Автоматы, разрешимость монадических теорий S1S и S2S и приложения

Владислав Макаров

30 октября

Общие замечания про решаемые задачи

- Всё будет в пределах классической логики.
- Главная (?) задача логики: по утверждению про какие-то объекты (натуральные числа, множества, ...), сказать, верно ли оно.
- Почти всегда алгоритмически неразрешима.
- Но иногда всё же разрешима.
- Аксиоматизация и выводимость нас не будут сильно волновать.
- Пример: теорема Тарского про $\langle \mathbb{R}, 0, 1, +, \cdot \rangle$. Делая элиминацию кванторов, мы думаем в терминах того, что мы проверяем какое-то утверждение про настоящие вещественные числа. Формальный вывод этого утверждения нас волнует в меньшей степени.
- Изоморфизмом и элементарной эквивалентностью моделей мы будем пользоваться лишь совсем чуть-чуть.

Что такое S1S?

- Первопорядковая теория $\langle \mathbb{N}, =, \mathrm{succ} \rangle$ (0 выражается), где предикат $\mathrm{succ}(x, y)$ говорит, верно ли, что $y = x + 1$.

\+ Очевидно разрешима (перебрать порядок переменных и то, больше ли разрывы между ними, чем 1 или нет).

– Абсолютно бесполезна, в таком языке не выразить даже $x \leqslant y$, тем более $x + y = z$ и ещё много простых предикатов.

- Добавим кванторы по подмножествам натуральных чисел!
- И предикаты $X \subseteq Y$, $x \in X$, конечно же.
- Получили монадическую теорию S1S (*монад*ическую, потому что подмножества — *одноместные* предикаты).

\+ Теперь можно выразить, что $x \leqslant y$. А именно, наименьшее по включению множество, содержащее x и замкнутое относительно взятия последователя, должно содержать y.

- $P(Z, x) := x \in Z \wedge (\forall y, z\ ((y \in Z \wedge \mathrm{succ}(y, z)) \to z \in Z))$
- $(x \leqslant y) := \exists X\ (P(X, x) \wedge (\forall Z\ (P(Z, x) \to X \subseteq Z)) \wedge y \in X)$

Почему разрешимость S1S полезна?

- Проинтерпретируем арифметику Пресбургера $\langle \mathbb{N}, +, =, 0, 1 \rangle$ в S1S.
- Раз S1S разрешима, то и арифметика Пресбургера — тоже.
- Мы и так это знали, но всё равно прикольно.
- $n \in N \to$ конечное подмножество $\mathbb{N}$ (двоичная запись).
- Конечность выразима в S1S: $\mathrm{Finite}(X) := \exists y \forall x \ (x \in X \to x \leqslant y)$.
- Интерпретация $a + b = c$: есть множества A, B, C, угадаем, чему будет равен перенос D при сложении (он тоже должен быть конечным множеством).
- Если перенос известен, то проверка правильности сложения — локальная вещь (должно выполниться много условий, но каждое из них зависит от поведения A, B, C и D в двух соседних битах).
- У нас как раз в языка есть оператор succ, так что всё сходится!

Тренируемся на кошках: S1SF

- Рассмотрим чуть более простую теорию (S1SF): монадическую теорию всех множеств вида $\{1, 2, \ldots, m\}$ с предикатами $=, \mathrm{succ}, \subseteq, \in$. Утверждение считается верным, если оно верно для всех множеств $\{1, 2, \ldots, m\}$.
- Интересно именно “асимптотическое поведение”, для фиксированного m можно просто всё перебрать. НУО $m \geqslant 2$.
- Эквивалентно, но менее естественно: $\langle =, \subseteq, \mathrm{SUCC} \rangle$, где $\mathrm{SUCC}(X, Y) := ((X = \{x\} \wedge Y = \{x + 1\})$ для какого-то $x \in \mathbb{N})$.
- То, что $x \in \mathbb{N}$ выражается как $\exists Y\ (\mathrm{SUCC}(X, Y) \vee \mathrm{SUCC}(Y, X))$.
- Неестественно, но мало предикатов, легко будет строить автомат.

Обычные автоматы и S1SF

- Для модели $\{1, 2, \ldots, m\}$ и подмножеств $X_1, X_2, \ldots, X_n$ определим слово $W(m, X_1, X_2, \ldots, X_n) = w_1 w_2 \ldots w_m$ над алфавитом Σ_n размера 2^n, так: w_i соответствует тому, для каких j верно, что $i \in X_j$ (как раз 2^n вариантов).
- В частности, для $n = 0$ это слово над односимвольным алфавитом.
- В чём смысл?

