Counting Subspaces of a Finite Vector Space – 1

Amritanshu Prasad

This is the first of a two-part series 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.

1. Background

The Gaussian binomial coefficients were introduced two hundred years ago by Carl Friedrich Gauss [1] as a tool to find a formula for the following sums, now called *Gauss sums*:

$$G = \sum_{n=0}^{p-1} e^{2\pi i n^2/p} \quad \text{for all primes } p.$$

Gauss had easily computed these sums up to sign in 1801, but it took him four years of intense effort to resolve the sign ambiguity; he solved the problem only in 1805. This aspect of Gaussian binomial coefficients makes for a fascinating story in itself, but we shall simply refer the reader to [2], where an exposition of Gauss's proof (among other things) can be found.

This article concentrates on a different aspect of Gaussian binomial coefficients: they arise as the answer to a counting problem in linear algebra involving finite fields. Vectors with real coordinates arise naturally in our efforts to describe nature by mathematics. Space is described by three real coordinates, space-time by four. Physicists need to keep track of the position and momentum of a particle in space in order to be able to predict its position in the future, leading to the use of six real coordinates for each particle.

This article deals with a combinatorial aspect of the Gaussian coefficients.

Keywords
Gaussian binomial coefficients, finite vector spaces.

A powerful weapon in the armoury of a mathematician is the notion of modular arithmetic.

Number theorists like to work with vectors with integer or rational coordinates. Prospective solutions to Fermat's famous equation

$$x^n + y^n = z^n \tag{1}$$

are vectors with three integer or rational coordinates.

Finding out whether integer solutions exist to given Diophantine equations can be notoriously difficult, as evidenced by all the fuss over (1). The most powerful weapon in a mathematician's arsenal to tackle this problem is also due to Gauss: the notion of *modular arithmetic*, or the arithmetic of remainders. Four hours after 9 o'clock, it is 1 o'clock, because the remainder when $9+4=13$ is divided by 12 is 1. The clock does arithmetic modulo 12, but one can do it modulo any number $n \geq 2$. In arithmetic modulo n, two integers a and b are identified if their remainders after division by n are the same; or, as number theorists say it, their residues modulo n are the same. We write

$$a \equiv b \mod n \ .$$

Thus, there are n residue classes of integers modulo n, represented by

$$0, 1, 2, \ldots, n-1.$$

Addition and multiplication carry over to modular arithmetic and satisfy the same rules of commutativity, associativity and distributivity that hold for the integers.

When n is a prime number (call it p), something special happens: it is possible to divide by any non-zero residue modulo p, meaning to say that for any x not divisible by p, there exists an integer y such that

For a prime modulus p, each non-zero number possesses a reciprocal mod p.

$$xy \equiv 1 \mod p.$$

This integer y can be thought of as the reciprocal of x modulo p, and we may write it as $1/x$. A number

system, namely a set with the operations of addition and multiplication, which satisfies the usual axioms of commutativity, associativity and distributivity (it is assumed that the set comes with a '0' and a '1'), where division by any element different from 0 makes sense, is called a *field*. For every prime power q, Évariste Galois (1811–1832) constructed a finite field with q elements [3]. In 1903, E H Moore showed that for each prime power q, all fields with q elements are isomorphic [4]. In other words there is, in essence, just one field with q elements for each prime power q.

In essence, there is just one field with a given number q of elements, where q is a prime power.

Vectors with coordinates in any field behave very much like vectors with real numbers as coordinates. The usual notions of linear independence, basis, and subspace carry over from vectors with real coordinates to vectors with coordinates in finite fields, and will be used freely throughout this article. We recall the essentials: a set of vectors which is closed under addition and scalar multiplication (a scalar is an element of the underlying field) is called a *linear subspace*. A collection $v_1, \ldots, v_n$ of vectors is said to be *linearly independent* if, for each $1 \leq i < n$, there exists a linear subspace which contains $v_1, \ldots, v_{i-1}$ but not v_i. A *basis* of a linear subspace is any maximal linearly independent subset. Every vector in the subspace can be written as a sum of scalar multiples of elements from a basis. All bases of a linear subspace have the same number of elements, and this number is called the *dimension* of the linear subspace.

