УДК 519.713.1

А.Н. ЧЕБОТАРЕВ

ПРОБЛЕМЫ СИНТЕЗА Σ-АВТОМАТОВ, СПЕЦИФИЦИРОВАННЫХ В ЯЗЫКАХ LP И LF ЛОГИКИ ПЕРВОГО ПОРЯДКА

Аннотация. Для двух фрагментов, LP и LF, логики первого порядка с ограниченными кванторами сформулированы и доказаны соответствующие варианты теоремы о спецификации, позволяющие свести процедуру синтеза Σ-автоматов, специфицированных формулами этих логик, к эквивалентному преобразованию формул.

Ключевые слова: логики первого порядка, спецификация, Σ-автомат, LP-формула, LF-формула, автоматная семантика, теорема о спецификации.

ВВЕДЕНИЕ

Проблема синтеза реактивной системы заключается в построении такой системы, поведение которой при ее взаимодействии со средой будет удовлетворять требованиям спецификации независимо от возможного поведения среды. В качестве моделей проектируемой системы и среды используются автоматные модели, например автоматы-распознаватели над бесконечными словами или деревьями, транзиционные системы, трансдьюсеры (автоматы с входом и выходом) и др. При этом возникает задача выяснения возможности реализации требований к поведению реактивной системы в виде поведения соответствующей автоматной модели. Для решения этой задачи обычно используется игровой подход, основанный на рассмотрении бесконечной игры между системой и средой, с которой она взаимодействует. Построение корректного алгоритма функционирования системы состоит в нахождении выигрышной для нее стратегии. Спецификации, для которых выигрышные стратегии существуют, называются реализуемыми [1]. Сложность построения такой стратегии зависит от способа задания условия выигрыша и, следовательно, от класса свойств системы, характеризуемых этим условием. Так, при задании условия LTL-формулой задача построения стратегии полна в классе 2EXPTIME [2]. Поэтому при практическом использовании игровых моделей ограничиваются более узкими классами свойств, выразимых в подходящих фрагментах логики LTL или аналогичных логик первого порядка, для которых проблема синтеза может решаться гораздо эффективнее [3–5].

Следует отметить, что рассматриваемые в статье задача синтеза ориентированы на раздельное решение проблемы реализуемости и синтеза. Предполагается, что спецификация реактивной системы состоит из двух частей: спецификации требований к поведению проектируемой системы, управляющая часть которой моделируется Σ-автоматом, и информации о возможном поведении среды, также представленной в виде спецификации Σ-автомата. Очевидно, что требования к поведению синтезируемого автомата, в явной или неявной форме ограничивающие поведение среды, не могут быть реализованы. Отсюда возникает проблема согласования спецификации системы со спецификацией среды [6]. Понятие согласуемости спецификации системы со средой, в отличие от более общего понятия реализуемости спецификации системы, связано с ограничением свойств, определяемых спецификациями системы и среды, свойствами безопасности (safety) [7], что позволяет решать задачу согласования как на уровне спецификаций, так и на уровне синтезированных автоматов [8]. Что касается свойств живости (liveness) [7], то они учитываются при написании спецификации и верифицируются на модели, в качестве которой выступает синтезированный автомат.

Как отмечено выше, при решении проблемы синтеза существенное значение имеет использование такого языка спецификации, который позволяет специфицировать достаточно широкий класс автоматов определенного вида и обеспечивает приемлемую сложность процедуры синтеза. Очевидно, что чем проще синтаксис языка спецификации, тем меньше сложность процедуры синтеза. Исходя из этих соображений, в качестве языка спецификации был предложен язык L [9], формулы которого имеют вид $\forall tF(t)$, где $F(t)$ — формула, не содержащая кванторов и символов числовых отношений. Класс автоматов, специфицируемых в этом языке, составляют автоматы с конечной памятью. Для увеличения выразительных возможностей языка L, как в смысле свойств, необходимых для описания требований к функционированию устройств, так и в смысле класса специфицируемых автоматов, предложен язык L* [10], представляющий собой расширение языка L за счет добавления в него конструкции, содержащей ограниченные кванторы, что позволило специфицировать некоторые автоматы, не обладающие конечной памятью. В качестве области интерпретации обоих языков выступает множество целых чисел. Это упрощает как процесс написания спецификации, делая его более естественным, так и преобразование формул спецификации в процессе синтеза.

Для спецификаций в языке L* разработан метод синтеза [11], позволяющий синтезировать управляющие автоматы, с количеством состояний порядка нескольких тысяч. Суть метода заключается в приведении исходной спецификации к некоторой нормальной форме, структура которой соответствует графу переходов синтезируемого автомата. Доказательство корректности этого метода, т.е. того, что результат синтеза соответствует семантике языка спецификации, основано на теореме о спецификации, сформулированной и доказанной в [10].

В работе [12] рассмотрены два фрагмента, LP и LF, монадической логики первого порядка с ограниченными кванторами, существенно расширяющие выразительные возможности языка L*, являющегося подмножеством языка LP. Для языков LP и LF, также интерпретируемых на целых числах, определены две семантики — детерминированная и недетерминированная, устанавливающие соответствие между формулами спецификации и специфицируемыми ими автоматами как из класса детерминированных, так и недетерминированных Σ-автоматов. Расширение, по сравнению с языком L*, класса используемых для спецификации формул потребовало корректировки алгоритма синтеза, хотя основная идея метода синтеза сохранилась. В настоящей статье сформулирована и доказана теорема о спецификации в более общем виде и в двух вариантах, соответствующих языкам LP и LF. Причем для языка LP теорема определяется детерминированной семантикой, а для языка LF — недетерминированной. Установленная в [12] связь между автоматами, специфицированными симметричными формулами языков LP и LF, позволяет для каждого из этих языков синтезировать автоматы в соответствии с обеими семантиками.

