Due: Sunday, 13th October, 23:59

Submission is through WebCMS/give and should be a single pdf file, maximum size 2Mb. Prose should be typed, not handwritten. Use of LaTeX is encouraged, but not required.

Discussion of assignment material with others is permitted, but the work submitted *must* be your own in line with the University's plagiarism policy.

Problem 1 (20 marks)

(a) List all possible functions $f : \{a, b, c\} \to \{0, 1\}$. (4 marks)

(b) Describe a connection between your answer for (a) and $\text{Pow}(\{a, b, c\})$. (4 marks)

(c) In general, if $\text{card}(A) = m$ and $\text{card}(B) = n$, how many:

- (i) functions are there from A to B? (4 marks)
- (ii) relations are there between A and B? (4 marks)
- (iii) symmetric relations are there on A? (4 marks)

Solution

(a) There are eight functions from $\{a, b, c\}$ to $\{0, 1\}$:

- f_0: $a \mapsto 0$, $b \mapsto 0$, $c \mapsto 0$
- f_1: $a \mapsto 0$, $b \mapsto 0$, $c \mapsto 1$
- f_2: $a \mapsto 0$, $b \mapsto 1$, $c \mapsto 0$
- f_3: $a \mapsto 0$, $b \mapsto 1$, $c \mapsto 1$
- f_4: $a \mapsto 1$, $b \mapsto 0$, $c \mapsto 0$
- f_5: $a \mapsto 1$, $b \mapsto 0$, $c \mapsto 1$
- f_6: $a \mapsto 1$, $b \mapsto 1$, $c \mapsto 0$
- f_7: $a \mapsto 1$, $b \mapsto 1$, $c \mapsto 1$

(b) We observe that the cardinality of $\mathrm{Pow}(\{a, b, c\})$ is equal to the number of functions from $\{a, b, c\}$ to $\{0, 1\}$. Indeed, for each function $f : \{a, b, c\} \to \{0, 1\}$ we can associate a unique element of $\mathrm{Pow}(\{a, b, c\})$ given by $f^{\leftarrow}(1)$. For example, f_0 corresponds to $\emptyset$; f_5 corresponds to $\{a, c\}$.

(c) In general, if $\mathrm{card}(A) = m$ and $\mathrm{card}(B) = n$, there are:

(i) n^m functions from A to B because each of the m elements of A can map to one of n elements of B – yielding $n \times n \times \cdots n = n^m$ possible functions.

(ii) 2^{mn} relations between A and B because a relation is a subset of $A \times B$ and there are $2^{|A \times B|} = 2^{mn}$ subsets of $A \times B$.

(iii) There are $m(m + 1)/2$ unordered pairs of elements taken from A. Each symmetric relation is a subset of this set, so there are $2^{m(m+1)/2}$ such relations.

Discussion

- For full marks, functions should be clearly defined; the full connection between the sets should be identified; each numeric answer should have a small justification
- Minor errors include small typos that do induce an incorrect answer (e.g. doubling up on a function)
- Major errors include unclear function definitions; only matching cardinalities; numeric answers without justification; incorrect numeric answers with small justification
- Shows promise includes: one or more functions defined; well-founded incorrect numeric answers (e.g. $m \times n$) without justification.

Problem 2 (26 marks)

For $x, y \in \mathbb{Z}$ we define the set:

$$S_{x,y} = \{mx + ny : m, n \in \mathbb{Z}\}.$$

(a) Give five elements of $S_{2,-3}$. (5 marks)

(b) Give five elements of $S_{12,16}$. (5 marks)

For the following questions, let $d = \gcd(x, y)$ and z be the smallest positive number in $S_{x,y}$.

(c) Show that $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$. (4 marks)

(d) Show that $\{n : n \in \mathbb{Z} \text{ and } z|n\} \subseteq S_{x,y}$. (4 marks)

(e) Show that $d \leq z$. (*Hint: use (c)*) (4 marks)

(f) Show that $z \leq d$. (*Hint: use (d)*) (4 marks)

Solution

Note: we need to assume that x and y are not both 0 (so $d > 0$).

