(1) Dynkes – Février 2012 – Nancy

(1) <u>"Arrow logic" associative</u>

VARPRO = ensemble des variables propositionnelles
Énumération : $(p_1, p_2, \ldots)$
FOR = ensemble des formules.

<u>Syntaxe</u>

$$\phi ::= p \mid \bot \mid \neg\phi \mid (\phi \vee \psi) \mid (\phi \circ \psi).$$

$$(\phi \bullet \psi) := \neg(\neg\phi \circ \neg\psi).$$

JoLLI 4 (1995) 191-20

Référence principale : Kurucz, Németi, Sain, Simon
Decidable and undecidable logics with a binary modality.

②

Sémantique

$\underline{B} = (\underbrace{B, \emptyset_B, \neg_B, \cup_B}_{\text{algèbre de Boole}}, \underbrace{\circ_B}_{\text{opérateur binaire sur } B})$, algèbre de Boole avec opérateur binaire,

$$(a \circ_B b) \circ_B c = a \circ_B (b \circ_B c),$$

$$(a \cup_B b) \circ_B c = (a \circ_B c) \cup_B (b \circ_B c),$$

$$a \circ_B (b \cup_B c) = (a \circ_B b) \cup_B (a \circ_B c),$$

$$\emptyset_B \circ_B a = \emptyset_B,$$

$$a \circ_B \emptyset_B = \emptyset_B .$$

$I : p \longmapsto I(p) \in B$,

$\bar{I}(p) = I(p)$, $\bar{I}(\bot) = \emptyset_B$, $\bar{I}(\neg\phi) = \neg_B \bar{I}(\phi)$, $\bar{I}(\phi \vee \psi) = \bar{I}(\phi) \cup_B \bar{I}(\psi)$, $\bar{I}(\phi \circ \psi) = \bar{I}(\phi) \circ_B \bar{I}(\psi)$,

$\underline{B}, I \models \phi \iff \bar{I}(\phi) = 1_B$, $\underline{B} \models \phi \iff \forall I, \underline{B}, I \models \phi$, $\models \phi \iff \forall \underline{B}, \underline{B} \models \phi$.

Axiomatisation

Tautologies propositionnelles,

$\phi \circ (\psi \to \chi) \to (\phi \circ \psi \to \phi \circ \chi)$,

$(\phi \to \psi) \circ \chi \to (\phi \circ \chi \to \psi \circ \chi)$,

Modus Ponens,

$$\frac{\psi}{\phi \circ \psi}, \quad \frac{\phi}{\phi \circ \psi}, \qquad (\phi \circ \psi) \circ \chi \Longleftrightarrow \phi \circ (\psi \circ \chi).$$

Soit L l'ensemble des théorèmes.

Complétude

* Théorème 1 : $\boxed{\phi \in L \iff \models \phi, \quad \text{(Jónsson et Tarski, 1948)}}$.

Problème de décision

$\phi \in L \Rightarrow\ \models \phi$	facile : par induction
$\models \phi \Rightarrow B(L) \models \phi$	facile : par définition
$B(L) \models \phi \Rightarrow \phi \in L$	Lindenbaum–Tarski ($\simeq 1935$)

Entrée : ϕ,
Sortie : $\phi \in L$? $\models \phi$?

Ce problème est-il décidable ?

Roorda, D. Resource Logics. Proof-Theoretical Investigations. Thèse de l'université d'Amsterdam (1991).

Algèbre de Lindenbaum–Tarski de L

Soit $\equiv$ la relation d'équivalence sur l'ensemble des formules définies par :

$$\phi \equiv_L \psi \iff (\phi \longleftrightarrow \psi) \in L.$$

* Lemme 2 : $\equiv_L$ est une congruence sur l'ensemble des formules.

Soit $\underline{B(L)} = (B(L), \ominus_{B(L)}, \bar{\ }_{B(L)}, \cup_{B(L)}, 0_{B(L)})$ la structure algébrique définie par :

$B(L) = FOR/_{\equiv_L}$, $0_{B(L)} = |\bot|_{\equiv_L}$, $\neg_{B(L)} |\phi|_{\equiv_L} = |\neg\phi|_{\equiv_L}$, $|\phi|_{\equiv_L} \cup_{B(L)} |\psi|_{\equiv_L} = |\phi \vee \psi|_{\equiv_L}$, $|\phi|_{\equiv_L} \circ_{B(L)} |\psi|_{\equiv_L} = |\phi \circ \psi|_{\equiv_L}$.

Théorème 3 : $\underline{B(L)}$ est une algèbre de Boole avec opérateur binaire telle que :

$\phi \in L \Leftrightarrow \underline{B(L)} \models \phi$.
(Lindenbaum et Tarski, $\simeq$ 1935).

