CSI - 2101 Structures Discrètes
Cours 1

Jean-Lou De Carufel

Été 2020

Plan de cours

- Page web
  - `http://cglab.ca/~jdecaruf/CSI2101.html`
  - BrightSpace
- Bureau : jdecaruf @ uottawa dot ca
- Le livre suivant est très intéressant.
  - Kenneth Rosen.
    Discrete Mathematics and Its Applications, 7th Edition.
    McGraw Hill, 2012.
- Évaluations

4 mini-tests :	15%
Examen 1 :	17.5%
Examen 2 :	17.5%
Examen final :	50%
Total :	100%

- Exercices
- Tutoriels
- Mini-tests
- Examens

Mini-Tests

Il y aura quatre mini-tests pendant la session. Ces mini-tests auront lieu sur BrightSpace. Assurez-vous que vous êtes équipés pour **rapidement** numériser, ou prendre une photo de, environ $2 \sim 3$ pages et convertir en pdf. Vous devrez répondre à chacun des mini-tests sur une feuille de papier et uploader vos réponses sur BrightSpace. Aucun mini-test ne sera accepté par courriel.

- Mini-Test 1 : 21 mai 2020 de 11h30 à 12h00 (sur BrightSpace)
- Mini-Test 2 : 28 mai 2020 de 11h30 à 12h00 (sur BrightSpace)
- Mini-Test 3 : 25 juin 2020 de 11h30 à 12h00 (sur BrightSpace)
- Mini-Test 4 : 16 juillet 2020 de 11h30 à 12h00 (sur BrightSpace)

Examens

Il y aura deux examens pendant la session. Ces examens auront lieu sur BrightSpace. Assurez-vous que vous êtes équipés pour rapidement numériser, ou prendre une photo de, environ $5 \sim 6$ pages et convertir en pdf. Vous devrez répondre à chacun des examens sur une feuille de papier et uploader vos réponses sur BrightSpace. Aucun examen ne sera accepté par courriel.

- Examen 1 : 4 juin 2020 de 11h30 à 12h50 (sur BrightSpace)
- Examen 2 : 2 juillet 2020 de 11h30 à 12h50 (sur BrightSpace)

Il y aura un examen final d'une durée de 3 heures. Cet examen aura lieu sur BrightSpace. Assurez-vous que vous êtes équipés pour rapidement numériser, ou prendre une photo de, environ $9 \sim 10$ pages et convertir en pdf. Vous devrez répondre à l'examen final sur une feuille de papier et uploader vos réponses sur BrightSpace. Aucun examen ne sera accepté par courriel.

Chapitre 0 : Introduction

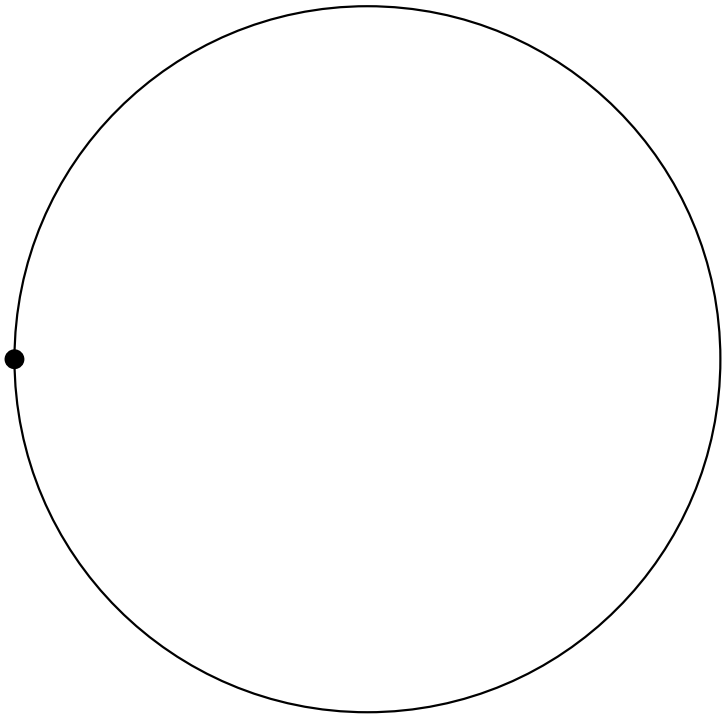
Qu'est-ce qu'on étudie en « mathématiques discrètes » ?

