МНОГОСОРТНАЯ МОНОТОННАЯ ЛОГИКА ФЛОЙДА-ХОАРА

Андрей Криволап, Николай Никитченко

***Аннотация**: Рассматривается проблема построения монотонной логики Флойда-Хоара, которая является расширением классической логики Флойда-Хоара для случая частичных предикатов. Обобщается построенная монотонная логика на случай многосортных логик. Для этого вводятся номинативные данные с типами. Доказывается монотонность композиций представленной логики, а также непрерывность композиции Флойда-Хоара.*

***Ключевые слова**: программные логики, композиционно-номинативный подход, монотонные композиции, типизированные данные.*

***ACM Classification Keywords**: F.3.1 Specifying and Verifying and Reasoning about Programs – Logics of Programs*

Введение

Верификация является одним из основных этапов разработки программного обеспечения, важность которого нельзя недооценивать. Логика Флойда-Хоара [Floyd, 1967; Hoare, 1969] широко применяется в формальной верификации, поэтому ее исследование и расширение представляет большой интерес. Среди расширений можно выделить логику разделения [Reynolds, 2002] в которой вводятся понятия указателя и новый тип импликации.

Одним из возможных подходов к обобщению логики Флойда-Хоара является переход к частичным квазиарным предикатам над номинативными данными. Использование таких предикатов позволит более адекватно описывать свойства программ и вести рассуждения, ведь в программах мы работаем с именами переменных, присваивая им значения, или оперируя с их значениями.

В случае использования частичных предикатов, все композиции должны быть монотонны в том понимании, что если одна из компонент композиции становиться определенной на новых данных, то если композиция уже была определена на этих данных, ее значение не должно измениться. Таким образом, можно доказывать утверждения для частей программы, и быть уверенными, что они будут истинными и для программы в целом. Логика Флойда-Хоара в классическом определении не монотонна при расширении на частичные квазиарные предикаты, так как композиция Флойда-Хоара не будет монотонной. Монотонный вариант композиции был определен в [Никитченко, Криволап, 2002], где также были исследованы проблемы, возникающие при построении правил вывода.

Так как переменные в программах имеют не только определенные имена, но и типы, возникает проблема перехода от монотонной логики Флойда-Хоара, где значения все переменных принадлежат одному множеству, к многосортной монотонной логике Флойда-Хоара, в которой с каждой переменной ассоциируется определенный тип. Такое обобщение проводится согласно подходу, предложенному в [Nikitchenko, Tymofieiev, 2013]. После чего нужно показать, что композиции полученной логики будут также обладать необходимым свойством монотонности.

Алгебры квазиарных предикатов и функций над типизированными номинативными множествами

Чтобы задать многосортную монотонную логику Флойда-Хоара, будем использовать семантико-синтаксический подход. Для этого сначала зададим семантическую часть в виде алгебр квазиарных предикатов, функций и биквазиарных функций. На основе соответствующих алгебр определим синтаксис в виде языка, композиционные символы которого будут представлять композиции в алгебрах. Таким образом, семантика задает синтаксис. Третьей составляющей будет интерпретация, которая формулам и термам языка будет сопоставлять предикаты и функции соответствующих алгебр.

Для того чтобы говорить про алгебры квазиарных предикатов и функции, определим сначала понятия типизированного номинативного множества, квазиарного предиката, квазиарной функции, биквазиарной функции.

Пускай V – множество имен, T – класс типов, а $\tau : V \to T$ – тотальное отображение, которое задает типы переменных.

Если задано V, T и τ, то класс типизированных номинативных множеств (обозначим $NST(V,T,\tau)$, или если множества V и T фиксированные, то $NST(\tau)$) задается следующей формулой:

$$NST(\tau) = \{d : V \to \bigcup_{A \in T} A \mid \forall v \in V(d(v)\downarrow \Rightarrow d(v) \in \tau(v))\}$$

Тут d – частичное отображение, которое именам переменных ставит в соответствие их значения, которые должны принадлежать типам соответствующих переменных. Другими словами можно сказать, что номинативное множество задает состояние переменных, для которых определен их тип. Будем представлять d в следующем виде: $d = [v_i \mapsto a_i \mid i \in I]$, что обозначает, что переменная v_i имеет значение a_i. При помощи $d(v)\uparrow$ будем обозначать, что значение переменной v не определено в номинативном множестве d. При помощи же $d(v)\downarrow$, что определено, аналогично $d(v)\downarrow = a$ обозначает, что значение переменной v определено в номинативном множестве d и равно a.

Пусть $Bool = \{F,T\}$ – множество истинных значений. Рассмотрим множество $Pr(V,T,\tau) : NST(V,T,\tau) \to Bool$ частичных предикатов над типизированными номинативными данными. Будем обозначать его $Pr(\tau)$ если V,T – зафиксированы. Тогда все предикаты из $Pr(\tau)$ будем называть многосортными частичными квазиарными предикатами.

Аналогичным образом определим многосортные квазиарные и многосортные биквазиарные функции.