(2) Quasiéquations dans les semigroupes

Syntaxe

VARIND = ensemble des variables individuelles
Enumération : $(x_1, x_2, \ldots)$.

Termes : $t ::= x \mid (t \circ u)$.

TER = ensemble des termes

Equations : $t = u$.

Quasiéquations : $t_1 = u_1 \,\&\, \ldots \,\&\, t_n = u_n \Rightarrow t_0 = u_0$.

Sémantique

Semigroupes : $\underline{S} = (S, \circ_S)$ où S est un ensemble non vide $\circ_S$ est une opération binaire associative sur S.

$I : x \mapsto I(x) \in S$,

$\bar{I}(x) = I(x)$, $\bar{I}(t \circ u) = \bar{I}(t) \circ_S \bar{I}(u)$,

(5) $\models q \Rightarrow B(L) \models \phi(q) \Rightarrow \phi(q) \in L \Rightarrow \models \phi(q) \Rightarrow \models q$

Th5   Lindenbaum-Tarski   sound   Th 6

$\underline{S}, I \models t = u \Leftrightarrow \bar{I}(t) = \bar{I}(u)$, $\underline{S}, I \models t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0 \Leftrightarrow (\underline{S}, I \models t_1 = u_1, \dots, \underline{S}, I \models t_n = u_n \Rightarrow \underline{S}, I \models t_0 = u_0)$, $\underline{S} \models t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0 \Leftrightarrow \forall I,\ \underline{S}, I \models t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0$, $\models t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0 \Leftrightarrow \forall \underline{S},\ \underline{S} \models t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0$.

Problème de décision (Post)

Entrée : $t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0$,
Sortie : $\models t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0$?

* Théorème 4 : Ce problème est indécidable, (Post 1947).

(3) Réduction du problème de Post au problème de l'appartenance des formules à L.

Soit $q = (t_1 = u_1 \,\&\dots\&\, t_n = u_n \Rightarrow t_0 = u_0)$ une quasiéquation.

Traduction des termes vers les formules

$\phi(x_i) = p_i$, $\phi(t \circ u) = \phi(t) \circ \phi(u)$.

Soit $\tau = (\phi(t_1) \oplus \phi(u_1)) \vee \dots \vee (\phi(t_n) \oplus \phi(u_n))$.

Soit $\tau^+ = \tau \vee (T \circ \tau) \vee (\tau \circ T) \vee (T \circ \tau \circ T)$.

Soit $\phi(q) = (\phi(t_0) \oplus \phi(u_0)) \to \tau^+$.

* Théorème 5 : $\boxed{\models q \Rightarrow B(L) \models \phi(q)}$

Démonstration : Supposons que [redacted] $\underline{B(L)} \nVdash \phi(q)$. Par conséquent, il existe

$I : p_i \longmapsto I(p_i) \in B(L)$ telle que $\underline{B(L)}, I \nVdash \phi(q)$.

Donc $\overline{I}(\phi(q)) \neq 1_{B(L)}$. Soit $\underline{S} = (S, \circ_S)$ la structure algébrique définie par :

$$S = \{ |\phi \vee \tau^+|_{\equiv_L} : \phi \text{ est une formule quelconque} \},$$

$$|\phi \vee \tau^+|_{\equiv_L} \circ_S |\psi \vee \tau^+|_{\equiv_L} = \text{[redacted]}$$
$$|\phi \circ \psi \vee \tau^+|_{\equiv_L}.$$

Montrons que cela définit bien un semigroupe.
Soit ϕ, ψ, ϕ', ψ' des formules telles que

artie où est
tilisée l'as-
ociativité

$$(\phi \vee \tau^+ \leftrightarrow \phi' \vee \tau^+) \in L \text{ et } (\psi \vee \tau^+ \leftrightarrow \psi' \vee \tau^+) \in L.$$

Donc $\big(((\phi \vee \tau^+) \circ (\psi \vee \tau^+)) \vee \tau^+ \leftrightarrow ((\phi' \vee \tau^+) \circ (\psi' \vee \tau^+)) \vee \tau^+\big) \in L$

Donc
$$\begin{array}{l} (\phi \circ \psi \vee \tau^+) \vee (\phi \circ \tau^+ \vee \tau^+ \circ \psi \vee \tau^+ \circ \tau^+) \leftrightarrow \\ (\phi' \circ \psi' \vee \tau^+) \vee (\phi' \circ \tau^+ \vee \tau^+ \circ \psi' \vee \tau^+ \circ \tau^+) \end{array} \in L.$$

Or $\tau^+ \vee \phi \circ \tau^+ \vee \tau^+ \circ \psi \vee \tau^+ \circ \tau^+ \leftrightarrow \tau^+ \quad \in L$
et $\tau^+ \vee \phi' \circ \tau^+ \vee \tau^+ \circ \psi' \vee \tau^+ \circ \tau^+ \leftrightarrow \tau^+ \quad \in L$.