Pourquoi faire des mathématiques ?

Qu'est-ce qui est vrai ?

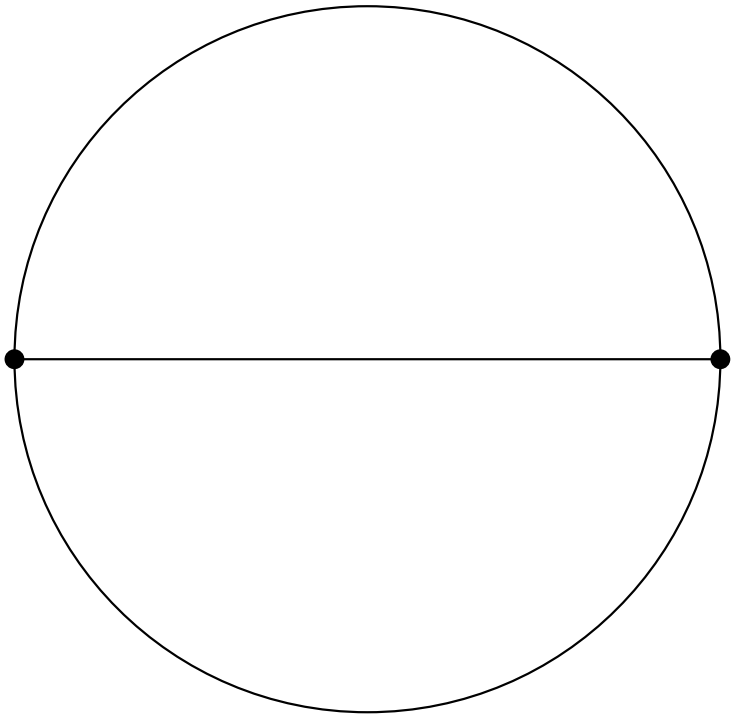
Qu'est-ce qui est faux ?

On place n points sur la circonférence d'un cercle et on trace tous les segments de droite possibles définis par ces points. Combien de régions obtient-on à l'intérieur du cerle au maximum ?



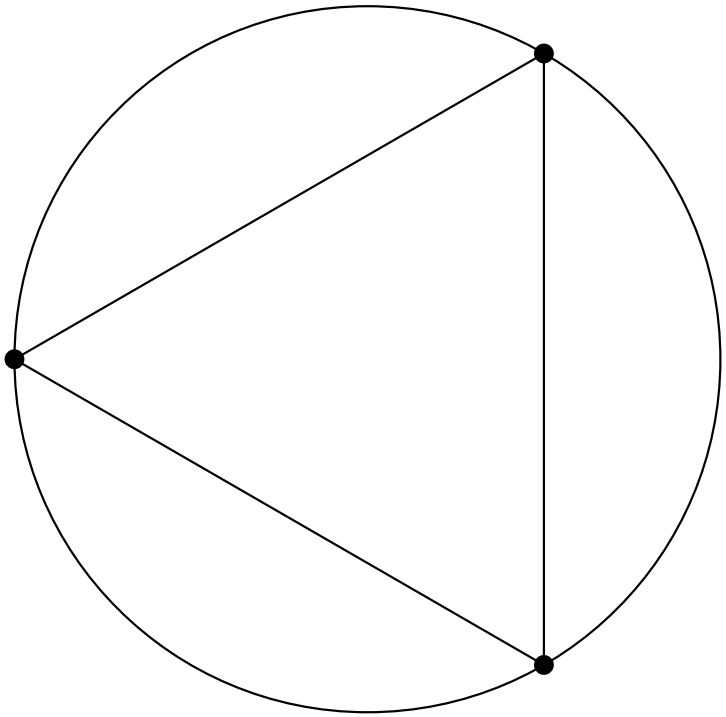
1 point $\longrightarrow$ 1 région

On place n points sur la circonférence d'un cercle et on trace tous les segments de droite possibles définis par ces points. Combien de régions obtient-on à l'intérieur du cerle au maximum ?



