УДК 519.713.1

А.Н. ЧЕБОТАРЕВ

СОГЛАСОВАНИЕ ВЗАИМОДЕЙСТВУЮЩИХ АВТОМАТОВ

Аннотация. Проблема согласования автоматов состоит в том, чтобы спроектировать систему, поведение которой при ее взаимодействии со средой будет удовлетворять заданным требованиям независимо от возможного поведения среды. Приведен ряд теоретических результатов, используемых при решении проблемы согласования, и основанные на них алгоритмы ее решения.

Ключевые слова: взаимодействие автоматов, композиции автоматов, сдвиг автомата по входу, согласование автоматов, корректность композиции.

ВВЕДЕНИЕ

Задачи согласования автоматов возникают при использовании теоретико-автоматного подхода к проектированию реактивных алгоритмов, т.е. алгоритмов взаимодействия проектируемой системы со средой, в которой она функционирует. Среда, как правило, недетерминированна и в силу этого может различным образом реагировать на действия проектируемой системы. Задача состоит в том, чтобы спроектировать алгоритм функционирования такой системы, поведение которой при ее взаимодействии со средой будет удовлетворять заданным требованиям независимо от возможного поведения среды. Требования к совместному поведению системы и среды, с которой она взаимодействует, обычно формулируются в каком-либо логическом языке, таком как различного рода темпоральные логики, логики первого порядка или ограниченные логики второго порядка. 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 проблема выяснения возможности реализации (реализуемости) требований к поведению реактивной системы в виде поведения соответствующей автоматной модели. Очевидно, что требования, в явной или неявной форме ограничивающие поведение среды, не могут быть реализованы, поскольку предполагается, что никакие дополнительные ограничения на поведение среды, кроме тех, что определяются ее спецификацией, не должны налагаться.

Эта проблема была сформулирована А. Черчем [1] в виде следующей проблемы разрешимости. Пусть X и Y — конечные алфавиты, а $R \subseteq X^{\omega} \times Y^{\omega}$ — регулярное отношение, т.е. отношение, которое может быть задано каким-либо автоматом-распознавателем над бесконечными словами в алфавите $X \times Y$. Проблема разрешимости формулируется следующим образом: существует ли такая функция $f: X^{\omega} \to Y^{\omega}$, что для всех $w \in X^{\omega}$ имеет место $R(w, f(w))$? Различные ограничения и уточнения этой проблемы связаны со способом задания отношения R, например формулой логики LTL или CTL*, и ограничениями, налагаемыми на функцию f, также связанными со способом ее задания, скажем, в виде X / Y-трансдьюсера. Такие модификации проблемы разрешимости Черча обычно называются проблемами реализуемости.

Применительно к проектированию реактивных систем задание отношения R рассматривается как спецификация проектируемой системы, а функция f реализуется трансдьюсером [2]. В простейшем случае, когда информация о поведении среды отсутствует, а спецификация системы задана в виде неинициализированного трансдьюсера A или любой другой эквивалентной модели конечного автомата, она реализуема, если автомат A содержит циклический вполне определенный подавтомат. Заметим, что множество состояний такого подавтомата замкнуто относительно функции переходов. Ситуация усложняется при наличии информации о среде, которая задается аналогичным образом. В этом случае спецификация системы реализуема, даже если соответствующий ей автомат не имеет циклического вполне определенного подавтомата, однако имеет циклический подавтомат, частичность которого согласована со средой, т.е. не налагает дополнительных ограничений на ее поведение. Отсюда возникает проблема согласования спецификации системы со спецификацией среды. 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) [3]. Ограничение свойств, определяемых спецификацией, свойствами, представимыми трансдьюсером, позволяет решать задачу согласования как на уровне спецификаций, так и на уровне синтезированных автоматов.

Впервые проблема согласования автоматов была сформулирована в 1991 г. в [4], где было определено понятие согласованности двух частичных недетерминированных автоматов Мура и предложены алгоритмы согласования автоматов с конечной памятью. Понятие согласованности недетерминированных автоматов определялось неконструктивно через понятие согласованности детерминированных автоматов и бесконечные множества детерминизаций недетерминированных автоматов. Для конструктивного решения задачи согласования пришлось ограничиться автоматами с конечной памятью. В [5] соответствующие задачи рассматривались на уровне логических спецификаций автоматов. Приведены алгоритмы согласования спецификаций в языке L, гарантирующие, что автоматы, синтезированные по согласованным спецификациям, будут согласованы.

В настоящей работе дается более общее конструктивное определение понятия согласованности автоматов, не ограничивающееся автоматами с конечной памятью. Приводится ряд теоретических результатов, используемых при решении задачи согласования, а также описывается подход, основанный на понятии корректности параллельной композиции Σ-автоматов.

Работа состоит из двух частей. Первая, представленная настоящей статьей, посвящена решению проблемы согласования автоматов, вторая — проблеме согласования спецификаций автоматов в языке L.

МОДЕЛИ АВТОМАТОВ И ИХ КОМПОЗИЦИИ

Рассматриваются частичные недетерминированные X/Y-автоматы Мура. Такой автомат A определяется пятеркой $\langle X, Y, Q, \chi_A, \mu_A \rangle$, где X, Y, Q — конечные множества соответственно входных символов, выходных символов и состояний, а $\chi_A : Q \times X \to 2^Q$ и $\mu_A : Q \to Y$ — всюду определенные функции переходов и выходов. Если $|X| = 1$, то автомат A называется автономным Y-автоматом, который определяется четверкой $\langle Y, Q, \chi_A, \mu_A \rangle$. Функция переходов такого автомата имеет вид $\chi_A : Q \to 2^Q$.

Недетерминированный X/Y-автомат A будем называть квазидетерминированным, если для любых $q, q_1, q_2 \in Q$ и $x \in X$ из $q_1, q_2 \in \chi_A(q, x)$ следует $\mu_A(q_1) \neq \mu_A(q_2)$. Аналогично недетерминированный автономный Y-автомат $A = \langle Y, Q, \chi_A, \mu_A \rangle$ называется квазидетерминированным, если для каждого $q \in Q$ и любых $q_1, q_2 \in \chi_A(q)$ выполняется $\mu_A(q_1) \neq \mu_A(q_2)$.

Квазидетерминированный X/Y-автомат иногда удобно представлять в виде детерминированного автомата без выходов с тем же множеством состояний и с входным алфавитом $\Sigma_A = X \times Y$. Такой автомат $A = \langle \Sigma_A, Q_A, \delta_A \rangle$, где Σ_A — входной алфавит, Q_A — множество состояний, а $\delta_A : Q_A \times \Sigma_A \to Q_A$ — частичная функция переходов, назовем Σ-автоматом (заметим, что в понятии «Σ-автомат» символ Σ обозначает тип автомата, а не название алфавита, как это имеет место для автономного Y-автомата). В дальнейшем символы алфавита $\Sigma = X \times Y$ будем записывать в виде *xy*, где $x \in X$, $y \in Y$. Функция переходов Σ-автомата, соответствующего квазидетерминированному X/Y-автомату Мура A, определяется следующим образом: $\delta_A(q, xy) = q_1$ тогда и только тогда, когда для X/Y-автомата A $q_1 \in \chi_A(q, x)$ и $\mu_A(q_1) = y$. Утверждение вида $\delta_A(q, xy) = q_1$ будем называть переходом и записывать в виде $q{:}xy \to q_1$. Символ входного алфавита xy в такой записи называется отметкой перехода.

