УДК 519.713.4

И.К. РЫСЦОВ

ПРОБЛЕМА МОРТАЛЬНОСТИ И АФФИННЫЕ АВТОМАТЫ

Ключевые слова: *проблема мортальности, алгоритмические проблемы, линейные автоматы, аффинные автоматы.*

ВВЕДЕНИЕ

Множество квадратных матриц называется мортальным, если существует последовательность матриц из этого множества, произведение которых равно нулевой матрице. Проблема мортальности — это алгоритмическая проблема, в которой по заданному множеству квадратных матриц нужно определить, является ли это множество мортальным.

М. Патерсон в [1] доказал, что уже для квадратных матриц третьего порядка проблема мортальности алгоритмически неразрешима над полем рациональных чисел. Но для матриц второго порядка проблема остается до сих пор открытой. В [2] показано, что восьми матриц третьего порядка достаточно для неразрешимости проблемы мортальности. Подробный обзор по проблеме мортальности и мотивировки для ее исследования можно найти в [3]. В [4] показано, что ограниченная проблема мортальности для двух булевых матриц является NP-полной.

В данной работе проблема мортальности рассматривается с автоматной точки зрения. Показано, что она тесно связана с проблемой достижимости состояний в линейных и аффинных автоматах малой размерности. Кроме того, показано, что проблема достижимости состояний алгоритмически разрешима для одномерных линейных автоматов и для некоторых подклассов одномерных аффинных автоматов.

1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Напомним, что линейным n-мерным автоматом над полем рациональных чисел Q называется тройка $A = (Q^n, X, f)$, где Q^n — линейное пространство состояний (векторов длины n), X — конечное множество входных символов, а f — отображение вида $f: X \to \mathrm{Mat}(n, Q)$, которое отображает множество X во множество квадратных матриц n-го порядка с рациональными элементами. Отображение f определяет функцию переходов $F(s, x) = s \cdot f(x)$, где справа стоит произведение вектора строки s на матрицу $f(x)$. Другими словами, функция переходов будет линейной по первому аргументу, но, вообще говоря, нелинейной по второму. Число n называется размерностью линейного автомата [5].

Поскольку множество матриц $\mathrm{Mat}(n, Q)$ является мультипликативным моноидом, то отображение f можно продолжить до гомоморфизма, определенного на свободном моноиде $f: X^* \to \mathrm{Mat}(n, Q)$, который каждому входному слову $w = x_1 x_2 \ldots x_m$ сопоставляет произведение базовых матриц $f(w) = f(x_1) f(x_2) \cdot \ldots \cdot f(x_m)$. Тогда функция переходов определяется для любых входных слов по формуле $F(s, w) = s \cdot f(w)$, где правая часть по-прежнему понимается как произведение вектора на матрицу. Множеством достижимых состояний (множеством достижимости) для состояния $s \in Q^n$ в автомате A называется множество $R_A(s) = \{F(s, w) \mid w \in X^*\}$.

Пусть $A = (Q^2, X, f)$ — двумерный линейный автомат, тогда входное слово w назовем нулевым для A, если $f(w) = 0$. Множество всех нулевых слов для A обозначим $Z(A) = \{w \mid f(w) = 0\}$. Тогда проблему мортальности можно сформулировать следующим образом.

Проблема 1 (мортальность). Задан двумерный линейный автомат A, требуется определить, является ли множество $Z(A)$ непустым.

Линейный автомат $A = (Q^2, X, f)$ называется групповым, если матрицы $f(x)$ обратимые (неособенные) для всех $x \in X$. Конечно, если автомат A имеет нулевое слово, то у него должен быть, по крайней мере, один сингулярный входной символ x_1, для которого матрица $f(x_1)$ сингулярная (особенная). Удивительно, но одного сингулярного символа оказывается достаточно для существования нулевого слова. Следующее предложение доказано в работах [3, 6] для матриц второго порядка.

Предложение 1. Для любого двумерного линейного автомата A существует двумерный линейный автомат B, имеющий только один сингулярный входной символ, такой, что $Z(A) \neq \varnothing$ тогда и только тогда, когда $Z(B) \neq \varnothing$.

