Questions to understand the topic of the lecture

- ▶ If exists a symmetric form that corresponds to a given quadratic form, then it is unique.
- How the coefficients of an analytic expression change if we change the basis?
- ▶ Is is true that no form over a vector space of characteristic two can be diagonalized?
- ▶ Is it true that if symmetric matrix A can be diagonalized by RAR^T, then R can always be chosen lower triangular?
- ▶ Is it true that when a quadratic form g on V over \mathbb{R} has diagonal matrix with some 1 and some -1, then there exist vectors \mathbf{u} , $\mathbf{w} \in V$ such that $g(\mathbf{u}) < 0 < g(\mathbf{w})$?

Bilinear and quadratic forms

Definition: Let V be a vector space over a field \mathbb{K} and let a mapping $f: V \times V \to \mathbb{K}$ satisfies:

$$\forall u, v \in V, \forall a \in \mathbb{K} : f(au, v) = f(u, av) = af(u, v)$$

$$\forall u, v, w \in V : f(u + v, w) = f(u, w) + f(v, w)$$

$$\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V : f(\mathbf{u}, \mathbf{v} + \mathbf{w}) = f(\mathbf{u}, \mathbf{v}) + f(\mathbf{u}, \mathbf{w})$$

Then f is called a *bilinear form* on V.

A bilinear form is *symmetric* if $\forall u, v \in V : f(u, v) = f(v, u)$.

A mapping $g: V \to \mathbb{K}$ is called a *quadratic form*, if there exists a bilinear form f such that $g(\mathbf{u}) = f(\mathbf{u}, \mathbf{u})$ for all $\mathbf{u} \in V$.

Examples: Any inner product on a space over \mathbb{R} , but not over $\mathbb{C}!$

For $V = \mathbb{Z}_5^2$, a bilinear form:

$$f(\mathbf{u}, \mathbf{v}) = u_1 v_1 + 2u_1 v_2 + 4u_2 v_1 + 3u_2 v_2$$

The corresponding quadratic form:

$$g(\mathbf{u}) = f(\mathbf{u}, \mathbf{u}) = u_1 u_1 + 2u_1 u_2 + 4u_2 u_1 + 3u_2 u_2 = u_1^2 + u_1 u_2 + 3u_2^2$$

Matrices of forms

Definition: Let V be a vector space over a field \mathbb{K} and let $X = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ be its basis. The *matrix of a bilinear form f w.r.t.* the basis X is the matrix \mathbf{B} defined as $b_{i,j} = f(\mathbf{v}_i, \mathbf{v}_j)$.

The matrix of a quadratic form g is the matrix of a symmetric bilinear form f corresponding to g, if such symmetric f exists.

Example: For $V = \mathbb{Z}_5^2$, and the canonical basis K, the bilinear form

$$f(\mathbf{u}, \mathbf{v}) = u_1 v_1 + 2u_1 v_2 + 4u_2 v_1 + 3u_2 v_2$$
 has matrix $\mathbf{B} = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$ and $g(\mathbf{u}) = u_1^2 + u_1 u_2 + 3u_2^2$ has matrix $\mathbf{B} = \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}$

On $V = \mathbb{Z}_2^2$ the quadratic form $g(\mathbf{u}) = u_1 u_2$ corresponds e.g. to the bilinear form with matrix $\mathbf{B} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ but to no symmetric.

Matrices of forms

Definition: Let V be a vector space over a field \mathbb{K} and let $X = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ be its basis. The matrix of a bilinear form f w.r.t. the basis X is the matrix \mathbf{B} defined as $b_{i,j} = f(\mathbf{v}_i, \mathbf{v}_i)$.

The matrix of a quadratic form g is the matrix of a symmetric bilinear form f corresponding to g, if such symmetric f exists.

Observation:
$$b_{i,j} = f(\mathbf{v}_i, \mathbf{v}_j) = \frac{1}{2}(g(\mathbf{v}_i + \mathbf{v}_j) - g(\mathbf{v}_i) - g(\mathbf{v}_j))$$

Proof: $g(\mathbf{v}_i + \mathbf{v}_j) = f(\mathbf{v}_i + \mathbf{v}_j, \mathbf{v}_i + \mathbf{v}_j)$
 $= f(\mathbf{v}_i, \mathbf{v}_i) + f(\mathbf{v}_i, \mathbf{v}_j) + f(\mathbf{v}_j, \mathbf{v}_i) + f(\mathbf{v}_j, \mathbf{v}_j)$
 $g(\mathbf{v}_i + \mathbf{v}_j) - g(\mathbf{v}_i) - g(\mathbf{v}_j) = f(\mathbf{v}_i, \mathbf{v}_j) + f(\mathbf{v}_j, \mathbf{v}_i)$

