Connecteur de Sheffer et axiome de Nicod

Marc SAGE

16 mai 2015

Table des matières

Résumé. On montre ici que le calcul des prédicats, muni des 5 connecteurs $\neg \wedge \vee \implies \iff$ régis par les 14 axiomes de Hilbert et de la règle du *modus ponens* peut se réduire à un seul connecteur $|$ et un seul axiome (avec toujours une seule règle).

Remarque historique. D'après Mordechaj Wasjberg, Jean Nicod est le premier à avoir réalisé cela, dans l'article (disponible sur wikisource) *A reduction in the number of the Primitive Propositions of Logic* publié[1] en 1920. Dans ce DM, nous avons en substance traduit, (corrigé,)distillé et commenté cet article. Le lecteur uniquement intéressé par le résultat optimal de Wajsberg consultera l'autre DM, bien mieux rédigé et mis en forme que celui-ci et qui contient tout le fond de ce dernier[2].

Notations.
La négation d'une proposition sera indifféremment notée $\neg A$ ou $\overline{A}$.
Les variables propositionnelles seront $a, b, c...$ ou $p, q, r...$

[1] *Proceedings of the Cambridge Philosophical Society* **19** (1917-1920), 32-41
[2] seule diffèrent les preuves de l'identité $a \implies a$

1 Le connecteur de Sheffer en logique classique

En logique classique, on définir le connecteur de Sheffer, ou d'incompatibilité, par $a|b := \overline{a} \vee \overline{b}$ (connecteur NAND). On pourra noter / pour signifier que les autres connecteurs sont prioritaires sur / (par exemple, $a|b/c$ signifie $a|\,(b|c)$).

1. *Exprimer tous les connecteurs usuels à l'aide de* $|$. *Faite 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* $d|b \implies a|d$.
3. *Montrer que* $a \implies b$ *implique* $p|b \implies a|p$.

Solution proposée.

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

   En revanche, l'implication $a \implies b = \overline{a} \vee b = \overline{\overline{a}}|\overline{b}$ s'écrit $a|\overline{b} = \overline{a||b}$, ce qui s'exprime plus facilement avec $|$ qu'avec $||$ (de même pour $\impliedby$). *A contrario*, l'équivalence $a \iff b = (a \implies b) \wedge (a \impliedby b)$ s'écrit $\overline{a/\overline{b}|\overline{a}/b} = \big(a||\overline{b}\big)\,||\,(\overline{a}||b)$ 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 $p|q = p|\overline{\overline{q}} = p \implies \overline{q}$ (dire que p et q sont incompatibles, c'est dire que p entraîne la négation de l'autre), puis que que $\overline{x|y} = \overline{\overline{x} \vee \overline{y}} = x \wedge y$ (nier l'incompatibilité de x et y, c'est dire qu'ils sont tous deux vérifiés), on traduit $a|b/c = a \implies \overline{b|c} = a \implies b \wedge c$, autrement dit "$a$ entraîne b et c". 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 $a \implies b$; si p et b sont incompatibles, alors a et p le sont nécessairement (si a était vrai, b le serait d'après $a \implies b$, donc p serait infirmé d'après $p|b$).

2 Logique de Nicod

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

$$\begin{array}{cccc} \overline{a} & a \wedge b & a \vee b & a \implies b \\ a|a & \overline{a|b} & \overline{a}|\overline{b} & a|\overline{b} \end{array} .$$

On se donne pour seule règle (dénotée par la suite RÈG) de pouvoir déduire de a et $a|b/c$ la proposition c.
On se donne pour axiomes toute instance de l'unique formule

$$[a|b/c]\,|\,[e|e/e]\,/\,[(d|b)\,|\,(a|d)\,/\,(a|d)]\,.$$

On abrégera par la suite $\begin{array}{ccc} \alpha := & i := & \gamma := \\ a|b/c & e|e/e & (d|b)\,|\,(a|d)\,/\,(a|d) \end{array}$.

1. *Vérifier la validité de la règle et de l'axiome en logique classique.*
2. *Expliquer en quoi la forme de l'axiome permet d'établir des théorèmes autres que des instances de celui-ci. En établir un.*
3. *Montrer que la règle du* modus ponens *est valide.* (Ce dernier sera invoqué par le sigle MOD.)
4. *Montrer que, de* $a \implies b$, *on peut déduire* $p|b \implies a|p$. (Cette règle mélangeant les connecteurs $|$ et $\implies$ sera appelée RÈG$_{|\implies}$)

Solution proposée.

