Gaussian Coefficients

Frank R. Kschischang
Department of Electrical and Computer Engineering
University of Toronto

December 10, 2008

1 The Basics

Let p be a prime, let $q = p^m$ for some integer $m \geq 1$, and let F_q be the finite field with q elements.

For any positive integer n, define $[[n]]$ as

$$[[n]] \stackrel{\text{def}}{=} q^n - 1,$$

a quantity that counts the number of nonzero vectors in a vector space of dimension n over F_q.

For $n \geq i$, we have

$$[[n]] - [[i]] = q^i [[n-i]] \text{ and } [[n]] - [[n-i]] = q^{n-i}[[i]].$$

Let

$$[[n]]! \stackrel{\text{def}}{=} \prod_{i=1}^{n} [[i]],$$

and define

$$[[0]]! \stackrel{\text{def}}{=} 1.$$

For any non-negative integer n and any integer i satisfying $0 \leq i \leq n$, define

$$\begin{bmatrix} n \\ i \end{bmatrix} \stackrel{\text{def}}{=} \frac{[[n]]!}{[[i]]![[n-i]]!}. \tag{1}$$

The quantity $\begin{bmatrix} n \\ i \end{bmatrix}$, a q-analogue of the binomial coefficient, is known as a *Gaussian coefficient* (or a *Gaussian binomial* or a *q-binomial coefficient*). To denote the dependence of $\begin{bmatrix} n \\ i \end{bmatrix}$ on q, the notation $\begin{bmatrix} n \\ i \end{bmatrix}_q$ is often used, but we will tend to drop the subscript when q is fixed.

Note that

$$\lim_{q \to 1} \frac{[[a]]}{[[b]]} = \frac{a}{b},$$

from which it follows that

$$\lim_{q \to 1} \begin{bmatrix} n \\ i \end{bmatrix} = \binom{n}{i};$$

thus in the slightly strange limit as $q \to 1$, the Gaussian coefficient reduces to the ordinary binomial coefficient.

As we will explore in this note, Gaussian coefficients turn out to be useful in counting subspaces of vector spaces over F_q as well as certain matrix families.

Let us start by writing $\begin{bmatrix} n \\ i \end{bmatrix}$ explicitly in several different ways as

$$\begin{aligned}
\begin{bmatrix} n \\ i \end{bmatrix} &= \frac{(q^n - 1)(q^{n-1} - 1)(q^{n-2} - 1) \cdots (q^{n-i+1} - 1)}{(q^i - 1)(q^{i-1} - 1)(q^{i-2} - 1) \cdots (q - 1)} \\
&= \frac{(1 - q^n)(1 - q^{n-1})(1 - q^{n-2}) \cdots (1 - q^{n-i+1})}{(1 - q)(1 - q^2)(1 - q^3) \cdots (1 - q^i)} \\
&= \frac{(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{i-1})}{(q^i - 1)(q^i - q)(q^i - q^2) \cdots (q^i - q^{i-1})},
\end{aligned}$$

where, in each case, an empty product (that occurs when $i = 0$) is taken as unity.

Note that $\begin{bmatrix} n \\ n \end{bmatrix} = \begin{bmatrix} n \\ 0 \end{bmatrix} = 1$. From (1) it is easy to see that

$$\begin{bmatrix} n \\ i \end{bmatrix} = \begin{bmatrix} n \\ n-i \end{bmatrix}.$$

We can obtain two "Pascal-type" identities by observing that, for $0 < i < n$,

$$[[n]][[n-i]] \begin{bmatrix} n-1 \\ i-1 \end{bmatrix} = [[n]][[i]] \begin{bmatrix} n-1 \\ i \end{bmatrix} = [[i]][[n-i]] \begin{bmatrix} n \\ i \end{bmatrix}. \tag{2}$$

From this it follows that, for any A,

$$\begin{bmatrix} n \\ i \end{bmatrix} = A \frac{[[n]]}{[[i]]} \begin{bmatrix} n-1 \\ i-1 \end{bmatrix} + (1 - A) \frac{[[n]]}{[[n-i]]} \begin{bmatrix} n-1 \\ i \end{bmatrix}.$$

