Logique propositionnelle

I) Logique classique bi-valuée

1. (a) Soit :
   L **:** « j'étudie la logique »
   H **:** « je serai heureux et sage »
   Alors on peut formaliser le raisonnement ainsi : $((L \Rightarrow H) \wedge H) \Rightarrow L$.
   Cependant ce raisonnement n'est pas valide. Dans le cas où $I(L) = 0$ et $I(H) = 1$, alors $I(L \Rightarrow H) = 1$, puis $I((L \Rightarrow H) \wedge H) = 1$, mais alors $I(((L \Rightarrow H) \wedge H) \Rightarrow L) = 0$.

   (b) Soit :
   N **:** « être Napoléon »
   A **:** « être Allemand »
   E **:** « être Européen »
   Alors on peut formaliser ainsi : $((N \Rightarrow A) \wedge (A \Rightarrow E)) \Rightarrow (N \Rightarrow E)$
   Ce raisonnement est valide.
   Cependant, on pourrait considérer que c'est une traduction pas tout à fait littérale de l'énoncé, et qu'il faudrait en fait une formule logique du premier ordre avec donc des variables, et une constante n (pour Napoléon).
   On aurait plutôt quelque chose comme $(A(n) \wedge \forall x(A(x) \Rightarrow E(x))) \Rightarrow E(n)$.
   Qui est valide aussi et traduit mieux l'énoncé, mais n'est pas propositionnelle.

2. Sans réfléchir, on regarde les lignes qui donnent V.
   On fait un « ou » des « et » (une disjonction des conjonctions) :

   $$(\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge Q \wedge R)$$

   On peut ici faire plus court :

   $$(\neg P \wedge (Q \Rightarrow R)) \vee (P \wedge Q \wedge R)$$

3. (a) Une formule valide évidente : $P \Rightarrow P$.
   Une un peu moins évidente : $((L \Rightarrow H) \wedge L) \Rightarrow H$.

   (b) Une formule satisfiable mais non valide : $A \Rightarrow B$.
   Elle est satisfaite quand $I(A) = 0$, mais fausse si $I(A) = 1$ et $I(B) = 0$.

   (c) Une formule insatisfiable évidente : $A \wedge \neg A$.

   (d) La négation d'une formule insatisfiable est valide.

4. La première affirmation est vraie, car le fait que $G \vee H$ soit insatisfiable implique qu'on a toujours $I(G \vee H) = 0$, ce qui n'est possible que si $I(G) = 0$ et $I(H) = 0$. Autrement dit, G et H sont insatisfiables.
   Autre manière de raisonner : On suppose que $G \vee H$ est insatisfiable, et on suppose que G et H ne sont pas toutes les deux insatisfiables. Sans perte de généralité on peut donc supposer que c'est G qui est satisfiable (le raisonnement suivant serait identique avec H). Dans ce cas, $G \vee H$ serait satisfiable, ce qui est contradictoire. Donc à la fois G et H sont insatisfiables.
   La seconde affirmation est fausse, car on peut avoir $I(G \vee H) = 1$ en ayant $I(G) = 0$ ou $I(H) = 0$, tant que l'interprétation de l'autre vaut 1. Exemple : $G = A \wedge \neg A$ (insatisfiable) et $H = B \Rightarrow B$ (valide). Alors $G \vee H$ est valide, alors que G ne l'est pas.

5. (a) Il suffit de montrer que l'on peut traduire tout connecteur de base à l'aide de la négation et de l'implication. C'est évidemment vrai pour l'implication. Il en reste deux :
   - $A \vee B$ est équivalent à $\neg A \Rightarrow B$
   - $A \wedge B$ est équivalent à $\neg(A \Rightarrow \neg B)$

   (b) On a :

$$\begin{aligned}
& (P \vee Q) \Leftrightarrow (R \vee S) \\
\equiv\ & ((P \vee Q) \Rightarrow (R \vee S)) \wedge ((R \vee S) \Rightarrow (P \vee Q)) \\
\equiv\ & ((\neg P \Rightarrow Q) \Rightarrow (\neg R \Rightarrow S)) \wedge ((\neg R \Rightarrow S) \Rightarrow (\neg P \Rightarrow Q)) \\
\equiv\ & \neg(((\neg P \Rightarrow Q) \Rightarrow (\neg R \Rightarrow S)) \Rightarrow \neg((\neg R \Rightarrow S) \Rightarrow (\neg P \Rightarrow Q))) \\
\equiv\ & \neg(((\neg P \Rightarrow Q) \Rightarrow \neg R \Rightarrow S) \Rightarrow \neg((\neg R \Rightarrow S) \Rightarrow \neg P \Rightarrow Q))
\end{aligned}$$

6. On remarque que $|$ est la négation de $\wedge$ (et réciproquement), et que si on échange les entrées du tableau de $|$, on obtient celui de $\vee$. Alors :
   - $A \wedge B$ s'écrit $\neg(A|B)$
   - $A \vee B$ s'écrit $(\neg A|\neg B)$

7. (a) L'implication est vraie si et seulement si $(m = 1)$ est fausse ou $(m = 2)$ est vraie. Autrement dit, si $m \neq 1$ ou $m = 2$. Cela revient à dire que pour toute valeur $m \neq 1$, la formule est vraie.

