Chapter 1. Linear equations

Review of matrix theory

Fields

System of linear equations

Row-reduced echelon form

Invertible matrices

Fields

- Field F, +, •
  F is a set. +:FxF➜F, •:FxF➜F
  - x+y = y+x, x+(y+z)=(x+y)+z
  - $\exists$ unique 0 in F s.t. x+0=x
  - $\forall x \in F, \exists$ unique -x s.t. x+(-x) = 0
  - xy=yx, x(yz)= (xy)z
  - $\exists$ unique 1 in F s.t. x1 = x
  - $\forall x \in F - \{0\}, \exists$ unique x^{-1} s.t. $xx^{-1} = 1$
  - x(y+z) = xy+yz

- A field can be thought of as generalizations of real numbers useful for some other purposes which has all the important properties of real numbers. There are many nontrivial examples.
- To verify something is a field, we need to show that the axioms are satisfied.
  - Example:
  - Real number field R
  - Complex number field $\mathbf{C} = \{x + yi | x, y \in \mathbf{R}\}$
  - The field of rational numbers Q

    (We learn this already. Verify it!)
  - The set of natural numbers N is not a field.
    - For example 2x z = 1 for no z in N.
  - The set of real valued 2x2 matrices is not a field.
    - For example   for no A.

$$\begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} A = I$$

- $$\mathbf{Z}_p = \{0, 1, 2, \ldots, p\}$$

$x + y = z(\text{mod} \quad p) z \in \mathbf{Z_p}$ is the remainder of $x + y$ under the division by p

$xy = t(\text{mod} \quad p) t \in \mathbf{Z_p}$ is the remainder of xy under the division by p

  – For p =5, 9=4 mod 5. 1+4 = 0 mod 5.
    3 4 = 2 mod 5. 3 2 = 1 mod 5.

  – If p is not prime, then the above is not a field. For example, let p=6. 2.3= 0 mod 6. If 2.x = 1 mod 6, then 3=1.3=2.x.3=2.3.x=0.x=0.
    A contradiction.

  – If p is a prime, like 2,3,5,…, then it is a field. The proof follows:

0 and 1 are obvious. For each x, -x equals p-x.

For $x \in \mathbf{Z}_p - \{0\}, gcd(x, p) = 1. \exists a, b \in \mathbf{Z}$ s.t. $ax + bp = 1$.

Let $a' = a, b' = b \bmod p$. Then $a'x + b'p = 1 \bmod p$. and $a'x = 1 \bmod p$.

Thus a' is the inverse of x.

Other axioms are easy to verify by following remainder rules well.

In fact, only the multiplicative inverse axiom fails if p is not a prime.

- A characteristic of a field is the smallest number p such that p.1=1+…+1 = 0. p is always a prime. If no p exists, then the characteristic is defined to 0.

- A subfield F' of a field F is a subset where F' contains 0, 1, and the operations preserve F' and inverses are in F'.

  - Example:

    $$Q \subset R \subset C$$

    $$Q + Qi = \{x + yi \,|\, x, y \in Q\} \subset C$$
    $$Q + Q\sqrt{2} = \{x + y\sqrt{2} \,|\, x, y \in Q\} \subset \mathbf{R}$$

  - A subfield F'' of a subfield F' of a field F is a subfield of F.

A system of linear equations

- Solve for $x_1, x_2, \ldots, x_n \in F$ given $A_{ij} \in F, y_j \in F$

$$
\begin{array}{ccccccc}
A_{11}x_1 + & A_{12}x_2 + & \cdots + & A_{1n}x_n & = & y_1 \\
A_{21}x_1 + & A_{22}x_2 + & \cdots + & A_{2n}x_n + & = & y_2 \\
\vdots & \vdots & \ddots & \vdots & & \vdots \\
A_{m1}x_1 + & A_{m2}x_2 + & \cdots & A_{mn}x_n & = & y_m
\end{array}
$$

$$
\begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \text{ or } AX = Y
$$

- This is homogeneous if $y_i = 0$ for $i = 1, \ldots, m$
- To solve we change to easier problem by row operations.

