УДК 519.7

Е.А. Пряничникова
Донецкий национальный технический университет, г. Донецк
кафедра Программного обеспечения интеллектуальных систем

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Аннотация.
Пряничникова Е.А. Математические основы проектирования вычислительных систем. *В работе выполнен обзор и анализ современных математических методов проектирования и верификации вычислительных систем. Рассматривается новая автоматно-алгебраическая модель вычислительной системы, основанная на использовании графов с отмеченными вершинами. Исследуются основные свойства алгебры языков, представимых в графах с отмеченными вершинными: алгебраическая и лингвистическая характеризации языков, представимых регулярными выражениями этой алгебры, методы анализа и синтеза рассматриваемых языков, способы детерминизации и минимизации графов с отмеченными вершинами.*

Ключевые слова: *вычислительные системы, конечные автоматы, отмеченные графы, временная логика.*

Постановка проблемы. Под вычислительной системой понимается любая техническая система преобразования информации, поведение которой может быть описано с помощью алгоритма. Процесс проектирования вычислительной системы представляет собой последовательность этапов, на каждом из которых проект системы представлен с помощью совокупности математических моделей, описывающих отдельные ее части [1].

В настоящее время аппаратные и программные системы широко используется во многих приложениях, где любой отказ считается недопустимым, таких как электронная коммерция, сети телефонных коммутаторов, системы управления воздушным и дорожным движением, медицинская аппаратура. Задача проверки правильности проектируемой системы, т. е. обеспечения ее корректности начиная с самых ранних этапов проектирования, является основной проблемой в процессе разработки любой надежной системы, и усилия, затрачиваемые на ее решение, поглощают все возрастающую долю стоимости и времени проектировочного цикла. Сложность разработки качественных и надежных вычислительных систем стимулирует развитие теоретических основ проектирования вычислительных систем, создание теоретически обоснованных методов и средств их разработки [2].

В разное время было предложено несколько подходов к формальной верификации вычислительных систем. В последние годы очень активно развивается метод верификации моделей (или проверки на модели), при помощи которого желаемые свойства поведения системы проверяются на заданной модели путем исчерпывающего перебора всех состояний, достижимых системой, и всех поведений, проходящих через эти состояния. При таком подходе спецификации представляются формулами пропозициональной темпоральной логики, а вычислительные системы моделируются отмеченными графами - системами переходов. Чтобы проверить, верна ли спецификация на системе переходов, применяется эффективная процедура поиска [3].

Чтобы модель была пригодна для верификации, в ней должны проявляться те свойства, анализ которых необходим для установления ее корректности. С другой стороны, она должна быть свободна от частных особенностей, не влияющих на проверяемые свойства, но усложняющих верификацию. Различают три основных вида моделей – функциональные, динамические и структурные. Функциональные модели определяют функции, которые вычисляет проектируемая система, динамические модели определяют процессы функционирования системы или процессы вычислений, а структурные модели представляют систему в виде параллельной композиции компонент. Обычно процесс проектирования «сверху вниз» протекает от функциональных к динамическим, а затем к структурным моделям.

Основными математическими моделями, которые используются для описания вычислительных систем, являются отмеченные графы. Чаще всего используются графы с отмеченными дугами (конечные автоматы) и графы с отмеченными вершинами, важной разновидностью которых являются модели Крипке. Модель Крипке состоит из множества состояний, множества переходов между состояниями и функции, которая помечает каждое состояние набором свойств, истинных в этом состоянии. Пути в модели Крипке соответствуют вычислениям системы [3].

При построении всех рассматриваемых моделей широко применяется алгебраическая точка зрения, при которой операции некоторой базовой алгебры рассматриваются как исходные алгоритмы, используемые для порождения новых объектов из заданных (порождающих элементов алгебры) или построения функций над этими объектами [1].

Наиболее полно изученными из таких моделей являются конечные автоматы. Алгебраическая теории графов с отмеченными вершинами разработана значительно меньше, чем алгебраическая теория конечных автоматов [4]. Хотя графы с отмеченными вершинами широко используются в различных прикладных задачах проектирования вычислительных систем, многие вопросы теории таких графов еще не достаточно проработаны. Создание и исследование алгебраических методов для решения различных задач, связанных с такими графами, существенно отстает от исследований в области алгебраической теории конечных автоматов, поэтому задача разработки алгебраического аппарата для задач, представимых в этих графах является важной и актуальной.