Observation: The use of matrices of forms:

$$f(\mathbf{u}, \mathbf{v}) = [\mathbf{u}]_{\mathbf{v}}^{\mathsf{T}} \mathbf{B}[\mathbf{v}]_{\mathbf{x}}, \quad g(\mathbf{u}) = [\mathbf{u}]_{\mathbf{v}}^{\mathsf{T}} \mathbf{B}[\mathbf{u}]_{\mathbf{x}}.$$

Proof: When $\mathbf{u} = \sum_{i=1}^{n} a_i \mathbf{v}_i$ and $\mathbf{w} = \sum_{i=1}^{n} b_i \mathbf{v}_i$, then

$$f(\boldsymbol{u}, \boldsymbol{w}) = f\left(\sum_{i=1}^{n} a_i \boldsymbol{v}_i, \sum_{i=1}^{n} b_j \boldsymbol{v}_i\right) = \sum_{i=1}^{n} \sum_{i=1}^{n} a_i f(\boldsymbol{v}_i, \boldsymbol{v}_j) b_j = [\boldsymbol{u}]_X^T \boldsymbol{B}[\boldsymbol{w}]_X$$

Definition: The *analytic expression* of a bilinear form f over \mathbb{K}^n with matrix B is the homogeneous polynomial

$$f((x_1,...,x_n)^T,(y_1,...,y_n)^T) = \sum_{i=1}^n \sum_{i=1}^n b_{i,j} x_i y_j$$

 \dots analogously for quadratic forms and/or relative to a basis X.

Observation: Let **B** be a matrix of a b/q form w.r.t. a basis X. Then $[id]_{YX}^T \mathbf{B}[id]_{YX}$ is the matrix of the same form w.r.t. Y.

Proof:
$$[\mathbf{u}]_X = [id]_{YX}[\mathbf{u}]_Y$$
, $[\mathbf{v}]_X = [id]_{YX}[\mathbf{v}]_Y$,
 $f(\mathbf{u}, \mathbf{v}) = [\mathbf{u}]_X^T \mathbf{B}[\mathbf{v}]_X = ([id]_{YX}[\mathbf{u}]_Y)^T \mathbf{B}[id]_{YX}[\mathbf{v}]_Y$

$$= [\boldsymbol{u}]_{Y}^{T}[id]_{YX}^{T}\boldsymbol{B}[id]_{YX}[\boldsymbol{v}]_{Y}.$$

Diagonalization of forms

Theorem: If g is a quadratic form on a vector space V of finite dimension n over a field \mathbb{K} other characteristics than 2, then the form g allows a diagonal matrix B w.r.t. a suitable basis X.

(holds also for symmetric bilinear forms)

Rephrased in terms of matrices:

Theorem: For any symmetric matrix $A \in \mathbb{K}^{n \times n}$ with char(\mathbb{K}) $\neq 2$ there is a regular matrix R such that $R^T A R$ is diagonal.

Compare with the diagonalization of *real* symmetric matrices (of linear maps) — there R could indeed be *orthogonal*: $R^T = R^{-1}$, hence $R^T A R = R^{-1} A R$.

Example: No way to diagonalize $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ over \mathbb{Z}_2 ,

but over
$$\mathbb{Z}_3$$
 it is possible: $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$

Theorem: For any symmetric matrix $A \in \mathbb{K}^{n \times n}$ with char(\mathbb{K}) $\neq 2$ there is a regular matrix R such that RAR^T is diagonal.

Proof: By induction on
$$n$$
.

Denote $\mathbf{A} = \mathbf{A}_n = \begin{bmatrix} \alpha & \mathbf{a}^T \\ \mathbf{a} & \tilde{\mathbf{A}} \end{bmatrix}$.

If $\alpha \neq 0$, let $\mathbf{P}_n = \begin{bmatrix} 1 & \mathbf{0}^T \\ -\frac{1}{\alpha}\mathbf{a} & \mathbf{I}_{n-1} \end{bmatrix}$.

Then $\mathbf{P}_n \mathbf{A}_n \mathbf{P}_n^T = \begin{bmatrix} 1 & \mathbf{0}^T \\ -\frac{1}{\alpha}\mathbf{a} & \mathbf{I}_{n-1} \end{bmatrix}$.