В дальнейшем ограничимся рассмотрением квазидетерминированных автоматов.

Σ-автомат $A = \langle \Sigma_A, Q_A, \delta_A \rangle$ называется циклическим, если для каждого $q \in Q_A$ существуют такие $\sigma_1, \sigma_2 \in \Sigma_A$ и $q_1, q_2 \in Q_A$, что $q_1 = \delta_A(q, \sigma_1)$ и $q = \delta_A(q_2, \sigma_2)$. Автомат, удовлетворяющий только первому из указанных требований, назовем квазициклическим. Очевидно, что автоматная модель реактивной системы должна быть по крайней мере квазициклическим автоматом. Любой инициальный квазициклический автомат, т.е. автомат с выделенными начальными состояниями, может быть задан в виде пары $\langle A, Q_0 \rangle$, где A — циклический автомат, а Q_0 — множество начальных состояний. Максимальный циклический подавтомат автомата назовем его ядром.

Поведение циклического автомата характеризуется множеством допустимых для него сверхслов (бесконечных слов).

Сверхслово $l = \sigma_1 \sigma_2 \sigma_3 \ldots$ в алфавите Σ_A 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 $i = 0, 1, 2, \ldots$ $q_{i+1} = \delta_A(q_i, \sigma_{i+1})$. Будем говорить, что сверхслово состояний $q_0 q_1 q_2 \ldots$ соответствует входному сверхслову l.

Сверхслово $l = \sigma_0 \sigma_1 \sigma_2 \ldots$ в алфавите Y допустимо в состоянии q автономного Y-автомата A, если существует такое сверхслово состояний $q_0 q_1 q_2 \ldots$, где $q_0 = q$, что для любого $i = 0, 1, 2, \ldots$ $q_{i+1} \in \delta_A(q_i)$ и $\mu_A(q_{i+1}) = \sigma_i$.

Эти определения легко переформулировать для X/Y-автоматов.

Множество всех сверхслов, допустимых в состоянии q, обозначается $W(q)$. Состояния q_1 и q_2 одного и того же или различных автоматов называются эквивалентными, если $W(q_1) = W(q_2)$.

Сверхслово l допустимо для автомата A, если оно допустимо хотя бы в одном из его состояний. Множество всех сверхслов, допустимых для автомата A, обозначается $W(A)$.

Автоматы A и B называются строго эквивалентными (обозначается $A \sim B$), если для каждого состояния автомата A имеется эквивалентное ему состояние автомата B и наоборот.

Пусть $q(t)$ обозначает состояние автомата A в момент дискретного времени t, а $s(t)$ — состояние автомата B в этот же момент. Рассматриваемый способ взаимодействия недетерминированных автоматов Мура $A = \langle X, Y, Q_A, \chi_A, \mu_A \rangle$ и $B = \langle Y, X, Q_B, \chi_B, \mu_B \rangle$ можно описать соотношениями

$$q(t) \in \chi_A(q(t-1), x(t)), \;\; y(t) = \mu_A(q(t)),$$

$$s(t) \in \chi_B(s(t-1), y(t-1)), \;\; x(t) = \mu_B(s(t)).$$

Возможны и другие способы организации взаимодействия автоматов. Выбор той или иной модели взаимодействия определяется способом реализации проектируемого алгоритма. Рассматриваемая здесь модель взаимодействия ориентирована на аппаратурную реализацию, когда взаимодействие осуществляется с помощью передачи сигналов, а не сообщений. Совместное поведение автоматов, взаимодействующих согласно описанному выше способу, характеризуется их правой композицией.

Определение 1. Правая композиция автоматов $A = \langle X, Y, Q_A, \chi_A, \mu_A \rangle$ и $B = \langle Y, X, Q_B, \chi_B, \mu_B \rangle$ (обозначается $A \triangleright B$) представляет собой автономный, недетерминированный Z-автомат Мура $C = \langle Z, Q_C, \chi_C, \mu_C \rangle$, где $Z = Y \times X$, $Q_C = Q_A \times Q_B$, а функция переходов χ_C и функция выходов μ_C определяются следующим образом. Для $q \in Q_A$, $s \in Q_B$ $\chi_C(q, s) = \{(q', s') \mid s' \in \chi_B(s, \mu_A(q)),$ $q' \in \chi_A(q, \mu_B(s'))\}$, $\mu_C(q, s) = (\mu_A(q), \mu_B(s))$.

Это определение не симметрично относительно автоматов A и B. Очевидно, что композиция A и B не совпадает с композицией B и A. Заметим, что правая композиция квазидетерминированных автоматов также является квазидетерминированным автоматом.

Рассматривая автомат C как Σ-автомат, приведенное определение можно переформулировать так: $C = \langle Z, Q_C, \delta_C \rangle$, где $Z = X \times Y$, $Q_C = Q_A \times Q_B$, а функция переходов δ_C определяется следующим образом. Для любых $q \in Q_A$, $s \in Q_B$, $x \in X$, $y \in Y$ $\delta_C((q, s), xy) = (q', s')$ тогда и только тогда, когда в Y / X-автомате B $s' \in \chi_B(s, \mu_A(q))$, $\mu_B(s') = x$ и в X / Y-автомате A $q' \in \chi_A(q, x)$, $\mu_A(q') = y$.

СОГЛАСОВАННОСТЬ АВТОМАТОВ

Неформально X / Y-автомат A согласован с Y / X-автоматом B, если при их взаимодействии не может возникнуть ситуации, когда переход в одном из автоматов под действием сигнала, поступающего из другого автомата, будет не определен. Такое взаимодействие автоматов назовем корректным. Очевидно, что вполне определенный автомат A согласован с любым вполне определенным автоматом B. Кроме того, если правая композиция автоматов A и B не содержит циклического подавтомата, то автомат A не согласован с автоматом B.

Композиция $C = A \triangleright B$ определяет множество $X \times Y$-сверхслов, которые могут быть порождены в процессе взаимодействия автоматов A и B. Однако не все эти сверхслова соответствуют корректному взаимодействию. Состояние (q, s), для которого существует $s' \in \chi_B(s, \mu_A(q))$ такое, что $\chi_A(q, \mu_B(s')) = \varnothing$, назовем критическим. В таком состоянии возможно прекращение совместной работы автоматов A и B. Поэтому поведение автомата A должно быть ограничено так, чтобы его композиция с автоматом B не могла перейти в критическое состояние.

