Доклады Национальной академии наук Беларуси

2016 **июль–август** **Том 60 № 4**

УДК 510.5

В. Г. НАЙДЕНКО

РЕКУРСИВНОЕ ПРЕДСТАВЛЕНИЕ КЛАССА СЛОЖНОСТИ NP ∩ coNP

(Представлено академиком И. В. Гайшуном)

Институт математики НАН Беларуси, Минск, Беларусь
vladimir.naidenko@gmail.com

Впервые получена рекурсивная представимость одного из базовых классов сложности NP ∩ coNP с использованием полиномиальных недетерминированных машин Тьюринга.

Ключевые слова: вычислительная сложность, рекурсивная представимость.

V. G. NAIDENKO

RECURSIVE PRESENTATION OF THE COMPLEXITY CLASS NP∩coNP

Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus
vladimir.naidenko@gmail.com

Using nondeterministic polynomial time Turing machines, a recursive presentation of the complexity class NP ∩ coNP has been constructed for the first time.

Keywords: computational complexity, recursive presentation.

Класс сложности NP ∩ coNP занимает важное положение в теории вычислительной сложности и играет исключительную роль в криптографии с открытым ключом [1], поскольку последняя во многом основана на задаче факторизации, лежащей в NP ∩ coNP. По определению, язык находится в NP ∩ coNP, если существуют две недетерминированные полиномиальные машины Тьюринга: одна машина для распознавания языка, а вторая машина для распознавания дополнения этого языка. Такие машины называются комплементарными друг другу. Однако требование комплементарности препятствует эффективной характеризации класса NP ∩ coNP. Так, Wojciech Kowalczyk [2] показал, что представление языков из NP ∩ coNP с помощью пар комплементарных машин весьма затруднительно. А именно, если NP ∩ coNP не содержит полной проблемы, то невозможно рекурсивно перечислить все языки из NP ∩ coNP с помощью пар комплементарных машин. Из этого вытекает следующее утверждение. Какую бы мощную формальную математическую теорию (типа арифметики Пеано, теории множеств Цермело–Френкеля и т. д.) мы не взяли, всегда найдется такая пара (T, M) полиномиальных недетерминированных машин Тьюринга, что невозможно доказать их комплементарность в рамках этой теории, а следовательно, доказать принадлежность распознаваемого машиной T языка классу NP ∩ coNP. В связи с этим ведущими специалистами в теории вычислительной сложности предполагалось крайне маловероятным нахождение какого-либо рекурсивного представления класса сложности NP ∩ coNP [3; 4]. Так, Президент Европейской ассоциации по логике и информатике профессор Anuj Dawar в своей работе [3] предполагал, что классы сложности, определяемые семантическими ограничениями на удостоверяющие машины, такие как, например, классы NP ∩ coNP и RP, не допускают очевидных рекурсивных представлений: «...complexity classes that are defined by semantic restrictions on the witnessing machines, such as NP ∩ coNP and RP, do not admit obvious recursive presentations or complete problems and to prove that they do would require fundamental new characterizations of

these classes», «...the natural set of witnesses for NP ∩ coNP is not recursively enumerable». Кроме того, он считал, что нахождение рекурсивного представления для класса NP ∩ coNP требует фундаментально новой характеризации данного класса и явится главным прорывом в теории сложности: «Thus, finding a recursively enumerable set of witnesses would require a fundamentally new characterization of the class and would be a major breakthrough in complexity theory».

Цель исследования – найти рекурсивное представление класса сложности NP ∩ coNP.

Дадим необходимые определения. Пусть Σ – конечный алфавит. Как обычно, через Σ* обозначим множество всех слов (или конечных цепочек) в алфавите Σ. Языком называется некоторое подмножество множества Σ*. Через $|w|$ обозначим длину слова *w*. Язык *L* распознается машиной Тьюринга *T*, если *T* допускает слово *w* (т. е. если *T* останавливается на входе *w* в специальном допускающем состоянии) тогда и только тогда, когда *w* принадлежит *L*. Через *T*(*w*) обозначим предикат, который принимает значение ИСТИНА, если *T* допускает слово *w*; в противном случае, значение *T*(*w*) – ЛОЖЬ.

