom* skupa S u prostoru V.

Tvrdjenje. (1) $S^\perp$ je potprostor ortogonalan na S.

(2) Ako je S' skup ortogonalan na S, tada je $S'\subset S^\perp$ (maksimalnost $S^\perp$).

(3) $S_1\subset S_2\Rightarrow S_2^\perp\subset S_2^\perp$.

(4) $S^\perp=\mathcal{L}(S)^\perp$.

(5) Ako je $S=W=\mathcal{L}(a_1,\ldots,a_k)$ potprostor, onda je $W^\perp$ skup rešenja sistema

$$(v,a_1)=\ldots=(v,a_k)=0,$$

tj. $v\in W^\perp\Leftrightarrow v\perp a_1,\ldots,v\perp a_k$.

Dokaz. (1) Naime, ako su $w,w'\in S^\perp$ i $v\in S$, tada je $(v,\alpha w+\alpha'w')=\alpha(v,w)+\alpha'(v,w')=0$, tj. $\alpha w+\alpha'w'\in S^\perp$.

Svojstvo (2) je očigledno iz definicije $S^\perp$.

(3) $w \in S_2^\perp \Rightarrow \forall v \in S_2,\ v \perp w \Rightarrow \forall v \in S_1 \subset S_2,\ v \perp w \Rightarrow w \in S_2^\perp$.

(4) Na osnovu svojstva (2) je $\mathcal{L}(S)^\perp \subset S^\perp$. Ako $w \in S^\perp$, onda je, za svako $v \in S$, $(v, w) = 0$. Neka je $v \in \mathcal{L}(S)$. Tada je $v = \alpha_1 v_1 + \ldots + \alpha_k v_k$ za neke $v_1, \ldots, v_k \in S$. Sada je

$$(v, w) = (\alpha_1 v_1 + \cdots + \alpha_k v_k, w) = \alpha_1 (w_1, v) + \ldots + \alpha_k (w_k, v) = 0,$$

što znači da je $w \in \mathcal{L}(S)^\perp$.

(5) $W^\perp \subset \{\text{rešenja}\}$ jer ako je v ortogonalan na sve $w \in W$, onda je ortogonalan i na a_i. Ali svaki vektor $w \in W$ je oblika $w = \alpha_1 a_1 + \ldots + \alpha_k a_k$ pa je svako rešenje sistema, ortogonalno na sve a_i, ortogonalno i na w. To upravo znači da je $\{\text{rešenja}\} \subset W^\perp$. ∎

Teorema (o ortogonalnom komplementu). Za svaki potprostor $W \subset V$ je

$$V = W \oplus W^\perp.$$

Ova je dekompozicija jednoznačna: ako je $V = W \oplus W'$ za neki drugi potprostor W' ortogonalan na W, tada je $W' = W^\perp$.

Dokaz. Dokažimo da je $V = W + W^\perp$. Neka je $v \in V$. Dokažimo da $\exists w \in W$ takav da je $v - w = w' \in W^\perp$. Neka je $e_1, \ldots, e_k$ baza u W. Treba naći koeficijente $\alpha_1, \ldots, \alpha_k$ takve da je $v - (\alpha_1 e_1 + \cdots + \alpha_k e_k) = w' \in W^\perp$. Na osnovu prethodnog tvrdjenja

$$w' \in W^\perp \Leftrightarrow (w', e_1) = \ldots = (w', e_k) = 0.$$

Kad ovde uzmemo da je $w' = v - (\alpha_1 e_1 + \cdots + \alpha_k e_k)$ i sredimo, dobijamo linearni sistem

$$\begin{array}{ccccccc} (e_1, e_1)\alpha_1 & + & \cdots & + & (e_k, e_1)\alpha_k & = & (v, e_1) \\ & & \cdots & & & & \\ (e_1, e_k)\alpha_1 & + & \cdots & + & (e_k, e_k)\alpha_k & = & (v, e_k) \end{array}$$

sa determinantom $\det G(e_1, \ldots, e_k) \neq 0$ jer je e baza. Zato sistem ima (jedinstveno) rešenje $(\alpha_1, \ldots, \alpha_k)$, za koje je $w' \in W^\perp$.

