CSI - 2101 Discrete Structures
Course 1

Jean-Lou De Carufel

Summer 2020

Course Outline

- Web page
  - `http://cglab.ca/~jdecaruf/CSI2101.html`
  - BrightSpace
- Office : jdecaruf @ uottawa dot ca
- The following book is very interesting.
  - Kenneth Rosen.
    Discrete Mathematics and Its Applications, 7th Edition.
    McGraw Hill, 2012.
- Evaluation

4 mini-tests :	15%
Exam 1 :	17.5%
Exam 2 :	17.5%
Final exam :	50%
Total :	100%

- Exercices
- Tutorials
- Mini-tests
- Exams

Mini-Tests

There will be four mini-tests during the semester. These mini-tests will take place on BrightSpace. Make sure you are equipped to **quickly** scan, or take a picture of, $2 \sim 3$ pages and create a pdf. You will have to answer each mini-test on a piece of paper and upload your answers to BrightSpace. No mini-tests will be accepted by email.

- Mini-Test 1 : May 21, 2020 from 11h30 to 12h00 (on BrightSpace)
- Mini-Test 2 : May 28, 2020 from 11h30 to 12h00 (on BrightSpace)
- Mini-Test 3 : June 25, 2020 from 11h30 to 12h00 (on BrightSpace)
- Mini-Test 4 : July 16, 2020 from 11h30 to 12h00 (on BrightSpace)

Exams

There will be two exams during the semester. These exams will take place on BrightSpace. Make sure you are equipped to **quickly** scan, or take a picture of, $5 \sim 6$ pages and create a pdf. You will have to answer each exam on a piece of paper and upload your answers to BrightSpace. No exam will be accepted by email.

- Exam 1 : June 4, 2020 from 11h30 to 12h50 (on BrightSpace)
- Exam 2 : July 2, 2020 from 11h30 to 12h50 (on BrightSpace)

There will be a 3 hour final exam. This exam will take place on BrightSpace. Make sure you are equipped to **quickly** scan, or take a picture of, $9 \sim 10$ pages and create a pdf. You will have to answer the final exam on a piece of paper and upload your answers to BrightSpace. No exam will be accepted by email.

Chapter 0 : Introduction

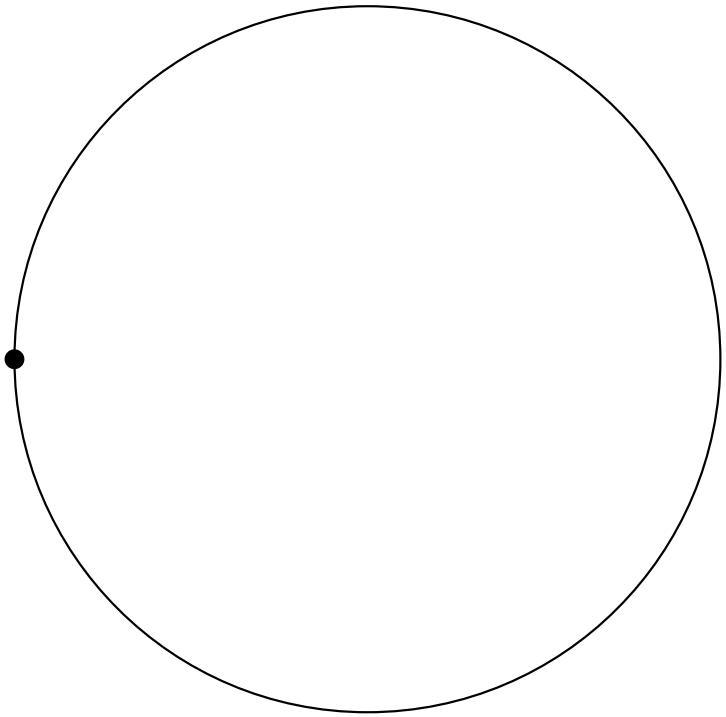
What do we study in « discrete math » ?

Why doing math ?

What is true ?

