EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Természettudományi Kar

Árendás Péter

Polinomok négyzetösszeggé alakítása és alkalmazásai

Témavezető: Dr. Szabó Csaba

BSc szakdogozat

Matematika BSc szakon

2010. június 7.

Nyilatkozat

- NÉV: *Árendás Péter*
- ELTE Természettudományi Kar, Szak: *matematika BSc*
- ETR azonosító: *ARPPAAT.ELTE*
- Szakdolgozat címe: *Polinomok négyzetösszeggé alakítása és alkalmazásai*

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló munkám eredménye, saját szellemi termékem, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Aláírás:

____

Dátum:

____

Köszönetnyilvánítás

Itt szeretném megköszönni dr. Szabó Csabának, hogy három éve felkeltette az érdeklődésemet az algebra iránt, valamint ezen dolgozat megírását is nagyban elősegítette a téma felvetésével, később pedig észrevételeivel, tanácsaival.

Köszönet illeti a családomat, amiért biztosították a tanuláshoz szükséges feltételeket.

Külön köszönet Biszak Elődnek és Stark Andrásnak a technikai segítségért.

Köszönöm továbbá minden volt csoporttársamnak, támogatásuk nélkül valószínűleg el sem jutottam volna a szakdolgozat írásáig.

Tartalomjegyzék

1. fejezet

Bevezetés

A dolgozat témáját Domokos Mátyás [4] cikkében szereplő egyik probléma ihlette. Azt a kérdést vetjük fel, hogy a nulla nyomú, 3×3-as szimmetrikus mátrixok diszkriminánsát legkevesebb hány polinom négyzeteként tudjuk felírni. Ennek a megválaszolására most egy, a [4] cikkben szereplő érveléstől eltérő igazolást fogunk mutatni, melynek alapja egy algoritmus, melyet Victoria Powers és Thorsten Wörmann [1] értekezésében találtam.

Ezután pedig megemlítjük az algoritmus egy másik érdekes, valós algebrai geometriai alkalmazását is.

A diszkrimináns

Legyen A egy olyan 3×3-as, valós együtthatós, szimmetrikus mátrix, melynek nyoma $Tr(A) = 0$. Általános alakban:

$$A := \begin{pmatrix} a_1 & b_1 & b_2 \\ b_1 & a_2 & b_3 \\ b_2 & b_3 & -a_1 - a_2 \end{pmatrix}.$$

A karakterisztikus polinomját kifejezve a következőt kapjuk:

$k_A(x) = x^3 - a_1^2x - a_1a_2x - a_2^2x - b_1^2x - b_2^2x - b_3^2x + a_1^2a_2 + a_1a_2^2 - a_1b_1^2 + a_1b_3^2 - a_2b_1^2 + a_2b_2^2 - 2b_1b_2b_3.$

1.1.1. Megjegyzés. Tekintsük a következő polinomot: $a_3z^3+a_2z^2+a_1z+a_0 = 0$. Ezen általános harmadfokú egyenlet diszkriminánsa a következő:

$$D_3 = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 + 18a_0a_1a_2a_3 - 27a_0^2a_3^2.$$

Vegyük észre, hogy mivel $Tr(A) = 0$, a diszkrimináns képlete ebben az esetben $a_2 = 0$ miatt a következő alakúra módosul:

$$D_3' = -4a_1^3a_3 - 27a_0^2a_3^2.$$

Ha beírjuk az egyszerűsített összefüggésbe $k_A(x)$-et, a következő polinomot kapjuk:

$f = -4(-a_1^2 - a_1a_2 - a_2^2 - b_1^2 - b_2^2 - b_3^2)^3 - 27(a_1^2a_2 + a_1a_2^2 - a_1b_1^2 + a_1b_3^2 - a_2b_1^2 + a_2b_2^2 - 2b_1b_2b_3)^2.$

Ezt kifejtve pedig a következő összeg adódik:

$f = 24a_1^3a_2b_2^2 + 78a_1a_2b_1^2b_2^2 + 78a_1a_2b_1^2b_3^2 - 30a_1a_2b_2^2b_3^2 - 108a_1b_1^3b_2b_3 + 108a_1b_1b_2b_3^3 - 108a_2b_1^3b_2b_3 - 30a_1^3a_2b_3^2 + 78a_1^3a_2b_1^2 + 144a_1^2a_2^2b_1^2 - 18a_1^2a_2^2b_2^2 - 18a_1^2a_2^2b_3^2 + 24a_1^2b_1^2b_2^2 + 78a_1^2b_1^2b_3^2 + 24a_1^2b_2^2b_3^2 - 42a_1a_2b_1^4 + 12a_1a_2b_2^4 + 12a_1a_2b_3^4 + 4a_1^6 + 4a_2^6 + 4b_1^6 + 4b_2^6 + 4b_3^6 + 78a_1a_2^3b_1^2 + 12a_1^5a_2 - 3a_1^4a_2^2 + 12a_1^4b_1^2 - 3a_1^2a_2^4 - 15a_1^2b_1^4 + 12a_1^2b_2^4 - 15a_1^2b_3^4 + 12a_1^4b_2^2 + 12a_1^4b_3^2 - 26a_1^3a_2^3 + 12a_1a_2^5 - 15a_2^2b_1^4 - 15a_2^2b_2^4 + 12a_2^2b_3^4 + 12a_2^4b_1^2 + 12a_2^4b_2^2 + 12a_2^4b_3^2 + 12b_1^2b_2^4 + 12b_1^2b_3^4 + 12b_1^4b_2^2 + 12b_1^4b_3^2 + 12b_2^2b_3^4 + 12b_2^4b_3^2 - 30a_1a_2^3b_2^2 + 24a_1a_2^3b_3^2 + 78a_2^2b_1^2b_2^2 + 24a_2^2b_1^2b_3^2 + 24a_2^2b_2^2b_3^2 + 108a_1^2a_2b_1b_2b_3 + 108a_1a_2^2b_1b_2b_3 + 108a_2b_1b_2^3b_3 - 84b_1^2b_2^2b_3^2.$

Ezt a polinomot szeretnénk felírni a lehető legkevesebb valós együtthatós polinom négyzetének összegeként.

2. fejezet

Valós együtthatós polinomok négyzetösszegre bontása

A bevezetésben említett négyzetösszeggé alakításra az alábbiakban ismertetünk egy alkalmas eljárást.

Az algoritmus azon a tényen alapul, hogy egy valós számtest feletti polinom négyzetösszeg-felbontása megfelel egy valós, szimmetrikus, pozitív szemidefinit mátrixnak, mely elemei kielégítenek bizonyos lineáris egyenleteket.

