О ПОИСКЕ ИНВАРИАНТНЫХ СООТНОШЕНИЙ В ПРОГРАММАХ

А.А.Летичевский

Киев, СССР

Алгоритм как математический объект представляет собой дискретную динамическую систему, которая порождает процессы вычислений. В случае простых динамических моделей последовательных вычислений, эта система состоит из двух компонент: управляющей компоненты и информационной среды. Современная технология проектирования алгоритмов сводится к решению совокупности задач, которые формулируются в терминах математических моделей систем, которые должны реализовать проектируемые алгоритмы [I] . Эти задачи носят математический характер, и для их решения могут быть разработаны математические методы.

Примером таких методов могут служить: методы последовательного превращения формализованных спецификаций или формулировки задачи в программу ее решения, методы доказательства корректности и других свойств программ, формальные преобразования, оптимизация.

В докладе рассматривается проблема поиска инвариантов программ. В общем виде задача формулируется следующим образом. Что можно сказать о состоянии информационной среды, когда управляющая компонента находится в данном состоянии? Хорошо известно, что этот вопрос является основным при доказательстве корректности методом Флойда. В [2] было показано, что многие оптимизирующие процедуры сводятся к проблеме поиска инвариантов.

Решение рассматриваемой задачи зависит от языка, который используется для представления свойств информационной среды. Если в качестве такого языка используется язык исчисления предикатов первого порядка, то множество всех инвариантов легко может быть описано средствами алгоритмической логики. Но с этим описанием трудно работать, поскольку оно использует,

например, геделевскую нумерацию всех путей в программе. Поэтому интересно рассмотреть задачу для более ограниченных языков. Важными примерами таких языков являются язык равенств и язык атомарных условий. Эти языки рассматриваются здесь. Некоторые частные случаи были рассмотрены раньше в [3].

О п р е д е л е н и я. В качестве модели программы будем пользоваться понятием интерпретированной U - Y - схемы программы над памятью или U - Y - программы. Пусть задано некоторое множество D, называемое областью данных. На этом множестве действуют операции, обозначаемые символами сигнатуры Ω. Рассматриваемое вместе с этими операциями множество D есть универсальная Ω-алгебра, которая называется алгеброй данных. На множестве D определены также предикаты, обозначаемые символами сигнатуры Π. Рассмотрим множество R переменных (память) и множество $B = D^R$ состояний памяти. Элементарным условием назовем пропозициональную функцию от атомарных условий вида $\pi(t_1,\ldots,t_n)$, где π - символ n-местного предиката сигнатуры Π, $t_1,\ldots,t_n$ - термы, построенные из переменных множества R и операций сигнатуры Ω. Операторами присваивания назовем выражение вида $(r_1 := t_1, \ldots, r_n := t_n)$, где $r_1,\ldots,r_n$ - переменные, $t_1,\ldots,t_n$ - термы над R. При заданном состоянии памяти термы принимают значение в D, а элементарные условия - истину или ложь. Каждый оператор присваивания $y = (r_1 := t_1,\ldots,r_n := t_n)$ определяет преобразование множества B. Если $b \in B$, то $b' = y(b)$ есть состояние памяти, которое получается в результате одновременного присваивания всем переменным $r_1,\ldots,r_n$ значений термов $t_1,\ldots,t_n$ на состоянии b. Иными словами, $b'(r_i) = b(t_i)$, $b'(s) = b(s)$, если $s \in R$, $s \neq r_i$, $i = 1,\ldots,n$.

Пусть U - некоторое множество элементарных условий, а Y - некоторое множество операторов присваивания. U - Y - программа A - это множество состояний вместе с множеством переходов. Каждый переход есть четверка (a, u, y, a'), где a, a' - суть состояния программы, u есть элементарное условие, $y \in Y$ - оператор присваивания. В множестве A выделено начальное состояние a_0 и заключительное состояние a^*. Если

(a,u,y,a') есть переход программы A, то пишем $a \xrightarrow[A]{u/y} a'$ или просто $a \xrightarrow{u/y} a'$, если программа A фиксирована. Процесс выполнения U - Y - программы A при заданном начальном состоянии b_0 информационной среды есть конечная или бесконечная последовательность пар (a_0, b) $(a_1, b_1),\ldots,$ a_0 - начальное состояние программы, $b = b_0$, для любой пары (a_i, a_{i+1}) в программе есть переход $a_i \xrightarrow{u_i/y_i} a_{i+1}$, такой, что $u(b_i) = 1$, $b_{i+1} = y(b_i)$. Процесс называется терминальным, если он конечен и последняя пара есть (a_n, b_n), где $a_n = a^*$.