БЕСКОНЕЧНЫЕ СЛОВА И АВТОМАТЫ

Пусть Σ — конечный алфавит, $\mathbf{Z}$ — множество целых чисел, $\mathbf{N}^+ = \{z \in \mathbf{Z} | \, z > 0\}$, $\mathbf{N}^- = \{z \in \mathbf{Z} | \, z \le 0\}$. Отображение r множества $\{1, \ldots, n\}$ $(n \ge 0)$ в Σ называется словом длины n в алфавите Σ и обозначается $\sigma_1 \sigma_2 \ldots \sigma_n$, где $\sigma_i = r(i)$ для всех $1 \le i \le n$. Слово длины 0 (пустое слово) обозначается ε. Отображение $u : \mathbf{Z} \to \Sigma$ называется двусторонним сверхсловом ($\mathbf{Z}$-словом) в алфавите Σ и обозначается

$\ldots \sigma_{-2}\sigma_{-1}\sigma_0\sigma_1\sigma_2\ldots$, где $\sigma_i = u(i)$, $i \in \mathbf{Z}$. Отображения $l : \mathbf{N}^+ \to \Sigma$ и $g : \mathbf{N}^- \to \Sigma$ называются соответственно сверхсловом (обозначается $\sigma_1\sigma_2\ldots$, где $\sigma_i = l(i)$, $i \in \mathbf{N}^+$) и обратным сверхсловом (обозначается $\cdots\sigma_{-2}\sigma_{-1}\sigma_0$, где $\sigma_i = g(i)$ для $i \in \mathbf{N}^-$). Множество всех слов в алфавите Σ, включая пустое слово, обозначается Σ^*, множество всех сверхслов — Σ^ω, а множество всех обратных сверхслов — $\Sigma^{-\omega}$. Множество всех двусторонних сверхслов в алфавите Σ обозначим $\Sigma^{\mathbf{Z}}$. На множестве $\Sigma^* \cup \Sigma^{-\omega} \cup \Sigma^\omega$ обычным образом определена (частичная) операция конкатенации «$\cdot$», которую распространим также на множества слов и сверхслов. Бесконечные отрезки двустороннего сверхслова u $\ldots u(k-2)u(k-1)u(k)$ и $u(k+1)u(k+2)\ldots$, где $k \in \mathbf{Z}$, назовем соответственно его k-префиксом и k-суффиксом. Для $n \in \mathbf{N}^+$ n-префиксом сверхслова l называется слово $l(1)\ldots l(n)$. Если значение позиции в $\mathbf{Z}$-слове несущественно, то понятия префикса и суффикса определяются следующим образом. Обратное сверхслово g называется префиксом $\mathbf{Z}$-слова u, а сверхслово l — его суффиксом, если $g \cdot l = u$.

Множество Σ^ω будем рассматривать как топологическое пространство с канторовой топологией [13]. Открытыми множествами в этой топологии являются все множества вида $K \cdot \Sigma^\omega$, где $K \subseteq \Sigma^*$. Дополнение открытого множества в Σ^ω называется замкнутым множеством. Замкнутые множества характеризуются следующим утверждением [13].

Утверждение 1. Множество L замкнуто тогда и только тогда, когда каждое сверхслово, не принадлежащее L, имеет конечный префикс, не являющийся префиксом никакого сверхслова из L.

Пусть $R \subseteq \Sigma^\omega$. Наименьшее замкнутое множество, включающее R, называется его замыканием и обозначается $\overline{R}$.

Утверждение 2. Сверхслово $l \in \Sigma^\omega$ принадлежит $\overline{R}$ тогда и только тогда, когда каждый префикс сверхслова l есть префикс сверхслова из R.

В качестве автоматов над сверхсловами, ассоциируемых с формулами рассматриваемых в работе логик, используются частичные неинициальные автоматы без выхода. Такой автомат $A = <\Sigma, Q, \delta>$, где Σ — входной алфавит, Q — конечное множество состояний, а $\delta : Q \times \Sigma \to Q$ — частичная функция переходов, назовем детерминированным Σ-автоматом. Если функция переходов имеет вид $\delta : Q \times \Sigma \to 2^Q$, Σ-автомат называется недетерминированным.

Пусть $q_1, q_2 \in Q$, а $\sigma \in \Sigma$. Тройку $< q_1, \sigma, q_2 >$, такую что $q_2 \in \delta(q_1, \sigma)$, назовем переходом в автомате A, а символ σ — отметкой этого перехода. Предполагается, что символы алфавита Σ представляют собой двоичные векторы длины m, что соответствует кодированию абстрактных символов наборами значений двоичных переменных из множества $\Omega = \{p_1, \ldots, p_m\}$. Этим переменным соответствуют одноименные предикатные символы в логических спецификациях автоматов. Поэтому каждому такому вектору из Σ поставим в соответствие конъюнкцию вида $\widetilde{p}_1(t) \& \ldots \& \widetilde{p}_m(t)$, где $\widetilde{p}_i(t) \in \{p_i(t), \neg p_i(t)\}$, принимающую значение «истина» на этом векторе. Произвольное множество символов алфавита удобно задавать в виде пропозициональной формулы с именами переменных $p_1(t), \ldots, p_m(t)$.

Определение 1. Σ-автомат $A = <\Sigma, Q, \delta>$ называется циклическим, если для каждого $q \in Q$ существуют такие $\sigma_1, \sigma_2 \in \Sigma$ и $q_1, q_2 \in Q$, что $q_1 \in \delta(q, \sigma_1)$ и $q \in \delta(q_2, \sigma_2)$.

В дальнейшем под Σ-автоматом будем понимать циклический Σ-автомат. Такой автомат можно однозначно охарактеризовать в терминах допустимых сверхслов.

Определение 2. Сверхслово $l = \sigma_1\sigma_2\ldots$ в алфавите Σ допустимо в состоянии q Σ-автомата A, если существует такое сверхслово состояний $q_0 q_1 q_2 \ldots$, где $q_0 = q$, что для любого $i = 0, 1, 2, \ldots$ $q_{i+1} \in \delta(q_i, \sigma_{i+1})$.

