Нормализация вычислений

Теория формальных языков

2021 г.

Алг. типы данных как TRS

Отношение одношаговой редукции $\to_{\mathcal{T}}$, определяемое $\mathcal{T}$ – это наименьшее отношение на термах такое, что $M[v := \sigma(L)] \to_{\mathcal{T}} M[v := \sigma(R)]$, где x входит в терм M однажды, и $L \to R$ — правило переписывания $\mathcal{T}$.
Многошаговая редукция: $M \twoheadrightarrow N$.

В общем случае редукция требует сделать унификацию левой части правила, L, с некоторым подтермом терма M. Пример: $A(x, S(y)) \to S(A(x, y))$ может применяться к терму $A(A(Z, S(Z)), S(S(Z)))$ двумя разными способами: через подстановку $x := A(Z, S(Z)),\ y := S(Z)$ и через $x := Z,\ y := Z$.

Пусть $\mathcal{T}$ — конфлюэнтная TRS. Тогда
$\mathcal{T} \vdash M = N \Leftrightarrow M \twoheadrightarrow \circ \twoheadleftarrow N$.

Виды конфлюэнтности

- (Глобальная) конфлюэнтность:
  $N_1 \twoheadleftarrow M \twoheadrightarrow N_2 \Rightarrow N_1 \twoheadrightarrow \circ \twoheadleftarrow N_2.$
- Локальная конфлюэнтность:
  $N_1 \leftarrow M \rightarrow N_2 \Rightarrow N_1 \twoheadrightarrow \circ \twoheadleftarrow N_2.$

Виды конфлюэнтности

- (Глобальная) конфлюэнтность:
  $N_1 \twoheadleftarrow M \twoheadrightarrow N_2 \Rightarrow N_1 \twoheadrightarrow \circ \twoheadleftarrow N_2$.
- Локальная конфлюэнтность:
  $N_1 \leftarrow M \rightarrow N_2 \Rightarrow N_1 \twoheadrightarrow \circ \twoheadleftarrow N_2$.

Рассмотрим следующую TRS:
$\infty \to S(\infty) \quad Eq?(x,\ x) \to True \quad Eq?(x,\ S(x)) \to False$
Она локально конфлюэнтна (проверьте), но не является конфлюэнтной.

Виды конфлюэнтности

- (Глобальная) конфлюэнтность:
  $N_1 \twoheadleftarrow M \twoheadrightarrow N_2 \Rightarrow N_1 \twoheadrightarrow \circ \twoheadleftarrow N_2$.
- Локальная конфлюэнтность:
  $N_1 \leftarrow M \rightarrow N_2 \Rightarrow N_1 \twoheadrightarrow \circ \twoheadleftarrow N_2$.

Рассмотрим следующую TRS:
$\infty \to S(\infty) \quad Eq?(x,\ x) \to True \quad Eq?(x,\ S(x)) \to False$
Она локально конфлюэнтна (проверьте), но не является конфлюэнтной.

Лемма Ньюмана

В завершающихся TRS локальная конфлюэнтность эквивалентна конфлюэнтности.

Критические пары

Напоминание

Термы T_1 и T_2 унифицируются, если $\exists\sigma(T_1\sigma = T_2\sigma)$. Если для всех σ' таких, что $T_1\sigma' = T_2\sigma'$ существует подстановка η такая, что $T_1\sigma' = (T_1\sigma)\eta$, тогда σ — most general unifier для T_1 и T_2 ($\sigma = mgu(T_1, T_2)$).

Критические пары

Напоминание

Термы T_1 и T_2 унифицируются, если $\exists\sigma(T_1\sigma = T_2\sigma)$. Если для всех σ' таких, что $T_1\sigma' = T_2\sigma'$ существует подстановка η такая, что $T_1\sigma' = (T_1\sigma)\eta$, тогда σ — most general unifier для T_1 и T_2 ($\sigma = mgu(T_1, T_2)$).