Это предложение показывает, что основная трудность в проблеме мортальности заключается в достижимости состояний соответствующего группового линейного автомата. Действительно, ненулевая сингулярная матрица второго порядка $M = f(x_1)$ характеризуется своим одномерным образом $\mathrm{Im}(M)$ и одномерным ядром $\mathrm{Ker}(M)$, которые являются прямыми линиями, проходящими через начало координат. Значит, нулевое слово в автомате B будет существовать тогда и только тогда, когда с помощью групповых символов прямую $\mathrm{Im}(M)$ можно преобразовать в прямую $\mathrm{Ker}(M)$. Это позволяет сформулировать проблему достижимости состояний автомата.

Очевидно, что в проблеме мортальности матрицы можно рассматривать с точностью до ненулевого скалярного множителя, поэтому будем говорить, что состояния s и t автомата A эквивалентны, если $s = \lambda t$, где λ — ненулевое рациональное число (скаляр). Это отношение будет конгруэнцией в линейном автомате, поэтому можно построить фактор-автомат по этой конгруэнции, который будет действовать в проективном пространстве. Но вместо этого введенное отношение позволяет сформулировать проблему достижимости состояний как «поточечную».

Проблема 2 (достижимость). Задан двумерный линейный групповой автомат B и два его состояния — s и t. Требуется определить, существует ли рациональное число λ такое, что $\lambda t \in R_B(s)$.

Интересно отметить, что впервые проблема мортальности была сформулирована именно как проблема достижимости прямых на плоскости [7]. Это показывает, что автор проблемы, по-видимому, знал о предложении 1, но не сформулировал его явно. Из предложения 1 получаем следующее утверждение.

Предложение 2. Проблема мортальности разрешима тогда и только тогда, когда разрешима проблема достижимости.

В общем случае проблемы 1 и 2 являются трудными алгоритмическими проблемами, поэтому в [3] было предложено рассмотреть эти проблемы для треугольных автоматов, т.е. двумерных линейных автоматов, у которых все обратимые матрицы $f(x)$ треугольные. Для определенности можно считать эти матрицы нижне-треугольными, т.е. имеющими вид

$$f(x) = \begin{bmatrix} a(x) & 0 \\ b(x) & 1 \end{bmatrix}, \tag{1}$$

где $a(x)$, $b(x)$ — рациональные числа, причем $a(x) \neq 0$ для всех $x \in X$.

Заметим, что все прямые параллельные оси абсцисс инвариантны под действием треугольного автомата, поэтому в проблеме достижимости 2 для треугольных автоматов можно опустить множитель λ и сформулировать ее как обычную достижимость для состояний, находящихся, например, на прямой $y = 1$.

Проблема 3. Задан двумерный линейный треугольный автомат $A = (Q^2, X, f)$ и два его состояния: $(s, 1)$, $(t, 1)$, где $s, t \in Q$. Требуется определить, достигается ли из состояния $(s, 1)$ состояние $(t, 1)$.

Как видно из формулировки этой проблемы, процесс достижимости состояний в треугольном автомате можно считать в некотором смысле одномерным, поэтому естественно перейти к рассмотрению одномерных автоматов, но для этого нужны автоматы более общего вида.

Одномерным аффинным автоматом назовем тройку объектов $A = (Q, X, f)$, где Q — поле рациональных чисел (множество состояний), X — конечное множество входных символов, а f — функция переходов $f(s, x) = s \cdot a(x) + b(x)$, где $a(x)$, $b(x)$ — рациональные числа, зависящие от входного символа x. Такие автоматы будем называть просто аффинными автоматами, поскольку их многомерные аналоги в данной работе не рассматриваются. Отметим, что линейные автоматы являются частным случаем аффинных, когда $b(x) = 0$ для всех $x \in X$. Аффинный автомат A называется групповым, если $a(x) \neq 0$ для всех $x \in X$.

Функция переходов аффинного автомата обычным образом продолжается на все входные слова и для входного слова $w = x_1 x_2 \ldots x_m$ преобразование состояний осуществляется по формуле $f(s, w) = s \cdot a(w) + b(w)$, где $a(w) = a(x_1)\, a(x_2) \cdot \ldots \cdot a(x_m)$, а $b(w)$ зависит от $a(x_i)$, $b(x_i)$, $1 \le i \le m$. Конкретный вид этой зависимости укажем далее. Множество достижимых состояний из состояния s определяется обычным образом: $R_A(s) = \{f(s, w) \mid w \in X^*\}$. Следующее предложение в других терминах доказано в работе [3].