Программа не предполагается детерминированной, т.е. процесс ее выполнения, вообще говоря, не определяется однозначно начальным состоянием. Программа A вычисляет отношение $f_A \subset B^2$, которое определяется следующим образом: $(b, b') \in f_A \Leftrightarrow$ существует терминальный процесс $p = (a_0,b),\ldots,(a^*, b')$, где a_0 -начальное, a^* - заключительное состояние программы.

Относительно языка L, используемого для записи свойств информационной среды, будем предполагать следующее. Каждое предложение этого языка может быть представлено формулой $p(r_1, r_2,..,r_n)$ языка исчисления предикатов первого порядка, содержащей свободные переменные $r_1,\ldots, r_n$ и интерпретированной на области D. Сигнатура предикатов и функциональных символов рассматриваемого исчисления предикатов содержит все символы сигнатуры Π и Ω. Предложения языка L будем называть условиями или L-условиями.

Условие $p(r_1,\ldots, r_n)$ будем называть инвариантом состояния a программы A, если оно истинно при каждом прохождении состояния a в процессе ее выполнения не зависимо от начального состояния информационной среды. Иногда полезно рассматривать относительные инварианты, если задано начальное условие $u(r_1,\ldots, r_n)$. Это условие ограничивает множество рассматриваемых начальных состояний информационной среды только теми состояниями, на которых условие $u(r_1,\ldots,r_n)$ истинно.

Язык соотношений в алгебре данных. Зафиксируем алфавит $R = \{r_1, \ldots, r_n\}$ переменных и рассмотрим язык L, предложениями которого являются равенства вида $g(r) = h(r)$, $r = (r_1, \ldots, r_n)$, $g(r)$ и $h(r)$ – Ω – термы над R, т.е. выражения, построенные из переменных с помощью операций алгебры данных. Пусть $M \subset L$ – система равенств. Обозначим через $D(M)$ множество наборов $z \in D^n$, которые удовлетворяют всем равенствам системы M, т.е. таких z, что для любого равенства $g(r) = h(z) \in M$ имеет место равенство $g(z) = h(z)$ в алгебре D. Таким образом, $D(M)$ есть множество всех решений системы M, рассматриваемой как система уравнений в алгебре D.

Пусть $a_i \xrightarrow{u_i/y_i} a$, $i = 1, \ldots, k$ – все переходы, которые ведут в состояние a программы A. Пусть в состоянии a_i выполняется система равенств $M_i \subset L$. Если $y_i = (r := t_i(r)) = (r_1 := t_{i1}(r), \ldots, r_n := t_{in}(r, n))$, то все равенства множества $M = M_1' \cap \ldots \cap M_k'$, $g(r) = h(r) \in M_i' \Leftrightarrow g(t_i(z)) = h(t_i(z))$, для всех $z \in D(M_i')$, являются инвариантами состояния $a \neq a_o$. Если же $a = a_o$, то M надо еще пересечь с множеством всех равенств, которые выполняются на начальном состоянии информационной средн. При этом, если в момент перехода из состояния a_i в a информационная среда может находиться в любом из состояний b, таких, что $b(r) \in D(M_i)$, а M_i есть множество всех инвариантов состояния a, то множеством M исчерпываются все инварианты состояния a. Используя описанную конструкцию, можно организовать процесс порождения в каждом из состояний программы последовательности множеств $M_a^{(o)} \subset M_a^{(1)} \subset \ldots$ соотношений, которые выполняются в этом состоянии. При этом, $M_a^{(o)} = M_o$ состоит из всех тождеств алгебры D, $M_a^{(i+1)}$ получается из $M_a^{(i)}, \ldots, M_{a_k}^{(i)}$ описанным выше способом. Множество $M_a = \bigcup_{i=o}^{\infty} M_a^{(i)}$ есть максимальное множество соотношений, которое можно получить, не используя информации о действии элементарных условий.

