

Diagonalization

Given an $n \times n$ invertible symmetric matrix Q the function $Q(v, w) = v^T Q w$ is an example of a nondegenerate symmetric bilinear form

More generally, a nondegenerate symmetric bilinear form on \mathbb{Z}^n is a function $Q: \mathbb{Z}^n \times \mathbb{Z}^n \rightarrow \mathbb{Z}$ satisfying:

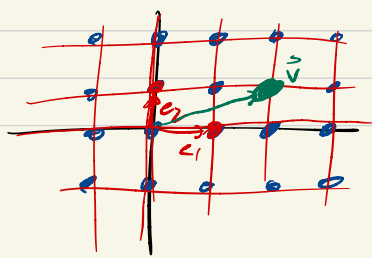
- $Q(v, w) = Q(w, v) \quad \forall v, w \in \mathbb{Z}^n$ (symmetric)
 - $Q(v_1 + v_2, w) = Q(v_1, w) + Q(v_2, w)$
 - $Q(c v, w) = c Q(v, w)$
 - $Q(v, w) = 0 \quad \forall w \in \mathbb{Z}^n \Rightarrow v = 0$ (nondegenerate)
- } linear in 1st factor

Any such function can be expressed as a matrix
But to write down the matrix, one needs a basis for \mathbb{Z}^n . If $B = \{b_1, \dots, b_n\}$, then the matrix for Q is written as Q_B and it is defined by:
(i, j)-th entry of $Q_B = Q(b_i, b_j)$

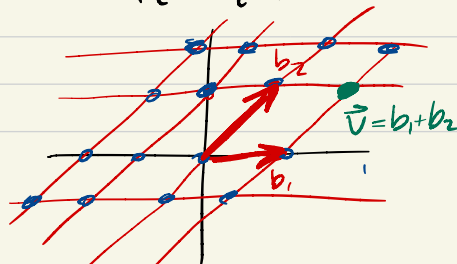
We have been using $\Sigma = \{e_1, \dots, e_n\}$ (the standard basis)

If we choose a different basis, then the matrix will look different

Ex: Consider bases $\Sigma = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ and $B = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$ for \mathbb{Z}^2



$$\vec{v} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}_B$$



Consider the symmetric bilinear form Q , given by
 $Q\left(\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = ac + bd$

$$\begin{aligned} \text{In } \Sigma, \quad Q(e_1, e_1) &= 1 \\ Q(e_1, e_2) &= 0 \\ Q(e_2, e_2) &= 1 \end{aligned} \Rightarrow Q_\Sigma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{aligned} \text{In } \mathcal{B}, \quad Q(b_1, b_1) &= Q\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = 1 \\ Q(b_1, b_2) &= Q\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = 1 \\ Q(b_2, b_2) &= Q\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = 2 \end{aligned} \Rightarrow Q_{\mathcal{B}} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

Sanity Check: Let $v = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_\Sigma = \begin{bmatrix} 1 \\ 1 \end{bmatrix}_{\mathcal{B}}$

$$\begin{aligned} \text{Then } Q(v, v) &= \begin{bmatrix} 2 & 1 \end{bmatrix}_\Sigma Q_\Sigma \begin{bmatrix} 2 \\ 1 \end{bmatrix}_\Sigma = 5 \\ Q(v, v) &= \begin{bmatrix} 1 & 1 \end{bmatrix}_{\mathcal{B}} Q_{\mathcal{B}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}_{\mathcal{B}} = 5 \end{aligned} \quad \checkmark$$

How are Q_Σ and $Q_{\mathcal{B}}$ related?

Theorem:

Let $\mathcal{B} = \{b_1, \dots, b_n\}$ be a basis for \mathbb{R}^n . Let $P = [b_1 \dots b_n]$
Then $Q_{\mathcal{B}} = P^T Q_\Sigma P$

Proof: Note that $P e_i = b_i \forall i$. Thus:

$$\begin{aligned} (i, j)\text{-th entry of } Q_{\mathcal{B}} &= Q(b_i, b_j) = b_i^T Q_\Sigma b_j = (P e_i)^T Q_\Sigma (P e_j) \\ &= e_i^T (P^T Q_\Sigma P) e_j = (i, j)\text{-th entry of } P^T Q_\Sigma P \end{aligned}$$

$$\Rightarrow Q_{\mathcal{B}} = P^T Q_\Sigma P$$

□

Def: A symmetric bilinear form Q is diagonalizable over \mathbb{Z} if \exists a basis B of \mathbb{Z}^n such that Q_B is diagonal (i.e. \exists matrix P such that $P^T Q_\mathbb{Z} P$ is diagonal)

Ex: $Q = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$ is diagonalizable over \mathbb{Z} :

$$B = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}, P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\text{then } P^T Q P = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix} \quad \checkmark$$

We can view changing basis as a

lattice isomorphism $\varphi: (\mathbb{Z}^n, Q_\mathbb{Z}) \rightarrow (\mathbb{Z}^n, Q_B)$
 $e_i \mapsto P e_i = b_i$

$$\left[\begin{array}{l} \text{by construction,} \\ Q_B(\varphi(e_i), \varphi(e_j)) = Q_B(b_i, b_j) = Q_\mathbb{Z}(e_i, e_j) \end{array} \right]$$

$\leadsto Q$ is diagonalizable iff \exists lattice isomorphism $\varphi: (\mathbb{Z}^n, Q_\mathbb{Z}) \rightarrow (\mathbb{Z}^n, Q_B)$ s.t. Q_B is diagonal.

