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

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

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

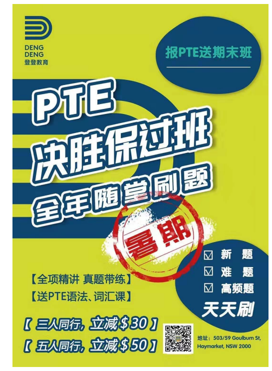
3. (a) List all possible functions $f : \{a, b, c\} \to \{0, 1\}$

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

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

Due: 16th of September 2018 at 11:59pm

COMP 9020 – Assignment 2

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. If $R_1 \subseteq S \times T$ and $R_2 \subseteq T \times U$ are binary relations, the *composition* of R_1 and R_2 is the relation $R_1; R_2$ defined as:

$$R_1; R_2 := \{(a, c) : \text{There exists } b \in T \text{ such that } (a, b) \in R_1 \text{ and } (b, c) \in R_2\}$$

(a) If $f : S \to T$ and $g : T \to U$ are functions is $f; g$ a function?

(b) If $R \subseteq S \times S$ is transitive, show that $R = R \cup (R; R)$. (*Hint: One way to show $A = B$ is to show $A \subseteq B$ and $B \subseteq A$. One of these directions is trivial.*)

Solution:

(a) Yes. If f and g are functions then for any $x \in S$ there is a unique $y \in T$ (namely $y = f(x)$) such that $(x, y) \in f$; and for any $y \in T$ there is a unique $z \in U$ (namely $z = g(y)$) such that $(y, z) \in g$. Therefore, for any $x \in S$ there is a unique $z \in U$ (namely $z = g(f(x))$ such that $(x, z) \in f; g$. In other words, $f; g = g \circ f$ where $\circ$ is function composition.

(2 marks)

(b) It is clear that $R \subseteq R \cup (R; R)$, so, following the hint, it is sufficient to show that $(R; R) \cup R \subseteq R$. For this, it is sufficient to show that $(R; R) \subseteq R$. Consider $(a, c) \in (R; R)$. From the definition of ; there is a b such that $(a, b) \in R$ and $(b, c) \in R$. But then, by the transitivity of R, it follows that $(a, c) \in R$. So $(R; R) \subseteq R$ as required.

(3 marks)

Let $R \subseteq S \times S$ be any binary relation on a set S. Consider the sequence of relations $R^0, R^1, R^2, \ldots$, defined as follows:

$$\begin{aligned} R^0 &:= R, \text{ and} \\ R^{i+1} &:= R^i \cup (R^i; R) \text{ for } i \geq 0 \end{aligned}$$

(c) Prove that if $R^i = R^{i+1}$ for some i, then $R^i = R^j$ for all $j \geq i$.

(d) Prove that if $R^i = R^{i+1}$ for some i, then $R^k \subseteq R^i$ for all $k \geq 0$.

(e) If $|S| = n$, explain why $R^n = R^{n+1}$. (*Hint: Show that if* $(a, b) \in R^{n+1}$ *then* $(a, b) \in R^i$ *for some* $i < n + 1$.)

Solution:

(c) Let $P(j)$ be the proposition that $R^j = R^i$. We will show that $P(j)$ holds for all $j \geq i$ by induction on j.

Base case. $P(i)$ is clearly true.

Inductive case: Assume $P(k)$ is true for some $k \geq i$. That is, $R^k = R^i$. Consider R^{k+1}:

$$\begin{aligned} R^{k+1} &:= R^k \cup (R^k; R) \quad (\text{definition of } R^{k+1}) \\ &= R^i \cup (R^i; R) \quad (\text{IH}) \\ &= R^{i+1} \quad (\text{definition of } R^{i+1}) \\ &= R^i \quad (\text{definition of } i) \end{aligned}$$

So $P(k)$ implies $P(k+1)$. Therefore $P(j)$ is true for all $j \geq i$.

(5 marks)

(d) We have for all $j \geq 0$, $R^j \subseteq R^{j+1}$, so by the transitivity of $\subseteq$ (covered in lectures) we have that $R^k \subseteq R^i$ for all $k \leq i$. Question 1(c) established that $R^k \subseteq R^i$ for all $k > i$, so $R^k \subseteq R^i$ for all $k \geq 0$.

