9020 Assignment 1

Wanqing Yang - z5325987

October 11, 2021

Problem 1

(a)

$S_{4,-6} = \{4m - 6n : m, n \in \mathbb{Z}\}$

$\begin{cases} m = 1 \\ n = 1 \end{cases} = -2 \qquad \begin{cases} m = 1 \\ n = 2 \end{cases} = -8 \qquad \begin{cases} m = 2 \\ n = 1 \end{cases} = 2 \qquad \begin{cases} m = 0 \\ n = 0 \end{cases} = 0 \qquad \begin{cases} m = 0 \\ n = 1 \end{cases} = -6$

(b)

$S_{12,18} = \{12m + 18n : m, n \in \mathbb{Z}\}$

$\begin{cases} m = 0 \\ n = 0 \end{cases} = 0 \qquad \begin{cases} m = 0 \\ n = 1 \end{cases} = 18 \qquad \begin{cases} m = 1 \\ n = 0 \end{cases} = 12 \qquad \begin{cases} m = 1 \\ n = 1 \end{cases} = 30 \qquad \begin{cases} m = 1 \\ n = 2 \end{cases} = 48$

(c)

(i)

$\because d = gdc(x, y) \qquad \therefore d|x \ and \ d|y, \ for \ some \ m, n \ d|(mx + ny)$

$\therefore \forall k \in S_{x,y} \ d|k \ \Leftrightarrow \forall k \in S_{x,y} \ then \ k \in \{n : n \in \mathbb{Z} \ and \ d|n\}$

$\therefore S_{x,y} \subseteq \{n : n \in \mathbb{Z} \ and \ d|n\}$

(ii)

$\because S_{x,y} \subseteq \{n : n \in \mathbb{Z}\ and\ d|n\}\ and\ z \in S_{x,y}$
$\therefore d|z \therefore for\ some\ integer\ k,\ such\ that\ z = kd$
$\therefore z \geqslant d$

(d)

(i)

suppose that $q = \lfloor \frac{x}{z} \rfloor\ \therefore x\%z = x - \lfloor \frac{x}{z} \rfloor z = x - qz$
$\because z \in S_{x,y}$ then
$z = mx + ny,\ \therefore x\%z = x - qz = x - q(mx + ny) = x(1 - qm) + y(-qn)$
$\therefore x\%z \in S_{x,y} \because 0 \leqslant x\%z < z$ (definition) $\therefore x\%z = 0$
Therefore, $x\%z = 0\ and\ y\%z = 0 \Leftrightarrow z|x\ and\ z|y$

(ii)

Because $z|x$ and $z|y$ then z is the common divisor of x, y.
Therefore, $z \leqslant d$

Problem 2

(a)

$\because gcd(x, y) = 1$, then for some integer w and n, $wx + ny = 1$ (Bézout's identity)
$wx =_{(y)} 1$ is equals to $wx - 1 = ny$
Introduce an integer t to $wx + ny = 1$, $\therefore (w + ty)x + (n - tx)y = 1$ is equals to $wx + ny = 1$ when $t = -\lfloor \frac{w}{y} \rfloor$
$w + ty = w - \lfloor \frac{w}{y} \rfloor w = w\%y \in [0, y)$
Therefore, there are at least one $w_0 \in [0, y) \cap \mathbb{N}$ such that, $wx =_{(y)} 1$

(b)

$gcd(x, y) = 1$ then for some integer m,n $mx + ny = 1$ (Bézout's identity)
$y|kx$ then for some integer a, $kx = ay$
$\because mx + ny = 1 \therefore kmx + kny = k$
$\because kx = ay$ then $may + nky = k \Rightarrow (ma + nk)y = k$ and ma+nk is an integer.
Therefore, $y|k$

(c)

Suppose there are two integers w_1 and w_2 such that $w_1x =_{(y)} 1$ and $w_2x =_{(y)} 1$

Therefore, $w_1x =_{(y)} w_2x, w_1, w_2 \in [0, y)$
Therefore, $(w_1x - w_2x)\%y = 0$, then $y|(w_1 - w_2)x$
From (b), we know that if $gcd(x, y) = 1$ and $y|kx$ then $y|k$
Therefore, $y|(w_1 - w_2)$ is equal to $w_1 - w_2 = ty$ t is an integer.
If both w_1 and $w_2 \in [0, y)$, then the equation $w_1 - w_2 = ty$ is false.
Therefore, if $gcd(x, y) = 1$ then there is at most one $w \in [0, y) \cap N$ such that $wx =_{(y)} 1$

Problem 3

$\frac{3}{2}(n + (m\%n)) < m + n \Leftrightarrow 3(n + (m\%n)) < 2(m + n)$
$\because m\%n = m - n\lfloor \frac{m}{n} \rfloor \ \therefore n + (m\%n) = n + m - n\lfloor \frac{m}{n} \rfloor = n(1 - \lfloor \frac{m}{n} \rfloor) + m$
Equivalent to prove $3(n + (m\%n)) = 3n - 3n\lfloor \frac{m}{n} \rfloor + 3m < 2m + 2n$
Equivalent to prove $n + m - 3n\lfloor \frac{m}{n} \rfloor < 0$
Equivalent to prove $n + m < 3n\lfloor \frac{m}{n} \rfloor$
$\because \frac{m}{n} < 1 + \lfloor \frac{m}{n} \rfloor \ \therefore 3n\lfloor \frac{m}{n} \rfloor > 3n(1 - \frac{m}{n}) = 3n - 3m$
Equivalent to prove $n - m > 0$
$\because n \leqslant m$ Therefore, the original proposition is proved.

