Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета

г. Иваново, 21–24 марта 2018 г.

НЕКОТОРЫЕ МЕТОДЫ СИМВОЛЬНОГО АНАЛИЗА ОДНОСЧЕТЧИКОВЫХ СЕТЕЙ ПЕТРИ[1]

В. А. Башкин (Ярославль)[2]

1. Введение

Односчетчиковые сети, известные также как одномерные системы векторного сложения с состояниями (1-dim Vector Addition Systems with States — VASS), эквивалентны сетям Петри с одной неограниченной позицией, а также магазинным автоматам с односимвольным стековым алфавитом. Ограничение количества счетчиков делает их менее выразительными, чем обыкновенные сети Петри. С другой стороны, многие алгоритмические проблемы становятся разрешимыми, и в результате сама модель оказывается более удобной для различных специфических задач моделирования и анализа систем.

В работе [1] мы использовали теоретико-числовой метод, основанный на числах Фробениуса, для изучения периодичности значений счетчика односчетчиковой сети. Было доказано, что бесконечное множество достижимых значений счетчика полностью описывается конечным числом арифметических прогрессий с общей разностью.

В работе [2] был представлен метод приближения наибольшей бисимуляции в односчетчиковой сети, основанный на использовании однопериодической символьной арифметики и понятия расслоенной бисимуляции.

В работах [3, 4] введено и исследовано сужение класса односчетчиковых сетей — положительные односчетчиковые контуры. Показано, что в контуре бесконечная часть множества достижимости описывается арифметической прогрессией; получены оценки параметров этой прогрессии через структурные свойства диаграммы переходов. Показано, что для любой односчетчиковой сети существует эквивалентная (в смысле достижимости) правильно сформированная сеть, которая может быть эффективно построена из соответствующего дерева контуров.

В данной работе приводятся результаты, лежащие в основе методов символьных вычислений над одномерными полулинейными множествами, используемых для анализа односчетчиковых сетей Петри.

2. Однопериодические базисы

Для удобства введём новое обозначение одномерных линейных множеств (линейных множеств натуральных чисел). Пусть $m \subseteq Nat$ линейно, тогда для некоторого $l \in \mathbf{Z}_+$ выполняется $m = Lin\{v, \{w_1, \ldots, w_l\}\} =_{\text{def}} \{v + n_1 w_1 + \ldots + n_l w_l \mid n_1, \ldots, n_l \in Nat\}$, где $v, w_1, \ldots, w_l \in Nat$ фиксированы.

Линейное множество $m \subseteq Nat$ назовём *ограниченно неполным,* если $m = m' \setminus m''$, где m' — линейное, а m'' — конечное множество. Если $m' = Lin\{v, \{w_1, \ldots, w_l\}\}$ и $w \in Nat$ — наибольший элемент m'', то обозначим m как $DLin\{v, w + 1, \{w_1, \ldots, w_l\}\}$. Отметим, что выражение $DLin\{v, w, E\}$ не является точным описанием m — это приближение сверху.

Рассмотрим решение задачи Фробениуса о размене монет, называемое также числами Фробениуса. Требуется найти число, являющееся крупнейшей денежной суммой, не набираемой монетами указанных номиналов. Например, крупнейшая сумма, которая не может быть получена, используя только монеты в 3 и 5 единиц, составляет 7. Задачу для двух переменных (двух номиналов монет) решил Сильвестр в [8]:

 Получено 14.01.2018. УДК 519.71.

[1]Работа выполнена при финансовой поддержке РФФИ, проект № 17-07-00823.

[2]Ярославский государственный университет им. П. Г. Демидова. E-mail: v_bashkin@mail.ru.

Факт. *Для любых взаимно простых натуральных a и b и натурального c, такого что $c \geq (a-1)(b-1)$, диофантово уравнение $ax+by=c$ имеет натуральное решение; при этом уравнение $ax+by=c-1$ не имеет натурального решения.*

Обобщение для произвольного числа переменных (номиналов монет) до сих пор не имеет точного решения. Насколько нам известно, наилучшим приближением сверху является квадрат наибольшего номинала [5, 6]. Использование чисел Фробениуса позволяет доказать, что линейное множество с двумя периодами представимо как ограниченно неполное множество с одним периодом:

Лемма 1. *Пусть $m = Lin\{v, \{w_1, w_2\}\}$, $p = НОД(w_1, w_2)$ и $b = v + p(\frac{w_1}{p} - 1)(\frac{w_2}{p} - 1)$. Тогда $m = DLin\{v, b, \{p\}\}$.*

Будем говорить, что множество m распадается на "неполную" (в некотором смысле хаотичную) "голову" $m_0 \subseteq \{b - kp \mid k \in \{1, 2, \ldots, (\frac{w_1}{p} - 1)(\frac{w_2}{p} - 1)\}\}$ и простой бесконечный периодический "хвост" $m_\infty = \{b + kp \mid k \in Nat\}$.