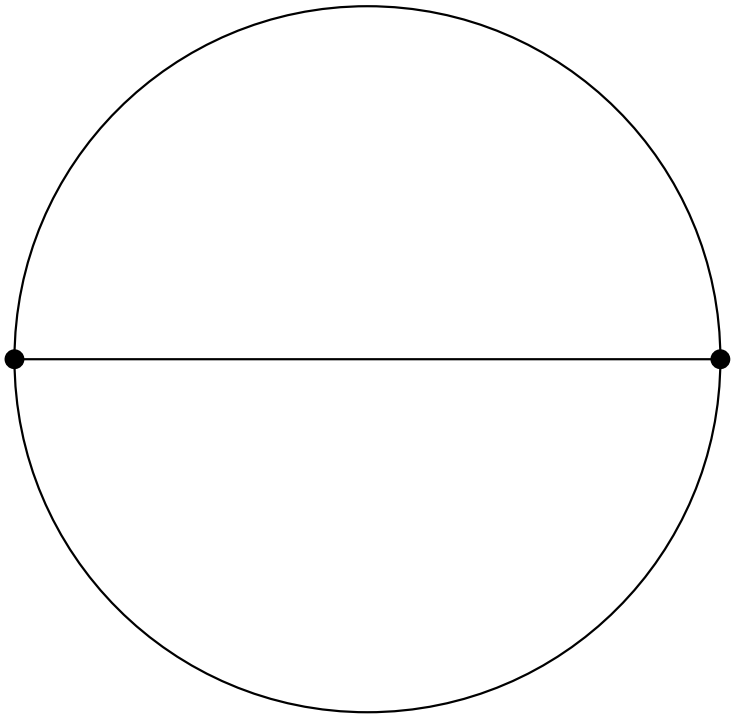
What is false ?

Place n points on a circle, and connect each pair of points by a line segment. What is the maximum number of regions we obtain inside the circle ?



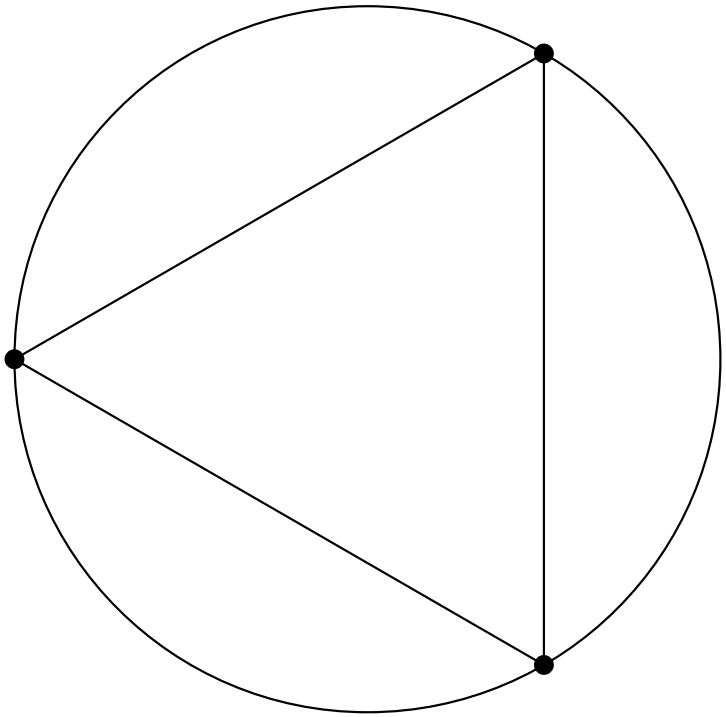
1 point $\longrightarrow$ 1 region

Place n points on a circle, and connect each pair of points by a line segment. What is the maximum number of regions we obtain inside the circle ?



