

Compulsory Assignment 3

Alexander Bergenholtz
MNF130V2020

Due on: Friday 13 March 2020, 14:00

- Submit your assignment by leaving it in the box marked **MNF130** at the **reception of the Department of Informatics (Datablokken, 4th floor)**. The box will be available from Monday 9 March.
- If you cannot deliver the assignment in person, only use a **UiB Pullprint scanner** and **submit on Mitt**. Assignments sent by email, or from camera pictures instead of scans, or otherwise illegible, will not count as a valid submission and will not be graded.
- Write your answers **one-sided** (don't use both sides of a page), and start a new page for every exercise.
- Write **your name** on every page.
- You may write your answers in English or Norwegian.
- The assignment covers the entire syllabus covered during the lectures so far.
- The assignment is scored on **30 points**. Hence you need to score **at least 10.5 points to pass**.

1 Propositional and predicate logic (8 points)

- a) Fill out the truth table:

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r)$	$p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

- b) Let
- p, q, r
- be propositions. Is the compound proposition
- $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
- a tautology? Explain why/why not.

The compound proposition is a tautology, because it is true for all cases in the truth table.

By definition, a tautology is an assertion that is true in every possible case/interpretation.

□

- c) Let
- p, q, r
- be propositions. Use basic logical equivalences to prove that the compound propositions
- $(p \wedge \neg q) \rightarrow r$
- and
- $p \rightarrow (q \vee r)$
- are logically equivalent.

Write as disjunction.

$$(p \wedge \neg q) \rightarrow r \equiv \neg(p \wedge \neg q) \vee r$$

De Morgan.

$$\neg(p \wedge \neg q) \vee r \equiv (\neg p \vee q) \vee r$$

Associative laws.

$$(\neg p \vee q) \vee r \equiv \neg p \vee (q \vee r)$$

Logical equivalence for conditional statements.

$$\neg p \vee (q \vee r) \equiv p \rightarrow (q \vee r)$$

□

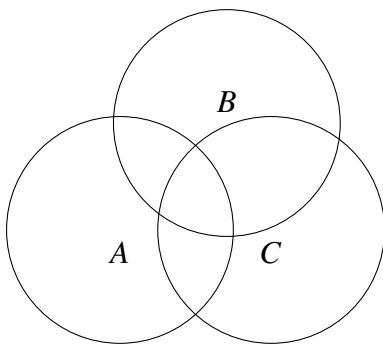
- d) What are the truth values of the statements
- $\forall n \exists m (n + m = 0)$
- and
- $\exists n \forall m (n < m^2)$
- if the domain for all variables consists of
- \mathbb{Z}
- , the set of all integers? Explain your answer.

- The first statement, $\forall n \exists m (n + m = 0)$ is **true**, because the domain of integers contains a negative/positive counterpart for every value. For the particular statement, it means that for all n , there exists a counterpart such that the sum will be 0. This works because there only has to exist a single m for any n value.
- The second statement, $\exists n \forall m (n < m^2)$ is **true**, because there has to exist a value of \mathbb{Z} such that all values in \mathbb{Z} squared are greater than this number. You can pick n to be a negative number, and all m values will be strictly greater. So the statement is true.

□

2 Set theory and functions (8 points)

- a) Let A, B, C be sets. Draw a Venn diagram and color the region $(A - C) \cap (C - B)$. Prove (using set identities) or disprove (give a counterexample) that $(A - C) \cap (C - B) = \emptyset$.



Let $x \in (A - C) \wedge x \in (C - B)$.

For the first part of the intersection, x is in A and not in C , for the second part of the intersection, x is in C and not in B .

Expanding this, we get:

$$x \in C \wedge \neg(x \in C)$$

Which is **F** by the negation law.

The proposition now looks like:

$$x \in A \wedge \neg(x \in B) \wedge F.$$

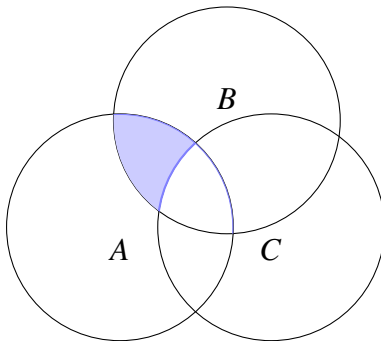
With set identities, this can be written as:

$$(A - C) \cap (C - B) \equiv (A \cap \overline{C}) \cap (C \cap \overline{B}) \equiv (A \cap \overline{B}) \cap (C \cap \overline{C})$$

$$(A \cap \overline{B}) \cap (C \cap \overline{C}) \equiv (A \cap \overline{B}) \cap \emptyset \equiv \emptyset$$

This means that $(A - C) \cap (C - B) \subseteq \emptyset$. And thus the initial proposition is a subset of the empty set. □

- b) Let A, B, C be sets. Draw a Venn diagram and color the region $(A - C) \cap (B - C)$. Prove (using set identities) or disprove (give a counterexample) that $(A - C) \cap (B - C) = \emptyset$.



