1.1 Matrices over Finite Fields

This project is about the elementary properties of vector spaces, which are introduced in the Part IA course Vectors and Matrices and are considered more generally in the Part IB course Linear Algebra.

1 Fields of Prime Order

We shall be considering algorithms for computing algebraic invariants attached to vector spaces and linear maps over a field F. In applications the field is often that of the real or complex numbers. In this project F will be $\mathrm{GF}(p)$, the finite field of p elements, represented by the integers modulo p for some prime p.

In the examples you will work with, p will be small (at most 30), as will the matrices (at most 10×10). However, when answering questions about complexity for large p you should be thinking about how the program would behave for *very* large p (i.e., let p tend to infinity).

2 Division

It will be necessary to be able to divide modulo p; that is, for each a, $1 \leqslant a \leqslant p-1$, you will need to know its inverse a^{-1}, $1 \leqslant a^{-1} \leqslant p-1$, such that $aa^{-1} \equiv 1 \pmod{p}$. Rather than compute a^{-1} afresh each time it is needed, the inverses should be computed once and stored.

> **Question 1** Write a program to store the inverses of the non-zero elements of F in an array of length $p-1$. Find the inverses by testing, for each a in the range $1 \leqslant a \leqslant p-1$, all values of b in the range $1 \leqslant b \leqslant p-1$ until you find one which works and then store it. (Note that the MATLAB command `mod(a,p)` gives the value of a modulo p.) Describe any *very* simple modification to speed up this procedure (say by a factor of 2).

> **Question 2** Estimate the complexity of the procedure of Question 1 in terms of p.
>
> [That is, give a simple function $f(p)$ of p, such as $\sqrt{p}$, p or 2^p, such that the number of steps is $\Theta\big(f(p)\big)$, meaning of the order of magnitude of $f(p)$. To be exact, a function $g(p)$ is $\Theta\big(f(p)\big)$ if there are positive constants c and C such that $c \leqslant g(p)/f(p) \leqslant C$ for all sufficiently large p.
>
> You may assume that in a single step your ideal computer can perform any elementary operation such as to store a number, or to add, subtract, multiply, divide or compare two numbers.]

3 Gaussian Elimination

A non zero matrix $M = (m_{ij})$ over F, with m rows and n columns, is in *row echelon* form if

- for some r, $1 \leqslant r \leqslant m$, the last $m-r$ rows have only zero entries;
- for each i, $1 \leqslant i \leqslant r$, there is a number $1 \leqslant l(i) \leqslant n$ such that $m_{ij} = 0$ for $j < l(i)$ and $m_{ij} = 1$ for $j = l(i)$;
- $l(1) < l(2) < \cdots < l(r)$;

- for each k, $2 \leqslant k \leqslant r$, we have $m_{ij} = 0$ when $j = l(k)$ and $i < k$.

Here is a 4×5 matrix which is in row echelon form if we take the entries mod 7 (but not if we take the entries mod 2); in this case $r = 3$, $l(1) = 1$, $l(2) = 3$, $l(3) = 4$.

$$\begin{pmatrix} 1 & 4 & 0 & 7 & 5 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 15 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \pmod 7$$

The *rank* of a matrix is the dimension of its *row space*; that is, the vector space (over F) spanned by its rows. The rank of the matrix M above is r. The following operations on a matrix leave its row space unaltered:

- $T(i, j)$, transpose rows i and j
- $D(i, a)$, divide row i by the element $a \in F \setminus \{0\}$
- $S(i, a, j)$, subtract a times row $j \neq i$ from row i.

Gaussian elimination uses the operations T, D, S to convert a matrix into row echelon form.