Правила $L_1 \to R_1$ и $L_2 \to R_2$ образуют критическую пару $\langle R_1\sigma,\ (L_1\sigma)[P\sigma := R_2\sigma]\rangle$, если в L_1 существует подтерм P, не равный переменной, такой что $P\sigma = L_2\sigma$.

Леволинейные TRS

TRS называется леволинейной, если в левых частях её правил нет повторных переменных.

Если TRS леволинейна и не имеет нетривиальных критических пар, то она конфлюэнтна.

Если HOF редуцируется к нормальной форме, эта нормальная форма единственна. (см. алгебру комбинаторной логики)

Все завершающиеся функции HOF имеют нормальную форму.

Теорема о конфлюэнтности

Пара термов $\langle T_1, T_2 \rangle$ объединяема $\Leftrightarrow$ $T_1 \twoheadrightarrow \circ \twoheadleftarrow T_2$.
TRS локально конфлюэнтна $\Leftrightarrow$ все её критические пары объединяемы.

Рассмотрим TRS $\mathcal{T} = \{f(g(x)) \to x,\ g(f(x)) \to x\}$. В $\mathcal{T}$ единственные критические пары — это $\langle f(x), f(x) \rangle$ для $f(g(f(x)))$ и $\langle g(x), g(x) \rangle$ для $g(f(g(x)))$ — объединяемые.

Теорема о конфлюэнтности

Пара термов $\langle T_1, T_2\rangle$ объединяема $\Leftrightarrow$ $T_1 \twoheadrightarrow \circ \twoheadleftarrow T_2$.
TRS локально конфлюэнтна $\Leftrightarrow$ все её критические пары объединяемы.

Рассмотрим TRS $\mathcal{T} = \{f(g(x)) \to x,\ g(f(x)) \to x\}$. В $\mathcal{T}$ единственные критические пары — это $\langle f(x), f(x)\rangle$ для $f(g(f(x)))$ и $\langle g(x), g(x)\rangle$ для $g(f(g(x)))$ — объединяемые.

Рассмотрим TRS $\mathcal{T}$ с правилом $f(f(x)) \to g(x)$. Она порождает критическую пару $\langle f(g(x)), g(f(x))\rangle$, не сводимую к общему терму. Если добавить к $\mathcal{T}$ правило $f(g(x)) \to g(f(x))$, оно не испортит завершаемость (почему?), но появится конфлюэнтность.

Пример

Аксиомы списка	Аксиомы ошибки
car(cons x l) = x	car nil = error_a
cdr(cons x l) = l	cdr nil = error_l
isempty? nil = true	cons error_a l = error_l
isempty? (cons x l) = false	cons x error_l = error_l
cond_a true x y = x	car error_l = error_a
cond_a false x y = y	cdr error_l = error_l
cond_b true v1 v2 = v1	isempty? error_l = error_b
cond_b false v1 v2 = v2	cond_a error_b x y = error_a
cond_l true l1 l2 = l1	cond_b error_b x y = error_b
cond_l false l1 l2 = l2	cond_l error_b x y = error_l

Пример

Аксиомы списка	Аксиомы ошибки
car(cons x l) = x	car nil = error$_\mathfrak{a}$
cdr(cons x l) = l	cdr nil = error$_\mathfrak{l}$
isempty? nil = true	cons error$_\mathfrak{a}$ l = error$_\mathfrak{l}$
isempty? (cons x l) = false	cons x error$_\mathfrak{l}$ = error$_\mathfrak{l}$
cond$_\mathfrak{a}$ true x y = x	car error$_\mathfrak{l}$ = error$_\mathfrak{a}$
cond$_\mathfrak{a}$ false x y = y	cdr error$_\mathfrak{l}$ = error$_\mathfrak{l}$
cond$_\mathfrak{b}$ true v1 v2 = v1	isempty? error$_\mathfrak{l}$ = error$_\mathfrak{b}$
cond$_\mathfrak{b}$ false v1 v2 = v2	cond$_\mathfrak{a}$ error$_\mathfrak{b}$ x y = error$_\mathfrak{a}$
cond$_\mathfrak{l}$ true l1 l2 = l1	cond$_\mathfrak{b}$ error$_\mathfrak{b}$ x y = error$_\mathfrak{b}$
cond$_\mathfrak{l}$ false l1 l2 = l2	cond$_\mathfrak{l}$ error$_\mathfrak{b}$ x y = error$_\mathfrak{l}$