2. Introduction

Let F be a finite field of order q. Let $V = F^n$ be the space of vectors with n coordinates in F. For every $k \quad n$, define $\binom{n}{k}_q$ as the number of linear subspaces of V of dimension k. The number $\binom{n}{k}_q$ is called a *Gaussian binomial coefficient*. One of the goals of this article is to explore the relationship between $\binom{n}{k}_q$ and the binomial coefficient $\binom{n}{k}$, which is the number of ways of choosing

A Gussian binomial coefficient counts the number of linear subspaces of V of a particular dimension.

k objects out of n.

It is not difficult to write down a formula for $\binom{n}{k}_q$. Note that a k-dimensional subspace is specified by giving k linearly independent vectors $\{v_1, \ldots, v_k\}$ in V. In how many ways can this be done? Firstly, v_1 can be taken to be any non-zero vector in V. Therefore there are $q^n - 1$ choices for v_1. Given v_1, v_2 can be chosen to be any vector which is not in the subspace spanned by v_1. Since this subspace has q elements, there are $q^n - q$ choices for v_2. Continuing in this manner, we see that given $v_1, \ldots, v_l$ for $l < k$, there are $q^n - q^l$ choices for v_{l+1}. The number of sets of k linearly independent vectors in V is therefore

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}).$$

Applying the above formula to the special case where $n = k$, we see that each k-dimensional subspace of V has

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$$

bases. To obtain the number of k-dimensional subspaces, we divide the first expression by the second one. Thus the number of k-dimensional subspaces of V is

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}. \qquad (2)$$

So far, q has been the order of a finite field (which can be any prime power), but the above expression is also a rational function of q with a denominator that vanishes only at $q = 1$. This allows us to get a value for $\binom{n}{k}_q$ for any complex number $q \neq 1$. Using L'Hôpital's rule one computes

The ordinary binomial coefficients are a limiting case of the Gaussian binomial coefficients.

$$\lim_{q \to 1} \frac{q^n - q^i}{q^k - q^i} = \frac{n - i}{k - i}$$

for $i = 0, \ldots, n - 1$. Therefore

$$\lim_{q \to 1} \binom{n}{k}_q = \frac{n(n-1) \cdots (n-k+1)}{k(k-1) \cdots 1} = \binom{n}{k}. \qquad (3)$$

3. Counting using Echelon Form

Every subspace has a basis which is in 'reduced echelon form'. Identity (3) can be understood starting from this fact.

In 1971, D E Knuth [5] provided an elegant explanation for the identity (3) based on the idea that every subspace has a unique basis which is in *reduced row echelon form*.

Let F be a field with q elements. Any k linearly independent vectors in F^n can be arranged into a $k \times n$ matrix of rank k, where the entries of the ith row are the coordinat of the ith vector. In other words, every k-dimensional subspace of F^n is the row space of a $k \times n$ matrix of rank k. The row space of such a matrix does not change under the following elementary row operations:

- Permutation of the rows.
- Addition of a scalar multiple of one row to another.
- Multiplication of a row by a non-zero scalar.

A $k \times n$ matrix is said to be in reduced row echelon form if

- the left-most non-zero entry of each row is 1 (the *leading* 1),
- all the other entries in the column of a leading 1 are zero,
- the leading 1 in any row occurs to the right of the leading 1 in the row above it.

A matrix in reduced row echelon form looks something like

$$\begin{pmatrix} 0\cdots0 & 1 & *\cdots* & 0 & *\cdots* & 0 & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & 0 & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix},$$

From a matrix in reduced echelon form, one obtains a 'Ferrers diagram'.

where the $*$'s represent arbitrary elements of F.

The reader should not have much difficulty in seeing that the elementary row operations described above can be used to reduce any $k \times n$ matrix to reduced row echelon form. If the matrix has rank k, then all the rows in the reduced row echelon form are non-zero. Moreover, if two matrices in reduced row echelon form have the same row space, they are equal.