Proverimo sada da li je suma direktna. Ako je $v \in W \cap W^\perp$, tada je $v \perp v$, tj. $(v, v) = \|v\|^2 = 0$, pa je $v = o$. Zato je $W \cap W^\perp = \{o\}$ i suma je direktna.

Najzad, ako je $V = W \oplus W'$ i $W' \perp W$, tada je $W' \subset W^\perp$, pa je $\dim V - \dim W = \dim W' \leq \dim W^\perp = \dim V - \dim W$, odakle sledi da je $\dim W' = \dim W^\perp$ i $W' = W^\perp$. ∎

Posledica. Za svaki skup $S \subset V$ je $(S^\perp)^\perp = \mathcal{L}(S)$. Posebno, ako je W potprostor, tada je $(W^\perp)^\perp = W$.

Dokaz. Naime, iz $V = \mathcal{L}(S) \oplus \mathcal{L}(S)^\perp$ sledi da je $\mathcal{L}(S) = (\mathcal{L}(S)^\perp)^\perp = (S^\perp)^\perp$. ∎

Navedena teorema nam kaže da, u slučaju euklidskog prostora V, medju svim komplementima W' potprostora W takvim da je $W \oplus W' = V$ (kojih ima beskonačno mnogo) postoji tačno jedan koji je na W ortogonalan.

Ako je $W \subset V$ potprostor, tada se, na osnovu teoreme, svaki vektor $v \in V$ jednoznačno predstavlja u obliku $v = v' + v''$ sa $v' \in W$ i $v'' \perp W$.

Definicija. Vektor v' se naziva *ortogonalnom projekcijom* vektora v na potprostor W, a v'' - *ortogonalnom komponentom* vektora v u odnosu na W.

U dokazu teoreme opisan je eksplicitni postupak izračunavanja ortogonalne projekcije i komponente vektora ako je potprostor zadat kao lineal $W = \mathcal{L}(e_1, \ldots, e_k)$. Pri tom baza e ne mora da bude ortonormirana i tada dobijamo pun sistem jednačina za izračunavanje koeficijenata α_i. Ukoliko je baza ortonormirana, sistem se veoma pojednostavljuje jer je u tom slučaju njegova matrica $G(e) = E$, pa je on trivijalan: $\alpha_i = (v, e_i)$. Zbog toga je važno da nadjemo postupak koji od proizvoljne baze potprostora može da napravi ortonormiranu. Jedan takav postupak opisuje sledeća teorema.

Teorema (Gram-Šmitov postupak ortogonalizacije). Neka je V euklidski prostor, a $W \subset V$ potprostor s bazom $e = (e_1, \ldots, e_k)$. Tada postoji ortogonalna baza $e' = (e'_1, \ldots, e'_k)$ u W takva da je $\mathcal{L}(e_1, \ldots, e_i) = \mathcal{L}(e'_1, \ldots, e'_i) \quad (i = 1, \ldots, k)$,

$$\begin{aligned} e'_1 &= e_1 \\ e'_2 &= e_2 + \alpha_{21} e'_1 \\ &\ldots \\ e'_k &= e_k + (\alpha_{k1} e'_1 + \ldots + \alpha_{k,k-1} e'_{k-1}), \end{aligned}$$

pri čemu je

$$\alpha_{ij} = \frac{(e'_i, e'_j)}{(e_j, e'_j)} \quad (j = 1, \ldots, i-1).$$

Dokaz. Prvi korak je očigledno $e'_1 = e_1$, pri čemu je $W_1 = \mathcal{L}(e'_1) = \mathcal{L}(e_1)$. Pretpostavimo da smo već odredili ortogonalne $e'_1, \ldots, e'_{i-1}$ sa svojstvom da je $W_{i-1} = \mathcal{L}(e_1, ., e_{i-1}) = \mathcal{L}(e'_1, \ldots, e'_{i-1})$. Vektor e_i ne pripada W_{i-1}. Neka je e'_i njegova ortogonalna komponenta u odnosu na W_{i-1}, a $e''_i \in W_{i-1}$ ortogonalna projekcija. Tada je $e''_i = \alpha_{i,1} e'_1 + \ldots + \alpha_{i,i-1} e'_{i-1}$. Kao u dokazu teoreme o ortogonalnom komplementu, skalarnim množenjem jednakosti