2.1. Kapcsolat a Gram-mátrixokkal

Tegyük fel, hogy az átalakítandó polinomunk n változós. Rögzítsük le ezt az n számot, valamint az alábbi jelölésrendszert $R := \mathbb{R}[x_1, \ldots, x_n]$-ben: minden $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}$ számra jelölje x^α az $x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$ szorzatot. Ez szemléletesen annyit jelent, hogy a polinom egy-egy tagjának megfeleltetünk egy-egy α karakterisztikus vektort annak alapján, hogy az adott tagban melyik változó hányadik hatványon szerepel. Minden $m \in \mathbb{N}_0$ számra legyen

$$\Lambda_m := \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n | \alpha_1 + \cdots + \alpha_n \leq m\},$$

azaz Λ_m-nek azok az α vektorok lesznek elemei, melyek egy m fokú polinomban előfordulhatnak. Ekkor egy valós együtthatós f polinom, melyre $deg(f) = m$, a következő alakba írható:

$$f = \sum_{\alpha \in \Lambda_m} a_\alpha x^\alpha.$$

Azt mondjuk, hogy az f polinom *négyzetösszeg*, ha f előáll R-beli elemek négyzetei összegeként.

Tegyük fel, hogy f négyzetösszeg, például t darab R-beli tag négyzeteként áll elő. Ekkor f foka páros, jelöljük ezt $2m$-mel. Mivel négyzetösszeg, f felírható az alábbi formában:

$$f = \sum_{i=1}^{t} h_i^2,$$

ahol bármely i-re h_i foka nem nagyobb, mint m.

Tegyük fel, hogy $|\Lambda_m| = k$, azaz k különböző α vektor szerepelhet f-ben. Ekkor Λ_m elemeit felsorolhatjuk a következőképp: $\Lambda_m = \{\beta_1, \ldots, \beta_k\}$.

Legyen $\overline{x} := (x^{\beta_1}, \ldots, x^{\beta_k})$, valamint legyen A egy olyan $k \times t$ méretű mátrix, melynek i-edik oszlopában h_i együtthatói találhatóak. Ekkor az $f = \sum h_i^2$ összefüggés felírható a következő alakban:

$$f = \overline{x} \cdot (AA^T) \cdot \overline{x}^T.$$

A fenti $k \times k$-as $B := AA^T$ mátrixot f *Gram-mátrix*ának is nevezik.

2.1.1. Megjegyzés. A B mátrix pozitív szemidefinit, azaz $\overline{y} \cdot B \cdot \overline{y}^T \geq 0$ minden $\overline{y} = (y_1, \ldots, y_k) \in \mathbb{R}^k$ esetén.

2.1.2. Tétel. Tegyük fel, hogy $f \in R$ egy $2m$ fokú polinom, $\overline{x}$ pedig mint fent. Ekkor f akkor és csak akkor áll elő R-beli tagok négyzetének összegeként, ha létezik egy valós, szimmetrikus, pozitív szemidefinit B mátrix, melyre

$$f = \overline{x} \cdot B \cdot \overline{x}^T.$$

Ha létezik egy ilyen t rangú B mátrix, akkor előállíthatóak $h_1, \ldots, h_t$ polinomok, hogy $f = \sum h_i^2$. Ekkor a B mátrix az f polinom h_i tagokhoz társított Gram-mátrixa.

2.1.2. Bizonyítás. Ha $f = \sum h_i^2$ négyzetösszeg, akkor a fenti módon vegyük $B = A \cdot A^T$-t, ahol az A mátrix oszlopaiban h_i együtthatói találhatóak.

Tegyük fel, hogy létezik egy valós, szimmetrikus, pozitív szemidefinit B mátrix, mely t rangú, és $f = \overline{x} \cdot B \cdot \overline{x}^T$. Mivel $rank(B) = t$, valamint B valós szimmetrikus, ezért létezik egy valós V és egy valós, diagonális $D = diag(d_1, \ldots, d_t, 0, \ldots, 0)$ mátrix, melyekre $B = V \cdot D \cdot V^T$, valamint $d_i \neq 0$ minden i indexre. Mivel B pozitív szemidefinit, $d_i > 0$ minden i-re. Ekkor

$$f = \overline{x} \cdot V \cdot D \cdot V^T \cdot \overline{x}^T.$$

A V mátrix elemeit indexeljük $v_{i,j}$ alakban. Ekkor $i = 1, \ldots, t$ esetén legyen

$$h_i := \sqrt{d_i} \sum_{j=1}^{k} v_{j,i} x^{\beta_i} \in R.$$

A fenti összefüggésből következik, hogy $f = h_1^2 + \cdots + h_t^2$. $\square$

Hogy f egy négyzetösszeg-reprezentációját meg tudjuk adni, elég csak egy olyan B mátrixot találnunk, amely kielégíti a tételt. Továbbá, ha meg tudjuk mutatni, hogy nem létezik ilyen B, akkor ebből következik, hogy f nem áll elő R-beli elemek négyzeteinek összegeként.

2.1.3. Megjegyzés. Amennyiben $f = \sum a_\alpha x^\alpha$, valamint $B = (b_{i,j})$ egy $k \times k$-as szimmetrikus mátrix, akkor $f = \overline{x} \cdot B \cdot \overline{x}^T$ akkor és csak akkor, ha $\forall \alpha \in \Lambda_{2m}$ esetén

$$\spadesuit \sum_{\beta_i + \beta_j = \alpha} b_{i,j} = a_\alpha.$$

2.2. Az algoritmus

$f \in R$ adott, rangja legyen $2m$.

1. lépés. Legyen $B = (b_{i,j})$ szimmetrikus mátrix, változó együtthatókkal. Az $f = \overline{x} \cdot B \cdot \overline{x}^T$ összefüggésből adódó lineáris rendszer megoldását keressük, azaz azon rendszerét, mely $\spadesuit$-ből adódik, méghozzá úgy, hogy minden $\alpha \in \Lambda_{2m}$-re egy egyenletet kapunk. Jegyezzük meg, hogy minden $b_{i,j}$ változó pontosan egy egyenletben jelenik meg, ennek következtében pedig megtehetjük, hogy egy kivételével minden változónak egy paramétert adunk értékül, és az így kapott rendszer megoldását keressük a továbbiakban.

Ekkor a megoldás előáll $B = B_0 + \lambda_1 B_1 + \cdots + \lambda_l B_l$ alakban, ahol minden B_i valós, $k \times k$ méretű szimmetrikus mátrix, $\lambda_1, \ldots, \lambda_l$ pedig a paraméterek. Ebben az esetben $l = k(k+1)/2 - |\Lambda_{2m}|$.

2.2.1. Megjegyzés. Általánosan elmondható, hogy B mérete nagyon gyorsan nő, amint a változók száma és a polinom foka emelkedik, mivel $k = |\Lambda_m| = \binom{n+m}{n}$. Ennek ellenére speciális polinomok esetén egyes esetekben csökkenteni tudjuk a Gram-mátrix rangját a szükségtelen Λ_m-beli elemek eliminálásával. Tegyük fel például, hogy $\alpha \in \Lambda_{2m}$, $\alpha = 2\beta$, valamint α nem írható fel Λ_m-beli elemek semely más összegeként. Ekkor α együtthatója f-ben 0, x^β nem fordulhat elő egy h_i-ben sem.

