1. Bilinear forms

1.1. Bilinear forms and matrices.

Definition 1.1. Suppose that $F$ is a field and $V$ is a vector space over $F$. A bilinear form on $V$ is a map $B : V \times V \to F$ having the property that for all $w, x, y \in V$ and all $\lambda \in F$, the following hold
\[
B(w, x + y) = B(w, x) + B(w, y)
\]
\[
B(w, \lambda x) = \lambda B(w, x)
\]
\[
B(w + x, y) = B(w, y) + B(x, y)
\]
\[
B(\lambda w, x) = \lambda B(w, x).
\]

Definition 1.2. Suppose that $F$ is a field. A bilinear form over $F$ is a pair $B = (V, B)$ consisting of a finite dimensional vector space $V$ over $F$ and a bilinear form $B$ on $V$.

Example 1.3. Suppose that $V = F^n$ and for
\[
x = (x_1, \ldots, x_n)
\]
\[
y = (y_1, \ldots, y_n)
\]
we define $B(x, y) = x \cdot y = x_1y_1 + \cdots + x_ny_n$. Then $B$ is a bilinear form (this is the usual dot product).

Example 1.4. More generally suppose we are given $\lambda_1, \ldots, \lambda_n \in F$ and we define
\[
B(x, y) = \lambda_1x_1y_1 + \cdots + \lambda_nx_ny_n.
\]
Then $B$ is a bilinear form.

Example 1.5. Even more generally suppose we are given an $n \times n$ matrix $M = (\lambda_{ij})$. Then
\[
B(x, y) = \sum \lambda_{ij}x_iy_j
\]
is a bilinear form.
**Example 1.7.** The most degenerate case of Example 1.5 is when the matrix $M$ is zero. We will call this the zero form. There is one zero bilinear form of every dimension over $F$. We denote it by $0^n = (F^n, 0)$.

We should probably check that (1.6) is actually bilinear. There’s a relatively painless way to do this. Write $x$ and $y$ as column vectors. Then (1.6) can be re-written as

$$B(x, y) = x^T \cdot M \cdot y.$$ 

From this is easy to check the conditions.

Now we will show that every bilinear form arises in this way from a matrix. Suppose that $V$ is finite dimensional of dimension $n$, and that $\alpha = \{v_1, \ldots, v_n\}$ is an ordered basis of $V$. Define a matrix $B_\alpha$ by

$$(B_\alpha)_{ij} = B(v_i, v_j).$$

By writing $x \in V$ as $x = x_1v_1 + \cdots + x_nv_n$ we can represent each $x$ uniquely as a column vector

$$x_\alpha = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$ 

Then

$$B(x, y) = x_\alpha^T My_\alpha.$$ 

We now have two structures in linear algebra that correspond to square matrices. For a linear transformation $T : V \to V$ a choice of ordered basis $\alpha = \{v_1, \ldots, v_n\}$ of $V$ allows us to identify $V$ with $F^n$ and express $T$ as a matrix $T_\alpha^\alpha$. For another choice of ordered basis $\beta = \{w_1, \ldots, w_n\}$ we get another matrix $T_\beta^\beta$. The matrices $T_\alpha^\alpha$ and $T_\beta^\beta$ are related by

$$T_\beta^\beta = S^{-1}T_\alpha^\alpha S$$

where $S$ is the matrix constructed by solving

$$w_j = \sum s_{ij}v_i.$$ 

For a bilinear form $B : V \times V \to F$ a choice of ordered basis allows us to represent $B$ by a matrix $B_\alpha$ (your book denotes this as $\psi_\alpha(B)$). The bilinear form may then be computed as (1.9). If $\alpha$ and $\beta$ are two ordered bases, related by a matrix $S$ as above, then

$$B_\beta = S^T B_\alpha S.$$ 

Two matrices $M_1$ and $M_2$ are similar if there is an invertible matrix $S$ for which $M_2 = S^{-1}M_1S$. Thus linear transformations $T : V \to V$ correspond to matrices up to similarity. Two matrices $M_1$ and $M_2$ are congruent if there is an invertible matrix $S$ for which $M_2 = S^T M_1 S$. Bilinear forms correspond to matrices up to congruence.
1.2. Symmetric bilinear forms.

**Definition 1.10.** A bilinear form \( B \) is *symmetric* if \( B(x, y) = B(y, x) \) for all \( x, y \in V \).

**Exercise 1.1.** Show that \( B \) is symmetric if and only if for every ordered basis \( \alpha \), the matrix \( B_\alpha \) is a symmetric matrix.

**Definition 1.11.** A bilinear form \( B \) is *non-degenerate* for every \( 0 \neq v \in V \) there exists \( w \in V \) such that \( B(v, w) \neq 0 \).