   (b) Ici, la réciproque devant être vraie également, il faut en plus que $m \neq 2$: pour toute valeur m telle que $m \neq 1$ et $m \neq 2$, la formule est vraie.

8. (a) Vraie si $I(p) = 1$ et $I(q) = 0$
   Fausse si $I(p) = 0$

   (b) valide : si on a p et si p implique q, alors on a q.

   (c) Vraie si $I(q) = 1$
   Fausse si $I(p) = 1$ et $I(q) = 0$

   (d) valide : si on a p et q, on a forcément p.

   (e) Vraie si $I(q) = 1$
   Fausse si $I(q) = 0$ et $I(p) = 1$

   (f) valide : si on a p alors on a p ou autre chose.

   (g) Vraie si $I(q) = 1$
   Fausse si $I(q) = 0$ et $I(p) = 1$

   (h) valide : si on n'a pas p, alors p implique n'importe quoi.

   (i) Vraie si $I(q) = 1$
   Fausse si $I(q) = 0$ et $I(p) = 1$

   (j) Vraie si $I(p) = 1$ et $I(q) = 1$
   Fausse si $I(p) = 0$

   (k) Vraie si $I(p) = 1$ et $I(q) = 1$
   Fausse si $I(p) = 0$

   (l) Vraie si $I(p) = 1$
   Fausse si $I(p) = 0$ et $I(q) = 0$

   (m) contradictoire : on ne peut pas avoir p et son contraire.

   (n) valide : dans tous les cas selon p, on a q, donc on a q.

   (o) valide : si p implique à la fois q et $\neg q$, on aurait une contradiction. Alors nécessairement on n'a pas p.

(p) valide : si ne pas avoir p implique avoir p, on aurait une contradiction, donc on a p.

(q) (les parenthèses ne servent à rien)
valide : si on a non p (et autre chose, y compris p) alors on a non p

(r) (la dernière parenthèse est de trop)
Vraie si $I(q) = 1$
Fausse si $I(q) = 0$ et $I(p) = 1$

9. • Si p est fausse, alors l'implication est vraie.
Si p est vraie, alors comme on a soit q, soit non q, on a nécessairement $p \wedge q$ ou $p \wedge \neg q$.

p	q	$\neg q$	$p \wedge q$	$p \wedge \neg q$	$(p \wedge q) \vee (p \wedge \neg q)$	$p \Rightarrow (p \wedge q) \vee (p \wedge \neg q)$
0	0	1	0	0	0	1
0	1	0	0	0	0	1
1	0	1	0	1	1	1
1	1	0	1	0	1	1

• Il faut que l'implication soit fausse, donc nécessairement p doit être vraie et la conclusion doit être fausse, mais alors il faut avoir q fausse (sans quoi $q \Rightarrow p$ est vraie aussi).
Tableau de vérité donnant une valeur vraie pour la formule :

p	q	$q \Rightarrow p$	$q \vee (q \Rightarrow p)$	$p \Rightarrow (q \vee (q \Rightarrow p))$	$\neg(p \Rightarrow (q \vee (q \Rightarrow p)))$
1	0	1	0	0	1

10. (a) En définissant :

a : « A est coupable »

b : « B est coupable »

c : « C est coupable »

Comme un vol a été commis et que nul autre que A, B ou C ne peut être impliqué, on a en particulier le fait que $(a \vee b \vee c)$ est vraie (au moins l'un des trois est coupable).

Comme A ne travaille pas sans complice et que nul autre que A, B ou C ne peut être impliqué, alors $(a \Rightarrow (b \vee c))$ est vraie (si A est coupable, alors B ou C l'est aussi, en tant que complice ; personne d'autre ne peut être complice/coupable).

D'autre part, C est innocent, donc $(\neg c)$ est vraie.

(b) Si $I(a) = 1$, alors comme $(a \Rightarrow (b \vee c))$, on a nécessairement $I(b \vee c) = 1$. Or $I(\neg c) = 1$, donc $I(c) = 0$, et donc nécessairement $I(b) = 1$.

Si $I(a) = 0$, comme on a $I(a \vee b \vee c) = 1$, et comme $I(c) = 0$, on a nécessairement $I(b) = 1$.

Dans tous les cas sur a, on a bien $I(b) = 1$.

Autrement dit :

Si A est coupable, comme il a nécessairement un complice, et comme nul autre que A, B ou C ne peut être impliqué, et comme C est innocent, alors B est le seul complice possible, et il est donc coupable comme A.

Si A est innocent, comme comme nul autre que A, B ou C ne peut être impliqué et que C est également innocent, alors B est coupable.

