CSCE 785

9/5/2023

Linear Algebra over $\mathbb{Z}_2$ ($\mathbb{F}_2$) ①

For any field F, $n>0$, $1 \le i \le n$

$(n \times 1)$ matrix (column vector) $e_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ ← ith place

$\{e_i : 1 \le i \le n\}$ is the standard basis for F^n

$m > 0$: $1 \le j \le m$

$$e_i^T e_j = \overbrace{\begin{bmatrix} \cdots & 1 & \cdots \end{bmatrix}}^{m} \left.\begin{bmatrix} \vdots \\ 1 \\ \vdots \end{bmatrix}\right\}n = [\delta_{ij}]$$

conformant iff $m = n$

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \ne j \end{cases}$$

"Kronecker δ"

always conformant

$$E_{ij} := e_i e_j^T = n\left\{\begin{bmatrix} 1 \end{bmatrix}\right. \overbrace{\begin{bmatrix} & 1 & \end{bmatrix}}^{m} = \begin{array}{c} \quad j\text{th column} \\ n\begin{bmatrix} & 0 & \downarrow & 0 & \\ 0 & & 1 & & 0 \\ & & 0 & & \end{bmatrix} \leftarrow i\text{th row} \\ m \end{array}$$

$\{E_{ij} : 1 \le i \le n, 1 \le j \le m\}$ is the standard basis for $\underbrace{F^{n \times m}}_{n \times m \text{ matrices over } F}$

Let $F := \mathbb{Z}_2$.

Elementary Row & column operations

elementary matrix $R_{ij} := I + E_{ij} = \begin{array}{c c} & \begin{array}{c} j \\ \downarrow \end{array} \\ i \rightarrow & \begin{bmatrix} 1 & & \\ & \ddots & 1 \\ & & 1 \end{bmatrix} \end{array}$

$I_n = I = \underbrace{\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}}_{n \times n}$ identity matrix

Elementary Row op

$$R_{ij} \overbrace{\begin{bmatrix} & & \\ & & \end{bmatrix}}^{M} = \overbrace{\begin{bmatrix} \text{Replace } \cancel{\text{ith}} \text{ ith row of } M \text{ with the sum of the ith \& jth rows} \end{bmatrix}}^{M}$$

~~F~~ Fact: $E_{ij}E_{kl} = \begin{cases} E_{il} & \text{if } j = k \\ 0 & \text{otherwise} \end{cases}$

Elementary column ops

$$\overbrace{\begin{bmatrix} & & \\ & & \end{bmatrix}}^{M} R_{ij} = \overbrace{\begin{bmatrix} \text{Replace jth column with the sum of the ith \& jth columns} \end{bmatrix}}^{M}$$

$i \neq j$ iff R_{ij} is invertible

$R_{ij}R_{ij} = (I + E_{ij})(I + E_{ij})$
$= I + E_{ij} + E_{ij} + E_{ij}E_{ij}$
$= I$
$\therefore R_{ij} = R_{ij}^{-1}$

Given any $M \in \mathbb{Z}_2^{m \times n}$

There exists a sequence of elementary matrices (invertible) R, S s.t. $RMS = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right]$

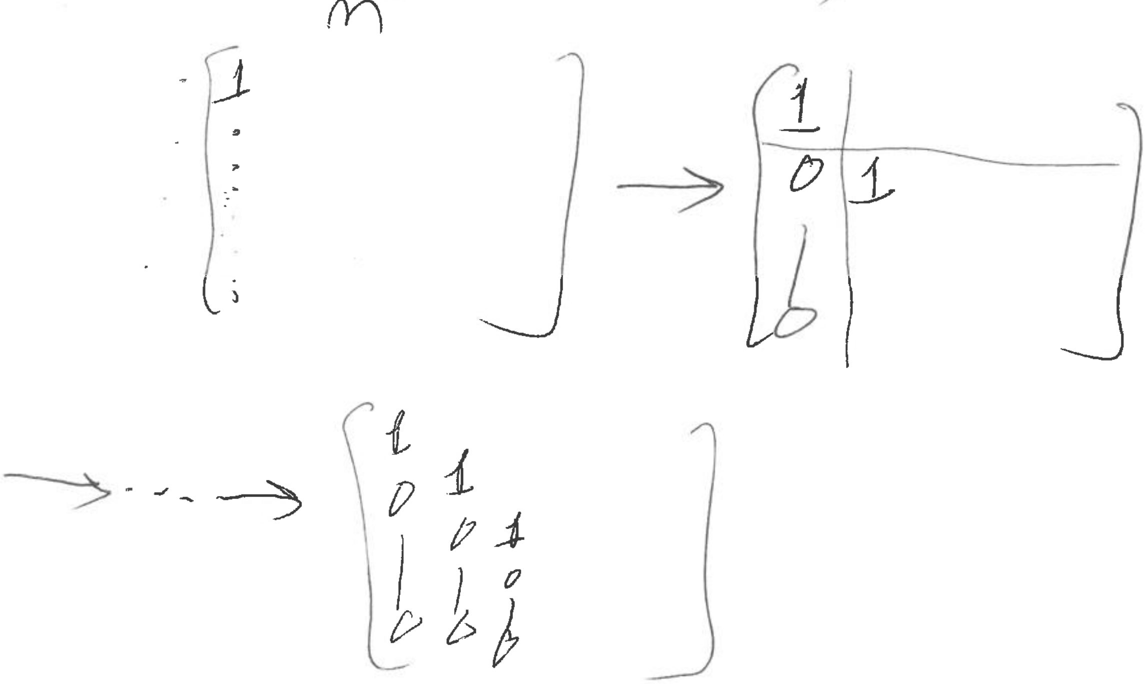
where $R = \prod R_{ij}$ products of elementary matrices

