Solutions of Systems of Linear Equations in a Finite Field
Nick Rimes

Abstract: In this paper, the solutions for the system of linear equations of the form $Av = x$ is analyzed. In particular, this paper focuses on the solutions for all $2 \times 2$ matrices in the field $\mathbb{Z}_p$ where $p$ is a prime number. The results will show that the expected properties from the real numbers do not necessarily hold in a finite field.

1. Introduction

Linear algebra has roots which date back as far as the birth of calculus. In the late 1600’s, Leibnitz used coefficients of linear equations in much of his work, and later in the 1700’s Lagrange further developed the idea of determinants through his Lagrangian multipliers. The term “matrix” wasn’t actually coined until the mid 1800’s when J.J. Sylvester used the term, which is Latin for womb, to describe an array of numbers. In the same century, Gauss further developed the idea of using matrices to solve systems of linear equations through the use of Gaussian elimination. Later, Wilhelm Jordan would introduce the technique of Gauss-Jordan elimination in a handbook on geodesy. In the field of geodesy, mathematicians use concepts of linear algebra to examine the dimensions of the planet Earth. Finally, in the late 1800’s vector algebra, and more advanced matrix mathematics was cultivated by mathematicians such as Arthur Cayley and Hermann Grassmann.

It wasn’t until the twentieth century though, that linear algebra really took off as a mathematical field. The development of ring theory and abstract algebra opened up new avenues to take advantage of the techniques in the field of linear algebra. The use of Cramer’s rule, in particular, was used so widely to solve partial differential equations, that it led to the widespread introduction of linear algebra into the curriculum of modern universities. Thus, linear algebra came into its own as the widely used and respected mathematical field that is used today. To learn more about this subject, please look to the references section for the works of Tucker, Athloen, and Mclaughlin.

2. Preliminary Information

Throughout the paper the following variables will be used:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad q = (ad - bc)^{-1}, \quad \text{and} \quad B = q \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}. $$

Definition: The determinant of an $n \times n$ matrix is the sum of all $n$ possible signed products formed from the matrix using each row and each column only once for each product. The sign to be attached to the product is the same as the one determined by the formula $(-1)^n$.

We denote $\det(A)$ as the determinant of $A$. 
Note: It is known that $A$ is non-singular iff $\det(A) \neq 0$, and $A^{-1}$ exists iff $A$ is non-singular.

Figure 1. Comparison table for Singular and Non-Singular Matrices.

<table>
<thead>
<tr>
<th>Property</th>
<th>Singular</th>
<th>Non-Singular</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determinant</td>
<td>Zero</td>
<td>Non-zero</td>
</tr>
<tr>
<td>Invertible</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Linearly Independent rows/columns</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Unique Solution exists</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Zero is an eigenvalue</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Problem: Given an $n \times n$ matrix $A$ and an $n \times 1$ vector $x$, find an $n \times 1$ vector $v$ such that $Av = x$. Let us first consider the solution in the real numbers.

Note: There are three different cases which must be analyzed when discussing the solution of a system of linear equations $Av = x$.

Case 1.

Determinant of $A$ is non-zero. In this case, the matrix $A$ is non-singular and its inverse exists. The linear system $Av = x$ has a unique solution of the form: $v = A^{-1}x$.

Case 2.

Determinant of $A$ is zero, and rank of $A$ is equal to the rank of the augmented matrix $[A \mid v]$. In this case, there are infinitely many solutions in $\mathbb{R}$.

Case 3.

Determinant of $A$ is zero, and the rank of $A$ is less than the rank of the augmented matrix $[A \mid v]$. In this case, the linear system $Av = x$ has no solutions.

3. Solutions of $Av = x$ in a finite field

Note: Let $p$ be a prime number. Consider now $A$, $v$, and $x$ in the finite field $\mathbb{Z}_p$.

Part 1. Possible matrices and their determinants in a finite field
In order to accurately examine the solutions of the system of linear equations $A\mathbf{v} = \mathbf{x}$, we must first determine the different matrix compositions for all possible matrices in $\mathbb{Z}_p$, and also determine which of these matrices are singular, and which are non-singular.

**Note:** In $\mathbb{Z}_p$, the number of total possible $2 \times 2$ matrices is $p^4$.

**Case 1.** The triple-zero matrix: $\begin{bmatrix} \times & 0 \\ 0 & 0 \end{bmatrix}$.

There are four different variations of this matrix with $p-1$ possible values for $\times$. This gives us $4(p-1)$ possible matrices in $\mathbb{Z}_p$. For this type of matrix the determinant shall always be zero since

$$\det A = ad - bc \Rightarrow \times 0 - 0 = 0.$$ 

Hence, the matrix will be singular.

