Counting symmetric nilpotent matrices

A. E. Brouwer, R. Gow & J. Sheekey

March 2012 / March 9, 2013

Abstract

We determine the number of nilpotent matrices of order n over $\mathbb{F}_q$ that are self-adjoint for a given nondegenerate symmetric bilinear form, and in particular find the number of symmetric nilpotent matrices.

1 Introduction

Consider matrices of order n over the finite field $\mathbb{F}_q$. Trivially, the total number of such matrices is q^{n^2}, of which $q^{n(n+1)/2}$ are symmetric. Less trivially, the number of nilpotent matrices is $q^{n(n-1)}$—see below for references and yet another proof. The aim of this note is to count symmetric nilpotent matrices, and more generally nilpotent matrices that are self-adjoint for a given nondegenerate symmetric bilinear form.

1.1 Nilpotent matrices

A linear transformation N of a vector space V is called *nilpotent* when $N^e = 0$ for some nonnegative integer e. The smallest such e is called the *exponent* of N.

1.2 Self-adjoint matrices

Let V be a vector space of dimension n over $\mathbb{F}_q$, and let $g : V \times V \to \mathbb{F}_q$ be a nondegenerate symmetric bilinear form. The linear transformation N of V is called *self-adjoint* with respect to g if $g(Nx, y) = g(x, Ny)$ for all $x, y \in V$. If we fix a basis for V, the form g is represented by a nonsingular symmetric matrix G, so that $g(x, y) = x^\top G y$ (for column vectors x, y). Now N (given by a matrix also called N) is self-adjoint when $(GN)^\top = GN$, that is, when the matrix GN is symmetric. Thus, counting symmetric nilpotent matrices is the same as counting nilpotent linear transformations that are self-adjoint for the *standard form*, the form with $G = I$ so that $g(x, y) = \sum x_i y_i$.

1.3 Nondegenerate symmetric bilinear forms

For nonzero constants c the forms g and cg lead to the same self-adjoint N. For nonsingular linear transformations A the (congruent) forms given by the matrices G and $A^\top G A$ lead to the same number of self-adjoint N. (When GN is symmetric, then so is $A^\top G N A$, so that $A^{-1} N A$ is self-adjoint for $A^\top G A$.) Therefore, if we are interested in the number of self-adjoint nilpotent N, we need only look at g up to scaling and congruence.

For odd n (and for $n = 0$), there is up to scaling and congruence only one nondegenerate symmetric bilinear form. We can take the standard form as representative. For nonzero even n, there are two types. For odd q the form can be elliptic or hyperbolic. For even q the form can be symplectic or not (cf. [1]).

The counts (of nilpotent linear transformations that are self-adjoint for a given form) that we shall determine are $e(2m), h(2m), p(2m+1)$ (for odd q and an elliptic, hyperbolic or standard form) and $z(2m), s(2m), s(2m+1)$ (for even q, and a symplectic or standard form), where the parameter is the dimension n. The letters e, h, p, z, s are intended to be mnemonic of *elliptic, hyperbolic, parabolic, zero* (diagonal), and *standard*. If $n = 0$, there is no elliptic form so that $e(0)$ is undefined. We define $e(0) = 1$.

1.4 Results

Proposition 1.1 *Each of $e(2m)$, $h(2m)$, $p(2m+1)$, $z(2m)$, $s(2m)$, $s(2m+1)$ is a polynomial in q for each $m \geq 0$. We have $e(0) = h(0) = z(0) = s(0) = p(1) = s(1) = e(2) = 1$.*

The identities below are identities as polynomials in q.

Proposition 1.2 $z(2m) = q^{2m^2}$.

Proposition 1.3 $s(2m+1) = p(2m+1)$.

Put $a(2m) = (h(2m) + e(2m))/2$ and $d(2m) = (h(2m) - e(2m))/2$, so that $h(2m) = a(2m) + d(2m)$ and $e(2m) = a(2m) - d(2m)$.

Proposition 1.4 $s(2m) = a(2m)$.

Proposition 1.5 $p(2m+1) = q^{2m}a(2m) + q^m d(2m)$.

Proposition 1.6 $p(2m+1) = (q^{2m} - 1)a(2m) + z(2m)$.

The preceding two identities allow one to express $d(2m)$ in terms of $a(2m)$.

Proposition 1.7 $a(2m) = q^{2m-1}p(2m-1)$ for $m > 0$.

Corollary 1.8 $p(2m+1) = q^{2m-1}(q^{2m} - 1)p(2m-1) + q^{2m^2}$ for $m > 0$.

This determines all polynomials $e(2m)$, $h(2m)$, $p(2m+1)$, $z(2m)$, $s(2m)$, $s(2m+1)$.

Proposition 1.9 *The number $\#(n)$ of symmetric nilpotent matrices of order n is given by*

$$\#(n) = \begin{cases} s(n) & \text{when } n \text{ is odd or } q \text{ is even,} \\ e(n) & \text{when } n \equiv 2 \pmod 4 \text{ and } q \equiv 3 \pmod 4, \\ h(n) & \text{otherwise.} \end{cases}$$

As a side result we find the mysterious equality

Proposition 1.10 *If n is odd, and also if n and q are even and the form is not symplectic, then $\sum_N 1 = \sum_{N,x} 1$, where the sums are over selfadjoint nilpotent matrices N, and nonisotropic projective points x such that $Nx = 0$.*

2 Fitting decomposition

Let V be a finite-dimensional vector space, and M a linear transformation of V. The map M determines a unique decomposition $V = U \oplus W$ as direct sum of subspaces U, W, both invariant under M, where the restriction of M to U is nilpotent, and the restriction of M to W is invertible. This decomposition is known as the *Fitting decomposition*.

[Proof: Take $U = \ker M^e$ and $W = \operatorname{im} M^e$ for sufficiently large e.]

