Table des matières

La réalisabilité classique de Krivine associe à chaque *modèle de calcul*[i] et chaque modèle de la théorie des ensembles un nouveau modèle[ii] de la théorie des ensembles (appelé *modèle de réalisabilité*). Cette construction est similaire au forcing[iii], qui à chaque *ensemble de conditions de forcing* et chaque modèle de la théorie des ensembles associe un nouveau modèle de la théorie des ensembles (appelé *modèle de forcing*).

Chaque modèle de réalisabilité est muni d'une *algèbre de Boole caractéristique* $\mathbb{2}$, dont la structure donne des informations sur les propriétés du modèle de réalisabilité. En particulier, les modèles de forcing correspondent au cas où $\mathbb{2}$ est réduite à l'algèbre de Boole $\{0,1\}$. Pour souligner le rôle central de $\mathbb{2}$, rappelons que la réalisabilité classique permet de construire des modèles de ZF dotés de propriétés ensemblistes surprenantes (notamment le *modèle des threads* [Kri12]), et que celles-ci découlent principalement des propriétés de leur algèbre de Boole $\mathbb{2}$.

L'objectif de ce document est de présenter un nouvel outil pour étudier les modèles obtenus par réalisabilité classique (et notamment leur algèbre de Boole caractéristique) : les relations de multi-évaluation.

La théorie du forcing établit de nombreux liens entre les propriétés combinatoires de l'ensemble de conditions et les propriétés ensemblistes du modèle de forcing associé : par exemple, si l'ensemble de conditions vérifie la condition de chaîne dénombrable, alors le modèle de forcing a les mêmes cardinaux que le modèle de départ. La combinatoire finie a peu d'importance en forcing[iv], et ces liens concernent donc en général des propriétés de combinatoire infinie. En revanche, du côté de la réalisabilité classique, les travaux de Krivine [Kri12, Kri18, Kri15] donnent à penser qu'il existe une sorte de *combinatoire finie* du modèle de calcul qui a une grande influence sur le modèle de réalisabilité, et en particulier sur son algèbre de Boole caractéristique[v]. On verra que le langage des relations de multi-évaluation permet de mettre le doigt sur cette combinatoire finie et de la relier effectivement aux propriétés de l'algèbre de Boole caractéristique du modèle de réalisabilité. De plus, les relations de multi-évaluation permettent aussi d'adapter au cadre de la réalisabilité classique des propriétés de combinatoire infinie qui ont déjà leur importance en forcing (comme la condition de chaîne dénombrable).

Par ailleurs, on verra également que cette « combinatoire finie » a une interprétation calculatoire : elle est reliée à la capacité ou non des programmes à tester plusieurs chemins de calcul en parallèle pour savoir si l'un d'entre eux aboutit[vi]. Les relations de multi-évaluation permettent donc de relier les capacités de parallélisme[vii] du modèle calcul aux propriétés de l'algèbre de Boole caractéristique du modèle de réalisabilité. Par exemple, on montrera qu'il existe un programme qui calcule le *ou parallèle* [Kle52, Plo77] si et seulement si l'algèbre de Boole caractéristique du modèle de réalisabilité a au plus 4 éléments, et qu'il existe un programme qui calcule la *fonction de Gustave* [Ber76] si et seulement si elle en a au plus 8.

Conventions

Le modèle de départ $\mathcal{M}$

On fixe $\mathcal{M}$ un modèle standard de la théorie des ensembles (voir annexe B).

Pour toute notion ensembliste *foo*, on appelle $\mathcal{M}$*-foo* la même notion prise du point de vue de $\mathcal{M}$: par exemple, dans l'annexe B, on a défini les notions de $\mathcal{M}$-relation, $\mathcal{M}$-fonction, $\mathcal{M}$-relationnelle, $\mathcal{M}$-fonctionnelle, $\mathcal{M}$-partie, $\mathcal{M}$-cardinal, etc. En particulier, les éléments de $\mathcal{M}$ sont appelés des $\mathcal{M}$*-ensembles* et les parties définissables de $\mathcal{M}$ des $\mathcal{M}$*-classes*.

i. Ou du moins, à chaque modèle de calcul suffisamment expressif.
ii. On devrait plutôt dire une classe de modèles, mais pour simplifier, on se permettra pour l'instant cette imprécision.
iii. Qui peut être vu comme un cas particulier de réalisabilité.
iv. Étant donnés deux conditions de forcing, soit elles sont compatibles, soit elles sont incompatibles, et c'est à peu près tout ce qui compte.
v. Par exemple, l'algèbre de Boole caractéristique est réduite à deux éléments si et seulement si le modèle de calcul contient une instruction *fork*.
vi. Ou de façon équivalente, à demander à un oracle quel chemin emprunter pour que le calcul aboutisse.
vii. Ou de non-déterminisme, selon le point de vue.

On suppose que $\mathcal{M}$ vérifie l'axiome du choix global, c'est-à-dire qu'il existe une $\mathcal{M}$-fonctionnelle $\epsilon_{\mathcal{M}} : \mathcal{M} \setminus \{\emptyset\} \to \mathcal{M}$ telle que pour tout $X \in \mathcal{M} \setminus \{\emptyset\}$, $\epsilon_{\mathcal{M}}(X) \in X$.

Pour tout $\mathcal{M}$-ensemble X, on note $\mathcal{P}_{\mathcal{M}}(X)$ le $\mathcal{M}$-ensemble des $\mathcal{M}$-parties de X.

On fixe un $\mathcal{M}$-cardinal infini λ.

Notation $\overline{X}^n$ pour les listes

Toute liste de longueur n de la forme $X_1, \ldots, X_n$ (ou $X_0, \ldots, X_{n-1}$) pourra être abrégée en $\overline{X}^n$ (voire $\overline{X}$ s'il n'y a pas d'ambiguïté), quelle que soit la nature des objets X_i.

On utilisera cette notation avec beaucoup de souplesse, par exemple :

— un type $T_1 \to \ldots \to T_n \to U$ pourra être noté $\overline{T}^n \to U$,

— un λ-terme $t\ u_1\ \ldots\ u_n$ pourra être noté $t\ \overline{u}^n$,

— on pourra écrire « soient $\overline{x}^n \in A$ » pour « soient $x_1, \ldots, x_n \in A$ »,

— on pourra écrire « soient $\overline{x}^n \in \overline{A}^n$ » pour « soient $x_1 \in A_1, \ldots, x_n \in A_n$ ».

Conventions diverses

On identifie les entiers et les ordinaux finis, de sorte que pour tout $n \in \mathbb{N}$, $n = \{0, \ldots, n-1\}$.

Pour tout ensemble X, on note $\mathcal{P}_f(X)$ l'ensemble des parties finies de X. Si X est un $\mathcal{M}$-ensemble alors $\mathcal{P}_f(X)$ est également un $\mathcal{M}$-ensemble.

1 Structures de réalisabilité

1.1 Le λ_c-calcul

Le λ_c-calcul est un modèle de calcul qui étend le λ-calcul pur par l'ajout d'un *opérateur de contrôle* $\mathcal{C}$ *call-with-current-continuation*). Il comprend trois types d'objets syntaxiques : les λ_c*-termes*, les *piles* et les *processus*.

Définition 1.1. On fixe un $\mathcal{M}$-ensemble infini $\mathcal{M}$-dénombrable de variables (que l'on notera le plus souvent $x, y, z, \ldots$). L'ensemble des λ_c*-termes*, l'ensemble des *piles* et l'ensemble des *processus* sont les $\mathcal{M}$-ensembles définis dans $\mathcal{M}$ par les grammaires suivantes, quotientés par la $\mathcal{M}$-relation d'α-équivalence (les notions de variable libre et liée sont définies de la manière habituelle, la seule construction liante étant l'abstraction) :

λ_c-termes :

$$
\begin{array}{rcll}
t, u & ::= & x & (x \text{ variable}) \\
 & | & tu & (t, u\ \lambda_c\text{-termes} - \text{application}) \\
 & | & \lambda x.t & (x \text{ variable}, t\ \lambda_c\text{-terme} - \text{abstraction}) \\
 & | & \mathcal{C} & (\textit{call-with-current-continuation}) \\
 & | & k_\pi & (\pi \text{ pile} - \text{constantes de continuation}) \\
 & | & \xi_\nu & (\nu < \lambda - \text{instructions non protégées}) \\
 & | & \eta_\nu & (\nu < \lambda - \text{instructions protégées}),
\end{array}
$$

Piles :

$$
\begin{array}{rcll}
\pi & ::= & \omega_\nu & (\nu < \lambda - \text{fonds de pile}) \\
 & | & t \cdot \pi & (t\ \lambda_c\text{-terme } \textit{clos}, \pi \text{ pile}),
\end{array}
$$

Processus :

$$p \quad ::= \qquad t \star \pi \quad (t\ \lambda_c\text{-terme } \textit{clos}, \pi \text{ pile}).$$

Les *instructions additionnelles* (ξ_ν et η_ν) serviront d'instructions « paramétrables ». La *relation d'évaluation du λ_c-calcul*, définie plus loin dans cette section, ne leur associe aucune règle d'évaluation, et les traite donc comme des constantes inertes, mais les *relations de multi-évaluation*, définies à la section 1.3, pourront associer des règles d'évaluation à ces instruction. Ainsi, l'interprétation d'une instruction additionnelle donnée dépendra de la relation d'évaluation que l'on a en tête.

Intuitivement, les instructions protégées correspondent aux *instructions privilégiées* que l'on trouve dans les processeurs de nos ordinateurs : celles-ci sont réservées au système d'exploitation et ne peuvent pas être appelées directement par un utilisateur. Les instructions non protégées, quant à elles, correspondent aux *appels système*, qui permettent entre autres à l'utilisateur d'accéder aux instructions privilégiées de manière indirecte et contrôlée.

On appelle *termes* les λ_c-termes clos.

Le $\mathcal{M}$-ensemble des termes est noté Λ, celui des piles Π et celui des processus $\Lambda \star \Pi$.

Pour les notations, l'application associe par la gauche, de sorte que $tuvw = ((tu)v)w$, et est prioritaire devant l'abstraction, de sorte que $\lambda x.tu = \lambda x.(tu)$.

On note $t^n u$ pour t appliqué n fois à u.

Remarque. Les $\mathcal{M}$-ensembles Λ, Π et $\Lambda \star \Pi$ sont de $\mathcal{M}$-cardinal λ.

Notation (Substitutions)**.** Soient $t, u_1, \dots, u_n$ des λ_c-termes et $x_1, \dots, x_n$ des variables distinctes. On note $t[x_1 := u_1, \dots, x_n := u_n]$ le λ_c-terme obtenu à partir de t en remplaçant simultanément chaque occurrence libre de x_i par u_i pour $i = 1, \dots, n$ (de façon compatible avec l'α-équivalence, c'est-à-dire en évitant la capture de variables).

Définition 1.2. La *relation d'évaluation en une étape du λ_c-calcul*, notée $\succ_{\mathrm{K}}^1$, est la plus petite $\mathcal{M}$-*relation binaire* sur $\Lambda \star \Pi$ telle que pout tous λ_c-termes t, u, toutes piles π, π' et toute variable x :

si t et u sont clos,	$tu \star \pi$	$\succ_{\mathrm{K}}^1$	$t \star u \bullet \pi$	(push),
si $\lambda x.t$ et u sont clos,	$\lambda x.t \star u \bullet \pi$	$\succ_{\mathrm{K}}^1$	$t[x := u] \star \pi$	(grab),
si t est clos,	$cc \star t \bullet \pi$	$\succ_{\mathrm{K}}^1$	$t \star k_\pi \bullet \pi$	(save),
si t est clos,	$k_{\pi'} \star t \bullet \pi$	$\succ_{\mathrm{K}}^1$	$t \star \pi'$	(restore).

La *relation d'évaluation du λ_c-calcul*, notée $\succ_{\mathrm{K}}$, est la clôture réflexive et transitive de $\succ_{\mathrm{K}}^1$.

Les règles *push* et *grab* simulent la *β-réduction faible de tête* ; elles permettront à la réalisabilité d'être compatible avec la *logique intuitionniste*. Les règles *save* et *restore* permettent à un programme (c'est-à-dire un terme) de sauvegarder son contexte d'évaluation (la pile), puis de le restaurer ; elles permettront à la réalisabilité d'être compatible avec la *logique classique*.

Remarque. La relation d'évaluation en une étape est déterministe : pour tous p, q, q', si $p \succ_{\mathrm{K}}^1 q$ et $p \succ_{\mathrm{K}}^1 q'$, alors $q = q'$.

Remarque. On n'a pas précisé comment les objets du λ_c-calcul sont codés sous forme de $\mathcal{M}$-ensembles car cela n'a pas vraiment d'importance. On va simplement supposer que ce codage est fait entièrement « à l'intérieur de $\mathcal{M}$ » et en particulier que l'opération de substitution $(t, \overline{x}, \overline{u}) \mapsto t[\overline{x} := \overline{u}]$ est une $\mathcal{M}$-fonction.

1.2 Structures de réalisabilité

Les structures de réalisabilité sont les objets auxquels on pourra directement associer des théories de réalisabilité :

Définition 1.3. Un *pôle* est un $\mathcal{M}$-ensemble de processus *clos par anti-évaluation*, c'est-à-dire un $\mathcal{M}$-ensemble $\perp\!\!\!\perp \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tel que pour tous $p, q \in \Lambda \star \Pi$, si $p \succ_{\mathrm{K}} q$ et $q \in \perp\!\!\!\perp$, alors $p \in \perp\!\!\!\perp$.

Le $\mathcal{M}$-ensemble de tous les pôles est noté $\mathcal{S}_0$.

Définition 1.4. Une *structure de réalisabilité* est un $\mathcal{M}$-ensemble de pôles.

1.3 Relations de multi-évaluation

Dans cette section, on va établir une correspondance entre les structures de réalisabilité et une catégorie d'objets appelés *relations de multi-évaluation*, qui étendent la relation d'évaluation du λ_c-calcul.

Les relations de multi-évaluation sont des relations entre *ensembles de processus* qui vérifient certaines propriétés (alors que la relation d'évaluation du λ_c-calcul est une relation entre processus).

1.3.1 Relation associée à une structure

On va commencer par décrire une correspondance bijective entre les structures de réalisabilité et une certaine classe de relations binaires sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$. Ensuite, on cherchera à caractériser cette classe (c'est-à-dire à caractériser l'image de cette correspondance).

Définition 1.5. Soient $\succ$ une $\mathcal{M}$-relation binaire sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ et $\perp\!\!\!\perp$ un $\mathcal{M}$-ensemble de processus. On dit que $\perp\!\!\!\perp$ et $\succ$ sont *compatibles* si pour tous P et Q tels que $P \succ Q$, si $Q \subseteq \perp\!\!\!\perp$, alors $P \cap \perp\!\!\!\perp \neq \emptyset$.

Définition 1.6. Soit $\succ$ une $\mathcal{M}$-relation binaire sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$. La *structure de réalisabilité engendrée par* $\succ$, notée $\mathcal{S}_{\succ}$, est le $\mathcal{M}$-ensemble de toutes les pôles compatibles avec $\succ$.

Définition 1.7. Soit $\mathcal{S}$ une structure de réalisabilité. La *relation de multi-évaluation associée à* $\mathcal{S}$, notée « $\succ_{\mathcal{S}}$ », est la $\mathcal{M}$-relation binaire sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ définie de la façon suivante : pour tous $P, Q \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$, $P \succ_{\mathcal{S}} Q$ si et seulement si pour tout $\perp\!\!\!\perp \in \mathcal{S}$, si $Q \subseteq \perp\!\!\!\perp$, alors $P \cap \perp\!\!\!\perp \neq \emptyset$. C'est la plus grande $\mathcal{M}$-relation binaire compatible avec tous les éléments de $\mathcal{S}$.

Proposition 1.8. Cette correspondance est décroissante pour l'inclusion :

— Soient $\mathcal{S}_1$ et $\mathcal{S}_2$ deux structures de réalisabilité : si $\mathcal{S}_1 \subseteq \mathcal{S}_2$, alors $\succ_{\mathcal{S}_1} \supseteq \succ_{\mathcal{S}_2}$,

— Soient $\succ_1$ et $\succ_2$ $\mathcal{M}$-relations binaires sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$: si $\succ_1 \subseteq \succ_2$, alors $\mathcal{S}_{\succ_1} \supseteq \mathcal{S}_{\succ_2}$.

Proposition 1.9. Soit $\mathcal{S}$ une structure de réalisabilité. On a $\mathcal{S}_{\succ_{\mathcal{S}}} = \mathcal{S}$.

Démonstration. Soit $\perp\!\!\!\perp \in \mathcal{S}$. Par définition de $\succ_{\mathcal{S}}$, $\perp\!\!\!\perp \in \mathcal{S}_{\succ_{\mathcal{S}}}$. Soit $\perp\!\!\!\perp \in \mathcal{S}_0 \setminus \mathcal{S}$. Pour tout $\perp\!\!\!\perp' \in \mathcal{S}$, $\perp\!\!\!\perp' \neq \perp\!\!\!\perp$, ce qui veut dire que si $\perp\!\!\!\perp \subseteq \perp\!\!\!\perp'$, alors il existe $p \in \perp\!\!\!\perp'$ tel que $p \notin \perp\!\!\!\perp$. En d'autres termes, $(\Lambda \star \Pi \setminus \perp\!\!\!\perp) \succ_{\mathcal{S}} \perp\!\!\!\perp$, et donc $\perp\!\!\!\perp \notin \mathcal{S}_{\succ_{\mathcal{S}}}$. □

La correspondance ainsi définie est donc bien injective : on va caractériser son image. Pour commencer, on va en donner une première approximation :

1.3.2 Relations de multi-évaluation

Définition 1.10. Une *relation de multi-évaluation* est une $\mathcal{M}$-relation binaire $\succ$ sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ telle que :

— Pour tous $p, q \in \Lambda \star \Pi$ tels que $p \succ^1_{\mathrm{K}} q$, $\{p\} \succ \{q\}$,

— Pour tous $p \in \Lambda \star \Pi$, $\{p\} \succ \{p\}$ *(identité)*,

— Pour tous $P, Q, P', Q' \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$, pour tout $r \in \Lambda \star \Pi$, si $P \succ Q \cup \{r\}$ et $P' \cup \{r\} \succ Q'$, alors $P \cup P' \succ Q \cup Q'$ *(coupure)*,

— Pour tous $P, Q, P', Q' \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \succ Q$, si $P \subseteq P'$ et $Q \subseteq Q'$, alors $P' \succ Q'$ *(affaiblissement)*.

Proposition 1.11. Soit $\mathcal{S}$ une structure de réalisabilité. La relation $\succ_{\mathcal{S}}$ est une relation de multi-évaluation.

Démonstration. Soient $p, q \in \Lambda \star \Pi$ tels que $p \succ^1_{\mathrm{K}} q$. Pour tout $\perp\!\!\!\perp \in \mathcal{S}$ tel que $q \in \perp\!\!\!\perp$, on a bien $p \in \perp\!\!\!\perp$, puisque $\perp\!\!\!\perp$ est un pôle.

Soit $p \in \Lambda \star \Pi$. Pour tout $\perp\!\!\!\perp \in \mathcal{S}$ tel que $\{p\} \subseteq \perp\!\!\!\perp$, on a bien $\{p\} \cap \perp\!\!\!\perp \neq \emptyset$.

Soient $P, Q, P', Q' \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ et $r \in \Lambda \star \Pi$ tels que $P \succ_{\mathcal{S}} Q \cup \{r\}$ et $P' \cup \{r\} \succ_{\mathcal{S}} Q'$. Pour tout $\perp\!\!\!\perp \in \mathcal{S}$ tel que $Q \cup Q' \subseteq \perp\!\!\!\perp$, on a $(P' \cup \{r\}) \cap \perp\!\!\!\perp \neq \emptyset$, donc soit $P' \cap \perp\!\!\!\perp \neq \emptyset$, soit $r \in \perp\!\!\!\perp$. Dans le premier cas, $(P \cup P') \cap \perp\!\!\!\perp \supseteq P' \cap \perp\!\!\!\perp \neq \emptyset$, et dans le deuxième, $Q \cup \{r\} \subseteq \perp\!\!\!\perp$, donc $P \cap \perp\!\!\!\perp \neq \emptyset$, et donc $(P \cup P') \cap \perp\!\!\!\perp \neq \emptyset$.

Soient $P, Q, P', Q' \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \subseteq P'$, $Q \subseteq Q'$ et $P \succ_{\mathcal{S}} Q$. Pour tout $\perp\!\!\!\perp \in \mathcal{S}$ tel que $P' \subseteq \perp\!\!\!\perp$, on a $P \subseteq P' \subseteq \perp\!\!\!\perp$, donc $Q \cap \perp\!\!\!\perp \neq \emptyset$, et donc $Q' \cap \perp\!\!\!\perp \supseteq Q \cap \perp\!\!\!\perp \neq \emptyset$. □

Lemme 1.12. Soit $\succ$ une $\mathcal{M}$-relation binaire sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$. Il existe une plus petite relation de multi-évaluation contenant $\succ$. De plus, si l'on note $\succ^*$ cette relation de multi-évaluation, on a $\mathcal{S}_{\succ^*} = \mathcal{S}_{\succ}$.

Démonstration. L'ensemble des relations de multi-évaluation contenant $\succ$ est stable par intersections arbitraires, donc il possède un plus petit élément pour l'inclusion.

Comme $\succ \subseteq \succ^*$, $\mathcal{S}_{\succ} \supseteq \mathcal{S}_{\succ^*}$. De plus, $\succ_{\mathcal{S}_{\succ}}$ est une relation de multi-évaluation qui contient $\succ$, donc elle contient $\succ^*$. Par conséquent, $\mathcal{S}_{\succ^*} \subseteq \mathcal{S}_{\succ_{\mathcal{S}_{\succ}}} = \mathcal{S}_{\succ}$, par la proposition 1.9. □

Si $\succ$ est une relation de multi-évaluation, on a en général $\succ \subseteq \succ_{\mathcal{S}_{\succ}}$, mais pas l'inclusion inverse. Autrement-dit, il n'est pas vrai que toute relation de multi-évaluation peut s'écrire comme $\succ_{\mathcal{S}}$ pour une certaine structure de réalisabilité $\mathcal{S}$.

La classe des relations d'évaluation ne constitue donc qu'une approximation (par excès) de l'image que l'on cherche à caractériser. Elle joue cependant un rôle essentiel, car cette classe a l'avantage d'être définie par dès règles de clôture *finitaires* : pour aller plus loin, il faudra ajouter une règle de *coupure infinitaire*.

1.3.3 Relations de multi-évaluation complètes

Définition 1.13. Une relation de multi-évaluation $\succ$ est *complète* lorsqu'elle vérifie la règle de *coupure infinitaire*, c'est-à-dire lorsque pour tous $P, Q, R \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$, si pour tous $R_0, R_1 \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ vérifiant $R_0 \cup R_1 = R$ on a $P \cup R_0 \succ R_1 \cup Q$, alors $P \succ Q$.

Remarque. En prenant $R = \{r\}$, modulo identité et affaiblissement, on retrouve exactement la règle de coupure. De plus, si l'on restreint la propriété ci-dessus aux cas où R est fini, on peut montrer qu'elle est vérifiée par toute relation de multi-évaluation : c'est donc la possibilité d'avoir R infini qui fait la différence.

Proposition 1.14. Soit $\mathcal{S}$ une structure de réalisabilité. La relation de multi-évaluation associée à $\mathcal{S}$ est complète.

Démonstration. Soient $P, Q, R \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que pour tous $R_0, R_1 \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ vérifiant $R_0 \cup R_1 = R$, on ait $P \cup R_0 \succ_{\mathcal{S}} R_1 \cup Q$. Soit $\perp\!\!\!\perp \in \mathcal{S}$ tel que $Q \subseteq \perp\!\!\!\perp$, et montrons que $P \cap \perp\!\!\!\perp \neq \emptyset$.

Notons $R_0 = R \cap (\Lambda \star \Pi \setminus \perp\!\!\!\perp)$ et $R_1 = R \cap \perp\!\!\!\perp$. On a $R_0 \cup R_1 = R$ et $R_1 \cup Q \subseteq \perp\!\!\!\perp$, donc $(R_0 \cup P) \cap \perp\!\!\!\perp \neq \emptyset$, et donc $P \cap \perp\!\!\!\perp \neq \emptyset$. □

Proposition 1.15. Soit $\succ$ une relation de multi-évaluation complète. On a $\succ_{\mathcal{S}_{\succ}} = \succ$.

Démonstration. Soient $P, Q \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \succ Q$. Pour tout $\perp\!\!\!\perp \in \mathcal{S}_{\succ}$ tel que $Q \subseteq \perp\!\!\!\perp$, on a $P \cap \perp\!\!\!\perp \neq \emptyset$ par définition de $\mathcal{S}_{\succ}$, autrement-dit, $P \succ_{\mathcal{S}_{\succ}} Q$. On a donc bien $\succ \subseteq \succ_{\mathcal{S}_{\succ}}$.

Soient $P, Q \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \not\succ Q$. Posons $R = \Lambda \star \Pi$. Il existe alors $R_0, R_1 \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \cup R_0 \not\succ Q \cup R_1$. Par affaiblissement et identité, on doit avoir en particulier $(P \cup R_0) \cap (Q \cup R_1) = \emptyset$, donc $P \subseteq R_0$ et $Q \subseteq R_1$, et en particulier $R_0 \not\succ R_1$.

On a $R_1 \in \mathcal{S}_{\succ}$. En effet, pour tous $S, T \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $S \succ T$ et $T \subseteq R_1$, on doit avoir $S \not\subseteq R_0$ (sinon on aurait $R_0 \succ R_1$ par affaiblissement), et donc $S \cap R_1 \neq \emptyset$.

Ainsi, comme $Q \subseteq R_1$ et $P \cap R_1 = \emptyset$, on a $P \not\succ_{\mathcal{S}_{\succ}} Q$. □

Lemme 1.16. Soit $\succ$ une $\mathcal{M}$-relation binaire sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$. Il existe une plus petite relation de multi-évaluation complète contenant $\succ$. De plus, si l'on note $\succ^{**}$ cette relation de multi-évaluation, on a $\mathcal{S}_{\succ^{**}} = \mathcal{S}_{\succ}$.

On a donc trouvé l'image de la correspondance : il s'agit des relations de multi-évaluation complètes. On peut en donner une autre approximation, par défaut cette fois, qui s'avèrera utile par la suite :

Définition 1.17. Une relation de multi-évaluation $\succ$ est *compacte* si pour tous $P, Q \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \succ Q$, il existe $P_0 \subseteq P$ et $Q_0 \subseteq Q$ finis tels que $P_0 \succ Q_0$.

Lemme 1.18. Une relation de multi-évaluation $\succ$ est compacte si et seulement s'il existe une $\mathcal{M}$-relation binaire $\succ^1$ sur $\mathcal{P}_f(\Lambda \star \Pi)$ telle que $\succ$ soit la plus petite relation de multi-évaluation contenant $\succ^1$.

Démonstration. Supposons que $\succ$ est compacte. Soit $\succ^1 = \{ (P_0, Q_0) \in \mathcal{P}_f(\Lambda \star \Pi) \times \mathcal{P}_f(\Lambda \star \Pi);\ P_0 \succ Q_0 \}$. Soit $\succ^{1^*}$ la plus petite relation d'évaluation contenant $\succ^1$. Par définition, $\succ^1 \subseteq \succ$, donc $\succ^{1^*} \subseteq \succ$. Par ailleurs, pour tous $P, Q \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \succ Q$, il existe $P_0, Q_0 \in \mathcal{P}_f(\Lambda \star \Pi)$ tels que $P_0 \subseteq Q$, $Q_0 \subseteq Q$ et $P_0 \succ Q_0$; on a alors $P_0 \succ^1 Q_0$, donc $P_0 \succ^{1^*} Q_0$, et donc $P \succ^{1^*} Q$.

Supposons maintenant qu'il existe $\succ^1$ une relation binaire sur $\mathcal{P}_f(\Lambda \star \Pi)$ telle que $\succ$ soit la plus petite relation de multi-évaluation contenant $\succ^1$. Soit $\widetilde{\succ} = \{ (P, Q) \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi);$ in existe $P_0, Q_0 \in \mathcal{P}_f(\Lambda \star \Pi)$ tels que $P_0 \subseteq P$, $Q_0 \subseteq Q$ et $P_0 \succ Q_0 \}$. On a $\widetilde{\succ} \subseteq \succ$ par affaiblissement. De plus, $\succ^1 \subseteq (\succ \cap \mathcal{P}_f(\Lambda \star \Pi) \times \mathcal{P}_f(\Lambda \star \Pi)) \subseteq \widetilde{\succ}$ et l'on peut vérifier que $\widetilde{\succ}$ est une relation de multi-évaluation, donc $\succ \subseteq \widetilde{\succ}$. Enfin, $\widetilde{\succ}$ est compacte, donc $\succ$ est compacte. □

Proposition 1.19. Toute relation de multi-évaluation compacte est complète.

Démonstration. Soit $\succ$ un relation de multi-évaluation compacte. Soient $P, Q, R \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $P \not\succ Q$ et montrons qu'il existe $S, T \in \mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ tels que $S \cup T = R$ et $P \cup S \not\succ T \cup Q$.

Soient κ le $\mathcal{M}$-cardinal de R et $(r_\alpha)_{\alpha<\kappa}$ une $\mathcal{M}$-énumération de R. On va construire par induction deux $\mathcal{M}$-séquences croissantes $(S_\alpha)_{\alpha<\kappa}$ et $(T_\alpha)_{\alpha<\kappa}$ d'éléments de $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ telles que :

— Pour tout α, $P \cup S_\alpha \not\succ Q \cup T_\alpha$;

— Pour tout α, $S_\alpha \cup T_\alpha = \{ r_\beta;\ \beta \leq \alpha \}$.

On construit S_α et T_α à partir de $(S_\beta)_{\beta<\alpha}$ et $(T_\beta)_{\beta<\alpha}$ de la façon suivante :

Tout d'abord, remarquons que l'on a $P \cup \left(\bigcup_{\beta<\alpha} S_\beta\right) \not\succ Q \cup \left(\bigcup_{\beta<\alpha} T_\beta\right)$. En effet, sinon, comme $\succ$ est compacte, il existerait $S'_\alpha \subseteq \left(\bigcup_{\beta<\alpha} S_\beta\right)$ et $T'_\alpha \subseteq \left(\bigcup_{\beta<\alpha} T_\beta\right)$ finies telles que $P \cup S'_\alpha \succ Q \cup T'_\alpha$. En posant $\beta = \max\{ \beta < \alpha;\ r_\beta \in S'_\alpha \cup T'_\alpha \} < \alpha$, on aurait alors $P \cup S_\beta \succ Q \cup T_\beta$, alors que l'on a supposé le contraire.

Par conséquent, d'après la règle de coupure, on a $P \cup \left(\bigcup_{\beta<\alpha} S_\beta\right) \cup \{r_\alpha\} \not\succ Q \cup \left(\bigcup_{\beta<\alpha} T_\beta\right)$ ou $P \cup \left(\bigcup_{\beta<\alpha} S_\beta\right) \not\succ Q \cup \left(\bigcup_{\beta<\alpha} T_\beta\right) \cup \{r_\alpha\}$. Dans le premier cas, on pose $S_\alpha = \left(\bigcup_{\beta<\alpha} S_\beta\right) \cup \{r_\alpha\}$ et $T_\alpha = \left(\bigcup_{\beta<\alpha} T_\beta\right)$ et dans le second, on pose $S_\alpha = \left(\bigcup_{\beta<\alpha} S_\beta\right)$ et $T_\alpha = \left(\bigcup_{\beta<\alpha} T_\beta\right) \cup \{r_\alpha\}$.

On pose maintenant $S = \bigcup_{\alpha<\kappa} S_\alpha$ et $T = \bigcup_{\alpha<\kappa} T_\alpha$: là encore, comme $\succ$ est compacte, on a $P \cup S \not\succ Q \cup T$, et par ailleurs, $S \cup T = \{ r_\alpha;\ \alpha < \kappa \} = R$. □

2 Extension de la théorie des ensembles par réalisabilité classique

La réalisabilité établit une relation entre programmes et formules. Le but de cette section est d'arriver à définir les deux notions suivantes et d'en étudier quelques propriétés :

— la relation « t réalise A modulo $\mathcal{S}$ » ($t \Vdash_{\mathcal{S}} A$) pour t un terme, A une formule, et $\mathcal{S}$ une structure de réalisabilité,

— la notion de « théorie engendrée par $\mathcal{S}$ » ($\mathrm{Th}(\mathcal{S})$), constituée de l'ensemble des formules « réalisées » modulo $\mathcal{S}$, pour $\mathcal{S}$ une structure de réalisabilité.

Les notions de terme et de structure de réalisabilité ont déjà été définies, mais il reste à préciser celle de formule.

Puisque l'on cherche à faire de la théorie des ensembles, on va vouloir faire en sorte que la théorie engendrée par une structure de réalisabilité soit toujours, dans un certain sens, une extension de la théorie des ensemble de Zermelo-Frænkel. En particulier, le *langage de réalisabilité* (c'est-à-dire le langage dans lequel on exprimera les formules) doit être une extension du langage habituel de la théorie des ensembles, c'est-à-dire qu'il doit contenir un symbole d'appartenance $\in$ et un symbole d'égalité $\approx$. De plus, la théorie devra contenir un *axiome d'extensionnalité* qui lie ces deux symboles. On appellera le premier *appartenance extensionnelle* et le second *égalité extensionnelle*. Les raisons de l'ajout de l'adjectif *extensionnel* et de l'utilisation du symbole $\approx$ (plutôt que $=$) seront expliquées plus loin dans cette section.

Que ce soit à cause d'un manque de maturité de la théorie ou de difficultés propres, l'étude des « modèles de réalisabilité de ZF », c'est-à-dire des extensions de la théorie des ensembles de Zermelo-Frænkel obtenues par réalisabilité classique, oblige à l'heure actuelle à accorder beaucoup d'attention à des détails techniques, en particulier de codage. L'idée de se pencher sur la distinction entre les formules $\top$ et $\bot \to \bot$ pourra faire sourire ou grimacer les théoricien(ne)s des ensembles (qui ont pris l'habitude de soigneusement éviter précisément ce genre de considérations), pourtant, non seulement cette distinction existe, au-delà de la syntaxe (la réalisabilité classique donne à ces deux formules deux *valeurs de vérité* bien différentes), mais elle est même essentielle : la première formule ne donne aucune information sur les termes qui la réalisent, la seconde un tout petit peu. Ce n'est pas grand chose, mais cette distinction sera au cœur des considérations des chapitres suivants sur l'*algèbre de Boole caractéristique* [12] (section 3). Par comparaison avec le forcing, on a donc un peu l'impression de rouler avec le capot ouvert. Ce phénomène se manifeste d'au moins trois manières dès la définition du langage de réalisabilité (ci-dessous) :

— Dans la distinction entre *extensionnel* et *non extensionnel*. Là où la théorie des ensembles usuelle (que l'on appellera *théorie des ensembles extensionnelle*) repose sur deux symboles de base (appartenance et égalité), la *théorie des ensembles non extensionnelle*, raffinement de la théorie usuelle qui servira de base au langage de réalisabilité, en nécessite quatre : *appartenance et égalité non extensionnelles* (ε et $=$), et *appartenance et égalité extensionnelles* ($\in$ et $\approx$). À ces quatre symboles, on peut également ajouter l'*inclusion non extensionnelle* ($\subseteq$) et l'*inclusion extensionnelle* ($\subseteqq$). Plus loin dans ce chapitre, on définira les théories extensionnelle et non extensionnelle des ensembles, et l'on verra comment elles sont reliées. La réalisabilité donne naturellement une interprétations des symboles non extensionnels, mais comme leur nom l'indique, l'« axiome d'extensionnalité » exprimé en termes de ces symboles (c'est-à-dire la formule $\forall a \forall b\ (\forall x\ (x\ \varepsilon\ a \leftrightarrow x\ \varepsilon\ b) \to a = b)$) n'est en général pas réalisé. Au contraire, l'interprétation des symboles extensionnels est plus compliquée, mais elle permet de réaliser l'axiome d'extensionnalité ($\forall a \forall b\ (\forall x\ (x \in a \leftrightarrow x \in b) \to a \approx b)$). D'ailleurs, le même problème se pose en forcing, et dans ce cas la solution généralement choisie est de ne définir que les symboles extensionnels (qui sont alors notés $\in$ et $=$). C'est la raison pour laquelle les relations « p force $a \in b$ » et « p force $a = b$ » doivent être définies par induction mutuelle, et c'est exactement cette induction mutuelle que l'on retrouvera dans la définition des relations « t réalise $a \in b$ » et « t réalise $a \approx b$ ». Dans le cas du forcing, cela marche si bien que l'on en oublie facilement que le problème s'est jamais posé. Malheureusement, avec la réalisabilité, on ne peut pas se permettre de « refermer le capot » en oubliant les symboles non extensionnels, car beaucoup de considérations techniques importantes se formulent précisément en termes de ces symboles.

— Dans le choix des symboles de relation et des connecteurs logiques primitifs, qui peut surprendre (en particulier celui des symboles de relation). L'idée est simplement de sélectionner comme construc-

tions primitives celles dont l'interprétation par réalisabilité sera facile à décrire. Pour les connecteurs logiques, on choisit $\top$, $\bot$, $\to$ et $\forall$ et l'on définit les autres par des codages du premier ordre à la De Morgan (ce que l'on peut se permettre de faire, puisqu'il s'agit de réalisabilité classique). Pour les symboles de relation, on choisit $\neq$, $\not\in$, $\subsetneq$ et $\notin$ comme symboles primitifs et l'on définit $a = b$, $a \mathrel{\varepsilon} b$, $a \approx b$ et $a \in b$ comme $\neg(a \neq b)$, $\neg(a \not\in b)$, $(a \subsetneq b) \wedge (b \subsetneq a)$ et $\neg(a \notin b)$ respectivement.

— Dans l'ajout des constructions non logiques $\cap$ et $\cup$. Ces constructions servent à effectuer des opérations de bas niveau sur l'interprétation des formules : par exemple, par construction, un terme t réalisera $A \cap B$ si et seulement s'il réalise à la fois A et B (le connecteur $\cup$ est un peu plus compliqué). Elles ne peuvent pas s'interpréter comme des connecteurs logiques : en particulier ce n'est pas parce qu'à la fois $A \cap B$ et $A \leftrightarrow A'$ sont réalisées que $A' \cap B$ l'est forcément.

2.1 Langage de réalisabilité

Définition 2.1 (Langage de réalisabilité)**.** On fixe un $\mathcal{M}$-ensemble infini $\mathcal{M}$-dénombrable de variables du premier ordre (que l'on notera le plus souvent $x, y, z, \ldots$). L'ensemble des *termes du premier ordre* et l'ensemble des *formules* (qui ne sont pas des $\mathcal{M}$-ensembles, ni même des $\mathcal{M}$-classes) sont définis par les grammaires suivantes, modulo α-équivalence :

Termes du premier ordre :

$$\begin{array}{rcll} a, b & ::= & x & (x \text{ variable du premier ordre}) \\ & | & f(a_1, \ldots, a_n) & (n \in \mathbb{N},\ f : \mathcal{S}_0 \times \mathcal{M}^n \to \mathcal{M}\ \mathcal{M}\text{-fonctionnelle}, \\ & & & a_1, \ldots a_n \text{ termes du premier ordre}), \end{array}$$

Formules :

$$\begin{array}{rcll} A, B & ::= & \left\{\begin{array}{ll} a \neq b \mid a \not\in b & (a \text{ et } b \text{ termes du premier ordre – relations non extensionnelles}) \\ \mid a \subsetneq b \mid a \notin b & (a \text{ et } b \text{ termes du premier ordre – relations extensionnelles}) \\ \mid \top \mid \bot & \\ \mid A \to B & (A \text{ et } B \text{ formules}) \\ \mid \forall x\ A & (x \text{ variable du premier ordre, } A \text{ formule}) \end{array}\right. \\ \left(\begin{array}{c}\textit{Constructions de la}\\ \textit{théorie des ensembles}\\ \textit{non extensionnelle}\end{array}\right) & & & \\ \left(\begin{array}{c}\textit{Constructions propres}\\ \textit{à la réalisabilité}\end{array}\right) & & \left\{\begin{array}{ll} \mid A \cap B & (A \text{ et } B \text{ formules}) \\ \mid A \cup B & (A \text{ et } B \text{ formules}). \end{array}\right. \end{array}$$

Notation. On définit les connecteurs logiques et les symboles de relation manquants de la manière suivante :

— on note $A \wedge B$ pour $(A \to B \to \bot) \to \bot$,

— on note $A \vee B$ pour $(A \to \bot) \to (B \to \bot) \to \bot$,

— on note $\neg A$ pour $A \to \bot$,

— on note $A \leftrightarrow B$ pour $(A \to B) \wedge (B \to A)$,

— on note $\exists x\ A$ pour $\neg(\forall x\ \neg A)$,

— on note $a = b$ pour $\neg(a \neq b)$,

— on note $a \mathrel{\varepsilon} b$ pour $\neg(a \not\in b)$,

— on note $a \subseteq b$ pour $\forall x\ (x \mathrel{\varepsilon} a \to x \mathrel{\varepsilon} b)$,

— on note $a \approx b$ pour $(a \subsetneq b) \wedge (b \subsetneq a)$,

— on note $a \in b$ pour $\neg(a \notin b)$.

Notation. Si A est une formule, b un terme du premier ordre, x une variable du premier ordre et $\lessdot$ un symbole de relation binaire ($\notin$, $\in$, $\subsetneq$, ε, etc.), on notera $\forall x \lessdot b\ A$ pour $\forall x\ (x \lessdot b \to A)$ et $\exists x \lessdot b\ A$ pour $\neg(\forall x \lessdot b\ \neg A)$.

Remarque. Si $f : \mathcal{M}^n \to \mathcal{M}$ est une $\mathcal{M}$-fonctionnelle, on s'autorisera à écrire $f(a_1, \ldots, a_n)$ dans les termes du premier ordre, en identifiant f à la $\mathcal{M}$-fonctionnelle de $\mathcal{S}_0 \times \mathcal{M}^n$ dans $\mathcal{M}$ qui à $(\perp\!\!\!\perp, x_1, \ldots, x_n)$ associe $f(x_1, \ldots, x_n)$.

Notation (Substitutions)**.** Soient A une formule, $b_1, \ldots, b_n$ des termes du premier ordre et $x_1, \ldots, x_n$ des variables du premier ordre distinctes. On note $A[x_1 := b_1, \ldots, x_n := b_n]$ la formule obtenue à partir de A en remplaçant simultanément chaque occurrence libre de x_i par b_i pour $i = 1, \ldots, n$ (de façon compatible avec l'α-équivalence, c'est-à-dire en évitant la capture de variables).

Notation (Termes et formules à paramètres)**.** Si α est un terme du premier ordre ou une formule et si $x_1, \ldots, x_n$ est une liste de variables du premier ordre distinctes contenant au moins toutes les variables libres de α, on pourra noter $\alpha(x_1, \ldots, x_n)$ pour α (l'intérêt de cette notation étant d'ordonner les variables libres de α). Dans ce cas, si $a_1, \ldots, a_n$ est une liste de termes du premier ordre, on notera $\alpha(a_1, \ldots, a_n)$ pour $\alpha[x_1 := a_1, \ldots, x_n := a_n]$.

2.2 Preuves et théories

Un *jugement de prouvabilité* est un séquent de la forme $\Gamma \vdash A$, avec Γ un ensemble fini de formules et A une formule. Si Γ est une ensemble fini de formules et A une formule, on pourra noter « Γ, A » pour « $\Gamma \cup \{A\}$ ».

Un *arbre de preuve* est un arbre formé à partir des règles suivantes. Sa racine (en bas) est appelée sa *conclusion* :

$$\text{(Axiome)}\ \frac{}{\Gamma, A \vdash A}$$

$$\text{(Peirce)}\ \frac{}{\Gamma \vdash ((A \to B) \to A) \to A}$$

$$(\top\text{-intro})\ \frac{}{\Gamma \vdash \top} \qquad (\perp\text{-élim})\ \frac{\Gamma \vdash \perp}{\Gamma \vdash A}$$

$$(\to\text{-intro})\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \qquad (\to\text{-élim})\ \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$(\forall\text{-intro})\ \frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\ \text{(si } x \text{ n'apparaît pas librement dans } \Gamma) \qquad (\forall\text{-élim})\ \frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A[x := a]}$$

Un jugement de prouvabilité est dit *dérivable* s'il est la conclusion d'au moins un arbre de preuve.

Une *théorie* est un ensemble de formules closes. Si $\mathcal{T}$ est une théorie et A une formule, on dit que $\mathcal{T}$ *prouve* A, que A *est conséquence de* $\mathcal{T}$ ou encore que A *est prouvable dans* $\mathcal{T}$ s'il existe un ensemble fini $\Gamma \subseteq \mathcal{T}$ tel que le jugement $\Gamma \vdash A$ soit dérivable.

Une formule est une *tautologie* si elle est conséquence de la théorie vide. Deux formules A et B sont *logiquement équivalentes* si la formule $A \leftrightarrow B$ est une tautologie.

Deux formules A et B sont *équivalentes modulo* une théorie $\mathcal{T}$ si la formule $A \leftrightarrow B$ est conséquence de $\mathcal{T}$.

Si $\mathcal{T}_1$ et $\mathcal{T}_2$ sont des théories, on dit que $\mathcal{T}_1$ *prouve* $\mathcal{T}_2$, ou que $\mathcal{T}_2$ *est conséquence de* $\mathcal{T}_1$ si $\mathcal{T}_1$ prouve A pour toute $A \in \mathcal{T}_2$.

On dit qu'une théorie $\mathcal{T}$ est *close par déduction* si $A \in \mathcal{T}$ pour toute A close telle que $\mathcal{T}$ prouve A.

On dit qu'une théorie $\mathcal{T}$ est *cohérente* lorsqu'elle ne prouve pas $\perp$.

2.3 Modèles

Définition 2.2. Un *modèle* est la donnée

— d'un ensemble non vide $\mathcal{N}$ (appelé *ensemble de base*),

— d'une d'une fonction (appelée *fonction d'évaluation*) qui à tout terme du premier ordre a, toute liste $x_1, \dots, x_n$ de variables du premier ordre distinctes contenant au moins toutes les variables libres de a et toute liste $b_1, \dots, b_n$ d'éléments de $\mathcal{N}$ associe un élément de $\mathcal{N}$, noté $a[x_1 := b_1, \dots, x_n := b_n]_{\mathcal{N}}$ (ou $a_{\mathcal{N}}$ si $n = 0$),

— d'une fonction (appelée *fonction de vérité*) qui à toute formule A, toute liste $x_1, \dots, x_n$ de variables du premier ordre distinctes contenant au moins toutes les variables libres de A et toute liste $b_1, \dots, b_n$ d'éléments de $\mathcal{N}$ associe un élément de $\{0, 1\}$, noté $|A|[x_1 := b_1, \dots, x_n := b_n]_{\mathcal{N}}$ (ou $|A|_{\mathcal{N}}$ si $n = 0$)

tels que :

— pour toute liste $x_1, \dots, x_n$ de variables du premier ordre distinctes, pour tous $c_1, \dots, c_n \in \mathcal{N}$ et tout $i \in \{1, \dots, n\}$, $x_i[x_1 := c_1, \dots, x_n := c_n] = c_i$,

— pour tout terme $a(y_i, \dots, y_m)$, pour tous termes $b_1(z_1, \dots, z_n), \dots, b_m(z_1, \dots, z_n)$, pour tous $c_1, \dots, c_n \in \mathcal{N}$,

$$\begin{aligned}&(a[y_1 := b_1, \dots, y_m := b_m])[z_1 := c_1, \dots, z_n := c_n]_{\mathcal{N}}\\ = a[y_1 &:= b_1[z_1 := c_1, \dots, z_n := c_n]_{\mathcal{N}}, \dots, y_m := b_m[z_1 := c_1, \dots, z_n := c_n]_{\mathcal{N}}]_{\mathcal{N}},\end{aligned}$$

— pour toute formule $A(y_i, \dots, y_m)$, pour tous termes $b_1(z_1, \dots, z_n), \dots, b_m(z_1, \dots, z_n)$, pour tous $c_1, \dots, c_n \in \mathcal{N}$,

$$\begin{aligned}&|A[y_1 := b_1, \dots, y_m := b_m]|\,[z_1 := c_1, \dots, z_n := c_n]_{\mathcal{N}}\\ = |A|\,[y_1 &:= b_1[z_1 := c_1, \dots, z_n := c_n]_{\mathcal{N}}, \dots, y_m := b_m[z_1 := c_1, \dots, z_n := c_n]_{\mathcal{N}}]_{\mathcal{N}},\end{aligned}$$

— $|\top|_{\mathcal{N}} = 1$,

— $|\bot|_{\mathcal{N}} = 0$,

— pour toutes formules $A(x_1, \dots, x_n)$ et $B(x_1, \dots, x_n)$, pour tous $c_1, \dots, c_n \in \mathcal{N}$,

$$|A \to B|[x_1 := c_1, \dots, x_n := c_n]_{\mathcal{N}} = \begin{cases} 0 & \text{si } |A|[x_1 := c_1, \dots, x_n := c_n]_{\mathcal{N}} = 1 \\ & \text{et } |B|[x_1 := c_1, \dots, x_n := c_n]_{\mathcal{N}} = 0 \\ 1 & \text{sinon} \end{cases},$$

— pour toute formule $A(x_1, \dots, x_n, y)$, pour tous $c_1, \dots, c_n \in \mathcal{N}$,

$$|\forall y\ A|[x_1 := c_1, \dots, x_n := c_n]_{\mathcal{N}} = \min\{\ |A|[x_1 := c_1, \dots, x_n := c_n, y := b]_{\mathcal{N}};\ b \in \mathcal{N}\ \}.$$

Pour simplifier les notations, on identifiera systématiquement un modèle avec son ensemble de base. Les éléments de l'ensemble de base sont également appelés les *objets* du modèle.

Remarquons que l'on n'a imposé aucune condition sur la vérité des formules de la forme $A \cap B$ ou $A \cup B$, pas même que $|A \cap B|_{\mathcal{N}} \leq |A|_{\mathcal{N}}$. En revanche, on verra par exemple que tout *modèle de réalisabilité* $\mathcal{N}$ vérifie bien $|A \cap B \to A|_{\mathcal{N}} = 1$ et donc $|A \cap B|_{\mathcal{N}} \leq |A|_{\mathcal{N}}$.

Si $\mathcal{N}$ est un modèle, $A(x_1, \dots, x_n)$ une formule et $b_1, \dots, b_n$ des éléments de $\mathcal{N}$, on dit que $\mathcal{N}$ *vérifie* $A[x_1 := b_1, \dots, x_n := b_n]$ et l'on note $\mathcal{N} \models A[x_1 := b_1, \dots, x_n := b_n]$ (ou respectivement que $\mathcal{N}$ vérifie A et $\mathcal{N} \models A$ si $n = 0$) lorsque $|A|[x_1 := b_1, \dots, x_n := b_n]_{\mathcal{N}} = 1$.

De plus, si $\mathcal{N}$ est un modèle et $\mathcal{T}$ une théorie, on dit que $\mathcal{N}$ *vérifie* $\mathcal{T}$ ou encore que $\mathcal{N}$ *est un modèle de* $\mathcal{T}$ et l'on note $\mathcal{N} \models \mathcal{T}$ lorsque $\mathcal{N}$ vérifie A pour toute $A \in \mathcal{T}$.

Enfin, si $\mathcal{N}$ est un modèle, on s'autorisera par abus de notation à utiliser les objets de $\mathcal{N}$ comme des constantes dans les termes et les formules destinés à être évalués dans $\mathcal{N}$. Par exemple, si a et b sont des objets de $\mathcal{N}$, on dira « $\mathcal{N}$ vérifie $\forall x\ (x \in a \to x \in b)$ » pour « $\mathcal{N}$ vérifie $(\forall x\ (x \in y \to x \in z))[y := a, z := b]$ », et si f est une $\mathcal{M}$-fonctionnelle de $\mathcal{S}_0 \times \mathcal{M}^2$ dans $\mathcal{M}$, on notera $f(a, b)$ pour $(f(y, z))[y := a, z := b]_{\mathcal{N}}$.

Lemme 2.3. Soient $\mathcal{N}$ un modèle, a un terme du premier ordre, A une formule, $\overline{y}^m$ et $\overline{z}^n$ deux listes chacune composée de variables distinctes et chacune contenant toutes les variables libres de a et de A, et $\overline{b}^m$ et $\overline{c}^n$ deux listes d'éléments de $\mathcal{N}$ telles que pour tous i et j vérifiant $y_i = z_j$, on ait $b_i = c_j$. Alors $a[\overline{y}^m := \overline{b}^m]_\mathcal{N} = a[\overline{z}^n := \overline{c}^n]_\mathcal{N}$ et $|A|[\overline{y}^m := \overline{b}^m]_\mathcal{N} = |A|[\overline{z}^n := \overline{c}^n]_\mathcal{N}$.

Démonstration. On va montrer que $a[\overline{y}^m := \overline{b}^m]_\mathcal{N} = a[\overline{z}^n := \overline{c}^n]_\mathcal{N}$ (l'autre preuve est similaire). Sans perte de généralité, on peut supposer que la liste $\overline{y}^m$ est contenue dans la liste $\overline{z}^n$ (sinon, il suffit d'appliquer le résultat deux fois : à l'intersection de $\overline{y}^m$ avec $\overline{z}^n$ et à $\overline{y}^m$, puis à l'intersection de $\overline{y}^m$ avec $\overline{z}^n$ et à $\overline{z}^n$).

Pour tout $i \in \{1, \dots m\}$, $y_i[\overline{z}^n := \overline{c}^n]_\mathcal{N} = b_i$. Par conséquent, $a[\overline{y}^m := \overline{b}^m]_\mathcal{N} = a[\overline{y}^m := \overline{y}^m[\overline{z}^n := \overline{c}^n]_\mathcal{N}]_\mathcal{N}$ $= (a[\overline{y}^m := \overline{y}^m])[\overline{z}^n := \overline{c}^n]_\mathcal{N} = a[\overline{z}^n := \overline{c}^n]_\mathcal{N}$. □

Proposition 2.4 (Théorème de complétude de Gödel)**.** Soit $\mathcal{T}$ une théorie. Il existe un modèle de $\mathcal{T}$ si et seulement si $\mathcal{T}$ est cohérente.

Pour une preuve de ce résultat (dans un cadre plus général), voir *Mathematical Logic – A Course with Exercises Part I* [RC02], p. 208, théorème 4.29.

Corollaire. Soient $\mathcal{T}$ une théorie et A une formule close. A est conséquence de $\mathcal{T}$ si et seulement si tout modèle de $\mathcal{T}$ vérifie A.

2.4 La théorie des ensembles extensionnelle

La théorie des ensemble extensionnelle correspond à la théorie des ensembles telle qu'on l'entend habituellement. Elle ne s'intéresse qu'aux « propriétés extensionnelles », celles qui s'expriment uniquement à partir des symboles extensionnels et des connecteurs logiques :

Définition 2.5. Une formule est *strictement extensionnelle* si elle est construite sur la grammaire suivante :

$$
\begin{array}{lll}
A, B \ ::= & a \subsetneq b \mid a \notin b & (a \text{ et } b \text{ termes du premier ordre}) \\
\mid & \top \mid \bot & \\
\mid & A \to B & (A \text{ et } B \text{ formules } \textit{strictement extensionnelles}) \\
\mid & \forall x\, A & (x \text{ variable du premier ordre, } A \text{ formule } \textit{strictement extensionnelle}).
\end{array}
$$

Définition 2.6. La *théorie des ensembles extensionnelle*, notée ZF, est la plus petite théorie close par déduction contenant les formules suivantes (qui sont toutes strictement extensionnelles) :

— L'axiome de définition de $\subsetneq$:

$$\forall a \forall b \ \left(a \subsetneq b \leftrightarrow \forall x{\in}a \ (x \in b)\right),$$

— Le schéma d'axiomes d'extensionnalité : pour toute formule *strictement extensionnelle* $A(\overline{w}, x)$, la formule

$$\forall \overline{w} \ \forall a \forall b \ (a \approx b \to A(\overline{w}, a) \to A(\overline{w}, b)),$$

— Le schéma d'axiomes de fondation : pour toute formule *strictement extensionnelle* $A(\overline{w}, x)$, la formule

$$\forall \overline{w} \ \left(\forall x \ (\forall y{\in}x \ A(\overline{w}, y) \to A(\overline{w}, x)) \to \forall x \ A(\overline{w}, x)\right),$$

— Le schéma d'axiomes de compréhension : pour toute formule *strictement extensionnelle* $A(\overline{w}, x)$, la formule

$$\forall \overline{w} \ \forall a \ \exists b \ \forall x \ (x \in b \leftrightarrow (x \in a \wedge A(\overline{w}, x))),$$

— L'axiome de la paire :

$$\forall a \ \forall b \ \exists c \ (a \in c \wedge b \in c),$$

— L'axiome de l'union :

$$\forall a \ \exists u \ \forall x{\in}a \ (x \subsetneq u),$$

— Le schéma d'axiomes de collection : pour toute formule *strictement extensionnelle* $A(\overline{w}, x, y)$, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ \forall x{\in}a\ (\exists y\ A(\overline{w}, x, y) \to \exists y{\in}b\ A(\overline{w}, x, y)),$$

— Le schéma d'axiomes de l'infini : pour toute formule *strictement extensionnelle* $A(\overline{w}, x, y)$, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ (a \in b \wedge \forall x{\in}b\ (\exists y\ A(\overline{w}, x, y) \to \exists y{\in}b\ A(\overline{w}, x, y))),$$

— L'axiome des parties :

$$\forall a\ \exists p\ \forall z\ (z \subsetneqq a \to z \in p).$$

L'axiome d'extensionnalité dit que si a et b ont les mêmes éléments (ce qui est la définition de $a \approx b$), alors a et b sont égaux au sens de l'« égalité de Leibniz extensionnelle », c'est-à-dire qu'ils satisfont exactement les mêmes « propriétés extensionnelles ». Notons que dans les formulations habituelles de la théorie des ensembles, c'est l'égalité de Leibniz qui est notée avec un unique symbole ($=$) et le fait d'avoir les mêmes éléments qui est noté avec une formule, alors qu'ici, c'est le contraire.

Notation (Couples de Kuratowski extensionnels)**.** On note $\mathrm{Couple}_{\in}(a, b, c)$ la formule $\exists u\ \exists v\ (\forall w\ (w \in c \leftrightarrow w \approx u \vee w \approx v) \wedge \forall x\ (x \in u \leftrightarrow x \approx a) \wedge \forall x\ (x \in v \leftrightarrow x \approx a \vee x \approx b))$. Elle est strictement extensionnelle.

La formule $\mathrm{Couple}_{\in}(a, b, c)$ dit que c « est le couple (a, b) », avec la définition ensembliste usuelle. On a donc le résultat suivant :

Proposition 2.7. Les formules suivantes sont conséquences de la théorie des ensembles extensionnelle :

— $\forall a\ \forall b\ \exists c\ \ \mathrm{Couple}_{\in}(a, b, c)$,

— $\forall a\ \forall b\ \forall c\ \forall a'\ \forall b'\ \forall c'\ (\mathrm{Couple}_{\in}(a, b, c) \to \mathrm{Couple}_{\in}(a', b', c') \to (c \approx c' \leftrightarrow a \approx a' \wedge b \approx b'))$.