2. lépés. Olyan módon szeretnénk a λ_l paraméterek értékét megválasztani, hogy $B = B_0 + \lambda_1 B_1 + \cdots + \lambda_l B_l$ pozitív szemidefinit legyen. B akkor és csak akkor lesz pozitív szemidefinit, ha az összes sajátértéke nemnegatív. Legyen $F(y) = y^k + b_{k-1}y^{k-1} + \cdots + b_0$ a B mátrix karakterisztikus polinomja. Jegyezzük meg, hogy $\forall i\ b_i \in \mathbb{R}[\lambda_1, \ldots, \lambda_l]$. A Descartes-féle előjelszabály alapján $F(y)$-nak pontosan akkor vannak csak nemnegatív gyökei, ha $(-1)^{(i+k)}b_i \geq 0$ igaz $\forall i = 0, \ldots, k-1$ esetén. Vegyük ezért a következő félalgebrai halmazt:

$$S := \{(\lambda_1, \ldots, \lambda_l) \in \mathbb{R}^l | (-1)^{(i+k)} b_i(\lambda_1, \ldots, \lambda_l) \geq 0\}.$$

Ekkor f pontosan akkor négyzetösszeg, ha S nemüres, és egy adott S-beli pont megfelel egy, a *2.1.2. Tétel* feltételeit kielégítő mátrixnak.

2.2.2. Megjegyzés. Különféle algoritmusok léteznek annak meghatározására, hogy egy félalgebrai halmaz üres-e, vagy sem, például a kvantoreliminációó módszere. Sajnos egy ilyen algoritmus sem praktikus ebben az esetben, a "kis" esetektől eltekintve.

3. lépés. Legyen $B = (b_{i,j})$ olyan mátrix, mely kielégíti a *2.1.2. Tétel* feltételeit. Ekkor a tétel bizonyításában felhasznált eljárást alkalmazva kereshetjük f egy négyzetösszeg-előállítását.

2.3. Egy példa az alkalmazásra

Tekintsük a következő polinomot: $f = x^2y^2 + x^2 + y^2 + 1$. Ez láthatóan előáll négyzetösszegként, ezért keressük f összes lehetséges előállítását ilyen alakban.

Észrevétel: $f = \sum h_i^2$ esetén csak xy, x, y és 1 fordulhatnak elő monomként a h_i-k között (monom alatt egyetlen tagból álló polinomot értünk). Ennek megfelelően $\beta_1 = (1, 1)$, $\beta_2 = (1, 0)$, $\beta_3 = (0, 1)$, $\beta_4 = (0, 0)$. Ezekre felírva az algoritmus első lépésében szereplő lineáris rendszert:

$b_{1,1} = 1; \quad 2b_{1,2} = 0; \quad 2b_{1,3} = 0; \quad 2b_{1,4} + 2b_{2,3} = 0;$

$b_{2,2} = 1; \quad 2b_{2,4} = 0;$

$b_{3,3} = 1; \quad 2b_{3,4} = 0;$

$b_{4,4} = 1.$

A fentiek alapján már fel tudjuk írni f Gram-mátrixát:

$$B := \begin{pmatrix} 1 & 0 & 0 & \lambda \\ 0 & 1 & -\lambda & 0 \\ 0 & -\lambda & 1 & 0 \\ \lambda & 0 & 0 & 1 \end{pmatrix}.$$

A következő lépésben B karakterisztikus polinomját kell meghatároznunk.

$$k_B(y) = y^4 - 4y^3 + (6 - 2\lambda^2)y^2 + (4\lambda^2 - 4)y + (\lambda^4 - 2\lambda^2 + 1).$$

A B mátrix akkor és csak akkor lesz pozitív szemidefinit, ha teljesül $-1 \leq \lambda \leq 1$. Vegyük észre, hogy $\lambda = \pm 1$ esetén $rank(B) = 2$, minden más esetben pedig B rangja 4. Ennek következtében tehát f 2 vagy 4 négyzet összegeként írható fel.

Tekintsük a B mátrix előállítását az alábbi 3 mátrix szorzataként: $B = V \cdot D \cdot V^T$. A szorzatban szereplő D mátrixot B diagonalizálásával kaptuk, V-t pedig B-ből elhagyva a szigorú felsőháromszög-mátrixot, tehát:

$$D := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1-\lambda^2 & 0 \\ 0 & 0 & 0 & 1-\lambda^2 \end{pmatrix},$$

$$V := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -\lambda & 1 & 0 \\ \lambda & 0 & 0 & 1 \end{pmatrix}.$$

Ez pedig a következő általános négyzetösszeg-felbontáshoz vezet:

$$f = (xy + \lambda)^2 + (x - \lambda y)^2 + (\sqrt{1 - \lambda^2} y)^2 + (\sqrt{1 - \lambda^2})^2.$$

2.3.1. Megjegyzés. A $\lambda = 0$ eset az eredeti f polinomot adja, 4 tag négyzeteként előállítva.

3. fejezet

0 nyomú, 3×3-as szimmetrikus mátrix diszkriminánsa

Az első fejezet alapján a következő polinomot szeretnénk tehát átalakítani:

$$f = 24a_1^3a_2b_2^2 + 78a_1a_2b_1^2b_2^2 + 78a_1a_2b_1^2b_3^2 - 30a_1a_2b_2^2b_3^2 - 108a_1b_1^3b_2b_3 + 108a_1b_1b_2b_3^3 - 108a_2b_1^3b_2b_3 - 30a_1^3a_2b_3^2 + 78a_1^3a_2b_1^2 + 144a_1^2a_2^2b_1^2 - 18a_1^2a_2^2b_2^2 - 18a_1^2a_2^2b_3^2 + 24a_1^2b_1^2b_2^2 + 78a_1^2b_1^2b_3^2 + 24a_1^2b_2^2b_3^2 - 42a_1a_2b_1^4 + 12a_1a_2b_2^4 + 12a_1a_2b_3^4 + 4a_1^6 + 4a_2^6 + 4b_1^6 + 4b_2^6 + 4b_3^6 + 78a_1a_2^3b_1^2 + 12a_1^5a_2 - 3a_1^4a_2^2 + 12a_1^4b_1^2 - 3a_1^2a_2^4 - 15a_1^2b_1^4 + 12a_1^2b_2^4 - 15a_1^2b_3^4 + 12a_1^4b_2^2 + 12a_1^4b_3^2 - 26a_1^3a_2^3 + 12a_1a_2^5 - 15a_2^2b_1^4 - 15a_2^2b_2^4 + 12a_2^2b_3^4 + 12a_2^4b_1^2 + 12a_2^4b_2^2 + 12a_2^4b_3^2 + 12b_1^2b_2^4 + 12b_1^2b_3^4 + 12b_1^4b_2^2 + 12b_1^4b_3^2 + 12b_2^2b_3^4 + 12b_2^4b_3^2 - 30a_1a_2^3b_2^2 + 24a_1a_2^3b_3^2 + 78a_2^2b_1^2b_2^2 + 24a_2^2b_1^2b_3^2 + 24a_2^2b_2^2b_3^2 + 108a_1^2a_2b_1b_2b_3 + 108a_1a_2^2b_1b_2b_3 + 108a_2b_1b_2^3b_3 - 84b_1^2b_2^2b_3^2.$$

Alkalmazzuk az imént ismertetett algoritmust f-re.