If g is a nondegenerate symmetric or alternating bilinear form on V, and M is self-adjoint for g, then U and W are g-orthogonal, that is, $g(U, W) = 0$. It follows that U and W are nondegenerate (that is, that the restriction of g to U and W is nondegenerate), and $V = U \perp W$, and $U = W^\perp$, $W = U^\perp$ (where $A^\perp := \{v \in V \mid g(a, v) = 0 \text{ for all } a \in A\}$).

2.1 Counting nilpotent matrices

For a finite-dimensional vector space V over $\mathbb{F}_q$, let $N(V)$ (resp. $S(V)$) be the number of nilpotent (resp. invertible) linear transformations on V. These numbers only depend on the dimension n of V, so we can write $N(V) = N(n)$ and $S(V) = S(n)$. Clearly, $S(V) = |\mathrm{GL}(V)|$, so that $S(n) = |\mathrm{GL}_n(q)| = q^{n(n-1)/2} \prod_{i=1}^{n}(q^i - 1)$.

Theorem 2.1 (Philip Hall) $N(n) = q^{n(n-1)}$.

There are many proofs, see [7, 5, 6, 4]. Hall [7] contains two different proofs, one involving a form of Möbius inversion, the other exploiting the theory of partitions. Here we use the method that will be used again to count symmetric nilpotent matrices.

Proof. Considering the Fitting decomposition of all linear transformations of V yields the equality
$$q^{n^2} = \sum_{V = U \oplus W} N(U)S(W).$$

The number of ways to write V as a direct sum of an m-space and an $(n-m)$-space is $q^{m(n-m)} \begin{bmatrix} n \\ m \end{bmatrix}_q \ (= \frac{S(n)}{S(m)S(n-m)})$, where $\begin{bmatrix} n \\ m \end{bmatrix}_q$ denotes the Gaussian coefficient, and we obtain

$$q^{n^2} = S(n) \sum_{m=0}^{n} \frac{N(m)}{S(m)}.$$

By induction on n it now follows that $N(n) = q^{n(n-1)}$. $\qquad\square$

2.2 Counting symplectic nilpotent matrices

Let V be a vector space of dimension $2m$ over $\mathbb{F}_q$, and consider the symplectic form g on V defined with respect to some basis by $g(x, y) = \sum_{i=1}^{m} x_i y_{2m-i} - x_{2m-i} y_i$ so that its matrix is $G = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$ where D is the backdiagonal matrix of order m with $D_{ij} = 1$ when $i + j = m + 1$ and $D_{ij} = 0$ otherwise. Now $D^2 = I$ and $D^\top = D$ and $G^\top = -G$.

The corresponding Lie algebra $\mathfrak{sp}_{2m}$ consists of the matrices X (of order $2m$) with $g(Xx, y) + g(x, Xy) = 0$ for all x, y, i.e., with $(GX)^\top = GX$. Writing $X = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$, we see that the condition is that DQ and DR are symmetric, and $DP + (DS)^\top = 0$. If we write M' for $DM^\top D$, which is M reflected in the back diagonal, this becomes $Q = Q'$ and $R = R'$ and $S = -P'$. It follows immediately that the total number of such matrices X equals q^{2m^2+m}. For even q these are the matrices symmetric w.r.t. the backdiagonal.

Theorem 2.2 (Steinberg [10], Springer [9]) *The number of nilpotent elements of $\mathfrak{sp}_{2m}$ is q^{2m^2}. In particular we have $z(2m) = q^{2m^2}$ for even q.*

Proof. Considering the Fitting decomposition of all elements X of $\mathfrak{sp}_{2m}$, we find
$$q^{2m^2+m} = \sum_U N(U)S(U^\perp)$$
where the sum is over all nondegenerate subspaces U of V, and $N(U)$ is the number of nilpotent symplectic maps on U (provided with $g|_U$) and $S(W)$ is the number of invertible symplectic maps on W (provided with $g|_W$).

It is easy to determine the number of nondegenerate U of any given dimension $2h$, and the result is $\begin{bmatrix} m \\ h \end{bmatrix}_{q^2} q^{2h(m-h)}$.

It is also easy to determine the number of invertible symplectic maps on a given $2h$-space, and the result is $(q-1)(q^3-1)\cdots(q^{2h-1}-1)q^{h(h+1)}$.

That means that our claim follows by induction on m if we prove the identity

$$q^{2m^2+m} = \sum_{h=0}^m q^{2(m-h)^2} \begin{bmatrix} m \\ h \end{bmatrix}_{q^2} q^{2h(m-h)}(q-1)(q^3-1)\cdots(q^{2h-1}-1)q^{h(h+1)}.$$

One can ask a computer algebra system, e.g. invoke the Maple `qzeil` function, or one can rewrite the equation to be proved as $_2\phi_0[q^{1/2}, q^{-m}; q, q] = q^{m/2}$. But this is a trivial case of the q-Chu-Vandermonde identity. □

More generally Steinberg [10, 15.3] shows for unipotent elements in connected reductive linear algebraic groups, and Springer [9, (7)] for nilpotent elements in the corresponding Lie algebras, that there are q^N of them, where $N = |\Phi|$ is the number of roots of the root system.

For A_{n-1}, that is, $GL(n)$, we have $|\Phi| = n(n-1)$, and we see again that there are $q^{n(n-1)}$ nilpotent matrices of order n.

For C_m, that is, $Sp(2m)$, we have $|\Phi| = 2m^2$. If q is even, there are q^{2m^2} nilpotent back-symmetric matrices of order $2m$.

A matrix N is *skew-symmetric* when N has zero diagonal and $N = -N^\top$. For D_m, that is, $O^+(2m)$, we have $|\Phi| = 2m(m-1)$. There are $q^{2m(m-1)}$ skew-symmetric nilpotent matrices of order $2m$.