Сверхслово l допустимо для автомата A, если оно допустимо хотя бы в одном из его состояний. Множество всех сверхслов, допустимых для автомата A, обозначим $W(A)$. Два Σ-автомата, A_1 и A_2, назовем слабо эквивалентными, если $W(A_1) = W(A_2)$.

Определение 3. Пусть множество Q состояний Σ-автомата A равно $\{q_1, \ldots, q_n\}$. Семейство множеств сверхслов $S(A) = (W_1, \ldots, W_n)$, где $W_i = W(q_i)$ $(i = 1, \ldots, n)$, назовем поведением автомата A.

Два Σ-автомата, A_1 и A_2, с поведениями соответственно $(W_1', \ldots, W_n')$ и $(W_1'', \ldots, W_m'')$ называются строго эквивалентными, если каждое W_i' $(i = 1, \ldots, n)$ содержится среди $W_1'', \ldots, W_m''$ и каждое $W_i''(i = 1, \ldots, m)$ содержится среди $W_1', \ldots, W_n'$.

ЛОГИКИ LP И LF С ОГРАНИЧЕННЫМИ КВАНТОРАМИ

Логики LP и LF — это фрагменты монадической логики первого порядка с ограниченными кванторами, предназначенные для спецификации циклических Σ-автоматов. Поэтому для них определена автоматная семантика, т.е. правила, согласно которым формуле логики однозначно ставится в соответствие специфицируемый ею Σ-автомат. Обе логики интерпретируются на множестве $\mathbf{Z}$ целых чисел, рассматриваемом как множество моментов дискретного времени, в котором функционируют специфицируемые автоматы. Синтаксис этих логик соответствует общепринятому синтаксису логики первого порядка с одноместными предикатами, двуместными отношениями $\le, \ge$, интерпретируемыми на множестве $\mathbf{Z}$ обычным образом, и функцией следования или предшествования [12]. В качестве сокращения для функций следования и предшествования введены операции прибавления и вычитания единицы, что приводит к термам вида $(t + k)$, где t — предметная переменная, а $k \in \mathbf{Z}$. Атомарные формулы могут быть двух типов: $P_i(\tau)$ или $\tau_1\rho\tau_2$, где P_i — одноместный предикатный символ, $\rho \in \{<, >, \le, \ge\}$, а τ, τ_1, τ_2 — термы. Формулы строятся из атомарных формул с помощью логических связок, кванторов, применяемых к предметным переменным, и, возможно, скобок. Обозначение $\varphi(t_1, \ldots, t_n)$ указывает на то, что множество всех свободных переменных в формуле φ равно $\{t_1, \ldots, t_n\}$. Формула, не содержащая свободных переменных, называется предложением.

Пусть $\Omega = \{p_1, \ldots, p_m\}$ — множество всех одноместных предикатных символов, имеющихся в формуле F. Поскольку в формуле не интерпретированы только одноместные предикатные символы, ее интерпретацию можно рассматривать как упорядоченный набор определенных на $\mathbf{Z}$ одноместных предикатов $P_1, \ldots, P_m$, соответствующих предикатным символам из Ω. Пусть Σ — множество всех двоичных векторов длины m, тогда интерпретацию формулы F можно представить в виде $\mathbf{Z}$-слова в алфавите Σ. В дальнейшем не будем различать интерпретации для формулы F и соответствующие им $\mathbf{Z}$-слова, поэтому будем говорить об истинности или ложности F на $\mathbf{Z}$-слове.

Спецификации в логиках LP и LF представляют собой формулы вида $\forall t F(t)$. Существенное различие между этими логиками состоит в особенностях формул $F(t)$ с одной свободной переменной. Так, в логике LP истинность такой формулы в некоторый момент времени определяется значениями встречающихся в ней предикатных символов в этот и предыдущие моменты времени, а в логике LF — в текущий и последующие моменты. Для уточнения этого утверждения введем следующие определения.

Определение 4. Формула $F(t)$ с единственной свободной переменной t называется k-ограниченной справа ($k \in \mathbf{Z}$), если для любого $\tau \in \mathbf{Z}$ значения формулы $F(\tau)$ на всех двусторонних сверхсловах, имеющих одинаковые $(\tau + k)$-префиксы, совпадают.

Определение 5. Формула $F(t)$ с единственной свободной переменной t называется k-ограниченной слева ($k \in \mathbf{Z}$), если для любого $\tau \in \mathbf{Z}$ значения формулы $F(\tau)$ на всех двусторонних сверхсловах, имеющих одинаковые $(\tau + k)$-суффиксы, совпадают.

Очевидно, что для всякого $k_1 > k$ формула $F(t)$, k-ограниченная справа, также k_1-ограничена справа, а для $k_1 < k$ формула $F(t)$, k-ограниченная слева, также k_1-ограничена слева. Формула $F(t)$ ограничена с обеих сторон, если существуют такие $k_1, k_2 \in \mathbf{Z}$, что $k_1 < k_2$ и $F(t)$ k_1-ограничена слева и k_2-ограничена справа. Формулы вида $\forall t F(t)$ называются формулами прошедшего времени (P-формулами), если $F(t)$ ограничена справа, и формулами будущего времени (F-формулами), если $F(t)$ ограничена слева. Если $F(t)$ ограничена с двух сторон, то формулу $\forall t F(t)$ можно трактовать либо как P-формулу, либо как F-формулу.

Итак, предложения логики LP представляют собой P-формулы, а предложения логики LF — F-формулы.

В дальнейшем формулы $F(t)$, 0-ограниченные справа и (-1)-ограниченные слева, будут рассматриваться как способ задания соответственно сверхслов и обратных сверхслов. Будем говорить, что 0-ограниченная справа формула $F(t)$ истинна на обратном сверхслове g, если $F(0)$ истинна на любом двустороннем сверхслове с 0-префиксом g. Аналогично (-1)-ограниченная слева формула $F(t)$ истинна на сверхслове l, если $F(0)$ истинна на любом двустороннем сверхслове, с (-1)-суффиксом l.