Безопасная кр. пара: $\langle$ error$_\mathfrak{a}$, car error$_\mathfrak{l}$$\rangle$ (правила car(cons x l) = x и cons error$_\mathfrak{a}$ l = error$_\mathfrak{l}$).

Пример

Аксиомы списка	Аксиомы ошибки
car(cons x l) = x	car nil = error$_a$
cdr(cons x l) = l	cdr nil = error$_l$
isempty? nil = true	cons error$_a$ l = error$_l$
isempty? (cons x l) = false	cons x error$_l$ = error$_l$
cond$_a$ true x y = x	car error$_l$ = error$_a$
cond$_a$ false x y = y	cdr error$_l$ = error$_l$
cond$_b$ true v1 v2 = v1	isempty? error$_l$ = error$_b$
cond$_b$ false v1 v2 = v2	cond$_a$ error$_b$ x y = error$_a$
cond$_l$ true l1 l2 = l1	cond$_b$ error$_b$ x y = error$_b$
cond$_l$ false l1 l2 = l2	cond$_l$ error$_b$ x y = error$_l$

Безопасная кр. пара: $\langle$ error$_a$, car error$_l\rangle$ (правила car(cons x l) = x и cons error$_a$ l = error$_l$).

Проблемная кр. пара: $\langle$ l, cdr error$_l\rangle$ (правила cdr(cons x l) = l и cons error$_a$ l = error$_l$). Спецификация противоречива.

Исправление ошибок

car(cons x l) = x

cdr(cons x l) = l

isempty? nil = true

isempty? (cons x l) = false

$\text{cond}_{\mathfrak{a}}$ true x y = x

$\text{cond}_{\mathfrak{a}}$ false x y = y

$\text{cond}_{\mathfrak{b}}$ true v1 v2 = v1

$\text{cond}_{\mathfrak{b}}$ false v1 v2 = v2

$\text{cond}_{\mathfrak{l}}$ true l1 l2 = l1

$\text{cond}_{\mathfrak{l}}$ false l1 l2 = l2

$\text{error?}_{\mathfrak{l}}$ $\text{error}_{\mathfrak{l}}$ = true

car nil = $\text{error}_{\mathfrak{a}}$

cdr nil = $\text{error}_{\mathfrak{l}}$

cons $\text{error}_{\mathfrak{a}}$ l = $\text{error}_{\mathfrak{l}}$

cons x $\text{error}_{\mathfrak{l}}$ = $\text{error}_{\mathfrak{l}}$

car $\text{error}_{\mathfrak{l}}$ = $\text{error}_{\mathfrak{a}}$

cdr $\text{error}_{\mathfrak{l}}$ = $\text{error}_{\mathfrak{l}}$

isempty? $\text{error}_{\mathfrak{l}}$ = $\text{error}_{\mathfrak{b}}$

$\text{cond}_{\mathfrak{a}}$ $\text{error}_{\mathfrak{b}}$ x y = $\text{error}_{\mathfrak{a}}$

$\text{cond}_{\mathfrak{b}}$ $\text{error}_{\mathfrak{b}}$ x y = $\text{error}_{\mathfrak{b}}$

$\text{cond}_{\mathfrak{l}}$ $\text{error}_{\mathfrak{b}}$ x y = $\text{error}_{\mathfrak{l}}$