Dans tous les cas (pour A), on a déduit que B est coupable.

Donc B est coupable.

II) Logique tri-valuée

1. (a) Dans le cas où $I(A) = I$, on a $I(\neg A) = I$, donc $I(A \vee \neg A) = I \neq V$: ce n'est effectivement pas une tautologie.

(b) $A \Rightarrow A$ est une tautologie

(c) Table de vérité pour $\neg A \vee B$:

A	B	$\neg A$	$\neg A \vee B$
V	V	F	V
V	F	F	F
V	I	F	I
F	V	V	V
F	F	V	V
F	I	V	V
I	V	I	V
I	F	I	I
I	I	I	I

Pour $A \Rightarrow B$:

A	B	$A \Rightarrow B$
V	V	V
V	F	F
V	I	I
F	V	V
F	F	V
F	I	V
I	V	V
I	F	I
I	I	V

Il y a une différence : il est vrai que l'inconnu implique l'inconnu, alors que le « ou » de deux inconnus reste inconnu.

(d) Table de vérité pour $\neg B \Rightarrow \neg A$:

A	B	$\neg B$	$\neg A$	$\neg B \Rightarrow \neg A$
V	V	F	F	V
V	F	V	F	F
V	I	I	F	I
F	V	F	V	V
F	F	V	V	V
F	I	I	V	V
I	V	F	I	V
I	F	V	I	I
I	I	I	I	V

Pour $A \Rightarrow B$ voir la question précédente.
On voit ici que c'est la même chose.

2. (a) Table de vérité pour $\neg B \rightarrow \neg A$:

A	B	$\neg B$	$\neg A$	$\neg B \rightarrow \neg A$
V	V	F	F	V
V	F	V	F	F
V	I	I	F	I
F	V	F	V	V
F	F	V	V	V
F	I	I	V	V
I	V	F	I	V
I	F	V	I	I
I	I	I	I	I

C'est la même que celle de $A \to B$ (et que celle de $\neg A \vee B$).

(b) $A \to A$ n'est pas une tautologie, car quand A est inconnue, cette implication l'est aussi.

(c) Avec cette définition de l'implication, on observe que toutes les tables donnent un résultat inconnu dès que les deux propositions sont inconnues. Autrement dit, en prenant n'importe quelle formule, en utilisant la valuation qui associe l'inconnue à toutes les variables, l'interprétation termine systématiquement par inconnue, donc aucune formule ne peut être valide.

(d) Si $A \to B$ est une tautologie (autrement dit si $\models_3 A \to B$), alors A est fausse ou B est vraie.

Si A est fausse, alors $A \models_3 B$ est vraie car aucune interprétation ne peut satisfaire A.

Si B est vraie, alors $A \models_3 B$ est nécessairement vraie.

Réciproquement, si $A \models_3 B$, alors toute interprétation qui rend A vraie rend B vraie. Or, une interprétation qui rend A inconnue pourrait rendre B inconnue également, et on ne pourrait pas avoir $\models_3 A \to B$.

Exemple : $A \models_3 A$ (de manière évidente), mais $\not\models_3 A \to A$, comme on l'a remarqué plus haut.

On n'a donc pas l'équivalence.

Systèmes formels

a) Premier exemple

Les théorèmes sont les (a,b) tels que $a \geqslant b$.
Autrement dit, l'ensemble des théorèmes est $\{(a;b) \in \mathbb{N}^2; a \geqslant b\}$.
Soit la propriété $\mathcal{P}$: « si (a,b) est inférée, alors $a \geqslant b$ ».
On démontre cette propriété par induction (récurrence) sur le nombre n de règles utilisées.

⋆ **Initialisation :** On doit démontrer que la propriété est vraie pour les inférences utilisant une seule règle, autrement dit pour les axiomes.

Or, il n'y a ici qu'un seul axiome, qui permet d'inférer le couple (0,0), et $0 \geqslant 0$, donc la propriété est vraie

⋆ **Hérédité :** On suppose que la propriété est vraie pour toutes les inférences utilisant (au plus) n règles (avec $n \geqslant 1$) (c'est l'hypothèse d'induction) ; autrement dit que quel que soit le couple (a,b) obtenu en utilisant (au plus) n règles, on a $a \geqslant b$.

On doit démontrer que la propriété reste vraie pour toute inférence utilisant $n + 1$ règles.

Soit donc un couple (a,b) obtenu en utilisant $n+1$ règles. On regarde les cas selon la dernière règle ; On a :

- soit

$$\dfrac{\dfrac{\vdots}{(a-1,b-1)}}{(a,b)}$$

Dans ce cas, on a obtenu le couple $(a - 1,b - 1)$ en utilisant n règles, et l'hypothèse d'induction permet d'affirmer que $a - 1 \geqslant b - 1$.
Alors (en ajoutant 1 des deux côtés), on obtient $a \geqslant b$.

