ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXIII 1976 4

УДК 681.142.2.

МАТЕМАТИКА

С. А. Солахян

Аксиоматический подход к доказательству корректности программ

(Представлено чл.-корр. АН Армянской ССР Ф. Т. Саркисяном 23/VI 1976)

Проблема доказательства корректности программ становится все более актуальной. Существенной причиной этого является то, что решение ее есть первый важный шаг на пути написания „правильных" программ, для которых не требуется приводить их доказательство.

В ([1–3]) были разработаны аксиоматические методы для доказательства частичной корректности программ. Существенным их недостатком является то, что заранее предполагается сходимость доказываемой программы. В ([4]) рассматривался метод доказательства сходимости, основанный на использовании некоторой монотонно убывающей функции u, отображающей область программных переменных X в некоторое вполне упорядоченное множество $(W, \leqslant)$ с отношением порядка $\leqslant$. Однако, нахождение этой функции основано на полном понимании смысла программы и весьма затруднительно.

В настоящей работе рассматривается проблема (полной) корректности. Приводится система аксиом и правил вывода, позволяющая провести формальное доказательство. При этом необязательно полное понимание смысла программы. Мы будем использовать понятия и методы формального описания семантики языков программирования, приведенные в ([5]).

Рассмотрим:

1) непустое, конечное или счетное множество символов, называемых элементарными объектами:

$$EO = \{eo_1, eo_2, \cdots\};$$

2) непустое, конечное или счетное множество символов, называемых селекторами:

$$S = \{s_1, s_2, \cdots\}.$$

Абстрактный объект (или просто: объект) определяется как любой элементарный объект или любой составной объект. Составной объект является конечным множеством пар

$$|\langle s_1 : A_1\rangle, \cdots, \langle s_n : A_n\rangle|,$$

где компонента $\langle s : A\rangle$ навывается именованным объектом, s— именем объекта A, $s \in S$, $n \geqslant 0$, $s_i \neq s_j$ для $i \neq j$. Единственный составной объект Ω, состоящий из нулевого числа компонент, называется нуль объектом.

Для преобразования объектов вводится операция μ, операндами которой являются объект A и пары $\langle s_i : B_i\rangle$, где $s_i \in S$, B_i—объекты. Эта операция записывается следующим образом:

$$\mu(A; \langle s_1 : B_1\rangle, \cdots, \langle s_n : B_n\rangle).$$

Ее результатом является снова объект, а именно, объект A, где $s_i(A)$ объект заменяется на объект B_i, $1 \leqslant i \leqslant n$.

Если $A = \Omega$, то имеем новую операцию μ_0, которая определяется в терминах операции μ следующим образом:

$$\mu_0(\langle s_1 : B_1\rangle, \cdots, \langle s_n : B_n\rangle) = \mu(\Omega; \langle s_1 : B_1\rangle, \cdots, \langle s_n : B_n\rangle).$$

Таким образом, можно сказать, что оператор μ_0 собирает именованные объекты в новый составной объект, т. е.:

$$\mu_0(\langle s_1 : B_1\rangle, \cdots, \langle s_n : B_n\rangle) = |\langle s_1 : B_1\rangle, \cdots, \langle s_n : B_n\rangle|.$$

В ([6]) были выведены условия $P(i, \pi, \xi)$, при которых выполнение оператора присваивания и оператора цикла *завершается* и дает определенный результат. Эти условия имеют следующий вид:

$$P(i, \pi, \xi) \supset \text{result}(x, \langle i, \pi\rangle) = \text{val}(x, \xi_n),$$

где: a) $\langle i, \pi\rangle$—i-ый сегмент программы π;
в) ξ—состояние памяти (значения входных переменных);
c) ξ_n—заключительное состояние памяти;
d) result$(x, \langle i, \pi\rangle)$—результат, выработанный при выполнении i-го сегмента со входом x;
e) $P(i, \pi, \xi) = P_{ass}(i, \pi, \xi) \vee P_{\text{while}}(i, \pi, \xi)$.

Вычисление функции val рассмотрено в ([6]).

Даны:

1) некоторый предикат $\varphi(x)$, называемый входным предикатом;
2) некоторый предикат $\psi(x, x')$, называемый выходным предикатом.

Определение 1. *Программа π корректна относительно предикатов φ и ψ, если для любого x, такого, что $\varphi(x) = T$, выполнение программы π завершается и $\psi(x, \text{result}(x, \pi)) = T$.*

Теоремы, которые мы будем использовать, имеют следующий вид:

$$|r(\xi) \& P(l, \pi, \xi)|\langle l, \pi\rangle|s(\xi, \xi')|,$$

что является условием корректности сегмента $<i, \pi>$ относительно предикатов $r(\xi)\,\&\,P(i, \pi, \xi)$ и $s(\xi, \xi')$:

$$r(\xi)\,\&\,P(i, \pi, \xi) \supset * <i, \pi>\,\&\,s(\xi, \xi'),$$

где $* <i, \pi>$ означает, что выполнение сегмента $<i, \pi>$ завершается.

