УДК 004.423

КОМПОЗИЦИОННАЯ СЕМАНТИКА ПОДСТАНОВОК В МЕТОДА

Буй Дмитрий, Колегаев Алексей

Киевский национальный университет имени Тараса Шевченко

Аннотация

В статье рассмотрены понятия подстановки и слабейшего предусловия, применяемые при построении абстрактных моделей в B методе, являющемся популярным формальным методом разработки программ. Указана формализация этих понятий на основе композиционного подхода.

Abstract

The article describes concepts of substitution and the weakest precondition used in the construction of abstract models in the B method, which is a popular method of formal development of programs. Formalization of these concepts on the basis of compositional approach are considered.

Введение

В метод – формальный метод разработки программ, включающий в себя весь цикл создания программы: от абстрактной модели, реализуемой с помощью языка AMN (Abstract Machine Notation), до получения готового программного кода. Ключевым понятием B метода, описание которого Жан-Раймонд Абриал (Jean-Raymond Abrial) предоставил в [1], является подстановка (substitution). Идея подстановки предложена в работе Хоара [2], в которой также было введено понятие тройки Хоара $P\{Q\}R$, где P (предусловие) и R (постусловие) являются предикатами, а Q – командой. Интерпретация тройки Хоара такова: если команда Q выполняется при условии P, то предикат R обращается в истину после выполнения команды Q. Описанная позже Дейкстрой в [3] модель «языка охраняемых команд» предусматривала введение понятия «слабейшего предусловия» (weakest precondition, $wp(Q,R)$), которое базировалось на терминологии троек Хоара. Предикат $wp(Q,R)$ принимает значение $true$ на всех тех и только тех начальных состояниях, для которых запуск команды Q обязательно приведёт к корректному завершению и при этом система перейдет в заключительное состояние, удовлетворяющее постусловию R. С помощью композиционного подхода (см., например, [4, 5]) в этой работе уточняются указанные выше основополагающие понятия B метода.

Обозначения и терминология композиционного подхода

В рамках композиционного подхода рассматриваются множество имён V и множество исходных денотатов Σ. Элементы множества Σ^V будем называть состояниями (памяти). Здесь $\Sigma^V = \{\alpha \mid \exists V'(V' \in 2^V \wedge \alpha : V' \to \Sigma)\}$ – множество всех конечных функций из V в Σ, а $2^V = \{V' \mid V' \subseteq V \wedge V' - конечно\}$ – множество всех конечных подмножеств множества V.

Рассмотрим две операции: разыменования $v \Rightarrow : \Sigma^V \xrightarrow{\sim} \Sigma^V$ и наложения $\nabla : \Sigma^V \times \Sigma^V \to \Sigma^V$, определяемые следующим образом:

$$v \Rightarrow (\alpha) \stackrel{def}{\simeq} \alpha(v);\ \alpha \nabla \beta \stackrel{def}{=} \beta \cup (\alpha \mid (\mathrm{dom}\,\alpha \setminus \mathrm{dom}\,\beta)), \alpha, \beta \in \Sigma^V.$$

Здесь и далее символ $\xrightarrow{\sim}$ используется для записи частичных функций; символ $\simeq$ означает обобщенное равенство; а $\mathrm{dom}\,\alpha$ – область определенности функции α.

Композиционная семантика для записи частичных функций в виде термов

Рассмотрим частичную алгебраическую систему $\langle \Sigma, \Omega_F, \Omega_P \rangle$, носителем которой является Σ, а Ω_F и Ω_P – множества, вообще говоря, частичных функций и предикатов, определённых на множестве Σ.

Для записи функций будем использовать конструкции формального языка, предложенного А.И. Мальцевым в [6], а для записи предикатов – правила, указанные Ж.-Р. Абриалем в [1, с. 715]. В роли предметных символов (точнее говоря, переменных) используем элементы множества имён V.

Под значением предметного символа v на состоянии $\alpha \in \Sigma^V$ будем понимать значение функции $v \Rightarrow (\alpha)$. Под значением функции, представленной термом $f(v_1,...,v_n)$, на состоянии $\alpha \in \Sigma^V$ будем понимать значение данной функции на кортеже $\langle v_1 \Rightarrow (\alpha),..., v_n \Rightarrow (\alpha) \rangle$. Аналогично определяем и значение предиката, представленного термом $p(v_1,...,v_n)$, на состоянии α.

Пусть терм t имеет вид $f_j^{n_j}(\lambda_1,...,\lambda_{n_j})$, где $f_j^{n_j}$ – n_j-арный функциональный символ, а λ_1, …, λ_{n_j} – термы меньшей длины. Если значения термов λ_1, …, λ_{n_j} определены на некотором состоянии α и равны соответственно элементам σ_1, … , σ_{n_j} множества Σ, то значение операции $f_j^{n_j}$ в точке $\langle \sigma_1,..., \sigma_{n_j} \rangle$ будет значением терма t на состоянии α, которое обозначим как $t(\alpha)$.

