Mathematical Toolkit Assignment

Yota Toyama

October 19, 2016

1. (a)

$$dim(A) = rank(A) + null(A)$$
$$n = m + null(A)$$
$$null(A) = n - m$$

   (b)

$$null(A) = dim(\ker(A))$$

Then, $\ker(A)$ can have a basis B s.t. $\mathrm{Span}(B) = \ker(A)$. i.e.

$$\forall \mathbf{v} \in \ker(A), \exists a_1, ..., a_{n-m} \in \mathbb{F}_2,$$
$$\mathbf{v} = a_1\mathbf{b}_1 + \cdots + a_{n-m}\mathbf{b}_{n-m} (b_i \in B)$$

$\therefore$ The answer is 2^{n-m}.

   (c)

$$\forall \mathbf{x} \text{ s.t. } \begin{cases} A\mathbf{x} = \mathbf{b} \\ A\mathbf{x_0} = \mathbf{b} \end{cases}$$
$$\therefore \ A(\mathbf{x} - \mathbf{x}_0) = 0$$
$$\mathbf{x} - \mathbf{x}_0 \in \ker(A)$$

Then, choosing each element of $\mathbf{x}$ carefully (1 or 0), $\mathbf{x} - \mathbf{x}_0$ can be any element of $\mathbb{F}_2^n$.

$$\therefore \ \{\mathbf{x} - \mathbf{x}_0 | A\mathbf{x} = b\} = \ker(A)$$

$\therefore \mathbf{x} - \mathbf{x}_0$ has 2^{n-m} solutions.
$\therefore \mathbf{x}$ has 2^{n-m} solutions.

2. (a)

$$f(c\mathbf{v} + (-c)\mathbf{v}) \geq \min\{f(\mathbf{v}), f(\mathbf{v})\}$$
$$\therefore \ f(\mathbf{0}_V) \geq f(\mathbf{v})$$

(b) Because every element $\mathbf{v}_t \in V_t$ is in V by definition.

$$V_t \subseteq V$$

3.

$$\begin{aligned} p(x) &= x^2 + bx + c \\ &= (x - r_1)(x - r_2) \\ &= x^2 - (r_1 + r_2)x + r_1 r_2 \end{aligned}$$

$$\therefore \; b = -r_1 - r_2, c = r_1 r_2$$

4.

$$\begin{aligned} \mu(P, Q) &= degree(PQ) \\ &= degree(QP) \\ &= \mu(Q, P) \end{aligned}$$

$$\begin{aligned} \mu(0, 0) &= degree(0) \\ &= 0 \end{aligned}$$

$$\begin{aligned} &\forall P \neq 0, \\ &\mu(P, P) = degree(P^2) \\ &\qquad\quad = 2degree(P) \\ &\qquad\quad > 0 \end{aligned}$$

$$\begin{aligned} \mu(P + Q, R) &= degree((P + Q)R) \\ &= \max \{degree(P), degree(Q)\} + degree(R) \end{aligned}$$

$$\begin{aligned} \mu(P, R) + \mu(Q, R) &= \max \{degree(P) + degree(R), degree(Q) + degree(R)\} \\ &= \max \{degree(P), degree(Q)\} + degree(R) \end{aligned}$$

$$\therefore \; \mu(P + Q, R) = \mu(P, R) + \mu(P, Q)$$

$$\begin{aligned} &c \in \mathbb{R}, \\ &\mu(cP, R) = degree(cPR) \\ &\qquad\qquad = degree(PR) \\ &\qquad\qquad \neq c \cdot degree(P, R) \end{aligned}$$

$\therefore \mu(\cdot, R)$ is not a LT.
$\therefore \mu$ is not a IP.

5.

$$\begin{aligned}\alpha\beta\mathbf{x} &= \lambda\mathbf{x}\\ \beta\alpha\beta\mathbf{x} &= \beta(\lambda\mathbf{x})\\ \beta\alpha(\beta\mathbf{x}) &= \lambda(\beta\mathbf{x})\end{aligned}$$

$\therefore \lambda$ is an eigenvalue of $\beta\alpha$.