Пусть $A \in T$ – множество значений принадлежащих одному из типов класса T. Рассмотрим множество $Fn^A(V,T,\tau) : NST(V,T,\tau) \to A$ частичных функций над типизированными номинативными данными. Будем обозначать соответственно $Fn^A(\tau)$ если V,T – зафиксированы. Тогда все функции из $Fn^A(\tau)$ для некоторого типа $A \in T$ будем называть многосортными частичными квазиарными функциями с типом A.

Рассмотрим множество $FPrg(V,T,\tau) : NST(V,T,\tau) \to NST(V,T,\tau)$ частичных функций над типизированными номинативными данными. Если V,T – зафиксированы будем обозначать это множество $FPrg(\tau)$. Функции из $FPrg(\tau)$ будем называть многосортными частичными биквазиарными функциями, или многосортными частичными программными функциями. Если номинативные множества понимать как состояние значений переменных, то биквазиарная функция, которая принимает на вход

одно состояние переменных и выдает результат определенных преобразований переменных в виде состояния, может трактоваться как формальное представление интуитивного понятия программы.

Далее постепенно определим алгебры трех уровней:

- Алгебра с единственной основой $Pr(V,T,\tau)$, которая представляет семантику многосортной логики чистых квазиарных предикатов.
- Алгебра с основами $Pr(V,T,\tau)$ и $Fn^A(V,T,\tau)$ для всех $A \in T$, она задает семантику многосортной квазиарной предикатно-функциональной логики.
- Алгебра с основами $Pr(V,T,\tau)$, $Fn^A(V,T,\tau)$ для всех $A \in T$ и $FPrg(V,T,\tau)$ для задания многосортных программных логик, одной из которых является многосортная монотонная логика Флойда-Хоара.

Операции в соответствующих алгебрах будем называть композициями. Рассмотрим алгебру на первом уровне. Тогда можно выделить такие композиции над $Pr(V,T,\tau)$, как $C_{Pr}(V,T,\tau) = \{\vee, \neg, R^{\bar{v}}_{\bar{x}}, \exists x, =_{xy}\}$. Они определяются следующим образом, где $p(\mathrm{d})\downarrow = T$ обозначает, что предикат $p \in Pr(\tau)$ определен на состоянии d и равен T, аналогично $p(\mathrm{d})\downarrow = F$, а $p(\mathrm{d})\uparrow$ обозначает, что предикат $p \in Pr(\tau)$ не определен на состоянии d.

Бинарная композиция дизъюнкции $\vee : Pr(\tau) \times Pr(\tau) \to Pr(\tau)$:

$$p \vee q(d) = \begin{cases} T, \text{если } p(d)\downarrow = T \text{ или } q(d)\downarrow = T \\ F, \text{если } p(d)\downarrow = F \text{ и } q(d)\downarrow = F \\ \perp, \text{иначе} \end{cases}$$

Унарная композиция отрицания $\neg : Pr(\tau) \to Pr(\tau)$:

$$\neg p(d) = \begin{cases} T, \text{если } p(d)\downarrow = F \\ F, \text{если } p(d)\downarrow = T \\ \perp, \text{иначе} \end{cases}$$

Унарная параметрическая композиция реноминации $R^{v_1,v_2,\ldots,v_n}_{x_1,x_2,\ldots,x_n} : Pr(\tau) \to Pr(\tau)$, где $x_1, x_2, \ldots, x_n, v_1, v_2, \ldots, v_n \in V$ – имена переменных таких, что $v_1, v_2, \ldots, v_n$ – различные имена, и $\tau(v_1) = \tau(x_1), \tau(v_2) = \tau(x_2), \ldots, \tau(v_n) = \tau(x_n)$, тогда:

$$R^{v_1,v_2,\ldots,v_n}_{x_1,x_2,\ldots,x_n} p(d) = p([v \mapsto a \in d \mid v \notin \{v_1, v_2, \ldots, v_n\}] \nabla [v_i \mapsto d(x_i) \mid d(x_i)\downarrow, i = \overline{1,n}])$$

Операция накладки $\nabla : NST(\tau) \times NST(\tau) \to NST(\tau)$ определяется на номинативных множествах следующим образом:

$$d_1 \nabla d_2(v) = \begin{cases} d_1(v), \text{если } d_1(v)\downarrow \text{ и } d_2(v)\uparrow \\ d_2(v), \text{если } d_2(v)\downarrow \\ \perp, \text{иначе} \end{cases}$$

Унарная параметрическая композиция квантификации существования $\exists x : Pr(\tau) \to Pr(\tau)$ с параметром $x \in V$:

$$\exists x\, p(d) = \begin{cases} T, \text{если существует } a \in \tau(x) : p(d\nabla[x \mapsto a])\downarrow = T \\ F, \text{если для каждого } a \in \tau(x) : p(d\nabla[x \mapsto a])\downarrow = F \\ \perp, \text{иначе} \end{cases}$$

Нуль-арная композиция равенства $=_{xy} : Pr(\tau)$ с параметрами $x, y \in V$, такими, что $\tau(x) = \tau(y)$:

$$=_{xy}(d) = \begin{cases} T, \text{если } x(d)\downarrow, y(d)\downarrow u\ x(d) = y(d) \\ \text{F}, \text{если } x(d)\downarrow, y(d)\downarrow u\ x(d) \neq y(d) \\ \perp, \text{иначе} \end{cases}$$

Определив все композиции, получаем алгебру для логики чистых квазиарных предикатов. Будем в дальнейшем называть пару $< Pr(V,T,\tau), C_{Pr}(V,T,\tau) >$ многосортной алгеброй квазиарных предикатов.

