These exercises are meant to resemble material we’ve covered in lecture on proofs and combining implication. You will receive 20% of the relevant marks for any portion you leave blank, or write “I cannot answer this” on.

You must write up your exercise alone. You may discuss general approaches to solutions with other students, but be very careful not to take notes (electronic, or on paper), and to wait an hour after such a conversation before writing up your solution.

Submit your work as a PDF file e2.pdf to the CDF secure web site:
https://www.cdf.toronto.edu/students/

1. Use the techniques from pages 30–31 of the course notes (Chapter 3 “Manipulation rules”) to verify the following equivalences. Indicate which rule (e.g. commutativity, associativity) you are using at each step.

Equivalence # 1: 

\[(P \Rightarrow R_1) \land (P \Rightarrow R_2) \Leftrightarrow (P \Rightarrow (R_1 \land R_2))\]

Sample solution: Since there are two versions of the distributive laws (\(\land\) over \(\lor\) versus \(\lor\) over \(\land\)), it’s easy to have too many transformations to choose from. However, in this case, starting from the right-hand side it seems pretty direct to transform it into the left-hand side.

\[(P \Rightarrow (R_1 \land R_2)) \Leftrightarrow (\neg P \lor (R_1 \land R_2)) \text{ implication}\]

\%(\neg P \lor (R_1 \land R_2)) \Leftrightarrow ((\neg P \lor R_1) \land (\neg P \lor R_2)) \text{ distribute } \lor \land\%

\%(\neg P \lor R_1) \land (\neg P \lor R_2)) \text{ implication}\%

Equivalence # 2: 

\[((R_1 \Rightarrow Q) \land (R_2 \Rightarrow Q)) \Leftrightarrow ((R_1 \lor R_2) \Rightarrow Q)\]

Sample solution: Begin with the right-hand side, and transform it into the left-hand side:

\[((R_1 \lor R_2) \Rightarrow Q) \Leftrightarrow (\neg (R_1 \lor R_2) \lor Q) \text{ implication}\]

\%(\neg (R_1 \lor R_2) \lor Q) \Leftrightarrow ((\neg R_1 \land \neg R_2) \lor Q) \text{ De Morgan’s}\%

\%(\neg R_1 \lor \neg R_2 \lor Q) \text{ distribute } \lor \land\%

\%(\neg R_1 \lor \neg R_2 \lor Q) \text{ implication}\%

2. Define two predicates, \(U(n)\) and \(V(n)\), on natural numbers as follows:

\[\forall n \in \mathbb{N} \quad U(n) \Leftrightarrow \exists k \in \mathbb{N}, n = 5k + 1\]

\[\forall n \in \mathbb{N} \quad V(n) \Leftrightarrow \exists j \in \mathbb{N}, n = 5j + 4\]

Use the proof structure from this course to prove each claim:
(i) \( \forall n \in \mathbb{N}, U(n) \Rightarrow U(n^2) \)

**Sample solution:** The structure here is for a universally-quantified implication.

Assume that \( n \) is a generic natural number.

Assume \( U(n) \). \# assume antecedent.

Then \( \exists k' \in \mathbb{N}, n = 5k' + 1 \). \# definition of \( U(n) \).

Let \( k \in \mathbb{N}, n = 5k + 1 \). \# instantiate existential

Then \( n^2 = 5(5k^2 + 2k) + 1 \). \# square both sides

Then \( \exists j \in \mathbb{N}, n^2 = 5j + 1 \).

\# \( j = 5k^2 + 2k \in \mathbb{N}, \) since \( 5, k, 2 \in \mathbb{N}, \) and \( n \) is closed under \(+ \) and \( \times \).

Then \( U(n^2) \). \# definition of \( U(n^2) \).

Then \( U(n) \Rightarrow U(n^2) \). \# assumed antecedent, derived consequent

Then \( \forall n \in \mathbb{N}, U(n) \Rightarrow V(n) \). \# introduced \( \forall \)

(ii) \( \forall n \in \mathbb{N}, V(n) \Rightarrow U(n^2) \)

**Sample solution:** Again, the structure is universally-quantified implication.

Assume \( n \) is a generic element of \( \mathbb{N} \)

Assume \( V(n) \). \# assume the antecedent

Then \( \exists k' \in \mathbb{N}, n = 5k' + 4 \). \# definition of \( V(n) \).

Pick \( k \in \mathbb{N}, n = 5k + 4 \). \# since it exists

Then \( n^2 = 5(5k^2 + 8k + 3) + 1 \). \# square both sides

Then \( \exists j \in \mathbb{N}, n^2 = 5j + 1 \).

\# \( j = 5k^2 + 8k + 3 \in \mathbb{N}, \) since \( 5, k, 8, 3 \in \mathbb{N} \) and \( \mathbb{N} \) is closed under \(+ \); \( \times \).

Then \( U(n^2) \). \# Use the definition of \( U(n^2) \)

Then \( V(n) \Rightarrow U(n^2) \). \# assumed antecedent, derived consequent

Then \( \forall n \in \mathbb{N}, V(n) \Rightarrow U(n^2) \). \# introduced \( \forall \)