1. Au vu de la définition de $\Longrightarrow$, l'axiome se réécrit plus joliment

$$(a|b/c)\,|\,(e \implies e)\,/\,(d/b \implies a/d)\,.$$

En logique classique, c'est dire que $a|b/c$ implique d'une part la tautologie $e \implies e$ (ce qui est tautologique) d'autre part l'implication $d/b \implies a/d$, ce que nous avons déjà montré. Par ailleurs, nous avons montré que $a|b/c$ entraînait b et c, en particulier c, d'où la validité de RÈG.

2. Vue la règle, on ne peut partir que de deux énoncés a et $a|b/c$ qui soient tous deux axiomes. Par conséquent, la forme $\alpha|i/\gamma$ de l'axiome *doit* permettre de substituer à α un axiome – or c'est le cas puique α est de la forme $a|b/c$. Par exemple, en remplaçant $(a,b,c) \leftarrow (\alpha, i, \gamma)$, on peut déduire des deux axiomes $\alpha|i/\gamma$ et $(\alpha|i/\gamma)\,|i/\,(d|i \implies \alpha|d)$ le théorème $d|\,(e \implies e) \implies (a|b/c)\,|d$.
3. Prendre $b = c$ dans la règle donne $a|b/b = a|\overline{b} = a \implies b$.
4. Prendre $b = c$ dans l'axiome montre que, de $a \implies b$, on peut déduire $d|b \implies a|d$.

2.1 L'identité $a \implies a$ et la commutativité $a|b \implies b|a$

On note *co* l'énoncé (de **co**mmutativité) $d|e \implies e|d$.

1. *Montrer l'énoncé $V := i|i/co$, puis en déduire $p|i/q \implies q/i|p$.*
2. *Expliquer pourquoi la proposition $co/i|i$ est de la forme α. Montrer $\gamma/i|\alpha \implies V|\gamma/i$ et conclure à i puis à co.*

La règle de commutation (de $x|y$ déduire $y|x$) sera notée COM.
La règle découlant de i (de $a|\overline{a} \implies b$ déduire b) sera notée ID.

Solution proposée.

1. La forme de V nous incite à montrer qu'il s'agit d'une instance de l'axiome : pour faire apparaître $e \implies e$ à gauche, on prend $a, b, c \leftarrow e$, ce qui suffit à notre bonheur.

   Ensuite, pour utiliser V, on fait apparaître du $V|?/?$ en prenant l'axiome avec $a, b \leftarrow i$ et $c \leftarrow co$, d'où l'on déduit (RÈG) $d/i \implies i/d$ puis (RÈG$_{|\,\Longrightarrow}$ avec p) $p|i/d \implies d/i|p$ comme voulu (les variables d, p et celle apparaissant dans i sont indépendantes). Cet énoncé permet d'échanger deux lettres de part et d'autre de i ; on le notera (très temporairement) *éch.*
2. L'énoncé i est une implication, donc de la forme $x|y$, de sorte que n'importe quoi du type $?|i$ est de la forme $?|x/y$ et donc de celle de α.

   L'implication demandée découlera de RÈG$_{|\,\Longrightarrow}$ utilisée avec γ/i sur l'implication $V \implies \alpha$; or cette dernière s'écrit $i|i/co \implies co/i|i$, ce qui est une instance de *éch.*

   Pour conclure, on écrit l'axiome $\alpha|i/\gamma$, d'où (*éch* et MOD) $\gamma/i|\alpha$ et (MOD) $V|\gamma/i$, d'où l'on tire (RÈG) i et (RÈG$_{|\,\Longrightarrow}$ avec d) co.

Reprise linéaire de la preuve de $a \implies a$.

• l'axiome $\alpha|i/\gamma$, après remplacement $\begin{matrix} a & b & c \\ e & e & e \end{matrix}$, s'écrit $i|i/co =: V$;

• remplacer[3] $\begin{matrix} a & b & c & d \\ i & i & co & \dot\gamma \end{matrix}$ dans l'axiome $\alpha|i/\gamma$ réalise la prémisse V, d'où (RÈG) le conséquent $\dot\gamma|i \implies i|\dot\gamma$, d'où (RÈG$_{|\Longrightarrow}$) $\dot\alpha|i/\dot\gamma \implies \dot\gamma|i/\dot\alpha$ dont la prémisse est un axiome, d'où (MOD) $\dot\gamma|i/\dot\alpha$;

• remplacer $\begin{matrix} a & b & c & d \\ i & i & co & V \end{matrix}$ dans l'axiome $\alpha|i/\gamma$ réalise la prémisse V, d'où (RÈG) le conséquent $co|i \implies i|co$, d'où (RÈG$_{|\Longrightarrow}$) $i|i/co \implies co|i/i$, qui est de la forme $V \implies \dot\alpha$ après remplacement $\begin{matrix} a & b & c \\ co|i & e & \overline{e} \end{matrix}$, d'où (RÈG$_{|\Longrightarrow}$) $\dot\gamma/i|\dot\alpha \implies V|\dot\gamma/i$ puis (MOD) $V|\dot\gamma/i$ et (RÈG) i.

