ЧЕБОТАРЬОВ А. М., **д-р техн. наук, проф.**

КУРІВЧАК О. І.

РЕГУЛЯРНА ФОРМА СПЕЦИФІКАЦІЇ МОВОЮ L ДЕТЕРМІНОВАНИХ АВТОМАТІВ

Досліджуються деякі форми подання специфікацій детермінованих автоматів у мові L. Використання таких форм при побудові специфікації зменшує вірогідність допущення помилок.

Some forms of representation of deterministic automata specifications in the language L are investigated. The use of such forms in the construction of specifications decreases the possibility of errors.

Вступ

Формальна специфікація автомата — це сукупність тверджень, які визначають вимоги до його функціонування, тобто його темпоральні властивості. Ці твердження формулюються у вигляді формул формальної мови, для чого зазвичай використовуються логічні мови, такі як темпоральні логіки, числення предикатів першого порядку та ін. У цій праці як така мова розглядається проста логічна мова L, яка є підмножиною мови одномісних предикатів першого порядку. Процес побудови фор-мальної специфікації автомата починається з усвідомлення всіх вимог до його функціонування з нас-тупним формулюванням їх у вигляді формул мови L. Для специфікацій, розрахованих на синтез, тобто на використання автоматичної процедури перетворення специфікації у процедурне подання алгоритму функціонування автомата, необхідно забезпечити їх повноту, яка полягає у тому, що мають бути наведені всі обмеження на функціонування автомата. Оскільки побудова специфікації — це неформальний процес, який виконується людиною, то побудована специфікація може містити помилки, усунення яких після синтезу та на наступних етапах перетворюється у дуже складну задачу. Тому необхідно так організувати процес побудови специфікації, щоб вірогідність помилки в ній була малою. Цього можна досягти двома шляхами:

1) дотримуватися суворих правил написання специфікації у чітко визначеній формі;

2) використовувати засоби формальної верифікації, тобто перевірки наявності важливих властивостей специфікації.

Зазвичай використовується як перший, так і другий шляхи зменшення кількості помилок. Ця праця присвячена дослідженню деяких форм подання специфікацій детермінованих автоматів та визначенню їхніх властивостей, які можна просто перевіряти у процесі побудови специфікації. Написання специфікації у розглянутих формах суттєво зменшує вірогідність допущення помилок та можливості не врахування деяких обмежень на функціонування автомата.

Мова специфікації L

Мова L [1] є фрагментом логіки предикатів першого порядку з одномісними предикатами й фіксованою областю інтерпретації, якою виступає множина $\mathbf{Z}$ цілих чисел (моментів часу). Специфікація у мові L має вигляд формули $\forall tF(t)$, де $F(t)$ — формула з єдиною змінною t, яка побудована за допомогою логічних зв'язок із атомарних формул (атомів) вигляду $p(t + k)$, де p — одномісний предикатний символ, t — змінна, що набуває значення з множини $\mathbf{Z}$, а k — ціла константа, що зветься *рангом атома*. Різниця між максимальним та мінімальним рангами атомів у формулі $F(t)$ називається її *глибиною*. Оскільки $F(t)$ інтерпретується на множині цілих чисел, то для довільного цілого k має місце еквівалентність $\forall tF(t) \Leftrightarrow \forall tF(t + k)$, де $F(t + k)$ позначає формулу, яка здобута з $F(t)$ додаванням k до рангів усіх її атомів. Таким чином, можна обмежитися розглядом формул $F(t)$, у яких максимальний ранг атомів дорівнює 0.

При визначенні семантики мови L вона розглядається як формалізм для задання множин надслів в алфавіті двійкових векторів, довжина яких дорівнює кількості предикатних символів у формулі.

Нехай Σ — скінченний алфавіт, $\mathbf{Z}$ — множина цілих чисел, $\mathbf{N}^+ = \{z \in \mathbf{Z} \mid z > 0\}$ і $\mathbf{N}^- = \{z \in \mathbf{Z} \mid z \leq 0\}$. Відображення u: $\mathbf{Z} \to \Sigma$ і l: $\mathbf{N}^+ \to \Sigma$ називаються відповідно *двостороннім надсловом* (позначається $\ldots u(-2)\, u(-1)\, u(0)\, u(1)\, u(2)\ldots$), та *надсловом* (позначається $l(1)l(2)\ldots$) в алфавіті Σ. Множина всіх двосторонніх надслів у алфавіті Σ, позначається $\Sigma^{\mathbf{Z}}$, а множина всіх надслів — Σ^{ω}. Для двостороннього надслова u і $n \in \mathbf{Z}$ визначимо n-*суфікс* $u(n+1, \infty)$ як надслово $u(n+1)u(n+2)\ldots$.

