Journal of Integer Sequences, Vol. 13 (2010),
Article 10.3.6

On q-Analogs of Recursions for the Number of Involutions and Prime Order Elements in Symmetric Groups

Max B. Kutler
Department of Mathematics
Harvey Mudd College 301 Platt Boulevard
Claremont, CA 91711
USA
mkutler@hmc.edu

C. Ryan Vinroot
Department of Mathematics
College of William and Mary
P. O. Box 8795
Williamsburg, VA 23187
USA
vinroot@math.wm.edu

Abstract

The number of elements whose square is the identity in the symmetric group S_n is recursive in n. This recursion may be proved combinatorially, and there is also a nice exponential generating function for this sequence. We study q-analogs of this phenomenon. We begin with sums involving q-binomial coefficients which come up naturally when counting elements in finite classical groups which square to the identity, and we obtain a recursive-like identity for the number of such elements in finite special orthogonal groups. We then study a q-analog for the number of elements in the symmetric group whose pth power is the identity, for some fixed prime p. We find an Eulerian generating function for these numbers, and we prove the q-analog of the recursion for these numbers by giving a combinatorial interpretation in terms of vector spaces over finite fields.

1 Introduction

Let S_n denote the symmetric group on the first n positive integers, and let T_n be the number of elements g in S_n such that g^2 is the identity permutation. Chowla, Herstein, and Moore [2] studied the sequence $\{T_n\}$ (A000085), and they began by observing that it is recursive. In particular, $T_0 = T_1 = 1$ (where we let S_0 and S_1 be trivial groups), and for $n \geq 1$,

$$T_{n+1} = T_n + nT_{n-1}. \tag{1}$$

There is a direct combinatorial argument that gives (1). Namely, an element in S_{n+1} whose square is the identity either fixes the point $n+1$, the number of which is T_n, or moves $n+1$. In the latter case, $n+1$ can be paired with one of the n other points to form a transposition, which may be combined with a permutation of the remaining $n-1$ points whose square is the identity, giving nT_{n-1} such elements.

Another property of the sequence $\{T_n\}$ noticed by Chowla, Herstein, and Moore [2], is that it has a particularly nice exponential generating function, in that we have

$$\sum_{n=0}^{\infty} \frac{T_n}{n!} x^n = e^{x+x^2/2}.$$

Chowla, Herstein, and Moore [2] applied the above properties of the numbers T_n to obtain asymptotic formulas in n for T_n/T_{n-1} and T_n, as well as several divisibility properties of T_n. Jacobsthal [8] studied similar properties of the number of elements in S_n of order some fixed prime (which we discuss in Section 4.1); Chowla, Herstein, and Scott [3] gave an exponential generating function for the number of elements g of S_n that satisfy $g^d = 1$ for any fixed positive integer d; and Moser and Wyman [10] obtained further results on asymptotic formulas for these quantities. More recently, these ideas have been applied to study related exponential generating functions for larger classes of groups, such as in the papers of Chigira [1] and Müller [11].

The purpose of this paper is to study q-analogs of recursions similar to (1). In Section 2, we introduce properties of the q-binomial coefficients. In Section 3, we study sums involving q-binomial coefficients that are related to counting elements in finite classical groups whose square is the identity. We prove a recursive-like formula for these numbers in Theorem 5, and we apply this to obtain an interesting result on the number of order two elements in finite special orthogonal groups in Corollary 6.

In Section 4, we turn to the problem of counting elements g in the symmetric group S_n which satisfy $g^p = 1$, for some fixed prime p (yielding the sequence A052501 when $p = 5$). Section 4.1 summarizes the classical results on this problem. In Section 4.2, we give a q-analog for these numbers, for which we give a combinatorial interpretation in terms of $\mathbb{F}_q$-vector spaces (Proposition 7) and an Eulerian generating function (Proposition 8). We then prove Theorem 9, a recursive-like formula for these numbers. Finally, in Section 4.3, we specialize to the case $p = 2$, and relate our results to other results on involutions in the symmetric groups.

