

**РЕГУЛЯРНАЯ ФОРМА СПЕЦИФИКАЦИИ
ДЕТЕРМИНИРОВАННЫХ АВТОМАТОВ В ЯЗЫКЕ L**

А. Н. Чеботарев

*Институт кибернетики НАН Украины, г. Киев, Украина***E-mail:** ancheb@gmail.com

Исследуются некоторые формы представления спецификаций детерминированных циклических автоматов в языке L. Использование таких форм при построении спецификации уменьшает возможность допущения ошибок.

Ключевые слова: язык спецификации, конечный автомат, циклический автомат, сверхслово.

Введение

Формальная спецификация автомата — это совокупность утверждений, которые определяют требования к его функционированию, т. е. его темпоральные свойства. Эти утверждения формулируются в виде формул формального языка, для чего обычно используются логические языки, такие, как темпоральные логики, исчисление предикатов первого порядка и др. В работе в качестве такого языка рассматривается простой логический язык L, являющийся подмножеством языка одноместных предикатов первого порядка. Процесс построения формальной спецификации автомата начинается с осмысления всех требований к его функционированию с последующим формулированием их в виде формул языка L. Для спецификаций, рассчитанных на синтез, т. е. на использование автоматической процедуры преобразования спецификации в процедурное представление алгоритма функционирования автомата, необходимо обеспечить их полноту, состоящую в том, что должны быть приведены все ограничения на функционирование автомата. Поскольку построение спецификации — это неформальный процесс, осуществляемый человеком, построенная спецификация может содержать ошибки, устранение которых после синтеза и на последующих этапах превращается в очень сложную задачу. Поэтому необходимо так организовать процесс построения спецификации, чтобы уменьшить вероятность допущения в ней ошибки. Этого можно достичь двумя путями: 1) придерживаться строгих правил написания спецификации в четко определенной форме; 2) использовать средства формальной верификации, т. е. проверки наличия важных свойств спецификации. Обычно используется как первый, так и второй пути уменьшения количества ошибок. Настоящая работа посвящена исследованию некоторых форм представления спецификаций детерминированных автоматов и определению их свойств, которые можно просто проверять в процессе построения спецификации. Написание спецификации в рассматриваемых формах существенно уменьшает вероятность допущения ошибок, а также возможность того, что некоторые ограничения на функционирование автомата не будут учтены.

1. Язык спецификации

Язык L [1] представляет собой фрагмент логики предикатов первого порядка с одноместными предикатами и фиксированной областью интерпретации, в качестве которой выступает множество $\mathbb{Z}$ целых чисел (моментов времени). Спецификация в языке L имеет вид формулы $\forall t F(t)$, где $F(t)$ — формула с одной переменной t , построенная

с помощью логических связок из атомарных формул (атомов) вида $p(t + j)$, где p — одноместный предикатный символ, t — переменная, принимающая значения из множества $\mathbb{Z}$, а j — целочисленная константа, называемая *рангом атома*. Разность между максимальным и минимальным рангами атомов в формуле $F(t)$ называется её *глубиной*. Поскольку $F(t)$ интерпретируется на множестве целых чисел, то для произвольного целого j имеет место эквивалентность $\forall t F(t) \Leftrightarrow \forall t F(t + j)$, где $F(t + j)$ обозначает формулу, полученную из $F(t)$ путем увеличения на j рангов всех ее атомов. Таким образом, можно ограничиться рассмотрением только таких формул $F(t)$, у которых максимальный ранг атомов равен нулю.

При определении семантики языка L он рассматривается как формализм для задания множеств сверхслов в алфавите двоичных векторов, длина которых равна количеству предикатных символов в формуле.

Пусть Σ — конечный алфавит и $\mathbb{N}^+ = \{z \in \mathbb{Z} : z > 0\}$. Отображения $u: \mathbb{Z} \rightarrow \Sigma$ и $l: \mathbb{N}^+ \rightarrow \Sigma$ называются соответственно *двусторонним сверхсловом* (обозначается $\dots u(-2)u(-1)u(0)u(1)u(2)\dots$) и *сверхсловом* (обозначается $l(1)l(2)\dots$) в алфавите Σ . Для двустороннего сверхслова u и $n \in \mathbb{Z}$ определим *n-суффикс* $u(n + 1, \infty)$ как сверхслово $u(n + 1)u(n + 2)\dots$.

