П. Г. Ключарев

О ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ НЕКОТОРЫХ ЗАДАЧ НА ОБОБЩЕННЫХ КЛЕТОЧНЫХ АВТОМАТАХ

Клеточные автоматы широко применяются в целом ряде задач, относящихся к криптографии и математическому моделированию. Известен ряд задач на клеточных автоматах, являющихся *NP*-полными. Настоящая статья посвящена доказательству *NP*-полноты еще одной задачи, связанной с обобщением клеточных автоматов, — задачи о существовании предыдущего состояния обобщенного клеточного автомата.

Классические клеточные автоматы впервые были предложены в работе [1]. В работах [2,3] исследовалась *NP*-полнота ряда задач, связанных с клеточными автоматами. В последнее время, в работах [4,5], было предложено обобщение клеточных автоматов.

Будем называть *обобщенным клеточным автоматом* пару (G, f), где $G = (V, E)$ — ориентированный мультиграф ($V = \{v_1,...,v_N\}$ — множество вершин, а E — мультимножество ребер). Каждой вершине приписана булева переменная. Переменную, приписанную вершине v_i, будем обозначать m_i. Такие переменные мы будем называть *ячейками*. Для каждой вершины входящие в нее ребра пронумерованы числами $1...k$. Функция $f : \{0;1\}^k \to \{0;1\}$ называется *локальной функцией связи*.

Обобщенный клеточный автомат работает следующим образом. В начальный момент времени каждая ячейка памяти m_i, $i = 1...N$, имеет некоторое начальное значение $m_i(0)$. Далее автомат работает по шагам. На шаге с номером *t* вычисляются новые значения ячеек:

$$m_i(t)=f(m_{\eta(i,1)}(t-1),\ m_{\eta}(i,2)(t-1),\ ...,\ m_{\eta(i,k)}(t-1)), \qquad (1)$$

где $\eta(i, j)$— номер вершины, из которой исходит ребро, входящее в вершину *i* и имеющее номер *j*. Заполнение клеточного автомата на шаге *t* будем обозначать $M(t) = (m_1(t), m_2(t),..., m_N(t))$.

Пусть дан обобщенный клеточный автомат $C = (G, f)$ и его заполнение после первого шага $M(1)$. Задачу нахождения такого начального заполнения клеточного автомата $M(0)$, которое после первого шага перейдет в заполнение $M(1)$, назовем *задачей о восстановлении предыдущего состояния обобщенного клеточного автомата*.

Сформулируем теперь эту задачу в форме распознавания. Назовем *задачей о существовании предыдущего состояния обобщенного клеточного автомата* следующую задачу. Дан обобщенный клеточный автомат $C = (G, f)$ и его заполнение после первого шага $M(1)$. Требуется определить, существует ли начальное заполнение клеточного автомата $M(0)$, которое после первого шага перейдет в заполнение $M(1)$.

Основным результатом этой работы является следующая теорема.

Теорема 1. Задача о существовании предыдущего состояния обобщенного клеточного автомата является *NP*-полной.

Доказательство. Легко видеть, что задача о существовании предыдущего состояния принадлежит классу *NP*. Действительно, в качестве сертификата можно рассматривать начальное заполнение.

Теперь сведем задачу о 3-выполнимости (3-SAT), *NP*-полнота которой известна, к задаче о существовании предыдущего состояния.

Рассмотрим 3-КНФ вида:

$$h(x_1,x_2,\ ...,\ x_n) = \bigwedge_{j=1}^{q} (x_{ij1}^{(\sigma_{j1})} \vee x_{ij2}^{(\sigma_{j2})} \vee x_{ij3}^{(\sigma_{j3})}).$$

Как известно, задача о 3-выполнимости состоит в том, чтобы определить, существует ли такой набор аргументов $x_1, x_2, ..., x_n$, для которого $h(x_1, x_2, ..., x_n) = 1$.

Построим теперь искомое сведение следующим образом. Построим обобщенный клеточный автомат, граф которого состоит из $N = n + \max(q, n) + 1$ вершин. В качестве локальной функции связи обобщенного клеточного автомата выберем функцию

$$f(x_1, x_2, x_3, x_4) = (x_1 \vee x_2 \vee x_3) \oplus x_4. \quad (3)$$

Теперь определим ребра графа (всего их $4N$). Ориентированное ребро, исходящее из вершины *a* и входящее в вершину *b*, будем обозначать (a, b). Рассмотрим *j*-ю дизъюнкцию, входящую в: $x_{ij1}^{(\sigma_{j1})} \vee x_{ij2}^{(\sigma_{j2})} \vee x_{ij3}^{(\sigma_{j3})}$. Для каждой такой дизъюнкции добавим в граф четыре ребра следующим образом.

- Для каждого литерала $x_{ij1}^{(\sigma_{j1})}$ из трех, входящих в рассматриваемую дизъюнкцию, добавим в граф ребро $(v_{i_{jt}}, v_j)$ в случае, если $x_{ij1} = 1$ и $(v_{i_{jt}+n}, v_j)$ — в противном случае. Поставим в соответствие каждому такому ребру номер *t*.
- Четвертым будет ребро (v_N, v_j) с номером 4. Мы будем полагать, что $m_N(1) = 1$.

