An enumeration of flags in finite vector spaces

Ryan C. Vinroot
William & Mary, crvinroot@wm.edu

Follow this and additional works at: https://scholarworks.wm.edu/aspubs

Recommended Citation

This Article is brought to you for free and open access by the Arts and Sciences at W&M ScholarWorks. It has been accepted for inclusion in Arts & Sciences Articles by an authorized administrator of W&M ScholarWorks. For more information, please contact scholarworks@wm.edu.
An enumeration of flags in finite vector spaces

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

Submitted: Feb 2, 2012; Accepted: Jun 27, 2012; Published: Jul 12, 2012
Mathematics Subject Classifications: 05A19, 05A15, 05A30

Abstract
By counting flags in finite vector spaces, we obtain a \( q \)-multinomial analog of a recursion for \( q \)-binomial coefficients proved by Nijenhuis, Solow, and Wilf. We use the identity to give a combinatorial proof of a known recurrence for the generalized Galois numbers.

1 Introduction

For a parameter \( q \neq 1 \), and a positive integer \( n \), let \( (q)_n = (1 - q)(1 - q^2) \cdots (1 - q^n) \), and \( (q)_0 = 1 \). For non-negative integers \( n \) and \( k \), with \( n \geq k \), the \( q \)-binomial coefficient or Gaussian polynomial, denoted \( \binom{n}{k}_q \), is defined as \( \binom{n}{k}_q = \frac{(q)_n}{(q)_k(q)_{n-k}} \).

The Rogers-Szegö polynomial in a single variable, denoted \( H_n(t) \), is defined as

\[
H_n(t) = \sum_{k=0}^{n} \binom{n}{k}_q t^k.
\]

The Rogers-Szegö polynomials first appeared in papers of Rogers [16, 17] which led up to the famous Rogers-Ramanujan identities, and later were independently studied by Szegő [19]. They are important in combinatorial number theory ([1, Ex. 3.3–3.9] and [5, Sec. 20]), symmetric function theory [20], and are key examples of orthogonal polynomials [2]. They also have applications in mathematical physics [11, 13].

The Rogers-Szegö polynomials satisfy the recursion (see [1, p. 49])

\[
H_{n+1}(t) = (1 + t)H_n(t) + t(q^n - 1)H_{n-1}(t).
\]  

∗Supported by NSF grant DMS-0854849.
Letting $t = 1$, we have $H_n(1) = \sum_{k=0}^n \binom{n}{k} q^k$, which, when $q$ is the power of a prime, is the total number of subspaces of an $n$-dimensional vector space over a field with $q$ elements. The numbers $G_n = H_n(1)$ are the Galois numbers, and from (1.1), satisfy the recursion

$$G_{n+1} = 2G_n + (q^n - 1)G_{n-1}. \quad (1.2)$$

The Galois numbers were studied from the point of view of finite vector spaces by Goldman and Rota [6], and have been studied extensively elsewhere, for example, in [15, 9]. In particular, Nijenhuis, Solow, and Wilf [15] give a bijective proof of the recursion (1.2) using finite vector spaces, by proving, for integers $n \geq k \geq 1$,

$$\binom{n+1}{k}_q = \binom{n}{k}_q + \binom{n}{k-1}_q + (q^n - 1)\binom{n-1}{k-1}_q. \quad (1.3)$$

For non-negative integers $k_1, k_2, \ldots, k_m$ such that $k_1 + \cdots + k_m = n$, we define the $q$-multinomial coefficient of length $m$ as

$$\binom{n}{k_1, k_2, \ldots, k_m}_q = \frac{(q)_n}{(q)_{k_1}(q)_{k_2} \cdots (q)_{k_m}},$$

so that $\binom{n}{k}_q = \binom{n}{k, n-k}_q$. If $k$ denotes the $m$-tuple $(k_1, \ldots, k_m)$, write the corresponding $q$-multinomial coefficient as $\binom{n}{k_1, \ldots, k_m}_q = \binom{n}{k}_q$. For a subset $J \subseteq \{1, \ldots, m\}$, let $\varepsilon_J$ denote the $m$-tuple $(e_1, \ldots, e_m)$, where

$$e_i = \begin{cases} 1 & \text{if } i \in J, \\ 0 & \text{if } i \not\in J. \end{cases}$$