For example, setting $A = [[i]]/[[n]]$ yields

$$\begin{bmatrix} n \\ i \end{bmatrix} = \begin{bmatrix} n-1 \\ i-1 \end{bmatrix} + q^i \begin{bmatrix} n-1 \\ i \end{bmatrix}, \tag{3}$$

while setting $1 - A = [[n-i]]/[[n]]$ yields

$$\begin{bmatrix} n \\ i \end{bmatrix} = q^{n-i} \begin{bmatrix} n-1 \\ i-1 \end{bmatrix} + \begin{bmatrix} n-1 \\ i \end{bmatrix}. \tag{4}$$

Of course, setting $A = 1$ and $A = 0$ yields

$$\begin{bmatrix} n \\ i \end{bmatrix} = \frac{[[n]]}{[[i]]} \begin{bmatrix} n-1 \\ i-1 \end{bmatrix} = \frac{[[n]]}{[[n-i]]} \begin{bmatrix} n-1 \\ i \end{bmatrix}.$$

Since $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$, from (3) or (4) and from the boundary cases $\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1$, it follows by induction that $\begin{bmatrix} n \\ i \end{bmatrix}$ is a polynomial of degree $i(n-i)$ in q. For example,

$$\begin{aligned} \begin{bmatrix} n \\ 1 \end{bmatrix} &= 1 + q + q^2 + \cdots + q^{n-1}, \\ \begin{bmatrix} 4 \\ 2 \end{bmatrix} &= 1 + q + 2q^2 + q^3 + q^4, \\ \begin{bmatrix} 5 \\ 2 \end{bmatrix} &= 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6, \end{aligned}$$

etc. Let $p_{n,i}(q)$ denote the polynomial corresponding to $\begin{bmatrix} n \\ i \end{bmatrix}$. It is easy to verify that each such polynomial is self-reciprocal, i.e., for $0 \le j \le i(n-i)$, the coefficient of q^j is the same as that of $q^{i(n-i)-j}$. Equivalently,

$$p_{n,i}(q) = q^{i(n-i)} p_{n,i}(1/q).$$

From this observation, we get yet another expression for $\begin{bmatrix} n \\ i \end{bmatrix}$, namely

$$\begin{bmatrix} n \\ i \end{bmatrix} = q^{i(n-i)} \frac{(1-q^{-(n-i+1)})(1-q^{-(n-i+2)})(1-q^{-(n-i+3)}) \cdots (1-q^{-n})}{(1-q^{-1})(1-q^{-2})(1-q^{-3}) \cdots (1-q^{-i})}. \tag{5}$$

2 Combinatorics

2.1 Ordered Bases and Full-Rank Matrices

Let V be an n-dimensional vector space over F_q. By an *ordered k-basis* we mean an ordered k-tuple $(b_1, \ldots, b_k)$ of linearly independent vectors $b_1, b_2, \ldots, b_k$ from V. How many distinct ordered k-bases can be constructed? Let us denote this number as $B(n,k)$.

In a generic k-basis $(b_1, \ldots, b_k)$, the vector b_1 can be chosen in $q^n - 1 = [[n]]$ ways, as b_1 can be any nonzero vector in V. Once b_1 is chosen, b_2 can be chosen in $q^n - q = q[[n-1]]$ ways, as b_2 can be any vector not in the one-dimensional subspace spanned by b_1. Once b_1 and b_2 are chosen, b_3 can be chosen in $q^n - q^2 = q^2[[n-2]]$ ways, as b_3 can be any vector not in the two-dimensional subspace spanned by b_1 and b_2. Continuing in this way, we find that V has

$$\begin{aligned} B(n,k) &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{k-1}) \\ &= q^{k(k-1)/2}\frac{[[n]]!}{[[n-k]]!} \end{aligned}$$

distinct ordered k-bases.