**Exercise 1.2.** Show that a bilinear form on a finite dimensional vector space \( V \) is non-degenerate if and only if for every ordered basis \( (v_1, \ldots, v_n) \) the matrix \( B_\alpha \) is an invertible matrix.

**Exercise 1.3.** A bilinear form \( B \) on \( V \) gives a map \( \tilde{B} : V \to V^* \) defined by

\[
\tilde{B}(x)(y) = B(x, y).
\]

Show that \( B \) is non-degenerate if and only if \( \tilde{B} \) is a monomorphism.

We will now restrict our attention to symmetric bilinear forms. When the characteristic of \( F \) is not equal to 2 it turns out that every symmetric bilinear form can be put into the form of Example 1.5. This fact is called the *diagonalizability of quadratic forms* (over fields of characteristic not equal to 2). Danny and I went through the proof in class, but it’s worth thinking through some of the details.

**Theorem 1.12.** Suppose that \( B \) is a symmetric bilinear form on a finite dimensional vector space \( V \) over a field \( F \). If the characteristic of \( F \) is not equal to 2, then there is an ordered basis \( \alpha = \{v_1, \ldots, v_n\} \) of \( V \) having the property that

\[
B(v_i, v_j) = 0 \quad \text{if} \quad i \neq j. \tag{1.13}
\]

(equivalently the matrix \( B_\alpha \) is diagonal).

Let’s go through the proof. For the rest of this section we will assume that the characteristic of \( F \) is not 2.

**Lemma 1.14.** Suppose that \( B \) is a symmetric bilinear form on \( V \). If \( B \) is non-zero then there is a vector \( v \in V \) for which

\[
B(v, v) \neq 0.
\]

**Proof:** If \( B \) is non-zero there are vectors \( x, y \in V \) for which \( B(x, y) \neq 0 \). Using bilinearity and the fact that \( B \) is symmetric, we expand

\[
B(x + y, x + y) = B(x, x) + B(y, y) + 2B(x, y).
\]

Since \( 2 \neq 0 \in F \) the rightmost term is non-zero. It follows that at least one of the other terms must be non-zero. We can choose \( v \) to be \( x, y, \) or \( x + y \) accordingly. \( \square \)

It will also be useful to have some more terminology. Suppose that \((V, B)\) is a symmetric bilinear form over \( F \) and \( W \subset V \) is a subspace. We can then define a symmetric bilinear form \((W, B_W)\) by setting

\[
B_W(x, y) = B(x, y).
\]

**Definition 1.15.** The *restriction of \( B \) to \( W \) is the bilinear form \((W, B_W)\) constructed above.
Definition 1.16. Suppose that $U \subset V$ is a subset of $V$. The $B$-orthogonal complement (or just orthogonal complement) of $U$ is the set $U^\perp = \{ v \in V \mid B(u, v) = 0 \ \forall u \in U \}$.

Exercise 1.4. Show that $U^\perp$ is always a subspace of $V$.

Proof of Theorem 1.12: We prove the result by induction on the dimension of $V$. The result is obvious when $\dim V = 1$. Suppose then that $\dim V = n$ and we have proved the result for all symmetric bilinear forms on vector spaces of dimension less than $n$. If $B(x, y)$ is zero for all $x$ and $y$ then any basis of $V$ will satisfy. We may therefore suppose that $B$ is non-zero. By Lemma 1.14 there is a $v \in V$ for which $B(v, v) \neq 0$. Let $W = \{ v \}^\perp = \{ x \in V \mid B(v, x) = 0 \}$, and let $B_W$ be the restriction of $B$ to $W$, so that $B_W(x, y) = B(x, y)$.

Note that $W$ is the kernel of the linear transformation $B(v, -) : V \to F$.

Since $B(v, v) \neq 0$, this transformation is surjective, and so its kernel $W$ has dimension $(n - 1)$. We may therefore employ the induction hypothesis and produce a basis $\{v_1, \ldots, v_{n-1}\}$ of $W$ satisfying $B_W(v_i, v_j) = B(v_i, v_j) = 0$ if $i \neq j$.

Now one easily checks that $\{v_1, \ldots, v_{n-1}, v\}$ is a basis of $W$ satisfying (1.13). 

Exercise 1.5. Prove the last two assertions in the above proof: that $\{v_1, \ldots, v_{n-1}, v\}$ is indeed a basis of $W$ and that it satisfies (1.13).

Exercise 1.6. With the notation of the proof of Theorem 1.12, show that if $B$ is non-degenerate then so is $B_W$.

Exercise 1.7. Suppose that the characteristic of $F$ is not 2, and that $B$ is a symmetric bilinear form on a vector space $V$ of dimension $n$. Let $\{v_1, \ldots, v_n\}$ be a basis of $V$ satisfying (1.13), and let $\lambda_i = B(v_i, v_i)$. Is the set $\{\lambda_1, \ldots, \lambda_n\}$ determined by $B$? In other words does another basis satisfying (1.13) lead to the same set of $\lambda_i$’s?