 $\begin{bmatrix} \alpha & \mathbf{a}^T \\ \mathbf{a} & \tilde{\mathbf{A}} \end{bmatrix}$.

 $\begin{bmatrix} 1 & -\frac{1}{\alpha}\mathbf{a}^T \\ \mathbf{a} & \tilde{\mathbf{A}} \end{bmatrix}$.

$$= \frac{\alpha}{0} \frac{\boldsymbol{a}^{T}}{-\frac{1}{\alpha}\boldsymbol{a}\boldsymbol{a}^{T} + \tilde{\boldsymbol{A}}} \cdot \frac{1}{0} \frac{-\frac{1}{\alpha}\boldsymbol{a}^{T}}{0} = \frac{\alpha}{0} \frac{0^{T}}{\boldsymbol{A}_{n-1}}$$

where $\mathbf{A}_{n-1} = \tilde{\mathbf{A}} - \frac{1}{\alpha} \mathbf{a} \mathbf{a}^T$ is symmetric.

Theorem: For any symmetric matrix $\mathbf{A} \in \mathbb{K}^{n \times n}$ with char(\mathbb{K}) $\neq 2$ there is a regular matrix R such that RAR^T is diagonal.

Proof: By induction on
$$n$$
.

Denote $\mathbf{A} = \mathbf{A}_n = \begin{bmatrix} \alpha & \mathbf{a}^T \\ \mathbf{a} & \tilde{\mathbf{A}} \end{bmatrix}$.

If
$$\alpha \neq 0$$
, let $P_n = \begin{bmatrix} 1 & 0^T \\ -\frac{1}{\alpha} \mathbf{a} & \mathbf{I}_{n-1} \end{bmatrix}$. Then $P_n \mathbf{A}_n P_n^T = \begin{bmatrix} \alpha & 0^T \\ 0 & \mathbf{A}_{n-1} \end{bmatrix}$

with A_{n-1} symmetric. By induction hyp.

there exists R_{n-1} for A_{n-1} . We choose $R_n =$

Then
$$\mathbf{R}_{n}\mathbf{A}_{n}\mathbf{R}_{n}^{T} = \begin{bmatrix} 1 & 0^{T} \\ 0 & \mathbf{R}_{n-1} \end{bmatrix} \cdot \mathbf{P}_{n}\mathbf{A}_{n}\mathbf{P}_{n}^{T} \cdot \begin{bmatrix} 1 & 0^{T} \\ 0 & \mathbf{R}_{n-1}^{T} \end{bmatrix}$$

$$= \begin{bmatrix} \alpha & 0^{T} \\ 0 & \mathbf{R}_{n-1}^{T} \end{bmatrix}$$
 is diagonal.

Theorem: For any symmetric matrix $\mathbf{A} \in \mathbb{K}^{n \times n}$ with char(\mathbb{K}) $\neq 2$ there is a regular matrix \mathbf{R} such that $\mathbf{R}\mathbf{A}\mathbf{R}^{\mathsf{T}}$ is diagonal.

Proof: By induction on
$$n$$
.

Denote $\mathbf{A} = \mathbf{A}_n = \begin{bmatrix} \alpha & \mathbf{a}^T \\ \mathbf{a} & \tilde{\mathbf{A}} \end{bmatrix}$.

If
$$\alpha \neq 0$$
, let $P_n = \begin{bmatrix} 1 & 0^T \\ -\frac{1}{\alpha} \mathbf{a} & \mathbf{I}_{n-1} \end{bmatrix}$. Then $P_n \mathbf{A}_n P_n^T = \begin{bmatrix} \alpha & 0^T \\ 0 & \mathbf{A}_{n-1} \end{bmatrix}$, with \mathbf{A}_{n-1} symmetric. By induction hyp.

with A_{n-1} symmetric. By induction hyp. there exists R_{n-1} for A_{n-1} . We choose $R_n = \begin{bmatrix} 1 & 0^T \\ 0 & R_{n-1} \end{bmatrix} \cdot P_n$ Then $R_n A_n R_n^T$ is diagonal.

Example:
$$\mathbb{K} = \mathbb{Z}_3$$
, $\mathbf{A}_3 = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 0 & 2 \\ 1 & 2 & 1 \end{pmatrix}$, $\alpha = 2$, $\mathbf{P}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$,

$$\mathbf{A}_{2} = \tilde{\mathbf{A}} - \frac{1}{\alpha} \mathbf{a} \mathbf{a}^{T} = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 2 \\ 1 \end{pmatrix} (2, 1) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \ \mathbf{R}_{2} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$

$$\mathbf{R}_{3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 2 & 1 \end{pmatrix}, \ \mathbf{R}_{3} \mathbf{A}_{3} \mathbf{R}_{3}^{T} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Theorem: For any symmetric matrix $A \in \mathbb{K}^{n \times n}$ with char(\mathbb{K}) $\neq 2$ there is a regular matrix R such that RAR^T is diagonal.