2.5 La théorie des ensembles non extensionnelle

Définition 2.8. La *théorie des ensembles non extensionnelle*, notée notée $\mathrm{ZF}_{\varepsilon}$, est la plus petite théorie close par déduction contenant les formules suivantes :

— L'axiome de définition de $\in$:

$$\forall a \forall b\ \ (a \in b \leftrightarrow \exists a' \varepsilon b\ (a' \approx a))\,,$$

— L'axiome de définition de $\subsetneqq$:

$$\forall a \forall b\ \ \left(a \subsetneqq b \leftrightarrow \forall x \varepsilon a\ (x \in b)\right),$$

— L'axiome d'introduction de l'égalité :

$$\forall a\ (a = a),$$

— Le schéma d'axiomes d'élimination de l'égalité : pour toute formule $A(\overline{w}, x)$, la formule

$$\forall \overline{w}\ \forall a \forall b\ (a = b \to A(\overline{w}, a) \to A(\overline{w}, b)),$$

— Le schéma d'axiomes de fondation : pour toute formule $A(\overline{w}, x)$, la formule

$$\forall \overline{w}\ \ (\forall x\ (\forall y \varepsilon x\ A(\overline{w}, y) \to A(\overline{w}, x)) \to \forall x\ A(\overline{w}, x))\,,$$

— Le schéma d'axiomes de compréhension : pour toute formule $A(\overline{w}, x)$, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ \forall x\ (x\ \varepsilon\ b \leftrightarrow (x\ \varepsilon\ a \wedge A(\overline{w}, x))),$$

— L'axiome de la paire :

$$\forall a\ \forall b\ \exists c\ (a\ \varepsilon\ c \wedge b\ \varepsilon\ c),$$

— L'axiome de l'union :

$$\forall a\ \exists u\ \forall x \varepsilon a\ (x \subseteq u),$$

— Le schéma d'axiomes de collection : pour toute formule $A(\overline{w}, x, y)$, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ \forall x \varepsilon a\ (\exists y\ A(\overline{w}, x, y) \to \exists y \varepsilon b\ A(\overline{w}, x, y)),$$

— Le schéma d'axiomes de l'infini : pour toute formule $A(\overline{w}, x, y)$, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ (a\ \varepsilon\ b \wedge \forall x \varepsilon b\ (\exists y\ A(\overline{w}, x, y) \to \exists y \varepsilon b\ A(\overline{w}, x, y))),$$

— L'axiome des parties :

$$\forall a\ \exists p\ \forall z\ (z \subseteq a \to \exists z' \varepsilon p\ \forall x\ (x\ \varepsilon\ z' \leftrightarrow x\ \varepsilon\ z)).$$

Il s'agit (à part pour les trois premiers) des mêmes axiomes que pour la théorie extensionnelle, mais formulés avec les symboles non extensionnels. Remarquons que pour l'axiome des parties, il a fallu « déplier » un niveau d'extensionnalité, c'est-à-dire qu'au lieu d'écrire $\forall a\ \exists p\ \forall z\ (z \subseteq a \to \exists z' \varepsilon p\ (z = z'))$, qui aurait correspondu exactement à l'axiome extensionnel, on a écrit $\forall a\ \exists p\ \forall z\ (z \subseteq a \to \exists z' \varepsilon p\ \forall x\ (x\ \varepsilon\ z' \leftrightarrow x\ \varepsilon\ z))$. La raison est que la première formule est très « forte », à tel point qu'elle n'est en général pas vraie dans les modèles de réalisabilité, alors que la seconde l'est.

La similitude formelle entre l'axiome d'élimination de l'égalité de cette théorie et l'axiome d'extensionnalité de la précédente s'explique ainsi : l'axiome d'extensionnalité est censé dire que, tant qu'on ne parle que de propriétés extensionnelles, l'égalité extensionnelle « $\approx$ » se comporte *exactement comme une égalité*, ce qui s'exprime naturellement en donnant à $\approx$ les mêmes axiomes que $=$ restreints à ce cadre (notons que dans la théorie extensionnelle, la version adaptée à $\approx$ de l'axiome d'*introduction* de l'égalité, c'est-à-dire la formule $\forall a\ a \approx a$, est une conséquence de l'axiome de définition de $\subsetneq$, elle n'a donc pas besoin d'un axiome à part).

On va montrer que ZF_ε est une extension conservatrice de ZF (c'est-à-dire que ZF est conséquence de ZF_ε et que toute formule strictement extensionnelle conséquence de ZF_ε est également conséquence de ZF).

La première étape consiste à montrer à partir des axiomes de ZF_ε que la relation $\approx$ est une relation d'équivalence compatible avec $\in$ et $\subsetneq$. Pour montrer que $\approx$ est une relation d'équivalence, il suffira de montrer que $\subsetneq$ est un préordre.

Lemme 2.9. Les formules suivantes sont conséquences de ZF_ε :

(1) $\forall x\ (x \subsetneq x)$,

(2) $\forall x\ \forall y\ \forall z\ (x \subsetneq y \to y \subsetneq z \to x \subsetneq z)$,

(3) $\forall x\ (x \approx x)$,

(4) $\forall x\ \forall y\ (x \approx y \to y \approx x)$,

(5) $\forall x\ \forall y\ \forall z\ (x \approx y \to y \approx z \to x \approx z)$,

(6) $\forall x\ \forall x'\ \forall y\ (x \approx x' \to x \in y \to x' \in y)$,

(7) $\forall x\ \forall y\ \forall y'\ (y \approx y' \to x \in y \to x \in y')$,

(8) $\forall x\ \forall x'\ \forall y\ (x \approx x' \to x \subsetneq y \to x' \subsetneq y)$,

(9) $\forall x\ \forall y\ \forall y'\ (y \approx y' \to x \subsetneq y \to x \subsetneq y')$.

Démonstration. Preuve de (1) : d'après l'axiome de définition de $\subsetneq$, il suffit de démontrer à partir des axiomes de ZF_ε la formule $\forall x\ \forall y\ (y\ \varepsilon\ x \to y \in x)$. Pour cela, on applique le schéma de fondation à la formule $\forall y\ (y\ \varepsilon\ x \to y \in x)$: il suffit alors de démontrer la formule $\forall x\ (\forall y\ (y\ \varepsilon\ x \to \forall z\ (z\ \varepsilon\ y \to z \in y)) \to \forall y\ (y\ \varepsilon\ x \to y \in x))$. Grâce à l'axiome de définition de $\subsetneq$, il suffit de montrer la formule $\forall x\ (\forall y\ (y\ \varepsilon\ x \to y \subsetneq y) \to \forall y\ (y\ \varepsilon\ x \to y \in x))$. Grâce à l'axiome de définition de $\in$, il suffit de montrer la formule $\forall x\ (\forall y\ (y\ \varepsilon\ x \to y \subsetneq y) \to \forall y\ (y\ \varepsilon\ x \to (y\ \varepsilon\ x \wedge y \approx y)))$, qui est une tautologie.

Preuve de (2) : d'après le théorème de complétude (proposition 2.4), il suffit de montrer que cette formule est vraie dans tout modèle de ZF_ε. Considérons donc un modèle $\mathcal{N}$ de ZF_ε. On applique le schéma de fondation à la formule $\forall x\ \forall z\ (x \subsetneq y \to y \subsetneq z \to x \subsetneq z)$: il suffit alors de démontrer que la formule $\forall y\ (\forall b \varepsilon y\ \forall a\ \forall c\ (a \subsetneq b \to b \subsetneq c \to a \subsetneq c) \to \forall x\ \forall z\ (x \subsetneq y \to y \subsetneq z \to x \subsetneq z))$ est vraie dans $\mathcal{N}$. Soit y un objet de $\mathcal{N}$ tel que $\forall b \varepsilon y\ \forall a\ \forall c\ (a \subsetneq b \to b \subsetneq z \to a \subsetneq c)$ (l'hypothèse d'induction) soit vraie. Soient x et y des objets de $\mathcal{N}$ tels que $x \subsetneq y$ et $y \subsetneq z$. On doit montrer que $\forall a \varepsilon x\ a \in z$ est vraie : soit donc $a\ \varepsilon\ x$. Comme $x \subsetneq y$, $a \in y$, donc il existe $b\ \varepsilon\ y$ tel que $b \approx a$. Comme $y \subsetneq z$, $b \in z$, donc il existe $c\ \varepsilon\ z$ tel que $c \approx b$. On a donc $a \subsetneq b$, $b \subsetneq c$, $c \subsetneq b$ et $b \subsetneq a$. Par conséquent, d'après l'hypothèse d'induction, $a \subsetneq c$ et $c \subsetneq a$, autrement-dit $a \approx c$. Comme $c\ \varepsilon\ z$, $a \in z$.

Preuve de (3) : conséquence de (1).

Preuve de (4) : c'est une tautologie.

Preuve de (5) : conséquence de (2).

Preuve de (6) : il suffit de montrer $\forall x\ \forall x'\ \forall x''\ \forall y\ (x \approx x' \to x \approx x'' \to x''\ \varepsilon\ y \to x' \approx x'')$, qui est conséquence de (4) et (5).

Preuve de (7) : il suffit de montrer $\forall x\ \forall x'\ \forall y\ \forall y'\ (y \subsetneq y' \to x \approx x' \to x'\ \varepsilon\ y \to x \in y')$. D'après l'axiome de définition de $\subsetneq$, il suffit de montrer $\forall x\ \forall x'\ \forall y'\ (x \approx x' \to x' \in y' \to x \in y')$, qui est équivalente à (6).

Preuve de (8) : conséquence de (2).

Preuve de (9) : conséquence de (2). □

Corollaire. Les formules $\forall x\ \forall y\ (x\ \varepsilon\ y \to x \in y)$ et $\forall x\ \forall y\ (x \subseteq y \to x \subsetneq y)$ sont conséquences de ZF_ε.

On va maintenant montrer que ZF_ε prouve un raffinement de ZF, dans lequel les conditions de stricte extensionnalité sont remplacées par des conditions plus faibles :

Définition 2.10. Soient A une formule et x une variable du premier ordre. A est *extensionnelle en* x si :

— toutes les occurrences libres de x dans A sont de la forme $x \in a$, $a \in x$, $x \subsetneq a$ ou $a \subsetneq x$ avec a un terme du premier ordre,

— aucune sous-formule de A de la forme $B \cap C$ ou $B \cup C$ ne contient une occurrence libre de x.

En particulier, une formule strictement extensionnelle est extensionnelle en toute variable.

Proposition 2.11. Les formules suivantes sont conséquences de ZF_ε :

(1) $\forall a \forall b\ \big(a \subsetneq b \leftrightarrow \forall x{\in}a\ (x \in b)\big)$,

(2) pour toute formule $A(\overline{w}, x)$ *extensionnelle en* x, la formule

$$\forall \overline{w}\ \forall a \forall b\ (a \approx b \to A(\overline{w}, a) \to A(\overline{w}, b)),$$

(c'est ce qui donne un sens à la notion d'extensionnalité en une variable).

(3) pour toute formule $A(\overline{w}, x)$, la formule

$$\forall \overline{w}\ \ (\forall x\ (\forall y{\in}x\ A(\overline{w}, y) \to A(\overline{w}, x)) \to \forall x\ A(\overline{w}, x))\,,$$

(4) pour toute formule $A(\overline{w}, x)$ *extensionnelle en* x, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ \forall x\ (x \in b \leftrightarrow (x \in a \wedge A(\overline{w}, x))),$$

(5) $\forall a\ \forall b\ \exists c\ (a \in c \wedge b \in c)$,

(6) $\forall a\ \exists u\ \forall x{\in}a\ (x \subsetneq u)$,

(7) pour toute formule $A(\overline{w}, x, y)$ *extensionnelle en* x, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ \forall x{\in}a\ (\exists y\ A(\overline{w}, x, y) \to \exists y{\in}b\ A(\overline{w}, x, y)),$$

(8) pour toute formule $A(\overline{w}, x, y)$ *extensionnelle en* x, la formule

$$\forall \overline{w}\ \forall a\ \exists b\ (a \in b \wedge \forall x{\in}b\ (\exists y\ A(\overline{w}, x, y) \rightarrow \exists y{\in}b\ A(\overline{w}, x, y))),$$

(9) $\forall a\ \exists p\ \forall z\ (z \subsetneq a \rightarrow z \in p)$.

Démonstration. Preuve de (1) : conséquence du lemme 2.9

Preuve de (2) : il suffit de procéder par induction sur la structure de la formule $A(\overline{w}, x)$. Pour les formules n'ayant pas x comme variable libre, il n'y a rien à montrer. Pour les formules atomiques contenant x, on utilise le lemme 2.9. Enfin, pour les formules de la forme $B(\overline{w}, x) \rightarrow C(\overline{w}, x)$ ou $\forall y\ B(\overline{w}, y, x)$, on utilise l'hypothèse d'induction et le fait que la formule $(\forall \overline{w}\ (B(\overline{w}, a) \leftrightarrow B(\overline{w}, b))) \rightarrow (\forall \overline{w}\ (C(\overline{w}, a) \leftrightarrow C(\overline{w}, b))) \rightarrow (\forall \overline{w}\ ((B(\overline{w}, a) \rightarrow C(\overline{w}, a)) \leftrightarrow (B(\overline{w}, b) \rightarrow C(\overline{w}, b))))$ et la formule $(\forall \overline{w}\ \forall y\ (B(\overline{w}, y, a) \leftrightarrow B(\overline{w}, y, b))) \rightarrow (\forall \overline{w}\ (\forall y\ B(\overline{w}, y, a) \leftrightarrow \forall y\ B(\overline{w}, y, b)))$ sont des tautologies[i].

Preuve de (3) : notons $\widetilde{A}(\overline{w}, x)$ la formule $\forall x' {\approx} x\ A(\overline{w}, x')$. Considérons un modèle $\mathcal{N}$ de ZF_ε. Comme $\forall \overline{w}\ (\forall x\ A(\overline{w}, x) \leftrightarrow \forall x\ \widetilde{A}(\overline{w}, x))$ est vraie (le sens de gauche à droite est une tautologie, le sens de droite à gauche découle de $\forall x\ x{\approx}x$), il suffit de montrer que $\forall \overline{w}\ (\forall x\ (\forall y{\in}x\ A(\overline{w}, y) \rightarrow A(\overline{w}, x)) \rightarrow \forall x\ \widetilde{A}(\overline{w}, x))$ est vraie. Par le schéma de fondation, il suffit de montrer que $\forall \overline{w}\ (\forall x\ (\forall y{\in}x\ A(\overline{w}, y) \rightarrow A(\overline{w}, x)) \rightarrow \forall x\ (\forall y \varepsilon x\ \widetilde{A}(\overline{w}, y) \rightarrow \widetilde{A}(\overline{w}, x)))$ est vraie. Soient $\overline{w}$ des objets de $\mathcal{N}$ tels que $\forall x\ (\forall y{\in}x\ A(\overline{w}, y) \rightarrow A(\overline{w}, x))$ soit vraie et x un objet tel que $\forall y \varepsilon x\ \widetilde{A}(\overline{w}, y)$ soit vraie. On doit montrer que $\widetilde{A}(\overline{w}, x)$ est vraie. Soit donc $x' \approx x$, et montrons que $A(\overline{w}, x')$ est vraie. Pour tout $y \in x'$, $y \in x$, donc il existe $y'\ \varepsilon\ x$ tel que $y' \approx y$, donc $\widetilde{A}(\overline{w}, y')$ est vraie, et donc $A(\overline{w}, y)$ est vraie. Par conséquent, $A(\overline{w}, x')$ est vraie.

Preuve de (4) : il suffit d'appliquer le schéma de compréhension à $A(\overline{w}, x)$ et d'utiliser (2).

Preuve de (5) : il suffit d'utiliser l'axiome de la paire et le lemme 2.9.

Preuve de (6) : il suffit d'utiliser l'axiome de l'union et le lemme 2.9.

Preuve de (7) : il suffit d'appliquer le schéma de collection à $A(\overline{w}, x, y)$ et d'utiliser (2).

Preuve de (8) : il suffit d'appliquer le schéma de l'infini à $A(\overline{w}, x, y)$ et d'utiliser (2).

Preuve de (9) : Considérons un modèle $\mathcal{N}$ de ZF_ε. Soit a un objet de $\mathcal{N}$ et soit p tel que $\forall y\ (y \subseteq a \rightarrow \exists y' \varepsilon p\ \forall x\ (x\ \varepsilon\ y' \leftrightarrow x\ \varepsilon\ y)$ soit vraie (un tel p existe d'après l'axiome des parties). Soit $z \subsetneq a$. Soit y tel que $\forall x\ (x\ \varepsilon\ y \leftrightarrow (x\ \varepsilon\ a \wedge \exists x'\ \varepsilon\ z\ (x' \approx x)))$ soit vraie (un tel y existe d'après le schéma de compréhension). On a $y \subseteq a$, donc il existe $y'\ \varepsilon\ p$ tel que $y' \subseteq y$ et $y \subseteq y'$, et donc $y \in p$. De plus, $y \approx z$, par conséquent, $z \in p$. □

Proposition 2.12. Toute formule prouvable dans ZF est prouvable dans ZF_ε, et réciproquement, toute formule extensionnelle prouvable dans ZF_ε est prouvable dans ZF. Autrement-dit, ZF_ε est une extension conservatrice de ZF.

Démonstration. D'après la proposition précédente, tous les axiomes de ZF sont conséquences de ZF_ε, donc toute formule prouvable dans ZF est prouvable dans ZF_ε.

Pour la conservation, il suffit de constater que d'une part, si l'on prend un arbre de preuve quelconque et que l'on remplace tous les $\not\varepsilon$ par des $\notin$, tous les $\neq$ par des $\not\approx$, tous les $\cap$ par des $\wedge$[ii] et tous les $\cup$ par des $\vee$[iii], on obtient encore un arbre de preuve, et que d'autre part, si l'on applique le même traitement à n'importe quel axiome de ZF_ε, on obtient une formule prouvable dans ZF. Par conséquent, si l'on applique cette transformation à une formule prouvable dans ZF_ε, on obtient toujours une formule prouvable dans ZF. Comme les formules extensionnelles sont préservées par cette transformation, ZF_ε est conservatrice sur ZF pour ces formules. □

i. Remarquons qu'en revanche, ni la formule $(\forall \overline{w}\ (B(\overline{w}, a) \leftrightarrow B(\overline{w}, b))) \rightarrow (\forall \overline{w}\ (C(\overline{w}, a) \leftrightarrow C(\overline{w}, b))) \rightarrow (\forall \overline{w}\ ((B(\overline{w}, a) \cap C(\overline{w}, a)) \leftrightarrow (B(\overline{w}, b) \cap C(\overline{w}, b))))$ ni son analogue avec $\cup$ ne sont des tautologies, d'où la restriction sur ces connecteurs dans la définition 2.10

ii. Ou par n'importe quoi, d'ailleurs, et pour cause : pour l'instant on ne sait rien ni sur $\cap$ ni sur $\cup$.

iii. Idem.

2.6 Interprétation des termes et formules

Le but de cette section est de définir la relation « t réalise A modulo $\perp\!\!\!\perp$ », pour t un terme, A une formule close et $\perp\!\!\!\perp$ un pôle.

Pour cela, on va d'abord associer à A un ensemble de piles appelé sa *valeur de fausseté* et noté $\|A\|_{\perp\!\!\!\perp}$, qui représente l'ensemble des *arguments contre* A. Ensuite, on associera à A un ensemble de termes appelé sa *valeur de vérité*, notée $|A|_{\perp\!\!\!\perp}$ et définie comme le *dual* de $\|A\|_{\perp\!\!\!\perp}$, dans un sens à préciser. On dira alors que t réalise A modulo $\perp\!\!\!\perp$ lorsque $t \in |A|_{\perp\!\!\!\perp}$. Intuitivement, t réalise A modulo $\perp\!\!\!\perp$ si $\perp\!\!\!\perp$ juge que t est capable de réfuter tout argument contre A.

La définition de $\|A\|_{\perp\!\!\!\perp}$ sera guidée par deux critères. Premièrement, la réalisabilité doit être *compatible avec la logique classique*, c'est-à-dire que par exemple, si t réalise $A \to B$ et u réalise A, il faudra que tu réalise B ; le *lemme d'adéquation*, énoncé et démontré plus loin (proposition 2.19), donnera un sens précis à cette notion de compatibilité avec la logique classique. Deuxièmement, il faudra pouvoir réaliser les axiomes de ZF_ε.

Chaque terme clos du premier ordre doit *désigner* un élément du modèle de réalisabilité. Pour cela, on va considérer que chaque élément de $\mathcal{M}$ *nomme* un objet du modèle de réalisabilité, et l'on va donc *évaluer* chaque terme clos du premier ordre en un élément de $\mathcal{M}$:

Définition 2.13. Soient a un terme clos du premier ordre et $\perp\!\!\!\perp$ un pôle. La *valeur de a modulo $\perp\!\!\!\perp$*, notée $[a]_{\perp\!\!\!\perp}$ est le $\mathcal{M}$-ensemble défini inductivement par $[f(a_1, \dots, a_n)]_{\perp\!\!\!\perp} = f(\perp\!\!\!\perp, [a_1]_{\perp\!\!\!\perp}, \dots, [a_n]_{\perp\!\!\!\perp})$.

Définition 2.14. Soient $\perp\!\!\!\perp$ un pôle et $X \in \mathcal{P}_{\mathcal{M}}(\Pi)$. Le *dual de X modulo $\perp\!\!\!\perp$*, noté $X^{\perp\!\!\!\perp}$, est le $\mathcal{M}$-ensemble de termes $\{\ t \in \Lambda; \forall \pi \in X,\ t \star \pi \in \perp\!\!\!\perp\ \}$.

Définition 2.15. Soient $\perp\!\!\!\perp$ un pôle et A une formule close. La *valeur de fausseté de A modulo $\perp\!\!\!\perp$*, notée $\|A\|_{\perp\!\!\!\perp}$, est le $\mathcal{M}$-ensemble de piles défini ci-dessous, et la *valeur de vérité de A modulo $\perp\!\!\!\perp$*, notée $|A|_{\perp\!\!\!\perp}$, est définie comme le dual de $\|A\|_{\perp\!\!\!\perp}$ modulo $\perp\!\!\!\perp$.

Les valeurs de fausseté des formules non atomiques est définie ainsi :

— $\|\top\|_{\perp\!\!\!\perp} = \emptyset$, $\|\perp\|_{\perp\!\!\!\perp} = \Pi$,
— $\|A \to B\|_{\perp\!\!\!\perp} = \{\ t \cdot \pi;\ t \in |A|_{\perp\!\!\!\perp}, \pi \in \|B\|_{\perp\!\!\!\perp}\ \}$,
— $\|\forall x\ A\|_{\perp\!\!\!\perp} = \bigcup_{a \in \mathcal{M}} \|A[x := a]\|_{\perp\!\!\!\perp}$,
— $\|A \cap B\|_{\perp\!\!\!\perp} = \|A\|_{\perp\!\!\!\perp} \cup \|B\|_{\perp\!\!\!\perp}$,
— $\|A \cup B\|_{\perp\!\!\!\perp} = \|A\|_{\perp\!\!\!\perp} \cap \|B\|_{\perp\!\!\!\perp}$.

La valeur de fausseté des relations non extensionnelles ($a \neq b$ et $a \not\in b$) est définie ainsi :

— $\|a \neq b\|_{\perp\!\!\!\perp} = \begin{cases} \|\perp\|_{\perp\!\!\!\perp} & \text{si } [a]_{\perp\!\!\!\perp} = [b]_{\perp\!\!\!\perp} \\ \|\top\|_{\perp\!\!\!\perp} & \text{sinon,} \end{cases}$
— $\|a \not\in b\|_{\perp\!\!\!\perp} = \{\ \pi \in \Pi;\ ([a]_{\perp\!\!\!\perp}, \pi) \in [b]_{\perp\!\!\!\perp}\ \}$.

Enfin, la valeur de fausseté des relations extensionnelles ($a \subsetneq b$ et $a \not\in b$) est définie par induction sur le couple d'ordinaux $(\max(\mathrm{rg}([a]_{\perp\!\!\!\perp}), \mathrm{rg}([b]_{\perp\!\!\!\perp})), \min(\mathrm{rg}([a]_{\perp\!\!\!\perp}), \mathrm{rg}([b]_{\perp\!\!\!\perp})))$ ordonné lexicographiquement (où $\mathrm{rg}(x)$ désigne le rang de x, et le poids le plus important est donné au membre de gauche du couple) :

— $\left\|a \subsetneq b\right\|_{\perp\!\!\!\perp} = \{\ t \cdot \pi;\ t \in |c \not\in b|_{\perp\!\!\!\perp}, (c, \pi) \in [a]_{\perp\!\!\!\perp}\ \}$,
— $\|a \not\in b\|_{\perp\!\!\!\perp} = \left\{\ t \cdot u \cdot \pi;\ t \in \left|a \subsetneq c\right|_{\perp\!\!\!\perp}, u \in \left|c \subsetneq a\right|_{\perp\!\!\!\perp}, (c, \pi) \in [b]_{\perp\!\!\!\perp}\ \right\}$.

Quelques intuitions derrière ces définitions :

— $\|\top\|_{\perp\!\!\!\perp} = \emptyset$ signifie qu'il n'existe aucun argument contre $\top$, et assure que tout terme t réalise $\top$,
— $\|\perp\|_{\perp\!\!\!\perp} = \Pi$ signifie que n'importe quelle pile est un argument contre $\perp$, et assure qu'un terme qui réalise $\perp$ réalise toute formule close,
— $\|A \to B\|_{\perp\!\!\!\perp} = \{\ t \cdot \pi;\ t \in |A|_{\perp\!\!\!\perp}, \pi \in \|B\|_{\perp\!\!\!\perp}\ \}$ signifie qu'un argument contre $A \to B$ est la donnée d'une preuve de A et d'un argument contre B, et assure que si t réalise $A \to B$ et u réalise A, alors tu réalise B (grâce à la clôture de $\perp\!\!\!\perp$ par anti-réduction),

— $\|\forall x\ A\|_{\perp\!\!\!\perp} = \bigcup_{a\in\mathcal{M}} \|A[x := a]\|_{\perp\!\!\!\perp}$ signifie qu'un argument contre $\forall x\ A(x)$ est la donnée d'un argument contre $A(a)$ pour un $a \in \mathcal{M}$ quelconque, et assure que t réalise $\forall x\ A(x)$ si et seulement si t réalise $A(a)$ pour tout $a \in \mathcal{M}$,

— les connecteurs $\cap$ et $\cup$ n'ont pas d'interprétation logique et servent uniquement à manipuler directement les valeurs de fausseté ; toutefois, on peut remarquer que la définition de $\|A \cap B\|$ a été choisie pour que t réalise $A \cap B$ si et seulement si t réalise A et t réalise B,

— $\|a \not\in b\|_{\perp\!\!\!\perp} = \{\ \pi \in \Pi;\ ([a]_{\perp\!\!\!\perp}, \pi) \in [b]_{\perp\!\!\!\perp}\ \}$ signifie que pour tout $b \in \mathcal{M}$, pour tout $(a, \pi) \in b$, a désigne un ε-*élément potentiel* de b, et π est un argument contre $a \not\in b$, c'est-à-dire un *argument pour* $a\ \varepsilon\ b$; de cette façon, l'ensemble b contient toute l'information nécessaire pour savoir qui sont les ε-éléments de l'objet du modèle de réalisabilité qu'il nomme,

— la définition de $\left\|a \subsetneq b\right\|_{\perp\!\!\!\perp}$ a été choisie pour que $\left\|a \subsetneq b\right\|_{\perp\!\!\!\perp} = \|\forall x\ (x \notin b \to x \not\in a)\|_{\perp\!\!\!\perp}$, ce qui permet de réaliser facilement l'axiome de définition de $\subsetneq$,

— la définition de $\|a \notin b\|_{\perp\!\!\!\perp}$ a été choisie pour que $\|a \notin b\|_{\perp\!\!\!\perp} = \left\|\forall a'\ (a \subsetneq a' \to a' \subsetneq a \to a' \not\in b)\right\|_{\perp\!\!\!\perp}$, ce qui permet de réaliser facilement l'axiome de définition de $\in$.

Remarque. On peut montrer par induction que pour toute formule $A(\overline{x})$ et tout terme du premier ordre $a(\overline{x})$, les opérations $(\perp\!\!\!\perp, \overline{b}) \mapsto \left\|A\left(\overline{b}\right)\right\|_{\perp\!\!\!\perp}$, $(\perp\!\!\!\perp, \overline{b}) \mapsto \left|A\left(\overline{b}\right)\right|_{\perp\!\!\!\perp}$ et $(\perp\!\!\!\perp, \overline{b}) \mapsto \left[a\left(\overline{b}\right)\right]_{\perp\!\!\!\perp}$ sont des $\mathcal{M}$-fonctionnelles.

Notation. Soit A une formule close. On note $\|A\|$ la fonction qui à $\perp\!\!\!\perp$ associe $\|A\|_{\perp\!\!\!\perp}$, et $|A|$ la fonction qui à $\perp\!\!\!\perp$ associe $|A|_{\perp\!\!\!\perp}$.

Définition 2.16. Soient A une formule close, t un terme et $\perp\!\!\!\perp$ un pôle. Si $t \in |A|_{\perp\!\!\!\perp}$, on dit que t *réalise* A *modulo* $\perp\!\!\!\perp$, et l'on note $t \Vdash_{\perp\!\!\!\perp} A$.

Remarque. Pour toute formule $A(\overline{w}^n)$, les ensembles $\{\ (\pi, \perp\!\!\!\perp, \overline{c}) \in \Pi \times \mathcal{S}_0 \times \mathcal{M}^n;\ \pi \in \|A(\overline{c}^n)\|_{\perp\!\!\!\perp}\ \}$ et $\{\ (t, \perp\!\!\!\perp, \overline{c}^n) \in \Lambda \times \mathcal{S}_0 \times \mathcal{M}^n;\ t \Vdash_{\perp\!\!\!\perp} A(\overline{c}^n)\ \}$ sont des $\mathcal{M}$-classes.

Définition 2.17. Soient A une formule close et t un terme. On dit que t *réalise universellement* A si t réalise A modulo tout pôle.

Remarque. Soit $\perp\!\!\!\perp$ un pôle. Pour tous $X, Y \in \mathcal{P}_{\mathcal{M}}(\Pi)$, si $X \supseteq Y$, alors $X^{\perp\!\!\!\perp} \subseteq Y^{\perp\!\!\!\perp}$. Par conséquent, pour toutes formules closes A et B, si $\|A\|_{\perp\!\!\!\perp} \supseteq \|B\|_{\perp\!\!\!\perp}$, alors $|A|_{\perp\!\!\!\perp} \subseteq |B|_{\perp\!\!\!\perp}$, et en particulier, l'identité $\lambda x.x$ réalise $A \to B$ par rapport à $\perp\!\!\!\perp$.

Notation (Équivalence et sous-typage sémantiques)**.** Soient $A(\overline{x})$ et $B(\overline{x})$ deux formules. Pour tout pôle $\perp\!\!\!\perp$, on note $A \equiv_{\perp\!\!\!\perp} B$ lorsque $\|A(\overline{c})\|_{\perp\!\!\!\perp} = \|B(\overline{c})\|_{\perp\!\!\!\perp}$ pour tous $\overline{c} \in \mathcal{M}$ et $A \leqq_{\perp\!\!\!\perp} B$ lorsque $\|A(\overline{c})\|_{\perp\!\!\!\perp} \supseteq \|B(\overline{c})\|_{\perp\!\!\!\perp}$ pour tous $\overline{c} \in \mathcal{M}$. De plus, pour toute structure de réalisabilité $\mathcal{S}$, on note $A \equiv_{\mathcal{S}} B$ lorsque $A \equiv_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$, et $A \leqq_{\mathcal{S}} B$ lorsque $A \leqq_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$. Enfin, on note $A \equiv B$ lorsque $A \equiv_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp$, et $A \leqq B$ lorsque $A \leqq_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp$.

2.7 Typage et adéquation

Le but de cette section est de formuler et de démontrer le *lemme d'adéquation*, qui garantira que la réalisabilité est compatible avec le raisonnement classique. En particulier, plus loin, il permettra de démontrer que la théorie engendrée par une structure de réalisabilité (qui reste encore à définir) est toujours close par déduction.

La première étape est de définir une notion de *typage* d'un λ_c-terme par une formule, qui affine la notion de prouvabilité :

Un *contexte* est un ensemble fini d'*hypothèses* de la forme $x : B$ (avec x une variable du λ_c-calcul et B aune formule) tel qu'aucune variable du λ_c-calcul n'apparaît à gauche de plus d'une hypothèse. Les variable du λ_c-calcul qui apparaissent à gauche d'une hypothèse sont dites *déclarées* dans le contexte, et les variables du premier ordre qui apparaissent librement à droite d'au moins une hypothèse sont dites *libres* dans le contexte.

Un *jugement de typage* est un séquent de la forme $\Gamma \vdash t : A$, avec Γ un contexte, t un λ_c-terme dont toutes les variables libres sont déclarées dans Γ et A une formule. Si Γ est un contexte, x une variable du λ_c-calcul non déclarée dans Γ et A une formule, on pourra noter « $\Gamma, x : A$ » pour $\Gamma \cup \{x : A\}$.

Un *arbre de typage* est un arbre formé à partir des règles suivantes. Sa racine (en bas) est appelée sa *conclusion* :

$$\text{(Axiome)}\ \frac{}{\Gamma, x : A \vdash x : A}$$

$$\text{(Peirce)}\ \frac{}{\Gamma \vdash \mathcal{C} : ((A \to B) \to A) \to A}$$

$$(\top\text{-intro})\ \frac{}{\Gamma \vdash t : \top} \qquad (\bot\text{-élim})\ \frac{\Gamma \vdash t : \bot}{\Gamma \vdash t : A}$$

$$(\to\text{-intro})\ \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B} \qquad (\to\text{-élim})\ \frac{\Gamma \vdash t : A \to B \quad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$$

$$(\forall\text{-intro})\ \frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall x\ A}\ \text{(si } x \text{ n'est pas libre dans } \Gamma) \qquad (\forall\text{-élim})\ \frac{\Gamma \vdash t : \forall x\ A}{\Gamma \vdash t : A[x := a]}$$

Un jugement de typage est dit *dérivable* s'il est la conclusion d'au moins un arbre de typage.

La notion de typage affine celle de prouvabilité au sens suivant :

Lemme 2.18. Soient $A, B_1, \ldots, B_n$ des formules. Le jugement de prouvabilité $B_1, \ldots, B_n \vdash A$ est dérivable si et seulement s'il existe un λ_c-terme t et une liste $x_1, \ldots, x_n$ de variables distinctes contenant toutes les variables libres de t tels que le jugement de typage $x_1 : B_1, \ldots, x_n : B_n \vdash t : A$ soit dérivable. De plus, dans ce cas, on peut demander que t ne contienne ni constante de continuation ni instruction protégée.

Démonstration. Immédiat par induction sur la structure des arbres de preuve et de typage. □

Proposition 2.19 (Lemme d'adéquation)**.** Soient $A(\overline{w}), B_1(\overline{w}), \ldots, B_n(\overline{w})$ des formules, t un λ_c-terme, $x_1, \ldots, x_n$ une liste de variables libres distinctes contenant au moins les variables libres de t, $\overline{c}$ des termes clos du premier ordre, $u_1, \ldots, u_n$ des termes et $\bot\!\!\bot$ un pôle. Si le jugement de typage $x_1 : B_1, \ldots, x_n : B_n \vdash t : A$ est dérivable et que u_i réalise $B_i(\overline{c})$ modulo $\bot\!\!\bot$ pour tout i, alors $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $A(\overline{c})$ modulo $\bot\!\!\bot$.

Démonstration. On procède par induction sur la structure de l'arbre de typage qui aboutit au jugement $x_1 : B_1, \ldots, x_n : B_n \vdash t : A$.

Si l'arbre est de la forme $\dfrac{}{\Gamma, x : A \vdash x : A}$, il n'y a rien à montrer.

Si l'arbre est de la forme $\dfrac{}{\Gamma \vdash \mathcal{C} : ((D \to E) \to D) \to D}$, il suffit de montrer que $\mathcal{C}$ réalise $((D(\overline{c}) \to E(\overline{c})) \to D(\overline{c})) \to D(\overline{c})$ modulo $\bot\!\!\bot$. Soient donc $t \Vdash_{\bot\!\!\bot} (D(\overline{c}) \to E(\overline{c})) \to D(\overline{c})$ et $\pi \in \|D(\overline{c})\|_{\bot\!\!\bot}$. On a $\mathcal{C} \star t \cdot \pi \succ_{\mathrm{K}} t \star k_\pi \cdot \pi$, donc il suffit de montrer que k_π réalise $D(\overline{c}) \to E(\overline{c})$ modulo $\bot\!\!\bot$. Soient $u \Vdash_{\bot\!\!\bot} D(\overline{c})$ et $\pi' \in \|E(\overline{c})\|_{\bot\!\!\bot}$. On a bien $k_\pi \star u \cdot \pi' \succ_{\mathrm{K}} u \star \pi \in \bot\!\!\bot$.

Si l'arbre est de la forme $\dfrac{}{\Gamma \vdash t : \top}$ avec $\Gamma = x_1 : B_1, \ldots, x_n : B_n$, il suffit de montrer que $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $\top$ modulo $\bot\!\!\bot$, ce qui est clair puisque $\|\top\|_{\bot\!\!\bot} = \emptyset$.

Si l'arbre est de la forme $\dfrac{\dfrac{\Theta}{\Gamma \vdash t : \bot}}{\Gamma \vdash t : A}$ avec $\Gamma = x_1 : B_1, \ldots, x_n : B_n$, on sait par hypothèse d'induction que $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $\bot$. Comme $\bot \subseteq A(\overline{c})$, il réalise également $A(\overline{c})$.

Si l'arbre est de la forme $\dfrac{\dfrac{\Theta}{\Gamma, y : D \vdash t : E}}{\Gamma \vdash \lambda y.t : D \to E}$ avec $\Gamma = x_1 : B_1, \ldots, x_n : B_n$, on sait par hypothèse

d'induction que pour tout $v \Vdash_{\perp\!\!\!\perp} D(\overline{c})$, $t[x_1 := u_1, \ldots, x_n := u_n, y := v]$ réalise $E(\overline{c})$. Par conséquent, pour tout $\pi \in \|E(\overline{c})\|_{\perp\!\!\!\perp}$, $(\lambda y.t)[x_1 := u_1, \ldots, x_n := u_n] \star v \cdot \pi \succ_K t[x_1 := u_1, \ldots, x_n := u_n, y := v] \star \pi \in \perp\!\!\!\perp$.

Si l'arbre est de la forme $\dfrac{\dfrac{\Theta_1}{\Gamma \vdash t : A \to B} \quad \dfrac{\Theta_2}{\Gamma \vdash v : D}}{\Gamma \vdash tv : E}$ avec $\Gamma = x_1 : B_1, \ldots, x_n : B_n$, on sait par hypothèse d'induction que $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $D(\overline{c}) \to E(\overline{c})$ et que $v[x_1 := u_1, \ldots, x_n := u_n]$ réalise $D(\overline{c})$. Par conséquent, pour tout $\pi \in \|E(\overline{c})\|_{\perp\!\!\!\perp}$, $(tv)[x_1 := u_1, \ldots, x_n := u_n] \star \pi \succ_K t[x_1 := u_1, \ldots, x_n := u_n] \star v[x_1 := u_1, \ldots, x_n := u_n] \cdot \pi \in \perp\!\!\!\perp$.

Si l'arbre est de la forme $\dfrac{\dfrac{\Theta}{\Gamma \vdash t : A(\overline{w}, y)}}{\Gamma \vdash t : \forall y\ A(\overline{w}, y)}$ avec $\Gamma = x_1 : B_1, \ldots, x_n : B_n$, on sait par hypothèse d'induction, et car y n'est pas libre dans Γ, que pour tout terme clos du premier ordre d, $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $A(\overline{c}, d)$. Par conséquent, pour tout $d \in \mathcal{M}$, $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $A(\overline{c}, d)$, c'est-à-dire que $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $\forall y\ A(\overline{w}, y)$.

Si l'arbre est de la forme $\dfrac{\dfrac{\Theta}{\Gamma \vdash t : \forall y\ A(\overline{w}, y)}}{\Gamma \vdash t : A(\overline{w}, a(\overline{w}))}$ avec $\Gamma = x_1 : B_1, \ldots, x_n : B_n$, on sait par hypothèse d'induction que $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $\forall y\ A(\overline{c}, y)$, or $\forall y\ A(\overline{c}, y) \leqq A(\overline{c}, a(\overline{c}))$, donc $t[x_1 := u_1, \ldots, x_n := u_n]$ réalise $A(\overline{c}, a(\overline{c}))$.

□

2.8 Théorie engendrée par une structure de réalisabilité

Maintenant que l'on a défini la notion de réalisation modulo un pôle, on peut passer à la réalisation modulo une structure :

Définition 2.20. Soient $\mathcal{S}$ une structure de réalisabilité, t un terme et A une formule close. On dit que t *réalise* A modulo $\mathcal{S}$, et l'on note $t \Vdash_{\mathcal{S}} A$, lorsque t réalise A modulo $\perp\!\!\!\perp$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$.

Remarque. Pour simplifier les notations, lorsque l'on aura fixé une structure de réalisabilité $\mathcal{S}$ mais pas un pôle particulier, on dira que t réalise A et l'on notera $t \Vdash A$ pour $t \Vdash_{\mathcal{S}} A$. Lorsque l'on aura fixé un pôle $\perp\!\!\!\perp$, on dira que t réalise A et l'on notera $t \Vdash A$ pour $t \Vdash_{\perp\!\!\!\perp} A$.

On pourrait être tenté de définir la théorie engendrée par une structure de réalisabilité comme l'ensemble des formules qui sont réalisées par au moins un terme modulo cette structure. Cependant, une caractéristique importante de la réalisabilité classique (par rapport à la réalisabilité intuitionniste) est que pour tout pôle non vide $\perp\!\!\!\perp$, il existe des termes qui réalisent $\bot$ modulo $\perp\!\!\!\perp$. En effet, soit $t \star \pi \in \perp\!\!\!\perp$, et considérons le terme $k_\pi t$: lorsque l'on l'évalue, ce terme ignore son contexte et le remplace par le contexte « gagnant » π, par conséquent il réalise $\bot$ modulo $\perp\!\!\!\perp$. Par conséquent, afin d'éviter d'obtenir des théories incohérentes, on imposera la restriction suivante :

Définition 2.21. Une *quasi-preuve* est un terme qui ne contient aucune constante de continuation (k_π) ni aucune instruction protégée (η_ν). Le $\mathcal{M}$-ensemble des quasi-preuves est noté $\mathcal{Q}$.

Intuitivement, les quasi-preuves correspondent aux programmes non-privilégiés, exécutables directement par l'utilisateur d'un système (*user space programs*).

En plus des constantes de continuation, on exclut également les instructions protégées de la syntaxe des quasi-preuves, car il sera parfois nécessaire de faire en sorte que certaines d'entre elles réalisent $\bot$ (ou d'autres formules incohérentes), et l'on souhaite pouvoir le faire sans rendre la théorie incohérente.

Définition 2.22. Soient $\mathcal{S}$ une structure de réalisabilité et A une formule close. La formule A est *réalisée modulo* $\mathcal{S}$ s'il existe une *quasi-preuve* t qui réalise A modulo $\mathcal{S}$.

Définition 2.23. Soit $\mathcal{S}$ une structure de réalisabilité. La *théorie engendrée par* $\mathcal{S}$, notée $\mathrm{Th}(\mathcal{S})$, est l'ensemble de toutes les formules closes réalisées modulo $\mathcal{S}$.

En combinant le lemme d'adéquation (proposition 2.19) et le lemme 2.18, on obtient un résultat essentiel :

Proposition 2.24. Pour toute structure de réalisabilité $\mathcal{S}$, la théorie $\mathrm{Th}(\mathcal{S})$ est close par déduction.

On dira qu'une structure de réalisabilité $\mathcal{S}$ est *cohérente* si la théorie qu'elle engendre l'est. D'après le résultat précédent, cela revient à dire qu'il n'existe aucune quasi-preuve t telle que $t \star \pi \in \perp\!\!\!\perp$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$ et toute $\pi \in \Pi$.

Un *modèle de réalisabilité* d'une structure de réalisabilité $\mathcal{S}$ est un modèle de la théorie $\mathrm{Th}(\mathcal{S})$. D'après la proposition 2.4, une structure de réalisabilité admet un modèle si et seulement si elle est cohérente.

Proposition 2.25. Soit $\mathcal{S}$ une structure de réalisabilité. $\mathcal{S}$ est cohérente si et seulement si pour toute quasi preuve t, il existe une pile π telle que $\{t \star \pi\} \not\succ_{\mathrm{K}_\mathcal{S}} \emptyset$.

Corollaire. Soit $\succ_\mathrm{K}$ une relation de multi-évaluation complète. La structure de réalisabilité engendrée par $\succ_\mathrm{K}$ est cohérente si et seulement si pour toute quasi preuve t, il existe une pile π telle que $\{t \star \pi\} \not\succ_\mathrm{K} \emptyset$.

On dira qu'une formule close est *universellement réalisée* s'il existe une *quasi-preuve* qui la réalise universellement. Cela revient à dire qu'elle est réalisée modulo toute structure de réalisabilité, ou encore qu'elle est conséquence de $\mathrm{Th}(\mathcal{S})$ pour toute $\mathcal{S}$.

On dira que deux formules $A(\overline{x})$ et $B(\overline{x})$ sont *universellement équivalentes* si la formule $\forall \overline{x}\ (A \leftrightarrow B)$ est universellement réalisée.

2.9 Formules préservées par réalisabilité classique

On va voir que les modèles de réalisabilité héritent automatiquement certaines propriétés du modèle de départ $\mathcal{M}$.

2.9.1 Axiomes de la théorie des ensembles

La classe la plus importante de propriétés préservées par réalisabilité classique est celles des axiomes de la théorie des ensembles. Pour être précis, en utilisant les axiomes de la théorie des ensembles $\mathcal{M}$ (voir annexe B), on va montrer que les axiomes de ZF_ε sont universellement réalisés.

Certains des axiomes de ZF_ε sont des axiomes d'existence : ils disent que dans une situation donnée, il existe un ensemble avec certaines propriétés. Pour les réaliser, l'idée est de construire explicitement un nom pour l'ensemble en question. Il faut tout de même garder à l'esprit que (contrairement à ce qui se passe dans les modèles de forcing) tous les éléments du modèle de réalisabilité ne sont pas nommés, au sens où, pour certaines structures de réalisabilité, il est possible de trouver une formule $A(x)$ telle que $\exists x\ A(x)$ soit réalisée mais que $\neg A(b)$ soit réalisée pour tout $b \in \mathcal{M}$ (on verra un exemple au chapitre 3). En revanche, pour tout objet x du modèle de réalisabilité, on peut bien nommer le singleton $\{x\}$:

Proposition 2.26 (Nommage des singletons)**.** Pour toute formule $A(\overline{w}^n, x)$, il existe une $\mathcal{M}$-fonctionnelle $s_A : \mathcal{S}_0 \times \mathcal{M}^n \to \mathcal{M}$ telle que les formules suivantes soient universellement réalisées :

— $\forall \overline{w}\ \forall x\ (x\ \varepsilon\ s_A(\overline{w}) \to A(\overline{w}, x))$,

— $\forall \overline{w}\ (\exists x\ A(\overline{w}, x) \to \exists x\ (x\ \varepsilon\ s_A(\overline{w})))$.

En particulier, lorsque $A(\overline{w}, x)$ définit un singleton, le terme $s_A(\overline{w})$ désigne ce singleton.

Démonstration. L'idée naturelle serait de simplement poser $s_A(\bot\!\!\bot, \overline{w}) = \{ (x, \pi); \pi \in \|\neg A(\overline{w}, x)\|_{\bot\!\!\bot}, x \in \mathcal{M} \}$, mais l'ensemble ainsi défini n'est pas nécessairement un $\mathcal{M}$-ensemble (il peut s'agir d'une $\mathcal{M}$-classe propre).

À la place, on va construire la $\mathcal{M}$-fonctionnelle s_A de façon à ce que $\neg A(\overline{w}, x) \leqq a \not\in s_A(\overline{w})$ (donc l'identité réalise $\forall \overline{w}\ \forall x\ ((A(\overline{w}, x) \to \bot) \to x \not\in s_A(\overline{w}))$, qui est équivalente à la première formule) et $\forall x\ (x \not\in s_A(\overline{w})) \equiv \forall x\ (A(\overline{w}, x) \to \bot)$ (donc l'identité réalise $\forall \overline{w}\ (\forall x\ (x \not\in s_A(\overline{w})) \to \forall x\ (A(\overline{w}, x) \to \bot))$, qui est équivalente à la seconde).

En utilisant l'axiome du choix global dans $\mathcal{M}$, on construit une $\mathcal{M}$-fonctionnelle partielle $a : \mathcal{S}_0 \times \mathcal{M}^n \times \Lambda \nrightarrow \mathcal{M}$ telle que pour tout pôle $\bot\!\!\bot$, tous $\overline{w} \in \mathcal{M}$ et tout $t \in \Lambda$, $a(\bot\!\!\bot, \overline{w}, t)$ est un élément de la $\mathcal{M}$-classe $\{x \in \mathcal{M}; t \Vdash_{\bot\!\!\bot} A(\overline{w}, x)\}$ si celle-ci est non vide, et $a(\bot\!\!\bot, \overline{w}, t)$ est non défini sinon.

On pose maintenant $s_A(\bot\!\!\bot, \overline{w}) = \{ (a(\bot\!\!\bot, \overline{w}, t), t \cdot \pi); \pi \in \Pi, t \in \Lambda$ tel que $a(\bot\!\!\bot, \overline{w}, t)$ est défini $\}$.

On peut alors vérifier que pour tout $x \in \mathcal{M}$, $\neg A(\overline{w}, x) \leqq x \not\in s_A(\overline{w})$ et $\forall x\ (x \not\in s_A(\overline{w})) \equiv \forall x\ (A(\overline{w}, x) \to \bot)$. □

Proposition 2.27. Toute formule prouvable dans ZF_ε est universellement réalisée.

Corollaire. Pour toute structure de réalisabilité $\mathcal{S}$, ZF_ε est contenue dans $\mathrm{Th}(\mathcal{S})$.

Preuve de la proposition 2.27. Il suffit de montrer que tous les axiomes de ZF_ε sont universellement réalisés.

Pour l'axiome de définition de $\in$ ($\forall a \forall b\ (a \in b \leftrightarrow \exists a' \varepsilon b\ (a' \approx a))$), il suffit de montrer que les formules $\forall a'\ (a \subsetneqq a' \to a' \subsetneqq a \to a' \not\in b)$ et $a \notin b$ sont universellement équivalentes, ce qui est le cas car $\forall a'\ (a \subsetneqq a' \to a' \subsetneqq a \to a' \not\in b) \equiv a \notin b$.

Pour l'axiome de définition de $\subsetneqq$ ($\forall a \forall b\ (a \subsetneqq b \leftrightarrow \forall x \varepsilon a\ (x \in b))$) il suffit de montrer que les formules $\forall x\ (x \in b \to x \not\in a)$ et $a \subsetneqq b$ sont universellement équivalentes, ce qui est le cas car $\forall x\ (x \in b \to x \not\in a) \equiv a \subsetneqq b$.

L'axiome d'introduction de l'égalité ($\forall a\ (a \neq a \to \bot)$) est universellement réalisé par l'identité ($\lambda x.x$) (car $a \neq a \equiv \bot$).

Pour toute formule $A(\overline{w}, x)$, l'axiome d'élimination de l'égalité pour A (c'est-à-dire $\forall \overline{w}\ \forall a \forall b\ (a = b \to A(\overline{w}, a) \to A(\overline{w}, b))$) est universellement réalisé par le terme $\theta = \lambda e.\ \lambda t.\ \mathrm{cc}(\lambda k.\ e(kt))$. En effet, soient $\bot\!\!\bot$ un pôle, $\overline{w}, a, b \in \mathcal{M}$, $e \Vdash_{\bot\!\!\bot} a \neq b \to \bot$, $t \Vdash_{\bot\!\!\bot} A(\overline{w}, a)$ et $\pi \in \|A(\overline{w}, b)\|_{\bot\!\!\bot}$. Le terme $k_\pi t$ réalise $a \neq b$ car si $a = b$, $\pi \in \|A(\overline{w}, a)\|_{\bot\!\!\bot}$ et donc $k_\pi t$ réalise $\bot$. On a donc $\theta \star e \cdot t \cdot \pi \succ_{\mathrm{K}} e \star k_\pi t \cdot \pi \in \bot\!\!\bot$.

Pour toute formule $A(\overline{w}, x)$, l'axiome de fondation pour A est logiquement équivalent à la formule $\forall \overline{w}$ $(\forall x\ (\forall y\ (\neg A(\overline{w}, y) \to y \not\in x) \to \neg A(\overline{w}, x) \to \bot) \to \forall x\ (\neg A(\overline{w}, x) \to \bot))$, et celle-ci est réalisée par le combinateur de point fixe de Turing $\theta = \delta\delta$, où $\delta = \lambda d.\ \lambda t.\ t(ddt)$. En effet, soient $\bot\!\!\bot$ un pôle, $\overline{w} \in \mathcal{M}$ et $t \Vdash_{\bot\!\!\bot} \forall x\ (\forall y\ (\neg A(\overline{w}, y) \to y \not\in x) \to \neg A(\overline{w}, x) \to \bot)$. On va montrer par induction sur le rang de a que pour tout $a \in \mathcal{M}$, pour tout $u \Vdash_{\bot\!\!\bot} \neg A(\overline{w}, a)$ et tout $\pi \in \Pi$, $\theta \star t \cdot u \cdot \pi \in \bot\!\!\bot$. Soit $a \in \mathcal{M}$ de rang minimal ne vérifiant pas cette propriété. Soient $u \Vdash_{\bot\!\!\bot} \neg A(\overline{w}, a)$ et $\pi \in \Pi$ tels que $\theta \star t \cdot u \cdot \pi \notin \bot\!\!\bot$. On constate que $\theta \star t \cdot u \cdot \pi \succ_{\mathrm{K}} t \star \theta t \cdot u \cdot \pi$, par conséquent $t \star \theta t \cdot u \cdot \pi \notin \bot\!\!\bot$, or t réalise $\forall y\ (\neg A(\overline{w}, y) \to y \not\in a) \to \neg A(\overline{w}, a) \to \bot$ et u réalise $\neg A(\overline{w}, a)$, par conséquent θt ne réalise pas $\forall y\ (\neg A(\overline{w}, y) \to y \not\in a)$, donc il existe $(b, \pi') \in a$ et $v \Vdash \neg A(\overline{w}, b)$ tels que $\theta \star t \cdot v \cdot \pi' \notin \bot\!\!\bot$, ce qui contredit la minimalité de a puisque le rang de b est plus petit que celui de a.

Chacun des axiomes restant impose l'existence d'un objet. Pour montrer qu'ils sont réalisés, l'idée sera de construire à chaque fois un nom explicite pour l'objet en question.

Pour toute formule $A(\overline{w}^n, x)$ et toute $\mathcal{M}$-fonctionnelle $h_A : \mathcal{S}_0 \times \mathcal{M}^{n+1} \to \mathcal{M}$, l'axiome de compréhension pour A est conséquence de la formule $\forall \overline{w}\ \forall a\ \forall x\ (x \not\in h_A(\overline{w}, a) \leftrightarrow (A(\overline{w}, x) \to x \not\in a))$. Il suffit donc de construire h_A telle que $x \not\in h_A(\overline{w}, a) \equiv A(\overline{w}^n, x) \to x \not\in a$. Pour cela, il suffit de poser $h_A(\bot\!\!\bot, \overline{w}, a) = \{ (x, t \cdot \pi); t \Vdash_{\bot\!\!\bot} A(\overline{w}, x), (x, \pi) \in a \}$.

Pour toute $\mathcal{M}$-fonctionnelle $c : \mathcal{S}_0 \times \mathcal{M}^2 \to \mathcal{M}$, l'axiome de la paire est conséquence de la théorie $\{ \forall a\ \forall b\ (a\ \varepsilon\ c(a, b)), \forall a\ \forall b\ (b\ \varepsilon\ c(a, b)) \}$, il suffit donc de construire c telle que ces deux formules soient

universellement réalisées. Pour cela, il suffit de poser $c(\perp\!\!\!\perp, a, b) = \{\ (a, \pi);\ \pi \in \Pi\ \} \cup \{\ (b, \pi);\ \pi \in \Pi\ \}$. En effet, on a alors $a \notin c(a, b) \equiv \bot$ et $b \notin c(a, b) \equiv \bot$.

Pour toute $\mathcal{M}$-fonctionnelle $u : \mathcal{S}_0 \times \mathcal{M} \to \mathcal{M}$, l'axiome de l'union est conséquence de la formule $\forall a\ \forall x\ \forall y\ (y \notin u(a) \to y\ \varepsilon\ x \to x \notin a)$. Il suffit donc de construire u telle que cette formule soit réalisée. Pour cela, on pose $u(\perp\!\!\!\perp, a) = \{\ (y, k_\pi \star \pi');\ (y, \pi') \in x, (x, \pi) \in a\ \}$. La formule $\forall a\ \forall x\ \forall y\ (y \notin u(a) \to y\ \varepsilon\ x \to x \notin a)$ est alors universellement réalisée par le terme $\beta = \lambda t.\ \lambda v.\ cc(\lambda k.\ v(tk))$. En effet, soient $\perp\!\!\!\perp$ un pôle, $a, x, y \in \mathcal{M}$, $t \Vdash_{\perp\!\!\!\perp} y \notin u(a)$, $v \Vdash y\ \varepsilon\ x$ et $\pi \in \|x\ \varepsilon\ a\|_{\perp\!\!\!\perp}$. On a $\beta \star t \star v \star \pi \succ_K v \star tk_\pi \star \pi$. Comme $(x, \pi) \in a$, tk_π réalise $y \notin x$, et donc $v \star tk_\pi \star \pi \in \perp\!\!\!\perp$.

Pour les axiomes de collection, de l'infini et des parties, il y a une difficulté supplémentaire, car il faudra s'assurer que le nom que l'on construit est bien un $\mathcal{M}$-ensemble et non une $\mathcal{M}$-classe propre. Pour les deux premiers, on utilisera le lemme de nommage des singletons (proposition 2.26), et pour le dernier, il faudra simplement être soigneux.

Pour toute formule $A(\overline{w}^n, x, y)$ et toutes $\mathcal{M}$-fonctionnelles $r_A, s_A : \mathcal{S}_0 \times \mathcal{M}^{n+1} \to \mathcal{M}$, l'axiome de collection pour A est conséquence de la formule $\forall \overline{w}\ \forall a\ \forall x \varepsilon a\ (s_A(\overline{w}, x)\ \varepsilon\ r_A(\overline{w}, a) \wedge (\exists y\ A(\overline{w}, x, y) \to \exists y \varepsilon s_A(\overline{w}, x)\ A(\overline{w}, x, y)))$ et de l'axiome de l'union. Soit $s_A : \mathcal{S}_0 \times \mathcal{M}^{n+1} \to \mathcal{M}$ la $\mathcal{M}$-fonctionnelle donnée par le lemme de nommage des singletons (proposition 2.26) pour $A(\overline{w}, x, y)$. Ainsi, les formules $\forall \overline{w}\ \forall x\ \forall y\ (y\ \varepsilon\ s_A(\overline{w}, x) \to A(\overline{w}, x, y))$ et $\forall \overline{w}\ \forall x\ (\exists y\ A(\overline{w}, y)) \to \exists y\ (y\ \varepsilon\ s_A(\overline{w}, x))$ sont universellement réalisées, donc la formule $\forall \overline{w}\ \forall x\ (\exists y\ A(\overline{w}, y)) \to \exists y \varepsilon s_A(\overline{w}, x)\ A(\overline{w}, x, y))$ est universellement réalisée. Il ne reste plus qu'à poser $r_A(\perp\!\!\!\perp, \overline{w}, a) = \{\ (s_A(\overline{w}, x), \pi);\ (x, \pi) \in a\ \}$ pour que $\forall \overline{w}\ \forall a\ \forall x \varepsilon a\ (s_A(\overline{w}, x)\ \varepsilon\ r_A(\overline{w}, a))$ soit universellement réalisée.