Рассмотрим алгебру на втором уровне. В данном случае основами будут множества $Pr(V,T,\tau)$ и $Fn^A(V,T,\tau)$ для всех $A \in T$ и к определенным ранее композициям добавляются композиции над квазиарными функциями, такие как суперпозиция, деноминация, тогда композицию реноминации можно выразить через суперпозицию и разыменование, а параметрическая унарная композиция равенства заменяется бинарной композицией, аргументами которой являются две функции, а параметром их тип. Таким образом, множество композиций будет таким $C_{Fn}(V,T,\tau) = \{\vee, \neg, S^{\bar{v}}, \exists x, =_A, `x\}$. Композицию суперпозиции будем определять как строгую суперпозицию, в которой если значения хоть одной функции на состоянии не будет определенным, то и результат композиции будет неопределенным. На самом деле, для многосортных квазиарных функций и предикатов возникает целый класс суперпозиций. Их параметром будет тип результата, который возвращает первая функция, в которую и производиться подстановка. Для простоты мы будем использовать одну общую суперпозицию, заданную для всех типов квазиарных функций одновременно. Далее определим лишь новые композиции.

N-арная параметрическая композиция суперпозиции $S^{v_1,v_2,\ldots,v_n} : (\bigcup_{A\in T} Fn^A(\tau) \cup Pr(\tau)) \times$

$\times Fn^{\tau(v_1)}(\tau) \times \ldots \times Fn^{\tau(v_n)}(\tau) \to \bigcup_{A\in T} Fn^A(\tau) \cup Pr(\tau)$, где $v_1, v_2, \ldots, v_n \in V$ – имена переменных таких, что $v_1, v_2, \ldots, v_n$ – различные имена, тогда:

$$S^{v_1,v_2,\ldots,v_n}(f, g_1, g_2, \ldots, g_n)(d) = \begin{cases} f(d\nabla[v_i \mapsto g_i(d) \mid i = \overline{1,n}]), \text{если } g_i(d)\downarrow \text{ для всех } i \in \{1,\ldots n\} \\ \perp, \text{иначе} \end{cases}$$

Бинарная параметрическая композиция равенства $=_A : Fn^A(\tau) \times Fn^A(\tau) \to Pr(\tau)$ с параметром $A \in T$:

$$(f =_A \text{g})(d) = \begin{cases} T, \text{если } f(d)\downarrow, \text{g}(d)\downarrow u\ f(d) = g(d) \\ \text{F}, \text{если } f(d)\downarrow, \text{g}(d)\downarrow u\ f(d) \neq g(d) \\ \perp, \text{иначе} \end{cases}$$

Нуль-арная композиция деноминации $`x : Fn^{\tau(x)}(\tau)$ с параметром $x \in V$:

$$`x(d) = \begin{cases} x(d), \text{если } x(d)\downarrow \\ \perp, \text{иначе} \end{cases}$$

Покажем, что реноминация и унарное равенство выражается через новые композиции.

$$R^{v_1,v_2,\ldots,v_n}_{x_1,x_2,\ldots,x_n} p = S^{v_1,v_2,\ldots,v_n}(p, `x_1, `x_2, \ldots, `x_n)$$

$$=_{xy}(d) = (\grave{}x =_{\tau(x)} \grave{}y)(d)$$

Определив все композиции, получаем алгебру для многосортной квазиарной предикатно-функциональной логики. Будем в дальнейшем называть кортеж $< Pr(V,T,\tau), \{Fn^A(V,T,\tau) \mid A \in T\}, C_{Fn}(V,T,\tau) >$ многосортной алгеброй квазиарных предикатов и функций.

Рассмотрим алгебру на третьем уровне. В данном случае основами будут множества $Pr(V,T,\tau)$, $Fn^A(V,T,\tau)$ для всех $A \in T$ и $FPrg(V,T,\tau)$. Уровень программных логик более широк, чем два предыдущих, можно вводить различные композиции над биквазиарными функциями, получая разные логики. Ограничимся одним из простейших случаев и введем композиции присваивания, условную композицию, композицию последовательного исполнения, композицию цикла и композицию тождественной программы. Также возможно ввести специальные композиции, которые позволили бы получать предикаты, при помощи которых можно вести рассуждения о свойствах программ. Одной из таких специальных композиций является композиция Флойда-Хоара. Таким образом, множество композиций будет таким: $C_{FPrg}(V,T,\tau) = \{\vee, \neg, S^{\bar{v}}, \exists x, =_A, \grave{}x, AS^x, IF, \bullet, WH, id, FH\}$. Далее определим новые композиции.