For B_n, that is, $O(2m+1)$, we have $|\Phi| = 2m^2$. There are q^{2m^2} skew-symmetric nilpotent matrices of order $2m+1$.

Lusztig [8] gives counts of nilpotent (skew symmetric) matrices of given rank.

3   Young diagrams

A *partition* λ of a nonnegative integer n is a nonincreasing sequence $\lambda_1, \ldots, \lambda_m$ of positive integers with $\sum \lambda_i = n$. The *Young diagram* Y_λ of a partition λ is the

shape obtained by placing left-adjusted rows of squares of lengths $\lambda_1, \ldots, \lambda_m$ below each other. For example, if $\lambda = (4, 2, 2, 1)$, then $Y_\lambda =$ ⊞⊞⊞⊞ . The *order* of a Young diagram is the number of cells (squares). A *row group* of a Young diagram is a maximal set of rows of equal length.

3.1 The Young diagram of a nilpotent map

Let N be a nilpotent linear transformation of exponent e on an n-dimensional vector space V. The map N determines a unique Young diagram Y of order n, with $d := \dim \ker N$ rows and e columns, that has a square in row i, column j, if $\dim \ker N \cap \operatorname{im} N^{j-1} \geq i$. We call Y the *shape* of N.

We can choose a basis $B = \{u_1, \ldots, u_n\}$ for V such that $B \cup \{0\}$ is closed under N, and $Nu_i = Nu_j$, $i \neq j$ implies $Nu_i = Nu_j = 0$. (This is equivalent to finding a Jordan normal form of N.) We say that such a B *fits* N. Each element u of B can be assigned a square (i, j) of Y in such a way that either $j = 1$ and $Nu = 0$, or $j > 1$ and Nu is the element of B assigned to square $(i, j - 1)$. Thus, the rows (resp. squares) of Y correspond to the Jordan blocks of N (resp. the elements of B). Multiplication by N corresponds to a left shift on Y.

We see that the Young diagrams Y of order n label the GL_n-conjugacy classes of nilpotent maps on V.

3.2 Size of a conjugacy class

Let V be a vector space over $\mathbb{F}_q$. Let $N(Y)$ be the number of nilpotent linear transformations of V with given Young diagram Y, i.e., the size of the $GL(n, q)$-conjugacy class labeled by Y. Then $N(Y) = |G|/|G_N|$, where $G = GL(n, q)$, so that $|G| = \prod_{i=0}^{n-1}(q^n - q^i) = q^{n(n-1)/2}[1][2]\ldots[n-1]$ (with $[a] := q^a - 1$) is the total number of ordered bases of V, and $G_N = \{A \in G \mid AN = NA\}$ for some N of shape Y, so that $|G_N| = f(Y)$ is the number of ordered bases that fit N (in the sense that the j-th basis vector is assigned the j-th cell of Y, with cells enumerated in some fixed order).

3.3 Number of ordered bases that fit a nilpotent map

We saw that $N(Y) = |G|/f(Y)$. We now determine $f(Y)$. First choose the basis for $\ker N$. Each row group, say with rows $i+1, \ldots, j$, contributes a factor

$$(q^j - q^i)(q^j - q^{i+1})\ldots(q^j - q^{j-1}) = [1][2]\ldots[j-i]q^{j(j-1)/2 - i(i-1)/2}.$$

Altogether we found $[1]^{e_1}[2]^{e_2}\ldots q^{d(d-1)/2}$ so far, where $d = \dim \ker N$ and e_h is the number of row groups of size at least h. Next choose the rest of the basis. Each square of Y not in the first column contributes a factor q^a, where a is the number of squares in the previous column. This defines $f(Y)$, e.g. $f(\boxminus\boxminus) = (q-1)(q^2-q).q^2.q = [1]^2 q^4$. (Proof: the vector for the rightmost square of each row determines the row, and is chosen modulo $\ker N^{j-1}$ if the square is in column j.)

4 Forms

As noted above, for nonzero even dimension n nondegenerate symmetric bilinear forms g (with matrix G) have two types.

For odd q the form can be elliptic or hyperbolic. It will be hyperbolic precisely when $(-1)^{n/2} \det G$ is a square. The standard form is hyperbolic when $q \equiv 1 \pmod 4$, and also when $4|n$, and elliptic otherwise.

For even q the form can be symplectic or not. Symplectic forms are characterized by $g(x,x) = 0$ for all x, or, equivalently, by the fact that G has zero diagonal. For a non-symplectic form the set of x with $g(x,x) = 0$ is a hyperplane. The standard form is symplectic only for $n = 0$. Its hyperplane is the orthogonal complement $\mathbf{1}^\perp$ of the all-1 vector $\mathbf{1}$.

4.1 Numbers of forms

Let $g_s := g_s(n)$ be the total number of nondegenerate symmetric bilinear forms on the vector space V of dimension n, and let g_0, g_1, g_e, g_h be the numbers of such forms that are symplectic, non-symplectic, elliptic or hyperbolic, respectively. (Then $g_s = g_0 + g_1$ and $g_s = g_e + g_h$ for even n and even/odd q.)

We have:

$$g_s = g_s(n) = \begin{cases} [1][3]\ldots[2m-1]q^{m(m+1)} & \text{for} \quad n = 2m \\ [1][3]\ldots[2m+1]q^{m(m+1)} & \text{for} \quad n = 2m+1 \end{cases}$$

and for $n = 2m$: if q is even, then

$$g_0 = q^{-2m}g_s, \quad g_1 = (1 - q^{-2m})g_s,$$

and if q is odd,

$$g_e = \frac{1}{2}(1 - q^{-m})g_s, \quad g_h = \frac{1}{2}(1 + q^{-m})g_s.$$

(Proof: For g_s, cf. [3, 9.5.9]. The values g_0, g_e, g_h follow as quotients of the size of GL_n and the sizes of the subgroup Sp_{2m}, GO_{2m}^-, GO_{2m}^+ preserving the form.)

