C50 Enumerative & Asymptotic Combinatorics

Solutions to Exercises 4 — Spring 2003

1 Induction on k. For $k = 0$, we have $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$ and

$$\begin{bmatrix} n \\ 1 \end{bmatrix}_{-1} = 1 + (-1) + (-1)^2 + \cdots + (-1)^{n-1} = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \text{ is odd.} \end{cases}$$

Suppose the result is true for $k-1$. Then

$$\begin{aligned} \begin{bmatrix} 2n \\ 2k \end{bmatrix}_{-1} &= \begin{bmatrix} 2n-1 \\ 2k-1 \end{bmatrix}_{-1} + (-1)^{2k} \begin{bmatrix} 2n-1 \\ 2k \end{bmatrix}_{-1} \\ &= \binom{n-1}{k-1} + \binom{n-1}{k} \\ &= \binom{n}{k}. \end{aligned}$$

The other three cases are similar.

2 (a) Using the two recurrence relations,

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_q &= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \\ &= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^n \begin{bmatrix} n-2 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-2 \\ k \end{bmatrix}_q \\ &= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + (q^n - 1) \begin{bmatrix} n-2 \\ k-1 \end{bmatrix}_q . \end{aligned}$$

(b) Sum the result over k. (The values for $n = 0$ and $n = 1$ are computed straightforwardly.)

(c) Since clearly $F_q(n)$ is an increasing function of n (when q is a prime power), we have $F_q(n) \geq (q^{n-1} + 1) F_q(n-2)$. So, assuming that $F_q(n-2) \geq c\,q^{(n-2)^2/4}$, we have

$$F_q(n) \geq c\,q^{(n-2)^2/4 + (n-1)} = c q^{n^2/4}.$$

So we are done by induction as long as we choose c large enough that the result holds for $n = 1$ and $n = 1$ (for which $c = \min\{1, 2q^{-1/4}\}$ suffices).

3 The proof is by induction on k. For $k = 1$, only the empty matrix is in reduced echelon form.

For $k > 0$, there are two cases for a matrix A in reduced echelon form:

- The leading one in the last row occurs in the last column. In this case, removing the last row and column gives a $(k-1) \times (n-1)$ matrix in reduced echelon form; and the process uniquely reverses, by adding a row and column with all entries zero except for one in the lower right corner.
- The leading one in the last row occurs earlier than the last column. Then the matrix is obtained from a $k \times (n-1)$ matrix in reduced echelon form by adding an arbitrary column.

By the induction hypotheses, the number of $k \times n$ matrices is

$$\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

4 Consider matrices in echelon form with k non-zero rows. Such a matrix is obtained from a $k \times n$ matrix in reduced echelon form with no zero rows by replacing the zeros in the $0+1+\cdots+(k-1) = k(k-1)/2$ positions in columns above the leading ones by anything at all, and then adding $n-k$ rows of zeros. So the total number of matrices in echelon form is

$$\sum_{k=0} nq^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=1}^{n} (1+q^{i-1}),$$

by the q-Binomial Theorem.

For matrices in reduced echelon, the number is

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q = F_q(n),$$

where $F_q(n)$ is the function considered in Question 2.

5 (a) $h_k(1,\ldots,1)$ is just the number of monomials of degree k in $x_1,\ldots,x_n)$, which is the number of ways of choosing k of the variables (with repetition allowed); we have seen that this is $\binom{n+k-1}{k}$.

(b) This depends on the identity

$$\prod_{i=1}^{n} (1-x_i t)^{-1} = \sum_{k\geq 0} h_k(x_1,\ldots,x_n) t^k.$$

This can be proved in two ways. Either multiply out the geometric series on the left, and observe that every monomial of degree n occurs exactly once mutiplied by t^n; or show that

$$h_k(x_1,\ldots,x_n) = \sum_{i=0}^{n} h_i(x_1,\ldots,x_{n-1}) x_n^{k-i}$$

and use induction.

Putting $x_i = q^{i-1}$, we have

$$\prod_{i=1}^{n}(1-q^{i-1}t)^{-1} = \sum_{k\geq 0} h_k(1,\ldots,q^{n-1})t^k.$$

So we have to prove the *negative q-binomial theorem*:

$$\prod_{i=1}^{n}(1-q^{i-1}t)^{-1} = \sum_{k\geq 0} \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q t^k.$$

This can be shown by induction. The case $n=0$ is trivial. For the inductive step, we need to prove that

$$\left(\sum_{k\geq 0} \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q t^k\right)(1-q^{n-1}t) = \sum_{k\geq 0} \begin{bmatrix} n+k-2 \\ k \end{bmatrix}_q t^k,$$

or in other words

$$\begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q - q^{n-1}\begin{bmatrix} n+k-2 \\ k-1 \end{bmatrix}_q = \begin{bmatrix} n+k-2 \\ k \end{bmatrix}_q,$$

which is immediate from the recurence relation for the Gaussian coefficients.

Note that by letting $q \to 1$ we get another proof of (a).

6 The formula

$$\sum_{m|n} f_m(q) = q^n$$

shows that the number of roots of all irreducible polynomials of degree dividing n over $\mathrm{GF}(q)$ is equal to q^n. Now every element of the field of order q^n satisfies such a polynomial, so the field must consist of all the roots of all such polynomials. Thus any field of order q^n is the splitting field of the product of all these polynomials over $\mathrm{GF}(q)$.

Take q to be a prime. The field with q elements is now obviously unique, and by the uniqueness of the splitting field of a polynomial, the field with q^n elements is therefore also unique (up to isomorphism).