Нехай $\Omega = \{p_1, p_2, \ldots, p_q\}$ — множина всіх предикатних символів, які зустрічаються у формулі $F(t)$ (сигнатура формули). Областю інтерпретації мови L є множина $\mathbf{Z}$, і неінтерпретованими є лише предикатні символи. Отже, інтерпретація формули $\forall tF(t)$ — це набір $<\pi_1, \pi_2, \ldots, \pi_q>$

визначених на **Z** одномісних предикатів, які відповідають усім предикатним символам із множини Ω. Кожен такий предикат π_i можна розглядати як двостороннє надслово в алфавіті $\{0, 1\}$, а набір q таких предикатів — як двостороннє надслово в алфавіті $\Sigma = \{0, 1\}^q$. Ми не будемо розрізняти інтерпретації і відповідні двосторонні надслова в алфавіті Σ, тому говоритимемо про істинність та хибність формули $F(t)$ у позиції τ ($\tau \in \mathbf{Z}$) двостороннього надслова u, маючи на увазі значення формули $F(\tau)$ при інтерпретації u. Смисл поняття глибини формули полягає у тому, що значення формули $F(t)$ глибини r у позиції τ інтерпретації u визначається відрізком $u(\tau-r, \tau)$ відповідного двостороннього надслова u. Інтерпретація, при якій формула $\forall tF(t)$ істинна, називається *моделлю* для цієї формули. З кожною формулою $\mathrm{F} = \forall tF(t)$ асоціюється множина $M(\mathrm{F})$ усіх моделей для неї. Кожна формула $\mathrm{F} = \forall tF(t)$ визначає множину надслів над Σ, яка позначатиметься $W(\mathrm{F})$, а саме, множину 0-суфіксів усіх двосторонніх надслів з $M(\mathrm{F})$.

Визначимо автоматну семантику мови L.

Визначення 1. Скінченний X-Y-автомат A — це четвірка $<X, Y, Q, \chi>$, де X і Y — вхідний і вихідний алфавіти відповідно; Q — скінченна множина станів, а χ: $Q \times X \times Y \to 2^Q$ — функція переходів. Іноді відношення переходів зручно задавати у вигляді функції переходів-виходів λ: $Q \times X \to 2^{Q \times Y}$.

Автомат A називається *детермінованим*, якщо для будь-яких $x \in X$, $q \in Q$ $|\lambda(q, x)| \le 1$; у супротивному разі він називається *недетермінованим*.

Визначення 2. X-Y-автомат $A = <X, Y, Q, \chi>$ називається *квазідетермінованим*, якщо для будь-яких $q \in Q$, $x \in X$ та $y \in Y$ $|\chi(q, x, y)| \le 1$.

Квазідетермінований X-Y-автомат зручно розглядати як детермінований частковий автомат без виходів і з вхідним алфавітом $\Sigma = X \times Y$. Такий автомат $A = <\Sigma, Q, \delta>$, де δ: $Q \times \Sigma \to Q$ — часткова функція переходів, будемо називати *Σ-автоматом A*.

Визначення 3. Σ-автомат $A = <\Sigma, Q, \delta>$ називається *циклічним*, якщо для кожного $q \in Q$ існують такі $q_1, q_2 \in Q$ та $\sigma_1, \sigma_2 \in \Sigma$, що $q_1 \in \delta(q, \sigma_1)$ і $q \in \delta(q_2, \sigma_2)$.

Циклічний Σ—автомат можна охарактеризувати у термінах допустимих надслів.

Визначення 4. Надслово $l = \sigma_1\sigma_2 \ldots$ *допустиме у стані* q Σ-автомата A, якщо існує таке надслово станів $q_0\, q_1\, q_2 \ldots$, де $q_0 = q$, що для будь-якого $i = 0, 1, 2, \ldots$ $\delta(q_i, \sigma_{i+1}) = q_{i+1}$. Надслово l *допустиме для автомата A*, якщо воно допустиме хоча б в одному із його станів.

