Connecteur de Sheffer et axiome de Wajsberg

Marc SAGE

8 mai 2015

Table des matières

Résumé. On montre ici que le calcul des propositions, muni des cinq connecteurs $\neg$, $\wedge$, $\vee$, $\Rightarrow$ et $\Leftrightarrow$, régi par les quatorze axiomes de Hilbert et par la règle du *modus ponens* peut se réduire à un seul connecteur $|$ et un seul axiome (avec toujours une seule règle).

Conventions & notations.

La négation d'une proposition A sera indifféremment notée $\neg A$ ou $\overline{A}$.

Les atomes propositionnels, *i. e.* les symboles (instanciables) de propositions, seront principalement

$$a, b, c, d, e..., \ p, q, r, s... \text{ ou } x, y.$$

Les règles d'inférences seront notées en majuscules : RÈG, MP, COM, TRANS...

Les substitutions/instanciations/remplacements seront notés avec une flèche $\leftarrow$. Ainsi, la substitution

$$"\square \leftarrow \triangle" \qquad \text{se lira} \qquad "\textit{dans } \square \textit{ mettre } \triangle"$$

et signifiera "*remplacer* $\square$ *par* $\triangle$", "*substituer* $\triangle$ *à* $\square$".

Les substitutions simultanées pourront être notées en utilisant deux dimensions, par exemple $\left\uparrow \begin{matrix} a & b & c \\ \overline{p} & \overline{p} & \overline{p} \end{matrix} \right\uparrow$ signifiera "remplacer a, b et c par $\overline{p}$".

L'interchangeabilité des notations sera signifiée par un symbole d'égalité $=$, en particulier pour *expliciter* des instances d'énoncés. Aucune confusion ne sera possible (avec d'éventuelles propositions affirmant une égalité) car il sera ici uniquement question de logique des *propositions* et non de celle de *prédicats* (écrite dans un langage comportant éventuellement une relation d'égalité).

1 Le connecteur de Sheffer en logique classique

En logique classique, on définir le connecteur de Sheffer, ou d'***incompatibilité***, par[1]

$$a|b := \overline{a} \vee \overline{b}$$

On pourra noter / pour signifier que les autres connecteurs sont prioritaires sur /. Par exemple :

$$a/b|c/d \text{ signifiera } (a|b)\,|\,(c|d)\,.$$

Mise en jambe.

1. *Exprimer tous les connecteurs usuels à l'aide de* $|$*. Faire de même à partir du connecteur NOR* $a||b := \overline{a} \wedge \overline{b}$ *et donner un argument en faveur de* $|$*.*
2. *Que signifie la proposition* $a|b/c$ *? Montrer que l'on peut en déduire* $d|b \Rightarrow a|d$*.*
3. *Montrer que* $a \Rightarrow b$ *implique* $p|b \Rightarrow a|p$*.*

Solution proposée. La notation $A \equiv B$ signifiera que $A \Leftrightarrow B$ est une tautologie.

1. Les connecteurs , $\Leftrightarrow$ et $\Leftarrow$ s'exprimant à l'aide de $\wedge$, $\vee$ et $\neg$, il suffit de récupérer ces derniers. Or on observe $\overline{a} \equiv a|a$, d'où $\begin{cases} a \wedge b \equiv \overline{\overline{a} \wedge \overline{b}} \equiv \overline{a|b} \\ a \vee b \equiv \overline{\overline{a}} \vee \overline{\overline{b}} \equiv \overline{a}|\overline{b} \end{cases}$. On aurait de même $\overline{a} \equiv a||a$ et $\begin{cases} a \vee b \equiv \overline{a||b} \\ a \wedge b \equiv \overline{a}||\overline{b} \end{cases}$. Jusqu'à ce stade, les connecteurs $|$ et $||$ jouent un rôle symétrique (en échangeant $\wedge$ et $\vee$).

   En revanche, l'implication $a \Rightarrow b \equiv \overline{a} \vee b \equiv \overline{\overline{a}}|\overline{b}$ s'écrit $a|\overline{b} \equiv \overline{\overline{a}||b}$, ce qui s'exprime plus facilement avec $|$ qu'avec $||$ (de même pour $\Leftarrow$). *A contrario*, l'équivalence $a \Leftrightarrow b \equiv (a \Rightarrow b) \wedge (a \Leftarrow b)$ s'écrit $\overline{a/\overline{b}|\overline{a}/b} \equiv \left(a||\overline{b}\right) || \left(\overline{a}||b\right)$ et s'exprime plus facilement avec $||$ qu'avec $|$. Précisément parce qu'une équivalence est une conjonction d'implications (et parce que beaucoup de théorèmes sont seulement des implications), nous préférerons $|$ sur $||$.
2. En remarquant $p|q \equiv p|\overline{\overline{q}} \equiv p \Rightarrow \overline{q}$ (dire que p et q sont incompatibles, c'est dire que p entraîne la négation de l'autre), puis que que $\overline{x|y} \equiv \overline{\overline{x} \vee \overline{y}} \equiv x \wedge y$ (nier l'incompatibilité de x et y, c'est dire qu'ils sont tous deux vérifiés), on traduit $a|b/c \equiv a \Rightarrow \overline{b|c} \equiv a \Rightarrow b \wedge c$, autrement dit

   $$a|b/c \text{ signifie "} a \text{ entraîne } b \text{ et } c\text{"}.$$

   Si l'on suppose de plus $d|b$, alors a et d sont nécessairement incompatibles (si a est vérifié, b et c le sont d'après $a|b/c$, donc b l'est, d'où la fausseté de d d'après $d|b$).
3. Supposons $a \Rightarrow b$; si p et b sont incompatibles, alors a et p le sont nécessairement (si a était vrai, b le serait d'après $a \Rightarrow b$, donc p serait infirmé d'après $p|b$).