2 Properties of q-binomial coefficients

Let q denote a parameter different from 1. For the sake of combinatorial interpretation it will often be useful to think of q as the power of some prime. For any positive integer n, we let $[n]$ denote the nth *q-integer*, defined as

$$[n] = q^{n-1} + q^{n-2} + \cdots + q + 1 = \frac{q^n - 1}{q - 1}.$$

The q-integer $[n]$ is an example of a *q-analog* of an expression, since we have $\lim_{q\to 1}[n] = n$. We define the *q-factorial* of the integer $n \geq 0$, denoted $[n]!$, recursively as

$$[n]! = \begin{cases} 1, & \text{if } n = 0; \\ [n][n-1]!, & \text{if } n > 0. \end{cases}$$

Once we have the q-factorial, we may define the *q-binomial coefficients* in a natural way. That is, if n and k are non-negative integers with $n \geq k$, we define $\binom{n}{k}_q$ as

$$\binom{n}{k}_q = \frac{[n]!}{[k]![n-k]!}. \tag{2}$$

We recognize the q-binomial coefficient as a q-analog of the classical binomial coefficient since we have $\lim_{q\to 1} \binom{n}{k}_q = \binom{n}{k}$.

The q-binomial coefficient has an important combinatorial interpretation when q is the power of a prime. In this case, $\binom{n}{k}_q$ is equal to the number of k-dimensional subspaces of an n-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements [13, Proposition 1.3.18].

Note that it follows immediately from (2) that we have

$$\binom{n}{k}_q = \binom{n}{n-k}_q. \tag{3}$$

The q-binomial coefficients have many other properties which are very similar to those of the classical binomial coefficients, and these properties can be proven using the definition (2) directly, as well as bijectively in terms of $\mathbb{F}_q$-vector spaces.

The following result is the *q-Pascal identity* for the q-binomial coefficients, which follows quickly from (2). In a bijective proof of the Proposition 1, the key observation is that in an n-dimensional $\mathbb{F}_q$-vector space V, the number of k-dimensional subspaces of V which are not contained in some fixed $(n-1)$-dimensional subspace of V is exactly $q^{n-k}\binom{n-1}{k-1}_q$.

Proposition 1. *The q-binomial coefficients satisfy the following property, when $n, k \geq 1$:*

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q.$$

It follows from Proposition 1 and an induction argument that the q-binomial coefficients are always polynomials in q. The next result is also most directly obtained by the definition (2), although an $\mathbb{F}_q$-vector space proof may be obtained by induction on d.

Proposition 2. *The q-binomial coefficients satisfy the following property, for any $d \geq 1$, and any n and k such that $n \geq k \geq d$:*

$$[k][k-1]\cdots[k-d+1]\binom{n}{k}_q = [n][n-1]\cdots[n-d+1]\binom{n-d}{k-d}_q.$$

Finally, define a q-analog of the exponential function as $e_q^x = \sum_{j=0}^{\infty} \frac{x^j}{[j]!}$. If $\{A_n\}_{n=0}^{\infty}$ is any sequence, then we define the *Eulerian generating function* for the sequence $\{A_n\}$ to be the power series $\sum_{j=0}^{\infty} \frac{A_j}{[j]!} x^j$. That is, an Eulerian generating function is just a q-analog of an exponential generating function.

3 Counting order 2 elements in finite classical groups

For q the power of a prime, and $n \geq 1$ an integer, define

$$I_n(q) = \sum_{k=0}^{n} q^{k(n-k)} \binom{n}{k}_q.$$

The following result is given by Morrison [9, Section 1.11].

Proposition 3. *If q is the power of an odd prime, then $I_n(q)$ is the number of elements in $\mathrm{GL}(n, \mathbb{F}_q)$ whose square is the identity.*

We note that Proposition 3 also follows by noticing that an element in $\mathrm{GL}(n, \mathbb{F}_q)$ whose square is the identity is determined by a choice of the eigenspaces for $+1$ and -1, which are complementary subspaces in $\mathbb{F}_q^n$. The number of ways to choose one of these spaces of dimension k is $\binom{n}{k}_q$, and the number of complements is $q^{k(n-k)}$ [12, Lemma 3].

If q is the power of an odd prime, and V is an n-dimensional vector space over $\mathbb{F}_q$, let $\langle \cdot, \cdot \rangle$ be a non-degenerate symmetric form on V. The *special orthogonal group for* $\langle \cdot, \cdot \rangle$ is defined to be the group of invertible $\mathbb{F}_q$-linear transformations of V with determinant 1 which preserve the form $\langle \cdot, \cdot \rangle$. See [7], for example, for the classification of symmetric bilinear forms over $\mathbb{F}_q$, and the isomorphism classes of the corresponding special orthogonal groups. In particular, when n is odd, there is exactly one isomorphism class of special orthogonal group, which we denote by $\mathrm{SO}(n, \mathbb{F}_q)$, and when n is even, there are two classes of these groups, which we denote by $\mathrm{SO}^+(n, \mathbb{F}_q)$ and $\mathrm{SO}^-(n, \mathbb{F}_q)$, or by $\mathrm{SO}^{\pm}(n, \mathbb{F}_q)$ to denote either class of group simultaneously.

