Минимальная логика. Отрицание, конъюнкция, дизъюнкция

А.Н. Непейвода

2023 г.

Возникновение понятия типа

Изначально возник в трудах Б.Рассела, который заметил, что в наивной теории множеств существует парадокс:

Парадокс Рассела

$$\Omega = \{A \mid A \notin A\} \Rightarrow (\Omega \in \Omega \Leftrightarrow \Omega \notin \Omega)$$

Понятие типа ограничивает возможные операции над его сущностями $\Rightarrow$ исключает парадоксы (неверное поведение программ).

Определение типа

> Система типов — гибко управляемый синтаксический метод доказательства отсутствия в программе определенных видов поведения при помощи классификации выражений языка по разновидностям вычисляемых ими значений.
>
> Б.Пирс

В λ-исчислении типы — синтаксические конструкции, приписываемые термам по определенным правилам:

$$M : \sigma$$

Свойства типизации

- Статические vs динамические
- Явные vs неявные
- Сильные vs слабые

Сильные статические типы в функциональном языке ограничивают его синтаксические конструкции, но позволяют строить программы, которые уже частично верифицированы с помощью проверки типов.

Простые типы λ-исчисления

Определение

Множество типов $\mathbb{T}$ в $\lambda_{\to}$ определяется индуктивно.

- Переменные типа (α, β, γ etc) принадлежат $\mathbb{T}$.
- Если $\sigma \in \mathbb{T}$, $\phi \in \mathbb{T}$, то $(\sigma \to \phi) \in \mathbb{T}$.

Стрелка $\to$ правоассоциативна: $\sigma_1 \to \sigma_2 \to \ldots \sigma_n$ — сокращение для $\sigma_1 \to (\sigma_2 \to (\ldots \sigma_n) \ldots))$.
В силу наличия частичных вычислений тип $\sigma_1 \to \sigma_2 \ldots \to \sigma_n$ можно понимать как тип функции с $n-1$ аргументами типов $\sigma_1, \ldots, \sigma_{n-1}$ и типом результата σ_n; а можно как тип функции с одним аргументом σ_1 и типом результата — функцией с типом $\sigma_2 \to \ldots \to \sigma_n$ (а также все промежуточные варианты).

Полуформальный алгоритм типизации λ-функций

1. Если $M[x]$ имеет тип σ в контексте $x : \tau$, тогда естественно, что $\lambda x.M$ имеет тип $\tau \to \sigma$;
2. Если $(M\ N)$ имеет тип σ, а N имеет тип τ, тогда естественно, что M имеет тип $\sigma \to \tau$.

Полуформальный алгоритм типизации λ-функций

1. Если $M[x]$ имеет тип σ в контексте $x : \tau$, тогда естественно, что $\lambda x.M$ имеет тип $\tau \to \sigma$;
2. Если $(M\ N)$ имеет тип σ, а N имеет тип τ, тогда естественно, что M имеет тип $\sigma \to \tau$.

Логическая спецификация

$$\frac{\Gamma, x : \tau \vdash M : \sigma}{\Gamma \vdash \lambda x.M : \tau \to \sigma}$$

$$\frac{\Gamma \vdash M : \tau \to \sigma, \Gamma \vdash N : \tau}{\Gamma \vdash (M\ N) : \sigma}$$

Проблема типизации λ-функций

Рассмотрим терм $\lambda x.(x\ x)$. Какой у него тип?

Проблема типизации λ-функций

Рассмотрим терм $\lambda x.(x\ x)$. Какой у него тип?

- Пусть тип аргумента применения (то есть x) — это τ, а тип результата применения (то есть $(x\ x)$) — это σ. Тогда $\tau = \tau \to \sigma$. Ничего не напоминает?

Проблема типизации λ-функций

Рассмотрим терм $\lambda x.(x\ x)$. Какой у него тип?

- Пусть тип аргумента применения (то есть x) — это τ, а тип результата применения (то есть $(x\ x)$) — это σ. Тогда $\tau = \tau \rightarrow \sigma$. Ничего не напоминает?

Уравнение $\tau = \tau \rightarrow \sigma$ — это предложение Карри! Оно не имеет неподвижной точки, отличной от $\perp$.

Проблема типизации λ-функций

Рассмотрим терм $\lambda x.(x\ x)$. Какой у него тип?

- Пусть тип аргумента применения (то есть x) — это τ, а тип результата применения (то есть $(x\ x)$) — это σ. Тогда $\tau = \tau \to \sigma$. Ничего не напоминает?

Уравнение $\tau = \tau \to \sigma$ — это предложение Карри! Оно не имеет неподвижной точки, отличной от $\perp$.

Зацикливается не только унификация: см. $(\lambda x.(x\ x))\ (\lambda x.(x\ x))$. Иногда успешно вычисляется: напр. $(\lambda x.(x\ x))\ (\lambda x.(\lambda y.(y\ x)))$.

Проблема типизации λ-функций

Рассмотрим терм $\lambda x.(x\ x)$. Какой у него тип?

- Пусть тип аргумента применения (то есть x) — это τ, а тип результата применения (то есть $(x\ x)$) — это σ. Тогда $\tau = \tau \to \sigma$. Ничего не напоминает?

Уравнение $\tau = \tau \to \sigma$ — это предложение Карри! Оно не имеет неподвижной точки, отличной от $\perp$.

Зацикливается не только унификация: см. $(\lambda x.(x\ x))\ (\lambda x.(x\ x))$. Иногда успешно вычисляется: напр. $(\lambda x.(x\ x))\ (\lambda x.(\lambda y.(y\ x)))$.

$\lambda x.(x\ x)$ — частичная функция и не может быть конечным образом определена на всех полиморфных типах.

Просто типизированное λ-исчисление

Ограничим множество λ-термов только такими, типы которых всегда выводимы по описанным выше правилам.

$$\frac{\Gamma, x : \tau \vdash M : \sigma}{\Gamma \vdash \lambda x.M : \tau \to \sigma} \qquad \frac{\Gamma \vdash M : \tau \to \sigma, \Gamma \vdash N : \tau}{\Gamma \vdash (M\ N) : \sigma}$$

Просто типизированное λ-исчисление

Ограничим множество λ-термов только такими, типы которых всегда выводимы по описанным выше правилам.

$$\frac{\Gamma, x : \tau \vdash M : \sigma}{\Gamma \vdash \lambda x.M : \tau \to \sigma} \qquad \frac{\Gamma \vdash M : \tau \to \sigma, \Gamma \vdash N : \tau}{\Gamma \vdash (M\ N) : \sigma}$$

...а теперь забудем про термы и посмотрим только на типы. Что получилось?

$$\frac{\Gamma, \tau \vdash \sigma}{\Gamma \vdash \tau \to \sigma}$$ (правило введения импликации)

$$\frac{\Gamma \vdash \tau \to \sigma, \Gamma \vdash \tau}{\Gamma \vdash \sigma}$$ (правило удаления импликации aka *modus ponens*)

Связь логики и ФВП: соответствие Карри–Ховарда

- Существует взаимно-однозначное соответствие между типами замкнутых термов в просто типизированном λ-исчислении и тавтологиями в минимальной импликативной логике.
- (теорема о нормализации) Все термы просто типизированного λ-исчисления имеют нормальную форму.
- Доказательствам в минимальной логике соответствуют всюду определенные полиморфные функции высшего порядка.

Естественный вывод в форме Фитча

Правила вывода для $\Rightarrow$

Применению и абстракции соответствуют следующие правила вывода (modus ponens и правило дедукции):

$$(\;) : \;\frac{A \quad A \Rightarrow B}{B} \qquad\qquad \lambda. : \;\begin{array}{l} * A \\ \left| \; B \right. \\ \hline A \Rightarrow B \end{array}$$

Каждое применение правила вывода в доказательстве соответствует использованию в терме из $\lambda_{\rightarrow}$ конструкции с именем этого правила вывода.

В контексте соответствия Карри-Ховарда стрелочный тип далее обозначаем и как $\alpha \rightarrow \beta$, и как $\alpha \Rightarrow \beta$.

Вывод = конструкция

Покажем, что тип $((A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C) \Rightarrow C$ населён? то есть существует терм, имеющий такой тип. Поскольку это — функциональный тип, то внешним конструктором его терма будет абстракция (соответствует правилу дедукции).

