LATTICE BASIS REDUCTION

3. GRAM-SCHMIDT ORTHOGONALIZATION

Alfred Menezes
cryptography101.ca

October 2025

Outline

1. Orthogonal bases
2. Projections
3. Existence of orthogonal bases
4. Gram-Schmidt orthogonalization
5. Gram-Schmidt and lattices

Orthogonal bases

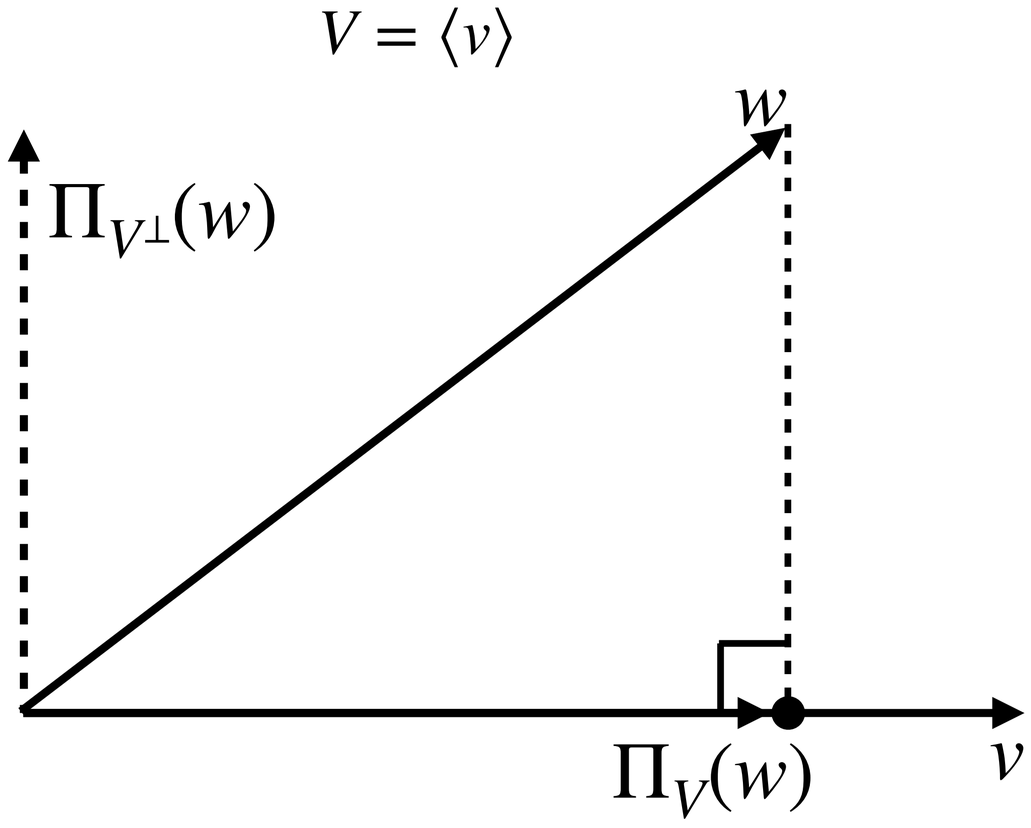
- Let V be a k-dimensional vector subspace of $\mathbb{R}^n$ with ordered basis $B = [b_1, \ldots, b_k]$.
- B is called an orthogonal basis for V if $\langle b_i, b_j \rangle = 0$ for all $1 \leq j < i \leq k$.
  - The dot product (or inner product) of $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{R}^n$ is $\langle u, v \rangle = u_1 v_1 + \cdots + u_n v_n$.
  - u and v are orthogonal if $\langle u, v \rangle = 0$.
  - The length of a vector u is $\|u\| = \sqrt{u_1^2 + \cdots + u_n^2} = \sqrt{\langle u, u \rangle}$, so $\langle u, u \rangle = \|u\|^2$.
- **Theorem**: V has an orthogonal basis.