The second-named author [14, Section 4] proved the following, using results on the centralizers of conjugacy classes in the finite special orthogonal groups.

Proposition 4. *Let q be the power of an odd prime. If $G = \mathrm{SO}^{\pm}(2m, \mathbb{F}_q)$, then the number of elements in G whose sequare is the identity is $I_m(q^2)$. If $G = \mathrm{SO}(2m+1, \mathbb{F}_q)$, then the number of elements in G whose square is the identity is*

$$\sum_{k=0}^{m} q^{2k(m-k+1)} \binom{m}{k}_{q^2}.$$

Proposition 4 prompts the following definition generalizing $I_n(q)$. For any integer j, define $I_n^{(j)}(q)$ by

$$I_n^{(j)}(q) = \sum_{k=0}^{n} q^{k(n-k+j)} \binom{n}{k}_q.$$

So, $I_n^{(0)}(q) = I_n(q)$, and the number of elements in $\mathrm{SO}(2m+1, \mathbb{F}_q)$ whose square is the identity is $I_m^{(1)}(q^2)$. The numbers $I_n^{(j)}(q)$ have the following property.

Theorem 5. *The numbers $I_n^{(j)}(q)$ satisfy the formula*

$$I_{n+1}^{(j)}(q) = I_n^{(j)}(q) + q^{nj}(q^n - 1) I_{n-1}^{(1-j)}(q) + q^{(n+1)j} I_n^{(2-j)}(q).$$

Proof. First, by Proposition 1, we have

$$I_{n+1}^{(j)}(q) = \sum_{k=0}^{n+1} q^{k(n+1-k+j)} \binom{n+1}{k}_q = 1 + \sum_{k=1}^{n+1} q^{k(n+1-k+j)} \left(\binom{n}{k}_q + q^{n+1-k} \binom{n}{k-1}_q \right).$$

We may rewrite this as

$$\begin{aligned} &\sum_{k=0}^{n} q^{k(n-k+j)} \binom{n}{k}_q + \sum_{k=0}^{n} (q^{k(n+1-k+j)} - q^{k(n-k+j)}) \binom{n}{k}_q + \sum_{k=1}^{n+1} q^{(k+1)(n+1-k)+kj} \binom{n}{k-1}_q \\ &= I_n^{(j)}(q) + \sum_{k=0}^{n} q^{k(n-k+j)} (q^k - 1) \binom{n}{k}_q + \sum_{k=0}^{n} q^{(k+2)(n-k)+(k+1)j} \binom{n}{k}_q. \end{aligned}$$

Now, by applying Proposition 2 with $d = 1$, and then reindexing the first summation, we have

$$\begin{aligned} I_{n+1}^{(j)}(q) &= I_n^{(j)}(q) + (q^n - 1) \sum_{k=1}^{n} q^{k(n-k+j)} \binom{n-1}{k-1}_q + \sum_{k=0}^{n} q^{(k+2)(n-k)+(k+1)j} \binom{n}{k}_q \\ &= I_n^{(j)}(q) + (q^n - 1) \sum_{k=0}^{n-1} q^{(k+1)(n-k-1+j)} \binom{n-1}{k}_q + \sum_{k=0}^{n} q^{(k+2)(n-k)+(k+1)j} \binom{n}{k}_q. \end{aligned}$$

Finally, by (3), we may switch k with $n-1-k$ in the first summation, and k with $n-k$ in the second summation above to obtain

$$\begin{aligned} I_{n+1}^{(j)}(q) &= I_n^{(j)}(q) + (q^n - 1) \sum_{k=0}^{n-1} q^{(n-k)(k+j)} \binom{n-1}{k}_q + \sum_{k=0}^{n} q^{k(n-k+2)+(n-k+1)j} \binom{n}{k}_q \\ &= I_n^{(j)}(q) + (q^n - 1) \sum_{k=0}^{n-1} q^{nj} q^{k(n-k-j)} \binom{n-1}{k}_q + \sum_{k=0}^{n} q^{(n+1)j} q^{k(n-k+2-j)} \binom{n}{k}_q \\ &= I_n^{(j)}(q) + q^{nj}(q^n - 1) I_{n-1}^{(1-j)}(q) + q^{(n+1)j} I_n^{(2-j)}(q), \end{aligned}$$

