School of Mathematics and Physics, UQ

MATH1081 Advanced Discrete Mathematics
Semester 1 2025
Problem Set 1

Michael Kasumagic, 44302669
Tutorial Group #3
Due 5pm Friday 28 March 2025

Question 1: 10 marks

Prove that XOR satisfies the associative law; that is:

$$p \oplus (q \oplus r) \equiv (p \oplus q) \oplus r.$$

Solution:
Definition 1.1 (XOR). For two predicates, p and q, the XOR of them, denoted $p \oplus q \equiv (p \vee q) \wedge \sim(p \wedge q)$.

Theorem 1.1. XOR satisfies the associative law; that is: $p \oplus (q \oplus r) \equiv (p \oplus q) \oplus r$.

Proof. By considering all cases with a truth table.

p	q	r	$p \oplus q$	$q \oplus r$	$p \oplus (q \oplus r)$	$(p \oplus q) \oplus r$	$p \oplus (q \oplus r) \leftrightarrow (p \oplus q) \oplus r$
T	T	T	F	F	T	T	T
T	T	F	F	T	F	F	T
T	F	T	T	T	F	F	T
T	F	F	T	F	T	T	T
F	T	T	T	F	F	F	T
F	T	F	T	T	T	T	T
F	F	T	F	T	T	T	T
F	F	F	F	F	F	F	T

As we can see in the final column, $p \oplus (q \oplus r)$ is logically equivalent to $(p \oplus q) \oplus r$, for all possible value combinations of (p, q, r).
Therefore XOR satisfies the associative law. □

Which makes sense! Since the group $(\{T, F\}, \oplus)$ is isomorphic to $(\{0, 1\}, +)$ (which I won't prove here ☺).

Question 2: 10 marks

Using the laws of logical equivalence, prove that for any fixed $n \in \mathbb{N}$ and statement variables $p, q_1, q_2, \ldots, q_n$:

$$p \wedge (q_1 \oplus q_2 \oplus \ldots \oplus q_n) \equiv (p \wedge q_1) \oplus (p \wedge q_2) \oplus \ldots \oplus (p \wedge q_n)$$

Solution: Let's first make sure that $\wedge$ distributes over $\oplus$.

Theorem 2.1. For three statement variables, p, q_1, q_2, $p \wedge (q_1 \oplus q_2) \equiv (p \wedge q_1) \oplus (p \wedge q_2)$.

Proof. By considering all cases with a truth table.

p	q_1	q_2	$q_1 \oplus q_2$	$p \wedge q_1$	$p \wedge q_2$	$\mathcal{L} := p \wedge (q_1 \oplus q_2)$	$\mathcal{R} := (p \wedge q_1) \oplus (p \wedge q_2)$	$\mathcal{L} \leftrightarrow \mathcal{R}$
T	T	T	F	T	T	F	F	T
T	T	F	T	T	F	T	T	T
T	F	T	T	F	T	T	T	T
T	F	F	F	F	F	F	F	T
F	T	T	F	F	F	F	F	T
F	T	F	T	F	F	F	F	T
F	F	T	F	F	F	F	F	T
F	F	F	F	F	F	F	F	T

As we can see in the final column, $p \wedge (q_1 \oplus q_2)$ is logically equivalent to $(p \wedge q_1) \oplus (p \wedge q_2)$, for all possible value combinations of (p, q, r).
Therefore $\wedge$ distributes over $\oplus$. $\square$

Theorem 2.2. For a fixed $n \in \mathbb{N}$, and statement variables $p, q_1, q_2, \ldots, q_n$, $p \wedge (q_1 \oplus q_2 \oplus \ldots \oplus q_n) \equiv (p \wedge q_1) \oplus (p \wedge q_2) \oplus \ldots \oplus (p \wedge q_n)$.

Note: I will express $(q_1 \oplus q_2 \oplus \ldots \oplus q_n) \equiv \bigoplus_{i=1}^{n} q_i$.

Proof. Suppose $n \in \mathbb{N}$ is fixed and $p, q_1, q_2, \ldots, q_n$ are statement variables.

Let's consider $p \wedge \left(\bigoplus_{i=1}^{n} q_i\right) \equiv p \wedge \left(q_1 \oplus \bigoplus_{i=2}^{n} q_i\right)$.

Let's define a statement variable $r_2 = \bigoplus_{i=2}^{n} q_i$.

Then we can rewrite the statement $p \wedge \left(\bigoplus_{i=1}^{n} q_i\right) \equiv p \wedge (q_1 \oplus r_2)$.

We can apply Theorem 2.1, $p \wedge \left(\bigoplus_{i=1}^{n} q_i\right) \equiv (p \wedge q_1) \oplus \left(p \wedge \bigoplus_{i=2}^{n} q_i\right)$.