Каждое сверхслово w, допустимое для композиции C (рассматриваемой как Σ-автомат), допустимо для автомата A. $X \times Y$-сверхслово, которому в автомате C соответствует сверхслово состояний, содержащее критическое состояние, также назовем критическим. Задача согласования автомата A с автоматом B заключается в том, чтобы автомат A заменить автоматом A^*, для которого $W(A^*)$ состоит из всех сверхслов из $W(A)$, не являющихся критическими. X / Y-автомат A может быть согласован с Y / X-автоматом B только тогда, когда правая композиция $C = A \triangleright B$ имеет непустой циклический подавтомат C', любое состояние (q, s) которого удовлетворяет следующему условию согласованности: для каждого $s' \in \chi_B(s, \mu_A(q))$ существует такое $q' \in \chi_A(q, \mu_B(s'))$, что (q', s') принадлежит множеству состояний подавтомата C'. Максимальный такой циклический подавтомат композиции C обозначим C^*. Заметим, что если состояние (q, s) принадлежит циклическому подавтомату композиции, то $\chi_B(s, \mu_A(q)) \neq \varnothing$, т.е. переход в автомате B из состояния s под действием сигнала $\mu_A(q)$ определен.

Дадим теперь формальное определение согласованности автомата A с автоматом B.

Обычно представляет интерес инициальное поведение взаимодействующих автоматов, т.е. поведение, определяемое начальными состояниями этих автоматов. Инициальным подавтоматом автомата A, порожденным состоянием q, называется минимальный подавтомат автомата A, содержащий q и все достижимые из него состояния. Инициальный квазициклический подавтомат автомата A, порожденный состоянием q (обозначается $\langle A, q \rangle$), — это максимальный квазициклический подавтомат автомата, порожденного состоянием q.

Определение 2. Инициальный квазициклический X / Y-автомат $\langle A, q_0 \rangle$ согласован с инициальным квазициклическим Y / X-автоматом $\langle B, s_0 \rangle$ тогда и только тогда, когда инициальный квазициклический подавтомат C_0 композиции $A \triangleright B$, порожденный состоянием (q_0, s_0), не пуст и каждое его состояние (q, s) удовлетворяет условию согласованности. В этом случае говорим, что автомат A согласован с автоматом B в состоянии (q_0, s_0) композиции $A \triangleright B$.

Задача согласования X / Y-автомата A с Y / X-автоматом B сводится к нахождению подавтомата C^* композиции $A \triangleright B$. Если такой подавтомат не пуст, то результатом согласования является автомат A^* с состояниями $q_i(s_j)$, соответствующими состояниям (q_i, s_j) подавтомата C^*. Отметка состояния $q_i(s_j)$ равна $\mu_A(q_i)$, а функция переходов определяется следующим образом. Из состояния $q_i(s_j)$ имеется переход в состояние $q_l(s_k)$ под действием $x \in X$ тогда и только тогда, когда из состояния (q_i, s_j) автомата C^* есть переход в состояние (q_l, s_k) и $x = \mu_B(s_k)$. Автомат A^* является ограничением автомата A в том смысле, что, во-первых, не для каждого состояния q автомата A автомат A^* может иметь состояние $q(s)$ и, во-вторых, множество сверхслов, допустимых в состоянии $q(s)$ автомата A^*, содержится в аналогичном множестве для q, т.е. $W(q(s)) \subseteq W(q)$.

Каждое состояние (q, s) подавтомата C^* композиции $C = A^* \triangleright B$ определяет пару взаимодействующих инициальных квазициклических автоматов $\langle A^*, q(s)\rangle$ и $\langle B, s\rangle$ таких, что автомат $\langle A^*, q(s)\rangle$ согласован с автоматом $\langle B, s\rangle$. Таким образом, множество Q_{C^*} состояний автомата C^* — это множество всех тех состояний композиции $A^* \triangleright B$, в которых автомат A^* согласован с автоматом B.

Для описания алгоритма построения автомата C^* в [4] введено понятие закрытого состояния правой композиции. Приведем индуктивное определение этого понятия.

Определение 3. Состояние (q, s) ядра правой композиции автоматов A и B называется закрытым, если существует такое $s' \in \chi_B(s, \mu_A(q))$, что выполняется одно из условий: 1) $\chi_A(q, \mu_B(s')) = \varnothing$; 2) для каждого $q' \in \chi_A(q, \mu_B(s'))$ состояние (q', s') закрыто.

Выделение подавтомата C^* из ядра композиции $A \triangleright B$ состоит в итеративном построении множества всех закрытых состояний этого ядра. Построение начинается с нахождения всех закрытых состояний, удовлетворяющих условию 1. Затем осуществляется расширение этого множества на основании условия 2. Если полученное множество закрытых состояний совпадает с множеством всех состояний ядра композиции, то автомат A нельзя согласовать с B. В противном случае, после удаления из ядра композиции всех закрытых состояний и выделения циклического подавтомата, будет получен автомат C^*, которому ставится в соответствие автомат A^*.

Заметим, что вместо автомата A^* можно использовать любую его минимизированную форму при подходящем доопределении значений функции переходов в частичных состояниях. Для пар начальных состояний, определяемых автоматом C^*, совместное поведение соответствующих инициальных автоматов сохраняется при любом доопределении автомата A^* до вполне определенного. Действительно, при любом доопределении функции переходов в частичном состоянии $q(s)$ автомата A^* множество входных символов, которые могут появиться на входе полученного автомата A_1^*, когда правая композиция $A_1^* \triangleright B$ находится в состоянии $(q(s), s)$, остается таким же, как и в композиции $A^* \triangleright B$. Таким образом, доопределение не влияет на поведение композиции.

Пример 1. Пусть X / Y-автомат Мура A представлен следующим множеством строк:

$$
\begin{aligned}
&(y)\, a : x \to b.\\
&(\bar{y})\, b : x \to b,\\
&\qquad \bar{x} \to a.\\
&(y)\, c : x \to c,\\
&\qquad \bar{x} \to d.\\
&(\bar{y})\, d : x \to b,\\
&\qquad \bar{x} \to \{b, c\}.
\end{aligned}
$$

Здесь $X = \{x, \bar{x}\}$, $Y = \{y, \bar{y}\}$, $Q_A = \{a, b, c, d\}$. Слева от символа состояния в скобках указана его отметка. Описание Y / X-автомата B имеет вид

$$\begin{aligned} (\bar{x})\,1&: y \to \{1, 2\}, \\ &\ \ \bar{y} \to 1. \\ (x)\,2&: y \to 1, \\ &\ \ \bar{y} \to 1. \end{aligned}$$

Согласование автомата A с автоматом B начинается с построения правой композиции $A \rhd B$, в которой выделим максимальный циклический подавтомат. Этот автономный автомат имеет следующий вид:

$$\begin{aligned} &(y\bar{x})\,(a, 1) :\to (b, 2). \\ &(\bar{y}\bar{x})\,(b, 1) :\to (a, 1). \\ &(\bar{y}x)\,(b, 2) :\to (a, 1). \\ &(y\bar{x})\,(c, 1) :\to \{(d, 1), (c, 2)\}. \\ &(yx)\,(c, 2) :\to (d, 1). \\ &(\bar{y}\bar{x})\,(d, 1) :\to \{(b, 1), (c, 1)\}. \end{aligned}$$

Состояние $(a,1)$ закрыто в силу условия 1. Согласно условию 2 закрытыми становятся состояния $(b,1)$ и $(b,2)$. Других закрытых состояний нет. После удаления всех закрытых состояний получим подавтомат композиции

$$\begin{aligned} &(y\bar{x})\,(c, 1) :\to \{(d, 1), (c, 2)\}. \\ &(yx)\,(c, 2) :\to (d, 1). \\ &(\bar{y}\bar{x})\,(d, 1) :\to (c, 1). \end{aligned}$$

Поскольку этот подавтомат циклический, он совпадает с автоматом C^*, которому соответствует следующий X / Y-автомат Мура A^*:

$$\begin{aligned} (y)\,c_1&: x \to c_2, \\ &\ \ \bar{x} \to d_1. \\ (y)\,c_2&: \bar{x} \to d_1. \\ (\bar{y})\,d_1&: \bar{x} \to c_1. \end{aligned}$$

Доопределив состояние c_2 переходом под действием x в c_2 и минимизировав полученный автомат, будем иметь автомат

$$\begin{aligned} (y)\,c&: x \to c, \\ &\ \ \bar{x} \to d_1. \\ (\bar{y})\,d_1&: \bar{x} \to c. \end{aligned}$$

Конец примера.