(2 marks)

(e) It suffices to show that $R^{n+1} \subseteq R^n$. If $(a, c) \in R^{n+1}$ then there exists $b_0, b_1, \ldots, b_n, b_{n+1} \in S$ such that $a = b_0$, $c = b_{n+1}$ and $(b_i, b_{i+1}) \in R$ for $0 \leq i \leq n$. As S only has n elements, there must be i, j with $0 \leq i < j \leq n + 1$ such that $b_i = b_j$. But this means that $(b_i, b_{j+1}) \in R$, and so $(a, c) \in R^{n+1-(j-i)}$. As $j > i$, $n + 1 - (j - 1) \leq n$, so $(a, c) \in R^k$ for some $k \leq n$. From our earlier observation at the start of 1(d), $R^k \subseteq R^n$, so $(a, c) \in R^n$, as required.

(4 marks)

In the above sequence, R^n is defined to be the *transitive closure* of R, denoted R^* (closely related to the * operator used to describe the set of all words over an alphabet).

(f) Show that R^* is transitive.

Solution:

(f) Suppose $(a, b) \in R^*$ and $(b, c) \in R^*$. Then there exists $b_1, \ldots, b_k$ (where $k \leq n$) and $c_1, \ldots, c_r$ (where $r \leq n$) such that the following pairs are all in R:

$$(a, b_1), (b_i, b_{i+1}) \text{ for } 1 \leq i < k, (b_k, b), (b, c_1), (c_i, c_{i+1}) \text{ for } 1 \leq i < r, (c_r, c).$$

This means that $(a, c) \in R^{k+r+1}$. From 1(d) and 1(e), $R^{k+r+1} \subseteq R^n$, so $(a, c) \in R^n = R^*$. Hence R^* is transitive.

(4 marks)

(20 marks)

2. The following table describes several subjects and the students taking them:

Potions	**Charms**	**Herbology**	**Astronomy**	**Transfiguration**
Harry	Ron	Harry	Hermione	Hermione
Ron	Luna	George	Neville	Fred
Malfoy	Ginny	Neville	Seamus	Luna

You have been tasked to create an examination timetable for these subjects, and your goal is to find the *smallest number* of timeslots needed so that all subjects can be examined, without any conflicts occurring (i.e. no students having to take two or more exams at the same time).

(a) Explain how this can be formulated as a graph-based problem. That is, describe what the vertices and edges would be, and how to relate the given problem to a common graph problem.

(b) For this problem in particular determine the minimum number of timeslots required.

Solution:

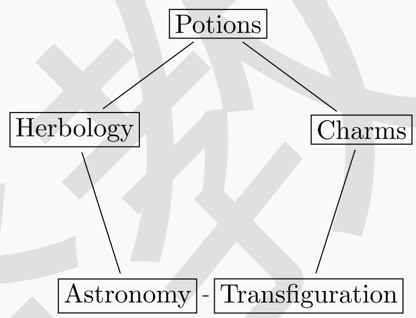
(a) Define a graph G as follows:

- The set of vertices correspond to the subjects
- An edge between a pair of vertices (subjects) if they have a student in common (i.e. the subjects are in *conflict*)

The *chromatic number* of G then indicates the minimum number of timeslots required: each colour in a valid colouring corresponds to a choice of timeslot. Subjects that are in conflict share an edge so they will have to have a different colour.

(3 marks)

(b) For this problem, the associated graph would be:



This graph, being an odd-length cycle, has chromatic number 3, so the minimum number of timeslots is three. An example allocation might be:

Timeslot 1	Timeslot 2	Timeslot 3
Potions	Charms	Herbology
Transfiguration	Astronomy	

(2 marks)

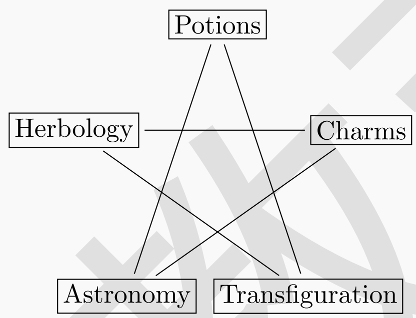
(c) Suppose instead your goal was to determine the *largest number* of subjects that can be examined at the same time without conflicts. How do your answers to (a) and (b) change?

(10 marks)

Solution:

(c) Use the same set of vertices, but put an edge between vertices if the corresponding subjects are *not* in conflict. The *clique number* of this graph then indicates the largest number of subjects that are mutually not in conflict – i.e. the largest number of subjects that can be examined at the same time.