Пусть $\Omega = \{p_1, p_2, \dots, p_k\}$ — множество всех предикатных символов, которые встречаются в формуле $F(t)$ (сигнатура формулы). Областью интерпретации языка L является множество $\mathbb{Z}$, и в формулах не интерпретированы только предикатные символы. Таким образом, интерпретация формулы $\forall t F(t)$ — это набор $\langle \pi_1, \pi_2, \dots, \pi_k \rangle$ определённых на $\mathbb{Z}$ одноместных предикатов, соответствующих всем предикатным символам из множества Ω . Каждый такой предикат π_i можно рассматривать как двустороннее сверхслово в алфавите $\{0, 1\}$, а набор k таких предикатов — как двустороннее сверхслово в алфавите $\Sigma = \{0, 1\}^k$. Мы не будем различать интерпретации и соответствующие двусторонние сверхслова в алфавите Σ , поэтому будем говорить об истинности или ложности формулы $F(t)$ в позиции τ ($\tau \in \mathbb{Z}$) двустороннего сверхслова u , имея в виду значения формулы $F(\tau)$ при интерпретации u . Смысл понятия глубины формулы состоит в том, что значение формулы $F(t)$ глубины r в позиции τ интерпретации u определяется отрезком $u(\tau - r, \tau)$ соответствующего двустороннего сверхслова u . Интерпретация, при которой формула $\forall t F(t)$ истинна, называется *моделью* для этой формулы. С каждой формулой $F = \forall t F(t)$ ассоциируется множество $M(F)$ всех моделей для нее. Каждая формула $F = \forall t F(t)$ определяет множество $W(F)$ сверхслов над Σ , а именно множество 0-суффиксов всех двусторонних сверхслов из $M(F)$.

Определим автоматную семантику языка L.

Определение 1. Конечный $(X - Y)$ -автомат A — это четвёрка $\langle X, Y, Q, \chi \rangle$, где X и Y — соответственно входной и выходной алфавиты; Q — конечное множество состояний; $\chi: Q \times X \times Y \rightarrow 2^Q$ — функция переходов. Иногда отношение переходов удобно задавать в виде функции переходов-выходов $\lambda: Q \times X \rightarrow 2^{Q \times Y}$.

Автомат A называется *детерминированным*, если для любых $x \in X$, $q \in Q$ верно $|\lambda(q, x)| \leq 1$; в противном случае он называется *недетерминированным*.

Определение 2. $(X - Y)$ -автомат $A = \langle X, Y, Q, \chi \rangle$ называется *квазидетерминированным*, если для всяких $q \in Q$, $x \in X$ и $y \in Y$ справедливо $|\chi(q, x, y)| \leq 1$.

Квазидетерминированный $(X - Y)$ -автомат удобно рассматривать как детерминированный частичный автомат без выходов $A = \langle \Sigma, Q, \delta \rangle$ с входным алфавитом $\Sigma = X \times Y$, с множеством состояний Q и с функцией переходов δ , являющейся отображением из $Q \times \Sigma$ в Q . Будем называть его Σ -автоматом A .

Определение 3. Σ -автомат $A = \langle \Sigma, Q, \delta \rangle$ называется *циклическим*, если для каждого $q \in Q$ существуют такие $q_1, q_2 \in Q$ и $\sigma_1, \sigma_2 \in \Sigma$, что $q_1 = \delta(q, \sigma_1)$ и $q = \delta(q_2, \sigma_2)$.

Циклический Σ -автомат можно охарактеризовать в терминах допустимых сверхслов.

Определение 4. Сверхслово $l = \sigma_1 \sigma_2 \dots$ *допустимо* в состоянии q Σ -автомата A , если существует такое сверхслово состояний $q_0 q_1 q_2 \dots$, где $q_0 = q$, что для любого $i = 0, 1, 2, \dots$ имеет место $\delta(q_i, \sigma_{i+1}) = q_{i+1}$. Сверхслово l *допустимо для автомата A* , если оно допустимо хотя бы в одном из его состояний.

Обозначим $W(A)$ множество всех сверхслов, допустимых для автомата A . Формула F *специфицирует* автомат A , если $W(A) = W(F)$. Как показано в [2], класс автоматов, специфицируемых формулами языка L , совпадает с классом циклических автоматов с конечной памятью [3]. Рассмотрим способ построения автомата $A(F)$, специфицируемого формулой $F = \forall t F(t)$ [4].