Soit $A(\overline{w}^n, x, y)$ une formule. Pour toute $\mathcal{M}$-fonctionnelle $\iota_A : \mathcal{S}_0 \times \mathcal{M}^{n+1} \to \mathcal{M}$, l'axiome de l'infini pour A est conséquence de la théorie $\{\ \forall \overline{w}\ \forall a\ (a\ \varepsilon\ \iota_A(\overline{w}, a)), \forall \overline{w}\ \forall a\ \forall x\ (x\ \varepsilon\ \iota_A(\overline{w}, a) \to \exists y\ A(\overline{w}, x, y) \to \exists y\ \varepsilon\ \iota_A(\overline{w}, a)\ A(\overline{w}, x, y))\ \}$. Notons de nouveau s_A la $\mathcal{M}$-fonctionnelle donnée par le lemme de nommage des singletons (proposition 2.26) pour $A(\overline{w}, x, y)$. Posons $\iota_{A,0}(\perp\!\!\!\perp, \overline{w}, a) = \{\ (a, \pi);\ \pi \in \Pi\ \}$ et pour tout $m \in \mathbb{N}$, $\iota_{A,m+1}(\perp\!\!\!\perp, \overline{w}, a) = \iota_{m,A}(\perp\!\!\!\perp, \overline{w}, a) \cup \{\ (y, k_\pi \star \pi');\ (y, \pi') \in s_A(\overline{w}, x), (x, \pi) \in \iota_{A,m}(\perp\!\!\!\perp, \overline{w}, a)\ \}$. Enfin, posons $\iota_A(\perp\!\!\!\perp, \overline{w}, a) = \bigcup_{m \in \mathbb{N}} \iota_{A,m}(\perp\!\!\!\perp, \overline{w}, a)$. La formule $\forall a\ \forall x\ \forall y\ (y \notin \iota_A(\overline{w}, a) \to y\ \varepsilon\ s_A(\overline{w}, x) \to x \notin \iota_A(\overline{w}, a))$ est alors universellement réalisée par le terme $\beta = \lambda t.\ \lambda v.\ cc(\lambda k.\ v(tk))$ (on a montré un résultat similaire pour l'axiome de l'union, et la même preuve fonctionne ici). Par conséquent, la formule $\forall \overline{w}\ \forall a\ \forall x\ (x\ \varepsilon\ \iota_A(\overline{w}, a) \to \exists y\ A(\overline{w}, x, y) \to \exists y\ \varepsilon\ \iota_A(\overline{w}, a)\ A(\overline{w}, x, y))$ est universellement réalisée. Comme par ailleurs la formule $\forall \overline{w}\ \forall a\ (a\ \varepsilon\ \iota_A(\overline{w}, a))$ est universellement réalisée (car $a \notin \iota_A(\overline{w}, a) \equiv \bot$), l'axiome de l'infini pour A est universellement réalisé.

Pour toute formule $A(\overline{w}^n, x, y)$ et toutes $\mathcal{M}$-fonctionnelles $q : \mathcal{S}_0 \times \mathcal{M} \to \mathcal{M}$ et $f : \mathcal{S}_0 \times \mathcal{M}^2 \to \mathcal{M}$, l'axiome des parties est conséquence de la théorie $\{\ \forall a\ \forall z\ (f(a, z)\ \varepsilon\ q(a)), \forall a\ \forall z\ \forall x\ (x\ \varepsilon\ f(a, z) \leftrightarrow (x\ \varepsilon\ z \wedge x\ \varepsilon\ a))\ \}$, qui est elle-même conséquence de la théorie $\{\ \forall a\ \forall z\ (f(a, z)\ \varepsilon\ q(a)), \forall a\ \forall z\ \forall x\ (x \notin f(a, z) \leftrightarrow (x\ \varepsilon\ z \to x \notin a))\ \}$. On pose $f(\perp\!\!\!\perp, a, z) = \{\ (x, t \star \pi);\ t \Vdash_{\perp\!\!\!\perp} x\ \varepsilon\ z, (x, \pi) \in a\ \}$: on a alors $x \notin f(a, z) \equiv x\ \varepsilon\ z \to x \notin a$. Par ailleurs, pour tous $\perp\!\!\!\perp, a, z$, on a $f(\perp\!\!\!\perp, a, z) \in \mathcal{P}_{\mathcal{M}}(\{\ (x, \pi'); (x, \pi) \in a, \pi' \in \Pi\ \})$, donc si l'on pose $q(\perp\!\!\!\perp, a) = \{\ (f(\perp\!\!\!\perp, a, z), \pi);\ z \in \mathcal{M}, \pi \in \Pi\ \}$, $q(\perp\!\!\!\perp, a)$ est bien un $\mathcal{M}$-ensemble (et pas une $\mathcal{M}$-classe propre), donc q est bien une $\mathcal{M}$-fonctionnelle. D'autre part, la formule $\forall a\ \forall z\ (f(a, z)\ \varepsilon\ q(a))$ est bien universellement réalisée (car $f(a, z) \notin q(a) \equiv \bot$), donc l'axiome des parties est universellement réalisé.

□

2.9.2 Clauses de Horn

Une autre classe de formules préservées par réalisabilité classique est celle des clauses de Horn (qui contient en particulier les équations et les inéquations) :

Définition 2.28. Une *clause de Horn* est une formule close de la forme $\forall \overline{x}\ (E_1 \to \ldots \to E_n \to G)$, où chaque E_i est de la forme $a_i = b_i$ et G est soit de la forme $c = d$ (*clause définie*), soit de la forme $c \neq d$ (*clause négative*).

Pour tout pôle $\perp\!\!\!\perp$, on dit que H est *vraie modulo* $\perp\!\!\!\perp$ si pour tous $\overline{w} \in \mathcal{M}$ tels que $[a_i[\overline{x} := \overline{w}]]_{\perp\!\!\!\perp} = [b_i[\overline{x} := \overline{w}]]_{\perp\!\!\!\perp}$ pour tout i, on a $[c[\overline{x} := \overline{w}]]_{\perp\!\!\!\perp} = [d[\overline{x} := \overline{w}]]_{\perp\!\!\!\perp}$ si H est définie, et $[c[\overline{x} := \overline{w}]]_{\perp\!\!\!\perp} \neq [d[\overline{x} := \overline{w}]]_{\perp\!\!\!\perp}$

si H est négative[i]. Sinon, on dit que H est *fausse modulo* $\perp\!\!\!\perp$.

Pour toute structure de réalisabilité $\mathcal{S}$, on dit que H est *vraie modulo* $\mathcal{S}$ si H est vraie modulo $\perp\!\!\!\perp$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$, et que H est *fausse modulo* $\mathcal{S}$ si H est fausse modulo $\perp\!\!\!\perp$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$

Enfin, on dit que H est *vraie* si elle est vraie modulo $\mathcal{S}_0$, et *fausse* si elle est fausse modulo $\mathcal{S}_0$.

Notation (Implication équationnelle)**.** Soient A une formule et b, c deux termes du premier ordre. On note $b = c \hookrightarrow A$ la formule $(b \neq c) \cup A$.

Ainsi, lorsque A, b et c sont clos, pour tout pôle $\perp\!\!\!\perp$, $\|b = c \hookrightarrow A\|_{\perp\!\!\!\perp} = \begin{cases} \|A\|_{\perp\!\!\!\perp} & \text{si } [a]_{\perp\!\!\!\perp} = [b]_{\perp\!\!\!\perp} \\ \emptyset & \text{sinon} \end{cases}$.

Lemme 2.29. Pour toute formule A et tous termes du premier ordre b et c, les formules $b = c \hookrightarrow A$ et $b = c \to A$ sont universellement équivalentes.

Démonstration. On peut supposer sans perte de généralité que A, b et c sont clos (à condition que les réalisateurs que l'on obtient ne dépendent pas de A, b et c).

Montrons que l'implication de gauche à droite est réalisée par le terme $\delta = \lambda t.\ \lambda e.\ cc(\lambda k.\ e(kt))$. Soient $\perp\!\!\!\perp$ un pôle, $t \Vdash_{\perp\!\!\!\perp} b = c \hookrightarrow A$, $e \Vdash_{\perp\!\!\!\perp} b = c$ et $\pi \in \|A\|_{\perp\!\!\!\perp}$. On a $\delta \star t \cdot e \cdot \pi \succ_K e \star k_\pi t \cdot \pi$, donc il suffit de montrer que $k_\pi t$ réalise $b \neq c$. Si $b = c$, alors t réalise A, donc $k_\pi t$ réalise $\perp$. Si $b \neq c$, alors $b \neq c \equiv_{\perp\!\!\!\perp} \top$, donc $k_\pi t$ réalise $b \neq c$.

Montrons que l'implication de droite à gauche est réalisée par $\gamma = \lambda u.\ u(\lambda x.\ x)$. Soient $\perp\!\!\!\perp$ un pôle, $u \Vdash_{\perp\!\!\!\perp} b = c \to A$, et $\pi \in \|b = c \hookrightarrow A\|_{\perp\!\!\!\perp}$. On a $\gamma \star u \cdot \pi \succ_K u \star (\lambda x.\ x) \cdot \pi$, donc il suffit de montrer que $\lambda x.\ x$ réalise $b = c$. Comme $\pi \in \|b = c \hookrightarrow A\|_{\perp\!\!\!\perp}$, on doit avoir $\|b = c \hookrightarrow A\|_{\perp\!\!\!\perp} \neq \emptyset$, donc $[b]_{\perp\!\!\!\perp} = [c]_{\perp\!\!\!\perp}$, et par conséquent $b = c \equiv_{\perp\!\!\!\perp} \perp \to \perp$. □

Proposition 2.30 (Préservation des clauses de Horn)**.** Soient H une clause de Horn et $\mathcal{S}$ une structure de réalisabilité. Si H est vraie modulo $\mathcal{S}$ alors H est réalisée modulo $\mathcal{S}$, et si H est fausse modulo $\mathcal{S}$ alors $\neg H$ est réalisée modulo $\mathcal{S}$.

Démonstration. H est de la forme $\forall \overline{x}\ ((a_1(\overline{x}) = b_1(\overline{x})) \to \ldots \to (a_n(\overline{x}) = b_n(\overline{x})) \to G(\overline{x}))$, avec $G(\overline{x})$ de la forme $c(\overline{x}) = d(\overline{x})$ ou $c(\overline{x}) \neq d(\overline{x})$.

D'après le lemme 2.29, H est universellement équivalente à la formule $\forall \overline{x}\ ((a_1(\overline{x}) = b_1(\overline{x})) \hookrightarrow \ldots \hookrightarrow (a_n(\overline{x}) = b_n(\overline{x})) \hookrightarrow G(\overline{x}))$, que l'on notera $\widetilde{H}$.

Il suffit alors de vérifier par le calcul que si H est définie et vraie modulo $\mathcal{S}$ alors $\widetilde{H} \geqq_{\mathcal{S}} \perp \to \perp$, que si H est définie et fausse modulo $\mathcal{S}$ alors $\widetilde{H} \equiv_{\mathcal{S}} \top \to \perp$, gue si H est négative et vraie modulo $\mathcal{S}$, alors $\widetilde{H} \equiv_{\mathcal{S}} \top$, et que si H est négative et fausse modulo $\mathcal{S}$, alors $\widetilde{H} \equiv_{\mathcal{S}} \perp$. □

2.9.3 Bonne fondation

Enfin, on peut montrer que toute relation bien fondée dans $\mathcal{M}$ donne une relation bien fondée dans le modèle de réalisabilité :

Définition 2.31. Une $\mathcal{M}$-relationnelle binaire $\lessdot$ est *$\mathcal{M}$-bien fondée* si pour tout $\mathcal{M}$-ensemble non vide A, A possède un élément *$\lessdot$-minimal*, c'est-à-dire qu'il existe $x \in A$ tel que pour tout $y \in A$, $y \not\lessdot x$.

Lemme 2.32. Soit $\lessdot$ une $\mathcal{M}$-relationnelle binaire $\mathcal{M}$-bien-fondée. Pour toute $\mathcal{M}$-classe non vide A, il existe $x \in A$ $\lessdot$-minimal dans A.

Démonstration. Supposons par l'absurde que A n'a pas d'élément $\lessdot$-minimal, c'est-à-dire que pour tout $x \in A$, il existe $y \in A$ tel que $y \lessdot x$. Pour tout $x \in A$, notons $f(x)$ le $\mathcal{M}$-ensemble des y *de rang ensembliste*

i. Ce qui est *a priori* très différent de dire que H est *réalisée* modulo $\perp\!\!\!\perp$.

minimal tels que $y \prec x$, et pour tout $X \in \mathcal{M}$ tel que $X \subseteq A$, notons $F(X) = \bigcup_{x \in X} f(x)$: ainsi, pour tout $x \in X$, il existe $y \in F(X)$ tel que $y \prec x$. Enfin, prenons $a \in A$ quelconque et posons $B = \bigcup_{n \in \mathbb{N}} F^n(\{a\})$: B est un $\mathcal{M}$-ensemble qui ne contient pas d'élément $\prec$-minimal. □

Proposition 2.33. Soient $\mathcal{S}$ une structure de réalisabilité, $\prec$ une $\mathcal{M}$-relationnelle binaire et $R_\prec(x, y)$ une formule. Si $\prec$ est bien fondée et si pour tous $x, y \in \mathcal{M}$ tels que $y \not\prec x$, $R_\prec(y, x) \equiv_\mathcal{S} \top$, alors pour toute formule $A(\overline{w}, x)$, la formule

$$\forall \overline{w}\ (\forall x\ (\forall y\ (\neg R_\prec(y, x) \to A(\overline{w}, y)) \to A(\overline{w}, x)) \to \forall x\ A(\overline{w}, x))$$

(qui dit que $\neg R_\prec(y, x)$ définit une relation bien fondée) est réalisée modulo $\mathcal{S}$.

Démonstration. Il s'agit d'une généralisation du schéma d'axiomes de fondation de ZF_ϵ (qui correspond au cas où l'on a $x \prec y$ si et seulement si le rang de x est strictement plus petit que y et où $R_\prec(x, y)$ désigne la formule $x \notin y$). On va donc employer une preuve presque identique.

La formule que l'on cherche à réaliser est logiquement équivalente à la formule $\forall \overline{w}\ (\forall x\ (\forall y\ (\neg A(\overline{w}, y) \to R_\prec(y, x)) \to \neg A(\overline{w}, x) \to \bot) \to \forall x\ (\neg A(\overline{w}, x) \to \bot))$, et elle-ci est réalisée par le combinateur de point fixe de Turing $\theta = \delta\delta$, où $\delta = \lambda d.\ \lambda t.\ t(ddt)$. En effet, soient $\perp\!\!\!\perp \in \mathcal{S}$, $\overline{w} \in \mathcal{M}$ et $t \Vdash_{\perp\!\!\!\perp} \forall x\ (\forall y\ (\neg A(\overline{w}, y) \to R_\prec(y, x)) \to \neg A(\overline{w}, x) \to \bot)$. Supposons par l'absurde qu'il existe $x \in \mathcal{M}$, $u \Vdash_{\perp\!\!\!\perp} \neg A(\overline{w}, x)$ et $\pi \in \Pi$ tels que $\theta \star t \bullet u \bullet \pi \notin \perp\!\!\!\perp$. Comme $\prec$ est $\mathcal{M}$-bien-fondée, on peut supposer x $\prec$-minimal pour cette propriété.

On constate que $\theta \star t \bullet u \bullet \pi \succ_K t \star \theta t \bullet u \bullet \pi$, par conséquent $t \star \theta t \bullet u \bullet \pi \notin \perp\!\!\!\perp$, or t réalise $\forall y\ (\neg A(\overline{w}, y) \to R_\prec(y, x)) \to \neg A(\overline{w}, x) \to \bot$ et u réalise $\neg A(\overline{w}, x)$, par conséquent θt ne réalise pas $\forall y\ (\neg A(\overline{w}, y) \to y \notin a)$, donc il existe $y \in \mathcal{M}$ et $\pi' \in \|R_\prec(y, x)\|_{\perp\!\!\!\perp}$ et $v \Vdash \neg A(\overline{w}, y)$ tels que $\theta \star t \bullet v \bullet \pi' \notin \perp\!\!\!\perp$. Ceci contredit la $\prec$-minimalité de x, car $\pi' \in \|R_\prec(y, x)\|_{\perp\!\!\!\perp}$ implique $\|R_\prec(y, x)\| \not\equiv_{\perp\!\!\!\perp} \top$, et donc $y \prec x$. □

2.10 Interprétation dans $\mathcal{M}$ des formules strictement extensionnelles

Puisque les formules strictement extensionnelles sont les formules usuelles de la théorie des ensembles, on doit pouvoir les interpréter dans $\mathcal{M}$:

Notation. Pour toute formule strictement extensionnelle A et toute liste $\overline{x}^n$ de variables du premier ordre contenant au moins les variables libres de A, on note $\langle A(\overline{x}^n) \rangle_\mathcal{M}$ la $\mathcal{M}$-fonctionnelle de $\mathcal{S}_0 \times \mathcal{M}^n$ dans $\mathcal{M}$ définie de façon suivante :

— $\langle (a \subsetneq b)(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}) = \begin{cases} 1 & \text{si } [a(\overline{w})]_{\perp\!\!\!\perp} \subseteq [b(\overline{w})]_{\perp\!\!\!\perp} \\ 0 & \text{sinon,} \end{cases}$

— $\langle (a \not\in b)(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}) = \begin{cases} 1 & \text{si } [a(\overline{w})]_{\perp\!\!\!\perp} \not\in [b(\overline{w})]_{\perp\!\!\!\perp} \\ 0 & \text{sinon,} \end{cases}$

— $\langle \top(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}) = 1$,

— $\langle \bot(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}) = 0$,

— $\langle (A \to B)(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}) = \begin{cases} 1 & \text{si } \langle A(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}) = 0 \text{ ou } \langle B(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp \overline{w}) = 1 \\ 0 & \text{sinon,} \end{cases}$

— $\langle (\forall y\ A)(\overline{x}) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}) = \begin{cases} 1 & \text{si } \langle A(\overline{x}, y) \rangle_\mathcal{M} (\perp\!\!\!\perp, \overline{w}, v) = 1 \text{ pour tout } v \in \mathcal{M} \\ 0 & \text{sinon.} \end{cases}$

De plus, pour toute formule strictement extensionnelle A, on s'autorise à noter simplement $\langle A \rangle_\mathcal{M}$ le terme du premier ordre $\langle A(\overline{x}) \rangle_\mathcal{M} (\overline{x})$, où $\overline{x}$ désigne la liste des variables libres de A.

2.11 Le pôle vide

Le pôle vide a un statut particulier, car le modèle de réalisabilité associé est isomorphe à $\mathcal{M}$ (du point de vue extensionnel) :

Proposition 2.34. Pour toute formule close A, $|A|_\emptyset = \emptyset = |\bot|_\emptyset$ ou $|A|_\emptyset = \Lambda = |\top|_\emptyset$. De plus :

— pour toutes formules closes A et B, $|A \to B|_\emptyset = \begin{cases} \Lambda & \text{si } |A|_\emptyset = \emptyset \text{ ou } |B|_\emptyset = \Lambda, \\ \emptyset & \text{sinon,} \end{cases}$

— pour toute formule $A(x)$, $|\forall x\ A(x)|_\emptyset = \begin{cases} \Lambda & \text{s'il existe } b \in \mathcal{M} \text{ tel que } |A(b)|_\emptyset = \Lambda, \\ \emptyset & \text{sinon.} \end{cases}$

Enfin, il existe une $\mathcal{M}$-fonctionnelle surjective $p : \mathcal{M} \to \mathcal{M}$ telle que :

— pour tous $a, b \in \mathcal{M}$, $|a \notin b|_\emptyset = \begin{cases} \Lambda & \text{si } p(a) \notin p(b), \\ \emptyset & \text{si } p(a) \in p(b), \end{cases}$

— pour tous $a, b \in \mathcal{M}$, $\left|a \subsetneq b\right|_\emptyset = \begin{cases} \Lambda & \text{si } p(a) \subsetneq p(b), \\ \emptyset & \text{si } p(a) \not\subsetneq p(b). \end{cases}$

Démonstration. Pour la première partie, il suffit de remarquer que pour tout $X \in \mathcal{P}_\mathcal{M}(\Pi)$, le dual de X modulo $\emptyset$ est Λ si X est vide, et $\emptyset$ sinon. Pour la deuxième, il suffit de poser inductivement $p(x) = \{\ p(y);\ (y, \pi) \in x, \pi \in \Pi\ \}$ et de raisonner par induction sur le rang de a et de b. □

Corollaire. Soit A une formule close strictement extensionnelle. La théorie $\mathrm{Th}\,(\{\emptyset\})$ prouve A si $\langle A \rangle_\mathcal{M}\,(\emptyset) = 1$ (c'est-à-dire si A est « vraie dans $\mathcal{M}$ ») et prouve $\neg A$ sinon.

Corollaire. Soient $\mathcal{S}$ une structure de réalisabilité contenant le pôle vide. Pour toute formule close strictement extensionnelle A, si $\mathrm{Th}\,(\{\emptyset\})$ prouve A alors $\langle A \rangle_\mathcal{M}\,(\emptyset) = 1$ (c'est-à-dire que A est « vraie dans $\mathcal{M}$ »).

3 L'algèbre de Boole caractéristique ⅁2

Chaque modèle de réalisabilité est muni d'une *algèbre de Boole caractéristique* ⅁2 dont la structure donne beaucoup d'information sur les propriétés du modèle. En particulier, les modèles de forcing correspondent au cas dégénéré ou ⅁2 est l'algèbre de Boole $\{0, 1\}$ [Kri18, Kri15].

Pour souligner le rôle central de l'algèbre de Boole caractéristique dans la théorie de la réalisabilité classique de Krivine, rappelons que cette dernière permet de construire des modèles de ZF dotés de propriétés ensemblistes surprenantes, qui découlent essentiellement de la structure de leur algèbre de Boole caractéristique (par exemple, le *modèle des threads* [Kri12]).

3.1 L'opérateur ⅁ *(gimel)*

L'idée est d'associer à chaque $\mathcal{M}$-ensemble X un $\mathcal{M}$-ensemble $⅁X$ tel que pour tout $x \in \mathcal{M}$, on puisse réaliser $x \ \varepsilon\ ⅁X$ si $x \in X$ et sa négation si $x \notin X$. L'opérateur ⅁ fonctionnerait donc comme une sorte de plongement de $\mathcal{M}$ dans les modèles de réalisabilité (à l'instar de l'opérateur « ˇ » pour le forcing). Cependant, on verra qu'à cause de l'existence d'éléments non nommés, il ne s'agit en réalité pas du tout d'un plongement, car même pour $X = 2 = \{0, 1\}$, les propriétés de $⅁X$ dans les modèles de réalisabilité peuvent être bien différentes de celles de X dans $\mathcal{M}$.

Notation. On note ⅁ la $\mathcal{M}$-fonctionnelle de $\mathcal{M}$ dans $\mathcal{M}$ qui à X associe $⅁X = \{\ (x, \pi);\ x \in X, \pi \in \Pi\ \}$.

Pour tous $x, X \in \mathcal{M}$, $x \ \varepsilon\ ⅁X$ est universellement réalisée si $x \in X$ (par l'identité $\lambda y.\ y$), et $x \not\varepsilon ⅁X$ est universellement réalisée si $x \notin X$ (par n'importe quel terme) : on a donc bien rempli l'objectif initial.

On va voir que les formules de la forme $a \ \varepsilon\ ⅁b$ se comportent comme des égalités, ce qui permettra d'utiliser les résultats de la section 2.9.2 pour les étudier.

Lemme 3.1. Pour tous termes du premier ordre a et b, $a \not\varepsilon ⅁b \equiv \langle a \in b \rangle_\mathcal{M} \neq 1$.

Par conséquent, tous les résultats qui s'appliquent aux égalités s'appliquent aux formules de la forme $a \in \mathfrak{I}b$, et tout ceux qui s'appliquent aux différences s'applique aux formules de la forme $a \notin \mathfrak{I}b$. En particulier, on étendra désormais la notion de clause de Horn pour autoriser des prémisses et des conclusions de la forme $a \in \mathfrak{I}A$ ainsi que des conclusions de la forme $a \notin \mathfrak{I}b$. La proposition 2.30 reste valable *mutatis mutandis*.

Remarque. Pour tout pôle $\perp\!\!\!\perp$, pour tous termes du premier ordre $a(\overline{w})$ et $b(\overline{w})$, la clause de Horn $\forall \overline{w}\ (a \in \mathfrak{I}b)$ est vraie modulo $\perp\!\!\!\perp$ si et seulement si pour tous $\overline{w} \in \mathcal{M}$, $[a(\overline{w})]_{\perp\!\!\!\perp} \in [b(\overline{w})]_{\perp\!\!\!\perp}$. De même, la clause de Horn $\forall \overline{w}\ (a \notin \mathfrak{I}b)$ est vraie modulo $\perp\!\!\!\perp$ si et seulement si pour tous $\overline{w} \in \mathcal{M}$, $[a(\overline{w})]_{\perp\!\!\!\perp} \notin [b(\overline{w})]_{\perp\!\!\!\perp}$.

En s'inspirant de la section 2.9.2, on peut également définir la notation $a \in \mathfrak{I}b \hookrightarrow A$:

Notation. Pour tous termes du premier ordre a et b et toute formule A, on note $a \in \mathfrak{I}b \hookrightarrow A$ la formule $\langle a \in b \rangle_{\mathcal{M}} = 1 \hookrightarrow A$ (autrement-dit, $a \in \mathfrak{I}b \hookrightarrow A \equiv (a \notin \mathfrak{I}b) \cup A$).

Ainsi, on peut définir une notation pour les quantifications relativisées à $\mathfrak{I}b$:

Notation. Pour tout terme du premier ordre b, toute formule A et toute variable du premier ordre x, on note $\forall x^{\mathfrak{I}b}\ A$ la formule $\forall x\ (x \in \mathfrak{I}b \hookrightarrow A)$.

Ainsi, pour tout terme clos du premier ordre b, toute formule $A(x)$ et tout pôle $\perp\!\!\!\perp$, on a $\left\|\forall x^{\mathfrak{I}b}\ A\right\|_{\perp\!\!\!\perp} = \bigcup_{x \in [b]_{\perp\!\!\!\perp}} \|A(x)\|_{\perp\!\!\!\perp}$, c'est-à-dire que $\pi \in \left\|\forall x^{\mathfrak{I}b}\ A\right\|_{\perp\!\!\!\perp}$ si et seulement s'il existe x *dans* $[b]_{\perp\!\!\!\perp}$ tel que $\pi \in \|A(x)\|_{\perp\!\!\!\perp}$.

D'après le lemme 2.29, ces notations font bien ce à quoi l'on s'attend :

Lemme 3.2. Pour tous termes du premier ordre a et b et toute formule A, les formules $a \in \mathfrak{I}b \hookrightarrow A$ et $a \in \mathfrak{I}b \to A$ sont universellement équivalentes.

Pour tout terme du premier ordre b, toute formule A et toute variable du premier ordre x, les formules $\forall x^{\mathfrak{I}b}\ A$ et $\forall x\ (x \in \mathfrak{I}b \to A)$ sont universellement équivalentes.

Enfin, une propriété essentielle de l'opérateur $\mathfrak{I}$ est qu'il se comporte comme une sorte de foncteur, au sens où chaque $\mathcal{M}$-fonctionnelle de $X_1 \times \ldots \times X_n$ dans Y donne dans les modèles de réalisabilité une fonctionnelle de $\mathfrak{I}X_1 \times \ldots \times \mathfrak{I}X_n$ dans $\mathfrak{I}Y$:

Proposition 3.3. Soient $\mathcal{S}$ une structure de réalisabilité, $a_1(\overline{w}), \ldots, a_n(\overline{w})$, $b(\overline{w})$ des termes du premier ordre et $f : \mathcal{S}_0 \times \mathcal{M}^n \to \mathcal{M}$ une $\mathcal{M}$-fonctionnelle. Si pour tout $\perp\!\!\!\perp \in \mathcal{S}$, tous $\overline{w} \in \mathcal{M}$ et tous $x_1 \in [a_1(\overline{w})]_{\perp\!\!\!\perp}, \ldots, x_n \in [a_n(\overline{w})]_{\perp\!\!\!\perp}$, $f(\perp\!\!\!\perp, x_1, \ldots, x_n) \in [b(\overline{w})]_{\perp\!\!\!\perp}$, alors la formule $\forall \overline{w}\ \forall x_1^{\mathfrak{I}a_1}\ \ldots\ \forall x_n^{\mathfrak{I}a_n}\ (f(x_1, \ldots, x_n) \in \mathfrak{I}b)$ est réalisée modulo $\mathcal{S}$.

Démonstration. Conséquence de la préservation des clauses de Horn (proposition 2.30). □

Comme conséquence de la proposition 2.30, on a également que pour chaque singleton $\{x\} = X \in \mathcal{M}$, la formule $\forall y\ (y \in \mathfrak{I}X \leftrightarrow y = x)$ est réalisée, autrement dit, $\mathfrak{I}X$ désigne bien le singleton contenant uniquement x. En revanche, dès que X a au moins deux éléments, la situation devient plus compliquée.

3.2 L'algèbre de Boole $\mathfrak{I}2$

On va donc chercher à étudier l'objet désigné par $\mathfrak{I}X$ quand X a deux éléments. Comme on a pris pour convention que pour tout $n \in \mathbb{N}$, $n = \{0, \ldots, n-1\}$, on va simplement étudier $\mathfrak{I}2$.

Tout d'abord, il faut clarifier ce que l'on entend lorsque l'on dit que $\mathfrak{I}2$ est une algèbre de Boole.

Dans $\mathcal{M}$, l'ensemble $2 = \{0, 1\}$ est muni d'opérations $\wedge$, $\vee$, $\neg$, 0 et 1 (on voit les constantes comme des opérations 0-aires), qui font de lui une algèbre de Boole. D'après la proposition 3.3, ces opérations se relèvent en des opérations sur $\mathfrak{I}2$: c'est $\mathfrak{I}2$ munie de ces opérations qui est une algèbre de Boole.

Pour $x, y \in \mathcal{M}$, on pose

— $x \wedge y = \begin{cases} 0 & \text{si } x = 0 \text{ ou } y = 0 \\ 1 & \text{sinon} \end{cases}$,

— $x \vee y = \begin{cases} 0 & \text{si } x = 0 \text{ et } y = 0 \\ 1 & \text{sinon} \end{cases}$,

— $\neg x = \begin{cases} 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases}$.

Ces trois $\mathcal{M}$-fonctionnelles définissent chacune un symbole de fonction du langage de réalisabilité.

Notation. Soit A une formule du langage des algèbres de Boole. On note $\mathbb{2} \models A$ la formule du langage de réalisabilité obtenue en remplaçant chaque symbole de fonction, chaque symbole de relation et chaque connecteur du langage des algèbres de Boole par son équivalent dans le langage de réalisabilité, et chaque $\forall$ par $\forall^{\mathbb{2}}$.

Proposition 3.4 ($\mathbb{2}$ est une algèbre de Boole à aux moins deux éléments)**.** Soit A une formule close du langage des algèbres de Boole (voir annexe A). Si A est vraie dans toute algèbre de Boole à au moins deux éléments, alors $\mathbb{2} \models A$ est universellement réalisée.

Démonstration. Soit $H_1, \dots, H_n$ la liste des axiomes des algèbres de Boole augmentée de l'axiome $0 \neq 1$. Toutes ces formules sont des clauses de Horn, et l'on peut vérifier que les formules $(\mathbb{2} \models H_1), \dots, (\mathbb{2} \models H_n)$ sont universellement équivalentes à des clauses de Horn, et que ces dernières sont vraies (essentiellement parce que les formules $H_1, \dots, H_n$ sont vraies dans l'algèbre de Boole $\{0, 1\}$). Le résultat découle donc du lemme d'adéquation et du théorème de complétude pour le langage des algèbres de Boole (proposition A.18). □

Notation (Équivalence et sous-typage sémantiques – Algèbres de Boole)**.** Soient $A(\overline{x})$ et $B(\overline{x})$ deux formules du langage des algèbres de Boole. Pour tout pôle $\perp\!\!\!\perp$, on note $A \equiv_{\perp\!\!\!\perp} B$ lorsque $\|\mathbb{2} \models A(\overline{c})\|_{\perp\!\!\!\perp} = \|\mathbb{2} \models B(\overline{c})\|_{\perp\!\!\!\perp}$ pour tous $\overline{c} \in \{0, 1\}$ et $A \leqq_{\perp\!\!\!\perp} B$ lorsque $\|\mathbb{2} \models A(\overline{c})\|_{\perp\!\!\!\perp} \supseteq \|\mathbb{2} \models B(\overline{c})\|_{\perp\!\!\!\perp}$ pour tous $\overline{c} \in \{0, 1\}$. De plus, pour toute structure de réalisabilité $\mathcal{S}$, on note $A \equiv_{\mathcal{S}} B$ lorsque $A \equiv_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$, et $A \leqq_{\mathcal{S}} B$ lorsque $A \leqq_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp \in \mathcal{S}$. Enfin, on note $A \equiv B$ lorsque $A \equiv_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp$, et $A \leqq B$ lorsque $A \leqq_{\perp\!\!\!\perp} B$ pour tout $\perp\!\!\!\perp$.

On va voir qu'étant donnée une structure de réalisabilité $\mathcal{S}$, la structure de l'algèbre de Boole caractéristique de ses modèles de réalisabilité (plus précisément, l'ensemble des formules A telle que $\mathbb{2} \models A$ soit réalisée) est liée à des propriétés de non-déterminisme sur $\succ_{\mathcal{S}}$.

3.3 Forme des formules et intersection

Pour toute formule F du langage des algèbres de Boole et toute variable x, on a $(\mathbb{2} \models F[x := 0]) \cap (\mathbb{2} \models F[x := 1]) \equiv (\mathbb{2} \models \forall x\, F)$. Cela veut dire que l'intersection, qui n'a a priori qu'une interprétation calculatoire et pas d'interprétation logique, peut dans certains cas être ré-interprétée comme une quantification universelle sur $\mathbb{2}$, qui elle en a une. Cette remarque sera le moteur du chapitre 4, et pour l'exploiter pleinement, on va préciser dans quel cas elle s'applique :

On dit que deux formules A et B du langage des algèbres de Boole ont *la même forme* s'il existe une formule F du langage des algèbres de Boole et une variable x telles que $A \equiv F[x := 0]$ et $B \equiv F[x := 1]$. Dans ce cas, on choisit arbitrairement une telle formule F et l'on note $A \cap B$ pour $\forall x\, F$. On peut vérifier que $(\mathbb{2} \models A \cap B) \equiv (\mathbb{2} \models A) \cap (\mathbb{2} \models B)$, et que par conséquent, la formule ainsi définie ne dépend pas *modulo* $\equiv$ de la formule F choisie. Cette nouvelle opération $\cap$ est compatible avec $\equiv$, et l'on fera attention à ne l'utiliser que dans des situations où seule sa valeur *modulo* $\equiv$ importe (c'est-à-dire des situations où le choix de F n'importe pas).

3.4 Le cardinal de $\beth 2$

L'une des propriétés de $\beth 2$ que l'on peut vouloir étudier est son cardinal. Dans cette section, on va développer quelques outils pour parler de ce cardinal.

Si $\mathbb{B}$ est une algèbre de Boole et n en entier naturel non nul, la formule $\forall x_1 \dots x_n \ \bigvee_{i \neq j}(x_i = x_j)$ est vraie dans $\mathbb{B}$ si et seulement si $\mathbb{B}$ a strictement moins de n éléments. Ceci justifie la notation suivante :

Notation (Cardinal de $\beth 2$)**.** Soit n un entier naturel non nul.

— On note $|\beth 2| < n$ (ou $|\beth 2| \leq n+1$) la formule $\beth 2 \models \forall x_1 \dots x_n \ \bigvee_{i \neq j}(x_i = x_j)$,

— On note $|\beth 2| \geq n$ la formule $(|\beth 2| < n) \to \bot$,

— On note $|\beth 2| = n$ la formule $(|\beth 2| \geq n) \wedge (|\beth 2| < n+1)$.

Remarque. Le cardinal d'une algèbre de Boole finie est toujours une puissance de 2. Par conséquent, d'après la proposition 3.4, pour tout entier naturel n, les formules $|\beth 2| \leq 2^n$ et $|\beth 2| < 2^{n+1}$ sont universellement équivalentes, et par conséquent, les formules $|\beth 2| = 2^n$ et $|\beth 2| \geq 2^n \wedge |\beth 2| < 2^{n+1}$ sont universellement équivalentes.

En général, une algèbre de Boole a au moins 2^n éléments si et seulement si elle contient une séquence de n éléments non nuls deux à deux disjoints [GH08, chapitre 15, conséquence du lemme 1]. Par conséquent, d'après la proposition 3.4, les formules « $\beth 2$ a au moins 2^n éléments » et « $\beth 2$ contient une séquence de n éléments non nuls deux à deux disjoints » doivent être universellement équivalentes. On utilisera plutôt la seconde formulation, car sa valeur de fausseté est plus simple à manipuler.

Notation. Pour tout entier naturel non nul n, notons $\mathcal{D}^n$ la formule suivante du langage des algèbres de Boole :

$$\forall x_1 \ \dots \ \forall x_n \ \left(x_1 \neq 0 \to \dots \to x_n \neq 0 \to \left(\bigvee_{i \neq j} x_i \wedge x_j \right) \neq 0 \right).$$

Pour toute algèbre de Boole $\mathbb{B}$, la formule $\mathcal{D}^n$ est vraie dans $\mathbb{B}$ si et seulement s'il n'est pas possible de trouver n éléments non nuls deux à deux disjoints dans $\mathbb{B}$. Par conséquent, les formules $|\beth 2| < 2^n$ et $\beth 2 \models \mathcal{D}^n$ sont universellement équivalentes.

Le lemme suivant décrit explicitement la valeur de fausseté de $\beth 2 \models \mathcal{D}^n$, qui est en effet assez simple :

Lemme 3.5. Soient n un entier naturel non nul, $\perp\!\!\!\perp$ un pôle, $t_1, \dots, t_n$ des termes et π une pile. On a $t_1 \bullet \dots \bullet t_n \bullet \pi \in \|\beth 2 \models \mathcal{D}^n\|_{\perp\!\!\!\perp}$ si et seulement si au plus un des t_i ne réalise pas $\bot$ modulo $\perp\!\!\!\perp$.

Démonstration. Pour tous $x_1, \dots, x_n \in \{0,1\}$, on peut vérifier que $\left(\bigvee_{i \neq j} x_i \wedge x_j\right) = 0$ si et seulement si au plus un des x_i est différent de 0. Par conséquent, $t_1 \bullet \dots \bullet t_n \bullet \pi \in \|\beth 2 \models \mathcal{D}^n\|_{\perp\!\!\!\perp}$ si et seulement s'il existe $x_1, \dots, x_n \in \{0,1\}$ tels que t_i réalise $x_i \neq 0$ pour tout i et qu'au plus un des x_i soit différent de 0. □

La notation suivante donne une troisième manière d'exprimer le cardinal de $\beth 2$. D'une certaine manière, c'est la plus importante, car c'est elle qui fournira le lien avec le non-déterminisme :

Notation. Soit n un entier naturel non nul. On note $\mathcal{E}^n$ la formule

$$\forall x \begin{pmatrix} & \top & \to & (0 \not\in x) & \to & \cdots & \to & (0 \not\in x) & \to & (0 \not\in x) \\ \cap & (0 \not\in x) & \to & \top & \to & \cdots & \to & (0 \not\in x) & \to & (0 \not\in x) \\ \vdots & & & & & \vdots & & & & \\ \cap & (0 \not\in x) & \to & (0 \not\in x) & \to & \cdots & \to & \top & \to & (0 \not\in x) \end{pmatrix} \begin{matrix} \textit{(1)} \\ \textit{(2)} \\ \vdots \\ \textit{(n)} \end{matrix}.$$

Remarque. La combinaison de la quantification sur x et de l'utilisation d'atomes de la forme $0 \not\frown x$ simule une quantification du second ordre (le choix de l'élément 0 est arbitraire) : si la syntaxe des formules avait permis les quantifications du second ordre, on aurait simplement défini $\mathcal{E}^n$ comme la formule

$$\forall X \begin{pmatrix} & \top \to X \to \cdots \to X \to & X \\ \cap & X \to \top \to \cdots \to X \to & X \\ \vdots & \vdots & \vdots \\ \cap & X \to X \to \cdots \to \top \to & X \end{pmatrix}.$$

La valeur de fausseté de $\mathcal{E}^n$ ressemble à celle de $\daleth 2 \models \mathcal{D}^n$ (ce qui explique qu'elles soient équivalentes) :

Lemme 3.6. Soient n un entier naturel non nul, $\perp\!\!\!\perp$ un pôle, $t_1, \ldots, t_n$ des termes et π une pile. On a $t_1 \cdot \ldots \cdot t_n \cdot \pi \in \|\mathcal{E}^n\|_{\perp\!\!\!\perp}$ si et seulement s'il existe au plus un i tel que $t_i \star \pi \notin \perp\!\!\!\perp$.

Démonstration. Similaire à celle du lemme 3.5. □

Proposition 3.7. Soit n un entier naturel non nul. Les formules $|\daleth 2| < 2^n$, $\daleth 2 \models \mathcal{D}^n$ et $\mathcal{E}^n$ sont universellement équivalentes.

Démonstration. On a déjà vu que $|\daleth 2| < n$ et $\daleth 2 \models \mathcal{D}^n$ sont universellement équivalentes.

Par les lemmes 3.5 et 3.6, $\mathcal{E}^n \leqq (\daleth 2 \models \mathcal{D}^n)$, donc $\mathcal{E}^n \to (\daleth 2 \models \mathcal{D}^n)$ est universellement réalisée par $\lambda u.u$. De plus, par les mêmes lemmes, $(\daleth 2 \models \mathcal{D}^n) \to \mathcal{E}^n$ est universellement réalisée par $\lambda u.\ \lambda t_1 \ldots . \lambda t_n.\ cc\ (\lambda k.\ u\ (k t_1) \ldots (k t_n))$, car pour tous $\perp\!\!\!\perp$, π et i, $t_i \star \pi \in \perp\!\!\!\perp$ implique $k_\pi t_i \Vdash_{\perp\!\!\!\perp} \perp$. □

3.5 Instructions de vote et fork

À l'aide du langage des relations de multi-évaluation, on peut définir la notion d'*instruction de vote* et formuler un résultat de spécification qui relie ces instructions à $\daleth 2$:

Définition 3.8. Soient k et n deux entiers naturels tels que $k \leq n$ et $n > 0$ et $\succ$ une relation d'évaluation. Une *instruction de* (n,k)*-vote modulo* $\succ$ est un terme φ tel que pour tous termes $t_1, \ldots, t_n$ et toute pile π, pour tout $J \subseteq \{1, \ldots, n\}$ de cardinal au moins $n-k$, $\{\varphi \star t_1 \cdot \ldots \cdot t_n \cdot \pi\} \succ \{t_i \star \pi;\ i \in J\}$.

Théorème 3.9. Soient $\mathcal{S}$ une structure de réalisabilité et n un entier naturel non nul. Un terme φ réalise $\mathcal{E}^n$ modulo $\mathcal{S}$ si et seulement si φ est une instruction de $(n,1)$-vote modulo $\succ_{\mathcal{S}}$.

Démonstration. Tout d'abord, d'après lemme 3.5, pour tout pôle $\perp\!\!\!\perp$, $t_1 \cdot \ldots \cdot t_n \cdot \pi \in \|\mathcal{E}^n\|_{\perp\!\!\!\perp}$ si et seulement si l'ensemble $\{\, j \in \{1, \ldots, n\};\ t_j \star \pi \in \perp\!\!\!\perp \,\}$ est de cardinal au moins $n-1$. Par conséquent, les deux termes de l'équivalence reviennent à dire que pour tout $\perp\!\!\!\perp \in \mathcal{S}$, pour tous $t_1 \cdot \ldots \cdot t_n \cdot \pi \in \|\mathcal{E}^n\|_{\perp\!\!\!\perp}$, $\varphi \star t_1 \cdot \ldots \cdot t_n \cdot \pi \in \perp\!\!\!\perp$: ils sont donc équivalents. □

Corollaire. Soient $\mathcal{S}$ une structure de réalisabilité et n un entier naturel non nul. La formule $|\daleth 2| < 2^n$ est conséquence de $\mathrm{Th}(\mathcal{S})$ si et seulement s'il existe une *quasi-preuve* qui est une instruction de $(n,1)$-vote modulo $\succ_{\mathcal{S}}$.

Remarque. On peut faire le point sur ce qui fait marcher cette correspondance entre instructions de vote et formules sur $\daleth 2$, car il s'agit d'un motif qui sera repris au cours de ce chapitre et du suivant. Les trois ingrédients essentiels sont les suivants :

— les formules $\mathcal{E}^n$ sont construites pour spécifier les instructions de vote,

— grâce à l'instruction cc (c'est-à-dire à la logique classique), on peut traduire $\forall x\ (0 \not\frown x \to \top \to 0 \not\frown x)$ en $\daleth 2 \models \bot \to \top \to \bot$, $\forall x\ (0 \not\frown x \to \top \to 0 \not\frown x \to 0 \not\frown x)$ en $\daleth 2 \models \bot \to \top \to \bot \to \bot$, etc.,

— quantifier universellement sur $\mathfrak{I}2$ (opération logique) revient à faire une intersection[i] (opération *a priori* non logique). Par ailleurs, quantifier existentiellement sur $\mathfrak{I}2$ revient à faire une union[ii].

On verra à la section suivante un résultat analogue pour les instructions de (n, k)-vote en général.

Le nom d'*instruction de vote* vient du fait que si tous les t_i sauf k « s'accordent » sur un comportement, alors $\varphi\ t_1 \dots t_n$ « choisit » ce comportement. Par exemple, si tous les t_i sauf k sont égaux à l'entier de Church $\overline{0} = \lambda f.\ \lambda x.\ x$, alors $\varphi\ t_1 \dots t_n$ se comporte comme l'entier de Church $\overline{0}$. (La notion d'instruction de $(3, 1)$-vote a été introduite par Trakhtenbrot [Tra74].)

Considérons maintenant les définitions suivantes :

Définition 3.10. Soit $\succ$ une relation d'évaluation.

— Une *instruction de choix non-déterministe-may* (ou *instruction fork*[iii]) modulo $\succ$ est un terme ψ tel que pour tous termes u, v et toute pile π, $\{\psi \star u \cdot v \cdot \pi\} \succ \{u \star \pi\}$ *et* $\{\psi \star u \cdot v \cdot \pi\} \succ \{v \star \pi\}$ (autrement-dit, une instruction de $(2, 1)$-vote).

— Une *instruction de choix non-déterministe-must* modulo $\succ$ est un terme χ tel que pour tous termes u, v et toute pile π, $\{\chi \star u \cdot v \cdot \pi\} \succ \{u \star \pi, v \star \pi\}$.

Proposition 3.11. Soit $\mathcal{S}$ une structure de réalisabilité. Un terme t est une instruction de choix non-déterministe-may modulo $\succ_{\mathcal{S}}$ si et seulement si pour toutes formules $A(\overline{x})$ et $B(\overline{x})$, il réalise $\forall \overline{x}\ (A \to B \to A \cap B)$ modulo $\mathcal{S}$, et c'est une instruction de choix non-déterministe-must modulo $\succ_{\mathcal{S}}$ si et seulement si pour toutes formules $A(\overline{x})$ et $B(\overline{x})$, il réalise $\forall \overline{x}\ A \to B \to A \cup B$ modulo $\mathcal{S}$

Démonstration. Si t est une instruction fork, soient $\perp\!\!\!\perp \in \mathcal{S}$, $A(\overline{x})$ et $B(\overline{x})$ deux formules, $\overline{x} \in \mathcal{M}$, $u \Vdash_{\perp\!\!\!\perp} A(\overline{x})$, $v \Vdash_{\perp\!\!\!\perp} B(\overline{y})$ et $\pi \in \|A(\overline{x}) \cap B(\overline{x})\|_{\perp\!\!\!\perp}$. Si $\pi \in \|A(\overline{x})\|_{\perp\!\!\!\perp}$, alors $\{t \star u \cdot v \cdot \pi\} \succ_{\mathcal{S}} \{u \star \pi\} \subseteq \perp\!\!\!\perp$, et de même, si $\pi \in \|B(\overline{x})\|_{\perp\!\!\!\perp}$, alors $\{t \star u \cdot v \cdot \pi\} \succ_{\mathcal{S}} \{v \star \pi\} \subseteq \perp\!\!\!\perp$.

Supposons que t n'est pas une instruction fork. On peut supposer sans perte de généralité qu'il existe u, v et π tels que $\{t \star u \cdot v \cdot \pi\} \not\succ_{\mathcal{S}} \{u \star \pi\}$. Soit donc $\perp\!\!\!\perp \in \mathcal{S}$ tel que $u \star \pi \in \perp\!\!\!\perp$ et $t \star u \cdot v \cdot \pi \notin \perp\!\!\!\perp$, notons A la formule $0 \not\in \{(0, \pi)\}$ et B la formule $\top$ (de sorte que $\|A\|_{\perp\!\!\!\perp} = \{\pi\}$ et $\|B\|_{\perp\!\!\!\perp} = \emptyset$). Alors, $u \cdot v \cdot \pi \in \|A \to B \to A \cap B\|_{\perp\!\!\!\perp}$, et donc t ne réalise pas $A \to B \to A \cap B$ modulo $\perp\!\!\!\perp$.

Le preuve du second point est similaire. □

Proposition 3.12. Soit $\mathcal{S}$ une structure de réalisabilité. La formule $|\mathfrak{I}2| = 2$ est conséquence de $\mathrm{Th}(\mathcal{S})$ si et seulement s'il existe une *quasi-preuve* qui est une instruction fork modulo $\succ_{\mathcal{S}}$.

Démonstration. Conséquence du théorème 3.9 et de la proposition 3.4. □

3.6 Instructions de vote généralisées

On va montrer un résultat similaire au théorème 3.9 et à son corollaire pour les instructions de (n, k)-vote en général, et même en fait pour une généralisation de ces instructions de vote.

Définition 3.13. Soient n un entier naturel non nul, K une partie de $\mathcal{P}(n)$ décroissante pour l'inclusion et $\succ$ une relation d'évaluation. Une *instruction de* (n, K)*-vote modulo* $\succ$ est un terme φ tel que pour tous termes $t_1, \dots, t_n$ et toute pile π, pour tout $p \in K$, $\{\varphi \star t_1 \cdot \dots \cdot t_n \cdot \pi\} \succ \{t_i \star \pi; i \notin p\}$.

En notant $\mathcal{P}_{\leq k}(n)$ l'ensemble des parties de n à au plus k éléments, les instructions de $(n, \mathcal{P}_{\leq k}(n))$-vote coïncident avec les instructions de (n, k)-vote.

i. C'est-à-dire que $(\mathfrak{I}2 \models \forall x\ A) \equiv (\mathfrak{I}2 \models A[x := 0]) \cap (\mathfrak{I}2 \models A[x := 1])$.

ii. On peut vérifier que $(\mathfrak{I}2 \models \exists x\ A) \equiv (\mathfrak{I}2 \models \neg\neg A[x := 0]) \cup (\mathfrak{I}2 \models \neg\neg A[x := 1])$.

iii. Krivine appelle cette instruction *ou parallèle*. Cependant, pour rester cohérent avec la littérature antérieure [Plo77], on réservera le nom de *ou parallèle* à une autre instruction, définie à la section 4.2.1.

Si φ est une instruction de (n, K)-vote et si tous les les t_i sauf $t_{i_1}, \ldots, t_{i_m}$ avec $\{i_1, \ldots, i_m\} \in K$ « s'accordent » sur un comportement, alors $\varphi\ t_1 \ldots t_n$ « choisit » ce comportement.

Pour étudier ces instructions de vote généralisées, on va construire des outils analogues à ceux de la section 3.4 :

Notation. Pour tout entier naturel non nul n et toute K parie décroissante de $\mathcal{P}(n)$, notons $\mathcal{D}_K^n$ la formule suivante du langage des algèbres de Boole :

$$\forall x_1\ \ldots\ \forall x_n\ \left(x_1 \neq 0 \to \ldots \to x_n \neq 0 \to \left(\bigvee_{p \in K}\ \bigwedge_{i=0,\ldots,n-1} x_i^p \right) \neq 1 \right),$$

où x_i^p désigne le terme du premier ordre x_i si $i \in p$, et $\neg x_i$ sinon.

Lemme 3.14. Soient n un entier naturel non nul K une partie décroissante de $\mathcal{P}(n)$, $\perp\!\!\!\perp$ un pôle, $t_1, \ldots, t_n$ des termes et π une pile. On a $t_1 \bullet \ldots \bullet t_n \bullet \pi \in \|\mathbb{I}2 \models \mathcal{D}_K^n\|_{\perp\!\!\!\perp}$ si et seulement si l'ensemble des i tels que t_i ne réalise pas $\perp$ modulo $\perp\!\!\!\perp$ est dans K.

Notation. Pour tout entier naturel non nul n et toute K parie décroissante de $\mathcal{P}(n)$, notons $\mathcal{E}_K^n$ la formule suivante :

$$\forall x_1\ \ldots\ \forall x_n\ \forall y\ \left((x_1 = 0 \hookrightarrow 0\ \not\wr\ y) \to \ldots \to (x_n = 0 \hookrightarrow 0\ \not\wr\ y) \to \left(\bigvee_{p \in K}\ \bigwedge_{i=0,\ldots,n-1} x_i^p \right) = 1 \hookrightarrow 0\ \not\wr\ y \right),$$

où x_i^p désigne le terme du premier ordre x_i si $i \in p$, et $\neg x_i$ sinon.

Lemme 3.15. Soient n un entier naturel non nul K une parie décroissante de $\mathcal{P}(n)$, $\perp\!\!\!\perp$ un pôle, $t_1, \ldots, t_n$ des termes et π une pile. On a $t_1 \bullet \ldots \bullet t_n \bullet \pi \in \|\mathcal{E}_K^n\|_{\perp\!\!\!\perp}$ si et seulement si l'ensemble des i tels que $t_i \star \pi \notin \perp\!\!\!\perp$ est dans K.

Corollaire. Pour tout entier naturel non nul n et toute K partie décroissante de $\mathcal{P}(n)$, les formules $\mathcal{E}_K^n$ et $\mathbb{I}2 \models \mathcal{D}_K^n$ sont universellement équivalentes.

Théorème 3.16. Soient $\mathcal{S}$ une structure de réalisabilité, n un entier naturel non nul et K une partie décroissante de $\mathcal{P}(n)$. Un terme t est une instruction de (n, K)-vote modulo $\succ_{\mathcal{S}}$ si et seulement s'il réalise $\mathcal{E}_K^n$ modulo $\mathcal{S}$.

Pour pouvoir relier les instructions de (n, K)-vote à $\mathbb{I}2$, il ne reste plus qu'à comprendre ce que signifie la formule $\mathcal{D}_K^n$. On va voie qu'elle est soit toujours vraie, soit équivalente à une formule qui dit « il y a strictement moins de μ éléments » pour un certain μ à déterminer.

Pour unifier les deux cas et simplifier les énoncés, on va utiliser la notation ∞ avec les conventions suivantes :

— L'énoncé « $\infty > n$ » est vrai pour tout entier naturel n,

— $\inf(\emptyset) = \infty$,

— Pour tous n et k entiers naturels avec $k \leq n$, $\lceil \frac{n}{k} \rceil = 1$ si $n = k = 0$, et $\lceil \frac{n}{k} \rceil = \infty$ si $k = 0$ et $n > 0$,

— $2^\infty = \infty$,

— Les énoncés « X a strictement moins de ∞ éléments » et « X a au plus ∞ éléments » sont vrais pour tout ensemble X,

— Les énoncés « X a strictement plus de ∞ éléments » et « X a au moins ∞ éléments » sont faux pour tout ensemble X,

— Les notations $|\mathbb{I}2| < \infty$ et $|\mathbb{I}2| \leq \infty$ désignent la formule $\top$,

— Les notations $|\mathbb{I}2| \geq \infty$ et $|\mathbb{I}2| > \infty$ désignent la formule $\top \to \perp$.

Notation. Soient n un entier naturel et K une partie de $\mathcal{P}(n)$. On notera

$$\mu^n(K) = \inf\{m \in \mathbb{N}^*; \exists p_1, \dots, p_m \in K,\ (p_1 \cup \dots \cup p_m) = n\} \in \mathbb{N}^* \cup \{\infty\}.$$

S'il n'y a pas d'ambiguïté, on le notera simplement $\mu(K)$.

Lemme 3.17. Pour tout entier naturel non nul n, toute K partie décroissante de $\mathcal{P}(n)$ et toute algèbre de Boole $\mathbb{B}$, la formule $\mathcal{D}_K^n$ est vraie dans $\mathbb{B}$ si et seulement si $\mathbb{B}$ a strictement moins de $\mu^n(K)$ éléments.

Démonstration. — Par contraposée, supposons que $\mathbb{B}$ a au moins $2^{\mu(K)}$ éléments. Nécessairement, $\mu(K)$ est fini (car par convention, aucun ensemble n'a au moins ∞ éléments). On peut donc trouver $a_1, \dots, a_{\mu(K)} \in \mathbb{B}$ non nuls deux à deux disjoints. Quitte à agrandir, par exemple, a_1, on peut supposer que $a_1 \vee \dots \vee a_{\mu(K)} = 1$. Soient $p_1, \dots, p_{\mu(K)} \in K$ tels que $(p_1 \cup \dots \cup p_{\mu(K)}) = n$.
Pour tout $i < n$, posons $x_i = \bigvee_{j=1,\dots,\mu(K)}^{i \in p_j} a_j$.
Pour tout $i < n$, pour tout $j \in \{1, \dots, \mu(K)\}$, on a $a_j \leq x_i^{p_j}$. En effet, on a soit $i \in p_j$, soit $i \notin p_j$. Si $i \in p_j$, alors $a_j \leq x_i = x_i^{p_j}$. Si $i \notin p_j$, alors $a_j \wedge x_i = a_j \wedge \left(\bigvee_{k=1,\dots,\mu(K)}^{i \in p_k} a_k\right) = \bigvee_{k=1,\dots,\mu(K)}^{i \in p_k} (a_j \wedge a_k) = 0$, donc $a_j \leq \neg x_i = x_i^{p_j}$.
Par conséquent, pour tout $j \in \{1, \dots, \mu(K)\}$, on a $\bigwedge_{i=0,\dots,n-1} x_i^{p_j} \geq a_j$, et donc $\bigvee_{j=1,\dots,\mu(K)} \bigwedge_{i=0,\dots,n-1} x_i^{p_j} \geq \bigvee_{j=1,\dots,\mu(K)} a_j$.
De plus, pour tout $i < n$, x_i est non nul. En effet, $(p_1 \cup \dots \cup p_{\mu(K)}) = n$, donc il existe j tel que $i \in p_j$.
On a donc à la fois $\left(\bigvee_{p \in K} \bigwedge_{i=0,\dots,n-1} x_i^p\right) \geq \left(\bigvee_{j=1,\dots,\mu(K)} a_j\right) = 1$ et $\bigwedge_{i<n} (x_i \neq 0)$, par conséquent, $\mathbb{B}$ ne vérifie pas $\mathcal{D}_K^n$.

— Supposons que $\mathbb{B}$ a strictement moins de $2^{\mu(K)}$ éléments, et montrons que $\mathbb{B}$ vérifie $\mathcal{D}_K^n$.
Dans un premier temps, supposons que $\mu(K)$ est fini. Ainsi, $\mathbb{B}$ est finie et a m atomes, avec $m < \mu(K)$. Notons $a_1, \dots, a_m$ ces atomes.
Soient $x_0, \dots, x_{n-1}$ des éléments non nuls de $\mathbb{B}$, et supposons par l'absurde que $\left(\bigvee_{p \in K} \bigwedge_{i=0,\dots,n-1} x_i^p\right) = 1$. Pour tout $j \in \{1, \dots, m\}$, il existe donc $p_j \in K$ tel que $\bigwedge_{i=0,\dots,n-1} x_i^{p_j} \geq a_j$.
Pour tout $i < n$, $x_i > 0$, donc il existe $j \in \{1, \dots, m\}$ tel que $x_i \geq a_j$. Comme $\bigwedge_{i=0,\dots,n-1} x_i^{p_j} \geq a_j$, on a $i \in p_j$ (car sinon, on aurait $\bigwedge_{i=0,\dots,n-1} x_i^{p_j} \leq \neg a_j$).
Par conséquent, on a $(p_1 \cup \dots \cup p_m) = n$, ce qui contredit $m < \mu(K)$.
Supposons maintenant que $\mu(K) = \infty$. Il existe donc $k < n$ tel que pour tout $p \in K$, $k \notin p$. Pour tous $x_0, \dots, x_{n-1}$ éléments non nuls de $\mathbb{B}$, on a donc $\left(\bigvee_{p \in K} \bigwedge_{i=0,\dots,n-1} x_i^p\right) \leq \neg x_k$, et $\neg x_k < 1$ car $x_k \neq 0$.
Autrement dit, $\mathbb{B}$ vérifie $\mathcal{D}_K^n$.

□

Finalement, on en déduit le résultat suivant, qui relie le cardinal de $\daleth 2$ aux instructions de vote généralisées :

Théorème 3.18. Soient n un entier naturel non nul et K une partie décroissante de $\mathcal{P}(n)$. Les formules $|\daleth 2| < 2^{\mu_n(K)}$, $\daleth 2 \models \mathcal{D}_K^n$ et $\mathcal{E}_K^n$ sont universellement équivalentes.