Позначимо $W(A)$ множину всіх надслів, допустимих для автомата A. Автомат A *задовольняє специфікацію* F, якщо $W(A) = W(\mathrm{F})$. Розглянемо спосіб побудови автомата $A(\mathrm{F})$, який задовольняє специфікацію $\mathrm{F} = \forall tF(t)$ [2].

Нехай $\Omega = \{p_1, p_2, \ldots, p_q\}$ — сигнатура формули $F(t)$, а r — глибина цієї формули. Позначимо S_Ω множину всіх двійкових векторів довжини $|\Omega|$, де $|\Omega|$ — потужність множини Ω.

Послідовність $s_0, s_1, \ldots, s_r$ векторів із S_Ω назвемо *станом* глибини r, а множину $Q(r, \Omega)$ усіх таких послідовностей — *простором станів* глибини r для формули $F(t)$. Формулу $F(t)$ розглядатимемо як пропозиційну формулу від змінних $p_1(t), \ldots, p_q(t), p_1(t-1), \ldots, p_q(t-1), \ldots, p_1(t-r), \ldots, p_q(t-r)$. Якщо компоненти вектора s_i у стані $q = s_0, s_1, \ldots, s_r$ розглядати як істинністні значення відповідних атомів рангу $i - r$ при певному впорядкуванні множини Ω, то можна говорити про значення формули $F(t)$ на стані q.

На множині $Q(r, \Omega)$ визначимо відношення N *безпосереднього слідування* так, що за кожним станом $q = s_0, s_1, \ldots, s_r$ безпосередньо слідують $2^{|\Omega|}$ станів вигляду $s_1, \ldots, s_r, s$, де $s \in S_\Omega$. Множину всіх станів, які безпосередньо слідують за q, будемо позначати $N(q)$.

При використанні мови L для специфікації автоматів предикатні символи ставляться у відповідність вхідним і вихідним двійковим каналам автомата, що специфікується. Тому множина предикатних символів Ω розбивається на два класи: вхідні й вихідні, які позначаються відповідно U і W. Визначимо вхідний алфавіт X і вихідний алфавіт Y автомата $A(\mathrm{F})$ як множини всіх двійкових векторів довжини відповідно $|U|$ і $|W|$. Кожний вектор із S_Ω можна розглядати як пару $<x, y>$, де $x \in X$, $y \in Y$, тому нарівні з позначенням $s_0, \ldots, s_r$ для стану глибини r будемо використовувати позначення
$<x_0, y_0>, \ldots, <x_r, y_r>$.

Побудуємо допоміжний автомат $A'(F) = <X, Y, Q', \chi_{A'}>$. Множина станів Q' — це усі ті стани із
$Q(r, \Omega)$, на яких $F(t)$ істинна. Функцію переходів цього автомата визначимо у такий спосіб. Нехай
$q \in Q'$, $x \in X$ і $y \in Y$, тоді $\chi_{A'}(q, x, y)$ — це множина всіх тих станів $<x_0, y_0>, \ldots, <x_r, y_r>$ із $N(q) \cap Q'$, у яких $x_r = x$; $y_r = y$, якщо таких станів немає, то значення $\chi_{A'}(q, x, y)$ не визначене. Автомат $A(\mathrm{F})$ є максимальним циклічним підавтоматом автомата $A'(\mathrm{F})$.

Властивості специфікацій детермінованих автоматів

Будемо розглядати зображння формули $F(t)$ у просторі станів відповідної глибини. Говоритимемо, що формула $F(t)$ істинна на області простору станів, якщо вона істинна хоча б на одному стані цієї області, і формула хибна на області, якщо вона хибна на усіх її станах. Якщо q — стан простору станів, то $N(q)$ називається *областю переходів* для стану q. Частина області переходів, що відповідає символу x вхідного алфавіту X, тобто всі ті стани $< x_0, y_0 >, \ldots, < x_r, y_r >$ із $N(q)$, у яких $x_r = x$, називається *областю переходу* під дією символу x. Властивості специфікацій, що відповідають детермінованості та всюдивизначеності автомата, визначаються властивостями областей переходів мінімальної форми подання специфікації [3]. Мінімальна форма специфікації $\mathrm{F} = \forall tF(t)$ — це така специфікація $\forall t \min(F(t))$ автомата $A(\mathrm{F})$, що множина станів простору $Q(r, \Omega)$, на яких істинна формула $\min(F(t))$, збігається з множиною станів автомата $A(\mathrm{F})$ у цьому просторі.