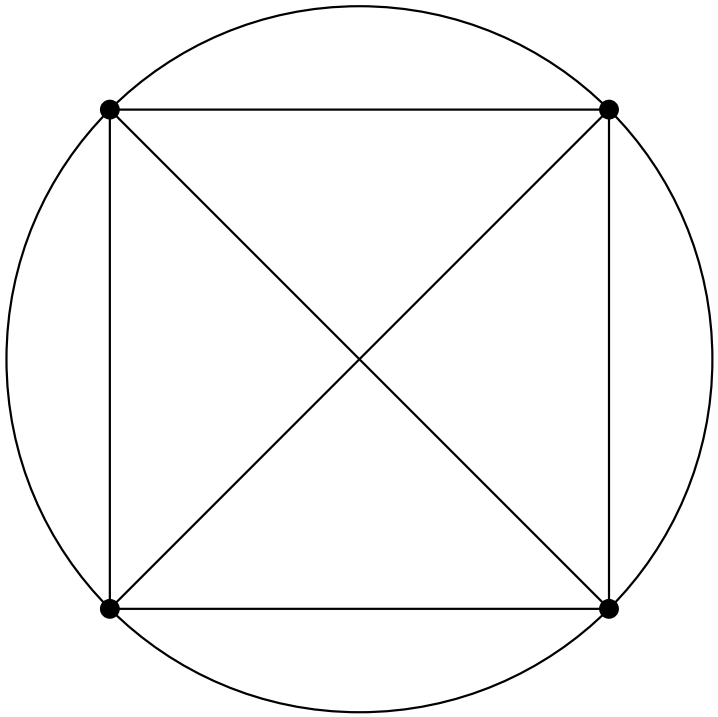
2 points $\longrightarrow$ 2 regions

Place n points on a circle, and connect each pair of points by a line segment. What is the maximum number of regions we obtain inside the circle ?



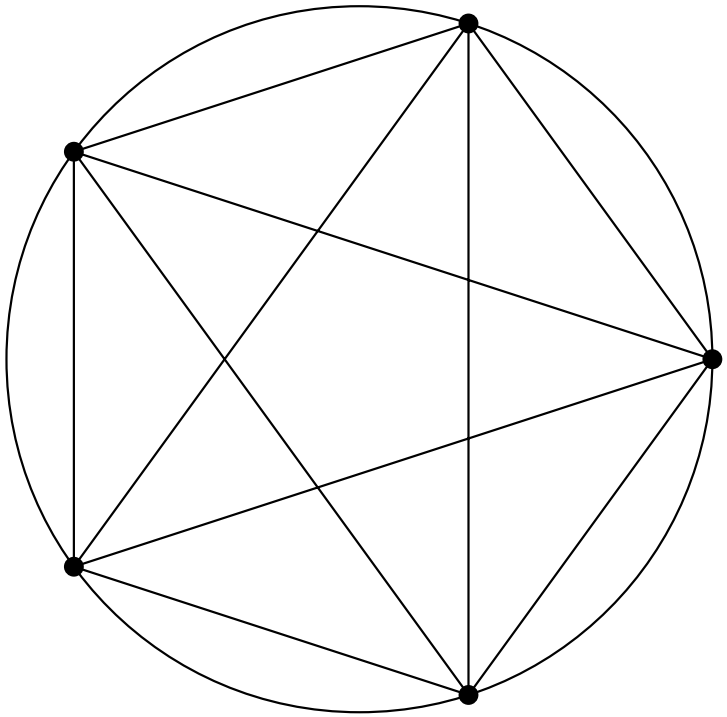
3 points $\longrightarrow$ 4 regions

Place n points on a circle, and connect each pair of points by a line segment. What is the maximum number of regions we obtain inside the circle ?