$$e_i = e'_i + e''_i = e'_i + \alpha_{i1} e'_1 + \ldots + \alpha_{i,i-1} e'_{i-1}$$

sa $e'_j \quad (j = 1, \ldots, i-1)$, uz korišćenje ortogonalnosti vektora $e'_1, \ldots, e'_{i-1}$ dobijamo jednostavan sistem

$$(e_i, e'_j) = (e'_i, e'_j) + \alpha_{ij} (e'_j, e'_j) \quad (j = 1, \ldots, i-1)$$

iz kojeg deljenjem sa $(e'_j, e'_j) = \|e'_j\|^2 \neq 0$ dobijamo tražene koeficijente. ∎

Dobijena baza e' može se normirati u toku rada ili na kraju, što je, sa praktičnog stanovišta, bolje. U dokazu je eksplicitno opisan postupak ortogonalizacije.

Primedbe. (1) (O pravouglom trouglu). Neka je $W \subset V$ potprostor, $v \in V \backslash \{o\}$ proizvoljan vektor, $v' \in W$ njegova ortogonalna projekcija na W i v'' njegova ortogonalna komponenta. Tada je ugao $\varphi = \measuredangle(v, v') \in [0, \pi/2]$, pri čemu je $\varphi = 0 \Leftrightarrow v \in W$, a $\varphi = \pi/2 \Leftrightarrow v \perp W$. Zaista, množenjem jednakosti

$v = v' + v''$ sa v', uz uslov da je $v' \perp v''$, dobijamo $(v, v') = (v', v') = \|v'\|^2$, odakle sledi da je

$$\cos\varphi = \frac{(v, v')}{\|v\| \cdot \|v'\|} = \frac{\|v'\|}{\|v\|} \geq 0.$$

Ako primenimo sad Pitagorinu teoremu $\|v'\|^2 + \|v''\|^2 = \|v' + v''\|^2 = \|v\|^2$, podelimo tu jednakost sa $\|v\|^2$ i iskoristimo prethodno rečeno, dobijamo:

$$\sin\varphi = \frac{\|v''\|}{\|v\|} = \cos\left(\frac{\pi}{2} - \varphi\right).$$

To se može interpretirati na elementarno geometrijski način: vektori v, v' i v'' čine pravougli trougao (pravilo trougla za sabiranje vektora), kod kojeg je dužina hipotenuze $\|v\|$, kateta $\|v'\|$ i $\|v''\|$, a uglovi φ i $\pi/2-\varphi$. Pri tom trigonometrijske funkcije sin i cos ugla φ dobijamo upravo kao količnike dužina odgovarajućih kateta i hipotenuze.

(2) Pojam projekcije se može iskoristiti i za definiciju ugla izmedju vektora i potprostora. Neka je $V = W \oplus W^{\perp}$ i $v \in V$ sa ortogonalnom projekcijom $v' \in W$ i ortogonalnom komponentom $v'' \in W^{\perp}$. *Ugao* $\measuredangle(v, W)$ *izmedju vektora* v *i potprostora* W je (neorijentisani) ugao $\measuredangle(v, v')$ izmedju v i njegove projekcije v'. Jasno je da je v'' ortogonalna projekcija v na $W^{\perp}$, $\measuredangle(v, W^{\perp}) = \measuredangle(v, v'')$ i na osnovu prethodne primedbe

$$\measuredangle(v, W) + \measuredangle(v, W^{\perp}) = \frac{\pi}{2}.$$