- soit

$$\dfrac{\dfrac{\vdots}{(a-1,b)}}{(a,b)}$$

Dans ce cas, on a obtenu le couple $(a - 1,b)$ en utilisant n règles, et l'hypothèse d'induction permet d'affirmer que $a - 1 \geqslant b$.
Alors (en ajoutant 1 des deux côtés), on obtient $a \geqslant b + 1 \geqslant b$.

Ainsi, dans tous les cas on a bien $a \geqslant b$.

⋆ **Conclusion :** Quel que soit le nombre $n \geqslant 1$ de règles utilisées pour inférer un couple (a,b), on a $a \geqslant b$. Autrement dit, $\mathcal{P}$ est vraie.

Réciproquement (On doit démontrer la réciproque de $\mathcal{P}$ pour être sûr d'avoir bien identifié les théorèmes), soit un couple (a,b) tel que $a \geqslant b$.
Il est facile de fabriquer ce couple à l'aide des règles d'inférence :
À partir de l'axiome (0,0) on utilise la première règle jusqu'à obtenir (b,b), puis on applique la seconde jusqu'à obtenir (a,b) (possible puisque a est supérieur à b).

On a donc démontré dans un sens que la propriété $a \geqslant b$ est nécessaire, et dans l'autre sens qu'elle est suffisante à exprimer tous les couples (a,b) obtenus en utilisant les règles d'induction du système. Autrement dit, l'ensemble des théorèmes est bien $\{(a;b) \in \mathbb{N}^2; a \geqslant b\}$.

b) Second exemple

Les théorèmes sont les (a,b,c) tels que $a = b + c$.
Soit la propriété : si (a,b,c) est inférée, alors $a = b + c$.
On peut la démontrer (proprement) là aussi par induction sur le nombre de règles d'inductions utilisées pour obtenir les triplets (a,b,c). Nous rédigerons cependant plus simplement ici.
Elle est vraie pour l'axiome donc elle est initialisée, et elle est héréditaire puisque avec l'utilisation des règles, à chaque étape, a augmente de 1 et soit (uniquement) b, soit (uniquement) c fait de même. Donc la propriété est vraie.
Réciproquement, soit un triplet (a,b,c) tel que $a = b + c$.
À partir de l'axiome $(0,0,0)$ on utilise la première règle jusqu'à obtenir $(b,b,0)$, puis on utilise la seconde règle jusqu'à obtenir $(b + c,b,c)$, c'est à dire (a,b,c).

c) Le Loup, la chèvre et le chou

On note 'h' l'homme, 'l' le loup, 'g' la chèvre et 'c' le chou.
On note un état sous la forme d'un triplet d'ensembles (R_1,R_2), Où :

- R_1 est l'ensemble des protagonistes sur la rive de départ ;
- R_2 est l'ensemble des protagonistes sur la rive d'arrivée.

On a les règles suivantes :

$$\frac{(R_1 \cup \{h,g\},R_2)}{(R_1,R_2 \cup \{h,g\})}\, g_d \qquad \frac{(R_1,R_2 \cup \{h,g\})}{(R_1 \cup \{h,g\},R_2)}\, g_g$$

$$\frac{(R_1 \cup \{h,l\},R_2) \quad \{g,c\} \not\subset R_1}{(R_1,R_2 \cup \{h,l\})}\, l_d \qquad \frac{(R_1,R_2 \cup \{h,l\}) \quad \{g,c\} \not\subset R_2}{(R_1 \cup \{h,l\},R_2)}\, l_g$$

$$\frac{(R_1 \cup \{h,c\},R_2) \quad \{l,g\} \not\subset R_1}{(R_1,R_2 \cup \{h,c\})}\, c_d \qquad \frac{(R_1,R_2 \cup \{h,c\}) \quad \{l,g\} \not\subset R_2}{(R_1 \cup \{h,c\},R_2)}\, c_g$$

$$\frac{(R_1 \cup \{h\},R_2) \quad \{l,g\} \not\subset R_1 \wedge \{g,c\} \not\subset R_1}{(R_1,R_2 \cup \{h\})}\, h_d \qquad \frac{(R_1,R_2 \cup \{h\}) \quad \{l,g\} \not\subset R_2 \wedge \{g,c\} \not\subset R_2}{(R_1 \cup \{h\},R_2)}\, h_g$$

On a l'axiome suivant :

$$\frac{}{(\{h,l,g,c\},\{\})}\, ax$$

Le but est d'obtenir :

$$\frac{\dots}{(\{\},\{h,l,g,c\})}$$

On l'obtient de la manière suivante :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(\{h,l,g,c\},\{\})}\,ax}{(\{l,c\},\{h,g\})}\,g_d \qquad \{l,g\}\not\subset\{g\}\wedge\{g,c\}\not\subset\{g\}}{(\{h,l,c\},\{g\})}\,h_g \qquad \{l,g\}\not\subset\{l\}}{(\{l\},\{h,g,c\})}\,c_d}{(\{h,l,g\},\{c\})}\,g_g \qquad \{g,c\}\not\subset\{g\}}{(\{g\},\{h,l,c\})}\,l_d \qquad \{l,g\}\not\subset\{l,c\}\wedge\{g,c\}\not\subset\{l,c\}}{(\{h,g\},\{l,c\})}\,h_g}{(\{\},\{h,l,g,c\})}\,g_d$$

d) Système `fg`

1. Quelques axiomes :

$$\dfrac{}{\texttt{f-g}} \qquad \dfrac{}{\texttt{-f-g}} \qquad \dfrac{}{\texttt{---f-g}}$$