Exercise 1.8. Show that if $F$ is the field of real numbers and $B$ is non-degenerate then one can find a basis $\{v_1, \ldots, v_n\}$ of $V$ for which $B(v_i, v_j) = 0$ if $i \neq j$ and for which $B(v_i, v_i) = \pm 1$ for $i = 1, \ldots, n$. Let $p$ be the number of $i$ for which $B(v_i, v_i) = 1$ and $q$ the number of $i$ for which $B(v_i, v_i) = -1$. The number $p - q$ is called the signature of $B$ and is independent of the choice of basis. The number $n$ is called the rank of $B$. A symmetric bilinear form over $\mathbb{R}$ is thus determined by its rank and its signature.

The exercise above ended with a slightly vague assertion which I’d like to make clearer. It will help to have some terminology. Suppose that $B_1 = (V_1, B_1)$ and $B_2 = (V_1, B_2)$ are two symmetric bilinear forms over $F$. 
Definition 1.17. An isometry of $B_1$ and $B_2$ is an invertible linear transformation $T : V_1 \to V_2$ having the property that for all $x, y \in V_1$

$$B_2(Tx, Ty) = B_1(x, y).$$

Two symmetric bilinear forms are isometric if there is an isometry between them.

Now we can state the conclusion of Exercise 1.8 more precisely. Let $\mathbb{R}^{p,q}$ be the bilinear form over $\mathbb{R}$ consisting of the vector space $\mathbb{R}^{p+q}$ and the bilinear form given by the diagonal matrix whose first $p$ entries are 1 and whose last $q$ entries are $-1$.

Exercise 1.9. Show that every symmetric bilinear form over $\mathbb{R}$ is isometric to $\mathbb{R}^{p,q}$ for some $p$ and $q$.

Here is another useful construction. Suppose at $B_1 = (V_1, B_1)$ and $B_2 = (V_2, B_2)$ are two symmetric bilinear forms over $F$.

Definition 1.18. The orthogonal sum of $B_1$ and $B_2$, is the bilinear form

$$B_1 \oplus B_2 = (V_1 \oplus V_2, B_1 \oplus B_2)$$

in which $B_1 \oplus B_2$ is given by

$$(B_1 \oplus B_2)((x_1, y_1), (x_2, y_2)) = B_V(x_1, y_1) + B_W(x_2, y_2).$$

The $n$-fold iterated orthogonal sum of $B$ with itself will be denoted $B^{\oplus n}$ (or just $B^n$ if no confusion is likely).

If $(V, B)$ is a bilinear form we say that vectors $x, y \in V$ are orthogonal (or $B$-orthogonal) if $B(x, y) = 0$.

Exercise 1.10. Show that in the orthogonal sum of $(V, B_1)$ with $(V_1, B_2)$, the vectors in $V_1$ are orthogonal to the vectors in $V_2$.

Exercise 1.11. Suppose that $(V, B)$ is a non-degenerate symmetric bilinear form, $W \subset V$ is a subspace and write $B_W$ for the restriction of $B$ to $W$. If $(V, B)$ is non-degenerate, must $(W, B_W)$ also be non-degenerate?

Exercise 1.12. Suppose that $(V, B)$ is asymmetric bilinear form and $W \subset B$ is a subspace. Define a map

$$B^T : V \to W^*$$

by $B^T(v)(w) = B(v, w)$. Show that if $B$ is non-degenerate then $B^T$ is surjective and that $\dim W^\perp + \dim W = \dim V$. Find an example of a non-degenerate $B$ for which the map $W \oplus W^\perp \to V$ is not an isomorphism.

As you may be guessing, we think of a symmetric bilinear form as a “generalized dot product” and borrow the terminology from there. Some things are a bit different in the usual case. For instance the expression $B(v, v)$ is analogous to the “squared norm” of $v$, but there is no reason it has to be a square, or even be non-zero. And there is generalized sense in which one might talk about it being “positive.”
2. Characteristic 2

Now let’s turn to the situation when $F = \mathbb{F}_2$ is the field with two elements. We begin with a few examples.

Example 2.1. Let $R = (F, R)$ be the bilinear form of rank 1 with $R(x, y) = xy$. Note that the $n$-fold orthogonal sum $R^n$ is just $F^n$ with the usual dot product. The matrix associated to $R \oplus \cdots \oplus R$ in the standard basis is the identity matrix.