Corollaire. Soient $\mathcal{S}$ une structure de réalisabilité, n un entier naturel non nul et K une partie décroissante de $\mathcal{P}(n)$. La formule $|\daleth 2| < 2^{\mu_n(K)}$ est conséquence de $\mathrm{Th}(\mathcal{S})$ si et seulement s'il existe une *quasi-preuve* qui est une instruction de (n, K)-vote modulo $\succ_{\mathcal{S}}$.

Corollaire. Soient $\mathcal{S}$ une structure de réalisabilité, n un entier naturel non nul et $k \in \{0, \dots, n\}$. La formule $|\daleth 2| < 2^{\lceil \frac{n}{k} \rceil}$ est conséquence de $\mathrm{Th}(\mathcal{S})$ si et seulement s'il existe une *quasi-preuve* qui est une instruction de (n, k)-vote modulo $\succ_{\mathcal{S}}$.

Démonstration. Il suffit de vérifier que $\mu_n(\mathcal{P}_{\leq k}) = \lceil \frac{n}{k} \rceil$. □

On va maintenant démontrer la réciproque de la proposition 3.4.

3.7 Complétude de la théorie des algèbres de Boole à au moins deux éléments pour $\daleth 2$

L'objectif de cette section est de démontrer le résultat suivant :

Théorème 3.19. Soit $\mathcal{T}$ un $\mathcal{M}$-ensemble de formules closes du langage des algèbres de Boole. Sont équivalents :

— Il existe une structure de réalisabilité cohérente $\mathcal{S}$ telle que pour tout $A \in \mathcal{T}$, la formule $\daleth 2 \models A$ est réalisée modulo $\mathcal{S}$,

— Il existe une algèbre de Boole à au moins deux éléments qui vérifie $\mathcal{T}$.

Corollaire. Pour toute formule close A du langage des algèbres de Boole, si $\daleth 2 \models A$ est universellement réalisée, alors A est vraie dans toute algèbre de Boole à au moins deux éléments.

Corollaire. Pour toutes formules $A(\overline{x})$ et $B(\overline{x})$ du langage des algèbres de Boole, si $A \leqq B$ alors la formule $\forall \overline{x}\ (A \to B)$ est vraie dans toute algèbre de Boole à au moins deux éléments.

Remarque. Le fait que le premier énoncé implique le second est une conséquence de la proposition 3.4 et du théorème de compacité de la logique du premier ordre.

On fixe un $\mathcal{M}$-ensemble $\mathcal{T}$ de formules closes du langage des algèbres de Boole.

3.7.1 Construction de la structure

Fixons une $\mathcal{M}$-injection $A \mapsto \gamma_A$ de l'ensemble des formules (non nécessairement closes) du langage des algèbres de Boole dans Λ telle que pour toute formule A :

— Si $A \in \mathcal{T}$, γ_A est une instruction non protégée ;

— Sinon, γ_A est une instruction protégée.

Remarque. Comme remarqué au début de l'annexe A, toute formule $A(\overline{x})$ du langage des algèbres de Boole peut se lire de manière unique (à renommage des variables $\overline{y}_0, \dots, \overline{y}_m$ près) comme $\forall \overline{y}_0\ (B_0 \to \dots \to \forall \overline{y}_{m-1}\ (B_{m-1} \to \forall \overline{y}_m\ b \neq b') \dots)$. Par conséquent, toute formule $A(\overline{x})$ du langage des algèbres de Boole peut se lire de manière unique (à renommage des variables $\overline{y}_0, \dots, \overline{z}_{0,0}, \dots$ près) comme

$$\begin{aligned}\forall \overline{y}_0\ (\forall \overline{z}_{0,0}\ (B_{0,0} \to \dots \to \forall \overline{z}_{0,n_0-1}\ (B_{0,n_0-1} \to \forall \overline{z}_{0,n_0}\ c_1 \neq c_1') \dots) \quad &\to \dots \to \\ \forall \overline{y}_{m-1}\ (\forall \overline{z}_{m-1,0}\ (B_{m-1,0} \to \dots \to \forall \overline{z}_{m-1,n_{m-1}-1}\ (B_{m-1,n_{m-1}-1} \to \forall \overline{z}_{m-1,n_{m-1}}\ c_{m-1} \neq c'_{m-1}) \dots) \\ &\to \forall \overline{z}_m\ b \neq b') \dots).\end{aligned}$$

De plus, on peut faire en sorte que les variables $\overline{x}, \overline{y}_0, \dots, \overline{z}_{0,0}, \dots$ soient distinctes.

Dans cette situation :

— On note $\dot{y}$ pour $\overline{y}_0, \dots, \overline{y}_m$ (et de manière générale, $\dot{Y}$ pour $\overline{Y}_0, \dots, \overline{Y}_m$ quelle que soit la nature des expressions $\overline{Y}_i$) ;

— Pour tout $i < m$, on note $\dot{z}_i$ pour $\overline{z}_{i,0}, \dots, \overline{z}_{i,n_i}$ (et de manière générale, $\dot{Z}_i$ pour $\overline{Z}_{i,0}, \dots, \overline{Z}_{i,n_i}$ quelle que soit la nature des expressions $\overline{Z}_{i,j}$).

Soit $\succ^1$ la plus petite relation binaire sur $\mathcal{P}_{\mathcal{M}}(\Lambda \star \Pi)$ telle que :

— Pour tous $p, q \in \Lambda \star \Pi$, si $p \succ^1_{\mathrm{K}} q$, alors $\{p\} \succ^1 \{q\}$;

— Pour toute formule close $\forall \overline{y}_0\ (\forall \overline{z}_{0,0}\ (B_{0,0} \to \dots \to \forall \overline{z}_{0,n_0}\ c_0 \neq c_0' \dots) \to \dots \to \forall \overline{y}_m\ b \neq b' \dots)$ (notée A) du langage des algèbres de Boole avec $\overline{x}, \overline{y}_0, \dots, \overline{z}_{0,0}, \dots$ distinctes, pour tous $\dot{\beta} \in \{0,1\}$ tels que $\{0,1\} \models (b = b')[\dot{y} := \dot{\beta}]$, pour tous termes $t_0, \dots, t_{m-1}$ et toute pile π,

$$\{\ \gamma_A \star t_0 \bullet \ldots \bullet t_{m-1} \bullet \pi\ \} \ \succ^1 \ \left\{ \begin{array}{l} t_i \star \gamma_{B_{i,0}}[\dot{z}_i := \dot{\delta}_i, \dot{y} := \dot{\beta}] \bullet \ldots \bullet \gamma_{B_{i,n_i-1}}[\dot{z}_i := \dot{\delta}_i, \dot{y} := \dot{\beta}] \bullet \pi; \\ i < m,\ \dot{\delta}_i \in \{0,1\} \text{ tels que } \{0,1\} \models (c_i = c_i')[\dot{z}_i := \dot{\delta}_i, \dot{y} := \dot{\beta}] \end{array} \right\}.$$

On note $\succ$ la plus petite relation de multi-évaluation contenant $\succ^1$, et l'on considère la structure $\mathcal{S} = \mathcal{S}_\succ$.

Remarque. La relation d'évaluation $\succ$ est compacte.

Proposition 3.20. Pour toute formule close A du langage des algèbres de Boole, γ_A réalise $(\beth 2 \models A)$.

Corollaire. Pour toute $A \in \mathcal{T}$, $\beth 2 \models A$ est réalisée modulo $\mathcal{S}$.

Démonstration. Fixons un pôle $\perp\!\!\!\perp \in \mathcal{S}$, et procédons par induction sur la profondeur de la formule :

Soient

— Une formule close $\forall \overline{y}_0\ (\forall \overline{z}_{0,0}\ (B_{0,0} \to \ldots \to \forall \overline{z}_{0,n_0}\ c_0 \neq c_0' \ldots) \ \to\ \ldots\ \to\ \forall \overline{y}_m\ b \neq b' \ldots)$ (notée A) avec $\overline{x}, \overline{y}_0, \ldots, \overline{z}_{0,0}, \ldots$ distinctes,

— $\dot{\beta}$ des éléments de $\{0,1\}$,

— $t_0, \ldots, t_{m-1}$ des termes tels que pour tout i, $t_i \Vdash (\beth 2 \models (\forall \overline{z}_{i,0}\ (B_{i,0} \to \ldots \to \forall \overline{z}_{i,n_i}\ c_i \neq c_i' \ldots))\ [\dot{y} := \dot{\beta}])$,

— $\pi \in \left\| \beth 2 \models (b \neq b')[\dot{y} := \dot{\beta}] \right\|_{\perp\!\!\!\perp}$.

Montrons que $\gamma_A \star t_0 \bullet \ldots \bullet t_{m-1} \bullet \pi \in \perp\!\!\!\perp$.

Pour alléger les notations, on supposera que $m = 1$ et $n_0 = 1$ et que les listes $\overline{y}_1$ et $\overline{z}_{0,1}$ sont vides, et l'on omettra les indices correspondants (par exemple on notera $\overline{y}$ et $\overline{z}$ pour $\overline{y}_0$ et $\overline{z}_{0,0}$ respectivement) : la preuve est très similaire dans le cas général.

Pour tous $\overline{\delta} \in \{0,1\}$ tels que $\{0,1\} \models (c = c')[\overline{z} := \overline{\delta}, \overline{y} := \overline{\beta}]$, d'une part, par hypothèse d'induction, $\gamma_{B[\overline{z}:=\overline{\delta},\overline{y}:=\overline{\beta}]} \Vdash (\beth 2 \models B[\overline{z} := \overline{\delta}, \overline{y} := \overline{\beta}])$, et d'autre part, $t \Vdash (\beth 2 \models B[\overline{z} := \overline{\delta}, \overline{y} := \overline{\beta}] \to \bot)$: par conséquent, $t \star \gamma_{B[\overline{z}:=\overline{\delta},\overline{y}:=\overline{\beta}]} \bullet \pi \in \bot$.

De plus, comme $\pi \in \left\| \beth 2 \models (b \neq b')[\overline{y} := \overline{\beta}] \right\|_{\perp\!\!\!\perp}$, $\{0,1\} \models (b = b')[\overline{y} := \overline{\beta}]$, donc finalement, $\gamma_A \star t \bullet \pi \in \perp\!\!\!\perp$ par définition de $\succ$. □

Notation. Soient θ un λ_c-terme ou une pile, $\overline{x}$ des variables *du premier ordre* distinctes, et $\overline{a}$ des termes *du langage des algèbres de Boole*. On note $\theta[\overline{x} := \overline{a}]$ le λ_c-terme ou la pile défini(e) par induction sur θ de la façon suivante :

Pour les termes :

— $\gamma_A[\overline{x} := \overline{a}] = \gamma_{A[\overline{x}:=\overline{a}]}$;

— $y[\overline{x} := \overline{a}] = y$;

— $(tu)[\overline{x} := \overline{a}] = (t[\overline{x} := \overline{a}])(u[\overline{x} := \overline{a}])$;

— $(\lambda y.\ t)[\overline{x} := \overline{a}] = \lambda y.\ (t[\overline{x} := \overline{a}])$;

— $c[\overline{x} := \overline{a}] = c$;

— $k_\pi[\overline{x} := \overline{a}] = k_{\pi[\overline{x}:=\overline{a}]}$;

— $\delta[\overline{x} := \overline{a}] = \delta$ si δ est une instruction protégée ou non protégée qui n'est pas de la forme γ_A ;

Pour les piles :

— $\omega_n[\overline{x} := \overline{a}] = \omega_n$;

— $(t \bullet \pi)[\overline{x} := \overline{a}] = (t[\overline{x} := \overline{a}]) \bullet (\pi[\overline{x} := \overline{a}])$.

Les λ_c-termes t et $t[\overline{x} := \overline{a}]$ ont les mêmes variables libres. En particulier, si $t \in \Lambda$, $t[\overline{x} := \overline{a}] \in \Lambda$.

3.7.2 Contenu d'un programme

Définition 3.21. Soit θ un λ_c-terme ou une pile. Le *contenu de* θ, noté $\mathcal{C}_\theta$, est la formule du langage des algèbres de Boole définie, par induction sur θ, de la façon suivante :

Pour les termes :

— $\mathcal{C}_{\gamma_A}$ est la formule A,

— $\mathcal{C}_x$ est la formule $\top$,

— $\mathcal{C}_{tu}$ est la formule $\mathcal{C}_t \wedge \mathcal{C}_u$,

— $\mathcal{C}_{\lambda x.\ t}$ est la formule $\mathcal{C}_t$,

— $\mathcal{C}_{cc}$ est la formule $\top$,

— $\mathcal{C}_{k_\pi}$ est la formule $\mathcal{C}_\pi$,

— $\mathcal{C}_\delta$ est la formule $\top$ si δ est une instruction accessible ou non-accessible qui n'est pas de la forme γ_A,

Pour les piles :

— $\mathcal{C}_{\omega_n}$ est la formule $\top$,

— $\mathcal{C}_{t \cdot \pi}$ est la formule $\mathcal{C}_t \wedge \mathcal{C}_\pi$.

Lemme 3.22. Pour toute quasi-preuve t, $\mathcal{T} \models \mathcal{C}_t$.

Lemme 3.23. Soient t et t' deux termes, π et π' deux piles, et $\overline{x}$ des variables du premier ordre distinctes contenant au moins toutes les variables libres de $\mathcal{C}_t$ et $\mathcal{C}_\pi$. Si $t \star \pi \succ_K t' \star \pi'$, alors $\overline{x}$ contient toutes les variables libres de $\mathcal{C}_{t'}$ et $\mathcal{C}_{\pi'}$, et toute algèbre de Boole à au moins deux éléments vérifie $\forall \overline{x}\ ((\mathcal{C}_t \wedge \mathcal{C}_\pi) \rightarrow (\mathcal{C}_{t'} \wedge \mathcal{C}_{\pi'}))$.

3.7.3 Cohérence de la structure

Posons $\perp\!\!\!\perp = \{p \in \Lambda \star \Pi;\ \{p\} \succ \emptyset\}$.

Lemme 3.24. L'ensemble $\perp\!\!\!\perp$ est un pôle, et c'est le plus petit élément de $\mathcal{S}$ (pour l'inclusion).

Pour tout entier n, posons $\perp\!\!\!\perp_n = \{p \in \Lambda \star \Pi;$ il existe $m < n$ et $Q \in \mathcal{P}_\mathcal{M}(\perp\!\!\!\perp_m)$ tels que $\{p\} \succ^1 Q\}$ (par induction sur n). En particulier, $\perp\!\!\!\perp_0 = \emptyset$.

Lemme 3.25. On a $\perp\!\!\!\perp = \bigcup_{n \in \mathbb{N}} \perp\!\!\!\perp_n$.

Lemme 3.26. Soient n un entier, t un terme, π une pile, $\overline{x}$ des variables du premier ordres distinctes contenant au moins toutes les variables libres de $\mathcal{C}_t$ et $\mathcal{C}_\pi$, et $\overline{a}$ et $\overline{b}$ des termes clos du langage des algèbres de Boole tels que $\{0,1\} \models a = b$. On a $t[\overline{x} := \overline{a}] \star \pi[\overline{x} := \overline{a}] \in \perp\!\!\!\perp_n$ si et seulement si $t[\overline{x} := \overline{b}] \star \pi[\overline{x} := \overline{b}] \in \perp\!\!\!\perp_n$.

Proposition 3.27. Soient t un terme, π une pile, $\overline{a'}^p$ et $\overline{a}^p$ des termes du langage des algèbres de Boole et $\overline{x}^q$ des variables du premier ordre distinctes contenant au moins toutes les variables libres de $\mathcal{C}_t$, $\mathcal{C}_\pi$, $\overline{a}$, et $\overline{a'}$:

Si pour tous $\overline{\alpha}^q \in \{0,1\}$ tels que $\{0,1\}$ vérifie $(\overline{a} = \overline{a'})[\overline{x} := \overline{\alpha}]$, on a $t[\overline{x} := \overline{\alpha}] \star \pi[\overline{x} := \overline{\alpha}] \in \perp\!\!\!\perp$, alors la formule $\exists \overline{x}\ (\mathcal{C}_t \wedge \mathcal{C}_\pi \wedge (\overline{a} = \overline{a'}))$ est contradictoire.

Corollaire. Pour toute formule close A du langage des algèbres de Boole, pour tout terme t, si t réalise $\beth 2 \models A$ dans $\mathcal{S}$, alors $\mathcal{C}_t \models A$.

Démonstration. Si t réalise $\beth 2 \models A$ dans $\mathcal{S}$, alors en particulier $\gamma_{\neg A} \star t \cdot \omega_0 \in \perp\!\!\!\perp$, donc $\neg A \wedge \mathcal{C}_t$ est contradictoire, et par conséquent, $\mathcal{C}_t \models A$. □

Corollaire. Pour toute formule close A du langage des algèbres de Boole, $\mathfrak{I}2 \models A$ est réalisée modulo $\mathcal{S}$ si et seulement si et seulement si $\mathcal{T} \models A$.

Corollaire. S'il existe une algèbre de Boole à au moins deux éléments qui vérifie $\mathcal{T}$, alors la structure de réalisabilité $\mathcal{S}$ est cohérente.

Démonstration de la proposition. On va montrer par induction que pour tout entier μ, pour tous tels t, π, $\overline{a}^p$, $\overline{a'}^p$ et $\overline{x}^q$, si pour tous $\overline{\alpha}^q \in \{0,1\}$ tels que $\{0,1\} \models (\overline{a} = \overline{a'})[\overline{x} := \overline{\alpha}]$, on a $t[\overline{x} := \overline{\alpha}] \star \pi[\overline{x} := \overline{\alpha}] \in \perp\!\!\!\perp_\mu$, alors la formule $\exists \overline{x}\ (\mathcal{C}_t \wedge \mathcal{C}_\pi \wedge (\overline{a} = \overline{a'}))$ est contradictoire.

Soit μ un entier tel que le résultat soit vrai pour tout $\nu < \mu$, et soient t, π, $\overline{a'}^p$, $\overline{a'}^p$ et $\overline{x}^q$ tels que pour tous $\overline{\alpha}^q \in \{0,1\}$ tels que $\{0,1\} \models (\overline{a} = \overline{a'})[\overline{x} := \overline{\alpha}]$, $t[\overline{x} := \overline{\alpha}] \star \pi[\overline{x} := \overline{\alpha}] \in \perp\!\!\!\perp_\mu$.

Par définition de $\perp\!\!\!\perp_\mu$, il existe $\nu < \mu$ tel que pour tous $\overline{\alpha}^q \in \{0,1\}$ tels que $\{0,1\} \models (\overline{a} = \overline{a'})[\overline{x} := \overline{\alpha}]$, il existe $Q \in \mathcal{P}_\mathcal{M}(\perp\!\!\!\perp_\nu)$ tel que $\{t[\overline{x} := \overline{\alpha}] \star \pi[\overline{x} := \overline{\alpha}]\} \succ^1 Q$.

On est donc dans l'une des situations suivantes :

— Pour tous $\overline{\alpha}^q \in \{0,1\}$, $\{0,1\} \models (\overline{a} \neq \overline{a'})[\overline{x} := \overline{\alpha}]$. Dans ce cas, d'après le premier corollaire de la proposition A.10, la formule $\exists \overline{x}\ \overline{a} = \overline{a'}$ est contradictoire, donc à plus forte raison, la formule $\exists \overline{x}\ (\mathcal{C}_t \wedge \mathcal{C}_\pi \wedge (\overline{a} = \overline{a'}))$ l'est aussi.

— Il existe t' et π' tels que $t \star \pi \succ^1_{\mathrm{K}} t' \star \pi'$ et pour tous $\overline{\alpha}^q \in \{0,1\}$ tels que $\{0,1\} \models (\overline{a} = \overline{a'})[\overline{x} := \overline{\alpha}]$, $t'[\overline{x} := \overline{\alpha}] \star \pi'[\overline{x} := \overline{\alpha}] \in \perp\!\!\!\perp_\nu$. Dans ce cas, par hypothèse de récurrence, la formule $\exists \overline{x}\ (\mathcal{C}_{t'} \wedge \mathcal{C}_{\pi'} \wedge (\overline{a} = \overline{a'}))$ est contradictoire, et d'après le lemme 3.23, la formule $\exists \overline{x}\ (\mathcal{C}_t \wedge \mathcal{C}_\pi \wedge (\overline{a} = \overline{a'}))$ est contradictoire.

— t est de la forme $\gamma_{A(\overline{x})}$, avec A de la forme $\forall \overline{y}_0\ (\forall \overline{z}_{0,0}\ (B_{0,0} \to \ldots \to \forall \overline{z}_{0,n_0}\ c_0 \neq c'_0 \ldots) \to \ldots \to \forall \overline{y}_m\ b \neq b' \ldots)$ et $\overline{x}, \overline{y}_0, \ldots, \overline{z}_{0,0}, \ldots$ distinctes, π est de la forme $u_0 \bullet \ldots \bullet u_{m-1} \bullet \pi'$, et pour tous $\overline{\alpha}^q \in \{0,1\}$ tels que $\{0,1\} \models (\overline{a} = \overline{a'})[\overline{x} := \overline{\alpha}]$, il existe $\dot{\beta} \in \{0,1\}$ tels que tels que $\{0,1\} \models (\overline{b} = \overline{b'})[\overline{y} := \overline{\beta}, \overline{x} := \overline{\alpha}]$ et que pour tout $i < m$, pour tous $\dot{\delta}_i \in \{0,1\}$ tels que $\{0,1\} \models (c_i = c'_i)[\dot{z}_i := \dot{\delta}_i, \dot{y} := \dot{\beta}, \overline{x} := \overline{\alpha}]$,

$$u_i[\overline{x} := \overline{\alpha}] \star \gamma_{B_{i,0}}[\dot{z}_i := \dot{\delta}_i, \dot{y} := \dot{\beta}, \overline{x} := \overline{\alpha}] \bullet \ldots \bullet \pi'[\overline{x} := \overline{\alpha}] \in \perp\!\!\!\perp_\nu.$$

Pour alléger les notations, on supposera que $m = 1$ et $n_0 = 1$ et que les listes $\overline{y}_1$ et $\overline{z}_{0,1}$ sont vides, et l'on omettra les indices correspondants (par exemple on notera $\overline{y}$ et $\overline{z}$ pour $\overline{y}_0$ et $\overline{z}_{0,0}$ respectivement) : la preuve est très similaire dans le cas général.

Ainsi, $A(\overline{x}$ est la formule $\forall \overline{y}\ (\forall \overline{z}\ (B \to c \neq c') \to b \neq b')$.

Soit donc $\overline{f}$ une liste de fonctions de $\{0,1\}^q$ dans $\{0,1\}$ telle que pour tous $\overline{\alpha}^q \in \{0,1\}$ vérifiant $\{0,1\} \models (\overline{a} = \overline{a'})[\overline{x} := \overline{\alpha}]$, on ait $\{0,1\} \models (\overline{b} = \overline{b'})[\overline{y} := \overline{f}(\overline{\alpha}), \overline{x} := \overline{\alpha}]$ et pour tous $\overline{\delta} \in \{0,1\}$ vérifiant $\{0,1\} \models (c = c')[\overline{z} := \overline{\delta}, \overline{y} := \overline{f}(\overline{\alpha}), \overline{x} := \overline{\alpha}]$, on ait

$$u[\overline{x} := \overline{\alpha}] \star \gamma_B[\overline{z} := \overline{\delta}, \overline{y} := \overline{f}(\overline{\alpha}), \overline{x} := \overline{\alpha}] \bullet \pi'[\overline{x} := \overline{\alpha}] \in \perp\!\!\!\perp_\nu.$$

On choisit une liste de termes du langage des algèbres de Boole, que l'on note $\underline{\overline{f}}(\overline{y})$, dont l'interprétation dans $\{0,1\}$ est $\overline{f}$, c'est-à-dire telle que pour tous $\overline{\alpha} \in \{0,1\}$, $\underline{\overline{f}}^{\{0,1\}}(\overline{\alpha}) = \overline{f}(\overline{\alpha})$ (voir proposition A.11).

D'après le lemme 3.26, cela revient à dire que

$$u[\overline{x} := \overline{\alpha}] \star \gamma_B[\overline{z} := \overline{\delta}, \overline{y} := \underline{\overline{f}}(\overline{\alpha}), \overline{x} := \overline{\alpha}] \bullet \pi'[\overline{x} := \overline{\alpha}] \in \perp\!\!\!\perp_\nu,$$

Par hypothèse d'induction, la formule

$$\exists \overline{x}\ \exists \overline{z}\ (\mathcal{C}_u \wedge \mathcal{C}_{\pi'} \wedge B[\overline{y} := \underline{\overline{f}}(\overline{x})] \wedge (\overline{a} = \overline{a'}) \wedge (c = c)[\overline{y} := \underline{\overline{f}}(\overline{x})])$$

est donc contradictoire. À plus forte raison, la formule

$$\exists \overline{x}\ (\mathcal{C}_u \wedge \mathcal{C}_{\pi'} \wedge (\overline{a} = \overline{a'}) \wedge \forall \overline{y}\ ((b = b') \to \exists \overline{z}\ (B \wedge (c = c'))))$$

est contradictoire (en effet, la formule $\forall \overline{x}\ (b = b')[\overline{y} := \underline{\overline{f}}(\overline{x})]$ est vraie dans toute algèbre de Boole d'après la proposition A.11).

Enfin, la formule $\forall\overline{x}\ (A \to \forall\overline{y}\ (b = b' \to \exists\overline{z}\ (B \wedge (c = c'))))$ est vraie dans toute algèbre de Boole (elle est même vraie dans toute structure sur le langage des algèbres de Boole), donc finalement, la formule $\exists\overline{x}\ (\mathcal{C}_t \wedge \mathcal{C}_\pi \wedge (\overline{a} = \overline{a}'))$ est contradictoire.

□

Ceci achève de démontrer le théorème 3.19.

3.8 Les ensembles ℶ*n*

Comprendre ℶ2 est suffisant pour comprendre ℶ*n* pour tout *n* fini. En effet, pour tout $n \in \mathbb{N}$, ℶ*n* est en bijection avec l'ensemble des partitions de longueur *n* de ℶ2 :

Proposition 3.28. Soit *n* un entier naturel. Soient :

- $A(y_0, \ldots, y_{n-1})$ la formule $\left(\bigwedge_{i<n} (y_i\ \varepsilon\ \beth 2)\right) \wedge \left(\bigwedge_{i<j<n} (y_i \wedge y_j = 0)\right) \wedge \left(\left(\bigvee_{i<n} y_i\right) = 1\right)$ (qui dit que $y_0, \ldots, y_{n-1}$ est une partition de ℶ2),
- pour tout $k < n$, f_k la fonction de *n* dans $\{0, 1\}$ qui à $j < n$ associe 1 si $j = k$ et 0 sinon,
- *g* un inverse à gauche de $(f_0, \ldots, f_{n-1})$ (vue comme une fonction de *n* dans $\{0, 1\}^n$).

Alors les formules suivantes sont universellement réalisées :

- $\forall x \varepsilon \beth n\ A(f_0(x), \ldots, f_{n-1}(x))$,
- $\forall y_0 \ldots \forall y_{n-1}\ \left(A(y_0, \ldots, y_{n-1}) \to g(y_0, \ldots, y_{n-1})\ \varepsilon\ \beth n\right)$,
- $\forall x \varepsilon \beth n\ g(f_0(x), \ldots, f_{n-1}(x)) = x$,
- $\forall y_0 \ldots \forall y_{n-1}\ \left(A(y_0, \ldots, y_{n-1}) \to \bigwedge_{i<n} f_i(g(y_0, \ldots, y_{n-1})) = y_i\right)$.

Démonstration. Chacune de ces formules est équivalente à une conjonction de clauses de Horn vraies (voir proposition 2.30 : préservation des clauses de Horn). □

4 Degrés de parallélisme

4.1 Modèles de calcul finis

4.1.1 Syntaxe

Le $\mathcal{M}$-ensemble des *types simples* est défini par la grammaire suivante (où pour tout *n*, le type Δ_n représente le *type récursif* avec *n* constructeurs 0-aires) :

$$\begin{array}{rcll} T, U & ::= & \Delta_n & (n \in \mathbb{N}) \\ & | & T \to U & (T,U \text{ types simples}) \end{array}$$

On peut remarquer que tout type simple est de la forme $T_1 \to \ldots \to T_m \to \Delta_n$ avec $T_1, \ldots, T_m$ des types simples.

Pour tout entier naturel *n* et tous types simples *T* et *U*, on notera $T^n \to U$ le type simple $T \to \ldots \to T \to U$ (où *T* apparaît *n* fois).

Pour tout type simple *T*, on fixe un $\mathcal{M}$-ensemble infini $\mathcal{M}$-dénombrable de *variables de type T*, notées $x^T, y^T, z^T, \ldots$ (ou simplement $x, y, z, \ldots$ s'il n'y a pas d'ambiguïté). Ces ensembles sont pris deux à deux disjoints.

La grammaire suivante, considérée modulo α-équivalence, définit pour tout type simple *T* le $\mathcal{M}$-ensemble des *termes simples de type T* (notés génériquement $t, u, \ldots$) :

— pour tout type simple T et toute variable x^T de type T, x^T est un terme simple de type T,

— pour tous types simple T, U, tout terme simple t de type $U \to T$ et tout terme simple u de type U, $t\,u$ est un terme simple de type T,

— pour tous types simples T, U, toute variable x^T de type T et tout terme u de type U, $\mathsf{fun}\ x^T \to u$ est un terme simple de type $T \to U$,

— pour tout entier naturel n et tout $k \in \{0, \ldots, n-1\}$, ∂_k^n est un terme simple de type Δ_n (que l'on notera simplement ∂_k s'il n'y a pas d'ambiguïté),

— pour tout entier naturel n et tout type simple T, $\mathsf{match}^{n,T}$ est un terme simple de type $\Delta_n \to T^n \to T$ (que l'on notera simplement match s'il n'y a pas d'ambiguïté),

— pour tout type simple T, Ω^T est un terme simple de type T (que l'on notera simplement Ω s'il n'y a pas d'ambiguïté). Ce terme représente un calcul qui diverge.

— pour tous types simples T, U, $\mathcal{cc}^{T,U}$ est un terme simple de type $((T \to U) \to T) \to T$ (que l'on notera simplement $\mathcal{cc}$ s'il n'y a pas d'ambiguïté).

Pour tout n, les termes $\partial_0^n, \ldots, \partial_{n-1}^n$ représente les n constructeurs du type Δ_n, et les termes simples $\mathsf{match}^{n,T}$ permettent de faire du *filtrage par motif*.

De plus la grammaire suivante, considérée modulo α-équivalence, définit pour tous types simples T et U le $\mathcal{M}$-ensemble des *contextes de type* $T \to U$ (notés génériquement $C[\,], D[\,], \ldots$) :

— pour tout type simple T, $[\,]^T$ est un contexte de type $T \to T$ (que l'on notera simplement $[\,]$ s'il n'y a pas d'ambiguïté),

— pour tous types simple T, U, V, tout contexte $C[\,]$ de type $T \to U$ et toute variable x^V de type V, $\mathsf{fun}\ x^V \to C[\,]$ est un contexte de type $T \to V \to U$,

— pour tous types simples T, U, V, tout contexte $C[\,]$ de type $T \to U \to V$ et tout terme u de type U, $(C[\,])\ u$ est un contexte de type $T \to V$,

— pour tous type simples T, U, tout entier naturel n et tout contexte $C[\,]$ de type $T \to \Delta_n$, $\mathsf{match}^{n,U}(C[\,])$ est un contexte de type $T \to U^n \to U$.

Pour alléger les notations, on notera $\mathsf{fun}\ x_1^{T_1}\ \ldots\ x_n^{T_n} \to u$ pour $\mathsf{fun}\ {x_1}^{T_1} \to \ldots \to \mathsf{fun}\ {x_n}^{T_n} \to u$.

Si t est un terme simple de type T, $x_1, \ldots, x_n$ des variables distinctes de types respectifs $U_1, \ldots, U_n$ et $u_1, \ldots, u_n$ des termes simples de types respectifs $U_1, \ldots, U_n$, on note $t[x_1 := u_1, \ldots, x_1 := u_1]$ le terme simple de type T obtenu à partir de t en remplaçant simultanément chaque occurrence de x_i par u_i pour $i \in \{1, \ldots, n\}$ (sans capturer les variables libres des u_i).

Si $C[\,]$ est un contexte de type $U \to V$ et u un terme simple de type U, on note $C[u]$ le terme simple de type V obtenu en remplaçant l'unique occurrence de $[\,]$ dans $C[\,]$ par u (de façon compatible avec l'α-équivalence, c'est-à-dire sans capturer les variables libres de u : par exemple, si $C[\,] = \mathsf{fun}\ x \to x\ [\,]$ et $u = x$, alors $C[u] = \mathsf{fun}\ y \to y\ x$).

Enfin, si $C[\,]$ est un contexte de type $U \to V$ et $D[\,]$ un contexte de type $T \to U$, on note $C[D[\,]]$ le contexte de type $T \to V$ obtenu en remplaçant l'unique occurrence de $[\,]$ dans $C[\,]$ par $D[\,]$ (à nouveau sans capturer les variables libres de $D[\,]$).

Remarque. On considère seulement des contextes dont le « trou » $[\,]$ est en tête. En fait, il faut imaginer les termes simples et les contextes comme des suites de commandes à faire exécuter par une machine abstraite dans un certain environnement. Ainsi, le terme simple $C[t]$ correspond à la commande « exécuter $C[\,]$ puis exécuter t ». Le terme $\mathcal{cc}\ (\mathsf{fun}\ k \to t)$ correspond de son côté à la commande « sauvegarder l'environnement dans la variable k puis exécuter t ».

Un terme simple ou un contexte est *sans contrôle* s'il ne contient pas $\mathcal{cc}$.

4.1.2 Sémantique

Un *modèle de calcul fini* $\mathbb{C}$ est la donnée :

— pour tout type simple T, d'un ensemble ordonné fini non vide $(\llparenthesis T \rrparenthesis_{\mathbb{C}}, \sqsubseteq^T_{\mathbb{C}})$ dont toute partie non vide a une borne inférieure[i] (la *dénotation* de T), dont on notera $\Omega^T_{\mathbb{C}}$ le plus petit élément et $\wedge^T_{\mathbb{C}}$ l'opération (binaire) borne inférieure,

— pour tout type simple T, tout terme simple t de type T et toute liste de variables distinctes $x_1^{U_1}, \ldots, x_n^{U_n}$ contenant au moins toute les variables libres de t, d'une fonction $\llparenthesis x_1^{U_1}, \ldots, x_n^{U_n} \mid t \rrparenthesis_{\mathbb{C}}$[ii] de $\llparenthesis U_1 \rrparenthesis_{\mathbb{C}} \times \ldots \times \llparenthesis U_n \rrparenthesis_{\mathbb{C}}$ dans $\llparenthesis T \rrparenthesis_{\mathbb{C}}$ croissante en chacun de ses arguments (la *dénotation* de t).

tels que (pour toute instanciation adéquate des méta-variables) :

— $\llparenthesis \overline{x} \mid t[\overline{y} := \overline{u}] \rrparenthesis_{\mathbb{C}} = \llparenthesis \overline{y} \mid t \rrparenthesis_{\mathbb{C}} \circ \overline{\llparenthesis \overline{x} \mid u \rrparenthesis_{\mathbb{C}}}$,

— $\llparenthesis \overline{x} \mid x_k \rrparenthesis_{\mathbb{C}}$ est la k-ème projection de $\llparenthesis U_1 \rrparenthesis_{\mathbb{C}} \times \ldots \times \llparenthesis U_n \rrparenthesis_{\mathbb{C}}$ sur $\llparenthesis U_k \rrparenthesis_{\mathbb{C}}$,

— $\llparenthesis \overline{x} \mid \mathsf{fun}\ y^U \to t\ y \rrparenthesis_{\mathbb{C}} = \llparenthesis \overline{x} \mid t \rrparenthesis_{\mathbb{C}}$,

— $\llparenthesis \overline{x} \mid (\mathsf{fun}\ y^U \to t)u \rrparenthesis_{\mathbb{C}} \sqsupseteq \llparenthesis \overline{x} \mid t[y := u] \rrparenthesis_{\mathbb{C}}$,

— $\llparenthesis \overline{x} \mid \mathsf{match}^{n,U}\ \partial_k^n\ u_0 \ldots u_n \rrparenthesis_{\mathbb{C}} \sqsupseteq \llparenthesis \overline{x} \mid u_k \rrparenthesis_{\mathbb{C}}$,

— $\llparenthesis \overline{x} \mid C[\alpha^{T,U}(\mathsf{fun}\ k^{T\to U} \to t)] \rrparenthesis_{\mathbb{C}} = \llparenthesis \overline{x} \mid \alpha^{V,U}(\mathsf{fun}\ j^{V\to U} \to C[t[k := \mathsf{fun}\ x^T \to j\ C[x]]]) \rrparenthesis_{\mathbb{C}}$ ($C[\ ]$ contexte de type $T \to V$, t terme simple de type T),

— $\llparenthesis \overline{x} \mid \alpha^{T,U}\ (\mathsf{fun}\ k^{T\to U} \to C[k\ t]) \rrparenthesis_{\mathbb{C}} = \llparenthesis \overline{x} \mid \alpha^{T,U}\ (\mathsf{fun}\ k^{T\to U} \to t) \rrparenthesis_{\mathbb{C}}$ ($C[\ ]$ contexte de type $U \to T$, t terme simple de type T),

— $\llparenthesis \overline{x} \mid \alpha^{T,U}\ (\mathsf{fun}\ k^{T\to U} \to t) \rrparenthesis_{\mathbb{C}} = \llparenthesis \overline{x} \mid t \rrparenthesis_{\mathbb{C}}$ (si k n'est pas libre dans t).

Un *modèle de calcul fini sans contrôle* est défini de façon analogue, mais en ne demandant de définir $\llparenthesis x_1^{U_1}, \ldots, x_n^{U_n} \mid t \rrparenthesis_{\mathbb{C}}$ que lorsque t est in terme simple sans contrôle et en enlevant les conditions sur α.

S'il n'y a pas d'ambiguïté, on notera $\llparenthesis \ldots \rrparenthesis$ plutôt que $\llparenthesis \ldots \rrparenthesis_{\mathbb{C}}$ et $\sqsubseteq^T$, Ω^T et $\wedge^T$ (voire $\sqsubseteq$, Ω et $\wedge$) plutôt que $\sqsubseteq^T_{\mathbb{C}}$, $\Omega^T_{\mathbb{C}}$ et $\wedge^T_{\mathbb{C}}$.

Soit $\mathbb{C}$ un modèle de calcul fini :

— Étant donné un type simple T et a un élément de $\llparenthesis T \rrparenthesis$, on dit que a est *séquentiel* (ou que a est une *fonction séquentielle*) s'il existe un terme simple clos t de type T tel que $a = \llparenthesis t \rrparenthesis$. On note Seq^T l'ensemble des éléments séquentiels de $\llparenthesis T \rrparenthesis$.

— Étant donnés $T_1, \ldots, T_n, U$ des types simples et $a_1 \in \llparenthesis T_1 \rrparenthesis, \ldots, a_n \in \llparenthesis T_n \rrparenthesis, b \in \llparenthesis U \rrparenthesis$, on dit que b *est simulable par* $a_1, \ldots, a_n$ s'il existe un terme simple u de type U et une liste de variables distinctes $x_1^{T_1}, \ldots, x_n^{T_n}$ contenant au moins toute les variables libres de u tels que $\llparenthesis \overline{x} \mid u \rrparenthesis(\overline{a}) \sqsupseteq b$,

— Un *degré de parallélisme* de $\mathbb{C}$ est une $\mathcal{M}$-famille $X = (X_T)_{T \text{ type simple}}$ telle que

  — pour tout type simple T, X_T est un segment initial de $\llparenthesis T \rrparenthesis$,

  — pour tous $a_1 \in X_{T_1}, \ldots, a_n \in X_{T_n}$ et tout $b \in \llparenthesis U \rrparenthesis$, si b est simulable par $a_1, \ldots, a_n$ alors $b \in X_U$.

L'ensemble des degrés de parallélisme de $\mathbb{C}$, noté $\mathbb{P}_{\mathbb{C}}$, est naturellement ordonné par l'inclusion point-à-point et forme un treillis $\mathcal{M}$-complet dont la borne inférieure est donnée par l'intersection point-à-point. Son plus grand élément est la famille pleine $(\llparenthesis T \rrparenthesis)_{T \text{ type simple}}$ et son plus petit élément est la famille $(\mathsf{Seq}^T)_{T \text{ type simple}}$ des fonctions séquentielles.

On donne des définitions analogues dans le cas où $\mathbb{C}$ est un modèle de calcul fini sans contrôle en remplaçant *terme simple* par *terme simple sans contrôle*.

On va montrer à travers trois exemple que la théorie de la réalisabilité classique (et plus précisément, la construction ∃2) permet d'étudier la structure de l'ensemble des degrés de parallélisme de certains modèles de calcul fini. L'idée sera d'associer à tout $a \in \llparenthesis T \rrparenthesis$ une formule du langage des algèbres de Boole dont la force logique correspondra à la force calculatoire de a (c'est-à-dire à la position de a dans la hiérarchie des degrés de parallélisme).

i. C'est-à-dire d'un domaine de Scott fini.

ii. Que l'on notera également $\llparenthesis t \rrparenthesis_{\mathbb{C}}$ si $n = 0$.

4.2 Les domaines de Scott plats

Le premier exemple concerne un modèle de calcul fini sans contrôle : cela permettra d'expliquer dans un cadre simple des intuitions qui serviront par la suite.

On considère le modèle de calcul sans contrôle $\mathbb{C}_{\mathsf{Flat}}$ défini de la façon suivante[i] :

Interprétation des types :

— $(\!|\Delta_n|\!) = \{\Omega, 0, \ldots, n-1\}$ (où Ω est un $\mathcal{M}$-ensemble quelconque qui n'est pas dans $\mathbb{N}$), et pour tous $x, y \in (\!|\Delta_n|\!)$, $x \sqsubseteq^{\Delta_n} y$ si et seulement si $x = y$ ou $x = \Omega$,

— $(\!|T \to U|\!)$ est l'ensemble des fonctions croissantes de $(\!|T|\!)$ dans $(\!|U|\!)$, ordonné par la comparaison point-à-point.

(On peut vérifier que pour tout T, $(\!|T|\!)$ est bien un inf-semi-treillis fini.)

Interprétation des termes :

— $(\!|\overline{x} \mid \partial_k^n|\!)(\overline{a}) = k$,

— $(\!|\overline{x} \mid \Omega^T|\!)(\overline{a}) = \Omega^T$,

— $(\!|\overline{x} \mid x_i|\!)(\overline{a}) = a_i$,

— $(\!|\overline{x} \mid t\,u|\!)(\overline{a}) = (\!|\overline{x} \mid t|\!)(\overline{a})((\!|\overline{x} \mid u|\!)(\overline{a}))$,

— $(\!|\overline{x} \mid \mathsf{fun}\ y^U \to t|\!)(\overline{a})$ est la fonction qui à b associe $(\!|\overline{x}, y \mid t|\!)(\overline{a}, b)$ (comme les termes simples sont définis à α-équivalence près, on peut supposer que y n'est pas dans la liste $\overline{x}$),

— $(\!|\overline{x} \mid \mathsf{match}^{n,U}|\!)(\overline{a})$ est la fonction qui à $k, b_0, \ldots, b_{n-1}$ associe b_k si $k \neq \Omega$ et Ω^U sinon.

On peut vérifier que cette construction définit bien un modèle de calcul sans contrôle.

Pour simplifier, si $f \in (\!|T_1 \to \ldots \to T_n \to U|\!)$ et $t_1 \in (\!|T_1|\!), \ldots, t_n \in (\!|T_n|\!)$, on notera $f(t_1, \ldots, t_n)$ pour $f(t_1)\ldots(t_n)$.

4.2.1 Exemples de fonctions séquentielles et non séquentielles

Le type simple $\Delta_2 \to \Delta_2 \to \Delta_2$ représente les fonctions de deux arguments booléens à valeurs booléennes. On peut considérer les trois éléments suivants de sa dénotation $(\!|\Delta_2 \to \Delta_2 \to \Delta_2|\!)$:

— le *ou gauche* $\overrightarrow{\mathsf{or}}$, qui à x, y associe 1 si $x = 1$, y si $x = 0$ et Ω si $x = \Omega$,

— le *ou droit* $\overleftarrow{\mathsf{or}}$, qui à x, y associe 1 si $y = 1$, x si $y = 0$ et Ω si $y = \Omega$,

— le *ou parallèle* $\overleftrightarrow{\mathsf{or}}$, qui à x, y associe 1 si $x = 1$ ou $y = 1$, 0 si $x = y = 0$ et Ω dans les autres cas.

Les deux premiers sont séquentiels : en effet, $\overrightarrow{\mathsf{or}} = (\!|\mathsf{fun}\ x_2^\Delta\ y_2^\Delta \to \mathsf{match}\ x\ y\ x|\!)$ et $\overleftarrow{\mathsf{or}} = (\!|\mathsf{fun}\ x_2^\Delta\ y_2^\Delta \to \mathsf{match}\ y\ x\ y|\!)$ (on notera ces termes simples respectivement $\overrightarrow{or}$ et $\overleftarrow{\mathsf{or}}$). En revanche, le troisième ne l'est pas.

De la même façon, on peut définir un *et gauche* $\overrightarrow{\mathsf{and}}$, un *et droit* $\overleftarrow{\mathsf{and}}$ et un *et parallèle* $\overleftrightarrow{\mathsf{and}}$. Là encore, les deux premiers sont séquentiels, mais pas le troisième. De plus, le ou parallèle et le et parallèle sont équivalents, au sens où chacun est simulable par l'autre sans utiliser cc. En effet, en posant $\mathsf{neg} = (\mathsf{fun}\ x^{\Delta_2} \to \mathsf{match}\ x\ \partial_1\ \partial_0)$, on a :

— $(\!|o \mid \mathsf{fun}\ x^{\Delta_2}\ y^{\Delta_2} \to \mathsf{neg}\ (o\ (\mathsf{neg}\ x)\ (\mathsf{neg}\ y))|\!)\ \left(\overleftrightarrow{\mathsf{or}}\right) = \overleftrightarrow{\mathsf{and}}$,

i. Tous les objets définis dans cette section le sont par rapport à $\mathbb{C}_{\mathsf{Flat}}$, donc on omettra systématiquement le « $\mathbb{C}_{\mathsf{Flat}}$ » qu'ils devraient tous porter en indice.

— $(\!|a \mid \text{fun } x^{\Delta_2}\ y^{\Delta_2} \to \text{neg } (a\ (\text{neg } x)\ (\text{neg } y))|\!)\ \left(\overleftrightarrow{\text{and}}\right) = \overleftrightarrow{\text{or}}$.

Par ailleurs, pour tout entier naturel n, on peut considérer la *fonction de vote* $\text{vote}^n \in (\!|\Delta_n \to \Delta_n \to \Delta_n \to \Delta_n|\!)$ qui à x, y, z associe Ω si x, y et z sont deux à deux distincts et associe l'élément majoritaire parmi les trois sinon. Trakhtenbrot [Tra74] a montré que les fonctions $\overleftrightarrow{\text{or}}$ et vote^2 sont aussi équivalentes :

— $(\!|v \mid \text{fun } x_2^{\Delta}\ y_2^{\Delta} \to v\ (\overrightarrow{\text{or}}\ x\ y)\ (\overleftarrow{\text{or}}\ x\ y)\ \partial_1|\!)\ \left(\text{vote}^2\right) = \overleftrightarrow{\text{or}}$,

— $(\!|o, a \mid \text{fun } x_2^{\Delta}\ y_2^{\Delta}\ z_2^{\Delta} \to o\ (o\ (a\ x\ y)\ (a\ y\ z))\ (a\ z\ x)|\!)\ \left(\overleftrightarrow{\text{or}}, \overleftrightarrow{\text{and}}\right) = \text{vote}^2$ (et l'on a déjà vu que $\overleftrightarrow{\text{and}}$ est simulable par $\overleftrightarrow{\text{or}}$).

Enfin, on peut mentionner la *fonction de Gustave* [Ber76] $\text{gustave} \in (\!|\Delta_n \to \Delta_n \to \Delta_n \to \Delta_n|\!)$, définie comme la plus petite fonction telle que :

— $\text{gustave}(1, 0, \Omega) = \text{gustave}(\Omega, 1, 0) = \text{gustave}(0, \Omega, 1) = 1$,

— $\text{gustave}(0, 0, 0) = \text{gustave}(1, 1, 1) = 0$.

En particulier, pour tous $x, y, z \in \{0, 1\}$, $\text{gustave}(x, y, z)$ vaut 0 si x, y et z sont égaux et 1 sinon. Cette fonction n'est pas séquentielle, et l'on peut vérifier qu'elle est simulable par $\overleftrightarrow{\text{or}}$ (et donc par vote^2) mais pas l'inverse.

4.2.2 Traduction dans les algèbres de Boole

Comme on l'a dit plus haut, on veut associer à chaque type simple T et chaque $t \in (\!|T|\!)$ une formule du langage des algèbres de Boole, que l'on notera provisoirement F_t^T, qui représente le comportement de t, et dont la force logique corresponde à la position de t dans la hiérarchie des degrés de parallélisme. L'idée sera d'avoir :

— pour $k \in \{0, \ldots, n-1\}$, $F_k^{\Delta_n} \equiv \top \to \ldots \to \top \to \bot \to \top \to \ldots \to \top \to \bot$ (avec n arguments numérotés $0, \ldots, n-1$, dont le numéro k est $\bot$ et les autres $\top$),

— $F_f^{T \to U} \equiv \bigcap_{t \in (\!|T|\!)} (F_t^T \to F_{f(t)}^U)$,

— $F_t^T \leqq F_u^T$ si $t \sqsupseteq u$,

— $F_\Omega^T \equiv \top$.

Le premier point sert à faire en sorte que le réalisateur-type de $F_{(\!|\partial_k|\!)}^{\Delta_n}$ soit $\lambda x_0.\ \ldots \lambda x_{n-1}.\ x_k$.

Le deuxième point impose que la forme de F_t^T ne dépende que de T. Pour cela, on va définir pour chaque type T une formule $[\![T]\!]\,(x_1, \ldots, x_n)$ et pour chaque $t \in (\!|T|\!)$ un n-uplet $(a_1, \ldots, a_n) \in \{0, 1\}^n$, puis on prendra pour F_t^T la formule $[\![T]\!]\,(a_1, \ldots, a_n)$. Voici comment on va procéder :

Tout d'abord, pour tout type simple T, on fixe un entier ν_T et une surjection σ_T de $\{0, 1\}^{\nu_T}$ dans $(\!|T|\!)$ (ce que l'on peut faire puisque $(\!|T|\!)$ est fini), ainsi qu'un inverse à droite σ_T^* de σ_T.

Ensuite, pour toute fonction f de $(\!|T_1|\!) \times \ldots \times (\!|T_n|\!)$ dans $(\!|U|\!)$, on fixe une fonction $\widetilde{f} : \{0, 1\}^{\nu_{T_1}} \to \ldots \to \{0, 1\}^{\nu_{T_n}} \to \{0, 1\}^{\nu_U}$ telle que pour tous $(\overline{x}_1, \ldots, \overline{x}_n) \in \{0, 1\}^{\nu_{T_1} + \ldots + \nu_{T_n}}$, $\widetilde{f}(\overline{x}_1, \ldots, \overline{x}_n) = \sigma_U^*(f(\sigma_{T_1}(\overline{x}_1), \ldots, \sigma_{T_n}(\overline{x}_n)))$. Enfin, on fixe une liste de ν_U termes du langage des algèbres de Boole, que l'on notera également $\widetilde{f}(\overline{x}_1, \ldots, \overline{x}_n)$, dont l'interprétation dans l'algèbre de Boole $\{0, 1\}$ est la fonction $\widetilde{f}$.

En particulier, pour tous types simples T et U, on a donc une liste de termes $\widetilde{\text{app}}^{T,U}(\overline{f}^{\nu_{T \to U}}, \overline{x}^{\nu_T})$ telle que pour tous $\overline{f} \in \{0, 1\}^{\nu_{T \to U}}$ et tous $\overline{x} \in \{0, 1\}^{\nu_T}$, l'interprétation de la liste de termes $\widetilde{\text{app}}^{T,U}(\overline{f}, \overline{x})$ dans l'algèbre de Boole $\{0, 1\}$ est égale à $\sigma_U^*(\sigma_{T \to U}(\overline{f})(\sigma_T(\overline{x})))$.

Pour tout entier naturel n, pour tout $k \in (\!|\Delta_n|\!)$, on note δ_k^n la fonction de $\{0, 1\}^{\nu_{\Delta_n}}$ dans $\{0, 1\}$ qui à $\overline{x}$ associe 1 si $\sigma_{\Delta_n}(\overline{x}) = k$ et 0 sinon. Ensuite, on choisit un terme $\delta_k^n(\overline{x})$ du langage des algèbres de Boole dont l'interprétation dans $\{0, 1\}$ est la fonction δ_k^n.

Pour tout entier naturel n, on note $[\![\Delta_n]\!]\,(\overline{x}^{\nu_{\Delta_n}})$ la formule $\delta_0^n(\overline{x}^{\nu_{\Delta_n}}) \neq 1 \to \ldots \to \delta_{n-1}^n(\overline{x}^{\nu_{\Delta_n}}) \neq 1 \to \delta_\Omega^n(\overline{x}^{\nu_{\Delta_n}}) \neq 0$.

Enfin, pour tous types simples T et U, on note $[\![T \to U]\!]\left(\overline{f}^{\nu_{T\to U}}\right)$ la formule $\forall \overline{x}^{\nu T}\ \left([\![T]\!](\overline{x}) \to [\![U]\!]\left(\widetilde{\mathsf{app}}(\overline{f},\overline{x})\right)\right)$.

Avec ces définitions, on peut vérifier que l'on a bien :

— pour $k \in \{0,\dots,n-1\}$, $[\![\Delta_n]\!](\sigma^*(k)) \equiv \top \to \dots \to \top \to \bot \to \top \to \dots \to \top \to \bot$ (avec n arguments numérotés $0,\dots,n-1$, dont le numéro k est $\bot$ et les autres $\top$),

— $[\![T \to U]\!](\sigma^*(f)) \equiv \bigcap_{t\in(\!|T|\!)}([\![T]\!](\sigma^*(t)) \to [\![U]\!](\sigma^*(f(u))))$,

— $[\![T]\!](\sigma^*(t)) \leqq [\![T]\!](\sigma^*(u))$ si $t \sqsupseteq u$,

— $[\![T]\!]\left(\sigma^*\left(\Omega^T\right)\right) \equiv \top$.

4.2.3 Fonctions séquentielles

Proposition 4.1. Pour tout type simple T, pour tout terme simple sans contrôle f de type T et toute liste $x_1^{U_1},\dots,x_n^{U_n}$ de variables distinctes contenant toutes les variables libres de f, la formule

$$\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to T]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to f|\!))\right)$$

est universellement réalisée.

Démonstration. On va procéder par induction sur f :

— Si $f = \partial_k^m$ et $T = \Delta_m$, la formule $(\mathfrak{I}2 \models [\![T]\!](\sigma^*((\!|f|\!))) \equiv \top \to \dots \to \top \to \bot \to \top \to \dots \to \top \to \bot$ est universellement réalisée par $\lambda z_0.\ \dots \lambda z_{m-1}.\ z_k$, donc la formule $\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to T]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to f|\!))\right)$ est universellement réalisée par $\lambda y_1.\ \dots\ \lambda y_n.\ \lambda z_0.\ \dots \lambda z_{m-1}.\ z_k$.

— Si $f = \Omega^T$, la formule $\left(\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to T]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to f|\!))\right)\right) \equiv \top$ est universellement réalisée par n'importe quel terme.

— Si $f = x_j$ et $T = U_j$, la formule $\left(\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to T]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to f|\!))\right)\right) \equiv \mathfrak{I}2 \models \bigcup_{x_1\in(\!|U_1|\!)}\cdots\bigcup_{x_n\in(\!|U_n|\!)}([\![U_1]\!](\sigma^*(x_1)) \to \dots \to [\![U_n]\!](\sigma^*(x_n)) \to [\![U_j]\!](\sigma^*(x_j)))$ est réalisée par le terme $\lambda y_1.\ \dots\ \lambda y_n.\ y_j$.

— Si $f = ab$ avec a de type $V \to T$ et b de type V, et si les formules $\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to (V \to T)]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to a|\!))\right)$ et $\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to V]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to v|\!))\right)$ sont universellement réalisées par t et v respectivement, alors la formule

$$\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to T]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to f|\!))\right)$$

est universellement réalisée par $\lambda y_1.\dots.\ \lambda y_n.\ (ty_1\dots y_n)(vy_1\dots y_n)$.

— Si $f = \mathsf{fun}\ z^V \to w$ avec w de type W et $T = V \to W$, et si la formule $\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to V \to W]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n}\ z^V \to t|\!))\right)$ est réalisée par un terme t, alors la formule $\mathfrak{I}2 \models [\![U_1 \to \dots \to U_n \to T]\!]\left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \dots\ x_n^{U_n} \to f|\!))\right)$ est réalisée par le même terme t.

— Si $f = \mathsf{match}^{m,V}$ et $T = \Delta_m \to V^m \to V$, on a pour tout pôle $\perp\!\!\!\perp$:

  — pour tout $j \in \{0\dots,n-1\}$, on a $\mathfrak{I}2 \models \|[\![\Delta_m]\!](j)\|_{\perp\!\!\!\perp} = \{\ v_0 \bullet \dots \bullet v_{m-1} \bullet \pi;\ v_j \Vdash_{\perp\!\!\!\perp} \bot\ \}$ et $\left\|\mathfrak{I}2 \models [\![V^m \to V]\!]\left((\!|\mathsf{match}^{m,V}|\!)(j)\right)\right\|_{\perp\!\!\!\perp} \subseteq \{\ v_0 \bullet \dots \bullet v_{m-1} \bullet \pi;\ v_j \star \pi \in \perp\!\!\!\perp\ \}$,

  — $\|\mathfrak{I}2 \models [\![\Delta_m]\!](\Omega)\|_{\perp\!\!\!\perp} = \left\|\mathfrak{I}2 \models [\![V^m \to V]\!]\left((\!|\mathsf{match}^{m,V}|\!)(\Omega)\right)\right\|_{\perp\!\!\!\perp}$,

par conséquent, la formule $\mathfrak{I}2 \models [\![\Delta_m \to V^m \to V]\!] \left(\sigma^*((\!|\mathsf{match}^{m,V}|\!))\right)$ est universellement réalisée par $\lambda d.\ \lambda v_0.\ \ldots\ \lambda v_{m-1}.\ cc\ (\lambda k.\ d(kv_0)\ldots(kv_{m-1}))$, et donc la formule

$$\mathfrak{I}2 \models [\![U_1 \to \ldots \to U_n \to T]\!] \left(\sigma^*((\!|\mathsf{fun}\ x_1^{U_1}\ \ldots\ x_n^{U_n} \to f|\!))\right)$$

est universellement réalisée.

□

D'après le théorème 3.19, on a les corollaires suivants :

Corollaire. Pour tout type simple T, pour tout terme simple sans contrôle clos f de type T, la formule $[\![T]\!]\ (\sigma^*((\!|t|\!)))$ est vraie dans toute algèbre de Boole à au moins deux éléments.

Corollaire. Pour tous types simples $T_1, \ldots, T_n, U$, pour tous $a_1 \in (\!|T_1|\!), \ldots, a_n \in (\!|T_n|\!), b \in (\!|U|\!)$, si b est simulable par $a_1, \ldots, a_n$, alors la formule $[\![U]\!]\ (\sigma^*(b))$ est conséquence de $\{\ [\![T_1]\!]\ (\sigma^*(a_1)), \ldots, [\![T_n]\!]\ (\sigma^*(a_n))\ \}$.

Dans ce dernier corollaire, on voit se dessiner une correspondance entre les degrés de parallélisme et les extensions de la théorie des algèbres de Boole à au moins deux éléments. Cependant, pour que cette correspondance soit complète, il faudrait pouvoir donner une réciproque à ce corollaire, et l'absence de traduction pour cc nous en empêche : s'il faut utiliser la loi de Peirce pour déduire $[\![U]\!]\ (\sigma^*(b))$ à partir de $\{\ [\![T_1]\!]\ (\sigma^*(a_1)), \ldots, [\![T_n]\!]\ (\sigma^*(a_n))\ \}$, alors on voit mal comment simuler b par $a_1, \ldots, a_n$ sans utiliser cc.

