

## Sample Midterm

---

# CSCA67 - Discrete Mathematics

---

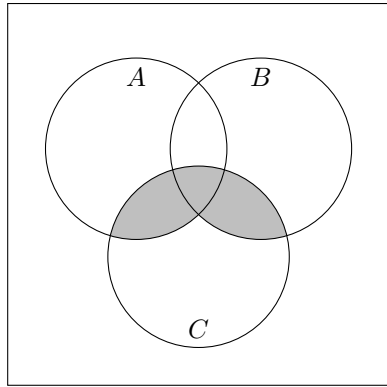


### Instructors:

	<b>Dr. Anna Bretscher</b>	<b>Dr. Richard Pancer</b>
<b>Email:</b>	bretscher@utsc.utoronto.ca	pancer@utsc.utoronto.ca
<b>Office:</b>	IC493	IC490
<b>Office Hours:</b>	Monday 12:10 - 1:30 Wednesday 1:10 - 2:00 Friday 1:10 - 2:00 (will change after week 6)	Monday 11:10 - 12:30 Friday 1:30 - 3:00

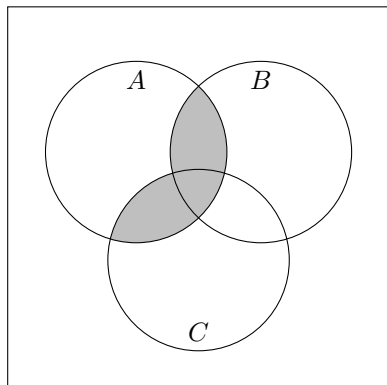
**Question 1.**

**Part (a)** Each option below is a predicate formula. Circle all (I bolded ones that i think are correct) answers equivalent to the given.



- (a)  $a \wedge b \wedge c$   
**(b)**  $(a \wedge c) \vee (b \wedge c)$   
**(c)**  $(\neg b \rightarrow a) \wedge c$   
**(d)**  $c \wedge (b \vee a)$   
 (e) None

**Part (b)** Write a propositional statement using  $\rightarrow$  and  $\neg$  if necessary equivalent to regions 3, 5, and 6. marks you can leave your solution using  $\wedge, \vee, \neg$  and  $\rightarrow$ . You do not need to specify which equivalence laws you use if you need them.



- $(a \wedge b) \vee (a \wedge c)$   
 $a \wedge r(b \vee c)$   
 $\neg(a \rightarrow \neg(\neg b \rightarrow c))$

**Part (c)** Circle (I just bolded.) every statement equivalent to  $\neg a \rightarrow b$ .

- |                                   |  |
|-----------------------------------|--|
| <b>(a)</b> $\neg b \rightarrow a$ | <b>(f)</b> a is necessary for $\neg b$ |
| (b) $a \rightarrow \neg b$        | (g) $\neg a$ is necessary for b        |
| (c) a is sufficient for $\neg b$  | <b>(h)</b> b if $\neg a$               |
| (d) $\neg(a \wedge \neg b)$       | <b>(i)</b> $b \vee a$                  |
| (e) b is sufficient for $\neg a$  |  |

**Question 2.**

Determine whether  $\forall$  can be factored from an implication. In other words is

$$\forall x \in X, (p(x) \rightarrow q(x)) \iff \forall x \in X, p(x) \rightarrow \forall x \in X, q(x)$$

true? Explain your reasoning. Marks will only be given for your explanation.

No.

let  $p(x) = x > 5$  and  $q(x) = x^2 > 25$

$$\forall x \in \mathbb{Z}, (p(x) \rightarrow q(x)) \iff \forall x \in \mathbb{Z}, (x > 5 \rightarrow x^2 > 25)$$

which means: for all integers  $x$ , if  $x$  is greater than 5, then  $x^2$  is greater than 25.

vs.

$$\forall x \in \mathbb{Z}, p(x) \rightarrow \forall x \in \mathbb{Z}, q(x) \iff \forall x \in \mathbb{Z}, x > 5 \rightarrow \forall x \in \mathbb{Z}, x^2 > 25$$

which means: if all integers are greater than 5, then all integers squared are greater than 25.

Sometimes, factoring in  $\forall$  can lead to a statement that is true, but never equivalent.

$\forall x \in X, (p(x) \rightarrow q(x))$  is saying for every  $x$ , if predicate  $p$  is true, then predicate  $q$  is true.

