

COMP9020 Assignment 1

1.

- | | |
|---|---|
| <p>(a) 1 $f(a) = 0 \quad f(b) = 0 \quad f(c) = 0$</p> <p>3 $f(a) = 0 \quad f(b) = 1 \quad f(c) = 0$</p> <p>5 $f(a) = 1 \quad f(b) = 0 \quad f(c) = 0$</p> <p>7 $f(a) = 1 \quad f(b) = 1 \quad f(c) = 0$</p> | <p>2 $f(a) = 0 \quad f(b) = 0 \quad f(c) = 1$</p> <p>4 $f(a) = 0 \quad f(b) = 1 \quad f(c) = 1$</p> <p>6 $f(a) = 1 \quad f(b) = 0 \quad f(c) = 1$</p> <p>8 $f(a) = 1 \quad f(b) = 1 \quad f(c) = 1$</p> |
|---|---|

(b) In question a, we have 8 possible functions. We can know from the question that $\text{Pow}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$, so $|\text{Pow}(\{a,b,c\})| = 8$, which is equal to the number of possible functions in (a).

- (c) (i) n^m , because for each element in A, it has n possible output after functions, every element in A is independent, so in sum there is $n \cdot n \cdot \dots = n^m$ functions.
- (ii) 2^{nm} , apart from the functions relation, it has no relation, multiple outputs from single element in A, so we have to take every possibility into account, we can conclude that for each element in A, it has 2^n possibilities, so in sum it has 2^{nm} relations.
- (iii) $2^{(1/2)(1+m)m}$, we use matrix to make it simple be understood. In a matrix of $m \times m$, we only have to calculate the number of the upper half of the matrix, which is $(1/2)(1+m)m$, so that the lower half of the matrix should have the same value to make it symmetric. For each element of the matrix, it has two choices, having relation or not. So in summary it has $2^{(1/2)(1+m)m}$ different symmetric relations.

2.

(a) $S_{2,-3} = \{2m-3n : m,n \in \mathbb{Z}\}$, let us assign (m,n) to $(0,1), (1,0), (0,0), (2,0), (0,2)$.
Then we get $S_{2,-3}$ (five elements) = $\{-3, 2, 0, 4, -6\}$.

(b) $S_{12,16} = \{12m+16n : m,n \in \mathbb{Z}\}$, this time I assign (m,n) to $(0,0), (1,0), (0,1), (1,-1), (-1,1)$.
And we get $S_{12,16}$ (five elements) = $\{0, 12, 16, -4, 4\}$.

(c) We let $x = k_1 \cdot d$, $y = k_2 \cdot d$ ($k_1, k_2 \in \mathbb{Z}$), then we can get $S_{x,y} = \{k_1 \cdot d \cdot m + k_2 \cdot d \cdot n : m,n \in \mathbb{Z}\}$.
Then $S_{x,y} = \{(k_1 \cdot m + k_2 \cdot n) \cdot d : m,n \in \mathbb{Z}\}$, we assume $K = k_1 \cdot m + k_2 \cdot n$, then we get $S_{x,y} = \{K \cdot d : K, m,n \in \mathbb{Z}\}$. So every element in S is a multiple of d, and we can conclude that S is a subset of all multiples of d, which is $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$.

(d) Because $z|n$, we can know that $n = a \cdot z$ ($a \in \mathbb{Z}$). And we know that $z = m \cdot x + n \cdot y > 0$.
So $a \cdot z = a \cdot (m \cdot x + n \cdot y) = a \cdot m \cdot x + a \cdot n \cdot y$, and $a \cdot m, a \cdot n \in \mathbb{Z}$, they share the same domain as m and n, so for every element in $\{n : n \in \mathbb{Z} \text{ and } z|n\}$, it is included in $S_{x,y}$. We can get the result.