Пусть M – некоторое множество равенств. Если все равенства из M выполняются в состоянии a, то в этом же состоянии выполняются также все равенства $g(r) = h(r)$, такие, что

$g(z) = h(z)$ для всех $z \in D(M)$. Множество всех таких равенств обозначим через $C_D(M)$ и будем называть D - замыканием множества M. Множество M назовем D - замкнутым, если оно совпадает со своим D-замыканием. Подмножество $N \subset M$ D-замкнутого множества назовем его D-базисом, если $C_D(M) = M$. Поскольку $D(\emptyset) = D^n$, то $C_D(\emptyset)$ состоит из всех тождеств алгебры D и содержится в любом D-замкнутом множестве равенств.

Множества $M_a^{(i)}$ являются D-замкнутыми. Если они обладают конечными D-базисами, то эти базисы можно использовать для конструктивного задания множеств $M_a^{(i)}$. Тогда все сводится к решению задач

о соотношениях: зная D-базис D-замкнутого множества M, найти D-базис множества

$$M' = \{g(r) = h(r) \mid g(t(z)) = h(t(z)),\ z \in D(M)\},$$

и задач о пересечении: зная D-базисы множеств M_1 и M_2, найти D-базис множества $M_1 \cap M_2$.

Умея решать две указанные задачи, можем приступить к построению последовательностей $M_a^{(i)}$. Для некоторых программ и алгебр этот процесс оборвется через определенное количество шагов, и тогда мы получим полное описание всех инвариантных равенств. В других случаях можно остановиться на некотором шаге, получив достаточное количество инвариантов. Практически, если не стремиться к полноте, можно вместо построения D-базисов M' и $M_1 \cap M_2$ находить D-базисы их подмножеств. Можно также использовать более слабые, т.е. порождающие меньшее число равенств, операции замыкания, например, описанную ниже операцию алгебраического замыкания.

Рассмотрим некоторые построения, полезные при решении сформулированных выше основных задач. Пусть $T_D(R)$ обозначает множество Ω-термов, рассматриваемых с точностью до тождеств алгебры данных D. Иными словами, два терма $g(r)$ и $h(r)$ считаются равными, если $g(r) = h(r)$ есть тождество алгебры D, т.е. $g(z) = h(z)$ для любых $z \in D^n$. Множество $T_D(R)$ есть Ω-алгебра, свободная в наименьшем многообразии, которому принадлежит D. Будем называть это многообразие ос-

новным. Каждое равенство можно рассматривать как пару термов, а множество M равенств, как бинарное отношение на множестве T(R) всех Ω-термов над R. Определим операцию алгебраического замыкания C(M) системы равенств M относительно основного многообразия. Множество C(M) есть наименьшее множество равенств, которое содержит рефлексивное, симметричное и транзитивное замыкание множества M, все тождества основного многообразия и для любой m-арной операции $\omega \in \Omega$ вместе с равенствами $g_1(r) = h_1(r), \ldots, g_m(r) = h_m(r)$ содержит равенство $\omega(g_1(r),\ldots,g_m(r)) = \omega(h_1(r),\ldots,h_m(r))$. Множество M называется (алгебраически) замкнутым, если $C(M) = M$. Подмножество $N \subset M$ замкнутого множества называется его (алгебраическим) базисом, если $C(N) = M$. Очевидно, D - замкнутое множество замкнуто и алгебраически, а базис D - замкнутого множества является также его D-базисом. Обратные утверждения, вообще говоря, не верны.

Рассматриваемое, как отношение на T(R), множество M алгебраически замкнуто тогда и только тогда, когда оно есть конгруэнтность абсолютно свободной алгебры T(R), содержащей все тождества основного многообразия. Поэтому, M также индуцирует конгруэнтность на $T_D(R)$. Соответствующую факторалгебру будем обозначать через $T_D(R)/M$, ее элементы–через $t \pmod M$, $t \in T_D(R)$, а равенство–в виде $t = t' \pmod M$. С каждым оператором присваивания $y = (r := t(r))$ и множеством равенств M свяжем гомоморфизм $\gamma_{y,M} : T_D(R) \to T_D(R)/C_D(M)$, полагая $\gamma_{y,M}(r_i) = t_i \pmod{C_D(M)}$. Пусть M' определяется из равенства (5). Имеет место следующее утверждение.