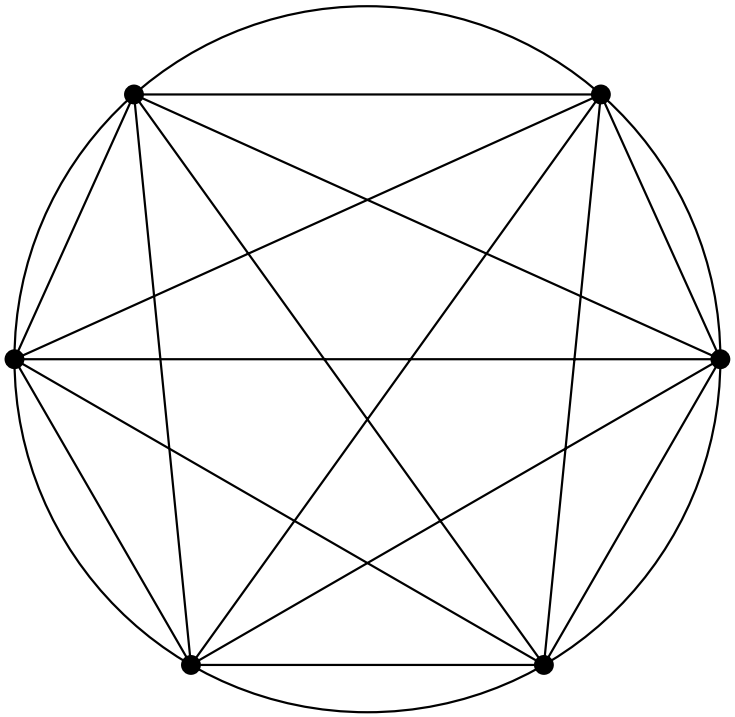
4 points $\longrightarrow$ 8 regions

Place n points on a circle, and connect each pair of points by a line segment. What is the maximum number of regions we obtain inside the circle ?



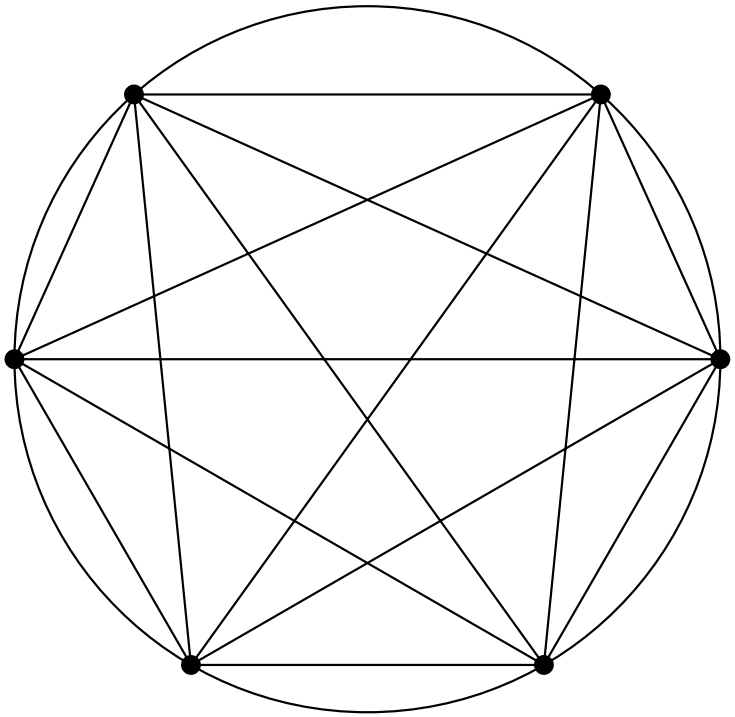
5 points $\longrightarrow$ 16 regions

Place n points on a circle, and connect each pair of points by a line segment. What is the maximum number of regions we obtain inside the circle ?



6 points $\longrightarrow$?? regions

Place n points on a circle, and connect each pair of points by a line segment. What is the maximum number of regions we obtain inside the circle ?



6 points $\longrightarrow$ 31 regions !

Consider the function

$$f(n) = n^2 + n + 41.$$

$f(0) = 41$ is a prime number.

Consider the function

$$f(n) = n^2 + n + 41.$$

$f(0) = 41$ is a prime number.

$f(1) = 43$ is a prime number.

Consider the function

$$f(n) = n^2 + n + 41.$$

$f(0) = 41$ is a prime number.

$f(1) = 43$ is a prime number.

$f(2) = 47$ is a prime number.

Consider the function

$$f(n) = n^2 + n + 41.$$

$f(0) = 41$ is a prime number.

$f(1) = 43$ is a prime number.

$f(2) = 47$ is a prime number.

$f(3) = 53$ is a prime number.

