Допустимые правила вывода в интуиционистской логике высказываний IPC

Лукашов Никита
lnv619@gmail.com

Национальный исследовательский университет
«Высшая школа экономики»

16 февраля 2024 год

$$\mathcal{A} \mathrel{|\!\sim}_{\mathrm{IPC}} \mathcal{B}$$

Аксиоматика IPC

Язык IPC

- переменные $p_1, p_2, \ldots$;
- константы $\top$ и $\bot$;
- булевы связки $\wedge, \vee \to$.

- $\neg A = (A \to \bot)$
- $A, B, C, \ldots$ — формулы;
- $\Gamma, \Delta, \ldots$ — множества формул.

Аксиоматика IPC

Аксиомы:

1. $A \to (B \to A)$;
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$;
3. $(A \wedge B) \to A$;
4. $(A \wedge B) \to B$;
5. $A \to (B \to (A \wedge B))$;
6. $A \to (A \vee B)$;
7. $B \to (A \vee B)$;
8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$;
9. $\perp \to A$.

Правила вывода:

- *modus ponens* $(A, A \to B / B)$

Выводимость из гипотез

Определение

$\Gamma \vdash_{\mathrm{IPC}} A \Leftrightarrow \exists A_1, A_2, \ldots, A_n$, такая что $A_n = A$ каждая формула A_i является либо аксиомой, либо формулой из Γ, либо получена из двух ей предшествующих по правилу *modus ponens*.

Теорема о дедукции

$\Gamma, A \vdash_{\mathrm{IPC}} B \Leftrightarrow \ \Gamma \vdash_{\mathrm{IPC}} A \to B$.

Семантика Крипке

Определение

Пара $\mathcal{F} = \langle W, \leqslant \rangle$, где $\leqslant$ — рефлексивное и транзитивное отношение на W, называется шкалой Крипке.
Тройка $\mathcal{W} = \langle W, \leqslant, \Vdash \rangle$ называется моделью Крипке, если $\langle W, \leqslant \rangle$ — шкала Крипке и $\Vdash$ удовлетворяет следующим условиям:

- $\forall p \in \mathrm{Var}, w \leqslant v \; (w \Vdash p \Rightarrow v \Vdash p)$;
- $w \Vdash A \wedge B \Leftrightarrow (w \Vdash A$ и $w \Vdash B)$;
- $w \Vdash A \vee B \Leftrightarrow (w \Vdash A$ или $w \Vdash B)$;
- $w \Vdash A \to B \Leftrightarrow \forall w \leqslant v \; (v \Vdash A \Rightarrow v \Vdash B)$;
- $w \nVdash \bot$.

- $\mathcal{W} \vDash A \Leftrightarrow \forall x \in \mathcal{W} \; (\mathcal{W}, x \Vdash A)$.
- $\mathcal{W}_x = \{v | x \leqslant v\}$ — пораждённая подмодель; мир x называется корнем модели $\mathcal{W}_x$.

Корректность и полнота

Лемма о монотонности

Если $w \Vdash A$, то $\forall w \leqslant v\ (v \Vdash A)$.

Теорема

1. $\mathrm{IPC} \vdash A \Rightarrow (\mathcal{W} \vDash A$ для любой модели Крипке $\mathcal{W})$;
2. $\mathrm{IPC} \nvdash A \Rightarrow \exists \mathcal{W}$— конечная модель Крипке с корнем r $(\mathcal{W}, r \nVdash A)$.

Дизъюнктивное свойство

Если $\mathrm{IPC} \vdash A \vee B$, то $\mathrm{IPC} \vdash A$ или $\mathrm{IPC} \vdash B$.

Подстановки

Определение

Подстановкой σ называется функция $\sigma : \mathrm{Var} \to Form(L)$.

- $\sigma(A(\overrightarrow{p})) := A(p_1/\sigma(p_1), \ldots, p_n/\sigma(p_n)) \Rightarrow \sigma : Form(L) \to Form(L)$;
- $(\tau\sigma)(p) = \tau(\sigma(p))$ для всех $p \in \mathrm{Var}$;
- σ — унификатор для $\varphi(\overrightarrow{p})$ в $L \Leftrightarrow \vdash_L \sigma(\varphi)$.