4.2 Gram matrix of a form for which N is self-adjoint

We show that the Gram matrix of a form for which a nilpotent map N is self-adjoint has a block structure that only depends on the shape Y of N.

Let g be a symmetric bilinear form for which a fixed nilpotent map N of shape Y is self-adjoint. Let $B = \{u_1, \ldots, u_n\}$ be a basis that fits N. The Gram matrix $G = (g_{ij})_{ij}$ with $g_{ij} = g(u_i, u_j)$ uniquely determines the form g (since g is bilinear). The form g will be nondegenerate precisely when G is nonsingular.

The basis vectors u_i can be identified with squares in Y. Then N acts on $Y \cup \{0\}$ via 'left shift', and the rows and columns of G can be indexed by Y.

Let row i in Y have length r_i. Since N is self-adjoint, we have $g(Ny, z) = g(y, Nz)$ for $y, z \in Y$. It follows that $g((h, i), (j, k)) = 0$ when $i \leq r_j - k$ or $k \leq r_h - i$. In words: $G_{yz} = 0$ when square y has fewer squares to the left than z has to the right (or vice versa). This is the 'forced zero' region of G.

Now let g also be nondegenerate. For each row group R consisting of r rows of length s, and each i, $1 \le i \le s$, there is a nonsingular $r \times r$ subblock in G with rows indexed by $\{(h, i) \in Y \mid h \in R\}$, and columns indexed by $\{(h, s + 1 - i) \in Y \mid h \in R\}$.

(Indeed, suppose $\{(y, y') \mid y \in Y\}$ is a transversal of G that contributes to $\det G$. If $y = (h, i)$, then write $\delta(y) = r_h + 1 - 2i$. Now $\sum_{y \in Y} \delta(y) = 0$, and $g(y, y') = 0$ if $\delta(y) + \delta(y') > 0$, so $\delta(y) + \delta(y') = 0$ for all $y \in Y$. It follows that if $y = (h, i)$ and $y' = (j, k)$, then $\max(r_h, r_j) + 1 \le i + k = \frac{1}{2}(r_h + r_j) + 1$, so $r_h = r_j$, so that y, y' belong to the same row group, and $i + k = 1 + r_h$.)

We proved: G has a forced zero region; the positions that occur in a nonzero transversal are decomposed into square blocks determined by Y, and the rest of G can be filled in arbitrarily without influencing $\det G$.

The block with rows indexed by $\{(h, i) \in Y \mid h \in R\}$ and columns indexed by $\{(h, s + 1 - i) \in Y \mid h \in R\}$ (for fixed i) is symmetric: $g((h, i), (h', s + 1 - i)) = g((h', i), (h, s + 1 - i))$. Moreover, this block is the same for fixed R and all i.

(Indeed, $g((h, i), (h', s + 1 - i)) = g((h, i'), (h', s + 1 - i'))$.)

Finally, in the free part, some positions must equal other positions, again because of $g(Ny, z) = g(y, Nz)$.

Example: Let $Y = \begin{array}{|c|c|c|} \hline 1 & 5 & 8 \\ \hline 2 & 6 \\ \cline{1-2} 3 & 7 \\ \cline{1-2} 4 \\ \cline{1-1} \end{array}$. We find $G = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \boxed{a} \\ 0 & 0 & 0 & 0 & 0 & \boxed{b} & c & . \\ 0 & 0 & 0 & 0 & 0 & c & d & . \\ 0 & 0 & 0 & \boxed{e} & 0 & . & . & . \\ 0 & 0 & 0 & 0 & \boxed{a} & . & . & . \\ 0 & \boxed{b} & c & . & . & . & . & . \\ 0 & c & d & . & . & . & . & . \\ \boxed{a} & . & . & . & . & . & . & . \end{bmatrix}$,

where $a = g(u_1, u_8) = g(u_5, u_5) = g(u_8, u_1)$, etc.

4.3 Number of forms for which N is self-adjoint

Let $g(Y) := g_s(Y)$ be the number of nondegenerate symmetric bilinear forms for which a fixed nilpotent map N of shape Y is self-adjoint.

Computation of $g(Y)$: Let g be one of the counted forms. Above we found the structure of G. There is a forced zero region: no choice. For each row group R there is a series of nonsingular symmetric blocks of order r, where $r = |R|$, all equal. The number of choices (for each R) is the number $g_s(r)$ of nonsingular symmetric matrices of order r, that is $q^{t(t+1)}[1][3] \ldots [r-1]$ if $r = 2t$, and $q^{t(t+1)}[1][3] \ldots [r]$ if $r = 2t + 1$. Having chosen these, all remaining entries that do not have to be zero, can be chosen arbitrarily (but symmetrically), still subject to $g(Nu_i, u_j) = g(u_i, Nu_j)$. This means that we can choose the inner product of the final element of each row of Y with the noninitial squares in the same row or subsequent rows in the same row group, and with all squares in subsequent row groups.

For example, in $Y = \begin{array}{cc} & \\ & \\ & \end{array}$ there are two row groups, one of one row that gives a factor $[1]$, and one of two rows that gives a factor $q^2[1]$, and $6 + 2 + 1 = 9$ inner products that can be chosen freely, for a total of $g(Y) = [1]^2 q^{11}$.

For example, in $Y =$ there are two row groups, one of two rows that gives

a factor $q^2[1]$, and one of three rows that gives a factor $q^2[1][3]$, and $5 + 4 = 9$ inner products that can be chosen freely, for a total of $g(Y) = [1]^2[3]q^{13}$.