[3] on pointe α et γ pour signaler que les variables a, b, c peuvent être instanciées par *d'autres* lettres, afin d'éviter toute confusion entre les lettres instanciées a, b, c et celles qui apparaissent dans les instances

2.2 La tautologie $a \implies (b \implies a)$ et le tiers exclu

1. *Montrer* $(a \implies b) \implies \big(\overline{b}|a\big)$*, en déduire* $\overline{q \implies p}|\overline{p}/q$*, d'où conclure* $p \implies (q \implies p)$*.*
2. *Montrer les énoncés* $a \underset{\Longleftarrow}{\overset{\Longrightarrow}{}} \overline{\overline{a}}$*.*

La règle tautologique (de a déduire $b \implies a$) sera notée TAUT.
La règle du tiers exclu (de a déduire $\overline{\overline{a}}$) sera notée TE.

Solution proposée.

1. On veut $a|\overline{b} \implies \overline{b}|a$, ce qui est une instance de COM.

   Pour réaliser la prémisse $a \implies b$, on peut réaliser une instance de COM, par exemple en prenant $\binom{a}{b} \leftarrow \binom{p/q}{q/p}$, d'où (MOD) $\overline{q/p}|p/q$. La forme voulue $\overline{q/\overline{p}}|\overline{p}/q$ s'obtient en remplaçant p par $\overline{p}$.

   On fait apparaître la proposition $\overline{q \implies p}|\overline{p}/q$ en tête de l'axiome en substituant dans ce dernier $(a, b, c) \leftarrow (\overline{q \implies p}, \overline{p}, q)$, d'où l'on déduit $(d|\overline{p}) \implies (\overline{q \implies p}|d)$. On réalise ensuite $d|\overline{p}$ en remplaçant $d \leftarrow p$ (c'est l'identité $p \implies p$), d'où l'on tire (ID) $\overline{q \implies p}|p$, d'où (COM) $p|\overline{q \implies p}$, ce qui est la forme cherchée.
2. Puisque $\overline{\overline{a}}$ se réécrit $\overline{a}|\overline{a}$, à savoir $\overline{a} \implies a$, l'énoncé $a \implies \overline{\overline{a}}$ est une instance de $p \implies (q \implies p)$.

   L'énoncé $\overline{\overline{a}} \implies a$ se réécrit $\overline{\overline{a}}|\overline{a}$, qui est équivalent (COM) à $\overline{a}|\overline{\overline{a}}$, donc à l'identité $\overline{a} \implies \overline{a}$.

2.3 La transitivité de l'implication $(a|b/c) \implies (b|d \implies a|d)$

On souhaite établir le théorème (appelé par la suite *trans*)

$$a|b/c \implies (b|d \implies a|d)\,.$$

Commentaires.

1. *Déduire de trans la règle TRANS :*

   $$\textit{de } a \implies b \textit{ et } b \implies c \textit{ l'on peut déduire } a \implies c.$$

2. *Établir la règle "de* $a|b/c$ *déduire* $(d|b \implies a|d)$*" et commenter.*

   Preuve.
3. *En utilisant l'énoncé* $\overline{q/p}|p/q$ *prouvé dans la preuve de TAUT, montrer* $x \vee y/x$ *et en déduire* $\alpha \implies \gamma$ *(utiliser l'axiome en prémisse d'une implication).*
4. *En invoquant à deux reprises le théorème* $p|x/y \implies y/x|p$ *(à établir), montrer* $\overline{b/d|e|}\,(e|d/b)$ *puis* $\overline{b|d \implies a|d}|\gamma$*.*
5. *Conclure en appliquant RÈG*$_{|\implies}$ *sur le théorème* $\alpha \implies \gamma$*.*

Solution proposée.

1. En prenant $c = b$ et $d \leftarrow \overline{d}$, on obtient $(a \implies b) \implies ((b \implies d) \implies (a \implies d))$, d'où la règle TRANS en appliquant deux fois MOD.
2. Il s'agit de déduire de α la conclusion γ. L'axiome $\alpha|i/\gamma$ et la règle RÈG sont faits pour cela.