Определение 6. 0-ограниченная справа формула $F(t)$ задает множество $R(F(t))$ всех тех обратных сверхслов, на которых она истинна.

Определение 7. (-1)-ограниченная слева формула $F(t)$ задает множество $S(F(t))$ всех тех сверхслов, на которых она истинна.

Рассмотрим теперь подробнее ограничения, которым удовлетворяют формулы логики LP. Каждая подформула формулы $F(t)$ имеет не более двух свободных (в этой подформуле) переменных. Все подформулы, начинающиеся квантором (кванторные подформулы), с одной свободной переменной имеют вид $\exists t_1 (t_1 \le t + k) F_1(t_1)$ или $\forall t_1 (t_1 \le t + k) \to F_1(t_1)$, а кванторные подформулы с двумя свободными переменными — $\exists t_2 (t_1 < t_2 \le t + k) F_2(t_2)$ или $\forall t_2 (t_1 < t_2 \le \le t + k) \to F_2(t_2)$, где $k \in \mathbf{Z}$. Выражения $(t_1 \le t + k)$ и $(t_1 < t_2 \le t + k)$ в этих подформулах называются ограничениями области действия кванторов, а сами кванторы — ограниченными. Из сказанного следует, что свободные переменные в кванторных подформулах встречаются только в ограничениях области действия кванторов. Атомарные формулы вида $\tau_1 \rho \tau_2$, где τ_1 и τ_2 — термы, а $\rho \in \in \{<, >, \le, \ge\}$, также встречаются только в ограничениях области действия кванторов. Каждая такая формула равносильна формуле вида $(t_1 \le t_2 + k)$, где $k \in \mathbf{Z}$. Заметим, что выражение $(t_1 < t_2 \le t + k)$ представляет собой сокращение для выражения $(t_1 < t_2) \& (t_2 \le t + k)$. Очевидно, что формулы с одной свободной переменной, удовлетворяющие приведенным выше требованиям, ограничены справа. Таким образом, язык LP составляют P-формулы.

Логика LF представляет собой фрагмент монадической логики первого порядка, в некотором смысле симметричный логике LP. Синтаксис языка LF совпадает с синтаксисом языка LP во всем, кроме ограничений области действия кванторов. Так, все кванторные подформулы с одной свободной переменной имеют вид $\exists t_1 (t_1 \ge t + k) F_1(t_1)$ или $\forall t_1 (t_1 \ge t + k) \to F_1(t_1)$, а кванторные подформулы с двумя свободными переменными — $\exists t_2 (t_1 > t_2 \geq t+k) F_2(t_2)$ или $\forall t_2$ $(t_1 > t_2 \geq t+k) \to F_2(t_2)$, где $k \in \mathbf{Z}$. Таким образом, язык LF составляют F-формулы.

АВТОМАТНАЯ СЕМАНТИКА ЛОГИК LP И LF

С формулой F логики одноместных предикатов первого порядка, интерпретируемой на множестве $\mathbf{Z}$, ассоциируется множество **Z**-слов, представляющих собой модели для F. При установлении соответствия между автоматами и логическими формулами те и другие рассматриваются как формализмы для задания множеств сверхслов (ω-языков). Переход от **Z**-слов, ассоциируемых с формулами, к сверхсловам осуществляется путем рассмотрения всех суффиксов **Z**-слов. Таким образом для формулы F, имеющей множество моделей $M(F)$, получается множество сверхслов $W(F) = \bigcup\limits_{u \in M(F)} \{w \mid w \in \mathrm{Suf}(u)\}$, где $\mathrm{Suf}(u)$ — множество всех суффиксов **Z**-слова *u*. Аналогично определяется множество обратных сверхслов $P(F) = \bigcup\limits_{u \in M(F)} \{g \mid g \in \mathrm{Pref}(u)\}$, где $\mathrm{Pref}(u)$ — множество всех префиксов **Z**-слова *u*. Для Σ-автомата A ассоциируемый с ним ω-язык представляет собой множество $W(A)$ сверхслов, допустимых для A. Поскольку это множество топологически замкнуто, при сравнении его с множеством $W(F)$ рассматривается замыкание последнего. Однако множество $W(A)$ не определяет однозначно Σ-автомат — существуют различные автоматы, как детерминированные, так и недетерминированные, имеющие одно и то же множество допустимых сверхслов. Поэтому, чтобы идентифицировать детерминированные автоматы с точностью до строгой эквивалентности, введено понятие поведения $S(A) = (W_1, \ldots, W_n)$ для автомата A с множеством состояний $\{q_1, \ldots, q_n\}$, где $W_i = W(q_i)$, $i = 1, \ldots, n$. Так же определяется и поведение недетерминированного автомата. Для того чтобы поведение недетерминированного автомата однозначно определяло его функцию переходов, на $S(A)$ налагается дополнительное ограничение: для $i, j \in \{1, \ldots, n\}$, $i \neq j$, $W(q_i) \cap W(q_j) = \varnothing$.

Σ-автомат, специфицируемый формулой, определяется автоматной семантикой. Поскольку в задачах проектирования реактивных систем могут использоваться как детерминированные, так и недетерминированные Σ-автоматы, в [12] предложено использовать две автоматные семантики: детерминированную и недетерминированную. Детерминированная семантика однозначно ставит в соответствие формуле F детерминированный Σ-автомат $A(F)$, а недетерминированная — недетерминированный Σ-автомат $A'(F)$.