**Case 2.** The zero-row/column matrix: $\begin{bmatrix} \times & \times \\ 0 & 0 \end{bmatrix}$.

There are four different variations of this matrix with $4(p-1)^2$ possible matrices. The determinant of this matrix shall always be zero since

$$\det A = ad - bc \Rightarrow \times 0 - \times 0 = 0.$$ 

**Case 3.** The single-zero matrix: $\begin{bmatrix} \times & \times \\ \times & 0 \end{bmatrix}$.

There are four different variations of this matrix with $4(p-1)^3$ possible matrices. The determinant of matrices of this form will always be non-zero. The reason is as follows. Since $p$ is a prime:

$$\forall \times < p, \times \times \neq np \forall n = 0,1,2\ldots$$ 

Thus,

$$\det A = ad - bc \Rightarrow \times 0 - \times \times \neq 0.$$ 

**Case 4.** The zero-diagonal matrix: $\begin{bmatrix} \times & 0 \\ 0 & \times \end{bmatrix}$.

There are 2 different variations of this matrix for a total of $2(p-1)^2$ possible matrices. The determinant of this matrix is always non-zero since:

$$\forall \times < p, \times \times \neq np \forall n = 0,1,2\ldots$$ 

Thus:
\[ \det A = ad - bc \Rightarrow \times 0 - \times \times \times \neq 0. \]

Case 5. The zero matrix: 
\[
\begin{bmatrix}
0 & 0 \\
0 & 0
\end{bmatrix}
\]

There is only one matrix of this form and it is trivial to prove that the determinant of this matrix will always be zero.

Case 6. The non-zero matrix: 
\[
\begin{bmatrix}
\times & \times \\
\times & \times
\end{bmatrix}
\]

For this case we will have four variables with \( p - 1 \) possible values for each variable, thus we have \( (p - 1)^4 \) possible matrices of this form. In order to determine the determinant of these matrices, we must further analyze this form.

For non-zero matrices with determinant equal to zero:
\[ ad - bc = 0 \text{ or } ad = bc \]

The rows must be linear combinations of each other, and for each row there are \( (p - 1)^2 \) possible combinations of \( \times \)'s. Given any possible row combination, there are \( (p - 1) \) multiples by which the rows may be multiplied to form a linear combination. Thus for the non-zero matrix with determinant equal to zero, there are \( (p - 1)^2(p - 1) \) or \( (p - 1)^3 \) possible matrices. Since we know there are \( (p - 1)^4 \) total non-zero matrices, by elimination we have \( (p - 1)^4 - (p - 1)^3 \) or \( (p - 1)^2(p - 2) \) non-zero matrices with determinant not equal to zero.

Therefore, when we add all possible cases we should find that there are \( p^4 \) total matrices:
\[
(p - 1)^3 + (p - 1)^2(p - 2) + 4(p - 1) + 4(p - 1)^2 + 4(p - 1)^3 + 2(p - 1)^2 + 1 = p^4.
\]

Part 2. Invertability of a non-singular matrix in a finite field.

Now, we prove that for these given matrices, if \( A \) is non-singular then \( A \) is invertible in a finite field. Let
\[
A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad q = (ad - bc)^{-1}, \quad \text{and} \quad B = q \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.
\]

We will show the following:
If \( \det(A) \neq 0 \), then \( AB = BA = I \) where \( I \) is the identity matrix and \( B \) is the inverse of the matrix \( A \)

Proof:
\[ AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad - bc & ab - ab \\ cd - ca & ad - bc \end{bmatrix} = I \]

and

\[ BA = q \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ad - bc & db - bd \\ ca - ca & ad - bc \end{bmatrix} = I \]

Therefore, over a finite field, if \( A \) is non-singular then \( A \) is invertible.

**Part 3. Solution of \( Av = x \) in a finite field when \( A \) is non-singular.**

In \( \mathbb{R} \), the system \( Av = x \) has a unique solution. We will show that the system also has a unique solution over a finite field. Let

\[ x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \text{ and } v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}. \]

Then

\[ Av = x \Rightarrow BAv = Bx \Rightarrow v = Bx \]

and

\[ Bx = q \begin{bmatrix} (dx_1 - bx_2) \\ (cx_1 - ax_2) \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \]

Therefore for a given vector \( x \), there is a unique solution for the vector \( v \), and

\[ v = q \begin{bmatrix} (dx_1 - bx_2) \\ (cx_1 - ax_2) \end{bmatrix}. \]

**Part 4. Solution of \( Av = x \) in a finite field when \( A \) is singular.**

When \( A \) is singular, we must examine two cases for the system \( Av = x \). Case 1 occurs when the rank of \( A \) is less than the rank of the augmented matrix \([A \mid x]\), and Case 2 is when the rank of \( A \) is equal to the rank of the augmented matrix \([A \mid x]\).