$*(A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C$ (тип терма x)

(Тут нужно придумать, как построить терм типа C, имея только x)

C

$((A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C) \Rightarrow C$ (тип терма $\lambda x. \ldots$)

Поскольку x — это функциональный терм, принимающий аргументом функцию типа $\tau = A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$, нужно попробовать построить терм, имеющий тип τ. Для этого опять понадобится абстракция (даже две).

Вывод = конструкция

$*(A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C$ (тип терма x)

$*A$ (тип терма y)

Тут опять не хватает шагов: нужно построить терм типа $(A \Rightarrow B) \Rightarrow B$, *имея* y.

Так как это функция, добавляем ещё абстракцию.

$(A \Rightarrow B) \Rightarrow B$

$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$ (тип терма $\lambda y. \dots$)

C (тип терма $x\ (\lambda y. \dots)$)

$((A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C) \Rightarrow C$ (тип терма $\lambda x. x\ (\lambda y. \dots)$)

Вывод = конструкция

$*(A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C$ (тип терма x)

$*A$ (тип терма y)

$*A \Rightarrow B$ (тип терма z)

Как получить терм типа B *из* y *и* z*?*

B

$(A \Rightarrow B) \Rightarrow B$ (тип терма $\lambda z. \ldots$)

$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$ (тип терма $\lambda y.(\lambda z. \ldots)$)

C (тип терма $x\ (\lambda y.(\lambda z. \ldots))$)

$((A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C) \Rightarrow C$ (тип терма $\lambda x.x\ (\lambda y.\lambda z. \ldots)$)

Вывод = конструкция

$*(A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C$ (тип терма x)

$*A$ (тип терма y)

$*A \Rightarrow B$ (тип терма z)

B (тип терма $z\ y$)

$(A \Rightarrow B) \Rightarrow B$ (тип терма $\lambda z.(z\ y)$)

$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$ (тип терма $\lambda y.(\lambda z.(z\ y))$)

C (тип терма $x\ (\lambda y.(\lambda z.(z\ y)))$)

$((A \Rightarrow ((A \Rightarrow B) \Rightarrow B)) \Rightarrow C) \Rightarrow C$ (тип терма $\lambda x.x\ (\lambda y.\lambda z.(z\ y))$)

Вывод = конструкция

Вывести термы следующих типов:

- $A \Rightarrow (B \Rightarrow A)$
- $(A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$

Вывод = конструкция

Вывести термы следующих типов:

- комбинатор $\mathbf{K} :: A \Rightarrow (B \Rightarrow A)$
- комбинатор $\mathbf{S} ::$
  $(A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$

Вывод = конструкция

Комбинаторная логика Карри

- комбинатор $\mathbf{K} :: A \Rightarrow (B \Rightarrow A)$
- комбинатор $\mathbf{S} ::$
  $(A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$

А теперь перенесёмся на 100 лет назад, во времена Д. Гильберта...

Схемы аксиом для минимальной импликативной логики:

- $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$, где Φ, Ψ — любые формулы;
- $(\Phi \Rightarrow (\Psi \Rightarrow \Xi)) \Rightarrow (\Phi \Rightarrow \Psi) \Rightarrow (\Phi \Rightarrow \Xi)$, где Φ, Ψ, Ξ — любые формулы.

Правила вывода — подстановка + дедукция: $\mathcal{T} \vdash \Phi \Rightarrow \Psi$ влечёт $\mathcal{T}; \Phi \vdash \Psi$. Перенос в контекст отсутствует.

Гильбертовский вывод

Выведем $A \Rightarrow A$ в стиле логики 100-летней давности...

1. Возьмём $(\Phi \Rightarrow (\Psi \Rightarrow \Xi)) \Rightarrow (\Phi \Rightarrow \Psi) \Rightarrow (\Phi \Rightarrow \Xi)$ и положим $\Xi := A$ и $\Phi := A$, $\Psi := A \Rightarrow (B \Rightarrow A)$. Заметим, что Ψ — теорема (частный случай схемы $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$).

Гильбертовский вывод

Выведем $A \Rightarrow A$ в стиле логики 100-летней давности...

1. Возьмём $(\Phi \Rightarrow (\Psi \Rightarrow \Xi)) \Rightarrow (\Phi \Rightarrow \Psi) \Rightarrow (\Phi \Rightarrow \Xi)$ и положим $\Xi := A$ и $\Phi := A$, $\Psi := A \Rightarrow (B \Rightarrow A)$. Заметим, что Ψ — теорема (частный случай схемы $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$).
2. Получается теорема $(A \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow A)) \Rightarrow (A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A)$.

Гильбертовский вывод

Выведем $A \Rightarrow A$ в стиле логики 100-летней давности...

1. Возьмём $(\Phi \Rightarrow (\Psi \Rightarrow \Xi)) \Rightarrow (\Phi \Rightarrow \Psi) \Rightarrow (\Phi \Rightarrow \Xi)$ и положим $\Xi := A$ и $\Phi := A$, $\Psi := A \Rightarrow (B \Rightarrow A)$. Заметим, что Ψ — теорема (частный случай схемы $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$).
2. Получается теорема $(A \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow A)) \Rightarrow (A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A)$.
3. Теперь возьмём $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$ и положим $\Phi := A$, $\Psi := A \Rightarrow (B \Rightarrow A)$. Получим $A \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow A)$.

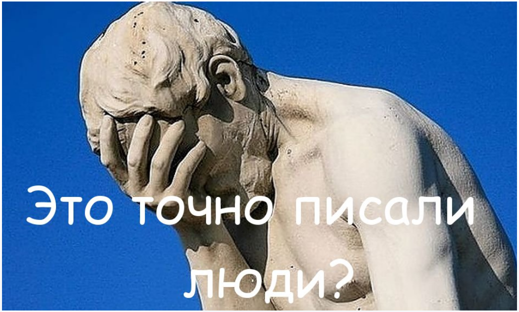
Гильбертовский вывод

Выведем $A \Rightarrow A$ в стиле логики 100-летней давности...

1. Возьмём $(\Phi \Rightarrow (\Psi \Rightarrow \Xi)) \Rightarrow (\Phi \Rightarrow \Psi) \Rightarrow (\Phi \Rightarrow \Xi)$ и положим $\Xi := A$ и $\Phi := A$, $\Psi := A \Rightarrow (B \Rightarrow A)$. Заметим, что Ψ — теорема (частный случай схемы $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$).
2. Получается теорема $(A \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow A)) \Rightarrow (A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A)$.
3. Теперь возьмём $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$ и положим $\Phi := A$, $\Psi := A \Rightarrow (B \Rightarrow A)$. Получим $A \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow A)$.
4. Применим дедукцию дважды. Теорема $A \Rightarrow A$ доказана.

Выведем $A \Rightarrow A$ в стиле логики 100-летней давности...

$$
\begin{array}{rl}
\mathbf{S}: & (A \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow A)) \Rightarrow (A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A) \\
\mathbf{K}: & A \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow A) \\
\text{дедукция}: & (A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A) \\
\mathbf{K}: & A \Rightarrow (B \Rightarrow A) \\
\text{дедукция}: & A \Rightarrow A
\end{array}
$$



"I'm not logician! I'm human!"
(c) R. Glück

Вывод = конструкция

Схемы аксиом S и K + дедукция (применение) полностью описывают минимальную логику $\Rightarrow$ с помощью λ-функций S (т.е. $\lambda f\, g\, x.f\ x\ (g\ x)$) и K (т.е. $\lambda x\, y.x$) можно построить любую λ-функцию.

Вывод из комбинатора

Тип терма $\lambda x\, y.y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

Механически выпишем построение терма в комбинаторах по шагам и начнём добавлять подстановки.

$$
\begin{aligned}
\mathbf{S} &: \\
\mathbf{K} &: \\
\mathbf{S} &: \\
\mathbf{I} &: \\
\mathbf{S}\mathbf{I} &: \\
\mathbf{K}(\mathbf{S}\mathbf{I}) &: \\
\mathbf{S}(\mathbf{K}(\mathbf{S}\mathbf{I})) &: \\
\mathbf{K} &: \\
\mathbf{S}(\mathbf{K}(\mathbf{S}\mathbf{I}))\mathbf{K} &:
\end{aligned}
$$

Вывод из комбинатора

Тип терма $\lambda x\, y.y\; x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в **S**, **K**-базисе? (для простоты включаем в него также схему аксиом **I**: $\Phi \Rightarrow \Phi$).