Problem 4

(a)

$A \cap \varnothing = A \cap (A \cap A^c)$ [Complementation]
$= (A \cap A) \cap A^c$ [Associativity]
$= A \cap A^c$
$= \varnothing$ [Complementation]

(b)

$(A \backslash C^c) \cup (B \cap C) = (A \cap (C^c)^c) \cup (B \cap C)$ [Definition]
$= (A \cap C) \cup (B \cap C)$ [Double complementation]
$= (C \cap A) \cup (C \cap B)$[Complementation]
$= C \cap (A \cup B)$[Distribution]
$= C \cap (B \cup A)$[Complementation]

(c)

$A^c \oplus \mathcal{U} = (A^c \backslash \mathcal{U}) \cup (\mathcal{U} \backslash A^c)$[Definition]
$= (A^c \cap \varnothing) \cup (\mathcal{U} \cap A)$[Definition]
$= (A^c \cap \varnothing) \cup A$[Identity]
$= (A^c \cap (A^c \cap A)) \cup A$[Complementation]
$= ((A^c \cap A^c) \cap A) \cup A$[Associativity]
$= (A^c \cap A) \cup A$[Idempotence]
$= \varnothing \cup A$[Complementation]

$= A$[Identity]

(d)

$(A \cap B)^c = \mathcal{U} \cap (A^c \cup B^c)$[Identity]
$= (\mathcal{U} \cap A^c) \cup (\mathcal{U} \cap B^c)$[Associativity]
$= (\mathcal{U} \backslash A) \cup (\mathcal{U} \backslash B)$[Definition]
$= A^c \cup B^c$[Definition]

Problem 5

(a)

False
For example, $X = \{1\}$, $Y = \{11\}$, $X, Y \subseteq \Sigma^*$
Then $X \cap Y = \varnothing$, $(X \cap Y)^* = \varnothing^* = \{\lambda\}$
$X^* = \{\lambda, 1, 11, ...\}$, $Y^* = \{\lambda, 11, 1111, ...\}$
$X^* \cap Y^* = \{\lambda, 11, 1111, ...\}$
Because $(X \cap Y)^* = \{\lambda\} \neq \{\lambda, 11, 1111, ...\} = X^* \cap Y^*$
Therefore, $(X \cap Y)^* \neq X^* \cap Y^*$

(b)

False
For example, $X = \{0\}$, $Y = \{1\}$, $X, Y \in \Sigma^*$
$XY = \{01\}$ $YX = \{10\}$
$\therefore (XY)^* = (XY)^0 \cup (XY)^1 \cup ... = \{\lambda, 01, 0101, ...\}$
$(YX)^* = (YX)^0 \cup (YX)^1 \cup ... = \{\lambda, 10, 1010, ...\}$
$\therefore (XY)^* \neq (YX)^*$

(c)

$X(Y \cap Z) = \{x : x \in X\}\{y : y \in Y \ and \ y \in Z\}$
$= \{xy : x \in X, y \in Y \ and \ x \in X, y \in Z\}$
$= \{xy : x \in X, y \in Y\}\{xy : x \in X, y \in Z\} = (XY) \cap (XZ)$

Problem 6

(a)

For function $f : \{a, b, c\} \to \{0, 1\}$ there are 8 elements:
1. $f(a) = 0$ $f(b) = 0$ $f(c) = 0$
2. $f(a) = 0$ $f(b) = 0$ $f(c) = 1$
3. $f(a) = 0$ $f(b) = 1$ $f(c) = 0$
4. $f(a) = 0$ $f(b) = 1$ $f(c) = 1$
5. $f(a) = 1$ $f(b) = 0$ $f(c) = 0$
6. $f(a) = 1$ $f(b) = 0$ $f(c) = 1$
7. $f(a) = 1$ $f(b) = 1$ $f(c) = 0$
8. $f(a) = 1$ $f(b) = 1$ $f(c) = 1$

(b)