Elementary row operations

- – Multiplication of one row of A by a scalar in F.
- – Replacement of r th row of A by row r plus c times s th row of A (c in F, r ≠ s)
- – Interchanging two rows

- An inverse operation of elementary row operation is a row operation,

- Two matrices A, B are row-equivalent if one can make A into B by a series of elementary row operations. (This is an equivalence relation)

$$(1) A \sim A, (2) A \sim B \leftrightarrow B \sim A, (3) A \sim B, B \sim C \rightarrow A \sim C$$

- Theorem: A, B row-equivalent mxn matrices. AX=0 and BX=0 has the exactly same solutions.

- Definition: mxn matrix R is row-reduced if
  - The first nonzero entry in each non-zero row of R is 1.
  - Each colume of R which contains the leading non-zero entry of some row has all its other entries 0

- Definition: R is a row-reduced echelon matrix if
  - R is row-reduced
  - Zero rows of R lie below all the nonzero rows
  - Leading nonzero entry A_{ik_i} of row i:

$$k_1 < k_2 < \cdots < k_r, 1 \le k_j \le n$$

(r ≤ n since strictly increasing)

$$\begin{pmatrix} 1 & 1 & i & 0 \\ 0 & 2 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & i & 0 \\ 0 & 2 & 0 & 1 \\ 0 & -1 & -i & 0 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} 1 & 0 & i & -1/2 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & -i & 1/2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & -i & 1/2 \end{pmatrix} \rightarrow \cdots$$

- The main point is to use the first nonzero entry of the rows to eliminate entries in the colume. Sometimes, we need to exchange rows. This is algorithmic.

- In this example: $k_1 = 1, k_2 = 2, k_3 = 3$

- Theorem: Every mxn matrix A is row-equivalent to a row-reduced echelon form.

- **Analysis of RX=0. R mxn matrix**
  - Let r be the number of nonzero rows of R. Then r $\leq$ n
  - Take k_i Variables of X: $x_{k_1}, x_{k_2}, \ldots, x_{k_r}$
  - Remaining variables of X: $u_1, u_2, \ldots u_{n-r}$
  - RX=0 becomes

$$
\begin{aligned}
x_{k_1} & & + & \sum_{j=1}^{n-r} C_{1j} u_j & = 0 \\
& x_{k_2} & + & \sum_{j=1}^{n-r} C_{2j} u_j & = 0 \\
& \ddots & + & \vdots & = \vdots \\
& x_{k_r} & + & \sum_{j=1}^{n-r} C_{rj} u_j & = 0
\end{aligned}
$$

  - All the solutions are obtained by assigning any values whatsoever to $u_1, u_2, \ldots u_{n-r}$
  - If r < n, n-r is the dimension of the solution space.
  - If r = n, then only X=O is the solution.

- Theorem 6: A mxn m< n. Then AX=0 has a nontrivial solutions.
- Proof:
  - R r-r-e matrix of A.
  - AX=0 and RX=0 has same solutions.
  - Let r be the number of nonzero rows of R.
  - $r \leq m < n$.
- Theorem 7. A nxn. A is row-equivalent to I iff AX=0 has only trivial solutions.
- Proof: ➜ AX=0, IX=0 has same solutions.
  - ⬅ AX=0 has only trivial solutions. So does RX=0.
  - Let r be the no of nonzero rows of R.
  - $r \geq n$ since RX=0 has only trivial solutions.
  - But $r \leq n$ always. Thus r=n.
  - R has leading 1 at each row. R = I.

- Matrix multiplications $C = AB, c_{ij} = \sum_{r=1}^{n} A_{ir} B_{rj}$

$$I = (\delta_{ij}), IA = A = AI, O.A = O = A.O$$

- A(BC) = (AB)C A: mxn B:nxr C:rxk
- Elementary matrix E (nxn) is obtained from I by a single elementary move.

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ c & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} d & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- Theorem 9: e elementary row-operation E mxm elementary matrix E = e(I). Then e(A)=E.A= e(I).A.