3.1. A β-k meghatározása

Megnézzük, a fenti f polinom mely tagjaiban szerepel minden változó páros fokú hatványon. Ezekből a tagokból tudjuk ugyanis az algoritmushoz szükséges β_i

vektorokat meghatározni.

Rendeljünk ezért a fenti összeg minden tagjához egy-egy 5 hosszú karakterisztikus vektort, annak megfelelően, hogy az $(a_1, a_2, b_1, b_2, b_3)$ változók milyen hatványon szerepelnek a szorzatban.

Példa: a $24a_1^3a_2b_2^2$ taghoz az alábbi vektort rendeljük: $(3, 1, 0, 2, 0)$.

Ennek alapján a β_i-k meghatározása a következőképpen történik: a fenti összeg tagjaihoz rendelt vektorok közül válasszuk ki azokat, melyekben minden koordináta páros, ezen vektorok hosszát felezzük meg, majd indexeljük őket. Ily módon a következőre juthatunk:

$\beta_1 = (3, 0, 0, 0, 0)$, $\beta_2 = (0, 3, 0, 0, 0)$, $\beta_3 = (0, 0, 3, 0, 0)$, $\beta_4 = (0, 0, 0, 3, 0)$,
$\beta_5 = (0, 0, 0, 0, 3)$, $\beta_6 = (2, 1, 0, 0, 0)$, $\beta_7 = (1, 2, 0, 0, 0)$, $\beta_8 = (2, 0, 1, 0, 0)$,
$\beta_9 = (1, 0, 2, 0, 0)$, $\beta_{10} = (2, 0, 0, 1, 0)$, $\beta_{11} = (1, 0, 0, 2, 0)$, $\beta_{12} = (2, 0, 0, 0, 1)$,
$\beta_{13} = (1, 0, 0, 0, 2)$, $\beta_{14} = (0, 2, 1, 0, 0)$, $\beta_{15} = (0, 1, 2, 0, 0)$, $\beta_{16} = (0, 2, 0, 1, 0)$,
$\beta_{17} = (0, 1, 0, 2, 0)$, $\beta_{18} = (0, 2, 0, 0, 1)$, $\beta_{19} = (0, 1, 0, 0, 2)$, $\beta_{20} = (0, 0, 2, 1, 0)$,
$\beta_{21} = (0, 0, 1, 2, 0)$, $\beta_{22} = (0, 0, 2, 0, 1)$, $\beta_{23} = (0, 0, 1, 0, 2)$, $\beta_{24} = (0, 0, 0, 2, 1)$,
$\beta_{25} = (0, 0, 0, 1, 2)$, $\beta_{26} = (1, 1, 1, 0, 0)$, $\beta_{27} = (1, 1, 0, 1, 0)$, $\beta_{28} = (1, 1, 0, 0, 1)$,
$\beta_{29} = (1, 0, 1, 1, 0)$, $\beta_{30} = (1, 0, 1, 0, 1)$, $\beta_{31} = (1, 0, 0, 1, 1)$, $\beta_{32} = (0, 1, 1, 1, 0)$,
$\beta_{33} = (0, 1, 1, 0, 1)$, $\beta_{34} = (0, 1, 0, 1, 1)$, $\beta_{35} = (0, 0, 1, 1, 1)$.

3.1.1. Emlékeztető. Az imént meghatározott β_i vektorok segítségével most már fel tudjuk írni a ♠-rendszert, azaz a

$$\sum_{\beta_i + \beta_j = \alpha} b_{i,j} = a_\alpha$$

kifejezést kell megoldanunk.

3.2. A ♠-rendszer

Veszünk egy α vektort, mely előáll néhány β_i vektor összegeként, majd megkeressük az összes lehetséges, β-kra való felbontását. Tudjuk emellett, hogy a keresett B mátrix egy adott elemét két-két β-vektor összege határozza meg, például a $b_{1,2}$ és $b_{2,1}$ elemeknek a $\beta_1 + \beta_2$ összeg felel meg. Ha pedig meghatároztuk egy α tagra a lehetséges β-beli felbontásokat, az ezeknek megfelelő mátrixbeli elemek összegét kell már csak egyenlővé tennünk az adott α tag f-beli együtthatójával.

A ♠-rendszer megoldásai az f polinom nemnulla együtthatójú tagjainak karakterisztikus vektoraira:

$(6,0,0,0,0)$: $\beta_1 + \beta_1$;

$(0,6,0,0,0)$: $\beta_2 + \beta_2$;

$(0,0,6,0,0)$: $\beta_3 + \beta_3$;

$(0,0,0,6,0)$: $\beta_4 + \beta_4$;

$(0,0,0,0,6)$: $\beta_5 + \beta_5$;

$(5,1,0,0,0)$: $\beta_1 + \beta_6$;

$(1,5,0,0,0)$: $\beta_2 + \beta_7$;

$(2,1,0,0,0)$: $\beta_6 + \beta_6$, $\beta_1 + \beta_7$;

$(1,2,0,0,0)$: $\beta_7 + \beta_7$, $\beta_2 + \beta_6$;

$(2,0,1,0,0)$: $\beta_8 + \beta_8$, $\beta_1 + \beta_9$;

$(1,0,2,0,0)$: $\beta_9 + \beta_9$, $\beta_3 + \beta_8$;

$(2,0,0,1,0)$: $\beta_{10} + \beta_{10}$, $\beta_1 + \beta_{11}$;

$(1,0,0,2,0)$: $\beta_{11} + \beta_{11}$, $\beta_4 + \beta_{10}$;

$(2,0,0,0,1)$: $\beta_{12} + \beta_{12}$, $\beta_1 + \beta_{13}$;

$(1,0,0,0,2)$: $\beta_{13} + \beta_{13}$, $\beta_5 + \beta_{12}$;

$(0,2,1,0,0)$: $\beta_{14}+\beta_{14}$, $\beta_2+\beta_{15}$;

$(0,1,2,0,0)$: $\beta_{15}+\beta_{15}$, $\beta_3+\beta_{14}$;

$(0,2,0,1,0)$: $\beta_{16}+\beta_{16}$, $\beta_2+\beta_{17}$;

$(0,1,0,2,0)$: $\beta_{17}+\beta_{17}$, $\beta_4+\beta_{16}$;

$(0,2,0,0,1)$: $\beta_{18}+\beta_{18}$, $\beta_2+\beta_{19}$;

$(0,1,0,0,2)$: $\beta_{19}+\beta_{19}$, $\beta_5+\beta_{18}$;

$(0,0,2,1,0)$: $\beta_{20}+\beta_{20}$, $\beta_3+\beta_{21}$;

$(0,0,1,2,0)$: $\beta_{21}+\beta_{21}$, $\beta_4+\beta_{20}$;