Пусть $\Omega = \{p_1, p_2, \dots, p_k\}$ — сигнатура формулы $F(t)$, r — её глубина и $S_\Omega = \{0, 1\}^k$. Последовательность $s_0 s_1 \dots s_r$ векторов $s_0, s_1, \dots, s_r$ из S_Ω назовем *состоянием* глубины r , а множество $Q(r, \Omega)$ всех таких последовательностей — *пространством состояний* глубины r для формулы $F(t)$. Формулу $F(t)$ будем рассматривать как пропозициональную формулу от переменных $p_1(t), \dots, p_k(t), p_1(t-1), \dots, p_k(t-1), \dots, p_1(t-r), \dots, p_k(t-r)$. Если компоненты вектора s_i в состоянии $q = s_0 s_1 \dots s_r$ рассматривать как истинностные значения соответствующих атомов ранга $i - r$ при определенном упорядочении множества Ω , то можно говорить о значении формулы $F(t)$ на состоянии q .

На множестве $Q(r, \Omega)$ определим отношение N *непосредственного следования* так, что за каждым состоянием $q = s_0 s_1 \dots s_r$ непосредственно следуют 2^k состояний вида $s_1 \dots s_r s$, где $s \in S_\Omega$. Множество всех состояний, которые непосредственно следуют за q , будем обозначать $N(q)$.

При использовании языка L для спецификации автоматов предикатные символы ставятся в соответствие входным и выходным двоичным каналам специфицируемого автомата. Поэтому множество предикатных символов Ω разбивается на два класса: входные и выходные, которые обозначаются соответственно U и W . Определим входной алфавит X и выходной алфавит Y автомата $A(F)$ как множества всех двоичных векторов соответственно длины $|U|$ и $|W|$. Каждый вектор из S_Ω можно рассматривать как пару $\langle x, y \rangle$, где $x \in X$, $y \in Y$, поэтому наряду с обозначением $s_0 \dots s_r$ для состояния глубины r будем использовать обозначение $\langle x_0, y_0 \rangle \dots \langle x_r, y_r \rangle$.

Построим вспомогательный автомат $A'(F) = \langle X, Y, Q', \chi_{A'} \rangle$. Множество состояний Q' — это все те состояния из $Q(r, \Omega)$, на которых $F(t)$ истинна. Функцию переходов этого автомата определим следующим образом. Пусть $q \in Q'$, $x \in X$ и $y \in Y$, тогда $\chi_{A'}(q, x, y)$ — это множество всех тех состояний $\langle x_0, y_0 \rangle \dots \langle x_r, y_r \rangle$ из $N(q) \cap Q'$, у которых $x_r = x$ и $y_r = y$. Если таких состояний нет, то значение $\chi_{A'}(q, x, y)$ не определено. Автомат $A(F)$ — это максимальный циклический подавтомат автомата $A'(F)$.

2. Свойства спецификаций детерминированных автоматов

Рассмотрим представление формулы $F(t)$ в пространстве состояний соответствующей глубины. Будем говорить, что формула $F(t)$ истинна на области пространства состояний, если она истинна хотя бы на одном состоянии этой области, и формула ложна на области, если она ложна на всех ее состояниях. Если q — состояние пространства состояний, то $N(q)$ называется *областью переходов* для состояния q . Часть области переходов, соответствующая символу x входного алфавита X , т. е. все такие состояния

$(\langle x_0, y_0 \rangle \dots \langle x_r, y_r \rangle)$ из $N(q)$, у которых $x_r = x$, называется *областью перехода* под действием символа x .

Пусть $F(t)$ — формула глубины r с сигнатурой $\Omega = \{x_1, \dots, x_n, y_1, \dots, y_m\}$, где $x_1, \dots, x_n$ — входные переменные, а $y_1, \dots, y_m$ — выходные. Область перехода в пространстве состояний $Q(r, \Omega)$ задается формулой, представляющей собой конституенту единицы от переменных $x_1(t), \dots, x_n(t), x_1(t-1), \dots, x_n(t-1), y_1(t-1), \dots, y_m(t-1), \dots, x_1(t-r), \dots, x_n(t-r), y_1(t-r), \dots, y_m(t-r)$. Заметим, что формула ложна на области переходов, задаваемой конституентой единицы l , тогда и только тогда, когда в её разложении по указанным переменным остаточная функция, соответствующая l , равна нулю.