Given a matrix in reduced row echelon form, delete all the entries in each row to the left of the leading 1. Then remove the columns containing the leading 1's. Finally, replace each remaining entry with a $*$. The result is a pattern of $*$'s inside a grid with k rows and $n-k$ columns. These patterns are characterized by the property that except for the $*$'s in the first row, every $*$ has a $*$ above it, and except for the $*$'s in the $(n-k)$th column, every $*$ has a $*$ to the right of it. They are called 'Ferrers diagrams'. *Figure* 1 illustrates an example of this process when $n = 7$ and $k = 3$. On the left is a matrix in reduced row echelon form. The leading 1's occur in the second, fourth and fifth columns. After deleting the entries to the left of the leading 1's, deleting the columns with leading 1's, and replacing the remaining entries with $*$'s the Ferrers diagram on the right is obtained.

The above process can be easily reversed: let $e_1, \ldots, e_k$ denote the k coordinate vectors in F^n, written as columns. Starting with a Ferrers diagram λ in a $k \times (n-k)$ grid, replace each $*$ with an element of F (this can be done in $q^{|\lambda|}$ ways, where $|\lambda|$ denotes the number of $*$'s in λ) and each vacant square in the grid by a 0. Insert

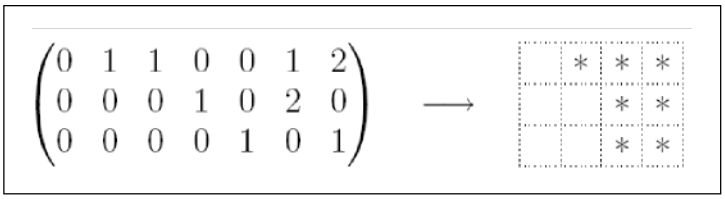

Figure 1. From a matrix to its Ferrers diagram.

$e_1, \ldots, e_k$ in reverse order as follows: insert e_k to the left of the left-most $*$ in the bottom row. Having inserted $e_{i+1}, \ldots, e_k$, insert e_i to the left of all the $*$'s in the ith row and all the columns $e_{i+1}, \ldots, e_n$. This gives all the matrices associated with λ.

The problem of counting the k-dimensional subspaces of F^n is equivalent to counting the number of $k \times n$ matrices of rank k in reduced row echelon form. Each matrix in reduced row echelon form gives rise to a Ferrers diagram inside a $k \times (n-k)$ grid. Each Ferrers diagram λ can be obtained from $q^{|\lambda|}$ matrices in reduced row echelon form. We have shown that

$$\binom{n}{k}_q = \sum_{\lambda \subset k \times n-k} q^{|\lambda|}\ , \qquad (4)$$

where $\lambda \subset k \times n-k$ is supposed to indicate that λ is a Ferrers diagram in a grid with k rows and $n-k$ columns.

The problem of counting subspaces of a particular dimension is seen to be equivalent to counting the number of matrices of a particular rank, written in reduced echelon form.

The expression (4) for q-binomial coefficients demonstrates that $\binom{n}{k}_q$ is a monic polynomial in q of degree $k(n-k)$ with positive integer coefficients, which is not evident from (2). In the next section, we take a closer look at the right-hand side of (4) to give, among other things, another proof of (3).

A *partition* of a natural number n is a decomposition

$$n = n_1 + \cdots + n_k,$$

where each part n_i is positive. If one does not distinguish between different reorderings of the same summands, one may assume that $n_1 \geq \ldots \geq n_k$. A Ferrers diagram λ with $|\lambda| = n$ can be thought of as a partition of n, the parts being the number of $*$'s in each row of λ. Thus, (4) has the following interpretation:

> *The coefficient of q^r in $\binom{n}{k}_q$ is the number of partitions of r into no more than $n-k$ parts, with each part being no larger than k.*

A Ferrers diagram with n stars may be associated with a partition of n.