Т е о р е м а I . M' есть ядро гомоморфизма $\gamma_{y,M}$, т.е.

$$(g = h) \in M' \Leftrightarrow \gamma_{y,M}(g) = \gamma_{y,M}(h).$$

С л е д с т в и е I. Алгебра $T_D(R)/M'$ изоморфна подалгебре $F[t_1,\ldots, t_n]$ алгебры $F = T_D(R)|_{C_D(M)}$, порожденной элементами $t_1,\ldots,t_n$.

Рассмотрим более подробно структуру соотношений, порождаю-

щих множество M', считая, что M D-замкнуто, т.е. $M = C_D(M)$. Пусть $\vartheta_1, \ldots, \vartheta_m$ – неприводимая система образующих алгебры $F[t_1, \ldots, t_m]$. Поскольку между элементами $t_1, \ldots, t_n$ и F возможны зависимости, m может быть меньше, чем n. Выразим t_i через $\vartheta = (\vartheta_1, \ldots, \vartheta_m)$, $t_i = u_i(\vartheta) \pmod M$, $i = 1, \ldots, n$. Поскольку t_i также является образующими рассматриваемой алгебры, то $\vartheta_i = f_i(t) \pmod M$, $i = 1, \ldots, m$. Поскольку $\gamma_{y,M}(r_i) = t_i = u_i(\vartheta) = u_i(f(t)) = \gamma_{y,M}(u_i(f(r))) \pmod M$, то все соотношения $r_i = u_i(f(r))$, $i = 1, \ldots, n$, содержатся в M'. Обозначим множество этих соотношений через M'_0. Если $g(\vartheta) = h(\vartheta) \pmod M$, $g(f(t)) = h(f(t)) \pmod M$, откуда $g(f(t)) = h(f(t)) \in M'$. Обозначим через M'_1 множество всех соотношений вида $g(f(r)) = h(f(r))$ таких, что $g(\vartheta) = h(\vartheta) \pmod M$ и $g(x) = h(x)$ не есть тождество $(x = (x_1, x_2, \ldots, x_n))$.

Т е о р е м а 2. Множество M' порождается множеством $M'_0 \cup M'_1$. Система элементов $a_1, \ldots, a_m$ алгебры A называется алгебраически независимой в A, если любое соотношение $g(a) = h(a)$ между ними есть следствие тождества $g(x) = h(x)$.

С л е д с т в и е 2. Если система элементов $\vartheta_1, \ldots, \vartheta_m$ алгебраически независима в $T_D(R)|_M$, то M' порождается множеством M'_0, алгебра $T_D(R)|_{M'}$ – свободная, а $f_1(r), \ldots, f_m(r)$ – ее свободные образующие.

Рассмотрим последовательность $M_a^{(0)} \subset M_a^{(1)} \subset \ldots$. Этой последовательности соответствует последовательность алгебр

$$F_a^{(0)} = T_D(R)\Big|_{M_a^{(0)}}, \quad F_a^{(1)} = T_D(R)\Big|_{M_a^{(1)}}, \quad \ldots .$$

Отображение $\gamma_i : F_a^{(i)} \longrightarrow F_a^{(i+1)}$, определенное равенством $\gamma_i(t \bmod M_a^{(i)}) = t' \pmod{M_a^{(i+1)}}$, является, очевидно, гомоморфизмом $F_a^{(i)}$ на $F_a^{(i+1)}$. При этом, если γ_i есть изоморфизм, то $M_a^{(i)} = M_a^{(i+1)}$, т.е. M_a получается конечным числом итераций. Рассмотрим несколько примеров конкретных классов алгебр, для которых можно конструктивно определить множества M_a.