   La différence avec l'énoncé *trans* est, d'une part dans l'ordre $b|d$ au lieu de $d|b$ (ce qui expliquera l'intervention lourde de COM dans la preuve qui suit) d'autre part dans le fait que *trans* est un *théorème* (ce qui est plus fort que la *règle* qui en découle).
3. Vue la définition de $\vee$, la règle COM permet d'écrire la commutativité de $\vee$. On fait apparaître en tête de l'axiome l'énoncé rappelé en substituant $\dfrac{a \quad b \quad c \quad d}{q|p \quad p \quad q \quad \overline{p}}$, d'où (RÈG) $\overline{p}/p \implies q/p \vee p$ et (ID) $q/p \vee p$, ce qui conclut par COM.

   On veut obtenir $\alpha|\overline{\gamma}$ (ce qui revient à $\overline{\gamma}|\alpha$ par COM) et l'on aimerait utiliser l'axiome $\alpha|i/\gamma$ en prémisse d'une implication : suffirait à notre bonheur l'implication $\alpha|i/\gamma \implies \overline{\gamma}|\alpha$. Or cette dernière peut être obtenue par RÈG$_{|\implies}$ (avec α) depuis l'implication $\overline{\gamma} \implies i/\gamma$, laquelle est une réécriture du théorème $\gamma \vee i/\gamma$.

4. Le théorème à établir se déduit en appliquant $\text{RÈG}_{|\Longrightarrow}$ avec p au théorème $y|x \Longrightarrow x|y$ (c'est *co*).

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

   On le réinjecte alors en prémisse dans le théorème ci-dessus en prenant $(p,x,y) \leftarrow \left(\overline{b/d|e}, e, d/b\right)$, d'où (RÈG) $(d|b)\,/e|\overline{b/d|e}$ et (COM) $\overline{b/d|e|}\,(d|b)\,/e$: il suffit alors de prendre $e \leftarrow \overline{a|d}$ pour obtenir le second énoncé voulu.

5. Pour conclure, la règle indiquée permet de déduire de $\alpha \Longrightarrow \gamma$ des théorèmes $p|\gamma \Longrightarrow \alpha|p$; or on vient de montrer $\overline{b|d \Longrightarrow a|d}|\gamma$, ce qui incite (afin de réaliser $p|\gamma$) à prendre $p \leftarrow \overline{b|d \Longrightarrow a|d}$. On en tire (RÈG) $(a|b/c)\,|p$, ce qui se réécrit $a|b/c \Longrightarrow (b|d \Longrightarrow a|d)$, *CQFD.*

2.4 Complétude de la logique de Nicod

Vers le théorème de la déduction.

1. *Prouver les théorèmes suivants (contraposée)* $(a \Longrightarrow b) \Longrightarrow \left(\overline{b} \Longrightarrow \overline{a}\right)$ *et* $\left(\overline{b} \Longrightarrow \overline{a}\right) \Longrightarrow (a \Longrightarrow b)$.
   En déduire que, si un énoncé est impliqué par une formule f et sa négation $\overline{f}$, alors cet énoncé est un théorème. Prouver alors la validité de la règle "de $a \Longrightarrow (a \Longrightarrow b)$ déduire $a \Longrightarrow b$"
2. *En utilisant deux fois la règle (à légitimer) "de $p \Longrightarrow q$ déduire $(q \Longrightarrow E) \Longrightarrow (p \Longrightarrow E)$", établir la règle "de $a \Longrightarrow b$ et $a \Longrightarrow (b \Longrightarrow c)$ déduire $a \Longrightarrow c$".*
3. *Montrer l'implication $a|b/c \Longrightarrow (a \Longrightarrow c)$ et conclure au théorème de la déduction ; 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 e revient à affirmer que l'on peut de $\mathcal{A}$ déduire $a \Longrightarrow e$.*

Vers le théorème de complétude.

4. *Pour v distribution de vérité, on note A_v l'ensemble formé des variables satisfaites par v et des négations des autres variables. Montrer qu'un v (ne) satisfait (pas) une formule ssi A_v prouve (nie) cette dernière.*
5. *Conclure au théorème de complétude.*

Solution proposée.

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

   Notons E notre énoncé : on a alors $f \Longrightarrow E$ et $\overline{f} \Longrightarrow E$, d'où par contraposée $\overline{E} \Longrightarrow \overline{\overline{f}}$ et (TE et TRANS) $\overline{E} \Longrightarrow f$, d'où (TRANS) $\overline{E} \Longrightarrow E$, ce qui s'écrit $\overline{E}|\overline{E}$, ou encore $\overline{\overline{E}}$, d'où (TE) E.