Linear algebra background

- Let V be a k-dimensional vector subspace of $\mathbb{R}^n$ with ordered basis $B = [b_1, \ldots, b_k]$.
- The orthogonal complement of V is $V^\perp = \{x \in \mathbb{R}^n : \langle x, v \rangle = 0, \ \forall v \in V\}$.
  - $V^\perp$ is an $(n-k)$-dimensional subspace of $\mathbb{R}^n$.
- The basis B can be extended to a basis $[b_1, \ldots, b_k, b_{k+1}, \ldots, b_n]$ for $\mathbb{R}^n$, where $B^\perp = [b_{k+1}, \ldots, b_n]$ is a basis for $V^\perp$.
- Now, let $w \in \mathbb{R}^n$ and write $w = c_1 b_1 + \cdots + c_n b_n$ where $c_i \in \mathbb{R}$.
- Let $w_1 = c_1 b_1 + \cdots + c_k b_k$ and $w_2 = c_{k+1} b_{k+1} + \cdots + c_n b_n$.
- Then $w = w_1 + w_2$, where $w_1 \in V$ and $w_2 \in V^\perp$.

Projections

- **Definition**. The projection of $w \in \mathbb{R}^n$ onto V is $\Pi_V(w) = w_1$.
  - The projection of w onto $V^\perp$ is $\Pi_{V^\perp}(w) = w_2 = w - w_1 = w - \Pi_V(w)$.
  - Thus, $w = \Pi_V(w) + \Pi_{V^\perp}(w)$.



Exercises

1. Let $w, w_1, w_2 \in \mathbb{R}^n$, and suppose that $w = w_1 + w_2$ and $\langle w_1, w_2 \rangle = 0$.
   Prove that $\|w\|^2 = \|w_1\|^2 + \|w_2\|^2$.

2. Let V be a subspace of $\mathbb{R}^n$.
   Prove that $\Pi_{V^\perp}(w + u) = \Pi_{V^\perp}(w)$ for all $w \in \mathbb{R}^n$ and $u \in V$.

3. Let V be a subspace of $\mathbb{R}^n$.
   Prove that $\|w\| \geq \|\Pi_V(w)\|$ for all $w \in \mathbb{R}^n$.

Application of orthogonal bases

- **Lemma**. Let $B = [b_1, \ldots, b_k]$ be an orthogonal basis for $V \subseteq \mathbb{R}^n$, and let $w \in \mathbb{R}^n$.
  Then $\Pi_V(w) = \sum_{j=1}^{k} \frac{\langle w, b_j \rangle}{\|b_j\|^2} b_j$.

- **Proof**. Extend B to a basis $[b_1, \ldots, b_n]$ for $\mathbb{R}^n$, where $[b_{k+1}, \ldots, b_n]$ is a basis for $V^\perp$, and write $w = c_1 b_1 + \cdots + c_n b_n$ where $c_i \in \mathbb{R}$.

- For each $1 \leq j \leq k$, we have
  $$\langle w, b_j \rangle = \langle c_1 b_1 + \cdots + c_n b_n, b_j \rangle = c_1 \langle b_1, b_j \rangle + \cdots + c_n \langle b_n, b_j \rangle = c_j \langle b_j, b_j \rangle,$$
  whence, $c_j = \langle w, b_j \rangle / \langle b_j, b_j \rangle$.

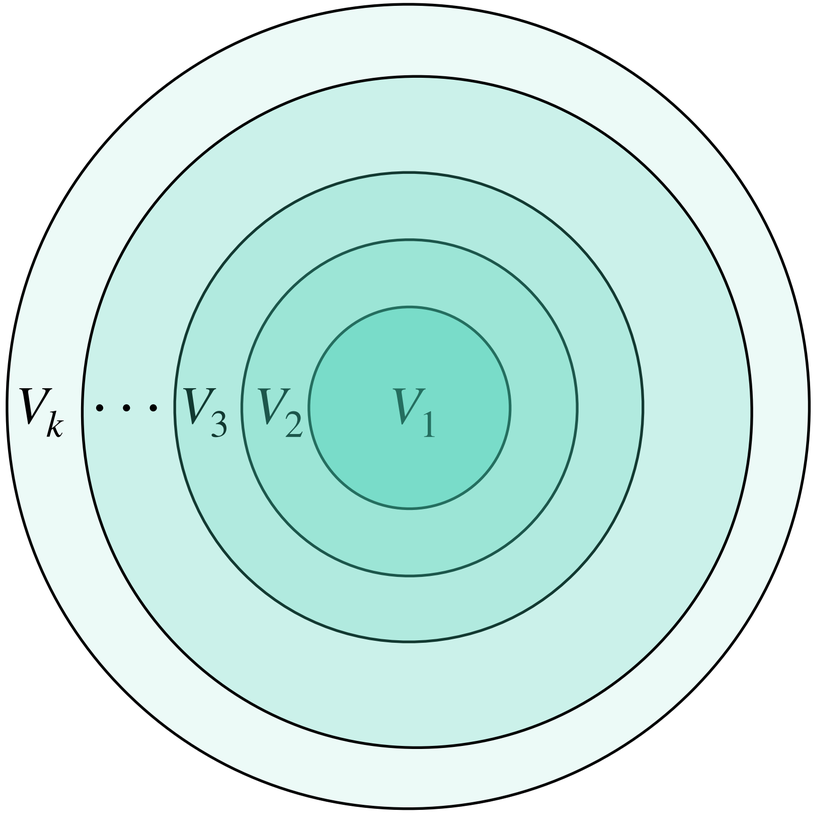
- Thus, $\Pi_V(w) = \sum_{j=1}^{k} \frac{\langle w, b_j \rangle}{\|b_j\|^2} b_j$. $\square$

