Mathematical Toolkit Assignment

Yota Toyama

October 19, 2016

1. (a)

$$dim(A) = rank(A) + null(A) \tag{1}$$
$$n = m + null(A) \tag{2}$$
$$null(A) = n - m \tag{3}$$

(b)

$$null(A) = dim(ker(A)) \tag{4}$$

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

$$\forall \mathbf{v} \in ker(A), \exists a_1, ..., a_{n-m} \in \mathbb{F}_2, \tag{5}$$
$$\mathbf{v} = a_1\mathbf{b}_1 + \cdots + a_{n-m}\mathbf{b}_{n-m} (b_i \in B) \tag{6}$$

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

(c)

$$\forall \mathbf{x} \text{s.t.} \begin{cases} A\mathbf{x} = \mathbf{b} \\ A\mathbf{x_0} = \mathbf{b} \end{cases} \tag{7}$$
$$\therefore \ A(\mathbf{x} - \mathbf{x}_0) = 0 \tag{8}$$
$$\mathbf{x} - \mathbf{x}_0 \in ker(A) \tag{9}$$

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

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

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

2. (a)

$$f(c\mathbf{v} + (-c)\mathbf{v}) \geq \min\{f(\mathbf{v}), f(\mathbf{v})\} \tag{11}$$
$$\therefore \ f(\mathbf{0}_V) \geq f(\mathbf{v}) \tag{12}$$

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

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

3.

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

$$\therefore\ b = -r_1 - r_2, c = r_1 r_2 \tag{18}$$

$$\tag{19}$$

4.

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

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

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

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

$$\mu(P, R) + \mu(Q, R) = \max\{degree(P) + degree(R), degree(Q) + degree(R)\} \tag{31}$$

$$= \max\{degree(P), degree(Q)\} + degree(R) \tag{32}$$

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

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

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