Свойства спецификаций, соответствующие детерминированности и всюду определённости автомата, определяются свойствами областей перехода минимальной формы представления спецификации [5]. Минимальная форма спецификации $F = \forall t F(t)$ — это такая эквивалентная спецификация $\forall t \min(F(t))$ автомата $A(F)$, что множество состояний пространства $Q(r, \Omega)$, на которых истинна формула $\min(F(t))$, совпадает с множеством состояний циклического автомата $A(F)$ в этом пространстве. В [5] показано, как по формуле $F(t)$ построить формулу $\min(F(t))$.

Утверждение 1. Формула $\forall t F(t)$ специфицирует детерминированный автомат тогда и только тогда, когда в каждой области перехода пространства состояний формула $\min(F(t))$ истинна не более чем на одном состоянии.

Утверждение 2. Формула $\forall t F(t)$ специфицирует всюду определённый автомат тогда и только тогда, когда для каждой области переходов пространства состояний, на которой истинна $\min(F(t))$, она истинна на всех входящих в нее областях перехода.

В терминах свойств булевых функций, задаваемых формулами $F(t)$ и $\min(F(t))$, эти утверждения можно переформулировать следующим образом.

Утверждение 3. Формула $\forall t F(t)$ специфицирует детерминированный автомат тогда и только тогда, когда каждая остаточная функция в разложении функции $\min(F(t))$ по переменным $x_1(t), \dots, x_n(t), x_1(t-1), \dots, x_n(t-1), y_1(t-1), \dots, y_m(t-1), \dots, x_1(t-r), \dots, x_n(t-r), y_1(t-r), \dots, y_m(t-r)$ либо равна нулю, либо представляет собой конституенту единицы от переменных $y_1(t), \dots, y_m(t)$.

Очевидно, что такое разложение представляет собой совершенную ДНФ.

Утверждение 4. Формула $\forall t F(t)$ специфицирует всюду определённый автомат, если и только если из того, что остаточная функция $f_i(t)$ в разложении $\min(F(t))$ по переменным $x_1(t-1), \dots, x_n(t-1), y_1(t-1), \dots, y_m(t-1), \dots, x_1(t-r), \dots, x_n(t-r), y_1(t-r), \dots, y_m(t-r)$ не равна нулю, следует, что все остаточные функции в разложении $f_i(t)$ по переменным $x_1(t), \dots, x_n(t)$ также не равны нулю.

Пусть $F(x_1, \dots, x_n, y)$ — булева функция от переменных $x_1, \dots, x_n, y$. $\exists$ -проекцией функции $F(x_1, \dots, x_n, y)$ на $\{x_1, \dots, x_n\}$ называется функция $\exists y F(x_1, \dots, x_n, y)$, которая задается формулой $F(x_1, \dots, x_n, 0) \vee F(x_1, \dots, x_n, 1)$. Аналогично, $\exists$ -проекцией функции $F(x_1, \dots, x_n, y_1, \dots, y_m)$ на множество переменных $\{x_1, \dots, x_n\}$ называется функция $\exists y_1 \dots \exists y_m F(x_1, \dots, x_n, y_1, \dots, y_m)$.

Теорема 1. Функция $F(x_1, \dots, x_n, y_1, \dots, y_m)$ может быть представлена в виде

$$F = \bigwedge_{i=1}^m (y_i \leftrightarrow f_i(x_1, \dots, x_n))$$

тогда и только тогда, когда каждая остаточная функция в разложении функции F по переменным $x_1, \dots, x_n$ является конституентой единицы от переменных $y_1, \dots, y_m$.

Доказательство. Необходимость. Пусть $F(x_1, \dots, x_n, y_1, \dots, y_m)$ имеет вид $(y_1 \leftrightarrow f_1) \& \dots \& (y_m \leftrightarrow f_m) = (y_1 f_1 \vee \neg y_1 \neg f_1) \& \dots \& (y_m f_m \vee \neg y_m \neg f_m) = y_1 \dots y_m f_1 \dots f_m \vee \neg y_1 \dots \neg y_m f_1 \dots \neg f_m \vee \dots \vee \neg y_1 \dots \neg y_m \neg f_1 \dots \neg f_m$, где $f_1, \dots, f_m$ — функции от переменных $x_1, \dots, x_n$. На каждом наборе значений переменных $x_1, \dots, x_n$ истинно только одно из 2^m произведений вида $\tilde{f}_1 \dots \tilde{f}_m$, где $\tilde{f}_i \in \{f_i, \neg f_i\}$. Отсюда следует, что каждая остаточная функция в разложении $F(x_1, \dots, x_n, y_1, \dots, y_m)$ по переменным $x_1, \dots, x_n$ является конституентой единицы от переменных $y_1, \dots, y_m$.