Детерминированная семантика определяется следующим образом. Каждому обратному сверхслову $g \in P(F)$ поставим в соответствие множество сверхслов $S_g = \{l \in W(F) \mid g \cdot l \in M(F)\}$, т.е. S_g состоит из всех тех сверхслов, конкатенация каждого из которых с префиксом g соответствует модели для F. Назовем такие сверхслова допустимыми продолжениями префикса g. На множестве префиксов $P(F)$ определим отношение эквивалентности так, что два префикса, g_1 и g_2, эквивалентны, если они имеют одно и то же множество допустимых продолжений. Эта эквивалентность разбивает множество $P(F)$ на классы эквивалентности $P_1, P_2, \ldots, P_n$, и классу P_i соответствует состояние автомата q_i, для которого $W(q_i)$ равно замыканию множества допустимых продолжений для префиксов из P_i. Таким образом, поведение специфицируемого автомата имеет вид $S(A(F)) = (W_1, \ldots, W_n)$, где $W_i = W(q_i)$, $i = 1, \ldots, n$. При этом $\delta(q_i, \sigma) = q_j$ тогда и только тогда, когда $P_i \sigma \subseteq P_j$. Отсюда следует, что функция переходов детерминирована. Действительно, поскольку множества $P_1, P_2, \ldots, P_n$ попарно не пересекаются, приведенному соотношению может удовлетворять только единственное множество P_j. Построение автомата $A(F)$, специфицируемого формулой F, сводится к построению такого разбиения. Как правило, этот автомат приведенный. На практике строится не приведенный автомат, а автомат, строго эквивалентный ему, чему соответствует разбиение множества $P(F)$ на классы эквивалентных префиксов. В результате несколько таких классов может включаться в один класс эквивалентности.

Недетерминированная семантика определяется симметричным образом.

Каждый суффикс $l \in W(F)$ определяет множество $P(l)$ допустимых для него префиксов, т.е. $P(l) = \{g \in P(F) | g \cdot l \in M(F)\}$. На множестве суффиксов $W(F)$ определим отношение эквивалентности так, что два суффикса, l_1 и l_2, эквивалентны, если они имеют одно и то же множество допустимых для них префиксов. Эта эквивалентность разбивает множество $W(F)$ на классы эквивалентности $S_1, S_2, \ldots, S_n$, каждому из которых соответствует состояние специфицируемого Σ-автомата $A'(F)$ с поведением $(\bar{S}_1, \ldots, \bar{S}_n)$, где $\bar{S}_i$ — замыкание множества S_i. Функция переходов определяется следующим образом: для $\sigma \in \Sigma$ $\delta'(q_i, \sigma) = \{q_{i_j}\}$, где $\{q_{i_j}\}$ — множество всех таких q_{i_j}, для которых выполняется соотношение $\sigma S_{i_j} \subseteq S_i$. Как следует из приведенных выше семантик, детерминированный и недетерминированный автоматы, специфицируемые формулой F, слабо эквивалентны, т.е. имеют одно и то же множество допустимых сверхслов.

Рассмотрим топологические свойства множеств допустимых продолжений префиксов **Z**-слов из $M(F)$ для P-формул и F-формул. Пусть $L \subseteq \Sigma^\omega$, обозначим $\mathrm{Pref}(L)$ множество всех конечных префиксов всех сверхслов, принадлежащих L.

Утверждение 3. Для P-формулы F множество S_g допустимых продолжений для любого префикса $g \in P(F)$ замкнуто.

Для простоты будем считать, что подформула $F(t)$ в формуле $F = \forall t F(t)$ 0-ограничена справа, что не уменьшает общности рассмотрения. Напомним, что для P-формулы $F = \forall t F(t)$ истинность 0-ограниченной справа формулы $F(t)$ в позиции τ **Z**-слова определяется его τ-префиксом. Пусть сверхслово l не принадлежит S_g, тогда **Z**-слово gl не является моделью для формулы F. Если каждый (конечный) префикс сверхслова l принадлежит $\mathrm{Pref}(S_g)$, то в любой позиции **Z**-слова gl формула $F(t)$ истинна и, следовательно, **Z**-слово gl — модель для F, что противоречит предположению. Из этого следует, что существует префикс сверхслова l, не принадлежащий $\mathrm{Pref}(S_g)$. Таким образом, согласно утверждению 1 множество S_g замкнуто.

Прежде чем сформулировать подобную характеристику для F-формул, приведем без доказательства следующее достаточно очевидное утверждение.

Утверждение 4. Для F-формулы F существует такое $g \in P(F)$, что $S_g = \Sigma^\omega$, тогда и только тогда, когда $M(F) = \Sigma^{\mathbf{Z}}$.

Очевидно, что всякая формула $F(t)$, такая что $M(\forall t F(t)) = \Sigma^{\mathbf{Z}}$, ограничена с обеих сторон, например, 0-ограничена справа и (-1)-ограничена слева. Примером такой формулы может служить $1(t)$, где $1(t)$ — тождественно истинная формула.

Утверждение 5. Для F-формулы F, ограниченной только слева, множество суффиксов S_g для любого $g \in P(F)$ не замкнуто.

Как следует из утверждения 1, множество $L \subseteq \Sigma^\omega$ не замкнуто, если существует не принадлежащее ему сверхслово l, каждый префикс которого принадлежит $\mathrm{Pref}(L)$. Для F-формулы $F = \forall t F(t)$ истинность 0-ограниченной слева формулы $F(t)$ в позиции τ **Z**-слова определяется его τ-суффиксом. Сверхслово l, каждый префикс которого принадлежит $\mathrm{Pref}(S_g)$, будем строить пошагово, добавляя на каждом шаге символ из Σ так, чтобы слово r, получаемое на каждом шаге, принадлежало $\mathrm{Pref}\,(S_g)$. Поскольку $F(t)$ не ограничена справа, $S_g \neq \Sigma^\omega$, поэтому для полученного таким образом слова r любой длины найдется такое сверхслово l_1, что grl_1 не принадлежит $M(F)$, т.е. rl_1 не принадлежит S_g. Отсюда следует, что существует сверхслово $l \notin S_g$, каждый префикс которого принадлежит $\mathrm{Pref}(S_g)$.

Из утверждения 3 вытекает, что в определении детерминированной семантики Р-формул в качестве множества $W(q)$ для состояния q автомата $A(F)$ можно рассматривать множество допустимых продолжений для соответствующего ему класса эквивалентности префиксов из $P(F)$, поскольку оно замкнуто. Это замечание касается и недетерминированной семантики Р-формул.

