Chapter 1

More Matrix Algebra

1.1 Linear Equations over the Integers Mod 2

1.1.1 Row reduction mod 2

The methods we have studied for solving systems of equations up to this point can be applied to systems in which all arithmetic is done over other algebraic systems, including the integers modulo 2. In this section we will examine a few examples. This will become particularly useful in our later study of coding theory.

When solving systems of equations with mod 2 arithmetic, the elementary row operations are still fundamental. However, since there is only one nozero element, 1, we never need to multiply a row by a nonzero constant. One other big difference is that the number of possible solutions is always finite. If we have m linear equations in n unknowns, each unknown can only take on one of two values, 0 or 1. Therefore there are only 2^n possible n-tuples to from which to draw a solution set. Assuming $m \leq n$, we typically (but not always) will have m basic variables after row-reduction and $n - m$ free variable. If this is the case, and any solution exists, there will be 2^{n-m} different solutions.

Let's look at an example, which we will convert to matrix form immediately.

$$\begin{array}{rrrrrrr} x_1 & + x_2 & + x_3 & + x_4 & & & = 1 \\ x_1 & & + x_3 & & + x_5 & & = 0 \\ & & x_2 & + x_3 & & + x_6 & = 1 \end{array}$$

The augmented matrix of the system is

$$\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right)$$

The steps in row-reducing this matrix follow. We circle the entries on which we "pivot" to make it easy to identify the basic variables.

$$\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right) \xrightarrow{\text{add } R_1 \text{ to } R_2} \left(\begin{array}{cccccc|c} \textcircled{1} & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{\text{add } R_2 \text{ to } R_1} \left(\begin{array}{cccccc|c} \textcircled{1} & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & \textcircled{1} & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{\text{add } R_2 \text{ to } R_3} \left(\begin{array}{cccccc|c} \textcircled{1} & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & \textcircled{1} & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

Notice that at this point, we cannot pivot on the third row, third column since that entry is zero. Therefore we move over to the next column, making the x_4 basic.

$$\xrightarrow{\text{add } R_3 \text{ to } R_2} \left(\begin{array}{cccccc|c} \textcircled{1} & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & \textcircled{1} & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \textcircled{1} & 1 & 1 & 1 \end{array}\right)$$

This completes the row reduction and we can now write down the solutions, keeping in mind that since addition is subtraction, terms can be moved to either side of an equals sign without any change in sign. The basic variables are x_1, x_2, and x_4, while the other three variables are free. The general solution of the system is

$$\begin{aligned} x_1 &= x_3 + x_5 \\ x_2 &= x_3 + x_6 \\ x_3 &= x_3 \\ x_4 &= 1 + x_5 + x_6 \\ x_5 &= x_5 \\ x_6 &= x_6 \end{aligned}$$

With three free variables, there are $2^3 = 8$ solutions to this systme. For example, one of them is obtained by setting $x_3 = 1$, $x_5 = 1$, and $x_6 = 0$, which produces $(x_1, x_2, x_3, x_4, x_5, x_6) = (0, 1, 1, 0, 1, 0)$.

We can check our row reduction with SageMath:

```
H=Matrix(Integers(2),[[1,1,0,1,0,0,1],[1,0,1,0,1,0,0],[0,1,1,0,0,1,0]])
H.echelon_form()
```

```
[1 0 1 0 1 0 0]
[0 1 1 0 0 1 0]
[0 0 0 1 1 1 1]
```

1.1.2 Exercises for this section

1. Solve the following systems, describing the solution sets completely:

(a)
$$\begin{array}{rl} x_1 + x_2 & = 0 \\ x_2 + x_3 & = 0 \end{array}$$

(b)
$$\begin{array}{rl} x_1 + x_2 & = 0 \\ x_2 + x_3 & = 0 \\ x_3 + x_4 & = 1 \\ x_1 + x_2 + x_3 & = 1 \end{array}$$

2. This exercise motivates the concept of a coset in Chapter 15.

(a) Solve the following system and prove that the solution set is a subgroup of the group $\mathbb{Z}_2^5$ under coordinatewise mod 2 addition.

$$\begin{array}{rl} x_1 + x_2 + x_5 & = 0 \\ x_1 + x_3 + x_5 & = 0 \\ x_1 + x_3 + x_4 & = 0 \\ x_2 + x_3 + x_4 & = 0 \end{array}$$

(b) Describe the solution set to the following system as it relates to the solution set to the system in the previous part of this exercise.

$$\begin{array}{rl} x_1 + x_2 + x_5 & = 1 \\ x_1 + x_3 + x_5 & = 0 \\ x_1 + x_3 + x_4 & = 1 \\ x_2 + x_3 + x_4 & = 0 \end{array}$$