Множество языков $\{L_i \mid i = 1, 2, ...\}$ называется рекурсивно представимым, если существует рекурсивное перечисление машин Тьюринга $\{T_i \mid i = 1, 2, ...\}$ такое, что выполняются два условия:

1) Для каждого языка из $\{L_i \mid i = 1, 2, ...\}$ существует машина Тьюринга из $\{T_i \mid i = 1, 2, ...\}$, распознающая этот язык.

2) Для каждой машины Тьюринга из $\{T_i \mid i = 1, 2, ...\}$ существует распознаваемый ею язык из $\{L_i \mid i = 1, 2, ...\}$.

Перейдем к рассмотрению класса сложности NP ∩ coNP. Для каждой пары полиномиальных недетерминированных машин Тьюринга (*T*, *M*) сопоставим следующий язык:

$$L_{T,M} \triangleq \{x \in \Sigma^* \mid T(x) \wedge (\forall y \in \Sigma^*)[|y| > \log_2(\log_2(|x|+1)+1) \vee (T(y) \Leftrightarrow \neg M(y))]\}. \quad (1)$$

Покажем, что язык $L_{T,M}$ принадлежит классу NP. Сначала оценим количество времени, достаточное для проверки условия, входящего в определение (1):

$$(\forall y \in \Sigma^*)[|y| > \log_2(\log_2(|x|+1)+1) \vee (T(y) \Leftrightarrow \neg M(y))]. \quad (2)$$

Заметим, нам необходимо проверить соотношение $T(y) \Leftrightarrow \neg M(y)$ для всех цепочек *y* достаточно малой длины, т. е. для $|y| \le \log_2(\log_2(|x|+1)+1)$. Отметим, что проверка отдельного условия $T(y) \Leftrightarrow \neg M(y)$ занимает экспоненциальное время по длине |*y*|. Но поскольку длина |*y*| достаточно мала, то общее время проверки условия (2) будет полиномиально по длине входа |*x*|. Следовательно, язык $L_{T,M}$ принадлежит классу NP и можно представить некоторую полиномиальную недетерминированную машину Тьюринга $D_{T,M}$ для распознавания языка. Работа машины $D_{T,M}$ на входной цепочке $x \in \Sigma^*$ описывается следующим образом.

Для всех цепочек $y \in \Sigma^*$ таких, что $|y| \le \log_2(\log_2(|x|+1)+1)$, машина $D_{T,M}$ моделирует работу машин *T* и *M* на входе *y*. Если для некоторой цепочки *y* окажется, что либо обе машины *T* и *M* допускают *y*, либо обе отвергают *y*, то $D_{T,M}$ отвергает входную цепочку *x* и завершает работу. Иначе, после проверки всех цепочек *y*, машина $D_{T,M}$ начинает работать в точности как машина *T* на входе *x*.

Справедлива следующая теорема.

Т е о р е м а. *Пусть* $\{(T_i, M_i) \mid i = 1, 2, ...\}$ *– рекурсивное перечисление всех пар полиномиальных недетерминированных машин Тьюринга. Тогда, взяв рекурсивное перечисление* $\{D_{T_i,M_i} \mid i = 1, 2, ...\}$, *получим рекурсивное представление класса сложности* NP ∩ coNP *с помощью этих полиномиальных недерминированных машин Тьюринга*.

Д о к а з а т е л ь с т в о. Сначала покажем, что любой язык $L_{T,M}$ из перечисления $\{L_{T_i,M_i} \mid i = 1, 2, ...\}$ находится в классе NP ∩ coNP. Заметим, что если соотношение $T(y) \Leftrightarrow \neg M(y)$ выполняется вообще для всех цепочек *y* (независимо от их длин), то язык $L_{T,M}$ по определению будет принадлежать классу NP ∩ coNP (поскольку в этом случае $L_{T,M}$ будет распознаваться машиной *T*, а его дополнение – машиной *M*). В противном случае, язык $L_{T,M}$ будет конечным множеством, и следовательно, опять $L_{T,M} \in$ NP ∩ coNP. Таким образом, в любом случае мы доказали принадлежность $L_{T,M}$ классу NP ∩ coNP.