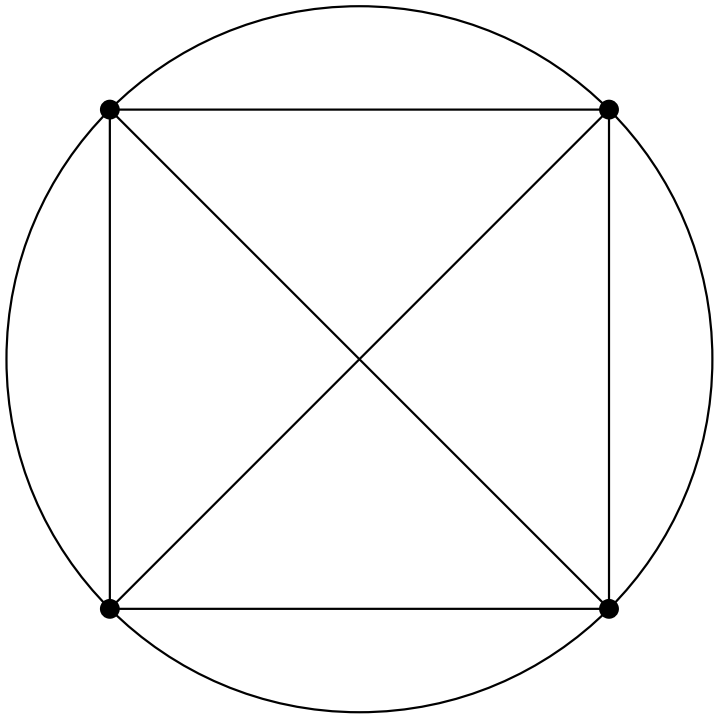
2 points $\longrightarrow$ 2 régions

On place n points sur la circonférence d'un cercle et on trace tous les segments de droite possibles définis par ces points. Combien de régions obtient-on à l'intérieur du cerle au maximum ?



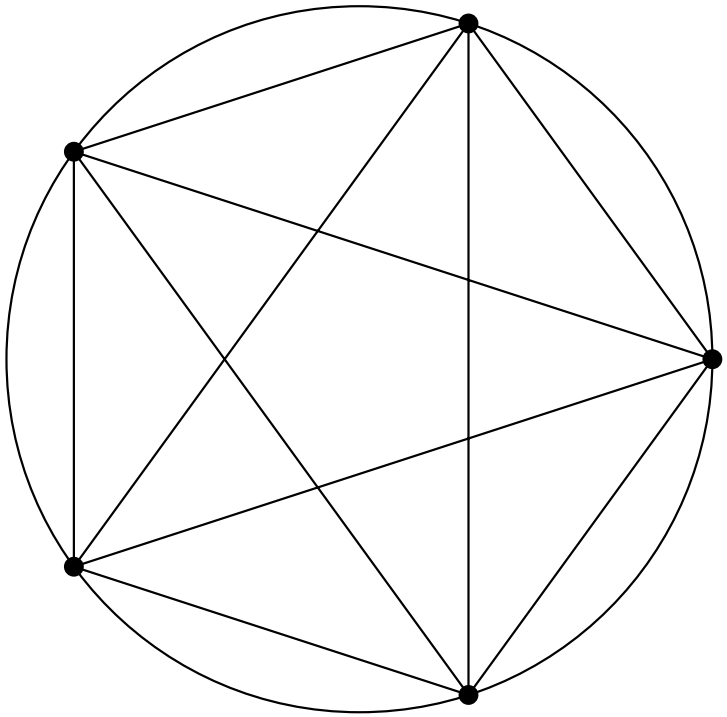
3 points $\longrightarrow$ 4 régions

On place n points sur la circonférence d'un cercle et on trace tous les segments de droite possibles définis par ces points. Combien de régions obtient-on à l'intérieur du cerle au maximum ?