We can repeat this for $r_3 = \bigoplus_{i=3}^{n} q_i$, and applying Theorem 2.1,

$$p \wedge \left(\bigoplus_{i=1}^{n} q_i\right) \equiv (p \wedge q_1) \oplus (p \wedge q_2) \oplus (p \wedge r_3) \equiv (p \wedge q_1) \oplus (p \wedge q_2) \oplus \left(p \wedge \bigoplus_{i=3}^{n} q_i\right)$$

We can continue this process, repeatedly taking $r_k = \bigoplus_{i=k}^{n} q_i,\ k \le n$, and then distributing $p\wedge$, according to Theorem 2.1.

Eventually, when $k = n,\ r_k \equiv r_n \equiv \bigoplus_{i=k=n}^{n} q_i \equiv q_n$,

and $p \wedge \left(\bigoplus_{i=1}^{n} q_i \right) \equiv \bigoplus_{i=1}^{n-1} (p \wedge q_i) \oplus (p \wedge r_n) \equiv \bigoplus_{i=1}^{n} (p \wedge q_i)$.

which is equivalent to $(p \wedge q_1) \oplus \ldots \oplus (p \wedge q_n)$, which is what we wanted to show.

Therefore, $p \wedge (q_1 \oplus q_2 \oplus \ldots \oplus q_n) \equiv (p \wedge q_1) \oplus (p \wedge q_2) \oplus \ldots \oplus (p \wedge q_n)$ $\square$

Question 3: 10 marks

Show that the following argument is valid, using the rules of inference and/or logical equivalences. Clearly label which rule you used in each step.

$$
\begin{array}{ll}
1. & r \to \sim a \\
2. & \sim r \to \sim b \\
3. & \sim c \to a \\
4. & \sim c \to b \\
\hline
\therefore & c
\end{array}
$$

Solution:

$$
\begin{array}{lll}
1. & r \to \sim a & \\
2. & \sim r \to \sim b & \\
3. & \sim c \to a & \\
4. & \sim c \to b & \\
5. & a \to \sim r & \text{(Contrapositive of 1.)} \\
6. & a \to \sim b & \text{(Transitivity of 5. and 2.)} \\
7. & \sim b \to c & \text{(Contrapositive of 4.)} \\
8. & a \to c & \text{(Transitivity of 6. and 7.)} \\
9. & \sim c \to \sim a & \text{(Contrapositive of 8.)} \\
10. & (\sim c \to a) \wedge (\sim c \to \sim a) & \text{(Conjunction of 3. and 9.)} \\
11. & (c \vee a) \wedge (c \vee \sim a) & \text{(Logically Equivalent to 10. (Def. of } \to\text{))} \\
12. & c \vee (a \wedge \sim a) & \text{(Logically Equivalent to 10. (Distributivity))} \\
13. & c \vee \perp & \text{(Logically Equivalent to 10. (Negation))} \\
14. & c & \text{(Logically Equivalent to 10. (Identity))} \\
\hline
\therefore & c &
\end{array}
$$

Question 4: 10 marks

Let D be some domain, and let $p(x)$ and $q(x)$ be predicates in the variable $x \in D$. Write the following English sentences symbolically, i.e., using logical symbols, logical operations, and/or quantifiers. Your answers should not contain any English other than possibly the phrase "such that".

(a) $p(x)$ is never true.

(b) $p(x)$ is a necessary condition for $q(x)$.

(c) It is impossible for $p(x)$ and $q(x)$ to both be true for the same value of x.

(d) Every x satisfies exactly one of $p(x)$ or $q(x)$ (not both).

(e) There is exactly one value of x (no more, no less) for which $p(x)$ is true.

Solution:

(a) $\forall x \in D, \sim p(x)$

(b) $\forall x \in D, q(x) \rightarrow p(x)$

(c) $\forall x \in D, \sim(q(x) \wedge p(x))$

(d) $\forall x \in D, (p(x) \wedge \sim q(x)) \vee (q(x) \wedge \sim p(x))$

(e) $\exists x \in D : p(x) \wedge \forall y \in D,\ p(y) \rightarrow (y = x)$

Question 5: 10 marks

(a) Prove that for all integers $n \in \mathbb{N}$, if n is prime and $n > 2$ then n is odd.

(b) Prove that for all integers $n \in \mathbb{N}$, if $n^2 + 3$ is prime then n is even.

(c) Prove that for all integers $n \in \mathbb{N}$, if $n^2 - 1$ is prime then $n^2 + 1$ is also prime.

Solution: (a)

Proof. The statement's contrapositive is $\forall n \in \mathbb{N}, n > 2,\ n$ is even $\rightarrow n$ is composite.

Suppose $n \in \mathbb{N}$, $n > 2$ and n is even.
Then $n = 2k,\ k \in \mathbb{Z}$.
Hence, $2 \mid 2k \iff 2 \mid n$.
Therefore n is composite.
Therefore, $\forall n \in \mathbb{N}, n > 2,\ n$ is even $\rightarrow n$ is composite.

Therefore, $\forall n \in \mathbb{N}, n > 2,\ n$ is prime $\rightarrow n$ is odd.

$\square$

Solution: (b)

Proof. The statement's contrapositive is $\forall n \in \mathbb{N},\ n$ is odd $\rightarrow n^2 + 3$ is composite.