Н а с л е д с т в е н н о с в о б о д н ы е а л г е б-

р и . Алгебра, свободная в некотором многообразии, называется наследственно свободной, если всякая ее подалгебра является свободной в том же самом многообразии. Примерами наследственно свободных алгебр является абсолютно свободные алгебры, свободные абелевы группы, свободные группы, конечномерные векторные пространства.

Пусть алгебра $T_D(R)$ - наследственно свободная. Тогда все алгебры $F_a^{(i)}$ являются свободными алгебрами основного многообразия. Действительно, $M_a^{(i+1)} = M_1' \cap \ldots \cap M_k'$, M_i' строятся по формуле (5) из $M = M_a^{(i)}$. Если $F_a^{(i)}$ - свободная алгебра основного многообразия, то в силу наследственности и следствия 2, алгебра $T_D(R)\big|_{M_i'}$ также является свободной алгеброй многообразия. Но такой же будет и $F_a^{(i+1)}$, поскольку она гомоморфно отображается на $T_D(R)\big|_{M_i'}$.

Рангом алгебры назовем минимальное число элементов неприводимой системы образующих. Поскольку все алгебры $F_a^{(i)}$ - свободны, то $F_a^{(i+1)}$ либо изоморфна алгебре $F_a^{(i)}$, либо имеет ранг строго меньший, чем ранг $F_a^{(i)}$. Поэтому последовательность $M_a^{(o)} \subset M_a^{(1)} \subset \ldots$ обрывается через конечное число шагов. Таким образом, для наследственно свободных алгебр нахождение M_a сводится к решению следующих двух задач:

а) найти неприводимую систему образующих подалгебры $F[t_1,\ldots,t_n]$ свободной алгебры $F = T_D(R)$, M - порождается системой равенств вида $r_i = \varphi_i(r)$, $i = 1,\ldots,n$;

б) найти базис или D-базис пересечения двух D-замкнутых систем равенств, каждая из которых порождается равенствами вида $r_i = \varphi_i(r)$, $i = 1,\ldots, n$, и таких, что $T_D(R)\big|_{M_1}$ и $T_D(R)\big|_{M_2}$ свободны.

Примерами наследственно свободных алгебр являются абсолютно свободные алгебры, свободные группы, свободные абелевы группы и линейные пространства. Для этих алгебр можно построить алгоритмы решения двух основных задач, используя хорошо известные алгебраические результаты. Таким образом, имеет место следующая теорема.

Т е о р е м а 3. Если $T_D(R)$ - абсолютно свободная ал-

гебра или свободная группа, абелева группа или линейное пространство, то существует алгоритм для отыскания множества M_a.

Указанные типы алгебр часто встречаются на практике. Например, абсолютно свободные алгебры связаны с обработкой формул и структур данных. Обработка строк приводит к свободным полугруппам, которые не являются наследственно свободными алгебрами. Однако, каждая свободная полугруппа может быть вложена в свободную группу и вопрос об отыскании инвариантов для полугруппы сводится к соответствующему вопросу для групп.

Пусть D есть множество рациональных чисел. Если мы используем только сложение и вычитание, то $T_D(R)$ есть свободная абелева группа, порожденная множеством R. Добавление констант (каждая программа использует только конечное число их) только увеличивает ранг этой группы. Если используется умножение на константы, то $T_D(R)$ есть линейное пространство и теорема 2 работает. Но если допускается умножение любых двух элементов D, то $T_D(R)$ есть кольцо полиномов с целыми коэффициентами. Эта алгебра не является наследственно свободной, но можно использовать результаты коммутативной алгебры. Каждое равенство в алгебре полиномов может быть представлено в виде $t = 0$ и, следовательно, отождествлено с элементом t кольца $T_D(R)$. Тогда каждое алгебраически замкнутое множество есть идеал кольца $T_D(R)$.

В силу теоремы Гильберта о базисе [4], кольцо многочленов с целыми коэффициентами является нётеровым и, следовательно, каждый идеал $M_a^{(1)}$ имеет конечный базис, а последовательность $M_a^{(o)} \subset M_a^{(1)} \subset \ldots$ обрывается через конечное число шагов. Если D - алгебраически замкнутое поле, то D - замыкание идеала M совпадает с его радикалом (теорема Гильберта о корнях). Поэтому задачу о пересечении удобно решать с помощью D-базиса. Действительно, радикал пересечения $M_1 \cap M_2$ совпадает с радикалом произведения $M_1 \cdot M_2$ идеалов, а базис последнего состоит из всевозможных произведений вида $g \cdot h$, где g - элемент базиса M_1, h - элемент базиса M_2.