Твердження 1. Формула $\forall tF(t)$ специфікує детермінований автомат тоді і тільки тоді, коли у кожній області переходу простору станів формула $\min(F(t))$ істинна не більш ніж на одному стані.

Твердження 2. Формула $\forall tF(t)$ специфікує всюди визначений автомат тоді і тільки тоді, коли для кожної області переходів простору станів, на якій істинна $\min(F(t))$, вона істинна на усіх її областях переходу.

Нехай $F(x_1, \ldots, x_n, y)$ — булева функція від змінних $x_1, \ldots, x_n, y$. $\exists$-*проекцією* функції $F(x_1, \ldots, x_n, y)$ на $\{x_1, \ldots, x_n\}$ називається функція, що задається формулою

$$F(x_1, \ldots, x_n, 0) \vee F(x_1, \ldots, x_n, 1) = \exists yF(x_1, \ldots, x_n, y).$$

Аналогічно, $\exists$-проекцією $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ на множину змінних $\{x_1, \ldots, x_n\}$ називається формула $\exists y_1 \ldots \exists y_m F(x_1, \ldots, x_n, y_1, \ldots, y_m)$.

Теорема 1. Функція $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ може бути подана у вигляді $F = \mathop{\&}\limits_{i=1}^{m} (y_i \leftrightarrow f_i(x_1, \ldots, x_n))$ тоді і тільки тоді, коли кожна залишкова функція у розкладі Шеннона функції F за змінними $x_1, \ldots, x_n$ є конституентою одиниці від змінних $y_1, \ldots, y_m$.

Доведення.

1. Необхідність. Нехай $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ може має вигляд $(y_1 \leftrightarrow f_1)\& \ldots \& (y_m \leftrightarrow f_m) = (y_1 f_1 \vee \neg y_1 \neg f_1)\& \ldots \&(y_m f_m \vee \neg y_m \neg f_m) = y_1 \ldots y_m f_1 \ldots f_m \vee y_1 \ldots \neg y_m f_1 \ldots \neg f_m \vee \ldots \ldots \vee \neg y_1 \ldots \neg y_m \neg f_1 \ldots \neg f_m$, де $f_1, \ldots, f_m$ — функції від змінних $x_1, \ldots, x_n$. На кожному наборі значень змінних $x_1, \ldots, x_n$ істинний тільки один із 2^m добутків вигляду $f_1 \ldots f_m$, де $f_i \in \{f_i, \neg f_i\}$. Звідси випливає, що кожна залишкова функція у розкладі $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ за змінними $x_1, \ldots, x_n$ є конституентою одиниці від змінних $y_1, \ldots, y_m$.

2. *Достатність*. Нехай $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ задовольняє умови теореми. Ці умови можна переформулювати у вигляді таких властивостей функції.

а. Досконала д.н.ф. формули $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ містить рівно 2^n конституент одиниці.

б. Кожна конституента одиниці від змінних $x_1, \ldots, x_n$ є складовою однієї і тільки однієї з конституент одиниці функції $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$.

Ці ж властивості має і кожна $\exists$-проекція формули $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ на множину змінних $\{x_1, \ldots, x_n, y_i\}$ $(i = 1, 2, .., m)$, і добуток усіх таких проекцій. Звідси випливає, що кожна проекція на $\{x_1, \ldots, x_n, y_i\}$ має вигляд $f_i(x_1, \ldots, x_n)y_i \vee \neg f_i(x_1, \ldots, x_n) \neg y_i = y_i \leftrightarrow f_i(x_1, \ldots, x_n)$. Крім того, $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ є імплікантою кожної такої проекції, отже і їхнього добутку.

Лема. Якщо $f(x_1, \ldots, x_n)$ — імпліканта функції $f'(x_1, \ldots, x_n)$ і досконалі д.н.ф. цих функцій мають однакову кількість конституент одиниці, то $f(x_1, \ldots, x_n) = f'(x_1, \ldots, x_n)$.

Із цієї леми і наведених вище властивостей функції $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$ випливає, що добуток усіх m її проекцій збігається з цією функцією.