Рассмотрим теперь подход к согласованию автоматов, основанный на другом, более просто вычисляемом виде их композиции, которую назовем параллельной. При построении параллельной композиции X / Y-автомат A и Y / X-автомат B удобно рассматривать как детерминированные Σ-автоматы с одним и тем же алфавитом $\Sigma = X \times Y$. При этом для обоих автоматов отметки переходов имеют вид xy, где $x \in X$, $y \in Y$.

Определение 4. Параллельная композиция Σ-автоматов $A = \langle \Sigma, Q_A, \delta_A \rangle$ и $B = \langle \Sigma, Q_B, \delta_B \rangle$ (обозначается $A || B$) представляет собой Σ-автомат $D = \langle \Sigma, Q_D, \delta_D \rangle$, где $Q_D = Q_A \times Q_B$. Обозначим $\Sigma(q)$ множество всех символов $\sigma \in \Sigma$, для которых переход из состояния q определен, тогда $\Sigma((q, s)) = \Sigma(q) \cap \Sigma(s)$ и $\delta_D((q, s), \sigma) = (\delta_A(q, \sigma), \delta_B(s, \sigma))$ для всех $\sigma \in \Sigma((q, s))$.

Максимальный циклический подавтомат параллельной композиции Σ-автоматов A и B назовем параллельной циклической композицией этих автоматов.

Утверждение 1. Из $A \sim A_1$ и $B \sim B_1$ следует строгая эквивалентность композиций $D = A || B$ и $D_1 = A_1 || B_1$.

Доказательство. Для произвольного состояния (q, s) одной из композиций, скажем D, рассмотрим состояние (q', s') композиции D_1 такое, что q эквивалентно q', а s эквивалентно s'. Из $q \sim q'$ и $s \sim s'$ следует, что $\Sigma(q, s) = \Sigma(q', s')$ и для каждого $\sigma \in \Sigma(q,s)$ выполняется $\delta_A(q,\sigma) \sim \delta_{A_1}(q',\sigma)$, $\delta_B(s,\sigma) \sim \delta_{B_1}(s',\sigma)$. Пусть $\delta_D((q,s),\sigma) = (q_1, s_1)$ и $\delta_{D_1}((q',s'),\sigma) = (q_1', s_1')$, тогда $q_1 \sim q_1'$ и $s_1 \sim s_1'$. Отсюда вытекает, что каждое сверхслово в алфавите Σ, допустимое в состоянии (q,s), допустимо в состоянии (q',s'), и наоборот, а значит, состояния (q,s) и (q',s') эквивалентны. Таким образом, для каждого состояния композиции D имеется эквивалентное ему состояние композиции D_1, и наоборот, из чего следует строгая эквивалентность этих автоматов.

При исследовании согласуемости автоматов A и B, исходя из свойств параллельной композиции, вместо автомата B используется его так называемый левый сдвиг по входу [4].

Левым сдвигом по Y $Y \times X$-сверхслова $l = (y_1, x_1)(y_2, x_2)(y_3, x_3)\ldots$ называется сверхслово $\widetilde{l} = (y_2, x_1)(y_3, x_2)(y_4, x_3)\ldots$ Понятие левого сдвига по Y естественным образом распространяется на множества $Y \times X$-сверхслов. Левым сдвигом по Y множества $Y \times X$-сверхслов W назовем множество $\widetilde{W} = \{\widetilde{l} \mid l \in W\}$. В [4] показано, что для всякого циклического Y / X-автомата $B = \langle Y, X, Q_B, \chi_B, \mu_B \rangle$ существует такой циклический Y / X-автомат $\widetilde{B}$, называемый левым сдвигом по входу автомата B, что $W(\widetilde{B}) = \widetilde{W}(B)$. В качестве такого автомата используется Y / X-автомат $\widetilde{B} = \langle Y, X, Q_{\widetilde{B}}, \chi_{\widetilde{B}}, \mu_{\widetilde{B}} \rangle$, где $Q_{\widetilde{B}} = \{(s, y) \mid s \in Q_B, y \in Y, \chi_B(s, y) \neq$ $\neq \varnothing\}$, $\chi_{\widetilde{B}}((s, y), y_1) = \{(s_i, y_1) \mid s_i \in \chi_B(s, y), \chi_B(s_i, y_1) \neq \varnothing\}$, $\mu_{\widetilde{B}}((s, y)) = \mu_B(s)$. Для соответствующего Σ-автомата $\widetilde{B}$ с входным алфавитом $X \times Y$ функция переходов определяется следующим образом: $\delta_{\widetilde{B}}((s, y), x_1 y_1) = (s_1, y_1)$ тогда и только тогда, когда $s_1 \in \chi_B(s, y)$, $\mu_B(s_1) = x_1$ и $\chi_B(s_1, y_1) \neq \varnothing$.

Как следует из этого определения, левый сдвиг по входу квазициклического (циклического) квазидетерминированного автомата также является квазициклическим (циклическим) квазидетерминированным автоматом. Утверждение 1 позволяет минимизировать автомат $\widetilde{B}$, полученный описанным способом.

Утверждение 2. Пусть $(q', (s', y'))$ — состояние параллельной композиции D автоматов A и $\widetilde{B}$, для которого $\Sigma((q', (s', y'))) \neq \varnothing$, тогда любой переход из такого состояния осуществляется в состояние вида $(q, (s, \mu_A(q)))$.

Доказательство. Пусть для Σ-автомата D $\delta_D((q', (s', y')), x_1 y_1) = (q, (s, y))$. В соответствии с определением параллельной композиции Σ-автоматов $\delta_A(q', x_1 y_1) = q$, $\delta_{\widetilde{B}}((s', y'), x_1 y_1) = (s, y)$. Это значит, что для X / Y-автомата A $\mu_A(q) = y_1$, а для Y / X-автомата $\widetilde{B}$ $(s, y) \in \chi_{\widetilde{B}}((s', y'), y_1)$. Согласно определению левого сдвига по входу правая компонента всех состояний, принадлежащих $\chi_{\widetilde{B}}((s', y'), y_1)$, равна y_1 и, следовательно, $y = y_1 = \mu_A(q)$. Таким образом, всякое состояние, в которое осуществляется переход в автомате D, имеет вид $(q, (s, \mu_A(q)))$. Конец доказательства.