Dans les sections suivantes, on présentera donc des modèles de calcul fini *avec contrôle* ainsi que les traductions correspondantes vers le langage des algèbres de Boole, et l'on verra que la correspondance fonctionne pleinement.

4.2.4 Retour sur le ou parallèle et les fonctions de vote

Avant de laisser de côté ce modèle de calcul sans contrôle, on peut se demander ce que « signifient » les formules $[\![\Delta_2 \to \Delta_2 \to \Delta_2]\!]\ (\sigma^*(\overleftrightarrow{\mathsf{or}}))$ et $[\![\Delta_2 \to \Delta_2 \to \Delta_2 \to \Delta_2]\!]\ (\sigma^*(\mathsf{vote}^2))$, c'est-à-dire quelle est la classe des algèbres de Boole à au moins deux éléments qui les vérifient (comme ces deux fonctions sont simulables l'une par l'autre sans utiliser cc, d'après le deuxième corollaire de la proposition 4.1, elles doivent correspondre à la même classe). D'après le corollaire du théorème 3.9, on peut s'attendre à ce qu'il s'agisse de la classe des algèbres de Boole à au moins deux éléments et au plus quatre éléments, et c'est effectivement ce que l'on va montrer :

Proposition 4.2. Une algèbre de Boole à au moins deux éléments vérifie $[\![\Delta_2 \to \Delta_2 \to \Delta_2]\!]\ (\sigma^*(\overleftrightarrow{\mathsf{or}}))$ si et seulement si elle a au plus quatre éléments.

Démonstration. On a

$$\begin{array}{rcl}
[\![\Delta_2 \to \Delta_2 \to \Delta_2]\!]\ (\overleftrightarrow{\mathsf{or}}) \equiv & (\top \to \bot \to \bot) & \to\ \top\ \to\ (\top \to \bot \to \bot) \\
\cap & \top & \to\ (\top \to \bot \to \bot)\ \to\ (\top \to \bot \to \bot) \\
\cap & (\bot \to \top \to \bot) & \to\ (\bot \to \top \to \bot)\ \to\ (\bot \to \top \to \bot)
\end{array}$$

$$\equiv \quad \forall x\ \forall y \begin{pmatrix} & (x \neq 0 \to x \neq 1 \to (y \wedge \neg x) \neq 0) \\ \to & (y \neq 0 \to y \neq 1 \to (x \wedge \neg y) \neq 0) \\ \to & ((x \vee y) \neq 0 \to (x \vee y) \neq 1 \to \bot) \end{pmatrix}.$$

□

Corollaire. Une algèbre de Boole à au moins deux éléments vérifie $[\![\Delta_2 \to \Delta_2 \to \Delta_2 \to \Delta_2]\!]\ (\sigma^*(\mathsf{vote}^2))$ si et seulement si elle a au plus quatre éléments.

Par des arguments similaires, on peut montrer le résultat suivant :

Proposition 4.3. Une algèbre de Boole à au moins deux éléments vérifie $[\![\Delta_2 \to \Delta_2 \to \Delta_2 \to \Delta_2]\!]\ (\sigma^*(\mathsf{gustave}))$ si et seulement si elle a au plus huit éléments.

4.3 L'espace de Sierpinski

Streicher & Reus [SR98] ont montré que l'espace de Sierpinski (qui correspond à la construction D_∞ de Scott lorsque D est le treillis à deux éléments) donne un modèle de continuations du λ_c calcul. On va s'inspirer de cette construction pour produire un modèle de calcul fini $\mathbb{C}_{\mathsf{Sierp}}$ [i] :

Interprétation des types. Tout d'abord, on munit l'ensemble $\Sigma = \{\Omega, 0\}$ d'une relation d'ordre $\sqsubseteq^\Sigma$ (que l'on pourra noter simplement $\sqsubseteq$) en posant $a \sqsubseteq^\Sigma b$ si et seulement si $a = b$ ou $a = \Omega$. On va définir $\mathbb{C}_{\mathsf{Sierp}}$ en utilisant une traduction CPS avec Σ comme type de réponse.

Pour l'interprétation des types, on pose :

— $(\!|T \to U|\!)$ est l'ensemble des fonctions croissantes de $(\!|T|\!)$ dans $(\!|U|\!)$, ordonné par la comparaison point-à-point.

— $(\!|\Delta_0|\!) = \Sigma$ (Δ_0 va donc jouer à la fois le rôle du type sans constructeur et le rôle du type des réponses : pour la première utilisation, on continuera de le noter Δ_0, et pour la seconde, on le notera plutôt Σ, de sorte que $(\!|\Sigma|\!) = \Sigma$),

— $(\!|\Delta_n|\!) = (\!|\Sigma^n \to \Sigma|\!)$.

On peut vérifier que tout tout T, $(\!|T|\!)$ est bien un inf-semi-treillis fini, et même un treillis dont le plus grand élément est la fonction constante égale à 0 et le plus petit la fonction constante égale à Ω.

Pour simplifier, si $f \in (\!|T_1 \to \ldots \to T_n \to U|\!)$ et $t_1 \in (\!|T_1|\!), \ldots, t_n \in (\!|T_n|\!)$, on notera $f(t_1, \ldots, t_n)$ pour $f(t_1)\ldots(t_n)$.

Traduction CPS. Pour tout type simple T, on note T^{cps} le type simple obtenu en remplaçant dans T chaque Δ_n par $\Sigma^n \to \Sigma$: on a donc $(\!|T^{\mathsf{cps}}|\!) = (\!|T|\!)$.

On associe de façon injective à tout couple (T, x^T) (où T est un type simple et x^T une variable de type T) une variable de type T^{cps} que l'on notera $x^{T^{\mathsf{cps}}}$.

Pour tous types simples $S = \overline{R} \to \Delta_n$ et $V = \overline{U} \to \Delta_p$, on note $(\mathsf{cont}^{S,V})^{\mathsf{cps}}$ (ou simplement $\mathsf{cont}^{\mathsf{cps}}$ s'il n'y a pas d'ambiguïté) le terme simple clos de type $\overline{R}^{\mathsf{cps}} \to \Sigma^n \to (S \to V)^{\mathsf{cps}}$ suivant [ii] :

$$\mathsf{fun}\ \overline{r}^{\overline{R}^{\mathsf{cps}}}\ \overline{x}^{n\Sigma}\ s^{S^{\mathsf{cps}}}\ \overline{u}^{\overline{U}^{\mathsf{cps}}}\ \overline{y}^{p\Sigma} \to s\ \overline{r}\ \overline{x}^n.$$

Pour tout type simple T et tout terme simple t de type T, on définit un terme simple t^{cps} de type T^{cps} en posant :

— $(x^T)^{\mathsf{cps}} = x^{T^{\mathsf{cps}}}$,

— $(tu)^{\mathsf{cps}} = t^{\mathsf{cps}} u^{\mathsf{cps}}$,

— $(\mathsf{fun}\ x^T \to u)^{\mathsf{cps}} = \mathsf{fun}\ x^{T^{\mathsf{cps}}} \to u^{\mathsf{cps}}$,

— $(\Omega^T)^{\mathsf{cps}} = \Omega^{T^{\mathsf{cps}}}$,

— $(\partial_k^n)^{\mathsf{cps}} = \mathsf{fun}\ x_0^\Sigma\ \ldots\ x_{n-1}^\Sigma \to x_k$,

— Si $U = \overline{T} \to \Delta_p$, alors $(\mathsf{match}^{n,U})^{\mathsf{cps}} = \mathsf{fun}\ k^{\Sigma^n \to \Sigma}\ \overline{u}^{nU^{\mathsf{cps}}}\ \overline{t}^{\overline{T}^{\mathsf{cps}}}\ \overline{x}^{p\Sigma} \to k\ (u_0\ \overline{t}\ \overline{x})\ldots(u_{n-1}\ \overline{t}\ \overline{x})$,

— Si $S = \overline{R} \to \Delta_n$, alors $(\mathfrak{cc}^{S,V})^{\mathsf{cps}} = \mathsf{fun}\ f^{((S\to V)\to S)^{\mathsf{cps}}}\ \overline{r}^{\overline{R}^{\mathsf{cps}}}\ \overline{x}^{n\Sigma} \to f\ ((\mathsf{cont}^{S,V})^{\mathsf{cps}}\ \overline{r}\ \overline{x}^n)$.

On dit qu'un type simple T est *CPS-traduit* s'il s'écrit sans utiliser Δ_n pour $n > 0$ (ce qui revient à dire que $T^{\mathsf{cps}} = T$).

i. Tous les objets définis dans cette section le sont par rapport à $\mathbb{C}_{\mathsf{Sierp}}$, donc on omettra systématiquement le « $\mathbb{C}_{\mathsf{Sierp}}$ » qu'ils devraient tous porter en indice.

ii. Il s'agit d'une notation purement formelle, puisqu'il n'y a pas de terme simple $\mathsf{cont}^{S,V}$.

On dit qu'un terme simple t est *CPS-traduit* s'il ne contient ni $\mathtt{match}$, ni $\mathscr{C}$, ni aucun sous-terme d'un type non CPS-traduit. Le type d'un terme simple CPS-traduit est nécessairement lui-même CPS-traduit. Pour tout contexte t, t^{cps} est CPS-traduit.

Pour tout terme simple CPS-traduit t et toute liste $x_1^{U_1}, \ldots, x_n^{U_n}$ de variables distinctes contenant toutes les variables libres de t, $t^{\mathrm{cps}} = t[x_1^{U_1} := x_1^{U_1{}^{\mathrm{cps}}}, \ldots, x_n^{U_n} := x_1^{U_n{}^{\mathrm{cps}}}]$ (les termes simples sont considérés modulo α-équivalence). En particulier, si t est clos et CPS-traduit, alors $t^{\mathrm{cps}} = t$.

Pour tous types simples T et U et tout contexte $C[\,]$ de type $T \to U$, on définit un contexte $C^{\mathrm{cps}}[\,]$ de type $T^{\mathrm{cps}} \to U^{\mathrm{cps}}$ en posant :

— $([\,]^T)^{\mathrm{cps}} = [\,]^{T^{\mathrm{cps}}}$,

— $(\mathsf{fun}\ x^V \to C[\,])^{\mathrm{cps}} = \mathsf{fun}\ x^{V^{\mathrm{cps}}} \to C^{\mathrm{cps}}[\,]$,

— $(C[\,]\ u)^{\mathrm{cps}} = C^{\mathrm{cps}}[\,]\ u^{\mathrm{cps}}$,

— Si $U = \overline{V} \to \Delta_m$, $(\mathsf{match}^{n,U}\, C[\,])^{\mathrm{cps}} = \mathsf{fun}\ \overline{u}^{nU^{\mathrm{cps}}}\ \overline{v}^{\overline{V}^{\mathrm{cps}}}\ \overline{x}^{m\Sigma} \to C^{\mathrm{cps}}[\,]\ \overline{(u\ \overline{v}\ \overline{x})}$,

On dit qu'un contexte $C[\,]$ est *CPS-traduit* s'il ne contient ni $\mathtt{match}$, ni $\mathscr{C}$, ni aucun sous-terme d'un type non CPS-traduit. Le type d'un contexte CPS-traduit est nécessairement lui-même CPS-traduit. Pour tout contexte $C[\,]$, $C[\,]^{\mathrm{cps}}$ est CPS-traduit.

On peut vérifier que l'on a toujours $C^{\mathrm{cps}}[t^{\mathrm{cps}}] = C[t]^{\mathrm{cps}}$.

Interprétation des termes. On définit $(\!|x_1^{U_1}, \ldots, x_m^{U_m} \mid t|\!)_{\mathbb{C}_{\mathsf{Sierp}}}$ quand t et $U_1, \ldots, U_m$ sont CPS-traduits en posant :

— $(\!|\overline{x} \mid \Omega^T|\!)(\overline{a}) = \Omega^T$,

— $(\!|\overline{x} \mid x_i|\!)(\overline{a}) = a_i$,

— $(\!|\overline{x} \mid tu|\!)(\overline{a}) = (\!|\overline{x} \mid t|\!)(\overline{a})((\!|\overline{x} \mid u|\!)(\overline{a}))$,

— $(\!|\overline{x} \mid \mathsf{fun}\ y^V \to t|\!)(\overline{a})$ est la fonction qui à b associe $(\!|\overline{x}, y \mid t|\!)(\overline{a}, b)$ (comme les termes simples sont définis à α-équivalence près, on peut supposer que y n'est pas dans la liste $\overline{x}$),

Enfin, si t ou l'un des U_j n'est pas CPS-traduit, on pose $(\!|x_1^{U_m}, \ldots, x_m^{U_m} \mid t|\!) = (\!|x_1^{U_1{}^{\mathrm{cps}}}, \ldots, x_m^{U_m{}^{\mathrm{cps}}} \mid t^{\mathrm{cps}}|\!)$.

On peut vérifier qu'avec cette définition, on a toujours $(\!|x_1^{U_m}, \ldots, x_m^{U_m} \mid t|\!) = (\!|x_1^{U_1{}^{\mathrm{cps}}}, \ldots, x_m^{U_m{}^{\mathrm{cps}}} \mid t^{\mathrm{cps}}|\!)$, y compris quand t et $U_1, \ldots, U_m$ sont CPS-traduits.

Proposition 4.4. Ceci définit bien un modèle de calcul fini.

Démonstration.

1. Par construction, $\mathbb{C}_{\mathsf{Sierp}}$ vérifie au moins :

— $(\!|\overline{x} \mid t[\overline{y} := \overline{u}]|\!) = (\!|\overline{y} \mid t|\!) \circ \overline{(\!|\overline{x} \mid u|\!)}$,

— $(\!|\overline{x} \mid x_k|\!)$ est la k-ème projection de $(\!|U_1|\!) \times \ldots \times (\!|U_n|\!)$ sur $(\!|U_k|\!)$,

— $(\!|\overline{x} \mid \mathsf{fun}\ y^U \to t\ y|\!) = (\!|\overline{x} \mid t|\!)$,

— $(\!|\overline{x} \mid (\mathsf{fun}\ y^U \to t)u|\!) = (\!|\overline{x} \mid t[y := u]|\!)$.

2. Soient n un entier naturel, $k \in \{0, \ldots, n-1\}$, $U = V_1 \to \ldots \to V_m \to \Delta_q$ un type simple, $u_1, \ldots, u_n$ des termes simples de type U et $x_1^{T_1}, \ldots, x_p^{T_p}$ une liste de variables deux à deux distinctes contenant au moins

toutes les variables libres de $u_1, \ldots, u_n$. Pour tous $t_1 \in (\!|T_1|\!), \ldots, t_p \in (\!|T_p|\!)$, $v_1 \in (\!|V_1|\!), \ldots, v_m \in (\!|V_m|\!)$, $\overline{s}^q \in \Sigma$, on a

$$\begin{array}{rl}
& (\!|\overline{x}^{\overline{T}} \mid \mathsf{match}^{n,U}\ \partial_k^n\ \overline{u}|\!)(\overline{t})(\overline{v},\overline{s}) \\
= & (\!|\overline{x}^{\overline{T}^{\mathsf{cps}}} \mid (\mathsf{match}^{n,U}\ \partial_k^n\ \overline{u})^{\mathsf{cps}}|\!)(\overline{t})(\overline{v},\overline{s}) \\
= & (\!|\overline{x}^{\overline{T}^{\mathsf{cps}}} \mid \left(\mathsf{fun}\ k^{\Sigma^n\to\Sigma}\ \overline{y}^{nU^{\mathsf{cps}}}\ \overline{z}^{m\overline{V}^{\mathsf{cps}}}\ \overline{w}^{q\Sigma} \to k\ \overline{(y\ \overline{z}\ \overline{w})}\right)\ (\mathsf{fun}\ \overline{r}^{n\Sigma} \to r_k)\ \overline{u}^{\mathsf{cps}}|\!)\ (\overline{t})(\overline{v},\overline{s}) \\
= & (\!|\overline{x}^{\overline{T}^{\mathsf{cps}}}\ \overline{z}^{\overline{V}^{\mathsf{cps}}}\ \overline{w}^{q\Sigma} \mid u_k\ \overline{z}\ \overline{w}|\!)(\overline{t},\overline{v},\overline{s}) \\
= & (\!|\overline{x}^{\overline{T}} \mid u_k|\!)(\overline{t})(\overline{v},\overline{s}),
\end{array}$$

par conséquent $(\!|\overline{x}^{\overline{T}} \mid \mathsf{match}^{n,U}\ \partial_k^n\ \overline{u}|\!) = (\!|\overline{x}^{\overline{T}} \mid u_k|\!)$.

2. On remarque que pour tout contexte $C[\,]$ CPS-traduit de type $(\overline{S}\to\Sigma)\to(\overline{W}\to\Sigma)$ et toute liste $\overline{x}^{\overline{X}}$ de variables libres distinctes contenant toutes les variables libres de $C[\,]$, on peut trouver des variables $\overline{z}^{\overline{W}}$ (deux à deux distinctes et distinctes des $\overline{x}$) et des termes $\overline{s}$ de types $\overline{S}$ sans variables libres autres que $\overline{x},\overline{z}$ tels que pour tous $\overline{\xi}\in\overline{(\!|X|\!)}$,tout $r\in(\!|\overline{S}\to\Sigma|\!)$ et tous $\overline{w}\in\overline{(\!|W|\!)}$,

$$(\!|\overline{x}\ \rho \mid C[\rho]|\!)(\overline{\xi},r)(\overline{w}) = (\!|\overline{x}\ \rho\ \overline{z} \mid \rho\ \overline{s}|\!)(\overline{\xi},r,\overline{w}).$$

3. Soient $R=\overline{S}\to\Delta_m$, $T=\overline{U}\to\Delta_n$ et $V=\overline{W}\to\Delta_p$ des types simples, $C[\,]$ un contexte de type $R\to V$, r un terme simple de type R et $\overline{x}^{\overline{X}}$ une liste de variables distinctes contenant toutes les variables libres de $C[\,]$ et de $\mathsf{fun}\ k^{R\to T}\to r$. Pour tous $\overline{\xi}\in\overline{(\!|X|\!)}$, tous $\overline{w}\in\overline{(\!|W|\!)}$ et tous $\overline{c}^p\in\Sigma$, on a

$$\begin{array}{rl}
& (\!|\overline{x}^{\overline{X}} \mid C[\mathfrak{cc}^{R,T}\ (\mathsf{fun}\ k^{R\to T}\to r)]|\!)(\overline{\xi})(\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}} \mid C^{\mathsf{cps}}[(\mathfrak{cc}^{R,T})^{\mathsf{cps}}\ (\mathsf{fun}\ k^{R^{\mathsf{cps}}\to T^{\mathsf{cps}}}\to r^{\mathsf{cps}})]|\!)(\overline{\xi})(\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}}\ \overline{z}^{\overline{W}^{\mathsf{cps}}}\ \overline{\gamma}^{p\Sigma} \mid (\mathfrak{cc}^{R,T})^{\mathsf{cps}}\ (\mathsf{fun}\ k^{R^{\mathsf{cps}}\to T^{\mathsf{cps}}}\to r^{\mathsf{cps}})\ \overline{s}\ \overline{\alpha}^m|\!)(\overline{\xi},\overline{w},\overline{c})
\end{array}$$

[pour certains termes $\overline{s}$ de types S^{cps} et certains termes $\overline{\alpha}^m$ de type Σ (d'après la remarque 2. ci-dessus)]

$$\begin{array}{rl}
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}}\ \overline{z}^{\overline{W}^{\mathsf{cps}}}\ \overline{\gamma}^{p\Sigma} \mid r^{\mathsf{cps}}[k := (\mathsf{cont}^{R,T})^{\mathsf{cps}}\ \overline{s}\ \overline{\alpha}]\ \overline{s}\ \overline{\alpha}|\!)(\overline{\xi},\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}}\ \overline{z}^{\overline{W}^{\mathsf{cps}}}\ \overline{\gamma}^{p\Sigma} \mid r^{\mathsf{cps}}[k := \mathsf{fun}\ \rho^R\ \overline{y}^{\overline{U}}\ \overline{\beta}^{n\Sigma}\to\rho\ \overline{s}\ \overline{\alpha}]\ \overline{s}\ \overline{\alpha}|\!)(\overline{\xi},\overline{w},\overline{c}).
\end{array}$$

Par ailleurs,

$$\begin{array}{rl}
& (\!|\overline{x}^{\overline{X}} \mid \mathfrak{cc}^{V,T}(\mathsf{fun}\ j^{V\to T}\to C[r[k := \mathsf{fun}\ \rho^R\to j\ C[\rho]]])|\!)(\overline{\xi})(\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}} \mid (\mathfrak{cc}^{V,T})^{\mathsf{cps}}(\mathsf{fun}\ j^{V^{\mathsf{cps}}\to T^{\mathsf{cps}}}\to C^{\mathsf{cps}}[r^{\mathsf{cps}}[k := \mathsf{fun}\ \rho^{R^{\mathsf{cps}}}\to j\ C^{\mathsf{cps}}[\rho]]])|\!)(\overline{\xi})(\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}}\ \overline{z}^{\overline{W}^{\mathsf{cps}}}\ \overline{\gamma}^{p\Sigma} \mid C^{\mathsf{cps}}[r^{\mathsf{cps}}[k := \mathsf{fun}\ \rho^{R^{\mathsf{cps}}}\to(\mathsf{fun}\ \overline{y}^{\overline{U}}\ \overline{\beta}^{n\Sigma}\to C^{\mathsf{cps}}[\rho]\ \overline{z}\ \overline{\gamma})]]\ \overline{z}\ \overline{\gamma}|\!)(\overline{\xi},\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}}\ \overline{z}^{\overline{W}^{\mathsf{cps}}}\ \overline{\gamma}^{p\Sigma} \mid C^{\mathsf{cps}}[r^{\mathsf{cps}}[k := \mathsf{fun}\ \rho^{R^{\mathsf{cps}}}\to(\mathsf{fun}\ \overline{y}^{\overline{U}}\ \overline{\beta}^{n\Sigma}\to\rho\ \overline{s}\ \overline{\alpha})]]\ \overline{z}\ \overline{\gamma}|\!)(\overline{\xi},\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}}\ \overline{z}^{\overline{W}^{\mathsf{cps}}}\ \overline{\gamma}^{p\Sigma} \mid C^{\mathsf{cps}}[r^{\mathsf{cps}}[k := \mathsf{fun}\ \rho^{R^{\mathsf{cps}}}\ \overline{y}^{\overline{U}}\ \overline{\beta}^{n\Sigma}\to\rho\ \overline{s}\ \overline{\alpha}]]\ \overline{z}\ \overline{\gamma}|\!)(\overline{\xi},\overline{w},\overline{c}) \\
= & (\!|\overline{x}^{\overline{X}^{\mathsf{cps}}}\ \overline{z}^{\overline{W}^{\mathsf{cps}}}\ \overline{\gamma}^{p\Sigma} \mid r^{\mathsf{cps}}[k := \mathsf{fun}\ \rho^{R^{\mathsf{cps}}}\ \overline{y}^{\overline{U}}\ \overline{\beta}^{n\Sigma}\to\rho\ \overline{s}\ \overline{\alpha}]\ \overline{s}\ \overline{\alpha}|\!)(\overline{\xi},\overline{w},\overline{c}),
\end{array}$$

Par conséquent, $(\!|\overline{x}^{\overline{X}} \mid C[\mathfrak{cc}^{R,T}\ (\mathsf{fun}\ k^{R\to T}\to r)]|\!) = (\!|\overline{x}^{\overline{X}} \mid \mathfrak{cc}^{V,T}(\mathsf{fun}\ j^{V\to T}\to C[r[k := \mathsf{fun}\ \rho^R\to j\ C[\rho]]])|\!)$.

4. Soient $T=\overline{U}\to\Delta_n$ et $V=\overline{W}\to\Delta_p$ des types simples, $C[\,]$ un contexte de type $V\to T$, t un terme simple de type T et $\overline{x}^{\overline{X}}$ une liste de variables distinctes contenant toutes les variables libres de

$\mathsf{fun}\ k^{T\to V} \to C[k\ t]$ et de $\mathsf{fun}\ k^{T\to V} \to t$. Pour tous $\overline{\xi} \in \overline{(\!|X|\!)}$, tous $\overline{u} \in \overline{(\!|U|\!)}$ et tous $\overline{b}^n \in \Sigma$, on a

$$\begin{aligned}
& (\!|\overline{x}^{\overline{X}} \mid \mathcal{CC}^{T,V}\ (\mathsf{fun}\ k^{T\to U} \to C[k\ t])|\!)(\overline{\xi})(\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}} \mid (\mathcal{CC}^{T,V})^{\mathrm{cps}}\ (\mathsf{fun}\ k^{T^{\mathrm{cps}}\to V^{\mathrm{cps}}} \to C^{\mathrm{cps}}[k\ t^{\mathrm{cps}}])|\!)(\overline{\xi})(\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}}\ \overline{y}^{\overline{U}^{\mathrm{cps}}}\ \overline{\beta}^{\Sigma} \mid (\mathcal{CC}^{T,V})^{\mathrm{cps}}\ (\mathsf{fun}\ k^{T^{\mathrm{cps}}\to V^{\mathrm{cps}}} \to C^{\mathrm{cps}}[k\ t^{\mathrm{cps}}])\ \overline{y}\ \overline{\beta}|\!)(\overline{\xi},\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}}\ \overline{y}^{\overline{V}^{\mathrm{cps}}}\ \overline{\beta}^{\Sigma} \mid C^{\mathrm{cps}}[(\mathsf{cont}^{T,V})^{\mathrm{cps}}\ \overline{y}\ \overline{\beta}\ t^{\mathrm{cps}}[k := (\mathsf{cont}^{T,V})^{\mathrm{cps}}\ \overline{y}\ \overline{\beta}]]\ \overline{y}\ \overline{\beta}|\!)(\overline{\xi},\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}}\ \overline{y}^{\overline{U}^{\mathrm{cps}}}\ \overline{\beta}^{\Sigma} \mid (\mathsf{cont}^{T,V})^{\mathrm{cps}}\ \overline{y}\ \overline{\beta}\ t^{\mathrm{cps}}[k := (\mathsf{cont}^{T,V})^{\mathrm{cps}}\ \overline{y}\ \overline{\beta}]\ \overline{w}\ \overline{\gamma}|\!)(\overline{\xi},\overline{u},\overline{b}) \\
& \text{[pour certains termes } \overline{w} \text{ de types } \overline{W}^{\mathrm{cps}} \text{ et certains termes } \overline{\gamma}^p \text{ de type } \Sigma \text{ (d'après la remarque 2. ci-dessus)]} \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}}\ \overline{y}^{\overline{U}^{\mathrm{cps}}}\ \overline{\beta}^{\Sigma} \mid t^{\mathrm{cps}}[k := (\mathsf{cont}^{T,V})^{\mathrm{cps}}\ \overline{y}\ \overline{\beta}]\ \overline{y}\ \overline{\beta}|\!)(\overline{\xi},\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}}\ \overline{y}^{\overline{U}^{\mathrm{cps}}}\ \overline{\beta}^{\Sigma} \mid (\mathcal{CC}^{T,V})^{\mathrm{cps}}\ (\mathsf{fun}\ k^{T^{\mathrm{cps}}\to V^{\mathrm{cps}}} \to t^{\mathrm{cps}})\ \overline{y}\ \overline{\beta}|\!)(\overline{\xi},\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}} \mid \mathcal{CC}^{T,V}\ (\mathsf{fun}\ k^{T\to V} \to t)|\!)(\overline{\xi})(\overline{u},\overline{b}).
\end{aligned}$$

Par conséquent, $(\!|\overline{x} \mid \mathcal{CC}^{T,V}\ (\mathsf{fun}\ k^{T\to V} \to C[k\ t])|\!) = (\!|\overline{x} \mid \mathcal{CC}^{T,V}\ (\mathsf{fun}\ k^{T\to V} \to t)|\!)$.

5. Soient $T = \overline{U} \to \Delta_n$ et $V = \overline{W} \to \Delta_p$ des types simples, $C[\,]$ un contexte de type $V \to T$, t un terme simple de type T et $\overline{x}^{\overline{X}}$ une liste de variables distinctes contenant toutes les variables libres de t et $k^{T\to V}$ une variable qui n'est pas libre dans t. Pour tous $\overline{\xi} \in \overline{(\!|X|\!)}$, tous $\overline{u} \in \overline{(\!|U|\!)}$ et tous $\overline{b}^n \in \Sigma$, on a

$$\begin{aligned}
& (\!|\overline{x}^{\overline{X}} \mid \mathcal{CC}^{T,V}\ (\mathsf{fun}\ k^{T\to V} \to t)|\!)(\overline{\xi})(\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}}\ \overline{y}^{\overline{U}^{\mathrm{cps}}}\ \overline{\beta}^{\Sigma} \mid (\mathcal{CC}^{T,V})^{\mathrm{cps}}\ (\mathsf{fun}\ k^{T^{\mathrm{cps}}\to V^{\mathrm{cps}}} \to t^{\mathrm{cps}})\ \overline{y}\ \overline{\beta}|\!)(\overline{\xi},\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}^{\mathrm{cps}}}\ \overline{y}^{\overline{U}^{\mathrm{cps}}}\ \overline{\beta}^{\Sigma} \mid t^{\mathrm{cps}}\ \overline{y}\ \overline{\beta}|\!)(\overline{\xi},\overline{u},\overline{b}) \\
= \ & (\!|\overline{x}^{\overline{X}} \mid t|\!)(\overline{\xi})(\overline{u},\overline{b}).
\end{aligned}$$

Par conséquent, $(\!|\overline{x} \mid \mathcal{CC}^{T,V}\ (\mathsf{fun}\ k^{T\to V} \to t)|\!) = (\!|\overline{x} \mid t|\!)$. □

Proposition 4.5. Pour tout type simple T, les éléments séquentiels de T^{cps} sont les mêmes que ceux de T.

Démonstration. Il suffit de montrer qu'il existe des termes simples i_T et j_T de types respectifs $T \to T^{\mathrm{cps}}$ et $T^{\mathrm{cps}} \to T$ tels que $(\!|i|\!)$ et $(\!|j|\!)$ soient l'identité sur $(\!|T|\!) = (\!|T^{\mathrm{cps}}|\!)$. On les construits par induction : si $T = \overline{U} \to \Delta_n$, on pose

— $i_T = \mathsf{fun}\ t^T\ \overline{u}^{\overline{U}^{\mathrm{cps}}}\ \overline{a}^{n\Sigma} \to \mathsf{match}^{n,\Sigma}\ \left(t\ \overline{(j_U\ u)}\right)\ \overline{a}$,

— $j_T = \mathsf{fun}\ t^{T^{\mathrm{cps}}}\ \overline{u}^{\overline{U}} \to \mathcal{CC}^{\Delta_n,\Sigma}\ \left(\mathsf{fun}\ k^{\Delta_n\to\Sigma} \to \mathsf{match}^{0,\Delta_n}\ \left(t\ \overline{(i_U\ u)}\ (k\partial_0^n)\ldots(k\partial_{n-1}^n)\right)\right)$.

□

4.3.1 Traduction dans les algèbres de Boole

On procède comme à la section précédente : tout d'abord, pour tout type simple T, on fixe un entier ν_T et une surjection σ_T de $\{0,1\}^{\nu_T}$ dans $(\!|T|\!)$ (ce que l'on peut faire puisque $(\!|T|\!)$ est fini), ainsi qu'un inverse à droite σ_T^* de σ_T. De plus, on impose que pour tout type T, $\nu_{T^{\mathrm{cps}}} = \nu_T$, $\sigma_{T^{\mathrm{cps}}} = \sigma_T$ et $\sigma^*_{T^{\mathrm{cps}}} = \sigma^*_T$.

Ensuite, pour toute fonction f de $(\!|T_1|\!) \times \ldots \times (\!|T_n|\!)$ dans $(\!|U|\!)$, on fixe une fonction $\widetilde{f} : \{0,1\}^{\nu_{T_1}} \to \ldots \to \{0,1\}^{\nu_{T_n}} \to \{0,1\}^{\nu_U}$ telle que pour tous $(\overline{x}_1,\ldots,\overline{x}_n) \in \{0,1\}^{\nu_{T_1}+\ldots+\nu_{T_n}}$, $\widetilde{f}(\overline{x}_1,\ldots,\overline{x}_n) = \sigma^*_U(f(\sigma_{T_1}(\overline{x}_1),\ldots,\sigma_{T_n}(\overline{x}_n)))$. Enfin, on fixe une liste de ν_U termes du langage des algèbres de Boole, que l'on notera également $\widetilde{f}(\overline{x}_1,\ldots,\overline{x}_n)$, dont l'interprétation dans l'algèbre de Boole $\{0,1\}$ est la fonction $\widetilde{f}$.

En particulier, pour tous types simples T et U, on a donc une liste de termes $\widetilde{\mathsf{app}}^{T,U}(\overline{f}^{\nu_{T\to U}}, \overline{x}^{\nu_T})$ telle que pour tous $\overline{f} \in \{0,1\}^{\nu_{T\to U}}$ et tous $\overline{x} \in \{0,1\}^{\nu_T}$, l'interprétation de la liste de termes $\widetilde{\mathsf{app}}^{T,U}(\overline{f},\overline{x})$ dans l'algèbre de Boole $\{0,1\}$ est égale à $\sigma^*_U(\sigma_{T\to U}(\overline{f})(\sigma_T(\overline{x})))$.

Pour tout entier naturel n, pour tout $k \in \sigma$, on note δ la fonction de $\{0,1\}^{\nu_\Sigma}$ dans $\{0,1\}$ qui à $\overline{x}$ associe 0 si $\sigma_\Sigma(\overline{x}) = 0$ et 1 sinon. Ensuite, on choisit un terme $\delta(\overline{x})$ du langage des algèbres de Boole dont l'interprétation dans $\{0,1\}$ est la fonction δ.

On commence par définir $[\![T]\!](\overline{x}^{\nu_T})$ quand T est CPS-traduit :

On note $[\![\Sigma]\!](\overline{x}^{\nu_\Sigma})$ la formule $\delta(\overline{x}^{\nu_\Sigma}) \neq 0$ (de sorte que $[\![\Sigma]\!](\sigma^*(\Omega)) \equiv \top$ et $[\![\Sigma]\!](\sigma^*(0)) \equiv \bot$).

Pour tous types simples CPS-traduits T et U, on note $[\![T \to U]\!]\left(\overline{f}^{\nu_{T\to U}}\right)$ la formule $\forall \overline{x}^{\nu_T}\ \left([\![T]\!](\overline{x}) \to [\![U]\!]\left(\widetilde{\mathsf{app}}(\overline{f},\overline{x})\right)\right)$.

Enfin, si T n'est pas CPS-traduit, on note $[\![T]\!](\overline{x}^{\nu_T})$ la formule $[\![T^{\mathrm{cps}}]\!](\overline{x}^{\nu_{T^{\mathrm{cps}}}})$ (ce qui a un sens car $\nu_{T^{\mathrm{cps}}} = \nu_T$, $\sigma_{T^{\mathrm{cps}}} = \sigma_T$ et $\sigma^*_{T^{\mathrm{cps}}} = \sigma^*_T$).

Ainsi, pour tout type T, $[\![T]\!](\overline{x}) \equiv [\![T^{\mathrm{cps}}]\!](\overline{x})$ (y compris si T est déjà CPS-traduit).

Avec ces définitions, on peut vérifier que l'on a bien :

— $[\![\Delta_n]\!](\sigma^*(\Vert\partial^n_k\Vert)) \equiv \top \to \ldots \to \top \to \bot \to \top \to \ldots \to \top \to \bot$ (avec n arguments numérotés $0,\ldots,n-1$, dont le numéro k est $\bot$ et les autres $\top$),

— $[\![T \to U]\!](\sigma^*(f)) \equiv \bigcap_{t\in\Vert T\Vert}([\![T]\!](\sigma^*(t)) \to [\![U]\!](\sigma^*(f(t))))$,

— $[\![T]\!](\sigma^*(t)) \leqq [\![T]\!](\sigma^*(u))$ si $t \sqsupseteq u$,

— $[\![T]\!]\left(\sigma^*\left(\Omega^T\right)\right) \equiv \top$.

4.3.2 Fonctions séquentielles

Proposition 4.6. Pour tout type simple T, pour tout terme simple t de type T et toute liste $x_1^{U_1},\ldots,x_n^{U_n}$ de variables distinctes contenant toutes les variables libres de t, la formule $\daleth 2 \models [\![U_1 \to \ldots \to U_n \to T]\!]\left(\sigma^*(\Vert\mathsf{fun}\ x_1^{U_1}\ \ldots\ x_n^{U_n} \to t\Vert)\right)$ est universellement réalisée.

Démonstration. On a $[\![{U_1}^{\mathrm{cps}} \to \ldots \to {U_n}^{\mathrm{cps}} \to T^{\mathrm{cps}}]\!]\left(\sigma^*(\Vert\mathsf{fun}\ x_1^{{U_1}^{\mathrm{cps}}}\ \ldots\ x_n^{{U_n}^{\mathrm{cps}}} \to t^{\mathrm{cps}}\Vert)\right) \equiv [\![U_1 \to \ldots \to U_n \to T]\!]\left(\sigma^*(\Vert\mathsf{fun}\ x_1^{U_1}\ \ldots\ x_n^{U_n} \to t\Vert)\right)$, et comme t^{cps} est CPS-traduit, on peut à peu de choses près réutiliser la preuve de la proposition 4.1 pour montrer que $[\![{U_1}^{\mathrm{cps}} \to \ldots \to {U_n}^{\mathrm{cps}} \to T^{\mathrm{cps}}]\!]\left(\sigma^*(\Vert\mathsf{fun}\ x_1^{{U_1}^{\mathrm{cps}}}\ \ldots\ x_n^{{U_n}^{\mathrm{cps}}} \to t^{\mathrm{cps}}\Vert)\right)$ est universellement réalisée. □

D'après le théorème 3.19, on a les corollaires suivants :

Corollaire. Pour tout type simple T, pour tout terme simple clos f de type T, la formule $[\![T]\!](\sigma^*(\Vert t\Vert))$ est vraie dans toute algèbre de Boole à au moins deux éléments.

Corollaire. Pour tous types simples $T_1,\ldots,T_n,U$, pour tous $a_1 \in \Vert T_1\Vert,\ldots,a_n \in \Vert T_n\Vert, b \in \Vert U\Vert$, si b est simulable par $a_1,\ldots,a_n$, alors la formule $[\![U]\!](\sigma^*(b))$ est conséquence de $\{\,[\![T_1]\!](\sigma^*(a_1)),\ldots,[\![T_n]\!](\sigma^*(a_n))\,\}$.

On va maintenant tâcher de donner une réciproque à ce résultat.

Proposition 4.7. Soient $T_1,\ldots,T_m,U$ des types simples, $\overline{x_1}^{\nu_{T_1}},\ldots,\overline{x_m}^{\nu_{T_m}}$ des variables du langage des algèbres de Boole deux à deux distinctes et f un élément de $\Vert T_1 \to \ldots \to T_m \to U\Vert$.

Si le séquent booléen $[\![T_1]\!](\overline{x_1}),\ldots,[\![T_m]\!](\overline{x_m}) \vdash [\![U]\!]\left(\widetilde{f}(\overline{x_1},\ldots,\overline{x_n})\right)$ est dérivable, alors f est séquentielle.

Démonstration. La proposition découle de la construction suivante :

Pour tous types simples CPS-traduits $T_1,\ldots,T_m$, toutes variables $\overline{x_1}^{\nu_{T_1}},\ldots,\overline{x_m}^{\nu_{T_m}}$ deux à deux distinctes, tous atomes $\alpha,\beta_1,\ldots,\beta_n$ et toute démonstration booléenne *sans coupure* S de conclusion $[\![T_1]\!]$

$(\overline{x_1}), \ldots, [\![T_{m^*}]\!](\overline{x_{m^*}}) \vdash \forall \overline{y}\ ([\![T_{m^*+1}]\!](\overline{x_{m^*+1}}) \to \ldots \to \forall \overline{x_m}\ ([\![T_m]\!](\overline{x_m}) \to \alpha)\ldots); \beta_1, \ldots, \beta_n$ avec $\overline{y}$ un suffixe (éventuellement vide) de $\overline{x_{m^*+1}}$, on va construire (par induction sur la hauteur de S) un terme simple clos CPS-traduit f_S de type $T_1 \to \ldots \to T_m \to \Sigma$ tel que pour toute liste $\overline{\xi^\mu}$ de variables distinctes contenant toutes les variables libres de $[\![T_1]\!](\overline{x_1}), \ldots, [\![T_m]\!](\overline{x_m}), \alpha, \beta_1, \ldots, \beta_n$ et tous $\overline{\zeta^\mu} \in \{0,1\}$, si $(\alpha \oplus \beta_1 \oplus \ldots \oplus \beta_n)[\overline{\xi} := \overline{\zeta}]$ est faux alors en notant pour tout $i \in \{1, \ldots, m\}$ $t_i = \sigma_{T_i}(\overline{x_i}[\overline{\xi} := \overline{\zeta}]) \in (\!|T_i|\!)$, on a $(\!|y_1, \ldots, y_m \mid f_S\ y_1 \ldots y_m|\!)(t_1, \ldots, t_m) = 0 \in \Sigma$.

Si la dernière règle de S est la règle $\to$*-intro*, S est de la forme :

$$\dfrac{\dfrac{S'}{[\![T_1]\!](\overline{x_1}), \ldots, [\![T_{m^*+1}]\!](\overline{x_{m^*+1}}) \vdash \forall \overline{x_{m^*+2}}\ ([\![T_{m^*+2}]\!](\overline{x_{m^*+2}}) \to \ldots \to \forall \overline{x_m}\ ([\![T_m]\!](\overline{x_m}) \to \alpha)\ldots); \beta_1, \ldots, \beta_n}}{[\![T_1]\!](\overline{x_1}), \ldots, [\![T_{m^*}]\!](\overline{x_{m^*}}) \vdash ([\![T_{m^*+1}]\!](\overline{x_{m^*+1}}) \to \ldots \to \forall \overline{x_m}\ ([\![T_m]\!](\overline{x_m}) \to \alpha)\ldots); \beta_1, \ldots, \beta_n}$$

et il n'y a qu'à poser $f_S = f_{S'}$.

Si la dernière règle de S est la règle $\forall$*-intro*, S est de la forme :

$$\dfrac{\dfrac{S'}{[\![T_1]\!](\overline{x_1}), \ldots, [\![T_{m^*}]\!](\overline{x_{m^*}}) \vdash \forall \overline{y'}\ ([\![T_{m^*+1}]\!](\overline{x_{m^*+1}}) \to \ldots \to \forall \overline{x_m}\ ([\![T_m]\!](\overline{x_m}) \to \alpha)\ldots); \beta_1, \ldots, \beta_n}}{[\![T_1]\!](\overline{x_1}), \ldots, [\![T_{m^*}]\!](\overline{x_{m^*}}) \vdash \forall \overline{y}\ ([\![T_{m^*+1}]\!](\overline{x_{m^*+1}}) \to \ldots \to \forall \overline{x_m}\ ([\![T_m]\!](\overline{x_m}) \to \alpha)\ldots); \beta_1, \ldots, \beta_n}$$

(où $\overline{y'}$ est la liste obtenue en enlevant le premier élément de $\overline{y}$) et il n'y a qu'à poser $f_S = f_{S'}$.

Si la dernière règle de S est une règle *Axiome*, alors la conclusion de S est $\overline{y}$ est la liste $\overline{x_{m^*+1}}$ complète (sauf si $m^* = m$) et $\forall \overline{x_{m^*+1}}\ ([\![T_{m^*+1}]\!](\overline{x_{m^*+1}}) \to \ldots \to \forall \overline{x_m}\ ([\![T_m]\!](\overline{x_m}) \to \alpha)\ldots)$ est la formule $[\![T_j]\!](\overline{x_j})$ pour un certain $j \leq m^*$. Dans ce cas, T_j est le type $T_{m^*+1} \to \ldots \to T_m \to \Sigma$ et il n'y a qu'à poser $f_S = \mathsf{fun}\ t_1^{T_1} \ldots t_{m^*}^{T_{m^*}} \to t_j$.

Les règles restantes ont pour conclusion un atome, par conséquent on peut désormais supposer $m^* = m$.

Si la dernière règle de S est la règle *Équation*, S est de la forme :

$$(\text{Équation})\ \dfrac{\dfrac{S'}{[\![T_1]\!](\overline{x_1}), \ldots, [\![T_m]\!](\overline{x_m}) \vdash \alpha'; \beta'_1, \ldots, \beta'_{n'}}}{[\![T_1]\!](\overline{x_1}), \ldots, [\![T_m]\!](\overline{x_m}) \vdash \alpha; \beta_1, \ldots, \beta_n}$$

et l'on a $\{\alpha' \oplus \beta'_1 \oplus \ldots \oplus \beta'_{n'}\} \Rightarrow \{\alpha \oplus \beta_1 \oplus \ldots \oplus \beta_n\}$, par conséquent il n'y a qu'à poser $f_S = f_{S'}$.

Si la dernière règle de S est la règle *Tautologie* alors $\emptyset \Rightarrow \{\alpha \oplus \beta_1 \oplus \ldots \oplus \beta_n\}$, donc n'importe quel t_S convient.

Supposons à partir de maintenant que la dernière règle de S est la règle *Élim*. On note $\Gamma = [\![T_1]\!](\overline{x_1}), \ldots, [\![T_m]\!](\overline{x_m})$ et $\mathcal{E} = \beta_1, \ldots, \beta_m$. La démonstration S est de la forme :

$$(\text{Élim})\ \dfrac{R}{\Gamma \vdash \forall \overline{z_1}\ (A_1 \to \ldots \to (\forall \overline{z_{p+1}}\ \gamma)\ldots); \mathcal{E}} \quad \dfrac{Q_1}{\Gamma \vdash A_1[\overline{z_1} := \overline{a_1}]; \mathcal{E}} \quad \ldots \quad \dfrac{Q_p}{\Gamma \vdash A_p[\overline{z_1} := \overline{a_1}, \ldots, \overline{z_p} := \overline{a_p}]; \mathcal{E}}$$
$$\Gamma \vdash \gamma[\overline{z_1} := \overline{a_1}, \ldots, \overline{z_{p+1}} := \overline{a_{p+1}}]; \mathcal{E}$$

pour $\overline{z_1}, \ldots, \overline{z_{p+1}}$ des variables deux à deux distinctes (où γ est tel que $\gamma[\overline{z_1} := \overline{a_1}, \ldots, \overline{z_{p+1}} := \overline{a_{p+1}}]$ est l'atome α).

Puisque S est sans coupure, la dernière (et unique) étape de R doit être une application de la règle axiome. Par conséquent, $\overline{z_1}\ (A_1 \to \ldots \to (\forall \overline{z_{p+1}}\ \gamma)\ldots)$ est la formule $[\![T_q]\!](\overline{x_q})$ pour un certain $q \in \{1, \ldots, m\}$.

Ainsi, le type simple (CPS-traduit) T_q est de la forme $U_1 \to \ldots \to U_p \to \Sigma$ et pour tout $j \in \{1, \ldots, p\}$, A_j est la formule $[\![U_i]\!](\overline{z_i})$.

Le reste de la preuve consiste à montrer que $f_{Q_1}, \ldots, f_{Q_p}$ sont bien définies (c'est-à-dire que les formules $A_1, \ldots, A_p$ respectent le bon modèle) et qu'il suffit de poser $f_S = \mathsf{fun}\ t_1^{T_1}\ \ldots\ t_m^{T_m} \to t_q\ (f_{Q_1}\ t_1 \ldots t_m)\ \ldots\ (f_{Q_p}\ t_1 \ldots t_m)$.

Pour tout $j \in \{1, \ldots, p\}$, U_j est de la forme $V_{j,1} \to \ldots \to V_{j,s_j} \to \Sigma$ et donc $A_j(\overline{z_j})$ est la formule $\forall \overline{w_{j,1}}\ (\llbracket V_{j,1} \rrbracket\ (\overline{w_{j,1}}) \to \ldots \forall \overline{w_{j,s_j}} (\llbracket V_{j,s_j} \rrbracket\ (\overline{w_{j,s_j}}) \to \llbracket \Sigma \rrbracket\ (\overline{\eta_j}^{\nu_\Sigma})) \ldots)$, où les $\overline{\eta_j}^{\nu_\Sigma}$ sont tels que si l'on note $\overline{\xi}$ la liste $\overline{w_{j,1}}, \ldots, \overline{w_{j,s_j}}, \overline{z_j}$, pour tous $\overline{\zeta} \in \{0,1\}$, on a

$$\sigma_\Sigma(\overline{\eta_j}^{\nu_\Sigma}[\overline{\xi} := \overline{\zeta}]) = \sigma_{U_j}(\overline{z_j}[\overline{\xi} := \overline{\zeta}])(\sigma_{V_{j,1}}(\overline{w_{j,1}}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{V_{j,s_j}}(\overline{w_{j,s_j}}[\overline{\xi} := \overline{\zeta}])).$$

Par conséquent, par hypothèse d'induction, pour toute liste $\overline{\xi}$ de variables distinctes contenant toutes les variables libres de la conclusion de Q_j plus les variables $\overline{w_{j,1}}, \ldots, \overline{w_{j,s_j}}$, pour tous $\overline{\zeta} \in \{0,1\}$, si $(\beta_1 \oplus \ldots \oplus \beta_n)[\overline{\xi} := \overline{\zeta}]$ est faux, alors

$$\begin{array}{rl} & (\!|t_1\ \ldots\ t_m\ v_{j,1}\ \ldots\ v_{j,s_j} \mid f_{Q_j}\ t_1\ \ldots\ t_m\ v_{j,1}\ \ldots\ v_{j,s_j}|\!)(\ \sigma_{T_1}(\overline{x_1}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{T_m}(\overline{x_m}[\overline{\xi} := \overline{\zeta}]), \\ & \qquad\qquad \sigma_{V_{j,1}}(\overline{w_{j,1}}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{V_{j,s_j}}(\overline{w_{j,s_j}}[\overline{\xi} := \overline{\zeta}])\ ) \\ \sqsupseteq & \sigma_{U_j}(\overline{a_j}[\overline{\xi} := \overline{\zeta}])(\sigma_{V_{j,1}}(\overline{w_{j,1}}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{V_{j,s_j}}(\overline{w_{j,s_j}}[\overline{\xi} := \overline{\zeta}])). \end{array}$$

En résumé, pour tout $j \in \{1, \ldots, p\}$, pour toute liste $\overline{\xi}$ de variables distinctes contenant toutes les variables libres de la conclusion de Q_j, si $(\beta_1 \oplus \ldots \oplus \beta_n)[\overline{\xi} := \overline{\zeta}]$ est faux, alors

$$(\!|t_1\ \ldots\ t_m \mid f_{Q_j}\ t_1\ \ldots\ t_m|\!)(\sigma_{T_1}(\overline{x_1}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{T_m}(\overline{x_m}[\overline{\xi} := \overline{\zeta}])) \sqsupseteq \sigma_{U_j}(\overline{a_j}[\overline{\xi} := \overline{\zeta}]).$$

Par ailleurs, γ est de la forme $\llbracket \Sigma \rrbracket\ (\overline{\theta})$, où $\overline{\theta}$ est tel que si l'on note $\overline{\xi}$ la liste $\overline{x_1}, \ldots, \overline{x_m}, \overline{z_1}, \ldots, \overline{z_{p+1}}$, pour tous $\overline{\zeta} \in \{0,1\}$, on a

$$\sigma_\Sigma(\overline{\theta}[\overline{\xi} := \overline{\zeta}]) = \sigma_{T_q}(\overline{x_q}[\overline{\xi} := \overline{\zeta}])(\sigma_{U_1}(\overline{z_1}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{U_p}(\overline{z_p}[\overline{\xi} := \overline{\zeta}])).$$

Ainsi, α est la formule $\llbracket \Sigma \rrbracket\ (\overline{\theta}[\overline{z_1} := \overline{a_1}, \ldots, \overline{z_{p+1}} := \overline{a_{p+1}}])$, et pour toute liste $\overline{\xi}$ de variables distinctes contenant toutes les variables libres de $\llbracket T_1 \rrbracket\ (\overline{x_1}), \ldots, \llbracket T_m \rrbracket\ (\overline{x_m}), \alpha, \beta_1, \ldots, \beta_n$ et tous $\overline{\zeta} \in \{0,1\}$, si $(\beta_1 \oplus \ldots \oplus \beta_n)[\overline{\xi} := \overline{\zeta}]$ est faux alors

$$\begin{array}{rl} & (\!|t_1 \ldots t_m \mid t_q\ (f_{Q_1}\ t_1 \ldots t_m)\ \ldots\ (f_{Q_p}\ t_1 \ldots t_m)|\!)(\sigma_{T_1}(\overline{x_1}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{T_m}(\overline{x_m}[\overline{\xi} := \overline{\zeta}])) \\ \sqsupseteq & \sigma_\Sigma(\overline{\theta}[\overline{z_1} := \overline{a_1}, \ldots, \overline{z_{p+1}} := \overline{a_{p+1}}][\overline{\xi} := \overline{\zeta}]). \end{array}$$

Autrement-dit, si $(\alpha \oplus \beta_1 \oplus \ldots \oplus \beta_n)[\overline{\xi} := \overline{\zeta}]$ est faux alors

$$(\!|t_1 \ldots t_m \mid t_q\ (f_{Q_1}\ t_1 \ldots t_m)\ \ldots\ (f_{Q_p}\ t_1 \ldots t_m)|\!)(\sigma_{T_1}(\overline{x_1}[\overline{\xi} := \overline{\zeta}]), \ldots, \sigma_{T_m}(\overline{x_m}[\overline{\xi} := \overline{\zeta}])) = 0,$$

il suffit donc bien de poser $f_S = \mathsf{fun}\ t_1^{T_1}\ \ldots\ t_m^{T_m} \to t_q\ (f_{Q_1}\ t_1 \ldots t_m)\ \ldots\ (f_{Q_p}\ t_1 \ldots t_m)$. □

Corollaire. Pour tous types simples $T_1, \ldots, T_n, U$, pour tous $a_1 \in (\!|T_1|\!), \ldots, a_n \in (\!|T_n|\!), b \in (\!|U|\!)$, b est simulable par $a_1, \ldots, a_n$ si et seulement si la formule $\llbracket U \rrbracket\ (\sigma^*(b))$ est conséquence de $\{\ \llbracket T_1 \rrbracket\ (\sigma^*(a_1)), \ldots, \llbracket T_n \rrbracket\ (\sigma^*(a_n))\ \}$.

4.3.3 Classification des degrés de parallélisme de $\mathbb{C}_{\mathsf{Sierp}}$

Lemme 4.8. Pour toute formule $A(\overline{x})$ du langage des algèbres de Boole, il existe un type simple T et une liste $\overline{a}^{\nu_T}(\overline{x})$ de termes du langage des algèbres de Boole tels que $A(\overline{x}) \equiv \llbracket T \rrbracket\ (\overline{a}^{\nu_T}(\overline{x}))$

Démonstration. On procède par induction sur A.

Si A est un atome, on prend $T = \Sigma = \Delta_0$ et l'on choisit $\overline{a}^{\nu_T}(\overline{x})$ tels que pour tous $\overline{x} \in \{0,1\}$, $\overline{a}(\overline{x})$ soit égal à $\sigma^*(\Omega)$ si $A(\overline{x})$ est vraie et à $\sigma^*(0)$ sinon.

Si $A(\overline{x})$ est la formule $B(\overline{x}) \to C(\overline{x})$ et que l'on a U, V, $\overline{b}^{\nu_U}(\overline{x})$ et $\overline{c}^{\nu_V}(\overline{x})$ tels que $B(\overline{x}) \equiv [\![U]\!]\left(\overline{b}(\overline{x})\right)$ et $C(\overline{x}) \equiv [\![V]\!]\left(\overline{C}(\overline{x})\right)$, on prend $T = U \to V$ et l'on choisit $\overline{a}^{\nu_T}(\overline{x})$ de telle sorte que pour tous $\overline{x} \in \{0,1\}$, $\overline{a}(\overline{x})$ soit l'image par σ^* du plus petit $f \in (\!|T|\!)$ tel que $f(\sigma(b(\overline{x}))) \sqsupseteq \sigma(c(\overline{x}))$.

Si $A(\overline{x})$ est la formule $\forall y\ B(\overline{x}, y)$ et que l'on a U et $\overline{b}^{\nu_U}(\overline{x}, y)$ tels que $B(\overline{x}) \equiv [\![U]\!]\left(\overline{b}(\overline{x}, y)\right)$, alors on prend $T = U$ et l'on choisit $\overline{a}^{\nu_T}(\overline{x})$ de telle sorte que pour tous $\overline{x} \in \{0,1\}$, $\overline{a}(\overline{x})$ soit l'image par σ^* de la borne supérieure de $\sigma(\overline{b}(\overline{x}, 0))$ et $\sigma(\overline{b}(\overline{x}, 1))$. □

Proposition 4.9. Pour toute formule close A, il existe un type simple T et un élément t de $(\!|T|\!)$ tels que $[\![T]\!]\left(\sigma_T^*(t)\right) =\!|\!\models A$.

Démonstration. D'après le lemme précédent, il existe un type simple T et un élément t de $(\!|T|\!)$ tels que $[\![T]\!]\left(\sigma_T^*(t)\right) \equiv A$. En particulier, ces deux formules sont universellement équivalentes, et donc d'après le corollaire du théorème 3.19, on a $[\![T]\!]\left(\sigma_T^*(t)\right) =\!|\!\models A$. □

La proposition ci-dessus et le corollaire de la proposition 4.7 entraînent le résultat suivant :

Théorème 4.10. Le $\mathcal{M}$-ensemble des degrés de parallélisme de $\mathbb{C}_{\mathsf{Sierp}}$ ordonné par l'inclusion est $\mathcal{M}$-isomorphe au $\mathcal{M}$-ensemble des extensions de la théorie des algèbres de Boole à au moins deux éléments ordonné par l'inclusion.

4.4 L'espace des votes

À l'aide d'une traduction CPS similaire à celle utilisée pour $\mathbb{C}_{\mathsf{Sierp}}$, on va construire un troisième modèle de calcul fini $\mathbb{C}_{\mathsf{Vote}}$.

Dans ce modèle, un programme « évalué jusqu'au bout » (c'est-à-dire placé dans un contexte dont le type de retour est le type de réponses de la traduction CPS) peut soit répondre 0, soit répondre 1, soit ne pas répondre. Par comparaison, dans $\mathbb{C}_{\mathsf{Sierp}}$, un programme évalué jusqu'au bout peut soit répondre 0, soit ne pas répondre.

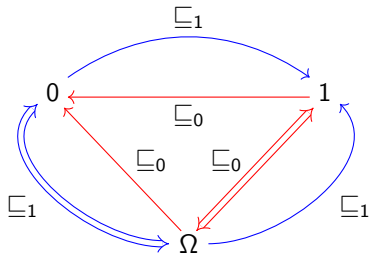
Avoir deux réponses possibles permet dans certains cas de « tester » l'égalité entre deux programmes en les évaluant. Par exemple, il existe un contexte dans lequel ∂_0^2 répond 0 et ∂_1^2 répond 1.

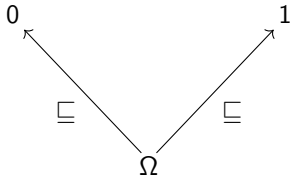
Dans $\mathbb{C}_{\mathsf{Vote}}$, les programmes doivent faire des choix, puisqu'ils ne peuvent pas répondre à la fois 0 et 1. En particulier, contrairement à $\mathbb{C}_{\mathsf{Sierp}}$, $\mathbb{C}_{\mathsf{Vote}}$ ne contient pas d'instruction *fork* (car *fork* appliqué à 0 et à 1 répondrait à la fois 0 et 1).