Достаточность. Пусть $F(x_1, \dots, x_n, y_1, \dots, y_m)$ удовлетворяет условиям теоремы. Эти условия можно переформулировать в виде следующих свойств функции F .

1. Совершенная ДНФ функции $F(x_1, \dots, x_n, y_1, \dots, y_m)$ содержит ровно 2^n конституент единицы.

2. Каждая конституента единицы от переменных $x_1, \dots, x_n$ является составной частью одной и только одной из конституент единицы функции $F(x_1, \dots, x_n, y_1, \dots, y_m)$.

Этим же свойствами обладает и каждая $\exists$ -проекция функции $F(x_1, \dots, x_n, y_1, \dots, y_m)$ на множество переменных $\{x_1, \dots, x_n, y_i\}$ ($i = 1, 2, \dots, m$). Отсюда следует, что каждая проекция функции $F(x_1, \dots, x_n, y_1, \dots, y_m)$ на $\{x_1, \dots, x_n, y_i\}$ имеет вид $f_i(x_1, \dots, x_n) y_i \vee \neg f_i(x_1, \dots, x_n) \neg y_i = y_i \leftrightarrow f_i(x_1, \dots, x_n)$. Поскольку рассматриваемые проекции обладают указанными свойствами, то и произведение всех этих проекций также обладает ими. Кроме того, $F(x_1, \dots, x_n, y_1, \dots, y_m)$ является импликантой каждой такой проекции, а следовательно, и импликантой их произведения.

Лемма 1. Если $f(x_1, \dots, x_n)$ — импликанта функции $f'(x_1, \dots, x_n)$ и совершенные ДНФ этих функций имеют одинаковое количество конституент единицы, то $f(x_1, \dots, x_n) = f'(x_1, \dots, x_n)$.

Из этой леммы следует, что произведение всех m проекций функции $F(x_1, \dots, x_n, y_1, \dots, y_m)$ совпадает с этой функцией, что завершает вторую часть доказательства. ■

Теорема 2. Любой всюду определённый, детерминированный автомат с конечной памятью может быть специфицирован в виде

$$\forall t \bigwedge_{i=1}^m (y_i(t) \leftrightarrow f_i(t)),$$

где $y_1, \dots, y_m$ — все выходные предикатные символы спецификации и $f_i(t)$ не зависит от атомов $y_1(t), \dots, y_m(t)$.

Доказательство. Пусть $F(t)$ в спецификации $\forall t F(t)$ такова, что все остаточные функции в её разложении по переменным $x_1(t), \dots, x_n(t), x_1(t-1), \dots, x_n(t-1), y_1(t-1), \dots, y_m(t-1), \dots, x_1(t-r), \dots, x_n(t-r), y_1(t-r), \dots, y_m(t-r)$ равны конституентам единицы от переменных $y_1(t), \dots, y_m(t)$. В силу теоремы 1 она может быть представлена в виде $\bigwedge_{i=1}^m (y_i(t) \leftrightarrow f_i(t))$, где формулы $f_i(t)$ не зависят от атомов $y_1(t), \dots, y_m(t)$.

Таким образом, для доказательства теоремы 2 достаточно показать, что минимальная форма спецификации детерминированного, всюду определённого автомата может быть эквивалентно преобразована в формулу, удовлетворяющую указанному выше условию. Такое преобразование состоит в том, чтобы формулу $\min(F(t))$ сделать истинной на тех областях переходов, на которых она ложна, и таким образом, чтобы в каждой области перехода она была истинна не более чем на одном состоянии. Это осуществляется путем замены в разложении функции $\min(F(t))$ по переменным $x_1(t), \dots, x_n(t), x_1(t-1), \dots, x_n(t-1), y_1(t-1), \dots, y_m(t-1), \dots, x_1(t-r), \dots, x_n(t-r), y_1(t-r), \dots, y_m(t-r)$

$\dots, y_m(t-r)$ всех нулевых остаточных функций ненулевыми. Эквивалентность этого преобразования можно обеспечить, если для замены использовать имеющиеся в этом разложении ненулевые остаточные функции. ■

Такая спецификация — это совокупность утверждений, определяющих необходимые и достаточные условия истинности каждого выходного предиката в произвольный момент времени t , причем эти условия не зависят от значений выходных предикатов в этот момент времени.