Конструктивное решение задачи о соотношениях оказывается значительно сложнее. Автору не известно ее решение, даже ес-

ли область коэффициентов P является алгебраически замкнутым полем, хотя в этом случае коммутативная алгебра дает много полезных фактов о строении идеалов соотношений, которые можно использовать для фактического вычисления их базисов в конкретных случаях. Нетрудно видеть, что для каждого из множеств $M_a^{(i)}$ существует и может быть фактически построен алгоритм распознавания принадлежности многочленов этому множеству. Этим алгоритмом можно воспользоваться для представления $M_a^{(i)}$, однако остается вопрос о том, как выяснить, что $M_a^{(i)} = M_a^{(i+1)}$. Известно только, что при достаточно большом i это равенство должно иметь место. Практически можно либо ограничиться заданным числом итераций, либо искать часть идеала M', порожденную многочленами, степень которого не превосходит некоторого заданного числа. Последняя задача может быть решена сведением к системам алгебраических уравнений в поле P.

Язык атомарных условий. Расширим язык L, добавив к равенствам атомарные условия, т.е. формулы вида $\pi(t_1,\ldots,t_n)$, где $\pi \in \Pi$, $t_1,\ldots,t_n \in T(R)$, $R = (r_1,\ldots, r_n)$. Чтобы не делать оговорок, будем считать, что предикат равенства с обычной интерпретацией на D входит в Π, т.е. равенства также являются атомарными условиями. Пусть $M \subset L$—некоторое множество атомарных условий. Через D(M) будем теперь обозначать множество всех наборов $z \in D^n$, которые удовлетворяют всем условиям из M, т.е. таких, что $\pi(t(z)) = 1$ для всех $\pi(t(r)) \in M(t = (t_1,\ldots,t_m), z = (z_1,\ldots,z_n), r = (r_1,\ldots,r_n))$.

Пусть M – некоторое множество атомарных условий, u – атомарное условие, $y = (r_i := t) = (r_1 := t_1,\ldots,r_n := t_n)$ – оператор присваивания. Обозначим через J(M, u, y) множество атомарных условий M' такое, что $\pi(v(r)) \in M' \langle\Rightarrow\rangle \pi(v(t(z))) = 1$ для всех $z \in D(M \cup \{u\})$.

Снова рассмотрим все переходы $a_i \xrightarrow{u_1/y_i} a$, которые ведут в состояние a программы A. Пусть в состоянии a_i выполняется система атомарных условий M_i. Если $y_i = (r_i := t_i(r))$, $u_i = \pi_i(s_{i_1},\ldots,s_{i_m}) = \pi(s_1)$, то множество $M = M_1' \cap \ldots \cap M_k'$

будет множеством инвариантов состояния $a \neq a_0$, если $M_1' = J(M_1, u_1, y_1)$. Если $a = a_0$, то M надо еще пересечь с множеством всех атомарных условий, которые выполняются на начальном состоянии информационной среды. Если в момент перехода из состояния a_1 в состояние a информационная среда может находиться в любом из состояний b таких, что $b(r) = (b(r_1),\ldots,b(r_n)) \in D(M_1)$, M_1 есть множество всех инвариантных атомарных условий состояния a_1, то M исчерпывает все информационные атомарные условия состояния a. Рассмотрим последовательность $M_a^{(0)} \subset M_a^{(1)} \subset \ldots$ множеств атомарных условий, где $M_a^{(0)}$ состоит из всех тождеств алгебры D (включая тождество истинные атомарные условия), а $M_a^{(i+1)} = J(M_a^{(i)}, u_1, y_1) \cap \ldots \cap J(M_{a_k}^{(i)}, u_k, y_k)$. Предельное множество $M_a = \bigcup_{i=0}^{\infty} M_a^{(i)}$ дает хорошее приближение для множества всех инвариантных атомарных условий в состоянии a .