Example 2.2. Let $H = (F^2, H)$ be the rank 2 symmetric bilinear form associated to the matrix

\[
\begin{pmatrix}
0 & 1 \\
1 & 0 \\
\end{pmatrix}
\]

Thus

\[
H\left(\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}\right) = x_1 y_2 + x_2 y_1.
\]

The matrix associated to $H \oplus \cdots \oplus H$ in the standard basis is the block diagonal matrix

\[
\begin{pmatrix}
0 & 1 & & & \\
1 & 0 & & & \\
& & \ddots & & \\
& & & 0 & 1 \\
& & & 1 & 0 \\
\end{pmatrix}
\]

This example gives me an occasion to talk about some further notation. When you’re talking about points in $F^n$ it’s customary to denote them by

\[
(x_1, \ldots, x_n).
\]

But when you’re doing linear algebra it is more useful to denote them by column vectors

\[
\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}
\]

This latter expression is inconvenient from the point of view of typography. There are a couple of ways around this. One is to refer to (2.5) as $[x_1, \ldots, x_n]^T$. Another is to use (2.4) and (2.5) interchangeably. That’s what I will do here. Thus I could write (2.3) as

\[
H((x_1, y_1), (x_2, y_2)) = x_1 y_2 + x_2 y_1.
\]

This does, however allow for a conflict of notation. The symbol (2.4) can refer to a $1 \times n$ matrix, or to the column vector (2.5), which is an $n \times 1$ matrix. In these notes we’re only going to have square matrices, so this will never come up.

Exercise 2.1. Show that $H$ is non-degenerate. Show that for every $x \in F^2$, $H(x, x) = 0$, so that Lemma 1.14 definitely does not hold in characteristic 2.

Exercise 2.2. Consider the symmetric bilinear form $R^3$. Show that the matrix of this symmetric bilinear form in the basis $\{(1,1,1),(1,1,0),(1,0,1)\}$ is

\[
\begin{pmatrix}
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0 \\
\end{pmatrix}
\]
so that \( \mathbb{R}^3 \) is isometric to \( \mathbb{R} \oplus \mathbb{H} \), and that more generally \( \mathbb{R}^{2n+1} \) is isometric to \( \mathbb{R} \oplus \mathbb{H}^n \) and \( \mathbb{R}^{2n+2} \) is isometric to \( \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{H}^n \).

The following “decomposition” result will be useful to us.

**Exercise 2.3.** Suppose that \((B, V)\) is a symmetric bilinear form, \(W \subset V\) is a subspace, and that the restriction of \(B_W\) of \(B\) to \(W\) is non-degenerate. Let \(B_{W^\perp}\) be the restriction of \(B\) to \(W^\perp\). Show that the map

\[
(W, B_W) \oplus (W^\perp, B_{W^\perp}) \to (V, B)
\]
sending \((w, v)\) to \(w + v\) is an isometry.

We need one more piece of terminology.

**Definition 2.6.** A symmetric bilinear form \((V, B)\) over \(\mathbb{F}_2\) is **even** if for all \(x \in V\),

\[
B(x, x) = 0.
\]

A symmetric bilinear form is **odd** if there exists \(x \in V\) with \(B(x, x) = 1\).

**Exercise 2.4.** Suppose that \(B_1\) and \(B_2\) are symmetric bilinear forms over \(F = \mathbb{F}_2\). Show that \(B_1 \oplus B_2\) is even if and only if both of \(B_1\) and \(B_2\) are even.

Now let’s pursue the analogue of Theorem 1.12. We start with a symmetric bilinear form \((V, B)\) over \(\mathbb{Z}/2\). Suppose that there is a vector \(v \in V\) with \(B(v, v) = 1\). As in the proof of Theorem 1.12 we let \(W\) be the kernel of \(B(v, -) : V \to F\) and \(B_W\) the restriction of \(B\) to \(W\), so that \(B_W(x, y) = B(x, y)\). Then by Exercise 2.3 the map

\[
F \oplus W \to V
\]

\[
(t, x) \mapsto t + x
\]
is an isometry of \(\mathbb{R} \oplus (W, B_W)\) with \((V, B)\). Iterating this we see that \((V, B)\) is isometric to \(\mathbb{R}^m \oplus (V', B')\) where \((V', B')\) is even.

Armed with this we now restrict our attention to even symmetric bilinear forms. Suppose that \((V, B)\) is even. Either \(B\) is zero, or we can find two vectors \(x, y \in V\) with \(B(x, y) = 1\). Let \(W \subset V\) be the subspace spanned by \(x\) and \(y\). Note that \(x\) cannot equal \(y\) since \(B\) is even. This means that \(W\) has dimension 2, and that the map \(F^2 \to W\) sending \(e_1\) to \(x\) and \(e_2\) to \(y\) is an isometry of \(\mathbb{H}\) with \((W, B_W)\), where, as above, \(B_W\) is the restriction of \(B\). Let \(V' = W^\perp \subset V\) be the orthogonal complement of \(W\). Note that \(V'\) is the kernel of the map

\[
T : V \to F^2
\]
sending \(v\) to \((B(x, v), B(y, v))\). This map is surjective since \(T(x) = (0, 1)\) and \(T(y) = (1, 0)\). This implies that \(\dim V' = \dim V - 2\).