2 Logique de Wajsberg

On se donne pour langage un unique symbole $|$, à partir duquel on définit quatre connecteurs (un singulaire et trois binaires)

$\overline{a}$	$a \wedge b$	$a \vee b$	$a \Rightarrow b$
$a\|a$	$\overline{a\|b}$	$\overline{a}\|\overline{b}$	$a\|\overline{b}$

On se donne pour seule règle de pouvoir

$$\text{(RÈG)} \qquad \textit{de } a \textit{ et } a|b/c \textit{ déduire la proposition } c \text{ :} \qquad \frac{a \qquad a|b/c}{c}.$$

Un énoncé P sera qualifié de ***prémisse*** dans tout énoncé de la forme $P|Q/R$.

[1] Ce connecteur NAND est parfois noté $\uparrow$, le chapeau $\wedge$ en haut de la flèche rappelant le AND nié (puisque barré par $|$) dans le NAND. Le NOR pourrait pour les mêmes raisons être noté $\downarrow$, comme si l'on avait barré verticalement le $\vee$.

On se donne pour unique (schéma d')axiome(s) toute instance de l'unique formule[2]

$$\begin{array}{c} \underline{a|b/c} \mid \underline{(d|c)\,|\,(a|d)\,/\,(a|d)} \;/\; \underline{a|a/b} \\ \text{axiome schématique :} \quad \alpha|\beta/\gamma \end{array} \quad \text{où l'on a abrégé} \left\{ \begin{array}{l} \alpha := a|b/c \\ \beta := (d|c)\,|\,(a|d)\,/\,(a|d) \\ \gamma := a|a/b \end{array} \right. .$$

Prise en main.

1. *Vérifier la validité de la règle et de l'axiome en logique classique.*
2. *Montrer que les règles suivantes[3] sont valides :*

$$\begin{array}{rcccc} & de & a|b/c & déduire & a|a/b, \\ & de & a \text{ et } a|b/c & déduire & b \text{ et } c, \\ \text{(MP)} & de & a \text{ et } a \Rightarrow b & déduire & b, \\ (\text{RÈG}|_{\Rightarrow}) & de & a \Rightarrow b & déduire & p|b \Rightarrow a|p. \end{array}$$

3. *Montrer que les (instances des) énoncés suivants sont des théorèmes :*

$$\alpha|\beta/\gamma, \qquad \alpha|\alpha/\beta, \qquad \alpha|\alpha/\alpha, \qquad p|\alpha \Rightarrow \alpha|p \qquad et \qquad \beta/\gamma|\alpha.$$

Solution proposée.

1. Nous avons montré en logique classique que $a|b/c$ entraînait b et c, en particulier c, d'où la validité de RÈG. De plus, se rappelant cette interprétation de $a|b/c$, il est clair que $a|b/c$ implique $a|a/b$. Enfin, au vu de la définition de $\Rightarrow$, l'axiome se réécrit plus joliment

$$\underline{a|b/c} \mid \underline{d|c \implies a|d} \;/\; \underline{a|a/b},$$

signifiant que $a|b/c$ implique d'une part l'implication $d|c \implies a|d$ (ce que nous avons déjà montré), d'autre part $a|a/b$ (ce que nous avons rappelé).

2. Supposant $a|b/c$, utiliser l'axiome et la règle donne $a|a/b$.
Supposant de plus a, réutiliser la règle donne b ; or la règle appliquée à a et $a|b/c$ donne également c.
Imposer $b = c$ dans la règle donne (pour conséquent b et) pour antécédents a et $a|b/b = a|\overline{b} = a \Rightarrow b$.
Imposer $b = c$ dans l'axiome montre que, de $a \Rightarrow b$, on peut déduire $d|b \Rightarrow a|d$.

3. L'énoncé $\alpha|\beta/\gamma$ est l'axiome. Lui appliquer deux fois de suite la règle $a|b/c \vdash a|a/b$ donne $\alpha|\alpha/\beta$, puis $\alpha|\alpha/\alpha$ (*i. e.* $\alpha \Rightarrow \alpha$). Ce dernier instancie l'antécédent de la règle RÈG$|_{\Rightarrow}$ (replacer a et b par α), d'où le conséquent $p|\alpha \Rightarrow \alpha|p$.
Enfin, la conclusion désirée $\beta/\gamma|\alpha$ est de la forme $a|p$ en remplaçant (a,p) par $(\beta/\gamma, \alpha)$, donc sera déduite par la règle RÈG$|_{\Rightarrow}$ de $a \Rightarrow b$ et de $p|b$. Or en imposant $a = b$ (tous deux remplacés par β/γ), ces implication et incompatibilité deviennent $\beta|\gamma \Rightarrow \beta|\gamma$ et $\alpha|\beta/\gamma$: deux théorèmes.

Rmarques (caractère optimal). L'axiome de Wajsberg (1926) $\underline{a|b/c} \mid \underline{d|c \implies a|d} \;/\; \underline{a|a/b}$ améliore l'axiome de Nicod[4] (1917) $\underline{a|b/c} \mid \underline{e \Rightarrow e} \;/\; \underline{d|b \Rightarrow a|d}$ à deux égards : il possède *moins d'atomes* et est *organique* (au sens où il ne contient pas de tautologies). Sur un pdf disponible[5] sur sa page web, Branden Fitelson donne deux autres exemples de tels axiomes, l'un dû à Łukasiewicz $\underline{a|b/c} \mid \underline{a|c/a} \;/\; \underline{d|b \implies a|d}$ et l'autre dû à Ken Harris et lui-même $\underline{a|b/c} \mid \underline{a|b/c} \;/\; \underline{(d|c)\,|\,(c|d)\,/\,(a|d)}$. Fitelson affirme également avoir montré (sans référence) avec Harris qu'il n'existe pas d'axiomes de longueur plus petite. En ce sens, nous ne pourrons améliorer les résultats présentés dans ce devoir : *un seul* connecteur, *une seule* règle et *un seul* axiome de longueur *minimale*.