Orthogonal bases exist (1)

- **Theorem**. Let V be a subspace of $\mathbb{R}^n$. Then V has an orthogonal basis.
- **Proof**. Let $B = [b_1, \ldots, b_k]$ be a basis for V.
  Define $b_1^* = b_1$, and for $2 \leq i \leq k$ define $V_{i-1}^* = \text{Span}(b_1^*, \ldots, b_{i-1}^*)$ and $b_i^* = \Pi_{(V_{i-1}^*)^\perp}(b_i)$.
  - So, b_i^* is the projection of b_i onto the orthogonal complement of the subspace spanned by the previously defined vectors $b_1^*, \ldots, b_{i-1}^*$.
  - To ease the notation, we'll write Π_i instead of $\Pi_{(V_i^*)^\perp}$.

Orthogonal bases exist (2)

- **Claim**. For $1 \leq i \leq k$, define $V_i = \text{Span}(b_1, \ldots, b_i)$ and $V_i^* = \text{Span}(b_1^*, \ldots, b_i^*)$. Then $V_i^* = V_i$ and $[b_1^*, \ldots, b_i^*]$ is an orthogonal basis for V_i^*.



- **Proof**. (by induction on i)
  - $V_1^* = V_1$ since $b_1^* = b_1$, and $[b_1^*]$ is an orthogonal basis for V_1^*.
  - Let $i \geq 2$, and suppose that $V_{i-1}^* = V_{i-1}$ and $[b_1^*, \ldots, b_{i-1}^*]$ is an orthogonal basis for V_{i-1}^*.
  - Now, $b_i^* = \Pi_{i-1}(b_i) = b_i - \Pi_{V_{i-1}^*}(b_i) = b_i - \Pi_{V_{i-1}}(b_i) \in V_i$, so $V_i^* \subseteq V_i$.

Orthogonal bases exist (3)

- **Proof of Claim** (cont'd).
  - And, $b_i = b_i^* + \Pi_{V_{i-1}^*}(b_i) \in V_i^*$, so $V_i \subseteq V_i^*$.
  - Hence, $V_i^* = V_i$, so $[b_1^*, \ldots, b_i^*]$ is a basis for V_i^*.
  - Finally, since $b_i^* \in (V_{i-1}^*)^\perp$, $\langle b_i^*, b_j^* \rangle = 0$ for all $1 \leq j \leq i-1$.
  - Thus, $[b_1^*, \ldots, b_i^*]$ is an orthogonal basis for V_i^*. □
- **Proof of Theorem** (cont'd).
  - $B^* = [b_1^*, \ldots, b_k^*]$ is an orthogonal basis for $V_k^* = V_k = V$.
  - Thus, V has an orthogonal basis. □

Gram-Schmidt orthogonalization

Input: A basis $B = [b_1, \ldots, b_k]$ for a k-dimensional subspace V of $\mathbb{R}^n$.

Output: An orthogonal basis $B^* = [b_1^*, \ldots, b_k^*]$ for V.

1. $b_1^* \leftarrow b_1$.
2. For i from 2 to k do
   (a) Compute $\mu_{ij} = \langle b_i, b_j^* \rangle / \|b_j^*\|^2$ for $1 \leq j < i$.
   (b) $b_i^* \leftarrow b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$.
3. Return$(B^* = [b_1^*, \ldots, b_k^*])$.

$$b_i^* = \Pi_{(V_{i-1}^*)^\perp}(b_i) = b_i - \Pi_{V_{i-1}^*}(b_i)$$

The μ_{ij} are called Gram-Schmidt (GS) coefficients.