as desired. $\square$

If we let $j = 0$ in Theorem 5, then we have the following relationship between the number of elements in $\mathrm{GL}(n+1, \mathbb{F}_q)$ and in $\mathrm{GL}(n, \mathbb{F}_q)$ whose square is the identity, when q is the power of an odd prime:

$$I_{n+1}(q) = I_n(q) + (q^n - 1)I^{(1)}_{n-1}(q) + I^{(2)}_n(q).$$

This is reminiscent of the recursion of the numbers $G_n(q) = \sum_{k=0}^{n} \binom{n}{k}_q$, which satisfy $G_{n+1}(q) = 2G_n(q) + (q^n - 1)G_{n-1}(q)$, a result due to Goldman and Rota [6].

If we let $j = 1$ in Theorem 5, and replace q with q^2, where q is the power of an odd prime, then we get the following particularly nice result, which follows from Proposition 4.

Corollary 6. *Let q be the power of an odd prime, and let $n > 1$. The number of elements whose square is the identity in $\mathrm{SO}(2n+3, \mathbb{F}_q)$ (which is $I^{(1)}_{n+1}(q^2)$), in $\mathrm{SO}(2n+1, \mathbb{F}_q)$ (which is $I^{(1)}_n(q^2)$), and in $\mathrm{SO}(2n-2, \mathbb{F}_q)$ (which is $I^{(0)}_{n-1}(q^2)$) are related in the following way:*

$$I^{(1)}_{n+1}(q^2) = (q^{2n+2} + 1)I^{(1)}_n(q^2) + q^{2n}(q^{2n} - 1)I^{(0)}_{n-1}(q^2).$$

It would be interesting to have a purely combinatorial proof of Corollary 6, by directly counting elements whose square is the identity in these groups, but we have not been able to find such a proof.

4 A q-analog of the number of prime order elements in S_n

4.1 Counting prime order elements in S_n

Let p be prime, and let $T^{(p)}_n$ be the number of elements g in S_n such that g^p is the identity. In the Introduction, we gave some properties of the numbers $T_n = T^{(2)}_n$, and here we give the analogous properties of $T^{(p)}_n$ due to Jacobsthal [8].

An element g in S_{n+1} which satisfies $g^p = 1$ either fixes the point $n+1$, or it does not. There are $T^{(p)}_n$ such elements in S_{n+1} which fix the point $n+1$. If such an element does not fix the point $n+1$, then it contains a p-cycle permuting $n+1$. The number of such p-cycles can be seen to be $n(n-1)\cdots(n-p+2)$ by assuming that, in cycle notation, $n+1$ appears in the first position, and then choosing the remaining $p-1$ points in the cycle from the set $\{1, 2, \ldots, n\}$. To construct the rest of the element, we may permute the remaining $n-p+1$ points in such a way that our element still satisfies $g^p = 1$, and the number of ways in which to do this is exactly $T^{(p)}_{n-p+1}$. This implies that we have the following recursion:

$$T^{(p)}_{n+1} = T^{(p)}_n + n(n-1)\cdots(n-p+2)T^{(p)}_{n-p+1}. \tag{4}$$

We may also enumerate $T^{(p)}_n$ directly. An element g in S_n satisfying $g^p = 1$ may consist of anywhere from 0 (the identity element) to $\lfloor n/p \rfloor$ disjoint p-cycles. If g consists of exactly k disjoint p-cycles, then we may choose the points permuted in these p-cycles in $\binom{n}{pk}$ ways. We then order these points in one of $(pk)!$ ways, where each block of p points form a p-cycle.