Формула по автомату (скорее приятный бонус)

Теорема

Есть алгоритм, строящий по Σ_n-ДКА A такую S1SF-формулу φ что для любых $m \geqslant 2$ и $X_1, X_2, \ldots X_n$ верно, что
$\{1, 2, \ldots, m\} \models \varphi(X_1, \ldots, X_n) \Leftrightarrow W(m, X_1, \ldots, X_n) \in L(A)$

Доказательство.

Если $q_1, q_2, \ldots, q_d$ — состояния A, то формула будет проверять, что существуют такие $Y_1, Y_2, \ldots, Y_d \subseteq \{1, 2, \ldots, m\}$, описывающие, *когда* A бывал в соответствующем состоянии при чтении $W(m, X_1, \ldots, X_n)$. А именно,
$Y_i := \{\, \ell \mid A$ находится в q_i после чтения первых ℓ букв слова $\}$. Нужно уметь проверять, что угаданные Y_i действительно подходят, но это проверка правильности переходов автомата. Опять-таки, нужно много раз проверить “локальное свойство”. □

Автомат по формуле

Теорема

Есть алгоритм, строящий по S1SF-формуле $\varphi(X_1, X_2, \ldots, X_n)$ *со свободными переменными* X_i *такой* Σ_n*-ДКА* A*, что*
$\{1, 2, \ldots, m\} \models \varphi(X_1, \ldots, X_n) \Leftrightarrow W(m, X_1, \ldots, X_n) \in L(A)$.

Доказательство.

Индукция по сложности формулы. Атомарные формулы $X \subseteq Y$, $X = Y$, $\mathrm{SUCC}(X, Y)$ соответствуют регулярным языкам $\{(00), (01), (11)\}^*$, $\{(00), (11)\}^*$, $(00)^*(10)(01)(00)^*$ соответственно.
Для получения $\overline{\psi}$ и $\psi_1 \wedge \psi_2$ нужно воспользоваться конструкциями для дополнения и пересечения ДКА.
Если же φ выглядит как $\exists X_{n+1}\ (\psi(X_1, X_2, \ldots, X_n, X_{n+1}))$, то нужно на каждом ребре ДКА для ψ “угадывать” бит, соответствующий X_{n+1}. То есть если из вершины раньше исходило два рёбра по символам $(x0)$ и $(x1)$, то теперь будут исходить два ребра по символу (x). $\square$

Разрешимость S1SF

- Воспользуемся предыдущей теоремой для предложения.
- Получим язык L над Σ_0 (односимвольным алфавитом).
- $t^m \in L$ тогда и только тогда, когда $\{1, 2, \ldots, m\} \models \varphi$.
- Интересное следствие: множество тех m, для которых данная S1SF-формула истинна, нестрого периодично.
- Есть ли прямое доказательство этого следствия?
- "Предложение" $\exists X, Y\ (1 \in X \wedge m \in Y \wedge (\forall x \in X\ (x + 1 \in Y)) \wedge (\forall y \in Y, y < m\ (y + 1 \in X))$ верно только для чётных m.
- Ну и вообще, можно любое 1-автоматное множество получить, так как формулу по автомату тоже умеем строить.

Автоматы Мюллера

- Как обычные автоматы, только принимают слова “длины ω”.
- Единственное, что отличается от обычных (не)детерминированных автоматов — условие приёма.
- Бесконечное слово принимается недетерминированным автоматом Мюллера, если существует такое вычисление на этом слове, что множество всех состояний, посещённых бесконечное число раз, лежит в данном подмножестве $F \subseteq 2^Q$ (Q — множество состояний автомата).
- В отличие от автоматов Бюхи и других подобных формализмов, множество F абсолютно произвольное.
- Бесконечные слова — не конечный объект, но автоматы Мюллера — конечные объекты.
- Задача *принадлежности* не особо осмыслена, но задача *пустоты* — вполне себе да.

Детерминизация

Теорема

Для каждого недетерминированного автомата Мюллера есть эквивалентный детерминированный, при этом преобразование вычислимо.

Доказательство.

Поля слишком узки, взрыв по числу состояний — двойная экспонента. □

Разрешимость пустоты

Теорема

Есть алгоритм, который по данному детерминированному автомату Мюллера понимает, пуст ли порождаемый им язык.

Доказательство.

Для каждого элемента F проверим, есть ли вычисление, которое посещает в точности такие состояния бесконечное число раз. Такое вычисление есть тогда и только тогда, когда эти состояния образуют сильно связный подграф, достижимый из начального состояния. $\square$

Автоматы Мюллера к S1S-формулам

Определим бесконечное слово $W(X_1, X_2, \ldots, X_n)$ над алфавитом Σ_n, как мы раньше определяли конечные слова $W(m, X_1, \ldots, X_n)$. Можно доказать те же две теоремы, что и раньше (ДАМ — детерменированный автомат Мюллера).