$(0,0,2,0,1)$: $\beta_{22}+\beta_{22}$, $\beta_3+\beta_{23}$;

$(0,0,1,0,2)$: $\beta_{23}+\beta_{23}$, $\beta_5+\beta_{22}$;

$(0,0,0,2,1)$: $\beta_{24}+\beta_{24}$, $\beta_4+\beta_{25}$;

$(0,0,0,1,2)$: $\beta_{25}+\beta_{25}$, $\beta_5+\beta_{24}$;

$(1,1,4,0,0)$: $\beta_3+\beta_{26}$, $\beta_9+\beta_{15}$;

$(1,1,0,4,0)$: $\beta_4+\beta_{27}$, $\beta_{11}+\beta_{17}$;

$(1,1,0,0,4)$: $\beta_5+\beta_{28}$, $\beta_{13}+\beta_{19}$;

$(3,3,0,0,0)$: $\beta_1+\beta_2$, $\beta_6+\beta_7$;

$(3,1,2,0,0)$: $\beta_1+\beta_{15}$, $\beta_6+\beta_9$, $\beta_8+\beta_{26}$;

$(3,1,0,2,0)$: $\beta_1+\beta_{17}$, $\beta_6+\beta_{11}$, $\beta_{10}+\beta_{27}$;

$(3,1,0,0,2)$: $\beta_1+\beta_{19}$, $\beta_6+\beta_{13}$, $\beta_{12}+\beta_{28}$;

$(1,3,2,0,0)$: $\beta_2+\beta_9$, $\beta_7+\beta_{15}$, $\beta_{14}+\beta_{26}$;

$(1,3,0,2,0)$: $\beta_2+\beta_{11}$, $\beta_7+\beta_{17}$, $\beta_{16}+\beta_{27}$;

$(1,3,0,0,2)$: $\beta_2+\beta_{13}$, $\beta_7+\beta_{19}$, $\beta_{18}+\beta_{28}$;

$(1,0,3,1,1)$: $\beta_3+\beta_{31}$, $\beta_9+\beta_{35}$, $\beta_{20}+\beta_{30}$, $\beta_{22}+\beta_{29}$;

$(0,1,3,1,1)$: $\beta_3+\beta_{34}$, $\beta_{15}+\beta_{35}$, $\beta_{20}+\beta_{33}$, $\beta_{22}+\beta_{32}$;

$(0,1,1,3,1)$: $\beta_4+\beta_{33}$, $\beta_{17}+\beta_{35}$, $\beta_{21}+\beta_{34}$, $\beta_{24}+\beta_{32}$;

$(1,0,1,1,3)$: $\beta_5+\beta_{29}$, $\beta_{13}+\beta_{35}$, $\beta_{23}+\beta_{31}$, $\beta_{25}+\beta_{30}$;

$(2,2,2,0,0)$: $\beta_{26}+\beta_{26}$, $\beta_6+\beta_{15}$, $\beta_7+\beta_9$, $\beta_8+\beta_{14}$;

$(2,2,0,2,0)$: $\beta_{27}+\beta_{27}$, $\beta_6+\beta_{17}$, $\beta_7+\beta_{11}$, $\beta_{10}+\beta_{16}$;

$(2,2,0,0,2)$: $\beta_{28}+\beta_{28}$, $\beta_6+\beta_{19}$, $\beta_7+\beta_{13}$, $\beta_{12}+\beta_{18}$;

$$
\begin{array}{llllll}
(2,0,2,2,0): & \beta_{29}+\beta_{29}, & \beta_8+\beta_{21}, & \beta_9+\beta_{11}, & \beta_{10}+\beta_{20}; & \\
(2,0,2,0,2): & \beta_{30}+\beta_{30}, & \beta_8+\beta_{23}, & \beta_9+\beta_{13}, & \beta_{12}+\beta_{22}; & \\
(2,0,0,2,2): & \beta_{31}+\beta_{31}, & \beta_{10}+\beta_{25}, & \beta_{11}+\beta_{13}, & \beta_{12}+\beta_{24}; & \\
(0,2,2,2,0): & \beta_{32}+\beta_{32}, & \beta_{14}+\beta_{21}, & \beta_{15}+\beta_{17}, & \beta_{16}+\beta_{20}; & \\
(0,2,2,0,2): & \beta_{33}+\beta_{33}, & \beta_{14}+\beta_{23}, & \beta_{15}+\beta_{19}, & \beta_{18}+\beta_{22}; & \\
(0,2,0,2,2): & \beta_{34}+\beta_{34}, & \beta_{16}+\beta_{25}, & \beta_{17}+\beta_{19}, & \beta_{18}+\beta_{24}; & \\
(0,0,2,2,2): & \beta_{35}+\beta_{35}, & \beta_{20}+\beta_{25}, & \beta_{21}+\beta_{23}, & \beta_{22}+\beta_{24}; & \\
(1,1,2,2,0): & \beta_9+\beta_{17}, & \beta_{11}+\beta_{15}, & \beta_{29}+\beta_{32}, & \beta_{20}+\beta_{27}, & \beta_{21}+\beta_{26}; \\
(1,1,2,0,2): & \beta_9+\beta_{19}, & \beta_{13}+\beta_{15}, & \beta_{30}+\beta_{33}, & \beta_{22}+\beta_{28}, & \beta_{23}+\beta_{26}; \\
(1,1,0,2,2): & \beta_{11}+\beta_{19}, & \beta_{13}+\beta_{17}, & \beta_{31}+\beta_{34}, & \beta_{24}+\beta_{28}, & \beta_{25}+\beta_{27}; \\
(2,1,1,1,1): & \beta_6+\beta_{35}, & \beta_8+\beta_{34}, & \beta_{10}+\beta_{33}, & \beta_{12}+\beta_{32}, & \beta_{26}+\beta_{31}, \\
(1,2,1,1,1): & \beta_7+\beta_{35}, & \beta_{14}+\beta_{31}, & \beta_{16}+\beta_{30}, & \beta_{18}+\beta_{29}, & \beta_{23}+\beta_{26}; \\
 & \beta_{27}+\beta_{33}, & \beta_{28}+\beta_{32}. & & &
\end{array}
$$

3.3. A B mátrix elkészítése

A keresett B mátrixot a következőképp építjük fel a fenti β-felbontások segítségével: egy csupa 0-ból álló mátrixból indulunk ki, majd minden lépésben hozzávesszük a $\spadesuit$-rendszer egy-egy sorát, azaz az f polinom egy-egy tagját, míg minden tagot be nem vettünk. Egy újabb tag felvételét a következő három példán szemléltetjük:

Az a_1^6 tag, s az ennek megfeleltetett $(6,0,0,0,0)$ vektor csak egyféleképp áll elő β-k összegeként, méghozzá $2\beta_1$ alakban. a_1^6 együtthatója 4, ennek megfelelően tehát a B mátrixban: $b_{1,1} := 4$.