ТЕОРЕМА О СПЕЦИФИКАЦИИ

Спецификация в логическом языке характеризует требования к поведению проектируемого автомата в терминах временных (темпоральных) соотношений между входными и выходными сигналами. В настоящей работе в качестве автоматной модели рассматривается неинициальный циклический Σ-автомат (без выходов). Напомним, что символы алфавита Σ кодируются наборами значений двоичных переменных из множества $\Omega = \{p_1, \dots, p_m\}$, которым взаимно однозначно соответствуют предикатные символы спецификации. При установлении соответствия между формулами и автоматами каждому двоичному вектору $\sigma \in \Sigma$ ставится в соответствие выражение языка спецификации $\widetilde{\sigma}(t)$ вида $\widetilde{p}_1(t) \& \dots \& \widetilde{p}_m(t)$, где $\widetilde{p}_i(t) \in \{p_i(t), \neg p_i(t)\}$, а p_i — предикатный символ. Определив разбиение множества переменных Ω на входные и выходные, символы алфавита Σ можно рассматривать как пары (x, y), где $x \in X$ — набор значений входных переменных, а $y \in Y$ — выходных. Таким образом, алфавит Σ рассматривается как прямое произведение $X \times Y$, а Σ-автомат — как X/Y-трансдьюсер. Кроме того, для задания инициального автомата к спецификации вида $\forall t F(t)$ добавляется формула $F_0(t)$, которая позволяет выделить в синтезированном автомате начальные состояния, удовлетворяющие этой формуле.

Основная задача синтеза состоит в преобразовании спецификации вида $\forall t F(t)$ в представление неинициального Σ-автомата в терминах состояний и функции переходов так, чтобы он гарантированно удовлетворял требованиям этой спецификации, т.е. чтобы все последовательности символов, допустимые для синтезированного Σ-автомата, удовлетворяли требованиям спецификации. Это условие определяется автоматной семантикой формул спецификации. Следовательно, задачей синтеза является построение автомата, специфицируемого логической формулой в соответствии с рассматриваемой автоматной семантикой. Основное значение в обосновании соответствующей корректности процедуры синтеза имеет доказанная ниже теорема о спецификации.

Прежде чем перейти к формулировке этой теоремы, приведем утверждение, непосредственно вытекающее из определения детерминированной семантики Р-формулы.

Утверждение 6. Р-формула F специфицирует детерминированный Σ-автомат A с поведением $S(A) = (W_1, \dots, W_n)$ тогда и только тогда, когда существует такое разбиение $(P_1, \dots, P_n)$ множества $P(F)$ на классы эквивалентных префиксов, что для каждого P_i множество допустимых продолжений для префиксов из P_i совпадает с W_i.

Теорема 1 (о спецификации). Пусть A — неинициальный детерминированный циклический Σ-автомат с состояниями $q_1, \dots, q_n$, а $F_1(t), \dots, F_n(t)$ — такие 0-ограниченные справа формулы, что для всех $i, j = 1, \dots, n$ выполняются следующие условия:

1) $R(F_i(t)) \cap P(F) \neq \varnothing$, где $R(F_i(t))$ — множество обратных сверхслов, задаваемое формулой $F_i(t)$;

2) $R(F_i(t)) \cap R(F_j(t)) = \varnothing$ при $i \neq j$;

3) если σ — отметка перехода из q_i в q_j, то $R(F_i(t))\sigma \subseteq R(F_j(t))$.

Тогда формула $F = \forall t \left(\mathop{\vee}\limits_{i=1}^{n} F_i(t-1) \,\&\, \mathop{\vee}\limits_{j=1}^{m_i} \tilde{\sigma}_{i_j}(t) \right)$, где m_i — количество переходов в автомате A из состояния q_i, а $\tilde{\sigma}_{i_j}(t)$ — конъюнкция, соответствующая отметке σ_{i_j} j-го перехода из состояния q_i, специфицирует автомат A в соответствии с детерминированной семантикой.

Доказательство теоремы состоит в доказательстве того, что разбиением множества $P(F)$ на классы эквивалентных префиксов, удовлетворяющим утверждению 6, является совокупность множеств $\{P_i = P(F) \cap R(F_i(t) \mid i = 1, 2, \ldots, n\}$. Прежде всего, покажем, что определенная таким образом совокупность множеств $\{P_1, \ldots, P_n\}$ является разбиением множества $P(F)$, т.е. что объединение их совпадает с $P(F)$. (То, что эти множества попарно не пересекаются, следует из условия 2, а то, что они не пусты, — из условия 1 теоремы.) Из приведенной выше формулы F видно, что если в произвольной позиции τ какой-либо модели из $M(F)$ истинна формула $F_i(t-1) \,\&\, \mathop{\vee}\limits_{j=1}^{m_i} \tilde{\sigma}_{i_j}(t)$, то в позиции $\tau - 1$ истинна формула $F_i(t)$. Таким образом, в каждой позиции модели из $M(F)$ истинна какая-либо формула $F_i(t)$ и, следовательно, в силу 0-ограниченности справа формул $F_i(t)$ каждый префикс из $P(F)$ принадлежит некоторому множеству $R(F_i(t))$ $(i = 1, 2, \ldots, n)$. Отсюда следует, что $\bigcup\limits_{i=1}^{n} P_i = P(F)$.

Теперь покажем, что все префиксы из P_i имеют одно и то же множество допустимых продолжений, совпадающее с $W(q_i)$. Пусть $g \in P(F)$, а $r \in \Sigma^*$ — слово длины k. Будем говорить, что r — допустимое k-продолжение префикса g, если $gr \in R(F(t))$, т.е. $F(t)$ истинна на gr.

