COMP9020: Foundations of Computer Science

Assignment 1

Name: Hongpei Luo

zID: z5246892

Problem 1:

(a) There are 8 functions:

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. $f(a)=1$	$f(b)=0$	$f(c)=0$;
5. $f(a)=1$	$f(b)=1$	$f(c)=0$;	6. $f(a)=1$	$f(b)=0$	$f(c)=1$;
7. $f(a)=0$	$f(b)=1$	$f(c)=1$;	8. $f(a)=1$	$f(b)=1$	$f(c)=1$;

(b) Pow({a,b,c}) ={ λ, {a}, {b}, {c}, {a,b}, {a,c}, {b,c}, {a,b,c} }

The number of functions in $f:\{a,b,c\}\to\{0,1\}$ is exact equal to the number of sets in Pow({a,b,c}). As there are 3 elements in {a,b,c}, 2 elements in {0,1}, there would be 2^3 = 8 functions which applies t the relation. Above, there would be 8 one-to-one relations between them.

(c) (i) There are n^m functions from A to B.

(ii) A has $\Sigma_{i=0}^{n} C_n^i = 2^n$ possibly outputs, so there are $(2^n)^m$ = 2^{mn} relations are between A and B.

(iii) For A, because $\sum_{i=0}^{m} i = [m(m+1)]/2$, so there are $2^{[m(m+1)]/2}$ = $2^{(m^2+m/2)}$ symmetric relations on A.

Problem 2:

(a) Five element of $S_{2,-3}$: 0, 2, -3, 5, -5.

m	0	1	0	1	-1
n	0	0	1	-1	1
$S_{2,-3}$	0	2	-3	5	-5

(b) Five element of $S_{12,16}$:0, 12, 16, -4, 28.

m	0	1	0	1	1
n	0	0	1	-1	1
$S_{12,16}$	0	12	16	-4	28

(c) Prove $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \ and \ d \mid n\}$:

$\because$ d = gcd(x,y), $\therefore$ d | x and d | y, which means $x = k_1 d,\ y = k_2 d \quad (k_1, k_2 \in \mathbb{Z})$

$\therefore \ n = kd = mx + ny = k_1 dm + k_2 dn \quad (k, k_1, k_2, m, n \in \mathbb{Z})$.

$\therefore \ n = kd = (k_1 m + k_2 n)d$

So that $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \ and \ d \mid n\}$ is proved.

(d) We can assume $z = m'x + n'y \quad (m', n' \in \mathbb{Z})$,

$\because \ z \mid n \quad \therefore \ n = k'z \quad (k' \in \mathbb{Z})$

$\therefore \ n = k'z = k'(m'x + n'y) = (k'm')x + (k'n')y$

$\therefore \ \{n : n \in \mathbb{Z} \ and \ z \mid n\} \subseteq S_{x,y}$ is proved.

(e) According to content above, $z = m'x + n'y \quad (m', n' \in \mathbb{Z})$

$\therefore \ z = m'k_1 d + n'k_2 d = (m'k_1 + n'k_2)d$

$\because$ Also, $k_1, k_2 \in \mathbb{Z} \qquad \therefore \ d \mid z$

Because $z > 0, and \ d > 0, \quad z \geq d$ is proved.

(f) Assume that there has $a = m_1 x + n_1 y \quad (m_1, n_1 \in \mathbb{Z})$ in $S_{x,y}$,

at the same time, $z = m'x + n'y \quad (m', n' \in \mathbb{Z})$,

Because z is the smallest positive number in $S_{x,y}$, there has $a > z$.

So a can be shown as $a = cz + b \quad (c, b \in \mathbb{Z})$,

which means $b = m_1 x + n_1 y - c(m'x + n'y) = (m_2 - cm')x + (n_2 - cn')y.$

This is contradictory with z is the smallest element in $S_{x,y}$, so a, b doesn’t exist.

So, the smallest common divisor of $S_{x,y}$ is z .

Above, $z \leq d$ is proved.

Problem 3:

(a) $(A * B) * (A * B)$

$= (A^c \cup B^c) * (A^c \cup B^c)$

$= (A^c \cup B^c)^c \cup (A^c \cup B^c)^c$

$= ((A \cap B)^c)^c \cup ((A \cap B)^c)^c$ [de Morgan's Laws]

$= (A \cap B) \cup (A \cap B)$ [Double complementation]

$= A \cap B$ [Idempotence]

Therefore, $(A * B) * (A * B) = A \cap B$

(b) $A^c = A^c \cup A^c$ [Idempotence]

$= A * A$

Therefore, $A^c = A * A$

(c) $\varnothing = u^c$ [Idempotence]