Let $F_q^{k\times n}$ denote the set of $k \times n$ matrices with entries from F_q, with $k \leq n$. Among these matrices, how many have rank k? Since there is a one-to-one correspondence between such matrices and ordered bases from V, we see that there are $B(n,k)$ rank-k matrices in $F_q^{k\times n}$. In particular,

$$B(n,n) = q^{n(n-1)/2}[[n]]!$$

gives the number of invertible $n \times n$ matrices over F_q, i.e., the cardinality of the general linear group $\mathrm{GL}(n, F_q)$.

If C is a k-dimensional linear code over F_q, then C has $B(k,k) = q^{k(k-1)/2}[[k]]!$ distinct ordered k-bases, and hence C has $B(k,k)$ distinct full-rank generator matrices.

We will return to matrices in Section 2.3. However, it is useful, next, to count subspaces.

2.2 Subspaces, Superspaces and Intersection

2.2.1 Subspaces

Let V be an n-dimensional vector space over F_q. How many distinct k-dimensional subspaces does V possess?

From our work above, we know that we can draw $B(n,k)$ distinct ordered k-bases from V. On the other hand, any particular k-dimensional subspace has $B(k,k)$ distinct ordered k-bases. Since no two distinct k-dimensional subspaces can share a basis, we find that the $B(n,k)$ ordered k-bases can be partitioned into distinct classes, each of size $B(k,k)$, where each class corresponds to a distinct subspace of V. The number of distinct subspaces is, therefore, given as

$$\frac{B(n,k)}{B(k,k)} = \frac{q^{k(k-1)/2}[[n]]!/[[n-k]]!}{q^{k(k-1)/2}[[k]]!} = \frac{[[n]]!}{[[k]]![[n-k]]!} = \begin{bmatrix} n \\ k \end{bmatrix}.$$

Thus the Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ counts the number of distinct k-dimensional subspaces of an n-dimensional vector space over F_q, i.e., the size of the Grassmannian $G(n, k)$.

2.2.2 Superspaces

Let V be a k dimensional subspace of an n-dimensional vector space W over F_q. By a superspace of V we mean a subspace of W that contains V. Among the j-dimensional subspaces of W, how many contain V? In other words, how many distinct j-dimensional superspaces does V have?

We observe that W can be written as the direct sum $W = V \oplus U$, where U is an $n-k$-dimensional subspace of W, intersecting trivially with V. Every j-dimensional subspace of W containing V is the direct sum $V \oplus U'$, where U' is a $j-k$-dimensional subspace of U. Each different U' gives a different superspace of V. Since U' can be chosen in

$$\begin{bmatrix} n-k \\ j-k \end{bmatrix}$$

ways, this is the number of distinct j-dimensional superspaces of V.

For example, if V is zero-dimensional, i.e., $k = 0$, then every j-dimensional subspace of W contains V, and we recover the Gaussian coefficient $\begin{bmatrix} n \\ j \end{bmatrix}$ as in the previous subsection.

2.2.3 Intersections

Let W be an n-dimensional vector space over F_q and let V be a fixed k-dimensional subspace of W. How many j-dimensional subspaces of W intersect V in exactly an ℓ-dimensional subspace? Let us denote this number by $N(n, k, j, \ell)$.

The subspace U of intersection can be chosen in $\begin{bmatrix} k \\ \ell \end{bmatrix}$ ways. This subspace can be extended to a j-dimensional subspace in

$$\frac{(q^n - q^k)(q^n - q^{k+1})(q^n - q^{k+2}) \cdots (q^n - q^{k+j-\ell-1})}{(q^j - q^\ell)(q^j - q^{\ell+1})(q^j - q^{\ell+2}) \cdots (q^j - q^{j-1})} = q^{(j-\ell)(k-\ell)} \begin{bmatrix} n-k \\ j-l \end{bmatrix}$$