   $R = \{(X\texttt{f}Y\texttt{g}Z, X\texttt{f}Y\texttt{g}ZX) \quad | \quad X, Y, Z \in \Sigma^*\}$ (En fait, Y vaut toujours `-`).
   La règle ne fait qu'ajouter `X`, qui est situé devant `f`, à la fin ; ce `X` est déterminé dans l'axiome.
   Un théorème issu d'une déduction de longueur 0 est un axiome, on en a déjà donné plus haut.
   Deux théorèmes issus d'une déduction de longueur 1 :

$$\dfrac{\dfrac{}{\texttt{-f-g}}}{\texttt{-f-g-}} \qquad \dfrac{\dfrac{}{\texttt{---f-g}}}{\texttt{---f-g---}}$$

2. Les formules F_1 et F_2 ne peuvent pas être des théorèmes, car la règle d'inférence ne permet pas d'augmenter le nombre de tirets entre `f` et `g`, et les axiomes fixent ce nombre à 1.
3. Les théorèmes sont de la forme `Xf-g(X)`*, avec `X` $\in$ `-`*, c'est à dire que le nombre de tirets à droite de `g` est un multiple de celui à gauche de `f`.
   La démonstration se fait sur le même modèle que pour le système du premier exemple de la fiche. Autrement dit :
   On démontre par induction sur le nombre de règles utilisées que si on a inféré une expression E, alors E est de la forme `Xf-g(X)`*, avec `X` $\in$ `-`*.
   - Pour l'initialisation de l'induction, on regarde les axiomes, avec lesquels on obtient les expressions de la forme `Xf-g` avec `X` $\in$ `-`*.
   - Pour l'hérédité, on regarde la dernière règle utilisée, qui est ici l'unique règle, et qui ajoute `X` à droite. Comme l'hypothèse d'induction permet d'affirmer que `Z` est un multiple de `X` (et que `Y` est `-`), on en déduit que `ZX` en est un également.

   On démontre réciproquement que toute expression de la forme `Xf-g(X)`* peut être inférée (facilement) en appliquant les règles du système.

e) Système formel nB

Nous écrirons les noms des règles à droite, contrairement à l'énoncé, pour plus d'homogénéité avec le reste du document.

1.

(i) $$\dfrac{\dfrac{\dfrac{}{\sim\sim\sim\, NDP \sim}\,[\text{ax}]}{\sim\sim\sim\, NDP \sim\sim\sim\sim}\,[R_1]}{\sim\sim\sim\, NDP \sim\sim\sim\sim\sim\sim\sim}\,[R_1]$$

(ii) $$\dfrac{\dfrac{\dfrac{\dfrac{}{\sim\sim\, NDP \sim}\,[\text{ax}]}{\sim\sim\, NDP \sim\sim\sim}\,[R_1]}{\sim\sim\sim\, SD \sim\sim}\,[R_2]}{P \sim\sim\sim}\,[R_4]$$

(iii)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\sim\sim\sim\sim\, NDP \sim}\,[ax]}{\sim\sim\sim\sim\, NDP \sim\sim\sim\sim\sim}\,[R_1] \qquad \dfrac{\dfrac{\dfrac{}{\sim\sim\sim\, NDP \sim\sim}\,[ax]}{\sim\sim\sim\, NDP \sim\sim\sim\sim\sim}\,[R_1] \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\sim\sim\, NDP \sim}\,[ax]}{\sim\sim\, NDP \sim\sim\sim}\,[R_1]}{\sim\sim\, NDP \sim\sim\sim\sim\sim}\,[R_1]}{\sim\sim\sim\sim\sim\, SD \sim\sim}\,[R_2]}{\sim\sim\sim\sim\sim\, SD \sim\sim\sim}\,[R_3]}{\sim\sim\sim\sim\sim\, SD \sim\sim\sim\sim}\,[R_3]}{P \sim\sim\sim\sim\sim}\,[R_4]$$

2. $P \sim\sim\sim\sim$ ne peut pas être démontré, car pour cela il faudrait pouvoir démontrer
$\sim\sim\sim\sim\, SD \sim\sim\sim$ (R_4),
et pour cela $\sim\sim\sim\sim\, SD \sim\sim$ (R_3),
et pour cela $\sim\sim\, NDP \sim\sim\sim\sim$ (R_3),
ce qui n'est pas possible car cela revient à démontrer $\sim\sim\, NDP \sim\sim$ (R_1), ce qui revient à démontrer $\sim\sim\, NDP$ (R_1), qui n'est pas possible.