Теорема о подстановке

Для любой подстановки σ:

$$\Gamma \vdash_{\mathrm{IPC}} A \Rightarrow \sigma(\Gamma) \vdash_{\mathrm{IPC}} \sigma(A).$$

Выводимые и допустимые правила вывода

Запись Γ/A, где Γ — конечное множество формул и A — формула, называется **правилом**.

Определение

- Правило вывода Γ/A называется выводимым в логике L, если $\Gamma \vdash_L A$.
- Правило вывода Γ/A называется допустимым в логике L (обозначение $\Gamma \mathrel{|\!\!\sim}_L A$), если любой унификатор формул из множества Γ также является унификатор формулы A.

Примеры

В IPC:

- $\dfrac{p \to r, q \to r}{(p \lor q) \to r}$
- $\dfrac{\neg p \lor \neg q}{\neg(p \land q)}$
- $\dfrac{\neg\neg\neg p}{\neg p}$

— примеры выводимых правил.

Выводимые и допустимые правила вывода

Предложение

Любое выводимое правило является допустимым.

Доказательство

Теорема о подстановке.

Замечание

Для классической логики PC верно обратное: любое допустимое правило является выводимым.

Выводимые и допустимые правила вывода

Вопрос

Существуют ли допустимые, но невыводимые правила в IPC?

Ответ

Да, существуют. Например, правило Харропа (1960 г.):

$$\frac{\neg p \to (q \vee r)}{(\neg p \to q) \vee (\neg p \to r)}.$$

Проблема допустимости

Вопрос (Х. Фридман, 1975 г.)

Является ли проблема допустимости правил в IPC разрешимой?

Ответ (В. В. Рыбаков, 1984 г.)

- Да, является.
- Допустимые правила в IPC не имеют конечного базиса.

Наблюдения

- $\Gamma \mathrel{|\!\!\sim}_{\mathrm{IPC}} A \Leftrightarrow \bigwedge \Gamma \mathrel{|\!\!\sim}_{\mathrm{IPC}} A$;
- $A \mathrel{|\!\!\sim}_L B \Rightarrow \sigma(A) \mathrel{|\!\!\sim}_L \sigma(B)$;
- $A \mathrel{|\!\!\sim}_L B, B \mathrel{|\!\!\sim}_L C \Rightarrow A \mathrel{|\!\!\sim}_L C$.

Базис допустимых правил вывода

Определение

Множество допустимых правил $\mathcal{R}$ называется базисом, если для любого допустимого правила $A_1, A_2, \ldots, A_n / B$ логики L существует последовательность формул $B_1, B_2, \ldots, B_k$, такая что $B_k = B$ и для каждого i выполнено одно из условий:

1. B_i является одной из формул $A_1, A_2, \ldots, A_n$;
2. найдутся такие $i_1, i_2, \ldots, i_m < i$, что $B_{i_1}, \ldots B_{i_m} \vdash_L B_i$;
3. найдутся такие $i_1, i_2, \ldots, i_m < i$, что $B_{i_1}, \ldots B_{i_m} / B_i$ является подстановочным примером некоторого правила из множества $\mathcal{R}$.

Существование базиса

Гипотеза (де Йонг и А. Виссер)

$$\frac{(\bigwedge_{i=1}^{n}(p_i \to q_i) \to p_{n+1} \vee p_{n+2}) \vee r}{\bigvee_{j=1}^{n+2}(\bigwedge_{i=1}^{n}(p_i \to q_i) \to p_j) \vee r}\,(V_n)$$

образуют базис допустимых правил в IPC.