4.4 Counting self-adjoint nilpotent matrices of given shape

Let $N_s(Y)$ be the number of symmetric nilpotent matrices with shape Y. Let $N_0(Y)$, $N_1(Y)$, $N_e(Y)$, $N_h(Y)$ be the number of nilpotent maps of shape Y that are self-adjoint with respect to a fixed nondegenerate symplectic (standard, elliptic, hyperbolic) symmetric bilinear form.

Then for $n = 2m + 1$ we have

$$N_s(Y) = N(Y)\frac{g_s(Y)}{g_s} = [2][4]\ldots[2m]\,q^{m^2}\frac{g(Y)}{f(Y)}.$$

For $n = 2m$, and q even, we have

$$N_0(Y) = N(Y)\frac{g_0(Y)}{g_0} \quad \text{and} \quad N_1(Y) = N(Y)\frac{g_1(Y)}{g_1}.$$

For $n = 2m$, and q odd, we have

$$N_e(Y) = N(Y)\frac{g_e(Y)}{g_e} \quad \text{and} \quad N_h(Y) = N(Y)\frac{g_h(Y)}{g_h}.$$

Let N_s, N_0, N_1, N_e, N_h be the totals (defined by $N_x = \sum_Y N_x(Y)$ for $x \in \{s, 0, 1, e, h\}$).

Proposition 4.1 *The functions $N_x(Y)$ and totals N_x are polynomials in q. For even n these polynomials are related by $N_e(Y) + N_h(Y) = 2N_1(Y)$ for all Y, and (hence) $N_e + N_h = 2N_1$.*

Proof. That the $N_x(Y)$ are polynomials is clear, e.g. from the expressions given and the fact that their values for prime powers q must be integral. Let $n = 2m$. We have to show that

$$(g_e(Y)/g_e) + (g_h(Y)/g_h) = 2(g_1(Y)/g_1).$$

Multiply by $(q^m + 1)g_e = (q^m - 1)g_h = \frac{1}{2}q^m g_1$ to turn this into

$$(q^m + 1)g_e(Y) + (q^m - 1)g_h(Y) = q^m g_1(Y).$$

Since $g_e(Y) + g_h(Y) = g_s(Y) = g_0(Y) + g_1(Y)$ (both equalities give the total number of forms as the sum of the two types of forms; the LHS has geometric meaning for odd q, the RHS for even q, but the equality is valid for all q) this is equivalent to

$$g_h(Y) - g_e(Y) = q^m g_0(Y).$$

Each of $g_e(Y)$, $g_h(Y)$, $g_0(Y)$ counts nondegenerate symmetric bilinear forms g, and the earlier theory gives a block structure for the Gram matrix G. All blocks that are not diagonal blocks (principal submatrices) occur in pairs, so do not influence whether $\det G$ is a square. Also, they do not meet the diagonal,

so do not influence whether the form will be symplectic. Since they contribute the same factor to each of $g_e(Y)$, $g_h(Y)$, $g_0(Y)$, they can be ignored.

Similarly, we can ignore the free factors q for off-diagonal elements that are not forced to equal diagonal elements. They contribute the same power of q to each of $g_e(Y)$, $g_h(Y)$, $g_0(Y)$. It remains to consider the diagonal blocks and further diagonal elements.

If Y has a diagonal block of odd size, then $g_0(Y) = 0$ since it cannot be nonsingular and symmetric with zero diagonal. And $g_h(Y) = g_e(Y)$ since we can multiply all entries in the diagonal block by the same nonsquare and change the quadratic character of $\det G$.

Otherwise, if there are no diagonal blocks, then the determinant is $(-1)^m$ times a square, and the form is hyperbolic. Requiring a zero diagonal costs m factors q (since the other m diagonal entries were zero already). So we are done in this case.

If there is a single diagonal block, say of size $2t$, then we find $g_e(Y) = g_e(2t)C$ and $g_h(Y) = g_h(2t)C$ and $q^m g_0(Y) = q^t g_0(2t)C$, where C is the product of common factors. Now $g_h(2t) - g_e(2t) = q^{t^2}[1][3]\ldots[2t-1] = q^t g_0(2t)$, as desired.

For the general case, note that different diagonal blocks correspond to mutually orthonal subspaces (for any of the forms counted) and both $g_h - g_e$ and $q^{n/2}g_0$ are multiplicative (for taking orthogonal direct sums). $\qquad\square$

5   A mysterious equality

Let V be a vector space over $\mathbb{F}_q$ of dimension $n = 2m + 1$, provided with a nondegenerate symmetric bilinear form g. For both odd and even q we have the following.

Proposition 5.1 *The number of g-selfadjoint nilpotent linear transformations N on V equals the number of pairs (N, x) with N as before, and x a nonisotropic projective point such that $Nx = 0$.*

Proof.   Let N be nilpotent and self-adjoint w.r.t. g. Then

$$\operatorname{rad} \ker N = \ker N \cap \operatorname{im} N.$$

Indeed, if $u \in \ker N$ and $v \in \operatorname{im} N$, that is, if $Nu = 0$ and $v = Nw$, then $g(u, v) = g(u, Nw) = g(Nu, w) = 0$. It follows that $\ker N$ is orthogonal to $\operatorname{im} N$, and that $\ker N \cap \operatorname{im} N \subseteq \operatorname{rad} \ker N \subseteq (\ker N + \operatorname{im} N)^\perp$. But $\dim((\ker N + \operatorname{im} N)^\perp) = n - \dim(\ker N + \operatorname{im} N) = \dim(\ker N \cap \operatorname{im} N)$, so equality holds.

