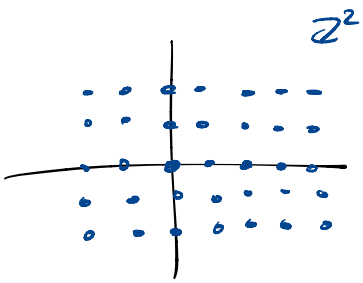
Symmetric Bilinear Forms on $\mathbb{Z}^n$

Let $\mathbb{Z}^n = \{(x_1, x_2, \dots, x_n) \in \mathbb{R}^n \mid x_i \in \mathbb{Z} \ \forall i\}$

(group under addition, $\mathbb{Z}$-module)

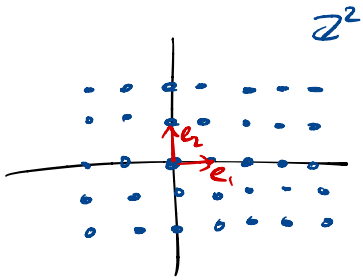


Def: A basis for $\mathbb{Z}^n$ is a set $B = \{b_1, \dots, b_n\} \subset \mathbb{Z}^n$ such that

- B is linearly independent
- $\forall\ v \in \mathbb{Z}^n$, $\exists\ c_1, \dots, c_n \in \mathbb{Z}$ such that $v = c_1 b_1 + \cdots + c_n b_n$

  (i.e. $\operatorname{Span}_{\mathbb{Z}}\{b_1, \dots, b_n\} = \mathbb{Z}^n$)

Ex: Let $e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}$, $\dots$, $e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$



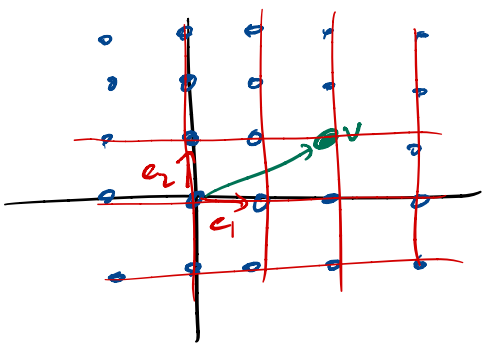
$\Sigma = \{e_1, \dots, e_n\}$ is the standard basis of $\mathbb{Z}^n$

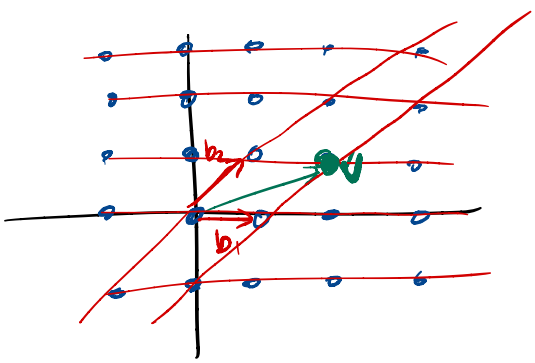
Any vector $v \in \mathbb{Z}^n$ can be expressed uniquely as a linear combination of $e_1, \dots, e_n$.

$$v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = v_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + v_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + v_n \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \sum_{i=1}^{n} v_i e_i \qquad (v_i \in \mathbb{Z})$$

Different bases give different coordinate systems

Ex: $\Sigma = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$ $\qquad$ $B = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right\}$





$v = 2e_1 + e_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_{\Sigma}$ $\qquad$ $v = b_1 + b_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}_{B}$

Def: A symmetric bilinear form on $\mathbb{Z}^n$ is a function $Q: \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}$ satisfying:

- $Q(v,w) = Q(w,v) \quad \forall \; v,w \in \mathbb{Z}^n$ (symmetric)
- $Q(v_1+v_2, w) = Q(v_1,w) + Q(v_2,w) \quad \forall \; v_1, v_2, w \in \mathbb{Z}^n$
- $Q(cv, w) = cQ(v,w) \quad \forall \; v,w \in \mathbb{Z}^n, \; c \in \mathbb{Z}$

(linearity)

Ex: $Q\left(\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = ac+bd$ (dot product)

- $Q\left(\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = ac+bd = ca+bd = Q\left(\begin{bmatrix} c \\ d \end{bmatrix}, \begin{bmatrix} a \\ b \end{bmatrix}\right)$
- $Q\left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} + \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = Q\left(\begin{bmatrix} a_1+a_2 \\ b_1+b_2 \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = (a_1+a_2)c + (b_1+b_2)d$

$$= (a_1c + b_1d) + (a_2c + b_2d)$$

$$= Q\left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) + Q\left(\begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right)$$