Замечание

Правило Харропа — *идейный вдохновитель* (V_n):

$$\frac{\neg p \to (q \vee r)}{(\neg p \to q) \vee (\neg p \to r)} = \frac{(p \to \bot) \to (q \vee r)}{((p \to \bot) \to q) \vee ((p \to \bot) \to r)}$$

Существование базиса

Наблюдение

Если логика L обладает дизъюнктивным свойством, то

$$A \mathrel{|\!\!\sim_L} C, B \mathrel{|\!\!\sim_L} C \Rightarrow A \vee B \mathrel{|\!\!\sim_L} C.$$

Теорема (П. Розьер, 1991 г. и Р. Имхофф, 1999 г.)

$$\frac{(\bigwedge_{i=1}^{n}(p_i \to q_i) \to p_{n+1} \vee p_{n+2}) \vee r}{\bigvee_{j=1}^{n+2}(\bigwedge_{i=1}^{n}(p_i \to q_i) \to p_j) \vee r}\,(V_n)$$

образуют базис допустимых правил в IPC.

Проективность

Определение

Формула A называется проективной в логике L, если для неё существует унификатор σ, такой что для любого $p \in \mathrm{Var}$:

$$A \vdash_L \sigma(p) \leftrightarrow p. \tag{P}$$

- (P) $\Leftrightarrow$ $A \vdash_L \sigma(B) \leftrightarrow B$ для любой $B \in Form(L)$

Примеры

- $A = p$;
- $A = \neg p$;
- $A = B \to p$.

$\sigma(p) = \top$, $\sigma(p) = \bot$ и $\sigma(p) = (B \to p) \to p$ их проективные унификаторы соответственно.

Свойство расширения

Определения

Вариантом модели Крипке $\mathcal{W} = \langle W, r \rangle$ называется модель Крипке $\mathcal{W}' = \langle W, r \rangle$, что $\mathcal{W}, w \Vdash p \Leftrightarrow \mathcal{W}', w \Vdash p$ для всех миров $w \neq r$.

Класс K обладает свойством расширения, если для любой модели Крипке $\mathcal{W}$, такой что $\mathcal{W}_w \in K$ для всех $w \neq r$, найдётся её вариант $\mathcal{W}' \in K$.

Теорема (С. Гилярди, 1999 г.)

Формула A проективна в IPC тогда и только тогда, когда класс её моделей Крипке $MOD(A) = \{\mathcal{W} \mid \mathcal{W} \vDash A\}$ обладает свойством расширения.

- $p \vee q$ не проективна
- посылки (V_n) тоже не проективны

Проективная аппроксимация

Определение

Проективной аппроксимацией Π_A формулы $A(\bar{p})$ называется множество формул, такое что для любой $B \in \Pi_A$:

1. $B \in Form(\bar{p}), n(B) \leqslant n(A)$, B — проективна и $B \vdash_{\mathrm{IPC}} A$;
2. для любой C с условием (1) найдётся $B \in \Pi_A$, т. ч. $C \vdash_{\mathrm{IPC}} B$.

Наблюдения

1. Для любой *проективной* формулы A: $A \mathrel{|\!\!\sim}_{\mathrm{IPC}} B \Leftrightarrow A \vdash_{\mathrm{IPC}} B$.
2. Для *любой* формулы A:
   - $\bigvee \Pi_A \mathrel{|\!\!\sim}_{\mathrm{IPC}} A$;
   - $\bigvee \Pi_A \mathrel{|\!\!\sim}_{\mathrm{IPC}} B \;\Leftrightarrow\; \bigvee \Pi_A \vdash_{\mathrm{IPC}} B$.

Проективная аппроксимация

Теорема (С. Гилярди, 1999 г.)

Для любой формулы A в IPC существует конечная проективная аппрокксимация Π_A. Более того, её можно построить так, что для любого унификатора σ для A найдётся формула $B \in \Pi_A$, для которой σ является также унификатором.Иными словами, $A \mathrel{|\!\!\sim}_{\mathrm{IPC}} \bigvee \Pi_A$.

Разрешимость проблемы допустимости в IPC

Пусть $A \mathrel{|\!\!\sim}_{\mathrm{IPC}} B$. Тогда:

$$\bigvee \Pi_A \mathrel{|\!\!\sim}_{\mathrm{IPC}} A \;\Rightarrow\; \bigvee \Pi_A \mathrel{|\!\!\sim}_{\mathrm{IPC}} B \;\Leftrightarrow\; \bigvee \Pi_A \vdash_{\mathrm{IPC}} B.$$

AR-система

- $A \rhd B$ — секвенты.