Унарная параметрическая композиция присваивания $AS^x : Fn^{\tau(x)}(\tau) \to FPrg(\tau)$, где $x \in V$ – имя переменной, тогда:

$$(AS^x\ f)(d) = \begin{cases} d\nabla[x \mapsto f(d)]), \text{если } f(d)\downarrow \\ \perp, \text{иначе} \end{cases}$$

Тернарная условная композиция $IF : Pr(\tau) \times FPrg(\tau) \times FPrg(\tau) \to FPrg(\tau)$:

$$IF(b,f,g)(d) = \begin{cases} f(d), \text{если } b(d)\downarrow = T \text{ и } f(d)\downarrow \\ g(d), \text{если } b(d)\downarrow = F \text{ и } g(d)\downarrow \\ \perp, \text{иначе} \end{cases}$$

Бинарная композиция последовательного исполнения $\bullet : FPrg(\tau) \times FPrg(\tau) \to FPrg(\tau)$:

$$f \bullet g(d) = g(f(d))$$

Бинарная композиция цикла $WH : Pr(\tau) \times FPrg(\tau) \to FPrg(\tau)$:

$$WH(b,f)(d) = \begin{cases} d_n, \text{если существуют } d_0, d_1, \ldots, d_n, \text{что } d_0 = d, f(d_0)\downarrow, d_1 = f(d_0), \ldots, f(d_{n-1})\downarrow, d_n = f(d_{n-1}), \\ b(d_0)\downarrow = T, \ldots, b(d_{n-1})\downarrow = T, b(d_n)\downarrow = F \\ \perp, \text{иначе} \end{cases}$$

Тернарная композиция Флойда-Хоара $WH : Pr(\tau) \times FPrg(\tau) \times Pr(\tau) \to Pr(\tau)$:

$$FH(p,prg,q)(d) = \begin{cases} T, \text{если } p(d)\downarrow = F \text{ или } prg(d)\downarrow \text{ и } q(prg(d))\downarrow = T \\ F, \text{если } p(d)\downarrow = T \text{ и } prg(d)\downarrow \text{ и } q(prg(d))\downarrow = F \\ \perp, \text{иначе} \end{cases}$$

Нуль-арная композиция тождественной программы $id : FPrg(\tau)$:

$$id(d) = d$$

Определив все композиции, получаем алгебру для многосортной квазиарной логики Флойда-Хоара. Будем в дальнейшем называть кортеж $< Pr(V,T,\tau),\{Fn^A(V,T,\tau) \mid A \in T\},FPrg(V,T,\tau),C_{FPrg}(V,T,\tau) >$ многосортной алгеброй квазиарных предикатов, функций и биквазиарных функций.

Стоит отметить, что параметрические композиции можно рассматривать как классы композиций, которые мы получаем, подставляя конкретные значения параметров.

Язык многосортной логики Флойда-Хоара

Синтаксис многосортной логики Флойда-Хоара зададим, описав ее язык, определив правила по которым строятся формулы, термы и программные тексты языка.

Пускай S – множество сортов, $\xi : V \to S$ – тотальное отображение, которое каждому имени переменной ставит в соответствие ее сорт. Тогда тройку $\Sigma^S = (V,S,\xi)$ будем называть сигнатурой задания сортов.

Множество композиционных символов будем обозначать $Cs(\Sigma^S)$. Композиционные символы представляют композиции алгебр, при помощи которых определяется семантика программной логики. Для удобства будем использовать такие же обозначения, как и в соответствующих алгебрах, и считать, что для каждого композиционного символа неявно заданы сорта его аргументов. Таким образом $Cs(\Sigma^S) = \{\vee,\neg,S^{\bar{v}},\exists x,=_A,`x,AS^x,IF,\bullet,WH,id,\{\}\{\}\}$, где $\{\}\{\}$ - композиционные символы, отвечающие за запись троек Хоара $\{p\}f\{q\}$.

Пусть Ps – множество предикатных символов, Fs – множество функциональных символов, $Prgs$ – множество программных символов, причем для функциональных символов задан их сорт при помощи тотального отображения $\zeta : Fs \to S$. Тогда кортеж $\Sigma^L = (\Sigma^S, Cs(\Sigma^S), Ps, Fs, Prgs, \zeta)$ будем называть сигнатурой языка. Имея сигнатуру, мы можем индуктивно задать язык логики как множество формул $Fr(\Sigma^L)$, термов $Tr(\Sigma^L)$ и программных текстов $Pt(\Sigma^L)$ а так же множество специальных формул, троек Хоара $FHFr(\Sigma^L)$. Для того чтобы это сделать, введем дополнительные обозначения: тотальное отображение $\psi : Tr(\Sigma^L) \to S$, которое каждому терму приписывает его сорт.