(a) We have:

$$\begin{array}{llllll} -2 & = (-1)2 + (0)(-3) & -1 & = (1)2 + (1)(-3) & 0 & = (0)2 + (0)(-3) \\ 1 & = (-1)2 + (-1)(-3) & 2 & = (1)2 + (0)(-3) & & \dots \end{array}$$

so

$$S_{2,-3} = \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$$

(b) We have:

$$\begin{array}{llllll} -4 & = (1)12 + (-1)16 & 0 & = (0)12 + (0)16 & 4 & = (-1)12 + (1)16 \\ 8 & = (-2)12 + (2)16 & 12 & = (1)12 + (0)16 & & \dots \end{array}$$

so

$$S_{12,16} = \{\dots, -4, 0, 4, 8, 12, \dots\} = 4\mathbb{Z}$$

(c) $d|x$ and $d|y$, so $d|(mx + ny)$ for any integers m, n. Therefore, if $w \in S_{x,y}$, $d|w$. So $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$.

(d) $z \in S_{x,y}$ so $z = mx + ny$ for some $m, n \in \mathbb{Z}$. Now suppose $z|w$. Then $w = kz$ for some $k \in \mathbb{Z}$, but then $w = (km)x + (kn)y$ so $w \in S_{x,y}$. Therefore $\{n : n \in \mathbb{Z} \text{ and } z|n\} \subseteq S_{x,y}$.

(e) Since $z \in S_{x,y}$, from (c) we have that $d|z$, so $z = kd$ for some $k \in \mathbb{Z}$. Since z and d are both positive, $k \geq 1$; so $z = kd \geq d$.

(f) $x = (1)x + (0)y$ and $y = (0)x + (1)y$ are both elements of $S_{x,y}$, so from (d) we have that $z|x$ and $z|y$. Hence z is a common divisor of x and y. Since d is the *greatest* common divisor, we have that $z \leq d$.

Discussion

- For (a) and (b): 1 mark for each element correctly identified (justification not needed). -1 mark for any incorrect elements.
- Full marks for clear and correct proofs. Assumption that x and y are not both 0 is not required.
- Minor errors include missing logical steps in arguments
- Major errors include two+ minor errors; right proof "idea" but not clearly explained
- Good progress includes some logical argument

Problem 3 (24 marks)

We define the operation $*$ on subsets of a universal set $\mathcal{U}$ as follows. For any two sets A and B:

$$A * B := A^c \cup B^c.$$

Answer the following questions using the Laws of Set Operations (and any derived results given in lectures) to justify your answer:

(a) What is $(A * B) * (A * B)$? (6 marks)

(b) Express A^c using only A, $*$ and parentheses (if necessary). (6 marks)

(c) Express $\emptyset$ using only A, $*$ and parentheses (if necessary). (6 marks)

(d) Express $A \setminus B$ using only A, B, $*$ and parentheses (if necessary). (6 marks)

Solution

(a)

$$\begin{aligned}
(A * B) * (A * B) &= (A^c \cup B^c)^c \cup (A^c \cup B^c)^c && \text{(Definition)} \\
&= (A^c \cup B^c)^c && \text{(Idempotence)} \\
&= ((A^c)^c \cap (B^c)^c) && \text{(De Morgan's laws)} \\
&= A \cap B && \text{(Double complement)}
\end{aligned}$$

(b)

$$\begin{aligned}
A^c &= A^c \cup A^c && \text{(Idempotence)} \\
&= A * A && \text{(Definition)}
\end{aligned}$$

(c)

$$\begin{aligned}
\emptyset &= A \cap A^c && \text{(Complement)} \\
&= A \cap (A * A) && \text{(from (b))} \\
&= (A * (A * A)) * (A * (A * A)) && \text{(from (a))}
\end{aligned}$$

(d)

$$\begin{aligned}
A \setminus B &= A \cap B^c && \text{(Definition)} \\
&= A \cap (B * B) && \text{(from (b))} \\
&= (A * (B * B)) * (A * (B * B)) && \text{(from (a))}
\end{aligned}$$

Discussion

- For top marks each rule should be on its own line, but multiple applications of the same rule on one line are ok.
- Minor errors include: one or two incorrect rule names; one or two rule omissions (name or logical step). Double complementation is a commonly omitted rule.
- Major errors include: Two+ minor errors; omitting all rule names; unfinished proofs (e.g. finishing (c) at $(A * A^c) * (A * A^c)$)
- Good progress includes: One or two correct logical steps.