Gram-Schmidt and lattices

- Let $B = [b_1, \ldots, b_n] \subseteq \mathbb{Z}^n$ be a basis for a full-rank integer lattice $L = L(B)$.
- Let $B^* = [b_1^*, \ldots, b_n^*]$ be its Gram-Schmidt basis, so $b_1^* = b_1$ and
  $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ for $2 \leq i \leq n$ where $\mu_{ij} = \langle b_i, b_j^* \rangle / \|b_j^*\|^2$.
- Note that B^* is in general *not* a basis for L since the μ_{ij} are typically not integers. Nonetheless, B^* reveals useful information about the lattice L.
- **Exercises**:
  1. Prove that $\|b_i^*\| \leq \|b_i\|$ for all $1 \leq i \leq n$.
  2. Prove that $\langle b_i, b_i^* \rangle = \langle b_i^*, b_i^* \rangle$ for all $1 \leq i \leq n$.

A lower bound for the first successive minimum

- **Theorem**. Let $B = [b_1, \ldots, b_n]$ be a basis for an integer lattice $L = L(B) \subseteq \mathbb{Z}^n$. Then $\lambda_1(L) \geq \min_i \|b_i^*\|$.

- **Proof**. Let $v \in L \backslash \{0\}$, and write $v = \sum_{i=1}^{n} v_i b_i$ where $v_i \in \mathbb{Z}$.

  Let k be the largest integer such that $v_k \neq 0$, so $v = \sum_{i=1}^{k} v_i b_i$.

  Now, $\langle v, b_k^* \rangle = \langle \sum_{i=1}^{k} v_i b_i, b_k^* \rangle = \langle \sum_{i=1}^{k-1} v_i b_i, b_k^* \rangle + \langle v_k b_k, b_k^* \rangle = v_k \langle b_k^*, b_k^* \rangle = v_k \|b_k^*\|^2$.

  Hence, $\Pi_{\langle b_k^* \rangle}(v) = \frac{\langle v, b_k^* \rangle}{\|b_k^*\|^2} b_k^* = v_k b_k^*$, from which we conclude that

  $\|v\| \geq \|v_k b_k^*\| = |v_k| \cdot \|b_k^*\| \geq \|b_k^*\| \geq \min_i \|b_i^*\|$. $\square$

Volume of a lattice (1)

- **Theorem**. Let $B = [b_1, \ldots, b_n]$ be a basis for an integer lattice $L = L(B) \subseteq \mathbb{Z}^n$. Then $\text{vol}(L) = \prod_{i=1}^{n} \|b_i^*\|$.

- **Proof**. Let B, B^* and Q be the $n \times n$ matrices whose ith columns are b_i, b_i^* and $b_i^*/\|b_i^*\|$, respectively. Let U be the following $n \times n$ upper-triangular matrix:

$$U = \begin{bmatrix} 1 & \mu_{21} & \mu_{31} & \cdots & \mu_{n1} \\ & 1 & \mu_{32} & \cdots & \mu_{n2} \\ & & 1 & \cdots & \mu_{n3} \\ & & & \ddots & \\ & & & & 1 \end{bmatrix},$$

and let D be the $n \times n$ diagonal matrix with diagonal entries $\|b_1^*\|, \ldots, \|b_n^*\|$.

Volume of a lattice (2)

- **Proof** (cont'd). By definition of the Gram-Schmidt basis, we have $B = B^*U$.
  Furthermore, $B^* = QD$.
  Since B^* is an orthogonal basis, Q is an orthogonal matrix, i.e., $Q^TQ = I_n$.
  Thus, $B = QDU$, whence

$$\text{vol}(L) = |\det(B)| = |\det(Q)\det(D)\det(U)| = |\det(D)| = \prod_{i=1}^{n} \|b_i^*\|. \ \square$$

- **Note**: Since L is an integer lattice, $\text{vol}(L) \in \mathbb{Z}_{\geq 1}$. Thus, $\prod_{i=1}^{n} \|b_i^*\| \in \mathbb{Z}_{\geq 1}$.