A $(3,3,0,0,0)$ karakterisztikus vektorú tag előáll úgy is, mint $\beta_1 + \beta_2$, és úgy is, mint $\beta_6 + \beta_7$. Ez a B mátrix $b_{1,2}, b_{2,1}, b_{6,7}, b_{7,6}$ elemeinek felel meg. Mivel tudjuk, hogy ezen elemek összege megfelel a tag együtthatójának (ami -26), valamint B szimmetrikussága miatt: $b_{1,2} = b_{2,1} := \mu$, $b_{6,7} = b_{7,6} := 13 - \mu$.

A 78 együtthatójú $(3, 1, 2, 0, 0)$ esetén pedig a következő három felbontás adódik: $\beta_1 + \beta_{15}$, $\beta_6 + \beta_9$ és $\beta_8 + \beta_{26}$, amiből pedig a következőt kapjuk: $b_{1,15} = b_{15,1} := \gamma$, $b_{6,9} = b_{9,6} := \zeta$, $b_{8,26} = b_{26,8} = 39 - \gamma - \zeta$.

3.3.1. Megjegyzés. Könnyen látható, hogy a B mátrix mérete 35×35, mivel pontosan ennyi β vektor határozza meg.

Ha a mátrixot elkészítjük a fenti módon, látható, hogy B sor- és oszlopcserék után gyakorlatilag négy diagonális blokkra bomlik, melyeket az alábbi β-k határoznak meg, a megfelelő sorrendben:

- B_1 blokk: a^3, b^3, a^2b, ab^2, ad^2, ae^2, af^2, bd^2, be^2, bf^2, def;
- B_2 blokk: a^2d, abd, aef, b^2d, bef, d^3, de^2, df^2;
- B_3 blokk: a^2e, abe, adf, b^2e, bdf, d^2e, e^3, ef^2;
- B_4 blokk: a^2f, abf, ade, b^2f, bde, d^2f, e^2f, f^3.

Azért csak gyakorlatilag, mivel a polinom 0 együtthatójú tagjai még nem szerepelnek a felbontásban. Ezek mátrixba írásával azonban már nem lesz blokkdiagonális alakú. Az egyszerűség kedvéért tegyük fel, hogy a blokkokon kívül eső változókat mind 0-nak választjuk, ezt megtehetjük. Ekkor felső becslést kapunk a négyzetes tagok számára.

3.4. Előállítás legkevesebb négyzet összegeként

3.4.1. Tétel. Az f diszkrimináns felbontható 5 négyzet összegeként, ez az előállítás pedig a következő:

$$f = 27(aef - bef - de^2 + df^2)^2$$

$$+ (2a^3 + 3a^2b - 3ab^2 - ad^2 + 2ae^2 - af^2 - 2b^3 + bd^2 + be^2 - 2bf^2)^2$$

$$+ (4a^2d + 10abd + 3aef + 4b^2d + 3bef - 2d^3 + de^2 + df^2)^2$$

$$+ 4(a^2e + abe + 3adf - 2b^2e + 3bdf - 2d^2e + e^3 + ef^2)^2$$

$$+ 4(2a^2f - abf - 3ade - b^2f - 3bde + 2d^2f - e^2f - f^3)^2.$$

3.4.1. Bizonyítás. Tekintsük a fent definiált blokkokban szereplő változók alábbi megválasztását:

$$B_1 := \begin{pmatrix} 4 & -4 & 6 & -6 & -2 & 4 & -2 & 2 & 2 & -4 & 0 \\ -4 & 4 & -6 & 6 & 2 & -4 & 2 & -2 & -2 & 4 & 0 \\ 6 & -6 & 9 & -9 & -3 & 6 & -3 & 3 & 3 & -6 & 0 \\ -6 & 6 & -9 & 9 & 3 & -6 & 3 & -3 & -3 & 6 & 0 \\ -2 & 2 & -3 & 3 & 1 & -2 & 1 & -1 & -1 & 2 & 0 \\ 4 & -4 & 6 & -6 & -2 & 4 & -2 & 2 & 2 & -4 & 0 \\ -2 & 2 & -3 & 3 & 1 & -2 & 1 & -1 & -1 & 2 & 0 \\ 2 & -2 & 3 & -3 & -1 & 2 & -1 & 1 & 1 & -2 & 0 \\ 2 & -2 & 3 & -3 & -1 & 2 & -1 & 1 & 1 & -2 & 0 \\ -4 & 4 & -6 & 6 & 2 & -4 & 2 & -2 & -2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$B_2 := \begin{pmatrix} 16 & 40 & 12 & 16 & 12 & -8 & 4 & 4 \\ 40 & 100 & 30 & 40 & 30 & -20 & 10 & 10 \\ 12 & 30 & 9+27 & 12 & 9-27 & -6 & 3-27 & 3+27 \\ 16 & 40 & 12 & 16 & 12 & -8 & 4 & 4 \\ 12 & 30 & 9-27 & 12 & 9+27 & -6 & 3+27 & 3-27 \\ -8 & -20 & -6 & -8 & -6 & 4 & -2 & -2 \\ 4 & 10 & 3-27 & 4 & 3+27 & -2 & 1+27 & 1-27 \\ 4 & 10 & 3+27 & 4 & 3-27 & -2 & 1-27 & 1+27 \end{pmatrix},$$

$$B_3 := \begin{pmatrix} 4 & 4 & 12 & -8 & 12 & -8 & 4 & 4 \\ 4 & 4 & 12 & -8 & 12 & -8 & 4 & 4 \\ 12 & 12 & 36 & -24 & 36 & -24 & 12 & 12 \\ -8 & -8 & -24 & 16 & -24 & 16 & -8 & -8 \\ 12 & 12 & 36 & -24 & 36 & -24 & 12 & 12 \\ -8 & -8 & -24 & 16 & -24 & 16 & -8 & -8 \\ 4 & 4 & 12 & -8 & 12 & -8 & 4 & 4 \\ 4 & 4 & 12 & -8 & 12 & -8 & 4 & 4 \end{pmatrix},$$

$$B_4 := \begin{pmatrix} 16 & -8 & -24 & -8 & -24 & 16 & -8 & -8 \\ -8 & 4 & 12 & 4 & 12 & -8 & 4 & 4 \\ -24 & 12 & 36 & 12 & 36 & -24 & 12 & 12 \\ -8 & 4 & 12 & 4 & 12 & -8 & 4 & 4 \\ -24 & 12 & 36 & 12 & 36 & -24 & 12 & 12 \\ 16 & -8 & -24 & -8 & -24 & 16 & -8 & -8 \\ -8 & 4 & 12 & 4 & 12 & -8 & 4 & 4 \\ -8 & 4 & 12 & 4 & 12 & -8 & 4 & 4 \end{pmatrix}.$$

Erre a kitöltésre

$$rank(B) = rank(B_1) + rank(B_2) + rank(B_3) + rank(B_4) = 5,$$

a 2. fejezetben ismertetett módon pedig a szorzat a fenti négyzetösszeget fogja adni az induló f polinomra. $\square$

4. fejezet

Ideálbővítések

A valós algebrai geometria egy kiemelkedő problémaköre a $Variety(I, \mathbb{R}^k)$ varietás valós megoldásai számának meghatározása. Bár a Hermite-féle kvadratikus forma használható erre, azonban ezen algoritmus műveletigénye $\mathcal{O}(n^4)$. Nagyon sok esetben n, azaz a dimenzió mérete elég nagy, így szeretnénk ezt a számot redukálni valamilyen úton.