Objectif. Afin de retrouver tous les théorèmes de la logique usuelle (les tautologies), nous n'allons pas dériver à la main les quatorze axiomes de Hilbert à partir de l'axiome et de la règle ci-dessus. Nous allons plutôt montrer juste ce qu'il suffit pour établir le théorème de complétude (dont toutes les tautologies découleront). Le lecteur connaisseur de ce dernier pourra dès à présent essayer de le démontrer afin de voir de quels théorèmes il aimerait disposer – et ainsi de comprendre le fil de ce devoir. On encourage fortement à dresser une "carte" des théorèmes et règles établis et utilisés[6].

[2] le soulignage n'est qu'une aide à la lecture

[3] La règle RÈG$|_{\Rightarrow}$ est ainsi notée car mélange les connecteurs $|$ et $\implies$.

[4] dont on trouvera une exposition dans *A reduction in the number of the Primitive Propositions of Logic* de Jean Nicod publié en 1920 dans les *Proceedings of the Cambridge Philosophical Society* **19** (1917-1920), 32-41 et disponible sur wikisource

[5] http ://fitelson.org/berkeley_logic_2x2.pdf

[6] **exercices ouverts** : reprendre ce devoir pour les axiomes de Łukasiewicz et de Harris-Fitelson sus-mentionnés (en particulier, trouver pour chacun une preuve de l'identité $x \Rightarrow x$)

2.1 Identité

Pour tout énoncé E, notons i_E l'énoncé (d'**i**dentité) $E \Rightarrow E$.

1. *Montrer que si* θ *et* $x|x/\theta$ *sont des théorèmes, alors* i_x *en est un.*
2. *Montrer qu'il suffit pour conclure à* i_x *de prouver* $\alpha| \bullet / (x|x/\alpha)$ *pour au moins un énoncé* $\bullet$*.*
3. *Montrer* $s|q/r \Rightarrow \bullet/\dot\gamma|s$ *pour un certain énoncé* $\bullet$ *à choisir (ici* $\dot\gamma$ *abrège* $p|p/q$*).*
4. *En déduire* $*/(x|x/\alpha)\,|\alpha$ *pour un certain énoncé* $*$*.*
5. *Conclure au théorème d'**identité*** $x \Rightarrow x$*.*

Solution proposée.

1. Dans l'axiome $\alpha|\beta/\gamma$, on remplace $(a,b,c) \leftarrow (x,x,\theta)$: la prémisse α devient alors $x|x/\theta$, qui est réalisée par hypothèse, d'où (*via* RÈG) le conséquent γ, lequel s'écrit $x|x/x = i_x$, *c. q. f. d.*.
2. Dans l'hypothèse $\alpha| \bullet / (x|x/\alpha)$, remplaçons a, b et c par[7] $\dot\alpha := p|q/r$. La prémisse s'écrit alors $i_{\dot\alpha}$, qui est un théorème, d'où l'on tire (*via* RÈG) $x|x/i_{\dot\alpha}$. Puisque $i_{\dot\alpha}$ est un théorème ($\dot\alpha \Rightarrow \dot\alpha$), la question 1 s'applique en prenant $i_{\dot\alpha}$ pour θ.
3. L'énoncé voulu est une implication de la forme β, donc une conséquence (d'une instance) du théorème $\alpha|\alpha/\beta$. En calquant sur la conclusion voulue $s|q/r \Rightarrow \bullet/\dot\gamma|s$ la forme visée $d/c \Rightarrow a/d$, on est amené à substituer $(s, q/r, \bullet/\dot\gamma)$ à (d,c,a) avec $\bullet$ à choisir (et b encore à remplacer) : il suffit alors (grâce à RÈG) de réaliser la prémisse du théorème $\alpha|\alpha/\beta$ obtenu après les substitutions précédentes. Cette prémisse s'écrit $\bullet/\dot\gamma \mid \underline{b/(q/r)}$, qui sera de la forme $\bullet/\dot\gamma|\underline{\dot\alpha}$ en substituant p à b et un théorème $\dot\beta/\dot\gamma|\dot\alpha$ en choisissant $\dot\beta$ pour $\bullet$.
4. La conclusion désirée étant de la forme $\bullet/\dot\gamma|s$ où l'on a remplacé $(p,q,s) \leftarrow (x,\alpha,\alpha)$, il suffit (d'après MP) de réaliser la prémisse $s|q/r$ de l'implication précédemment établie (après substitution). Cette prémisse s'écrit $\alpha|\alpha/r$, ce qui devient un théorème i_α en remplaçant de plus $r \leftarrow \alpha$.
5. La conclusion précédente est de la forme $p|\alpha$: l'implication $p|\alpha \Rightarrow \alpha|p$ nous donne alors (avec MP) $\alpha|p$, à savoir $\alpha| */(x|x/\alpha)$, et la question 2 conclut.