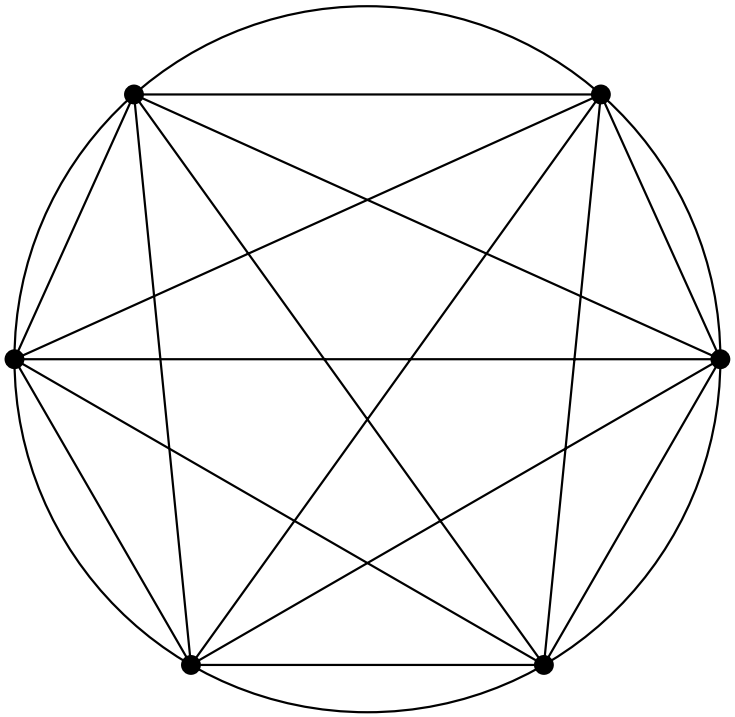
4 points $\longrightarrow$ 8 régions

On place n points sur la circonférence d'un cercle et on trace tous les segments de droite possibles définis par ces points. Combien de régions obtient-on à l'intérieur du cerle au maximum ?



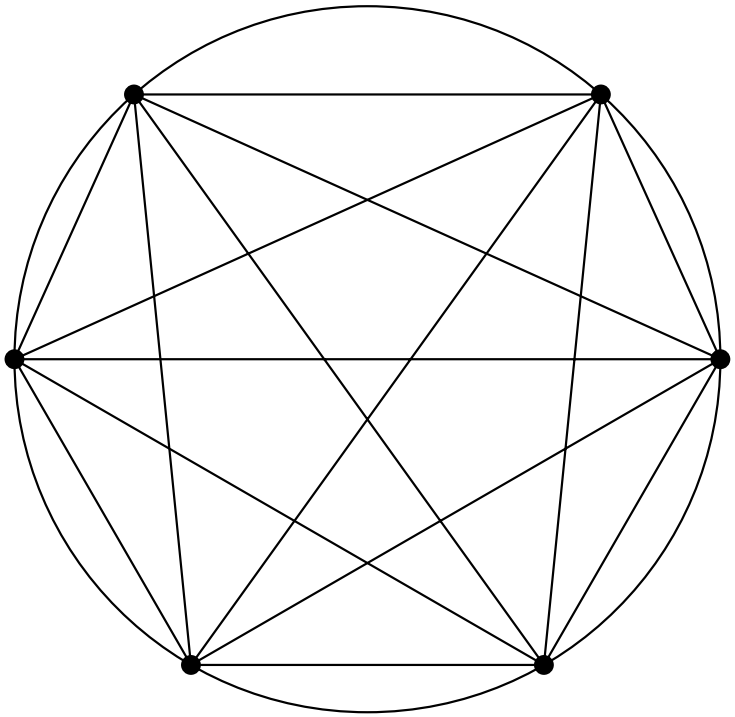
5 points $\longrightarrow$ 16 régions

On place n points sur la circonférence d'un cercle et on trace tous les segments de droite possibles définis par ces points. Combien de régions obtient-on à l'intérieur du cerle au maximum ?