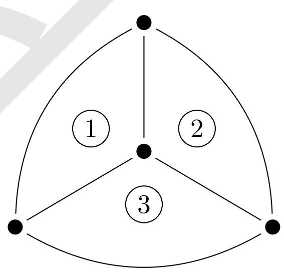
For the problem at hand, the graph becomes:



Which has clique number 2, implying that the maximum number of subjects assessible in any single timeslot is two. For example Potions and Transfiguration could be assessed at the same time.

(5 marks)

3. Given a plane-drawing (i.e. no crossing edges) of a *connected* planar graph G, a *face* is a region that is enclosed by edges. For example, the following plane-drawing of K_4 has 3 faces (labelled 1,2,3):



(a) How many edges must a connected graph with n vertices and 1 face have?

(b) By examining several planar graphs, come up with an equation that relates the number of vertices (n), the number of edges (m) and the number of faces (f) of a plane-drawing of a planar graph.

(c) Prove, by induction on f or otherwise, that your formula is correct. *Hint: What happens if you delete an edge of a plane-drawing that doesn't disconnect the graph?*

(10 marks)

Solution:

(a) A connected, planar graph with n vertices and 1 face contains a single cycle. Deleting an edge in that cycle creates a tree, which we know from lectures contains $n-1$ edges. Therefore the original graph has n edges. (2 marks)

(b) A simple equation would be $n - m + f = 1$ (or $n - m + f = 2$ if we consider the "exterior" region as a face). This is known as **Euler's formula**. (2 marks)

(c) Let $P(f)$ be the proposition that for all n, if there is a connected planar graph with n vertices and f faces then it has $n + f - 1$ edges. We will show that $P(f)$ holds for all $f \in \mathbb{N}$.

Base case ($f = 0$) A planar, connected graph with 0 faces is, as observed above, a tree. Therefore it has $n-1 = n+f-1$ edges. So $P(0)$ holds.

Inductive case Assume $P(f)$ holds for $f \geq 0$. Consider a planar, connected graph G with n vertices and $f + 1$ faces. Let G' be the graph that results from removing one edge that is adjacent to a face (since there are $f + 1 \geq 1$ faces, there is such an edge). We observe that:

- G' is planar since removing edges does not make a planar graph non-planar.
- G' is connected since the edge removed was part of a cycle: the cycle that defined the face it was adjacent to
- G' has n vertices
- G' has one fewer faces than G, i.e. G' has f faces: the face that was adjacent to the removed edge is now "merged with" the face (or exterior) on the other side of the removed edge.

It follows from the inductive hypothesis that G' has $n + f - 1$ edges, so G has $n + f = n + (f + 1) - 1$ edges.

Thus $P(f)$ implies $P(f + 1)$; and so $P(f)$ holds for all $f \in \mathbb{N}$. (6 marks)

4. Extend the syntactical definition of propositional formulae to include the connective $\circ$:

- If φ and ψ are propositional formulae, then $(\varphi \circ \psi)$ is a propositional formula.

Given a truth valuation $v : Prop \to \mathbb{B}$, define the semantics for $\circ$ as

$$v(\varphi \circ \psi) \ = !\big(v(\varphi)\ \&\ v(\psi)\big)$$

(a) Draw the truth table for $(p \circ q) \circ (p \circ q)$. Give a logically equivalent formula.

(b) For each of the following formulae, give a logically equivalent formula that only uses $\circ$ and propositional variables. Justify your answer.

i. $\neg p$

ii. $p \vee q$

iii. $p \to q$

iv. $p \leftrightarrow q$

Solution:

(a) Here is the truth table for $(p \circ q) \circ (p \circ q)$ and for $p \wedge q$ showing that they are logically equivalent.

p	q	$p \circ q$	$(p \circ q) \circ (p \circ q)$	$p \wedge q$
F	F	T	F	F
F	T	T	F	F
T	F	T	F	F
T	T	F	T	T

((2 marks)

(b) Here are some more truth tables for various combinations of p, q and $\circ$:

p	q	$p \circ p$	$q \circ q$	$(p \circ p) \circ (q \circ q)$	$p \circ (q \circ q)$	$((p \circ p) \circ (q \circ q)) \circ (p \circ q)$
F	F	T	T	F	T	T
F	T	T	F	T	T	F
T	F	F	T	T	F	F
T	T	F	F	T	T	T

This shows that:

i. $\neg p$ is logically equivalent to $p \circ p$

ii. $p \vee q$ is logically equivalent to $(p \circ p) \circ (q \circ q)$

iii. $p \to q$ is logically equivalent to $p \circ (q \circ q)$, and

iv. $p \leftrightarrow q$ is logically equivalent to $((p \circ p) \circ (q \circ q)) \circ (p \circ q)$. Alternatively, it is logically equivalent to $(p \to q) \wedge (q \to p)$, which islogically equivalent to $(A \circ B) \circ (A \circ B)$ where $A = p \circ (q \circ q)$ and $B = q \circ (p \circ p)$.

