

УДК 510.5

В.Г. Найденко

АЛГОРИТМИЧЕСКОЕ ПЕРЕЧИСЛЕНИЕ ЗАДАЧ В КЛАССЕ $NP \cap coNP$

Рассматривается проблема рекурсивного (алгоритмического) представления класса сложности $NP \cap coNP$. Предлагается новый метод алгоритмического перечисления всех задач в классе сложности $NP \cap coNP$ с использованием полиномиальных недетерминированных машин Тьюринга.

Введение

Класс сложности $NP \cap coNP$ 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 $NP \cap coNP$ (под задачей факторизации подразумевается следующая проблема: для заданных натуральных чисел n и k нужно ответить на вопрос, имеет ли число n простой делитель, меньший, чем k). Напомним, что язык находится в $NP \cap coNP$, если существуют две недетерминированные полиномиальные машины Тьюринга: одна машина для распознавания языка, а вторая – для распознавания дополнения этого языка. Такие машины называются комплементарными друг другу. Однако требование комплементарности препятствует эффективной характеристике класса $NP \cap coNP$. Так, Wojciech Kowalczyk [2] показал, что перечисление языков из $NP \cap coNP$ с помощью пар комплементарных машин весьма затруднительно. Известны оракулы, относительно которых не существует полной проблемы в релятивизированном классе $NP \cap coNP$. Поэтому вполне вероятно, что сам класс $NP \cap coNP$ не содержит полной проблемы. В таком случае невозможно рекурсивно перечислить все языки из $NP \cap coNP$ с помощью пар комплементарных машин. Из этого вытекает следующее утверждение: независимо от мощи формальной математической теории (типа арифметики Пеано, теории множеств Цермело – Френкеля и т. д.) всегда найдется такая пара (T, M) полиномиальных недетерминированных машин Тьюринга, что невозможно доказать их комплементарность в рамках данной теории, а следовательно, и принадлежность распознаваемого машиной T языка классу $NP \cap coNP$. В связи с этим ведущими специалистами в логике и теории вычислительной сложности предполагалось крайне маловероятным нахождение какого-либо алгоритмического представления класса сложности $NP \cap coNP$ [3, 4]. Так, президент Европейской ассоциации по логике в информатике, профессор Anuj Dawar [3] предполагал, что классы сложности, определяемые семантическими ограничениями на удостоверяющие машины, например, такие, как классы $NP \cap coNP$ и RP , не допускают очевидных рекурсивных представлений. Кроме того, он считал [3], что нахождение рекурсивного представления для класса $NP \cap coNP$ потребует фундаментально новой характеристики данного класса и явится главным прорывом в теории сложности.

Цель настоящей работы – найти такое алгоритмическое перечисление задач из класса сложности $NP \cap coNP$, которое не требует соблюдения условия комплементарности.

1. Основные результаты

Дадим необходимые определения. Пусть Σ – конечный алфавит. Как обычно, через Σ^* обозначим множество всех слов (или конечных цепочек) в алфавите Σ . Языком называется любое подмножество множества Σ^* . Через $|w|$ обозначим длину слова w . Язык L распознается машиной Тьюринга T , когда выполняются следующие условия: если $w \in L$, то T останавливается на слове w в специальном допускающем состоянии (T допускает слово w); если $w \notin L$, то T останавливается на слове w в специальном отвергающем состоянии (T отвергает слово w).

Через $T(w)$ обозначим предикат, который принимает значение ИСТИНА, если T допускает слово w ; в противном случае значение $T(w)$ – ЛОЖЬ.

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

- для каждого языка из $\{L_i \mid i=1, 2, \dots\}$ существует машина Тьюринга из $\{T_i \mid i=1, 2, \dots\}$, распознающая этот язык;
- для каждой машины Тьюринга из $\{T_i \mid i=1, 2, \dots\}$ существует распознаваемый ею язык из $\{L_i \mid i=1, 2, \dots\}$.

Перейдем к рассмотрению класса сложности $NP \cap coNP$. Каждой паре полиномиальных недетерминированных машин Тьюринга (T, M) сопоставим следующий язык $L_{T,M} \subseteq \Sigma^*$:

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

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

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

Необходимо проверить соотношение $T(y) \Leftrightarrow \neg M(y)$ для всех цепочек y достаточно малой длины, т. е. для $|y| \leq \log_2(\log_2(|x|+1)+1)$. Отметим, что проверка отдельного условия $T(y) \Leftrightarrow \neg M(y)$ занимает экспоненциальное время по длине $|y|$, но поскольку длина $|y|$ достаточно мала, 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 $L_{T,M}$. Работа машины $D_{T,M}$ на входной цепочке $x \in \Sigma^*$ описывается следующим образом.

Для всех цепочек $y \in \Sigma^*$, таких, что $|y| \leq \log_2(\log_2(|x|+1)+1)$, 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 так же, как машина T на входе x .

Справедлива следующая

Теорема. Пусть $\{(T_i, M_i) \mid i=1, 2, \dots\}$ – рекурсивное перечисление всех пар полиномиальных недетерминированных машин Тьюринга. Тогда, взяв рекурсивное перечисление $\{D_{T_i, M_i} \mid i=1, 2, \dots\}$, получим рекурсивное представление класса сложности $NP \cap coNP$.

Доказательство. Сначала покажем, что любой язык $L_{T,M}$ из перечисления $\{L_{T_i, M_i} \mid i=1, 2, \dots\}$ находится в классе $NP \cap coNP$. Заметим, что если соотношение $T(y) \Leftrightarrow \neg M(y)$ выполняется вообще для всех цепочек y (независимо от их длины), то язык $L_{T,M}$ по определению будет принадлежать классу $NP \cap coNP$ (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 $L_{T,M} \in NP \cap coNP$. Таким образом, в любом случае доказывается принадлежность $L_{T,M}$ классу $NP \cap coNP$.