Сначала определим термы:

- если $F \in Fs$, то $F \in Tr(\Sigma^L)$ и $\psi(F) = \zeta(F)$
- если $v \in V$, то $`v \in Tr(\Sigma^L)$ и $\psi(`v) = \xi(v)$
- если $F \in Fs$, $t_1,t_2,\ldots,t_n \in Tr(\Sigma^L)$ и $v_1,v_2,\ldots,v_n \in V$ – разные переменные, причем их сорта и сорта термов совпадают $\psi(t_1) = \xi(v_1),\psi(t_2) = \xi(v_2),\ldots,\psi(t_n) = \xi(v_n)$, то $S^{v_1,v_2,\ldots,v_n}(F,t_1,t_2,\ldots,t_n) \in Tr(\Sigma^L)$ и $\psi(S^{v_1,v_2,\ldots,v_n}(F,t_1,t_2,\ldots,t_n)) = \zeta(F)$

Определим формулы:

- если $P \in Ps$, то $P \in Fr(\Sigma^L)$
- если $\Phi \in Fr(\Sigma^L)$, то $\neg\Phi \in Fr(\Sigma^L)$
- если $\Phi \in Fr(\Sigma^L)$ и $v \in V$,то $\exists v\Phi \in Fr(\Sigma^L)$
- если $\Phi,\Psi \in Fr(\Sigma^L)$, то $\Phi \vee \Psi \in Fr(\Sigma^L)$

- если $P \in Ps$, $t_1, t_2, \ldots, t_n \in Tr(\Sigma^L)$ и $v_1, v_2, \ldots, v_n \in V$ – разные переменные, причем их сорта и сорта термов совпадают $\psi(t_1) = \xi(v_1), \psi(t_2) = \xi(v_2), \ldots, \psi(t_n) = \xi(v_n)$, то $S^{v_1, v_2, \ldots, v_n}(P, t_1, t_2, \ldots, t_n) \in Fr(\Sigma^L)$
- если $t_1, t_2 \in Tr(\Sigma^L)$ и $\psi(t_1) = \psi(t_2) = s$, то $t_1 =_S t_2 \in Fr(\Sigma^L)$

Определим программные тексты:

- $id \in Pt(\Sigma^L)$
- если $Pr \in Prgs$, то $Pr \in Pt(\Sigma^L)$
- если $T \in Tr(\Sigma^L)$, $v \in V$ и $\psi(T) = \xi(v)$, то $AS^v(T) \in Pt(\Sigma^L)$
- если $P, Q \in Pt(\Sigma^L)$, то $P \bullet Q \in Pt(\Sigma^L)$
- если $P, Q \in Pt(\Sigma^L)$, $F \in Fr(\Sigma^L)$ то $IF(F, P, Q) \in Pt(\Sigma^L)$
- если $P \in Pt(\Sigma^L)$, $F \in Fr(\Sigma^L)$ то $WH(F, P) \in Pt(\Sigma^L)$

Если $f \in Pt(\Sigma^L)$, $p, q \in Fr(\Sigma^L)$, то $\{p\}f\{q\} \in FHFr(\Sigma^L)$.

После того, как был определен язык логики, необходимо дать определение интерпретации. Обозначим $I^S : S \to T$ – отображение интерпретации сортов. Тогда имея отображение ξ, мы можем определить $\tau = I^S \circ \xi$ – отображение задающее типы, и соответственно алгебру $< Pr(V, T, \tau), \{Fn^A(V, T, \tau) \mid A \in T\}, FPrg(V, T, \tau), C_{FPrg}(V, T, \tau) >$. Также нам нужна дополнительно интерпретация предикатных символов $I^{Ps} : Ps \to Pr(\tau)$, интерпретация функциональных символов $I^{Fs} : Fs \to \bigcup_{A \in T} Fn^A(\tau)$, интерпретация программных символов $I^{Prgs} : Prgs \to FPrg(\tau)$. Интерпретация композиционных символов задается определением композиций, поэтому не выделяется явно. Кортеж $(\Sigma^S, I^{Ps}, I^{Fs}, I^{Prgs})$ будем называть интерпретацией языка. Теперь индукцией по построению формул, термов, программных текстов и троек Хоара, можно задать интерпретацию всех элементов языка: $J : Fr(\Sigma^L) \cup Tr(\Sigma^L) \cup FHFr(\Sigma^L) \cup Pt(\Sigma^L) \to Pr(\tau) \cup \bigcup_{A \in T} Fn^A(\tau) \cup FPrg(\tau)$.