Donc $\circ_S$ est bien défini. Montrons que $\circ_S$ est une opération

(7)

Partie où est utilisée l'associativité.

associative: $\left(|\phi \vee \tau^+|_{\equiv_L} \circ_S |\psi \vee \tau^+|_{\equiv_L}\right) \circ_S |\chi \vee \tau^+|_{\equiv_L} =$

$|\phi \circ \psi \vee \tau^+|_{\equiv_L} \circ_S |\chi \vee \tau^+|_{\equiv_L} = |(\phi \circ \psi) \circ \chi \vee \tau^+|_{\equiv_L} =$

$= |\phi \circ (\psi \circ \chi) \vee \tau^+|_{\equiv_L} = |\phi \vee \tau^+|_{\equiv_L} \circ_S |\psi \circ \chi \vee \tau^+|_{\equiv_L} =$

$|\phi \vee \tau^+|_{\equiv_L} \circ_S (|\psi \vee \tau^+|_{\equiv_L} \circ_S |\chi \vee \tau^+|_{\equiv_L})$.

Soit $I : x_i \mapsto |p_i \vee \tau^+|_{\equiv_L}$.

Montrons que pour tout terme t, $\overline{I}(t) = |\phi(t) \vee \tau^+|_{\equiv_L}$.

$\overline{I}(x_i) = I(x_i) = |p_i \vee \tau^+|_{\equiv_L} = |\phi(x_i) \vee \tau^+|_{\equiv_L}$.

$\overline{I}(t \circ u) = \overline{I}(t) \circ_S \overline{I}(u) = |\phi(t) \vee \tau^+|_{\equiv_L} \circ_S |\phi(u) \vee \tau^+|_{\equiv_L} =$

$|\phi(t) \circ \phi(u) \vee \tau^+|_{\equiv_L} = |\phi(t \circ u) \vee \tau^+|_{\equiv_L}$.

Montrons que $\underline{S}, I \not\models q$.

Si $\underline{S}, I \models t_i = u_i$ pour $i = 1..n$ alors $\overline{I}(t_i) \neq \overline{I}(u_i)$ et

$|\phi(t_i) \vee \tau^+|_{\equiv_L} \neq |\phi(u_i) \vee \tau^+|_{\equiv_L}$. Donc $(\phi(t_i) \vee \tau^+) \leftrightarrow$

$(\phi(u_i) \vee \tau^+) \notin L$. Or, τ^+ est de la forme $\phi(t_i) \oplus \phi(u_i)$

$\vee\, \tau^0$. Donc $(\phi(t_i) \vee \tau^+) \leftrightarrow (\phi(t_i) \vee \phi(t_i) \oplus \phi(u_i)$

$\vee\, \tau^0) \leftrightarrow (\phi(t_i) \vee \phi(u_i) \vee \tau^0) \leftrightarrow (\phi(u_i) \vee \phi(t_i) \vee \tau^0)$

$\leftrightarrow (\phi(u_i) \vee \phi(t_i) \oplus \phi(u_i) \vee \tau^0) \leftrightarrow (\phi(u_i) \vee \tau^+) \in L$: une contradiction. Donc $\underline{S}, I \models t_i = u_i$ pour $i = 1 \sim n$.

Si $\underline{S}, I \models t_0 = u_0$ alors $\bar{I}(t_0) = \bar{I}(u_0)$ et

$|\phi(t_0) \vee \tau^+|_{\equiv_L} = |\phi(u_0) \vee \tau^+|_{\equiv_L}$. Donc $(\phi(t_0) \vee \tau^+) \Longleftrightarrow$

$(\phi(u_0) \vee \tau^+) \in L$. Donc $(\phi(t_0) \oplus \phi(u_0) \to \tau^+) \in L$:

une contradiction.

* Théorème 6 : $\boxed{\vdash \phi(q) \Rightarrow\ \models q.}$

Démonstration : Supposons que $\not\models q$. Par suite, il existe un semigroupe $\underline{S} = (S, \circ_S)$ tel que $\underline{S} \not\models q$. Par conséquent, il existe $I : x \mapsto I(x) \in S$ telle que $\underline{S}, I \not\models q$, i.e. $\bar{I}(t_1) = \bar{I}(u_1), \ldots, \bar{I}(t_n) = \bar{I}(u_n)$ et $\bar{I}(t_0) \neq \bar{I}(u_0)$.

