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,

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

So,

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

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

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

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

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

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

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

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 $V = \{1, 2, \dots, n\}$ 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.