ways. To see this, observe that we can extend U by adjoining any of the $q^n - q^k$ vectors not in V, then adjoining any of the $q^n - q^{k+1}$ vectors not in the resulting $(k+1)$-space, etc., but that any specific choice is in an equivalent class of size $(q^j - q^\ell)(q^j - q^{\ell+1}) \cdots (q^j - q^{j-1})$. The total number of j-dimensional subspaces of W that intersect V in exactly an ℓ-dimensional subspace is therefore given as

$$N(n, k, j, \ell) = q^{(k-\ell)(j-\ell)} \begin{bmatrix} k \\ \ell \end{bmatrix} \begin{bmatrix} n-k \\ j-\ell \end{bmatrix}.$$

Some special cases are worth examining, as $N(n,k,j,\ell)$ subsumes some of our earlier work.

For example, $N(n,k,j,j)$ is the number of j-dimensional subspaces of W that intersect V in a j-dimensional subspace of V. This is equivalent to determining the number of j-dimensional subspaces of V, and is given as

$$N(n,k,j,j) = q^{(k-j)(j-j)} \begin{bmatrix} k \\ j \end{bmatrix} \begin{bmatrix} n-k \\ 0 \end{bmatrix} = \begin{bmatrix} k \\ j \end{bmatrix}.$$

Similarly, $N(n,k,j,k)$ is the number of j-dimensional subspaces of W that intersect V in a k-dimensional subspace of V (i.e., V itself). This is equivalent to determining the number of j-dimensional superspaces of V and is given as

$$N(n,k,j,k) = q^{(k-k)(j-k)} \begin{bmatrix} k \\ k \end{bmatrix} \begin{bmatrix} n-k \\ j-k \end{bmatrix} = \begin{bmatrix} n-k \\ j-k \end{bmatrix}.$$

Similarly, $N(n,k,j,0)$ counts the number of j-dimensional subspaces of W that intersect trivially with V; there are

$$N(n,k,j,0) = q^{(k-0)(j-0)} \begin{bmatrix} k \\ 0 \end{bmatrix} \begin{bmatrix} n-k \\ j \end{bmatrix} = q^{jk} \begin{bmatrix} n-k \\ j \end{bmatrix}$$

such subspaces. Finally, $N(n,k,k,k-i)$ counts the number of k-dimensional spaces that intersect V in a $(k-i)$-dimensional space; this is the number of vertices at graph distance i from V in the Grassmann graph containing V, and is given by

$$N(n,k,k,k-i) = q^{i^2} \begin{bmatrix} k \\ \ell \end{bmatrix} \begin{bmatrix} n-k \\ k-\ell \end{bmatrix}.$$

2.3 Matrices Revisited

We return now to counting matrices.

How many $m \times n$ matrices over F_q have rank r? Denote this number by $A(m,n,r)$.

Only the zero matrix has rank zero, so $A(m,n,0) = 1$.

A rank-1 matrix can be obtained as product of a nonzero $m \times 1$ column vector with a nonzero $1 \times n$ row vector. The column vector can be chosen in $[[m]]$ ways, and the row vector in $[[n]]$ ways. Thus there are $[[m]][[n]]$ such products, but not all are distinct, since, e.g., scaling the first vector by a nonzero α and the second by α^{-1} yields the same rank-1 matrix. Thus, we have over-counted by a factor of $[[1]]$, hence

$$A(m,n,1) = [[m]][[n]]/[[1]].$$

More generally, we will evaluate $A(m,n,r)$ in three different ways.