Предикат $r(\xi)$ является входным предикатом для сегмента $<i, \pi>$ и имеет следующую форму:

$$r(\xi) \equiv (\xi = \mu_0(|<x : \text{Is} - \text{Int}> \| \text{Is} - \text{var}(x)|) \vee \text{Is} - \Omega),$$

где предикаты Is—Int, Is—var и Is—Ω использованы для идентификации констант, переменных и нуль-объекта, соответственно; x—вектор входных переменных.

Предикат $s(\xi, \xi')$—выходной предикат для сегмента $<i, \pi>$. Его форма следующая:

$$s(\xi, \xi') \equiv (\xi' = \mu(\xi;\ |<x : \text{result}(x, <i, \pi>)> \| \text{Is} - \text{var}(x)|)).$$

Как мы видим, построение предикатов $r(\xi)$ и $s(\xi, \xi')$ для любого сегмента $<i, \pi>$ строго определено и не требует понимания процессов, происходящих при выполнении этих сегментов.

Определение 2. *Атомарным оператором будем называть:* a) *оператор присваивания*; b) *оператор цикла, тело которого содержит один единственный оператор присваивания.*

В качестве базисных теорем—*аксиом*, возьмем те теоремы, в которых сегмент $<i, \pi>$ является атомарным оператором. Таким образом, фактически, будем иметь две аксиомы.

Правила вывода, представленные ниже, являются некоторыми правилами, преобразующими множество предпосылок $H_1, \ldots, H_n$ (условий, при которых правило применимо) в следствие H_{n+1}, которое является выведенной теоремой. Такие правила обозначены через

$$R \cdot \frac{H_1, \ldots, H_n}{H_{n+1}}.$$

Каждая предпосылка является либо ранее выведенной теоремой либо логическим требованием.

Приведем, теперь, конкретные правила вывода.

R 1. Правило свертки.

Согласно этому правилу, сегмент $<i, \pi>$ заменяется на оператор присваивания.

$$\frac{|r(\xi)\,\&\,P(i, \pi, \xi)|<i, \pi>|s(\xi, \xi')|}{|r(\xi)\,\&\,P(i, \pi, \xi)|\xi \leftarrow \mu(\xi;\ |<x : \text{result}(x, <i, \pi>)>|\,)|s(\xi, \xi')|}.$$

Это означает, фактически, присваивание $x := \text{result}(x, <i, \pi>)$. Конечно, в том случае, когда сегмент $<i, \pi>$ является оператором присваивания, применение правила R1 не имеет смысла.

R2. Правило сцепления.

$$|r_1(\xi)\ \&\ P(i, \pi, \xi)|\xi \leftarrow \mu(\xi;\ |<x : \text{result}(x,\ <i, \pi>)>|)|s_1(\xi, \xi') \tag{1}$$

$$|r_2(\xi)\ \&\ P(j, \pi, \xi)|\xi \leftarrow \mu(\xi;\ |<x : \text{result}(x, <j, \pi>)>|)|s_2(\xi, \xi') \tag{2}$$

$$(\forall \xi_1, \xi_2)(s_1(\xi_1, \xi_2) \vdash r_2(\xi_2)) \tag{3}$$

$$(\forall \xi_1, \xi_2, \xi_3)(s_1(\xi_1, \xi_2)\ \&\ s_2(\xi_2, \xi_3) \vdash s_{1,2}(\xi_1, \xi_3) \tag{4}$$

$$\frac{}{|r_1(\xi)\ \&\ P(i, \pi, \xi)\ \&\ P(j, \pi, \xi)|}$$

$$\xi \leftarrow \mu(\xi;\ |<x : \text{result}(x, <i, \pi>;\ <j, \pi>)>|)|s_{1,2}(\xi, \xi')|.$$

Условие (4) характеризует предикат $s_{1,2}(\xi_1, \xi_3)$ как отношение между ξ_1 до выполнения и ξ_3 после выполнения составного оператора $<i, \pi>; <j, \pi>$.

Как показано в (⁵), результат, полученный при выполнении составного оператора может быть вычислен следующим образом:

$$\text{result}(x, <i, \pi>; <j, \pi>) = \text{result}\,(\text{result}(x, <i, \pi>), <j, \pi>).$$

Используя правила R1 и R2, мы добиваемся того, что в теле оператора цикла будет содержаться один единственный оператор присваивания. А это дает возможность применить соответствующую аксиому.

R3. Правило следствия.

$$\frac{|p(\xi)\ \&\ P(i, \pi, \xi)|<i, \pi>|q(\xi, \xi')|}{\begin{array}{l}(\forall \xi)(r(\xi) \vdash p(\xi)) \\ (\forall \xi_1, \xi_2)(q(\xi_1, \xi_2) \vdash s(\xi_1, \xi_2))\end{array}}$$

$$|r(\xi)\ \&\ P(i, \pi, \xi)|<i, \pi>|s(\xi, \xi')|$$

R4. Правила И/ИЛИ.

