Математическая логика: 3

Станислав Олегович Сперанский

Санкт-Петербургский государственный университет

Санкт-Петербург 2020

О кодировании термов и формул

Чтобы отождествлять алгоритмические проблемы над дискретным типом данных с вычислением функций над $\mathbb{N}$, прибегают к кодированию, или нумерации, входов.

Нас интересует нумерация для логики первого порядка над σ. Для наглядности возьмём в качестве σ сигнатуру арифметики.

Замечание

В контексте изучения алгоритмических вопросов мы ограничиваемся конечными и счётными сигнатурами, причём счётность должна быть в некотором смысле «эффективной».

Определим $\# : \mathrm{Term}_\sigma \cup \mathrm{Form}_\sigma \to \mathbb{N}$ следующим образом:

$$
\begin{aligned}
\#(v_n) &:= \mathrm{pair}(1, n);\\
\#(0) &:= \mathrm{pair}(2, 0);\\
\#(\mathrm{s}(t)) &:= \mathrm{pair}(3, \#(t));\\
\#(t_1 + t_2) &:= \mathrm{pair}(4, \mathrm{pair}(\#(t_1), \#(t_2)));\\
\#(t_1 \cdot t_2) &:= \mathrm{pair}(5, \mathrm{pair}(\#(t_1), \#(t_2)));\\
\#(t_1 = t_2) &:= \mathrm{pair}(6, \mathrm{pair}(\#(t_1), \#(t_2)));\\
\#(\neg\Psi) &:= \mathrm{pair}(7, \#(\Psi));\\
\#(\Psi \wedge \Theta) &:= \mathrm{pair}(8, \mathrm{pair}(\#(\Psi), \#(\Theta)));\\
\#(\Psi \vee \Theta) &:= \mathrm{pair}(9, \mathrm{pair}(\#(\Psi), \#(\Theta)));\\
\#(\Psi \to \Theta) &:= \mathrm{pair}(10, \mathrm{pair}(\#(\Psi), \#(\Theta)));\\
\#(\forall v_n \Psi) &:= \mathrm{pair}(11, \mathrm{pair}(n, \#(\Psi)));\\
\#(\exists v_n \Psi) &:= \mathrm{pair}(12, \mathrm{pair}(n, \#(\Psi))).
\end{aligned}
$$

Предложение

$\#$ *инъективна.*

Доказательство.

Очевидно, $\#[\mathrm{Term}_\sigma] \cap \#[\mathrm{Form}_\sigma] = \varnothing$, а потому достаточно показать инъективность

$$\#_{\mathsf{T}} := \# \restriction_{\mathrm{Term}_\sigma} \quad \text{и} \quad \#_{\mathsf{F}} := \# \restriction_{\mathrm{Form}_\sigma}.$$

Докажем, что для любых $t, t' \in \mathrm{Term}_\sigma$,

$$\#(t) = \#(t') \implies t = t'.$$

Сделаем это индукцией по построению t. Пусть $\#(t) = \#(t')$.

. . .

Доказательство (продолжение).

- Если $t = v_n$, где $n \in \mathbb{N}$, то, очевидно, $t' = v_n$.
- Если $t = 0$, то, очевидно, $t' = 0$.
- Предположим, что $t = \mathsf{s}(t_1)$. Тогда $\mathsf{left}(\#(t)) = 3 = \mathsf{left}(\#(t'))$, а потому $t' = \mathsf{s}(t_1')$ для некоторого t_1'. При этом

$$\#(t_1) \;=\; \mathsf{right}(\#(t)) \;=\; \mathsf{right}(\#(t')) \;=\; \#(t_1'),$$

  откуда $t_1 = t_1'$, в силу индукционной гипотезы.
- Случаи $t = t_1 + t_2$ или $t = t_1 \cdot t_2$ разбираются аналогично.

Значит, $\#_{\mathsf{T}}$ инъективна. Аналогично для $\#_{\mathsf{F}}$. □

Стало быть, $\mathrm{Term}_\sigma \cup \mathrm{Form}_\sigma$ можно мысленно отождествить с $\mathrm{range}\,\#$.