First, let $\mathrm{rs}(M)$ denote the r-dimensional row space of a rank-r matrix $M \in F_q^{m\times n}$. We can define an equivalence relation on the set of rank-r matrices in $F_q^{m\times n}$ by writing $M_1 \sim M_2$ if and only if $\mathrm{rs}(M_1) = \mathrm{rs}(M_2)$. There are $\begin{bmatrix} n \\ r \end{bmatrix}$ equivalence classes. How many matrices are in each equivalence class? Let V be a fixed r-dimensional subspace of F_q^n, and let R be a fixed $r \times n$ matrix with $\mathrm{rs}(R) = V$. Let M be $m \times n$ matrix with $\mathrm{rs}(M) = V$. Since each row of M can be expressed uniquely as a linear combination of the rows of R, there is a unique $m \times r$ matrix A such that $M = AR$. Since $r = \mathrm{rank}(M) \le \min\{\mathrm{rank}(A), \mathrm{rank}(R)\} \le \mathrm{rank}(A) \le r$, the matrix A must necessarily have rank r. Conversely, if A is any $m \times r$ matrix of rank r, then AR is an $m \times n$ matrix with row space V. Thus, denoting the equivalence class containing M as $[M]$, we have

$$[M] = \{AR : A \in F_q^{m\times r}, \mathrm{rank}(A) = r\}.$$

Since, for $A_1, A_2 \in F_q^{m\times r}$ and $\mathrm{rank}(A_1) = \mathrm{rank}(A_2) = r$, we have $A_1 R = A_2 R$ implies $A_1 = A_2$, the elements of $[M]$ are in one-to-one correspondence with the set of $m \times r$ matrices of rank r, of which there are $B(m,r) = q^{r(r-1)}[[m]]!/[[m-r]]!$. Thus,

$$\begin{aligned} A(m,n,r) &= \begin{bmatrix} n \\ r \end{bmatrix} B(m,r) \\ &= q^{r(r-1)/2} \frac{[[n]]!}{[[r]]![[n-r]]!} \frac{[[m]]!}{[[m-r]]!} \\ &= q^{r(r-1)/2} \prod_{i=0}^{r-1} \frac{[[m-i]][[n-i]]}{[[i+1]]}. \end{aligned}$$

A second way to obtain $A(m,n,r)$ is to interchange the roles of rows and columns in the previous paragraph, defining an equivalence relation in terms of column space (instead of row space). We find, in that case, that

$$\begin{aligned} A(m,n,r) &= \begin{bmatrix} m \\ r \end{bmatrix} B(n,r) \\ &= q^{r(r-1)/2} \frac{[[m]]!}{[[r]]![[m-r]]!} \frac{[[n]]!}{[[n-r]]!} \\ &= q^{r(r-1)/2} \prod_{i=0}^{r-1} \frac{[[m-i]][[n-i]]}{[[i+1]]}. \end{aligned}$$

Yet a third way to obtain $A(m,n,r)$ is to define two rank-r $m \times n$ matrices to be equivalent if and only if the have the same row space *and* the same column space. In this case, there are $\begin{bmatrix} m \\ r \end{bmatrix}\begin{bmatrix} n \\ r \end{bmatrix}$ equivalence classes. A given equivalence class corresponding to column space U and row space V is obtained as

$$\{LGR : G \in F_q^{r\times r}, \mathrm{rank}(G) = r\},$$

where L is a fixed $m \times r$ basis matrix for U and R is a fixed $r \times n$ basis matrix for V. Thus there are $B(r,r) = q^{r(r-1)/2}[[r]]!$ elements in each equivalence class, yielding

$$\begin{aligned} A(m,n,r) &= \begin{bmatrix} m \\ r \end{bmatrix} \begin{bmatrix} n \\ r \end{bmatrix} B(r,r) \\ &= q^{r(r-1)/2}[[r]]! \frac{[[m!]]}{[[r]]![[m-r]]!} \frac{[[n!]]}{[[r]]![[n-r]]!} \\ &= q^{r(r-1)/2} \prod_{i=0}^{r-1} \frac{[[m-i]][[n-i]]}{[[i+1]]}. \end{aligned}$$

