Math 422, Winter 2008
Review on Linear Algebra

Systems of Equations

In the following let F be a field. To solve a system of linear equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ \vdots \qquad &= \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

we proceed as follows: the set of solutions to this system is precisely the nullspace of the matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Here the nullspace of A is the set of all $n \times 1$ column vectors $\mathbf{x}$ satisfying $A\mathbf{x} = \mathbf{0}$. Thus, $(x_1, x_2, \dots, x_n)$ solves the above system if and only if

$$A \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \mathbf{0}$$

In coding theory it is common to write vectors in F^n as *row vectors*. That is we often write

$$\mathbf{x} = [x_1\, x_2\, \dots\, x_n]$$

for the vector $(x_1, x_2, \dots, x_n)$ in F^n. In this notation $(x_1, x_2, \dots, x_n)$ solves the above system if and only if $A\mathbf{x}^t = \mathbf{0}$ where $\mathbf{x} = [x_1\, x_2\, \dots\, x_n]$ and $?^t$ denotes the transpose.
How do we solve such a system? The answer is: Gaussian Elimination. That is, we need to bring the matrix A into reduced (row) echelon form. We can do this by performing the following operations:

- exchanging two rows
- adding a multiple of one row to another (different) row
- multiplying any row with a nonzero scalar

If we call the first nonzero entry in a row the *leading entry* of this row then using these operations we obtain a matrix that has the following properties:

- If a row has a leading entry, the leading entry is 1.
- If a row has a leading entry, it is (strictly) to the right of the leading entry of the preceding row. (In particular, if a row has a leading entry, then the preceding row has a leading entry.)
- The entries above each leading entry are zero.

(From the second property it follows that the rows containing all zeros are below the rows containing nonzero entries.)
A matrix satisfying these three properties is called a matrix in *reduced (row) echelon form.* A typical (but not the most general) matrix in this form looks like

$$\begin{bmatrix} 0 & 0 & \dots & 0 & 1 & * & \dots & * & 0 & * \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & * \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{bmatrix}$$

Here a $*$ denotes an arbitrary entry (zero or nonzero). Each column of the matrix corresponds to a variable. The variables corresponding to the columns without leading entry are called free variables.

IMPORTANT: The number of free variables is the dimension of the nullspace of this matrix. The nullspace of a matrix and that of its reduced row echelon form are equal. If solving the equation $A\mathbf{x} = \mathbf{0}$: if, in the reduced echelon form of A the column corresponding to a variable contains a leading entry (of any row), then the value of the corresponding variable is uniquely determined by the values of the free variables (cf. back substitution).

RECALL: This applies only to homogeneous systems. For general systems of the form $A\mathbf{x} = \mathbf{b}$, the matrix one needs to bring into reduced echelon form is the *augmented matrix* obtained from our A by adding $\mathbf{b}$ as an additional column. But here this column would be all zeros and would not change during the process of finding the reduced echelon form.

Example

Consider $F = \mathbb{Z}_3$ and

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 0 & -1 & 2 \\ 1 & -2 & 0 & 1 \end{bmatrix}$$

Using the fact that $F = \mathbb{Z}_3$, we add the first row to the second, and subtract it from the last to obtain

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

Erasing the second and third 1 in the first row by subtracting the second row and adding the third we arrive at the reduced echelon form (after scaling the last row by -1):

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Thus the nullspace of A is the set of vectors satisfying the equations $x_1 + x_4 = 0, x_2 = 0, x_3 = 0$. The only free variable is x_4, and we obtain as nullspace (or *kernel*, denoted $\ker A$)

$$\ker A = \left\{ t \begin{bmatrix} 2 \\ 0 \\ 0 \\ 1 \end{bmatrix} : t \in F \right\}$$

Since this is a one-dimensional subspace over F, it has three elements, corresponding to the three possible values of t $(0, 1, 2)$:

$$\ker A = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 2 \end{bmatrix} \right\}$$

Dimension and bases of vector spaces

Explicit case

How do we compute the dimension of a subspace W of F^n? It depends how W is given. Suppose we know that W is *explicitly* given, that is, W is spanned by given vectors $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$ (thought of as column vectors). Then we form the matrix

$$A = [\mathbf{w}_1\, \mathbf{w}_2\, \ldots\, \mathbf{w}_k]$$

Then W is equal to the column space of A (that is, the space spanned by the columns of A) and so

$$\dim W = \operatorname{rank} A$$

How do we find $\dim W = \operatorname{rank} A$? Again, by determining the reduced row echelon form (if you know what it means: *any* echelon form will do, it does not have to be reduced) and counting the number of leading entries. Alternatively, if F is finite with q elements, and if we know the number of elements W contains, then $|W| = q^k$ where $k = \dim W$, so $\dim W = \log_q |W|$.

How do we find a spanning set for W? This depends on the problem we are looking at. However, if we work over a finite field F, then W is finite. If we are given *all* elements of W,

then we may take as spanning set W itself, that is, the columns of A will be all elements of W. Of course, for large subspaces this is impractical.
How do we find a basis of a subspace W? Again, we form the matrix A whose columns form a spanning set of W. Then we compute the row echelon form. For each row with a leading entry we note the column which contains this leading entry. Then the corresponding columns of A (*not* those of the echelon form) will be a basis for W.

Implicit case

If W is implicitly given, that is $W = \ker A$ for some matrix A, then we find its dimension and a basis by solving the system $A\mathbf{x} = \mathbf{0}$. So $\dim W$ is the number of free variables, and a basis is obtained by the parameterized vector form of the solution, that is: for each free variable we obtain one basis vector as follows:
For the free variable x_i the vector is: its entry at the ith position is 1, its entry at a position $j \neq i$ is 0 if x_j is a free variable. Otherwise it is $-u_{ki}$ where u_{ki} is the entry in the kth row and ith column of the reduced row echelon form of A and k is the index of the row which contains the leading entry corresponding to x_j.
In the example above: the only free variable is x_4. The corresponding basis vector has $2 = -u_{14}$ as first entry. The second and third entries are $-u_{24} = -u_{34} = 0$.
Again, if we are only interested in the dimension of W, then $\dim W = n - \operatorname{rank} A$ where n is the number of columns of A (cf. the Rank Theorem).