- для всех $F \in Fs$, $J(F) = I^{Fs}(F)$
- для всех $P \in Ps$, $J(P) = I^{Ps}(\mathrm{P})$
- для всех $v \in V$, $J(\grave{v}) = \grave{v}$
- $J(id) = id$
- для всех $Pr \in Prs$, $J(Pr) = I^{Prs}(Pr)$
- $J(\neg\Phi) = \neg J(\Phi)$
- $J(\exists v \Phi) = \exists v J(\Phi)$
- $J(\Phi \vee \Psi) = J(\Phi) \vee J(\Psi)$
- $J(t_1 =_S t_2) = (J(t_1) =_{I^S(S)} J(t_2))$
- $J(S^{v_1, v_2, \ldots, v_n}(F, t_1, t_2, \ldots, t_n)) = S^{v_1, v_2, \ldots, v_n}(J(F), J(t_1), J(t_2), \ldots, J(t_n))$

- $J(AS^{v}(T)) = AS^{v}(J(T))$
- $J(P \bullet Q) = J(P) \bullet J(Q)$
- $J(IF(F,P,Q)) = IF(J(F),J(P),J(Q))$
- $J(WH(F,P)) = WH(J(F),J(P))$
- $J(\{p\}f\{q\}) = WH(J(p),J(f),J(q))$.

Монотонность композиций

Сначала дадим определение монотонной композиции для квазиарных предикатов, функций и биквазиарных функций.

Композиция $C : (FPrg(\tau))^n \times (Pr(\tau))^m \times (Fn^{A_1}(\tau)) \times (Fn^{A_2}(\tau)) \times \ldots \times (Fn^{A_k}(\tau)) \to Pr(\tau)$ называется монотонной, если выполняется следующее условие:

$$f_1 \subseteq g_1,\ldots,f_n \subseteq g_n, p_1 \subseteq q_1,\ldots,p_m \subseteq q_m, a_1 \subseteq b_1,\ldots,a_k \subseteq b_k \Rightarrow$$
$$\Rightarrow C(f_1,\ldots,f_n,p_1,\ldots,p_m,a_1,\ldots,a_k) \subseteq \mathrm{C}(g_1,\ldots,g_n,q_1,\ldots,q_m,b_1,\ldots,b_k)$$

Аналогично вводится определение монотонности композиций, имеющих результатом квазиарную функцию, или биквазиарную функцию, или имеющий другой порядок и набор аргументов.

Неформально определение монотонности можно понимать следующим образом. Если один из аргументов композиции заменить на более определенный, то значения композиции на тех данных, на которых они были определены, не изменятся. Можно сформулировать следующее утверждение.

$f \subseteq g \Leftrightarrow$ на всех данных $d \in NST(\tau)\ f(d)\downarrow \Rightarrow g(d)\downarrow = f(d)$.

Используя это утверждение докажем монотонность всех композиций, кроме нуль-арных $\{\vee, \neg, S^{\bar{v}}, \exists x, =_A, AS^x, IF, \bullet, WH, FH\}$.

Монотонность $\vee$.

Мы имеем некоторые $p \subseteq p', q \subseteq q'$, нужно показать, что $p \vee q \subseteq p' \vee q'$. Это аналогично тому, что на всех данных $d \in NST(\tau)\ p \vee q(d)\downarrow \Rightarrow p' \vee q'(d)\downarrow = p \vee q(d)$. Возьмем любое d такое, что $p \vee q(d)\downarrow$. Если $p \vee q(d) = T$, то или $p(d) = T \Rightarrow p'(d) = \mathrm{T} \Rightarrow p' \vee q'(d)\downarrow = T = p \vee q(d)$, или $q(d) = T \Rightarrow q'(d) = \mathrm{T} \Rightarrow p' \vee q'(d)\downarrow = T = p \vee q(d)$. В случае, когда $p \vee q(d) = F$, то $p(d) = F$ и $q(d) = F \Rightarrow p'(d) = F$ и $q'(d) = F \Rightarrow p' \vee q'(d)\downarrow = F = p \vee q(d)$.

Следовательно, композиция $\vee$ – монотонна.

Монотонность $\neg$.

Пускай $p \subseteq p'$, нужно показать, что $p \subseteq \neg p'$. Возьмем любое d такое, что $\neg p(d)\downarrow$. Тогда $p(d)\downarrow \Rightarrow p'(d)\downarrow = p(d)$, откуда по определению $\neg p'(d)\downarrow = \neg p(d)$.

Следовательно, композиция $\neg$ – монотонна.

Монотонность $S^{\bar{v}}$.

По определению, из $S^{v_1,v_2,\ldots,v_n}(f,g_1,g_2,\ldots,g_n)(d)\downarrow$ следует, что $g_i(d)\downarrow$ для всех $i \in \{1,\ldots n\}$ откуда будет следовать, что $g_i'(d)\downarrow = g_i(d)\downarrow$ для всех $i \in \{1,\ldots n\}$, и функции, в которые подставляются значения, будут вычисляться на одинаковых данных, откуда следует монотонность композиции.

Монотонность $\exists x$.

Пускай $p \subseteq p'$. Нужно показать $\exists x\, p \subseteq \exists x\, p'$. Возьмем произвольное d такое, что $\exists x\, p(d)\downarrow$.

Рассмотрим два случая.

$\exists x\, p(d) = T$, тогда существует $a \in \tau(x): p(d\nabla[x \mapsto a])\downarrow = T$, тогда $p'(d\nabla[x \mapsto a])\downarrow = T$, откуда $\exists x\, p'(d)\downarrow = T = \exists x\, p(d)$.