(2 marks each)

(10 marks)

Due: 14th of October 2018 at 11:59pm

COMP 9020 – Assignment 3

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. Let $(T, \wedge, \vee, ', 0, 1)$ be a Boolean Algebra.

   Define $* : T \times T \to T$ and $\circ : T \times T \to T$ as follows:

   $$x * y := (x \vee y)' \qquad\qquad x \circ y := (x \wedge y)'$$

   (a) Show, using the laws of Boolean Algebra, how to define $x * y$ using only x, y, $\circ$ and parentheses.

   (b) Show, using the laws of Boolean Algebra, how to define $x \circ y$ using only x, y, $*$ and parentheses.x

Solution:

(a) First we establish some results:

$$\begin{aligned} x \wedge x &= (x \wedge x) \vee 0 && \text{(Identity)} \\ &= (x \wedge x) \vee (x \wedge x') && \text{(Complement)} \\ &= x \wedge (x \vee x') && \text{(Distributivity)} \\ &= x \wedge 1 && \text{(Complement)} \\ &= x && \text{(Identity)} \end{aligned}$$

from which it follows that:

$$x \circ x = (x \wedge x)' = x'$$

and, using De Morgan's laws (given in lectures):

$$(x \circ x) \circ (y \circ y) = (x' \wedge y')' = (x \vee y).$$

Therefore,

$$x * y = (x \vee y)' = \big((x \circ x) \circ (y \circ y)\big) \circ \big((x \circ x) \circ (y \circ y)\big)$$

(b) We observe that $x * y$ is the dual of $x \circ y$, so by the principle of duality (given in lectures) we have, from part (a):

$$x \circ y = \big((x * x) * (y * y)\big) * \big((x * x) * (y * y)\big).$$

(10 marks)

Define $R \subseteq T \times T$ as follows:

$$(x, y) \in R \text{ if, and only if, } (x \wedge y) \vee (x' \wedge y') = 1$$

(c) Show, using the laws of Boolean Algebra, that R is an equivalence relation. *Hint: You may want to use the observation that if* $A = B = 1$ *then* $A \wedge B \wedge C = A \wedge B$ *implies* $C = 1$ *(why?)*

Solution: For simplicity and clarity, we will use associativity to omit parentheses when forming a meet/join of three or more elements. First we establish the hint: If $A = B = 1$ and $A \wedge B \wedge C = A \wedge B$ then, repeatedly using the Identity law:

$$C = 1 \wedge C = 1 \wedge 1 \wedge C = A \wedge B \wedge C = A \wedge B = 1 \wedge 1 = 1.$$

We also need the following result (using Complement, Associativity, Idempotency from part (a), and Complement):

$$x \wedge 0 = x \wedge (x \wedge x') = (x \wedge x) \wedge x' = x \wedge x' = 0$$

To show that R is an equivalence relation we must show Reflexivity, Symmetry, and Transitivity.

Reflexivity We have for all $x \in T$:

$$\begin{aligned} 1 &= x \vee x' && \text{(Complement)} \\ &= (x \wedge x) \vee (x' \wedge x') && \text{From (a)} \end{aligned}$$

So $(x, x) \in R$ for all $x \in T$. So R is reflexive.

Symmetry Suppose $(x, y) \in R$ then:

$$\begin{aligned} 1 &= (x \wedge y) \vee (x' \wedge y') \\ &= (y \wedge x) \vee (y' \wedge x') && \text{(Commutativity of } \wedge) \end{aligned}$$

so $(y, x) \in R$. Therefore R is symmetric.