Теорема 3. Любой детерминированный автомат с конечной памятью может быть специфицирован в виде

$$\forall t \bigwedge_{i=1}^m (y_i(t) \rightarrow g_i(t)) \& (\neg y_i(t) \rightarrow h_i(t)),$$

где $y_1, \dots, y_m$ — все выходные предикатные символы спецификации; $g_i(t), h_i(t)$ не зависят от атомов $y_1(t), \dots, y_m(t)$.

Доказательство. Пусть автомат задан формулой $\forall t F(t)$ с выходными предикатными символами $y_1, \dots, y_m$. Согласно утверждению 3, каждая остаточная функция в разложении функции $\min(F(t))$ по всем переменным, отличным от $y_1(t), \dots, y_m(t)$, либо равна нулю, либо представляет собой конститuentу единицы от переменных $y_1(t), \dots, y_m(t)$. Рассмотрим m $\exists$ -проекций функции $\min(F(t))$ на все атомы, кроме выходных атомов нулевого ранга, отличных от $y_i(t)$ ($i = 1, 2, \dots, m$). Аналогично тому, как это сделано в доказательстве теоремы 1, можно показать, что произведение всех этих проекций совпадает с функцией $\min(F(t))$. Каждая такая проекция может быть представлена в виде $y_i(t)g_i(t) \vee \neg y_i(t)h_i(t)$, что эквивалентно $(y_i(t) \rightarrow g_i(t)) \& (\neg y_i(t) \rightarrow h_i(t))$, где $g_i(t), h_i(t)$ не зависят от атомов $y_1(t), \dots, y_m(t)$. Так как формулы $\forall t \min(F(t))$ и $\forall t F(t)$ специфицируют один и тот же автомат, то теорема доказана. ■

Несложно показать, что $g_i(t) \& h_i(t) \equiv 0$ ($i = 1, 2, \dots, m$).

3. Необходимые и достаточные условия

Возникает вопрос, как построить формулы $g_i(t)$ и $h_i(t)$ в спецификации детерминированного автомата? Для ответа на него проанализируем понятия необходимого и достаточного условий.

Если $\forall t (a(t) \rightarrow b(t))$, то будем говорить, что $b(t)$ — необходимое условие истинности $a(t)$, а $a(t)$ — достаточное условие истинности $b(t)$. Таким образом, формулы $g_i(t)$ и $h_i(t)$ в спецификации детерминированного автомата — это необходимые условия соответственно истинности и ложности предиката $y_i(t)$ в момент t . Очевидно, что если $A(t)$ и $B(t)$ — необходимые условия истинности предиката $y(t)$, то $A(t) \& B(t)$ — также необходимое условие. Аналогично, если $A(t)$ и $B(t)$ — достаточные условия, то $A(t) \vee B(t)$ — также достаточное условие. В силу эквивалентности формул $y(t) \rightarrow A(t)$ и $\neg A(t) \rightarrow \neg y(t)$ отрицание необходимого условия истинности предиката $y(t)$ в момент t является достаточным условием ложности этого предиката. Поэтому возможны различные эквивалентные формы представления спецификации автомата с использованием необходимых или достаточных условий истинности (ложности) выходных предикатов. Однако если в формулах использовать произвольные необходимые или достаточные условия, то полученная таким образом спецификация может не специфицировать требуемый автомат. Поэтому следует уточнить вид этих условий.

Пусть $A_1, A_2, \dots, A_n$ — все возможные неэквивалентные формулы определённой глубины, которые задают необходимые условия истинности некоторого предиката,

тогда формулу $A_1 \& A_2 \& \dots \& A_n$ будем называть соответствующим *полным необходимым условием*. Аналогично, если формулы $A_1, A_2, \dots, A_n$ задают достаточные условия, то формулу $A_1 \vee A_2 \vee \dots \vee A_n$ будем называть *полным достаточным условием*. Заметим, что полные необходимые и полные достаточные условия представляют собой необходимые и достаточные условия. Использование в спецификации вида $\forall t \bigwedge_{i=1}^m (y_i(t) \rightarrow g_i(t)) \& (\neg y_i(t) \rightarrow h_i(t))$ в качестве $g_i(t)$ и $h_i(t)$ соответствующих необходимых и достаточных условий гарантирует правильность спецификации.