Понятие D- замыкания $C_D(M)$ множества M атомарных условий и понятие D- базиса вводятся так же, как и для равенств. Аналогично формулируются и две основные задачи. В качестве соотношений теперь выступают атомарные условия, а область данных D рассматривается как алгебраическая система с сигнатурой операций Ω и сигнатурой предикатов Π [4] . Алгебра $T_D(R)$ становится алгебраической системой, если атомарные условия $\pi(t_1,\ldots,t_m)$ считать истинным тогда и только тогда, когда оно является тождественно истинным, т.е. $\pi(t_1(z),\ldots,t_m(z)) = 1$ для любых $z \in D^n$. Эта система является свободной в основном многообразии, которое теперь является наименьшим многообразием алгебраических систем, которому принадлежит D. Понятие алгебраического замыкания C(M) множества атомарных условий определяется так же, как и для случая равенств с добавлением следующего требования: если $\pi(t_1,\ldots,t_m) \in C(M)$ и $t_1 = t_1',\ldots,t_m = t_m' \in C(M)$, то $\pi(t_1',\ldots,t_m') \in C(M)$. Если M - алгебраически замкнутое множество, то множество равенств из M является конгруэнцией абсолютно свободной алгебраической системы T(R), содержащей все тождества, и можно определить фактор-систему $T_D(R)|_M$, так же как

систему, построенную с помощью индуцированной конгруэнции. Определяя для каждого оператора присваивания $y = (r := t(r))$ и атомарного условия u гомоморфизм $\gamma_{u,y,M}: T_D(R) \to T_D(R)|C_D(M \cup \{u\})$ соотношением $\gamma_{u,y,M}(r_i) = t_i (\mathrm{mod}\ C_D(M \cup \{u\}))$, получим аналоги теоремы I и следствие из нее.

Т е о р е м а I. $J(M, u, y)$ есть ядро гомоморфизма $\gamma_{u,y,M}$.

С л е д с т в и е I. Система $T_D(R)|J(M, u, y)$ изоморфна подсистеме $F = [t_1, \ldots, t_n]$ системы $F = T_D(R)/C_D(M \cup \{u\})$, порожденной элементами $t_1, \ldots, t_n$.

Аналоги теоремы 2 и следствия 2 сохраняются для равенств множества $J(M, u, y)$, если вместо равенств по модулю M рассматривать равенства по модулю $C_D(M \cup \{u\})$. В частности, если сигнатура условий Π состоит только из одного равенства, то все результаты для наследственно свободных алгебр могут быть соответствующим образом усилены путем учета условий в переходах.

При рассмотрении атомарных условий иногда полезно выполнять сокращение сигнатуры предикатов, выбрасывая те из них, которые могут быть выражены через другие. Пусть в основном многообразии выполняется условие $\pi(g_1, \ldots, g_m) \langle\Rightarrow\rangle \pi'(h_1(g_1), \ldots, h_k(g))$. Тогда, очевидно, всякое замкнутое множество условий имеет D-базис, не содержащий условий вида $\pi(\ldots)$. Обозначим через $J^{\pi}(M, u, y)$ - множество условий вида $\pi(\ldots)$ из $J(M, u, y)$, а через $C_D^{\pi}(M)$ - множество таких условий из $C_D(M)$. Имея в виду зависмости между условиями основного многообразия, можно вычислять не все множества $J(M, u, y)$, а только $J^{\pi}(M, u, y)$ для тех π, через которые выражаются другие условия. Особенно просто J^{π} определяется для одноместных предикатов. Пусть $\gamma = \gamma_{u,y,M}$, $N^{\pi} = \{g \mid \pi(g) \in C_D^{\pi}(M \cup \{u\})\}$, $k^{\pi} = \{g \mid \pi(g) \in J^{\pi}(M, u, y)\}$. Тогда имеет место следующее предложение, очевидным образом вытекающее из теоремы I'.

С л е д с т в и е 2'. $k^{\pi} = \gamma^{-1}(N^{\pi})$.

Л и н е й н ы е а т о м а р н ы е у с л о в и я.