Отсюда следует, что все состояния параллельной циклической композиции имеют вид $(q, (s, \mu_A(q)))$.

Теорема 1. Правая композиция C X / Y-автомата A и Y / X-автомата B и параллельная композиция D Σ-автоматов A и $\widetilde{B}$ имеют изоморфные ядра.

Доказательство. 1. Пусть α — отображение состояний ядра автомата C в состояния автомата D, определенное следующим образом: $\alpha(q,s) =$ $= (q, (s, \mu_A(q)))$. Для любого состояния (q, s) ядра автомата C $\chi_B(s, \mu_A(q)) \neq \varnothing$, в силу чего состояние $(s, \mu_A(q))$ принадлежит левому сдвигу по входу автомата B и, следовательно, состояние $(q, (s, \mu_A(q)))$ принадлежит параллельной композиции D. Таким образом, это отображение определено для всех состояний ядра композиции C. Здесь автоматы B и $\widetilde{B}$ рассматриваются как Y / X-автоматы, а автомат D — как Σ-автомат. Покажем, что для Σ-автоматов C и D из $\delta_C((q,s), xy) = (q_1, s_1)$, где состояния (q, s) и (q_1, s_1) принадлежат ядру автомата C, следует $\delta_D(\alpha(q,s), xy) = \alpha(q_1, s_1)$, т.е. $\delta_D((q, (s, \mu_A(q))), xy) = (q_1, (s_1, \mu_A(q_1)))$. Согласно определению параллельной композиции это равенство соответствует двум равенствам: а) $\delta_A(q, xy) = q_1$; б) $\delta_{\widetilde{B}}((s, \mu_A(q)), xy) = (s_1, \mu_A(q_1))$.

Как следует из определения правой композиции, $\delta_C((q,s),xy)=(q_1,s_1)$ тогда и только тогда, когда $s_1\in\chi_B(s,\mu_A(q))$, $\mu_B(s_1)=x$ и $\delta_A(q,xy)=q_1$. Итак, равенство а) выполняется. Покажем теперь справедливость равенства б). В соответствии с определением левого сдвига автомата по входу это равенство имеет место тогда и только тогда, когда $s_1\in\chi_B(s,\mu_A(q))$, $\mu_B(s_1)=x$ и $\chi_B(s_1,y)\neq\varnothing$. Остается показать, что $\chi_B(s_1,y)\neq\varnothing$. Так как (q_1,s_1) принадлежит ядру автомата C, то $\chi_B(s_1,\mu_A(q_1))\neq\varnothing$, а из $\delta_A(q,xy)=q_1$ следует $\mu_A(q_1)=y$. Таким образом, необходимые и достаточные условия выполнения равенства $\delta_C((q,s),xy)=(q_1,s_1)$ для правой композиции C и соответствующего равенства для параллельной композиции D совпадают.

2. Пусть β — отображение состояний ядра автомата D в состояния автомата C такое, что $\beta(q,(s,\mu_A(q)))=(q,s)$. Покажем, что для Σ-автоматов C и D из $\delta_D((q,(s,\mu_A(q))),xy)=(q_1,(s_1,\mu_A(q_1)))$, где $(q,(s,\mu_A(q)))$ и $(q_1,(s_1,\mu_A(q_1)))$ — состояния ядра автомата D, следует $\delta_C(\beta(q,(s,\mu_A(q))),xy)=\beta(q_1,(s_1,\mu_A(q_1)))$, т.е. значение $\delta_C((q,s),xy)$ определено и равно (q_1,s_1). Это имеет место тогда и только тогда, когда $s_1\in\chi_B(s,\mu_A(q))$, $\mu_B(s_1)=x$ и $\delta_A(q,xy)=q_1$. Из $\delta_D((q,(s,\mu_A(q))),xy)=(q_1,(s_1,\mu_A(q_1)))$ следует $\delta_A(q,xy)=q_1$ и $\delta_{\widetilde{B}}((s,\mu_A(q)),xy)=(s_1,\mu_A(q_1))$, что, в свою очередь, дает $s_1\in\chi_B(s,\mu_A(q))$ и $\mu_B(s_1)=x$. Отсюда вытекает, что $\delta_C((q,s),xy)=(q_1,s_1)$.

Отображения α и β инъективны, поэтому из части 1 доказательства следует, что ядро автомата C изоморфно подмножеству состояний ядра автомата D, а из части 2 — что ядро автомата D изоморфно подмножеству состояний ядра автомата C. Таким образом, ядра автоматов C и D изоморфны. Конец доказательства.

Согласно теореме 1 для каждого циклического подавтомата правой композиции автоматов A и B существует изоморфный ему подавтомат параллельной композиции автоматов A и $\widetilde{B}$, и наоборот.

Отметим, что если $(s_1,y)\in\chi_{\widetilde{B}}((s,\mu_A(q)),y)$, то в Σ-автомате $\widetilde{B}$ этому утверждению соответствует $\delta_{\widetilde{B}}((s,\mu_A(q)),xy)=(s_1,y)$, где $x=\mu_B(s_1)$.

Для иллюстрации теоремы 1 рассмотрим поведение ядер правой и параллельной композиций соответственно в состоянии (q,s) и $(q,(s,\mu_A(q)))$.

Пример 2. Пусть переходы из состояния q в X/Y-автомате Мура A определены следующим образом:

$$
\begin{aligned}
q: x_1 &\to \{q_1(y_1), q_2(y_2)\},\\
x_2 &\to \{q_3(y_2)\},\\
x_3 &\to \{q_5(y_1), q_2(y_2)\},
\end{aligned}
$$

а множество состояний $\chi_B(s,\mu_A(q))$, в которые автомат B переходит из состояния s под действием $\mu_A(q)$, имеет вид $\{s_1(x_1),s_2(x_2),s_3(x_3)\}$. Здесь $X=\{x_1,x_2,x_3\}$, $Y=\{y_1,y_2,y_3\}$ и отметки состояний записаны в скобках непосредственно после символа состояния.

Множество $\bigcup\limits_{y\in Y}\chi_{\widetilde{B}}((s,\mu_A(q)),y)$ всех состояний, в которые имеются переходы из состояния $(s,\mu_A(q))$ автомата $\widetilde{B}$, получается, если во множестве $\chi_B(s,\mu_A(q))\times Y$ удалить все пары (s_i,y_j), для которых $\chi_B(s_i,y_j)=\varnothing$.