Question 3 Write a program to turn a matrix into row echelon form using Gaussian elimination. From your output, compute the ranks of each of the following matrices, and give bases for their row spaces.

$$A_1 = \begin{pmatrix} 0 & 1 & 7 & 2 & 10 \\ 8 & 0 & 2 & 5 & 1 \\ 2 & 1 & 2 & 5 & 5 \\ 7 & 4 & 5 & 3 & 0 \end{pmatrix} \text{(first mod 3 then mod 29)}, \quad A_2 = \begin{pmatrix} 6 & 16 & 11 & 14 & 1 & 4 \\ 7 & 9 & 1 & 1 & 21 & 0 \\ 8 & 2 & 9 & 12 & 17 & 7 \\ 2 & 19 & 2 & 19 & 7 & 12 \end{pmatrix} \pmod{23}$$

4 Kernels and Annihilators

Let A be an $m \times n$ matrix and $\mathbf{x} = (x_j)$ an $n \times 1$ column vector over F. The *kernel* of A, denoted $\ker A$, is the space of solutions to $A\mathbf{x} = 0$. A basis can be found by reducing A to row echelon form and then expressing $x_{l(1)}, x_{l(2)}, \ldots, x_{l(r)}$ in terms of the other x_j.

Question 4 Write a program to compute a basis for the kernel of a matrix. Describe briefly how your algorithm works. Find bases for the kernels of the following matrices.

$$B_1 = \begin{pmatrix} 4 & 6 & 5 & 2 & 3 & 1 \\ 5 & 0 & 3 & 0 & 1 & 0 \\ 1 & 5 & 7 & 1 & 0 & 12 \\ 5 & 5 & 0 & 3 & 1 & 7 \\ 2 & 1 & 2 & 4 & 0 & 5 \end{pmatrix} \text{(first mod 2 then mod 11 then mod 17)}, \quad B_2 = \begin{pmatrix} 3 & 7 & 19 & 3 & 9 & 6 \\ 10 & 2 & 20 & 15 & 3 & 0 \\ 14 & 1 & 3 & 14 & 11 & 3 \\ 26 & 1 & 21 & 6 & 3 & 5 \\ 0 & 1 & 3 & 19 & 0 & 3 \end{pmatrix} \pmod{23}$$

Let U be a subspace of the space of row vectors F^n. The annihilator U° consists of the set of column vectors $\mathbf{x}$ satisfying $\mathbf{u}\,\mathbf{x} = 0$ for every $\mathbf{u} \in U$. It is a subspace of the space of column vectors. Notice that if U is the row space of a matrix A, then U° is the kernel of A.

Question 5 State the relationship between the dimensions of U and U°.

If S is a subspace of the space of column vectors, then we make an analogous definition of S° as the space of row vectors $\mathbf{t}$ satisfying $\mathbf{t}\,\mathbf{s} = 0$ for every $\mathbf{s} \in S$. We have

$$(U^\circ)^\circ = U.$$

Question 6 Use your program from Question 4 to find U° where we work mod 19 and U is the row space of the matrix A_1. Similarly find $(U^\circ)^\circ$ and verify that it is equal to U.

For U and W subspaces of F^n it is known that

$$(U + W)^\circ = U^\circ \cap W^\circ$$

and

$$(U \cap W)^\circ = U^\circ + W^\circ.$$

Question 7 Write a program that, given matrices A and B with row spaces U and W, computes bases for U, W, $U + W$ and $U \cap W$. Explain briefly how your program works. Comment on the relationship between the dimensions of the four spaces computed. Run your program on the following examples:

- Modulo 11 with U the row space of A_2 and W the row space of B_1.
- Modulo 19 with U the row space of

$$A_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 5 & 0 & 1 & 6 & 3 & 0 \\ 0 & 0 & 5 & 0 & 2 & 0 & 0 \\ 2 & 4 & 0 & 0 & 0 & 5 & 1 \\ 4 & 3 & 0 & 0 & 6 & 2 & 6 \end{pmatrix}$$

  and W the kernel of A_3. (Although the kernel of A_3 is naturally a space of column vectors, you should re-write it as a space of row vectors in the obvious way.)
- Again take U the row space of A_3 and W the kernel of A_3, but this time modulo 7.

Question 8 What feature of the very last part of Question 7 would be surprising to someone who carried out a similar project working over the real numbers instead of $\mathrm{GF}(p)$?