6 points $\longrightarrow$?? régions

On place n points sur la circonférence d'un cercle et on trace tous les segments de droite possibles définis par ces points. Combien de régions obtient-on à l'intérieur du cerle au maximum ?



6 points $\longrightarrow$ 31 régions !

Considérons la fonction

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

$f(0) = 41$ est un nombre premier.

Considérons la fonction

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

$f(0) = 41$ est un nombre premier.

$f(1) = 43$ est un nombre premier.

Considérons la fonction

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

$f(0) = 41$ est un nombre premier.
$f(1) = 43$ est un nombre premier.
$f(2) = 47$ est un nombre premier.

Considérons la fonction

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

$f(0) = 41$ est un nombre premier.
$f(1) = 43$ est un nombre premier.
$f(2) = 47$ est un nombre premier.
$f(3) = 53$ est un nombre premier.

Considérons la fonction

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

$f(0) = 41$ est un nombre premier.
$f(1) = 43$ est un nombre premier.
$f(2) = 47$ est un nombre premier.
$f(3) = 53$ est un nombre premier.
$f(4) = 61$ est un nombre premier.

Considérons la fonction

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

$f(0) = 41$ est un nombre premier.
$f(1) = 43$ est un nombre premier.
$f(2) = 47$ est un nombre premier.
$f(3) = 53$ est un nombre premier.
$f(4) = 61$ est un nombre premier.
$f(5) = 71$ est un nombre premier.
$\vdots$

Considérons la fonction

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

$$\begin{aligned}
f(0) &= 41 && \text{est un nombre premier.}\\
f(1) &= 43 && \text{est un nombre premier.}\\
f(2) &= 47 && \text{est un nombre premier.}\\
f(3) &= 53 && \text{est un nombre premier.}\\
f(4) &= 61 && \text{est un nombre premier.}\\
f(5) &= 71 && \text{est un nombre premier.}\\
&\vdots\\
f(39) &= 1601 && \text{est un nombre premier.}
\end{aligned}$$

Considérons la fonction

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

$$\begin{aligned}
f(0) &= 41 && \text{est un nombre premier.}\\
f(1) &= 43 && \text{est un nombre premier.}\\
f(2) &= 47 && \text{est un nombre premier.}\\
f(3) &= 53 && \text{est un nombre premier.}\\
f(4) &= 61 && \text{est un nombre premier.}\\
f(5) &= 71 && \text{est un nombre premier.}\\
&\vdots\\
f(39) &= 1601 && \text{est un nombre premier.}\\
f(40) &= 1681
\end{aligned}$$

Considérons la fonction

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

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

Comment savoir si un programme est correct ?

Comment prouver qu'il n'existe pas d'input pour lequel le programme entre dans une boucle infinie ?

Comment s'assurer qu'un protocole cryptographique est sécuritaire ?

Avez-vous entendu parler de la mission Mars Probe qui date de 1999 ?

Chapitre 1 : Logique et Techniques de Preuve

Definition

Une *proposition* est une phrase qui est soit vraie soit fausse (mais pas les deux !)

On peut combiner des propositions pour obtenir une nouvelle proposition.
On utilise les *opérateurs logiques*.

Symbole	Nom	Intuition
$\neg$	négation	« non »
$\wedge$	conjonction	« et »
$\vee$	disjonction	« ou »
$\rightarrow$	implication	« si ... alors »
$\leftrightarrow$	équivalence	« si et seulement si »
$\oplus$	ou exclusif	« ou ... mais pas les deux »

On représente le comportement de ces opérateurs logiques à l'aide des *tables de vérité*.

(Voir les notes de cours de MAT-1748)

Formes propositionnelles et quantificateurs

La phrase mathématique

$$x > 5$$

n'est pas une proposition (parce n'elle n'a pas de valeur de vérité.)