Consider the function

$$f(n) = n^2 + n + 41.$$

$f(0) = 41$ is a prime number.
$f(1) = 43$ is a prime number.
$f(2) = 47$ is a prime number.
$f(3) = 53$ is a prime number.
$f(4) = 61$ is a prime number.

Consider the function

$$f(n) = n^2 + n + 41.$$

$$\begin{aligned}
f(0) &= 41 && \text{is a prime number.} \\
f(1) &= 43 && \text{is a prime number.} \\
f(2) &= 47 && \text{is a prime number.} \\
f(3) &= 53 && \text{is a prime number.} \\
f(4) &= 61 && \text{is a prime number.} \\
f(5) &= 71 && \text{is a prime number.} \\
&\vdots
\end{aligned}$$

Consider the function

$$f(n) = n^2 + n + 41.$$

$$\begin{aligned}
f(0) &= 41 && \text{is a prime number.}\\
f(1) &= 43 && \text{is a prime number.}\\
f(2) &= 47 && \text{is a prime number.}\\
f(3) &= 53 && \text{is a prime number.}\\
f(4) &= 61 && \text{is a prime number.}\\
f(5) &= 71 && \text{is a prime number.}\\
&\vdots\\
f(39) &= 1601 && \text{is a prime number.}
\end{aligned}$$

Consider the function

$$f(n) = n^2 + n + 41.$$

$$\begin{aligned}
f(0) &= 41 && \text{is a prime number.}\\
f(1) &= 43 && \text{is a prime number.}\\
f(2) &= 47 && \text{is a prime number.}\\
f(3) &= 53 && \text{is a prime number.}\\
f(4) &= 61 && \text{is a prime number.}\\
f(5) &= 71 && \text{is a prime number.}\\
&\vdots\\
f(39) &= 1601 && \text{is a prime number.}\\
f(40) &= 1681
\end{aligned}$$

Consider the function

$$f(n) = n^2 + n + 41.$$

$$\begin{aligned}
f(0) &= 41 && \text{is a prime number.}\\
f(1) &= 43 && \text{is a prime number.}\\
f(2) &= 47 && \text{is a prime number.}\\
f(3) &= 53 && \text{is a prime number.}\\
f(4) &= 61 && \text{is a prime number.}\\
f(5) &= 71 && \text{is a prime number.}\\
&\vdots\\
f(39) &= 1601 && \text{is a prime number.}\\
f(40) &= 1681 && = 41^2
\end{aligned}$$

How can we make sure that a program is correct ?

How can we prove that no input will lead to an infinite loop ?

How to make sure that a cryptographic protocol is safe ?

Do you know about the mission Mars Probe from 1999 ?

Chapiter 1 : Logic and Proof Techniques

Definition

A *proposition* is a sentence that is either true or false (not both !)

We can combine propositions to obtain a new proposition. In order to do that, we use *logical connectives*.

Symbol	Name	Intuition
$\neg$	negation	« not »
$\wedge$	conjunction	« and »
$\vee$	disjunction	« or »
$\rightarrow$	implication	« if ... then »
$\leftrightarrow$	equivalence	« is and only if »
$\oplus$	exclusive or	« either »

We represent the behaviour of logical connectives with *truth tables*.

(Refer to your MAT-1348 course notes.)

Propositional Functions and Quantifiers

The mathematical sentence

$$x > 5$$

is not a proposition (because it is neither true nor false.)

However, this is a *propositional function*. By giving a value to x, the sentence becomes a proposition. Let us denote this propositional function by $P(x)$. We have

$$\begin{aligned} P(x) &= \text{“}x > 5'' \\ P(0) &= \text{“}0 > 5'' \qquad \text{which is false.} \\ P(6) &= \text{“}6 > 5'' \qquad \text{which is true.} \end{aligned}$$

Hence, the truth value depends on the *domain* of the variable x. If the domain of x is $\{6, 7, 8, 9\}$, then $P(x)$ is true for all possible values of x in its domain. Indeed,

$$\begin{aligned} P(6) &= \text{“}6 > 5'' && \text{which is true.} \\ P(7) &= \text{“}7 > 5'' && \text{which is true.} \\ P(8) &= \text{“}8 > 5'' && \text{which is true.} \\ P(9) &= \text{“}9 > 5'' && \text{which is true.} \end{aligned}$$