6. (a)

$$\begin{gathered}\varphi(\mathbf{v}) = \lambda\mathbf{v}\\ \varphi(\mathbf{v}) = \lambda\varphi(\mathbf{v})\\ (\lambda - 1)\varphi(\mathbf{v}) = 0\\ \lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) = 0\\ \lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) = 0_{\mathbb{F}}\mathbf{v}\\ \therefore\ \lambda \in \{0_{\mathbb{F}}, 1_{\mathbb{F}}\}\end{gathered}$$

   (b) Let $\forall\mathbf{v}, \varphi(\mathbf{v}) = \mathbf{v}_0$. ($\mathbf{v}_0$ is fixed.)
   Then assume $\varphi = \varphi^*$.
   If $\mathbf{v} \neq \mathbf{w} \in V$,

$$\begin{gathered}\langle \mathbf{v}_0, \mathbf{w}\rangle = \langle \mathbf{v}, \varphi^*(\mathbf{w})\rangle\\ \langle \mathbf{v}_0, \mathbf{w}\rangle = \langle \mathbf{v}, \mathbf{v}_0\rangle\\ \langle \mathbf{w}, \mathbf{v}_0\rangle = \langle \mathbf{v}, \mathbf{v}_0\rangle\\ \mathbf{v} = \mathbf{w}\end{gathered}$$

   This is contradition.
   $\therefore$ not always $\varphi = \varphi^*$.

7. (a)

$$\begin{gathered}\langle \varphi(\mathbf{v}), \mathbf{w}\rangle = \langle \mathbf{v}, \varphi^*(\mathbf{w})\rangle\\ \langle \varphi^*(\mathbf{w}), \mathbf{v}\rangle = \langle \mathbf{w}, \varphi(\mathbf{w})\rangle\\ \therefore\ (\varphi^*)^* = \varphi\end{gathered}$$

(b)

$$\begin{gathered}
\forall \mathbf{v} \in \ker(\varphi), \varphi(\mathbf{v}) = 0 \\
\forall \mathbf{v'} \in (\mathrm{im}(\varphi^*))^{\perp}, \forall \mathbf{w} \in W, \\
\langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle = 0 \\
\langle \varphi(\mathbf{v}), \mathbf{w} \rangle = 0 \\
\therefore \quad \text{if } \mathbf{v} \in \ker(\varphi), \\
\varphi(\mathbf{v}) = 0 \therefore \ \forall \mathbf{w}, \langle \varphi(\mathbf{v}), \mathbf{w} \rangle = 0 \\
\langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle = 0 \\
\mathbf{v} \in (\mathrm{im}(\varphi^*))^{\perp}
\end{gathered}$$

(c)

$$\begin{gathered}
\forall \mathbf{v} \in V \\
\text{If } \mathbf{w} \in \mathrm{im}(\varphi), w = \varphi(\mathbf{v}) \\
\langle \varphi(\mathbf{v}), \mathbf{w'} \rangle = \langle \mathbf{v}, \varphi(\mathbf{w'}) \rangle = 0 \\
\therefore \ \mathbf{w} \in (\ker(\varphi^*))^{\perp} \\
\text{If } \mathbf{w} \in (\ker(\varphi^*))^{\perp}, \\
\forall \mathbf{w'} \in W \text{ s.t. } \varphi^*(\mathbf{w'}) = 0_V, \langle \mathbf{w}, \mathbf{w'} \rangle = 0 \\
\forall \mathbf{v} \in V, \langle \mathbf{v}, \varphi^*(\mathbf{w'}) \rangle = 0 \\
\langle \varphi(\mathbf{v}), \mathbf{w'} \rangle = 0 \quad \therefore \ \mathbf{w} \in \mathrm{im}(\varphi) \\
\varphi(\mathbf{v}) = \mathbf{w}
\end{gathered}$$

(d)

$$\begin{aligned}
rank(\varphi) &= dim(\mathrm{im}(\varphi)) \\
&= dim((\ker(\varphi^*))^{\perp}) \\
&= dim(W) - dim(\ker(()\varphi^*)) \\
&= dim(im(\varphi^*)) \\
&= rank(\varphi^*)
\end{aligned}$$

(e)

$$\text{Let } A = BC, B \in \mathbb{C}^{m \times r}, C \in \mathbb{C}^{r \times n}$$

$$\begin{aligned}
\text{then } A_{i,:} &= \sum_{j=1}^{r} B_{i,j} C_{i,:} \\
A_{:,i} &= \sum_{j=1}^{r} C_{j,i} B_{:,i}
\end{aligned} \quad \therefore \quad \left\{ rank_{row}(A) \leq rank_{row}(C) \leq r rank_{column}(A) \leq rank_{column}(B) \leq r \right.$$

Choose a minimal r.
Then rows of C form a minimal spanning set of rows of A.
And, columns of C form a minimal spanning set of columns of A.
$\therefore$ r is the rank of both row and column spaces of A.

$$\therefore \; rank_{row}(A) = rank_{column}(A)$$