But each of these p-cycles, written in cycle notation, may be written in p ways, and the k different p-cycles may be ordered in any of $k!$ ways to obtain the same element. Putting all of this together, we obtain the formula

$$T_n^{(p)} = \sum_{k=0}^{\lfloor n/p \rfloor} \frac{(pk)!}{p^k k!} \binom{n}{pk}. \tag{5}$$

We may rewrite (5) in a few different useful ways. For any integer $m \geq 2$, we define the *m-fold multifactorial* of an integer $r \geq 0$, denoted $r!^{(m)}$ as the product

$$r!^{(m)} = r(r-m)(r-2m)\cdots(r-tm), \text{ where } t \geq 0 \text{ is maximum such that } r > tm.$$

So, for example, $r!^{(2)}$, which is also written $r!!$, is the product of every other decreasing positive integer, starting with r. Using this notation, and by rewriting the binomial coefficients as factorials and reindexing, we may write $T_n^{(p)}$ as

$$T_n^{(p)} = \sum_{k=0}^{\lfloor n/p \rfloor} \frac{(pk)!}{(pk)!^{(p)}} \binom{n}{pk} = \sum_{i,j \geq 0, pi+j=n} \frac{n!}{p^i i! j!}. \tag{6}$$

It follows from the second formula for $T_n^{(p)}$ in (6) above, that $e^{x+x^p/p}$ is the exponential generating function for $T_n^{(p)}$.

4.2 A q-analog

For any integer $m \geq 2$, and a parameter q, define the *m-fold q-multifactorial* of an integer $r \geq 0$, denoted $[r]!^{(m)}$, by

$$[r]!^{(m)} = [r][r-m][r-2m]\cdots[r-tm], \text{ where } t \geq 0 \text{ is maximum such that } r > tm.$$

Continue to let p be a prime, and let $n \geq 0$. Define $T_n^{(p)}(q)$ to be the following:

$$T_n^{(p)}(q) = \sum_{k=0}^{\lfloor n/p \rfloor} \frac{[pk]!}{[pk]!^{(p)}} \binom{n}{pk}_q. \tag{7}$$

It is immediate from the first formula for $T_n^{(p)}$ in (6) that we have $\lim_{q\to 1} T_n^{(p)}(q) = T_n^{(p)}$, so that $T_n^{(p)}(q)$ is a q-analog of $T_n^{(p)}$. In the case that q is the power of a prime (independent of the prime p), there is a combinatorial interpretation of $T_n^{(p)}(q)$. Before that, we need a definition.

If V is any vector space of dimension n, define a *complete flag* of V to be a chain of subspaces of V,

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_{n-1} \subset V_n = V,$$

such that $\dim(V_i) = i$ for each i. For example, if we have a basis $\{v_1, v_2, \ldots, v_n\}$ of V, then a complete flag of V may be obtained by taking $V_i = \mathrm{span}\{v_1, \ldots, v_i\}$. Henceforth, we will let a *line* in a vector space V mean a one-dimensional subspace of V.

Proposition 7. *Let p be prime, q the power of a prime (independent of p), $n \geq 0$, and V an n-dimensional $\mathbb{F}_q$-vector space. Then $T_n^{(p)}(q)$ is the number of ways to choose a subspace W of V with dimension divisible by p, together with, for some complete flag of W, a sequence of lines, one in each subspace of the complete flag with dimension not divisible by p.*

Proof. First, to choose a subspace of V with dimension divisible by p, we must take some non-negative integer $k \leq \lfloor n/p \rfloor$, and choose a subspace W of V of dimension pk, the number of which is $\binom{n}{pk}_q$. Now, given a complete flag of W, if W_i is a subspace in the flag with $\dim(W_i) = i$, then the number of lines in W_i is $\binom{i}{1}_q = [i]$. So, the number of ways to choose a sequence of lines, one in each subspace of dimension not divisible by p in a given flag of W, is exactly

$$[pk-1][pk-2]\cdots[pk-p+1][pk-p-1][pk-p-2]\cdots[p+1][p-1]\cdots[2][1] = \frac{[pk]!}{[pk]!^{(p)}}.$$

Putting all of this together, we get exactly the formula for $T_n^{(p)}(q)$ in (7). □

We can also describe $T_n^{(p)}(q)$ in terms of an Eulerian generating function, as follows.

Proposition 8. *The Eulerian generating function for $T_n^{(p)}(q)$ is given by*

$$\left(\sum_{i=0}^{\infty} \frac{x^{pi}}{[pi]!^{(p)}}\right) e_q^x.$$

Proof. We have

$$\begin{aligned}\left(\sum_{i=0}^{\infty} \frac{x^{pi}}{[pi]!^{(p)}}\right) e_q^x &= \sum_{i=0}^{\infty} \frac{x^{pi}}{[pi]!^{(p)}} \sum_{j=0}^{\infty} \frac{x^j}{[j]!} = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{\lfloor n/p \rfloor} \frac{1}{[pk]!^{(p)}[n-pk]!}\right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{\lfloor n/p \rfloor} \frac{[pk]!}{[pk]!^{(p)}} \frac{[n]!}{[pk]![n-pk]!}\right) \frac{x^n}{[n]!} = \sum_{n=0}^{\infty} \frac{T_n^{(p)}(q)}{[n]!} x^n,\end{aligned}$$

as desired. □

Next, we see that the $T_n^{(p)}(q)$ have a property similar to the recursion in (4) of the $T_n^{(p)}$.