Пусть D – числовое поле, рассматриваемое с операциями сложения, вычитания, умножения на число и неравенством. Тогда алгебра $T_D(R)$ есть n-мерное векторное D – пространство, порожденное множеством R с неравенством $t_1 \le t_2$, которое выполняется для термов t_1 и t_2 тогда и только тогда, когда $t_1 = t_2$. Поскольку всякое равенство эквивалентно одноместному предикату $t = 0$, а неравенство – предикату $t \le 0$, то естественно ввести эти предикаты в сигнатуру системы D и оставить только их, отбросив бинарные равенство и неравенство.

Пусть M есть D – замкнутое множество атомарных условий. Обозначим через E(M) множество всех левых частей унарных равенств из M, а через E'(M) – множество всех левых частей унарных равенств. Очевидно, $E(M) \subset E'(M)$. Множество E(M) является подпространством пространства $T_D(R)$ и имеет, следовательно, конечный базис. Множество E'(M) замкнуто относительно сложения и умножения на неотрицательные скаляры, т.е. является линейным выпуклым конусом. Если E'(M) имеет конечное алгебраическое порождающее множество $h_1,\dots,h_k$, то оно состоит из всех неотрицательных линейных комбинаций $\sum_{i=1}^{k} \mu_i h_i (\mu_i \ge 0)$ векторов $h_1,\dots,h_k$. Отбросив векторы, принадлежащие подпространству E(M), а затем те из оставшихся векторов, которые представляются неотрицательными линейными комбинациями других, получим неприводимое порождающее множество $E'(M)\setminus E(M)$. Добавив к этому множеству векторы $h_1,\dots,h_m$, образующие базис подпространства E(M), и противоположные им векторы, получим D-базис множества E'(M) всех неравенств. При этом векторы $h_1,\dots,h_k$ определяются однозначно с точностью до постоянного неотрицательного множителя, а множество E'(M) состоит из всевозможных комбинаций вида $\sum_{i=1}^{m} \lambda_i g_i + \sum_{j=1}^{k} \mu_j h_j$, λ_i – произвольные числа, $\mu_j \ge 0$.

Если γ – линейное преобразование, M – замкнутое множество с конечным базисом, то $\gamma^{-1}(M)$ также будет иметь конечный базис. Действительно, выбрав по одному элементу из полных прообразов базиса неравенств множества M и добавив

к нему базис подпространства $\gamma^{-1}(E(M))$, получим порождающее множество для $\gamma^{-1}(M)$.

Задача о пересечении легко решается как простая геометрическая задача о пересечении подпространств и выпуклых линейных конусов.

Таким образом, последовательность $M_a^{(0)} \subset M_a^{(1)} \subset \ldots \subset M_a^{(k)} \subset \ldots$ определяется конструктивно. Однако она не всегда будет конечной, поскольку при вычислении $J(M, u, y)$ и M каждый раз добавляется условие u.

Рассмотренные методы легко распространить на случай аффинных равенств и неравенств, т.е. для алгебры данных, которая дополнительно включает в себя операцию добавления константы. Один из способов решения задачи об инвариантах состоит в следующем. Пусть программа содержит константы $a_1, \ldots, a_k$. Вводим новые переменные $r_1, \ldots, r_k, r_{k+1}$ и добавляем к начальным условиям соотношения $r_1 = a_1 r_{k+1}, \ldots, r_k = a_k r_{k+1}$. Далее рассматриваем линейную задачу для расширенного множества переменных.

Задача о линейных атомарных условиях рассматривалась в работе [3], однако приведенное в ней решение значительно менее полно, чем то, которое предлагается здесь, и, по-видимому, сложнее в вычислительном отношении.

Литература

1. В.М.Глушков, Ю.В.Капитонова, А.А.Летичевский. Теоретические основы проектирования дискретных систем.-Кибернетика, 1977, № 6.
2. Letichevsky A.A. Equivalence and optimization of programs, International Symposium on Theoretical Programming, Lecture Notes in Computer Science, 1974, N 5.
3. Cuasot P., Halbwachs N. Automatic discovwry of linear restrictions among variables of program, Conference Record of the 5-th Annual ACM Symposium on Principles of Programming Languages, Jan. 23-25, 1978, USA.