Reprise linéaire de la preuve de $x \Rightarrow x$:

• dans le théorème $\alpha|\alpha/\beta$, remplacer $\left\uparrow \begin{array}{cccc} a & b & c & d \\ \dot\beta|\dot\gamma & p & q|r & s \end{array} \right\uparrow$ donne pour prémisse $\dot\beta/\dot\gamma|\dot\alpha$, qui est un théorème, d'où l'on infère le conséquent $\beta \;=\; s|q/r \Rightarrow \dot\beta/\dot\gamma|s$;

• dans ce dernier, remplacer $\left\uparrow \begin{array}{cccc} p & q & r & s \\ x & \alpha & \alpha & \alpha \end{array} \right\uparrow$ donne pour prémisse $\alpha|\alpha/\alpha$, qui est un théorème, d'où la conclusion $\dot\beta/\dot\gamma|s \;=\; \dot\beta/(x|x/\alpha)\,|\alpha$;

• de cette dernière, l'on infère $\alpha|\dot\beta/(x|x/\alpha)$ grâce au théorème $p|\alpha \Rightarrow \alpha|p$ obtenu en instanciant p convenablement ;

• dans $\alpha|\dot\beta/(x|x/\alpha)$, remplacer $\left\uparrow \begin{array}{ccc} a & b & c \\ \dot\alpha & \dot\alpha & \dot\alpha \end{array} \right\uparrow$ réalise la prémisse $\alpha \;=\; i_{\dot\alpha}$, d'où le conséquent $x|x/i_{\dot\alpha}$;

• ce dernier réalise l'axiome $\alpha|\beta/\gamma$ après remplacement $\left\uparrow \begin{array}{ccc} a & b & c \\ x & x & i_{\dot\alpha} \end{array} \right\uparrow$, d'où le conséquent $\gamma \;=\; x|x/x \;=\; i_x$.

Remarques. Cette preuve de $x \Rightarrow x$ est extraite (et distillée) de la page[8] 38 de l'œuvre *Logical works* de Mordechaj Wasjsberg publiée en 1977 par la *Polish Academy of Sciences*. Dans cette page de l'article *A new axiom of propositional calculs in Sheffers's symbols*, Wasjberg dérive en dix-sept étapes l'axiome de Nicod depuis le sien[9], l'identité i_x étant obtenue au bout de la douzième étape (les troisième et quatrième n'y servant pas). Il est remarquable que, à l'exception d'une preuve de i_x, tout le reste de la preuve de la complétude de la logique de Nicod[10] s'adapte aisément pour montrer la complétude de la logique de Wasjberg. Ces quelques remarques pour éclairer la construction de ce devoir.

[7] dans ce qui suit, les points au-dessus de α, β et γ signifient que l'on a remplacé les variables (a,b,c) par celles (p,q,r)

[8] **Attention** : cette page (et d'autres) manquaient (début 2015) à l'exemplaire disponible à la BNF ! Nous avons pu nous procurer l'article complet (pages 37-39) auprès de la bibliothèque d'Orsay.

[9] il aurait déjà trouvé ce résultat en quatrième année d'étude, soit en 1926-27

[10] que nous présentons dans un autre devoir, après une patiente distillation de l'article de 1917 sus-cité

2.2 Commutativité, affaiblissement, tiers exclu, double-négation et incompatibilités

Conséquences de l'identité.

1. *Montrer la* ***commutativité*** $p|q \Rightarrow q|p$ *et le* ***tiers exclu*** $\overline{\overline{a}} \Rightarrow a$.
2. *En partant de* $\overline{q|p}|p/q$ *(à établir), montrer l'****incompatibilité*** $\overline{x} \Rightarrow x|y$.
3. *En partant de* $\overline{q|p}|q/p$ *(à établir), montrer l'(autre)* ***incompatibilité*** $\overline{x} \Rightarrow y|x$.
4. *En partant d'une instance de* $\overline{q|p}|q/p$, *montrer l'****affaiblissement*** $p \Rightarrow (q \Rightarrow p)$.
5. *En déduire la* ***double-négation*** $a \Rightarrow \overline{\overline{a}}$.

Solution proposée.

1. On applique la règle RÈG$|_{\Rightarrow}$ sur le théorème $q \Rightarrow q$. La règle de commutativité correspondante sera notée COM.
   L'énoncé $\overline{\overline{a}} \Rightarrow a$ se réécrit $\overline{\overline{a}}|\overline{a}$, *i. e.* (d'après COM) $\overline{a}|\overline{\overline{a}} \;=\; \overline{a} \Rightarrow \overline{a} \;=\; i_{\overline{a}}$.
2. L'énoncé $\overline{q/p}|p/q$ équivaut (par COM) au théorème $p/q|\overline{q/p} \;=\; p/q \Rightarrow q/p$ et réalise la prémisse de l'axiome $\alpha|\beta/\gamma$ après substitution $\left\uparrow \begin{array}{ccc} a & b & c \\ \overline{q/p} & p & q \end{array} \right\uparrow$, d'où (par RÈG) le conséquent $\beta \;=\; d|q \Rightarrow \overline{q|p}|d$. La prémisse de cette implication se réalisera (*via* COM) en i_p après remplacement $d \leftarrow \overline{q}$, d'où (MP) la conclusion $\overline{q|p}|\overline{q}$, *i. e.* (COM) $\overline{q}|\overline{q|p} \;=\; \overline{q} \Rightarrow q \vee p$.
3. Comme ci-dessus, l'énoncé $\overline{q/p}|q/p$ équivaut *via* COM à un théorème (cette fois $i_{q/p}$) : en substituant cette fois $\left\uparrow \begin{array}{cccc} a & b & c & d \\ \overline{q/p} & q & p & \overline{p} \end{array} \right\uparrow$ dans l'axiome $\alpha|\beta/\gamma$, on obtient le conséquent $\beta \;=\; \overline{p}|p \Rightarrow \overline{q|p}|\overline{p}$, d'où la conclusion $\overline{p}|\overline{q|p} \;=\; \overline{p} \Rightarrow q \vee p$.
4. On part cette fois du théorème $\overline{q/\overline{p}}|q/\overline{p}$ (équivalant à $i_{q/\overline{p}}$) et l'on remplace $\left\uparrow \begin{array}{cccc} a & b & c & d \\ \overline{q/\overline{p}} & q & \overline{p} & p \end{array} \right\uparrow$, d'où le conséquent $\beta \;=\; p|\overline{p} \Rightarrow \overline{q|\overline{p}}|p$ et.la conclusion $p|\overline{q|\overline{p}} \;=\; p \Rightarrow (q \Rightarrow p)$.
5. Puisque $\overline{\overline{a}}$ se réécrit $\overline{a}|\overline{a}$, à savoir $\overline{a} \Rightarrow a$, l'énoncé $a \Rightarrow \overline{\overline{a}}$ est une instance de $p \Rightarrow (q \Rightarrow p)$.