Suppose $n \in \mathbb{N}$ and n is odd.
Then, $n = 2k + 1,\ k \in \mathbb{Z}$.
Hence, $n^2 + 3 = (2k+1)^2 + 3 = 4k^2 + 4k + 1 + 3 = 4k^2 + 4k + 4$.
So, $n^2 + 3 = 2(2k^2 + 2k + 2) \iff 2 \mid n^2 + 3$.
Therefore, n is even. Therefore, $\forall n \in \mathbb{N},\ n$ is odd $\rightarrow n^2 + 3$ is composite.

Therefore, $\forall n \in \mathbb{N},\ n^2 + 3$ is prime $\rightarrow n$ is even.

$\square$

Solution: (c)

Proof. The statement's contrapositive is $\forall n \in \mathbb{N},\ n^2 + 1$ is composite $\rightarrow n^2 - 1$ is composite

Suppose $n \in \mathbb{N}$, $n^2 + 1$ is composite.
We note that $n^2 - 1$ can be factorised into $(n+1)(n-1)$.

For n=1, $(n+1)(n-1) = 2 \cdot 0 = 0 \notin \mathbb{N}$, so we can discard this case.

For n=2, $(n+1)(n-1) = 3 \cdot 1 = 3$, is not composite!
However, $n^2 + 1 = 5$, is not composite. Since the premise of the implication is not true, we can actually discard this case.

For n>2, $n + 1 > 2$, $n - 1 \geq 2$.
Which means, $n^2 - 1$ can be factorised into at least two factors.

This is the definition of composite, hence, $n^2 - 1$ is composite.

Therefore $\forall n \in \mathbb{N},\ n^2 + 1$ is composite $\rightarrow n^2 - 1$ is composite.

Therefore $\forall n \in \mathbb{N},\ n^2 - 1$ is prime $\rightarrow n^2 + 1$ is prime.

$\square$

Question 6: 10 marks

(a) Prove that there are infinitely many odd integers $n \in \mathbb{N}$ for which n and $n+100$ are both composite.

(b) Prove that there are infinitely many odd integers $n \in \mathbb{N}$ for which n, $n+2$, $n+4$, $n+6$, $\ldots$, $n+1000$ are all composite.

Solution: (a)

Proof. Directly.

Suppose $k \in \mathbb{N}$.
Choose $n = 5(2k+1) \in \mathbb{N}$.

Then $5 \mid n$, since 5 is trivially a factor.
Hence n is composite.
Consider, $n = 5(2k+1) = 10k+5 = 2(5k+2)+1 \iff 2 \nmid n$.
Hence, n is odd.

Consider $n+100 = 5(2k+1)+100 = 25k+5+100 = 25k+105 = 5(5k+21)$.
Since $5 \mid (n+100)$, then $n+100$ is composite.
Consider $n+100 = 5(2k+1)+100 = 25k+5+100 = 25k+105 = 2(12k+52)+(k+1) \iff 2 \nmid (n+100)$.
Hence, $n+100$ is odd.

Since there are infinite natural numbers k, there are infinite $n = 5(2k+1)$s.
Therefore, there are infinitely many odd integers, n for which n and $n+100$ are composite. $\square$

Solution: (b)

Proof. Directly.

Suppose $k \in \mathbb{N}$.
Choose $n = 2(1001!k+1)+1$. Therefore, n is odd.

$$\begin{aligned} n &= 2(1001!k+1)+1 \\ &= 2 \cdot 1001!k + 2 + 1 \\ &= 2 \cdot 1001!k + 3 \\ &= 3\left(\frac{2 \cdot 1001!k}{3} + 1\right) \end{aligned}$$

Therefore, n is composite.

Next, we'll consider $n+2$

$$\begin{aligned} n+2 &= 2(1001!k+1)+3 \\ &= 2 \cdot 1001!k + 2 + 3 \\ &= 2 \cdot 1001!k + 5 \\ &= 5\left(\frac{2 \cdot 1001!k}{5} + 1\right) \end{aligned}$$

Therefore, $n+2$ is composite.

Finally, we'll consider $n+1000$

$$n+1000 = 2(1001!k+1)+1001$$

$$
\begin{aligned}
&= 2 \cdot 1001!k + 2 + 1001 \\
&= 2 \cdot 1001!k + 1003 \\
&= 1001\,(2 \cdot 1000!k + 1)
\end{aligned}
$$

Therefore, n is composite.

In general, for every $m \in \{0, 2, 4, \ldots, 1000\}$, we can always factorise the expression

$$
n + m = 2(1001!k + 1) + 1 + m = (m + 1)\left(\frac{2 \cdot 1001!k}{m + 1} + 1\right)
$$

which shows that all of these numbers we've found are composite.

Since there are infinite natural numbers k, there are infinite n's $= 2(1001!k + 1) + 1$ with $n + m,\ \forall m \in \{0, 2, \ldots, 1000\}$ are all composite.

Therefore, there are infinitely many odd integers, n for which $n + m,\ \forall m \in \{0, 2, \ldots, 1000\}$ are composite.

$\square$