Proof: By induction on
$$n$$
.

Denote $\mathbf{A} = \mathbf{A}_n = \begin{bmatrix} \alpha & \mathbf{a}^T \\ \mathbf{a} & \tilde{\mathbf{A}} \end{bmatrix}$.

If $\alpha \neq 0$, let $\mathbf{P}_n = \begin{bmatrix} 1 & \mathbf{0}^T \\ -\frac{1}{\alpha}\mathbf{a} & \mathbf{I}_{n-1} \end{bmatrix}$. Then $\mathbf{P}_n\mathbf{A}_n\mathbf{P}_n^T = \begin{bmatrix} \alpha & \mathbf{0}^T \\ \mathbf{0} & \mathbf{A}_{n-1} \end{bmatrix}$.

with A_{n-1} symmetric. By induction hyp. there exists R_{n-1} for A_{n-1} . We choose $R_n = \begin{bmatrix} 1 & 0^T \\ 0 & R_{n-1} \end{bmatrix} \cdot P_n$ Then $R_n A_n R_n^T$ is diagonal.

If $\alpha=0$ but $a\neq 0$, then $a_{i,1}\neq 0$ for some i. Use the elementary matrix \boldsymbol{E} for adding the i-th row to the first. Take $\boldsymbol{A}'=\boldsymbol{E}\boldsymbol{A}\boldsymbol{E}^T$ instead of \boldsymbol{A} . As $\alpha'=2a_{i,1}\neq 0$, we may follow the previous case.

If
$$\alpha = 0$$
 and $\boldsymbol{a} = \boldsymbol{0}$, then let $\boldsymbol{A}_{n-1} = \tilde{\boldsymbol{A}}$ and get $\boldsymbol{R}_n = \begin{bmatrix} 1 & 0 \\ 0 & \boldsymbol{R}_{n-1} \end{bmatrix}$.

Sylvester's law of inertia

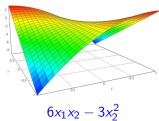
Theorem: Every quadratic form on a finitely generated real vector space allows a diagonal matrix with only 1, -1 and 0.

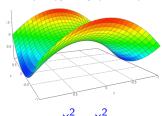
Moreover, all such diagonal matrices corresponding to the same form have the same number of 1's and the same number of -1's.

Example:
$$g: \mathbb{R}^2 \to \mathbb{R}$$
 given by $\mathbf{B} = \begin{pmatrix} 0 & 3 \\ 3 & -3 \end{pmatrix}$ w.r.t. K .

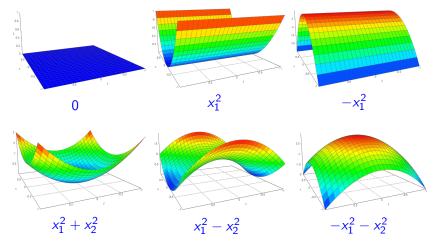
The matrix of g w.r.t. the basis: $X = \{(\frac{2}{3}, \frac{1}{3})^T, (-\frac{1}{3}, \frac{1}{3})^T\}$ is

$$\textbf{\textit{B}}' = [id]_{XK}^T \, \textbf{\textit{B}} \, [id]_{XK} = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 3 & -3 \end{pmatrix} \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$





The six cases of diagonalized quadratic forms $\mathbb{R}^2 \to \mathbb{R}$



(ordered by the rank and then 1 before -1)

Sylvester's law of inertia

Theorem: Every quadratic form on a finitely generated *real* vector space allows a diagonal matrix with only 1, -1 and 0.

Moreover, all such diagonal matrices corresponding to the same form have the same number of 1's and the same number of -1's.

Proof:

1. Existence: Let B be the matrix of the form. w.r.t. some basis X. Real symmetric matrices can be diagonalized, i.e. any $B = R^T DR$ for a regular R. $\begin{cases} = 0 & d'_{i,i} = 0, \\ = 0, \end{cases}$ si i = 1

for a regular
$$\emph{\textbf{R}}$$
. Split $\emph{\textbf{D}}$ as $\emph{\textbf{S}}^T\emph{\textbf{D}}'\emph{\textbf{S}}$ where $d_{i,i} = 0$, $d'_{i,i} = 0$, $s_{i,i} = 1$ > 0 $d'_{i,i} = 1$, $s_{i,i} = \sqrt{d_{i,i}}$ < 0 $d'_{i,i} = -1$, $s_{i,i} = \sqrt{-d_{i,i}}$

Now **SR** is regular and $\mathbf{B} = (\mathbf{SR})^T \mathbf{D}' \mathbf{SR}$.