Problem 4 (20 marks)

Let $\Sigma = \{a, b\}$. Define $R \subseteq \Sigma^* \times \Sigma^*$ as follows:

$$(w, v) \in R \text{ if there exists } z \in \Sigma^* \text{ such that } v = wz.$$

(a) Give two words $w, v \in \Sigma^*$ such that $(w, v) \notin R$ and $(v, w) \notin R$. (4 marks)

(b) What is $R^{\leftarrow}(\{aba\})$? (4 marks)

(c) Show that R is a partial order. (12 marks)

Solution

We observe that R is the prefix relation: $(w, v) \in R$ if w is a *prefix* of v.

(a) Consider $w = a$ and $v = b$. We observe that for any word $z \in \Sigma^*$, wz will always start with a and vz will always start with b. Therefore it cannot be the case that there is a z such that $w = vz$ or $v = wz$. Therefore $(w, v) \notin R$ and $(v, w) \notin R$.

(b)
$$R^{\leftarrow}(\{aba\}) = \{w : (w, aba) \in R\} = \{\lambda, a, ab, aba\}$$

(c) To show R is a partial order, we need to show Reflexivity, Anti-symmetry, and Transitivity.

- Reflexivity: Since $w = w\lambda$ for all $w \in \Sigma^*$ we have that $(w, w) \in R$ for all $w \in \Sigma^*$. So R is reflexive.
- Anti-symmetry: Suppose $(w, v) \in R$ and $(v, w) \in R$. Then there exists z, z' such that $v = wz$ and $w = vz'$. Therefore
$$w = vz' = wzz'$$
So $z = z' = \lambda$ (if length$(z) > 0$ or length$(z') > 0$ then we would have a contradiction). Therefore $w = v\lambda = v$. So R is anti-symmetric.
- Transitivity: Suppose $(u, v) \in R$ and $(v, w) \in R$. Then there exists z, z' such that $v = uz$ and $w = vz'$. But then $w = vz' = (uz)z' = u(zz')$. Wo $(u, w) \in R$, and hence R is transitive.

Discussion

- For (a) 2 marks for two (correct) words with no justification. 4 marks for two (correct) words with some attempt at justification. 0 marks for any incorrect answer.
- For (b) 1 mark for each correct answer (no justification needed).
- For (c) Each property out of 4.
  - Full marks for clear and correct proof.
  - Minor errors for missing logical steps.
  - Major errors include establishing the result for a particular instance (e.g. $(aba, aba) \in R$ therefore it is reflexive).
  - Good progress includes stating the property and its definition (e.g. Reflexive, so $(w, w) \in R$ for all w).
  - No marks for just naming the property without giving an indication of its definition.

Problem 5 (10 marks)

Show that for all $x, y, z \in \mathbb{Z}$:

$$\text{If } x|yz \text{ and } \gcd(x,y) = 1 \text{ then } x|z.$$

(Hint: Use the connection between $\gcd(x,y)$ *and* $S_{x,y}$ *shown in Problem 2.)*

Solution

From Problem 2 we have $1 \in S_{x,y}$, so there exists $m, n \in \mathbb{Z}$ such that

$$1 = mx + ny.$$

Multiplying this by z on both sides gives:

$$z = mxz + nyz.$$

Since $x|yz$ and $x|mxz$, it follows that $x|(mxz + nyz)$, so $x|z$.

Advice on how to do the assignment

All submitted work must be done individually without consulting someone else's solutions in accordance with the University's "Academic Dishonesty and Plagiarism" policies.

- Assignments are to be submitted via WebCMS (or give) as a single pdf file.
- Be careful with giving multiple or alternative answers. If you give multiple answers, then we will give you marks only for your worst answer, as this indicates how well you understood the question.
- Some of the questions are very easy (with the help of the lecture notes or book). You can use the material presented in the lecture or book (without proving it). You do not need to write more than necessary (see comment above).
- When giving answers to questions, we always would like you to prove/explain/motivate your answers.
- If you use further resources (books, scientific papers, the internet,...) to formulate your answers, then add references to your sources.