$\exists x\, p(d) = F$, тогда для всех $a \in \tau(x): p(d\nabla[x \mapsto a])\downarrow = F$, тогда для всех $a \in \tau(x): p'(d\nabla[x \mapsto a])\downarrow = F$, откуда $\exists x\, p'(d)\downarrow = F = \exists x\, p(d)$.

Следовательно, композиция $\exists x$ монотонна.

Монотонность $=_A$.

Пускай $f \subseteq f', g \subseteq g'$. Из определения композиции, можно сделать вывод, что $(f =_A g)(d)\downarrow \Rightarrow f(d)\downarrow$ и $g(d)\downarrow$. Откуда $f'(d)\downarrow = f(d)$ и $g'(d)\downarrow = g(d)$ и, следовательно $(f' =_A g')(d)\downarrow = (f =_A g)(d)$.

Таким образом, композиция $=_A$ монотонная.

Монотонность AS^x.

Из определения AS^x следует, что $(AS^x f)(d)\downarrow \Rightarrow f(d)\downarrow$, откуда аналогично предыдущим случаям можно сделать вывод, что композиция монотонна.

Монотонность IF.

Пускай $f \subseteq f', g \subseteq g', b \subseteq b'$ возьмем такое d, что $IF(b,f,g)(d)\downarrow$. Рассмотрим два случая.

Если $b(d)\downarrow = T$ и $f(d)\downarrow$, то $b'(d)\downarrow = T$ и $f'(d)\downarrow = f(d) \Rightarrow IF(b',f',g')(d)\downarrow = IF(b,f,g)(d)$.

Если $b(d)\downarrow = F$ и $g(d)\downarrow$, то $b'(d)\downarrow = F$ и $g'(d)\downarrow = g(d) \Rightarrow IF(b',f',g')(d)\downarrow = IF(b,f,g)(d)$.

Следовательно, композиция IF монотонна.

Монотонность $\bullet$.

Пускай $f \subseteq f', g \subseteq g'$ возьмем такое d, что $f \bullet g(d)\downarrow$. Тогда $g(f(d))\downarrow \Rightarrow f(d)\downarrow$, откуда $f'(d)\downarrow = f(d) \Rightarrow g(f'(\mathrm{d}))\downarrow = g(f(d)) \Rightarrow g'(f'(d))\downarrow = g(f(d))$.

Следовательно, композиция $\bullet$ монотонна.

Монотонность WH.

Из определенности композиции цикла на определенном данном следует существование последовательности данных, таких, что выполняются условия из определения. Откуда и для доопределенных функций и предиката, условия будут выполняться. Следовательно, общее значение не изменится, откуда композиция WH монотонна.

Монотонность FH.

Пускай $f \subseteq f', p \subseteq p', q \subseteq q'$. Возьмем произвольное d такое, что $FH(p,f,q)(d)\downarrow$. Рассмотрим несколько случаев.

$FH(p,f,q)(d)\downarrow = T$. Тогда либо $p(d)\downarrow = F \Rightarrow p'(d)\downarrow = F \Rightarrow FH(p',f',q')\downarrow = T = FH(p,f,q)$, либо $f(d)\downarrow$ и $q(f(d))\downarrow = T \Rightarrow f'(d)\downarrow = f(d)$ и $q'(f(d))\downarrow = T \Rightarrow FH(p',f',q')\downarrow = T = FH(p,f,q)$.

$FH(p,f,q)(d)\downarrow = F$, откуда $p(\mathrm{d})\downarrow = T$ и $f(d)\downarrow$ и $q(f(d))\downarrow = F$, тогда $p'(d)\downarrow = T$ и $f'(d)\downarrow = f(d)$ и $q'(f(d))\downarrow = F \Rightarrow q'(f'(d))\downarrow = F$, таким образом $FH(p',f',q')\downarrow = F = FH(p,f,q)$

Для всех случаев пришли к требуемому результату, следовательно, композиция будет монотонной.

Было показано, что все композиции будут монотонными, значит построенная квазиарная логика Флойда-Хоара монотонная.

Для композиции Флойда-Хоара можно доказать более сильный результат, а именно, она является непрерывной. Сначала дадим определение непрерывности композиции по одному из ее аргументов.

Цепью функций (предикатов) будем называть бесконечное множество функций (предикатов) $\{f_0, f_1, \ldots\}$, каждой из которых поставим в соответствие номер, такое, что $f_i \subseteq f_{i+1}\ \forall i \in \omega$.

Границей цепи функций (предикатов) будем называть супремум соответствующего множества, будем ее обозначать $\coprod_i f_i$.