   $P \sim\sim\sim\sim\sim\sim\sim$ est par contre démontrable. Cela passe par les démonstrations que 7 n'est divisible par aucun entier entre 2 et 6.

   En fait, ce système peut être interprété de la manière suivante, les suites de $\sim$ étant des nombres écrits en notation unaire :
   - $xNDPy$ se lit « x ne divise pas y »
   - Py se lit « y est un nombre premier »
   - $ySDx$ peut se lire « y est sans diviseur entre 2 et x »

   Alors les règles se comprennent ainsi :
   - R_1 dit que si x ne divise pas y, alors x ne divise pas $x + y$
   - R_2 dit que si 2 ne divise pas x, alors x est sans diviseur entre 2 et 2 »
   - R_3 dit que si $x + 1$ ne divise pas y et si y est sans diviseur entre 2 et x, alors y est sans diviseur entre 2 et $x + 1$.
   - R_4 dit que si $y + 1$ est sans diviseur entre 2 et y, alors $y + 1$ est premier.

   Les axiomes affirment que 2 est premier et que tout nombre $x + y$ avec x et y non nuls ne divise pas x.

   Ces règles et axiomes sont arithmétiquement justes. Ainsi, le système permet de démontrer des Py seulement si y est premier.

   Réciproquement, si y est premier, on peut démontrer Py.

f) Système MU de D. Hofstadter

1.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{MI}\,\text{ax}}{MII}\,r_2}{MIIII}\,r_2}{MUI}\,r_3 \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{MI}\,\text{ax}}{MII}\,r_2}{MIIII}\,r_2}{MUI}\,r_3}{MUIU}\,r_1$$

2. Le seul axiome commence par M. Aucune règle ne permet d'ajouter quelque chose à gauche, ni ne supprime ou échange/substitue à gauche, donc M reste à gauche.
3. Le reste de la division par 3 du nombre de I est toujours non nul. Autrement dit le nombre n de I n'est pas divisible par 3.
   - C'est le cas pour l'axiome (un seul I).
   - La seule règle qui permet d'éliminer des I en élimine 3. Or si $n + 3$ n'est pas divisible par 3, alors n non plus (la contraposée de cet énoncé est évidente, et lui équivaut).
   - Il y a une règle qui double le nombre de I, à savoir la règle 2. Or, si n n'est pas divisible par 3, alors $2n$ ne l'est pas non plus, car 2 et 3 sont premiers entre eux (c'est une conséquence du lemme de Gauss).
   - Les autres règles ne modifient pas le nombre de I.

   Ainsi, MU n'est pas un théorème (car 0 est divisible par 3).
4. On remarque que la règle 2 multiplie le nombre de I par 2.

   $MI = MI^{2^0}$ est un axiome, donc un théorème.

   Si MI^{2^t} est un théorème, alors en appliquant la règle 2, on obtient :

   $MI^{2^t}I^{2^t} = M^{2^t \times 2} = M^{2^{t+1}}$.

   Donc les MI^{2^t} sont bien des théorèmes.

   Puisque MI^{2^t} est un théorème, l'application de la règle 1 démontre que $MI^{2^t}U$ est également un théorème.
5. Les théorèmes sont les mots commençant par M, contenant n'importe quel nombre de U et un nombre de I non divisible par 3.

   Il est évident (ou déjà démontré) que les mots dérivés ont ces propriétés.

   Soit un mot quelconque vérifiant ces propriétés. On doit démontrer qu'il est un théorème du système.

   L'idée globale est d'obtenir un nombre N de I égal à celui souhaité plus trois fois celui de U, puis créer les U aux emplacements souhaités avec la règle 3.

   L'idée un peu moins globale (mais imprécise sur les valeurs) est d'appliquer la règle 2 suffisamment de fois pour obtenir autant de I que nécessaire (on en obtiendra 2^t comme déjà démontré), puis la règle 3 pour réduire le nombre de I à celui que l'on souhaite, ce qui fait apparaître des U à la fin (noter que g peut être vide). Le nombre de U peut être augmenté de 1 avec la règle 1 pour qu'il soit pair, ce qui fait que l'on peut les faire tous disparaître avec plusieurs applications de la règle 4. Une fois que l'on n'a plus que nos N symboles I souhaités, on fait apparaître les U aux emplacements souhaités comme indiqué précédemment.

   Voir cet article Wikipedia (en anglais) pour plus de précision.

g) Jeu des allumettes

1. (A,B,4) est effectivement valide, car quel que soit le nombre d'allumettes que prendra B (entre 1 et 3), il restera un nombre d'allumettes compris entre 1 et 3, et le joueur A pourra les prendre en totalité et gagner la partie.