Note: If $B = \{b_1, \dots, b_n\}$ is a basis for \mathbb{Z}^n and $P = [b_1, \dots, b_n]$, then $\det P = \pm 1$.

$$\text{Hence } \det Q_B = \det(P^T Q_\mathbb{Z} P) = \det P^T \det Q_\mathbb{Z} \det P = \det Q_\mathbb{Z}$$

If $\det Q_E = \pm 1$ and Q_E is diagonalizable, then

\exists basis B s.t. Q_B is diagonal

$$\neq |\det Q_B| = 1$$

$$\Rightarrow Q_B = \begin{bmatrix} \pm 1 & & & 0 \\ & \pm 1 & & \\ & & \ddots & \\ 0 & & & \pm 1 \end{bmatrix}$$

Def: A symmetric bilinear form Q is

- positive-definite if $Q(v,v) > 0 \quad \forall v \neq 0$
- negative-definite if $Q(v,v) < 0 \quad \forall v \neq 0$

Fact: Let Q be diagonalizable. Then:

- Q is pos-def iff all values of Q_E are positive
iff \exists basis B s.t. $Q_B = I$
- Q is neg-def iff all values of Q_E are negative.
iff \exists basis B s.t. $Q_B = -I$.

Def: The standard negative-definite lattice is $(\mathbb{Z}^n, -I_n)$
The standard positive-definite lattice is (\mathbb{Z}^n, I_n)

Putting this all together:

- If a positive-definite lattice (\mathbb{Z}^n, Q) with $\det Q = 1$ is diagonalizable then \exists lattice isomorphism $\varphi: (\mathbb{Z}^n, Q) \rightarrow (\mathbb{Z}^n, I)$
- If a negative-definite lattice (\mathbb{Z}^n, Q) with $\det Q = \pm 1$ is diagonalizable then \exists lattice isomorphism $\varphi: (\mathbb{Z}^n, Q) \rightarrow (\mathbb{Z}^n, -I)$

Ex: $Q = \begin{bmatrix} -2 & 3 \\ 3 & -5 \end{bmatrix}$. $\bullet \det Q = 1$
 \bullet eigenvalues both negative
 \Rightarrow neg-def

Let's show Q is diagonalizable over \mathbb{Z} by finding an isomorphism $\varphi: (\mathbb{Z}^2, Q) \rightarrow (\mathbb{Z}^2, -I_2)$

Let $\varphi(f_1) = x_1 e_1 + x_2 e_2 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, $\varphi(f_2) = y_1 e_1 + y_2 e_2 = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$

$\bullet -I(\varphi(f_1), \varphi(f_1)) = Q(f_1, f_1) = -2$
 $\bullet -I(x_1 e_1 + x_2 e_2, x_1 e_1 + x_2 e_2) = -x_1^2 - x_2^2$ } $\Rightarrow x_1, x_2 = \pm 1$

$\bullet -I(\varphi(f_2), \varphi(f_2)) = Q(f_2, f_2) = -5$
 $\bullet -I(y_1 e_1 + y_2 e_2, y_1 e_1 + y_2 e_2) = -y_1^2 - y_2^2$ } $\Rightarrow (y_1, y_2) \in \{(\pm 1, \pm 2), (\pm 2, \pm 1)\}$

$\bullet -I(\varphi(f_1), \varphi(f_2)) = Q(f_1, f_2) = 3$
 $\bullet -I(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}) = -x_1 y_1 - x_2 y_2$

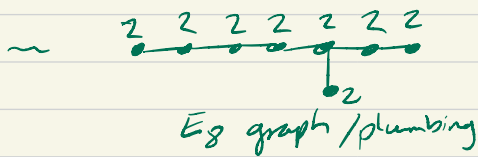
Set $x_1 = x_2 = 1$, $y_1 = -2$, $y_2 = -1 \Rightarrow$
 $\varphi(f_1) = e_1 + e_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
 $\varphi(f_2) = -2e_1 - e_2 = \begin{bmatrix} -2 \\ -1 \end{bmatrix}$
 \Rightarrow Embedding exists ✓

Note: $B = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -2 \\ -1 \end{bmatrix} \right\} \Rightarrow P = \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix}$

$\Rightarrow P^T Q P = \begin{bmatrix} 1 & 1 \\ -2 & -1 \end{bmatrix} \begin{bmatrix} -2 & 3 \\ 3 & -5 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ ✓

HW:

1. Let $E_8 = \begin{bmatrix} 2 & 1 & & & & & & 0 \\ & 1 & 2 & & & & & \\ & & 1 & 2 & & & & \\ & & & 1 & 2 & & & \\ & & & & 1 & 2 & & 1 \\ 0 & & & & & 1 & 2 & 0 \\ & & & & & & 1 & 2 & 0 \\ & & & & & & & 1 & 0 & 2 \end{bmatrix}$



Show that E_8 is not diagonalizable

(Hint: Show \nexists a lattice embedding into a suitable diagonal lattice)

2. Let Q be the incidence matrix for $\begin{array}{ccccccc} & \overbrace{-2 \dots -2}^{p-1} & & & & & \overbrace{-2 \dots -2}^{r-1} \\ & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \end{array}$ where $q \leq -2$, $p, r \geq 1$, and $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 0$

For which values of p, q, r does \exists embedding $(\mathbb{Z}^{p+r}, Q) \rightarrow (\mathbb{Z}^{p+r}, -I)$?

Read p.11, paragraph 3 to p.12 before section 3.2 in Greene-Sabukta