Пусть g — τ-префикс некоторой модели для F, принадлежащий P_i, а значит, и $R(F_i(t))$. Подформула $\mathop{\vee}\limits_{j=1}^{m_i} \tilde{\sigma}_{i_j}(t)$ в формуле F задает множество символов $\Sigma_i \subseteq \Sigma$, для которых определены переходы из состояния q_i. Рассмотрим множество 1-продолжений для g, совпадающих с Σ_i. Все эти продолжения допустимы для g, поскольку на каждом таком обратном сверхслове $g\sigma$ истинна подформула $F_i(t-1) \mathop{\vee}\limits_{j=1}^{m_i} \tilde{\sigma}_{i_j}(t)$, а следовательно, и формула $F(t)$. В силу условия 3 каждый префикс $g\sigma$ $(\sigma \in \Sigma_i)$ принадлежит одному из множеств $R(F_j(t))$, $j = 1, \ldots, n$. Построив для каждого префикса $g\sigma$ 1-продолжения, определяемые соответствующим множеством Σ_j, получим дерево допустимых 2-продолжений префикса g. Действуя так и далее, будем получать допустимые k-продолжения r_k префикса g $(k \geq 1)$. Каждый префикс gr_k принадлежит $R(F(t))$. Таким образом, для любого конечного $k \in \mathbf{N}^+$ множество всех допустимых k-продолжений для g совпадает с множеством k-префиксов сверхслов из $W(q_i)$. Поскольку $W(q_i)$ замкнуто, множество S_g всех допустимых продолжений префикса g совпадает с $W(q_i)$.

Приведенное рассуждение справедливо для любого обратного сверхслова из P_i, следовательно, множества допустимых продолжений для всех обратных сверхслов из P_i совпадают. Таким образом, P_i является классом эквивалентных префиксов из $P(F)$, совпадающим с S_i. На этом доказательство теоремы завершается.

Для F-формул логики LF соответствующая теорема формулируется симметрично теореме 1. В этом случае утверждение о специфицируемости Σ-автомата A, основанное на недетерминированной семантике, имеет следующий вид.

Утверждение 7. F-формула F специфицирует недетерминированный Σ-автомат A с поведением $S(A) = (W_1, \ldots, W_n)$, если существует такое разбиение $(S_1, \ldots, S_n)$ множества $W(F)$ на классы эквивалентных суффиксов, что замыкание каждого множества S_i $(i = 1, \ldots, n)$ совпадает с W_i.

Теорема 2. Пусть A — неинициальный недетерминированный циклический Σ-автомат с состояниями $q_1, \ldots, q_n$, а $F_1(t), \ldots, F_n(t)$ — такие (–1)-ограниченные слева формулы, что для всех $i, j = 1, \ldots, n$ выполняются следующие условия:

1) $S(F_i(t)) \cap W(F) \neq \varnothing$, где $S(F_i(t))$ — множество сверхслов, задаваемое формулой $F_i(t)$;

2) $S(F_i(t)) \cap S(F_j(t)) = \varnothing$ при $i \neq j$;

3) если σ — отметка перехода из q_i в q_j, то $\sigma S(F_j(t)) \subseteq S(F_i(t))$.

Тогда формула $F = \forall t \left(\overset{n}{\underset{i=1}{\vee}} F_i(t+1) \& \overset{m_i}{\underset{j=1}{\vee}} \tilde{\sigma}_{i_j}(t) \right)$, где m_i — количество переходов в автомате A из состояния q_i, а $\tilde{\sigma}_{i_j}(t)$ — элементарная конъюнкция, соответствующая отметке σ_{i_j} j-го перехода из состояния q_i, специфицирует автомат A.

Доказательство этой теоремы проводится аналогично доказательству теоремы 1 и состоит в доказательстве того, что разбиением множества $W(F)$ на классы эквивалентных суффиксов, удовлетворяющим утверждению 7, является совокупность множеств $\{S_i = W(F) \cap S(F_i(t) \mid i = 1, 2, \ldots, n\}$. При доказательстве того, что каждое S_i представляет собой множество эквивалентных суффиксов, вместо допустимых k-продолжений префикса рассматриваются допустимые $(-k)$-продолжения суффикса, т.е. продолжения в сторону уменьшения номеров позиций **Z**-слова. Поскольку согласно утверждению 5 множества S_i в общем случае не замкнуты, берется их замыкание.

Значение теорем 1 и 2 для синтеза Σ-автоматов состоит в том, что они устанавливают соответствие между структурой формулы спецификации и описанием специфицируемого ею автомата в терминах состояний и функции переходов. В основе метода синтеза детерминированного Σ-автомата по P-формуле или недетерминированного Σ-автомата по F-формуле лежит утверждение о том, что любая непротиворечивая формула может быть эквивалентно преобразована к виду, определяемому соответствующей теоремой. Однако проверка выполнимости условия 1 представляет собой очень сложную задачу, поэтому целесообразно преобразовывать спецификацию к виду, где подформулы $F_i(t)$ удовлетворяют условиям 2 и 3. Условие 1 удобнее проверять после синтеза автомата. При этом состояния, для которых соответствующие подформулы $F_i(t)$ не удовлетворяют условию 1, должны быть удалены. Таким образом, методы синтеза заключаются в преобразовании спецификации к требуемому виду и последующей проверке условия 1.