С каждым преобразованием, выполняемым командой Q в тройке Хоара $P\{Q\}R$, сопоставим частичную функцию на состояниях $f_Q : \Sigma^V \tilde{\to} \Sigma^V$

$$f_Q \overset{def}{=} \left\{ \langle \alpha_1, \alpha_2 \rangle \middle| \alpha_1, \alpha_2 \in D^V \wedge \alpha_1 \{Q\} \alpha_2 \right\}.$$

Функция f_Q задает семантику команды Q. Пусть задан предикат постусловия R. В терминах полных прообразов определим следующее множество состояний:

$$M(Q,R) \overset{def}{=} f_Q^{-1}(R^{-1}True). \tag{1}$$

Очевидно, что множество $M(Q,R)$ состоит из тех и только тех начальных состояний, для которых выполнение команды Q завершится заключительным состоянием, обеспечивающим истинность постусловия R. Множество M и является областью истинности предиката $wp(Q,R)$, тем самым задавая семантику слабейшего предусловия.

Композиционная семантика подстановок и слабейших предусловий присваиваний

Рассмотрим слабейшее предусловие $wp(Q,R)$, где Q – операция присваивания $v := t$. Семантика операции (команды) присваивания задается функцией $g : \Sigma^V \tilde{\to} \Sigma^V$

$$g(\alpha)_{v;t} \overset{def}{\simeq} \alpha \nabla \{ \langle v, t(\alpha) \rangle \}. \tag{2}$$

Перейдем к синтаксическим аспектам. Если предикат постусловия R представлен термом R^* над переменными программы, то, используя обозначения [7], получим запись терма предусловия $wp^*(v := t, R^*)$:

$$wp^*\left(v := t, R^*\right) = R_v^*[t], \tag{3}$$

где $R_v^*[t]$ обозначает терм, полученный из терма R^* заменой всех (свободных) вхождений переменной v термом t.

Аналогично, запишем также слабейшее предусловие для множественной подстановки (группового оператора присваивания), которая имеет вид

$$v_1 := t_1, v_2 := t_2, ..., v_n := t_n.$$

Семантика множественного присваивания задается функцией $\bar{g} : \Sigma^V \xrightarrow{\sim} \Sigma^V$

$$\bar{g}(\alpha)_{v_1,...v_n;\, t_1,...t_n} \overset{def}{\simeq} \alpha\nabla\left\{\left\langle v_1, t_1(\alpha)\right\rangle, \left\langle v_2, t_2(\alpha)\right\rangle, ..., \left\langle v_n, t_n(\alpha)\right\rangle\right\}. \tag{4}$$

Соответственно, терм, представляющий предикат слабейшего предусловия этой операции, таков:

$$wp^*\left(v_1 := t_1, v_2 := t_2, ..., v_n := t_n; R^*\right) = R^*_{v_1,..., v_n}[t_1, ..., t_2]. \tag{5}$$

Предложение (основной результат).

Семантика слабейшего предусловия для общего случая задается выражением (1); семантика присваивания и множественного присваивания – выражениями (2), (4) соответственно; синтаксический аспект слабейших предусловий для присваиваний и множественных присваиваний задан выражениями (3), (5) соответственно. □

Выводы

В работе предложена формализация подстановок B-метода, которая позволяет применить аппарат композиционного подхода для проверки и создания абстрактных моделей. С помощью указанных конструкций подлежат уточнению слабейшие предусловия конструкций AMN, которые используются для непосредственного создания абстрактных моделей. Помимо классического B метода данная формализация может быть применена и к Event-B [8].

Следующим этапом работы является уточнение основных управляющих конструкций: последовательного применения, ветвления и циклирования.

Список использованных источников:

1. Abrial J.-R. The B Book: Assigning Programs to Meanings / J.-R. Abrial // Cambridge University Press, 1996. – 816 p. – *ISBN* 978-0-521-02175-3.

2. Hoare C.A.R. An axiomatic basis for computer programming / C.A.R. Hoare // Communications of the ACM. – 1969. – Vol. 12. – P.576-583.

3. Дейкстра Э. Дисциплина программирования: [пер. с англ.] / Э. Дейкстра. – М.: Мир, 1978. – 274 с.

4. Редько В.Н. Композиции программ и композиционное программирование // Программирование. – 1978. – № 5. – С. 3-24.

5. Буй Д. Б., Губский Б. В., Редько В. Н. Проблемы полноты в классах вычислимых именных функций // Кибернетика. – 1988. – № 4. – С. 58-65.

6. Мальцев А. И. Алгоритмы и рекурсивные функции / А. И. Мальцев. – Москва: Наука, 1986. – 368 с.

7. Шенфилд Дж. Математическая логика: [пер. с англ.] / Дж. Шенфилд. – М.: Наука, 1975. – 528 стр.

8. Abrial J.-R. Modeling in Event-B System and Software Engineering / J.-R. Abrial // Cambridge University Press, 2010. – 612 p. – *ISBN* 978-0-521-89556-9.