Предложение 3. Проблема достижимости в двумерных линейных треугольных автоматах разрешима тогда и только тогда, когда разрешима проблема достижимости в одномерных аффинных групповых автоматах.

Доказательство. Сопоставим каждой треугольной матрице вида (1) треугольного автомата A переход $f(s, x) = s \cdot a(x) + b(x)$ в аффинном автомате B и, наоборот, каждому переходу в групповом аффинном автомате можно сопоставить треугольную матрицу вида (1). Нетрудно видеть, что для заданных рациональных чисел s и t будет выполняться условие $(t, 1) \in R_A((s, 1))$ тогда и только тогда, когда $t \in R_B(s)$ Таким образом, предложение доказано.

Целесообразно подробнее исследовать проблему достижимости состояний в аффинных автоматах. Основные результаты данной работы сформулируем следующим образом:

• доказана разрешимость проблемы достижимости состояний в одномерных линейных автоматах;

• доказана разрешимость проблемы достижимости состояний в аффинных автоматах, когда $a(x) = 1$ для всех $x \in X$, либо когда $0 < a(x) < 1$ для всех $x \in X$, либо когда $a(x) > 1$ для всех $x \in X$.

2. ЛИНЕЙНЫЕ АВТОМАТЫ

Сначала рассмотрим самый простой случай проблемы достижимости, а именно проблему достижимости состояний в одномерных линейных автоматах. Пусть $A = (Q, X, f)$ — одномерный линейный автомат, и пусть $w = x_1 x_2 \ldots x_m$ — входное слово, тогда по определению имеем равенство $f(s, wm) = s\, a(x_1)\, (a(x_2) \cdot \ldots \cdot a(x_m))$. Отсюда следует, что $t \in R_A(s)$ тогда и

только тогда, когда существуют неотрицательные целые числа $n(x)$, для которых выполняется равенство

$$s \prod_{x \in X} a(x)^{n(x)} = t. \tag{2}$$

Таким образом, получаем следующее утверждение.

Теорема 1. Проблема достижимости состояний в одномерных линейных автоматах является алгоритмически разрешимой.

Доказательство. Представим в равенстве (2) рациональные числа s, t и $a(x)$ их несократимыми целочисленными дробями и разложим все целые числа на простые. Тогда в (2) может встретиться только конечное число r простых чисел $p_1, p_2, \ldots, p_r$. Приравнивая показатели степени при каждом простом числе в левой и правой частях равенства, получим систему линейных диофантовых уравнений. Точнее, получим задачу линейного целочисленного программирования вида $M \cdot Y = C$, $Y \geq 0$, где M — целочисленная матрица размерности $r \times k$, $k = |X|$, $Y = (n(x_1), \ldots, n(x_k))$ — вектор неизвестных, C — вектор констант. Известно, что проблема существования допустимого решения у задачи линейного целочисленного программирования алгоритмически разрешима [8]. Отсюда вытекает справедливость утверждения теоремы.

Нетрудно видеть, что проблема достижимости в одномерных линейных автоматах соответствует проблеме мортальности для матриц второго порядка, когда все неособенные матрицы диагональные. Значит, в качестве следствия из теоремы 1 и предложения 1 получаем утверждение.

Следствие 1. Проблема мортальности разрешима для двумерных линейных автоматов, у которых всем групповым символам соответствуют диагональные матрицы.

3. АФФИННЫЕ АВТОМАТЫ

Начнем снова с простого случая. Аффинный автомат $A = (Q, X, f)$ назовем унитарным, если $a(x) = 1$ для всех $x \in X$. В этом случае для входного слова $w = x_1 x_2 \ldots x_m$ имеем $f(s, w) = s + b(x_1) + \ldots + b(x_m)$. Отсюда следует, что $t \in R_A(s)$ тогда и только тогда, когда существуют неотрицательные целые числа $n(x)$, $x \in X$, для которых выполняется следующее равенство:

$$s + \sum_{x \in X} b(x)\, n(x) = t. \tag{3}$$

Это линейное диофантово уравнение является аддитивным аналогом равенства (2). Тогда разрешимость проблемы существования решения уравнения (3) следует из разрешимости проблемы существования решения у линейных диофантовых уравнений [9]. Отсюда получаем следующее утверждение.

Теорема 2. Проблема достижимости состояний в унитарных аффинных автоматах является алгоритмически разрешимой.