Механически выпишем построение терма в комбинаторах по шагам и начнём добавлять подстановки.

$$
\begin{array}{rl}
\mathbf{S}: & \\
\mathbf{K}: & \\
\mathbf{S}: & \\
\mathbf{I}: & A \Rightarrow A \\
\mathbf{S}\mathbf{I}: & \\
\mathbf{K}(\mathbf{S}\mathbf{I}): & \\
\mathbf{S}(\mathbf{K}(\mathbf{S}\mathbf{I})): & \\
\mathbf{K}: & \\
\mathbf{S}(\mathbf{K}(\mathbf{S}\mathbf{I}))\mathbf{K}: &
\end{array}
$$

Вывод из комбинатора

Тип терма $\lambda x\, y.y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

Механически выпишем построение терма в комбинаторах по шагам и начнём добавлять подстановки.

$$
\begin{array}{rl}
\mathbf{S}: & \\
\mathbf{K}: & \\
\mathbf{S}: & ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: & A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: & \\
\mathbf{K}(\mathbf{SI}): & \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): & \\
\mathbf{K}: & \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &
\end{array}
$$

Вывод из комбинатора

Тип терма $\lambda x\,y.y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

Механически выпишем построение терма в комбинаторах по шагам и начнём добавлять подстановки.

$$\begin{array}{rl}
\mathbf{S}: & \\
\mathbf{K}: & \\
\mathbf{S}: & ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: & A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: & ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): & \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): & \\
\mathbf{K}: & \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &
\end{array}$$

Вывод из комбинатора

Тип терма $\lambda x\, y. y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{aligned}
\mathbf{S} &: \\
\mathbf{K} &: \quad (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
&\qquad\qquad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S} &: \quad ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I} &: \quad A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI} &: \quad ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}) &: \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})) &: \\
\mathbf{K} &: \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K} &:
\end{aligned}
$$

Вывод из комбинатора

Тип терма $\lambda x\, y. y\; x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{array}{rl}
\mathbf{S}: & \\
\mathbf{K}: & (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
 & \quad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}: & ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: & A \Rightarrow A,\; A = A_1 \Rightarrow B \\
\mathbf{SI}: & ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): & C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): & \\
\mathbf{K}: & \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &
\end{array}
$$

Вывод из комбинатора

Тип терма $\lambda x\, y.y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{array}{rl}
\mathbf{S}: & (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B))) \\
 & \quad \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{K}: & (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
 & \quad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}: & ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: & A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: & ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): & C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): & \\
\mathbf{K}: & \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &
\end{array}
$$

Вывод из комбинатора

Тип терма $\lambda x\, y.y\, x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{array}{rl}
\mathbf{S}: & (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B))) \\
 & \quad \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{K}: & (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
 & \quad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}: & ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: & A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: & ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): & C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): & (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{K}: & \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &
\end{array}
$$

Вывод из комбинатора

Тип терма $\lambda x\, y.y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{array}{rl}
\mathbf{S}: & (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B))) \\
& \quad \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{K}: & (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
& \quad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}: & ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: & A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: & ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): & C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): & (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)),\ C = A_1 \\
\color{red}{\mathbf{K}}: & A_1 \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &
\end{array}
$$

Вывод из комбинатора

Тип терма $\lambda x\,y.y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{aligned}
\mathbf{S}: &\quad (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B))) \\
&\qquad \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{K}: &\quad (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
&\qquad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}: &\quad ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: &\quad A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: &\quad ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): &\quad C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): &\quad (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)),\ C = A_1 \\
\mathbf{K}: &\quad A_1 \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &\quad A_1 \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)
\end{aligned}
$$

Вывод из комбинатора

Тип терма $\lambda x\, y. y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{array}{rl}
\mathbf{S}: & (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B))) \\
& \quad \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{K}: & (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
& \quad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}: & ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: & A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: & ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): & C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): & (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)),\ C = A_1 \\
\mathbf{K}: & A_1 \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: & A_1 \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)
\end{array}
$$

Очевидно!

Вывод из комбинатора

Тип терма $\lambda x\, y.y\ x$ — это $A \Rightarrow (A \Rightarrow B) \Rightarrow B$. Как вывести такую теорему в $\mathbf{S}$, $\mathbf{K}$-базисе? (для простоты включаем в него также схему аксиом $\mathbf{I}$: $\Phi \Rightarrow \Phi$).

$$
\begin{aligned}
\mathbf{S}: &\quad (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B))) \\
&\qquad\qquad \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{K}: &\quad (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A) \Rightarrow B)) \\
&\qquad\qquad \Rightarrow (C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}: &\quad ((A_1 \Rightarrow B) \Rightarrow (A_1 \Rightarrow B)) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{I}: &\quad A \Rightarrow A,\ A = A_1 \Rightarrow B \\
\mathbf{SI}: &\quad ((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B) \\
\mathbf{K}(\mathbf{SI}): &\quad C \Rightarrow (((A_1 \Rightarrow B) \Rightarrow A_1) \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI})): &\quad (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1)) \Rightarrow (C \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)),\ C = A_1 \\
\mathbf{K}: &\quad A_1 \Rightarrow ((A_1 \Rightarrow B) \Rightarrow A_1) \\
\mathbf{S}(\mathbf{K}(\mathbf{SI}))\mathbf{K}: &\quad A_1 \Rightarrow ((A_1 \Rightarrow B) \Rightarrow B)
\end{aligned}
$$

Очевидно!

(это и вправду не требует участия мозга, но из разряда «легче написать (и/или запрограммировать), чем потом читать»)

Конструктивность

Достаточно ли **S** и **K** для вывода всех теорем классической логики, содержащих только импликацию?

Построения конструктивны $\Rightarrow$ для них есть явно вычислимая конструкция. Вспомним закон исключённого третьего: $A \vee \neg A$. Если передать в виде A предикат «программа P завершается», тогда вычислимая конструкция $A \vee \neg A$ будет решать проблему останова.

Остаётся вопрос, есть ли такие теоремы, содержащие только $\Rightarrow$, что их можно доказать только с помощью $A \vee \neg A$, не ограничиваясь двумя правилами естественного вывода.

Формула Пирса: $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ не населена.

Относительное отрицание

Скажем, что $\neg_R \Phi = \Phi \Rightarrow R$.

Формула Пирса: $((A \Rightarrow B) \Rightarrow A) \Rightarrow A = (\neg_B A \Rightarrow A) \Rightarrow A$.
$(\neg_B A \Rightarrow A) \Rightarrow \neg_B \neg_B A$, и как следствие $\neg_B \neg_B A \Rightarrow A$ влечёт формулу Пирса.

Относительное отрицание

Скажем, что $\neg_R \Phi = \Phi \Rightarrow R$.

Формула Пирса: $((A \Rightarrow B) \Rightarrow A) \Rightarrow A = (\neg_B A \Rightarrow A) \Rightarrow A$.
$(\neg_B A \Rightarrow A) \Rightarrow \neg_B \neg_B A$, и как следствие $\neg_B \neg_B A \Rightarrow A$ влечёт формулу Пирса.

Парадокс Карри: пусть $D = \lambda x. \neg_A (x\ x)$, тогда
$(D\ D) \Leftrightarrow (\neg_A (D\ D))$ — относительная версия парадокса Рассела.

Относительное отрицание

Скажем, что $\neg_R \Phi = \Phi \Rightarrow R$.

Формула Пирса: $((A \Rightarrow B) \Rightarrow A) \Rightarrow A = (\neg_B A \Rightarrow A) \Rightarrow A$. $(\neg_B A \Rightarrow A) \Rightarrow \neg_B \neg_B A$, и как следствие $\neg_B \neg_B A \Rightarrow A$ влечёт формулу Пирса.

Парадокс Карри: пусть $D = \lambda x. \neg_A (x\ x)$, тогда $(D\ D) \Leftrightarrow (\neg_A (D\ D))$ — относительная версия парадокса Рассела.

А теперь посмотрим на двойное относительное отрицание с точки зрения функционального языка...

$\tau :: M \Rightarrow \lambda k.k\ \tau :: \neg_R \neg_R M$, где R не входит в число переменных M. Двойное отрицание порождает продолжения вычислений.

