Solutions to Exercises
Chapter 9: Finite geometry

---

1 How many additions and multiplications are needed (in the worst case) to transform an $m \times n$ matrix into reduced echelon form?

Assume that $m \le n$. (Consider the case $m > n$ as an exercise.) Starting with a matrix with a non-zero element in the first column (the worst case), we can assume that this element is in the first row. Then we require $n - 1$ divisions to make the first row begin with 1, and $(m-1)(n-1)$ multiplications and the same number of subtractions to make the remaining elements in the column equal to zero. Then we have to work on a $(m-1) \times (n-1)$ matrix. So, for the maximum number $f(m,n)$ of arithmetic operations to reduce the matrix to echelon form, we have

$$f(m,n) = (2m-1)(n-1) + f(m-1,n-1),$$

a recurrence with solution

$$f(m,n) = m^2(n-m) + m(m-1)(4m+1)/6.$$

To obtain reduced echelon, we have a further

$$1(n-1) + 2(n-2) + \cdots + (m-1)(n-m+1) = m(m-1)(3n-2m+1)/6$$

multiplications and the same number of subtractions. The total is

$$nm(3m-1)/2 + m(2m-1)(2m+1)/6.$$

Note that this number is $O(m^2 n)$; in particular, it is polynomial in the number of matrix entries.

---

2 For fixed q, show that the probability that a random $n \times n$ matrix over $\mathrm{GF}(q)$ is non-singular tends to a limit $c(q)$ as $n \to \infty$, where $0 < c(q) < 1$.

We use the following theorem of analysis. Let $a_1, a_2, \ldots$ be real numbers satisfying $0 < a_i < 1$ for all i, and assume that the series $\sum a_i^2$ converges. Then the product $\prod_{i=1}^{n}(1 - a_i)$ converges to a limit strictly between 0 and 1 if and only if $\sum a_i$ converges.

The number of $n \times n$ matrices is q^{n^2}, whereas the number of non-singular matrices is given by (9.2.6). The quotient (the probability that a random matrix is non-singular) is

$$\prod_{i=1}^{n}(1 - q^{-i}).$$

Since $\sum q^{-i}$ and *a fortiori* $\sum q^{-2i}$ both converge, the limit is strictly between 0 and 1. (For $q = 2$, it is approximately $0.2887\ldots$.)

---

3 Let $F_q(n)$ be the total number of subspaces of an n-dimensional vector space over $\mathrm{GF}(q)$. Prove that $F_q(0) = 1$, $F_q(1) = 2$, and

$$F_q(n+1) = 2F_q(n) + (q^n - 1)F_q(n-1)$$

for $n \geq 1$.

By (9.2.3) and the remark after (9.2.4) we have

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

as required. Sum over k from 1 to $n+1$: the Gaussian coefficient is zero if the bottom argument is negative or greater than the top argument. We obtain $F_q(n+1)$ on the left, $F_q(n) + F_q(n) + (q^n - 1)F_q(n-1)$ on the right.

Since $F_q(n) > F_q(n-1)$, we have $F_q(n+1) > q^n F_q(n-1)$. Hence

$$F_q(n) > q^{n-1} \cdot q^{n-3} \cdots = q^{\lfloor n^2/4 \rfloor}.$$

(Treat the cases n even and n odd separately.)

---

4 Prove
$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q + q^{n+1-k}\begin{bmatrix} n \\ k-1 \end{bmatrix}_q.$$
in two ways: by using (9.2.3) and (9.2.4), or by dividing the $k \times (n+1)$ matrices into two classes according to their first column.

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

2

Alternatively, the left-hand side counts $k \times (n+1)$ matrices in reduced echelon form, with no zero rows. There are $\begin{bmatrix} n \\ k \end{bmatrix}_q$ such matrices with the first column consisting entirely of zeros. In any other matrix, the first entry is 1 and the remaining elements in the first column are zero: the first row contains $k - 1$ zeros (above the leading ones in the other rows) and $n + 1 - k$ arbitrary elements (in the other positions); and the matrix with first row and column deleted is again in reduced echelon. So there are $q^{n+1-k} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q$ matrices of this form. The result follows.