For example, if $m = 3$, $J = \{1, 3\}$, and $k = (k_1, k_2, k_3)$, then $\binom{n}{k_{-J}}_q = \binom{n}{k_1-1, k_2, k_3-1}_q$. The main result of this paper, which is obtained in Section 2, Theorem 2.1, is a combinatorial proof through enumerating flags in finite vector spaces of the following generalization of the identity (1.3). For $m \geq 2$, and any $k_1, \ldots, k_m > 0$ such that $k_1 + \cdots + k_m = n + 1$, we have

$$\binom{n+1}{k_1, \ldots, k_m}_q = \sum_{J \subseteq \{1, \ldots, m\}, |J| > 0} (-1)^{|J|-1} \binom{n}{k_{-J}}_q \frac{(q)_n}{(q)_{n-|J|+1}} \binom{n+1-|J|}{k_{-\varepsilon_J}}_q.$$ 

In Section 3, we prove a recursion which generalizes (1.2). In particular, the generalized Galois number $G_{n}^{(m)}$ is defined as

$$G_{n}^{(m)} = \sum_{k_1 + \cdots + k_m = n} \binom{n}{k_1, k_2, \ldots, k_m}_q,$$

which, in the case that $q$ is the power of a prime, enumerates the total number of flags of length $m - 1$ of an $n$-dimensional $F_q$-vector space. Quite recently, the asymptotic statistics of these generalized Galois numbers have been studied by Bliem and Kousidis [3] and Kousidis [12].
Directly following from Theorem 2.1, we prove in Theorem 3.1 that, for \( n \geq m - 1 \),

\[
G_{n+1}^{(m)} = \sum_{i=0}^{m-1} \binom{m}{i+1} (-1)^i \frac{(q)^n}{(q)^{n-i}} G_{n-i}^{(m)},
\]

which also follows from a known recurrence for the multivariate Rogers-Szegő polynomials.

## 2 Flags in finite vector spaces

In this section, let \( q \) be the power of a prime, and let \( \mathbb{F}_q \) denote a finite field with \( q \) elements. If \( V \) is an \( n \)-dimensional vector space over \( \mathbb{F}_q \), then the \( q \)-binomial coefficient \( \binom{n}{k}_q \) is the number of \( k \)-dimensional subspaces of \( V \) (see [10, Thm. 7.1] or [18, Prop. 1.3.18]). So, the Galois number

\[
G_n = H_n(1) = \sum_{k=0}^{n} \binom{n}{k}_q,
\]

is the total number of subspaces of an \( n \)-dimensional vector space over \( \mathbb{F}_q \).

Now consider the \( q \)-multinomial coefficient in terms of vector spaces over \( \mathbb{F}_q \). It follows from the definition of a \( q \)- multinomial coefficient and the fact that \( \binom{n}{k}_q = \binom{n-k}{n-k}_q \) that we have

\[
\binom{n}{k_1, k_2, \ldots, k_m}_q = \binom{n}{k_1}_q \binom{n-k_1}{k_2}_q \cdots \binom{n-k_1-\cdots-k_{m-2}}{k_{m-1}}_q
\]

\[
= \binom{n}{n-k_1}_q \binom{n-k_1-k_2}{n-k_1}_q \cdots \binom{n-k_1-\cdots-k_{m-2}}{n-k_1-\cdots-k_{m-2}-k_{m-1}}_q.
\]