Композиция $C : (FPrg(\tau))^n \times (Pr(\tau))^m \times (Fn^{A_1}(\tau)) \times (Fn^{A_2}(\tau)) \times \ldots \times (Fn^{A_k}(\tau)) \to Pr(\tau)$ называется непрерывной по первому аргументу, если для произвольной цепи $\{f_i \mid i \in \omega\}$ выполняется:

$$C(\coprod_i f_i, g_2, \ldots, g_n, p_1, \ldots, p_m, a_1, \ldots, a_k) = \coprod_i \mathrm{C}(f_i, g_2, \ldots, g_n, p_1, \ldots, p_m, a_1, \ldots, a_k)$$

Аналогично определяется непрерывность по другим аргументам.

Покажем, что композиция Флойда-Хоара будет непрерывной по первому аргументу, для остальных доказательство проводится по аналогии.

Рассмотрим цепь предикатов $\{p_i \mid i \in \omega\}$. Так как композиция Флойда-Хоара монотонна, то $\{FH(p_i,f,q) \mid i \in \omega\}$ тоже будет цепью. Необходимо показать, что $FH(\coprod_i p_i, f, q) = \coprod_i FH(p_i,f,q)$.

Возьмем произвольное d , тогда возможны два варианта: либо граница будет определена на этом данном, либо нет. В первом случае из отношения, установленного на элементах цепи, ни один из элементов не будет определен на d . Тогда $\coprod_i p_i(d)\uparrow$ и $p_j(d)\uparrow\ \ \forall j \in \omega$, откуда $FH(\coprod_i p_i, f, q)(d) = FH(p_j,f,q)(d)\ \ \forall j \in \omega$, а значит и $FH(\coprod_i p_i, f, q)(d) = \coprod_i FH(p_i,f,q)(d)$.

Если граница определена на этом данном, то можно найти k такое, что $p_k(d)\downarrow$, и $\forall j > k, p_j(d)\downarrow = p_k(d) = \coprod_i p_i(d)$, тогда $FH(\coprod_i p_i, f, q)(d) = FH(p_k,f,q)(d)$ и $FH(p_k,f,q)(d) = \coprod_i FH(p_i,f,q)(d)$, так как $FH(p_k,f,q)(d) = FH(p_j,f,q)(d)\ \ \forall j > k$.

Следовательно, $FH(\coprod_i p_i, f, q)(d) = FH(p_k,f,q)(d) = \coprod_i FH(p_i,f,q)(d)$

Во всех случаях $FH(\coprod_i p_i, f, q)(d) = \coprod_i FH(p_i, f, q)(d)$, так как данное d произвольное, то получаем, что $FH(\coprod_i p_i, f, q) = \coprod_i FH(p_i, f, q)$, что и требовалось доказать.

Доказательство для остальных аргументов композиции не отличается от указанного доказательства для непрерывности по предусловию.

Заключение

Работа является дальнейшим развитием [Никитченко, Криволап, 2002] и [Nikitchenko, Tymofieiev, 2013]. Было построено алгебры более высоких уровней, которые включали в себя квазиарные функции, а не только предикаты. Было доказано, что при переходе к многосортным логикам, модифицированная композиция Флойда-Хоара остается монотонной. Использование многосортных логик позволяет более адекватно описывать свойства программ и является следующим шагом, после перехода к квазиарным частичным предикатам и функциям. Постает проблема исследования систем вывода в многосортных логиках и перенос результатов полученных для монотонных логик Флойда-Хоара без использования типов.

Благодарности

Статья частично финансирована из проекта ITHEA XXI организации ITHEA ISS (www.ithea.org) и ADUIS (www.aduis.com.ua)

Список литературы

[Floyd, 1967] R.W. Floyd Assigning meanings to programs / R.W. Floyd // Proceedings of the American Mathematical Society Symposia on Applied Mathematics. – 1967. – Vol. 19. – pp. 19-31.

[Hoare, 1969] C.A.R. Hoare An axiomatic basis for computer programming / C.A.R. Hoare // Communications of the ACM. – 1969. – № 12. – pp. 576-580,583.

[Nikitchenko, Tymofieiev, 2013] Mykola S. Nikitchenko, Valentyn G. Tymofieiev. Satisfiability and Validity Problems in Many-Sorted Composition-Nominative Pure Predicate Logics. ICT in Education, Research, and Industrial Applications Communications in Computer and Information Science. – 2013. – Volume 347. – pp. 89-110.

[Reynolds, 2002] John C. Reynolds. Separation Logic: A logic for Shared Mutable Data Structures. LICS 2002: p55-74.

[Никитченко, Криволап, 2002] Никитченко Н.С., Криволап А.В. Семантические свойства монотонных логик Флойда-Хоара // Вестник Киевского Университета. Серия: физико-математические науки. – 2012. – № 3. – С. 215-222 (На украинском).

Сведения об авторах

Андрей Владимирович Криволап *– Киевский национальный университет имени Тараса Шевченко, факультет кибернетики, Украина, аспирант, e-mail: krivolapa@gmail.com*

Николай Степанович Никитченко *– Киевский национальный университет имени Тараса Шевченко, факультет кибернетики, Украина, д. ф.-м. н., профессор, e-mail: nikitchenko@unicyb.kiev.ua*