---

5 Prove that the right-hand side of the q-binomial theorem (9.2.5) for $t = 1$ counts the number of $n \times n$ matrices in echelon form over $\mathrm{GF}(q)$, that is, satisfying the first two conditions in the definition of reduced echelon form. How many $n \times n$ matrices in reduced echelon form are there?

Take a matrix of rank k in reduced echelon form. There are $q^{0+1+\cdots+(k-1)} = q^{k(k-1)/2}$ matrices in echelon form which can be obtained by replacing the zeros above the leading ones by arbitrary field elements. Hence there are $q^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q$ matrices of rank k in echelon form. Summing over k gives the result.

Since every k-dimensional subspace of $\mathrm{GF}(q)^n$ has a unique basis in reduced echelon form, the number of such matrices is given by

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

where $F_q(n)$ is as in Question 3.

---

6 Prove that a set of points of a projective space is a flat if and only if it contains the line through any two of its points.

Let P be a set of 1-dimensional subspaces, U the set of all vectors lying in some of these spaces.

First, let U be a subspace. Then, if $p_1, p_2 \in P$, then the line L spanned by p_1 and P_2 is the 2-dimensional subspace they generate. Since $p_1, p_2 \subseteq U$, we have $L \subseteq U$, so every point on L is in P.

Conversely, suppose that P contains the line through any two of its points. As noted in the question, U is closed under scalar multiplication. (If $v \in U$, with $v \neq 0$, then $cv \in \langle v \rangle \in P$, so $cv \in U$. The assertion is trivial if $v = 0$.) So suppose that $v_1, v_2 \in U$. If v_1, v_2 are linearly dependent, the they lie in a 1-dimensional subspace in P, which also contains their sum; so $v_1 + v_2 \in U$. On the other hand, suppose that v_1 and v_2 are linearly independent, so that they span distinct points p_1, p_2 in P. Let L be the line joining $_1$ and p_2, so that $L = \langle v_1, v_2 \rangle$. By assumption,

$L \subseteq U$. Then $v_1 + v_2 \in L$, so $v_1 + v_2 \in U$, as required. Since U is closed under addition and scalar multiplication, it is a subspace.

---

7 Show that any set of $m-2$ MOLS of order m can be enlarged to a set of $m-1$ MOLS.

A set of $m-2$ MOLS of order m gives rise to a net of order m and degree m. This is a geometry with m^2 points and m^2 lines falling into m parallel classes of m lines each. Any point lies on m lines, and so is collinear with $m(m-1)$ other points, and non-collinear with $m-1$ points. If the point p is not on the line L, then one line through p is parallel to L, and so $m-1$ lines through p meet L, and just one point of L is not collinear with p.

We show that the relation of being equal or non-collinear is an equivalence relation on the points. It is clearly reflexive and symmetric. Suppose that p is non-collinear with q, and q is non-collinear with r, where $p \neq r$. If p and r lie on a line L, then q is non-collinear with two points of L, contrary to the preceding paragraph. So p and r are non-collinear.

So the points fall into m equivalence classes with m points in each. If we take the equivalence classes to be 'new lines', we have enlarged the net to an affine plane. Correspondingly, we have produced a new Latin square orthogonal to the previous ones.

---

8 Show that there are two non-isomorphic nets of order 4 and degree 3. (The corresponding Latin squares are the multiplication tables of the two groups of order 4.) Show that one, but not the other, can be enlarged to an affine plane.

In Exercise 1 of Chapter 6, we saw that there are just two Latin squares of order 4, up to row and column permutations. Thus there are at most two nets of order 4 and degree 3 up to isomorphism. But one square has an orthogonal mate (and so its net can be extended to one of degree 4), whereas the other does not. So the nets are not isomorphic. From a net of degree 4, we reach an affine plane (a net of degree 5) as in the preceding question.

---

9 (a) Prove that there is a unique projective plane of order 3.
(b) Prove that there is a unique projective plane of order 4.

(a) The proof of (9.5.7) shows that the uniqueness of the projective plane of order 3 follows from the uniqueness of the affine plane of order 3 (the STS(9)); this is shown in Exercise 3 of Chapter 8.

