Counting Subspaces of a Finite Vector Space – 2

Amritanshu Prasad

This is the second of a two-part article where we discuss the relation between the Gaussian binomial and multinomial coefficients and ordinary binomial and multinomial coefficients from a combinatorial viewpoint, based on expositions by Knuth, Stanley and Butler.

Amritanshu Prasad has been at the Institute of Mathematical Sciences, Chennai since 2003. His mathematical interests include representation theory, harmonic analysis, and combinatorics.

Previous part: *Resonance*, Vol.15,No.11, pp.977–987, 2010.

1. Recapitulation

In the first part of this article we defined the Gaussian binomial coefficient $\binom{n}{k}_q$ as the number of k-dimensional linear subspaces in the space of vectors with n coordinates in a finite field with q elements. Straightforward considerations led to its computation as

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}. \qquad (1)$$

This is in fact a rational function of the variable q, allowing us to substitute any complex number for q. The Gaussian binomial coefficient was found to be related to the ordinary binomial coefficient by the identity

$$\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}. \qquad (2)$$

Following Knuth [1], we used reduced row echelon forms, Ferrers diagrams, and paths in a rectangular grid to arrive at the identity

$$\binom{n}{k}_q = \sum_{\{\pi\in\Sigma_n : D(\pi)\subset\{k\}\}} q^{\mathrm{inv}(\pi)}. \qquad (3)$$

Here Σ_n denotes the group of permutations of n objects. For a permutation π, $D(\pi)$ denotes the descent set of π,

Keywords
Gaussian binomial coefficients, finite vector spaces.

which is defined as

$$D(\pi) = \{i \in \{1, \ldots, n-1\} : \pi(i) > \pi(i+1)\},$$

and $\mathrm{inv}(\pi)$ denotes the number of *inversions* of π, namely the number of pairs (i, j) such that $1 \leq i < j \leq n$ but $\pi(i) > \pi(j)$.

2. Multinomial Coefficients

Recall that multinomial coefficients given by the formula

$$\binom{n}{k_1 \quad \ldots \quad k_m} = \frac{n!}{k_1! \cdots k_m!} \tag{4}$$

count the number of ways of writing $\{1, \ldots, n\}$ as a disjoint union $X_1 \sqcup \cdots \sqcup X_m$, where $|X_i| = k_i$ for $i = 1, \ldots, m$ (of course, one assumes that $k_1 + \cdots + k_m = n$). Let

$$\begin{aligned} Y_1 &= X_1 \\ Y_2 &= X_1 \cup X_2 \\ &\vdots \\ Y_{m-1} &= X_1 \cup \cdots \cup X_{m-1} \\ Y_m &= X_1 \cup \cdots \cup X_m \quad = \{1, \ldots, n\}. \end{aligned}$$

Let $s_i = k_1 + \cdots + k_i$ for each $i \in \{1, \ldots, m-1\}$. Then $Y_1 \subset Y_2 \subset \cdots \subset Y_{m-1}$ is a nested sequence of subsets such that $|Y_i| = s_i$ for all $i \in \{1, \ldots, m-1\}$, and it is clear that the sequence of disjoint sets (X_i) can be recovered from the sequence of nested sets (Y_i). Writing S for an increasing sequence $(s_1, \ldots, s_{m-1})$ in $\{1, \ldots, n\}$, we shall use the notation

$$\begin{aligned} \binom{n}{S} \quad = \quad & \#\big\{S_1 \subset \cdots \subset S_m = \{1, \ldots, n\} : \\ & |S_i| = s_i \text{ for } 1 \leq i < m\big\}. \end{aligned}$$

We have:

$$\binom{n}{S} = \binom{n}{k_1 \quad \cdots \quad k_m},$$

This interpretation of the multinomial coefficients has an obvious analogue for vector spaces and subspaces.