Transitivity Suppose $(x, y) \in R$ and $(y, z) \in R$. For simplicity, let $A = (x \wedge y) \vee (x' \wedge y')$, $B = (y \wedge z) \vee (y' \wedge z')$, and $C = (x \wedge z) \vee (x' \wedge z')$. So $A = B = 1$ and,

$$\begin{aligned} A \wedge B &= \big((x \wedge y) \vee (x' \wedge y')\big) \wedge \big((y \wedge z) \vee (y' \wedge z')\big) \\ &= (x \wedge y \wedge y \wedge z) \vee (x' \wedge y' \wedge y \wedge z) \vee \\ &\quad (x \wedge y \wedge y' \wedge z') \vee (x' \wedge y' \wedge y' \wedge z') && \text{(Dist.)} \\ &= (x \wedge y \wedge z) \vee (x' \wedge 0 \wedge z) \vee \\ &\quad (x \wedge 0 \wedge z') \vee (x' \wedge y' \wedge z') && \text{((a), Comp.)} \\ &= (x \wedge y \wedge z) \vee 0 \vee 0 \vee (x' \wedge y' \wedge z') && \text{(Above)} \\ &= (x \wedge y \wedge z) \vee (x' \wedge y' \wedge z'). && \text{(Ident.)} \end{aligned}$$

So,

$$\begin{aligned} A \wedge B \wedge C &= \big((x \wedge y \wedge z) \vee (x' \wedge y' \wedge z')\big) \wedge \big((x \wedge z) \vee (x' \wedge z')\big) \\ &= (x \wedge y \wedge z \wedge x \wedge z) \vee (x' \wedge y' \wedge z' \wedge x \wedge z) \vee \\ &\quad (x \wedge y \wedge z \wedge x' \wedge z') \vee (x' \wedge y' \wedge z' \wedge x' \wedge z') && \text{(Dist.)} \\ &= (x \wedge y \wedge z) \vee (x' \wedge y' \wedge x \wedge z' \wedge z) \vee \\ &\quad (x \wedge y \wedge x' \wedge z \wedge z') \vee (x' \wedge y' \wedge z') && \text{((a), Comm.)} \\ &= (x \wedge y \wedge z) \vee 0 \vee 0 \vee (x' \wedge y' \wedge z') && \text{(Comp., above)} \\ &= (x \wedge y \wedge z) \vee (x' \wedge y' \wedge z') && \text{(Ident.)} \\ &= A \wedge B. \end{aligned}$$

So from the hint above we have that $C = 1$ and so $(x, z) \in R$ therefore R is transitive.

(10 marks)

2. Let PF denote the set of well-formed propositional formulas made up of propositional variables, $\top$, $\bot$, and the connectives $\neg$, $\wedge$, and $\vee$. Recall from Quiz 7 the definitions of dual and flip as functions from PF to PF:

- $\mathsf{dual}(p) = p$
- $\mathsf{dual}(\top) = \bot$; $\mathsf{dual}(\bot) = \top$
- $\mathsf{dual}(\neg\varphi) = \neg\mathsf{dual}(\varphi)$
- $\mathsf{dual}(\varphi \wedge \psi) = \mathsf{dual}(\varphi) \vee \mathsf{dual}(\psi)$
- $\mathsf{dual}(\varphi \vee \psi) = \mathsf{dual}(\varphi) \wedge \mathsf{dual}(\psi)$

- $\mathsf{flip}(p) = \neg p$
- $\mathsf{flip}(\top) = \top$; $\mathsf{flip}(\bot) = \bot$
- $\mathsf{flip}(\neg\varphi) = \neg\mathsf{flip}(\varphi)$
- $\mathsf{flip}(\varphi \wedge \psi) = \mathsf{flip}(\varphi) \wedge \mathsf{flip}(\psi)$
- $\mathsf{flip}(\varphi \vee \psi) = \mathsf{flip}(\varphi) \vee \mathsf{flip}(\psi)$

(a) For the formula $\varphi = p \vee (q \wedge \neg r)$:

(i) What is $\mathsf{dual}(\varphi)$?

(ii) What is $\mathsf{flip}(\varphi)$?