Choose the basis Y, the coordinates of vectors of Y w.r.t. X are the columns of SR, i.e. $[id]_{YX} = SR$ and also $[id]_{XY} = (SR)^{-1}$. Now $[id]_{XY}^T B[id]_{XY} = ((SR)^{-1})^T (SR)^T D' SR(SR)^{-1} = D'$ is the desired diagonal matrix of the form.

2. Uniqueness of the numbers of 1's, -1's (and hence also 0's): Let $X = (\mathbf{u}_1, \dots, \mathbf{u}_n)$, $Y = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ be two bases s.t. the corresponding matrices \mathbf{B} and \mathbf{B}' of the form g are diagonal with 1's, -1's and 0's ordered. s.t. 1's are first, then -1's and 0's are last.

As products with regular matrices $[id]_{XY}$ do not change the rank: #0's in $\mathbf{B} = n - \text{rank}(\mathbf{B}) = n - \text{rank}(\mathbf{B}') = \#0$'s in \mathbf{B}' .

Let r=#1's in \boldsymbol{B} , s=#1's in \boldsymbol{B}' . If r>s, then consider the subspaces $\mathcal{L}(\boldsymbol{u}_1,\ldots,\boldsymbol{u}_r)$ and $\mathcal{L}(\boldsymbol{v}_{s+1},\ldots,\boldsymbol{v}_n)$. The sum of their dimensions r+n-s exceeds n, hence have a nontrivial intersection.

Choose $\mathbf{w} \in (\mathcal{L}(\mathbf{u}_1, \dots, \mathbf{u}_r) \cap \mathcal{L}(\mathbf{v}_{s+1}, \dots, \mathbf{v}_n)) \setminus \mathbf{0}$, hence $[\mathbf{w}]_X = (x_1, \dots, x_r, 0, \dots, 0)^T$, $[\mathbf{w}]_Y = (0, \dots, 0, y_{s+1}, \dots, y_n)^T$. Now $g(\mathbf{w}) = [\mathbf{w}]_X^T \mathbf{B}[\mathbf{w}]_X = x_1^2 + \dots + x_r^2 > 0$ (> as $\mathbf{w} \neq \mathbf{0}$), but $g(\mathbf{w}) = [\mathbf{w}]_Y^T \mathbf{B}'[\mathbf{w}]_Y = -y_{s+1}^2 - \dots - y_{rank(\mathbf{B}')}^2 \leq 0$, contradiction.

Therefore $r \not > s$, by symmetry also $s \not > r$, hence r = s.

Comments

Observation: Forms with real positive definite matrices are those that could be diagonalized into l_n

— compare Cholesky factorization $\mathbf{A} = \mathbf{U}^H \mathbf{U} = \mathbf{U}^T \mathbf{I}_n \mathbf{U}$.

Observation: An analogous statement for *complex symmetric* forms (other property than Hermitian!) yields diagonal matrices with 1's and 0's on the diagonal; including the inertia.

Quizz

- 1. True or false? The quadratic form obtained from an inner product on \mathbb{R} is the norm.
- 2. How many bilinear forms correspond to a quad. form on \mathbb{Z}_5^3 ? a) 1 b) 5 c) 15 d) 125 e) infinitely many
- 3. True or false? For any bilinear form f it holds that $h(\mathbf{u}, \mathbf{w}) = f(\mathbf{u}, \mathbf{w}) + f(\mathbf{w}, \mathbf{u})$ is a symmetric bilinear form.
- 4. The analytic expressions $g((x_1, x_2)^T)$ of a quadratic form gover \mathbb{R}^2 w.r.t. K and w.r.t. the basis $\{(0,1)^T, (1,0)^T\}$
 - a) are the same, which holds even for any other basis
 - b) are the same for this particular choice of bases
 - c) have the coefficients by x_1^2 and x_2^2 are exchanged
 - d) have no direct relationship between the coefficients
- 5. The triple (#1, #-1, #0) is called the *signature* of a form. How many distinct signatures exist for forms in \mathbb{R}^3 ?

- a) 3 b) 9 c) 10 d) 27 e) infinitely many