а)
$$\frac{|r(\xi)\ \&\ P(i, \pi, \xi)|<i, \pi>|s_1(\xi, \xi')|}{|r(\xi)\ \&\ P(i, \pi, \xi)|<i, \pi>|s_2(\xi, \xi')|}$$

$$|r(\xi)\ \&\ P(i, \pi, \xi)|<i, \pi>|s_1(\xi, \xi')\ \&\ s_2(\xi, \xi')|$$

в)
$$\frac{\begin{array}{l}|r_1(\xi)\ \&\ P(i, \pi, \xi)|<i, \pi>|s(\xi, \xi')| \\ |r_2(\xi)\ \&\ P(i, \pi, \xi)|<i, \pi>|s(\xi, \xi')|\end{array}}{|(r_1(\xi) \vee r_2(\xi))\ \&\ P(i, \pi, \xi)|<i, \pi>|s(\xi, \xi')|}$$

Смысл правил R3 и R4 очевиден.

Если, используя правила вывода R1—R4, мы сумеем из аксиом вывести теорему

$$|\varphi(x)\ \&\ P(\pi, \xi)|\pi|\psi(x, \text{result}\,(x, \pi))|,$$

то это будет означать, что программа π корректна относительно предикатов φ и ψ, т. е. для любого x, удовлетворяющего предикату $\varphi(x)$, выполнение π завершается и предикат $\psi(x, x')$ истинен для начальных и заключительных значений x и x', соответственно.

Схема доказательства корректности программы π имеет следующий вид:

1. Выявляется „самый внутренний" сегмент программы, который обязательно является атомарным оператором. Для него строится предикат $P(i, \pi, \xi)$ согласно (6). В случае истинности этого предиката применяется соответствующая аксиома.

2. Применяется правило вывода R1. Предпосылка обеспечивается пунктом 1.

3. Снова ищется „самый внутренний" сегмент. Применяется правило R2, а затем снова R1 и т. д.

Правила R3 и R4 используются в необходимых случаях в качестве вспомогательных правил.

В итоге получается, что в результате применения аксиом и правил вывода программа π свернулась в один единственный оператор, к которому, предварительно проверив истинность предиката $P(\pi, \xi)$, применяется соответствующая аксиома, доказывающая корректность этой программы.

Ереванский НИИ математических машин

Ս. Ա. ՈՂԱԽՅԱՆ

Սրագրերի կոռեկտության ապացուցման ալխոմատիկ մոտեցում

Այս աշխատանքում դիտարկվում է աքսիոմատիկ մոտեցումը ծրագրերի կոռեկտության ապացույցի նկատմամբ։

Ներկում է աքսիոմաների և արտածման կանոնների համակարգ, որը հնարավորություն է տալիս կատարել ֆորմալ ապացույց՝ ընդ որում ծրագրի իմաստի լրիվ ըմբռնումը պարտադիր չէ։

(6) աշխատանքում արտածվել են $P(i, \pi, \xi)$ պայմանները, որոնց դեպքում π ծրագրի i-րդ անցմանի կատարումը ξ հիշողության վիճակում ավարտվում է և տալիս է որոշակի արդյունք։ Այդ պայմաններն ունեն հետևյալ տեսքը

$$P(i, \pi, \xi) \supset \text{result}(x, <i, \pi>) = \text{val}(x, \xi_n):$$

Օգտագործվող թեորեմները պրտավում են այսպես՝

$$|r(\xi) \;\&\; P(i, \pi, \xi)|<i, \pi>|s(\xi, \xi')|$$

և արտահայտում են $r(\xi) \;\&\; P(i, \pi, \xi)$ և $s(\xi, \xi')$ պրեդիկատների նկատմամբ $<i, \pi>$ անցմանի կոռեկտության պայմանը՝

$$r(\xi) \;\&\; P(i, \pi, \xi) \supset * \; <i, \pi> \;\&\; s(\xi, \xi'):$$

Որպես օրինակներ վերցված են այն թեորեմները, որոնցում $\langle l,\pi \rangle$ սեգմենտը հանդիսանում է ատոմար օպերատոր։ Բերված են արտածման չորս կանոններ, որոնք հնարավորություն են տալիս փոքր սեգմենտների համար թեորեմները համախմբել մեկ թեորեմում՝ ամբողջ ծրագրի համար։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *C. A. R. Houre*, Lecture Notes in Mathematics, 188, 102—116, (1971). [2] *S. Igarashi*, Lecture Notes in Mathematics, 188, 117—177, (1971). [3] *S. Igarashi et al.* Acta Informatica, 4, № 2, 145—182, (1975). [4] *Z. Manna, A. Pnueli*, Acta Informatica, 3, 243—263, (1974). [5] *С. А. Солахян*, „Программирование", № 3, 3—12, (1976). [6] *С. А. Солахян*, „Программирование", № 4, 33—42, (1976). [7] *C. A. R. Hoare, P. E. Lauer*, Acta Informatica, 3, № 2, 135—153, (1974).