18.704: Counting Points in $Sp(2n, \mathbb{F}_q)$/Maximal Parabolic Subgroup

Genevieve Hanlon

22 April 2005

1 $Sp(2n, \mathbb{F}_q)$ and Maximal Parabolic Subgroups

First we need to recall some definitions and results from previous lectures. (I've lifted some of this from previous notes, for the sake of brevity.)

Definition 1. Given a symplectic form B on $\mathbb{F}_q^{2n}$, the symplectic group is the subgroup of $GL(2n, \mathbb{F}_q)$ that preserves the form:

$$Sp(2n, \mathbb{F}_q) = \{g \in GL(2n, \mathbb{F}_q) \mid B(gv, gw) = B(v, w) \ \forall \ v, w \in \mathbb{F}_q^{2n}\}.$$

Definition 2. Given a vector space V, a subspace $S \subset V$ is *isotropic* if $B(v, w) = 0, \ \forall \ v, w \in S$. An isotropic subspace S determines a corresponding *maximal parabolic subgroup* of $Sp(V)$ that is the stablizer of S in $Sp(V)$:

$$P(S) = \{g \in Sp(V) \mid gS = S\}, \qquad S \subset V \ isotropic$$

From now on we will assume $V = \mathbb{F}_q^{2n}$, and $S \subset V$ is a k-dimensional isotropic subspace.

Other useful results. We will need a few results from previous lectures about the order of the general linear group and the symplectic groups over a finite field. They are:

$$|GL(m, \mathbb{F}_q)| = \prod_{i=0}^{m-1} (q^m - q^i)$$

and

$$|Sp(2n, \mathbb{F}_q)| = q^{n^2} \prod_{j=1}^{n} (q^{2j} - 1)$$

We already know several things about these maximal parabolic subgroups. We know that every element of $P(S)$ is uniquely expressed as a product of certain classes of elements of $P(S)$ (which we won't list here), and that a certain quotient of $P(S)$ is isomorphic to the direct product of a (smaller dimensional) general

linear group and a (smaller dimensional) symplectic group. More specifically, recall that if we choose a basis $\{e_1, ..., e_k\}$ of S, we can define a set of linearly independent vectors $\{f_1, ..., f_k\}$ such that

$$B(e_i, e_j) = B(f_i, f_j) = 0, \qquad B(e_i, f_j) = \delta_{ij} \quad (1 \leq i, j \leq k)$$

where δ_{ij} is the Kronecker delta. Thus $\{f_1, .., f_k\}$ is a basis for a k-dimensional isotropic subspace $T \subset V, T \neq S$. If we define

$$W = (S \oplus T)^{\perp} = \{w \in V \mid B(w, e_i) = B(w, f_i) = 0, \ (1 \leq i \leq k)\},$$

then W is a $2(n-k)$-dimensional subspace of V, and $V = \mathbb{F}_q^{2n} = (S \oplus T) \oplus W$. During a previous lecture, it was shown that there exists a normal subgroup N of $P(S)$ consisting of symplectic transformations, each uniquely determined by a $k \times k$ symmetric matrix over V and a linear map $A : T \to W$:

$$N = \{N_A Z_E \mid A \in Hom(T, W), E \ a \ (k \times k) \ symmetric \, matrix\}$$

.

The details of N_A and Z_E are rather hairy, so we omit them here (they can be found in previous notes). The important thing is that each element of N is uniquely determined by our choice of A and E, and that N is our normal subgroup such that

$$P(S)/N \cong GL(k, \mathbb{F}_q) \times Sp(W)$$

.