where $k_i = s_i - s_{i-1}$ for $1 < i < m$, $k_1 = s_1$ and $k_m = n - s_{m-1}$. This interpretation of the multinomial coefficients has an obvious analogue for vector spaces and subspaces. Define the Gaussian multinomial coefficient as

$$\binom{n}{S}_q = \#\{V_1 \subset \cdots \subset V_{m-1} \subset F^n : V_i \text{ is a subspace of dimension } s_i\}.$$

The multinomial coefficients can be expressed in terms of the binomial coefficients. Clearly, the number of choices for S_{n-1} inside S_n is $\binom{n}{s_{n-1}}$, the number of choices for S_{n-2} inside each choice of S_{n-1} is $\binom{s_{n-1}}{s_{n-2}}$ and so on, so that

$$\binom{n}{S} = \binom{s_2}{s_1} \cdots \binom{s_{m-1}}{s_{m-2}} \binom{n}{s_{m-1}}. \tag{5}$$

Similarly,

$$\binom{n}{S}_q = \binom{s_2}{s_1}_q \cdots \binom{s_{m-1}}{s_{m-2}}_q \binom{n}{s_{m-1}}_q. \tag{6}$$

These expressions allow us to easily deduce some properties of Gaussian multinomial coefficients from the corresponding properties of Gaussian binomial coefficients. For example, equation (1) that expresses a Gaussian binomial coefficient as a rational function in q with denominator non-zero except at $q = 1$ also shows that a Gaussian multinomial coefficient is a rational function of q with denominator non-zero except at $q = 1$. From the identity (2) we can deduce that

Expressions (5) and (6) allow us to easily deduce some properties of Gaussian multinomial coefficients from the corresponding properties of Gaussian binomial coefficients.

$$\lim_{q \to 1} \binom{n}{S}_q = \binom{n}{S}. \tag{7}$$

Similarly, from the identity (3) we can deduce that each q-multinomial coefficient is a monic polynomial in q of degree $k_1 \cdots k_m$ with positive coefficients. A slightly more careful analysis will allow us to find the analogue of (3) for multinomial coefficients. Not only will it give

us a combinatorial interpretation for the coefficient of a power of q in the multinomial coefficient, when combined with the principle of inclusion and exclusion, it will also have the rather surprising consequence that the alternating sum

$$\sum_{S \subset T} (-1)^{|T-S|} \binom{n}{S}_q$$

is a polynomial in q with non-negative coefficients. (Here $|T-S|$ denotes the number of elements of T which are not in S.)

This alternating sum is a polynomial in q with non-negative coefficients.

In order to simplify notation, for any $S \subset \{1, \ldots, n\}$, let

$$\Sigma_n(S) = \{\pi \in \Sigma_n \ : \ D(\pi) \subset S\}.$$

Then (3) can be rewritten as

$$\binom{n}{S}_q = \sum_{\pi \in \Sigma_n(\{k\})} q^{\mathrm{inv}(\pi)}.$$

If we expand the right-hand side of (6) using the above identity, we get

$$\sum_{\pi_1 \in \Sigma_{s_2}(\{s_1\})} \cdots \sum_{\pi_{m-2} \in \Sigma_{s_{m-1}}(\{s_{m-2}\})} \sum_{\pi_{m-1} \in \Sigma_n(\{s_{m-1}\})} q^{\mathrm{inv}(\pi_1)+\cdots+\mathrm{inv}(\pi_m)} \ . \quad (8)$$

We claim that the formula

$$\Phi(\pi_{m-1}, \pi_{m-2}, \ldots, \pi_1) = \pi_{m-1} \circ \pi_{m-2} \circ \cdots \circ \pi_1$$

defines a bijection

$$\Phi : \Sigma_{s_2}(\{s_1\}) \times \Sigma_{s_3}(\{s_2\}) \times \cdots \times \Sigma_{s_{m-1}}(\{s_{m-1}\}) \tilde{\to} \Sigma_n(S) \ ,$$