Цель статьи – исследование новой алгебры, подобной алгебре регулярных языков, но имеющей ряд особенностей (например, в свойствах операции итерации), позволяющих, на наш взгляд, более адекватно описывающей свойства языков, представимых в рассматриваемых графах. Разработка данной алгебры вызвана, в частности, тем, что описание языков, представимых в графах с отмеченными вершинами в виде регулярных выражений алгебры Клини плохо отражает структуру этих языков и вызывает трудности перехода от графов к формулам и наоборот.

Основные определения и обозначения. Назовем графом с отмеченными вершинами четверку $G = (Q, E, X, \mu)$, где Q - конечное множество вершин, $|Q| = n$, $E \subseteq Q \times Q$ - множество дуг, X - конечный алфавит отметок вершин, $\mu : Q \to X$ - функция отметок вершин. Пусть $I \subseteq Q$ - множество начальных, а $F \subseteq Q$ - множество финальных вершин графа.

Назовем граф G детерминированным, если для любой пары $(q_i, x_i) \in Q \times X$ найдется не больше одной вершины $q_j \in Q$, для которой выполняется, что $(q_i, q_j) \in E$ и $\mu(q_j) = x_i$.

Если для любой пары $(q_i, x_i) \in Q \times X$ в графе G найдется не меньше одной вершины $q_j \in Q$, для которой выполняется, что $(q_i, q_j) \in E$ и $\mu(q_j) = x_i$, то граф G назовем полным.

Путем в графе G будем называть конечную последовательность вершин $l = q_1\, q_2 ... q_k$, где $(q_i, q_{i+1}) \in E$, число $k - 1$ будем называть длиной пути, q_1 - начальная вершина пути, q_k - конечная вершина. Пусть X^+ - множество всех непустых слов конечной длины в алфавите X. Элемент $x = \mu(q_1)\, \mu(q_2) ... \mu(q_k) = x_1 x_2 ... x_k \in X^+$ будем называть отметкой пути l в графе G. Для каждой вершины q определим путь нулевой длины, начинающийся и заканчивающийся в этой вершине. Отметкой нулевого пути будет $x \in X$, такое, что $\mu(q) = x$. Множество отметок всех путей, начальной вершиной которых является вершина q_i, а конечная вершина $q_k \in F$, назовем языком, порожденным вершиной q_i. Языком, порождаемым графом G, назовем отметки всех путей в графе G, начальные вершины которых принадлежат множеству I, а конечные - множеству F. Язык, порождаемый графом G, обозначим $L(G)$.

Определим на множестве X^+ частичную бинарную операцию $\circ$ склеивания двух слов следующим образом: для всех для всех $w_1, w_2 \in X^+$ и всех $x, y \in X$

$$w_1 x \circ y w_2 = \begin{cases} w_1 x w_2, \; если \;\; x = y; \\ не определено, \; в противном \;\; случае. \end{cases}$$

Рассмотрим алгебру $\left\langle 2^{X^+}, \circ, \cup, \otimes, \varnothing, X \right\rangle$ со следующими операциями на языках $L, R \in 2^{X^+}$.

1) $L \cup R = \{ w | w \in L \quad или \quad w \in R \}$;

2) $L \circ R = \{ w_1 \circ w_2 | w_1 \in L \;\; и \;\; w_2 \in R \}$;

3) $L^* = \bigcup_{i=0}^{\infty} L^i$, где $L^0 = X; L^{n+1} = L^n \circ L, n \geq 0$;

4) $L^{\otimes} = L_{beg} \circ L^* \circ L_{end}$,

$L_{beg} = \{ x | xw \in L, \, x \in X, w \in X^* \}$, $L_{end} = \{ x | wx \in L, \, x \in X, w \in X^* \}$.

Регулярные выражения в алгебре $\left\langle 2^{X^+}, \circ, \cup, \otimes, \varnothing, X \right\rangle$ определим рекурсивно следующим образом:

1) $\varnothing$ является регулярным выражением, представляющим язык $\varnothing$;

2) x и xy являются регулярными выражениями и представляют языки $L(x) = \{x\}$ и $L(xy) = \{xy\}$ для всех $x, y \in X$;

3) Если p и q - регулярные выражения, представляющие языки $L(p)$ и $L(q)$ соответственно, то выражения $(p \circ q)$, $(p \cup q)$, $(p^{\otimes})$ также являются регулярными, причем $L(p \circ q) = L(p) \circ L(q)$, $L(p \cup q) = L(p) \cup L(q)$, $L(p^{\otimes}) = (L(p))^{\otimes}$.