Теорема

Есть алгоритм, строящий по S1S-формуле $\varphi(X_1, X_2, \ldots, X_n)$ со свободными переменными X_i такой Σ_n-ДАМ A, что
$\mathbb{N} \models \varphi(X_1, \ldots, X_n) \Leftrightarrow W(X_1, \ldots, X_n) \in L(A)$.

Доказательство.

Аналогично S1SF. Важно, что конечность множества выразимы, поэтому, если мы уже знаем Y_i, для проверки принятия автоматом слова достаточно написать огромную ДНФ с литералами, проверяющими бесконечность Y_i. □

S1S-формулы к автоматам Мюллера

Теорема

Есть алгоритм, строящий по S1S-формуле $\varphi(X_1, X_2, \ldots, X_n)$ *со свободными переменными* X_i *такой* Σ_n*-ДАМ* A*, что* $\mathbb{N} \models \varphi(X_1, \ldots, X_n) \Leftrightarrow W(X_1, \ldots, X_n) \in L(A)$.

Доказательство.

Индукция по сложности формулы. Атомарные формулы $X \subseteq Y$, $X = Y$, $\mathrm{SUCC}(X, Y)$ соответствуют "регулярным" языкам $\{(00), (01), (11)\}^\omega$, $\{(00), (11)\}^\omega$, $(00)^*(10)(01)(00)^\omega$ соответственно. Эти языки легко реализовывать с помощью ДАМ: все три выглядят как "возможно, дождаться какого-то простого события, после него крутиться в одном состоянии и проверять условие на букву, если нарушилось, то свалиться в мусор навсегда".
Для $\overline{\psi}$, $\psi_1 \vee \psi_2$ и $\exists X_{n+1}\ (\psi(X_1, X_2, \ldots, X_n, X_{n+1}))$ хватает детерминизации и дополнения. □

Деревья и логика S2S

- S1S значит “second-order, 1 successor”. То есть у любого элемента ровно один последователь.
- S2S — “second-order, 2 successors”
- Раньше было $\mathbb{N}$, теперь $\{0,1\}^*$.
- Первопорядковый язык $\langle =, \varepsilon, \text{Left}, \text{Right} \rangle$, S2S добавляет $\subseteq$.
- Очень мощная теория, но всё ещё разрешимая.
- Например “x — префикс y” выражается как “наименьшее по включению множество, содержащее x и замкнутое относительно Left и Right, содержит y”.
- “x лексикографически меньше y” — как “либо x — префикс y, либо есть такое слово z, что $z0$ — префикс x, а $z1$ — префикс y”.
- Можно выразить S3S, S4S, . . . (не очень удивительно; параллель с тем, как в теории формальных языков, где можно с помощью двух букв симулировать любой конечный алфавит, а с помощью одной нельзя). Даже $S\omega S$.

Теорема и дереве и применение к линейным порядкам

Теорема (теорема о дереве)

Теория S2S разрешима.

- Теория всех не более, чем счётных линейно упорядоченных множеств (с предикатами $=$ и $\leqslant$) разрешима.
- Действительно, множество $A := \{\, x1 \mid x \in \{0,1\}^* \,\}$ определимо в S2S, а также изоморфно $\mathbb{Q}$ как ЛУМ (в качестве неравенства используется лексикографическое сравнение).
- Тогда любое не более чем счётное ЛУМ изоморфно некоторому подмножеству A (следует из классификации счётных линейных порядков).
- Следовательно, утверждение φ про ЛУМы верно, тогда и только тогда, когда верно проинтерпретированное утверждение $\forall B \subseteq A\ (\ldots)$.
- В монадическом языке можно выразить вполне упорядоченность, поэтому на самом деле разрешима даже теория всех не более, чем счётных вполне упорядоченных множеств.

Топология канторова множества и теорема о дереве

- В S2S легко определить множество, являющееся бесконечным путём от корня вниз.
- Можно рассмотреть $\{0,1\}^\omega$ с тихоновской топологией.
- Это канторово множество.
- Подмножествам $\{0,1\}^\omega$ соответствуют какие-то подмножества дерева — объединения соответствующих путей.
- Могли появиться какие-то “фантомные пути”, потому что есть бесконечная последовательность путей, у которых общий префикс с фантомным путём всё больше и больше.
- Фантомный путь — предельная точка этой последовательность настоящих путей.
- Таким образом, получается, что для полного соответствия нужна замкнутость подмножества $\{0,1\}^\omega$ в тихоновской топологии (иначе получится не само множество, а его замыкание).
- Следовательно, монадическая теория $\{0,1\}^\omega$ с ограничением, что кванторы берутся по замкнутым множествам, разрешима.

Вопросы?


Завершение
Вопросы?
Вопросы?
Гаевой, Казменко, Макаров (СПбГУ)
Введение: библиотека C++
21.09.2020
18 / 18
Вопросы?
Вопросы?