   Supposons $a \Longrightarrow \theta$ où l'on a noté θ l'implication $a \Longrightarrow b$. Pour prouver la thèse θ, il suffit de montrer $\overline{a} \Longrightarrow \theta$, ce qui découle de la tautologie $\overline{a} \Longrightarrow \left(\overline{b} \Longrightarrow \overline{a}\right)$ et de la contraposée $\left(\overline{b} \Longrightarrow \overline{a}\right) \Longrightarrow \theta$.

2. Supposons $p \Longrightarrow q$. On en déduire $(\text{REG}_{|\Longrightarrow})$ $\overline{E}|q \Longrightarrow p|\overline{E}$, or (*co*) $q|\overline{E} \Longrightarrow \overline{E}|q$, d'où (TRANS) $q|\overline{E} \Longrightarrow p|\overline{E}$, cqfd.

   Appliquer la règle depuis l'hypothèse $a \Longrightarrow b$ en remplaçant $\begin{matrix} p & q & E \\ a & b & c \end{matrix}$ donne $(b \Longrightarrow c) \Longrightarrow (a \Longrightarrow c)$ et l'appliquer depuis l'hypothèse $a \Longrightarrow (b \Longrightarrow c)$ en remplaçant $\begin{matrix} p & q & E \\ a & b \Longrightarrow c & a \Longrightarrow c \end{matrix}$ donne $[(b \Longrightarrow c) \Longrightarrow (a \Longrightarrow c)] \Longrightarrow [a \Longrightarrow (a \Longrightarrow c)]$, d'où (TRANS) $a \Longrightarrow (a \Longrightarrow c)$ puis (question 1) $a \Longrightarrow c$.

3. On veut $a|b/c \Longrightarrow a|\overline{c}$, ce qui découlerait de l'implication $\overline{c} \overset{?}{\Longrightarrow} b/c$ en appliquant $\text{RÈG}_{|\Longrightarrow}$ avec a, laquelle s'écrit $\overline{c}|\overline{b|c}$. Or partir de l'identité $\overline{x|y}|x/y$ permet de récolter $d|y \Longrightarrow \overline{x|y}|d$ dont on réalise la prémisse en prenant $d \leftarrow \overline{y}$, ce qui fournit la conclusion recherchée. (modulo tous les COM et TRANS)

   Comme en logique usuelle, on récurre sur la longueur des preuves. Supposons que $\mathcal{A}$ et a prouve b. Il y a donc une suite de propositions $a_1, ..., a_n = b$ qui sont ou bien des axiomes (ou des formules de $\mathcal{A}$), ou bien a, ou bien déduites des précédentes.

   Le cas où b est un axiome ou une formule de $\mathcal{A}$ est trivialisé par la tautologie $b \Longrightarrow (a \Longrightarrow b)$; le cas $b = a$ également par l'identité $a \Longrightarrow a$. 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$\mathcal{A}$) $a \Longrightarrow p$ et $a \Longrightarrow p|q/b$. Vu enfin l'implication $p|q/b \Longrightarrow (p \Longrightarrow b)$ montrée en début de question, on en déduit (TRANS) $a \Longrightarrow (p \Longrightarrow b)$, d'où (question 2) $a \Longrightarrow b$ comme voulu.

4. On raisonne par récurrence sur la complexité de la formule f. Supposons f une variable : alors elle appartient à A_v dès que v la satisfait, tandis que sa négation est dans A_v dans le cas contraire. Supposons à présent f de la forme $g|h$: si v satisfait $g|h$, alors v ne peut satisfaire g et h, donc A_v prouve $\overline{g}$ ou prouve $\overline{h}$ et l'on conclut en invoquant le théorème sus-montré $\overline{x} \implies y|x$ (avec au besoin COM). L'argument est semblable lorsque v ne satisfait pas f.

5. (esquisse de preuve) Soit f une formule valide dont on note A l'ensemble des variables. On se donne une distribution de vérité v sur A. Pour toute variable $a \in A$, la distribution v_a définie par $a \mapsto \overline{v(a)}$ et v partout ailleurs satisfait f, donc A_{v_a} prouve f, tout comme A_{v_a}.Or ces deux ensembles sont de la forme $B \cup \{a\}$ et $B \cup \{\overline{a}\}$, donc B prouve f d'après la question 1. On récurre alors pour faire disparaître toutes les variables dans A (preuve détaillée dans le DM sur Wajsberg).

