Course 12

3.7 Linear systems of equations

In this section we present some aspects of the theory of linear systems of equations which can be approached by using tools of Linear Algebra.

As usual, throughout this section K will be a field. When needed, we use superior indices to denote vectors in K^n and inferior indices to denote their components. For instance, $x^0 = (x_1^0, \dots, x_n^0) \in K^n$.

Definition 3.7.1 Consider a *linear system* of m equations with n unknowns $x_1, \dots, x_n$:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases} \tag{S}$$

where the coefficients are $a_{ij}, b_i \in K$ $(i = 1, \dots, m,\ j = 1, \dots, n)$.
If $b_1 = \dots = b_m = 0$, then the system (S) is called *homogeneous* and is denoted by (S_0).
The matrix $A = (a_{ij}) \in M_{m,n}(K)$ is called the *matrix of the system* (S).
The matrix

$$\bar{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

is called the *augmented* (or *extended*) *matrix of the system* (S).

Next we present two equivalent forms of a linear system of equations.

First, denote

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Then the systems (S) and (S_0) can be written as:

$$A \cdot x = b\,, \tag{S}$$

$$A \cdot x = 0\,. \tag{S_0}$$

Furthermore, we know that there exists a bijective correspondence between K-linear maps and matrices. Thus, since $A \in M_{m,n}(K)$, there exists $f_A \in \mathrm{Hom}_K(K^n, K^m)$ such that $[f_A]_{EE'} = A$, where E and E' are the canonical bases in K^n and K^m respectively.

Denoting $x = (x_1, \dots, x_n) \in K^n$ and $b = (b_1, \dots, b_m) \in K^m$, it follows that

$$[f_A(x)]_{E'} = [f_A]_{EE'} \cdot [x]_E = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = [b]_{E'}\,.$$

Hence $f_A(x) = b$. Thus, the systems (S) and (S_0) can be written as:

$$f_A(x) = b\,, \tag{S}$$

$$f_A(x) = 0\,. \tag{S_0}$$

Remark 3.7.2 (1) Thus, for a linear system of equations we have three equivalent forms, namely: the classical one with coefficients and unknowns, the one using matrices and the one using the corresponding linear map.

(2) We have denoted by x and b first column-matrices and then row-matrices to get nicer results, without using any transposed matrices.

Definition 3.7.3 An element $x^0 \in M_{n1}(K)$ ($x^0 \in K^n$) is called a:
(1) *(particular) solution* of (S) if $A \cdot x^0 = b$ (or equivalently $f_A(x^0) = b$).
(2) *(particular) solution* of (S_0) if $A \cdot x^0 = 0$ (or equivalently $f_A(x^0) = 0$).

Denote the sets of solutions of (S) and (S_0) by

$$S = \{x^0 \in M_{n1}(K) \mid A \cdot x^0 = b\} \quad \text{or} \quad S = \{x^0 \in K^n \mid f_A(x^0) = b\}\,,$$

$$S_0 = \{x^0 \in M_{n1}(K) \mid A \cdot x^0 = 0\} \quad \text{or} \quad S_0 = \{x^0 \in K^n \mid f_A(x^0) = 0\}\,.$$

Theorem 3.7.4 *The set S_0 of solutions of the homogeneous linear system of equations (S_0) is a subspace of the canonical vector space K^n over K and*

$$\dim S_0 = n - \operatorname{rank}(A)\,.$$

Proof. Since

$$S_0 = \{x^0 \in K^n \mid f_A(x^0) = 0\} = \operatorname{Ker} f_A$$

and the kernel of a linear map is always a subspace of the domain vector space, it follows that $S_0 \leq K^n$. Now by the First Dimension Theorem, it follows that

$$\dim S_0 = \dim(\operatorname{Ker} f_A) = \dim K^n - \dim(\operatorname{Im} f_A) = n - \operatorname{rank}(f_A) = n - \operatorname{rank}(A)\,,$$

which finishes the proof. □

Theorem 3.7.5 *If $x^1 \in S$ is a particular solution of the system (S), then*

$$S = x^1 + S_0 = \{x^1 + x^0 \mid x^0 \in S_0\}\,.$$

Proof. Since $x^1 \in S$, we have $Ax^1 = b$. We prove the requested equality by double inclusion.

First, let $x^2 \in S$. Then

$$Ax^2 = b \Longrightarrow Ax^2 = Ax^1 \Longrightarrow A(x^2 - x^1) = 0 \Longrightarrow x^2 - x^1 \in S_0 \Longrightarrow x^2 \in x^1 + S_0\,.$$

Conversely, let $x^2 \in x^1 + S_0$. There exists $x^0 \in S_0$ such that $x^2 = x^1 + x^0$. Then:

$$Ax^2 = A(x^1 + x^0) = Ax^1 + Ax^0 = b + 0 = b,$$

and consequently $x^2 \in S$.