It now follows from Exercise 2.3 that \((V, B)\) is isometric to \(\mathbb{H} \oplus (V', B')\). By Exercise 2.4 we know that \((V', B')\) is even. If it is non-zero we may continue. If it is zero we just stop. Putting all of this together gives

**Theorem 2.7.** Any symmetric bilinear form \(B = (V, B)\) over the field \(F = \mathbb{F}_2\) is isometric to one of

\[
\mathbb{H}^n \oplus 0^n
\]

\[
\mathbb{R} \oplus \mathbb{H}^n \oplus 0^n
\]

\[
\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{H}^n \oplus 0^n.
\]
In the above, \((V, B)\) is non-degenerate if and only if \(n = 0\). Only the first case is even. This implies

Corollary 2.8. Any even non-degenerate symmetric bilinear form \((V, B)\) over \(\mathbb{F}_2\) is isometric to \(\mathbb{H}^m\) for some \(m\). In particular the dimension of \(V\) must be even.

Exercise 2.5. Suppose that \((V, B)\) is a non-degenerate symmetric bilinear form over \(F\). A subspace \(W \subset V\) is \(B\)-isotropic (or just isotropic if \(B\) is understood) if \(B(x, y) = 0\) for all \(x, y \in W\). Show that if \(W\) is an isotropic subspace of \(V\) then \(\dim W \leq \frac{1}{2} \dim V\). Show that equality can only hold if \((V, B)\) is even and that when \((V, B)\) is even there is an isotropic subspace of dimension \(\frac{1}{2} \dim V\). (Hint: What is the relationship between \(W\) and \(W^\perp\) when \(W\) is isotropic?)

Exercise 2.6. Show that the three cases listed in Theorem 2.7 are distinct in the sense that there is no isometry between any distinct two of the three cases.

3. Quadratic forms

3.1. Abstract quadratic forms. We now turn to quadratic forms. A quadratic form is a homogeneous polynomial of degree 2 in \(n\) variables. Examples are

\[
q(x) = \lambda x^2
\]
\[
q(x, y) = x^2 + xy
\]
\[
q(x, y, z) = x^2 + xz + z^2 + yz.
\]

In a standard course in linear algebra you would learn how to classify quadratic forms over \(\mathbb{R}\) and to understand the shape of the “quadrics” defined by \(q(v) = 1\). I gave a rapid discussion of this in class, and you can read more about it in your book. Here I want to focus on the case of \(F = \mathbb{F}_2\). But to begin we will work over an arbitrary field.

For convenience I want to work with a more abstract “coordinate free” definition of a quadratic form.

Definition 3.1. Suppose \(V\) is a vector space over a field \(F\). A quadratic function on \(V\) is a function

\[
q : V \rightarrow F
\]

having the property that

\[
B(x, y) = q(x + y) - q(x) - q(y)
\]

is a bilinear form on \(V\). A quadratic form on \(V\) is a quadratic function having the additional property that

\[
q(\lambda v) = \lambda^2 q(v)
\]

for all \(\lambda \in F\) and all \(v \in V\).

The bilinear form \(B(x, y) = q(x + y) - q(x) - q(y)\) is called the underlying bilinear form of \(q\) (or sometimes the associated bilinear form.) Note that bilinear form underlying a quadratic function is always symmetric.

Exercise 3.1. Show that if \(q\) and \(q'\) are two quadratic functions on \(V\) with the same underlying bilinear form then \(q - q'\) is linear. Show that if \(q\) and \(q'\) are actually quadratic forms and the characteristic of \(F\) is not 2 then in fact \(q - q' = 0\).
Exercise 3.2. Suppose that $V = F^n$ and that we are given elements $a_{ij} \in F$ for $i, j = 1, \ldots, n$. Define $f : V \to F$ by

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j.$$ 

Show that $f$ is a quadratic form.

3.2. Quadratic forms and quadratic polynomials. We now describe how a choice of basis lets one describe any quadratic form as a homogeneous polynomial of degree 2.

Suppose that $(V, q)$ is a quadratic form over a field $F$. We now make no restrictions on the characteristic of $F$. Suppose that $\alpha = \{v_1, \ldots, v_n\}$ is an ordered basis of $V$. Given a quadratic form $q : V \to F$ define elements $a_{ij} \in F$ by

$$a_{ij} = \begin{cases} q(v_i + v_j) & i \neq j \\ q(v_i) & i = j, \end{cases}$$

and set

$$q_{\alpha}(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j.$$ 

This is the quadratic polynomial associated to $q$ by the ordered basis $\alpha$.