3 Exercices divers (matériel originel inutile)

Pour ceux qui voudraient encore s'entraîner à pousser des symboles, on regroupe dans cette dernière section quelques énoncés, souvent tirés de l'article de Nicod (tous étant tautologiques et donc conséquences du théorème de complétude que nous venons d'établir). Ils n'apportent *rien* au fond et ont pour seul intérêt d'établir *directement* les axiomes usuels du calcul propositionnel (d'où le théorème de complétude) sans utiliser la section précédente. Le lecteur pourra ainsi juger de lui-même la concision de notre distillation de l'article de Nicod où nous avons choisi d'établir dès que possible le théorème de complétude.

3.1 Le *modus ponens* érigé en théorème

On se propose de montrer le théorème (ci-après dénommé *mo*)

$$a \implies (a/b|b)\,.$$

Commentaires.

1. *Déduire de mo le théorème* $a \implies ((a \implies b) \implies b)$ *et justifier le lien avec le théorème de la déduction de la logique classique.*

   Preuve.

2. *Montrer que l'on peut déduire des implications* $a \implies b$ *et* $a \implies (b \implies c)$ *l'implication* $a \implies (a \implies c)$.

3. *En utilisant le théorème* $x \vee (y/x)$ *établi plus haut, montrer que* $\overline{mo} \implies a$.

4. *En égalant certaines variables dans trans, établir* $a \implies \big(a|b \implies \overline{b}\big)$. *Montrer d'autre part à l'aide de trans l'énoncé* $\big(a|b \implies \overline{b}\big) \implies \big(\overline{b}|b \implies a/b|b\big)$.

5. *À l'aide du théorème* $b \implies \overline{a}|a$ *(à prouver), établir* $a \implies mo$ *et conclure à mo.*

Solution proposée.

1. Il suffit de remplacer $b \leftarrow \overline{b}$. Lorsque l'on dispose d'un théorème $a \implies b$, on en déduit immédiatement la règle "de a on peut déduire b". La réciproque est l'objet du théorème de la déduction : si d'un ensemble E de formules on peut déduire avec e un énoncé a, alors de E on peut dériver $e \implies a$. Dans le cas du *modus ponens* "de a et $a \implies b$ on déduit b", on obtient "de a on déduit $(a \implies b) \implies b$" puis "de rien on déduit $a \implies ((a \implies b) \implies b)$", ce qui est le théorème *mo*.

2. La conclusion peut s'obtenir à l'aide de TRANS

$$(a \implies ?) \implies [(? \implies (a \implies c)) \implies (a \implies (a \implies c))]$$

   si l'on trouve un ? réalisant les deux implications où il apparaît. Prendre b ou $b \implies c$ satisferait la première d'après les hypothèses – mais la seconde ? En observant que $(b \implies c) \implies (a \implies c)$ vient de $a \implies b$ et de TRANS, on est comblé.

3. L'énoncé voulu $\overline{mo} \implies a$ se récrit $\overline{mo}|\overline{a}$, ce qui équivaut (COM) à $\overline{a}|\overline{mo}$, *i. e.* à $\overline{a} \implies mo$, ou encore à $\overline{a} \implies (a \implies (a/b|b))$. Or le théorème rappelé $\overline{x \vee (y/x)}$ s'écrit aussi $\overline{x} \implies y|x$, ou encore (COM) $\overline{x} \implies x|y$. Il suffit pour conclure de prendre $y = \overline{a/b|b}$.

4. Prendre $\binom{c}{d} \leftarrow \binom{a}{b}$ dans *trans* donne $(b \implies a) \implies \big(a|b \implies \overline{b}\big)$. Or, on dispose de la tautologie $a \implies (b \implies a)$, d'où l'on déduit (TRANS) $a \implies \big(a|b \implies \overline{b}\big)$.

   Prendre $(a, b, c, d) \leftarrow \big(a/b, \overline{b}, \overline{b}, b\big)$ donne $\big(a|b \implies \overline{b}\big) \implies \big(\overline{b}|b \implies a/b|b\big)$ comme voulu.

5. La question précédente doit nous inciter immédiatement à établir (via TRANS) $a \implies \big(\overline{b}|b \implies a/b|b\big)$. Par ailleurs, vu le théorème $\overline{b}|b$, TAUT permet d'écrire $a \implies \overline{b}|b$. La question 2 permet alors d'obtenir $a \implies (a \implies a/b|b)$, à savoir $a \implies mo$. Pour conclure, on recolle $\overline{mo} \implies a$ et $a \implies mo$ via TRANS, ce qui donne $\overline{mo} \implies mo$, *i. e.* $\overline{\overline{mo}}$, ou encore (TE) mo, *CQFD.*

3.2 Axiomes du calcul propositionnel

Retrouver tous les axiomes usuels du calcul propositionnels.