Итак, любое двухпериодическое линейное множество является подмножеством некоего однопериодического множества, причем мы можем найти точную верхнюю границу "неполной" части. Лемма 1 может быть обобщена на случай s периодов:

Лемма 2. *Пусть $Lin\{v, \{w_1, \ldots, w_s\}\}$, $p = НОД(w_1, \ldots, w_s)$, $c = max\{w_1, \ldots, w_s\}^2$ и $b = v + \frac{c}{p}$. Тогда $m = DLin\{v, b, \{p\}\}$.*

Рассмотрим полулинейное множество над Nat. Оно также обладает единственным "периодом", однако в данном случае это уже не интервал, а вектор. Обозначим $\triangleleft$ и $\triangleright$ — операции сдвига множеств целых неотрицательных чисел соответственно влево и вправо на натуральное число (например, $\{1, 3, 12\} \triangleleft 5 = \{-4, -2, 7\}$).

Лемма 3. *Для любых ограниченно неполных линейных множеств с одним периодом $m' = DLin\{v', b', \{p'\}\}$ и $m'' = DLin\{v'', b'', \{p''\}\}$ полулинейное множество $m = m' \cup m''$ распадается на конечное множество и конечное семейство линейных множеств с одинаковым периодом. Обозначив $p = НОК(p', p'')$ и $b = max\{b', b''\}$, получим, что существует* характеристическое множество $\Psi \subseteq \{b, b+1, b+2, \ldots, b+(p-1)\}$, *такое, что*

$$m = m_0 \cup m_\infty, \quad \text{где} \quad m_0 \subseteq \bigcup_{k=1}^{[\frac{b}{p}]} \big(\Psi \triangleleft kp\big), \; m_\infty = \bigcup_{k=0}^{\infty} \big(\Psi \triangleright kp\big). \tag{1}$$

Дальнейшее обобщение Леммы 3 на произвольное число линейных множеств с произвольным числом периодов:

Теорема 1. *Любое полулинейное множество $m \subseteq Nat$ распадается на конечное множество и конечное семейство линейных множеств с одинаковым периодом: для некоторых $p, b \in Nat$, существует представление m в форме (1).*

Замечание. Пусть все линейные подмножества находятся в однопериодической форме. Тогда наименьшее b не превышает наибольшего базового элемента всех линейных подмножеств m, а наименьшее p равно наименьшему общему кратному всех их периодов. В частности, если все эти периоды попарно взаимно просты, то наименьшее b в точности равно наибольшему базовому элементу всех линейных подмножеств.

Теорема 2. *Пусть $m \subseteq Nat$ — полулинейное множество, представленное в форме (1), $x, y \in Nat$. Пусть $\{A^{(i)}\}$ — последовательность полулинейных множеств, такая что $A^{(0)} = m$, $A^{(i+1)} = (A^{(i)} \triangleleft x) \triangleright y$. Тогда существует $j \leq max\{[\frac{b}{|x-y|}], НОК(p, |x-y|)\} + 1$, такое, что* $\bigcup_{i=1}^{\infty} A^{(i)} = \bigcup_{i=1}^{j} A^{(i)}$.

Теорема раскрывает важное свойство одномерных полулинейных множеств: конечно определенная аддитивная последовательность стабилизируется за конечное число шагов. Это свойство стабилизации было доказано как лемма в [7], но только для сложения (сдвига вправо) и без каких-либо оценок требуемого количества шагов.

Рассмотрим двоичный вектор v длины p, такой что $v[i] = 0$ для $b + i \notin \Psi$ и $v[i] = 1$ для $b + i \in \Psi$. Теорема 1 утверждает, что этот вектор является "битовой маской" для периодического "закрашивания" натурального ряда справа от числа b. Таким образом, мы можем использовать в качестве конечного символьного представления произвольного полулинейного одномерного множества m его *однопериодический базис* (m_0, b, p, v), состоящий из

- конечного *базового множества* m_0,
- *базового элемента* b,
- *длины периода* p,
- *вектора периода* v.

Определение. Базис $Z = (m_0, b, p, v)$ полулинейного множества $m \subseteq Nat$ называется *минимальным*, если для любого базиса $Z' = (m'_0, b', p', v')$ множества m выполняется $p < p'$ или $(p = p'$ и $b \le b')$.