Proposition 3.2. If $v = x_1v_1 + \cdots + x_nv_n$ then

$$q(v) = q_{\alpha}(x_1, \ldots, x_n).$$

One way to prove this is to repeatedly use the properties of $q$ to expand $q(x_1v_1 + \cdots + x_nv_n)$. That’s actually not so bad. I want to outline a slightly more elegant approach that involves some useful other ideas.

Stepping back a bit we have two quadratic forms on $V$ and we wish to show they are the same. One of them is $q$. The other is the form $q'(v)$ computed by writing $v = x_1v_1 + \cdots + x_nv_n$ and setting $q'(v) = q_{\alpha}(x_1, \ldots, x_n)$.

Exercise 3.3. Show that $q$ and $q'$ have the same underlying bilinear forms, ie that

$$q(x + y) - q(x) - q(y) = q'(x + y) - q'(x) - q'(y).$$

(Hint: Since both sides are bilinear it suffices to do this for $x = v_i$ and $y = v_j$).

Exercise 3.4. Using Exercise 3.1 show that if $q_1$ and $q_2$ are two quadratic functions with the same underlying bilinear form, $\{v_1, \ldots, v_n\}$ generate $V$, and $q_1(v_i) = q_2(v_i)$ for $i = 1, \ldots, n$ then $q_1 = q_2$.

Exercise 3.5. Using the above exercises prove Proposition 3.2.
3.3. **Isometries and orthogonal sums.** Note that the bilinear form $B$ associated to a quadratic form $q$ satisfies

\[ B(x, x) = q(2x) - 2q(x) = 4q(x) - 2q(x) = 2q(x), \]

or in other words that

\[ q(x) = \frac{1}{2} B(x, x). \]

This means that if the characteristic of $F$ is not 2, the theory of quadratic forms is equivalent to the theory of symmetric bilinear forms. In characteristic 2 there is an interesting difference. In either case there is a close correspondence, and there is some terminology that reflects that.

**Definition 3.4.** Suppose that $F$ is a field. A quadratic form over $F$ is a pair $(V, q)$ consisting of a finite dimensional vector space over $F$ and a quadratic form $q : F \to V$.

**Definition 3.5.** A quadratic form $(V, q)$ over $F$ is non-degenerate if the associated symmetric bilinear form $B(x, y) = q(x + y) - q(x) - q(y)$ is non-degenerate.

**Definition 3.6.** The orthogonal sum of two quadratic forms $(V_1, q_1)$ and $(V_2, q_2)$ is the form $(V_1 \oplus V_2, q_1 \oplus q_2)$ in which

\[ (q_1 \oplus q_2)(v_1, v_2) = q_1(v_1) + q_2(v_2). \]

It is easy to check that the bilinear form associated to the orthogonal sum of two quadratic forms is the orthogonal sum of the two associated bilinear forms.

**Definition 3.7.** Suppose that $(V_1, q_1)$ and $(V_2, q_2)$ are quadratic forms over a field $F$. An isometry

\[ T : (V_1, q_1) \to (V_2, q_2) \]

between two quadratic forms over a field $F$ is an invertible linear transformation $T : V_1 \to V_2$ satisfying

\[ q_2(T(v)) = q_1(v) \]

for all $v \in V$.

Theorem 1.12 and the relation between quadratic forms and symmetric bilinear forms described above gives

**Theorem 3.8.** Suppose that $(V, q)$ is a quadratic form over a field $F$ whose characteristic is not 2. There is a basis $v_1, \ldots, v_n$ of $V$ and elements $\lambda_1, \ldots, \lambda_n \in F$ such that

\[ q(x_1 v_1 + \cdots + x_n v_n) = \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2. \]

This means that over fields of characteristic not equal to 2 one can find a change of variables for every homogeneous polynomial of degree 2 which makes it a sum of multiples of squares. The situation in characteristic 2 is a little more involved.

4. **Quadratic forms over $\mathbb{F}_2$**

For this section we assume the field $F$ is the field $\mathbb{F}_2$. Note that if $(V, q)$ is a quadratic form over $F$ then the identity (3.3) implies that the associated symmetric bilinear form is even. Corollary 2.8 then tells us that this symmetric bilinear form must be isometric to $H^n \oplus 0^m$. Our aim is to classify all of the quadratic forms. We will restrict our attention to those that are non-degenerate. In that case the
The associated symmetric bilinear form is isometric to $\mathbf{H}^n$ for some $n$. In particular this means that the dimension of $V$ must be even.