So, if \( V \) is an \( n \)-dimensional vector space over \( \mathbb{F}_q \), the \( q \)-multinomial coefficient \( \binom{n}{k_1, \ldots, k_m}_q \) is equal to the number of ways to choose an \( (n-k_1) \)-dimensional subspace \( W_1 \) of \( V \), an \( (n-k_1-k_2) \)-dimensional subspace \( W_2 \) of \( W_1 \), and so on, until finally we choose an \( (n-k_1-\cdots-k_{m-2}) \)-dimensional subspace \( W_{m-1} \) of some \( (n-k_1-\cdots-k_{m-2}) \)-dimensional subspace \( W_{m-2} \) (see also [14, Sec. 1.5]). That is,

\[
W_{m-1} \subseteq W_{m-2} \subseteq \cdots \subseteq W_2 \subseteq W_1
\]

is a flag of subspaces of \( V \) of length \( m - 1 \), where \( \dim W_i = n - \sum_{j=1}^{i} k_j \).

We now turn to a bijective proof of the identity (1.3), that for integers \( n \geq k \geq 1 \),

\[
\binom{n+1}{k}_q = \binom{n}{k}_q + \binom{n}{k-1}_q + (q^n - 1) \binom{n-1}{k-1}_q.
\]

While the bijective interpretation of this identity which we give now is different from the proof given by Nijenhuis, Solow, and Wilf in [15], it is the interpretation which is most
helpful for the proof of our main result. Fix $V$ to be an $(n + 1)$-dimensional $\mathbb{F}_q$-vector space. There are $\binom{n + 1}{k}$ ways to choose a $k$-dimensional subspace $W$ of $V$. Fix a basis $\{v_1, v_2, \ldots, v_{n+1}\}$ of $V$. Any $k$-dimensional subspace $W$ can be written as $\text{span}(W', v)$ where $W'$ is a $(k - 1)$-dimensional subspace of $V' = \text{span}(v_1, \ldots, v_n)$, for some $v$. We may choose $W$ in three distinct ways. If $v \in V'$, then $W$ is a subspace of $V'$, for which there are $\binom{n}{k}$ choices. Call this a type 1 subspace of $V$. If $v_{n+1} \in W$, then we may take $v = v_{n+1}$, and $W$ is determined by $W'$, for which there are $\binom{n}{k-1}$ choices. We call this a type 2 subspace of $V$. Finally, if both $W \not\subseteq V'$ and $v_{n+1} \not\in W$, then we call $W$ a type 3 subspace of $V$, and it follows from (1.3) (and can be shown directly, as well) that there are $(q^n - 1)\binom{n-1}{k-1}$ choices for $W$.

We may now prove our main result.

**Theorem 2.1.** For $m \geq 2$, and any $k_1, \ldots, k_m > 0$ such that $k_1 + \cdots + k_m = n + 1$, we have

$$
\binom{n+1}{k_1, \ldots, k_m}_q = \sum_{J \subseteq \{1, \ldots, m\}, |J| > 0} (-1)^{|J|-1} \frac{(q)_n}{(q)_{n-|J|+1}} \frac{(n + 1 - |J|)}{k - e_J}_q
$$

**Proof.** Fix $V$ to be an $(n + 1)$-dimensional vector space over $\mathbb{F}_q$. Fix a basis of each subspace $U$ in $V$, so that we may speak of subspaces of type 1, 2, or 3 of each subspace $U$ with respect to this fixed basis. Consider a flag $F$ of subspaces of $V = W_0, W_{m-1} \subset \cdots \subset W_2 \subset W_1$, such that if we define $k_i$ for $1 \leq i \leq m$ by $\sum_{j=1}^{i} k_j = n + 1 - \dim W_i$, then each $k_i > 0$. The total number of such flags is $\binom{n+1}{k_1, \ldots, k_m}_q$. Consider now a labeling of such flags in the following way. Given a flag $F$ as above, define

$$r = \min\{1 \leq j \leq m \mid W_j \text{ is a type 1 subspace of } W_{j-1}\},$$

and

$$J = \{r\} \cup \{1 \leq j \leq r - 1 \mid W_j \text{ is a type 3 subspace of } W_{j-1}\}.$$