So now we have enough information to determine the order of $P(S)$. First we must determine the order of the subgroup N: since every element of N is uniquely determined by our choice of A and E, we simply have to count how many such choices we can make. Since our generic A is simply a linear map from a k-dimensional subspace to a $2(n-k)$-dimensional subspace, A is determined by its associated $(k \times 2(n-k))$ matrix with entries in $\mathbb{F}_q$. There are $q^{2k(n-k)}$ such matrices, and thus $q^{2k(n-k)}$ choices for A. (Recall that A is not required to be invertible.) For our choice of $(k \times k)$ symmetric matrix E, we note that we can construct a basis for the (additive) group of all $(k \times k)$ symmetric matrices from the elementary matrices. In particular, the matrices of the form

$$e_{ii} \quad or \quad (e_{ij} + e_{ji}), \qquad (1 \leq i < j \leq k)$$

form a $k + \frac{k(k-1)}{2} = \frac{k(k+1)}{2}$ -dimensional basis $\mathcal{B}$ for the $(k \times k)$ symmetric matrices. Let $m = \frac{k(k+1)}{2}$, and relabel the basis elements of $\mathcal{B}$ as $\{v_1, ..., v_m\}$. Then every expression of the form

$$E = c_1 v_1 + ... + c_m v_m \qquad c_i \in \mathbb{F}_q$$

yields a unique $(k \times k)$ symmetric matrix, and so there are q^m such matrices. Combining our results, we see that there are $q^m q^{2k(n-k)}$ choices of A and E, and thus

$$|N| = q^{\frac{k(k+1)}{2}} q^{2k(n-k)} = q^{(\frac{k(k+1)}{2})+(2k(n-k))}.$$

Since we know that $P(S)/N \cong GL(k, \mathbb{F}_q) \times Sp(W)$, and we know how to compute the cardinality of both $GL(k, \mathbb{F}_q)$ and $Sp(W)$ (remembering that W is a $2(n-k)$-dimensional space), we can compute the cardinality of $P(S)$:

$$\begin{aligned}
|P(S)| &= |N| \cdot |GL(k, \mathbb{F}_q)| \cdot |Sp(W)| && (1)\\
&= q^{(\frac{k(k+1)}{2})+(2k(n-k))} \cdot \prod_{i=0}^{k-1}(q^k - q^i) \cdot q^{(n-k)^2} \cdot \prod_{j=1}^{n-k}(q^{2j}-1) && (2)\\
&= q^{(n^2-k^2)+\frac{k(k+1)}{2})} \cdot \prod_{i=0}^{k-1}(q^k - q^i) \cdot \prod_{j=1}^{n-k}(q^{2j}-1). && (3)\\
& && (4)
\end{aligned}$$

Now we can finally count the points in $Sp(2n, \mathbb{F}_q)/P(S)$. For convenience, let M $= |Sp(2n, \mathbb{F}_q)/P(S)|$. Then we have

$$\begin{aligned}
M &= \frac{|Sp(2n, \mathbb{F}_q)|}{|P(S)|} && (5)\\
&= \frac{q^{n^2} \cdot \prod_{l=1}^{n}(q^{2l}-1)}{q^{n^2-k^2+\frac{k(k+1)}{2}} \cdot \prod_{i=0}^{k-1}(q^k - q^i) \cdot \prod_{j=1}^{n-k}(q^{2j}-1)} && (6)\\
&= \frac{\prod_{l=1}^{n}(q^{2l}-1)}{q^{\frac{-k(k-1)}{2}} \cdot \prod_{i=0}^{k-1}(q^k - q^i) \cdot \prod_{j=1}^{n-k}(q^{2j}-1)} && (7)
\end{aligned}$$

Note that

$$\prod_{i=0}^{k-1}(q^k - q^i) = q^{\frac{k(k-1)}{2}} \cdot \prod_{i=1}^{k-1}(q^i - 1).$$

So we can cancel out the powers of q in the denominator, obtaining

$$M = \frac{\prod_{l=1}^{n}(q^{2l}-1)}{\prod_{i=1}^{k-1}(q^i - 1) \cdot \prod_{j=1}^{n-k}(q^{2j}-1)}.$$

Since $\prod_{j=1}^{n-k}(q^{2j}-1)$ clearly divides $\prod_{l=1}^{n}(q^{2l}-1)$, we can cancel further, obtaining

$$M = \frac{(q^{2n}-1)(q^{2n-2}-1)...(q^{2(n-k)+2}-1)}{(q^{k-1}-1)(q^{k-2}-1)...(q-1)}$$

.