2. $(A,B,5)$ n'est pas valide, car si B prend une seule allumette (il en reste alors 4), alors quel que soit le choix de A, il restera un nombre d'allumettes compris entre 1 et 3, et c'est alors B qui peut gagner, en prenant le total. A n'est donc pas certain de pouvoir gagner, si B fait les bons choix.
3. Les formules sont les suivantes : $(A,A,1)$, $(A,A,2)$, $(A,A,3)$, $(B,B,1)$, $(B,B,2)$, $(B,B,3)$.
4. (a)

$$\dfrac{\overline{(A,B,4)}}{(A,A,5)}$$

   (b) Les règles ne permettent pas d'avoir de formule de la forme $(B,B,*)$. Donc $(B,B,6)$ ne peut pas être un théorème.

   Les seuls théorèmes, hors axiomes, sont de la forme $(A,A,*)$. En fait, il n'y a d'ailleurs que 3 théorèmes (hors axiomes) dans ce système.

   À moins de considérer l'ajout des règles où l'on échange les lettres A et B... Mais ça ne ferait que 3 théorèmes supplémentaires.

   Il en faudrait également avec des prémisses de la forme $(A,A,*)$ et $(B,B,*)$...

   (c) Le système est effectivement correct. Étant donné que les seuls théorèmes, hors axiomes, sont en fait $(A,A,5)$, $(A,A,6)$ et $(A,A,7)$. Ces trois là sont valides car il suffit que A laisse à B 4 allumettes pour être sûr de pouvoir gagner.

   (d) Comme indiqué plus haut, il n'y a que trois théorèmes, donc c'est loin d'être complet.
5. L'implication est évidemment fausse, car si A était sûr de gagner avec B qui commence, B ne pourrait pas être sûr de gagner en commençant (B serait même certain de perdre si A joue parfaitement).

Déduction naturelle

1.

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$A \Rightarrow B, B \Rightarrow C, A \vdash B \Rightarrow C$}
\AxiomC{}
\UnaryInfC{$A \Rightarrow B, B \Rightarrow C, A \vdash A \Rightarrow B$}
\AxiomC{}
\UnaryInfC{$A \Rightarrow B, B \Rightarrow C, A \vdash A$}
\RightLabel{Elim $\Rightarrow$}
\BinaryInfC{$A \Rightarrow B, B \Rightarrow C, A \vdash B$}
\RightLabel{Elim $\Rightarrow$}
\BinaryInfC{$A \Rightarrow B, B \Rightarrow C, A \vdash C$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$A \Rightarrow B \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$\vdash (A \Rightarrow B) \Rightarrow (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$}
\end{prooftree}
$$

2. (a)

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$A \wedge B \vdash A \wedge B$}
\RightLabel{Elim$\wedge_g$}
\UnaryInfC{$A \wedge B \vdash A$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$\vdash A \wedge B \Rightarrow A$}
\end{prooftree}
$$

(b)

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$A \wedge B \vdash A \wedge B$}
\RightLabel{Elim$\wedge_g$}
\UnaryInfC{$A \wedge B \vdash A$}
\RightLabel{Intro$\vee_g$}
\UnaryInfC{$A \wedge B \vdash A \vee B$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$\vdash A \wedge B \Rightarrow A \vee B$}
\end{prooftree}
$$

(c)

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$A \wedge B \Rightarrow C, A, B \vdash A \wedge B \Rightarrow C$}
\AxiomC{}
\UnaryInfC{$A \wedge B \Rightarrow C, A, B \vdash A$}
\AxiomC{}
\UnaryInfC{$A \wedge B \Rightarrow C, A, B \vdash B$}
\RightLabel{Intro$\wedge$}
\BinaryInfC{$A \wedge B \Rightarrow C, A, B \vdash A \wedge B$}
\RightLabel{Elim $\Rightarrow$}
\BinaryInfC{$A \wedge B \Rightarrow C, A, B \vdash C$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$A \wedge B \Rightarrow C, A \vdash B \Rightarrow C$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$A \wedge B \Rightarrow C \vdash A \Rightarrow B \Rightarrow C$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$\vdash (A \wedge B \Rightarrow C) \Rightarrow A \Rightarrow B \Rightarrow C$}
\end{prooftree}
$$

(d)

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$A \Rightarrow B \Rightarrow C, A \wedge B \vdash A \Rightarrow B \Rightarrow C$}
\AxiomC{}
\UnaryInfC{$A \Rightarrow B \Rightarrow C, A \wedge B \vdash A \wedge B$}
\RightLabel{Elim$\wedge_g$}
\UnaryInfC{$A \Rightarrow B \Rightarrow C, A \wedge B \vdash A$}
\RightLabel{Elim $\Rightarrow$}
\BinaryInfC{$A \Rightarrow B \Rightarrow C, A \wedge B \vdash B \Rightarrow C$}
\AxiomC{}
\UnaryInfC{$A \Rightarrow B \Rightarrow C, A \wedge B \vdash A \wedge B$}
\RightLabel{Elim$\wedge_d$}
\UnaryInfC{$A \Rightarrow B \Rightarrow C, A \wedge B \vdash B$}
\RightLabel{Elim $\Rightarrow$}
\BinaryInfC{$A \Rightarrow B \Rightarrow C, A \wedge B \vdash C$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$A \Rightarrow B \Rightarrow C \vdash A \wedge B \Rightarrow C$}
\RightLabel{Intro $\Rightarrow$}
\UnaryInfC{$\vdash (A \Rightarrow B \Rightarrow C) \Rightarrow A \wedge B \Rightarrow C$}
\end{prooftree}
$$