Let’s try and work out all the non-degenerate quadratic forms on $F^2$. By Proposition 3.2 there are exactly 8 possibilities for $q$:

- $q(x, y) = 0$
- $q(x, y) = x^2$
- $q(x, y) = xy$
- $q(x, y) = x^2 + xy$
- $q(x, y) = y^2$
- $q(x, y) = x^2 + y^2$
- $q(x, y) = xy + y^2$
- $q(x, y) = x^2 + xy + y^2$.

Of these the only ones that are non-degenerate are

- $q(x, y) = xy$
- $q(x, y) = x^2 + xy$
- $q(x, y) = xy + y^2$
- $q(x, y) = x^2 + xy + y^2$.

As one can easily check, the underlying symmetric bilinear form in all four cases is just $\mathbf{H}$. To go further let’s make a table of values:

<table>
<thead>
<tr>
<th></th>
<th>$(0,0)$</th>
<th>$(1,0)$</th>
<th>$(0,1)$</th>
<th>$(1,1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$xy$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$x^2 + xy$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$xy + y^2$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x^2 + xy + y^2$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note that $q$ either takes the value 0 three times and 1 one time, or it takes the value 0 once and the value 1 three times.

**Exercise 4.1.** Show that the quadratic forms in the above table taking the value 0 three times are all isometric.

Now that you’ve done the above exercise you know that, up to isometry, there are exactly two non-degenerate quadratic forms over $F_2$ in dimension 2. We will see that this holds in general. To do this we need to name some quadratic forms. Set

- $\mathbf{H}_+ = (F^2, xy)$
- $\mathbf{H}_- = (F^2, x^2 + xy + y^2)$.

**Theorem 4.1.** Suppose that $(V, q)$ is a non-degenerate quadratic form over $F_2$. Then $(V, q)$ is isometric to one of

- $\mathbf{H}^n_+$
- $\mathbf{H}_- \oplus \mathbf{H}^{n-1}_+$.
Suppose that Lemma 4.2.

**Lemma 4.2.** Suppose that \((V, q)\) is a quadratic form over \(F = \mathbb{F}_2\) and that \(\dim V \geq 4\). There exists a vector \(v \in V\) with \(q(v) = 0\).

**Proof:** Write \(B(x, y) = q(x + y) - q(x) - q(y)\) for the underlying symmetric bilinear form. Since \(B\) is even and non-degenerate we know from Theorem 2.7 that \((V, B)\) is isometric to \(H^n\) for some \(n \geq 1\). We may therefore suppose that \(V = F^{2n}\) and that \(B\) is \(H^n\). Let \(v = e_1 + e_2 + e_3 + e_4\). We compute

\[
q(v) = q(e_1 + e_2 + e_3 + e_4) = q(e_1 + e_2) + q(e_3 + e_4) + B(e_1 + e_2, e_3 + e_4)
\]

\[
= q(e_1 + e_2) + q(e_3 + e_4)
\]

\[
= q(e_1) + q(e_2) + B(e_1, e_2) + q(e_3) + q(e_4) + B(e_3, e_4)
\]

\[
= 1 + 1 + 1 + 1 + 1 + 1 = 0.
\]

We now return to the proof of Theorem 4.1 and suppose we are given a non-degenerate quadratic form \((V, q)\) of dimension greater than 2. Since the dimension of \(V\) must be even we know that the dimension of \(V\) is at least 4. By Lemma 4.2 there is a vector \(v \in V\) with \(q(v) = 0\). Write \(B(x, y) = q(x + y) - q(x) - q(y)\) for the underlying symmetric bilinear form (I could have written + instead of − since we are in characteristic 2). Since \(B\) is non-degenerate there is a vector \(w \in V\) with \(B(v, w) = 1\). It follows that

\[
q(v + w) + q(w) = q(v + w) + q(v) + q(w) = 1.
\]

This means that one of \(q(w)\) or \(q(v + w)\) is equal to 1. Since

\[
B(v, v + w) = B(v, v) + B(v, w) = B(v, w)
\]

there is no loss of generality if we assume that \(q(w) = 0\). Let \(W \subset V\) be the subspace of \(V\) spanned by \(v\) and \(w\). As in the proof of Theorem 2.7 let

\[
V' = \{ x \in V \mid B(v, x) = B(w, x) = 0 \}.
\]

Write \(q_W\) for the restriction of \(q\) to \(W\) and \(q'\) for the restriction of \(q\) to \(V'\). I claim that

\[
(V, q) \approx (W, q_W) \oplus (V', q').
\]

We observed in the proof of Theorem 4.1 that this is true as vector spaces. So to verify the claim we have to check that for \(x \in W\) and \(y \in V'\) one has

\[
q(x + y) = q(x) + q(y).
\]

But \(q(x + y) - q(x) - q(y) = B(x, y) = 0\), so this does indeed hold.