Therefore, $S = x^1 + S_0$. □

Remark 3.7.6 By Theorem 3.7.5, the general solution of the system (S) can be obtained by knowing the general solution of the homogeneous system (S_0) and a particular solution of (S).

In the sequel, we are going to see when a linear system of equations has a solution.

Definition 3.7.7 The system (S) is called *compatible* (or *consistent*) if it has at least one solution. A compatible system (S) is called *determinate* if it has a unique solution.

Remark 3.7.8 (1) The system (S) is compatible if and only if $\exists x^0 \in K^n$ such that $f_A(x^0) = b$ if and only if $b \in \operatorname{Im} f_A$.

(2) The system (S_0) is compatible if and only if $\exists x^0 \in K^n$ such that $f_A(x^0) = 0$ if and only if $0 \in \operatorname{Im} f_A$. But the last condition always holds, since $\operatorname{Im} f_A$ is a subspace of K^m. Hence any homogeneous linear system of equations is compatible, having at least the zero (trivial) solution.

Theorem 3.7.9 *The system* (S_0) *has a non-zero solution if and only if* $\operatorname{rank}(A) < n$.

Proof. By Theorem 3.7.4, we have

$$S_0 = \operatorname{Ker} f_A \neq \{0\} \iff \dim S_0 \neq 0 \iff n - \operatorname{rank}(A) \neq 0 \iff \operatorname{rank}(A) < n\,,$$

which proves the result. □

Corollary 3.7.10 *Let* $A \in M_n(K)$. *Then*

$$S_0 = \{0\} \iff \operatorname{rank}(A) = n \iff \det(A) \neq 0\,.$$

Definition 3.7.11 If $A \in M_n(K)$ and $\det(A) \neq 0$, then the system (S) is called a *Cramer system*.

Theorem 3.7.12 *A Cramer system* $Ax = b$ *has a unique solution. More precisely, its unique solution* $(x_1, \dots, x_n)$ *is computed by*

$$x_i = \det(A)^{-1} \cdot d_i,$$

where d_i *is the determinant obtained from* $\det(A)$ *by replacing its* i^{th} *column by the column* b *for every* $i \in \{1, \dots, n\}$.

Proof. The matrix of a Cramer system is an invertible matrix $A \in M_n(K)$. Then we deduce that $x = A^{-1}b$ is the unique solution. Moreover, we have

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \det(A)^{-1} \cdot A^* \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \det(A)^{-1} \cdot \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}.$$

Hence $x_i = \det(A)^{-1} \cdot d_i$ for every $i \in \{1, \dots, n\}$. □

Corollary 3.7.13 *A homogeneous Cramer system has only the zero solution.*

Let us now give two classical compatibility theorems.

Theorem 3.7.14 (Kronecker-Capelli Theorem) *The system* (S) *is compatible if and only if* $\operatorname{rank}(\bar{A}) = \operatorname{rank}(A)$.

Proof. Let $(e_1, \dots, e_n)$ be the canonical basis of the canonical vector space K^n over K and denote by $a^1, \dots, a^n$ the columns of the matrix A. Then we have

$$\begin{aligned} (S) \text{ is compatible } &\iff \exists x^0 \in K^n :\ f_A(x^0) = b \iff b \in \operatorname{Im} f_A \\ &\iff b \in f_A(\langle e_1, \dots, e_n \rangle) \iff b \in \langle f_A(e_1), \dots, f_A(e_n) \rangle \\ &\iff b \in \langle a^1, \dots, a^n \rangle \iff \langle a^1, \dots, a^n, b \rangle = \langle a^1, \dots, a^n \rangle \\ &\iff \dim \langle a^1, \dots, a^n, b \rangle = \dim \langle a^1, \dots, a^n \rangle \iff \operatorname{rank}(\bar{A}) = \operatorname{rank}(A)\,, \end{aligned}$$

which proves the result. □

Definition 3.7.15 A minor d_p of the matrix A is called a *principal determinant* if $d_p \neq 0$ and d_p has the order $\operatorname{rank}(A)$.
We call *characteristic determinants associated to a principal determinant* d_p of A the minors of the augmented matrix $\bar{A}$ obtained by completing the matrix of d_p with a column containing the corresponding constants b_i and a row containing the corresponding elements of a row of $\bar{A}$.

Now we give the second compatibility theorem.

Theorem 3.7.16 (Rouché Theorem) *The system (S) is compatible if and only if all the characteristic determinants associated to a principal determinant are zero.*

Proof. $\boxed{\Longrightarrow}$ Suppose that the system (S) is compatible. Then by Theorem 3.7.14, $\operatorname{rank}(\bar{A}) = \operatorname{rank}(A)$. Denote this rank by r. Then there exists a principal determinant d_p of order r. Since $r = \operatorname{rank}(A)$, any determinant of order $r+1$ is zero and consequently any characteristic determinant associated to d_p is zero.