$S = \prod R_{ij}$

and $\quad RMS = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right]$

r is uniquely determined by M

$(r = \text{rank}(M))$



Hilbert spaces:

Def: A Hilbert space $\mathcal{H}$ is a vector space over $\mathbb{C}$ together with an "inner product"

$$\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$$

satisfying the following axioms: $\forall a \in \mathbb{C}$, $\forall u, v, w \in \mathcal{H}$

1a. $\langle u, v+w\rangle = \langle u,v\rangle + \langle u,w\rangle$
1b. $\langle u, av\rangle = a\langle u,v\rangle$
$\langle \cdot,\cdot\rangle$ is <u>linear</u> in the 2nd argument

2. $\langle u,v\rangle = \langle v,u\rangle^*$
$\langle \cdot,\cdot\rangle$ is <u>conjugate symmetric</u>

<u>Note:</u> $\langle u,u\rangle = \langle u,u\rangle^*$ $\therefore \langle u,u\rangle \in \mathbb{R}$

$[\mathbb{R} = \{z \in \mathbb{C} : z = z^*\}]$

3a. $\langle u,u\rangle \geq 0$
3b. $\langle u,u\rangle = 0 \Rightarrow u=0$
$\langle \cdot,\cdot\rangle$ is <u>positive definite</u>

<u>Define</u> $\|u\| = \sqrt{\langle u,u\rangle}$ (<u>norm</u> of u)

4. $\mathcal{H}$ is <u>complete</u> with respect to $\|\cdot\|$ (every Cauchy sequence converges)

[4 only needed if $\mathcal{H}$ is infinite dimensional. Finite dimensional Hilbert spaces are complete without needing axiom (4).]

<u>Define</u>: A <u>$\mathbb{C}$-space</u> is a finite dimensional Hilbert space

Some facts:

1. $\langle u+v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$

Proof:

$$\langle u+v, w\rangle = \langle w, u+v\rangle^*$$

$$= \left(\langle w, u\rangle + \langle w, v\rangle\right)^*$$

$$= \langle w, u\rangle^* + \langle w, v\rangle^*$$

$$= \langle u, w\rangle^{**} + \langle v, w\rangle^{**}$$

$$= \langle u, w\rangle + \langle v, w\rangle \quad \checkmark$$

$\boxed{\begin{array}{l} \cancel{z,w}\ x, y \in \mathbb{C} \\ (x+y)^* \\ = x^* + y^* \end{array}}$

2. $\langle au, v\rangle = a^* \langle u, v\rangle$

Proof: $\langle au, v\rangle = \langle v, au\rangle^* = \left(a\langle v, u\rangle\right)^*$

$$= a^* \langle v, u\rangle^* = a^* \langle u, v\rangle \quad \checkmark$$

$\boxed{\begin{array}{l} (xy)^* = x^* y^* \\ \text{(check)} \end{array}}$

$\langle \cdot, \cdot \rangle$ is conjugate linear

in the 1st argument

3. $\|u+v\| \leq \|u\| + \|v\|$ ($\|\cdot\|$ is subadditive)

with equality holding ~~iff~~ only if u, v are lin. dependent.

4. $\|au\| = |a| \cdot \|u\|$

Pf: $\|au\|^2 = \langle au, au \rangle = \underline{a^* a} \langle u, u \rangle$

$= |a|^2 \|u\|^2$

Take $\sqrt{\ }$ of both sides. ✓

Let $\mathcal{H} := \mathbb{C}^n$ $(n > 0)$

and define $\underline{\langle e_i, e_j \rangle} := \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

~~Let~~ $u, v \in \mathbb{C}^n$

$u = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}$ $\quad v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$ $\quad u_1, \ldots, u_n, v_1, \ldots, v_n \in \mathbb{C}$

$u = \sum_{j=1}^{n} u_j e_j \quad v = \sum_{k=1}^{n} v_k e_k$

$$\therefore \langle u, v \rangle = \left\langle \sum_j u_j e_j \, , \, \sum_k v_k e_k \right\rangle$$

$$= \cdots = \sum_k v_k \left\langle \sum_j u_j e_j \, , e_k \right\rangle$$

$$= \sum_{j,k} u_j^* v_k \underbrace{\langle e_j \, , e_k \rangle}_{\delta_{jk}}$$

$$= \sum_j u_j^* v_j = \underbrace{\begin{bmatrix} u_1^* & \cdots & u_n^* \end{bmatrix}}_{u^*} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = u^* v$$

Def: Let $A \in \mathbb{C}^{m \times n}$

Define the adjoint (Hermitian conjugate) of A, A^* ~~by~~ as the conjugate transpose of A (transpose A & complex conjugate each entry)