Box 1. Ramanujan's Work on the Partition Function

The partition function $p(n)$ is the number of partitions of n. Srinivasa Ramanujan pioneered the study of partition functions using analytic methods. Together with G H Hardy, he obtained a truly remarkable analytic approximation for $p(n)$. This formula outputs a complex number, but for large values of n, the integer nearest to it is the exact value of the partition function. (G H Hardy and S Ramanujan, Asymptotic formulæ in combinatory analysis, *Proc. London Math. Soc.*, Ser.2, Vol.17, No.1, pp.75–115, 1918.)

Ramanujan also discovered congruence relations satisfied by the partition function. (S Ramanujan, Some properties of $p(n)$, the number of partitions of n, *Proc. Cambridge Phil. Soc.*, Vol.19, pp.207–210, 1919.)

4. Paths, Subsets, and Permutations

A Ferrers diagram may be associated with a path from the top left to the bottom right of a rectangular grid of squares.

Given a Ferrers diagram $\lambda \subset k \times n-k$, we identify it with a path from the top-left corner to the bottom-right corner of a rectangular grid of squares of length k and height $n-k$ as follows: Begin at the top left corner; at each stage, if you find yourself at the top left corner of a square with a $*$ in it, move one step downwards; lf not, move one step to the right. For the example with $n = 7$ and $k = 3$ that we considered in *Figure* 1, this process is illustrated in *Figure* 2. Such a path always consists of n segments of unit length, of which k are vertical and $n-k$ are horizontal. Index the segments of such a path by the numbers $1, \ldots, n$, starting at the top-left corner and ending at the bottom-right corner. The path is completely determined by specifying which k of these n segments are vertical. *Figure* 3 shows all ten paths for $n = 5$ and $k = 2$. Directly beneath each path is listed the subset of $\{1, 2, 3, 4, 5\}$ corresponding to the vertical segments.

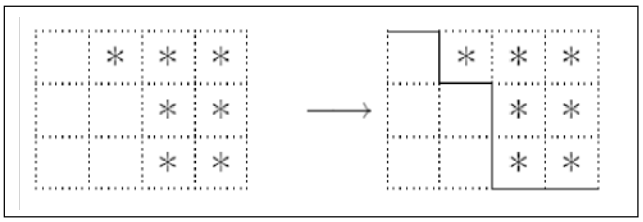

Figure 2. From a Ferrers diagram to its path.

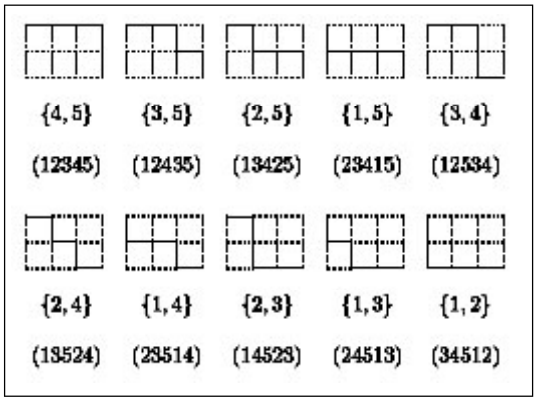

Figure 3. Paths, subsets and permutations.

Since the paths are completely specified by which k of the n segments are vertical, the number of such paths is $\binom{n}{k}$. This gives a more illuminating proof of the identity (3):

$$\lim_{q\to 1}\binom{n}{k}_q = \lim_{q\to 1}\sum_{\lambda\subset k\times n-k} q^{|\lambda|} = \sum_{\lambda\subset k\times n-k} 1 = \binom{n}{k}.$$

This proof trumps the one in Section 2 by virtue of being combinatorial; in effect, it constructs a surjective function K (call it a *collapse*) from the set of k-dimensional subspaces of F^n to the set of subsets of $\{1,\ldots,n\}$ of order k with all pre-images having cardinality a power of q. We shall now give a combinatorial interpretation of the number $|\lambda|$. In order to do this, we associate a permutation π_λ of $(1,\ldots,n)$ (namely a rearrangement of these symbols) to each Ferrers diagram λ contained in a $k\times n-k$ grid. The permutation π_λ is constructed as follows: look at the path corresponding to λ, with its segments indexed by the numbers $1,\ldots,n$ as before. First write down the indices corresponding to the horizontal segments in increasing order. Then write down the indices corresponding to the vertical segments in increasing order.