$\boxed{\Longleftarrow}$ Suppose that all the characteristic determinants associated to a principal determinant are zero. Denote $r = \operatorname{rank}(A)$. Then $r \leq \operatorname{rank}(\bar{A})$ and there exists a non-zero minor, actually a principal determinant, d_r of A. But d_r is also a minor of $\bar{A}$ of order r.

Now let d_{r+1} be a minor of $\bar{A}$ of order $r+1$. We have two possibilities, namely either d_{r+1} is a minor of $\bar{A}$ or d_{r+1} is just a minor of A. In the first case, d_{r+1} is a characteristic determinant associated to the principal determinant d_r, hence $d_{r+1} = 0$ by hypothesis. In the second case, we have $d_{r+1} = 0$, since $\operatorname{rank}(A) = r$.

Thus, $\operatorname{rank}(\bar{A}) = r = \operatorname{rank}(A)$. Now by Theorem 3.7.14, (S) is compatible. □

3.8 Gauss method

In this section we briefly present a very useful practical method to solve linear systems of equations, called the *Gauss method* (or *Gaussian elimination*).

In the sequel, suppose that $m \leq n$, that is, we talk about systems with less equations than unknowns. In fact, this is the interesting case.

The **Gauss method** consists of the following steps:

(1) *Write the augmented matrix $\bar{A}$ of the system (S).*

(2) *Apply elementary operations on rows for $\bar{A}$ to get to an echelon form A'.*

(3) *Use the Kronecker-Capelli Theorem to decide if the system is compatible or not.*

(4) *If compatible, write and solve the system corresponding to the echelon form, starting with the last equation.*

Remark 3.8.1 (1) Actually, the Gauss method simulates working with equations. When we apply an elementary operation on the rows of $\bar{A}$, say multiply a row by a scalar and add it to another row, in fact we multiply an equation by a scalar and add it to another equation. That is why it is important to apply elementary operations only on rows, in order not to interchange the order of the unknowns.

(2) The initial system and the system corresponding to the echelon form are equivalent, that is, they have the same solutions. The great advantage is that the last system can be easily solved, starting with the last equation.

(3) The Gauss method includes checking compatibility, done by the Kronecker-Capelli Theorem.

(4) If the system is compatible, we have a principal determinant of order $r = \operatorname{rank}(\bar{A}) = \operatorname{rank}(A)$ and it is possible to continue the procedure on the matrix A' to get to a diagonal form having r elements on the principal diagonal and all the other elements zero. Then, when writing the equivalent system, in fact we directly get the solution. This completion of the Gauss method is called the *Gauss-Jordan method*.

Example 3.8.2 (a) Consider the system

$$\begin{cases} x + y - z = 2 \\ 3x + 2y - 2z = 6 \\ -x + y + z = 0 \end{cases}$$

with real coefficients. Then its augmented matrix is

$$\bar{A} = \begin{pmatrix} 1 & 1 & -1 & 2 \\ 3 & 2 & -2 & 6 \\ -1 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & -1 & 2 \\ 0 & -1 & 1 & 0 \\ 0 & 2 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & -1 & 2 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

Since $\operatorname{rank}(\bar{A}) = 3 = \operatorname{rank}(A)$, the system is determinate compatible. The equivalent system is

$$\begin{cases} x + y - z = 2 \\ \quad -y + z = 0 \\ \qquad 2z = 2. \end{cases}$$

We immediately get the solution $x = 2$, $y = 1$, $z = 1$.

We could have got to the same solution by continuing with the Gauss-Jordan method. Indeed,

$$\bar{A} \sim \begin{pmatrix} 1 & 1 & -1 & 2 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & -1 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

whence we immediately read the solution $x = 2$, $y = 1$, $z = 1$.

(b) Consider the system

$$\begin{cases} x + y + z = 0 \\ x + 4y + 10z = 3 \\ 2x + 3y + 5z = 1 \end{cases}$$

with real coefficients. Then its augmented matrix is

$$\bar{A} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 4 & 10 & 3 \\ 2 & 3 & 5 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 3 & 9 & 3 \\ 0 & 1 & 3 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 3 & 1 \\ 0 & 1 & 3 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Since $\operatorname{rank}(\bar{A}) = 2 = \operatorname{rank}(A)$, the system is non-determinate compatible. The equivalent system is

$$\begin{cases} x + y + z = 0 \\ \quad y + 3z = 1. \end{cases}$$

Then x and y are principal unknowns and z is a secondary unknown. We immediately get the solution