Solution:

(i)

$$\begin{aligned}
\mathsf{dual}(\varphi) &= \mathsf{dual}(p \vee (q \wedge \neg r)) \\
&= \mathsf{dual}(p) \wedge \mathsf{dual}(q \wedge \neg r) \\
&= p \wedge (\mathsf{dual}(q) \vee \mathsf{dual}(\neg r)) \\
&= p \wedge (q \vee \neg\mathsf{dual}(r)) \\
&= p \wedge (q \vee \neg r).
\end{aligned}$$

(ii)

$$\begin{aligned}
\mathsf{flip}(\varphi) &= \mathsf{flip}(p \vee (q \wedge \neg r)) \\
&= \mathsf{flip}(p) \vee \mathsf{flip}(q \wedge \neg r) \\
&= \neg p \vee (\mathsf{flip}(q) \wedge \mathsf{flip}(\neg r)) \\
&= \neg p \vee (\neg q \wedge \neg\mathsf{flip}(r)) \\
&= \neg p \vee (\neg q \wedge \neg\neg r).
\end{aligned}$$

(Note that it is $\neg\neg r$, not r.)

(b) Prove that for all $\varphi \in PF$: $\mathsf{flip}(\varphi)$ is logically equivalent to $\neg\mathsf{dual}(\varphi)$.

Solution: Let $P(\varphi)$ be the proposition that $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$. We will show that $P(\varphi)$ holds for all $\varphi \in PF$ by structural induction.

Base case ($\top$): $\mathsf{dual}(\top) = \bot \equiv \neg\top = \neg\mathsf{flip}(\top)$. So $P(\top)$ holds.

Base case ($\bot$): $\mathsf{dual}(\bot) = \top \equiv \neg\bot = \neg\mathsf{flip}(\bot)$. So $P(\bot)$ holds.

Base case (p): For any propositional variable p we have

$$\mathsf{dual}(p) = p \equiv \neg\neg p = \neg\mathsf{flip}(p).$$

So $P(p)$ holds.

Inductive case ($\neg\varphi$): Suppose $P(\varphi)$ holds, that is $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$. Then

$$\begin{aligned} \mathsf{dual}(\neg\varphi) &= \neg\mathsf{dual}(\varphi) && \text{(Definition of dual)} \\ &\equiv \neg(\neg\mathsf{flip}(\varphi)) && \text{(IH)} \\ &= \neg\mathsf{flip}(\neg\varphi) && \text{(Definition of flip)} \end{aligned}$$

So $P(\neg\varphi)$ holds.

Inductive case ($\varphi \wedge \psi$): Suppose $P(\varphi)$ and $P(\psi)$ hold. That is, $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$ and $\mathsf{dual}(\psi) \equiv \neg\mathsf{flip}(\psi)$. Then

$$\begin{aligned} \mathsf{dual}(\varphi \wedge \psi) &= \mathsf{dual}(\varphi) \vee \mathsf{dual}(\psi) && \text{(Definition of dual)} \\ &\equiv (\neg\mathsf{flip}(\varphi)) \vee (\neg\mathsf{flip}(\psi)) && \text{(IH)} \\ &\equiv \neg(\mathsf{flip}(\varphi) \wedge \mathsf{flip}(\psi)) && \text{(De Morgan's law)} \\ &= \neg\mathsf{flip}(\varphi \wedge \psi). && \text{(Definition of flip)} \end{aligned}$$

So $P(\varphi \wedge \psi)$ holds.

Inductive case ($\varphi \vee \psi$): Suppose $P(\varphi)$ and $P(\psi)$ hold. That is, $\mathsf{dual}(\varphi) \equiv \neg\mathsf{flip}(\varphi)$ and $\mathsf{dual}(\psi) \equiv \neg\mathsf{flip}(\psi)$. Then

$$\begin{aligned} \mathsf{dual}(\varphi \vee \psi) &= \mathsf{dual}(\varphi) \wedge \mathsf{dual}(\psi) && \text{(Definition of dual)} \\ &\equiv (\neg\mathsf{flip}(\varphi)) \wedge (\neg\mathsf{flip}(\psi)) && \text{(IH)} \\ &\equiv \neg(\mathsf{flip}(\varphi) \vee \mathsf{flip}(\psi)) && \text{(De Morgan's law)} \\ &= \neg\mathsf{flip}(\varphi \vee \psi). && \text{(Definition of flip)} \end{aligned}$$

So $P(\varphi \vee \psi)$ holds.

By the principle of induction, $P(\varphi)$ holds for all $\varphi \in PF$.