Let $S := \ker N/(\ker N \cap \operatorname{im} N)$. Let $d = \dim \ker N$, and $e = \dim S$. We find that the number of nonisotropic points x of $\ker N$ is q^{d-e} times the number of nonisotropic points of S. For odd e that is $q^{d-e} \cdot q^{e-1} = q^{d-1}$. For even e, the number is not constant, since S can be hyperbolic or elliptic (for odd q) or standard or symplectic (for even q). Define

$$[e]' = \begin{cases} [e] & \text{if } e \text{ is odd,} \\ q^e & \text{if } e \text{ is even.} \end{cases} \qquad [e]'' = \begin{cases} q^e & \text{if } e \text{ is odd,} \\ [e] & \text{if } e \text{ is even.} \end{cases}$$

so that $[e]'[e]'' = q^e[e]$. We show that our claim is equivalent to

$$\sum_N 1 = \sum_N q^{d-e-1}[e]'',$$

9

where the sum is over self-adjoint nilpotent N (and d, e depend on N). Indeed, since there is up to isomorphism a unique form g, we can average over all forms g for which N is self-adjoint. Note that S, d, e do not depend on the choice of g. We already checked the case where e is odd, so let e be even, say $e = 2t$.

First suppose that q is odd. On the e-space S the various forms g induce $g_e(2t) = \frac{1}{2}q^{t^2}[1][3]\dots[2t-1](q^t-1)$ elliptic and $g_h(2t) = \frac{1}{2}q^{t^2}[1][3]\dots[2t-1](q^t+1)$ hyperbolic forms, with respectively $\frac{q^{2t-1}-1}{q-1}-q^{t-1}$ and $\frac{q^{2t-1}-1}{q-1}+q^{t-1}$ isotropic points, for an average of $\frac{q^{2t-1}-1}{q-1}+\frac{1}{q}$ isotropic points, and $q^{2t-1}-\frac{1}{q}=\frac{1}{q}(q^e-1)$ nonisotropic points, as claimed.

Now suppose that q is even. On the e-space S the various forms g induce $g_0(2t) = q^{-2t}g_s(2t)$ symplectic and $g_1(2t) = (q^{2t}-1)g_0(2t)$ standard forms, with respectively $\frac{q^{2t}-1}{q-1}$ and $\frac{q^{2t-1}-1}{q-1}$ isotropic points, with the same average as before.

Define a map $Y \mapsto Y'$ on Young diagrams (with odd n) as follows: find in Y the rightmost column with an odd number of squares, remove the bottom square from this column, and add it as a new row of length one at the bottom of the diagram. For example, the three diagrams here on the left all map to the diagram on the right.
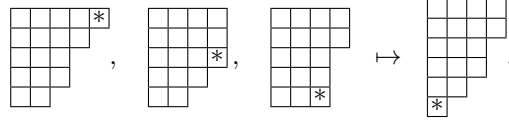
It may be that $Y' = Y$, namely when the only odd column is the first one. For example, the three diagrams here on the left all map to the diagram on the right.
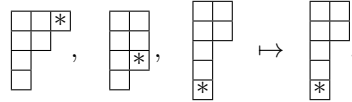
Our claim will now follow from

$$\sum_Y N_s(Y) = q^{d-e-1}[e]'' N_s(Y_0)$$

for each Young diagram Y_0 (with d rows, among which e of length 1), where the sum is over the Y with $Y' = Y_0$. We saw that $N_s(Y) = [2][4]\dots[2m]q^{m^2}\frac{g(Y)}{f(Y)}$, so have to show that $\sum_Y \frac{g(Y)f(Y_0)}{g(Y_0)f(Y)} = q^{d-e-1}[e]''$. Suppose the square moved in Y was at row s column t. Consulting the computation of $f(Y)$ and $g(Y)$, we see for $Y \neq Y_0$ that

$$\frac{f(Y_0)}{f(Y)} = \frac{[e][b]}{[c+1]}q^{2d-e-h-i-1}$$

and

$$\frac{g(Y)}{g(Y_0)} = \frac{[c+1]}{[e]'[b]'}q^{b+e+h-d}$$

where $b \geq 1$ is the size of the row group of Y_0 containing the row of the square that was removed in Y (with rows of length $t-1$), and $c \geq 0$ is the size of the row group of Y_0 with rows of length t, and $h \geq 0$ is the number of elements (in

Y or in Y_0) in column $t+1$, that is, the number of rows (in Y or in Y_0) with length larger than t, and $i \geq 0$ is the number of elements (in Y) in column $t-1$.

If $[e]'' = 0$, that is, if Y_0 has no row of length 1, there are no Y with $Y' = Y_0$, and we are done. Otherwise, we have to show that

$$\sum_Y [b]'' q^{-i} = \begin{cases} 1 & \text{if } Y_0' \neq Y_0 \\ 1 - (q^{d-e-1}[e]'')^{-1} & \text{if } Y_0' = Y_0. \end{cases}$$

where the sum is over the Y with $Y \neq Y_0$ and $Y' = Y_0$. If the LHS is empty, then $Y_0 = \square = Y_0'$ and $d = e = 1$ and $[e]'' = q$, and both sides are zero. Otherwise, let Y be the diagram with highest possible moving square (on the top row). If (its) b is odd, then the LHS has one term only, $i = b$, and $Y_0' \neq Y_0$, so that both sides are one. If b is even, then again $i = b$, and now $[b]'' q^{-i} = 1 - q^{-b}$. Now remove the first b rows from all Y and from Y_0 (so that d and all i are decreased by b), and apply induction. $\qquad \square$

Now, let V be a vector space over $\mathbb{F}_q$ of dimension $n = 2m > 0$, provided with a standard bilinear form g. For even q we prove the analog of Proposition 5.1. We use the Fitting decomposition and induction.

The Fitting decomposition shows that $q^{\frac{1}{2}n(n+1)} = \sum_M 1 = \sum_U N(U)S(U^\perp)$ where the sum is over self-adjoint M, nondegenerate subspaces U of V, and $N(U)$ is the number of self-adjoint nilpotent maps on U, and $S(W)$ is the number of self-adjoint invertible maps on W. We want to refine this equality.