(e) Because $S_{x,y} \subseteq \{n:n \in \mathbb{Z} \text{ and } d|n\}$, $z \in S_{x,y}$. We can know that $z \in \{n:n \in \mathbb{Z} \text{ and } d|n\}$. So z must be the element in $\{n:n \in \mathbb{Z} \text{ and } d|n\}$ which can be written as $z = i*d (i \in \mathbb{Z})$, as $z, d > 0$, so $i \geq 1$ and $i \in \mathbb{Z}$, so $z \geq d$.

(f) From (c), we could know that $S_{x,y} = \{(k_1*m + k_2*n)*d : m, n \in \mathbb{Z}\}$, and also we can know that k_1, k_2 are co-prime. As long as we prove there exist $m, n \in \mathbb{Z}$, so that $(k_1*m + k_2*n) = 1$, we can prove $d \in S_{x,y}$. This time $z \leq d$, since $d > 0$.

We retrace the steps of Euclid's algorithm, we assume $d = \gcd(a, b)$, and we have

$$r = a - b*q$$

$$r_1 = b - r*q_1 = -a*q_1 + b*(1 + q*q_1)$$

$$r_2 = r - r_1*q_2 = (1 + q_1*q_2)*a + (-q - q_2 - q*q_1*q_2)*b$$

Each step can be written as $r_k = a * \text{integer} + b * \text{integer}$. In particular, this is true for $r_n = d$, which proves $d = m*a + n*b$.

This time, k_1 and k_2 are co-prime, so $d = \gcd(k_1, k_2) = 1$, which means there certainly exist m, n to make $(k_1*m + k_2*n) = 1$.

3.

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

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

$$= (A \cap B) \cup (A \cap B) \quad (\text{double complementation})$$

$$= A \cap B \quad (\text{Idempotence})$$

$$(b) A^c = A^c \cup A^c = A * A \quad (\text{Idempotence})$$

$$(c) \phi = A \cap A^c \quad (\text{Complementation})$$

$$= (A^c \cup A)^c \quad (\text{de Morgan's Laws})$$

$$= (A^c \cup A) * (A^c \cup A) \quad (\text{proved in b})$$

$$= (A * A^c) * (A * A^c) \quad (\text{definition of the } * \text{ operation})$$

$$= (A * (A * A)) * (A * (A * A)) \quad (\text{proved in b})$$

$$(d) A \setminus B = A \cap B^c = (A^c \cup B)^c$$

(de Morgan's Laws)

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

(proved in b)

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

(definition of the * operation)

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

(proved in b)

4.

$$(1) (w, v) = (ab, b) \quad (w, v) = (bb, aa)$$

(2) From the question, we can assign v to aba , and see what values w can take. So the question turn to $aba = wz, w \in \Sigma^*, z \in \Sigma^*$. So $w = \{aba, ab, a, \lambda\}$.

(3) If R is a partial order, it should satisfy (R), (AS), (T).

R: for every $w \in \Sigma^*$, (w, w) is always included in R ($w = wz, z = \lambda$).

AS: for all $w, v \in \Sigma^*$, if $(w, v) \in R$ and $(v, w) \in R$, then $v = wz$ and $w = vz$, so $v = vzz$, only $z = \lambda$ can satisfy it, so $w = v$.

T: for all $w, v, y \in \Sigma^*$, if $(w, v) \in R$ and $(v, y) \in R$, then $v = wz$ and $y = vz$, so $y = wzz$. Since $z \in \Sigma^*$, so $zz \in \Sigma^*$ too. So $y = wZ$ ($Z \in \Sigma^*$), $(y, w) \in R$.

So R satisfies (R), (AS), (T), it is a partial order.

5.

$x|yz \Rightarrow y^*z = k^*x$ ($k \in \mathbb{Z}$), since $\gcd(x, y) = 1$, we can know that x and y are co-prime and If $y = 0$, x must be 1, which satisfies $x|z$, and if $x = 0$, y must be 1, this time $z = 0$, which also leads to $x|z$, and if both x and y is not equal to 0, we divide y on both sides, we get $z = x^*(k/y)$, because x and y are co-prime, they have no common divisor except 1, k must be a multiple of y , otherwise z can't be an integer. So we assume $K = k/y$, which is also an integer, so $z = K^*x$, therefore $x|z$.