Результаты исследований. Показано, что алгебра языков, представимых в графах с отмеченными вершинами, является свободной алгеброй в конечно-базируемом квазимногообразии, для этой алгебры разработана система аксиом (1), состоящая из тождеств и квазитождеств, и доказана ее полнота: два регулярных выражения p и q над конечным алфавитом X обозначают один и тот же язык, представимый графом, тогда и только тогда, когда формула $p = q$ является логическим следствием аксиом (1).

$p \cup q = q \cup p$	$\varnothing \circ p = \varnothing$
$p \cup \varnothing = p$	$p \circ \varnothing = \varnothing$
$p \cup p = p$	$p^{\otimes} \cup X \geq p^{\otimes} \circ p \cup p \cup X$
$p \circ (q \circ r) = (p \circ q) \circ r$	$p^{\otimes} \cup X \geq p \circ p^{\otimes} \cup p \cup X$ (1)
$X \circ p = p$	$q \cup p \circ y \leq y \Rightarrow p^{\otimes} \circ q \cup q \leq y$
$p \circ X = p$	$q \cup y \circ p \leq y \Rightarrow q \circ p^{\otimes} \cup q \leq y$
$(p \cup q) \circ r = p \circ r \cup q \circ r$	$p \leq X \Rightarrow p \circ p = p$

Отношение $\leq$ является естественным частичным порядком: $p \leq q$ тогда и только тогда, когда $p \cup q = q$.

Теорема 1. Для любого языка $L \subseteq X^{+}$ следующие утверждения эквивалентны:

1) L - язык, представимый регулярным выражением алгебры $\left\langle 2^{X^{+}}, \circ, \cup, *, \varnothing, X \right\rangle$;

2) L - язык, порождаемый графом с отмеченными вершинами.

На основе доказательства теоремы разработаны методы анализа и синтеза языков, представимых в графах с отмеченными вершинами.

Теорема 2. Для любого недетерминированного графа G, порождающего язык $L(G)$, существует такой полный детерминированный граф G', что $L(G) = L(G')$.

Теорема 3. Язык $L \subseteq X^{+}$ порождается конечным графом с отмеченными вершинами тогда и только тогда, когда отношение ρ_L разбивает X^{+} на конечное число классов эквивалентности.

Теорема 4. Любому языку, порождаемому графом с отмеченными вершинами, соответствует единственный с точностью до изоморфизма полный детерминированный граф с минимальным числом вершин и единственная система леволинейных уравнений с минимальным числом уравнений, за решения которой может быть получено регулярное выражение, описывающее этот язык.

На основании доказательства теоремы 3 разработан алгоритм построения для любого графа с отмеченными вершинами G полного детерминированного графа с минимальным числом вершин, порождающего язык $L(G)$.

Выводы. В данной работе выполнен обзор и анализ современных математических методов проектирования и верификации вычислительных систем и рассмотрена новая автоматно-алгебраическая модель вычислительной системы, основанная на использовании графов с отмеченными вершинами. Исследованы основные свойства алгебры языков, представимых в графах с отмеченными вершинными: найдены алгебраическая и лингвистическая характеризации языков, представимых регулярными выражениями этой алгебры, разработаны методы анализа и синтеза рассматриваемых языков, способы детерминизации и минимизации графов с отмеченными вершинами.

Список литературы

1. Капитонова Ю.В. . Математическая теория проектирования вычислительных систем / Ю.В. Капитонова, А.А. Летичевский. – Москва: Наука, 1988. – 296с.
2. Baier C. Principles of Model Checking / C. Baier, J.-P. Katoen. – Cambridge: MIT Press, 2008. – 975 p.
3. Clarke E. M. Model Checking / E. M. Clarke, O. Grumberg, D. Peled. – Cambridge: MIT Press, 1999. – 257 p.
4. Anderson J. Automata Theory with Modern Applications / J. Anderson. – Cambridge: Cambridge University Press, 2006. – 255 с.