$= u^c \cup u^c$ [Complementation]

$= (A \cup A^c)^c \cup (A \cup A^c)^c$

$= (A \cup A^c) * (A \cup A^c)$ [Idempotence]

$= ((A \cap A) \cup A^c) * ((A \cap A) \cup A^c)$ [de Morgan's Laws]

$= (((A^c)^c) \cap (A^c)^c) \cup A^c) * (((A^c)^c) \cap (A^c)^c) \cup A^c)$ [Double complementation]

$= ((A^c \cup A^c)^c \cup A^c) * ((A^c \cup A^c)^c \cup A^c)$

$= ((A * A) * A) * ((A * A) * A)$

Therefore, $\varnothing = ((A * A) * A) * ((A * A) * A)$

(d) $A / B = A \cap B^c$

$$= (A \cap B^c) \cup (A \cap B^c)$$ [Idempotence]

$$= (B^c \cap A) \cup (B^c \cap A)$$ [Commutativity]

$$= (B^c \cap (A^c)^c) \cup (B^c \cap (A^c)^c)$$ [Double complementation]

$$= (B \cup A^c)^c \cup (B \cup A^c)^c$$ [de Morgan's Laws]

$$= (B \cup A^c) * (B \cup A^c)$$

$$= (u \cap (B \cup A^c)) * (u \cap (B \cup A^c))$$

$$= ((A \cup A^c) \cap (B \cup A^c)) * ((A \cup A^c) \cap (B \cup A^c))$$ [de Morgan's Laws]

$$= ((A \cap B) \cup A^c) * ((A \cap B) \cup A^c)$$

$$= (((A^c)^c \cap (B^c)^c) \cup A^c) * (((A^c)^c \cap (B^c)^c) \cup A^c)$$ [de Morgan's Laws]

$$= ((A^c \cup B^c)^c \cup A^c) * ((A^c \cup B^c)^c \cup A^c)$$

$$= ((A^c \cup B^c) * A) * ((A^c \cup B^c) * A)$$

$$= ((A * B) * A) * ((A * B) * A)$$

Therefore, $A / B = ((A * B) * A) * ((A * B) * A)$

Problem 4:

(a) $\Sigma^* = \{\lambda, a, b, aa, bb, ab, ba, aaa, bbb, ...\}$

$\Sigma^* \times \Sigma^* = \{\lambda, aa, ab, ba, bb, aaaa, aabb, bbaa, bbbb, ...\}$

Two words can be {a}, {b}.

(b) $\because$ v = aba = wz, there has four possibilities:

1. z = λ , w = aba;
2. z = a, w = ba;
3. z = ab, w = a;
4. z = aba, w = λ.

$\therefore$ $R^{\leftarrow}(\{aba\}) = \{\lambda, a, ab, aba\}$

(c) To show that R is a partial order, the point is proving R can satisfy (R), (AS), (T).

(R): For all $w \in \Sigma^*, (w, w) \in R,$ so R is reflexive;

(AS): For all $w, v \in \Sigma^*,$ when (w,v) *and* $(v,w) \in R,$ it exists w=v, so R is antisymmetric;

(T): For all $w, v \in \Sigma^*,$ there exists a z fits $z \in \Sigma^*$ *such that* $v = wz$,

So, when $(w,v) \in R,$ *and* $(v,x) \in R$, then $v = wz',$ $x = vz'',$ besides, cause $z = z'z'',$ there must exist $x = wz,$ which means $(w,x) \in R.$ So R is transitive.

Above, R is a partial order.

Problem 5:

$\because \quad x \mid yz \qquad \therefore \quad yz = kx \quad (k \in \mathbb{Z})$

$\because$ gcd(x,y) =1 $\quad \therefore$ x and y are co-prime.

There are three situation for this proving:

1. $x = 1 \quad y \neq 1$

$\because \quad x, z \in \mathbb{Z}, \ and \ x \mid yz$

And 1 can be divided by any integers, so $x \mid z$ is proved.

2. $x \neq 1 \quad y = 1$

When y=1, $x \mid yz \ = \ x \mid z$, so it is proved.

3. $x \neq 1 \quad y \neq 1$

According to the known conditions in Problem 2, d = gcd (x,y), and gcd(x,y)=1 in Problem 5, we can know m'x+n'y=1. Also, $x \mid yz$, $\therefore \ x \mid [(1 - m'x)/n']z$, cause $n' \in \mathbb{Z}$, $x \mid [(1 - m'x)/n']z$ can be shown as $x \mid (1 - m'x)z$. Which means, $x \mid z - (m'z)x$, since $m', z \in \mathbb{Z}$, $x \mid z$.

Above, $x \mid z$ can be proved.