Пусть это множество равно

$$
\begin{gathered}
\{(s_1(x_1),y_1),[(s_2(x_2),y_1)],(s_3(x_3),y_1),\\
(s_1(x_1),y_2),(s_2(x_2),y_2),[(s_3(x_3),y_2)],\\
[(s_1(x_1),y_3)],(s_2(x_2),y_3),(s_3(x_3),y_3)\}.
\end{gathered}
$$

Здесь в квадратные скобки заключены такие состояния вида $(s_i(x_j),y_k)$, что $\chi_B(s_i,y_k)=\varnothing$. Переходы в эти состояния отсутствуют, так как они не принадлежат автомату $\widetilde{B}$. Соответствующие переходы в Σ-автоматах A и $\widetilde{B}$ имеют следующий вид:

$$q : x_1 y_1 \to q_1, \qquad (s, \mu_A(q)) : x_1 y_1 \to (s_1, y_1),$$
$$x_1 y_2 \to q_2, \qquad x_3 y_1 \to (s_3, y_1),$$
$$x_2 y_2 \to q_3, \qquad x_1 y_2 \to (s_1, y_2),$$
$$x_3 y_1 \to q_5, \qquad x_2 y_2 \to (s_2, y_2),$$
$$x_3 y_2 \to q_2. \qquad x_2 y_3 \to (s_2, y_3),$$
$$x_3 y_3 \to (s_3, y_3).$$

Построим все переходы из состояния $(q, (s, \mu_A(q)))$ параллельной композиции $A || \widetilde{B}$, рассматриваемой как Σ-автомат. Эти переходы определены для символов алфавита $X \times Y$, принадлежащих $\Sigma(q) \cap \Sigma(s, \mu_A(q)) = \{x_1 y_1, x_1 y_2, x_2 y_2, x_3 y_1\}$, и имеют вид

$$\begin{aligned}(q, (s, \mu_A(q))) : x_1 y_1 &\to (q_1, (s_1, y_1)),\\ x_1 y_2 &\to (q_2, (s_1, y_2)),\\ x_2 y_2 &\to (q_3, (s_2, y_2)),\\ x_3 y_1 &\to (q_5, (s_3, y_1)).\end{aligned}$$

Множество переходов правой композиции из состояния (q, s) равно

$$\{(q_1(y_1), s_1(x_1)), (q_2(y_2), s_1(x_1)), (q_3(y_2), s_2(x_2)),$$
$$(q_5(y_1), s_3(x_3)), [(q_2(y_2), s_3(x_3))]\}.$$

Состояние $(q_2(y_2), s_3(x_3))$ не принадлежит композиции, поскольку $\chi_B(s_3, y_2) = \varnothing$. Для Σ-автомата C это поведение в состоянии (q, s) описывается следующим образом:

$$\begin{aligned}(q, s) : x_1 y_1 &\to (q_1, s_1),\\ x_1 y_2 &\to (q_2, s_1),\\ x_2 y_2 &\to (q_3, s_2),\\ x_3 y_1 &\to (q_5, s_3).\end{aligned}$$

Отсюда видно, что отображение $\alpha(q, s) = (q, (s, \mu_A(q)))$ сохраняет функцию переходов. Конец примера.

Для описания предлагаемого подхода к согласованию автоматов на основе их параллельной композиции в условии σ, принадлежащем $X \times Y$, выделим две части: проекцию σ на X (обозначается $\mathrm{Pr}_X(\sigma)$) и проекцию σ на Y ($\mathrm{Pr}_Y(\sigma)$). Понятие проекции распространим на множества условий.

Условие возможности согласования X / Y-автомата A с Y / X-автоматом B в терминах их правой композиции, рассматриваемой как Σ-автомат, можно сформулировать таким образом. Автомат A может быть согласован с автоматом B тогда и только тогда, когда правая композиция автоматов A и B имеет циклический подавтомат C', любое состояние (q, s) которого удовлетворяет следующему условию: для каждого $x \in \{\mu_B(s_1) | s_1 \in \chi_B(s, \mu_A(q))\}$ существует такое $q_1 \in \chi_A(q, x)$, что состояние (q_1, s_1) принадлежит множеству состояний автомата C'. Напомним, что для Σ-автомата C' $\delta_{C'}((q, s), xy) = (q_1, s_1)$, если $s_1 \in \chi_B(s, \mu_A(q))$, $\mu_B(s_1) = x$ и $q_1 \in \chi_A(q, \mu_B(s_1))$, $\mu_A(q_1) = y$. Рассматривая композицию C как Σ-автомат и используя введенное понятие проекции, это условие можно записать в виде $\mathrm{Pr}_X(\Sigma_{C'}(q, s)) = \{\mu_B(s_1) | s_1 \in \chi_B(s, \mu_A(q))\}$. Нижний индекс при символе Σ указывает, какому автомату принадлежит состояние (q, s).

Сформулируем это свойство для состояний подавтомата параллельной композиции Σ-автоматов A и $\widetilde{B}$, изоморфного автомату C'. Состоянию (q, s) автомата C' соответствует состояние $(q, (s, \mu_A(q)))$ параллельной композиции D автоматов A и $\widetilde{B}$ такое, что $\Sigma_D((q, (s, \mu_A(q)))) = \Sigma_{C'}((q, s))$. Исходя из определения левого сдвига автомата по входу и из того, что в силу цикличности автомата B для каждого $s \in Q_B$ существует такой $y \in Y$, что $\chi_B(s, y) \neq \varnothing$, несложно показать, что для автомата $\widetilde{B}$ $\mathrm{Pr}_X(\Sigma_{\widetilde{B}}(s, \mu_A(q))) = \{\mu_B(s_1) | s_1 \in \chi_B(s, \mu_A(q))\}$. Теперь для параллельной циклической композиции возможность согласования охарактеризуем следующим образом. Автомат A может быть согласован с автоматом B тогда и только тогда, когда параллельная циклическая композиция Σ-автоматов A и $\widetilde{B}$ имеет циклический подавтомат D', любое состояние $(q,(s,\mu_A(q)))$ которого удовлетворяет условию $\mathrm{Pr}_X(\Sigma_{D'}(q,(s,\mu_A(q))))=\mathrm{Pr}_X(\Sigma_{\widetilde{B}}(s,\mu_A(q)))$. Таким образом, для Σ-автомата, соответствующего параллельной циклической композиции D, условие согласованности выполняется, если в каждом его состоянии $(q,(s,\mu_A(q)))$ проекция на X множества условий всех переходов из этого состояния совпадает с проекцией на X множества условий всех переходов в Σ-автомате $\widetilde{B}$ из состояния $(s,\mu_A(q))$. Это условие для состояния $(q,(s,\mu_A(q)))$ назовем условием корректности композиции в состоянии $(q,(s,\mu_A(q)))$. Параллельная циклическая композиция автоматов A и $\widetilde{B}$ корректна, если она корректна в каждом состоянии.

Процесс согласования автоматов A и B осуществляется следующим образом. Строится параллельная циклическая композиция Σ-автоматов A и $\widetilde{B}$. Затем для состояний этой композиции проверяется условие корректности. Все состояния композиции, не удовлетворяющие условию корректности, удаляются. В полученном автомате снова выделяется максимальный циклический подавтомат, для состояний которого проверяется условие корректности. Этот процесс продолжается до тех пор, пока не будет получен циклический подавтомат, все состояния которого удовлетворяют условию корректности. Результатом этого процесса согласования является Σ-автомат A^*, изоморфный полученному подавтомату параллельной композиции.