3 Asymptotics

Recall from (5) that

$$\begin{bmatrix} n \\ i \end{bmatrix} = q^{i(n-i)} \frac{(1-q^{-(n-i+1)})(1-q^{-(n-i+2)})(1-q^{-(n-i+3)})\cdots(1-q^{-n})}{(1-q^{-1})(1-q^{-2})(1-q^{-3})\cdots(1-q^{-i})},$$

hence, assuming that the complicated expression in the fraction is close to one, an "estimate" for $\begin{bmatrix} n \\ i \end{bmatrix}$ is

$$\begin{bmatrix} n \\ i \end{bmatrix} \approx q^{i(n-i)}. \tag{6}$$

Let

$$f_{n,i}(q) \stackrel{\text{def}}{=} q^{-i(n-i)} \begin{bmatrix} n \\ i \end{bmatrix}$$

be the factor that corrects the estimate (6). Note that $f_{n,i}(q) = f_{n,n-i}(q)$ and that $f_{n,0}(q) = f_{n,n}(q) = 1$ (i.e., the estimate is correct in the trivial extreme cases).

Next observe that

$$\frac{f_{n,i+1}(q)}{f_{n,i}(q)} = \frac{1-q^{-(n-i)}}{1-q^{-(i+1)}}.$$

From this we see that $n-1 \geq 2i$ implies $f_{n,i+1} \geq f_{n,i}$. When this condition is no longer satisfied, i.e., when $n-1 < 2i$, then $f_{n,i} > f_{n,i+1}$. Thus, for fixed n and q, $f_{n,i}(q)$ is monotonically non-decreasing with $i \leq \lceil n/2 \rceil$, reaching its peak at $i = \lceil n/2 \rceil$ or $i = \lfloor n/2 \rfloor$. Thus, for any i,

$$1 \leq f_{n,i}(q) \leq f_{n,\lfloor n/2 \rfloor}(q).$$

Since $f_{n,i}(q) \geq 1$, we see that $q^{i(n-i)}$ never overestimates $\begin{bmatrix} n \\ i \end{bmatrix}$.

Define

$$g_n(q) = f_{n,\lfloor n/2 \rfloor}(q).$$

Observe that

$$\frac{g_{n+1}(q)}{g_n(q)} > 1,$$

thus, for fixed q, $g_n(q)$ increases montonically with n. Let $h(q) = \lim_{n\to\infty} g_n(q)$. We have

$$h(q) = \prod_{i=1}^{\infty} \frac{1}{1 - q^{-i}}, \tag{7}$$

and $f_{n,i}(q) \le h(q)$ for all n and i. In summary, we may conclude that

$$q^{i(n-i)} \le \begin{bmatrix} n \\ i \end{bmatrix} \le h(q) q^{i(n-i)},$$

where $h(q)$ is given in (7).

The series for $h(q)$ converges rapidly; the following table lists $h(q)$ for various values of q.

q	$h(q)$
2	3.4627
3	1.7853
4	1.4523
5	1.3152
7	1.1950
8	1.1636
9	1.1408
11	1.1101
16	1.0711
32	1.0333
64	1.0161
128	1.0079
256	1.0039

Note that $h(q)$ decreases monotonically with q, approaching $q/(q-1)$ for large q.

To see that $h(q)$ decreases monotonically, recall that the function

$$p(x) = \prod_{i=1}^{\infty} \frac{1}{1 - x^{i}}$$

is a generating function for partitions of the integers. When written as a formal power series,

$$p(x) = \sum_{i\ge 0} p_i x^i,$$

the coefficient p_i of x_i, for $i > 0$, expresses the number of ways that the integer i can be written as a sum of positive integers. Note that

$$p(x) = (1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots.$$

From this we see that $p(x)$ is an infinite product of monotically increasing functions of x; hence $p(x)$ is monotonically increasing with x.

Still to Do

Add references.

Connect to the q-Pochhammer symbol?

Derive the Newton binomial formulas (see Wikipedia).

Find/solve other useful combinatorial problems involving Gaussian coefficients. Perhaps the book by Van Lint would be useful? One example of such a problem: let U and V be two spaces in a Grassmannian separated by (graph) distance d. Let V^+ denote the 1-neighbourhood of V (including V itself). Elements of V^+ are either at distance $d-1$, d or $d+1$ from U. How many of each?