Проделав это для всех $j \in \{1, ..., q\}$, получим, что, если в первых *n* ячейках разместить значения переменных, а в последующих *n* ячейках разместить значения отрицаний переменных, клеточный автомат за один шаг вычислит значения всех *q* дизъюнкций из 3-КНФ.

Теперь для каждого $j \in \{1, ..., n\}$ добавим в граф три одинаковых ребра (v_i, v_{q+i}) с номерами 1, 2, 3 и ребро (v_{n+i}, v_{q+i}) с номером 4. Эти ребра позволяют гарантировать, что $m_i(0) = \neg m_{n+i}(0)$.

Далее, добавим ребро (v_1, v_N) с номером 1; два одинаковых ребра (v_{n+1}, v_N) с номерами 2 и 3 и петлю (v_N, v_N) с номером 4. Теперь в вершине v_N будет вычисляться:

$$m_N(1) = f(m_1(0), m_{n+1}(0), m_{n+1}(0), m_N(0)) =$$
$$= (m_1(0) \vee m_{n+1}(0) \vee m_{n+1}(0)) \oplus m_N(0) =$$
$$= (m_1(0) \vee \neg m_1(0)) \oplus m_N(0) = \neg m_N(0).$$

Теперь, в случае, если выполняется условие $N \geq q + n + 2$, для каждого $i \in \{q + n + 1, ..., N - 1\}$ добавим по четыре одинаковые петли (v_i, v_i).

Положим теперь:

$m_j(1) = 1$ для $j \in \{1, ..., q + n\}$;

$m_N(1) = 1$.

если $N \geq q + n + 2$, то $m_i(1) = 0$ для $i \in \{q + n + 1, ..., N - 1\}$.

Легко видеть, что такое заполнение может получиться в том и только в том случае, если выполняются следующие условия:

$h(m_1(0), m_2(0), ..., m_n(0)) = 1$;

$m_i(0) = \neg m_{n+i}(0)$ для всех $i \in \{1, ..., n\}$;

$m_N(0) = 0$;

начальные значения остальных ячеек произвольны.

Другими словами, если начальное заполнение существует, то существует и набор, на котором выполняется 3-КНФ.

Таким образом, задача о 3-выполнимости сводится к задаче о существовании предыдущего состояния обобщенного клеточного автомата. Из этого следует NP-полнота этой задачи. Теорема доказана.

Итак, задача о существовании предыдущего состояния обобщенного клеточного автомата является NP-полной. Из этого следует, что задача восстановления предыдущего состояния

является NP-трудной. NP-трудность этой задачи сохраняется, если рассматривать все обобщенные клеточные автоматы, отличные от классических. Однако в случае двухместности локальной функции связи f рассматриваемая задача полиномиальна. Докажем этот факт.

Теорема 2. Если локальная функция связи обобщенного клеточного автомата зависит лишь от двух переменных, то для задачи о существовании предыдущего состояния в таком автомате существует полиномиальный алгоритм.

Доказательство. Если локальная функция связи f зависит от двух переменных, то задача о существовании предыдущего состояния состоит в том, чтобы определить, существует ли решение системы булевых уравнений:

$$\begin{aligned} m_1(1) &= f(m_{\eta(1,1)}(0), m_{\eta(1,2)}(0)) \\ m_2(1) &= f(m_{\eta(2,1)}(0), m_{\eta(2,2)}(0)) \\ &\cdot \\ &\cdot \\ &\cdot \\ m_N(1) &= f(m_{\eta(N,1)}(0), m_{\eta(N,2)}(0)) \end{aligned} \qquad (4)$$

относительно начального заполнения. Правые части этих уравнений легко представляются в виде 2-КНФ.

Эта система уравнений эквивалентна уравнению:

$$\bigwedge_{j=1}^{N}(m_i(1) \oplus f(\mathrm{m}_{\eta(i,1)}(0), \mathrm{m}_{\eta(i,2)}(0)) \oplus 1) = 1. \qquad (5)$$

Задача о наличии решений этого уравнения представляет собой принадлежащую классу P задачу о 2-выполнимости [3]. Из этого следует утверждение теоремы.

Полученные результаты полезны для обоснования стойкости криптосистем, основанных на обобщенных клеточных автоматах [4,5,6].

СПИСОК ЛИТЕРАТУРЫ:

1. *Neumann J. von*. The general and logical theory of automata // Cerebral mechanisms in behavior. 1951. P. 1–41.
2. *Durand B*. A random NP-complete problem for inversion of 2D cellular automata // Theoretical computer science. 1995. Vol. 148. № 1. P. 19–32.
3. *Krom M. R*. The Decision Problem for a Class of First Order Formulas in Which all Disjunctions are Binary // Mathematical Logic Quarterly. 1967. Vol. 13. № 1. P. 15–20.
4. *Сухинин Б. М*. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов // Наука и образование: электронное научно-техническое издание. 2010. № 8. URL: http://technomag.edu.ru/doc/159565.html.
5. *Сухинин Б. М*. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование: электронное научно-техническое издание. 2010. № 9. URL: http://technomag.edu.ru/doc/159714.html.
6. *Ключарев П. Г*. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. 2011. № 10. URL: http://technomag.edu.ru/doc/241308.html.