Рассмотрим пример построения спецификации автомата с одной входной двоичной переменной x и одной выходной двоичной переменной y . Требования к функционированию автомата описаны следующим образом. Значение y в момент t равняется единице тогда и только тогда, когда во входной последовательности до момента t включительно отсутствуют нулевые значения переменной x . Как можно видеть из этого описания, поведение автомата детерминировано и всюду определено. Необходимое и достаточное условие истинности $y(t)$ имеет вид $y(t-1) \& x(t)$. Таким образом, спецификация этого автомата может быть записана в виде $\forall t (y(t) \leftrightarrow y(t-1) \& x(t))$.

Еще один пример автомата с такими же входным и выходным алфавитами. Автомат функционирует следующим образом. Если x в момент t равен единице, то y также в этот момент равен единице. Если x изменился в нуль, то со следующего момента после этого изменения y также будет равен нулю (если x в этот момент равен нулю) до того момента, когда x изменится в единицу. Кроме того, в следующий момент времени после того, как x изменится в единицу, он не может равняться нулю. Последнее утверждение определяет частичность автомата. В этом случае автомат удобно специфицировать как всюду определённый, дополнив эту спецификацию условием частичности. Так, спецификацию соответствующего всюду определённого автомата запишем как $\forall t (y(t) \leftrightarrow (x(t-1) \vee x(t)))$. Действительно, всякий раз, когда $y(t)$ равен единице, условие $x(t-1) \vee x(t)$ также равно единице, таким образом, это — необходимое условие. Кроме того, $x(t-1)$ и $x(t)$ — достаточные условия истинности $y(t)$, следовательно, $x(t-1) \vee x(t)$ — необходимое и достаточное условие. Условие частичности имеет вид $\forall t (\neg x(t-2) \& x(t-1) \rightarrow x(t))$.

Более сложный пример спецификации реактивных систем можно найти в [6].

Следует также рассмотреть спецификацию автомата в виде необходимых условий изменения (сохранения) значения выходного сигнала. Так, утверждение, что $A(t)$ — необходимое условие изменения значения y с 0 на 1, имеет вид $\forall t (\neg y(t-1) \& y(t) \rightarrow A(t))$. Несложно показать, что спецификацию детерминированного автомата $\forall t \bigwedge_{i=1}^m (y_i(t) \rightarrow g_i(t)) \& (\neg y_i(t) \rightarrow h_i(t))$ можно представить в виде $\forall t \bigwedge_{i=1}^m F_i(t)$, где $F_i(t)$ — это конъюнкция четырёх утверждений: $(y_i(t-1) \& y_i(t) \rightarrow A_i(t))$, $(y_i(t-1) \& \neg y_i(t) \rightarrow B_i(t))$, $(\neg y_i(t-1) \& y_i(t) \rightarrow C_i(t))$, $(\neg y_i(t-1) \& \neg y_i(t) \rightarrow D_i(t))$. Чтобы перейти от этой формы спецификации к предыдущей, следует положить $g_i(t) = y_i(t-1) \& A_i(t) \vee \neg y_i(t-1) \& C_i(t)$, $h_i(t) = y_i(t-1) \& B_i(t) \vee \neg y_i(t-1) \& D_i(t)$.

Рассмотрим, как для первого примера построить такую спецификацию. Запишем спецификацию этого автомата в виде $\forall t (y(t) \rightarrow y(t-1) \& x(t)) \& (\neg y(t) \rightarrow (\neg y(t-1) \vee \neg x(t)))$. Таким образом, $y(t-1) \& x(t) = y(t-1) \& A(t) \vee \neg y(t-1) \& C(t)$, а $(\neg y(t-1) \vee \neg x(t)) = y(t-1) \& B(t) \vee \neg y(t-1) \& D(t)$. Отсюда находим такие значения для $A(t), B(t), C(t)$ и $D(t)$: $A(t) = x(t)$, $B(t) = \neg x(t)$, $C(t) = 0$, $D(t) = 1$.

