18.704: Classification of Bilinear Forms over Finite Fields

David Glasser

3/7/2005

1 Equivalence of Bilinear Forms

Today's goal will be to classify all of the bilinear forms over finite fields of odd order. In order to classify them, we need to know when we consider two bilinear forms to be the same. We call the forms B_1 and B_2 on vector spaces V_1 and V_2 "equivalent" if there is an isometry between V_1 and V_2; an isometry is an F-isomorphism $\sigma\colon V_1 \to V_2$ with $B_2(\sigma v, \sigma w) = B_1(v, w)$ for all $v, w \in V_1$. For example, the usual dot product on $\mathbb{R}^2$ (with matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$) is equivalent to the bilinear form with matrix $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, where $\sigma\colon v \mapsto \frac{v}{\sqrt{2}}$. Clearly V_1 and V_2 have to have the same dimension. One can show (Proposition 2.8) that the two bilinear forms are equivalent iff there are bases for V_1 and V_2, relative to which B_1 and B_2 have the same matrix.

2 Quadratic Forms

Recall that, given a *symmetric* bilinear form B (that is, $B(u, v) = B(v, u)$ for all $u, v \in V$) we can define the quadratic form $Q\colon V \to F$ by $Q(v) = B(v, v)$; and given any quadratic form Q we can pull out a symmetric bilinear form defined by $B(u, v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$. However, we can only do this if $\frac{1}{2}$ exists – that is, if the field does not have characteristic 2. *For the rest of today, we will assume that F does not have characteristic 2.* (Grove assumes this for all of chapter 4.) Thus, symmetric bilinear forms and quadratic forms are entirely equivalent concepts; classifying one is the same as classifying the other.

Proposition 2-1. *If B is a nonzero symmetric bilinear form on V with quadratic form Q, then $Q(v) \neq 0$ for some $v \in V$.*

Proof: If $Q(u) = 0$ for all u, then $0 = Q(u + v) = Q(u) + 2B(u, v) + Q(v) = 2B(u, v)$; so $B(u, v) = 0$ for all $u, v \in V$, contrary to assumption. □

Recall that a set of vectors $\{v_1, \ldots, v_n\}$ is said to be orthogonal if $B(v_i, v_j) = 0$ for all $i \neq j$.

Theorem 2-2 (Orthogonal Basis Theorem (my name)). *If B is a symmetric bilinear form on V then V has an orthogonal basis $\{v_1, \ldots, v_n\}$, relative to which B is a diagonal matrix $diag(b_1, \ldots, b_r, 0, \ldots, 0)$ with all $b_i \neq 0$.*

Proof: Assume $B \neq 0$ (because the theorem is clear for $B = 0$) and use induction on n. The proof is also clear for $n = 1$, because all 1-by-1 matrices are diagonal. We can use the previous proposition to find a $v_1 \in V$ with $Q(v_1) = b_1 \neq 0$, and let $W = Fv_1$ (that is, the 1-dimensional subspace spanned by v_1). Then W is non-degenerate (that is, $W \cap W^\perp = 0$); this implies that $V = W \oplus W^\perp$ with $W \perp W^\perp$. By induction, there are $v_2, \ldots, v_n$ comprising an orthogonal basis for $W^\perp$ such that $Q(v_i) = b_i \neq 0$ for $2 \leq i \leq r$ and $Q(v_i) = 0$ for $r + 1 \leq i \leq n$ for some r. The result follows. □

Note that, for any nonzero $c_i \in F$, we could have chosen $c_i v_i$ instead of v_i and the proof would still have held, except that the b_i in the matrix would have been replaced by $Q(c_i v_i) = c_i^2 b_i$; in fact, b_i can be made to be any element in the image of Q. This implies, for example, that if F is a field where every element has a square root (like $\mathbb{C}$), then every diagonal element can be chosen to be 1 or 0, so there are exactly n equivalency classes of symmetric bilinear forms, corresponding to how many diagonal elements are nonzero. That is, given any n-dimensional complex vector space, there is an isometry onto $\mathbb{C}^n$ with a bilinear form given by projection onto the first r coordinates followed by the standard bilinear form on $\mathbb{C}^r$ (though why you're using using symmetric forms on complex vector spaces instead of Hermitian forms may be a good question!).

3 Isotropic and Universal Forms

If B is a symmetric form on V with quadratic form Q, then we call a nonzero $v \in V$ with $Q(v) = 0$ *isotropic* and $v \neq 0$ with $Q(v) \neq 0$ *anisotropic* (0 is always considered to be anisotropic). The form is called isotropic if there exists any isotropic vector, and anisotropic otherwise. A form is called *universal* if $Q(V) = F$. Using the analogy with the dot product, where Q is the magnitude squared, a vector is isotropic if it is nonzero and yet has length zero; a form is universal if any scalar value can be the length-squared of a vector.

