Due: 26th of August 2018 at 11:59pm

COMP 9020 – Assignment 1

Note: In your assignment, *how* you arrived at your solution is as important (if not more so) than the solution itself and will be assessed accordingly. There may be more than one way to find a solution, and your approach should contain enough detail to justify its correctness. Lecture content can be assumed to be common knowledge.

1. (a) Compute $\gcd(132, 84)$.

   (b) Suppose $a, b \in \mathbb{N}$ are co-prime. What is $\gcd(a, a + b)$?

Solution:

(a) From the Euclidean algorithm (presented in lectures) we have:

$$\begin{aligned}
\gcd(132, 84) &= \gcd(132 - 84, 84) \\
&= \gcd(48, 84) \\
&= \gcd(48, 84 - 48) \\
&= \gcd(48, 36) \\
&= \gcd(48 - 36, 36) \\
&= \gcd(12, 36) \\
&= \gcd(12, 36 - 12) \\
&= \gcd(12, 24) \\
&= \gcd(12, 24 - 12) \\
&= \gcd(12, 12) \\
&= 12
\end{aligned}$$

(4 marks)

(b) We have $a + b \geq a$ and $\gcd(a, b) = 1$. Therefore, from the Euclidean algorithm we have:

$$\gcd(a, a + b) = \gcd(a, (a + b) - a) = \gcd(a, b) = 1.$$

That is, a and $a + b$ are co-prime. (6 marks)

2. For sets A and B, define $A * B$ to be $(A \cup B)^c$ (the complement of $A \cup B$).

   (a) Simplify $(A * B) * (A * B)$. Justify your answer (e.g. using a Venn diagram or some other technique).

(b) Express A^c using A and $*$. Justify your answer.

(c) Express $A \cap B$ using A, B, and $*$. Justify your answer.

Solution:

(a)
$$
\begin{aligned}
&(A * B) * (A * B) && \\
&\quad = ((A * B) \cup (A * B))^c && \text{(Definition of } *) \\
&\quad = (A * B)^c && \text{(Idempotence)} \\
&\quad = ((A \cup B)^c)^c && \text{(Definition of } *) \\
&\quad = A \cup B && \text{(Double complement)}
\end{aligned}
$$
(3 marks)

(b)
$$
\begin{aligned}
&A^c && \\
&\quad = (A \cup A)^c && \text{(Idempotence)} \\
&\quad = A * A && \text{(Definition of } *)
\end{aligned}
$$
(3 marks)

(c)
$$
\begin{aligned}
&A \cap B && \\
&\quad = ((A^c)^c \cap (B^c)^c) && \text{(Double complement)} \\
&\quad = (A^c \cup B^c)^c && \text{(De Morgan)} \\
&\quad = (A^c) * (B^c) && \text{(Definition of } *) \\
&\quad = (A * A) * (B * B) && \text{(from (b))}
\end{aligned}
$$
(4 marks)

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

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

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

(i) functions are there from A to B?

(ii) relations are there between A and B?

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: $a \mapsto 1$, $b \mapsto 1$, $c \mapsto 1$

(3 marks)

(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 $\{a, c\}$. (3 marks)

(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. (2 marks)

(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 $A \times B$. (2 marks)

4. Let $\Sigma = \{a, b\}$ and $L = \{w \in \Sigma^* \ : \ 3|\mathrm{length}(w)\}$.

(a) List the elements of $L^{\leq 3}$ in lexicographic order.

Define $R \subseteq \Sigma^* \times \Sigma^*$ as follows: $(w, w') \in R$ if there is a $v \in \Sigma^*$ such that: either $wv \in L$ and $w'v \notin L$, or $wv \notin L$ and $w'v \in L$. For example $(a, bbb) \in R$ because for $v = \lambda$, $av = a \notin L$ and $bbbv = bbb \in L$. On the other hand, $(a, b) \notin R$ because for any $v \in \Sigma^*$, $\mathrm{length}(av) = \mathrm{length}(bv)$; so whenever $av \in L$, $bv \in L$ and vice-versa.

(b) Which of the following are elements of R:

(i) $(abab, baba)$?

(ii) $(ab, abab)$?

(iii) (λ, b)?

(iv) (λ, bb)?

(v) (λ, bbb)?

Now define $S \subseteq \Sigma^* \times \Sigma^*$ as the complement of R. That is $(w, w') \in S$ if, and only if, $(w, w') \notin R$.

(b) State a simple rule for determining whether $(w, w') \in S$. *Hint: consider length*(w) $-$ *length(w')*

(c) Show that S is an equivalence relation. That is, show that S is reflexive, symmetric, and transitive.

(d) How many equivalence classes does S have?

Solution:

(a) The elements of $L^{\leq 3}$ in lexicographic order are:

$$\lambda, aaa, aab, aba, abb, baa, bab, bba, bbb$$

(2 marks)

(b) We observe that $(w, w') \in R$ if and only if $3 \nmid \text{length}(w) - \text{length}(w')$.

- (i) $(abab, baba)$? No because for all v: $\text{length}(ababv) = \text{length}(babav)$, so whenever $ababv \in L$, we have $babav \in L$ and vice versa.
- (ii) $(ab, abab)$? Yes because for $v = a$: $abv = aba \in L$ but $ababv = ababa \notin L$.
- (iii) (λ, b)? Yes because for $v = \lambda$: $\lambda v = \lambda \in L$ but $bv = b \notin L$.
- (iv) (λ, bb)? Yes because for $v = \lambda$: $\lambda v = \lambda \in L$ but $bbv = bb \notin L$.
- (v) (λ, bbb)? No because for all v: $\text{length}(\lambda v) - \text{length}(bbbv) = -3$, so whenever $\lambda v \in L$, we have $bbbv \in L$ and vice versa.

(1 mark each)

(b) $(w, w') \in S$ if and only if $3 | \text{length}(w) - \text{length}(w')$. (2 marks)

(c) We need to show reflexivity (R), symmetry (S), and transitivity (T):

- (R): Since $\text{length}(w) - \text{length}(w) = 0$ and $3|0$ we have that $(w, w) \in S$ for all $w \in \Sigma^*$.
(3 marks)
- (S): Suppose $(w, w') \in S$. Then $3|\text{length}(w) - \text{length}(w')$, i.e. $\text{length}(w) - \text{length}(w') = 3k$ for some $k \in \mathbb{Z}$. So $\text{length}(w') - \text{length}(w) = 3k'$ for some $k' \in \mathbb{Z}$ (namely $k' = -k$) so $3|\text{length}(w') - \text{length}(w)$. So $(w', w) \in S$.
(3 marks)
- (T): Suppose $(w, w') \in S$ and $(w', w'') \in S$. Then $3|\text{length}(w) - \text{length}(w')$ and $3|\text{length}(w') - \text{length}(w'')$. Therefore, $\text{length}(w) - \text{length}(w') = 3k$ and $\text{length}(w') - \text{length}(w'') = 3k'$ for some $k, k' \in \mathbb{Z}$. Therefore

$$\begin{aligned}
&\text{length}(w) - \text{length}(w'') \\
&\quad = \text{length}(w) - \text{length}(w') + \text{length}(w') - \text{length}(w'') \\
&\quad = 3k + 3k' \\
&\quad = 3(k + k').
\end{aligned}$$

So $3|\text{length}(w) - \text{length}(w'')$, and so $(w, w'') \in S$.
(3 marks)

(d) S has three equivalence classes: $[\lambda]$ (i.e. set of all words with length divisible by 3), $[a]$ (set of all words with length 1 more than a multiple of 3), and $[aa]$ (set of all words with length 2 more than a multiple of 3). (2 marks)