Finally, note that \((W, q_W)\) is isometric to \(H_+\):

\[
q(xv + yw) = q(xv) + q(yw) + B(xv, yw)
\]

\[
= x^2 q(v) + xyB(v, w) + y^2 q(w)
\]

\[
= xy.
\]

We have shown that if the dimension of \(V\) is greater than 2, there is an isometry of \((V, q)\) with \(H_+ \oplus (V', q')\). Theorem 4.1 then follows by induction.
5. The Arf invariant

We’d like to know that the two forms in Theorem 4.1 are not in fact isometric to each other. The situation is a little like that of Theorem 2.7, for which we were able to use the notion of “even” and “odd” forms to distinguish some of the cases, and the dimension of a maximal isotropic subspace to distinguish the others. There is an analogue of this notion for quadratic forms called the “Arf invariant.”

Suppose that \((V, q)\) is a non-degenerate quadratic form over \(\mathbb{F}_2\). One way of getting a measure of \(q\) is to compare the number of solutions to the equation \(q(v) = 0\) with the number of solutions to \(q(v) = 1\). This suggest looking at the number

\[
\#\{v \in V \mid q(v) = 0\} - \#\{v \in V \mid q(v) = 1\}.
\]

It turns out that there is a clever choice of normalizing factor for this difference.

**Definition 5.1.** Suppose that \((V, q)\) is a non-degenerate quadratic form over \(\mathbb{F}_2\). The **Arf invariant** of \((V, q)\) is the number

\[
\text{Arf}(V, q) = \frac{1}{2^{\dim V/2}} \sum_{v \in V} (-1)^q(v) = \frac{1}{2^{\dim V/2}} \left(\#\{v \in V \mid q(v) = 0\} - \#\{v \in V \mid q(v) = 1\}\right).
\]

**Exercise 5.1.** Show that \(\text{Arf}(H_+) = 1\) and \(\text{Arf}(H_-) = -1\).

**Proposition 5.2.** Suppose that \(q_1 = (V_1, q_1)\) and \(q_2 = (V_2, q_2)\) are non-degenerate symmetric bilinear forms over \(\mathbb{F}_2\). Then

\[
\text{Arf}(q_1 \oplus q_2) = \text{Arf}(q_1) \ast \text{Arf}(q_2).
\]

**Exercise 5.2.** Prove Proposition 5.2 by expanding out the right hand side.

Clearly isometric quadratic forms have the same Arf invariant. In fact

**Theorem 5.3.** Two non-degenerate quadratic forms over \(\mathbb{F}_2\) are isometric if and only if they have the same dimension and the same Arf invariant.

**Exercise 5.3.** Show that the forms \(H_{2n}^+\) and \(H_+ \oplus H_{2n-1}^+\) are not isometric by computing their Arf invariants.

**Exercise 5.4.** Using Theorem 4.1 and the previous exercise prove Theorem 5.3.

**Exercise 5.5.** The quadratic forms \(H_2^+\) and \(H_2^-\) both have Arf invariant 1. Can you find an isometry between them?

The important thing about the normalizing factor in the definition of the Arf invariant is the following fact which is immediate from Exercise 5.1, Theorem 4.1 and Proposition 5.2.

**Corollary 5.4.** If \(q\) is a non-degenerate quadratic form over \(\mathbb{F}_2\) then

\[
\text{Arf}(q) = \pm 1.
\]

\(\square\)

Corollary 5.4 has a pretty cool consequence. Suppose that \((V, q)\) is a non-degenerate quadratic form over \(\mathbb{F}_2\). Let \(a\) and \(b\) be the numbers

\[
a = \#\{v \in V \mid q(v) = 0\}, \quad b = \#\{v \in V \mid q(v) = 1\}.
\]
Write \( \dim V = 2m \). Then we have

\[
\begin{align*}
  a + b & = 2^n \\
  a - b & = \pm 1.
\end{align*}
\]

It follows that either

\[
\begin{align*}
  a & = 2^{m-1}(2^m - 1) \\
  b & = 2^{m-1}(2^m + 1)
\end{align*}
\]

or

\[
\begin{align*}
  a & = 2^{m-1}(2^m + 1) \\
  b & = 2^{m-1}(2^m - 1)
\end{align*}
\]

So we actually know the number of times \( q \) takes on the value 0 or 1. You can think of this as the analogue for \( \mathbb{F}_2 \) of knowing the shape of \( q(v) = 1 \). Just to highlight it, I’ll state it as a result.

**Corollary 5.5.** Suppose that \( q = (V,q) \) is a non-degenerate quadratic form over \( \mathbb{F}_2 \), with \( \dim V = 2m \). Then

\[
\# \{ v \in V \mid q(v) = 1 \} = \begin{cases}
  2^{m-1}(2^m - 1) & \text{Arf}(q) = 1 \\
  2^{m-1}(2^m + 1) & \text{Arf}(q) = -1.
\end{cases}
\]