Замечание

Ясно, что для любых $n, m \in \mathbb{N}$,

$$\begin{aligned} \mathrm{pair}\,(n, m) &= 2^n \cdot (2m + 1) - 1 \\ &\geqslant \max\{2^n - 1, 2m\} \\ &\geqslant \max\{n, m\}, \end{aligned}$$

а в случае, когда $n \neq 0$, мы имеем

$$\mathrm{pair}\,(n, m) \;\geqslant\; 4m + 1 \;>\; m.$$

В частности, легко показать, что для любых $o_1, o_2 \in \mathrm{Term}_\sigma \cup \mathrm{Form}_\sigma$,

$$o_1 \preccurlyeq o_2 \quad \text{и} \quad o_1 \neq o_2 \quad \Longrightarrow \quad \#(o_1) < \#(o_2).$$

Это позволяет пользоваться возвратной индукцией/рекурсией.

Предложение

$\#\,[\mathrm{Term}_\sigma]$ *и* $\#\,[\mathrm{Form}_\sigma]$ *разрешимы.*

Доказательство.

Хар. функцию $\#\,[\mathrm{Term}_\sigma]$ можно вычислить посредством следующего алгоритма.

0: Положим $S := \{n\}$.

1: Если $S = \varnothing$, то выдадим 1. Иначе положим $k := \max S$.

2: Если $\mathrm{left}\,(k) = 0$ или $\mathrm{left}\,(k) > 5$, то выдадим 0.

3: Если $\mathrm{left}\,(k) = 1$ или $k = \mathrm{pair}\,(2, 0)$, то положим $S := S \setminus \{k\}$ и GoTo 1.

...

Доказательство (продолжение).

4: Если $\mathrm{left}(k) = 3$, то положим

$$S := (S \setminus \{k\}) \cup \{\mathrm{right}(k)\}$$

и `GoTo 1`.

5: Если $\mathrm{left}(k) = 4$ или $\mathrm{left}(k) = 5$, то положим

$$S := (S \setminus \{k\}) \cup \{\mathrm{left}(\mathrm{right}(k)), \mathrm{right}(\mathrm{right}(k))\}$$

и `GoTo 1`.

Здесь n — это значение аргумента на входе.

Алгоритм всегда завершает работу, поскольку в случае добавления к S новых элементов (см. 4 и 5) уменьшается $\max S$.

Аналогично для $\#[\mathrm{Form}_\sigma]$. □

Далее, можно, например, построить алгоритмы A, B, C, D такие, что:

- A по кодам x и t вычисляет, входит ли x в t;
- B по кодам x и Φ вычисляет, свободна ли x в Φ;
- C по кодам x, t и Φ вычисляет, свободен ли t для x в Φ;
- D по кодам x, t и Φ вычисляет код $\Phi(x/t)$.

Здесь x, t и Φ пробегают Var, Term_σ и Form_σ соответственно. В частности, мы получаем разрешимость $\#[\mathrm{Sent}_\sigma]$.

Грубо говоря, мы можем делать с кодами то же самое, что с термами и формулами, руководствуясь интуицией и здравым смыслом.

Замечание

Так как в pair используется экспонента, для целей теории сложности требуется другая, вычислимая за полиномиальное время биекция. В литературе популярна функция

$$\lambda n.\lambda m.\left[\frac{(n+m+1)(n+m)}{2}+m\right].$$

называемая канторовской нумерующей функцией. В качестве упражнения проверьте, что она является биекцией из $\mathbb{N}\times\mathbb{N}$ на $\mathbb{N}$.

Для простоты давайте считать σ конечной. В дальнейшем мы будем предполагать наличие фикс. процедуры эф. кодирования σ-термов и σ-формул и нередко отождествлять объекты с их кодами.

Для удобства для каждого $\Gamma \subseteq \mathrm{Sent}_\sigma$ обозначим

$$[\Gamma] \;:=\; \{\Phi \in \mathrm{Sent}_\sigma \mid \Gamma \vdash \Phi\},$$

т.е. $[\Gamma]$ — это дедуктивное замыкание Γ; ясно, что $[\Gamma] = \mathrm{Th}\,(\mathrm{Mod}\,(\Gamma))$.

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *перечислимо. Тогда* $[\Gamma]$ *перечислимо.*

Доказательство.

Не ограничивая общности, можно считать, что Γ непусто, поскольку $[\varnothing] = [\{\Phi\}]$, где Φ — какое-н. σ-предложение, выводимое из $\varnothing$.

Очевидно, Form_σ, будучи разрешимым, перечислимо. Так как Form_σ и Γ непусты, сущ. вычислимые $f, g : \mathbb{N} \to \mathrm{Form}_\sigma$ такие, что

$$\operatorname{range} f \;=\; \mathrm{Form}_\sigma \quad \text{и} \quad \operatorname{range} g \;=\; \Gamma.$$

Тогда $\chi^*_{[\Gamma]}$ можно вычислить посредством следующего алгоритма.