Если $g_i(t)$ и $h_i(t)$ — необходимые и достаточные условия истинности $y_i(t)$ и $\neg y_i(t)$ соответственно, то полученные таким образом формулы $y_i(t-1) \& A_i(t)$, $\neg y_i(t-1) \& C_i(t)$,

$y_i(t-1) \& B_i(t)$ и $\neg y_i(t-1) \& D_i(t)$ будут необходимыми и достаточными условиями истинности $y_i(t-1) \& y_i(t)$, $\neg y_i(t-1) \& y_i(t)$, и т. д. Действительно, учитывая, что $y_i(t) \leftrightarrow g_i(t)$, а $\neg y_i(t) \leftrightarrow h_i(t)$, можно записать $y_i(t) \leftrightarrow (y_i(t-1) \& A_i(t) \vee \neg y_i(t-1) \& C_i(t))$, $\neg y_i(t) \leftrightarrow (y_i(t-1) \& B_i(t) \vee \neg y_i(t-1) \& D_i(t))$. Умножив обе части этих эквивалентностей на $y_i(t-1)$ и на $\neg y_i(t-1)$, получим $y_i(t-1) \& y_i(t) \leftrightarrow y_i(t-1) \& A_i(t)$, $\neg y_i(t-1) \& y_i(t) \leftrightarrow \neg y_i(t-1) \& C_i(t)$ и т. п. Поскольку условия $A_i(t)$, $B_i(t)$ и т. д. проще, чем условия $g_i(t)$ и $h_i(t)$, то обычно такая форма спецификации более удобна для её построения.

Часто спецификация пишется при некоторых предположениях, ограничивающих множества допустимых символов входного или выходного алфавитов, например, недопустимость одновременной истинности двух выходных предикатов. В этом случае формулы, характеризующие все такие предположения, должны быть включены в спецификацию.

Заключение

В работе показано, что спецификацию любого детерминированного автомата можно строить в стандартной форме, использующей необходимые и достаточные условия истинности и ложности каждого выходного предиката. Обычно из неформального описания требований к функционированию специфицируемого автомата можно заключить, является ли он детерминированным или вполне определённым. Это позволяет выбрать форму спецификации, удовлетворяющую формальным требованиям. Так, при спецификации детерминированного автомата в виде конъюнкции формул $(y_i(t) \rightarrow A_i(t)) \& (\neg y_i(t) \rightarrow B_i(t))$, ассоциируемых с каждым выходным предикатом y_i , должно выполняться равенство $A_i(t) \& B_i(t) = 0$. Причем в формулах $A_i(t)$ и $B_i(t)$ не должны встречаться выходные атомы нулевого ранга. Равенство $A_i(t) \vee B_i(t) = 1$ свидетельствует о полной определённости специфицируемого автомата. Заметим, что невыполнение этого равенства не всегда говорит о частичности автомата. Как показано во втором примере, спецификацию частичного автомата удобно записывать в виде конъюнкции $F_1 \& F_2$, где F_1 — спецификация всюду определённого автомата, а F_2 — спецификация условия частичности. Условия частичности — это требования к функционированию среды, с которой взаимодействует автомат. Если среду рассматривать как детерминированный автомат, то условия частичности можно записать в виде $\forall t \bigwedge_{i=1}^m (x_i(t) \rightarrow \alpha_i(t)) \& (\neg x_i(t) \rightarrow \beta_i(t))$, где x_i — входные предикатные символы, а формулы $\alpha_i(t)$ и $\beta_i(t)$ не зависят от атомов нулевого ранга.

Использование стандартной формы представления спецификации, удовлетворяющей определённым, легко проверяемым требованиям, облегчает её написание и уменьшает возможность допущения ошибок. Разделение спецификации автомата на две части, соответствующие собственно автомату и среде, с которой он взаимодействует, также упрощает процесс написания спецификации, а впоследствии и оптимизацию автомата, синтезированного по спецификации.

ЛИТЕРАТУРА

1. Чеботарев А. Н. Об одном подходе к функциональной спецификации автоматных систем. I // Кибернетика и системный анализ. 1993. № 3. С. 31–42.
2. Чеботарев А. Н. Синтез недетерминированного автомата по его логической спецификации. I // Кибернетика и системный анализ. 1995. № 6. С. 115–127.
3. Гилл А. Введение в теорию конечных автоматов. М.: Наука, 1966. 227 с.

4. Чеботарев А. Н. Синтез алгоритма по его логической спецификации // Управляющие системы и машины. 2004. № 5. С. 53–60.
5. Чеботарев А. Н., Куривчак О. И. Аппроксимация множеств сверхслов формулами языка L // Кибернетика и системный анализ. 2007. № 6. С. 18–26.
6. Чеботарев А. Н., Алистратов А. В. Построение логической спецификации реактивного алгоритма // Проблемы программирования. 2002. № 1–2. С. 154–160.