Населенность и определения

Некоторые типы имеют единственного обитателя.

Примеры типов с одним обитателем

- $\alpha \to \alpha$ — $\mathbf{I}$
- $\alpha \to \beta \to \alpha$ — $\mathbf{K}$

...но есть и другие

- $\alpha \to \alpha \to \alpha$
- $\alpha \to \alpha \to (\alpha \to \beta) \to \beta$

Населенность и определения

Некоторые типы имеют единственного обитателя.

Примеры типов с одним обитателем

- $\alpha \to \alpha$ — $\mathbf{I}$
- $\alpha \to \beta \to \alpha$ — $\mathbf{K}$

...но есть и другие

- $\alpha \to \alpha \to \alpha$ — нумералы Чёрча (кроме 0 и 1)
- $\alpha \to \alpha \to (\alpha \to \beta) \to \beta$

Нормализуемость

Определение

- Терм M сильно нормализуем, если любая последовательность редукций приводит его к нормальной форме.
- Система типов сильно нормализуема, если все ее обитаемые типы сильно нормализуемы.

Теорема

Система $\lambda_{\to}$ сильно нормализуема.

Унификация

Алгоритм построения $mgu(E_1, \ldots, E_k)$

$$\frac{t = x}{x = t} \qquad \frac{t = t}{} \qquad \frac{f\,t_1 \ldots t_n = f\,s_1 \ldots s_n}{t_1 = s_1 \ldots t_n = s_n}$$

$$\frac{x = t \quad x = s}{x = t \quad t = s} \qquad \frac{x = t \quad r = s}{x = t \quad r[x := t] = s[x := t]}$$

Условия завершения унификации

$$\left.\begin{array}{l}\text{1. Существует уравнение} \\ \quad f\,t_1 \ldots t_n = g\,s_1 \ldots s_m, \text{ где } f \neq g. \\ \text{2. Существует уравнение } x = f\,t_1 \ldots t_n, \\ \quad \text{где } x \text{ входит в некоторое } t_i.\end{array}\right\} \text{неудача}$$

3. Все уравнения имеют вид $x_i = t_i$, причем x_i не имеет вхождений в t_i — успех.

Алгоритм Хиндли для $\lambda_{\rightarrow}$

Пусть дан терм T. В изначально пустом контексте Γ параллельно строятся приближение Φ типа терма T и система уравнений E на переменные типа Φ.

Правила вывода

$$\frac{\Gamma, x : X \vdash P : \Psi,\ E \qquad (X \text{ — свежий тип})}{\Gamma \vdash \lambda x.P\ :\ X \rightarrow \Psi, E}$$

$$\frac{\Gamma \vdash P : \Phi,\ E_1 \quad \Gamma \vdash Q : \Psi,\ E_2}{\Gamma \vdash (P\ Q) : X, E_1 \cup E_2 \cup \{\Phi = \Psi \rightarrow X\} \quad (X \text{ — свежий тип})}$$

Пусть построено $\vdash T : \Phi, E$. Из этого приближения строится $\vdash T : \Phi[mgu(E)]$ — окончательный тип терма T.

Пример на типизацию в $\lambda_{\to}$

Вывести тип терма $(\lambda k.k\ (\lambda x\,y.(\lambda z.z\ x)\ y))\ (\lambda x.x)$

Соглашения об обозначениях:

- $\square$ — символ конца ветки подвывода.
- $\Phi = \Psi_1 \to \Psi_2$ — уравнение абстракции: при присваивании переменной, связанной λ, типа Ψ_1, если результат вычислений имеет тип Ψ_2, то абстракция имеет тип Φ (правило 1).
- $\Psi_1 = \Psi_2 \to \Phi$ — уравнение аппликации: при присваивании применяемому выражению типа Ψ_1, а ее аргументу типа Ψ_2, результат вычислений имеет тип Φ (правило 2).

По построению, уравнения абстракции не требуют решения уравнений для вычисления $\mathfrak{mgu}$. Их достаточно просто подставить.

Пример вывода типа

$(\lambda k.k\ (\lambda x\,y.(\lambda z.z\ x)\ y))\ (\lambda x.x) : X,\ \Phi = \Psi \to X$

$(\lambda k.k\ (\lambda x\,y.(\lambda z.z\ x)\ y)) : \Phi,\ \Phi = A \to B$ $\qquad$ $(\lambda x.x) : \Psi,\ \Psi = C \to C$

$k : A \vdash k\ (\lambda x\,y.(\lambda z.z\ x)\ y)) : B,\ A = D \to B$ $\qquad$ $x : C \vdash x : C\ \Box$

$k : A \vdash k : A\ \Box$ $\qquad$ $\lambda x\,y.(\lambda z.z\ x)\ y : D,\ D = F \to G$

$k : A, x : F \vdash \lambda y.(\lambda z.z\ x)\ y : G,\ G = H \to I$

$k : A, x : F, y : H \vdash (\lambda z.z\ x)\ y : I,\ J = H \to I$

$k : A, x : F, y : H \vdash \lambda z.z\ x : J,\ J = K \to L$ $\qquad$ $k : A, x : F, y : H \vdash y : H\ \Box$

$k : A, x : F, y : H, z : K \vdash z\ x : L,\ K = F \to L$

$k : A, x : F, y : H, z : K \vdash z : K\ \Box$ $\qquad$ $k : A, x : F, y : H, z : K \vdash x : F\ \Box$

Уравнения аппликации: $E_1 = \{\Phi = \Psi \to X,\ A = D \to B,\ J = H \to I,\ K = F \to L\}$.
Уравнения абстракции:

$E_2 = \{\Phi = A \to B, \Psi = C \to C, D = F \to G, G = H \to I, J = K \to L\}$.

Подставляем уравнения абстракции в уравнения аппликации (система $E_1 E_2$).
$\{A \to B = (C \to C) \to X, A = (F \to (H \to I)) \to B, K \to L = H \to I, K = F \to L\}$

Строим $mgu(E_1 E_2) = \{H = F \to L,\ I = L,\ K = F \to L\ A = (F \to ((F \to L) \to L)) \to (F \to ((F \to L) \to L)),\ B = F \to ((F \to L) \to L),\ C = F \to ((F \to L) \to L),\ X = F \to ((F \to L) \to L)\}$.

Ответ: искомый тип терма есть $F \to (F \to L) \to L$.

Альтернативная унификация. Алгоритм Мартелли–Монтанари

Мультиуравнение — это выражение вида $\{x_1, \ldots, x_n\} = (t_1, \ldots, t_m)$, где x_i — переменные, t_j — термы в выбранной сигнатуре (семантически означает, что все они равны друг другу).
Общая часть мультиуравнения — максимальное внешнее общее поддерево конструкторов t_i.
Граница мультиуравнения — множество мультиуравнений, подстановка которых в общую часть порождает термы t_i.

У мультиуравнения $\{x_1, x_2\} = (f(g(x_3), h(x_4, g(x_5))), f(x_4, h(g(g(x_6)), x_7)))$ общая часть — это $f(x_4, h(x_4, x_7))$, граница — это $\{\{x_4\} = (g(x_3), g(g(x_6))), \{x_7\} = g(x_5)\}$.

Описание алгоритма

Компактная форма системы мультиуравнений — такая, что для всех $S = T$, $S' = T'$, $S \cap S' = \varnothing$.

Строим исходную систему U: $\{x\} = (t_1, t_2), \{x_i\} = \varnothing$, где x — свежая переменная, x_i — переменные, входящие в термы t_1 и t_2.

1. Выбираем такое мультиуравнение $S = M$, что переменные из S не встречаются нигде больше в U. Если такого нет, объявляем о неудаче унификации.
2. Строим общую часть C и границу F. Если общей части нет, объявляем о неудаче унификации.
3. Делаем шаг редукции: заменяем $S = M$ на $\{S = C\} \cup F$, после чего приводим к компактной форме.
4. Перемещаем $S = C$ из U в результирующую систему T.

Если в U не остаётся мультиуравнений, то результат T — это искомая подстановка-унификатор t_1 и t_2.

Вычисления «от противного»

Проблема термов в типизированном λ-исчислении (и чистого функционального стиля): «что упало, то пропало». Если вычислено $(\mathsf{M}\ \mathsf{N})$, то M и N по отдельности уже потеряны навсегда.