Proposition 3-1. *If B is a nondegenerate isotropic symmetric bilinear form, then B is universal.*

Proof: Let $u \neq 0$ be an isotropic vector in V. Since B is nondegenerate there is some $w \in V$ with $B(u, w) = b \neq 0$. If we replace w with $\frac{w}{2b}$, we can assume that $B(u, w) = \frac{1}{2}$. Set $v = cu + w$, where $c \in F$ will be determined later. Then $Q(v) = B(cu+w, cu+w) = 2cB(u, w)+B(w, w)+c^2Q(u) = c+B(w, w)$. Given any $a \in F$, we can set $c = a-B(w, w)$. Then $Q(v) = c-B(w, w)+B(w, w) = a$. So B is universal. □

We need to make a quick aside into Galois theory to get a result we need for the next proposition. Let $b \in F^*$ be a nonsquare (half of the elements are), and adjoin a square root of b to F to get $K = F(\sqrt{b})$, a splitting field

for $x^2 - b$; then $[K : F] = 2$ and $|K| = q^2$ (where $|F| = q$). Then $K = \{a + c\sqrt{b} | a, c \in F\}$. The Galois group of a quadratic extension is always C_2, where the nontrivial automorphism is the Frobenius automorphism sending $x \mapsto x^q$; on the other hand, clearly the automorphism swapping $\sqrt{b}$ and $-\sqrt{b}$ is a nontrivial automorphism, so it must be the same as the Frobenius map. One defines the norm $N\colon K \to F$ by $N(x) = \pi_{\sigma \in G}\sigma(x)$ where G is the Galois group. It is clear that this is a multiplicative homomorphism, and that it is invariant under automorphisms (which is why we know that its image is in F). So using our two interpretations of the Frobenius automorphism, we see that both $N(x) = xx^q = x^{q+1}$ and $N(a + c\sqrt{b}) = (a + c\sqrt{b})(a - c\sqrt{b}) = a^2 - bc^2$. The kernel of the restriction $N\colon K^* \to F^*$ is $\{d \in K^* | d^{q+1} = 1\}$. Because K^* is cyclic of order $q^2 - 1 = (q+1)(q-1)$, the elements of $\ker N$ are the elements of the unique subgroup of order $q+1$. So $|\ker N| = q+1$ and thus $|\operatorname{im} N| = q-1$, so, $N\colon K^* \to F^*$ is surjective. Because $N(0) = 0$, we have that $N\colon K \to F$ is surjective too. The conclusion we will need later is the following: given a 2-dimensional F-vector space with basis $\{v_1, v_2\}$and a nonsquare b, the map $N(av_1 + bv_2) = a^2 - bc^2$ is surjective.

Given a symmetric form B and a nonzero scalar $a \in F$, let B^a be a quadratic form defined by $B^a(u, v) = B(u, v)/a$; this gives us $Q^a(u) = Q(u)/a$. We call this "scaling the form by a". Clearly B^a is still symmetric, and is nondegenerate iff B is. Similarly, B^a is universal iff B is.

Proposition 3-2. *If F is finite, and B is a nondegenerate symmetric bilinear form on a vector space V of dimension $n \geq 2$ over F, then B is universal.*

Proof: If B is isotropic, then we apply the previous proposition and are done. So we assume that B is anisotropic. We first choose a basis via the Orthogonal Basis Theorem; since B is nondegenerate, $r = n$. We then consider the 2-dimensional nondegenerate subspace generated by v_1 and v_2 and prove that B is universal when restricted to this 2-dimensional subspace; clearly it is universal on the entire space too. For simplicity we simply refer to the 2-dimensional subspace as V and the form as B and Q (that is, we assume we started with $n = 2$).

We let the matrix for B with our orthogonal basis $\{v_1, v_2\}$ be $\begin{bmatrix} a & 0 \\ 0 & -b \end{bmatrix}$; we have that $a \neq 0$ and $b \neq 0$ by nondegeneracy. Replacing B with B^a (which is universal iff B is), we get a matrix of $\begin{bmatrix} 1 & 0 \\ 0 & -b' \end{bmatrix}$ (with $b' = \frac{b}{a} \neq 0$). Let v be an arbitrary nonzero vector; then $v = av_1 + cv_2$ for some $a, c \in F$. Because B is anistropic, $Q(v) = a^2 - b'c^2 \neq 0$. Thus b' is a nonsquare in F; otherwise, if $g^2 = b'$, we could choose $a = g$ and $c = 1$ and find that $Q(gv_1 + v_2) = g^2 - b' = 0$. But by the result from Galois theory above, V has the same structure that K did, with $Q(v) = N(v)$! So Q is surjective, which implies that B is universal. $\square$

Theorem 3-3. *If F is finite (and odd characteristic), and B is a nondegenerate symmetric bilinear form on an F-space V of dimensional $n \geq 2$, then there is a basis for V for which B has the matrix $diag(1, \ldots, 1, d)$ for some nonzero $d \in F$.*

Proof: By the previous proposition, Q is universal, so we can choose the orthogonal basis like in the Orthogonal Basis Theorem setting b_1 to 1. We can do this inductively as long as we're guaranteed that the restriction of Q to $\langle v_1, \ldots, v_{i-1} \rangle^\perp$ has dimension at least 2. Once $i = n$, the previous proposition no longer applies, but since B is nondegenerate we can at least guarantee that $b_n = d \neq 0$. □

Thus, there are precisely two equivalence classes of nondegenerate symmetric bilinear forms over odd finite fields: those which have a matrix as above with $d = 1$, and those which have such a matrix with $d = x$ for some nonsquare x which depends only on F; this is because the subgroup $F^{\times 2}$ has index 2 in F^*. (These two types are inequivalent — one has determinant 1, which is in the squares coset of $F^{\times 2}$ in F^*, i and the other has determinant x, which is in the nonsquares coset.) As far as degenerate forms go, Witt's Extension Theorem (which we have not yet covered) implies that if a form on F^n has an m-dimensional radical, then it is equivalent the direct sum of the zero form on F^m and a nondegenerate form on F^{n-m}. So the symmetric forms are in bijection with the matrices $\begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} I & & 0 \\ & x & \\ 0 & & 0 \end{bmatrix}$ where the size of I can vary from 0 to n; there are $2n + 1$ in total.