Il suffit d'établir n'importe quel système d'axiomes aboutissant au théorème de complétude, par exemple les quatorze axiomes de HILBERT. Nous prendrons pour notre part les onze axiome du cours de Patrick DEHORNOY[4].

Axiomes de $\neg$.
Les énoncés du tiers exclu et de double négation ont été montrés. Reste la contraposée, qui s'écrit aussi $a|\overline{b} \underset{\Longleftarrow}{\Longrightarrow} \overline{b}|\overline{a}$, ce qui découle de RÈG$_{|\implies}$ appliquée aux théorèmes $a \underset{\Longleftarrow}{\Longrightarrow} \overline{\overline{a}}$ avec $\overline{b}$ ainsi que de COM et TRANS pour transformer $\overline{b}|a$ en l'implication $a|\overline{b}$.

Axiomes de $\vee$.
$a \implies (a \vee b)$ se réécrit $a \implies (\overline{a} \implies b)$, ce qui découlera de $a \implies \big(\overline{b} \implies \overline{\overline{a}}\big)$ (TRANS et contraposée), qui en retour peut être déduit de $\overline{\overline{a}} \implies \big(\overline{b} \implies \overline{\overline{a}}\big)$ (TRANS et TE), ce qui est *taut.*
$b \implies (a \vee b)$ se réécrit $b \implies \overline{a}|\overline{b}$, soit encore $b \implies (\overline{a} \implies b)$, ce qui est *taut.*
$\overline{a} \implies (a \vee b \implies b)$ se réécrit $\overline{a} \implies ((\overline{a} \implies b) \implies b)$, ce qui est *mo.*

Axiomes de $\wedge$.
$a \wedge b \implies \begin{smallmatrix} a \\ b \end{smallmatrix}$ se déduisent des contraposées de $\begin{smallmatrix} \overline{a} \\ \overline{b} \end{smallmatrix} \implies \overline{a} \vee \overline{b}$.
$a \implies (b \implies a \wedge b)$ se réécrit $a \implies \Big(b|\overline{\overline{a|b}}\Big)$, ce qui revient (TRANS et COM) à $a \implies \Big(\overline{\overline{a|b}}|b\Big)$, ou encore (on va le montre) à $a \implies (a/b|b)$, ce qui est *mo.* Pour combler notre lacune, on part du tiers exclu $\overline{\overline{a|b}} \underset{\Longleftarrow}{\Longrightarrow} a|b$, on applique RÈG$_{|\implies}$ avec b pour dériver $\overline{\overline{a|b}}|b \underset{\Longleftarrow}{\Longrightarrow} a/b|b$ (invoquer COM et TRANS pour rétablir l'ordre), puis on invoque TRANS pour obtenir l'équivalence annoncée.

Axiomes de $\Longleftrightarrow$.
Nous n'avons pas défini de symbole $\Longleftrightarrow$. Si l'on le fait à l'aide d'une conjonction d'implications réciproques, les axiomes de $\Longleftrightarrow$ découleront trivialement de ceux de $\wedge$.

Axiomes de $\implies$.
La tautologie $a \implies (b \implies a)$ a déjà été établie.
$(a \implies (b \implies c)) \implies ((a \implies b) \implies (a \implies c))$: il traduit en théorème la règle de la question 2 dont nous avons eu besoin pour établir le théorème de la déduction. Nous laissons le lecteur en trouver une preuve directe "courte", à défaut de laquelle la concision de notre démarche nous semblera acquise.

3.3 Quelques théorèmes en plus pour la route

1. *Établir les théorèmes*

$$a \implies b \underset{\Longleftarrow}{\Longrightarrow} \overline{a} \vee b \qquad a|b \underset{\Longleftarrow}{\Longrightarrow} \overline{a} \vee \overline{b} \qquad \overline{a \wedge b} \underset{\Longleftarrow}{\Longrightarrow} \overline{a} \vee \overline{b}.$$

2. *Montrer* $(a \implies b|c) \underset{\Longleftarrow}{\Longrightarrow} (b \implies a|c)$ *et en déduire*

$$(a \implies (b \implies c)) \underset{\Longleftarrow}{\Longrightarrow} (b \implies (a \implies c)).$$

[4] http ://www.math.unicaen.fr/~dehornoy/Surveys/DehornoyChap6.pdf (page 163 du cours, chapitre 6)

3. *Montrer* $(a \implies b) \implies (p \vee a \implies q \vee b)$.
4. *Montrer* $[a \implies (b \implies c)] \implies [(d \implies b) \implies (a \implies (d \implies c))]$ *puis* $[a \implies (b \implies c)] \implies [(b \vee c) \implies (a \implies c)]$.
5. *Montrer* $a \wedge (a|b/c) \implies c$ (traduit la règle RÈG en théorème).