4.4.1 Définition de $\mathbb{C}_{\mathsf{Vote}}$

Interprétation des types. À chaque type simple T, on va associer non seulement un inf-semi-treillis fini $((\!|T|\!), \sqsubseteq^T)$, mais également deux préordres $\sqsubseteq_0^T$ et $\sqsubseteq_1^T$ (qui interviendront dans la définition de $(\!|T \to U|\!)$) :

— $((\!|\Delta_0|\!), \sqsubseteq^{\Delta_0}, \sqsubseteq_0^{\Delta_0}, \sqsubseteq_1^{\Delta_0}) = (\Sigma_2, \sqsubseteq^{\Sigma_2}, \sqsubseteq_0^{\Sigma_2}, \sqsubseteq_1^{\Sigma_2})$, où Σ_2 est l'ensemble $\{\Omega, 0, 1\}$, $a \sqsubseteq_i^{\Sigma_2} b$ si et seulement si $a \neq i$ ou $b = i$, et $\sqsubseteq^{\Sigma_2} = \sqsubseteq_0^{\Sigma_2} \cap \sqsubseteq_1^{\Sigma_2}$. Graphiquement :



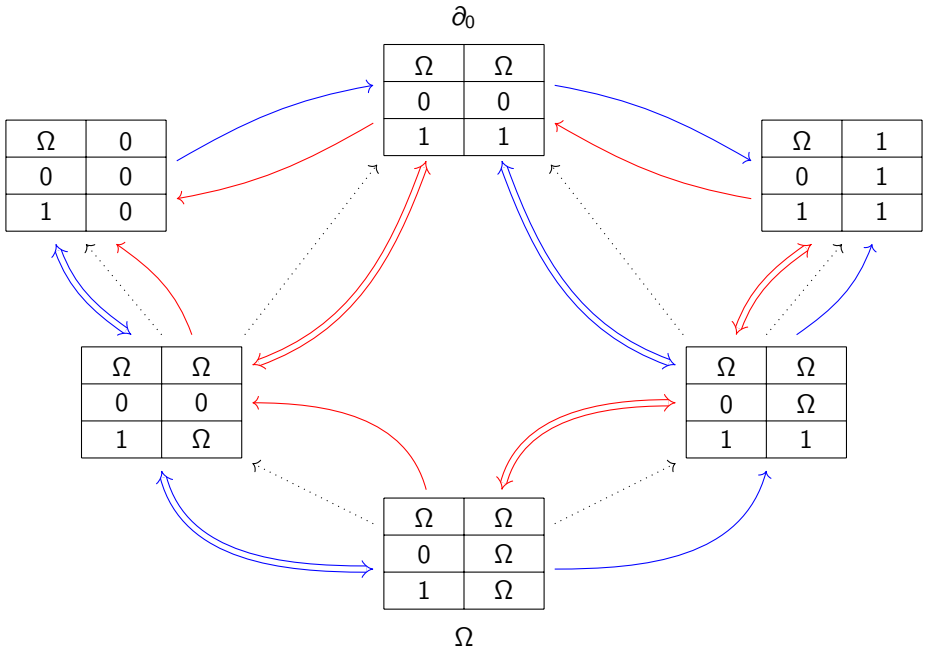


Comme pour $\mathbb{C}_{\text{Sierp}}$, Δ_0 jouera à la fois le rôle du type sans constructeur et du type des réponses : pour la première utilisation, on continuera de le noter Δ_0 et pour la seconde, on le notera plutôt Σ_2, de sorte que $(\!|\Sigma_2|\!) = \Sigma_2$.

— $(\!|T \to U|\!)$ est l'ensemble des fonctions de $(\!|T|\!)$ dans $(\!|U|\!)$ croissantes à la fois pour $\sqsubseteq_0$ et pour $\sqsubseteq_1$. On pose $f \sqsubseteq_i^{T\to U} g$ si et seulement si $f(a) \sqsubseteq_i g(a)$ pour tout $a \in (\!|T|\!)$. Enfin, on pose $\sqsubseteq^{\Sigma_2} = \sqsubseteq_0^{T\to U} \cap \sqsubseteq_1^{T\to U}$.

— $(\!|\Delta_n|\!) = (\!|{\Sigma_2}^n \to \Sigma_2|\!)$ (avec la même structure).

Par exemple, $(\!|\Delta_1|\!)$ peut se représenter ainsi :



Où $f \in (\!|\Delta_1|\!) = (\!|\Sigma_2 \to \Sigma_2|\!)$ est représentée par le tableau :

Ω	$f(\Omega)$
0	$f(0)$
1	$f(1)$

On vérifie par induction que pour tout type T :

— $(\!|T|\!)$ muni de $\sqsubseteq^T$ est un inf-semi-treillis fini dont le plus petit élément est la fonction constante égale à Ω,

— $(\!|T|\!)$ muni de $\sqsubseteq_i^T$ (pour $i = 0$ ou $i = 1$) est un préordre fini où toute paire d'éléments a une borne supérieure et une borne inférieure (non nécessairement uniques).

Pour simplifier, si $f \in (\!|T_1 \to \ldots \to T_n \to U|\!)$ et $t_1 \in (\!|T_1|\!), \ldots, t_n \in (\!|T_n|\!)$, on notera $f(t_1, \ldots, t_n)$ pour $f(t_1)\ldots(t_n)$.

Interprétation des termes. On définit $(\!|x_1^{U_1}, \ldots, x_m^{U_m} \mid t|\!)$ quand t et $U_1, \ldots, U_m$ sont CPS-traduits en posant :

— $(\!|\overline{x} \mid \Omega^T|\!)(\overline{a}) = \Omega^T$,

— $(\!|\overline{x} \mid x_i|\!)(\overline{a}) = a_i$,

— $(\!|\overline{x} \mid t\,u|\!)(\overline{a}) = (\!|\overline{x} \mid t|\!)(\overline{a})((\!|\overline{x} \mid u|\!)(\overline{a}))$,

— $(\!|\overline{x} \mid \text{fun } y^V \to t|\!)(\overline{a})$ est la fonction qui à b associe $(\!|\overline{x}, y \mid t|\!)(\overline{a}, b)$ (comme les termes simples sont définis à α-équivalence près, on peut supposer que y n'est pas dans la liste $\overline{x}$),

Enfin, si t ou l'un des U_j n'est pas CPS-traduit, on pose $(\!|x_1^{U_m}, \ldots, x_m^{U_m} \mid t|\!) = (\!|x_1^{U_1{}^{\text{cps}}}, \ldots, x_m^{U_m{}^{\text{cps}}} \mid t^{\text{cps}}|\!)$.

On peut vérifier qu'avec cette définition, on a toujours $(\!|x_1^{U_m}, \ldots, x_m^{U_m} \mid t|\!) = (\!|x_1^{U_1{}^{\text{cps}}}, \ldots, x_m^{U_m{}^{\text{cps}}} \mid t^{\text{cps}}|\!)$, y compris quand t et $U_1, \ldots, U_m$ sont CPS-traduits.

Comme pour $\mathbb{C}_{\text{Sierp}}$, on peut vérifier que ceci définit bien un modèle de calcul fini.

4.4.2 Traduction dans les algèbres de Boole

On procède comme à la section précédente : tout d'abord, pour tout type simple T, on fixe un entier ν_T et une surjection σ_T de $\{0,1\}^{\nu_T}$ dans $(\!|T|\!)$ (ce que l'on peut faire puisque $(\!|T|\!)$ est fini), ainsi qu'un inverse à droite σ_T^* de σ_T. De plus, on impose que pour tout type T, $\nu_{T^{\text{cps}}} = \nu_T$, $\sigma_{T^{\text{cps}}} = \sigma_T$ et $\sigma^*_{T^{\text{cps}}} = \sigma^*_T$.

Cependant, cette fois-ci, chaque type T sera associé à une formule $[\![T]\!](\tau, \overline{x}^{\nu_T})$ (au lieu de $[\![T]\!](\overline{x}^{\nu_T})$ comme dans les cas précédents).

Pour toute fonction f de $(\!|T_1|\!) \times \ldots \times (\!|T_n|\!)$ dans $(\!|U|\!)$, on fixe une fonction $\widetilde{f} : \{0,1\}^{\nu_{T_1}} \to \ldots \to \{0,1\}^{\nu_{T_n}} \to \{0,1\}^{\nu_U}$ telle que pour tous $(\overline{x}_1, \ldots, \overline{x}_n) \in \{0,1\}^{\nu_{T_1}+\ldots+\nu_{T_n}}$, $\widetilde{f}(\overline{x}_1, \ldots, \overline{x}_n) = \sigma^*_U(f(\sigma_{T_1}(\overline{x}_1), \ldots, \sigma_{T_n}(\overline{x}_n)))$. Ensuite, on fixe une liste de ν_U termes du langage des algèbres de Boole, que l'on notera également $\widetilde{f}(\overline{x}_1, \ldots, \overline{x}_n)$, dont l'interprétation dans l'algèbre de Boole $\{0,1\}$ est la fonction $\widetilde{f}$.

En particulier, pour tous types simples T et U, on a donc une liste de termes $\widetilde{\text{app}}^{T,U}(\overline{f}^{\nu_{T\to U}}, \overline{x}^{\nu_T})$ telle que pour tous $\overline{f} \in \{0,1\}^{\nu_{T\to U}}$ et tous $\overline{x} \in \{0,1\}^{\nu_T}$, l'interprétation de la liste de termes $\widetilde{\text{app}}^{T,U}(\overline{f}, \overline{x})$ dans l'algèbre de Boole $\{0,1\}$ est égale à $\sigma^*_U(\sigma_{T\to U}(\overline{f})(\sigma_T(\overline{x})))$.

Pour tout entier naturel n, pour tout $k \in \sigma$, on note δ la fonction de $\{0,1\} \times \{0,1\}^{\nu_{\Sigma_2}}$ dans $\{0,1\}$ qui à $(\tau, \overline{x})$ associe 0 si $\sigma_{\Sigma_2}(\overline{x}) = \tau$ et 1 sinon. Ensuite, on choisit un terme $\delta(\tau, \overline{x})$ du langage des algèbres de Boole dont l'interprétation dans $\{0,1\}$ est la fonction δ.

On commence par définir $[\![T]\!](\tau, \overline{x}^{\nu_T})$ quand T est CPS-traduit :

— On note $[\![\Sigma_2]\!](\tau, \overline{x}^{\nu_{\Sigma_2}})$ la formule $\delta(\tau, \overline{x}^{\nu_{\Sigma_2}}) \neq 0$, de sorte que pour tout $\tau \in \{0,1\}$ et tout $a \in \Sigma_2$, $[\![\Sigma_2]\!](\tau, \sigma^*(a)) \equiv \bot$ si $a = \tau$ (c'est-à-dire si a est le plus grand élément pour $\sqsubseteq_\tau$) et $[\![\Sigma_2]\!](\tau, \sigma^*(a)) \equiv \top$ sinon,

— Pour tous types simples CPS-traduits T et U, on note $[\![T \to U]\!]\left(\tau, \overline{f}^{\nu_{T\to U}}\right)$ la formule

$$\forall \overline{x}^{\nu_T} \ \left([\![T]\!](\tau, \overline{x}) \to [\![U]\!]\left(\tau, \widetilde{\text{app}}(\overline{f}, \overline{x})\right)\right).$$

Enfin, si T n'est pas CPS-traduit, on note $[\![T]\!](\tau, \overline{x}^{\nu_T})$ la formule $[\![T^{\text{cps}}]\!](\tau, \overline{x}^{\nu_{T^{\text{cps}}}})$ (ce qui a un sens car $\nu_{T^{\text{cps}}} = \nu_T$, $\sigma_{T^{\text{cps}}} = \sigma_T$ et $\sigma^*_{T^{\text{cps}}} = \sigma^*_T$).

Ainsi, pour tout type T, $[\![T]\!](\tau, \overline{x}) \equiv [\![T^{\text{cps}}]\!](\tau, \overline{x})$ (y compris si T est déjà CPS-traduit).

Avec ces définitions, on peut vérifier que l'on a bien :

— $[\![\Delta_n]\!](\tau, \sigma^*((\!|\partial^n_k|\!))) \equiv \top \to \ldots \to \top \to \bot \to \top \to \ldots \to \top \to \bot$ (avec n arguments numérotés $0, \ldots, n-1$, dont le numéro k est $\bot$ et les autres $\top$),

— $[\![T \to U]\!](\tau, \sigma^*(f)) \equiv \bigwedge_{t \in (\!|T|\!)}([\![T]\!](\tau, \sigma^*(t)) \to [\![U]\!](\tau, \sigma^*(f(t))))$,

— $[\![T]\!](\tau, \sigma^*(t)) \leqq [\![T]\!](\tau, \sigma^*(u))$ si $t \sqsupseteq_\tau u$ (pour $\tau \in \{0,1\}$),

— $[\![T]\!]\left(\tau, \sigma^*\left(\Omega^T\right)\right) \equiv \top$.

4.4.3 Fonctions séquentielles

À l'aide une construction analogue à celle utilisée pour démontrer la proposition 4.7, on peut montrer le lemme suivant :

Lemme 4.11. Pour tous types simples $T_1, \ldots, T_m$, toutes variables $\tau, \overline{x_1}^{\nu_{T_1}}, \ldots, \overline{x_m}^{\nu_{T_m}}$ deux à deux distinctes, tous atomes $\alpha, \beta_1, \ldots, \beta_n$, si le séquent $[\![T_1]\!](\tau, \overline{x_1}), \ldots, [\![T_m]\!](\tau, \overline{x_m}) \vdash \alpha; \beta_1, \ldots, \beta_n$, alors il existe un terme clos un terme simple clos f de type $T_1 \to \ldots \to T_m \to \Sigma_2$ tel que pour toute liste $\overline{\xi}^{\mu}$ de variables distinctes contenant toutes les variables libres de $[\![T_1]\!](\tau, \overline{x_1}), \ldots, [\![T_m]\!](\tau, \overline{x_m}), \tau, \alpha, \beta_1, \ldots, \beta_n$ et tous $\overline{\zeta}^{\mu} \in \{0,1\}$, si $(\alpha \oplus \beta_1 \oplus \ldots \oplus \beta_n)[\overline{\xi} := \overline{\zeta}]$ est faux alors en notant pour tout $i \in \{1, \ldots, m\}$ $t_i = \sigma_{T_i}(\overline{x_i}[\overline{\xi} := \overline{\zeta}]) \in (\!|T_i|\!)$, on a $(\!|y_1, \ldots, y_m \mid f_S\ y_1 \ldots y_m|\!)(t_1, \ldots, t_m) = \tau[\overline{\xi} := \overline{\zeta}] \in \Sigma_2$.

On en déduit alors un résultat analogue au corollaire de la proposition 4.7 :

Proposition 4.12. Pour tous types simples $T_1, \ldots, T_n, U$, pour tous $a_1 \in (\!|T_1|\!), \ldots, a_n \in (\!|T_n|\!)$, $b \in (\!|U|\!)$, b est simulable par $a_1, \ldots, a_n$ si et seulement si la formule $\forall \tau\ ([\![T_1]\!](\tau, \sigma^*(a_1)) \to \ldots \to [\![T_n]\!](\tau, \sigma^*(a_n)) \to [\![U]\!](\tau, \sigma^*(b)))$ est vraie dans toute algèbre de Boole à au moins deux éléments.

4.4.4 Classification des degrés de parallélisme de $\mathbb{C}_{\text{Vote}}$

Pour terminer la classification des degrés de parallélisme de $\mathbb{C}_{\text{Vote}}$, il reste à déterminer quelles sont les formules du langage des algèbres de Boole qui sont équivalentes à $[\![T]\!](\tau, \sigma^*(\overline{x}))$ pour un certain T et un certain $t \in (\!|T|\!)$.

Lemme 4.13. Soient $T_1, \ldots, T_n$ des domaines finis et $t_1 \in (\!|T_1|\!), \ldots, t_n \in (\!|T_n|\!)$. Le séquent $[\![T_1]\!](\tau, \sigma^*(t_1)), \ldots, [\![T_n]\!](\tau, \sigma^*(t_n)), \tau \neq 0, \tau \neq 1 \vdash \bot; \emptyset$ n'est pas dérivable.

Démonstration. Par l'absurde, supposons le contraire. Alors, le séquent $[\![T_1]\!](\tau, \overline{y_1}), \ldots, [\![T_n]\!](\tau, \overline{y_n}), [\![\Sigma_2]\!](\tau, \overline{z_0}), [\![\Sigma_2]\!](\tau, \overline{z_1}) \vdash \bot; (\overline{y_1} \neq \sigma^*(t_1)), \ldots, (\overline{y_n} \neq \sigma^*(t_n)), (\overline{z_0} \neq \sigma^*(0)), (\overline{z_1} \neq \sigma^*(1))$ est également dérivable. Par le lemme 4.11, il existe donc une fonction séquentielle $f \in \text{Seq}^{\overline{T} \to \Sigma_2 \to \Sigma_2 \to \Sigma_2}$ telle que pour tout $\tau \in \{0,1\}$, $f(\overline{t}^n, 0, 1) = (\!|\overline{u}^n\ v_0\ v_1 \mid f\ \overline{u}^n\ v_0\ v_1|\!)(\overline{t}^n, 0, 1) = \tau$. Autrement-dit, $f(\overline{t}^n, 0, 1) = 0$ et $f(\overline{t}^n, 0, 1) = 1$: contradiction. □

Lemme 4.14. Il existe $k \in (\!|\Delta_4|\!)$ tel que $[\![\Delta_4]\!](\tau, \sigma^*(k)) \leqq \forall x\ (x \neq 0 \to x \neq 1 \to x \neq \tau \to x \neq \neg\tau \to \bot)$.

Démonstration. Il suffit de poser $k(0, x, 0, y) = k(x, 0, y, 0) = 0$ et $k(1, x, y, 1) = k(x, 1, 1, y) = 1$ pour tous $x, y \in \Sigma_2$ et $k(w, x, y, z) = \Omega$ dans tous les autres cas. □

Proposition 4.15. Soient T un type simple et $t \in (\!|T|\!)$. Soient $\mathbb{B}$ une algèbre de Boole à 4 éléments et soit $\rho \in \mathbb{B} \setminus \{0,1\}$. On a $\mathbb{B} \models [\![T]\!](\rho, \sigma^*(t))$.

Démonstration. Par l'absurde, supposons le contraire. Comme l'opération de $\mathbb{B}$ dans $\mathbb{B}$ qui échange ρ et $\neg\rho$ et laisse fixe 0 et 1 est un automorphisme de $\mathbb{B}$, on a $\mathbb{B} \models \forall \tau\ ([\![T]\!](\tau, \sigma^*(t)) \to (\tau = 0 \vee \tau = 1))$. Comme il existe une seule algèbre de Boole à 4 éléments à isomorphisme près et que toute algèbre de Boole à deux éléments vérifie également $\forall \tau\ ([\![T]\!](\tau, \sigma^*(t)) \to (\tau = 0 \vee \tau = 1))$, toute algèbre de Boole à au moins deux éléments vérifie

$$\forall \tau\ (\forall x\ ((x = 0) \vee (x = 1) \vee (x = \tau) \vee (x = \neg\tau)) \to [\![T]\!](\tau, \sigma^*(t)) \to (\tau = 0 \vee \tau = 1)),$$

par conséquent, en prenant le $k \in (\!|\Delta_4|\!)$ du lemme précédent, le séquent booléen

$$[\![\Delta_4]\!](\tau, \sigma^*(k)), [\![T]\!](\tau, \sigma^*(t)), \tau \neq 0, \tau \neq 1 \vdash \bot; \emptyset$$

est dérivable, ce qui contredit le lemme 4.13. □

Lemme 4.16. Pour toute formule $A(\overline{x})$ du langage des algèbres de Boole, il existe un type simple CPS-traduit T tel que pour tout $\rho \in \{0,1\}$, il existe une liste de termes du langage des algèbres de Boole $\overline{t}^{\nu_T}(\overline{x})$ tels que $A(\overline{x}) \equiv [\![T]\!](\rho, \overline{t}(\overline{x}))$.

Démonstration. Procédons par induction sur $A(\overline{x})$.

Si $A(\overline{x})$ est un atome, il suffit de prendre $T = \Sigma_2 = \Delta_0$ et de choisir $\overline{t}(\overline{x})$ tels que pour tous $\overline{x} \in \{0,1\}$, $\overline{t}(\overline{x})$ soit égal à $\sigma^*(\Omega)$ si $A(\overline{x})$ est vraie et à $\sigma^*(\rho)$ sinon.

Si $A(\overline{x})$ est la formule $B(\overline{x}) \to C(\overline{x})$ et que l'on a U et V des types simples et $\overline{u}(\overline{x})$ et $\overline{v}(\overline{x})$ des termes du langage des algèbres de Boole tels que $B(\overline{x}) \equiv [\![U]\!](\rho, \overline{u}(\overline{x}))$ et $C(\overline{x}) \equiv [\![V]\!](\rho, \overline{v}(\overline{x}))$, il suffit de poser $T = U \to V$ et de choisir $\overline{t}(\overline{x})$ tels que pour tous $\overline{x} \in \{0,1\}$, $f = \sigma(\overline{t}(\overline{x}))$ soit un $\sqsubseteq_\rho$-plus petit élément de $(\!|T|\!)$ tel que $f(\sigma(\overline{u}(\overline{x}))) \sqsupseteq_\rho \sigma(\overline{v}(\overline{x}))$.

Si $A(\overline{x})$ est la formule $\forall y\ B(\overline{x}, y)$ et que l'on a U un type simple et $\overline{u}(\overline{x}, y)$ des termes du langage des algèbres de Boole tels que $B(\overline{x}) \equiv [\![U]\!](\rho, \overline{u}(\overline{x}, y))$, il suffit de poser $T = U$ et de prendre $\overline{t}(\overline{x})$ tels que pour tous $\overline{x} \in \{0,1\}$, $\sigma(\overline{t}(\overline{x}))$ soit une $\sqsubseteq_\rho$-borne supérieure de $\sigma(\overline{u}(\overline{x}, 0))$ et $\sigma(\overline{u}(\overline{x}, 1))$. □

Corollaire. Pour toute formule $A(\tau, \overline{x})$, il existe un type simple CPS-traduit T et une liste de termes du langage des algèbres de Boole $\overline{t}^{\nu_T}(\tau, \overline{x})$ tels que $A(\tau, \overline{x}) \equiv [\![T]\!](\tau, \overline{t}(\tau, \overline{x}))$.

Démonstration. D'après le lemme précédent, il existe un domaine fini T et des listes $\overline{t}_0(\tau, \overline{x})$ et $\overline{t}_1(\tau, \overline{x})$ telles que $A(\tau, \overline{x}) \equiv [\![T]\!](0, \overline{t}_0(\tau, \overline{x})) \equiv [\![D]\!](1, \overline{t}_1(\tau, \overline{x}))$. Par conséquent, il suffit de choisir $\overline{t}(\tau, \overline{x})$ telle que pour tous $\overline{x}, \rho \in \{0,1\}$, $\overline{t}(\rho, \overline{x}) = \overline{t}_\rho(\rho, \overline{x})$. □

Proposition 4.17. Soient $A(\tau)$ une formule du langage des algèbres de Boole telle que pour toute algèbre de Boole $\mathbb{B}$ à 4 éléments, pour tout $\rho \in \mathbb{B} \setminus \{0,1\}$, $\mathbb{B} \models A(\rho)$. Alors il existe un type simple T et $t \in (\!|T|\!)$ tels que $A(\tau) \equiv [\![T]\!](\tau, \sigma^*(t))$.

Démonstration. D'après le lemme précédent, on peut trouver T type simple CPS-traduit et $\overline{v}^{\nu_T}(\tau)$ des termes du langage des algèbres de Boole tels que $A(\tau) \equiv [\![T]\!](\tau, \overline{v}(\tau))$. On pose $t_0 = \sigma(\overline{v}(0)) \in (\!|T|\!)$ et $t_1 = \sigma(\overline{v}(1)) \in (\!|T|\!)$. Le type simple T est de la forme $U_1 \to \dots U_m \to \Sigma_2$ et

$$A(\tau) \equiv [\![T]\!](\tau, \overline{v}(\tau)) \equiv \forall \overline{y}_1\ \dots\ \forall \overline{y}_m\, ([\![U_1]\!](\overline{y}_1) \to \dots \to [\![U_m]\!](\overline{y}_m) \to \delta(\tau, \widetilde{\mathrm{app}}(\dots \widetilde{\mathrm{app}}(\overline{v}(\tau), \overline{y}_1) \dots, \overline{y}_m)) \neq 0).$$

Il suffirait de pouvoir poser $t \in (\!|T|\!)$ de telle sorte que pour tous $u_1 \in (\!|U_1|\!), \dots, u_m \in (\!|U_m|\!)$, $t(u_1, \dots, u_m)$ soit égal à 0 si $t_0(u_1, \dots, u_m) = 0$, à 1 si $t_1(u_1, \dots, u_m) = 1$, et à Ω sinon. Cependant, pour que cela ait un sens, il faut encore montrer que pour tous $u_1 \in (\!|U_1|\!), \dots, u_m \in (\!|U_m|\!)$, on a $t_0(u_1, \dots, u_m) \neq 0$ ou $t_1(u_1, \dots, u_m) \neq 1$.

Soient donc $u_1 \in (\!|U_1|\!), \dots, u_m \in (\!|U_m|\!)$. Soient $\mathbb{B} = \{0,1\} \times \{0,1\}$ et $\rho = (0,1) \in \mathbb{B}$. Pour tout $k \in \{1, \dots, m\}$, on a $\mathbb{B} \models [\![U_k]\!](\rho, \sigma^*(u_k))$ d'après la proposition 4.15.

Par hypothèse, $\mathbb{B} \models A(\rho)$. Par conséquent, $\mathbb{B} \models \delta(\rho, \widetilde{\mathrm{app}}(\dots \widetilde{\mathrm{app}}(\overline{v}(j), \sigma^*(u_1)) \dots, \sigma^*(u_m))) \neq 1$. Autrement-dit, on n'a pas à la fois $t_0(u_1, \dots, u_m) = 0$ et $t_0(u_1, \dots, u_m) = 1$. □

Ainsi, une formule $A(\tau)$ est équivalente à une formule de la forme $[\![T]\!](\tau, \sigma^*(t))$ si et seulement si pour toute algèbre de Boole $\mathbb{B}$ à 4 éléments et tout $\rho \in \mathbb{B} \setminus \{0,1\}$, $\mathbb{B} \models A(\rho)$. En combinant ce résultat à la proposition 4.12, on obtient la classification des degrés de parallélisme de $\mathbb{C}_{\mathrm{Vote}}$:

Théorème 4.18. Soit τ une variable du langage des algèbres de Boole. Les deux $\mathcal{M}$-ensembles suivants, ordonnés par l'inclusion, sont $\mathcal{M}$-isomorphes :

- l'ensemble des degrés de parallélisme de $\mathbb{C}_{\mathrm{Vote}}$,
- l'ensemble des $\mathcal{M}$-ensembles Φ de formules du langage des algèbres de Boole tels que :
  - pour toute $A \in \Phi$, A n'a pas de variable libre autre que τ,
  - pour toute $A(\tau) \in \Phi$, pour toute algèbre de Boole $\mathbb{B}$ à 4 éléments et tout $\rho \in \mathbb{B} \setminus \{0,1\}$, $\mathbb{B} \models A(\rho)$,

— pour toutes $A_1(\tau), \ldots, A_n(\tau) \in \Phi$ et toute formule $B(\tau)$, si pour toute algèbre de Boole $\mathbb{B}$ à 4 éléments et tout $\rho \in \mathbb{B} \setminus \{0,1\}$, $\mathbb{B} \models B(\rho)$ et si la formule $\forall \tau\ (A_1(\tau) \to \ldots \to A_n(\tau) \to B(\tau))$ est vraie dans toute algèbre de Boole à au moins deux éléments, alors $B(\tau) \in \Phi$.

5 Instructions de comparaison, ordinal générique et lemme de Zorn restreint

Krivine a montré qu'introduire une instruction « quote », qui prend un argument et renvoie son « code »sous forme d'un entier de Church permet de réaliser des formules intéressantes, dont en particulier l'axiome des choix dépendants [Kri03]. Toutefois, cela n'est possible que si l'ensemble des termes est $\mathcal{M}$-dénombrable. On va présenter ici une technique très similaire mais qui fonctionne quel que soit le $\mathcal{M}$-cardinal de l'ensemble des termes. Celle-ci permet de réaliser des généralisations de l'axiome des choix dépendants qui sont équivalentes aux axiomes DC_κ [Jec73] et que l'on peut voir comme des versions affaiblies du lemme de Zorn.

Par ailleurs, si l'on pouvait développer une théorie de la réalisabilité adaptée au cas où l'ensemble des termes est une $\mathcal{M}$-classe propre, peut-être qu'une technique similaire à celle présentée ici permettrait de réaliser le lemme de Zorn complet, et donc l'axiome du choix.

On fixe une $\mathcal{M}$-bijection $\nu : \Lambda \to \lambda$ et une instruction non protégée χ.

On note $\succ^1_\nu$ la plus petite relation binaire sur $\mathcal{P}_\mathcal{M}(\Lambda \star \Pi)$ telle que

— Pour tous p, q tels que $p \succ^1_{\mathsf{K}} q$, $\{p\} \succ^1_\nu \{q\}$,

— Pour tous termes a, b, t, u, v et toute pile π :

  — Si $\nu(a) < \nu(b)$, $\{\chi \star a \cdot b \cdot t \cdot u \cdot v \cdot \pi\} \succ^1_\nu \{t \cdot \pi\}$,

  — Si $\nu(a) = \nu(b)$, $\{\chi \star a \cdot b \cdot t \cdot u \cdot v \cdot \pi\} \succ^1_\nu \{u \cdot \pi\}$,

  — Si $\nu(a) > \nu(b)$, $\{\chi \star a \cdot b \cdot t \cdot u \cdot v \cdot \pi\} \succ^1_\nu \{v \cdot \pi\}$.

De plus, on note $\succ_\nu$ la plus petite relation de multi-évaluation contenant $\succ^1_\nu$ et $\mathcal{S}_\nu$ la structure de réalisabilité engendrée par $\succ_\nu$.

5.1 L'ordinal générique $\widehat{\lambda}$

5.1.1 Construction de l'ordinal générique

Pour tout $\alpha \leq \lambda$, on pose $\widehat{\alpha} = \{\ (\widehat{\beta}, \nu^{-1}(\beta) \cdot \pi);\ \pi \in \Pi, \beta < \alpha\ \}$.

Lemme 5.1. Pour tout $\alpha < \lambda$, $\lambda x.\ x(\nu^{-1}(\alpha))$ réalise $\widehat{\alpha}\ \varepsilon\ \widehat{\lambda}$ modulo $\mathcal{S}_\nu$.

Notation. Pour tout $\alpha \leq \lambda$, tout terme du premier ordre b et toute formule A, on note $b\ \varepsilon\ \widehat{\alpha} \hookrightarrow A$ la formule $(b \not\varepsilon \widehat{\alpha}) \cup (\top \to A)$.

Lemme 5.2. Pour tout $\alpha \leq \lambda$, tout terme du premier ordre clos b, toute formule close A et tout $\perp\!\!\!\perp \in \mathcal{S}_\nu$, si $[b]_{\perp\!\!\!\perp} = \widehat{\beta}$ pour un $\beta < \alpha$, alors $\|b\ \varepsilon\ \widehat{\alpha} \hookrightarrow A\|_{\perp\!\!\!\perp} = \{\nu^{-1}(\beta) \cdot \pi;\ \pi \in \|A\|\}$, et sinon, $\|b\ \varepsilon\ \widehat{\alpha} \hookrightarrow A\|_{\perp\!\!\!\perp} = \emptyset = \|\top\|_{\perp\!\!\!\perp}$.

Lemme 5.3. Pour tous $\beta < \alpha \leq \lambda$, $(\widehat{\beta} \not\varepsilon \widehat{\alpha}) \equiv_{\mathcal{S}_\nu} (\widehat{\beta}\ \varepsilon\ \widehat{\alpha} \hookrightarrow \bot)$.

Lemme 5.4. Pour tout $\alpha \leq \lambda$, tout terme du premier ordre b et toute formule A, les formules $b\ \varepsilon\ \widehat{\alpha} \hookrightarrow A$ et $b\ \varepsilon\ \widehat{\alpha} \to A$ sont équivalentes modulo $\mathcal{S}_\nu$.

Démonstration. On va réaliser l'implication de droite à gauche par le terme $d = \lambda t.\lambda u.t(\lambda x.xu)$ et l'implication de gauche à droite par le terme $g = \lambda t.\lambda u.\ c\!\!c(\lambda k.u(\lambda x.k(tx)))$.

On peut supposer sans perte de généralité que A et b sont clos.

Le fait que d réalise l'implication $(b\ \varepsilon\ \widehat{\alpha} \to A) \to (b\ \varepsilon\ \widehat{\alpha} \hookrightarrow A)$ est conséquence du lemme 5.1.

Montrons que g réalise $(b\ \varepsilon\ \widehat{\alpha} \hookrightarrow A) \to (b\ \varepsilon\ \widehat{\alpha} \to A)$. Soient $\perp\!\!\!\perp \in \mathcal{S}_\nu$, $t \in |b\ \varepsilon\ \widehat{\alpha} \hookrightarrow A|_{\perp\!\!\!\perp}$, $u \in |b\ \varepsilon\ \widehat{\alpha}|_{\perp\!\!\!\perp}$ et $\pi \in \|A\|$. D'une part $g \star t \cdot u \cdot \pi \succ_{\mathrm{K}} u \star (\lambda x.k_\pi(tx)) \cdot \pi$, et d'autre part u réalise $b \notin \widehat{\alpha} \to \bot$, donc il suffit de montrer que $\lambda x.k_\pi(tx)$ réalise $b \notin \widehat{\alpha}$. Dans le cas où $[b]_{\perp\!\!\!\perp} = \widehat{\beta}$ pour $\beta < \alpha$, on a bien que pour toute pile π', $\lambda x.k_\pi(tx) \star \nu^{-1}(\beta) \cdot \pi' \succ_{\mathrm{K}} t \star \nu^{-1}(\beta) \cdot \pi \in \perp\!\!\!\perp$. Dans le cas contraire, on a tout simplement $\|b \notin \widehat{\alpha}\|_{\perp\!\!\!\perp} = \emptyset$. □

Notation. Pour tout $\alpha \leq \lambda$, toute formule A et toute variable x, on note $\forall x^{\widehat{\alpha}}\ A$ pour $\forall x\ (x\ \varepsilon\ \widehat{\alpha} \hookrightarrow A)$ et $\exists x^{\widehat{\alpha}}\ A$ pour $\forall x\ (x\ \varepsilon\ \widehat{\alpha} \hookrightarrow A \to \bot) \to \bot$.

5.1.2 Propriétés d'ordinal

On va montrer que les objets (désignés par des noms) de la forme $\widehat{\alpha}$ sont bien des ordinaux.

Notation. On note $\mathrm{Ord}_\in(a)$ la formule suivante, qui dit que que a est un ordinal au sens usuel (extensionnel) :

$$\begin{array}{lll} & \forall x{\in}a\ \forall y{\in}x\ y{\in}a & \text{(l'ensemble } a \text{ est transitif)} \\ \wedge & \forall x{\in}a\ \forall y{\in}a\ \forall z{\in}a\ (x{\in}y \to y{\in}z \to x{\in}z) & \text{(la relation } \in \text{ définit un ordre strict sur } a) \\ \wedge & \forall x{\in}a\ \forall y{\in}a\ (x{\in}y \vee x{\approx}y \vee y{\in}x) & \text{(cet ordre est total).} \end{array}$$

Remarquons qu'il n'est pas nécessaire de demander que la relation $\in$ soit bien fondée ni qu'elle soit anti-réflexive, car cela est déjà garanti par le schéma d'axiomes de fondation.

On peut également définir une version non extensionnelle de cette formule :

Notation. On note $\mathrm{Ord}_\varepsilon(a)$ la formule suivante :

$$\begin{array}{lll} & \forall x\varepsilon a\ \forall y\varepsilon x\ y\varepsilon a & \text{(l'ensemble } a \text{ est transitif)} \\ \wedge & \forall x\varepsilon a\ \forall y\varepsilon a\ \forall z\varepsilon a\ (x\varepsilon y \to y\varepsilon z \to x\varepsilon z) & \text{(la relation } \varepsilon \text{ définit un ordre strict sur } a) \\ \wedge & \forall x\varepsilon a\ \forall y\varepsilon a\ (x\varepsilon y \vee x{=}y \vee y\varepsilon x) & \text{(cet ordre est total).} \end{array}$$

On peut vérifier facilement que tout ordinal au sens non extensionnel en est également un au sens extensionnel :

Lemme 5.5. La formule $\forall a\ (\mathrm{Ord}_\varepsilon(a) \to \mathrm{Ord}_\in(a))$ est conséquence de ZF_ε.

Les ordinaux au sens non extensionnel ont également la propriété (qui s'avèrera cruciale par la suite) de ε-contenir exactement un représentant de chacun de leurs $\in$-éléments :

Proposition 5.6. La formule $\forall a\ (\mathrm{Ord}_\varepsilon(a) \to \forall x\varepsilon a\ \forall y\varepsilon a\ (x \approx y \leftrightarrow x = y))$ est conséquence de ZF_ε.

Démonstration. Plaçons nous dans un modèle de ZF_ε. Soit a un ordinal au sens non extensionnel (c'est-à-dire a tel que $\mathrm{Ord}_\varepsilon(a)$ soit vraie). Soient x et y deux ε-éléments de a. Si $x = y$, on a bien $x \approx y$, et si $x \neq y$, alors on a soit $x\ \varepsilon\ y$, soit $y\ \varepsilon\ x$. Dans le premier cas, on a alors $x \in y$, et dans le deuxième $y \in x$: dans les deux cas, à cause du schéma d'axiomes de fondation (extensionnel), on a $x \not\approx y$. □

On a alors le résultat annoncé au début de cette section :

Proposition 5.7. Pour tout $\alpha \leq \lambda$, la formule $\mathrm{Ord}_\varepsilon(\widehat{\alpha})$ est réalisée modulo $\mathcal{S}_\nu$.

Démonstration. L'ensemble $\widehat{\alpha}$ est transitif : on va montrer montrer que la formule $\forall x^{\widehat{\alpha}}\ \forall y\ (y \notin \widehat{\alpha} \to y \notin x)$ (qui est équivalente à celle que l'on cherche à réaliser) est réalisée par $\theta = \lambda t.\lambda u.u$. Soient $\perp\!\!\!\perp \in \mathcal{S}_\nu$, $\beta < \alpha$, $c \in \mathcal{M}$, $u \in |y \notin \widehat{\alpha}|_{\perp\!\!\!\perp}$ et $\pi \in \left\|c \notin \widehat{\beta}\right\|_{\perp\!\!\!\perp}$: on doit montrer que $\theta \star \nu^{-1}(\beta) \cdot u \cdot \pi \in \perp\!\!\!\perp$. Tout d'abord, on a $\delta \star \nu^{-1}(\beta) \cdot u \cdot \pi \succ_{\mathrm{K}} u \star \pi$. Ensuite, comme $\pi \in \left\|c \notin \widehat{\beta}\right\|_{\perp\!\!\!\perp}$, $\left\|c \notin \widehat{\beta}\right\|_{\perp\!\!\!\perp} \neq \emptyset$, donc il existe $\gamma < \beta < \alpha$ tel que $c = \widehat{\gamma}$. Par conséquent, $\left\|c \notin \widehat{\beta}\right\|_{\perp\!\!\!\perp} = \{\nu^{-1}(\gamma) \cdot \pi';\ \pi' \in \Pi\} = \|c \notin \widehat{\alpha}\|_{\perp\!\!\!\perp}$, et donc $u \star \pi \in \perp\!\!\!\perp$.

La relation ε définit un ordre strict sur sur $\widehat{\alpha}$: similaire au point précédent.

Cet ordre est total : c'est là qu'entre en jeu l'instruction de comparaison χ. En effet, on va montrer que le terme $\tau = \lambda b.\lambda c.\ \lambda t.\lambda u\lambda v.\ \chi\ b\ c\ (tb)\ (u)\ (vc)$ réalise la formule $\forall x^{\widehat{a}}\ \forall y^{\widehat{\alpha}}\ (x \not\varepsilon y \to x \neq y \to y \not\varepsilon x \to \bot)$ (qui est équivalente à celle que l'on cherche à réaliser). Soient $\perp\!\!\!\perp \in \mathcal{S}_\nu$, $\beta < \alpha$, $\gamma < \alpha$, $t \in \left|\widehat{\beta} \not\varepsilon \widehat{\alpha}\right|_{\perp\!\!\!\perp}$, $u \in \left|\widehat{\beta} \neq \widehat{\alpha}\right|_{\perp\!\!\!\perp}$, $v \in \left|\widehat{\alpha} \not\varepsilon \widehat{\beta}\right|_{\perp\!\!\!\perp}$ et $\pi \in \Pi$: on doit montrer que $\tau \star \nu^{-1}(\beta) \cdot \nu^{-1}(\gamma) \cdot t \cdot u \cdot v \cdot \pi \in \perp\!\!\!\perp$.

Si $\beta < \gamma$ alors $\{\tau \star \nu^{-1}(\beta) \cdot \nu^{-1}(\gamma) \cdot t \cdot u \cdot v \cdot \pi\} \succ_\nu \{t \star \nu^{-1}(\beta) \star \pi\} \subseteq \perp\!\!\!\perp$ (car t réalise $\widehat{\beta} \not\varepsilon \widehat{\gamma}$ et $\beta < \gamma$). Si $\beta > \gamma$, la situation est symétrique. Enfin, si $\beta = \gamma$ alors $\{\tau \star \nu^{-1}(\beta) \cdot \nu^{-1}(\gamma) \cdot t \cdot u \cdot v \cdot \pi\} \succ_\nu \{v \star \pi\} \subseteq \perp\!\!\!\perp$ (car v réalise $(\widehat{\beta} \neq \widehat{\gamma}) \equiv_{\mathcal{S}_\nu} \bot$). □

5.2 Choix non extensionnel

On va formuler le choix non extensionnel comme un schéma de formules :

Définition 5.8. Un *schéma d'axiomes de choix non extensionnels* est un ensemble $\mathcal{T}$ de formules closes tel que pour toute formule $A(\overline{w}, x)$, il existe une formule $A^*(\overline{w}, x)$ telle que $\mathcal{T}$ contienne les trois formules suivantes :

— $\forall \overline{w}\ \forall x\ (A^*(\overline{w}, x) \to A(\overline{w}, x))$,

— $\forall \overline{w}\ \forall x\ \forall y\ (A^*(\overline{w}, x) \to A^*(\overline{w}, y) \to x = y)$,

— $\forall \overline{w}\ (\exists x\ A(\overline{w}, x) \to \exists x\ A^*(\overline{w}, x))$.

Autrement-dit, la formule A^* « choisit » exactement un des x qui vérifient $A(\overline{w}, x)$, s'il en existe.

L'objectif de cette section est donc de montrer le résultat suivant :

Proposition 5.9. La théorie $\mathrm{Th}(\mathcal{S}_\nu)$ contient un schéma d'axiomes de choix non extensionnels.

On va avoir besoin du lemme suivant :

Lemme 5.10. Pour toute formule $A(\overline{w}^n, x)$, il existe une $\mathcal{M}$-fonctionnelle $\mathsf{f}_A : \mathcal{S}_0 \times \mathcal{M}^{n+1} \to \mathcal{M}$ telle que la formule $\forall \overline{w}\ (\exists x\ A(\overline{w}, x) \to \exists a\varepsilon\, \widehat{\lambda}\ A(\overline{w}, \mathsf{f}_A(\overline{w}, a)))$ soit réalisée modulo $\mathcal{S}_\nu$.

Démonstration. Pour tout terme t et tout $\perp\!\!\!\perp \in \mathcal{S}_\nu$, on pose $P_{\perp\!\!\!\perp, t} = \{\pi; t \star t \cdot \pi \notin \perp\!\!\!\perp\}$.

Pour tout $\perp\!\!\!\perp \in \mathcal{S}_\nu$, tous $\overline{w} \in \mathcal{M}$ et tout $\alpha < \lambda$ tels que $P_{\perp\!\!\!\perp, \nu^{-1}(\alpha)} \cap \|\forall x\ \neg A(\overline{w}, x)\|_{\perp\!\!\!\perp} \neq \emptyset$, on choisit un $x \in \mathcal{M}$ tel que $P_{\perp\!\!\!\perp, \nu^{-1}(\alpha)} \cap \|\neg A(\overline{w}, x)\|_{\perp\!\!\!\perp} \neq \emptyset$ (ce que l'on peut faire car $\|\forall x\ \neg A(\overline{w}, x)\|_{\perp\!\!\!\perp} = \bigcup_{x \in \mathcal{M}} \|\neg A(\overline{w}, x)\|_{\perp\!\!\!\perp}$), et l'on pose $\mathrm{pch}_A(\perp\!\!\!\perp, \overline{w}, \widehat{\alpha}) = x$ (donc $P_{\perp\!\!\!\perp, \nu^{-1}(\alpha)} \cap \|\neg A(\overline{w}, f_A(\perp\!\!\!\perp, \overline{w}, \widehat{\alpha}))\|_{\perp\!\!\!\perp} \neq \emptyset$). Ensuite, on étend pch_A arbitrairement à tout $\mathcal{S}_0 \times \mathcal{M}^{n+1}$.

On va montrer que le terme $\lambda y.\ yy$ réalise la formule $\forall \overline{w}\ (\forall a^{\widehat{\lambda}}\ \neg A(\overline{w}, f_A(\overline{w}, a)) \to \forall x\ \neg A(\overline{w}, x))$. Soient $\perp\!\!\!\perp \in \mathcal{S}_\nu$, $\overline{w} \in \mathcal{M}$, $t \in \left|\forall a^{\widehat{\lambda}}\ \neg A(\overline{w}, f_A(\overline{w}, a))\right|_{\perp\!\!\!\perp}$ et $\pi \in \|\forall x\ \neg A(\overline{w}, x)\|$. Montrons que $t \star t \cdot \pi \in \perp\!\!\!\perp$:

Comme t réalise $\forall a^{\widehat{\lambda}}\ \neg A(\overline{w}, f_A(\overline{w}, a))$, en particulier, pour tout $\pi' \in \left\|\neg A(\overline{w}, f_A(\overline{w}, \widehat{\nu(t)}))\right\|_{\perp\!\!\!\perp}$, $t \star t \cdot \pi' \in \perp\!\!\!\perp$. Autrement-dit, $P_{\perp\!\!\!\perp, t} \cap \left\|\neg A(\overline{w}, f_A(\overline{w}, \widehat{\nu(t)}))\right\|_{\perp\!\!\!\perp} = \emptyset$, et par conséquent $P_{\perp\!\!\!\perp, t} \cap \|\forall x\ \neg A(\overline{w}, x)\|_{\perp\!\!\!\perp} = \emptyset$. Comme $\pi \in \|\forall x\ \neg A(\overline{w}, x)\|_{\perp\!\!\!\perp}$, on a donc $\pi \notin P_{\perp\!\!\!\perp, t}$, c'est-à-dire que $t \star t \cdot \pi \in \perp\!\!\!\perp$. □

Le lemme 5.10 permet de choisir pour chaque classe non vide A une sous-classe non vide (en fait un sous-ensemble) indexée par une partie de $\widehat{\lambda}$. Ensuite, il n'y a plus qu'à utiliser le bon ordre sur $\widehat{\lambda}$ pour choisir l'élément de cette sous-classe qui porte le plus petit indice :

Preuve de la proposition 5.9. Pour tout terme du premier ordre $f(\overline{w}, a)$, notons $A^*_f(\overline{w}, x, k)$ la formule $A(\overline{w}, x) \wedge \exists a \varepsilon k \ (x = f(\overline{w}, a) \wedge \forall b \varepsilon a \ \neg A(\overline{w}, f(\overline{w}, b)))$. La formule

$$\forall k \left(\left(\begin{array}{ll} & \forall \overline{w} \ (\exists x \ A(\overline{w}, x) \to \exists a \varepsilon k \ A(\overline{w}, f(\overline{w}, a))) \\ \wedge & \mathrm{Ord}_\varepsilon(k) \end{array} \right) \right.$$
$$\left. \to \left(\begin{array}{ll} & \forall \overline{w} \ \forall x \ (A^*_f(\overline{w}, x, k) \to A(\overline{w}, x)) \\ \wedge & \forall \overline{w} \ \forall x \ \forall y \ (A^*_f(\overline{w}, x, k) \to A^*_f(\overline{w}, y, k) \to x = y) \\ \wedge & \forall \overline{w} \ (\exists x \ A(\overline{w}, x) \to \exists x \ A^*_f(\overline{w}, x, k)) \end{array} \right) \right)$$

est conséquence de ZF_ε.

En effet, plaçons-nous dans un modèle de ZF_ε, et soit k un ordinal au sens non extensionnel tel que $\forall \overline{w} \ (\exists x \ A(\overline{w}, x) \to \exists a \varepsilon k \ A(\overline{w}, f(\overline{w}, a)))$ soit vraie :

La formule $\forall \overline{w} \ \forall x \ (A^*_f(\overline{w}, x, k) \to A(\overline{w}, x))$ est vraie par définition de A^*.

Soient $\overline{w}$, x et y tels que $A^*_f(\overline{w}, x, k)$ et $A^*_f(\overline{w}, y, k)$ soient vraies, et supposons par l'absurde que $x \neq y$. Soit $a \ \varepsilon \ k$ tel que $x = f(\overline{w}, a)$ et que $\forall a' \varepsilon a \ \neg A(\overline{w}, f(\overline{w}, a'))$ soit vraie. Soit $b \ \varepsilon \ k$ tel que $y = f(\overline{w}, b)$ et que $\forall b' \varepsilon b \ \neg A(\overline{w}, f(\overline{w}, b')$ soit vraie. Comme $x \neq y$, $a \neq b$, donc $a \ \varepsilon \ b$ ou $b \ \varepsilon \ a$ (car k est un ordinal au sens non extensionnel). Comme Dans le premier cas, on contredit $\forall b' \varepsilon b \ \neg A(\overline{w}, f(\overline{w}, b'))$ (car $A(\overline{w}, f(\overline{w}, a))$ est vraie), et dans le second, on contredit $\forall a' \varepsilon a \ \neg A(\overline{w}, f(\overline{w}, a'))$.

On va raisonner par contraposée. Soient $\overline{w}$ tels que pour tout x, $A^*_f(\overline{w}, x, k)$ soit fausse. Pour tout $a \ \varepsilon \ k$, si $A(\overline{w}, f(\overline{w}, a))$ est vraie, alors il existe $b \ \varepsilon \ a$ tel que $A(\overline{w}, f(\overline{w}, b))$ (sinon, $A^*_f(\overline{w}, a, k)$ serait vraie). Par conséquent, par le schéma d'axiomes de fondation (non extensionnel), $A(\overline{w}, f(\overline{w}, a))$ est fausse pour tout $a \ \varepsilon \ k$, ce qui implique que $A(\overline{w}, x)$ est fausse pour tout x.

Il n'y a plus qu'à poser $A^*(\overline{w}, x) = A^*_{\mathrm{f}_A(\overline{w}, x)}(\overline{w}, x, \widehat{\lambda})$, où f_A est la fonctionnelle donnée par le lemme 5.10. □

5.3 Lemme de Zorn restreint

On va montrer que $\mathrm{Th}(\mathcal{S}_\nu)$ contient une version du lemme de Zorn « restreinte à l'ordinal $\widehat{\lambda}$ ». Plus précisément, on va montrer que pour toute relationnelle R, si toute R-chaîne[i] admet un majorant strict, alors il existe une R-chaîne indexée par $\widehat{\lambda}$[ii]. Contrairement à la section précédente, il s'agira ici d'une version restreinte du lemme de Zorn *extensionnel*, c'est-à-dire du lemme de Zorn tel qu'on l'entend habituellement. Formellement, on va utiliser un schéma de formules, en se servant des notations suivantes :

Notation (Majorant strict d'un ensemble)**.** Pour toute formule $R(\overline{w}, x, y)$ et toutes variables du premier ordres m et c distinctes entre elles et distinctes de $\overline{m}$, x et y, on note $\mathrm{Maj}^R_\in(\overline{w}, c, m)$ la formule $\forall x \in c \ R(\overline{w}, x, m)$.

Notation (Chaîne)**.** Pour toute formule $R(\overline{w}, x, y)$ et toute variable du premier ordre c distincte de $\overline{m}$, x et y, on note $\mathrm{Chaine}^R_\in(\overline{w}, c)$ la formule $\forall x \in c \ \forall y \in c \ (x \not\approx y \to R(\overline{w}, x, y) \vee R(\overline{w}, y, x))$.

Définition 5.11. Soit α un terme clos du premier ordre. Un *schéma de Zorn restreint à* α est un ensemble $\mathcal{T}$ de formules closes qui contient la formule $\mathrm{Ord}_\in(\alpha)$ et tel que pour toute formule $R(\overline{w}, x, y)$ extensionnelle en x et y, il existe une formule $Z_R(\overline{w}, \beta, y)$ extensionnelle en β et y telle que $\mathcal{T}$ contienne les trois formules suivantes :

— $\forall \overline{w} \ \Big(\forall c \ (\mathrm{Chaine}^R_\in(\overline{w}, c) \to \exists m \ \mathrm{Maj}^R_\in(\overline{w}, c, m)) \to \forall \beta \in \alpha \ \exists y \ Z_R(\overline{w}, \beta, y)\Big)$,

— $\forall \overline{w} \ \forall \beta \in \alpha \ \forall \gamma \in \alpha \ \forall y \ \forall z \ \ (Z_R(\overline{w}, \beta, y) \to Z_R(\overline{w}, \gamma, z) \to \beta \in \gamma \to R(\overline{w}, y, z))$,

— $\forall \overline{w} \ \forall \beta \in \alpha \ \forall \gamma \in \alpha \ \forall y \ \forall z \ \ (Z_R(\overline{w}, \beta, y) \to Z_R(\overline{w}, \gamma, z) \to \beta \approx \gamma \to y \approx z)$.

i. Il faut imaginer R comme une relation d'ordre, mais il n'est pas nécessaire de supposer qu'elle l'est vraiment : cela ne ferait qu'alourdir les formules.

ii. Ce qui est équivalent à l'axiome $\mathrm{DC}_{\widehat{\lambda}}$ [Jec73, chapitre 8 : « Some weaker versions of the axiom of choice »].

Ces trois formules disent que si toute R-chaîne admet un majorant strict, alors Z_R définit une fonction strictement croissante pour R de domaine α. Plus précisément, la troisième dit que Z_R est fonctionnelle (au sens extensionnel), la deuxième que Z_R est strictement croissante pour R et la première que si toute R-chaîne admet un majorant strict, alors Z_R est totale sur le domaine α.

Remarque. Dans la définition ci-dessus, le troisième point impose que la relation $Z_R(\overline{w}, \beta, y)$ soit fonctionnelle au sens extensionnel *par rapport à l'argument* β, mais pas nécessairement par rapport aux arguments $\overline{w}$ (c'est-à-dire que si $Z_R(\overline{w}, \beta, z)$ et $Z_R(\overline{w}', \gamma, z')$ avec $\overline{w} \approx \overline{w}'$, on n'a pas nécessairement $z \approx z'$). Cependant, la proposition suivante montre que cette définition est satisfaisante :

Proposition 5.12. Soit $\mathrm{Rel}(w, x, y)$ la formule $\exists z{\in}w\ \ \mathrm{Couple}_{\in}(x, y, z)$ (qui dit que x et y sont liés par la relation binaire w, une relation binaire étant vue comme un ensemble de couples de Kuratowski). Soient α un terme clos du premier ordre et $\mathcal{T}$ une théorie contenant ZF_ε et un schéma de Zorn restreint à α. Alors la formule suivante (qui est strictement extensionnelle) est conséquence de $\mathcal{T}$:

$$\forall r \left(\begin{array}{c} \forall c\ (\mathrm{Chaine}^{\mathrm{Rel}}_{\in}(r, c) \to \exists m\ \mathrm{Maj}^{\mathrm{Rel}}_{\in}(r, c, m)) \\ \to \exists \zeta \left(\begin{array}{ll} & \forall \beta{\in}\alpha\ \exists y\ \ \mathrm{Rel}(\zeta, \beta, y) \\ \wedge & \forall \beta{\in}\alpha\ \forall \gamma{\in}\alpha\ \forall y\ \forall z\ (\mathrm{Rel}(\zeta, \beta, y) \to \mathrm{Rel}(\zeta, \gamma, z) \to \beta \in \gamma \to \mathrm{Rel}(r, y, z)) \\ \wedge & \forall \beta{\in}\alpha\ \forall \gamma{\in}\alpha\ \forall y\ \forall z\ (\mathrm{Rel}(\zeta, \beta, y) \to \mathrm{Rel}(\zeta, \gamma, z) \to \beta \approx \gamma \to y \approx z) \end{array} \right) \end{array} \right).$$

Démonstration. Il suffit d'appliquer le schéma de Zorn restreint pour la formule $\mathrm{Rel}(w, x, y)$ et de définir ζ par compréhension. □

Proposition 5.13. $\mathrm{Th}\,(\mathcal{S}_\nu)$ contient un schéma de Zorn restreint à $\widehat{\lambda}$.

Démonstration. Fixons une formule $R(\overline{w}, x, y)$ extensionnelle en x et y.

Informellement, l'idée de la preuve est la suivante. On se place à l'intérieur d'un modèle de $\mathrm{Th}\,(\mathcal{S}_\nu)$, on a une relation R (que l'on imagine être une relation d'ordre) telle que toute chaîne admet un majorant strict, et l'on veut choisir pour tout $\alpha \in \widehat{\lambda}$ un $\approx$-unique y_α de telle sorte que y_α croisse strictement avec α. Une première difficulté est qu'à priori, on n'a pas la possibilité d'effectuer des choix compatibles avec $\approx$. Cependant, puisque $\widehat{\lambda}$ est un ordinal au sens non extensionnel, il ε-contient un unique représentant de chacun de ses $\in$-éléments. Il suffit donc de choisir pour tout $\alpha\ \varepsilon\ \widehat{\lambda}$ un $=$-unique y_α (ensuite, à tout $\alpha' \in \widehat{\lambda}$ on associera le y_α choisi pour l'unique $\alpha\ \varepsilon\ \widehat{\lambda}$ tel que $\alpha \approx \alpha'$). Pour choisir cet y_α, l'idée est de procéder par induction sur α : si l'on a choisi y_β pour tout $\beta\ \varepsilon\ \alpha$, il suffit de choisir comme y_α un majorant strict de $\{y_\beta;\ \beta\ \varepsilon\ \alpha\}$, qui est une chaîne. Cependant, la seconde difficulté est que ZF_ε ne permet pas à priori de telles « constructions par induction non extensionnelle » : on va donc devoir faire l'induction « à l'extérieur du modèle ». En particulier, le point clé de la preuve qui suit, c'est qu'il faudra nommer pour chaque $\alpha \leq \lambda$ un unique représentant de la chaîne $\{y_\beta;\ \beta\ \varepsilon\ \alpha\}$: ce sera le rôle des fonctions $F_{<\alpha}(\perp\!\!\!\perp, \overline{w})$, qui seront définies un peu plus loin.

On va manipuler des graphes de fonctions non extensionnelles. Pour cela, on va avoir besoin de nommer des paires d'éléments de $\mathcal{M}$ dans les formules. Notons donc p la $\mathcal{M}$-fonctionnelle de $\mathcal{M}^2$ dans $\mathcal{M}$ définie par $p(a, b) = (a, b)$.

Notons img la $\mathcal{M}$-fonctionnelle de $\mathcal{M}$ dans $\mathcal{M}$ définie par $\mathrm{img}(f) = \{\ (y, \pi);\ (p(x, y), \pi) \in f\ \}$. On peut vérifier que pour tous $f, y \in \mathcal{M}$, $y \notin \mathrm{img}(f) \equiv \forall x\ p(x, y) \notin f$. Par conséquent, la formule $\forall f\ \forall y\ (y\ \varepsilon\ \mathrm{img}(f) \leftrightarrow \exists x\ p(x, y)\ \varepsilon\ f)$ est universellement réalisée.

Notons $\mathrm{MajImg}(\overline{w}, f, m)$ la formule $\mathrm{Maj}^R_{\in}(\overline{w}, \mathrm{img}(f), m)$.

Soient $\mathrm{MajImg}^*(\overline{w}, f, m)$ la formule donnée par le choix non extensionnel (proposition 5.9) appliqué à la formule $\mathrm{MajImg}(\overline{w}, f, m)$ et μ la $\mathcal{M}$-fonctionnelle de $\mathcal{S}_0 \times \mathcal{M}^{n+1}$ dans $\mathcal{M}$ donnée par le principe de nommage des singletons (proposition 2.26) appliqué à $\mathrm{MajImg}^*(\overline{w}, f, m)$.