$\text{error?}_{\mathfrak{l}}$ nil = false

Исправление ошибок

~~car(cons x l) = x~~

~~cdr(cons x l) = l~~

isempty? nil = true

~~isempty? (cons x l) = false~~

cond$_a$ true x y = x

cond$_a$ false x y = y

cond$_b$ true v1 v2 = v1

cond$_b$ false v1 v2 = v2

cond$_l$ true l1 l2 = l1

cond$_l$ false l1 l2 = l2

error?$_l$ error$_l$ = true

car nil = error$_a$

cdr nil = error$_l$

cons error$_a$ l = error$_l$

cons x error$_l$ = error$_l$

car error$_l$ = error$_a$

cdr error$_l$ = error$_l$

isempty? error$_l$ = error$_b$

cond$_a$ error$_b$ x y = error$_a$

cond$_b$ error$_b$ x y = error$_b$

cond$_l$ error$_b$ x y = error$_l$

error?$_l$ nil = false

error?$_l$ (cons x l) = cond$_b$ (error?$_a$ x) true
(cond$_b$ (error?$_l$ l) true false)

car(cons x l) = cond$_a$ (error?$_a$ x) error$_a$
(cond$_a$ (error?$_l$ l) error$_a$ x)

...и т.д. для error?$_a$ *и* error?$_b$ *и для двух других проблемных правил.*

Алгоритм Кнута–Бендикса

Пополнение правилами переписывания по критическим парам не меняет отношение доказуемого равенства в TRS, но может плохо повлиять на завершаемость $\Rightarrow$ пополнение должно контролироваться нетеровым (wfo) порядком $\preceq$.

Пусть дана TRS $\mathcal{T}$, доказуемо завершающаяся в ФуМА $\mathcal{A}$ с wfo $\preceq$. Будем расширять $\mathcal{T}$ правилами $L_i \to R_i$, где $\langle L_i, R_i \rangle$ — критические пары и $R_i^{\mathcal{A}} \preceq L_i^{\mathcal{A}}$ до неподвижной точки расширения. Результат — конфлюэнтная $\mathcal{T}$.

Проверка алг.типа данных с помощью TRS

- Анализ всех критических пар конечен.
- Если удалось получить конфлюэнтную систему пополнением, тогда легко проверить, корректны ли выполняющиеся в ней эквивалентности, построив нормальные формы всех термов.
- Если нашлась критическая пара вида $\langle x, t \rangle$, тогда спецификация противоречива.

Бесконечная пополняемость

Рассмотрим trs с двумя правилами:
$u(x) + u(y) \to u(x + y), \quad (x + y) + z \to x + (y + z)$.
Для доказательства завершаемости в ней положим
$x +^{\mathcal{A}} y = (y)^x$, $u^{\mathcal{A}}(x) = x^2$.

Бесконечная пополняемость

Рассмотрим trs с двумя правилами:
$u(x) + u(y) \to u(x + y), \quad (x + y) + z \to x + (y + z).$
Для доказательства завершаемости в ней положим
$x +^{\mathcal{A}} y = (y)^x$, $u^{\mathcal{A}}(x) = x^2$.

Первая критическая пара: $\langle u(x) + (u(y) + z), u(x + y) + z \rangle$.
Пополним trs правилом $u(x + y) + z \to u(x) + (u(y) + z)$ и проверим, сохранится ли монотонность в ФуМА.

Бесконечная пополняемость

Рассмотрим trs с двумя правилами:
$u(x) + u(y) \to u(x+y), \quad (x+y)+z \to x+(y+z)$.
Для доказательства завершаемости в ней положим
$x +^{\mathcal{A}} y = (y)^x$, $u^{\mathcal{A}}(x) = x^2$.

Первая критическая пара: $\langle u(x) + (u(y)+z), u(x+y)+z \rangle$.
Пополним trs правилом $u(x+y)+z \to u(x) + (u(y)+z)$ и проверим, сохранится ли монотонность в ФуМА.

Каждая новая критическая пара
$\langle u^n(x) + (u^n(y)+z), u^n(x+y)+z \rangle$ будет порождать очередное правило переписывания
$u^n(x+y)+z \to u^n(x) + (u^n(y)+z)$, убывающее в ФуМА.