La règle de commutation COM nous servira à de nombreuses reprises. Rappelons-la :

$$\text{(COM)} \qquad \textit{de } x|y \textit{ déduire } y|x.$$

2.3 Transitivité de l'implication

On souhaite établir la règle de transitivité de l'implication :

$$\text{(TRANS)} \qquad \textit{de } a \Rightarrow b \textit{ et } b \Rightarrow c \textit{ déduire } a \Rightarrow c.$$

1. *Déduire la validité de TRANS de l'énoncé* $(p|q/r) \Rightarrow (q|s \Rightarrow p|s)$.
   Preuve de l'énoncé suffisant.
2. *En utilisant une incompatibilité, montrer l'implication* $\alpha \Rightarrow \beta$.
3. *En instanciant à deux reprises le théorème* $p|x/y \Rightarrow y/x|p$ *(à établir), montrer* $\overline{b/d|e} \mid (e|d/b)$ *puis* $\overline{b|d \Rightarrow a|d} \mid \beta$.
4. *Conclure en appliquant* RÈG$|_{\Rightarrow}$ *sur le théorème* $\alpha \Rightarrow \beta$.

Solution proposée.

1. En remplaçant dans l'énoncé $\left\uparrow \begin{array}{cccc} p & q & r & s \\ a & b & b & \overline{c} \end{array} \right\uparrow$, on obtient $(a \Rightarrow b) \Rightarrow ((b \Rightarrow c) \Rightarrow (a \Rightarrow c))$, d'où la règle TRANS en appliquant deux fois MP.

2. On veut obtenir $\alpha|\overline{\beta}$, ce qui revient à $\overline{\beta}|\alpha$ par COM : suffirait à notre bonheur l'implication $\alpha|\beta/\gamma \Rightarrow \overline{\beta}|\alpha$. Or cette dernière peut être obtenue par RÈG$|_{\Rightarrow}$ (avec α) depuis l'implication $\overline{\beta} \Rightarrow \beta/\gamma$, laquelle est une instance de l'incompatibilité $\overline{x} \Rightarrow x|y$.

3. Le théorème $p|x/y \Rightarrow y/x|p$ s'établit en appliquant RÈG$|_{\Rightarrow}$ avec p au théorème $y|x \Rightarrow x|y$.

   Il se réécrit $(p|x/y) \mid \overline{y/x|p}$, ou encore (COM) $\overline{y/x|p} \mid (p|x/y)$, ce qui est le premier énoncé voulu (à un réétiquetage près).

   On réinjecte alors l'énoncé que l'on vient d'établir $\overline{b/d|e} \mid (e|d/b)$ en prémisse dans le théorème $p|x/y \Rightarrow y/x|p$ en substituant $\left\uparrow \begin{matrix} p & x & y \\ \overline{b/d|e} & e & d/b \end{matrix} \right\uparrow$, d'où (RÈG) $(d|b) \ / \ e \mid \overline{b/d|e}$ et (COM) $\overline{b/d|e} \mid (d|b) \ / \ e$: il suffit alors de remplacer $e \leftarrow \overline{a|d}$ pour obtenir le second énoncé voulu.

4. Pour conclure, la règle indiquée nous donne (à partir du théorème $\alpha \Rightarrow \beta$) des théorèmes $p|\beta \Rightarrow \alpha|p$; or on vient de montrer $\overline{b|d \Rightarrow a|d} \mid \beta$, ce qui incite (afin de réaliser $p|\beta$) à substituer $p \leftarrow \overline{b|d \Rightarrow a|d}$. On en tire (RÈG) $(a|b/c)\,|p$, ce qui se réécrit $a|b/c \Rightarrow (b|d \Rightarrow a|d)$, *CQFD*.

Remarque de détail. L'implication $\alpha \Rightarrow \beta$ peut en fait s'établir directement (sans utiliser les conséquences de l'identité sus-développées) et l'on en déduirait la règle TRANS $\dfrac{a \Rightarrow E \quad E \Rightarrow b}{a \Rightarrow b}$ (suivant l'exercice ci-dessus) uniquement pour les énoncés E tels que $x|\overline{E} \Rightarrow \overline{E}|x$; nous aurons hélas également besoin de cette règle pour les énoncés E *atomiques*, lesquels ne valident pas trivialement la condition $x|\overline{E} \Rightarrow \overline{E}|x$! C'est pourquoi, afin de simplifier, nous avons présenté dans ce travail une preuve de TRANS utilisant plus d'outils que nécessaire, ces outils devant de toute façon nous servir ailleurs.

Preuve (anecdotique) de $\alpha \Rightarrow \beta$. Notons CO la règle $s|\dot{\alpha} \vdash \dot{\alpha}|s$, validée par le théorème $s|\dot{\alpha} \Rightarrow \dot{\alpha}|s$.