Вычисления «от противного»

Проблема термов в типизированном λ-исчислении (и чистого функционального стиля): «что упало, то пропало». Если вычислено $(M\ N)$, то M и N по отдельности уже потеряны навсегда.

Логичный выход — возвраты, если стало ясно, что вычисления зашли в тупик. Аналог в доказательствах — работа с отрицанием.

$$\frac{\Gamma \vdash \tau,\ \Gamma \vdash \neg\tau}{\Gamma \vdash \sigma}$$ (из лжи следует всё что угодно)

$$\frac{\Gamma \vdash \neg\neg\tau}{\Gamma \vdash \tau}$$ (снятие двойного отрицания)

Теорема Гливенко

Пусть Φ — пропозициональная формула. Тогда $\vdash \Phi$ в классической логике $\Leftrightarrow \vdash \neg\neg\Phi$ в конструктивной интуиционистской логике.

Здесь под конструктивной интуиционистской логикой понимаем минимальную логику + «из лжи следует всё что угодно». Потом мы опять вернёмся к минимальной логике, но сначала посмотрим, как всё сложно с извлечением термов из отрицания.

Теорема Гливенко

Пусть Φ — пропозициональная формула. Тогда $\vdash \Phi$ в классической логике $\Leftrightarrow \vdash \neg\neg\Phi$ в конструктивной интуиционистской логике.

$*\neg(\neg\neg A \Rightarrow A)$

$*A$

$*\neg\neg A$

A

$\neg\neg A \Rightarrow A$

$\bot$

$\neg A$

$*\neg\neg A$

A Из $\neg\neg A$ и $\neg A$

$\neg\neg A \Rightarrow A$

$\bot$

$\neg\neg(\neg\neg A \Rightarrow A)$

Теорема Гливенко

Пусть Φ — пропозициональная формула. Тогда $\vdash \Phi$ в классической логике $\Leftrightarrow \vdash \neg\neg\Phi$ в конструктивной интуиционистской логике.

- $*\neg(\neg\neg A \Rightarrow A)$
  - $*A$
    - $*\neg\neg A$
      - A
    - $\neg\neg A \Rightarrow A$
    - $\perp$
  - $\neg A$
  - $*\neg\neg A$
    - A Из $\neg\neg A$ и $\neg A$
  - $\neg\neg A \Rightarrow A$
  - $\perp$
- $\neg\neg(\neg\neg A \Rightarrow A)$

- $*\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$
  - $*A$
    - $*(A \Rightarrow B) \Rightarrow A$
      - A
    - $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
    - $\perp$
  - $\neg A$
  - $*(A \Rightarrow B) \Rightarrow A$
    - $*A$
      - B из A и $\neg A$
    - $A \Rightarrow B$
    - A
  - $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
  - $\perp$
- $\neg\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$

Переход к относительному отрицанию

«Вычисления зашли в тупик» $\Rightarrow$ приводят к нежелательному результату. Интерпретация $\neg_{\mathsf{R}}\Phi = (\Phi \Rightarrow \mathsf{R})$.
Рассмотрим предыдущие два вывода с точки зрения извлечения термов из их конструкции.

Переход к относительному отрицанию

$$
\begin{array}{ll}
*(\neg_R \neg_R A \Rightarrow A) \Rightarrow R & \text{(тип } x\text{)} \\
\quad *A & \text{(тип } y\text{)} \\
\quad\quad * \neg_R \neg_R A & \text{(тип } z\text{)} \\
\quad\quad\quad A & \text{(терм } y\text{)} \\
\quad\quad \neg_R \neg_R A \Rightarrow A & \text{(терм } \lambda z.y\text{)} \\
\quad\quad R & \text{(терм } x\ (\lambda z.y)\text{)} \\
\quad A \Rightarrow R & \text{(терм } \lambda y.x\ (\lambda z.y)\text{)} \\
\quad *(A \Rightarrow R) \Rightarrow R & \text{(тип } w\text{)} \\
\quad\quad A & \text{(??!!! из } A \Rightarrow R \text{ и } (A \Rightarrow R) \Rightarrow R\text{)} \\
\quad \neg_R \neg_R A \Rightarrow A & \\
\quad R & \\
((\neg_R \neg_R A \Rightarrow A) \Rightarrow R) \Rightarrow R &
\end{array}
$$

Проблема с правилом «из лжи следует всё что угодно»: относительное отрицание даёт вывести из противоречия лишь одну формулу R. Вывод требует, чтобы $R = A$, но это превращает исходную формулу в тривиальность: $((((A \Rightarrow A) \Rightarrow A) \Rightarrow A) \Rightarrow A) \Rightarrow A$.

Переход к относительному отрицанию

«Вычисления зашли в тупик» $\Rightarrow$ приводят к нежелательному результату. Интерпретация $\neg_R \Phi = (\Phi \Rightarrow R)$.

$*(((A \Rightarrow B) \Rightarrow A) \Rightarrow A) \Rightarrow R$ (тип x)
| $*A$ (тип y)
| | $*(A \Rightarrow B) \Rightarrow A$ (тип z)
| | | A (терм y)
| | $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ (терм $\lambda z.y$)
| | R (терм $x\ (\lambda z.y)$)
| $A \Rightarrow R$ (терм $\lambda y.x\ (\lambda z.y)$)
| $*(A \Rightarrow B) \Rightarrow A$ (тип u)
| | $*A$ (тип w)
| | | B ??!!!
| | $A \Rightarrow B$
| | A
| $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
| R
$((((A \Rightarrow B) \Rightarrow A) \Rightarrow A) \Rightarrow R) \Rightarrow R$

Переход к относительному отрицанию

$*(((A \Rightarrow B) \Rightarrow A) \Rightarrow A) \Rightarrow B$ (тип x)

$*A$ (тип y)

$*(A \Rightarrow B) \Rightarrow A$ (тип z)

A (терм y)

$((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ (терм $\lambda z.y$)

B (терм $x\ (\lambda z.y)$)

$A \Rightarrow B$ (терм $\lambda y.x\ (\lambda z.y)$)

$*(A \Rightarrow B) \Rightarrow A$ (тип u)

$*A$ (тип w)

B (терм $(\lambda y.x\ (\lambda z.y))\ w$)

$A \Rightarrow B$ (терм $\lambda y.x\ (\lambda z.y)$)

A (терм $u\ (\lambda y.x\ (\lambda z.y))$)

$((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ (терм $\lambda u.u\ (\lambda y.x\ (\lambda z.y))$)

B (терм $x\ (\lambda u.u\ (\lambda y.x\ (\lambda z.y)))$)

$((((A \Rightarrow B) \Rightarrow A) \Rightarrow A) \Rightarrow B) \Rightarrow B$

(терм $(\lambda x.x\ (\lambda u.u\ (\lambda y.x\ (\lambda z.y))))$)

Здесь тоже сложно с правилом «из лжи следует всё что угодно», но вопрос решается, если положить $R = B$. Тогда мы получаем минимальный вывод нетривиальной формулы Крипке.

Навешивание двойного отрицания

Видно, что использование «возвратных» термов (переход от типа Φ к типу $\neg_R \neg_R \Phi$) расширяет возможности языка. Возникает вопрос, в каких подформулах лучше это делать?

- Преобразование Колмогорова:
  $\sigma_K(A) = \neg_R \neg_R A$
  $\sigma_K(\Phi \Rightarrow \Psi) = \neg_R \neg_R(\sigma_K(\Phi) \Rightarrow \sigma_K(\Psi))$
- Вариант более слабого преобразования (в стиле Куроды) — это $\sigma_W(\Phi) = \neg_R \neg_R \sigma'_W(\Phi)$, где:
  $\sigma'_W(A) = A$
  $\sigma'_W(\Phi \Rightarrow \Psi) = \sigma'_W(\Phi) \Rightarrow \neg_R \neg_R \sigma'_W(\Psi))$

В примерах для краткости $(\Phi \Rightarrow R) \Rightarrow R$ переобозначим как Φ'.