Define the flag $F$ to be a type $J$ flag of $V$. That is, for any nonempty $J \subseteq \{1, \ldots, m\}$, we may speak of flags of type $J$ of $V$. We shall prove that

$$(-1)^{|J|-1} \frac{(q)_n}{(q)_{n-|J|+1}} \frac{(n + 1 - |J|)}{k - e_J}_q
$$

is the number of type $J$ flags of length $m - 1$ of the $\mathbb{F}_q$-space $V$. Once this claim is proven, we will have accounted for all $2^m - 1$ terms on the right-side of the desired result of Theorem 2.1, and all possible ways to choose our flag.

We prove the claim by induction on $m$, where the base case of $m = 2$ follows from (1.3) and its interpretation in terms of subspaces of types 1, 2, and 3, as given above. We must consider each possible nonempty $J \subseteq \{1, \ldots, m\}$, and show that in each case, the quantity (2.1) counts the number of type $J$ flags. So, consider a flag of subspaces $W_{m-1} \subset \cdots \subset W_2 \subset W_1$ of $V$, where $\dim W_i = n + 1 - \sum_{j=1}^{i} k_j$.

First, if $J = \{1\}$, then the number of ways to choose $W_1$ to be a type 1 subspace of $V$ of dimension $n + 1 - k_1$ is $\binom{n}{n+1-k_1}_q$, while the number of ways to choose the remaining length

THE ELECTRONIC JOURNAL OF COMBINATORICS 19(3) (2012), #P5

4
$m-2$ flag $W_{m-1} \subset \cdots \subset W_2$ of $W_1$ is exactly $\binom{n+1-k_1}{k_2,\ldots,k_m}_q$. Thus, the total number of ways to choose our flag of type $J$ with $J = \{1\}$ is $(n+1-k_1)_q \binom{n}{k_2,\ldots,k_m}_q = \binom{n}{1-k_1,\ldots,k_m}_q$, which is exactly the expression (2.1) for $J = \{1\}$, as claimed. So, we now suppose $J \neq \{1\}$, so if $r$ is the maximum element of $J$, we have $r > 1$. We consider the cases of whether $1 \in J$ or $1 \notin J$ separately.

Suppose that $1 \notin J$. Then, we must choose our flag so that $W_1$ is a type 2 subspace of $V$, of which there are $(n\_l_q)^{-1}$ such subspaces. Now, if we define $I = J-I = \{j-1 \mid j \in J\}$, so that $I \subset \{1,\ldots,m-1\}$ and $|I| = |J|$, we must choose the rest of our type $J$ flag of $V$ by choosing a type $I$ flag of $W_1$ of length $m-2$. If we let $k' = (k_2,\ldots,k_m)$, then by our induction hypothesis, the number of type $I$ flags of length $m-2$ of the $(n+1-k_1)$-dimensional space $W_1$ is

$$(-1)^{|I|-1} \binom{n}{n-k_1} \binom{n+1-k_1-|I|}{k'-e_I},$$

So, the total number of ways to choose the type $J$ flag of length $m-1$ in $V$ is

$$\binom{n}{n-k_1} \binom{n+1-k_1-|I|}{k'-e_I}.$$ 

A direct computation yields

$$\binom{n}{n-k_1} \binom{n+1-k_1-|I|}{k'-e_I} = \binom{n}{n-k_1} \binom{n+1-|I|}{n-k_1-|I|+1},$$

and further note that

$$\binom{n+1-|I|}{n-k_1-|I|+1} \binom{n+1-k_1-|I|}{k'-e_I} = \binom{n+1-|J|}{k-e_J},$$

where $k = (k_1,\ldots,k_m)$. Together, these give

$$\binom{n}{n-k_1} (-1)^{|I|-1} \binom{n+1-k_1-|I|}{k'-e_I} = (-1)^{|I|-1} \binom{n}{n-k_1} \binom{n+1-|J|}{k-e_J},$$

giving the claim that when $1 \notin J$, the number of type $J$ subspaces of length $m-1$ of $V$ is given by (2.1).