(b) Again it suffices to show the uniqueness of the affine plane. For this, the uniqueness of the family of three MOLS of order 4 (up to row, column and entry

permutations) will show the result. In question 1(b) of Chapter 6, we showed that there is a unique Latin square of order 4 with an orthogonal mate; the proof shows that there are just two orthogonal mates, forming the required unique set of three MOLS with the original square.

Remark. A completely different proof is given in Chapter 6 of *Graphs, Codes, Designs and their Links*, by P. J. Cameron and J. H. van Lint, Cambridge University Press, 1991.

---

10 Let O be an oval in a projective plane of even order q. Prove that the tangents to O all pass through a common point p, and that $O \cup \{p\}$ is a set of $q+2$ points which meets every line in either 0 or 2 points. (Such a set is called a *hyperoval*. Note that, if any one of its points is omitted, the resulting set is an oval.)

The three equations at the foot of page 139 hold. From these, we deduce that

$$\sum (i-1)(i-q-1)x_i = 2q(q+1) - (q+2)q(q+1) + (q+1)q^2 = 0.$$

Now a point on no tangents would lie on $(q+1)/2$ secants, which is impossible, since $q+1$ is odd. So $x_0 =)$. Since no point can lie on more than $q+1$ tangents, every term in the sum on the left has $(i-1)(i-(q+1)) \le 0$, with strict inequality unless $i=1$ or $i=q+1$. So $x_i = 0$ unless $i=1$ or $q+1$. Now we have

$$
\begin{aligned}
x_1 + x_{q+1} &= q^2, \\
x_1 + (q+1)x_{q+1} &= q^2 + q,
\end{aligned}
$$

so $x_{q+1} = 1$.

This means that there is a point p with the property that every line containing p is a tangent to O. Thus, no line meets $O \cup \{p\}$ in more than two points. Also, no line meets it in one point either, since any tangent to O contains p.

---

11 Prove that, if q is a prime power, then any five points of $PG(2,q)$, such that no three of them are collinear, are contained in a unique conic. Deduce that the number of conics is

$$(q^2 + q + 1)q^2(q-1).$$

Let $p_1, \ldots, p_5$ be five points, with no three collinear. Let $p_i = \langle v_i \rangle$. Then v_1, v_2, v_3 are linearly independent, so that this set forms a basis. Relative to this basis, the coordinates of v_4 and v_5 are all non-zero. (If, for example, the first coordinate of v_4 were zero, then v_2, v_3, v_4 would be linearly dependent.) By multiplying v_1, v_2, v_3 by suitable non-zero scalars, we can assume that the coordinates

of v_4 are $(1,1,1)$. Let the coordinates of v_5 be (α, β, γ). Then α, β, γ are all distinct. (If, for example, $\alpha = \beta$, then v_3, v_4, v_5 would be linearly dependent.)

Now the equation of a conic has the form

$$ax^2 + by^2 + cz^2 + fyz + gzx + hxy = 0.$$

If this equation is satisfied by the coordinates of our five points, we have $a = b = c = 0$ and

$$
\begin{aligned}
f + g + h &= 0, \\
f/\alpha + g/\beta + h/\gamma &= 0.
\end{aligned}
$$

These equations are independent, and so have a unique solution up to scalar multiples. But a scalar multiple of the equation defines the same conic. So there is a unique conic containing the five points.

Now we count the number of choices of five points with no three collinear. There are $q^2 + q + 1$ choices for p_1; $q^2 + q$ for p_2 (any point different from p_1); and q^2 for p_3 (any point not on the line $p_1 p_2$). After this, the count becomes a bit more complicated, but may be done by PIE. For p_4, we must exclude three lines, any two meeting in a point but not all concurrent; so there are

$$q^2 + q + 1 - 3(q+1) + 3 = (q-1)^2$$

choices. For p_5, we must exclude the six lines joining pairs of points from $p_1, \ldots, p_4$. Again any two are concurrent but no three are except for the four triples through one of the p_i; no four of the lines are concurrent. So the number of choices is

$$q^2 + q + 1 - 6(q+1) + 15 - 4 = (q-2)(q-3).$$

So the total number of choices of the five points is

$$(q^2 + q + 1)(q+1)q^3(q-1)^2(q-2)(q-3).$$

Each choice defines a unique conic. But the $q+1$ points of a conic are pairwise non-collinear; so each conic contains $(q+1)q(q-1)(q-2)(q-3)$ such 5-tuples.