Виходячи з тверджень1, 2 і теореми 1, нескладно показати, що будь-яка мінімальна форма специфікації, детермінованого та всюдивизначеного автомата, може бути розширена до такої еквівалентної специфікації вигляду $\forall tF(t)$, що $F(t) = \mathop{\&}\limits_{i=1}^{m} (y_i(t) \leftrightarrow f_i(t))$, де $y_1, \ldots, y_m$ — усі вихідні предикатні символи специфікації й $f_i(t)$ не залежать від атомів $y_1(t), \ldots, y_m(t)$.

Побудова такої специфікації здійснюється через довизначення формули $\min(F(t))$ на тих областях переходів, на яких вона хибна; після чого будуються формули $y_i(t) \leftrightarrow f_i(t)$ як $\exists$-проекції одержаної формули на усі атоми за винятком вихідних атомів нульового рангу, відмінних від $y_i(t)$.

Твердження 3. Специфікація будь-якого всюди визначеного детермінованого автомата може бути подана у вигляді $\forall t \mathop{\&}\limits_{i=1}^{m} (y_i(t) \leftrightarrow f_i(t))$, де $y_1, \ldots, y_m$ — усі вихідні предикатні символи специфікації й $f_i(t)$ не залежать від атомів $y_1(t), \ldots, y_m(t)$.

Така специфікація — це сукупність тверджень, що визначають необхідні і достатні умови істинності кожного вихідного предиката у довільний момент часу t, причому ці умови не залежать від значень вихідних предикатів у цей момент часу.

Твердження 4. Специфікація будь-якого детермінованого автомата може бути подана у вигляді $F(t) = = \mathop{\&}_{i=1}^{m} (y_i(t) \to g_i(t))\&(\neg y_i(t) \to h_i(t))$, де $y_1, \ldots, y_m$ — усі вихідні предикатні символи специфікації і $g_i(t)$, $h_i(t)$ не залежать від атомів $y_1(t), \ldots, y_m(t)$.

Д о в е д е н н я . Нехай автомат заданий формулою $\forall tF(t)$ з вихідними предикатними символами $y_1, \ldots, y_m$. Розглянемо m $\exists$-проекцій формули $F(t)$ на усі атоми крім вихідних атомів нульового рангу, відмінних від $y_i(t)$ ($i = 1, 2, .., m$). Якщо $F(t)$ має такий вигляд, що в кожній області переходу простору станів вона істинна не більш ніж в одному стані, тобто кожна конституента одиниці від змінних $x_1(t), \ldots, x_n(t)$ міститься тільки в одній конституенті одиниці формули $F(t)$, то кон'юнкція усіх таких $\exists$-проекцій дорівнює $F(t)$. Кожна така проекція має вигляд $y_i(t)g_i(t) \vee \neg y_i(t)h_i(t)$, що еквівалентно $(y_i(t) \to g_i(t))\&(\neg y_i(t) \to h_i(t))$, де $g_i(t)$, $h_i(t)$ не залежать від атомів $y_1(t), \ldots, y_m(t)$. Неважко показати, що $g_i(t)\&h_i(t) \equiv 0$ ($i = 1, 2, .., m$).

Виникає питання, як побудувати формули $g_i(t)$ і $h_i(t)$ у специфікації детермінованого автомата? Для відповіді проаналізуємо поняття необхідної та достатньої умови.

Необхідні та достатні умови

Якщо $\forall t(p(t) \to q(t))$, то будемо казати, що $q(t)$ — необхідна умова істинності $p(t)$, а $p(t)$ — достатня умова істинності $q(t)$. Таким чином, формули $g_i(t)$ і $h_i(t)$ у специфікації детермінованого автомата — це необхідні умови відповідно істинності та хибності предиката $y_i(t)$. Але якщо в цих формулах брати довільні необхідні умови, то здобута таким чином специфікація може не бути специфікацією потрібного автомата. Тому необхідно накласти обмеження на ці умови.

Умова $A(t)$ є необхідною умовою істинності предиката $y(t)$, якщо кожного разу, коли предикат $y(t)$ істинний, умова $A(t)$ також істинна. Якщо не існує ситуації, коли предикат $y(t)$ істинний, то $A(t) = 0$. Відповідна достатня умова $B(t)$ має задовольняти такі вимоги.