- le théorème $i_{\dot{\alpha}}$ s'instancie en $i_\beta \ = \ \beta|\overline{\beta}$, d'où (CO) $\overline{\beta}|\beta$;
- le théorème $s|\dot{\alpha} \Rightarrow \dot{\alpha}|s$ s'instancie en $\gamma|\beta \Rightarrow \beta|\gamma \ = \ \gamma/\beta \mid \overline{\beta|\gamma}$, d'où (CO) $\overline{\beta|\gamma} \mid \gamma/\beta$;
- ce dernier est prémisse de l'axiome $\dot{\alpha}|\dot{\beta}/\dot{\gamma}$ instancié selon $\left\uparrow \begin{matrix} p & q & r & s \\ \overline{\beta|\gamma} & \gamma & \beta & \overline{\beta} \end{matrix} \right\uparrow$, d'où (RÈG) le conséquent $\dot{\gamma} \ = \ \overline{\beta}|\beta \Rightarrow \overline{\beta|\gamma} \mid \overline{\beta}$. Le premier point $\overline{\beta}|\beta$ donne alors (MP) $\overline{\beta|\gamma} \mid \overline{\beta}$, d'où (CO) $\overline{\beta} \mid \overline{\beta|\gamma} \ = \ \overline{\beta} \Rightarrow \beta/\gamma$, puis (RÈG$|_{\Rightarrow}$) $\alpha|\beta/\gamma \Rightarrow \overline{\beta}|\alpha$, d'où (MP) $\overline{\beta}|\alpha$ et (CO) $\alpha|\overline{\beta} \ = \ a \Rightarrow \beta$.

2.4 Théorème de la déduction

Rappelons l'énoncé du (méta-)**théorème de déduction** qui relie implications et inférences : *si $\mathcal{A}$ est un ensemble fini de formules et A une formule, alors affirmer que l'on peut déduire de $\mathcal{A}$ et de A un énoncé B revient à affirmer que l'on peut de $\mathcal{A}$ déduire $A \Rightarrow B$*. En bref[11] :

$$\mathcal{A}, A \vdash B \textit{ ssi } \mathcal{A} \vdash A \Rightarrow B.$$

Preuve du théorème de la déduction.

1. *Prouver les deux théorèmes de* ***contraposée*** *:* $(a \Rightarrow b) \Rightarrow \left(\overline{b} \Rightarrow \overline{a}\right)$ *et* $\left(\overline{b} \Rightarrow \overline{a}\right) \Rightarrow (a \Rightarrow b)$.
2. *Établir la règle de* ***disjonction des cas*** *:*

   "de deux implications de la forme $F \Rightarrow E$ et $\overline{F} \Rightarrow E$, on peut déduire E".

3. *Prouver la validité de la règle de* ***contraction*** *"de $a \Rightarrow (a \Rightarrow b)$ déduire $a \Rightarrow b$".*
4. *Légitimer la règle "de $p \Rightarrow q$ déduire $(q \Rightarrow E) \Rightarrow (p \Rightarrow E)$".*
5. *En utilisant deux fois la règle ci-dessus, établir la règle :*

   "de $a \Rightarrow b$ et $a \Rightarrow (b \Rightarrow c)$ déduire $a \Rightarrow c$".

6. *Montrer l'implication $a|b/c \Rightarrow (a \Rightarrow c)$ et conclure au théorème de la déduction.*

[11] la réciproque est laissée aux soins du lecteur

Solution proposée.

1. La contraposition s'écrit $a|\overline{b}\underset{\Leftarrow}{\overset{\Rightarrow}{}}\overline{b}|\overline{\overline{a}}$, ce qui découle de RÈG$|_{\Rightarrow}$ appliquée aux théorèmes $a\underset{\Leftarrow}{\overset{\Rightarrow}{}}\overline{\overline{a}}$ avec $\overline{b}$ ainsi que de COM et TRANS pour transformer $\overline{b}|a$ et $\overline{\overline{a}}|\overline{b}$ en les implications $a|\overline{b}$ et $\overline{b}|\overline{\overline{a}}$.

2. Appelons TE la règle "de $\overline{\overline{a}}$ déduire a". De $\overline{F} \Rightarrow E$ l'on tire (par contraposée) $\overline{E} \Rightarrow \overline{\overline{F}}$ et (TE et TRANS) $\overline{E} \Rightarrow F$, d'où (*via* $F \Rightarrow E$ et TRANS) $\overline{E} \Rightarrow E$, ce qui s'écrit $\overline{E}|\overline{E}$, ou encore $\overline{\overline{E}}$, d'où (TE) E.

3. Supposons $a \Rightarrow \theta$ où l'on a noté θ l'implication $a \Rightarrow b$. Pour prouver cette dernière, il suffit (par disjonction des cas) de montrer $\overline{a} \Rightarrow \theta$, ce qui découle (*via* TRANS) des théorèmes d'affaiblissement $\overline{a} \Rightarrow \left(\overline{b} \Rightarrow \overline{a}\right)$ et de contraposée $\left(\overline{b} \Rightarrow \overline{a}\right) \Rightarrow \theta$.

4. Supposons $p \Rightarrow q$. On en déduit (REG$_{|\Rightarrow}$) $\overline{E}|q \Rightarrow p|\overline{E}$, or on a le théorème $q|\overline{E} \Rightarrow \overline{E}|q$, d'où (TRANS) $q|\overline{E} \Rightarrow p|\overline{E}$, *c. q. f. d.*.