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

- **Corollary:** A, B mxn matrices. B is row-equivalent to A iff B=PA where P is a product of elementary matrices

Invertible matrices

- A nxn matrix.
  - If BA = I B nxn, then B is a left inverse of A.
  - If AC=I C nxn, then C is a right inverse of A
  - B s.t. BA=I=AB. B is the inverse of A
  - We will show finally, these notions are equivalent.
- Lemma: If A has a left inverse B and a right inverse C, then B = C.
  - Proof:B=BI=B(AC)=(BA)C=IC=C.

- **Theorem**: A, B nxn matrices.
  - (i) If A is invertibe, so is A^{-1}. $(A^{-1})^{-1}=A$.
  - (ii) If both A,B are invertibe, so is AB and $(AB)^{-1}=B^{-1}A^{-1}$.
  - Products of invertible matrices are invertible.
- **Theorem**: An elementary matrix is invertible. e an operation, e_1 inverse operation. Let $E = e(I)$. $E_1=e_1(I)$. Then $EE_1=e(E_1)= e(e_1(I))=I$. $E_1E=e_1(e(I))=I$.

- Theorem 12: A nxn matrix. TFAE:
  - (I) A is invertible.
  - (ii) A is row-equivalent to I.
  - (iii) A is a product of elementary matrices.
- proof:
  - Let R be the row reduced echelon matrix of A.
  - $R = E_k \ldots E_1 A$. $A = E_1^{-1} \ldots E_k^{-1} R$.
  - A is inv iff R is inv.
  - R is inv iff R=I
    - (($\rightarrow$) if R$\neq$I. Then exists 0 rows. R is not inv.($\leftarrow$) R=I is invertible.)
    - Fact: R = I iff R has no zero rows.

- Corollary: A $\rightarrow$ I by a series of row operations. Then I $\rightarrow$ A^{-1} by the same series of operations.
  - Proof:
    - I = $E_k \ldots E_1 A$.
    - By multiplying both sides by A^{-1} .
    - A^{-1}= $E_k \ldots E_1$. Thus, A^{-1}= $E_k \ldots E_1 I$.

$$\begin{pmatrix} 1 & i & 1 & | & 1 & 0 & 0 \\ 0 & 1 & 2 & | & 0 & 1 & 0 \\ 0 & 1 & 1 & | & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1-2i & | & 1 & -i & 0 \\ 0 & 1 & 2 & | & 0 & 1 & 0 \\ 0 & 0 & -1 & | & 0 & -1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & | & 1 & -1+i & 1-2i \\ 0 & 1 & 0 & | & 0 & -1 & 2 \\ 0 & 0 & -1 & | & 0 & -1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & | & 1 & -1+i & 1-2i \\ 0 & 1 & 0 & | & 0 & -1 & 2 \\ 0 & 0 & 1 & | & 0 & 1 & -1 \end{pmatrix}$$

- **Corollary**: A,B mxn matrices
  B is row-equivalent to A iff B=PA for an invertible mxm matrix P.

- **Theorem 13**: A nxn TFAE
  - (i) A is invertible
  - (ii) AX=O has only trivial solution.
  - (iii) AX=Y has a unique solution for each nx1 matrix Y.

- Proof: By Theorem 7, (ii) iff A is row-equiv. to I. Thus, (i) iff (ii).
  - (ii) iff (iii) ➔ A is invertible. AX=Y. Solution $Y=A^{-1}X$.

- • ← Let R be r-r-e of A. We show R=I.
  - – We show that the last row of R is not O.
  - – Let E=(0,0,..,1) nx1 colume matrix.
  - – If RX=E is solvable, then the last row of R is not O.
  - – R=PA➜A=P^{-1}R.
  - – RX=E iff AX=P^{-1}E which is always solvable by the assumption (iii).

- **Corollary**: nxn matrix A with either a left or a right inverse is invertible.
- Proof:
  - Suppose A has a left inverse.
    - $\exists B, BA = I.$
    - AX=0 has only trivial solutions. By Th 13, done.
      - BAX=0 -> X=0.
  - Suppose A has a right inverse.
    $\exists C, AC = I.$
    - C has a left-inverse A.
    - C is invertible by the first part. $C^{-1}=A$.
    - A is invertible.