1. Кожного разу, коли умова $B(t)$ істинна, предикат $y(t)$ також істинний.
2. Якщо не існує ситуації, коли умова $B(t)$ істинна, то $B(t)$ не є достатньою умовою.
3. Якщо $B(t) = B_1(t) \vee B_2(t)$, то $B(t)$ — достатня умова тоді і тільки тоді, коли $B_1(t)$ і $B_2(t)$ — достатні умови.

Якщо як $g_i(t)$ і $h_i(t)$ взяти необхідні і достатні умови відповідно істинності та хибності предиката $y_i(t)$, то будь-яка специфікація вигляду $\forall t \mathop{\&}_{i=1}^{m} (y_i(t) \to g_i(t))\&(\neg y_i(t) \to h_i(t))$, буде специфікацією потріб-ного автомата. Довести це твердження можна, визначивши для заданого автомата A поняття істинності умови на переході та інтерпретуючи слова «кожного разу» у вимогах до необхідних та достатніх умов як «на кожному переході». Після цього можна показати, що для одержаної за цими означеннями формули специфікації F виконується $W(A) = W(\mathrm{F})$, але це виходить за межі цієї статті.

Розглянемо приклад побудови специфікації автомата з однією вхідною двійковою змінною x, та однією вихідною двійковою змінною y. Вимоги до функціонування автомата описані таким чином. Значення y у момент t дорівнює одиниці тоді і тільки тоді, коли у вхідній послідовності до моменту t включно відсутні нульові значення змінної x. Як можна бачити з цього опису, поведінка автомата детермінована і всюдивизначена. Необхідна і достатня умова істинності $y(t)$ має вигляд $y(t-1)\,\&\,x(t)$. Таким чином, специфікація цього автомата може бути записана у вигляді $\forall t(y(t) \leftrightarrow y(t-1)\,\&\,x(t))$.

Ще один приклад автомата з такими самими вхідним та вихідним алфавітами. Автомат функціонує так. Якщо x у момент t дорівнює одиниці, то y теж у цей момент дорівнює одиниці. Коли x змінюється на нуль, то з наступного після зміни моменту часу y теж буде дорівнювати нулю, доки x зміниться на одиницю. Крім того, в наступний момент часу після того, як x зміниться на одиницю, він не може дорівнювати нулю. Останнє твердження визначає частковість автомата. У цьому випадку його зручно специфікувати як всюдивизначений автомат, доповнивши цю специфікацією умовою частковості. Так специфікацію відповідного всюди визначеного автомата запишемо як $\forall t(y(t) \leftrightarrow (x(t-1) \vee x(t)))$. Справді, кожного разу, коли $y(t)$ дорівнює одиниці, умова $x(t-1) \vee x(t)$ теж дорівнює одиниці, отже це — необхідна умова. Крім того, $x(t-1)$ та $x(t)$ є достатніми умови істинності $y(t)$, тож $x(t-1) \vee x(t)$ — необхідна і достатня умова. Умова частковості має вигляд: $\forall t(\neg x(t-2)\&x(t-1) \to x(t))$.

Більш складний приклад специфікації реактивних систем можна знайти в [4].

Варто також розглянути специфікацію автомата у вигляді необхідних умов зміни (зберігання) значення вихідного сигналу (предиката). Так, твердження, що $A(t)$ є необхідною умовою зміни значення $y(t)$ з 0 на 1 має вигляд: $\forall t(\neg y(t-1)\&y(t) \to A(t))$. Виходячи з того, що специфікація детермінованого автомата може бути подана у вигляді $\forall t \mathop{\&}\limits_{i=1}^{m} (y_i(t) \to g_i(t))\&(\neg y_i(t) \to h_i(t))$, нескладно показати, що її також можна подана у вигляді $\forall t \mathop{\&}\limits_{i=1}^{m} F_i(t)$, де $F_i(t)$ — це кон'юнкція чотирьох тверджень:

$$(y_i(t-1)\&y_i(t)\to A_i(t)),\ (y_i(t-1)\&\neg y_i(t)\to B_i(t)),\ (\neg y_i(t-1)\&y_i(t)\to C_i(t)),\ (\neg y_i(t-1)\&\neg y_i(t)\to D_i(t)).$$

У такому поданні специфікації формули $A_i(t)$, $B_i(t)$, $C_i(t)$, $D_i(t)$ не залежить від $y_j(t)$ (j = 1, 2, .., m) та $y_i(t–1)$, тобто не містять у собі цих атомів. Щоб перейти від цієї форми специфікації до попередньої, треба покласти $g_i(t) = y_i(t-1)\&A_i(t) \vee \neg y_i(t-1)\&C_i(t)$, $h_i(t) = y_i(t-1)\&B_i(t) \vee \neg y_i(t-1)\&D_i(t)$.