Solution proposée.

1. L'énoncé $\overline{a} \vee b$ se réécrit $\overline{\overline{a}}|\overline{b}$, autrement dit $\overline{\overline{a}} \implies b$. Vue l'équivalence $a \underset{\Longleftarrow}{\overset{\Longrightarrow}{}} \overline{\overline{a}}$, le premier duo de théorèmes tombe par TRANS.

   L'énoncé $\overline{a} \vee \overline{b}$ se réécrit $\overline{\overline{a}}|\overline{\overline{b}}$. Appliquer $\text{RÈG}_{|\implies}$ aux théorèmes $b \underset{\Longleftarrow}{\overset{\Longrightarrow}{}} \overline{\overline{b}}$ avec $\overline{\overline{a}}$ donne $\overline{\overline{a}}|\overline{\overline{b}} \underset{\Longleftarrow}{\overset{\Longrightarrow}{}} b|\overline{\overline{a}}$, ce qui revient (via TRANS et COM) à $\overline{\overline{a}}|\overline{\overline{b}} \underset{\Longleftarrow}{\overset{\Longrightarrow}{}} \overline{\overline{a}}|b$, tandis que l'appliquer aux théorèmes $a \underset{\Longleftarrow}{\overset{\Longrightarrow}{}} \overline{\overline{a}}$ avec b donne (modulo TRANS et COM) $\overline{\overline{a}}|b \underset{\Longleftarrow}{\overset{\Longrightarrow}{}} a|b$. On conclut en invoquant TRANS[5].

   L'énoncé $\overline{a \wedge b}$ se récrit $\overline{\overline{a|b}}$, ce qui équivaut (TE) à $a|b$, donc à $\overline{a} \vee \overline{b}$ par ce qui précède.
2. Vue la symétrie entre a et b (et TRANS), il suffit de ne traiter que un sens. Remplacer dans *trans* $(b, c, d) \leftarrow (b|c, b|c, c)$ donne $(a \implies b|c) \implies (b/c|c \implies a|c)$. Or, *mo* nous dit que $b \implies b/c|c$, d'où (TRANS) $(b/c|c \implies a|c) \implies (b \implies a|c)$ et (TRANS) le résultat.

   Le corollaire s'obtient en remplaçant $c \leftarrow \overline{c}$.
3. *trans* nous dit $a|b/c \implies (b|d \implies a|d)$, d'où appliquant le théorème précédent (avec TRANS) $b|d \implies (a|b/c \implies a|d)$. Pour conclure, il suffit de substituer $c = b$ et $\binom{a}{d} \leftarrow \binom{\overline{a}}{d}$.
4. C'est le théorème de la déduction pour la règle "de $d \implies b$ et $a \implies (b \implies c)$ on déduit $a \implies (d \implies c)$". Or on peut montrer celle-ci à l'aide des théorèmes (*trans*)

$$\begin{aligned} (d \implies b) &\implies [(b \implies c) \implies (d \implies c)] \text{ et} \\ [a \implies (b \implies c)] &\implies [((b \implies c) \implies (d \implies c)) \implies (a \implies (d \implies c))]\,. \end{aligned}$$

   Ainsi, en appliquant la règle que l'on vient de rappeler aux deux théorèmes ci-dessus (ils sont de la forme $D \implies B$ et $A \implies (B \implies C)$), on tombe sur le théorème voulu.

   Prendre $d = \overline{c}$ et invoquer TE donne le résultat.
5. On veut $\overline{c} \implies \left(\overline{a} \vee \overline{a|b/c}\right)$, *i. e.* $\overline{c} \implies [\overline{a} \vee (a \wedge (b \implies \overline{c}))]$. On fait apparaître l'implication $i := (b \implies \overline{c})$ en invoquant la tautologie $\overline{c} \implies i$; il suffit alors de montrer $i \implies (\overline{a} \vee (a \wedge i))$, *i. e.* $i \implies (a \implies (a \wedge i))$, ou encore $i \implies \left(\overline{a \wedge i} \implies \overline{a}\right)$, *i. e.* $i \implies ((i \implies \overline{a}) \implies \overline{a})$, ce qui est *mo.* (on laisse le détail des contraposées aux soins du lecteur).

[5] On déduirait plus généralement des implications $a \implies a'$ et $b \implies b'$ l'implication $a|b \impliedby a'|b'$