But we can simplify even further. If we divide both numerator and denominator by $(q-1)$, we see immediately that the denominator is

$$\frac{\prod_{i=1}^{k-1}(q^i-1)}{q-1} = [k]_q!.$$

The numerator is less obvious, but still (thankfully) manageable. Since every term of the numerator is the difference of two squares, we can factor it:

$$(q^{2n}-1)(q^{2n-2}-1)...(q^{2(n-k+1)}-1) = \prod_{i=n-k+1}^{n}(q^i-1)\cdot\prod_{j=n-k+1}^{n}(q^j+1)$$

and since we still need to divide the numerator by $(q-1)$, we find that

$$\frac{\prod_{i=n-k+1}^{n}(q^i-1)}{(q-1)} = \frac{[n]_q!}{[n-k]_q!},$$

which is nice, because now we have

$$M = \frac{|Sp(2n,\mathbb{F}_q)|}{|P(S)|} \tag{8}$$

$$= \frac{[n]_q!(q^n+1)(q^{n-1}+1)...(q^{n-k+1}+1)}{[k]_q![n-k]_q!} \tag{9}$$

.

So given a k-dimensional isotropic subspace $S \subset \mathbb{F}_q^{2n}$, we now know that

$$|Sp(2n,\mathbb{F}_q)/P(S)| = \frac{[n]_q!}{[k]_q![n-k]_q!}\cdot\prod_{i=(n-k+1)}^{n}(q^i+1).$$

2 What Does This Actually Mean?

So far we've counted points in $Sp(2n,\mathbb{F}_q)/P(S)$, but it's not entirely clear what these points represent. In fact, the construction $Sp(2n,\mathbb{F}_q)/P(S)$ is itself a little weird - since the stabilizer isn't necessarily a normal subgroup, this is not really a valid group decomposition, so we can really only concern ourselves with the underlying set and group action. Still, we have divided out by the stabilizer of subspace, and that should mean something. A version of Witt's Extension Theorem introduced in class can help:

Theorem 1. Suppose S and S' are k-dimensional isotropic subspaces of a symplectic vector space V. Then there is an element $g \in Sp(V)$ such that $gS = S'$.

From this we can conclude that the orbit of S under the action of $Sp(V)$ contains all isotropic k-dimensional subspaces of V. In fact, if we go back to

the definition of the symplectic group $Sp(V)$ and the definition of an isotropic subspace,

$$Sp(V) = \{g \in GL(V) \mid B(gv, gw) = B(v, w) \; \forall \; v, w \in V\}$$

$$S \subset V \; isotropic \iff B(v, w) = 0 \; \forall \; v, w \in S$$

we see that no element $g \in Sp(V)$ can carry an isotropic subspace $S \subset V$ to a non-isotropic space, i.e., for symplectic form B and $g \in Sp(V)$, if S isotropic, then $B(v, w) = 0 \; \forall \; v, w \in S$, and since $g \in Sp(V)$, $B(gv, gw) = B(v, w) = 0 \; \forall \; gv, gw \in gS = S'$. Thus the image of S under the action of g, S', is also isotropic. Clearly S and S' will have the same dimension. So the set of k-dimensional isotropic subspaces forms a single orbit under the action of $Sp(V)$. From elementary group theory we have the familiar orbit-stabilizer theorem:
Theorem 2. Suppose the group G acts on the set X, and let

$$G_x = \; stablizer \; of \; x \; in \; G = \{g \in G \mid gx = x\}$$

$$O_x = \; orbit \; of \; x \; under \; G = \{y \in X \mid gx = y for some g \in G\}$$

Then $|G| = |G_x||O_x| \quad \forall \; x \in X$.

So our "points" in $Sp(2n, \mathbb{F}_q)/P(S)$ actually represent all the k-dimensional isotropic subspaces of $\mathbb{F}_q^{2n}$. In other words, we've found the cardinality of the isotropic Grassmanian $IG(k, \mathbb{F}_q^{2n})$:

$$|IG(k, \mathbb{F}_q^{2n})| = \frac{[n]_q! \cdot \prod_{i=n-k+1}^{n}(q^i + 1)}{[k]_q![n-k]_q!}.$$