0: Положим $k := 1$.

1: Вычислим $f(0), \ldots, f(k)$, $g(0), \ldots, g(k)$. Затем переберем все последовательности элементов $\{f(0), \ldots, f(k)\}$ длины не более k: если среди них есть вывод Φ из $\{g(0), \ldots, g(k)\}$, то выдадим 1. Иначе положим $k := k + 1$ и GoTo 1.

Здесь $\Phi \in \mathrm{Sent}_\sigma$ — значение аргумента на входе. □

Следствие

$[\varnothing]$ *перечислимо.* □

Следствие

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *конечно. Тогда* $[\Gamma]$ *перечислимо.* □

Следствие

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *разрешимо. Тогда* $[\Gamma]$ *перечислимо.* □

Пример

Теория абелевых групп перечислима, так как она задаётся конечным множеством предложений. Далее, теории групп без кручения и делимых групп будут перечислимы, так как каждую из них можно задать разрешимым множеством предложений.

По аналогии с проп. логикой $\Gamma \subseteq \mathrm{Sent}_\sigma$ называется полным, если для любого $\Phi \in \mathrm{Sent}_\sigma$ верно $\Phi \in \Gamma$ или $\neg\Phi \in \Gamma$.

Замечание

Разумеется, когда Γ непротиворечиво и полно,

$$\Gamma \;=\; \mathrm{Th}\,(\mathfrak{A}) \quad \text{для всех } \mathfrak{A} \in \mathrm{Mod}\,(\Gamma),$$

а потому Γ можно отождествить с $\mathrm{Th}\,(\mathfrak{A})$ для какой-нибудь особой $\mathfrak{A}$.

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *непротиворечиво. Если* $[\Gamma]$ *перечислимо и полно, то* $[\Gamma]$ *разрешимо.*

Доказательство.

Пусть $[\Gamma]$ перечислимо и полно. Очевидно, $[\Gamma]$ непусто, а значит, найдётся вычислимая $f : \mathbb{N} \to \mathrm{Form}_\sigma$ такая, что $\mathrm{range}\, f = [\Gamma]$. Тогда $\chi_{[\Gamma]}$ можно вычислить посредством следующего алгоритма.

0: Положим $k := 0$.

1: Вычислим $f(k)$. Если $f(k)$ равно Φ, то выдадим 1. Если $f(k)$ равно $\neg\Phi$, то выдадим 0. Иначе положим $k := k + 1$ и GoTo 1.

Здесь $\Phi \in \mathrm{Sent}_\sigma$ — значение аргумента на входе.

Поскольку $[\Gamma]$ полно, алгоритм всегда завершает работу, причём Φ и $\neg\Phi$ не могут оба принадлежать $[\Gamma]$, в силу непротиворечивости Γ. □

Замечание

Пожалуй, основной недостаток этого подхода заключается в отсутствии явной оценки на количество шагов, нужное для решения вопроса о принадлежности σ-предложения к $[\Gamma]$.

Следствие

Для всякой σ-структуры $\mathfrak{A}$, если $\mathrm{Th}(\mathfrak{A})$ *перечислимо, то* $\mathrm{Th}(\mathfrak{A})$ *разр.*

Доказательство.

Достаточно заметить, что $\mathrm{Th}(\mathfrak{A})$ непротиворечиво и полно. $\square$

Замечание

Значит, чтобы доказать разрешимость $\mathrm{Th}(\mathfrak{A})$, достаточно построить перечислимое $\Gamma \subseteq \mathrm{Sent}_\sigma$ такое, что $[\Gamma] = \mathrm{Th}(\mathfrak{A})$.

Метод элиминации кванторов

Обозначим за $\mathrm{Form}_\sigma^\circ$ множество всех бескванторных σ-формул.

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$. Говорят, что Γ допускает (эффективную) элиминацию кванторов, если существует (вычислимая) функция τ, которая по каждой $\Phi \in \mathrm{Form}_\sigma$ строит $\tau(\Phi) \in \mathrm{Form}_\sigma^\circ$ такую, что

$$\Gamma \vdash \Phi \leftrightarrow \tau(\Phi) \quad \text{и} \quad \mathrm{FV}(\tau(\Phi)) \subseteq \mathrm{FV}(\Phi).$$

Замечание

Для удобства мы будем считать, что в нашем языке имеются специальные логические константы

$$\top \quad \text{и} \quad \bot,$$

которые являются замкнутыми атомарными σ-формулами. Поэтому $\mathrm{Atom}_\sigma \cap \mathrm{Sent}_\sigma$ будет непусто даже в случае, когда $\mathrm{Const}_\sigma = \varnothing$.