5. Appliquer la règle que l'on vient de légitimer depuis l'hypothèse $a \Rightarrow b$ en remplaçant $\left\uparrow\begin{array}{ccc} p & q & E \\ a & b & c \end{array}\right\uparrow$ donne $(b \Rightarrow c) \Rightarrow (a \Rightarrow c)$ et l'appliquer depuis l'hypothèse $a \Rightarrow (b \Rightarrow c)$ en remplaçant $\left\uparrow\begin{array}{ccc} p & q & E \\ a & b \Rightarrow c & a \Rightarrow c \end{array}\right\uparrow$ donne $[(b \Rightarrow c) \Rightarrow (a \Rightarrow c)] \Rightarrow [a \Rightarrow (a \Rightarrow c)]$, d'où (TRANS) $a \Rightarrow (a \Rightarrow c)$ puis (par contraction) $a \Rightarrow c$.

6. On veut $a|b/c \Rightarrow a|\overline{c}$, ce qui découle du théorème (incompatibilité) $\overline{c} \Rightarrow b|c$ en appliquant RÈG$|_{\Rightarrow}$ avec a puis TRANS avec $\overline{c}|a \Rightarrow a|\overline{c}$.

   Comme en logique usuelle, on récurre sur la longueur des preuves. Supposons que $\mathcal{A}$ et A prouvent B. Il y a donc une suite de propositions $A_1, ..., A_n = B$ qui sont ou bien des axiomes ou des formules de $\mathcal{A}$ (donc conséquences de $\mathcal{A}$), ou bien[12] A, ou bien déduites des précédentes.

   Le cas où B est un axiome ou une formule de $\mathcal{A}$ est trivialisé par l'affaiblissement $B \Rightarrow (A \Rightarrow B)$; le cas $B = A$ également par l'identité $A \Rightarrow A$. Reste la cas où B est déduit d'un A_i et d'un $A_{j>i}$, lesquels sont nécessairement (par définition de RÈG) de la forme P et $P|Q/B$. Par ailleurs, ils sont prouvés par $\mathcal{A}$ et A, d'où par hypothèse de récurrence les implications (prouvées par $\mathcal{A}$) $A \Rightarrow P$ et $A \Rightarrow P|Q/B$. Vu enfin l'implication $P|Q/B \Rightarrow (P \Rightarrow B)$ montrée en début de question, on en déduit (TRANS) $A \Rightarrow (P \Rightarrow B)$, d'où (question 5) $A \Rightarrow B$ comme voulu.

2.5 Théorème de complétude

On note At l'ensemble des atomes propositionnels de notre langage. Pour toute formule F écrite dans ce langage, on note $\operatorname{At} F$ la partie formée des atomes apparaissant dans F. De même, si $\mathcal{F}$ est un ensemble de telles formules, on notera $\operatorname{At} \mathcal{F} := \bigcup_{F \in \mathcal{F}} \operatorname{At} F$ l'ensemble des atomes de toutes les formules de $\mathcal{F}$.

On appelle ***valuation*** toute application v à valeurs dans $\{0, 1\}$ définie sur une partie de At (appelée le ***domaine*** de v et noté $\operatorname{Dom} v$). Toute valuation v peut être prolongée d'une unique manière aux formules F dont les atomes ont une image par v en imposant de manière inductive les quatre égalités[13] (pour toutes formules G et H dont les atomes tombent dans $\operatorname{Dom} v$)

$$v\,(G|H) = 0 \text{ ssi } v\,(G) = 1 = v\,(H)\,.$$

Lorsque $v\,(F) = 1$, on dit alors que v ***valide*** F et on note $v \models F$. On notera enfin

$$\mathcal{D}_v := \{a\ ;\ v\,(a) = 1\} \amalg \{\overline{a}\ ;\ v\,(a) = 0\} \qquad \text{(qui est validé par } v\text{)}$$

l'ensemble obtenu à partir de $\operatorname{Dom} v$ en remplaçant par leurs négations les atomes non validés par v.

Une ***tautologie*** Θ est une formule validée par toute valuation (définie partout[14]). On note alors $\models \Theta$.

1. *Montrer que les théorèmes sont des tautologies.*

   La réciproque fait l'objet du (méta-)**théorème de complétude** :

$$\models \Theta \ \textit{ssi}\ \vdash \Theta.$$

[12] bien sûr rien n'empêche $A \in \mathcal{A}$, auquel cas notre disjonction ne serait pas rigoureusement *exclusive*

[13] c'est-à-dire *via* la table de vérité du connecteur *NAND*

[14] cela revient à être validée par toute valuation dont le domaine contient $\operatorname{At} \Theta$

2. Fixons une valuation v. *Montrer que, pour toute formule F dont les atomes tombent dans* $\operatorname{Dom} v$ *:*

$$\begin{cases} \textit{si } v \models F, \textit{ alors } \mathcal{D}_v \vdash F \\ \textit{si } v \not\models F, \textit{ alors } \mathcal{D}_v \vdash \overline{F} \end{cases}.$$

3. *En déduire que les tautologies sont les théorèmes (on pourra utiliser la règle de disjonction des cas).*

Solution proposée.

1. On raisonne par récurrence sur la longueur de la preuve des théorèmes. (Nous avons en substance déjà fait le travail lorsque nous avons vérifié en logique classique.la validité de la règle RÈG et de l'axiome $\alpha|\beta/\gamma$.)

   Vérifions que les axiomes sont tautologiques (longueur minimale). Il n'y en a qu'un seul, de la forme $\alpha|\beta/\gamma$. Nous laissons le lecteur sceptique regarder les seize valuations possibles.