(10 marks)

3. Let $P(n)$ be the proposition that: for all k, with $1 \le k \le n$,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

(a) Prove that $P(n)$ holds for all $n \ge 1$. (*Note: it is possible to do this without using induction*)

Solution: One solution is to observe that $\binom{n}{k}$ is the number of subsets of size k of a set of size n. That is, if $V = \{1, 2, \ldots, n\}$ then there are $\binom{n}{k}$ subsets $X \subseteq V$ with $|X| = k$. Now consider $V' = V \setminus \{n\}$. For every subset $X \subseteq V$ we have two (disjoint) possibilities, either $X \subseteq V'$ or $n \in X$ and $X \setminus \{n\} \subseteq V'$. If $|X| = k$, then there are $\binom{n-1}{k}$ sets of the first kind (we are counting the subsets of size k from a set of size $n-1$) and there are $\binom{n-1}{k-1}$ sets of the second kind (since $X \setminus \{n\}$ is a subset of size $k-1$). Therefore there are $\binom{n-1}{k-1} + \binom{n-1}{k}$ possible subsets of size k from a set of size n. Therefore

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

(10 marks)

We can compute $\binom{n}{k}$ from the formula given in lectures, however this can often require computing unnecessarily large numbers. For example, $\binom{100}{15} = 253338471349988640$ which can be expressed as a 64-bit integer, but 100! is larger than a 512-bit integer. We can, however, make use of the equation above to compute $\binom{n}{k}$ more efficiently. Here are two algorithms for doing this:

```
chooseRec(n, k) :
  if k = 0 or k = n :  return 1
  else :
    x := chooseRec(n − 1, k − 1)
    y := chooseRec(n − 1, k)
    return x + y
```

```
chooseIter(n, k) :
  Let C be a n × n array
  for m = 1 to n :
    C[m][0]=C[m][m]=1
    for j = 1 to m − 1 :
      C[m][j]=C[m − 1][j − 1]
              + C[m − 1][j]
  return C[n][k]
```

Let $t_{\mathsf{rec}}(n,k)$ be the running time for $\mathsf{chooseRec}(n,k)$, and let $t_{\mathsf{iter}}(n)$ be the running time for $\mathsf{chooseIter}(n,k)$. Let $T_{\mathsf{rec}}(n) = \max_{0 \le k \le n} t_{\mathsf{rec}}(n,k)$ and $T_{\mathsf{iter}}(n) = \max_{0 \le k \le n} t_{\mathsf{iter}}(n,k)$ (so $T_{\mathsf{rec}}(n) \ge t_{\mathsf{rec}}(n,k)$ for all k, and likewise for $T_{\mathsf{iter}}(n)$).

(b) Give an asymptotic upper bound for $T_{\mathsf{rec}}(n)$. Justify your answer.

Solution: In the worst case, for all n and k we have:

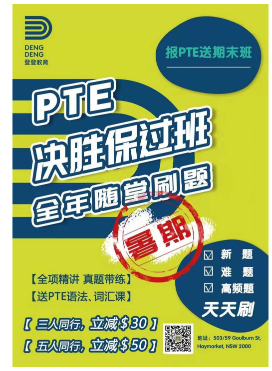
$$
\begin{aligned}
t_{\mathsf{rec}}(n,k) &= t_{\mathsf{rec}}(n-1,k-1) + t_{\mathsf{rec}}(n-1,k) + O(1) \\
&\leq T_{\mathsf{rec}}(n-1) + T_{\mathsf{rec}}(n-1) + O(1) \\
&= 2T_{\mathsf{rec}}(n-1) + O(1).
\end{aligned}
$$

So $T_{\mathsf{rec}}(n) \leq 2T_{\mathsf{rec}}(n-1) + O(1)$ (because $T_{\mathsf{rec}}(n) = t_{\mathsf{rec}}(n,k)$ for some k). It follows from the lectures that $T_{\mathsf{rec}}(n) \in O(2^n)$.

(c) Give an asymptotic upper bound for $T_{\mathsf{iter}}(n)$. Justify your answer.

Solution: In the worst case, both `for` loops run $O(n)$ times each. All other operations are $O(1)$, including line 5 which is contained within both `for` loops. Therefore the running time of this algorithm is $O(n) \times O(n) \times O(1) = O(n^2)$.

(10 marks)



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 (max size 2Mb). In Linux, the following command

  ```
  pdfjoin --outfile output.pdf input1.pdf input2.pdf ...
  ```

  can be used to combine multiple pdf files. The command

  ```
  convert -density 150x150 -compress jpeg input.pdf output.pdf
  ```

  can be used to reduce the filesize of a pdf (change 150 to reduce/improve quality/filesize). Please ensure your files are legible before submitting.

- 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.