Theorem 9. *For p a prime, and $n \geq 0$, define $R_n^{(p)}(q)$ to be the following polynomial:*

$$R_n^{(p)}(q) = \sum_{k=0}^{\lfloor n/p \rfloor} q^{n-pk} \frac{[pk]!}{[pk]!^{(p)}} \binom{n}{pk}_q.$$

Then for all $n \geq p-1$, the $T_n^{(p)}(q)$ satisfy

$$T_{n+1}^{(p)}(q) = T_n^{(p)}(q) + [n][n-1]\cdots[n-p+2] R_{n-p+1}^{(p)}(q),$$

and $T_n^{(p)}(q) = 1$ for $0 \leq n \leq p-2$.

Note that if we let $q \to 1$, the identity for the $T_n^{(p)}(q)$ in Theorem 9 turns into the recursion (4), since we have $\lim_{q\to 1} R_n^{(p)}(q) = T_n^{(p)}$. We now give a combinatorial proof of Theorem 9 using Proposition 7.

Proof of Theorem 9. Let V be an $(n+1)$-dimensional $\mathbb{F}_q$-vector space, and let $\{v_1, \ldots, v_{n+1}\}$ be a basis for V. By Proposition 7, $T_{n+1}^{(p)}(q)$ is the number of ways to choose a subspace W of V with dimension divisible by p, together with a line in each of the subspaces in some complete flag of W with dimension not divisible by p. We now count this quantity another way.

Define $V_0 = \{0\}$ and $V_i = \operatorname{span}\{v_1, \ldots, v_i\}$ for $1 \le i \le n+1$. For any subspace W of V of dimension divisible by p, say $\dim(W) = pk$, we take a complete flag of W as follows. Let $W_0 = W \cap V_0 = \{0\}$, and for each j such that $1 \le j \le pk$, define $W_j = W \cap V_i$, where i is minimal so that $\dim(W_j) = j$. Now, $W_0 \subset W_1 \subset \cdots \subset W_{pk} = W$ is a complete flag of W.

First suppose that the subspace W is contained in V_n. The number of ways to choose a subspace W of V_n of dimension divisible by p, along with a sequence of lines in each space of dimension not divisible by p in the complete flag of W defined above, is equal to $T_n^{(p)}(q)$ by Proposition 7.

Now consider the case that our subspace W with dimension divisible by p is not a subspace of V_n. Suppose that $\dim(W) = pk$, where k satisfies $1 \le k \le \lfloor \frac{n}{p} \rfloor$. Since W is not completely contained in V_n, we must have $\dim(W \cap V_n) = pk - 1$, and so $W \cap V_n = W_{pk-1}$. By the remarks given before Proposition 1, the number of ways to choose our subspace W is $q^{n+1-pk}\binom{n}{pk-1}_q$.

Now that we have chosen our subspace W, we now choose lines from the subspaces W_i, where $pk - p + 1 \le i \le pk - 1$. The number of ways to do this is exactly $[pk-p+1][pk-p+2]\cdots[pk-1]$. So now, the number of ways to select W, together with these lines, is

$$q^{n+1-pk}[pk-1]\cdots[pk-p+2][pk-p+1]\binom{n}{pk-1}_q,$$

where $[pk-1]\cdots[pk-p+2][pk-p+1]\binom{n}{pk-1}_q$ counts the number of ways to select our $W' = W_{pk-1}$, together with these lines. By Proposition 2 with $d = p-1$, we know that this is also counted by $[n][n-1]\cdots[n-p+2]\binom{n-p+1}{pk-p}_q$, by first choosing lines from V_i, for $n-p+2 \le i \le n$. So, the total number of ways to select our space W, together with these $p-1$ lines, is