   Soit ensuite E un énoncé déduit de deux théorèmes. Puisqu'il n'y a qu'une seule règle, ces théorèmes ont pour formes respectives P et $P|Q/E$. Par hypothèse de récurrence, ces théorèmes sont des tautologies. Soit v une valuation définie partout. Alors v valide P et $P|Q/E$, donc v ne valide pas $Q|E$, *i. e.* v valide Q et E, d'où $v \models E$, ce qui conclut.

2. On raisonne par récurrence sur la complexité de F.

   Soit f un atome tombant dans $\operatorname{Dom} v$. Si $v \models f$, *i. e.* $v(f) = 1$, ou encore $f \in \mathcal{D}_v$, alors $\mathcal{D}_v \vdash f$. Sinon, $\mathcal{D}_v$ contient alors $\overline{f}$, d'où $\mathcal{D}_v \vdash \overline{f}$.

   Soit F non atomique telle que $\operatorname{At} F \subset \operatorname{Dom} v$. Soient G et H deux formules telles que $F = G|H$. Observer que, v étant définie sur $\operatorname{At} F = \operatorname{At} G \cup \operatorname{At} H$, les validités de G et de H font sens. Si $v \models F$, alors v ne valide pas simultanément G et H (sinon v validerait la conjonction $G \wedge H = \overline{G|H} = \overline{F}$) ; supposant[15] $v \not\models \frac{G}{H}$, on obtient par hypothèse de récurrence $\mathcal{D}_v \vdash \frac{\overline{G}}{\overline{H}}$ et les théorèmes $\frac{\overline{G}}{\overline{H}} \Rightarrow G|H$ permettent de conclure dans chacun des deux cas. Si maintenant $v \not\models F$, alors v valide $\overline{G|H} = G \wedge H$, donc v valide à la fois G et H, d'où (par hypothèse de récurrence) $\begin{cases} \mathcal{D}_v \vdash G \\ \mathcal{D}_v \vdash H \end{cases}$ et la conclusion $\mathcal{D}_v \vdash G \wedge H = \overline{F}$.

3. Soit Θ une tautologie. Explicitons $\operatorname{At} \Theta = \{a, b, c, ..., z\}$ (qui est bien *fini*). Puisque toute valuation valide Θ, chaque valuation vérifiera $\mathcal{D}_v \vdash \Theta$, mettons $A, B, C, ..., X, Y, Z \vdash \Theta$ où chaque majuscule latine est un atome ou sa négation et où chaque atome apparaît une fois exactement. Le théorème de la déduction permet alors d'obtenir successivement

$$\begin{array}{rcl} A, B, ..., X, Y, Z & \vdash & \Theta \\ A, B, ..., X, Y & \vdash & Z \Rightarrow \Theta \\ A, B, ..., X & \vdash & Y \Rightarrow (Z \Rightarrow \Theta) \\ & \cdots & \\ A, B & \vdash & C \Rightarrow [D \Rightarrow (E \Rightarrow [\cdots (X \Rightarrow [Y \Rightarrow (Z \Rightarrow \Theta)]) \cdots])] \\ A & \vdash & B \Rightarrow (C \Rightarrow [D \Rightarrow (E \Rightarrow [\cdots (X \Rightarrow [Y \Rightarrow (Z \Rightarrow \Theta)]) \cdots])]) \\ & \vdash & A \Rightarrow [B \Rightarrow (C \Rightarrow [D \Rightarrow (E \Rightarrow [\cdots (X \Rightarrow [Y \Rightarrow (Z \Rightarrow \Theta)]) \cdots])])] . \end{array}$$

   L'idée est maintenant d'utiliser la règle de disjonction des cas afin de faire tomber chaque prémisse en tête de la longue implication ci-dessus : quand il n'en restera plus, seul survivra $\vdash \Theta$, notre souhait.

   Une notation *indexée* nous aidera à rédiger la récurrence : définissons n le nombre d'atomes de Θ et renommons-les $(a_1, a_2, ..., a_n) := (a, b, c, ..., z)$. Pour tout entier $k \in [1, n]$, on note E_k l'énoncé

$$\begin{array}{rcl} \text{pour tout } \overrightarrow{A} & \in & \{a_k, \overline{a_k}\} \times \{a_{k+1}, \overline{a_{k+1}}\} \times \cdots \times \{a_n, \overline{a_n}\} , \\ \text{on a} & \vdash & A_k \Rightarrow (A_{k+1} \Rightarrow (\cdots (A_{n-1} \Rightarrow (A_n \Rightarrow \Theta)) \cdots)) . \end{array}$$

   L'initialisation E_1 a été effectuée au paragraphe précédent : lorsque v décrit les valuations définies exactement sur $\operatorname{At} \Theta$, la suite $\overrightarrow{A}$ décrit tout le produit $\prod_{i=1}^{n} \{a_i, \overline{a_i}\}$. Soit alors $k \in [1, n]$ un entier tel que E_k. Soit $A \in \prod_{i>k}^{n} \{a_i, \overline{a_i}\}$. Notons

$$I := A_{k+1} \Rightarrow (\cdots (A_{n-1} \Rightarrow (A_n \Rightarrow \Theta)) \cdots) \text{ l'implication désirée (qui conclura à } E_{k+1}\text{)}.$$

   D'après E_k, on dispose des deux implications $\begin{cases} a_k \Rightarrow I \\ \overline{a_k} \Rightarrow I \end{cases}$, d'où I découle par disjonction des cas.

[15] en fait, seul nous suffira le conjoint "*si* $v \models F$, *alors* $\mathcal{D}_v \vdash F$" ; comme le montre la récurrence, il est plus que commode d'incorporer le deuxième conjoint "*si* $v \not\models F$, *alors* $\mathcal{D}_v \vdash \overline{F}$" dans l'énoncé à établir