Case 1.

In this case, there is no solution in the real numbers, therefore we will prove that there is no solution in a finite field.

Let \( \alpha \) be a constant integer and row 1 of \( A = \alpha \) row 2 of \( A \) but \( x_1 \neq \alpha x_2 \). Then
\[
\begin{bmatrix}
A \\ x
\end{bmatrix} = \begin{bmatrix}
a & b & x_1 \\
aa & ab & x_2
\end{bmatrix} \quad \xrightarrow{\text{row 2} - \alpha \text{row 1}} \quad \begin{bmatrix}
a & b & x_1 \\
0 & 0 & x_2 - \alpha x_1
\end{bmatrix}.
\]

Since the equation
\[0 + 0 = x_2 - \alpha x_1 \neq 0\]
ever holds in the finite field, the system \(Av = x\) has no solution in a finite field.

Case 2.

In this case the system \(Av = x\) has infinitely many solutions in \(\mathbb{R}\). We will show that the system \(Av = x\) in \(\mathbb{Z}_p\) field will have only \(p\) solutions.

Let \(\alpha\) be a constant integer and row 1 of \(A = a\) row 2 of \(A\) and \(x_1 = \alpha x_2\). Then
\[
\begin{bmatrix}
A \\ x
\end{bmatrix} = \begin{bmatrix}
a & b & x_1 \\
aa & ab & x_2
\end{bmatrix} \quad \xrightarrow{\text{row 2} - \alpha \text{row 1}} \quad \begin{bmatrix}
a & b & x_1 \\
0 & 0 & 0
\end{bmatrix}
\]
and we have only the equation \(av_1 + bv_2 = x_1\). Solving \(v_2\) in term of \(v_1\), we have
\[v_2 = b^{-1}(x_1 - av_1)\).

For a given \(x_1\) in \(\mathbb{Z}_p\), we have \(p\) different possibilities for \(v_1\) and \(p\) corresponding possibilities for \(v_2\). Thus there are only \(p\) solutions in \(\mathbb{Z}_p\).

Example: Consider \(Z_3\). Let \(A = \begin{bmatrix}
1 & 1 \\
2 & 2
\end{bmatrix}\) and \(x = \begin{bmatrix}
2 \\
1
\end{bmatrix}\). Then
\[
\begin{bmatrix}
A \\ x
\end{bmatrix} \equiv_3 \begin{bmatrix}
1 & 1 & 2 \\
2 & 2 & 1
\end{bmatrix} \quad \xrightarrow{\text{row 2} - \text{row 1}} \quad \begin{bmatrix}
1 & 1 & 2 \\
0 & 0 & 0
\end{bmatrix}
\]
Solving the equation \(v_1 + v_2 \equiv_3 2\), we have solutions for \(Av = x\):
\[v = \begin{bmatrix}
0 \\
2
\end{bmatrix}, \begin{bmatrix}
2 \\
0
\end{bmatrix}, \begin{bmatrix}
1 \\
1
\end{bmatrix}.
\]

Part 5. Results

The results lead us to the theorem:

**Rimes’ Little Magical Theorem:**
In the finite field $\mathbb{Z}_p$, where $p$ is a prime number, the equation $Av = x$ where $A$ is a 2x2 singular matrix and $\text{rank}[A] = \text{rank}[A | x]$, has $p$ solutions in $\mathbb{Z}_p$.

4. Conclusion

The results found in this paper have only been proven for the case where $A$ is a 2x2 matrix. It becomes exponentially more complicated to examine $n \times n$ matrices where $n \geq 3$. It does, however, follow from the research given here that a similar result should be obtained for matrices of higher dimensions. A singular 2X2 matrix can only have rank equal to one, but higher dimension singular matrices may have rank from 1 to $p - 1$. Thus for any given value you may have $p^{\text{rank}[A]}$ various possible values for the elements in your solution vector. This leads the researcher to hypothesis that for the singular $n \times n$ where $n \geq 3$, the number of possible solutions in $\mathbb{Z}_p$ is $p^{\text{rank}[A]}$. This remains to be proven.

References