Soit $\underline{S'} = (S', \circ_{S'})$ où $S' = S \cup \{e\}$ (avec $e \notin S$) et

* $a \circ_{S'} b = \left\| \begin{array}{l} \text{si } a \in S',\ b \in S' \text{ alors } a \circ_S b, \\ \text{si } a \in S',\ b = e \text{ alors } a, \\ \text{si } a = e,\ b \in S \text{ alors } b, \\ \text{si } a = e,\ b = e \text{ alors } e. \end{array} \right.$

Note : S' est un semigroupe et $h_1 : a \in S \mapsto h_1(a) = a \in S'$ est telle que : (h_1 est un homomorphisme injectif)

$$\left\| \begin{array}{l} h_1(a) = h_1(b) \Rightarrow a = b, \\ h_1(a \circ_S b) = h_1(a) \circ_{S'} h_1(b). \end{array} \right.$$

(9)

Pour chaque a dans S', soit $R_a = \{(b, b \circ_{S'} a) : b \in S'\}$

Soit $\underline{\mathcal{R}} = (\mathcal{R}, \circ_{\mathcal{R}})$ où $\mathcal{R} = \{R_a : a \in S'\}$ et $\circ_{\mathcal{R}}$ est la composition (habituelle) des relations binaires sur S'.

Note : $\underline{\mathcal{R}}$ est un semigroupe et $h_2 : a \in S' \mapsto h_2(a) = R_a \in \mathcal{R}$ est telle que : (h_2 est un homomorphisme injectif)

$$\left\| \begin{array}{l} h_2(a) = h_2(b) \Rightarrow a = b \\ h_2(a \circ_{S'} b) = h_2(a) \circ_{\mathcal{R}} h_2(b). \end{array} \right.$$

Soit $\underline{B} = (B, \mathcal{O}_B, \neg_B, \cup_B, \circ_B)$ où

$B = \mathcal{P}(S' \times S')$ est l'ensemble des relations binaires sur S'

$$\begin{array}{l} \mathcal{O}_B = \emptyset \\ \neg_B R = S' \times S' \setminus R \\ R_1 \cup_B R_2 = R_1 \cup R_2 \\ R_1 \circ_B R_2 = \{(a,b) \in S' \times S' : \exists c \in S' \mid (a,c) \in R_1 \,\&\, (c,b) \in R_2\} \end{array}$$

Note : $\underline{B}$ est une algèbre de Boole avec opérateur binaire telle que $h_3 : R_a \in \mathcal{R} \longmapsto h_3(R_a) = R_a \in B$ est telle que (h_3 est un homomorphisme injectif)

$$\left\| \begin{array}{l} h_3(R_a) = h_3(R_b) \Rightarrow R_a = R_b \\ h_3(R_a \circ_{\mathcal{R}} R_b) = h_3(R_a) \circ_B h_3(R_b). \end{array} \right.$$

Soit $h : a \in S \longmapsto h(a) = h_3(h_2(h_1(a))) = R_a \in B$.

On a :

Représentation de | Cayley (groupes) : 1850/1860
| Hall (semigroups) : 1959.

$$\left\| \begin{array}{l} h(a) = h(b) \Rightarrow a = b, \\ h(a \circ_S b) = h(a) \circ_B h(b). \end{array} \right.$$

h est un homomorphisme injectif,

Soit $I' : p_i \mapsto I'(p_i) = h(I(x_i)) \in B$.

I' est une interprétation sur $\underline{B}$. Montrons que pour tout terme t, $h(\overline{I}(t)) = \overline{I'}(\phi(t))$.

$$h(\overline{I}(x_i)) = h(I(x_i)) = I'(p_i) = \overline{I'}(p_i) = \overline{I'}(\phi(x_i)).$$

$$h(\overline{I}(t \circ u)) = h(\overline{I}(t) \circ_S \overline{I}(u)) = h(\overline{I}(t)) \circ_B h(\overline{I}(u))$$
$$= \overline{I'}(\phi(t)) \circ_B \overline{I'}(\phi(u)) = \overline{I'}(\phi(t) \circ \phi(u)) = \overline{I'}(\phi(t \circ u)).$$

Montrons que $\underline{B}, I' \not\models \phi(q)$. Pour cela, il suffit de montrer que $\overline{I'}(\phi(t_1)) = \overline{I'}(\phi(u_1))$, ..., $\overline{I'}(\phi(t_n)) = \overline{I'}(\phi(u_n))$ et $\overline{I'}(\phi(t_0)) \neq \overline{I'}(\phi(u_0))$.

Notons que pour chaque $i = 1..n$, $\overline{I'}(\phi(t_i)) = h(\overline{I}(t_i)) = h(\overline{I}(u_i)) = \overline{I'}(\phi(u_i))$.

De plus $\overline{I'}(\phi(t_0)) = h(\overline{I}(t_0)) \neq h(\overline{I}(u_0)) = \overline{I'}(\phi(u_0))$.

Donc $\underline{B}, I' \not\models \phi(q)$, $\underline{B} \not\models \phi(q)$ et $\not\models \phi(q)$.