First a lemma. Recall that in the present case (q even, n even, standard form) the isotropic points are precisely the points in $\mathbf{1}^\perp$. The subspace $\mathbf{1}^\perp$ is symplectic, with radical $\langle \mathbf{1} \rangle$.

Lemma 5.2 $\sum_U N(U)S(U^\perp) = q^{\frac{1}{2}n(n+1)-1}(q-1)$, where the sum is over the nondegenerate subspaces U of $\mathbf{1}^\perp$.

Proof. Put $a_s := |Sp(2s, q)| = q^{s^2} \prod_{i=1}^m [2i]$. A nondegenerate symplectic $2s$-space has $a_s/a_h a_{s-h} = q^{2h(s-h)} \prod_{i=0}^{h-1}[2s-2i]/\prod_{i=1}^h [2i]$ nondegenerate subspaces of dimension $2h$.

Let $\dim U = 2h$. Then $N(U) = q^{2h^2}$. The space $\mathbf{1}^\perp/\langle \mathbf{1} \rangle$ is a nondegenerate symplectic $(2m-2)$-space, and each nondegenerate $2h$-space in that quotient lifts to q^{2h} nondegenerate $2h$-spaces U in $\mathbf{1}^\perp$, so that the number of terms with $\dim U = 2h$ equals $q^{2h(m-h)} \prod_{i=0}^{h-1}[2m-2i-2]/\prod_{i=1}^h [2i]$. Finally, $S(U^\perp) = g_s(2m-2h) = q^{(m-h)(m-h+1)} \prod_{j=1}^{m-h}[2j-1]$. We see that our claim is equivalent to

$$\sum_{h=0}^{m-1} q^{2h(m-1)} \frac{\prod_{i=0}^{h-1}(1 - q^{-2m+2+2i})}{\prod_{i=1}^h (1-q^{2i})} \prod_{j=1}^{m-h-1}(1 - q^{2j+1}) = (-1)^{m-1} q^{m^2-1}.$$

Let $(a;q)_n = \prod_{i=0}^{n-1}(1 - aq^i)$. A simple computation shows that

$$\sum_{h=0}^{m-1} q^{h(m-1)}(q^{1-m};q)_h(q^{\frac{3}{2}};q)_{m-h-1}/(q;q)_h = (-1)^{m-1} q^{(m^2-1)/2}.$$

(For example, this is suitable as input for the Maple `qzeil` function.) Since this is our equation with q^2 replaced by q, we are done. $\qquad \square$

Proposition 5.3 *The number of g-selfadjoint nilpotent linear transformations N on V equals the number of pairs (N, x) with N as before, and x a nonisotropic projective point such that $Nx = 0$.*

(Yes, this says the same as Proposition 5.1, but this time $n = 2m$, q is even, and the form is not symplectic.)

Proof. We show by induction on n that $N(V) = \sum_N 1 = \sum_{N,x} 1$, where the sum is over nilpotent self-adjoint N and nonisotropic x in the kernel of N. This was shown above for odd n and all q. Here we settle the case of even n and even q, using the above result for odd n and even q.

Our claim is equivalent to $\sum_U N(U)S(U^\perp) = \sum_{U,N,x} S(U^\perp)$, where U runs over all nondegenerate subspaces of V containing a nonisotropic point (that is, all nondegenerate subspaces not contained in $\mathbf{1}^\perp$), and N over the self-adjoint nilpotent maps on U, and x over the nonisotropic points in U with $Nx = 0$. (Indeed, by induction we have termwise equality for all proper subspaces U of V, and $N(V)$ is multiplied by $S(V^\perp) = S(0) = 1$.)

Since $\sum_U N(U)S(U^\perp) = q^{\frac{1}{2}n(n+1)}$, the lemma gives $\sum_{U \nsubseteq \mathbf{1}^\perp} N(U)S(U^\perp) = q^{\frac{1}{2}n(n+1)-1}$. Hence, our claim is equivalent to $\sum_{U,N,x} S(U^\perp) = q^{\frac{1}{2}n(n+1)-1}$.

Using the Fitting decomposition of M, we see $\sum_{M,x} 1 = \sum_{U,N,x} S(U^\perp)$ where the left-hand sum is over the self-adjoint M and nonisotropic x with $Mx = 0$. The number of nonisotropic projective points in V is q^{n-1} (all points outside the hyperplane $\mathbf{1}^\perp$). Given a nonisotropic point x, the number of self-adjoint maps M with $Mx = 0$ is q^{-n} times the total number of self-adjoint maps M, that is, is $q^{\frac{1}{2}n(n-1)}$. It follows that $\sum_{M,x} 1 = q^{\frac{1}{2}n(n+1)-1}$ as desired.
□

6 Going down

Proposition 6.1 *For odd q, let $N_a = (N_h + N_e)/2$ and $N_d = (N_h - N_e)/2$. Then $N_s(2m+1) = q^{2m}N_a(2m) + q^m N_d(2m)$.*

Proof. The claim says that

$$N_s(2m+1) = \frac{1}{2}q^m(q^m+1)N_h(2m) + \frac{1}{2}q^m(q^m-1)N_e(2m).$$

In a nondegenerate orthogonal geometry of (vector space) dimension $2m+1$ there are $\frac{1}{2}q^m(q^m+1)$ nonisotropic projective points x such that $x^\perp$ is hyperbolic, and $\frac{1}{2}q^m(q^m-1)$ nonisotropic projective points x such that $x^\perp$ is elliptic. (This is well known, and easy to prove: Count pairs (x, z) of projective points, with x nonisotropic and z isotropic, and $g(x, z) = 0$. There are $(q^{2m}-1)/(q-1)$ choices for z, and given z there are q^{2m-1} choices for x. Conversely, if we choose x first, and $x^\perp$ is hyperbolic for h choices of x, and elliptic for e choices of x, then $h + e = q^{2m}$ and $h(\frac{q^{2m-1}-1}{q-1} + q^{m-1}) + e(\frac{q^{2m-1}-1}{q-1} - q^{m-1}) = q^{2m-1}(\frac{q^{2m}-1}{q-1})$ and we find the desired values for h, e.)