Осталось показать, что любой язык L из $NP \cap coNP$ находится в перечислении $\{L_{T_i, M_i} \mid i=1, 2, \dots\}$. Поскольку $L \in NP \cap coNP$, то существуют полиномиальные

недетерминированные машины Тьюринга T и M , распознающие язык L и его дополнение $\Sigma^* \setminus L$ соответственно. Так как $\{(T_i, M_i) \mid i=1, 2, \dots\}$ – рекурсивное перечисление всевозможных пар полиномиальных недетерминированных машин Тьюринга, 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 длины), 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, $L = L_{T_i, M_i}$ в связи с тем, что $T_i = T$. Таким образом, $L \in \{L_{T_i, M_i} \mid i=1, 2, \dots\}$.

Итак, показано, что $\{L_{T_i, M_i} \mid i=1, 2, \dots\} = \text{NP} \cap \text{coNP}$. Следовательно, $\{D_{T_i, M_i} \mid i=1, 2, \dots\}$ – рекурсивное представление класса сложности $\text{NP} \cap \text{coNP}$. ■

2. Методологическое значение

Отметим, что алгоритмическая неразрешимость проблемы установления комплементарности пары машин Тьюринга крайне затрудняет (если не делает невозможным) доказательство принадлежности многих задач классу $\text{NP} \cap \text{coNP}$. Разработанная характеристика задач из класса $\text{NP} \cap \text{coNP}$ не требует использования алгоритмически неразрешимого условия комплементарности машин Тьюринга, что дает возможность нахождения множества новых задач в $\text{NP} \cap \text{coNP}$. Действительно, общепринятый конструктивный способ доказательства принадлежности какого-либо языка L классу $\text{NP} \cap \text{coNP}$ предусматривает построение пары комплементарных полиномиальных недетерминированных машин Тьюринга. Однако Wojciech Kowalczyk [2] показал, что следующее перечисление «доказуемых» комплементарных пар:

$$\{(T_i, M_i, \text{«доказательство комплементарности машин } T_i \text{ и } M_i\text{»}) \mid i=1, 2, \dots\} \quad (3)$$

охватывает не все комплементарные пары, если класс $\text{NP} \cap \text{coNP}$ не содержит полной проблемы. Однако тогда в $\text{NP} \cap \text{coNP}$ существуют языки, для которых невозможно построить комплементарные пары машин Тьюринга в рамках формальной математической теории множеств Цермело – Френкеля [2].

Рассмотрим теперь другое перечисление:

$$\{(T_i, \text{«доказательство существования машины } M_i, \text{ комплементарной к машине } T_i\text{»}) \mid i=1, 2, \dots\}. \quad (4)$$

Поскольку перечисление (4) включает в себя все машины из перечисления $\{D_{T_i, M_i} \mid i=1, 2, \dots\}$, то оно является рекурсивным представлением класса сложности $\text{NP} \cap \text{coNP}$. Это подсказывает следующий неконструктивный способ установления принадлежности языка классу $\text{NP} \cap \text{coNP}$: вместо построения пары комплементарных машин (что может оказаться невозможным в рамках формальной теории) следует доказать существование пары комплементарных машин. Вполне возможно, что для ряда задач (например, для задачи изоморфизма графов), лежащих предположительно в классе $\text{NP} \cap \text{coNP}$, действительно нельзя построить пары комплементарных машин в рамках формальной математической теории множеств Цермело – Френкеля. Однако отыщется неконструктивное доказательство, если рассматриваемый язык действительно принадлежит классу $\text{NP} \cap \text{coNP}$.

Заключение

В работе впервые получено фундаментально новое описание задач из класса $\text{NP} \cap \text{coNP}$, при котором не требуется использование комплементарных пар машин Тьюринга.

С учетом центральной роли класса $\text{NP} \cap \text{coNP}$ в криптографии с открытым ключом новая характеристика имеет не только фундаментальное, но и важное прикладное значение. Кроме

того, алгоритмическое представление может быть использовано для логической характеристики данного класса сложности [5].

Работа профинансирована Институтом математики НАН Беларуси в рамках государственной программы фундаментальных исследований «Конвергенция – 2020».

Список литературы

1. Brassard, G. A Note on Cryptography and $NP \cap CoNP - P$ / G. Brassard, S. Fortune, J. Hopcroft // Technical Report TR-338, Department of Computer Science. – Ithaca, N.Y. : Cornell University, 1978.
2. Kowalczyk, W. Some Connections between Representability of Complexity Classes and the Power of Formal Systems of Reasoning / W. Kowalczyk // Proc. of the Mathematical Foundations of Computer Science. – Heidelberg : Springer, 1984. – Vol. 176. – 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, no. 3. – P. 498–532.
5. Naidenko, V. Logics for complexity classes / V. Naidenko // Logic J. of the IGPL. – 2014. – Vol. 22, no. 6. – P. 1075–1093.

Поступила 31.05.2016

*Институт математики НАН Беларуси,
Минск, ул. Сурганова, 11
e-mail: vladimir.naidenko@gmail.com*

V.G. Naidenko

ALGORITHMIC ENUMERATION OF PROBLEMS IN THE CLASS $NP \cap coNP$

The problem of recursive (algorithmic) representation is considered for the complexity class $NP \cap coNP$. A new method is proposed for algorithmically enumerating all problems in $NP \cap coNP$, using polynomial-time nondeterministic Turing machines.