Finally, suppose that $1 \in J$, and $J \neq \{1\}$. So, we must choose our flag so that $W_1$ is a type 3 subspace of $V$, and there are $(q^n-1)^{-1}(n-k_1)_q$ such subspaces. If we let $I = (J-1) \setminus \{0\}$ (so that now $|I| = |J|+1$), then we must choose the rest of our flag as a type $I$ flag of length $m-2$ of $W_1$. Letting again $k' = (k_2,\ldots,k_m)$, then by our induction hypothesis, the total number of flags of type $J$ of length $m-1$ of $V$ is given by

$$(q^n-1) \binom{n-1}{n-k_1} (-1)^{|I|-1} \binom{n+1-k_1-|I|}{k'-e_I}.$$
A computation gives
\[(q^n - 1) \frac{(n - 1)}{n - k_1} \frac{(q)_{n-k_1}}{(q)_{n-|I|+1}} = (-1) \frac{(q)_n}{(q)_{n-|I|}} \frac{(n - |I|)}{(n - k_1 - |I| + 1)} q,
\]
and also note
\[\left( \frac{n - |I|}{n - k_1 - |I| + 1} \right)_q \left( \frac{n + 1 - k_1 - |I|}{k' - \varepsilon_I} \right)_q = \left( \frac{n + 1 - |J|}{k - \varepsilon_J} \right)_q,
\]
where \(k = (k_1, \ldots, k_m)\), since \(|I| = |J| - 1\). We finally obtain that
\[(q^n - 1) \frac{(n - 1)}{n - k_1} \frac{(-1)^{|I|-1}}{(q)_{n-k_1-|I|+1}} \frac{(q)_{n-k_1}}{(q)_{n-|J|+1}} \frac{(n + 1 - k_1 - |I|)}{k' - \varepsilon_I} = (-1)^{|J|-1} \frac{(q)_n}{(q)_{n-|J|+1}} \frac{(n + 1 - |J|)}{k - \varepsilon_J} q,
\]
is the the number of type \(J\) subspaces of length \(m - 1\) of \(V\), as claimed. \(\square\)

3 Generalized Galois numbers

Define the homogeneous Rogers-Szegő polynomial in \(m\) variables for \(m \geq 2\), denoted \(\tilde{H}_n(t_1, t_2, \ldots, t_m)\), by
\[\tilde{H}_n(t_1, t_2, \ldots, t_m) = \sum_{k_1, \ldots, k_m = n} \left( k_1, \ldots, k_m \right)_q t_1^{k_1} \cdots t_m^{k_m},
\]
and define the Rogers-Szegő polynomial in \(m - 1\) variables, denoted \(H_n(t_1, \ldots, t_{m-1})\), by
\[H_n(t_1, \ldots, t_{m-1}) = \tilde{H}(t_1, \ldots, t_{m-1}, 1).
\]

The homogeneous multivariate Rogers-Szegő polynomials were first defined by Rogers [16] in terms of their generating function, and several of their properties are given by Fine [5, Section 21]. The definition of the multivariate Rogers-Szegő polynomial \(H_n\) is given by Andrews in [1, Chap. 3, Ex. 17], along with a generating function, although there is little other study of these polynomials elsewhere in the literature (however, there is a non-symmetric version of a bivariate Rogers-Szegő polynomial [4]).