$\forall x \in X, p(x) \rightarrow \forall x \in X, q(x)$  is saying for every  $x$ , if predicate  $p$  is true, then for every  $x$ , predicate  $q$  is true, since are not equivalent, therefore  $\forall$  cannot be factored into or from an implication.

**Question 3.**

Answer the following questions to construct a direct proof that:

$$\forall n \in \mathbb{N}, n \geq 2, \forall a, b \in \mathbb{N}, a \equiv_n b \rightarrow a^2 \equiv_n b^2$$

**Part (a)**

Write  $a$  and  $b$  in terms of  $n$  using the division theorem and taking into consideration any common variables.

$$\begin{aligned} a &= k_1 \cdot n + r \\ b &= k_2 \cdot n + r \\ k_1, k_2 &\in \mathbb{Z}, r \in [0, (n-1)] \end{aligned}$$

**Part (b)**

Now complete the proof.

Assume  $a \equiv_n b$ , then that means:

$$\begin{aligned} a &= k_1 \cdot n + r & a^2 &= k_1^2 \cdot n^2 + 2k_1 \cdot n + r^2 \\ b &= k_2 \cdot n + r & b^2 &= k_2^2 \cdot n^2 + 2k_2 \cdot n + r^2 \\ k_1, k_2 &\in \mathbb{Z}, r \in [0, (n-1)] \end{aligned}$$


---


$$\begin{aligned} a^2 &= k_1^2 \cdot n^2 + 2k_1 \cdot n + r^2 = n(k_1^2 \cdot n + 2k_1) + r^2 \\ b^2 &= k_2^2 \cdot n^2 + 2k_2 \cdot n + r^2 = n(k_2^2 \cdot n + 2k_2) + r^2 \end{aligned}$$

Since both  $a^2$  and  $b^2$  share the same remainder  $r^2$  when divided by  $n$ ,  
 $\therefore \forall n \in \mathbb{N}, n \geq 2, \forall a, b \in \mathbb{N}, a \equiv_n b \rightarrow a^2 \equiv_n b^2$ .

*QED*

**Question 4.**

Prove that  $\forall n \in \mathbb{N}, (n^2 - 1 \not\equiv_4 0) \rightarrow n$  is even.

Assume the contrapositive

$$n \in \{2k + 1\}, k \in \mathbb{Z} \rightarrow (n^2 - 1 \equiv_4 0)$$

$$\begin{aligned} n &= 2k + 1, k \in \mathbb{Z} \\ n^2 &= 4k^2 + 4k + 1 \\ n^2 - 1 &= 4k^2 + 4 = 4(k^2 + 1) \\ n^2 - 1 &\equiv_4 0 \end{aligned}$$

Since we prove the contrapositive to be true, and the contrapositive is logically equivalent to the original,  
 $\therefore n \in \{2k + 1\}, k \in \mathbb{Z} \rightarrow (n^2 - 1 \equiv_4 0)$

QED

**Question 5.**

**Part (a)** Write the following claim as an implication using quantifiers and  $\rightarrow$ . You may use  $p(x, y)$  to denote that  $x$  and  $y$  are relatively prime.

$a$  and  $n$  relatively prime is necessary for there to exist a unique natural number  $b < n$  such that  $a \cdot b \equiv_n 1$ .

$$\exists n \in \mathbb{N}, \exists: b < n, a \cdot b \equiv_n 1 \rightarrow \gcd(a, n) = 1$$

**Part (b)** Prove the claim.

Assume:  $\exists n \in \mathbb{N}, \exists: b < n, a \cdot b \equiv_n 1$

$$a \cdot b = n \cdot k + 1, k \in \mathbb{Z}$$

$$a \cdot b - n \cdot k = 1$$

---

**Bezout's Identity:**

if  $a$  and  $b$  are non zero integers, then there exists integers  $u$  and  $v$  such that:

$$\gcd(a, b) = au + bv$$

---

then by Bezout's Identity, since  $a \cdot b - n \cdot k$  is some linear combination that equals 1,

1 must be  $\gcd(a, n)$

$$a \cdot b - n \cdot k = 1 \rightarrow \gcd(a, n) = 1$$

$$\therefore \exists n \in \mathbb{N}, \exists: b < n, a \cdot b \equiv_n 1 \rightarrow \gcd(a, n) = 1$$

QED

**Question 6.**

Sorry, i just got chased out by care-takers in IC, i'll type up the rest tomorrow