A dimenzió méretét a komplex megoldások határozzák meg, ezekkel azonban általában nem törődünk. Eliminálni szeretnénk tehát bizonyos komplex megoldásokat úgy, hogy eközben a valós megoldások halmazát változatlanul hagyjuk. Az alábbiakban erre adunk egy módszert: belátjuk, hogy valós együtthatós polinomok négyzetösszegeinek segítségével bővíteni tudjuk az I ideált anélkül, hogy változtassunk a valós megoldások halmazán.

4.1. Definíciók

4.1.1. Definíció *(Algebra)*. Legyen T test. Azt mondjuk, hogy A algebra a T test felett, ha A-ban van értelmezve van az összeadás, a szorzás, és a T elemeivel mint skalárokkal való szorzás úgy, hogy (1) A az összeadásra és a szorzásra gyűrű;

(2) A az összeadásra és a skalárral való szorzásra vektortér T felett; (3) tetszőleges $a, b \in A$ és $\lambda \in T$ esetén $\lambda(ab) = (\lambda a)b = a(\lambda b)$.

4.1.2. Definíció *(Bal- és jobbideál).* Egy R gyűrű egy I részhalmazát balideálnak nevezzük, ha az összeadásra nézve részcsoport, és minden $a \in I$, $r \in R$ esetén $ra \in I$. Hasonlóképpen I jobbideál, ha részcsoport, és tetszőleges $a \in I$, $r \in R$ esetén $ar \in I$.

4.1.3. Definíció *(Ideál).* I (kétoldali) ideál, ha bal- és jobbideál is egyúttal. Azt, hogy I ideál R-ben, $I \triangleleft R$ jelöli.

4.1.4. Definíció *(Generált ideál).* Tegyük fel, hogy X részhalmaza az R gyűrűnek. Az R legszűkebb, X-et tartalmazó ideálját az X által generált ideálnak nevezzük.

4.1.5. Definíció *(Azonosság).* Legyen $t_1, t_2 \in F^\tau(x_1, \ldots, x_n)$ két τ típusú kifejezés, ahol n alkalmas egész szám. Azt mondjuk, hogy az n-változós $t_1 \approx t_2$ azonosság teljesül a τ típusú A algebrában, ha tetszőleges $a_1, \ldots, a_n \in A$ elemekre $t_1^A(a_1, \ldots, a_n) = t_2^A(a_1, \ldots, a_n)$. Ezt $A \vDash t_1 \approx t_2$ (vagy egyszerűen $A \vDash t_1 \vDash t_2$) jelöli.

4.1.6. Definíció *(Varietás).* Azonos típusú algebrák egy $\mathcal{V}$ osztályát varietásnak nevezzük, ha azonosságokkal definiálható, vagyis ha van azonosságok egy olyan I halmaza, hogy $A \in \mathcal{V}$ akkor és csak akkor, ha $A \vDash t_1 \vDash t_2$ teljesül minden I-beli $t_1 = t_2$ azonosságra.

Most kimondunk és bizonyítunk egy tételt, mely az imént említett ideálbővítésről szól.

4.1.7. Tétel. Legyenek $a_1, \ldots, a_n$ az R polinomalgebra elemei. Ha az $a_1^2 + \cdots + a_n^2$ polinom benne van az I ideálban, akkor

$$Variety(I, \mathbb{R}^k) = Variety(J, \mathbb{R}^k),$$

ahol J az $I \cup \{a_1, \dots, a_n\}$ elemek által generált ideál az R polinomalgebrában.

4.1.7. Bizonyítás.

$\supseteq$: $\forall P, Q$: $P \subseteq Q \subseteq R$ esetén $Variety(P, \mathbb{R}^k) \supseteq Variety(Q, \mathbb{R}^k)$.

$\subseteq$: Tekintsünk egy tetszőleges $x \in Variety(I, \mathbb{R}^k)$ elemet. Ebben az esetben teljesül az $a_1^2(x) + \dots + a_m^2(x) = 0$ összefüggés. Ebből pedig következik, hogy $a_1(x) = \dots = a_m(x) = 0$. Tehát $x \in Variety(I \cup \{a_1, \dots, a_m\}, \mathbb{R}^k)$. $\square$

Az alábbiakban ismertetünk két példát a fenti tétel alkalmazására.

4.1.8. Példa. Legyen $R := \mathbb{R}[X]$ az egyváltozós, valós polinomok feletti algebra. Legyen emellett I az $X^2 + 1$ polinom által generált ideál. Ekkor az $A := R/I$ algebrára $dim(A) = 2$, pontosabban az 1 és az X polinomok adják egy bázisát. Vegyük észre, hogy az $X^2 + 1^2$ polinom is benne van az I ideálban. Ebből adódóan hozzáadhatjuk X-et és 1-et az ideálhoz úgy, hogy eközben nem változik a valós megoldások halmaza. A J ideál viszont, melyet az 1, X és X^2 elemek generálnak, megfelel a teljes R polinomalgebrának, így pedig $R/J = R/R$ dimenziója 0.

4.1.9. Példa. Legyen ismét $R := \mathbb{R}[X]$. Tekinsük azt az I ideált R-ben, melyet az $X(X^2 + 1)$ polinom generál. Ebben az esetben az $A := R/I$ algebra dimenziója 3, egy lehetséges bázisát az 1, X és X^2 polinomok adják. Látható továbbá, hogy az $X^4 + X^2 = X^2(X^2 + 1)$ polinom is eleme az I ideálnak, ezért hozzávehetjük az ideálhoz az X^2 és X polinomokat. Az így kapott J bővített ideál, melyet az X, X^2 és $X(X^2 + 1)$ polinomok generálnak, megegyezik az X által generált ideállal. Az R/J algebrára pedig $dim(R/J) = 1$.

4.2. Pozitív szemidefinit mátrixok

4.2.1. Definíció *(Pozitív szemidefinit mátrix).* Legyen V valós vektortér a $\langle ., . \rangle$ belső szorzattal definiálva. Legyen M egy szimmetrikus mátrix (egy önadjungált lineáris leképezés $M : V \mapsto V$). Azt mondjuk, hogy az M mátrix pozitív szemidefinit, ha $\forall v \in V$ esetén $0 \leq \langle v, Mv \rangle$. Jelölés: $0 \leq M$.

A pozitív szemidefinit mátrixok halmazát számos eltérő karakterizációval is megadhatjuk. A következő tételben ezek közül ismertetünk néhányat.