ЗАКЛЮЧЕНИЕ

В работе [12] рассмотрены два фрагмента, LP и LF, монадической логики первого порядка с ограниченными кванторами, используемые для спецификации автоматов в целях их синтеза. Фрагмент LP, являясь расширением языка L*, позволяет специфицировать более широкий в сравнении с L* класс автоматов. Спецификация в языке LP описывает зависимость поведения системы в текущий момент времени от ее состояния в прошлом. В языке LF используется другой подход к описанию поведения системы, при котором так же, как и в логике LTL, описывается желаемое поведение системы в будущем. Предложены две автоматные семантики: детерминированная и недетерминированная, определяющие соответствие между формулами указанных логик и детерминированными и недетерминированными Σ-автоматами. Использование недетерминированной семантики позволяет специфицировать автоматы, обратные детерминированным автоматам, а также установить связь между детерминированными автоматами, специфицируемыми формулами логик LP и LF. Однако построить автомат, специфицируемый заданной формулой, основываясь только на ее автоматной семантике, — задача чрезвычайно сложная, поэтому необходима корректная процедура синтеза автомата. Для обоснования такой процедуры в [10] доказана теорема о спецификации, позволяющая процедуру синтеза автомата свести к эквивалентному преобразованию формулы спецификации. Вследствие расширения класса формул спецификации по сравнению с языком L* и использования двух различных фрагментов логики потребовалась более общая формулировка такой теоремы в двух вариантах — соответственно для логик LP и LF. Вариант для P-формул определяется детерминированной семантикой, а для F-формул — недетерминированной. В настоящей работе устранены топологические ограничения на фигурирующие в теореме множества сверхслов и обратных сверхслов, задаваемые ограниченными подформулами с одной свободной переменной, и получено более простое ее доказательство по сравнению с доказательством в [10].

В основе метода синтеза детерминированного Σ-автомата по P-формуле или недетерминированного Σ-автомата по F-формуле лежит утверждение о том, что любая формула может быть преобразована к виду, удовлетворяющему всем условиям соответствующей теоремы, кроме условия 1, которое может быть проверено после синтеза автомата. Таким образом, методы синтеза заключаются в преобразовании спецификации к требуемому виду и последующей проверке условия 1. В теореме о спецификации предполагается непротиворечивость исходной формулы. Для противоречивой формулы условие 1 не выполняется. Однако если такую формулу преобразовывать с учетом только условий 2 и 3, то результат синтеза будет неверным и противоречивость будет установлена после проверки условия 1.

В статье исследованы топологические свойства множеств допустимых продолжений префиксов из $P(F)$ для P-формулы и F-формулы F. Показано, что соответствующие множества для P-формулы замкнуты, а для F-формулы не замкнуты. Поэтому при определении поведения специфицируемого автомата используются их замыкания, что автоматически учитывается в процедуре синтеза. Подробное описание и обоснование процедур синтеза будет дано в последующих работах.

СПИСОК ЛИТЕРАТУРЫ

1. Abadi M., Lamport L., Wolper P. Realizable and unrealizable specifications of reactive systems. *Lecture Notes in Computer Science*. Berlin; Heidelberg: Springer-Verlag, 1989. Vol. 372. P. 1–17.
2. Pnueli A., Rosner R. On the synthesis of a reactive module. *Proc.* 16^{th} *ACM Symp. on Principles of Programming Languages.* Austin, 1989. P. 179–190.
3. Alur R., La Torre S. Deterministic generators and games for LTL fragments. *ACM Transactions on Computational Logic*. 2004. Vol. 5, N 1. P. 1–25.
4. Harding A., Ryan M., Schobbens P.-J. A new algorithm for strategy synthesis in LTL games. *Lecture Notes in Computer Science.* Berlin; Heidelberg: Springer-Verlag, 2005. Vol. 3440. P. 477–492.
5. Piterman N., Pnueli A., Sa’ar Y. Synthesis of reactive(1) designs. *Lecture Notes in Computer Science*. Berlin; Heidelberg: Springer-Verlag, 2006. Vol. 3855. P. 364–380.
6. Чеботарев А.Н. Согласование спецификаций автоматов, представленных в языке L. *Кибернетика и системный анализ*. 2016. Т. 52, № 3. С. 3–15.
7. Alpern B., Schneider F. Recognizing safety and liveness. *Distributed computing*. 1987. N 2. P. 117–126.

8. Чеботарев А.Н. Согласование взаимодействующих автоматов. *Кибернетика и системный анализ*. 2015. Т. 51, № 5. С. 13–25.
9. Чеботарев А.Н. Регулярная форма спецификации детерминированных автоматов в языке L. *Прикладная дискретная математика*. 2010. № 4. С. 64–72.
10. Чеботарев А.Н. Расширение логического языка спецификации и проблема синтеза. *Кибернетика и системный анализ*. 1996. № 6. С. 11–27.
11. Чеботарев А.Н. Синтез процедурного представления автомата, специфицированного в логическом языке L*. I. *Кибернетика и системный анализ*. 1997. № 4. С. 60–74.
12. Чеботарев А.Н. Некоторые подмножества монадической логики первого порядка (MFO), используемые для спецификации и синтеза Σ-автоматов. *Кибернетика и системный анализ*. 2017. Т. 53, № 4. С. 22–36.
13. Finkel O. Topological properties of omega context free languages. *Theoretical Computer. Science*. 2001. Vol. 262 (1–2). P. 669–697.

Надійшла до редакції 23.03.2017

А.М. Чеботарьов

ПРОБЛЕМИ СИНТЕЗУ Σ-АВТОМАТІВ, СПЕЦИФІКОВАНИХ МОВАМИ LP І LF ЛОГІКИ ПЕРШОГО ПОРЯДКУ

Анотація. Для двох фрагментів, LP і LF, логіки першого порядку з обмеженими кванторами сформульовано і доведено відповідні варіанти теореми про специфікацію, які дають можливість зведення процедури синтезу Σ-автоматів, що специфіковані формулами цих логік, до еквівалентного перетворення формул.

Ключові слова: логіки першого порядку, специфікація, Σ-автомат, LP-формула, LF-формула, автоматна семантика, теорема про специфікацію.

A.N. Chebotarev

PROBLEMS OF SYNTHESIS OF Σ-AUTOMATA SPECIFIED IN LANGUAGES LP AND LF OF FIRST ORDER LOGIC

Abstract. For two fragments LP and LF of monadic first-order logic with bounded quantifiers, the corresponding versions of specification theorem are formulated and proved, which enables the Σ-automata synthesis procedure to be reduced to the equivalent transformation of formulas.

Keywords: first order logics, specification, Σ-automaton, LP-formula, LF-formula, automatic semantics, specification theorem.

Чеботарев Анатолий Николаевич,
доктор техн. наук, ведущий научный сотрудник Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: ancheb@gmail.com.