If $q \geq 4$, we obtain the number of conics by division; the result is the number stated. This fails for $q < 4$, since both expressions are zero, so we must proceed differently. For $q = 3$, a conic is a set of four pairwise non-collinear points (by Segre's Theorem); the number of ordered 4-tuples is $(q^2 + q + 1)(q+1)q^3(q-1)^2$, and we must divide by $4! = (q+1)q(q-1)$, giving the cited result. For $q = 2$, every triangle is a conic (since, taking the three points as a basis, they satisfy the equation $xy + yz + zx = 0$); there are $7.6.4/3! = 28$ conics, in agreement with the formula.

12 Define a geometry as follows. The points are to be all the 2-element subsets of $\{1,2,3,4,5,6\}$; the lines are all the disjoint triples of 2-subsets. Prove that the geometry is a generalised quadrangle with $s = t = 2$, $\alpha = 1$.

Two disjoint 2-subsets of $\{1,2,3,4,5,6\}$ can be completed to a partition into three 2-sets in a unique way (adjoining the complement of their union); while two intersecting 2-sets are contained in no partition. So two points of the geometry lie on at most one line. Clearly every line has three points; and any point (say $\{1,2\}$, or for short 12) lies in three lines, $\{12,34,56\}$, $\{12,35,46\}$, and $\{12,36,45\}$.

Take a line L (without loss $\{12,34,56\}$, and a point p not on it. Then p is not one of the three parts of the partition; so it shares an element with two of the parts, and is disjoint from the third. But two points are collinear if and only if (as sets) they are disjoint. So p is collinear with a unique point of L.

13 Let p be an odd prime. Show that half the non-zero congruence classes mod p are quadratic residues and half are non-residues, and that the product of two non-residues is a residue.

If x is a square root of a non-zero element of $GF(p)$ then so is $-x$. On the other hand, no element can have more than two square roots. For, if $x, -x, y$ are square roots of the same element, then $0 = x^2 - y^2 = (x-y)(x+y)$, so $y = x$ or $y = -x$.

So, of the $p - 1$ non-zero elements, $(p-1)/2$ are quadratic residues (with two square roots each) and $(p-1)/2$ are non-residues.

The equations $x^2 y^2 = (xy)^2$ and $x^2/y^2 = (x/y)^2$ show that the product and quotient of two residues is a residue. It follows that the product of a residue and a non-residue is a non-residue. (If r and n are respectively a residue and a non-residue, if rn were a residue a, then $n = a/r$ would be a residue.) Now multiplication by a fixed non-residue n is a bijection on $GF(p)$, which maps the $(p-1)/2$ residues to the $(p-1)/2$ non-residues; it thus must map non-residues to residues. So the product of non-residues is a residue.

14 Write a quaternion formally as $a + \mathbf{x}$, where a is a real number and $\mathbf{x}$ a 3-dimensional vector (relative to the standard basis $(\mathbf{i}, \mathbf{j}, \mathbf{k})$). Show that

$$
\begin{aligned}
(a + \mathbf{x}) + (b + \mathbf{y}) &= (a+b) + (\mathbf{x} + \mathbf{y}), \\
(a + \mathbf{x}) \cdot (b + \mathbf{y}) &= (ab - \mathbf{x}.\mathbf{y}) + (a\mathbf{y} + b\mathbf{x} + \mathbf{x} \times \mathbf{y}),
\end{aligned}
$$

where $\mathbf{x}.\mathbf{y}$ and $\mathbf{x} \times \mathbf{y}$ are the usual scalar and vector products ('dot product' and 'cross product') of vectors.

The rule for addition is obvious. For multiplication, all that really needs checking is that, for any 'pure' quaternions $\mathbf{x}$ and $\mathbf{y}$, their product as quaternions is $-\mathbf{x}.\mathbf{y} + \mathbf{x} \times \mathbf{y}$. This is shown by writing it out in coordinates.