$$q^{n+1-pk}[n][n-1]\cdots[n-p+2]\binom{n-p+1}{pk-p}_q.$$

Now, consider the complete flag $\{0\} = W_0 \subset \cdots \subset W_{pk} = W$ of W, where $\{0\} = W_0 \subset \cdots \subset W_{pk-p}$ is a complete flag of W_{pk-p}. We have already selected lines from the subspaces $W_{pk-p+1}, \ldots, W_{pk-1}$, so we need only choose lines from the remaining W_i with dimension not divisible by p. By the argument in the proof of Proposition 7, the number of ways to do this is $\frac{[pk-p]!}{[pk-p]!^{(p)}}$. Putting all of this together, the number of ways to choose a dimension pk subspace W of V which is not contained in V_n, together with a sequence of lines, one each from the subspaces of dimension not divisible by p in our complete flag of W, is

$$[n][n-1]\cdots[n-p+2]q^{n+1-pk}\frac{[pk-p]!}{[pk-p]!^{(p)}}\binom{n-p+1}{pk-p}_q.$$

Summing over all possible k and reindexing, gives a total of $[n][n-1]\cdots[n-p+2]R^{(p)}_{n-p+1}(q)$. We note that it follows from this argument that $R^{(p)}_{n-p+1}(q)$ is the number of ways, after choosing lines from V_i for $n-p+2 \le i \le n$, to choose our subspace and the remaining lines appropriately. Adding $[n][n-1]\cdots[n-p+2]R^{(p)}_{n-p+1}(q)$ to $T^{(p)}_n(q)$, the count for the case where W is contained in V_n, gives the desired result. □

4.3 The case $p = 2$

We began in the Introduction with a discussion of the number of elements whose square is the identity, or *involutions*, in the symmetric group. The set of involutions of the symmetric group is of particular interest, because, for example, the centralizer of a fixed point free involution is a Weyl group of type B, and plays an important role in Lie theory. There are various statistics on involutions which are useful to keep track of using generating functions [4, 5]. Such generating functions can provide for more examples of q-analogs of the number $T^{(2)}_n$ of involutions in S_n.

Deodhar and Srinivasan [4], for example, define the *weight* of an involution $\delta \in S_n$, denoted $\mathrm{wt}(\delta)$, as follows. If δ is written in cycle notation, and $(i\ j)$ is one of the disjoint transpositions of δ, then write $(i\ j) \in \delta$ with the assumption $i < j$, and define $\mathrm{sp}(i\ j) = j-i-1$. If we draw an arc diagram for δ, where an arc from i to j denotes $(i\ j) \in \delta$, then let $c(\delta)$ denote the number of crossings of arcs in the diagram (see [4, Section 1]). Now define the weight of δ as

$$\mathrm{wt}(\delta) = \left(\sum_{(i\ j)\in\delta} \mathrm{sp}(i\ j)\right) - c(\delta).$$

Let $\mathrm{Inv}(n,k)$ denote the set of involutions in S_n which are a product of exactly k disjoint transpositions, and define $i_q(n,k)$ to be the generating function

$$i_q(n,k) = \sum_{\delta\in\mathrm{Inv}(n,k)} q^{\mathrm{wt}(\delta)}.$$

Deodhar and Srinivasan [4, Proposition 2.1] proved that the $i_q(n,k)$ satisfy the recursion

$$i_q(n+1,k) = i_q(n,k) + [n]i_q(n-1,k-1). \tag{8}$$

If we define $\mathcal{I}_n(q) = \sum_{k=0}^{\lfloor n/2\rfloor} i_q(n,k)$, then it follows from (8) that

$$\mathcal{I}_{n+1}(q) = \mathcal{I}_n(q) + [n]\mathcal{I}_{n-1}(q), \tag{9}$$

which is a q-analog of (1). Indeed, it follows from the definition of $i_q(n,k)$ as a generating function that $\lim_{q\to1}\mathcal{I}_n(q) = T^{(2)}_n$.