Пример 3. Рассмотрим те же автоматы, что и в примере 1, для случая, когда автоматы A и $\widetilde{B}$ представлены в виде Σ-автоматов:

Σ-автомат A имеет вид

$$\begin{array}{ll} a: x\bar{y}\to b. & d: \overline{xy}\to b, \\ b: \bar{x}y\to a, & \quad x\bar{y}\to b, \\ \quad x\bar{y}\to b. & \quad \bar{x}y\to c. \\ c: \overline{xy}\to d, & \\ \quad xy\to c. & \end{array}$$

Σ-автомат $\widetilde{B}$ выглядит следующим образом:

$$\begin{array}{ll} (1,y): \bar{x}y\to(1,y), & (2,y): \bar{x}y\to(1,y), \\ \quad xy\to(2,y), & \quad \overline{xy}\to(1,\bar{y}). \\ \quad x\bar{y}\to(2,\bar{y}), & (2,\bar{y}): \bar{x}y\to(1,y), \\ \quad \overline{xy}\to(1,\bar{y}). & \quad \overline{xy}\to(1,\bar{y}). \\ (1,\bar{y}): \bar{x}y\to(1,y), & \\ \quad \overline{xy}\to(1,\bar{y}). & \end{array}$$

При построении $A\|\widetilde{B}$ рассматриваются такие пары $(q,(s,y))$ состояний автоматов A и $\widetilde{B}$, для которых $\Sigma(q)\cap\Sigma(s,y)\neq\varnothing$. Напомним, если $\sigma\in\Sigma(q)\cap\Sigma(s,y)$, то $\delta_D((q,(s,y)),\sigma)=(\delta(q,\sigma),\delta((s,y),\sigma))$.

Приведем параллельную циклическую композицию, которая получается из параллельной композиции в результате удаления всех недостижимых состояний:

$$\begin{array}{ll} (a,(1,y)): x\bar{y}\to(b,(2,\bar{y})). & (c,(2,y)): \overline{xy}\to(d,(1,\bar{y})). \\ (b,(1,\bar{y})): \bar{x}y\to(a,(1,y)). & (d,(1,\bar{y})): \overline{xy}\to(b,(1,\bar{y})), \\ (b,(2,\bar{y})): \bar{x}y\to(a,(1,y)). & \quad \bar{x}y\to(c,(1,y)). \\ (c,(1,y)): \overline{xy}\to(d,(1,\bar{y})), & \\ \quad xy\to(c,(2,y)). & \end{array}$$

Композиция некорректна в состоянии $(a,(1,y))$, поскольку $\mathrm{Pr}_X(\Sigma(a,(1,y)))\neq$ $\neq\mathrm{Pr}_X(\Sigma(1,y))$. После удаления этого состояния максимальный циклический подавтомат полученного автомата принимает вид

$$\begin{array}{l} (c,(1,y)): \overline{xy}\to(d,(1,\bar{y})), \\ \quad xy\to(c,(2,y)). \\ (c,(2,y)): \overline{xy}\to(d,(1,\bar{y})). \\ (d,(1,\bar{y})): \bar{x}y\to(c,(1,y)). \end{array}$$

Этот подавтомат композиции корректен в каждом состоянии и изоморфен автомату A^*, полученному в примере 1 и рассматриваемому как Σ-автомат.

Заметим, что в приведенном выше автомате $\widetilde{B}$ состояния $(1, \bar{y})$, $(2, y)$, $(2, \bar{y})$ эквивалентны. Поэтому в качестве автомата $\widetilde{B}$ можно было использовать автомат

$$\begin{array}{llll} (1, y): & \bar{x}y \to (1, y), & \qquad (2): & \bar{x}y \to (1, y), \\ & xy \to (2), & & \overline{xy} \to (2). \\ & x\bar{y} \to (2), & & \\ & \overline{xy} \to (2). & & \end{array}$$

Конец примера.

Если рассматривается композиция инициальных автоматов, которая также является инициальным автоматом, то условие корректности проверяется только для тех состояний композиции, которые принадлежат ее инициальному циклическому подавтомату. Если в процессе работы алгоритма начальное состояние будет удалено, то алгоритм заканчивает работу в силу невозможности согласования инициальных автоматов. Таким образом, методы, основанные на понятии согласованности неинициальных автоматов, могут потребовать значительно большего количества вычислений, чем предложенный здесь способ преобразования инициального автомата.

ПРОБЛЕМА РЕАЛИЗУЕМОСТИ И СОГЛАСОВАНИЕ АВТОМАТОВ

Как отмечалось во введении, проблема согласования является частным случаем проблемы реализуемости спецификации системы. Обычно проблема реализуемости решается одновременно с проблемой синтеза автомата или алгоритма, исходя из спецификации требований к их функционированию, сформулированных в виде утверждений в подходящем логическом языке. Для того чтобы учесть требования реализуемости, Пнуэли и律Рознер [6], Абади, Лэмпорт и Волпер [7] предложили для синтеза реактивных систем использовать игровые модели, описывающие бесконечную игру между системой и средой, с которой она взаимодействует. Построение корректного алгоритма функционирования системы заключается в нахождении выигрышной стратегии в игре, моделирующей совместное поведение этой системы и среды. Выигрышную стратегию можно получить только за счет ограничения возможности выбора очередного хода системы, выбор очередного хода среды может быть любым в рамках ее возможностей. Спецификации, для которых выигрышные стратегии существуют, называются реализуемыми. Сложность построения такой стратегии зависит от вида свойств системы, задаваемых спецификацией. Так, если спецификация представляет собой формулу языка LTL, задача построения стратегии полна в классе 2EXPTIME [6]. Поэтому для практического использования игровых моделей ограничиваются более узкими классами свойств. Для получения приемлемой сложности решения проблемы реализуемости ограничивают выразительные возможности языка спецификации и соответственно класс свойств, выразимых в этом языке. Так, в [8] рассматривается фрагмент языка LTL, состоящий из булевых комбинаций формул вида Fp (или Gp), где F (когда-нибудь), G (всегда) — темпоральные операторы, а p — формула, не содержащая темпоральных операторов. Это позволило получить алгоритм проверки реализуемости, принадлежащий классу PSPACE. В [9] рассматриваются спецификации, представимые формулами вида $(\mathrm{GF}p_1 \wedge \mathrm{GF}p_2 \wedge \ldots \wedge \mathrm{GF}p_m) \to (\mathrm{GF}q_1 \vee \mathrm{GF}q_2 \vee \ldots \vee \mathrm{GF}q_n)$ где p_i, q_i — булевы формулы от атомарных высказываний из множества P. Показано, что в этом случае проблема реализуемости может быть решена со сложностью EXPTIME и количеством операций $O((mn \cdot 2^{|P|})^3)$. В настоящей работе предполагается, что совместное поведение системы и среды характеризуется только свойствами безопасности (safety).

Формально свойства рассматриваются как подмножества множества всех сверхслов в алфавите Σ, ассоциируемом со спецификацией. Множество сверхслов S определяет свойство безопасности тогда и только тогда, когда каждое сверхслово, не принадлежащее S, имеет конечный префикс, любое продолжение которого не принадлежит S. Для спецификации, задающей только инвариантные свойства безопасности, определение ее реализуемости сводится к согласованию спецификаций проектируемой системы и среды или специфицируемых ими автоматных моделей. Поскольку выразительные возможности спецификаций ограничены свойствами, представимыми Σ-автоматами, процесс согласования можно выполнять как на уровне спецификаций (чему будет посвящена вторая часть этой работы), так и на уровне синтезированных автоматов. Развиваемый здесь подход к согласованию автоматов характеризуется следующими особенностями.