Hence, the truth value depends on the *domain* of the variable x. If the domain of x is $\{6, 7, 8, 9\}$, then $P(x)$ is true for all possible values of x in its domain. Indeed,

$$\begin{aligned} P(6) &= \text{“}6 > 5'' \qquad \text{which is true.} \\ P(7) &= \text{“}7 > 5'' \qquad \text{which is true.} \\ P(8) &= \text{“}8 > 5'' \qquad \text{which is true.} \\ P(9) &= \text{“}9 > 5'' \qquad \text{which is true.} \end{aligned}$$

We could also write

$$P(6) \wedge P(7) \wedge P(8) \wedge P(9)$$

or

$$\forall x \; P(x)$$

$\ll$ for all x, $P(x)$ $\gg$.

If the domain of x is $\{3, 4, 5, 6, 7, 8\}$, then $P(x)$ is not true for all possible values of x in its domain. However, $P(x)$ is true for at least one value of x. Indeed, $P(7)$ is true.

If the domain of x is $\{3, 4, 5, 6, 7, 8\}$, then $P(x)$ is not true for all possible values of x in its domain. However, $P(x)$ is true for at least one value of x. Indeed, $P(7)$ is true.

We can also write

$$P(3) \vee P(4) \vee P(5) \vee P(6) \vee P(7) \vee P(8)$$

or

$$\exists x \; P(x)$$

$\ll$ there exists x such that $P(x)$ $\gg$.

Example : Suppose that the domain of x is the set of all human beings (dead or alive). Let us consider

$$P(x) = \text{“}x \text{ is a toddler.”}$$

we then have that $P(\text{Donald Trump})$ is false...

$\forall$ and $\exists$ are named *quantifiers*. We can combine logical connectives and quantifiers.

Example : Suppose that the domain of x is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

- $\forall x\ P(x)$

Example : Suppose that the domain of x is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$

Example : Suppose that the domain of x is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ is false since $P(2) \equiv \text{“}2^2 = 2''$ is false.

Example : Suppose that the domain of x is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ is false since $P(2) \equiv \text{“}2^2 = 2''$ is false.
- $\exists x\ P(x) \equiv$

Example : Suppose that the domain of x is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ is false since $P(2) \equiv \text{“}2^2 = 2''$ is false.
- $\exists x\ P(x) \equiv P(0) \vee P(1) \vee P(2) \vee P(3)$

Example : Suppose that the domain of x is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ is false since $P(2) \equiv \text{“}2^2 = 2''$ is false.
- $\exists x\ P(x) \equiv P(0) \vee P(1) \vee P(2) \vee P(3)$ is true since $P(1) \equiv \text{“}1^2 = 1''$ is true.

Example : Suppose that the domain of x is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

$\forall x\,(P(x) \vee Q(x))$ is true since

$$\begin{aligned}\forall x\,(P(x) \vee Q(x)) \;=\;& (P(0) \vee Q(0)) \\ & \wedge (P(1) \vee Q(1)) \\ & \wedge (P(2) \vee Q(2)) \\ & \wedge (P(3) \vee Q(3)) \\ =\;& (0^2 = 0 \vee 0 > 1) \\ & \wedge (1^2 = 1 \vee 1 > 1) \\ & \wedge (2^2 = 2 \vee 2 > 1) \\ & \wedge (3^2 = 3 \vee 3 > 1)\end{aligned}$$

is true.

Example : Suppose that the domain of x and y is $\{0, 1, 2, 3\}$. Let us consider

$$P(x) = \text{“}x^2 = x''$$
$$Q(x) = \text{“}x > 1''$$

$(\forall x\ P(x)) \vee (\forall y\ Q(y))$ is false since

- $\forall x\ P(x)$ is false (refer to the first example)
- and $\forall y\ Q(y)$ is false (since $0 > 1$ is false).