(where Σ_r is identified with the subgroup of Σ_n which permutes the first r elements of $\{1, \ldots, n\}$) such that

$$\begin{aligned} \mathrm{inv}(\Phi(\pi_{m-1}, \pi_{m-2}, \ldots, \pi_1)) &= \mathrm{inv}(\pi_{m-1}) + \mathrm{inv}(\pi_{m-2}) \\ &+ \cdots + \mathrm{inv}(\pi_1) \ , \end{aligned}$$

allowing us to rewrite (8) as

$$\binom{n}{k}_q = \sum_{\pi \in \Sigma_n(S)} q^{\mathrm{inv}}(\pi).$$

Indeed, using induction on m, it suffices to verify:

Lemma. *The formula*

$$(\pi', \pi_{m-1}) \mapsto \pi' \circ \pi_{m-1}$$

defines a bijection

$$\Sigma_{s_{m-1}}(\{s_1, \ldots, s_{m-2}\}) \times \Sigma_n(\{s_{m-1}\}) \to \Sigma_n(S)$$

such that

$$\mathrm{inv}(\pi_{m-1} \circ \pi') = \mathrm{inv}(\pi_{m-1}) + \mathrm{inv}(\pi'), \qquad (9)$$

(*where* $\Sigma_{s_{m-1}}$ *is identified with the subgroup of* Σ_n *which permutes the first* s_{m-1} *elements of* $\{1, \ldots, n\}$).

Proof. Firstly, note that if $\pi' \in \Sigma_{s_{m-1}}(\{s_1, \ldots, s_{m-2}\})$ and $\pi_{m-1} \in \Sigma_n(\{s_{m-1}\})$ then both π' and π_{m-1} are increasing functions on each of the segments $\{s_{r-1} + 1, \ldots, s_r\}$ for $r = 1, \ldots, m$, and therefore, their composition is also increasing on these segments. Therefore $\pi' \circ \pi_{m-1} \in \Sigma_n(S)$.

It remains to prove (9). For each permutation π, let $I(\pi)$ denote the set of pairs $i < j$ for which $\pi(i) > \pi(j)$. In general, if σ and τ are permutations then

$$I(\sigma \circ \tau) \subset \tau^{-1}(I(\sigma)) \cup I(\tau)$$

from which it follows that

$$\mathrm{inv}(\sigma \circ \tau) \leq \mathrm{inv}(\sigma) + \mathrm{inv}(\tau)\ .$$

If in addition, $\tau^{-1}(I(\sigma)) \cap I(\tau) = \emptyset$, then

$$I(\sigma \circ \tau) = \tau^{-1}(I(\sigma)) \cup I(\tau)$$

and therefore,

$$\text{inv}(\sigma \circ \tau) = \text{inv}(\sigma) + \text{inv}(\tau) \ .$$

Hence in order to prove (9), one must show that

$$\pi'^{-1}(I(\pi_{m-1})) \cap I(\pi') = \emptyset. \tag{10}$$

Since π' acts only on $\{1, \ldots, s_{m-1}\}$, if (i, j) is an inversion of π' then $\pi'(j) < \pi'(i) \leq s_{m-1}$. Since π_{m-1} has no descents in this range, $(\pi'(i), \pi'(j))$ cannot be an inversion of π_{m-1}, proving (10). □

Combining identity (12) with the PIE (principle of inclusion exclusion), we get a surprising result for alternating sums of multinomial coefficients.

We have succeeded in generalizing (3) to multinomial coefficients:

$$\binom{n}{k}_q = \sum_{D(\pi) \subset S} q^{\text{inv}(\pi)}. \tag{11}$$

Combining (7) with (11)

$$\binom{n}{S} = \#\{\pi \in \Sigma_n | D(\pi) \subset S\} \ . \tag{12}$$

We shall now combine this identity with the principle of inclusion and exclusion to get a surprising positivity result for alternating sums of multinomial coefficients.

3. Principle of Inclusion and Exclusion

This principle is most commonly known as a technique for computing the cardinality of a union of finite sets in terms of cardinalities of various intersections. What follows is a more abstract formulation (see [2, Section 2.1]).

The PIE is a technique for computing the cardinality of a union of finite sets in terms of cardinalities of various intersections.