This proof of identity (3) is combinatorial rather than analytic.

In *Figure* 3, for $n=5$ and $k=3$ the permutation associated to each Ferrers diagram appears below the subset corresponding to the horizontal segments. Note that

only ten of the 120 permutations of $(1,2,3,4,5)$ appear in *Figure* 3. These ten permutations are characterized by the property that each entry with the possible exception of the third one is smaller than the next one.

More generally, let $(\pi(1),\ldots,\pi(n))$ denote a permutation of $(1,\ldots,n)$. The descent set of π is defined as

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

The permutations π_λ that correspond to paths in a $k \times n-k$ grid are precisely the ones for which $D(\pi) \subset \{k\}$.

We are now ready to give an interpretation of $|\lambda|$ in terms of π_λ. For a permutation π of $(1,\ldots,n)$, an inversion of π is a pair (i,j) such that $1 \leq i < j \leq n$ but $\pi(i) > \pi(j)$. Let $\mathrm{inv}(\pi)$ denote the number of inversions of π. We claim that

$$|\lambda| = \mathrm{inv}(\pi_\lambda). \tag{5}$$

Indeed, if (i,j) is an inversion of π_λ, then since $(\pi_\lambda(1), \ldots, \pi_\lambda(k))$ and $(\pi_\lambda(k+1),\ldots,\pi_\lambda(n))$ are increasing sequences, we must have $1 \leq i \leq k$ and $k < j \leq n$. The box in the ith column and $(j-k)$th row of a Ferrers diagram λ in a $k \times n-k$ grid contains a $*$ if and only if the associated path has taken $j-k$ downward steps before it has taken i rightward steps. But this is precisely when $\pi(i)$ (the index of the ith rightward step) is greater than $\pi(j)$ (the index of the $(j-k)$th downward step). The reader who finds the above reasoning hard to follow should try at first to verify (5) for the paths in *Figure* 3.

By passing from λ to π_λ, we can rewrite (4) in yet another form:

$$\binom{n}{k}_q = \sum_{\{\pi \in \Sigma_n : D(\pi) \subset \{k\}\}} q^{\mathrm{inv}(\pi)}. \tag{6}$$

Thus the coefficient of q^r in $\binom{n}{k}_q$ is the number of permutations with r inversions and descent set contained in $\{k\}$.

In the second part of this article, we shall study Gaussian multinomial coefficients and their relationship to ordinary multinomial coefficients. In particular, we will generalize (6) to Gaussian multinomial coefficients. It will follow that these are also polynomials in q with positive coefficients. We shall then use the principle of inclusion and exclusion to show that the coefficient of q^i in a certain alternating sum of Gaussian binomial coefficients counts the number of permutations with a fixed descent set and i inversions, and is therefore non-negative.

In Part II we shall study Gaussian multinomial coefficients and their relation to the ordinary multinomial coefficients.

Suggested Reading

[1] **C F Gauss, Summatio quarumdam serienum singularium, *Comment. Soc. R. Scient. Göttingensis Rec*, 1811, Reprinted in *Werke*, Vol. 2, Königliche Gesellschaft der Wissenschaften, Göttingen, pp.9–46, 1863. also available from the Göttinger Digitalisierungszentrum at http://gdz.sub.uni-goettingen.de.**

[2] **B C Berndt and R J Evans, The determination of Gauss sums, *Bull. Amer. Math. Soc.*, (N.S.), Vol.5, No.2, pp.107–129, 1981.**

[3] **E Galois, Sur la théorie des nombres, *Bull. Sci. Math.*, Vol.XIII: p.428, 1830. Reprinted in *Oeuvres mathématiques d'Évariste Galois*, Sociéte Mathematiques de France, 1897.**

[4] **E H Moore, *The subgroups of the generalized finite modular group*, Decennial Publications, Chicago, 1903.**

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

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