Теорема 3. *Для любого одномерного полулинейного множества $m \subseteq Nat$ минимальный базис $Base(m)$ существует и единственен.*

Произвольный базис (m_0, b, p, v) полулинейного множества $m \subseteq Nat$ может быть преобразован в минимальный базис $Base(m)$ за полиномиальное время относительно $b * p$.

Множество, определяемое базисом Z, обозначим как $Set(Z)$. Обозначим процедуру минимизации базиса (m_0, b, p, v) как $Mmz(m_0, b, p, v)$. Для двоичных векторов $v, v' \in \{0, 1\}^p$ через $NOT(v)$, $AND(v, v')$ и $OR(v, v')$ обозначим покомпонентное умножение, сложение и отрицание: $AND(v, v')[i] =_{\text{def}} min\{v[i], v'[i]\}$, $OR(v, v')[i] =_{\text{def}} max\{v[i], v'[i]\}$, $NOT(v)[i] =_{\text{def}} (1 - v[i])$. Через v^k обозначим конкатенацию k векторов v.

Теоретико-множественные операции и отношения могут эффективно вычисляться не над множествами, а непосредственно над их одноперiодическими базисами:

Теорема 4. *Пусть $m, m' \subseteq Nat$ — полулинейные, $Base(m) = (m_0, b, p, v)$, $Base(m') = (m'_0, b', p', v')$, $y \in Nat$. Обозначим $K = max\{b, b'\}$ и $L = HOK(p, p')$. Пусть $K = b + ip = b' + jp'$ для некоторых $i, j \in Nat$. Тогда:*

(1) $Base(Nat) = (\varnothing, 0, 1, (1))$;

(2) $Base(m \cup m') = Mmz\big(\{x \in m \cup m' \mid x < K\}, K, L, OR(v^{\frac{L}{p}}, (v')^{\frac{L}{p'}})\big)$;

(3) $Base(m \cap m') = Mmz\big(\{x \in m \cap m' \mid x < K\}, K, L, AND(v^{\frac{L}{p}}, (v')^{\frac{L}{p'}})\big)$;

(4) $Base(m \setminus m') = Mmz\big(\{x \in m \setminus m' \mid x < K\}, K, L, AND(v^{\frac{L}{p}}, NOT((v')^{\frac{L}{p'}}))\big)$;

(5) $m \subseteq m' \iff AND(v^{\frac{L}{p}}, (v')^{\frac{L}{p'}}) = v^{\frac{L}{p}} \ \wedge \ \forall x \in m \ (x < K \Rightarrow x \in m')$;

(6) $Base(m \triangleright y) = Mmz(\{x + y \mid x \in m_0\}, b + y, p, v)$;

(7) $Base(m \triangleleft y) = Mmz(\{x - y \mid x \in m, x < B, x \ge y\}, B, p, v)$, *где* $B = min_{k \in Nat}\{b + kp - y \mid b + kp - y \ge 0\}$.

Заметим, что ограничение $K = b + ip = b' + jp'$ носит технический характер — оно позволяет записать формулы в более краткой форме. Приведенные операции эффективны, то есть выполняются за полиномиальное время относительно размеров входных базисов.

Литература

1. *Башкин В. А.* Верификация на основе моделей с одним неограниченным счетчиком // Информационные системы и технологии. 2010. № 4 (60). С. 5—12.
2. *Башкин В. А.* Построение приближений бисимуляции в односчетчиковых сетях // Моделирование и анализ информационных систем. 2011. Т. 18, № 4. С. 34—44.
3. *Башкин В. А.* Об эффективном моделировании неограниченного ресурса при помощи односчетчиковых контуров // Моделирование и анализ информационных систем. 2013. Т. 20, № 2. С. 139—156.
4. *Bashkin V. A.* One-counter Circuits // Concurrency, Specification and Programming. CSP 2012 Workshop Proceedings. Vol. 1. Berlin, Germany : Humboldt-Universitat zu Berlin, 2012. P. 25—36.
5. *Brauer A.* On a Problem of Partitions // American Journal of Mathematics. 1942. Vol. 64, № 1. P. 299—312.
6. *Erdös P., Graham R. L.* On a linear diophantine problem of Frobenius // Acta Arithm. 1972. Vol. 21. P. 399—408.
7. *Hopcroft J., Pansiot J.-J.* On the reachability problem for 5-dimensional vector addition systems // Theor. Comp. Science. 1979. Vol. 8, № 2. P. 135—159.
8. *Sylvester J. J.* Question 7382 // Mathematical Questions with their Solutions, Educ. Times. 1884. Vol. 41. P. 21.