(e)

$$\dfrac{\dfrac{}{A \vdash A} \qquad \dfrac{\dfrac{}{A \vdash A}}{A \vdash B \vee A}\,\text{Intro}\vee_d}{\dfrac{A \vdash A \wedge (B \vee A)}{\vdash A \Rightarrow (A \wedge (B \vee A))}\,\text{Intro} \Rightarrow}\,\text{Intro}\wedge$$

(f)

$$\dfrac{\dfrac{}{A \vee (B \wedge A) \vdash A \vee (B \wedge A)} \qquad \dfrac{}{A \vee (B \wedge A), A \vdash A} \qquad \dfrac{\dfrac{}{A \vee (B \wedge A), B \wedge A \vdash B \wedge A}}{A \vee (B \wedge A), B \wedge A \vdash A}\,\text{Elim}\wedge_d}{\dfrac{A \vee (B \wedge A) \vdash A}{\vdash (A \vee (B \wedge A)) \Rightarrow A}\,\text{Intro} \Rightarrow}\,\text{Elim}\vee$$

3. (a)

$$\dfrac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash B \Rightarrow A}{\Gamma \vdash A \Leftrightarrow B}\,\text{Intro} \Leftrightarrow$$

$$\dfrac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash A \Rightarrow B}\,\text{Elim} \Leftrightarrow_g$$

$$\dfrac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash B \Rightarrow A}\,\text{Elim} \Leftrightarrow_d$$

(b) Supposons que $\Gamma \models A \Rightarrow B$ et $\Gamma \models B \Rightarrow A$.
Alors $\Gamma \models (A \Rightarrow B) \wedge (B \Rightarrow A)$. Or $(A \Rightarrow B) \wedge (B \Rightarrow A) \equiv (A \Leftrightarrow B)$,
donc $\Gamma \models A \Leftrightarrow B$.
La règle d'introduction préserve donc la validité.
Supposons que $\Gamma \models A \Leftrightarrow B$.
Alors, par l'équivalence déjà indiquée, $\Gamma \models (A \Rightarrow B) \wedge (B \Rightarrow A)$.
Ainsi, on a $\Gamma \models A \Rightarrow B$ et $\Gamma \models B \Rightarrow A$.
Cela implique que les deux règles d'élimination préservent également la validité.

(c) On observe facilement, du fait que $(A \Leftrightarrow B) \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$, que ces règles sont simplement les règles d'introduction et d'élimination du $\wedge$, donc elles préservent la validité.

4. Soit une propriété portant sur des dérivations que l'on cherche à démontrer. Si :
En supposant qu'elle est vraie pour les dérivations de longueur inférieure ou égale à un certain entier $n \geqslant 0$, on peut démontrer qu'elle est vraie pour les dérivations de longueur $n + 1$,
Alors la propriété est vraie quelle que soit la longueur de la dérivation.
Démontrons notre propriété, le lemme d'affaiblissement :
On suppose que pour un $n \geqslant 0$ fixé, pour toute dérivation de longueur inférieure ou égale à n de la forme $\Gamma, A \vdash A$ et tout ensemble Γ' tel que $\Gamma \subset \Gamma'$, on a $\Gamma' \vdash A$.
On doit démontrer que pour toute dérivation de longueur $n + 1$ de la forme $\Gamma \vdash A$ et tout ensemble Γ' tel que $\Gamma \subset \Gamma'$, on a $\Gamma' \vdash A$.
Il suffit alors de regarder la dernière règle utilisée, et « remonter » l'arbre de déduction.
S'il s'agit d'un axiome, c'est évident : comme $\dfrac{}{\Gamma \vdash A}$ seulement si $A \in \Gamma$, et comme $\Gamma \subset \Gamma'$, alors $A \in \Gamma'$, donc $\dfrac{}{\Gamma' \vdash A}$, est encore un axiome.

(les axiomes sont en quelque sorte les règles qui permettent d'initialiser la démonstration de récurrence).

Sinon, c'est une règle avec des prémisses. Ces prémisses ont été obtenues par une dérivation de longueur inférieure ou égale à n, donc d'après l'hypothèse de récurrence, on peut ajouter des hypothèses pour obtenir Γ'.

Alors la dernière règle s'applique toujours, et on a bien $\Gamma' \vdash A$ (cela se vérifie facilement règle par règle).

Ainsi on a démontré le lemme d'affaiblissement.