- $Q\left(k\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = Q\left(\begin{bmatrix} ka \\ kb \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right)$

$$= kac + kbd$$

$$= k(ac+bd)$$

$$= k\, Q\left(\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right)$$

Ex: Let A be a symmetric matrix with integer entries. Then $Q(v,w) = v^T A w$ is a symmetric bilinear form

e.g. $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow Q\left(\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = \begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = ab+cd$,

which is the previous example

In general, any symmetric bilinear form Q can be expressed as a symmetric matrix A as in the previous example as follows:

the (i,j)-th entry of A is $Q(e_i, e_j)$

However, if we choose a different basis for $\mathbb{Z}^n$, then we will obtain a different matrix

In general, if $B = \{b_1, \dots b_n\}$ is a basis for $\mathbb{Z}^n$, then Q has matrix representation Q_B given by: (i,j)-th entry of Q_B is $Q(b_i, b_j)$.

This means that $Q(u,v) = [u]_B^T Q_B [v]_B$

Ex: Consider $Q\left(\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right) = 2ac - bc - ad + 3bd$

and bases: $\mathcal{E} = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$, $B = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right\}$

In $\mathcal{E}$, $Q(e_1, e_1) = 2$

$Q(e_2, e_2) = 3$

$Q(e_1, e_2) = -1$

$\Rightarrow Q_{\mathcal{E}} = \begin{bmatrix} 2 & -1 \\ -1 & 3 \end{bmatrix}$

In B, $Q(b_1,b_1) = Q(e_1,e_1) = 2$

$Q(b_2,b_2) = Q\left(\begin{bmatrix}1\\1\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}\right) = 3$ $\quad\Rightarrow\quad Q_B = \begin{bmatrix}2 & 1\\ 1 & 3\end{bmatrix}$

$Q(b_1,b_2) = Q\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}\right) = 1$

Sanity Check: Let $v = \begin{bmatrix}2\\1\end{bmatrix}_E$. Recall $v = \begin{bmatrix}1\\1\end{bmatrix}_B$

$Q(v,v) = \begin{bmatrix}2 & 1\end{bmatrix} Q_E \begin{bmatrix}2\\1\end{bmatrix} = 7$ ✓

$Q(v,v) = \begin{bmatrix}1 & 1\end{bmatrix} Q_B \begin{bmatrix}1\\1\end{bmatrix} = 7$

Question: How are Q_E and Q_B related?

Theorem: Let $B = \{b_1, \dots, b_n\}$ be a basis for $\mathbb{R}^n$.
Let $P = [b_1 \cdots b_n]$ ($n \times n$ matrix with $\det P = \pm 1$)
Then $Q_B = P^T Q_E P$

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

(i,j)th entry of $Q_B = Q(b_i,b_j) = b_i^T Q_E b_j$

$= (Pe_i)^T Q_E (Pe_j)$

$= e_i^T (P^T Q_E P) e_j$

$= (i,j)$th entry of $P^T Q_E P$

$\Rightarrow Q_B = P^T Q_E P$ ∎

Note: $\det Q_B = \det(P^T Q_E P) = \det P^T \cdot \det Q_E \cdot \det P = \det Q_E$

So writing $\det Q$ is unambiguous

Def: A symmetric bilinear form Q is called nondegenerate if $Q(v,w)=0 \ \forall \ w \in \mathbb{Z}^n \Rightarrow v=0$

Fact: Q is nondegenerate if and only if Q_B is invertible for any basis B (if and only if $\det Q_B \neq 0$).

We will work fairly exclusively with nondegenerate symmetric bilinear forms on $\mathbb{Z}^n$.

Def: A symmetric bilinear form Q is
- positive definite if $Q(v,v)>0 \ \forall \ v \neq 0$
- negative definite if $Q(v,v)<0 \ \forall \ v \neq 0$

Ex: $Q_\mathcal{E}=I \Rightarrow Q$ is positive definite since
$Q(v,v) = v^T I v = v \cdot v > 0 \ \forall \ v \neq 0$.

$Q_\mathcal{E} = -I \Rightarrow Q$ is negative definite.

Fact: Q is positive/negative definite if and only if the eigenvalues of Q_B are positive/negative for any basis B.