Example : Suppose that the domain of x is the set of all human beings (dead or alive). Let us consider.

$$S(x) = \text{“}x \text{ won the Stanley Cup.”}$$
$$F(x) = \text{“}x \text{ won the Super Bowl.”}$$

$\neg(\exists x\,(S(x) \wedge F(x)))$ is true. Indeed, nobody (as far as I know) won both the Stanley Cup and the Super Bowl.

Example : Suppose that the domain of x and y is the set of integers

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Prove or disprove :

$$\forall x \, \exists y \, (y > x)$$

In other words, for all integer x, we can always find an integer y such that $y > x$.

Example : Suppose that the domain of x and y is the set of integers

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Prove or disprove :

$$\forall x \, \exists y \, (y > x)$$

In other words, for all integer x, we can always find an integer y such that $y > x$.

Prove or disprove :

$$\exists x \, \forall y \, (y > x)$$

In other words, there exists an integer that is smaller that all other integers.

The negation of predicates

$$\neg(\forall x\ P(x)) \equiv \exists x\ \neg P(x)$$
$$\neg(\exists x\ P(x)) \equiv \forall x\ \neg P(x)$$

The negation of predicates

$$\neg(\forall x\ P(x)) \equiv \exists x\ \neg P(x)$$
$$\neg(\exists x\ P(x)) \equiv \forall x\ \neg P(x)$$

Hence,

$$\begin{aligned}\neg(\forall x\ \forall y\ P(x,y)) &\equiv \exists x\ \neg(\forall y\ P(x,y)) \\ &\equiv \exists x\ \exists y\ \neg P(x,y)\end{aligned}$$

$$\begin{aligned}\neg(\exists x\ \exists y\ P(x,y)) &\equiv \forall x\ \neg(\exists y\ P(x,y)) \\ &\equiv \forall x\ \forall y\ \neg P(x,y)\end{aligned}$$

etc !

Inference Rules

Given a collection of facts, what can we deduce ?

Example : If it snows today, we will sky. It snows today.

$$\frac{\begin{array}{lll} p & \rightarrow & q \\ p & & \end{array}}{q}$$

Therefore, we will sky !

Inference Rules

Given a collection of facts, what can we deduce ?

Example : If it snows today, we will sky. It snows today.

$$\frac{\begin{array}{ccc} p & \rightarrow & q \\ p & & \end{array}}{q}$$

Therefore, we will sky !

$((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology. This form of reasoning is called a *modus ponens*.

Example : If I am in the city of Ottawa, then I am in Ontario. I am in the province of Quebec.

$((p \to q) \wedge \neg q) \to \neg p$ is a tautology.

$$\begin{array}{ll} p & \to \quad q \\ \neg q & \\ \hline & \neg p \end{array}$$

Therefore, I am not in the city of Ottawa !

Example : If I am in the city of Ottawa, then I am in Ontario. I am in the province of Quebec.

$((p \to q) \wedge \neg q) \to \neg p$ is a tautology.

$$\begin{array}{lll} p & \to & q \\ \neg q & & \\ \hline & \neg p & \end{array}$$

Therefore, I am not in the city of Ottawa !

$((p \to q) \wedge \neg q) \to \neg p$ is a tautology. This form of reasoning is called a *modus tollens*.

Example : is the following reasoning valid ?

If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore, you did every problem in this book.

Is $((p \to q) \wedge q) \to p$ a tautology ?

Example : is the following reasoning valid ?

If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore, you did every problem in this book.

Is $((p \to q) \wedge q) \to p$ a tautology ?

NO ! Why ?

Example : is the following reasoning valid ?

If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore, you did every problem in this book.

Is $((p \to q) \wedge q) \to p$ a tautology ?

NO ! Why ?

If p is false and q is true, then $((p \to q) \wedge q) \to p$ is false.

Example : All human beings are mortal. Jean-Lou is a human being.

$$\frac{\forall x\ P(x)}{P(\text{Jean-Lou})}$$

Therefore, Jean-Lou is mortal !

This form of reasoning is called a *Universal Instantiation*.