Ainsi, les formules suivantes sont réalisées modulo $\mathcal{S}_\nu$:

— $\forall \overline{w}\ \forall f\ (\exists m\ \mathrm{Maj}^R_{\in}(\overline{w}, \mathrm{img}(f), m) \to \exists m\ (m\ \varepsilon\ \mu(\overline{w}, f)))$,

— $\forall \overline{w}\ \forall f\ \forall m\ (m\ \varepsilon\ \mu(\overline{w}, f) \to \mathrm{Maj}^R_{\in}(\overline{w}, \mathrm{img}(f), m))$,

— $\forall \overline{w}\ \forall f\ \forall m\ \forall m'\ (m\ \varepsilon\ \mu(\overline{w}, f) \to m'\ \varepsilon\ \mu(\overline{w}, f) \to m = m')$.

Pour tout $\perp\!\!\!\perp \in \mathcal{S}_\nu$ et tous $\overline{w} \in \mathcal{M}$, par induction mutuelle, on définit pour tout $\alpha < \lambda$ $F_{\leq\alpha}(\perp\!\!\!\perp, \overline{w}) = F_{<\alpha}(\perp\!\!\!\perp, \overline{w}) \cup \{\ (p(\widehat{\alpha}, y), t \bullet \pi);\ t \Vdash_{\perp\!\!\!\perp} \widehat{\alpha}\ \varepsilon\ \widehat{\lambda}, (y, \pi) \in \mu(\perp\!\!\!\perp, \overline{w}, F_{<\alpha}(\perp\!\!\!\perp, \overline{w}))\ \}$, et pour tout $\alpha \leq \lambda$ $F_{<\alpha}(\perp\!\!\!\perp, \overline{w}) = \bigcup_{\beta<\alpha} F_{\leq\beta}(\perp\!\!\!\perp, \overline{w})$. On étend arbitrairement les fonctions $F_{\leq\alpha}$ et $F_{<\alpha}$ à tout $\perp\!\!\!\perp \in \mathcal{S}_0$.

On définit alors $Z_R(\overline{w}, \alpha, y)$ comme $\exists \alpha' \varepsilon\, \widehat{\lambda}\ \exists y'\ (\alpha' \approx \alpha \wedge y' \approx y \wedge p(\alpha, y')\ \varepsilon\ F_{<\lambda}(\overline{w}))$.

En considérant la définition de $F_{<\alpha}$ pour $\alpha \leq \lambda$, on constate trois choses :

— pour tout $\alpha \leq \lambda$ la formule $\forall \overline{w}\ \forall \delta\ \forall y\ (\delta \not\varepsilon \widehat{\alpha} \to p(\delta, y) \not\varepsilon F_{<\alpha}(\overline{w}))$ est réalisée modulo $\mathcal{S}_\nu$ par $\lambda x.\ \lambda t.\ tx$,

— pour tout $\alpha < \lambda$ et tous $\overline{w}, y \in \mathcal{M}$, on a $p(\widehat{\alpha}, y) \not\varepsilon F_{<\lambda}(\overline{w}) \equiv_{\mathcal{S}_\nu} \widehat{\alpha}\ \varepsilon\ \widehat{\lambda} \to y \not\varepsilon \mu(\overline{w}, F_{<\alpha}(\overline{w}))$

— pour tous $\delta < \alpha < \lambda$ et tous $\overline{w}, z \in \mathcal{M}$, on a $p(\widehat{\delta}, z) \not\varepsilon F_{<\lambda}(\overline{w}) \equiv_{\mathcal{S}_\nu} p(\widehat{\delta}, z) \not\varepsilon F_{<\alpha}(\overline{w})$.

D'après le premier point, la formule $\forall \overline{w}\ \forall \beta\ \forall y\ (p(\beta, y)\ \varepsilon\ F_{<\lambda}(\overline{w}) \to \beta\ \varepsilon\ \widehat{\lambda})$ est réalisée modulo $\mathcal{S}_\nu$. D'après les trois points, la formule $\forall \overline{w}\ \forall \gamma \varepsilon\, \widehat{\lambda}\ \exists F\ (\forall \beta\ \forall y\ (p(\beta, y)\ \varepsilon\ F \to \beta\ \varepsilon\ \gamma) \wedge \forall z\ (p(\gamma, z)\ \varepsilon\ F_{<\lambda}(\overline{w}) \leftrightarrow z\ \varepsilon\ \mu(\overline{w}, F)) \wedge \forall \beta \varepsilon \gamma\ \forall y\ (p(\beta, y)\ \varepsilon\ F_{<\lambda}(\overline{w}) \leftrightarrow p(\beta, y)\ \varepsilon\ F))$ est réalisée modulo $\mathcal{S}_\nu$.

En utilisant ces remarques, on va montrer que les trois formules suivantes sont réalisées modulo $\mathcal{S}_\nu$:

(1) $\forall \overline{w}\ \Big(\forall c\ (\mathrm{Chaine}^R_\in(\overline{w}, c) \to \exists m\ \mathrm{Maj}^R_\in(\overline{w}, c, m)) \to \forall \beta \in \widehat{\lambda}\ \exists y\ Z_R(\overline{w}, \beta, y)\Big)$,

(2) $\forall \overline{w}\ \forall \beta \in \widehat{\lambda}\ \forall \gamma \in \widehat{\lambda}\ \forall y\ \forall z\ \ (Z_R(\overline{w}, \beta, y) \to Z_R(\overline{w}, \gamma, z) \to \beta \in \gamma \to R(\overline{w}, y, z))$,

(3) $\forall \overline{w}\ \forall \beta \in \widehat{\lambda}\ \forall \gamma \in \widehat{\lambda}\ \forall y\ \forall z\ \ (Z_R(\overline{w}, \beta, y) \to Z_R(\overline{w}, \gamma, z) \to \beta \approx \gamma \to y \approx z)$.

Considérons un modèle $\mathcal{N}$ de $\mathrm{Th}(\mathcal{S}_\nu)$, et montrons que ces trois formules sont vraies dans $\mathcal{N}$:

Preuve de (3) : Soient $\overline{w}, y, z$ des objets de $\mathcal{N}$ et soient $\beta, \gamma \in \widehat{\lambda}$ tels que $\beta \approx \gamma$ et que $Z_R(\overline{w}, \beta, y)$ et $Z_R(\overline{w}, \gamma, z)$ soient vraies. Soient $\beta' \approx \beta$, $\gamma' \approx \gamma$, $y' \approx y$ et $z' \approx z$ tels que $\beta'\ \varepsilon\ \widehat{\lambda}$, $\gamma'\ \varepsilon\ \widehat{\lambda}$, $p(\beta', y')\ \varepsilon\ F_{<\lambda}(\overline{w})$ et $p(\gamma', z')\ \varepsilon\ F_{<\lambda}(\overline{w})$. On a $\beta' \approx \beta \approx \gamma \approx \gamma'$, $\beta'\ \varepsilon\ \lambda$ et $\gamma'\ \varepsilon\ \lambda$, par conséquent, $\beta' = \gamma'$. Soit F tel que $\forall x\ (p(\gamma', x)\ \varepsilon\ F_{<\lambda}(\overline{w}) \leftrightarrow x\ \varepsilon\ \mu(\overline{w}, F))$ soit vraie (F existe par la remarque ci-dessus). On a $y'\ \varepsilon\ \mu(\overline{w}, F)$ et $z'\ \varepsilon\ \mu(\overline{w}, F)$, donc $y' = z'$ et donc $y \approx z$.

Preuve de (2) : Soient $\overline{w}, y, z$ des objets (de $\mathcal{N}$) et soient $\beta, \gamma \in \widehat{\lambda}$ tels que $\beta \in \gamma$ et que $Z_R(\overline{w}, \beta, y)$ et $Z_R(\overline{w}, \gamma, z)$ soient vraies. Soient $\beta' \approx \beta$ $\gamma' \approx \gamma$, $y \approx y'$ et $z \approx z'$ tels que $\beta'\ \varepsilon\ \widehat{\lambda}$, $\gamma'\ \varepsilon\ \widehat{\lambda}$, $p(\beta', y')\ \varepsilon\ F_{<\lambda}(\overline{w})$ et $p(\gamma', z')\ \varepsilon\ F_{<\lambda}(\overline{w})$: on a alors $\beta'\ \varepsilon\ \gamma'$. (En effet, $\beta' \in \gamma'$, donc il existe $\beta''\ \varepsilon\ \gamma'$ tel que $\beta'' \approx \beta'$. Comme $\beta'\ \varepsilon\ \widehat{\lambda}$ et $\beta''\ \varepsilon\ \widehat{\lambda}$ (car $\widehat{\lambda}$ est transitif), $\beta' = \beta''$, donc $\beta'\ \varepsilon\ \gamma'$.) Soit F tel que $p(\gamma', z')\ \varepsilon\ F_{<\lambda}(\overline{w}) \leftrightarrow z'\ \varepsilon\ \mu(\overline{w}, F)$ et $p(\beta', y')\ \varepsilon\ F_{<\lambda}(\overline{w}) \leftrightarrow p(\beta', y')\ \varepsilon\ F$ soient vraies. D'une part $z'\ \varepsilon\ \mu(\overline{w}, F)$, donc $\mathrm{Maj}^R_\in(\overline{w}, \mathrm{img}(F), z')$ est vraie, et d'autre part $p(\beta', y')\ \varepsilon\ F$, donc $R(\overline{w}, y', z')$ est vraie. Comme $R(\overline{w}, y, z)$ est extensionnelle en y et z, $R(\overline{w}, y, z)$ est vraie.

Preuve de (1) : Soient $\overline{w}$ des objets tels que $\forall c\ (\mathrm{Chaine}^R_\in(\overline{w}, c) \to \exists m\ \mathrm{Maj}^R_\in(\overline{w}, c, m))$ soit vraie et soit $\gamma \in \widehat{\lambda}$. Soit $\gamma'\ \varepsilon\ \widehat{\lambda}$ tel que $\gamma' \approx \gamma$. Soit F tel que les formules suivantes soient vraies :

(i) $\forall \beta\ \forall y'\ (p(\beta, y')\ \varepsilon\ F \to \beta\ \varepsilon\ \gamma')$,

(ii) $\forall z'\ (p(\gamma', z')\ \varepsilon\ F_{<\lambda}(\overline{w}) \leftrightarrow z'\ \varepsilon\ \mu(\overline{w}, F))$,

(iii) $\forall \beta \varepsilon \gamma'\ \forall y'\ (p(\beta, y')\ \varepsilon\ F_{<\lambda}(\overline{w}) \leftrightarrow p(\beta, y')\ \varepsilon\ F)$.

Pour conclure, il suffit maintenant de montrer que $\mathrm{Chaine}^R_\in(\overline{w}, \mathrm{img}(F))$ est vraie, car cela entraînera que $\exists m\ \mathrm{Maj}^R_\in(\overline{w}, c, m)$ est vraie, donc que $\mu(\overline{w}, F)$ est non vide, et donc (d'après (ii)) qu'il existe z' tel que $p(\gamma', z')\ \varepsilon\ F_{<\lambda}(\overline{w})$.

Soient donc $y, z \in \mathrm{img}(F)$ tels que $y \not\approx z$: on va devoir montrer que $R(\overline{w}, y, z)$ ou $R(\overline{w}, z, y)$ est vraie. Soient $y', z'\ \varepsilon\ \mathrm{img}(F)$ tels que $y' \approx y$ et $z' \approx z$. Soient β et δ tels que $p(\beta, y')\ \varepsilon\ F$ et $p(\delta, z')\ \varepsilon\ F$. D'après (i), $\beta\ \varepsilon\ \gamma'$ et $\delta\ \varepsilon\ \gamma'$. D'après (iii), $p(\beta, y')\ \varepsilon\ F_{<\lambda}(\overline{w})$ et $p(\delta, z')\ \varepsilon\ F_{<\lambda}(\overline{w})$, donc $Z_R(\overline{w}, \beta, y)$ et $Z_R(\overline{w}, \delta, z)$ sont vraies. Par conséquent, d'après (3), $\beta \not\approx \delta$. Comme γ' est un ordinal, β et δ sont des ordinaux, et donc on a $\beta \in \delta$ ou $\delta \in \beta$. Dans le premier cas, d'après (2), $R(\overline{w}, y, z)$ est vraie, et dans le second, c'est $R(\overline{w}, z, y)$ qui est vraie. □

5.4 Plongement de $\daleth_2$ dans le monde extensionnel

Une application de la réalisabilité classique, présentée par Krivine [Kri12], consiste à prendre une propriété P dont il n'est pas clair que l'énoncé « il existe un ensemble X qui vérifie P » soit cohérent avec ZF[i] et à construire un modèle de réalisabilité dont l'algèbre de Boole caractéristique $\daleth_2$ vérifie cette propriété P : on obtient ainsi un nouveau résultat de cohérence.

Obstacle de taille à un tel plan : les propriétés que l'on obtient naturellement sur $\daleth_2$ sont des propriétés *non extensionnelles*, alors que celles dont on peut vouloir montrer la cohérence sont des propriétés *extensionnelles*. Il faut donc faire communiquer les deux mondes : pour cela, on va plonger $\daleth_2$ dans le monde extensionnel, c'est-à-dire construire un ensemble X dont les propriétés extensionnelles reflètent dans un certain sens les propriétés non extensionnelles de $\daleth_2$. Le minimum que l'on doit demander, c'est que les $\in$-éléments de X soient en bijection avec les ε-éléments de $\daleth_2$. Krivine a montré comment procéder lorsque l'on dispose de l'instruction « quote », et l'on va montrer que la même technique peut s'appliquer en présence de l'instruction de comparaison χ.

Notons Δ la $\mathcal{M}$-fonctionnelle de $\mathcal{S}_0 \times \mathcal{M}$ dans $\{0,1\}$ telle que pour tout pôle $\perp\!\!\!\perp$ et tout $a \in \mathcal{M}$, $\Delta(\perp\!\!\!\perp, a) = 0$ s'il existe $\alpha < \lambda$ tel que $a = \widehat{\alpha}$ et $\nu^{-1}(\alpha) \Vdash_{\perp\!\!\!\perp} \bot$, et $\Delta(\perp\!\!\!\perp, a) = 1$ sinon.

Du point de vue du modèle de réalisabilité, Δ définit une fonctionnelle à un argument, définie partout et à valeurs dans $\daleth_2$: On va associer à chaque $x \in \daleth_2$ l'ensemble $\{ a \in \widehat{\lambda};\ 0 < \Delta(a) \leq x \} \subseteq \widehat{\lambda}$. On voudrait montrer que si x et y sont deux éléments distincts de $\daleth_2$, les deux ensembles associés ne sont pas extensionnellement équivalents. Puisque $\widehat{\lambda}$ ε-contient exactement un représentant de chacun de ses $\in$-éléments, il suffira de montrer que pour tous $x, y \in \daleth_2$, si $x \neq y$, alors il existe $a \in \widehat{\lambda}$ tel que $\Delta(a) > 0$ et que $x \leq \Delta(a)$ si et seulement si $y \not\leq \Delta(a)$.

Toujours du point de vue du modèle de réalisabilité, si $x = 0$, l'ensemble associé à x est vide. On peut donc commencer par montrer que si $x \neq 0$, alors l'ensemble associé à x n'est pas vide, c'est-à-dire qu'il existe $a \in \widehat{\lambda}$ tel que $0 < \Delta(a) \leq x$:

Lemme 5.14. La formule $\forall x^{\daleth_2}\ (x \neq 0 \to \exists a^{\widehat{\lambda}}\ ((\Delta(a) \neq 0) \wedge (\Delta(a) \leq x)))$ est réalisée modulo $\mathcal{S}_\nu$.

Démonstration. On va montrer que la formule équivalente $\forall x^{\daleth_2}\ (x \neq 0 \to \forall a^{\widehat{\lambda}}\ (\Delta(a) \neq 0 \to (\Delta(a) \wedge \neg x) \neq 0) \to \bot)$ est réalisée par le terme $\Theta = \lambda t.\ \lambda u.\ utt$.

Soient $\perp\!\!\!\perp \in \mathcal{S}_\nu$, $x \in \{0,1\}$, $t \Vdash_{\perp\!\!\!\perp} x \neq 0$, $u \Vdash \forall a^{\widehat{\lambda}}\ (\Delta(a) \neq 0 \to (\Delta(a) \wedge \neg x) \neq 0)$ et $\pi \in \Pi$. Notons $\alpha = \nu(t)$.

Si $t = \nu^{-1}(\alpha) \Vdash_{\perp\!\!\!\perp} \bot$, alors $t \Vdash_{\perp\!\!\!\perp} \Delta(\widehat{\alpha}) \neq 0$. Si $t \nVdash_{\perp\!\!\!\perp} \bot$, alors $[\Delta(\widehat{\alpha})]_{\perp\!\!\!\perp} = 1$, donc $t \Vdash_{\perp\!\!\!\perp} \Delta(\widehat{\alpha}) \neq 0$. Par conséquent, dans tous les cas, $t \Vdash_{\perp\!\!\!\perp} \Delta(\widehat{\alpha}) \neq 0$.

Si $x = 0$, alors $t = \nu^{-1}(\alpha) \Vdash_{\perp\!\!\!\perp} x \neq 0 \equiv \bot$, donc $[\Delta(\widehat{\alpha})]_{\perp\!\!\!\perp} = 0$, et donc $[\Delta(\widehat{\alpha}) \wedge \neg x]_{\perp\!\!\!\perp} = 0$. Si $x = 1$, alors $[\Delta(\widehat{\alpha}) \wedge \neg x]_{\perp\!\!\!\perp} = 0$. Par conséquent, dans tous les cas, $[\Delta(\widehat{\alpha}) \wedge \neg x]_{\perp\!\!\!\perp} = 0$.

Ainsi, comme $u \Vdash_{\perp\!\!\!\perp} \widehat{\alpha} \in \widehat{\lambda} \hookrightarrow \Delta(\widehat{\alpha}) \neq 0 \to (\Delta(\widehat{\alpha}) \wedge \neg x) \neq 0$, $tuu \Vdash_{\perp\!\!\!\perp} \bot$, et donc $\Theta \star u \bullet v \bullet \pi \in \perp\!\!\!\perp$. □

Proposition 5.15. Notons $F(x,p)$ la formule $(x \in \daleth_2) \wedge (p \subsetneq \widehat{\lambda}) \wedge \forall a^{\widehat{\lambda}}\ (a \in p \leftrightarrow ((\Delta(a) \neq 0) \wedge (\Delta(a) \leq x)))$. Les formules suivantes sont réalisées modulo $\mathcal{S}_\nu$:

— $\forall x^{\daleth_2}\ \exists p\ F(x,p)$,

— $\forall x^{\daleth_2}\ \forall p\ (F(x,p) \to p \subsetneq \widehat{\lambda})$,

— $\forall x^{\daleth_2}\ \forall p\ \forall q\ (F(x,p) \to F(x,q) \to p \approx q)$,

— $\forall x^{\daleth_2}\ \forall y^{\daleth_2}\ \forall p\ \forall q\ (F(x,p) \to F(y,q) \to p \approx q \to x = y)$.

En d'autres termes, $F(x,p)$ associe *de façon injective* une partie (au sens extensionnel) de $\widehat{\lambda}$ à chaque élément (au sens non extensionnel) de $\daleth_2$.

i. Par exemple, la propriété « X est un ensemble de parties de $\mathbb{N}$ et X pré-ordonné par relation de subpotence contient une copie de $\mathbb{Q}$ » [Kri12].

Démonstration. Il suffit de montrer que la formule $\forall x^{\daleth_2}\ \forall y^{\daleth_2}\ (x \neq y \to \exists a^{\widehat{\lambda}}\ (\Delta(a) \neq 0 \wedge \neg(\Delta(a) \leq x \leftrightarrow \Delta(a) \leq y)))$ est réalisée.

Comme la formule $\forall x\, \forall y\, (x \neq y \to (((x \wedge \neg y) \neq 0) \vee ((y \wedge \neg x) \neq 0)))$ est vraie dans toute algèbre de Boole, il suffit de montrer que la formule $\forall x^{\daleth_2}\ \forall y^{\daleth_2}\ ((x \wedge \neg y) \neq 0 \to \exists a^{\widehat{\lambda}}\ ((\Delta(a) \neq 0) \wedge (\Delta(a) \leq x) \wedge \neg(\Delta(a) \leq y)))$.

Comme la formule $\forall x\, \forall y\, \forall z\, (z \neq 0 \to z \leq (x \wedge \neg y) \to ((z \leq x) \wedge \neg(z \leq y)))$ est vraie dans toute algèbre de Boole, la formule précédente est réalisée modulo $\mathcal{S}_\nu$ d'après le lemme 5.14. □

5.5 Non-trivialité de $\daleth_2$

On sait d'après Krivine [Kri18, Kri15] que les modèles de réalisabilité où $\daleth_2$ est réduite à l'algèbre de Boole $\{0,1\}$ sont en fait des modèles de forcing, et qu'ils vérifient donc automatiquement l'axiome du choix complet (puisque le modèle de départ le vérifie). Le but de ce chapitre est de montrer que l'on peut réaliser des formes faibles de l'axiome du choix sans être dans cas particulier : il reste donc à montrer que la formule $|\daleth_2| = 2$ n'est pas réalisée modulo $\mathcal{S}_\nu$. On va même faire un peu mieux, en trouvant une structure de réalisabilité $\mathcal{S} \subseteq \mathcal{S}_\nu$ cohérente et telle que la formule $|\daleth_2| > 2$ soit réalisée modulo $\mathcal{S}$.

Fixons deux instructions non protégées δ_0 et δ_1 distinctes de χ. Notons $\succ^1$ la plus petite relation binaire sur $\mathcal{P}_\mathcal{M}(\Lambda \star \Pi)$ contenant $\succ^1_\nu$ et telle que pour toute pile π, $\{\delta_0 \star \pi, \delta_1 \star \pi\} \succ^1 \emptyset$. Notons enfin $\succ$ la plus petite relation d'évaluation contenant $\succ^1$ et $\mathcal{S}$ la structure de réalisabilité engendrée par $\succ$.

Lemme 5.16. La formule $|\daleth_2| > 2$ est réalisée modulo $\mathcal{S}$.

Démonstration. Il suffit de montrer que la formule $\forall x^{\daleth_2}\ (x \neq 0 \to x \neq 1 \to \bot) \to \bot$ est réalisée par $\theta = \lambda t.\ cc\ (\lambda k.\ t\ (k\delta_0)\ (k\delta_1))$.

Soient $\perp\!\!\!\perp \in \mathcal{S}$, $t \Vdash_{\perp\!\!\!\perp} \forall x^{\daleth_2}\ (x \neq 0 \to x \neq 1 \to \bot)$ et $\pi \in \Pi$. Comme $\emptyset \subseteq \perp\!\!\!\perp$, on a $\{\delta_0 \star \pi, \delta_1 \star \pi\} \cap \perp\!\!\!\perp \neq \emptyset$. Soit donc $i \in \{0,1\}$ tel que $\delta_i \star \pi \in \perp\!\!\!\perp$. On a alors $\delta_i \Vdash_{\perp\!\!\!\perp} \bot$, donc $k_\pi\delta_0 \Vdash_{\perp\!\!\!\perp} i \neq 0$ et $k_\pi\delta_1 \Vdash_{\perp\!\!\!\perp} i \neq 1$. Par conséquent, $t\ (k_\pi\delta_0)\ (k_\pi\delta_1) \Vdash_{\perp\!\!\!\perp} \bot$, et $\theta \star t \cdot \pi \in \perp\!\!\!\perp$. □

Il reste à montrer que la structure $\mathcal{S}$ est cohérente.

Pour tout $i \in \{0,1\}$, posons d'une part pour tout $n \in \mathbb{N}$, $\perp\!\!\!\perp^i_n = \{\ p \in \Lambda \star \Pi;$ il existe $m < n$ et $Q \in \mathcal{P}_\mathcal{M}(\perp\!\!\!\perp^i_m)$ tels que $\{p\} \succ^1_\nu Q\ \} \cup \{\ \delta_i \star \pi;\ \pi \in \Pi\ \}$, et d'autre part $\perp\!\!\!\perp^i = \bigcup_{n\in\mathbb{N}} \perp\!\!\!\perp^i_n$.

Lemme 5.17. On a $\perp\!\!\!\perp^0 \in \mathcal{S}$ et $\perp\!\!\!\perp^1 \in \mathcal{S}$.

Lemme 5.18. Pour tout $p \in \Lambda \star \Pi$, $p \notin \perp\!\!\!\perp^0$ ou $p \notin \perp\!\!\!\perp^1$.

Démonstration. Soit $p \in \perp\!\!\!\perp^0$. Soit n le plus petit entier tel que $p \in \perp\!\!\!\perp^i_n$. On peut vérifier qu'il existe une pile π telle que $\{p\} \succ_\nu \{\delta_0 \star \pi\}$ (en n étapes).

Par ailleurs, d'une part $\succ_\nu$ est déterministe (c'est-à-dire que pour tous $q, r, s \in \Lambda \star \Pi$, si $\{q\} \succ^1_\nu \{r\}$ et $\{q\} \succ^1_\nu \{s\}$, alors $q = s$), et d'autre part $\succ_\nu$ n'a pas de règle d'évaluation lorsque δ_0 ou δ_1 arrive en tête (c'est-à-dire que pour toute pile π' et tout Q, $\{\delta_i \star \pi'\} \not\succ^1_\nu Q$). Par conséquent, pour toute pile π', $\{p\} \not\succ_\nu \{\delta_1 \star \pi'\}$, et donc $p \notin \perp\!\!\!\perp^1$. □

Corollaire. La structure de réalisabilité $\mathcal{S}$ est cohérente.

Proposition 5.19. La formule $|\daleth_2| \leq 2$ n'est pas réalisée modulo $\mathcal{S}_\nu$

Démonstration. Si elle l'était, elle serait également réalisée modulo $\mathcal{S}$, et donc $\mathcal{S}$ ne serait pas cohérente. □

6 Un peu de combinatoire infinie : la condition d'antichaîne

Au chapitre précédent, on a montré comment obtenir des modèles de réalisabilité qui vérifient une version du lemme de Zorn restreinte à un certain « ordinal générique » $\widehat{\lambda}$. On voudrait pouvoir utiliser cette technique avec des λ de plus en plus grands pour réaliser des approximations de plus en plus puissantes du lemme de Zorn, et peut-être un jour finalement réaliser le lemme de Zorn lui-même (en prenant pour λ la classe des ordinaux de $\mathcal{M}$, et, comme indiqué plus haut, à condition d'adapter la théorie au cas où Λ est une $\mathcal{M}$-classe propre). Pour cela, il faudrait faire en sorte que le cardinal de $\widehat{\lambda}$ (du point de vue du modèle de réalisabilité) croisse « au moins aussi vite » que le $\mathcal{M}$-cardinal λ. Dans ce chapitre, on va faire un premier pas dans cette direction, en modifiant la structure de réalisabilité pour faire en sorte que si $\mathcal{M}$ vérifie $\lambda \geq \aleph_1$, alors le modèle de réalisabilité vérifie $\widehat{\lambda} \geq \aleph_1$. Pour cela, il suffit de faire en sorte que $\widehat{\lambda}$ soit un cardinal, car on peut montrer que si $\mathcal{M}$ vérifie $\lambda \geq \aleph_1$, alors le modèle de réalisabilité vérifie $\widehat{\lambda} > \omega$.

On fixe comme au chapitre précédent une $\mathcal{M}$-bijection $\nu : \Lambda \to \lambda$ et une instruction non protégée χ. Par ailleurs, on fixe deux autres instructions non protégées φ et η ainsi qu'une $\mathcal{M}$-famille $(\gamma_\alpha)_{\alpha<\lambda}$ d'instructions non protégées deux à deux distinctes qui ne contient ni χ, ni φ, ni η.

L'instruction η va jouer le rôle de la condition d'antichaîne dénombrable[i] qui intervient notamment dans construction par forcing d'un modèle de ZF ne satisfaisant pas l'hypothèse du continu. En réalité, elle correspond plutôt à une sorte de « condition d'antichaîne finie »(« toute antichaîne est finie »), qui n'aurait pas trop d'intérêt en forcing, mais ne pose aucun problème ici. Là où la condition d'antichaîne dénombrable sert à montrer que les cardinaux sont préservés, l'instruction η permettra ici de montrer que $\widehat{\lambda}$ n'est en bijection avec aucun de ses éléments (autrement-dit, que c'est un cardinal).

L'instruction φ joue le rôle d'une sorte d'instruction de (λ, κ)-vote pour tout $\kappa < \lambda$; elle sera nécessaire pour tirer parti de l'instruction η. Les instructions γ_α sont inertes et servent simplement à exprimer φ.

On note $\succ^1$ la plus petite relation binaire sur $\mathcal{P}_\mathcal{M}(\Lambda \star \Pi)$ telle que

— Pour tous p, q tels que $p \succ^1_{\mathrm{K}} q$, $\{p\} \succ^1 \{q\}$,

— Pour tous termes a, b, t, u, v et toute pile π :

  — Si $\nu(a) < \nu(b)$, $\{\chi \star a \cdot b \cdot t \cdot u \cdot v \cdot \pi\} \succ^1 \{t \cdot \pi\}$,

  — Si $\nu(a) = \nu(b)$, $\{\chi \star a \cdot b \cdot t \cdot u \cdot v \cdot \pi\} \succ^1 \{u \cdot \pi\}$,

  — Si $\nu(a) > \nu(b)$, $\{\chi \star a \cdot b \cdot t \cdot u \cdot v \cdot \pi\} \succ^1 \{v \cdot \pi\}$,

— Pour tout terme t, toute pile π et tout $U \in \mathcal{P}_\mathcal{M}(\lambda)$ tel que le $\mathcal{M}$-cardinal de $\lambda \setminus U$ soit strictement plus petit que λ :

$$\{\, \varphi \star t \cdot \pi \,\} \succ^1 \{\, t \star \gamma_\alpha \cdot \pi ;\ \alpha \in U \,\},$$

— Pour tout terme t, toute pile π et tout $A \in \mathcal{P}_\mathcal{M}(\Lambda)$ infinie :

$$\{\, \eta \star t \cdot a \cdot \pi ;\ a \in A \,\} \succ^1 \{\, t \star a \cdot b \cdot \pi ;\ a, b \in A, a \neq b \,\}.$$

De plus, on note $\succ$ la plus petite relation de multi-évaluation complète contenant $\succ^1$ et $\mathcal{S}$ la structure de réalisabilité engendrée par $\succ$.

Comme $\succ^1 \supseteq \succ^1_\nu$, on a $\mathrm{Th}(\mathcal{S}) \supseteq \mathrm{Th}(\mathcal{S}_\nu)$. En particulier, pour $\mathrm{Th}(\mathcal{S})$, $\widehat{\lambda}$ est un ordinal au sens non extensionnel, et $\mathrm{Th}(\mathcal{S})$ contient un schéma de Zorn restreint à $\widehat{\lambda}$.

Par ailleurs, le pôle vide est dans $\mathcal{S}_{\succ^1} = \mathcal{S}$, donc la structure $\mathcal{S}$ est cohérente.

On veut montrer qu'il n'existe aucune surjection *au sens extensionnel* d'un $\in$-élément de $\widehat{\lambda}$ dans $\widehat{\lambda}$. Cependant, puisque $\widehat{\lambda}$ est un ordinal au sens non extensionnel, il suffit de montrer qu'il n'existe aucune surjection *au sens non extensionnel* d'un ε-élément de $\widehat{\lambda}$ dans $\widehat{\lambda}$.

Pour toute formule $F(\overline{w}, x, y)$, on note $\mathrm{Fun}_F(\overline{w})$ la formule $\forall x\ \forall y\ \forall y'\ (F(\overline{w}, x, y) \to F(\overline{w}, x, y') \to y \neq y' \to \bot)$, qui dit que la relation binaire définie par F avec les paramètres $\overline{w}$ est fonctionnelle. De plus, on

i. On s'éloignera ici de la terminologie historique de *condition de chaîne dénombrable*, car celle-ci est trompeuse.

note $\mathrm{Surj}_F(\overline{w}, a, b)$ la formule $\forall y\ (\forall x\ (F(\overline{w}, x, y) \to x \not\in a) \to y \not\in b)$, qui dit que cette relation binaire est surjective de a dans b.

On doit alors montrer le résultat suivant :

Proposition 6.1. Pour toute formule $F(\overline{w}, x, y)$, la formule $\forall a^{\widehat{\lambda}}\ (\mathrm{Fun}_F(\overline{w}) \to \mathrm{Surj}_F(\overline{w}, a, \widehat{\lambda}) \to \bot)$ est réalisée modulo $\mathcal{S}$.

Démonstration. On pose :

— $\Theta_2 = k\ (\eta\ f\ z\ (\lambda r.\ r))$,

— $\Theta_1 = \lambda z.\ k\ (f\ z\ z\ \Theta_2)$,

— $\Theta_0 = \lambda a.\ \lambda f.\ \lambda s.\ \varphi\ (\lambda b.\ cc\ (\lambda k.\ s\ \Theta_1\ b))$.

On va montrer que la formule $\forall a^{\widehat{\lambda}}\ (\mathrm{Fun}_F(\overline{w}) \to \mathrm{Surj}_F(\overline{w}, a, \widehat{\lambda}) \to \bot)$ est réalisée modulo $\mathcal{S}$ par Θ_0.

Pour alléger les notations, on va supposer que la liste $\overline{w}$ est vide (la preuve est presque identique dans le cas général).

Soient $\perp\!\!\!\perp \in \mathcal{S}$, $\kappa < \lambda$, $t \in |\mathrm{Fun}_F|_{\perp\!\!\!\perp}$, $u \in \left|\mathrm{Surj}_F(\widehat{\kappa}, \widehat{\lambda})\right|_{\perp\!\!\!\perp}$ et $\pi \in \Pi$, et supposons par l'absurde que $\Theta_0 \star \nu^{-1}(\kappa) \cdot t \cdot u \cdot \pi \notin \perp\!\!\!\perp$.

Posons $v = \lambda b.\ cc\ (\lambda k.\ u\ \Theta_1[f := t, s := u]\ b)$. Pour alléger les notations, on notera désormais Θ_1 pour $\Theta_1[f := t, s := u, k := k_\pi]$ et Θ_2 pour $\Theta_2[f := t, s := u, k := k_\pi]$.

Posons $U = \{\ \alpha < \lambda;\ v \star \gamma_\alpha \cdot \pi \in \perp\!\!\!\perp\ \}$. On a $\varphi \star v \cdot \pi \notin \perp\!\!\!\perp$, et par conséquent, par définition de $\succ$, le $\mathcal{M}$-cardinal de $\lambda \setminus U$ est λ. Posons donc $B = \{\ \nu(\gamma_\alpha);\ \alpha \in \lambda \setminus U\ \}$: c'est un $\mathcal{M}$-sous-ensemble de λ qui est de $\mathcal{M}$-cardinal λ.

Pour tout $\beta \in B$, $v \star \nu^{-1}(\beta) \cdot \pi \notin \perp\!\!\!\perp$, donc $u \star \Theta_1 \cdot \nu^{-1}(\beta) \cdot \pi \notin \perp\!\!\!\perp$. On sait que $u \in \left|\forall x\ (F(x, \widehat{\beta}) \to x \not\in \widehat{\kappa}) \to \widehat{\beta} \not\in \widehat{\lambda}\right|_{\perp\!\!\!\perp}$ et $\nu^{-1}(\beta) \cdot \pi \in \left\|\widehat{\beta} \not\in \widehat{\lambda}\right\|_{\perp\!\!\!\perp}$, et donc on doit avoir $\Theta_1 \notin \left|\forall x\ (F(x, \widehat{\beta}) \to x \not\in \widehat{\kappa})\right|_{\perp\!\!\!\perp}$. Par conséquent, il existe $\alpha_\beta < \kappa$, $\zeta_\beta \in \left|F(\widehat{\alpha_\beta}, \widehat{\beta})\right|_{\perp\!\!\!\perp}$ et $\pi'_\beta \in \Pi$ tels que $\Theta_1 \star \zeta_\beta \cdot \nu^{-1}(\alpha_\beta) \cdot \pi'_\beta \notin \perp\!\!\!\perp$. En posant $\Theta_{2,\beta} = \Theta_2[z := \zeta_\beta]$, on a donc $t \star \zeta_\beta \cdot \zeta_\beta \cdot \Theta_{2,\beta} \cdot \pi \notin \perp\!\!\!\perp$.

L'ensemble $Z = \{\ \zeta_\beta;\ \beta \in B\ \}$ est de $\mathcal{M}$-cardinal λ. En effet, par l'absurde, supposons le contraire. Pour tout $\zeta \in Z$, notons $B_\zeta = \{\ \beta \in B;\ \zeta_\beta = \zeta\ \}$. Puisque B est de $\mathcal{M}$-cardinal λ, que $\kappa < \lambda$ et que $B = \bigcup_{\zeta \in Z} B_\zeta$, Z doit contenir un ζ tel que B_ζ soit de $\mathcal{M}$-cardinal strictement plus grand que celui de κ. Pour tout $\beta \in B_\zeta$, on a $\zeta \in \left|F(\widehat{\alpha_\beta}, \widehat{\beta})\right|_{\perp\!\!\!\perp}$, et pour tous $\beta, \beta' \in B_\zeta$ tels que $\beta \neq \beta'$, on a $t \star \zeta \cdot \zeta \cdot \Theta_2[z := \zeta] \cdot \pi \notin \perp\!\!\!\perp$, par conséquent, $\alpha_\beta \neq \alpha'_\beta$. Ainsi, le $\mathcal{M}$-ensemble $\{\ (\beta, \alpha_\beta);\ \beta \in B_\zeta\ \}$ définit une injection de B_ζ dans κ, ce qui est impossible.

Puisque Z est de $\mathcal{M}$-cardinal λ, il existe $B_0 \in \mathcal{P}_\mathcal{M}(B)$ de $\mathcal{M}$-cardinal λ tel que que pour tous $\beta, \beta' \in B_0$, si $\beta \neq \beta'$, alors $\zeta_\beta \neq \zeta_{\beta'}$.

Pour tout $\beta \in B_0$, on a $t \star \zeta_\beta \cdot \zeta_\beta \cdot \Theta_{2,\beta} \cdot \pi \notin \perp\!\!\!\perp$, $t \in \left|F(\widehat{\alpha_\beta}, \widehat{\beta}) \to F(\widehat{\alpha_\beta}, \widehat{\beta}) \to \widehat{\beta} \neq \widehat{\beta} \to \bot\right|_{\perp\!\!\!\perp}$ et $\zeta_\beta \in \left|F(\widehat{\alpha_\beta}, \widehat{\beta})\right|_{\perp\!\!\!\perp}$. Par conséquent, $\Theta_{2,\beta} \notin \left|\widehat{\beta} \neq \widehat{\beta}\right|_{\perp\!\!\!\perp} = |\bot|_{\perp\!\!\!\perp}$. Il existe donc une pile π''_β telle que $\Theta_{2,\beta} \star \pi''_\beta \notin \perp\!\!\!\perp$, et donc $\eta \star t \cdot \zeta_\beta \cdot (\lambda r.\ r) \cdot \pi \notin \perp\!\!\!\perp$

Pour tout $B_1 \in \mathcal{P}_\mathcal{M}(B_0)$ infini, le $\mathcal{M}$-ensemble $\{\ \zeta_\beta;\ \beta \in B_1\ \}$ est également infini, et donc par par définition de $\succ$, il existe $\beta, \beta' \in B_1$ tels que $\zeta_\beta \neq \zeta_{\beta'}$ (donc $\beta \neq \beta'$) et $t \star \eta_\beta \cdot \eta_{\beta'} \cdot (\lambda r.\ r) \cdot \pi \notin \perp\!\!\!\perp$. Comme $t \in \left|F(\widehat{\alpha}, \widehat{\beta}) \to F(\widehat{\alpha}, \widehat{\beta'}) \to \widehat{\beta} \neq \widehat{\beta'} \to \bot\right|_{\perp\!\!\!\perp}$ pour tout $\alpha < \lambda$ et que $\widehat{\beta} \neq \widehat{\beta'} \equiv_{\perp\!\!\!\perp} \top$, on ne peut pas avoir $\alpha_\beta = \alpha_{\beta'}$.

En d'autres termes,, si l'on considère que (α, β) et (α', β') sont incompatibles si $\alpha = \alpha'$ et $\beta \neq \beta'$, l'ensemble $\{\ (\alpha_\beta, \beta);\ \beta \in B_0\ \}$ n'a pas d'antichaîne infinie.

Par conséquent, pour tout $\alpha < \kappa$, le $\mathcal{M}$-ensemble $Y_\alpha = \{\ \beta \in B_0;\ \alpha = \alpha_\beta\ \}$ est fini, ce qui est impossible car $B_0 = \bigcup_{\alpha < \kappa} Y_\alpha$ est de $\mathcal{M}$-cardinal $\lambda > \kappa$. □

Pour aller plus loin, il faudrait faire en sorte que pour tous cardinaux $\mu < \kappa \leq \lambda$, il n'y ait pas de surjection de $\widehat{\mu}$ dans $\widehat{\kappa}$ (en tant que cardinaux du modèle de réalisabilité). Une idée pourrait être de créer pour chaque $\mathcal{M}$-cardinal $\kappa \leq \lambda$ une instruction φ_κ qui soit à $\widehat{\kappa}$ ce que φ est à $\widehat{\lambda}$. Il faudrait également s'assurer que l'on a pas fabriqué en cours de route des réalisateurs de $|\beth 2| = 2$ (ce qui n'est déjà même pas clair pour la structure $\mathcal{S}$ utilisée dans le présent chapitre).

A Annexe : Algèbres de Boole – Quelques outils

On va présenter quelques outils pour manipuler les algèbres de Boole.

A.1 Le langage des algèbres de Boole

Définition A.1. On prend le même $\mathcal{M}$-ensemble de variables du premier ordre que pour le langage de réalisabilité. Le *langage des algèbres de Boole* est le $\mathcal{M}$-ensemble défini par la grammaire suivante, quotienté par la relation d'α-équivalence :

Termes : $a, b \quad ::= \quad x \mid 0 \mid 1 \mid a \wedge b \mid a \vee b \mid \neg a$

Formules : $A, B \quad ::= \quad \top \mid \bot \mid a \neq b \mid A \to B \mid \forall x\ A$

On définit les connecteurs logiques et les symboles de relation manquants de la manière suivante :

— on note $A \wedge B$ pour $(A \to B \to \bot) \to \bot$,

— on note $A \vee B$ pour $(A \to \bot) \to (B \to \bot) \to \bot$,

— on note $\neg A$ pour $A \to \bot$,

— on note $A \leftrightarrow B$ pour $(A \to B) \wedge (B \to A)$,

— on note $\exists x\ A$ pour $\neg(\forall x\ \neg A)$,

— on note $a = b$ pour $\neg(a \neq b)$,

— on note $a \leq b$ pour $(a \wedge b) = a$.

Dans tout ce chapitre, terme signifiera « terme du langage des algèbres de Boole » et formule signifiera « formule du langage des algèbres de Boole ».

Notons que l'on utilise les mêmes notations $\wedge$, $\vee$ et $\neg$ pour les opérations des algèbres de Boole et pour les connecteurs logiques. En pratique, il ne devrait pas y avoir de confusion.

Remarque. Toute formule $A(\overline{x})$ du langage des algèbres de Boole peut se lire de manière unique (à renommage des variables $\overline{y}_0, \ldots, \overline{y}_m$ près) comme $\forall \overline{y}_0\ (B_0 \to \ldots \to \forall \overline{y}_{m-1}\ (B_{m-1} \to \forall \overline{y}_m\ b \neq b') \ldots)$, avec éventuellement $m = 0$. De plus, on peut faire en sorte que les variables $\overline{x}, \overline{y}_0, \ldots, \overline{y}_m$ soient distinctes.

Définition A.2. Une *structure sur le langage des algèbres de Boole* est un 6-uplet $(\mathbb{B}, 0^{\mathbb{B}}, 1^{\mathbb{B}}, \vee^{\mathbb{B}}, \wedge^{\mathbb{B}}, \neg^{\mathbb{B}})$ où :

— $\mathbb{B}$ est un $\mathcal{M}$-ensemble non vide ;

— $0^{\mathbb{B}}$ et $1^{\mathbb{B}}$ sont des éléments de $\mathbb{B}$;

— $\vee^{\mathbb{B}}$ et $\wedge^{\mathbb{B}}$ sont des $\mathcal{M}$-fonctions de $\mathbb{B}^2$ dans $\mathbb{B}$;

— $\neg^{\mathbb{B}}$ est une $\mathcal{M}$-fonction de $\mathbb{B}$ dans $\mathbb{B}$.

Définition A.3. Soient $(\mathbb{B}, 0^{\mathbb{B}}, 1^{\mathbb{B}}, \vee^{\mathbb{B}}, \wedge^{\mathbb{B}}, \neg^{\mathbb{B}})$ une structure sur le langage des algèbres de Boole.

— Pour toute terme $a(\overline{x})$ du langage des algèbres de Boole et tous $\overline{b} \in \mathbb{B}$, en suivant la définition habituelle des modèles de Tarski, on associe à $a(\overline{x})$ et $\overline{b}$ une *valeur dans* $\mathbb{B}$, notée $a^{\mathbb{B}}(\overline{b})$, qui est un élément de $\mathbb{B}$.

— Pour toute formule $A(\overline{x})$ du langage des algèbres de Boole et tous $\overline{b} \in \mathbb{B}$, en suivant la définition habituelle des modèles de Tarski, on associe à $A(\overline{x})$ et $\overline{b}$ une *valeur de vérité dans* $\mathbb{B}$, notée $\left|A(\overline{b})\right|_{\mathbb{B}}$, qui vaut 0 ou 1.
On dit que $\mathbb{B}$ *vérifie* $A(\overline{b})$, et l'on note $\mathbb{B} \models A(\overline{b})$, lorsque $\left|A(\overline{b})\right|_{\mathbb{B}} = 1$.

De plus, pour toute liste de termes $\overline{a}^m(\overline{x}^n)$ du langage des algèbres de Boole, on appelle *interprétation de* $\overline{a}^m(\overline{x}^n)$ *dans* $\mathbb{B}$ la fonction de $\mathbb{B}^n$ dans $\mathbb{B}^m$ qui $\overline{b}^n$ associe $\overline{a}^{\mathbb{B}}(\overline{b}) = (a_1^{\mathbb{B}}(\overline{b}), \ldots, a_m^{\mathbb{B}}(\overline{b}))$.

Définition A.4. Soient $(\mathbb{B}, 0^{\mathbb{B}}, 1^{\mathbb{B}}, \vee^{\mathbb{B}}, \wedge^{\mathbb{B}}, \neg^{\mathbb{B}})$ une structure sur le langage des algèbres de Boole et Φ un $\mathcal{M}$-ensemble de formules closes du langage des algèbres de Boole. On dit que $\mathbb{B}$ vérifie Φ, et l'on note $\mathbb{B} \models \Phi$, si $\mathbb{B} \models A$ pour toute $A \in \Phi$.

Définition A.5. Une *algèbre de Boole* est une structure sur le langage des algèbres de Boole qui vérifie les formules suivantes :

$\forall x, y, z\ (x \wedge y) \wedge z = x \wedge (y \wedge z)$	$\forall x, y, z\ (x \vee y) \vee z = x \vee (y \vee z)$	(associativité)
$\forall x, y\ x \wedge y = y \wedge x$	$\forall x, y\ x \vee y = y \vee x$	(commutativité)
$\forall x\ x \wedge x = x$	$\forall x\ x \vee x = x$	(idempotence)
$\forall x\ 1 \wedge x = x$	$\forall x\ 0 \vee x = x$	(éléments neutres)
$\forall x\ 0 \wedge x = 0$	$\forall x\ 1 \vee x = 1$	(éléments absorbants)
$\forall x, y, z\ x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$		
$\forall x, y, z\ x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$		(distributivité)
$\forall x\ x \wedge \neg x = 0$	$\forall x\ x \vee \neg x = 1$	(complément)
$\forall x\ \neg\neg x = x$		(involutivité du complément)
$\forall x, y\ \neg(x \wedge y) = \neg x \vee \neg y$	$\forall x, y\ \neg(x \vee y) = \neg x \wedge \neg y$	(lois de De Morgan)

On appelle ces formules les *axiomes des algèbres de Boole*.

Exemple. La structure $(\{0,1\}, 0, 1, \vee, \wedge, \neg)$ est une algèbre de Boole.

On identifiera parfois un terme du langage des algèbres de Boole avec son interprétation dans $\{0,1\}$.

Définition A.6. Soit Φ une formule close ou un $\mathcal{M}$-ensemble de formules closes du langage des algèbres de Boole. S'il existe une algèbre de Boole $\mathbb{B}$ *à au moins deux éléments* telle que $\mathbb{B} \models \Phi$, on dit que Φ est *cohérent(e)* . Sinon, on dit que Φ est *contradictoire* .

Définition A.7. Soient Φ et Ψ deux formules closes ou $\mathcal{M}$-ensembles de formules closes du langage des algèbres de Boole. On dit que Ψ est *conséquence logique* de Φ et l'on note $\Phi \models \Psi$ si toute algèbre de Boole *à au moins deux éléments* qui vérifie Φ vérifie Ψ.

Définition A.8. Soient Φ et Ψ deux formules closes ou $\mathcal{M}$-ensembles de formules closes du langage des algèbres de Boole. On dit que Ψ est *équivalent(e)* à Φ et l'on note $\Psi \dashv\models \Phi$ si $\Psi \models \varphi$ et $\Phi \models \Psi$.

Définition A.9. On appelle *extension de la théorie des algèbres de Boole à au moins deux éléments* tout $\mathcal{M}$-ensemble Φ de formules closes du langage des algèbres de Boole tel que pour toute formule close A du langage des algèbres de Boole, si $\Phi \models A$ alors $A \in \Phi$.

A.2 Termes sur mesure

La théorie des algèbres de Boole à au moins deux éléments décide toutes les équations. C'est un fait bien connu [GH08, chapitre 15, théorème 9] dont on va redonner une démonstration par souci de complétude, avant d'en tirer un résultat similaire sur les formules de Horn :

Proposition A.10 (Équations)**.** Soient $a(\overline{x})$ et $a'(\overline{x})$ deux termes du langage des algèbres de Boole. Si la formule $\forall \overline{x}\ a = a'$ est vraie dans l'algèbre de Boole $\{0,1\}$, alors elle est vraie dans toute algèbre de Boole.

Corollaire. Soient $\overline{a}^n(\overline{x}^p), \overline{a'}^n(\overline{x}^p)$ (respectivement, $\overline{a}^n(\overline{x}^p), \overline{a'}^n(\overline{x}^p), b(\overline{x}^p), b'(\overline{x}^p)$) des termes du langage des algèbres de Boole. Si la formule $\forall \overline{x}\ (a_1 \neq a'_1 \vee \ldots \vee a_n \neq a'_n)$ (respectivement, $\forall \overline{x}\ (a_1 \neq a'_1 \vee \ldots \vee a_n \neq a'_n \vee b = b')$) est vraie dans l'algèbre de Boole $\{0,1\}$, alors elle est vraie dans toute algèbre de Boole à au moins deux éléments.

Corollaire (Clauses de Horn)**.** Soient $\overline{a}^n(\overline{x}^p), \overline{a'}^n(\overline{x}^p), b(\overline{x}^p), b'(\overline{x}^p)$ des termes du langage des algèbres de Boole. Pour toute algèbre de Boole $\mathbb{B}$ à au moins deux éléments, la formule $\forall \overline{x}\ (a_1 = a'_1 \to \ldots a_n = a'_n \to b \neq b')$ (respectivement, la formule $\forall \overline{x}\ (a_1 = a'_1 \to \ldots \to a_n = a'_n \to b = b')$) est vraie dans $\mathbb{B}$ si et seulement si elle est vraie dans $\{0,1\}$.

Démonstration de la proposition. Pour tout terme $a(\overline{x})$ du langage des algèbres de Boole, posons :

$$\widetilde{a}(\overline{x}) = \bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } a^{\{0,1\}}(\overline{b})=1}} \bigwedge_{i=1,\ldots n} x_i^{b_i},$$

où $x_i^{b_i}$ désigne le terme x_i si $b_i = 1$, et le terme $\neg x_i$ sinon.

Fixons une algèbre de Boole $(\mathbb{B}, 0, 1, \vee, \wedge, \neg)$. Le terme $\widetilde{a}$ ne dépend que des valeurs de $a^{\{0,1\}}(\overline{b})$ pour $\overline{b} \in \{0,1\}^n$, par conséquent, pour démontrer la proposition, il suffit de montrer que pour tout terme a, pour tout $\overline{c} \in \mathbb{B}^n$, $a^{\mathbb{B}}(\overline{c}) = \widetilde{a}^{\,\mathbb{B}}(\overline{c})$, ce que l'on va faire par induction sur a :

— Si a est le terme 0, $\widetilde{a}^{\,\mathbb{B}}(\overline{c}) = \bigvee_{\overline{b}\in\emptyset} \bigwedge_{i=1,\ldots n} c_i^{b_i} = 0$.

— Si a est le terme 1, $\widetilde{a}^{\,\mathbb{B}}(\overline{c}) = \bigvee_{\overline{b}\in\{0,1\}^n} \bigwedge_{i=1,\ldots n} c_i^{b_i} = \bigwedge_{i=1,\ldots n}(c_i \vee \neg c_i) = 1$
(par distributivité de $\wedge$ sur $\vee$).

— Pour si a est le terme x_k, $\begin{aligned}\widetilde{a}^{\,\mathbb{B}}(\overline{c}) &= \bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } b_k=1}} \bigwedge_{i=1,\ldots n} c_i^{b_i} \\ &= c_k \wedge \bigwedge_{i\neq k}(c_i \vee \neg c_i) \text{ (par distributivité de } \wedge \text{ sur } \vee) \\ &= c_k.\end{aligned}$

— Si a est le terme $\neg t$, on a d'une part :

$$\begin{aligned}&\widetilde{a}^{\,\mathbb{B}}(\overline{c}) \vee \widetilde{t}^{\,\mathbb{B}}(\overline{c}) \\ =\ & \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{c})=0}} \bigwedge_{i=1,\ldots n} c_i^{b_i}\right) \vee \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{c})=1}} \bigwedge_{i=1,\ldots n} c_i^{b_i}\right) \\ =\ & \bigvee_{\overline{b}\in\{0,1\}^n} \bigwedge_{i=1,\ldots n} c_i^{b_i} \\ =\ & 1,\end{aligned}$$

et d'autre part :

$$\begin{aligned}&\widetilde{a}^{\,\mathbb{B}}(\overline{c}) \wedge \widetilde{t}^{\,\mathbb{B}}(\overline{c}) \\ =\ & \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{b})=0}} \bigwedge_{i=1,\ldots n} c_i^{b_i}\right) \wedge \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{b})=1}} \bigwedge_{i=1,\ldots n} c_i^{b_i}\right) \\ =\ & \bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{b})=0}} \ \bigvee_{\substack{\overline{b'}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{b'})=1}} \left(\bigwedge_{i=1,\ldots n} c_i^{b_i}\right) \wedge \left(\bigwedge_{i=1,\ldots n} c_i^{b'_i}\right)\end{aligned}$$

(par distributivité de $\wedge$ sur $\vee$)

$= 0$

(car, si $t^{\mathbb{B}}(\overline{b}) = 0$ et $t^{\mathbb{B}}(\overline{b'}) = 1$, il existe i tel que $b_i \neq b'_i$, et donc $c_i^{b_i} \wedge c_i^{b'_i} = 0$),

par conséquent, $\widetilde{a}^{\,\mathbb{B}}(\overline{c}) = \neg\widetilde{t}^{\,\mathbb{B}}(\overline{c}) = \neg t^{\mathbb{B}}(\overline{c}) = a^{\mathbb{B}}(\overline{c})$.

— Si a est le terme $t \vee u$:

$$\begin{aligned}
& \widetilde{a}^{\mathbb{B}}(\overline{c}) \\
= & \bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{c})=1 \\ \text{ou } u^{\mathbb{B}}(\overline{c})=1}} \bigwedge_{i=1,\dots n} c_i^{b_i} \\
= & \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{c})=0}} \bigwedge_{i=1,\dots n} c_i^{b_i}\right) \vee \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } u^{\mathbb{B}}(\overline{c})=1}} \bigwedge_{i=1,\dots n} c_i^{b_i}\right) \\
= & \widetilde{t}^{\,\mathbb{B}}(\overline{c}) \vee \widetilde{u}^{\,\mathbb{B}}(\overline{c}) \\
= & t^{\mathbb{B}}(\overline{c}) \vee u^{\mathbb{B}}(\overline{c}).
\end{aligned}$$

— Si a est le terme $t \wedge u$:

$$\begin{aligned}
& t^{\mathbb{B}}(\overline{c}) \wedge u^{\mathbb{B}}(\overline{c}) \\
= & \widetilde{t}^{\,\mathbb{B}}(\overline{c}) \wedge \widetilde{u}^{\,\mathbb{B}}(\overline{c}) \\
= & \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{c})=0}} \bigwedge_{i=1,\dots n} c_i^{b_i}\right) \wedge \left(\bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } u^{\mathbb{B}}(\overline{c})=1}} \bigwedge_{i=1,\dots n} c_i^{b_i}\right) \\
= & \bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{b})=1}} \bigvee_{\substack{\overline{b'}\in\{0,1\}^n \\ \text{tel que } u^{\mathbb{B}}(\overline{b'})=1}} \left(\bigwedge_{i=1,\dots n} c_i^{b_i}\right) \wedge \left(\bigwedge_{i=1,\dots n} c_i^{b'_i}\right) \\
= & \bigvee_{\substack{\overline{b}\in\{0,1\}^n \\ \text{tel que } t^{\mathbb{B}}(\overline{b})=1 \\ \text{et } u^{\mathbb{B}}(\overline{b})=1}} \bigwedge_{i=1,\dots n} c_i^{b_i} \\
& \text{(car, si } \overline{b} \neq \overline{b'}\text{, il existe } i \text{ tel que } b_i \neq b'_i\text{, et donc } c_i^{b_i} \wedge c_i^{b'_i} = 0) \\
= & \widetilde{a}^{\mathbb{B}}(\overline{c}).
\end{aligned}$$

□

Démonstration du premier corollaire. 1. Supposons que $\{0,1\} \models \forall \overline{x}\ (a_1 \neq a'_1 \vee \ldots \vee a_n \neq a'_n)$, et pour tous termes b et b' du langage des algèbres de Boole, notons $b \veebar b'$ pour $(b \vee b') \wedge (\neg b \vee \neg b')$ (opération *ou exclusif*). La formule $\forall \overline{x}\ \left(\bigvee_{i=1,\dots,n}(a_i \veebar a'_i)\right) = 1$ est vraie dans $\{0,1\}$ donc par la proposition précédente, elle est vraie dans toute algèbre de Boole.

De plus, la formule $\forall \overline{x}\ (a_1 = a'_1 \to \ldots \to a_n = a'_n \to \left(\bigvee_{i=1,\dots,n}(a_i \veebar a'_i)\right) = 0)$ est vraie dans toute algèbre de Boole, donc en particulier la formule $\forall \overline{x}\ (\left(\bigvee_{i=1,\dots,n}(a_i \veebar a'_i)\right) = 1 \to (a_1 \neq a'_1 \vee \ldots \vee a_n \neq a'_n))$ est vraie dans toute algèbre de Boole à au moins deux éléments, ce qui montre le résultat.

2. Supposons que $\{0,1\} \models \forall \overline{x}\ (a_1 \neq a'_1 \vee \ldots \vee a_n \neq a'_n \vee b = b')$. La formule $\forall \overline{x}\ \left(\bigvee_{i=1,\dots,n}(a_i \veebar a'_i)\right) \vee \neg(b \veebar b') = 1$ est vraie dans $\{0,1\}$ donc par la proposition précédente, elle est vraie dans toute algèbre de Boole.

   De plus, la formule $\forall \overline{x}\ (a_1 = a'_1 \to \ldots \to a_n = a'_n \to b \neq b' \to \left(\bigvee_{i=1,\dots,n}(a_i \veebar a'_i)\right) \vee \neg(b \veebar b') \neq 1)$ est vraie dans toute algèbre de Boole, donc la formule $\forall \overline{x}\ (\left(\bigvee_{i=1,\dots,n}(a_i \veebar a'_i)\right) \vee \neg(b \veebar b') = 1 \to (a_1 \neq a'_1 \vee \ldots \vee a_n \neq a'_n \vee b = b'))$ est vraie dans toute algèbre de Boole à au moins deux éléments, ce qui montre le résultat.