1. Проблемы согласования и синтеза рассматриваются независимо и могут решаться в любом порядке.

2. В большинстве работ, посвященных синтезу реактивных систем, проблема реализуемости рассматривается без какой-либо информации о поведении среды. Предполагается, что в любой момент времени на вход системы может поступить любой символ выходного алфавита среды. Следовательно, на любое входное сверхслово x система должна реагировать таким образом, чтобы соответствующее вход-выходное сверхслово (x, y) удовлетворяло требованиям спецификации. В действительности обычно имеется информация о поведении среды. Поэтому в настоящей работе среда рассматривается как реактивная система, взаимодействие с которой на уровне спецификаций описывается как их конъюнкция, а на уровне автоматов — как композиция соответствующих автоматов. Такой подход хотя и усложняет решение проблемы синтеза, однако дает более реалистичные оценки возможности реализации системы. Так, спецификация, не реализуемая при традиционном подходе, может оказаться реализуемой при учете информации о поведении среды.

Аналогичный подход рассматривался в [10] для спецификаций, представленных в языке CTL* и CTL, где показано, что соответствующая проблема реализуемости полна в классе 3EXPTIME и 2EXPTIME соответственно. Следует заметить, что проблема согласования автоматов даже с учетом информации о среде имеет полиномиальную сложность.

ЗАКЛЮЧЕНИЕ

Задача согласования автоматов или их логических спецификаций возникает при автоматном подходе к проектированию реактивных систем. При этом как для проектируемой системы, так и для среды, с которой она взаимодействует, используются автоматные модели. В настоящей работе в качестве таких моделей рассматриваются частичные недетерминированные автоматы Мура над бесконечными словами. Согласованность автомата со средой является частным случаем его реализуемости, когда свойства, характеризующие требуемое поведение автомата при его взаимодействии со средой, ограничиваются инвариантными относительно дискретного времени свойствами безопасности. Такие свойства представимы рассматриваемыми автоматами, поэтому задача согласования может решаться как на уровне спецификаций, так и на уровне синтезированных по ним автоматов. Автомат, синтезированный по его спецификации в логическом языке, вообще говоря, может быть частичным, что требует его согласования со средой.

Для описания взаимодействия автоматов используются два вида композиции: правая и параллельная. В обеих композициях предполагается, что изменения состояний автоматов происходят в один и тот же момент дискретного времени, однако в правой композиции в реальном времени они осуществляются последовательно. В зависимости от реализации автоматов параллельная композиция может описывать их взаимодействие без замены автомата B его левым сдвигом. Так, взаимодействие автоматов A и B, построенных на триггерах, переключающихся по переднему фронту тактирующего сигнала, описывается параллельной композицией этих автоматов. В игровых моделях взаимодействия автоматов изменения их состояний происходят последовательно в двух смежных тактах. Соответствующая композиция автоматов рассматривалась в [4], где она названа симметричной циклической композицией. Различия в этих моделях не влияют на методы и результаты решения задачи согласования.

Обычно рассматривается взаимодействие инициальных автоматов, однако имеется несколько причин, почему настоящая работа посвящена в основном вопросам согласования неинициальных автоматов. Предложенное здесь решение задачи согласования ориентировано на методологию проектирования реактивных алгоритмов, в которой спецификация автоматных модулей имеет вид $\langle S, \varphi_0 \rangle$, где S — спецификация неинициального автомата, а φ_0 — начальное условие, выделяющее в нем одно или несколько начальных состояний. Многие задачи проектирования, в том числе и проблема реализуемости, решаются на уровне спецификаций. Согласование спецификаций основывается на методах согласования автоматов, поэтому на автоматном уровне эту задачу естественно рассматривать для неинициальных автоматов. Кроме того, имеется ряд задач, связанных с синтезом неинициальных автоматов [11–13], в частности, такая задача возникает при композиционном подходе к проектированию реактивных алгоритмов [14].

В заключение заметим, что согласование автомата со средой имеет значение не только для обеспечения корректности функционирования системы, но и для увеличения возможностей оптимизации автомата, полученного в результате синтеза. Поэтому, если даже автомат заведомо согласован со средой, процедуру согласования иногда целесообразно выполнять, чтобы увеличить частичность автомата, используемую при оптимизации.

СПИСОК ЛИТЕРАТУРЫ

1. Church A. Applications of recursive arithmetic to the problem of circuit synthesis // Summaries of the Summer Inst. for Symbolic Logic. — New York: Cornell Univ., 1957. — P. 3–50.
2. Kupferman O. Recent challenges and ideas in temporal synthesis // Proc. 38th Conf. on Theory and Practice of Computer Science (SOFSEM 2012), Lect. Notes Comput. Sci. — 2012. — **7147.** — P. 88–98.
3. Alpern B., Schneider F.B. Defining liveness // Information Processing Letters. — 1985. — **21**, N 4. — P. 181–185.
4. Чеботарев А.Н. Взаимодействие автоматов // Кибернетика и системный анализ. — 1991. — № 6. — С. 17–29.
5. Чеботарев А.Н. Общий метод проверки согласованности взаимодействующих автоматов с конечной памятью // Кибернетика и системный анализ. — 1999. — № 6. — С. 25–37.
6. Pnueli A., Rosner R. On the synthesis of a reactive module // Proc. 16th ACM Symp. on Principles of Programming Languages. — New York: ACM Press, 1989. — P. 179–190.
7. Abadi M., Lamport L., Wolper P. Realizable and unrealizable specifications of reactive systems // Intern. Colloquium on Automata, Languages, and Programming, Lect. Notes Comput. Sci. — 1989. — **372.** — P. 1–17.
8. Alur R., La Torre S. Deterministic generators and games for LTL fragments // ACM Trans. Computational Logic. — 2004. — **5**, N 1. — P. 1–25.
9. Piterman N., Pnueli A., Sa'ar Y. Synthesis of Reactive(1) Designs // Proc. Intern. Conf. on Verification, Model Checking, and Abstract Interpretation, Lect. Notes Comput. Sci. — 2006. — **3855.** — P. 364–380.
10. Kupferman O., Madhusudan P., Thiagarajan P.S., Vardi M. Open systems in reactive environments: Control and synthesis // Proc. 11th Intern. Conf. on Concurrency Theory. Lect. Notes Comput. Sci. — 2000. — **1877.** — P. 92–107.
11. Singhal V., Pixley C. The verification problem for safe replaceability // Proc. Conf. on Computer-Aided Verification, Lect. Notes Comput. Sci. — 1994. — **818.** — P. 311–323.
12. Qadeer S., Brayton R. K., Singhal V., Pixley C. Latch redundancy removal without global reset // Proc. Intern. Conf. on Computer Design. — S.l.: IEEE Computer Society, 1996. — P. 432–439.
13. Henzinger T. A., Krishnan S. C., Kupferman O., Mang F. Y.C. Synthesis of uninitialized systems // Proc. Intern. Colloquium ICALP 2002, Lect. Notes Comput. Sci. — 2002. — **2380.** — P. 644–656.
14. Чеботарев А.Н. Композиционный подход к проектированию реактивных алгоритмов // Кибернетика и системный анализ. — 2013. — № 5. — С. 14–27.

Поступила 10.12.2014