Вычисление базисов Грёбнера

Зададим упорядочение $\lhd$ на n-ках из $\mathbb{N}$ (степенях переменных в мономе) такое, что:

- $\forall s([0,\ldots,0] \lhd s)$;
- $\forall s, t_1, t_2(t_1 \lhd t_2 \Rightarrow s + t_1 \lhd s + t_2)$.

Инициальный моном $in_\lhd(g)$ полинома g — это моном, больший всех других мономов g в смысле $\lhd$.

Выберем мономиальный порядок $\lhd$. Найти базис G идеала I полиномов над полем такой, что инициальный идеал $in_\lhd(I) = \langle in_\lhd(g) \mid g \in G \rangle$ (порождается инициальными мономами полиномов из G).

Критерий Бюхбергера: G — базис Грёбнера, если все $r = \frac{max(in_\lhd(g_i), in_\lhd(g_j))}{in_\lhd(g_i))} * g_i - \frac{max(in_\lhd(g_i), in_\lhd(g_j))}{in_\lhd(g_j))} * g_j$ имеют разложение в G. Операция максимума max — поэлементная.

Алгоритмы Бюхбергера и Кнута–Бендикса

1. Если в F выполнен критерий Бюхбергера $\Rightarrow$ базис построен.
2. Иначе существует критическая пара $\langle g_i, g_j \rangle$, порождающая неразложимый r. Добавляем r в базис и продолжаем.

Алгоритмы Бюхбергера и Кнута–Бендикса

1. Если в F выполнен критерий Бюхбергера $\Rightarrow$ базис построен.
2. Иначе существует критическая пара $\langle g_i, g_j \rangle$, порождающая неразложимый r. Добавляем r в базис и продолжаем.

Конечность вычисления lfp (наименьшей неподвижной точки) гарантируется теоремой Гильберта о конечнопорожденности идеалов.

Алгоритмы Бюхбергера и Кнута–Бендикса

1. Если в F выполнен критерий Бюхбергера $\Rightarrow$ базис построен.
2. Иначе существует критическая пара $\langle g_i, g_j \rangle$, порождающая неразложимый r. Добавляем r в базис и продолжаем.

Конечность вычисления lfp (наименьшей неподвижной точки) гарантируется теоремой Гильберта о конечнопорожденности идеалов.

Алгоритм Бюхбергера (почти) моделируется алгоритмом пополнения Кнута–Бендикса над алгеброй с правилами переписывания — аксиомами кольца. Для каждого полинома $p \in F$, где $p = in_{\triangleleft} p + p'$, добавляем правила $in_{\triangleleft} p \to p'$ и $in_{\triangleleft} px \to p' * x$.

Алгоритмы Бюхбергера и Кнута–Бендикса

1. Если в F выполнен критерий Бюхбергера $\Rightarrow$ базис построен.
2. Иначе существует критическая пара $\langle g_i, g_j \rangle$, порождающая неразложимый r. Добавляем r в базис и продолжаем.

Конечность вычисления lfp (наименьшей неподвижной точки) гарантируется теоремой Гильберта о конечнопорожденности идеалов.

Алгоритм Бюхбергера (почти) моделируется алгоритмом пополнения Кнута–Бендикса над алгеброй с правилами переписывания — аксиомами кольца. Для каждого полинома $p \in F$, где $p = \mathrm{in}_{\triangleleft} p + p'$, добавляем правила $\mathrm{in}_{\triangleleft} p \to p'$ и $\mathrm{in}_{\triangleleft} p x \to p' * x$.

Проблема: коммутативность и ассоциативность убивают нётеровость trs и завершаемость пополнения.

Свободные модели

Рассмотрим сигнатуру Σ и множество формул логики первого порядка P над Σ. Алгебра $\mathcal{A}$ называется свободной моделью (loose model) над $\langle \Sigma, \mathrm{P} \rangle$, если $\mathcal{A} \models \mathrm{P}$.