$pow(\{a,b,c\})$ is the set of all subset of $\{a,b,c\}$
$\therefore pow(\{a,b,c\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
First, $f : \{a,b,c\} \to \{0,1\}$ and $pow(\{a,b,c\})$ have 8 elements.
By observation, $f(a) = 0$ means there is no element A in the subset,
and $f(a) = 1$ means there is element A in the subset.
For example, function element $f(a) = 0$ $f(b) = 1$ is equal to subset $\{b,c\}$ of A.
Therefore, $f : \{a,b,c\} \to \{0,1\}$ represents all subsets of the set $\{a,b,c\}$

(c)

Let $\Sigma = \{0,1\}$ then $\Sigma^* = \{0,1\}^*$ and $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup ...$
$\therefore \{w \in \{0,1\}^* : length(w) = 3\}$ is equals to Σ^3
$\Sigma^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$
By observation, $f(a) = 0$ means that the first character in a string of length 3 consisting of 0,1 is 0.
$f(b) = 1$ means that the second character is 1
For example, function element $f(a) = 0$ $f(b) = 1$ $f(c) = 1$ is equals to an element 011 in Σ^3
Therefore, $f : \{a,b,c\} \to \{0,1\}$ represents all elements of a string of length 3 which consist of 0,1.

Problem 7

$A^{(B \times C)}$ represents the set of function from (B,C) to A, and (B,C) is the cartesian product of set B and set C, (B,C) is a pair.
$(A^B)^C$ represent the set of functions from C to A^B, where A^B represent the set of function from B to A.
$A^{(B \times C)}$ is a set of function which from a pair to a element of A.
$(A^B)^C$ is a set of function which from an element C to a set of function A^B
In order to proof bijection, we need to proof injection and surjection
For injection, we need to proof that
For surjection, we need to proof that the image of f is equal to its domain.

Problem 8

(a)

Suppose that $(a,d) \in (R_1; R_2); R_3$, then for some $c \in S$, $(a,c) \in R_1; R_2$ and $(c,d) \in R_3$
$\because (a,c) \in R_1; R_2$, $\therefore \exists b \in B$, such that $(a,b) \in R_1$ and $(b,c) \in R_2$
$\because (b,c) \in R_2$ and $(c,d) \in R_3$ then $(b,d) \in R_2; R_3$
$\therefore (a,d) \in R_1; (R_2; R_3)$
Therefore, $(R_1; R_2); R_3 \subseteq R_1; (R_2; R_3)$

Similarly, $R_1;(R_2;R_3) \subseteq (R_1;R_2);R_3$
Therefore, $(R_1;R_2);R_3 = R_1;(R_2;R_3)$

(b)

Suppose that $(a,b) \in I;R$ then for some $b \in S$ $(a,c) \in R_1$ and $(b,b) \in I$
$\because (a,b) \in R_1$, therefore $I;R_1 = R_1;I \subseteq R_1$
Suppose that $(a,b) \in R_1$, exists $b \in I$ such that $(b,b) \in I$
then $(a,b) \in R_1;I$, therefore $R_1 \subseteq R_1;I = I;R_1$
$\therefore I;R_1 = R_1;I \subseteq R_1$ and $R_1 \subseteq R_1;I = I;R_1$
Therefore, $I;R_1 = R_1;I = R_1$

(c)

Suppose that $(a,b) \in (R_1 \cup R_2);R_3$ and $a,b \in S$
exists $c \in S$, $((a,c) \in R_1 \cup R_2 \wedge (c,b) \in R_3)$
Then, $((a,c) \in R_1 \vee (a,c) \in R_2 \wedge (c,b) \in R_3)$
$((a,c) \in R_1 \wedge (c,b) \in R_3) \vee ((a,c) \in R_2 \wedge (c,b) \in R_3)$
$(a,b) \in R_1;R_3 \vee (a,b) \in R_2;R_3$
is equals to $(a,b) \in R_1;R_3 \cup R_2;R_3$

(d)

False.
Suppose that, $(a,b) \in R_1;(R_2 \cap R_3)$ and $a,b \in S$
$\Leftrightarrow \exists c \in S\ (a,c) \in R_1 \wedge (c,b) \in (R_2 \cap R_3)$
$\Leftrightarrow \exists c \in S\ (a,c) \in R_1 \wedge ((c,b) \in R_2 \wedge (c,b) \in R_3)$
$\Leftrightarrow \exists c \in S\ ((a,c) \in R_1 \wedge (c,b) \in R_2) \wedge ((a,c) \in R_1 \wedge (c,b) \in R_3)$
$\Rightarrow \exists c \in S((a,c) \in R_1 \wedge (c,b) \in R_2) \wedge \exists c \in S((a,c) \in R_1 \wedge (c,b) \in R_3)$
$\Leftrightarrow (a,b) \in R_1;R_2 \wedge (a,b) \in R_1;R_3$
$\Leftrightarrow (R_1;R_2) \cap (R_1;R_3)$
Then $R_1;(R_2 \cap R_3) \subseteq (R_1;R_2) \cap (R_1;R_3)$
Therefore, $R_1;(R_2 \cap R_3) = (R_1;R_2) \cap (R_1;R_3)$ is false.