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *допускает эф. элиминацию кванторов, и* $[\Gamma] \cap \mathrm{Form}^\circ_\sigma$ *разрешимо. Тогда* $[\Gamma]$ *разрешимо.*

Доказательство.

Пусть τ реализует эффективную элиминацию кванторов в Γ. Тогда, в частности, для любого $\Phi \in \mathrm{Sent}_\sigma$,

$$\Gamma \vdash \Phi \quad \Longleftrightarrow \quad \Gamma \vdash \tau(\Phi),$$

что можно переписать как

$$\Phi \in [\Gamma] \quad \Longleftrightarrow \quad \tau(\Phi) \in [\Gamma] \cap \mathrm{Form}^\circ_\sigma.$$

Стало быть, $[\Gamma] \leqslant [\Gamma] \cap \mathrm{Form}^\circ_\sigma$. Поэтому из разрешимости $[\Gamma] \cap \mathrm{Form}^\circ_\sigma$ следует разрешимость $[\Gamma]$. $\square$

Предложение

Пусть существует вычислимая функция ρ, которая по каждой σ-формуле Φ вида $\exists x\,\Psi$, где Ψ бескванторная, строит бескванторную σ-формулу $\rho(\Phi)$ такую, что

$$\Gamma \vdash \Phi \leftrightarrow \rho(\Phi) \quad \textit{и} \quad \mathrm{FV}(\rho(\Phi)) \subseteq \mathrm{FV}(\Phi).$$

Тогда Γ допускает эффективную элиминацию кванторов.

Доказательство.

Определим нужную τ по рекурсии следующим образом.

- Если Φ бескванторная, то $\tau(\Phi) := \Phi$.

. . .

Доказательство (продолжение).

- Если $\Phi = \Psi \circ \Theta$, где $\circ \in \{\wedge, \vee, \to\}$, то $\tau(\Phi) := \tau(\Psi) \circ \tau(\Theta)$.
- Если $\Phi = \neg\Psi$, то $\tau(\Phi) := \neg\tau(\Psi)$.
- Если $\Phi = \exists x\, \Psi$, то $\tau(\Phi) := \rho(\exists x\, \tau(\Psi))$.
- Если $\Phi = \forall x\, \Psi$, то $\tau(\Phi) := \neg\rho(\exists x\, \neg\tau(\Psi))$.

Легко проверить, что для всех $\Phi \in \mathrm{Form}_\sigma$,

$$\Gamma \vdash \Phi \leftrightarrow \tau(\Phi) \quad \text{и} \quad \mathrm{FV}(\tau(\Phi)) \subseteq \mathrm{FV}(\Phi),$$

т.е. τ реализует эффективную элиминацию кванторов в Γ. □

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *допускает элиминацию кванторов,* $[\Gamma]$ *перечислимо. Тогда* Γ *допускает эффективную элиминацию кванторов.*

Доказательство.

Очевидно, $[\Gamma]$ непусто, а значит, найдётся вычислимая $f : \mathbb{N} \to \mathrm{Form}_\sigma$ такая, что $\operatorname{range} f = [\Gamma]$. Рассмотрим следующий алгоритм.

`0:` Положим $k := 0$.

`1:` Вычислим $f(k)$. Если $f(k)$ имеет вид $\Phi \leftrightarrow \Psi$, где $\Psi \in \mathrm{Form}_\sigma^\circ$, то выдадим Ψ. Иначе положим $k := k + 1$ и `GoTo 1`.

Здесь $\Phi \in \mathrm{Form}_\sigma$ — значение аргумента на входе.

Раз Γ допускает элиминацию кванторов, алгоритм всегда завершает работу. Вычисляемая им функция τ является искомой. $\square$

Замечание

Недостаток этого подхода заключается в отсутствии явной оценки на количество шагов, нужное для нахождения эквивалентной по модулю Г бескванторной σ-формулы.

С другой стороны, в (неэффективной) элиминации кванторов можно применять более универсальные по своей природе теоретико-модельные методы, однако о них мы практически не говорили.