Розглянемо, як для першого прикладу побудувати таку специфікацію. Запишемо специфікацію цього автомата у вигляді $\forall t(y(t)\to y(t-1)\& x(t))\&(\neg y(t)\to(\neg y(t-1) \vee \neg x(t)))$.

Таким чином, $y(t–1)\&x(t) = y(t–1)\&A(t) \vee \neg y(t–1)\&C(t)$, а $(\neg y(t–1) \vee \neg x(t)) = y(t–1)\&B(t) \vee \neg y(t–1)\&D(t)$. Звідси знаходимо такі значення для $A(t)$, $B(t)$, $C(t)$ і $D(t)$: $A(t) = x(t)$, $B(t) = \neg x(t)$, $C(t) = 0$, $D(t) = 1$.

Зауважимо, що оскільки $g_i(t)$ і $h_i(t)$ — необхідні і достатні умови істинності $y_i(t)$ і $\neg y_i(t)$ відповідно, то $y_i(t-1)\&A_i(t)$, $\neg y_i(t-1)\&C_i(t)$, $y_i(t-1)\&B_i(t)$ і $\neg y_i(t-1)\&D_i(t)$ є необхідними і достатніми умовами істинності $y_i(t-1)\&y_i(t)$, $\neg y_i(t-1)\&y_i(t)$ тощо. Справді, враховуючи, що $y_i(t) \leftrightarrow g_i(t)$, а $\neg y_i(t) \leftrightarrow h_i(t)$, можна записати $y_i(t) \leftrightarrow (y_i(t-1)\&A_i(t) \vee \neg y_i(t-1)\&C_i(t))$, $\neg y_i(t) \leftrightarrow (y(t-1)\&B(t) \vee \neg y(t-1)\&D(t))$. Помноживши обидві частини цих еквівалентностей на $y_i(t-1)$ або $\neg y_i(t-1)$, одержимо $y_i(t-1)\&y_i(t) \leftrightarrow \leftrightarrow y_i(t-1)\&A_i(t)$, $\neg y_i(t-1)\&y_i(t) \leftrightarrow \neg y_i(t-1)\&C_i(t)$ і т.п. Оскільки умови $A_i(t)$, $B_i(t)$, тощо, простіші за умови $g_i(t)$ і $h_i(t)$, то зазвичай така форма подання специфікації більш зручна для її побудови.

Висновки

У праці показано, що для побудови специфікації детермінованого автомата можна використовувати деякі стандартні форми відповідної формули, яка задовольняє певні вимоги. Для визначення основних складових підформул такої специфікації використовується поняття необхідної і достатньої умови істинності вихідного предиката або його заперечення. У разі специфікації часткового автомата можна використовувати не будь-яку необхідну і достатню умову. Важливе обмеження на таку умову полягає у тому, що для будь-якого подання її у вигляді диз'юнкції умов кожна з них має бути достатньою умовою. Як показано у другому прикладі, специфікацію часткового автомата іноді зручно будувати у вигляді кон'юнкції $F_1\&F_2$, де F_1 — специфікація всюдивизначеного автомата, а F_2 — специфікація умови частковості. Умови частковості — це вимоги до функціонування оточення, з яким взаємодіє автомат. Якщо оточення розглядається як детермінований автомат, то умови частковості можна записати у вигляді $\forall t \mathop{\&}\limits_{i=1}^{m} (x_i(t) \to \alpha_i(t))\&(\neg x_i(t) \to \beta_i(t))$, де x_i — вхідні предикатні символи, а формули $\alpha_i(t)$ і $\beta_i(t)$ не залежать від атомів нульового рангу.

Використання стандартної форми подання специфікації, яка задовольняє певні вимоги, полегшує написання специфікації і зменшує можливість допущення помилок.

ЛІТЕРАТУРА

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