Let R be a finite set. The power set 2^R of R is the set of all subsets of R. The principle of inclusion and exclusion can be interpreted as saying that two functions $\alpha, \beta : 2^R \to \mathbf{C}$ satisfy the identities

$$\beta(T) = \sum_{S \subset T} \alpha(S). \tag{13}$$

for all $S, T \subset R$ if and only if they satisfy the identities

$$\alpha(T) = \sum_{S \subset T} (-1)^{|T-S|} \beta(S) \qquad (14)$$

for all $S, T \subset R$.

Proof. Assume (13). Then

$$\begin{aligned} \sum_{S \subset T} (-1)^{|T-S|} \beta(S) &= \sum_{S \subset T} (-1)^{|T-S|} \sum_{U \subset S} \alpha(U) \\ &= \sum_{U \subset T} \alpha(U) \sum_{U \subset S \subset T} (-1)^{|T-S|} . \end{aligned}$$

If $m = |T-U| > 0$, then the inner sum is $\sum_{i=0}^{m} (-1)^i \binom{m}{i} = 0$. Therefore, the expression reduces to $\alpha(T)$. Conversely, assume (14). Then

$$\begin{aligned} \sum_{S \subset T} \alpha(T) &= \sum_{S \subset T} \sum_{U \subset S} (-1)^{|S-U|} \beta(U) \\ &= \sum_{U \subset T} \beta(U) \sum_{U \subset S \subset T} (-1)^{|S-U|} , \end{aligned}$$

and as before, the inner sum is zero unless $U = T$, in which case it is one. □

4. Counting Permutations with a Given Descent Set

The principle of inclusion and exclusion allows us to use (12) to write a formula for the number of permutations with a given descent set in terms of multinomial coefficients. Take $R = \{1, \ldots, n\}$ and let

The PIE allows us to write a formula for the number of permutations with a given descent set in terms of multinomial coefficients.

$$\alpha(S) = \#\{\pi \in \Sigma_n | D(\pi) = S\}.$$

Then by (12)

$$\beta(T) = \sum_{S \subset T} \alpha(S) = \#\{\pi \in \Sigma_n | D(\pi) \subset T\} = \binom{n}{T}.$$

Thus, by the principle of inclusion and exclusion

$$\#\{\pi \in \Sigma_n | D(\pi) = T\} = \sum_{S \subset T} (-1)^{|T-S|} \binom{n}{S}.$$

The alternating sum in (15) is not just positive; it is a polynomial in q with non-negative coefficients.

5. A Surprising Positivity Result

Let

$$\alpha_q(S) = \sum_{D(\pi)=S} q^{\mathrm{inv}(\pi)}.$$

Then

$$\begin{aligned} \beta_q(T) &= \sum_{S \subset T} \alpha_q(S) \\ &= \sum_{S \subset T} \sum_{D(\pi)=S} q^{\mathrm{inv}(\pi)} \\ &= \sum_{D(\pi) \subset T} q^{\mathrm{inv}(\pi)} \\ &= \binom{n}{T}_q . \end{aligned}$$

The principle of inclusion and exclusion (Section 3) gives (see [2,Theorem 3.12.3])

$$\sum_{S \subset T} (-1)^{|T-S|} \binom{n}{S}_q = \sum_{D(\pi)=T} q^{\mathrm{inv}(\pi)}. \qquad (15)$$

Not only is this alternating sum positive; in fact it is a polynomial in q with non-negative coefficients! The identity (15) gives a formula for the number of permutations with descent set T and i inversions: it is the coefficient of q^i in the alternating sum of Gaussian multinomial coefficients on the left-hand side.

6. Closing Remarks

The combinatorics of Gaussian binomial coefficients continues to fascinate mathematicians today. That the binomial coefficients $\binom{n}{k}$ increase with k when $k \leq n/2$ and

Gaussian binomial coefficients continue to fascinate mathematicians today.