Переход по Колмогорову

$$*(A' \Rightarrow ((A' \Rightarrow B')' \Rightarrow B')') \Rightarrow R \qquad \text{(тип } k_0\text{)}$$

$$*(A \Rightarrow R) \Rightarrow R \qquad \text{(тип } x\text{)}$$

$$*((A' \Rightarrow B')' \Rightarrow B') \Rightarrow R \qquad \text{(тип } k_1\text{)}$$

$$*((A' \Rightarrow B') \Rightarrow R) \Rightarrow R \qquad \text{(тип } y\text{)}$$

$$*B \Rightarrow R \qquad \text{(тип } k_2\text{)}$$

$$*A' \Rightarrow B' \qquad \text{(тип } k_3\text{)}$$

$$*A \Rightarrow R \qquad \text{(тип } k_4\text{)}$$

$$R \qquad \text{(терм } x\ k_4\text{)}$$

$$(A \Rightarrow R) \Rightarrow R \qquad \text{(терм } \lambda k_4.x\ k_4\text{)}$$

$$(B \Rightarrow R) \Rightarrow R \qquad \text{(терм } k_3\ (\lambda k_4.x\ k_4)\text{)}$$

$$R \qquad \text{(терм } (k_3\ (\lambda k_4.x\ k_4))\ k_2\text{)}$$

$$(A' \Rightarrow B') \Rightarrow R \qquad \text{(терм } \lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2\text{)}$$

$$R \qquad \text{(терм } y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2)\text{)}$$

$$(B \Rightarrow R) \Rightarrow R \qquad \text{(терм } \lambda k_2.y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2)\text{)}$$

$$(A' \Rightarrow B')' \Rightarrow B' \qquad \text{(терм } \lambda y k_2.y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2)\text{)}$$

$$R \qquad \text{(терм } k_1\ (\lambda y k_2.y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2))\text{)}$$

$$(((A' \Rightarrow B')' \Rightarrow B') \Rightarrow R) \Rightarrow R \qquad \text{(терм } \lambda k_1.k_1\ (\lambda y k_2.y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2))\text{)}$$

$$A' \Rightarrow ((A' \Rightarrow B')' \Rightarrow B')' \qquad \text{(терм } \lambda x k_1.k_1\ (\lambda y k_2.y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2))\text{)}$$

$$R \qquad \text{(терм } k_0\ (\lambda x k_1.k_1\ (\lambda y k_2.y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2)))\text{)}$$

$$((A' \Rightarrow ((A' \Rightarrow B')' \Rightarrow B')') \Rightarrow R) \Rightarrow R$$

Извлечённый терм: $\lambda k_0.k_0\ (\lambda x k_1.k_1\ (\lambda y k_2.y\ (\lambda k_3.k_3\ (\lambda k_4.x\ k_4)\ k_2)))$

Слабый переход по Куроде

$*(A \Rightarrow ((A \Rightarrow B') \Rightarrow B')') \Rightarrow R$ (тип k_0)

$*A$ (тип x)

$*((A \Rightarrow B') \Rightarrow B') \Rightarrow R$ (тип k_1)

$*A \Rightarrow B'$ (тип y)

$*B \Rightarrow R$ (тип k_2)

$(B \Rightarrow R) \Rightarrow R$ (тип $y\ x$)

R (тип $y\ x\ k_2$)

$(B \Rightarrow R) \Rightarrow R$ (тип $\lambda k_2.y\ x\ k_2$)

$(A \Rightarrow B') \Rightarrow B'$ (тип $\lambda y k_2.y\ x\ k_2$)

R (тип $k_1\ (\lambda y k_2.y\ x\ k_2)$)

$(((A \Rightarrow B') \Rightarrow B') \Rightarrow R) \Rightarrow R$ (тип $\lambda k_1.k_1\ (\lambda k_2.y\ x\ k_2)$)

$A \Rightarrow ((A \Rightarrow B') \Rightarrow B')'$ (тип $\lambda x k_1.k_1\ (\lambda k_2.y\ x\ k_2)$)

R (тип $k_0\ (\lambda x k_1.k_1\ (\lambda k_2.y\ x\ k_2))$)

$((A \Rightarrow ((A \Rightarrow B') \Rightarrow B')') \Rightarrow R) \Rightarrow R$

Извлечённый терм: $\lambda k_0.k_0\ (\lambda x k_1.k_1\ (\lambda y k_2.y\ x\ k_2))$.

Детали преобразования

- Переменные x и y получают имена так: смотрим на исходный терм $\lambda xy.y\ x$. В нём тип x — это просто A, тип y — это $A \Rightarrow B$. Теперь преобразуем их типы по Колмогорову или Куроде как подформулы. Образы этих типов и породят термы x и y.
- В выводе терма по Куроде есть странный подвывод, в котором выводится $(B \Rightarrow R) \Rightarrow R$, и так выводимая без него:

$$
\begin{array}{lll}
*A \Rightarrow B' & & \text{(тип } y\text{)} \\
\quad *B \Rightarrow R & & \text{(тип } k_2\text{)} \\
\quad\quad (B \Rightarrow R) \Rightarrow R & & \text{(тип } y\ x\text{)} \\
\quad\quad R & & \text{(тип } y\ x\ k_2\text{)} \\
\quad (B \Rightarrow R) \Rightarrow R & & \text{(тип } \lambda k_2.y\ x\ k_2\text{)} \\
(A \Rightarrow B') \Rightarrow B' & & \text{(тип } \lambda y k_2.y\ x\ k_2\text{)}
\end{array}
$$

Однако если выводить формулу без подвывода с допущением $B \Rightarrow R$ напрямую, то вместо $A \Rightarrow B'$ можно просто подставить формулу $A \Rightarrow B$, и мы получим вывод не требуемой формулы, а более общей: $(A \Rightarrow ((A \Rightarrow B) \Rightarrow B)')'$, а мы хотим доказать именно ту формулу, которую получили преобразованием.

Система передачи продолжений

Система передачи продолжений в CBN-стиле:

- $\tau_N(\mathsf{const}) = \lambda k.k\ \mathsf{const}$
- $\tau_N(x) = \lambda k.x\ k$
- $\tau_N(\lambda x.M) = \lambda k.k\ (\lambda x.\tau_N(M))$
- $\tau_N(M\ N) = \lambda k.\tau_N(M)\ (\lambda f.f\ \tau_N(N)\ k)$

Система передачи продолжений

Система передачи продолжений в CBN-стиле:

- $\tau_N(const) = \lambda k.k\ const$
- $\tau_N(x) = \lambda k.x\ k$
- $\tau_N(\lambda x.M) = \lambda k.k\ (\lambda x.\tau_N(M))$
- $\tau_N(M\ N) = \lambda k.\tau_N(M)\ (\lambda f.f\ \tau_N(N)\ k)$

Система передачи продолжений в CBV-стиле:

- $\tau_V(const) = \lambda k.k\ const$
- $\tau_V(x) = \lambda k.k\ x$
- $\tau_V(\lambda x.M) = \lambda k.k\ (\lambda x.\tau_V(M))$
- $\tau_V(M\ N) = \lambda k.\tau_V(M)\ (\lambda f.\tau_V(N)\ (\lambda a.f\ a\ k))$

Применение CPS-преобразования

Утверждение

Если тип исходного терма M — это Φ, то тип терма $\tau_N(M)$ — это $\sigma_K(\Phi)$, тип терма $\tau_V(M)$ — это $\sigma_W(\Phi)$.

Пример формулы Пирса $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ показывает, что некоторые термы типизируются только после CPS-преобразования. Это и есть практический смысл теоремы Гливенко.

- $M \to^* \mathit{const}$ при CBV-стратегии $\Leftrightarrow$ $\tau_V(M)\ \mathit{id} \to^* \mathit{const}$ при какой угодно стратегии.
- $M \to^* \mathit{const}$ при CBN-стратегии $\Leftrightarrow$ $\tau_N(M)\ \mathit{id} \to^* \mathit{const}$ при какой угодно стратегии.

Пара и размеченное объединение

Расширенные λ-термы

- Конструкторы пары: $\langle x, y\rangle$, $\mathsf{fst}\ x$, $\mathsf{snd}\ x$.
  Аксиомы пары:
  - $\mathsf{fst}\ \langle x, y\rangle = x$;
  - $\mathsf{snd}\ \langle x, y\rangle = y$.
- Конструкторы размеченного объединения: $\mathsf{Left}\ x$, $\mathsf{Right}\ x$, $\mathsf{either}\,(\lambda x.\,\Phi_1,\ \lambda x.\,\Phi_2,\ z)$.
  Аксиомы размеченного объединения:
  - $\mathsf{either}\,(\lambda x.\,\Phi_1,\ \lambda x.\,\Phi_2,\ (\mathsf{Left}\ n)) = \Phi_1[x := n]$;
  - $\mathsf{either}\,(\lambda x.\,\Phi_1,\ \lambda x.\,\Phi_2,\ (\mathsf{Right}\ n)) = \Phi_2[x := n]$;.