Из доказательства предложения 3 видно, что проблеме достижимости в унитарных аффинных автоматах соответствует проблема достижимости для двумерных треугольных автоматов, у которых все матрицы унитреугольные:

$$f(x) = \begin{bmatrix} 1 & 0 \\ b(x) & 1 \end{bmatrix}. \tag{4}$$

Значит, в качестве следствия из теоремы 2 и предложений 2 и 3 получаем следующее утверждение.

Следствие 2. Проблема мортальности разрешима для двумерных линейных автоматов, у которых всем групповым символам соответствуют унитреугольные матрицы вида (4).

Теперь детальнее рассмотрим переходы в аффинном автомате $A = (Q, X, f)$. Пусть $l(w) = m$ — длина входного слова $w = x_1 x_2 \ldots x_m$, и пусть $\sigma_i(w) = x_{i+1} \ldots x_m$ — i-й суффикс слова w, $1 \le i \le m$. Предполагается, что $\sigma_m(w) = e$, где e — пустое слово. Далее, пусть $a(w) = a(x_1) \cdot a(x_2) \cdot \ldots \cdot a(x_m)$ — гомоморфизм свободного моноида $a : X^* \to Q$ в мультипликативную группу рациональных чисел. Следующая формула, которая легко доказывается индукцией по длине входного слова, может рассматриваться как обобщение формулы перехода для классических линейных автоматов [10]:

$$f(s, w) = s\, a(w) + \sum_{i=1}^{m} a(\sigma_i(w))\, b(x_i). \tag{5}$$

Определение 1. Аффинный автомат $A = (Q, X, f)$ назовем сжимающим, если $0 < a(x) < 1$ для всех $x \in X$.

Лемма. Если аффинный автомат $A = (Q, X, f)$ является сжимающим, то множество $R_A(s)$ будет ограниченным для любого $s \in Q$.

Доказательство. Положим $c = \max\{a(x) \mid x \in X\}$, $d = \max\{|b(x)| \mid x \in X\}$ и заметим, что $0 < c < 1$. Тогда из свойства (5) получаем следующие неравенства:

$$|f(s, w)| \le |s|\, c^m + \sum_{i=1}^{m} c^{m-i}\, d < |s| + \frac{d}{1-c}. \tag{6}$$

Таким образом, лемма доказана.

Введем теперь понятие обратного автомата для группового аффинного автомата, которое оказывается полезным во многих ситуациях. Напомним, что аффинный автомат $A = (Q, X, f)$ называется групповым, если $a(x) \ne 0$ для всех $x \in X$. В этом случае все входные символы действуют на множестве состояний Q линейно и взаимно однозначно, поэтому можно обычным образом определить обратный аффинный автомат $\mathrm{inv}(A) = (Q, X, g)$, в котором $g(t, x) = (t - b(x)) / a(x)$ для всех $x \in X$. Индукцией по длине входного слова $w = x_1 x_2 \ldots x_m$ легко показать, что в автомате A выполняется условие $f(s, w) = t$ тогда и только тогда, когда в автомате $\mathrm{inv}(A)$ выполняется условие $g(t, w^{-1}) = s$, где $w^{-1} = x_m x_{m-1} \ldots x_1$ — обратное для w слово. Таким образом, получаем следующее свойство:

$$t \in R_A(s) \Leftrightarrow s \in R_{\mathrm{inv}(A)}(t). \tag{7}$$

Определение 2. Аффинный автомат $A = (Q, X, f)$ назовем увеличивающим, если $a(x) > 1$ для всех $x \in X$.

Теорема 3. Проблема достижимости состояний в сжимающих и увеличивающих аффинных автоматах является алгоритмически разрешимой.

Доказательство. Пусть $A = (Q, X, f)$ — сжимающий аффинный автомат, и пусть заданы рациональные числа s и t, причем $t = p / q$, где p и q — взаимно простые целые числа. Тогда согласно лемме множество $R_A(s)$ и множество $R_A(s)\, q = \{u\, q \mid y \in R_A(s)\}$ ограниченные. Значит, множество $R_A(s) \cdot q$ содержит только конечное число целых чисел и их можно найти, например, перебирая все входные слова до заранее известной длины. Соответствующую границу на длину слов можно получить из свойства (6). Остается заметить, что условие $t \in R_A(s)$ равносильно условию $p \in R_A(s)\, q$, и теорема в этом случае доказана.