The first direct proof of the unimodal property for Gaussian binomial coefficients was found only in 1990.

decrease for $k \geq n/2$ is easy to see [3]. The first direct proof of the analogous statement for Gaussian binomial coefficients, that they increase in k up to some point, and then decrease, was found as late as 1990 by Kathleen M O'Hara [4] (see also an expository article on O'Hara's proof by Doron Zeilberger [5]).

Counting subspaces in a finite dimensional vector space over the field $\mathbf{Z}/p\mathbf{Z}$ is a special case of the problem of counting subgroups inside a finite abelian group. Every finite abelian group can be written as a product over a finite set of prime numbers of groups of the form

$$A_{p,\lambda} = \mathbf{Z}/p^{\lambda_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{\lambda_l}\mathbf{Z} \ , \qquad (16)$$

where $\lambda = (\lambda_1 \geq \cdots \geq \lambda_l)$ is a sequence of positive integers.

A generalization of the problem of counting k-dimensional subspaces in an n-dimensional space is the problem of counting subgroups of type $A_{p,\mu}$ inside $A_{p,\lambda}$ for $\mu = (\mu_1 \geq \cdots \geq \mu_m)$. The generalizations of (1) and (2) have been known for a long time (e.g., Delsarte [6]) and are related to multiset combinatorics (a multiset is a set where elements are allowed to appear with multiplicities, for example, as in the case of roots of a polynomial). However, the analogues of (11) and (15) are more subtle, and can be found in Lynne Butler's beautiful monograph [7].

In recent years, techniques from combinatorics have been combined with those from analytic number theory (namely, zeta functions) to study enumeration problems in algebra with great success (see, for example the survey article [8]). The reader who wishes to start learning the language and basic techniques of modern combinatorics need look no further than Richard P Stanley's amazing book [2] from which we have drawn extensively. A slightly different take on some of the contents of this article can be found in Henry Cohn's expository article [9].

Counting subspaces in a finite vector space is a special case of the problem of counting subgroups inside a finite abelian group.

Acknowledgements

I benefited from discussions with Kunal Dutta, Sanoli Gun, Anirban Mukhopadhyay and Shailesh Shirali while preparing these articles. It is a pleasure to thank them.

Suggested Reading

[1] D E Knuth, Subspaces, subsets, and partitions, *J. Combinatorial Theory Ser. A*, Vol.10, pp.178–180, 1971.

[2] R P Stanley, *Enumerative combinatorics*, Vol.1, volume 49 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[3] D Zeilberger, $\binom{5}{2}$ proofs that $\binom{n}{k} \leq \binom{n}{k+1}$ if $k < n/2$. Available online at http://arxiv.org/abs/1003.1273.

[4] K M O'Hara, Unimodality of Gaussian coefficients: A constructive proof, *J. Combinatorial Theory Ser. A*, Vol.53, No.1, pp.29–52, 1990.

[5] D Zeilberger, Kathy O'Hara's constructive proof of the unimodality of the Gaussian polynomials, *Amer. Math. Monthly*, Vol.96, No.7, pp.590–602, 1989.

[6] S Delsarte, Fonctions de Möbius sur les groupes abeliens finis, *Ann. of Math.*, Vol.49, No.2, pp.600–609, 1948.

[7] L M Butler, Subgroup lattices and symmetric functions, *Mem. Amer. Math. Soc.*, Vol.112, No.539, pp.vi+160, 1994.

[8] M du Sautoy and F Grunewald, Zeta functions of groups and rings, in *Proceedings of the International Congress of Mathematicians*, Madrid, Spain, pp.131–149, 2006.

[9] H Cohn, Projective geometry over $\mathbb{F}_1$ and the Gaussian binomial coefficients, *Amer. Math. Monthly*, Vol.111, No.6, pp.487–495, 2004.

In recent years, techniques from combinatorics have been combined with those from analytic number theory to study enumeration problems

Address for Correspondence
Amritanshu Prasad
The Institute of Mathematical Sciences
CIT Campus, Taramani
Chennai 600 113, India.
Email: amri@imsc.res.in