$$\begin{cases} x = 2z - 1 \\ y = 1 - 3z \\ z \in \mathbb{R}. \end{cases}$$

We could have got to the same solution by continuing with the Gauss-Jordan method. Indeed,

$$\bar{A} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 & -1 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The equivalent system is

$$\begin{cases} x - 2z = -1 \\ y + 3z = 1 \end{cases}$$

whence we get the solution

$$\begin{cases} x = 2z - 1 \\ y = 1 - 3z \\ z \in \mathbb{R}. \end{cases}$$

(c) Consider the system

$$\begin{cases} x+y+z=3 \\ x-y+z=1 \\ -2x+y-2z=-3 \\ x+z=4 \end{cases}$$

with real coefficients. Then its augmented matrix is

$$\bar{A} = \begin{pmatrix} 1 & 1 & 1 & 3 \\ 1 & -1 & 1 & 1 \\ -2 & 1 & -2 & -3 \\ 1 & 0 & 1 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 3 \\ 0 & -2 & 0 & -2 \\ 0 & 3 & 0 & 3 \\ 0 & -1 & 0 & 1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 1 & 1 & 3 \\ 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 3 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 3 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Since $\operatorname{rank}(\bar{A}) = 3$ and $\operatorname{rank}(A) = 2$, the system is not compatible.

Remark 3.8.3 Following [Robbiano], let us analyze how many operations are required to solve a linear system of equations $Ax = b$ with $A \in M_n(K)$ invertible by the Gauss method. We assume that the operations of interchanging rows are negligible.

Let us first compute the cost of the reduction to a triangular echelon form having all elements on the principal diagonal equal to 1. We may assume that $a_{11} \neq 0$. We reduce a_{11} to 1 by dividing the first row of A by a_{11}. Then we produce zeros on the first column under the $(1,1)$-entry. For each of the $n-1$ rows we need n multiplications and n additions. Adding the corresponding operations for b, we have 1 more division, $n-1$ more multiplications and $n-1$ more additions. After finishing working with the first row, we move on to the second row, and so on til we get the required triangular form with elements 1 on the principal diagonal. Counting up the operations we have

- $n + (n-1) + \cdots + 1$ divisions on A and n divisions on b;
- $n(n-1) + (n-1)(n-2) + \cdots + 2 \cdot 1$ multiplications on A and $(n-1) + \cdots + 1$ multiplications on b;
- $n(n-1) + (n-1)(n-2) + \cdots + 2 \cdot 1$ additions on A and $(n-1) + \cdots + 1$ additions on b.

So far we have

- $\frac{n(n+1)}{2} + n$ divisions;
- $\frac{n^3-n}{3} + \frac{n(n-1)}{2}$ multiplications;
- $\frac{n^3-n}{3} + \frac{n(n-1)}{2}$ additions.

Now let us compute the cost of substitutions in the reduced triangular system. From the last equation we already have the unknown x_n. For the substitution on the previous but last equation to find x_{n-1} we need 1 multiplication and 1 addition. Continuing the procedure, for the first equation to find x_1 we need $n-1$ multiplications and $n-1$ additions. Counting up the operations, we have

- $(n-1) + \cdots + 1 = \frac{n(n-1)}{2}$ multiplications;
- $(n-1) + \cdots + 1 = \frac{n(n-1)}{2}$ additions.

Adding up the numbers of operations from the above two stages, it turns out that one needs:

(1) $\frac{n(n+1)}{2} + n$ divisions;

(2) $\frac{n^3-n}{3} + n(n-1)$ multiplications;

(3) $\frac{n^3-n}{3} + n(n-1)$ additions.

Hence the order of magnitude is $\frac{2}{3}n^3$ operations.

Extra: LU decomposition and Gauss method (see [Crivei])

Extra: Simple authentication scheme

Let us consider the following simple authentication scheme from cryptography, following [Klein]. We denote by E the canonical basis of the canonical vector space $\mathbb{Z}_2^n$ over $\mathbb{Z}_2$.

- The password is a vector $v = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$.
- As a challenge, Computer sends a random vector $u = (u_1, \ldots, u_n) \in \mathbb{Z}_2^n$.
- As the response, Human sends back the dot-product vector

$$u \cdot v = u_1 x_1 + \cdots + u_n x_n \in \mathbb{Z}_2.$$

- The challenge-response interaction is repeated until Computer is convinced that Human knows password v.

Eve eavesdrops and learns m pairs (a_1, b_1), $\ldots$, (a_m, b_m) such that each b_i is the correct response to challenge a_i. For every $i \in \{1, \ldots, m\}$, denote $a_i = (a_{i1}, \ldots, a_{in})$.
Then the password $v = (x_1, \ldots, x_n)$ is a solution of the linear system of equations:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

Once the rank of the matrix of the system reaches n, the solution is unique, and Eve can use the Gauss method to find it, obtaining the password.