Если $A = (Q, X, f)$ — увеличивающий аффинный автомат, то его обратный $\mathrm{inv}(A) = (Q, X, g)$ будет в этом случае сжимающим, поскольку $0 < a(x)^{-1} < 1$ для всех $x \in X$. Тогда утверждение теоремы следует из свойства (7) и разрешимости проблемы достижимости для сжимающих автоматов. Таким образом, теорема полностью доказана.

В результате из этой теоремы и предложений 2 и 3 получаем следующее утверждение.

Следствие 3. Проблема мортальности разрешима для двумерных линейных автоматов, у которых всем групповым символам соответствуют треугольные матрицы (1), причем $0 < a(x) < 1$ для всех $x \in X$ или $a(x) > 1$ для всех $x \in X$.

В заключение рассмотрим самый сложный случай, когда в аффинном автомате есть два входных символа x и y, которые удовлетворяют условию $|a(x)| < 1 < |a(y)|$. Для иллюстрации возникающих здесь трудностей достаточно напомнить известную числовую задачу, которую называют «умножить на три и прибавить единицу» [11]. Пусть $A_1 = (N, \{x, y\}, f)$ — «частичный» аффинный автомат, определенный на множестве натуральных чисел N следующим образом: $f(s, x) = s/2$, если s — четное число, и $f(s, y) = 3 \cdot s + 1$, если s — нечетное число, большее единицы. Требуется доказать, что из любого состояния достигается первое состояние, т.е. автомат, в конце концов, останавливается независимо от начального состояния.

Хотя A_1 и не совсем «чистый» аффинный автомат, тем не менее родство этой проблемы с проблемой достижимости не вызывает сомнений. В данном случае также оказывается полезным «обратный» автомат, который помогает понять арифметическую структуру множеств состояний, находящихся на одном уровне достижимости [11]. Как показывают компьютерные эксперименты, если $s < 10^{40}$, то автомат всегда останавливается, но полного доказательства, насколько известно автору, до сих пор нет.

ЗАКЛЮЧЕНИЕ

Полученные результаты вселяют некоторую надежду на то, что проблема достижимости для одномерных аффинных автоматов может оказаться алгоритмически разрешимой. Здесь можно двигаться и дальше, например, объединить унитарный и сжимающий автоматы в один автомат и рассмотреть для него проблему достижимости. Однако множество достижимости для аффинного автомата может иметь очень сложную структуру. Например, нетрудно показать, что рациональные точки из множества Кантора образуют множество достижимости для некоторого аффинного автомата. Это свидетельствует в пользу неразрешимости этой проблемы.

СПИСОК ЛИТЕРАТУРЫ

1. Paterson M. Unsolvability in 3 × 3 matrices // Studies in Appl. Mathemat. — 1970. — **49**. — P. 105–107.
2. Halava V., Harji T. Mortality in matrix semigroups. — Turku: Turku Centre of Comput. Sci., 2000. — Techn. Rep. N 361. — P. 1–8.
3. Bournez O., Branicky M. The mortality problem for matrices of low dimensions // Theory Comput. Systems. — 2002. — **35**. — P. 433–448.
4. Blondel V., Tsitsiklis J. When is a pair of matrices mortal? // Inform. Process. Letters. — 1997. — **63.** — P. 283–286.
5. Рысцов И.К. Представление регулярных идеалов в конечных автоматах // Кибернетика и системный анализ. — 2003. — № 5. — С. 48–58.
6. Рысцов И.К. Минимальные нулевые слова для матриц второго порядка // Там же. — 2007. — № 4. — С. 10–18.
7. Schultz P. Mortality of 2 × 2 matrices // American Mathemat. Monthly. — 1977. — **84**, N 2. — P. 463–464.
8. Пападимитриу Х. Стайглиц К. Комбинаторная оптимизация. — М.: Мир, 1985. — 510 с.
9. Схрейвер А. Теория линейного и целочисленного программирования. Т.1. — М.: Мир, 1991. — 360 с.
10. Гилл А. Линейные последовательностные машины. — М.: Наука, 1974. — 287 с.
11. Нивергельт Ю., Фаррар Дж., Рейнгольд Э. Машинный подход к решению математических задач. — М.: Мир, 1977. — 351 с.

Поступила 02.08.2007