4.2.2. Tétel. Tekintsük az $\mathbb{R}^n$ teret a szokásos belső szorzattal. Legyen M egy $n \times n$ méretű valós, szimmetrikus mátrix. Ekkor a következők ekvivalensek:

- Az M mátrix pozitív szemidefinit, azaz $0 \leq M$.
- M sajátértékei nemnegatívak, azaz $\forall i$: $0 \leq \lambda_i$.
- Az M mátrix minden N minorára teljesül $0 \leq det(N)$, azaz M minorai pozitív szemidefinitek.
- M minden főminorának determinánsa nemnegatív, azaz ezek szemidefinitek.
- Létezik egy olyan $n \times n$ méretű W mátrix, hogy $M = W^T W$, azaz M szignatúrája megegyezik a rangjával.
- Létezik olyan $n \times n$ méretű L és D mátrix, hogy $M = LDL^T$, ahol L egy olyan alsóháromszög-mátrix, melynek minden diagonáleleme 1, valamint a $D := diag(d_1, \ldots, n)$ diagonális mátrixnak minden együtthatója nemnegatív, azaz $\forall i : 0 \leq d_i$.

(Bizonyítás nélkül.)

4.2.3. Megjegyzés. Az utolsó pontban említett felbontás Cholesky-felbontás néven is ismert.

A következő tétel szemléletesen azt mondja ki, hogy ha egy pozitív szemidefinit mátrixnak egy diagonáleleme 0, akkor az abban a sorban és oszlopban található összes többi elemnek is 0-nak kell lennie.

4.2.4. Tétel. Legyen M egy pozitív szemidefinit mátrix. Ha $m_{ii} = 0$, akkor $\forall j$ esetén $m_{ij} = 0$ és $m_{ji} = 0$.

4.2.4. Bizonyítás. Tekintsünk egy tetszőleges $j \neq i$ számot, és vegyük az i, j pár által meghatározott minort:

$$\begin{pmatrix} 0 & m_{ij} \\ m_{ji} & m_{jj} \end{pmatrix}.$$

(Tegyük fel, hogy $j > i$, a $j < i$ eset bizonyítása analóg módon történik.) A fenti aldeterminánsnak nemnegatívnak kell lennie: $0 \leq -m_{ij}^2$. Ebből pedig következik az $m_{ij} = 0$ összefüggés. $\square$

Az eddigiekben pusztán algebrai szemszögből közelítettük meg a pozitív szemidefinit mátrixok halmazát. Az alábbi tételben, valamint az azt követő példában teszünk egy kisebb geometriai kitekintést.

4.2.5. Tétel. A pozitív szemidefinit mátrixok terének burka konvex, azaz

1. ha M_1, M_2 pozitív szemidefinit mátrixok, akkor az $M_1 + M_2$ mátrix is pozitív szemidefinit;
2. ha p egy nemnegatív valós szám, azaz $p \in \mathbb{R}$ és $0 \leq p$, M pedig pozitív szemidefinit, akkor a pM mátrix is pozitív szemidefinit.

(Bizonyítás nélkül.)

4.2.6. Példa. Vegyük az alábbi 2×2-es szimmetrikus mátrixot:

$$M := \begin{pmatrix} x & z \\ z & y \end{pmatrix}.$$

M akkor lesz pozitív szemidefinit, ha $0 \leq x$ és $0 \leq xy - z^2$. Az ezen két összefüggéssel megadott $\{(x, y, z) \in \mathbb{R}^3 : 0 \leq x \wedge 0 \leq xy - z^2\}$ halmaz egy olyan kúp, melynek szimmetriatengelye az $\{(x, x, 0) \in \mathbb{R}^3 : 0 \leq x\}$ sugár.

4.3. Példa ideálbővítésre

Legyen $R := R[X]$, és tekintsük az $X(X^2 + 1)$ polinom által generált ideált.

Legyen $A := R/I$.

Az A algebra művelettáblája a $\mathbf{b} := (1, X, X^2)^T$ bázisra nézve:

$\cdot$	1	X	X^2
1	1	X	X^2
X	X	X^2	$-X$
X^2	X^2	$-X$	$-X^2$

.

(Itt felhasználtuk a $X^3 \mapsto -X$ helyettesítést.) Legyen M egy szimmetrikus, 3×3 méretű szimmetrikus mátrix:

$$M := \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{01} & m_{11} & m_{12} \\ m_{02} & m_{12} & m_{22} \end{pmatrix}.$$

Kezeljük M elemeit ismeretlenként. Azt szeretnénk, ha az M mátrix pozitív szemidefinit lenne, valamint az elemei kielégítenének bizonyos lineáris egyenleteket.

Tekintsük az alábbi összefüggést:

$$\mathbf{b}^T M\mathbf{b} = m_{00} + 2m_{01}X + (m_{11} + 2m_{02})X^2 + 2m_{12}X^3 + m_{22}X^4.$$

Vegyük észre, hogy ez a polinom akkor lesz benne az I ideálban, ha az A algebrában értéke 0.

Az A algebra felett a fenti polinom az alábbi alakra redukálódik:

$$m_{00} + 2(m_{01} - m_{12})X + (m_{11} - m_{22} + 2m_{02})X^2.$$

Ezen A-beli elem értéke akkor és csak akkor lesz 0, ha kielégíti az alábbi lineáris egyenleteket:

$$m_{00} = 0, m_{01} = m_{12}, m_{11} - m_{22} + 2m_{02} = 0.$$

Ez másképp azt jelenti, hogy az M mátrix formájára a következőt kaptuk:

$$M := \begin{pmatrix} 0 & s & u-t \\ s & 2t & s \\ u-t & s & 2t \end{pmatrix}.$$

Tekintsük most a $0 \leq M$ feltételt, azaz azt, hogy legyen M pozitív szemidefinit. Mivel $m_{00} = 0$, így M első sorának és oszlopának elemei mind 0-k lesznek, így $s = 0$ és $u = t$. A következő alakot kaptuk:

$$M := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2t & 0 \\ 0 & 0 & 2t \end{pmatrix}.$$

Vegyük észre, hogy $0 \leq M$ akkor és csak akkor, ha $0 \leq t$. Ezzel a következő négyzetösszeg-összefüggésre jutottunk az I ideálban:

$$\mathbf{b}^T M \mathbf{b} = 2t(X^2 + X^4).$$

Ennek következtében pedig bővíthetjük az I ideált az X és X^2 polinomokkal az X által generált J ideállá anélkül, hogy változna a valós megoldások halmaza.

Irodalomjegyzék

[1] Victoria Powers, Thorsten Wörmann: *An algorithm for sum of squares of real polynomials*. http://www.mathcs.emory.edu/˜vicki/pub/sos.pdf

[2] Kenneth R. Driessel: *Real algebraic geometry*. http://homepage.mac.com/driessel/IMA/realalg/sos.pdf

[3] Kiss Emil: *Bevezetés az algebrába*. Typotex, Budapest, 2007.

[4] Domokos Mátyás: *The discriminant of symmetric matrixes as a sum of squares and the orthogonal group*. http://arxiv.org/pdf/1003.0475