Mathematical Toolkit Assignment

Yota Toyama

October 19, 2016

1. (a)

$$\begin{aligned} dim(A) &= rank(A) + null(A) \quad (1) \\ n &= m + null(A) \quad (2) \\ null(A) &= n - m \quad (3) \end{aligned}$$

(b)

$$null(A) = dim(ker(A)) \quad (4)$$

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

$$\forall \mathbf{v} \in ker(A), \exists a_1, ..., a_{n-m} \in \mathbb{F}_2, \quad (5)$$

$$\mathbf{v} = a_1\mathbf{b_1} + \cdots + a_{n-m}\mathbf{b}_{n-m}(b_i \in B) \quad (6)$$

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

(c)

$$\forall \mathbf{x} \text{s.t.} \begin{cases} A\mathbf{x} = \mathbf{b} \\ A\mathbf{x_0} = \mathbf{b} \end{cases} \quad (7)$$

$$\therefore \quad A(\mathbf{x} - \mathbf{x}_0) = 0 \quad (8)$$

$$\mathbf{x} - \mathbf{x}_0 \in ker(A) \quad (9)$$

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

$$\therefore \quad \{\mathbf{x} - \mathbf{x}_0 | A\mathbf{x} = b\} = ker(A) \quad (10)$$

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

2. (a)

$$f(c\mathbf{v} + (-c)\mathbf{v}) \geq \min\{f(\mathbf{v}), f(\mathbf{v})\} \quad (11)$$

$$\therefore \quad f(\mathbf{0}_V) \geq f(\mathbf{v}) \quad (12)$$

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

$$V_t \subseteq V \tag{13}$$

3.

$$\begin{align}
p(x) &= x^2 + bx + c \tag{14}\\
&= (x - r_1)(x - r_2) \tag{15}\\
&= x^2 - (r_1 + r_2)x + r_1 r_2 \tag{16}\\
\tag{17}
\end{align}$$

$$\begin{align}
\therefore\ b = -r_1 - r_2, c = r_1 r_2 \tag{18}\\
\tag{19}
\end{align}$$

4.

$$\begin{align}
\mu(P, Q) &= degree(PQ) \tag{20}\\
&= degree(QP) \tag{21}\\
&= \mu(Q, P) \tag{22}
\end{align}$$

$$\begin{align}
\mu(0, 0) &= degree(0) \tag{23}\\
&= 0 \tag{24}
\end{align}$$

$$\begin{align}
\forall P &\neq 0, \tag{25}\\
\mu(P, P) &= degree(P^2) \tag{26}\\
&= 2degree(P) \tag{27}\\
&> 0 \tag{28}
\end{align}$$

$$\begin{align}
\mu(P + Q, R) &= degree((P + Q)R) \tag{29}\\
&= \max\{degree(P), degree(Q)\} + degree(R) \tag{30}
\end{align}$$

$$\begin{align}
\mu(P, R) + \mu(Q, R) &= \max\{degree(P) + degree(R), degree(Q) + degree(R)\} \tag{31}\\
&= \max\{degree(P), degree(Q)\} + degree(R) \tag{32}
\end{align}$$

$$\therefore\ \mu(P + Q, R) = \mu(P, R) + \mu(P, Q) \tag{33}$$

$$\begin{align}
c &\in \mathbb{R}, \tag{34}\\
\mu(cP, R) &= degree(cPR) \tag{35}\\
&= degree(PR) \tag{36}\\
&\neq c \cdot degree(P, R) \tag{37}
\end{align}$$

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

5.

$$\begin{aligned} \alpha\beta\mathbf{x} &= \lambda\mathbf{x} \quad (38) \\ \beta\alpha\beta\mathbf{x} &= \beta(\lambda\mathbf{x}) \quad (39) \\ \beta\alpha(\beta\mathbf{x}) &= \lambda(\beta\mathbf{x}) \quad (40) \\ & \quad (41) \end{aligned}$$

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

6. (a)

$$\begin{aligned} \varphi(\mathbf{v}) &= \lambda\mathbf{v} \quad (42) \\ \varphi(\mathbf{v}) &= \lambda\varphi(\mathbf{v}) \quad (43) \\ (\lambda - 1)\varphi(\mathbf{v}) &= 0 \quad (44) \\ \lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) &= 0 \quad (45) \\ \lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) &= 0_{\mathbb{F}}\mathbf{v} \quad (46) \\ \therefore \ \lambda &\in \{0_{\mathbb{F}}, 1_{\mathbb{F}}\} \quad (47) \end{aligned}$$

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

$$\begin{aligned} \langle \mathbf{v}_0, \mathbf{w} \rangle &= \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle \quad (48) \\ \langle \mathbf{v}_0, \mathbf{w} \rangle &= \langle \mathbf{v}, \mathbf{v}_0 \rangle \quad (49) \\ \langle \mathbf{w}, \mathbf{v}_0 \rangle &= \langle \mathbf{v}, \mathbf{v}_0 \rangle \quad (50) \\ \mathbf{v} &= \mathbf{w} \quad (51) \end{aligned}$$

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

7. (a)

$$\begin{aligned} \langle \varphi(\mathbf{v}), \mathbf{w} \rangle &= \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle \quad (52) \\ \langle \varphi^*(\mathbf{w}), \mathbf{v} \rangle &= \langle \mathbf{w}, \varphi(\mathbf{w}) \rangle \quad (53) \\ \therefore \ (\varphi^*)^* &= \varphi \quad (54) \end{aligned}$$