AR-система

Схемы аксиом:

$$V \quad (\bigwedge_{i=1}^{n}(p_i \to q_i) \to p_{n+1} \vee p_{n+2}) \vee r \rhd \bigvee_{i=1}^{n+2}(\bigwedge_{i=1}^{n}(p_i \to q_i) \to p_j) \vee r$$

I $\quad A \rhd B$, если $A \vdash_{\mathrm{IPC}} B$.

Правила:

$$Conj\ \frac{C \rhd A \quad C \rhd B}{C \rhd A \wedge B} \qquad Cut\ \frac{A \rhd B \quad B \rhd C}{A \rhd C}$$

$$Disj?\ \frac{A \rhd C \quad B \rhd C}{A \vee B \rhd C}$$

Корректность и полнота AR-системы

Лемма

Если AR $\vdash A \rhd C$ и AR $\vdash B \rhd C$, то AR $\vdash A \vee B \rhd C$.

Определение

AR-моделью назовём модель Крипке $\mathcal{W}$ с корнем, такую что для любого конечного множества миров $\{v_1, \ldots, v_n\} \subset \mathcal{W}$ найдётся *непосредственный предшественник*,т. е. такой мир v, что

$$(v \leqslant v_1, \ldots, v \leqslant v_n) \ \& \ \forall v \leqslant v' \, (v_i \leqslant v' \text{для некоторого } i).$$

Предложение (Р. Имхофф)

AR $\vdash A \rhd B$ тогда и только тогда, когда для любой AR-модели $\mathcal{W}$

$$\mathcal{W} \vDash A \Rightarrow \mathcal{W} \vDash B.$$

На пути к базису

Следствие из результатов С. Гилярди

Если $A \mathrel{|\!\sim}_{\mathrm{IPC}} B$, то для любого стабильного класса моделей Крипке K, обладающим свойством расширения, выполнено:

$$K \subseteq MOD(A) \;\Rightarrow\; K \subseteq MOD(B).$$

Предложение (Р. Имхофф)

1. Для любой AR-модели $\mathcal{W}$ найдётся стабильный класс K конечных моделей Крипке с корнем, обладающий свойством расширения и

$$\text{для всех } A \in Form(\bar{p}),\ \text{т. ч. } n(A) \leqslant k:\ \mathcal{W} \vDash A \Leftrightarrow K \vDash A. \qquad (*)$$

2. Для любого стабильного класса K конечных моделей Крипке с корнем, обладающего свойством расширения, найдётся AR-модель $\mathcal{W}$, такая что выполнено то же условие $(*)$.

Доказательство существования базиса

Следствие (Р. Имхофф)

Следующие утверждения эквиваленты:

1. B общезначима во всех AR-моделях, в которых общезначима A;
2. B общезначима в каждом стабильном классе конечных моделей Крипке с корнем, который обладает свойством расширения и в котором общезначима A.

Теорема (Р. Имхофф, 1999 г.)

$$A \mathrel{|\!\!\sim}_{\mathrm{IPC}} B \Leftrightarrow \mathsf{AR} \vdash A \rhd B.$$

Иными словами, (V_n) образуют базис допустимых правил логики IPC.

Список литературы

Silvio Ghilardi, Unification in intuitionistic logic, The Journal of Symbolic Logic **64** (1999), no. 2, 859–880.

Rosalie Iemhoff, On the admissible rules of intuitionistic propositional logic, The Journal of Symbolic Logic **66** (2001), no. 1, 281–294.

______, Intermediate logics and visser's rules, Notre Dame Journal of Formal Logic **46** (2005), no. 1, 65–81.

Paul Roziere, Admissible and derivable rules in intuitionistic logic, Mathematical Structures in Computer Science **3** (1993), no. 2, 129–136.

В. В. Рыбаков, Базисы допустимых правил логик s4 и int, Алгебра и логика **24** (1985), no. 1, 87–107.