□

Proposition A.11 (Termes sur mesure)**.** Soit f une fonction de $\{0,1\}^n$ dans $\{0,1\}$. Il existe un terme $a(\overline{x}^n)$ du langage des algèbres de Boole tel que pour tous $\overline{b}^n \in \{0,1\}$, $a^{\{0,1\}}\left(\overline{b}\right) = f\left(\overline{b}\right)$. De plus :

— Si $a(\overline{x})$ est un tel terme, alors pour toute algèbre de Boole $(\mathbb{B}, 0^{\mathbb{B}}, 1^{\mathbb{B}}, \vee^{\mathbb{B}}, \wedge^{\mathbb{B}}, \neg^{\mathbb{B}})$, pour tous $\overline{b} \in \{0,1\}$, $a^{\mathbb{B}}\left(\overline{b}^{\mathbb{B}}\right) = \left(f\left(\overline{b}\right)\right)^{\mathbb{B}}$,

— Si $a(\overline{x})$ et $a'(\overline{x})$ sont deux tels termes, alors la formule $\forall \overline{x}\ a = a'$ est vraie dans toute algèbre de Boole.

Démonstration. Pour obtenir un tel terme a, il suffit de poser :

$$a(\overline{x}) = \bigvee_{\substack{(b_1,\ldots,b_n)\in\{0,1\}^n \\ \text{tel que } f(b_1,\ldots,b_n)=1}} \bigwedge_{i=1,\ldots n} x_i^{b_i},$$

où $x_i^{b_i}$ désigne le terme x_i si $b_i = 1$, et le terme $\neg x_i$ sinon.

Pour les deux autres assertions :

— Pour tout terme clos t du langage des algèbres de Boole, on a soit que $t = 0$ est vraie dans toute algèbre de Boole, soit que $t = 1$ est vraie dans toute algèbre de Boole (on le montre par induction sur t). Or, pour tous $\overline{b} \in \{0,1\}$, en posant $c = f\left(\overline{b}\right) \in \{0,1\}$, la formule $a\left(\overline{b}\right) = c$ est vraie dans l'algèbre de Boole $\{0,1\}$, elle est donc vraie dans toute algèbre de Boole.

— Cela découle de la proposition A.10.

□

A.3 Atomes

Définition A.12. Un *atome* est une formule de la forme $\top$, $\bot$ ou $a \neq b$.

Soit $\mathcal{E}$ un $\mathcal{M}$-ensemble d'atomes. Les variables libres de $\mathcal{E}$ sont les variables qui sont libres dans au moins un élément de $\mathcal{E}$.

On lira les ensembles d'atomes comme des disjonctions : si $\mathcal{E} = \{\alpha_1, \ldots, \alpha_m\}$ et $\mathcal{F} = \{\beta_1, \ldots, \beta_n\}$ sont deux ensembles finis d'atomes, on dira que $\mathcal{E}$ *implique* $\mathcal{F}$, et l'on notera $\mathcal{E} \Rightarrow \mathcal{F}$, si $\{0,1\} \models \forall \overline{x}\ ((\alpha_1 \vee \ldots \vee \alpha_m) \rightarrow (\beta_1 \vee \ldots \vee \beta_n))$, où $\overline{x}$ désigne la liste des variables libres de $\mathcal{E} \cup \mathcal{F}$ (une disjonction 0-aire désigne la formule $\bot$). D'après le deuxième corollaire de la proposition A.10, cela revient dire que cette formule est vraie dans toute algèbre de Boole à au moins deux éléments.

Une disjonction d'atomes peut en fait être vue comme un seul atome :

Notation. Si α et β sont deux atomes, on note $\alpha \oplus \beta$ l'atome défini de la manière suivante :

— $\top \oplus \beta$ est l'atome $\top$,

— $\alpha \oplus \top$ est l'atome $\top$,

— $\bot \oplus \beta$ est l'atome β,

— $\alpha \oplus \bot$ est l'atome α,

— $(a \neq a') \oplus (b \neq b')$ est l'atome $((a \wedge \neg a') \vee (\neg a \wedge a') \vee (b \wedge \neg b') \vee (\neg b \wedge b')) \neq 0$.

Pour tous atomes $\alpha(\overline{x})$ et $\beta(\overline{x})$, la formule $\forall \overline{x}\ ((\alpha \oplus \beta) \leftrightarrow (\alpha \vee \beta))$ est vraie dans toute algèbre de Boole à au moins deux éléments. Pour les notations, on considère que $\oplus$ est prioritaire sur tous les connecteurs logiques et associe à gauche.

Notation. Si $a_1, \ldots, a_n$ et $b_1, \ldots, b_n$ sont des termes du langage des algèbres de Boole, on note $\overline{a}^n \neq \overline{b}^n$ l'atome $(a_1 \neq b_1) \oplus \ldots \oplus (a_n \neq b_n)$ (et donc $\overline{a}^n = \overline{b}^n$ la formule $((a_1 \neq b_1) \oplus \ldots \oplus (a_n \neq b_n)) \rightarrow \bot$).

A.4 Démonstrations formelles

On va présenter un système de preuve adapté spécifiquement aux algèbres de Boole à au moins deux éléments (c'est-à-dire qu'une formule du langage des algèbres de Boole sera démontrable dans ce système si et seulement si elle est vraie dans toute algèbre de Boole à au moins deux éléments). Il est construit pour avoir les deux caractéristiques suivantes :

— calculatoirement, les preuves correspondent aux termes du λ-calcul pur simplement typé[i] (en particulier, ce système ne contient pas la loi de Peirce comme « primitive », puisque celle-ci correspond à l'opérateur *call/cc*, qui ne fait pas partie du λ-calcul pur),

— les preuves[ii] sont toutes η-expansées au maximum (cf. la règle *Élim* ci-dessous). Du point de vue calculatoire, cela veut dire que l'on n'autorise pas l'application partielle des termes.

Les séquents de ce système ont, à gauche, un nombre arbitraire de formules, et à droite, une formule plus un nombre arbitraire d'atomes : on verra que c'est suffisant pour avoir accès à toute la logique classique. Ces atomes supplémentaires et les règles de dérivation qui les manipulent n'ont pas de contenu calculatoire.

Définition A.13 (Démonstrations booléennes)**.** Un *séquent booléen* est un séquent de la forme $\Gamma \vdash A; \mathcal{E}$, avec Γ un ensemble fini de formules, A une formule et $\mathcal{E}$ un ensemble fini d'atomes. On s'autorisera à noter Γ, B pour $\Gamma \cup \{B\}$ et $\mathcal{E}, \alpha$ pour $\mathcal{E} \cup \{\alpha\}$.

Une *démonstration booléenne* est un arbre formé à partir des règles suivantes. Sa racine (en bas) est appelée sa *conclusion* :

$$\text{(Axiome)}\ \frac{}{\Gamma, A \vdash A; \mathcal{E}} \qquad \text{(Tautologie)}\ \frac{}{\Gamma \vdash \alpha; \mathcal{E}}\ (\text{si } \top \Rightarrow (\mathcal{E}, \alpha))$$

$$\text{(Équation)}\ \frac{\Gamma \vdash \alpha; \mathcal{E}}{\Gamma \vdash \beta; \mathcal{F}}\ (\text{si } (\mathcal{E}, \alpha) \Rightarrow (\mathcal{F}, \beta))$$

$$\text{($\forall$-intro)}\ \frac{\Gamma \vdash A; \mathcal{E}}{\Gamma \vdash \forall x\ A; \mathcal{E}}\ (\text{si } x \text{ n'est libre ni dans } \Gamma \text{ ni dans } \mathcal{E}) \qquad \text{($\to$-intro)}\ \frac{\Gamma, A \vdash B; \mathcal{E}}{\Gamma \vdash A \to B; \mathcal{E}}$$

$$\text{(Élim)}\ \frac{\begin{array}{c}\Gamma \vdash \forall \overline{x_0}\ (A_0 \to \ldots \to \forall \overline{x_{n-1}}\ (A_{n-1} \to \forall \overline{x_n}\ \alpha)\ldots); \mathcal{E} \\ \Gamma \vdash A_0[\overline{x_0} := \overline{a_0}]; \mathcal{E} \quad \ldots \quad \Gamma \vdash A_{n-1}[\overline{x_0} := \overline{a_0}, \ldots, \overline{x_{n-1}} := \overline{a_{n-1}}]; \mathcal{E}\end{array}}{\Gamma \vdash \alpha[\overline{x_0} := \overline{a_0}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}\ \left(\begin{array}{l}\text{Si } \overline{x_0}, \ldots, \overline{x_n} \\ \text{2 à 2 distinctes}\end{array}\right)$$

Un séquent booléen est dit *dérivable* s'il est la conclusion d'au moins une démonstration booléenne.

Remarque. Dans la règle *Élim*, les variables $\overline{x_0}, \ldots, \overline{x_n}$ doivent être deux à deux distinctes. En revanche, chacune des liste $\overline{x_i}$ peut être vide, et n peut être nul, ce qui veut dire que la règle peut même avoir une seule prémisse, identique à sa conclusion.

L'intérêt de n'autoriser la règle d'élimination que lorsque la conclusion est un atome sera de forcer les démonstrations sans coupures (au moins celles dont la conclusion est un atome) à être η-expansées au maximum. On ne perd rien au change, puisque les règles habituelles d'élimination de $\forall$, $\to$ et $\bot$ sont admissibles :

Lemme A.14 (Règles d'élimination)**.** Pour tout ensemble fini de formules Γ, tout ensemble fini d'atomes $\mathcal{E}$, toute variable x, tout terme a et toutes formules A et B :

— si le séquent $\Gamma \vdash \forall x\ A; \mathcal{E}$ est dérivable, alors le séquent $\Gamma \vdash A[x := a]; \mathcal{E}$ l'est,

— si les séquents $\Gamma \vdash B \to A; \mathcal{E}$ et $\Gamma \vdash B; \mathcal{E}$ sont dérivables, alors $\Gamma \vdash A; \mathcal{E}$ l'est.

— si le séquent $\Gamma \vdash \bot; \mathcal{E}$ est dérivable, alors $\Gamma \vdash A; \mathcal{E}$ l'est.

Démonstration. Il suffit de décomposer A jusqu'à pouvoir utiliser la règle *Élim* (ou la règle *Équation*, pour le troisième point), puis de la reconstruire à l'aide des règles d'introduction. □

i. Ou encore, de façon équivalente, aux termes simples CPS-traduits du chapitre 4 : c'est grâce à cela que l'on peut démontrer les théorèmes 4.10 et 4.18.

ii. Du moins, celles dont la conclusion est un atome.

Corollaire (Règle de coupure)**.** Pour tout ensemble fini de formules Γ, tout ensemble fini d'atomes $\mathcal{E}$ et toute formules $A_1, \ldots, A_n$ et B, si les séquents $\Gamma, A_1, \ldots, A_n \vdash B; \mathcal{E}$ et $(\Gamma \vdash A_1; \mathcal{E}), \ldots, (\Gamma \vdash A_n; \mathcal{E})$ sont dérivables, alors le séquent $\Gamma \vdash B; \mathcal{E}$ l'est

Démonstration. Il suffit d'appliquer n fois la règle d'introduction de $\to$ puis n fois sa règle d'élimination (qui est admissible d'après la proposition précédente). □

On peut également vérifier que la règle d'affaiblissement est admissible :

Lemme A.15 (Règle d'affaiblissement)**.** Pour tous ensembles finis de formules Γ et Δ, tous ensembles finis d'atomes $\mathcal{E}$ et $\mathcal{F}$ et toute formule A, si $\Gamma \subseteq \Delta$, si $\mathcal{E} \Rightarrow \mathcal{F}$ et si le séquent $\Gamma \vdash A; \mathcal{E}$ est dérivable, alors le séquent $\Delta \vdash A; \mathcal{F}$ l'est.

Par conséquent, on peut s'attendre à ce que ce système de preuve soit complet pour les algèbres de Boole à au moins deux éléments. Le seul point qui pourrait poser problème, c'est qu'à part les atomes, on n'autorise pas plus d'une formule à droite du séquent, et qu'en même temps, on n'a pas inclus la loi de Peirce dans les règles de déduction. Heureusement, le fait d'autoriser plusieurs atomes à droite est suffisant pour rendre la loi de Peirce admissible :

Lemme A.16 (Loi de Peirce)**.** Soient A et B deux formules du langage des algèbres de Boole. Le séquent $\emptyset \vdash ((A \to B) \to A) \to A; \emptyset$ est dérivable.

Démonstration. Pour alléger les notations, on va supposer que A est de la forme $\forall x\ (D \to \alpha)$ et que B est de la forme $\forall y\ (E \to \beta)$ où α et β sont des atomes, y n'est pas libre dans $D \to \alpha$ et x n'est pas libre dans $E \to \beta$: la preuve est similaire dans le cas général. Notons T la démonstration suivante :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(A \to B) \to A, D, A, E \vdash \forall x\ (D \to \alpha); \emptyset} \quad \dfrac{}{(A \to B) \to A, D, A, E \vdash D; \emptyset}}{(A \to B) \to A, D, A, E \vdash \alpha; \emptyset}}{(A \to B) \to A, D, A, E \vdash \beta; \alpha}}{(A \to B) \to A, D, A \vdash E \to \beta; \alpha}}{(A \to B) \to A, D, A \vdash \forall y\ (E \to \beta); \alpha}}{(A \to B) \to A, D \vdash A \to B; \alpha}$$

La démonstration booléenne suivante convient alors :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(A \to B) \to A, D \vdash (A \to B) \to \forall x\ (D \to \alpha); \alpha} \quad \dfrac{\dfrac{}{T}}{(A \to B) \to A, D \vdash A \to B; \alpha}} \quad \dfrac{}{(A \to B) \to A, D \vdash D; \alpha}}{(A \to B) \to A, D \vdash \alpha; \alpha}}{(A \to B) \to A, D \vdash \alpha; \emptyset}}{(A \to B) \to A \vdash D \to \alpha; \emptyset}}{(A \to B) \to A \vdash \forall x\ (D \to \alpha); \emptyset}}{\emptyset \vdash ((A \to B) \to A) \to A; \emptyset}$$

□

Proposition A.17 (Règle de ré-écriture)**.** Pour tout ensemble fini de formules Γ, tout ensemble fini d'atomes $\mathcal{E}$, toute formule A, toute variable du premier ordre x et tous termes du langage des algèbres de Boole a et b, si $\{\ a \neq b\ \} \Rightarrow \mathcal{E}$ et si le séquent booléen $\Gamma[x := a] \vdash A[x := a]; \mathcal{E}$ est dérivable, alors le séquent booléen $\Gamma[x := b] \vdash A[x := b]; \mathcal{E}$ est dérivable.

Démonstration. Grâce au corollaire du lemme A.14, il suffit de montrer que pour toute formule B, les séquents $B[x := a] \vdash B[x := b]$ et $B[x := b] \vdash B[x := a]$ sont dérivables. On va procéder par induction sur la profondeur de B :

La formule B est de la forme $\forall \overline{y_0}\ D_0 \to \ldots \forall \overline{y_{n-1}}\ D_{p-1} \to \overline{y_n}\ \alpha$, où l'on peut supposer que les variables $\overline{y_0}, \ldots, \overline{y_n}$ sont deux à deux distinctes et différentes de x et ne sont libres ni dans Γ, ni dans $\mathcal{E}$, ni dans a, ni dans b. Supposons que pour tout $i \in \{0, \ldots, p-1\}$, les séquents $D_i[x := a] \vdash D_i[x := b]$ et $D_i[x := b] \vdash D_i[x := a]$ sont dérivables. Les séquents $B[x := b], D_0[x := a], \ldots, D_{n-1}[x := a] \vdash \alpha[x := b]$ et $B[x := a], D_0[x := b], \ldots, D_{n-1}[x := b] \vdash \alpha[x := a]$ sont dérivables grâce à la règle *Élim*.

Par ailleurs, comme $\{\ a \neq b\ \} \Rightarrow \mathcal{E}$, on a $(\mathcal{E}, \alpha[x := b]) \Rightarrow (\mathcal{E}, \alpha[x := a])$ et $(\mathcal{E}, \alpha[x := a]) \Rightarrow (\mathcal{E}, \alpha[x := b])$, donc les séquents $B[x := b], D_0[x := a], \ldots, D_{n-1}[x := a] \vdash \alpha[x := a]$ et $B[x := a], D_0[x := b], \ldots, D_{n-1}[x := b] \vdash \alpha[x := b]$ sont dérivables grâce à la règle *Équation*.

Finalement, les séquents $B[x := b] \vdash B[x := a]$ et $B[x := a] \vdash B[x := b]$ sont dérivables grâce aux règles d'introduction de $\forall$ et $\to$. □

Proposition A.18 (Correction et complétude)**.** Un séquent booléen $A_1(\overline{x}), \ldots, A_m(\overline{x}) \vdash B(\overline{x}); \alpha_1(\overline{x}), \ldots, \alpha_n(\overline{x})$ est dérivable si et seulement si la formule $\forall \overline{x}\ (A_1 \to \ldots \to A_m \to (B \vee \alpha_1 \vee \ldots \vee \alpha_n))$ est vraie dans toute algèbre de Boole à au moins deux éléments.

Démonstration. Le deuxième corollaire de la proposition A.10 garantit la correction des règles *Tautologie* et *Équation*, et celle des autres règles va de soi.

Il reste à montrer la complétude, c'est-à-dire que si le séquent $A_1(\overline{x}), \ldots, A_m(\overline{x}) \vdash B(\overline{x}); \alpha_1(\overline{x}), \ldots, \alpha_n(\overline{x})$ n'est pas dérivable, alors il existe une algèbre de Boole à au moins deux éléments qui vérifie $\neg(\forall \overline{x}\ (A_1 \to \ldots \to A_m \to (B \vee \alpha_1 \vee \ldots \vee \alpha_n)))$.

Remarquons d'abord que si B est la formule $\forall \overline{y_0}\ (D_0 \to \ldots \to \forall \overline{y_{p-1}}\ (D_{p-1} \to \forall \overline{y_p}\ \beta)\ldots)$ avec $\overline{x}, \overline{y_0}, \ldots, \overline{y_p}$ deux à deux distinctes, alors d'une part si le séquent $A_1, \ldots, A_m \vdash B; \alpha_1, \ldots, \alpha_n$ n'est pas dérivable, le séquent $A_1, \ldots, A_m, D_0, \ldots, D_{p-1} \vdash \bot; \beta, \alpha_1, \ldots, \alpha_n$ n'est pas dérivable non plus (car on passe du second au premier avec une règle *Équation* et quelques règles d'introduction), et d'autre part, si une algèbre de Boole vérifie $\neg(\forall \overline{x}\ \forall \overline{y_0}\ \ldots\ \forall \overline{y_p}\ (A_1 \to \ldots \to A_m \to D_0 \to \ldots \to D_p \to (\bot \vee \beta \vee \alpha_1 \vee \ldots \vee \alpha_n)\ldots))$, alors elle vérifie également $\neg(\forall \overline{x}\ (A_1 \to \ldots \to A_m \to (B \vee \alpha_1 \vee \ldots \vee \alpha_n)))$. On peut donc supposer sans perte de généralité que B est la formule $\bot$

Pour tout atome β, le séquent $\emptyset \vdash \neg(\beta); \beta$ est dérivable :

$$\dfrac{\dfrac{\dfrac{}{\beta \vdash \beta; \emptyset}\ \text{(Axiome)}}{\beta \vdash \bot; \beta}\ \text{(Équation)}}{\emptyset \vdash \neg(\beta); \beta}\ (\to\text{-intro})$$

Par conséquent, le séquent $\forall \overline{x}\ (A_1 \to \ldots \to A_m \to \neg(\alpha_1) \to \ldots \to \neg(\alpha_n) \to \bot), A_1, \ldots, A_m \vdash \bot; \alpha_1, \ldots, \alpha_n$ est dérivable, donc le séquent $A_1, \ldots, A_m \vdash (\forall \overline{x}\ (A_1 \to \ldots \to A_m \to \neg(\alpha_1) \to \ldots \to \neg(\alpha_n) \to \bot)) \to \bot; \alpha_1, \ldots, \alpha_n$ est dérivable, et donc le séquent $((\forall \overline{x}\ (A_1 \to \ldots \to A_m \to \neg(\alpha_1) \to \ldots \to \neg(\alpha_n) \to \bot)) \to \bot) \to \bot, A_1, \ldots, A_m \vdash \bot; \alpha_1, \ldots, \alpha_n$ est dérivable. Ainsi, si le séquent $A_1, \ldots, A_m \vdash \bot; \alpha_1, \ldots, \alpha_n$ n'est pas dérivable, alors le séquent $(\forall \overline{x}\ (A_1 \to \ldots \to A_m \to \neg(\alpha_1) \to \ldots \to \neg(\alpha_n) \to \bot)) \to \bot \vdash \bot; \emptyset$ n'est pas dérivable non plus. Par ailleurs, une algèbre de Boole qui vérifie $\neg((\forall \overline{x}\ (A_1 \to \ldots \to A_m \to \neg(\alpha_1) \to \ldots \to \neg(\alpha_n) \to \bot)) \to \bot)$ vérifie également $\neg(\forall \overline{x}\ (A_1 \to \ldots \to A_m \to (\bot \vee \alpha_1 \vee \ldots \vee \alpha_n)))$. Il suffit donc de montrer que pour toute formule close D, si le séquent $D \vdash \bot; \emptyset$ n'est pas dérivable, alors il existe une algèbre de Boole à au moins deux éléments qui vérifie D.

On va faire appel au théorème de complétude de Gödel tel que formulé dans *Mathematical Logic – A Course with Exercises Part I* [RC02, p. 208]. Selon les termes de cet ouvrage, une algèbre de Boole est une *réalisation* d'un certain langage L (dont les symboles de constantes sont 0 et 1, les symboles de fonctions $\vee$, $\wedge$ et $\neg$ et avec $=$ comme seul symbole de relation) vérifiant certains axiomes. On traduit de la manière naturelle toute formule du langage des algèbres de Boole en une formule de L et vice-versa (même si cela

ne définit pas une bijection), de sorte qu'une algèbre de Boole vérifie une formule du langage des algèbre de Boole si et seulement si elle vérifie sa traduction dans L, et réciproquement, elle vérifie une formule de L si et seulement si elle vérifie sa traduction dans le langage des algèbres de Boole.

Pour montrer la complétude, il suffit donc de montrer que pour toute formule close D du langage des algèbres de Boole telle que le séquent $D \vdash \bot; \emptyset$ ne soit pas dérivable, la théorie $\mathcal{T}_D$ de L composée de la formule D, des axiomes des algèbres de Boole à au moins deux éléments exprimés dans L et des *axiomes de l'égalité* tels que définis à la section 6.1 de *Mathematical Logic – A Course with Exercises Part I* est cohérente *au sens de ce dernier ouvrage*. Comme on sait déjà que le séquent $D \vdash \bot; \emptyset$ n'est pas dérivable, il suffit de montrer que pour toute formule E du langage des algèbres de Boole, si E est la traduction d'une formule de L qui est conséquence syntaxique de $\mathcal{T}_D$, alors $D \vdash E; \emptyset$ est dérivable. Vu la définition des démonstrations formelles donnée dans l'ouvrage en question, il suffit de montrer les points suivants :

1. Pour toutes formules E et F, si les séquents $D \vdash E \to F; \emptyset$ et $D \vdash E; \emptyset$ sont dérivables, alors $D \vdash E; \emptyset$ l'est,
2. Pour toute formule E et toute variable x, si le séquent $D \vdash E; \emptyset$ est dérivable, alors $D \vdash \forall x\ E; \emptyset$ l'est,
3. Pour toute formule E, si E est la traduction d'une tautologie propositionnelle, le séquent $\emptyset \vdash E; \emptyset$ est dérivable,
4. Pour toutes formules Eet F et toute variable x qui n'est pas libre dans E, le séquent $\emptyset \vdash \forall x\ (E \to F) \to E \to \forall x\ F; \emptyset$ est dérivable,
5. Pour toute formule E, toute variable x et tout terme a du langage des algèbres de Boole, le séquent $D \vdash \forall x\ E \to E[x := a]; \emptyset$ est dérivable,
6. Pour toute formule E, si E est la traduction d'un axiome de l'égalité, le séquent $\emptyset \vdash E; \emptyset$ est dérivable,
7. Pour toute formule E, si E est l'atome $0 \neq 1$ ou l'un des axiomes des algèbres de Boole, le séquent $\emptyset \vdash E; \emptyset$ est dérivable.

Les points 1., 2., 4., 5. et 7. sont immédiats.

Pour le point 3., le seul point épineux est la loi de Peirce, que l'on a déjà traitée avec le lemme A.16. On omettra donc le reste de la démonstration.

Pour le point 6., il suffit de montrer que les séquents suivants sont dérivables :

i. $\emptyset \vdash \forall x\ \neg(x \neq x); \emptyset$,

ii. $\emptyset \vdash \forall x\ \forall y\ (\neg(x \neq y) \to \neg(y \neq x)); \emptyset$,

iii. $\emptyset \vdash \forall x\ \forall y\ \forall z\ (\neg(x \neq y) \to \neg(y \neq z) \to \neg(x \neq z)); \emptyset$,

iv. $\emptyset \vdash \forall x\ \forall y\ \forall x'\ \forall y'\ (\neg(x \neq x') \to \neg(y \neq y') \to \neg((x \vee y) \neq (x' \vee y'))); \emptyset$,

v. $\emptyset \vdash \forall x\ \forall y\ \forall x'\ \forall y'\ (\neg(x \neq x') \to \neg(y \neq y') \to \neg((x \wedge y) \neq (x' \wedge y'))); \emptyset$,

vi. $\emptyset \vdash \forall x\ \forall x'\ (\neg(x \neq x') \to \neg(\neg x \neq \neg x')); \emptyset$.

On se contentera de monter iii. et iv. : les autres preuves sont similaires. Pour iii., en notant Γ pour $\neg(x \neq y), \neg(y \neq z), x \neq z$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash x \neq y \to \bot; \emptyset} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash y \neq z \to \bot; x \neq y} \qquad \dfrac{\dfrac{}{\Gamma \vdash x \neq z; x \neq y, y \neq z}}{\Gamma \vdash \bot; x \neq y, y \neq z}}{\Gamma \vdash y \neq z; x \neq y}}{\Gamma \vdash \bot; x \neq y}}{\Gamma \vdash x \neq y; \emptyset}}{\Gamma \vdash \bot; \emptyset}}{\vdots}}{\emptyset \vdash \forall x\ \forall y\ \forall z\ (\neg(x \neq y) \to \neg(y \neq z) \to \neg(x \neq z)); \emptyset}$$

Pour iv., en notant Γ pour $\neg(x \neq x'), \neg(y \neq y'), (x \vee y) \neq (x' \vee y')$:

$$\dfrac{\dfrac{\dfrac{}{\emptyset \vdash x \neq x' \to \bot; \emptyset} \quad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash y \neq y' \to \bot; x \neq x'} \quad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash (x \vee y) \neq (x' \vee y'); x \neq x', y \neq y'}}{\Gamma \vdash \bot; x \neq x', y \neq y'}}{\Gamma \vdash y \neq y'; x \neq x'}}{\Gamma \vdash \bot; x \neq x'}}{\Gamma \vdash x \neq x'; \emptyset}}{\Gamma \vdash \bot; \emptyset}}{\vdots}$$
$$\emptyset \vdash \forall x\, \forall y\, \forall x'\, \forall y'\, (\neg(x \neq x') \to \neg(y \neq y') \to \neg((x \vee y) \neq (x' \vee y')))); \emptyset$$

□

A.5 Élimination des coupures

Définition A.19. Une *coupure* est une démonstration booléenne S de la forme

$$(\text{Élim})\ \dfrac{\dfrac{T}{\Gamma \vdash \forall \overline{x_0}\ (A_0 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E}} \quad \dfrac{U_0}{\Gamma \vdash A_0[\overline{x_0} := \overline{a_0}]; \mathcal{E}} \quad \ldots \quad \dfrac{U_{n-1}}{\Gamma \vdash A_0[\overline{x_0} := \overline{a_0}, \ldots, \overline{x_{n-1}} := \overline{a_{n-1}}]; \mathcal{E}}}{\Gamma \vdash \alpha[\overline{x_0} := \overline{a_0}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}$$

où soit la dernière règle de la sous-démonstration T est une règle d'introduction, soit $n = 0$ et la liste $\overline{x_n}$ est vide (c'est-à-dire que la conclusion de S est identique à celle de T). La démonstration T est appelée *sous-démonstration principale* de la coupure.

Une démonstration booléenne T est *sans coupure* si aucune sous-démonstration (c'est-à-dire aucun sous-arbre) de T n'est une coupure.

Notation (Spécialisation)**.** Pour toute démonstration booléenne T de conclusion $\Gamma \vdash A; \mathcal{E}$, toutes variables du premier ordre $\overline{x}$ et tous termes $\overline{a}$ du langage des algèbres de Boole, on va définir une démonstration booléenne $T[\overline{x} := \overline{a}]$ de conclusion $\Gamma[\overline{x} := \overline{a}] \vdash A[\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]$, et possédant la même « structure » que T.

On procède par induction :

Si T est la démonstration $\dfrac{}{\Gamma, A \vdash A; \mathcal{E}}$ (Axiome), on définit $T[\overline{x} := \overline{a}]$ comme la démonstration : $\dfrac{}{\Gamma[\overline{x} := \overline{a}], A[\overline{x} := \overline{a}] \vdash A[\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]}$ (Axiome).

Si T est la démonstration $\dfrac{}{\Gamma \vdash \alpha; \mathcal{E}}$ (Tautologie), alors on a $\top \Rightarrow (\mathcal{E}, \alpha)$, et donc à plus forte raison $\top \Rightarrow (\mathcal{E}[\overline{x} := \overline{a}], \alpha[\overline{x} := \overline{a}])$. Par conséquent, on peut définir $T[\overline{x} := \overline{a}]$ comme la démonstration : $\dfrac{}{\Gamma[\overline{x} := \overline{a}] \vdash \alpha[\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]}$ (Tautologie).

Si T est la démonstration $\dfrac{\dfrac{S}{\Gamma \vdash \alpha; \mathcal{E}}}{\Gamma \vdash \beta; \mathcal{F}}$ (Équation), on a $(\mathcal{E}, \alpha) \Rightarrow (\mathcal{F}, \beta)$, et donc à plus forte raison $(\mathcal{E}[\overline{x} := \overline{a}], \alpha[\overline{x} := \overline{a}]) \Rightarrow (\mathcal{F}[\overline{x} := \overline{a}], \beta[\overline{x} := \overline{a}])$. Par conséquent, on peut définir $T[\overline{x} := \overline{a}]$ comme la démonstration : $\dfrac{\dfrac{S[\overline{x} := \overline{a}]}{\Gamma[\overline{x} := \overline{a}] \vdash \alpha[\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]}}{\Gamma[\overline{x} := \overline{a}] \vdash \beta[\overline{x} := \overline{a}]; \mathcal{F}[\overline{x} := \overline{a}]}$ (Équation).

Si T est la démonstration $\dfrac{\dfrac{S}{\Gamma \vdash A; \mathcal{E}}}{\Gamma \vdash \forall y\ A; \mathcal{E}}$ (∀-intro), alors on choisit une variable z qui n'est pas dans la liste $\overline{x}$ et qui n'est libre ni dans Γ, ni dans $\mathcal{E}$, ni dans A, ni dans $\overline{a}$, et l'on définit $T[\overline{x} := \overline{a}]$ comme la démonstration :

$$\dfrac{\dfrac{S[y := z][\overline{x} := \overline{a}]}{\Gamma[\overline{x} := \overline{a}] \vdash A[y := z][\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]}}{\Gamma[\overline{x} := \overline{a}] \vdash \forall z\ A[y := z][\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]} (\forall\text{-intro}).$$

Si T est la démonstration $\dfrac{\dfrac{S}{\Gamma, A \vdash B; \mathcal{E}}}{\Gamma \vdash A \to B; \mathcal{E}}$ (→-intro), on définit $T[\overline{x} := \overline{a}]$ comme la démonstration :

$$\dfrac{\dfrac{S[\overline{x} := \overline{a}]}{\Gamma[\overline{x} := \overline{a}], A[\overline{x} := \overline{a}] \vdash B[\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]}}{\Gamma[\overline{x} := \overline{a}] \vdash A[\overline{x} := \overline{a}] \to B[\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]} (\to\text{-intro}).$$

Si T est la démonstration $\dfrac{\dfrac{S}{\Gamma \vdash \forall \overline{y_0}\ (A_0 \to \ldots \to (\forall \overline{y_n}\ \alpha)\ldots); \mathcal{E}} \quad \dfrac{U_0}{\Gamma \vdash A_0[\overline{y_0} := \overline{b_0}]; \mathcal{E}} \quad \ldots}{\Gamma \vdash \alpha[\overline{y_0} := \overline{b_0}, \ldots, \overline{y_n} := \overline{b_n}]; \mathcal{E}}$ (Élim), alors on définit alors T comme la démonstration :

$$\dfrac{\dfrac{S[\overline{x} := \overline{a}]}{\Gamma[\overline{x} := \overline{a}] \vdash \forall \overline{y_0}\ (A_0 \to \ldots \to (\forall \overline{y_n}\ \alpha)\ldots)[\overline{x} := \overline{a}]} \quad \dfrac{U_0[\overline{x} := \overline{a}]}{\Gamma[\overline{x} := \overline{a}] \vdash A_0[\overline{y_0} := \overline{b_0}][\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]} \quad \ldots}{\Gamma[\overline{x} := \overline{a}] \vdash \alpha[\overline{y_0} := \overline{b_0}, \ldots, \overline{y_n} := \overline{b_n}][\overline{x} := \overline{a}]; \mathcal{E}[\overline{x} := \overline{a}]}$$

Ceci défini bien une démonstration booléenne. En effet, comme les formules sont définies à α-renommage près, on peut supposer que les variables $\overline{y_0}, \ldots, \overline{y_n}$ n'apparaissent pas dans $\overline{x}$ et ne sont libres ni dans $\overline{a}$, ni dans Γ, ni dans $\mathcal{E}$, et alors :

- La formule $\forall \overline{y_0}\ (A_0 \to \ldots \to (\forall \overline{y_n}\ \alpha)\ldots)[\overline{x} := \overline{a}]$ est identique à la formule $\forall \overline{y_0}\ (A_0[\overline{x} := \overline{a}] \to \ldots \to (\forall \overline{y_n}\ \alpha[\overline{x} := \overline{a}])\ldots)$,
- Pour tout $i \in \{0, \ldots, n-1\}$, la formule $A_i[\overline{y_0} := \overline{b_0}, \ldots, \overline{y_i} := \overline{b_i}][\overline{x} := \overline{a}]$ est identique à la formule $A_i[\overline{x} := \overline{a}][\overline{y_0} := \overline{b_0[\overline{x} := \overline{a}]}, \ldots, \overline{y_i} := \overline{b_i[\overline{x} := \overline{a}]}]$,
- La formule $\alpha[\overline{y_0} := \overline{b_0}, \ldots, \overline{y_n} := \overline{b_n}][\overline{x} := \overline{a}]$ est identique à la formule $\alpha[\overline{x} := \overline{a}][\overline{y_0} := \overline{b_0}[\overline{x} := \overline{a}], \ldots, \overline{y_n} := \overline{b_n}[\overline{x} := \overline{a}]]$.

Notation (Affaiblissement)**.** Pour toute démonstration booléenne T de conclusion $\Gamma \vdash A; \mathcal{E}$, tout $\Delta \supseteq \Gamma$ et tout $\mathcal{F}$ tel que $\mathcal{E} \Rightarrow \mathcal{F}$, on va définir une démonstration $T^{\Delta;\mathcal{F}}$ de conclusion $\Delta \vdash A; \mathcal{F}$ et possédant la même « structure » que T.

On procède par induction sur T :

Si T est de la forme

$$\dfrac{\dfrac{S_1}{\Gamma_1 \vdash A_1; \mathcal{E}_1} \quad \ldots \quad \dfrac{S_n}{\Gamma_n \vdash A_n; \mathcal{E}_n},}{\Gamma \vdash A; \mathcal{E}} (R)$$

pour une certaine règle R autre que $\forall$-*intro*, alors $T^{\Delta;\mathcal{F}}$ est la démonstration :

$$\dfrac{\dfrac{S_1^{\Gamma_1,\Delta;\mathcal{E}_1,\mathcal{F}}}{\Gamma_1, \Delta \vdash A_1; \mathcal{E}_1, \mathcal{F}} \quad \ldots \quad \dfrac{S_n^{\Gamma_n,\Delta;\mathcal{E}_n,\mathcal{F}}}{\Gamma_n, \Delta \vdash A_n; \mathcal{E}_n, \mathcal{F}}.}{\Delta \vdash A; \mathcal{F}} (R)$$

Si T est de la forme $\dfrac{\dfrac{S}{\Gamma \vdash A; \mathcal{E}}}{\Gamma \vdash \forall y\ A; \mathcal{E}}$ (∀-intro), alors on choisit une variable z qui n'est libre ni dans Δ, ni

dans $\mathcal{F}$, et $T^{\Delta;\mathcal{F}}$ est la démonstration $\text{(}\forall\text{-intro)}\ \dfrac{\dfrac{S[y := z]^{\Delta;\mathcal{F}}}{\Delta \vdash A[y := z]; \mathcal{F}}}{\Delta \vdash \forall z\ A[y := z]; \mathcal{F}}$.

Notation (Substitution)**.** Pour toute démonstration T de conclusion $\Gamma \vdash A; \mathcal{E}$ et toute démonstration S de conclusion $\Gamma, A \vdash B; \mathcal{E}$, on va définir une démonstration $S[A|T]$ de conclusion $\Gamma \vdash B; \mathcal{E}$.

On procède par induction sur S :

Si S est la démonstration $\text{(Axiome)}\ \dfrac{}{\Gamma, A \vdash A; \mathcal{E}}$, $S[A|T]$ est la démonstration T.

Si S est la démonstration $\text{(Axiome)}\ \dfrac{}{\Gamma, A \vdash D; \mathcal{E}}$, où D est une formule différente de A, $S[A|T]$ est la démonstration $\text{(Axiome)}\ \dfrac{}{\Gamma \vdash D; \mathcal{E}}$.

Si S est la démonstration $\text{(Tautologie)}\ \dfrac{}{\Gamma, A \vdash \alpha; \mathcal{E}}$, $S[A|T]$ est la démonstration $\text{(Tautologie)}\ \dfrac{}{\Gamma \vdash \alpha; \mathcal{E}}$.

Si S est la démonstration $\text{(Équation)}\ \dfrac{\dfrac{U}{\Gamma, A \vdash \beta; \mathcal{F}}}{\Gamma, A \vdash \alpha; \mathcal{E}}$, $S[A|T]$ est la démonstration $\text{(Équation)}\ \dfrac{\dfrac{U[A|T^{\Gamma;\mathcal{E},\mathcal{F}}]}{\Gamma \vdash \beta; \mathcal{E}, \mathcal{F}}}{\Gamma \vdash \alpha; \mathcal{E}}$.

Si S est la démonstration $\text{(}\forall\text{-intro)}\ \dfrac{\dfrac{U}{\Gamma, A \vdash D; \mathcal{E}}}{\Gamma, A \vdash \forall x\ D; \mathcal{E}}$, $S[A|T]$ est la démonstration $\text{(}\forall\text{-intro)}\ \dfrac{\dfrac{U[A|T]}{\Gamma \vdash D; \mathcal{E}}}{\Gamma \vdash \forall x\ D; \mathcal{E}}$.

Si S est la démonstration $\text{(}\to\text{-intro)}\ \dfrac{\dfrac{U}{\Gamma, A, A \vdash D; \mathcal{E}}}{\Gamma, A \vdash A \to D; \mathcal{E}}$, $S[A|T]$ est la démonstration $\text{(}\to\text{-intro)}\ \dfrac{\dfrac{U}{\Gamma, A \vdash D; \mathcal{E}}}{\Gamma \vdash A \to D; \mathcal{E}}$.

Si S est la démonstration $\text{(}\to\text{-intro)}\ \dfrac{\dfrac{U}{\Gamma, A, C \vdash D; \mathcal{E}}}{\Gamma, A \vdash C \to D; \mathcal{E}}$, où C est une formule différente de A, $S[A|T]$ est la démonstration $\text{(}\to\text{-intro)}\ \dfrac{\dfrac{U[A|T^{\Gamma,C;\mathcal{E}}]}{\Gamma, C \vdash D; \mathcal{E}}}{\Gamma \vdash C \to D; \mathcal{E}}$.

Si S est la démonstration $\text{(Élim)}\ \dfrac{\dfrac{U}{\Gamma, A \vdash \forall \overline{y_0}\ (D_0 \to \ldots \to (\forall \overline{y_n}\ \alpha)\ldots); \mathcal{E}} \quad \dfrac{V_0}{\Gamma, A \vdash D_0[\overline{y_0} := \overline{b_0}]; \mathcal{E}} \quad \ldots, S[A|T]}{\Gamma, A \vdash \alpha[\overline{y_0} := \overline{b_0}, \ldots, \overline{y_n} := \overline{b_n}]; \mathcal{E}}$
est la démonstration $\text{(Élim)}\ \dfrac{\dfrac{U[A|T]}{\Gamma \vdash \forall \overline{y_0}\ (D_0 \to \ldots \to (\forall \overline{y_n}\ \alpha)\ldots); \mathcal{E}} \quad \dfrac{V_0[A|T]}{\Gamma \vdash D_0[\overline{y_0} := \overline{b_0}]; \mathcal{E}} \quad \ldots}{\Gamma \vdash \alpha[\overline{y_0} := \overline{b_0}, \ldots, \overline{y_n} := \overline{b_n}]; \mathcal{E}}$

Proposition A.20 (Élimination des coupures)**.** Un séquent booléen est dérivable si et seulement s'il est la conclusion d'au moins une démonstration booléenne sans coupure.

Démonstration. On va procéder en deux étapes : d'abord, on va montrer comment réduire une coupure, puis, on va décrire une stratégie permettant d'éliminer toutes les coupures.

Une coupure de la forme $\text{(Élim)}\ \dfrac{\dfrac{T}{\Gamma \vdash \alpha; \mathcal{E}}}{\Gamma \vdash \alpha; \mathcal{E}}$ se réduit en $\dfrac{T}{\Gamma \vdash \alpha; \mathcal{E}}$.

Une coupure de la forme

$$\text{(∀-intro)}\ \dfrac{\dfrac{T}{\Gamma \vdash \forall \overline{x_0}\ (A_0 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E}}}{\text{(Élim)}\ \dfrac{\Gamma \vdash \forall y\ \forall \overline{x_0}\ (A_0 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E} \quad \dfrac{U_0}{\Gamma \vdash A_0[y := b, \overline{x_0} := \overline{a_0}]; \mathcal{E}} \quad \ldots}{\Gamma \vdash \alpha[y := b, \overline{x_0} := \overline{a_0}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}}$$

se réduit en :

$$\text{(Élim)}\ \dfrac{\dfrac{T[y := b]}{\Gamma \vdash (\forall \overline{x_0}\ (A_0 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots))[y := b]; \mathcal{E}} \quad \dfrac{U_0}{\Gamma \vdash A_0[y := b, \overline{x_0} := \overline{a_0}]; \mathcal{E}} \quad \ldots.}{\Gamma \vdash \alpha[y := b, \overline{x_0} := \overline{a_0}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}$$

Enfin, une coupure de la forme

$$\text{(→-intro)}\ \dfrac{\dfrac{T}{\Gamma, A_0 \vdash \forall \overline{x_1}\ (A_1 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E}}}{\text{(Élim)}\ \dfrac{\Gamma \vdash A_0 \to \forall \overline{x_1}\ (A_1 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E} \quad \dfrac{U_0}{\Gamma \vdash A_0; \mathcal{E}} \quad \ldots}{\Gamma \vdash \alpha[\overline{x_1} := \overline{a_1}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}}$$

se réduit en :

$$\text{(Élim)}\ \dfrac{\dfrac{T[A_0|U_0]}{\Gamma \vdash \forall \overline{x_1}\ (A_1 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E}} \quad \dfrac{U_1}{\Gamma \vdash A_1[\overline{x_1} := \overline{a_1}]; \mathcal{E}} \quad \ldots.}{\Gamma \vdash \alpha[\overline{x_1} := \overline{a_1}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}$$

Si S est une sous-démonstration T qui est une coupure, *réduire S dans T*, c'est transformer T en remplaçant S par la démonstration en laquelle elle se réduit selon les règles ci-dessus (ce que l'on peut faire, puisque celle-ci a la même conclusion que S).

Il faut maintenant définir une stratégie de réduction[i] qui transforme toute démonstration T en une démonstration sans coupure avec la même conclusion, en réduisant ses coupures dans le bon ordre.

Tout d'abord, à chaque formule A on associe une *hauteur* $\mathrm{haut}(A) \in \mathbb{N}$ en posant $\mathrm{haut}(\alpha) = 0$ si α est un atome, $\mathrm{haut}(\forall x\ A) = 1 + \mathrm{haut}(A)$ et $\mathrm{haut}(A \to B) = 1 + \max(\mathrm{haut}(A), \mathrm{haut}(B))$.

Pour chaque coupure T de la forme $\text{(Élim)}\ \dfrac{\dfrac{U}{\Gamma \vdash \forall \overline{x_0}\ (A_0 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E}} \quad \dfrac{V_0}{\Gamma \vdash A_0[\overline{x_0} := \overline{a_0}]; \mathcal{E}} \quad \ldots,}{\Gamma \vdash \alpha[\overline{x_0} := \overline{a_0}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}$
on appelle *hauteur de T* et l'on note $\mathrm{haut}(T)$ la hauteur de $\forall \overline{x_0}\ (A_0 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots)$.

Ensuite, pour chaque démonstration T, on munit les les sous-démonstrations de T d'un ordre total :
Pour toute sous-démonstration S de T de la forme $\text{(R)}\ \dfrac{\dfrac{U_1}{\Gamma_1 \vdash A_1; \mathcal{E}_1} \quad \ldots \quad \dfrac{U_n}{\Gamma_n \vdash A_n; \mathcal{E}_n}}{\Gamma \vdash A; \mathcal{E}}$, pour tous $i < j < n$,
les sous-démonstrations de U_j (y compris U_j elle-même) sont *plus à droite que* celles de U_i *dans T*, et pour tout $i < n$, les sous-démonstrations de U_i sont *plus à droite que S dans T*.

Lorsque l'on réduit dans T une coupure S de la forme

$$\text{(Élim)}\ \dfrac{\dfrac{U}{\Gamma \vdash \forall \overline{x_0}\ (A_0 \to \ldots \to (\forall \overline{x_n}\ \alpha)\ldots); \mathcal{E}} \quad \dfrac{V_0}{\Gamma \vdash A_0[\overline{x_0} := \overline{a_0}]; \mathcal{E}} \quad \ldots,}{\Gamma \vdash \alpha[\overline{x_0} := \overline{a_0}, \ldots, \overline{x_n} := \overline{a_n}]; \mathcal{E}}$$

i. En vérité, on peut probablement même montrer qu'avec ces règles, le processus de réduction est fortement normalisant, et donc qu'il n'est pas nécessaire de définir une stratégie, mais ce n'est pas l'objet de cette preuve.

d'un côté, on enlève la coupure S, mais de l'autre, on peut ajouter des coupures de trois façons :

— on peut dupliquer des coupures qui sont dans les V_i,

— on peut créer des coupures dont la sous-démonstration principale est l'une des V_i,

— si l'avant-dernière règle de U était aussi une règle d'introduction, elle deviendra la sous-démonstration principale d'une nouvelle coupure.

Cependant, dans le premier cas, on a dupliqué des coupures qui sont plus à droite que S dans T, et dans les deux autres, on a créé des coupures de hauteur strictement plus petite que celle de S. Il suffit donc de réduire en priorité la plus à droite des coupures de hauteur maximale dans T (car alors, à chaque étape, soit on fait baisser la hauteur maximale des coupures de T, soit on fait baisser le nombre de coupures de hauteur maximale dans T). □

B Annexe : Modèles standard de la théorie des ensembles

La réalisabilité classique permet, à partir d'un modèle de la théorie des ensembles (le *modèle de base*) de construire une classe de *modèles de réalisabilité*. Cette annexe a pour but de préciser ce que l'on entend par « modèle de la théorie des ensembles ». Intuitivement, on appellera *modèle standard de la théorie des ensembles* un modèle de la théorie des ensembles de von Neumann–Bernays–Gödel [Gö40] (une extension conservative de la théorie de Zermelo–Frænkel avec une notion primitive de classe) dont la relation d'appartenance est la relation d'appartenance usuelle, qui est un ensemble transitif et dont la relation d'appartenance est bien fondée. Pour éviter d'introduire une n-ième syntaxe, on va donner une définition sémantique de cette notion.

On identifie les entiers et les ordinaux finis, de sorte que pour tout $n \in \mathbb{N}$, $n = \{0, \dots, n-1\}$.

On identifie les couples et les paires de Kuratowski, de sorte que pour tout a et tout b, $(a, b) = \{\{a\}, \{a, b\}\}$. On identifie le 0-uplet $()$ et l'ensemble vide $\emptyset$. Enfin, pour tout $n > 2$ et tous $a_1, \dots, a_n$, on identifie le n-uplet $(a_1, \dots, a_n)$ et le couple $(a_1, (a_2, \dots, a_n))$.

On utilise le mot *fonction* comme synonyme de *application*. On identifie les fonctions à leur graphe, de sorte que pour tous ensemble x, y et toute fonction f de x dans y, $f = \{\ (a, f(a));\ a \in x\ \}$.

Pour tout ensemble x, on note $\mathcal{P}_f(x)$ l'ensemble des parties finies de x.

Un ensemble x est *transitif* si tout élément de x est un ensemble inclus dans x.

Un ensemble transitif x est *bien fondé* si pour tout $y \subseteq x$ non vide, il existe $z \in y$ tel que $y \cap z = \emptyset$.

Définition B.1. Un *modèle standard $\mathcal{M}$ de la théorie des ensembles* est la donnée d'un ensemble appelé *l'ensemble des $\mathcal{M}$-ensembles* (que l'on notera $\mathcal{M}$ par abus de notation) et d'un ensemble appelé *l'ensemble des $\mathcal{M}$-classes* tels que :

(Nature des objets)

1. l'ensemble des $\mathcal{M}$-ensembles est transitif,
2. l'ensemble des $\mathcal{M}$-ensembles est bien fondé,
3. toute $\mathcal{M}$-classe est un ensemble de $\mathcal{M}$-ensembles,
4. tout ensemble fini de $\mathcal{M}$-ensembles est un $\mathcal{M}$-ensemble (en particulier, tout n-uplet de $\mathcal{M}$-ensembles est un $\mathcal{M}$-ensemble),

(Logique)

5. pour tous $m, n \in \mathbb{N}$, toute fonction $j : n \to m$ et toute $\mathcal{M}$-classe X, l'ensemble des $(x_0, \dots, x_{m-1}) \in \mathcal{M}^m \subseteq \mathcal{M}$ tels que $(x_{j(0)}, \dots, x_{j(n-1)}) \in X$ est une $\mathcal{M}$-classe,
6. l'ensemble des $\mathcal{M}$-classes est clos par union finie, intersection finie et complémentaire,

7. pour tout $n > 0$, tout $j < n$ et toute $\mathcal{M}$-classe X, l'ensemble des $(x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_{n-1}) \in \mathcal{M}^{n-1}$ tels que pour tout $x_j \in \mathcal{M}$, $(x_0, \dots, x_{n-1}) \in X$ est une $\mathcal{M}$-classe,
8. pour tout $n > 0$, tout $j < n$ et toute $\mathcal{M}$-classe X, l'ensemble des $(x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_{n-1}) \in \mathcal{M}^{n-1}$ tels qu'il existe $x_j \in \mathcal{M}$ tel que $(x_0, \dots, x_{n-1}) \in X$ est une $\mathcal{M}$-classe,
9. pour tout $n \in \mathbb{N}$, tout $j \in \{0, \dots, n\}$, toute $\mathcal{M}$-classe X et tout $\mathcal{M}$-ensemble a, l'ensemble des $(x_0, \dots, x_{n-1}) \in \mathcal{M}^n$ tels que $(x_0, \dots, x_{j-1}, a, x_j, \dots, x_{n-1}) \in X$ est une $\mathcal{M}$-classe,
10. l'ensemble des $(x, y) \in \mathcal{M}^2$ tels que $x = y$ est une $\mathcal{M}$-classe,
11. l'ensemble des $(x, y) \in \mathcal{M}^2$ tels que $x \in y$ est une $\mathcal{M}$-classe,

(Axiomes de ZF*)*

12. toute $\mathcal{M}$-classe incluse dans un $\mathcal{M}$-ensemble est un $\mathcal{M}$-ensemble,
13. tout $\mathcal{M}$-ensemble est inclus dans un $\mathcal{M}$-ensemble transitif,
14. pour tout $\mathcal{M}$-ensemble x, l'ensemble des $\mathcal{M}$-ensembles inclus dans x (qui est *a priori* une $\mathcal{M}$-classe) est un $\mathcal{M}$-ensemble,
15. l'ensemble $\mathbb{N}$ est un $\mathcal{M}$-ensemble,
16. pour toute $\mathcal{M}$-classe Z et tout $\mathcal{M}$-ensemble x, il existe un $\mathcal{M}$-ensemble y tel que pour tout $a \in x$, s'il existe b tel que $(a, b) \in Z$, alors il existe $b \in y$ tel que $(a, b) \in Z$.

Notons que la cohérence de ZF n'implique pas l'existence d'un modèle standard de la théorie des ensembles. En revanche, s'il existe un cardinal faiblement inaccessible κ, alors il existe un modèle standard de la théorie des ensembles (en prenant par exemple L_κ comme ensemble d'ensembles et $\mathcal{P}(L_\kappa) \cap L$ comme ensemble de classes).

Fixons $\mathcal{M}$ un modèle standard de la théorie des ensembles.

Définition B.2.

— Pour tout $\mathcal{M}$-ensemble x, une *$\mathcal{M}$-partie* de x est une partie de x qui est un $\mathcal{M}$-ensemble. On note $\mathcal{P}_{\mathcal{M}}(x)$ le $\mathcal{M}$-ensemble des $\mathcal{M}$-parties de x,

— Pour tout $n \in \mathbb{N}$, une *$\mathcal{M}$-relation* n-aire est une partie de $\mathcal{M}^n$ qui est un $\mathcal{M}$-ensemble,

— Pour tous $\mathcal{M}$-ensembles x et y, une *$\mathcal{M}$-fonction* de x dans y est une fonction de x dans y qui est un $\mathcal{M}$-ensemble,

— Pour tout $n \in \mathbb{N}$, une *$\mathcal{M}$-relationnelle* n-aire est une partie de $\mathcal{M}^n$ qui est une $\mathcal{M}$-classe,

— Pour toutes $\mathcal{M}$-classes X et Y, une *$\mathcal{M}$-fonctionnelle* de X dans Y est une fonction de X dans Y qui est une $\mathcal{M}$-classe.

Remarquons qu'une partie d'un $\mathcal{M}$-ensemble n'est pas nécessairement un $\mathcal{M}$-ensemble et qu'une fonction d'un $\mathcal{M}$-ensemble dans un $\mathcal{M}$-ensemble n'est pas nécessairement une $\mathcal{M}$-fonction.

Définition B.3. Un *ordinal* est un ensemble transitif bien ordonné par la relation d'appartenance, c'est-à-dire un ensemble α tel que :

— pour tout $x \in \alpha$, $x \subseteq \alpha$,

— pour tout $x \in \alpha$, $x \notin x$,

— pour tout $x \in \alpha$, pour tout $y \in x$, $y \subseteq x$,

— pour tout $Z \subseteq \alpha$ non vide, il existe $x \in Z$ tel que pour tout $y \in Z \setminus \{x\}$, $x \in y$.

Étant donnés deux ordinaux α et β, on note $\alpha < \beta$ pour $\alpha \in \beta$ et $\alpha \leq \beta$ pour $\alpha \subseteq \beta$ (ce qui est équivalent à $\alpha < \beta$ ou $\alpha = \beta$).

Un *$\mathcal{M}$-ordinal* est un ordinal qui est un $\mathcal{M}$-ensemble.

Comme $\mathcal{M}$ est bien-fondé, on peut montrer qu'un $\mathcal{M}$-ensemble α est un $\mathcal{M}$-ordinal si et seulement si :

— pour tout $x \in \alpha$, $x \subseteq \alpha$,

— pour tous $x, y \in \alpha$, on a $x \in y$ ou $x = y$ ou $y \in x$.

Définition B.4. Un *cardinal* est un ordinal κ tel que pour tout ordinal $\alpha < \kappa$, il n'existe pas de fonction surjective de α sur κ.

Un $\mathcal{M}$*-cardinal* est un $\mathcal{M}$-ordinal κ tel que pour tout $\mathcal{M}$-ordinal $\alpha < \kappa$, il n'existe pas de $\mathcal{M}$-fonction surjective de α sur κ.

Remarquons qu'un $\mathcal{M}$-ensemble qui est un cardinal est en particulier un $\mathcal{M}$-cardinal, mais qu'un $\mathcal{M}$-cardinal n'est pas nécessairement un cardinal.

Définition B.5. Deux ensemble x et y sont *équipotents* s'il existe une bijection entre x et y.

Deux $\mathcal{M}$-ensembles x et y sont $\mathcal{M}$*-équipotents* s'il existe une $\mathcal{M}$-bijection (c'est-à-dire une $\mathcal{M}$-fonction bijective) entre x et y.

Soit x un ensemble. S'il existe un cardinal équipotent à x, celui-ci est unique : on l'appelle le *cardinal de* x.

Soit x un $\mathcal{M}$-ensemble. S'il existe un $\mathcal{M}$-cardinal $\mathcal{M}$-équipotent à x, celui-ci est unique : on l'appelle le $\mathcal{M}$*-cardinal de* x.

Définition B.6. On dit que $\mathcal{M}$ vérifie l'*axiome du choix global* s'il existe une $\mathcal{M}$-fonctionnelle $\epsilon_{\mathcal{M}} : \mathcal{M} \setminus \{\emptyset\} \to \mathcal{M}$ telle que pour tout $x \in \mathcal{M} \setminus \{\emptyset\}$, $\epsilon_{\mathcal{M}}(x) \in x$.

Proposition B.7 (Théorème de Zermelo)**.** Si $\mathcal{M}$ vérifie l'axiome du choix global, tout $\mathcal{M}$-ensemble est $\mathcal{M}$-équipotent à un unique $\mathcal{M}$-cardinal.

Références

[Ber76] G. Berry. Bottom-up computation of recursive programs. *RAIRO - Theoretical Informatics and Applications - Informatique Théorique et Applications*, 10(R1) :47–82, 1976.

[GH08] S. Givant and P. Halmos. *Introduction to Boolean Algebras*. Undergraduate Texts in Mathematics. Springer New York, 2008.

[Gö40] Kurt Gödel. *The Consistency of the Axiom of Choice and of the Generalized Continuum Hypothesis with the Axioms of Set Theory*. Princeton University Press, 1940.

[Jec73] Thomas Jech. *The Axiom of Choice*. North Holland, 1973.

[Kle52] S. Kleene. Introduction to Metamathematics, 1952.

[Kri03] Jean-Louis Krivine. Dependent choice, 'quote' and the clock. *Theor. Comput. Sci.*, 308(1-3) :259–276, November 2003.

[Kri12] Jean-Louis Krivine. Realizability algebras II : new models of ZF + DC. *Logical Methods in Computer Science*, 8(1 :10) :1–28, February 2012.

[Kri15] Jean-Louis Krivine. On the structure of classical realizability models of ZF. In *Proceedings TYPES 2014 - LIPIcs*, volume 39, pages 146–161, 2015.

[Kri18] Jean-Louis Krivine. Realizability algebras III : some examples. *Mathematical Structures in Computer Science*, 28(1) :45–76, 2018.

[Plo77] G.D. Plotkin. LCF considered as a programming language. *Theoretical Computer Science*, 5(3) :223 – 255, 1977.

[RC02] Donald H. Pelletier Rene Cori, Daniel Lascar. *Mathematical Logic : A Course with Exercises Part I : Propositional Calculus, Boolean Algebras, Predicate Calculus, Completeness Theorems*. Oxford University Press, USA, 2002.

[SR98] Th. Streicher and B. Reus. Classical logic, continuation semantics and abstract machines. *J. Funct. Program.*, 8(6) :543–572, November 1998.

[Tra74] Mark B Trakhtenbrot. On representation of sequential and parallel functions. In *International Symposium on Mathematical Foundations of Computer Science*, pages 411–417. Springer, 1975, Russian version 1974.