Свободные модели

Рассмотрим сигнатуру Σ и множество формул логики первого порядка P над Σ. Алгебра $\mathcal{A}$ называется свободной моделью (loose model) над $\langle \Sigma, P \rangle$, если $\mathcal{A} \models P$.

Теорема об изоморфизме

Пусть $\mathcal{A}$, $\mathcal{A}'$ — алгебры, ϕ — изоморфизм $\mathcal{A} \to \mathcal{A}'$. Тогда для всякой FO-формулы $P(X)$ и окружения $\alpha(X)$ выполняется эквивалентность $\mathcal{A}, \alpha \models P \Leftrightarrow \mathcal{A}', \phi \circ \alpha \models P$.

Свободные модели

Рассмотрим сигнатуру Σ и множество формул логики первого порядка P над Σ. Алгебра $\mathcal{A}$ называется свободной моделью (loose model) над $\langle \Sigma, P \rangle$, если $\mathcal{A} \models P$.

Теорема об изоморфизме

Пусть $\mathcal{A}$, $\mathcal{A}'$ — алгебры, ϕ — изоморфизм $\mathcal{A} \to \mathcal{A}'$. Тогда для всякой FO-формулы $P(X)$ и окружения $\alpha(X)$ выполняется эквивалентность $\mathcal{A}, \alpha \models P \Leftrightarrow \mathcal{A}', \phi \circ \alpha \models P$.

Невыразимость: $\mathcal{A}, \alpha(x) \models P(x) \Rightarrow \mathcal{A} \models \forall x P(x)$

Свободные модели

Рассмотрим сигнатуру Σ и множество формул логики первого порядка P над Σ. Алгебра $\mathcal{A}$ называется свободной моделью (loose model) над $\langle \Sigma, P \rangle$, если $\mathcal{A} \models P$.

Теорема об изоморфизме

Пусть $\mathcal{A}$, $\mathcal{A}'$ — алгебры, ϕ — изоморфизм $\mathcal{A} \to \mathcal{A}'$. Тогда для всякой FO-формулы $P(X)$ и окружения $\alpha(X)$ выполняется эквивалентность $\mathcal{A}, \alpha \models P \Leftrightarrow \mathcal{A}', \phi \circ \alpha \models P$.

Невыразимость: $\mathcal{A}, \alpha(x) \models P(x) \Rightarrow \mathcal{A} \models \forall x P(x)$

Рассмотрим алгебру над $\mathbb{R}$ с 0 и $+$ (со стандартными аксиомами). Единственные предикаты от одной переменной, выразимые в этой алгебре и не являющиеся общезначимыми — это $x = 0$ и $x \neq 0$.

Выразимость в модели $\mathbb{R}$

Рассмотрим алгебру $\mathcal{R}$ над $\mathbb{R}$ с константами 0 и 1 и операциями $+$, $*$ (в стандартной аксиоматике).

- Можно ли в $\mathcal{R}$ выразить $>$?
- Пусть ϕ — автоморфизм $\mathcal{R} \to \mathcal{R}$. Пусть q — рациональное число. Охарактеризовать предикат $P(\phi(q), q)$.
- Охарактеризовать все автоморфизмы $\mathcal{R}$.

Виды программных семантик

1. Аксиоматическая — логические правила вывода, описывающие пути вычислений. Определяет равенство между программами.

Виды программных семантик

1. Аксиоматическая — логические правила вывода, описывающие пути вычислений. Определяет равенство между программами.
2. Денотационная — алгебраическая модель, определяющая функцию означивания (денотат): $[\![\mathrm{P}]\!]$.
   - Инициальные модели — + рекурсия;
   - Свободные модели — выразимость.

Виды программных семантик

1. Аксиоматическая — логические правила вывода, описывающие пути вычислений. Определяет равенство между программами.
2. Денотационная — алгебраическая модель, определяющая функцию означивания (денотат): $[\![P]\!]$.
   - Инициальные модели — + рекурсия;
   - Свободные модели — выразимость.
3. Операционная — описание исполнения программ в конкретной модели вычислений.