δ-редукция — редукция с помощью применения аксиом для вводимых в λ-исчисление конструкторов. Расширенная система сохраняет свойство ромба.

Типизация пар и объединений

- Пара $\langle x^A, y^B \rangle$ имеет тип $A \ \&\ B$. Правила вывода:

$$\langle\,\rangle : \frac{A \quad B}{A \ \&\ B} \qquad \mathsf{fst} : \frac{A \ \&\ B}{A} \qquad \mathsf{snd} : \frac{A \ \&\ B}{B}$$

- Объединению, порожденному Left x^A, должен быть назначен тип $A \vee B$. Объединение, порождаемое Right x^A, имеет тип $B \vee A$. Правила вывода:

$$\mathsf{either} : \frac{\begin{array}{lll} A \vee B & & \\ * A & & * B \\ \mid\ C & & \mid\ C \end{array}}{C} \qquad \mathsf{Left} : \frac{A}{A \vee B} \qquad \mathsf{Right} : \frac{A}{B \vee A}$$

Если нет данных о типе второго элемента объединения, тип объединения должен быть задан вручную.

Естественный вывод в стиле Фитча

применение : $\dfrac{A \quad A \Rightarrow B}{B}$

$\lambda x_i \rightarrow$: $\begin{array}{l} *\,A \\ \;|\; B \\ \hline A \Rightarrow B \end{array}$

разбор пары : $\dfrac{A \,\&\, B}{A \quad B}$

пара : $\dfrac{A \quad B}{A \,\&\, B}$

дилемма : $\dfrac{A \vee B}{\begin{array}{ll} *\,A & *\,B \\ \;|\; C & \;|\; C \end{array}}$ C

Left : $\dfrac{A}{A \vee B}$

Right : $\dfrac{B}{A \vee B}$

Каждое применение правила вывода в доказательстве соответствует использованию в терме конструкции с именем этого правила вывода.

Типизация расширенных термов

- При типизации выражения either $(\lambda x_1.\Phi_1,\ \lambda x_2.\Phi_2, \Psi)$, Ψ получает тип $A \vee B$, $\lambda x_1.\Phi_1$ — тип $A \Rightarrow C$, $\lambda x_2.\Phi_2$ — тип $B \Rightarrow C$. При этом типы для Φ_1 и Φ_2 должны совпадать (тип C). Всё выражение получает тип C.

- Если в выражении есть подвыражения вида fst x, snd x, то x имеет тип A & B. Если в выражении есть подвыражения вида Left x, Right x, то эти подвыражения имеют тип $A \vee B$ (притом что типом x является A или B соответственно).

- Конструкторы типов &, $\vee$ обрабатываются алгоритмом построения унификатора каждый отдельно: например, сопоставление $A \to B = C \vee D$ считается неудачным.

Пример

Построить тип выражения
$\lambda n.\mathsf{either}\,(\lambda z_1.(\mathsf{snd}\ n)\ z_1,\ \lambda z_2.z_2,\ (\mathsf{fst}\ n)).$

Уравнения для типизации пар и объединений выделены зеленым.

$\lambda n.\mathsf{either}\,(\lambda z_1.(\mathsf{snd}\ n)\ z_1,\ \lambda z_2.z_2,\ (\mathsf{fst}\ n)) : X,\ X = A \to B$

$n : A \vdash \mathsf{either}\,(\lambda z_1.(\mathsf{snd}\ n)\ z_1,\ \lambda z_2.z_2,\ (\mathsf{fst}\ n)) : B,$

$C = E \to B,\ D = F \to B,\ G = E \vee F$

$n : A \vdash \lambda z_1.(\mathsf{snd}\ n)\ z_1 : C,\quad C = H \to I$

$n : A, z_1 : H \vdash (\mathsf{snd}\ n)\, z_1 : I,$

$L = H \to I$

$n : A, z_1 : H \vdash (\mathsf{snd}\ n) : L,$

$A = M \,\&\, L$

$n : A, z_1 : H \vdash n : M \,\&\, L\ \square$

$n : A, z_1 : H \vdash z_1 : H\ \square$

$n : A \vdash \lambda z_2.z_2 : D,\quad D = J \to J$

$n : A, z_2 : J \vdash z_2 : J\ \square$

$n : A \vdash (\mathsf{fst}\ n) : G,\quad A = G \,\&\, K$

$n : A \vdash n : G \,\&\, K\ \square$

$E_1 = \{X = A \to B, C = H \to I, D = J \to J\};$

$E_2 = \{C = E \to B, D = F \to B, G = E \vee F, A = G \,\&\, K, L = H \to I, A = M \,\&\, L\}.$

$E_2E_1 = \{H \to I = E \to B, J \to J = F \to B, G = E \vee F, A = G \,\&\, K, L = H \to I,$
$A = M \,\&\, L\}.$

$mgu(E_2E_1) = \{B = F = I = J, E = H, G = M = E \to B, L = E \to B,$
$A = (E \vee B) \,\&\, (E \to B)\}$, и ответ: $X = (E \vee B) \,\&\, (E \to B) \to B.$

Доказательство населенности типа

Пусть Φ — тип расширенного $\lambda_{\rightarrow}$-исчисления.

- Строится доказательство Φ в IL.
- По доказательству строится терм — обитатель Φ.

Пример

Пусть $\Phi = (A \Rightarrow B) \mathbin{\&} \neg B \Rightarrow \neg A$. Строим доказательство и заодно сразу терм (справа):

$$
\cfrac{\cfrac{\begin{array}{lcl}
* (A \Rightarrow B) \mathbin{\&} \neg B & : & \lambda x. \\
\quad * A & : & \lambda y. \\
\quad | \, A \Rightarrow B & : & (\mathsf{fst}\ x) \\
\quad | \, B & : & ((\mathsf{fst}\ x)\ y) \\
\quad | \, \neg B & : & (\mathsf{snd}\ x) \\
\quad | \, \bot & : & (\mathsf{snd}\ x\ ((\mathsf{fst}\ x)\ y))
\end{array}}{\neg A}}{(A \Rightarrow B) \mathbin{\&} \neg B \Rightarrow \neg A}
$$

Построенный обитатель: $\lambda x.\lambda y.(\mathsf{snd}\ x\ ((\mathsf{fst}\ x)\ y))$.

Принципы естественного вывода

- Если надо доказать выражение $A \Rightarrow B$, строим подвывод:

$$\dfrac{\begin{array}{l} *A \\ | \\ |\,B \end{array}}{A \Rightarrow B}$$

  Внутри этого подвывода всегда можно использовать формулу A как доказанную.

- Если в контексте (в допущении дедукции) есть формула $(A \Rightarrow B) \Rightarrow C$, а нужно доказать C, часто (но не всегда!) удобно внутри этого же контекста доказать $A \Rightarrow B$, а потом применить полученное доказательство.

- Отрицание — тоже импликация, и методы работы с ним точно такие же, но помним, что из $\perp$ внутри подвывода можно вывести всё что угодно.

Сложный пример естественного вывода

Пусть надо доказать $\neg\neg(A \Rightarrow B) \Rightarrow \neg\neg A \Rightarrow \neg\neg B$.
Несколько технических шагов (дедукция):

$*((A \Rightarrow B) \Rightarrow \bot) \Rightarrow \bot$

- $*(A \Rightarrow \bot) \Rightarrow \bot$
  - $*B \Rightarrow \bot$
    - *(Тут пока нет подвывода)*
    - $\bot$
  - $(B \Rightarrow \bot) \Rightarrow \bot$
- $((A \Rightarrow \bot) \Rightarrow \bot) \Rightarrow ((B \Rightarrow \bot) \Rightarrow \bot)$

$\neg\neg(A \Rightarrow B) \Rightarrow \neg\neg A \Rightarrow \neg\neg B$

Исходя из контекста, чтобы получить в нем $\bot$, можно пытаться доказывать либо B, либо $A \Rightarrow \bot$, либо $(A \Rightarrow B) \Rightarrow \bot$. Но доказать B можно только через ex falso, что означает, что $\bot$ уже доказано. Остается два варианта (они перестановочны).