If x is a nonisotropic point, then the self-adjoint nilpotent maps N for which $Nx = 0$ preserve $x^\perp$, and hence are in 1-1 correspondence with the self-adjoint nilpotent maps on $x^\perp$. Our claim can be reformulated as

$$\#\{N \mid N \text{ self-adjoint, nilpotent}\} =$$
$$\#\{(N, x) \mid N \text{ self-adjoint, nilpotent, } Nx = 0, \ g(x, x) \neq 0\}$$

for a vector space V of dimension $2m+1$ over $\mathbb{F}_q$ for odd q, provided with a nondegenerate symmetric bilinear form g. But this is precisely the statement of Proposition 5.1. □

Proposition 6.2 *Let q be even. Then $N_s(2m+1) = (q^{2m}-1)N_1(2m)+N_0(2m)$.*

Proof. Again apply Proposition 5.1, noting that there are q^{2m} nonisotropic points, precisely one of which has a symplectic perp. □

Proposition 6.3 *Let q be even. Then $N_1(2m) = q^{2m-1}N_s(2m-1)$.*

Proof. Apply Proposition 5.3, noting that there are q^{2m-1} nonisotropic points. □

Summary

In the introduction we used $e(2m), h(2m), p(2m+1), z(2m), s(2m), s(2m+1)$ for what we later called $N_e, N_h, N_s, N_0, N_1, N_s$, respectively. Proposition 4.1 proves Propositions 1.1, 1.3 and 1.4. Theorem 2.2 proves Proposition 1.2. Propositions 6.1, 6.2 and 6.3 prove Propositions 1.5, 1.6 and 1.7. Corollary 1.8 follows, and Proposition 1.8 says that the standard form is elliptic only when $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$, which we remarked in the intro of §4. Finally, Proposition 1.10 is proved in §5.

7 Ranks and exponents

From the Young diagram Y of a nilpotent map N one can read off its rank (n minus the number of rows) and exponent (the number of columns). By summing not over all Y but over the Y with a given number of rows or columns, one obtains results for the number of self-adjoint nilpotent matrices of a given rank or exponent.

We have precise conjectures for the values $e(2m, r)$, $h(2m, r)$ etc. that count self-adjoint nilpotent matrices of a given rank r. See [2].

Concerning the case of a given exponent, let $E_s(n, e)$ be the number of symmetric nilpotent matrices of order n and exponent e. Then $E_s(n, n) = N_s(Y)$ for Y a single row like ⬚⬚⬚⬚⬚⬚⬚, which we determined in §4.4. For small i, the function $E_s(n, n-i)$ has simple behaviour.

Lemma 7.1 *(i) If $n = 2m+1$, then $E_s(n,n) = [2][4]\ldots[2m]\,q^{m^2}$.*
(ii) For n odd, $n > 2i$, the ratio $E_s(n, n-i)/E_s(n,n)$ is independent of n.

Proof. Let n be odd. We saw in §4.4 that $N_s(Y) = [2][4]\ldots[2m]\,q^{m^2}\frac{g(Y)}{f(Y)}$.

(i) For Y a single row, we have $f(Y) = g(Y)$.

(ii) The ratio $E_s(n, n-i)/E_s(n,n)$ is $\sum_Y \frac{g(Y)}{f(Y)}$ where the sum is over the Y with $n-i$ columns. If Y has a unique longest row, and Y' is obtained from Y by adding two squares at the end of the first row, then Y and Y' have the same row groups, and $f(Y') = q^2 f(Y)$ and $g(Y') = q^2 g(Y)$ so that $g(Y')/f(Y') = g(Y)/f(Y)$. More generally, if the row group containing the longest row in Y has odd size $2t+1$, then $f(Y') = q^{2t+2}[1]f(Y)/[2t+1]$ and $g(Y') = q^{2t+2}[1]g(Y)/[2t+1]$ and again $g(Y')/f(Y') = g(Y)/f(Y)$. □

References

[1] A. A. Albert, *Symmetric and alternate matrices in an arbitrary field*, Trans. Amer. Math. Soc. **43** (1938) 386–436.

[2] A. E. Brouwer, `http://www.win.tue.nl/~aeb/math/symnilp.html`.

[3] A. E. Brouwer, A. M. Cohen & A. Neumaier, *Distance-regular graphs*, Springer, Heidelberg, 1989.

[4] M. C. Crabb, *Counting nilpotent endomorphisms*, Finite Fields Appl. **12** (2006) 151–154.

[5] N. J. Fine & I. N. Herstein, *The probability that a matrix be nilpotent*, Illinois J. Math. **2** (1958) 499–504.

[6] M. Gerstenhaber, *On the number of nilpotent matrices with coefficients in a finite field*, Illinois J. Math. **5** (1961) 330–333.

[7] Philip Hall, *Lectures by Philip Hall, St Andrews colloquium, 13–23 July, 1955*, transcribed by Clara Murray.

[8] G. Lusztig, *A note on counting nilpotent matrices of fixed rank*, Bull. London Math. Soc. **8** (1976) 77–80.

[9] T. A. Springer, *The Steinberg function of a finite Lie algebra*, Inventiones Math. **58** (1980) 211–215.

[10] Robert Steinberg, *Endomorphisms of linear algebraic groups*, Memoirs of the American Mathematical Society, vol. 80, AMS, Providence, R.I., 1968.