It is unclear what is exactly the connection between $\mathcal{I}_n(q)$ and $T_n^{(2)}(q)$, or whether $\mathcal{I}_n(q)$ has an interpretation in terms of $\mathbb{F}_q$-vector spaces. Such an interpretation seems possible, since $i_q(2n, n) = [2n]!/[2n]!! = [2n-1]!!$ for $n \geq 1$ [4, Corollary 2.2], while

$$T_n^{(2)}(q) = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{[2k]!}{[2k]!!} \binom{n}{2k}_q = 1 + \sum_{k=1}^{\lfloor n/2 \rfloor} [2k-1]!! \binom{n}{2k}_q .$$

We might expect a convenient Eulerian generating function $f(x)$ for $\mathcal{I}_n(q)$. Based on Proposition 8, we make the guess that $f(x)$ has the form $f(x) = F(x)e_q^x$ for some power series $F(x) = \sum_{m=0}^{\infty} a_n x^n$. We may in fact solve for the a_n from equations obtained from $f(x) = F(x)e_q^x$, starting with $a_0 = \mathcal{I}_0(q) = 1$, by computing the values of $\mathcal{I}_n(q)$. Calculating the first few values of a_n, we find

$$F(x) = 1 + \frac{1}{[2]!}x^2 + \frac{1-q^2}{[3]!}x^3 + \frac{q^5 + q^3 + 2q^2 + 3q + 1}{[4]!}x^4 + \cdots$$

Unfortunately, this does not seem to shed any light on the meaning of $\mathcal{I}_n(q)$ in terms of $\mathbb{F}_q$-vector spaces. Likewise, we also do not know if $T_n^{(2)}(q)$ has an interpretation as a generating function for involutions in S_n with respect to some statistic. It would be satisfying to understand any connections amongst these points of view.

We conclude by remarking that it would be of interest to have a statistic on order p elements of S_n to generalize the work of Deodhar and Srinivasan [4], and to understand the general connection between $T_n^{(p)}(q)$ and statistics on order p elements in symmetric groups.

5 Acknowledgments

The first-named author was supported by NSF grant DMS-0751964, at the College of William and Mary REU. The second-named author was supported by a summer research grant from the College of William and Mary. Both authors thank Shahla Nasserasr for several helpful discussions, and the anonymous referee for suggestions to improve this paper.

References

[1] N. Chigira, The solutions of $x^d = 1$ in finite groups, *J. Algebra* **180** (1996), 653–661.

[2] S. Chowla, I. N. Herstein, and W. K. Moore, On recursions connected with symmetric groups. I, *Canad. J. Math.* **3** (1951), 328–334.

[3] S. Chowla, I. N. Herstein, and W. R. Scott, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh., Trondheim* **25** (1952), 29–31.

[4] R. S. Deodhar and M. K. Srinivasan, A statistic on involutions, *J. Algebraic Combin.* **13** (2001), 187–198.

[5] W. M. B. Dukes, Permutation statistics on involutions, *European J. Combin.* **28** (2007), 186–198.

[6] J. Goldman, G.-C. Rota, The number of subspaces of a vector space, in *Recent Progress in Combinatorics (Proc. Third Waterloo Conf. on Combinatorics, 1968)*, Academic Press, 1969, pp. 75–83.

[7] L. C. Grove, *Classical Groups and Geometric Algebra*, Graduate Studies in Mathematics, 39, American Mathematical Society, 2002.

[8] E. Jacobsthal, Sur le nombre d'éléments du groupe symétrique S_n dont l'ordre est un nombre premier, *Norske Vid. Selsk. Forh., Trondheim* **21** (1949), 49–51.

[9] K. Morrison, Integer sequences and matrices over finite fields, *J. Integer Seq.* **9** (2006), Article 06.2.1.

[10] L. Moser and M. Wyman, On the solutions of $x^d = 1$ in symmetric groups, *Canad. J. Math.* **7** (1955), 159–168.

[11] T. Müller, Enumerating representations in finite wreath products, *Adv. Math.* **153** (2000), 118–154.

[12] M. K. Srinivasan, The Eulerian generating function of q-derangements, *Discrete Math.* **306** (2006), 2134–2140.

[13] R. P. Stanley, *Enumerative Combinatorics, Vol. 1*, Cambridge Studies in Advanced Mathematics, 49, Cambridge University Press, 1997.

[14] C. R. Vinroot, Character degree sums and real representations of finite classical groups of odd characteristic, to appear in *J. Algebra Appl.*, http://arxiv.org/abs/0908.2398.

2000 *Mathematics Subject Classification*: Primary 05A10; Secondary 05A15.
Keywords: q-analogs, q-binomial coefficients, vector spaces over finite fields, recursions, symmetric group, Eulerian generating functions.

(Concerned with sequences A000085 and A052501.)

Received August 31 2009; revised versions received December 4 2009; March 9 2010. Published in *Journal of Integer Sequences*, March 12 2010.

Return to Journal of Integer Sequences home page.