The multivariate Rogers-Szegő polynomials satisfy a recursion which generalizes (1.1), although it seems not to be very well-known, as the only proof and reference to it that the author has found is in the physics literature, in papers of Hikami [7, 8]. For any finite set of variables \(X\), let \(e_i(X)\) denote the \(i\)th elementary symmetric polynomial in the variables \(X\). Then the Rogers-Szegő polynomials in \(m - 1\) variables satisfy the following recursion:
\[H_{n+1}(t_1, \ldots, t_{m-1}) = \sum_{i=0}^{m-1} e_{i+1}(t_1, \ldots, t_{m-1}, 1) (-1)^i \frac{(q)_n}{(q)_{n-i}} H_{n-i}(t_1, \ldots, t_{m-1}). \quad (3.1)
\]
The sum of all \(q\)-multinomial coefficients of length \(m\), or the generalized Galois number \(G_n^{(m)}\), is then
\[
H_n(1, 1, \ldots, 1) = G_n^{(m)} = \sum_{k_1 + \cdots + k_m = n} \binom{n}{k_1, \ldots, k_m}_q.
\]

From the discussion at the beginning of Section 2, when \(q\) is the power of a prime, \(G_n^{(m)}\) is exactly the total number of flags of subspaces of length \(m - 1\) in an \(n\)-dimensional \(\mathbb{F}_q\)-vector space.

Since the number of terms in the elementary symmetric polynomial \(e_{i+1}(t_1, \ldots, t_{m-1}, 1)\) is \(\binom{m}{i+1}\), then the following, our last result, follows directly from the formal identity (3.1) proved by Hikami. However, we give a proof which follows directly from Theorem 2.1, and is thus a bijective proof through the enumeration of flags in a finite vector space.

**Theorem 3.1.** The generalized Galois numbers satisfy the recursion, for \(n \geq m - 1\),
\[
G_n^{(m)} = \sum_{i=0}^{m-1} \binom{m}{i+1} (-1)^i \frac{(q)_n}{(q)_{n-i}} G_{n-i}^{(m)}.
\]

**Proof.** For convenience, whenever any \(k_i < 0\), we define the \(q\)-multinomial coefficient \((k_1, k_2, \ldots, k_m)_q = 0\). Granting this, we have Theorem 2.1 holds for all \(k_i \geq 0\). We now begin with the definition of \(G_{n+1}^{(m)}\) as the sum of all \(q\)-multinomial coefficients, and we directly apply Theorem 2.1 to rewrite the sum, as follows:
\[
G_{n+1}^{(m)} = \sum_{k_1 + k_2 + \cdots + k_m = n+1} \binom{n+1}{k_1, \ldots, k_m}_q
\]
\[
= \sum_{k_1 + \cdots + k_m = n+1} \sum_{J \subseteq \{1, \ldots, m\}} (-1)^{|J|-1} \frac{(q)_n}{(q)_{n-|J|+1}} \binom{n+1-|J|}{k-\varepsilon_J}_q
\]
\[
= \sum_{J \subseteq \{1, \ldots, m\}} \sum_{|J|>0} (-1)^{|J|-1} \frac{(q)_n}{(q)_{n-|J|+1}} \binom{n+1-|J|}{k-\varepsilon_J}_q
\]
\[
= \sum_{i=0}^{m-1} \sum_{J \subseteq \{1, \ldots, m\}} (-1)^i \frac{(q)_n}{(q)_{n-i}} \binom{n-i}{k-\varepsilon_J}_q
\]
\[
= \sum_{i=0}^{m-1} \binom{m}{i+1} \sum_{k_1 + \cdots + k_m = n-i} (-1)^i \frac{(q)_n}{(q)_{n-i}} \binom{n-i}{k}_q
\]
\[
= \sum_{i=0}^{m-1} \binom{m}{i+1} (-1)^i \frac{(q)_n}{(q)_{n-i}} G_{n-i}^{(m)},
\]
where the next-to-last equality follows from the fact that each index \(k_i'\) may be obtained from an index \(k\) from any of the \(\binom{m}{i+1}\) subsets \(J\) of size \(i+1\). \(\square\)
By a very similar argument, we may see that in fact the recursion for the multinomial Rogers-Szegö polynomials in (3.1) also follows from Theorem 2.1.

Acknowledgements

The author thanks George Andrews and Kent Morrison for very helpful comments, and the anonymous referee for very useful suggestions to improve this paper.

References