Looking at the diagram, I will try to create a counterexample, because it looks like that's what's needed...

Let $A = B = \{1\}$ and $C = \emptyset$.

$$A - C = A - \emptyset = A = B = \{1\}.$$

$$B - C = B - \emptyset = B = A = \{1\}.$$

$$(A - C) \cap (B - C) = A \cap B = A \cap A = A = B = \{1\}.$$

$\{1\} \neq \emptyset$ and therefore we disproved the proposition by counterexample. \square

- c) Let $f(x) = x^2$ be a function from the set of real numbers to the set of real numbers. Is f one-to-one (injective)? Onto (surjective)? A one-to-one correspondence (bijective)? Explain why/why not.

- It is **not** injective for \mathbb{R} because multiple inputs will map to the same output. A quick example would be 3 and -3.
- It is also **not** surjective because the negative co-domain \mathbb{R}^- does not have pre-images mapping to them. No input x will map to a value $y < 0$. Thus is not surjective.
- It is also **not** bijective because it is neither injective or surjective. \square

3 Number theory (6 points)

- a) Let a be an integer that is not divisible by 3. Prove that $(a+1)(a+2)$ is divisible by 3.
- b) Use the Euclidean algorithm to find $\gcd(252, 356)$.

$356/252 = 1$, the remainder is 104. 356 can be written as $252 \cdot 1 + 104$. Continue with $\gcd(252, 104)$.

$252/104 = 2$, remainder 44. $252 = 104 \cdot 2 + 44$. $\gcd(104, 44)$.

$104/44 = 2$, remainder 16. $104 = 44 \cdot 2 + 16$. $\gcd(44, 16)$.

$44/16 = 2$, remainder 12. $44 = 16 \cdot 2 + 12$. $\gcd(16, 12)$

$16/12 = 1$, remainder 4. $16 = 12 \cdot 1 + 4$. $\gcd(12, 4)$

$12/4 = 3$. Greater common denominator with 356 and 252 is **3**. \square

- c) Find each of these values:

• $(177 \bmod 31 + 270 \bmod 31) \bmod 31$

$177 \bmod 31 = 22$ and $270 \bmod 31 = 22$.

Simplify the equation as $(22 + 22) \bmod 31 = 44 \bmod 31 = \mathbf{13}$. \square

• $[5(99^2 \bmod 32)] \bmod 15$

$99^2 = 9801$.

$9801 \bmod 32 = 9$.

$9 \cdot 5 = 45$.

$45 \bmod 15 = \mathbf{0}$. \square

4 Induction (8 points)

Use mathematical induction to prove that

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

for all integers $n \geq 1$.

Let $P(n) =$

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

- Basis step, verify $P(1)$ (smallest n in this case is 1).

$$P(1) = \sum_{k=1}^1 k^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6} \Rightarrow 1^2 = \frac{6}{6} = 1$$

- Next, we assume $P(m)$ is true for an arbitrary $m \geq 1$.
To write the function in terms of m :

$$P(m) = \sum_{k=1}^m k^2 = \frac{m(m+1)(2m+1)}{6}$$

- $P(m+1)$ can be written as:

$$\begin{aligned} P(m+1) &= \sum_{k=1}^m k^2 + (m+1)^2 = \frac{m(m+1)(2m+1)}{6} + (m+1)^2 \\ &= \frac{m(m+1)(2m+1) + 6(m+1)^2}{6} = \frac{m(m+1)(2m+1) + 6(m+1)(m+1)}{6} \\ &= \frac{(m+1)(m(2m+1) + 6(m+1))}{6} = \frac{(m+1)(m+2)(2(m+1)+1)}{6} \\ &= \frac{(m+1)((m+1)+1)(2(m+1)+1)}{6} \end{aligned}$$

Now we have shown that the basis is verified, and it will hold for $P(m)$ and some $P(m+1)$ where $m \geq 1$.

□