Осталось показать, что любой язык L из NP $\cap$ coNP находится в перечислении $\{L_{T_i, M_i} \mid i = 1, 2, ...\}$. Поскольку $L \in$ NP $\cap$ coNP, то существуют полиномиальные недерминированные машины Тьюринга T и M, распознающие язык L и его дополнение $\Sigma^* \setminus L$ соответственно. Так как $\{(T_i, M_i) \mid i = 1, 2, ...\}$ – рекурсивное перечисление всевозможных пар полиномиальных недетерминированных машин Тьюринга, то из этого перечисления найдется такая пара (T_i, M_i), что $T_i = T$ и $M_i = M$. Поскольку условие $T_i(y) \Leftrightarrow \neg M_i(y)$ выполняется для всех цепочек $y \in \Sigma^*$ (независимо от их длин), то условие (2) будет выполняться для всех входных цепочек $x \in \Sigma^*$. Поэтому язык L_{T_i, M_i} распознается не только машиной D_{T_i, M_i}, но и машиной T_i. Следовательно, $L = L_{T_i, M_i}$, так как $T_i = T$. Таким образом, $L \in \{L_{T_i, M_i} \mid i = 1, 2, ...\}$.

Итак, мы показали, что $\{L_{T_i, M_i} \mid i = 1, 2, ...\} =$ NP $\cap$ coNP. Следовательно, $\{D_{T_i, M_i} \mid i = 1, 2, ...\}$ – рекурсивное представление класса сложности NP $\cap$ coNP. Теорема доказана.

Таким образом, впервые получено фундаментально новое описание задач из класса NP $\cap$ coNP. При этом не требуется использование комплементарных пар машин Тьюринга для этой цели. Отметим, что проблема установления комплементарности пары машин Тьюринга алгоритмически неразрешима, что крайне затрудняет (если не делает невозможным) доказательство принадлежности многих задач классу NP $\cap$ coNP. Разработанная нами характеризация задач из класса NP $\cap$ coNP использует без каких-либо ограничений любые пары машин Тьюринга, что дает возможность нахождения множества новых задач в NP $\cap$ coNP. С учетом центральной роли класса NP $\cap$ coNP в криптографии с открытым ключом, новая характеризация имеет не только фундаментальное, но и важное прикладное значение. Кроме того, рекурсивное представление может быть использовано для логической характеризации данного класса сложности [5].

Работа профинансирована Институтом математики НАН Беларуси в рамках Государственной программы фундаментальных исследований «Конвергенция».

Список использованной литературы

1. *Brassard, G.* A Note on Cryptography and NP ∩ CoNP–P / G. Brassard, S. Fortune, J. Hopcroft // Technical Report TR-338, Department of Computer Science, Cornell University. – Ithaca; N.Y., 1978.

2. *Kowalczyk, W.* Some Connections between Representability of Complexity Classes and the Power of Formal Systems of Reasoning / W. Kowalczyk // Proceedings of the Mathematical Foundations of Computer Science. – 1984. – P. 364–369.

3. *Dawar, A.* On Complete Problems, Relativizations and Logics for Complexity Classes / A. Dawar // Lecture Notes in Computer Science. – 2010. – Vol. 6300. – P. 201–207.

4. *Papadimitriou, Ch.* On the Complexity of the Parity Argument and Other Inefficient Proofs of Existence / Ch. Papadimitriou // J. of Computer and System Sciences. – 1994. – Vol. 48, N 3. – P. 498–532.

5. *Naidenko, V.* Logics for complexity classes / V. Naidenko // Logic J. of the IGPL. – 2014. – Vol. 22, N 6. – P. 1075–1093.

Поступило в редакцию 15.02.2016