Продолжение вывода

$*((A \Rightarrow B) \Rightarrow \bot) \Rightarrow \bot$

- $*(A \Rightarrow \bot) \Rightarrow \bot$
  - $*B \Rightarrow \bot$
    - $*A$
      - *(Опять нужно доказывать $\bot$)*
      - $\bot$
    - $A \Rightarrow \bot$
    - $\bot$
  - $(B \Rightarrow \bot) \Rightarrow \bot$
- $((A \Rightarrow \bot) \Rightarrow \bot) \Rightarrow ((B \Rightarrow \bot) \Rightarrow \bot)$

$\neg\neg(A \Rightarrow B) \Rightarrow \neg\neg A \Rightarrow \neg\neg B$

В самом внутреннем подвыводе опять нужно доказать $\bot$, и остается только одна формула из контекста, которая может быть использована для этого: $((A \Rightarrow B) \Rightarrow \bot) \Rightarrow \bot$. Она позволяет замкнуть таблицу.

Завершение вывода

$*((A \Rightarrow B) \Rightarrow \bot) \Rightarrow \bot$

> $*(A \Rightarrow \bot) \Rightarrow \bot$
>
> > $*B \Rightarrow \bot$
> >
> > > $*A$
> > >
> > > > $*A \Rightarrow B$
> > > >
> > > > > B
> > > > >
> > > > > $\bot$ -- *Вследствие контекста* $B \Rightarrow \bot$
> > > >
> > > > $(A \Rightarrow B) \Rightarrow \bot$
> > > >
> > > > $\bot$
> > >
> > > $A \Rightarrow \bot$
> > >
> > > $\bot$
> >
> > $(B \Rightarrow \bot) \Rightarrow \bot$
>
> $((A \Rightarrow \bot) \Rightarrow \bot) \Rightarrow ((B \Rightarrow \bot) \Rightarrow \bot)$

$\neg\neg(A \Rightarrow B) \Rightarrow \neg\neg A \Rightarrow \neg\neg B$

Равноправный вариант: доказывать во внутреннем подвыводе $(A \Rightarrow B) \Rightarrow \bot$, внутри вывода которого доказывать $A \Rightarrow \bot$.

Извлечение λ-терма

$$
\begin{array}{ll}
*((A \Rightarrow B) \Rightarrow \bot) \Rightarrow \bot & : x \\
\quad *(A \Rightarrow \bot) \Rightarrow \bot & : y \\
\quad\quad *B \Rightarrow \bot & : z \\
\quad\quad\quad *A & : w \\
\quad\quad\quad\quad *A \Rightarrow B & : v \\
\quad\quad\quad\quad\quad B & : (v\ w) \\
\quad\quad\quad\quad\quad \bot & : (z\ (v\ w)) \\
\quad\quad\quad\quad (A \Rightarrow B) \Rightarrow \bot & : \lambda v.(z\ (v\ w)) \\
\quad\quad\quad\quad \bot & : (x\ (\lambda v.(z\ (v\ w)))) \\
\quad\quad\quad A \Rightarrow \bot & : \lambda w.x\ (\lambda v.(z\ (v\ w))) \\
\quad\quad\quad \bot & : (y\ (\lambda w.x\ (\lambda v.(z\ (v\ w))))) \\
\quad\quad (B \Rightarrow \bot) \Rightarrow \bot & : \lambda z.y\ (\lambda w.x\ (\lambda v.(z\ (v\ w)))) \\
\quad ((A \Rightarrow \bot) \Rightarrow \bot) \Rightarrow ((B \Rightarrow \bot) \Rightarrow \bot) & \\
 & : \lambda y\, z.y\ (\lambda w.x\ (\lambda v.(z\ (v\ w)))) \\
\neg\neg(A \Rightarrow B) \Rightarrow \neg\neg A \Rightarrow \neg\neg B & : \lambda x\, y\, z.y\ (\lambda w.x\ (\lambda v.(z\ (v\ w))))
\end{array}
$$

Задача проверки ненаселенности типа

Модели Крипке

На множестве моделей задан частичный порядок $\preceq$, формирующий пути вычислений. Выражение $M_i \models \Phi$ — «мир (модель) M_i вынуждает формулу Φ».

- Если $M_i \models A$, то $M_j \models A$ для всех M_j таких, что $M_i \preceq M_j$.
- $M_i \models A \mathbin{\&} B \Leftrightarrow M_i \models A \mathbin{\&} M_i \models B$.
- $M_i \models A \vee B \Leftrightarrow M_i \models A \vee M_i \models B$.
- $M_i \models A \Rightarrow B \Leftrightarrow \forall M_j (M_i \preceq M_j \Rightarrow (M_j \models A \Rightarrow M_j \models B))$.
- $M_i \not\models \bot$; $\neg A$ — то же, что $A \Rightarrow \bot$.

Для доказательства ненаселенности типа Φ достаточно построить такое дерево вычислений, что в некотором M_i этого дерева неверно, что $M_i \models \Phi$.

Семантика Крипке

- Нижняя полурешётка «возможных миров», населённых «событиями»: пропозициональными переменными.
- Внутри каждого «мира» каждое событие может произойти (пишем $w \models A$), а может не происходить.
- Если событие A случилось в мире w, тогда оно произошло и во всех мирах w', таких что $w \triangleleft w'$ (w' — возможное будущее относительно w).
- Событие «не A», произошедшее в мире w (т.е. $w \models \neg A$), обозначает, что ни в каком наследнике w событие A не произойдёт.
- Высказывание $w \models A \Rightarrow \mathrm{B}$ означает, что в мире w и всех его наследниках если случается A, то обязательно произошло и B.
- $w \models A \mathbin{\&} \mathrm{B}$ и $w \models A \vee \mathrm{B}$ понимаются классически.

Принципы построения контрмодели

- Опровержение Φ строится в начале вычислений (мире — корне дерева, в котором ни одна переменная не вынуждается).
- $M_i \models \neg\neg A$, если во всех путях вычислений, выходящих из M_i, все конечные точки (листы) M_j вынуждают A. При этом не обязательно $M_i \models A$.
- Если у мира M_i есть ровно два потомка: M_j и M_k, причем $M_j \models A$, $M_j \not\models B$, $M_k \models B$, $M_k \not\models A$, то $M_i \not\models A \vee B$.

Пример

Контрмодель (1) опровергает формулу $A \vee \neg A$: она не выполняется в M_0. Но ее же опровергает и более простая контрмодель (2), вдобавок она опровергает формулу $\neg\neg A \Rightarrow A$: $M_0' \models \neg\neg A$, но $M_0' \not\models A$.

$$\begin{tikzcd} M_1 \models \neg A & & M_2 \models A \\ & M_0 \arrow[ul] \arrow[ur] & \end{tikzcd} \qquad\qquad \begin{tikzcd} M_1' \models A \\ M_0' \arrow[u] \end{tikzcd}$$

(1) (2)

Законы моделей Крипке

- Если в листе M верно $M \models \neg A$ тогда и только тогда, когда всюду на пути от корня до узла M формула A либо ложна, либо неизвестна. Кроме того, если $M \models \neg A$, то для любого M' — потомка M выполнено $M' \models \neg A$.
- "Неизвестность"абсолютно распространяется до корня: если в некотором листе M формула A неизвестна (т.е. не верны ни $M \models A$, ни $M \models \neg A$), то во всех узлах на пути от корня до M (включая корень) формула A неизвестна. Обратное неверно.
- Если формула Ф классически верна (имеет тождественно истинную таблицу истинности), она будет верна на всех листах любой модели Крипке. Ее опровержение — построение такого корня дерева, в котором Ф неизвестна.

Парадокс «пьющего» (Drinker paradox)

«В каждой непустой группе найдётся такой человек, что если он пьёт, то все пьют».

Финитный вариант: $(A \Rightarrow A \ \&\ B) \vee (B \Rightarrow A \ \&\ B)$

Контрмодель:

$$
\begin{tikzcd}
w_1 \models A & & w_2 \models B \\
& w_0 \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Если время линейно и конечно, тогда парадокс пьющего конструктивно доказуем (назначим «пьющим» максимального трезвенника).