Par contre, c'est une *forme propositionnelle*. En donnant une valeur à x, la phrase devient une proposition. Dénotons cette forme propositionnelle par $P(x)$. On a

$$\begin{aligned} P(x) &= \text{“}x > 5'' \\ P(0) &= \text{“}0 > 5'' \qquad \text{qui est faux.} \\ P(6) &= \text{“}6 > 5'' \qquad \text{qui est vrai.} \end{aligned}$$

Donc la valeur de vérité dépend du *domaine* de la variable x. Si le domaine de x est $\{6, 7, 8, 9\}$, alors $P(x)$ est vrai pour tous les x dans le domaine. En effet,

$$\begin{aligned} P(6) &= \text{“}6 > 5'' && \text{qui est vrai.} \\ P(7) &= \text{“}7 > 5'' && \text{qui est vrai.} \\ P(8) &= \text{“}8 > 5'' && \text{qui est vrai.} \\ P(9) &= \text{“}9 > 5'' && \text{qui est vrai.} \end{aligned}$$

Donc la valeur de vérité dépend du *domaine* de la variable x. Si le domaine de x est $\{6, 7, 8, 9\}$, alors $P(x)$ est vrai pour tous les x dans le domaine. En effet,

$$\begin{aligned} P(6) &= \text{“}6 > 5\text{”} \qquad \text{qui est vrai.} \\ P(7) &= \text{“}7 > 5\text{”} \qquad \text{qui est vrai.} \\ P(8) &= \text{“}8 > 5\text{”} \qquad \text{qui est vrai.} \\ P(9) &= \text{“}9 > 5\text{”} \qquad \text{qui est vrai.} \end{aligned}$$

On peut aussi écrire

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

ou encore

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

« pour tout x, $P(x)$ ».

Si le domaine de x est $\{3, 4, 5, 6, 7, 8\}$, $P(x)$ n'est pas vrai pour tout x dans ce domaine. Par contre, $P(x)$ est vrai pour au moins un x. En effet, $P(7)$ est vrai.

Si le domaine de x est $\{3, 4, 5, 6, 7, 8\}$, $P(x)$ n'est pas vrai pour tout x dans ce domaine. Par contre, $P(x)$ est vrai pour au moins un x. En effet, $P(7)$ est vrai.

On peut aussi écrire

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

ou encore

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

« il existe x tel que $P(x)$ ».

Exemple : supposons que le domaine de x est l'ensemble de tous les êtres humains (vivants ou décédés). Considérons

$$P(x) = \text{“}x \text{ est un bébé.”}$$

On a alors que $P(\text{Donald Trump})$ est faux.

$\forall$ et $\exists$ sont des *quantificateurs*. On peut combiner les opérateurs logiques et les quantificateurs.

Exemple : Supposons que le domaine de x est $\{0, 1, 2, 3\}$. Considérons

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

- $\forall x\ P(x)$

Exemple : Supposons que le domaine de x est $\{0, 1, 2, 3\}$. Considérons

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

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

Exemple : Supposons que le domaine de x est $\{0, 1, 2, 3\}$. Considérons

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

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ est faux parce que $P(2) \equiv \text{“}2^2 = 2''$ est faux.

Exemple : Supposons que le domaine de x est $\{0, 1, 2, 3\}$. Considérons

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

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ est faux parce que $P(2) \equiv \text{“}2^2 = 2''$ est faux.
- $\exists x\ P(x) \equiv$

Exemple : Supposons que le domaine de x est $\{0, 1, 2, 3\}$. Considérons

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

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ est faux parce que $P(2) \equiv \text{“}2^2 = 2''$ est faux.
- $\exists x\ P(x) \equiv P(0) \vee P(1) \vee P(2) \vee P(3)$

Exemple : Supposons que le domaine de x est $\{0, 1, 2, 3\}$. Considérons

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

- $\forall x\ P(x) \equiv P(0) \wedge P(1) \wedge P(2) \wedge P(3)$ est faux parce que $P(2) \equiv \text{“}2^2 = 2''$ est faux.
- $\exists x\ P(x) \equiv P(0) \vee P(1) \vee P(2) \vee P(3)$ est vrai parce que $P(1) \equiv \text{“}1^2 = 1''$ est vrai.

Exemple : Supposons que le domaine de x est $\{0, 1, 2, 3\}$. Considérons

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

$\forall x\,(P(x) \vee Q(x))$ est vrai parce que

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

est vrai.

Exemple : Supposons que le domaine de x et de y est $\{0, 1, 2, 3\}$. Considérons

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

$(\forall x\ P(x)) \vee (\forall y\ Q(y))$ est faux parce que

- $\forall x\ P(x)$ est faux (voir le premier exemple)
- et $\forall y\ Q(y)$ est faux (puisque $0 > 1$ est faux).

Exemple : Supposons que le domaine de x est l'ensemble de tous les êtres humains (vivants ou décédés). Considérons

$$S(x) = \text{“}x \text{ a gagné la Coupe Stanley.”}$$
$$F(x) = \text{“}x \text{ a remporté le Super Bowl.”}$$

$\neg(\exists x\,(S(x) \wedge F(x)))$ est vrai. En effet, personne n'a remporté et la Coupe Stanley et le Super Bowl.

Exemple : Supposons que le domaine de x et de y est l'ensemble des entiers

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

Vrai ou faux ? Démontrer.

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

Autrement dit, pour tout entier x, on peut toujours trouver un entier y tel que $y > x$.

Exemple : Supposons que le domaine de x et de y est l'ensemble des entiers

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

Vrai ou faux ? Démontrer.

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

Autrement dit, pour tout entier x, on peut toujours trouver un entier y tel que $y > x$.

Vrai ou faux ? Démontrer.

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

Autrement dit, il existe un entier x qui est plus petit que tous les entiers.

La négation des prédicats :

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

La négation des prédicats :

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

Donc

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

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

etc !

Règles d'inférence

Étant donné un ensemble de faits, que peut-on en déduire ?

Exemple : S'il neige aujourd'hui, nous irons skier. Il neige aujourd'hui.

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

Donc nous irons skier !

Règles d'inférence

Étant donné un ensemble de faits, que peut-on en déduire ?

Exemple : S'il neige aujourd'hui, nous irons skier. Il neige aujourd'hui.

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

Donc nous irons skier !

$((p \rightarrow q) \wedge p) \rightarrow q$ est une tautologie. Cette forme de déduction est appelée le *modus ponens*.

Exemple : Si je suis dans la ville d'Ottawa, alors je suis en Ontario. Je suis dans la province de Québec.

$((p \to q) \wedge \neg q) \to \neg p$ est une tautologie.

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

Donc je ne suis pas dans la ville d'Ottawa.

Exemple : Si je suis dans la ville d'Ottawa, alors je suis en Ontario. Je suis dans la province de Québec.

$((p \to q) \wedge \neg q) \to \neg p$ est une tautologie.

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

Donc je ne suis pas dans la ville d'Ottawa.

$((p \to q) \wedge \neg q) \to \neg p$ est une tautologie. Cette forme de déduction est appelée le *modus tollens*.

Exemple : Est-ce que le raisonnement suivant est valide ?

Si tu résouds tous les problèmes du livre, alors tu apprendras les mathématiques discrètes. Tu as appris les mathématiques discrètes. Donc tu as résolu tous les problèmes du livre.

Est-ce que $((p \to q) \wedge q) \to p$ est une tautologie ?

Exemple : Est-ce que le raisonnement suivant est valide ?

Si tu résouds tous les problèmes du livre, alors tu apprendras les mathématiques discrètes. Tu as appris les mathématiques discrètes. Donc tu as résolu tous les problèmes du livre.

Est-ce que $((p \to q) \wedge q) \to p$ est une tautologie ?

NON ! Pourquoi ?

Exemple : Est-ce que le raisonnement suivant est valide ?

Si tu résouds tous les problèmes du livre, alors tu apprendras les mathématiques discrètes. Tu as appris les mathématiques discrètes. Donc tu as résolu tous les problèmes du livre.

Est-ce que $((p \to q) \wedge q) \to p$ est une tautologie ?

NON ! Pourquoi ?

Si p est faux et q est vrai, alors $((p \to q) \wedge q) \to p$ est faux.

Exemple : Tous les êtres humains sont mortels. Jean-Lou est un être humain.

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

Donc Jean-Lou est mortel.

Cette forme de déduction est appelée l'*instanciation universelle*.