дится понятие реализуемости формулы в вычислительной среде. Абсолютно реализуемыми называем формулы, реализуемые в любой вычислительной среде. Будем рассматривать вычисления с конечным числом занимаемых ячеек ленты. Абсолютную реализуемость в такой модели будем называть конечной реализуемостью.

ТЕОРЕМА 1 (о полноте и непротиворечивости теории для модели вычислителя с конечной памятью). *В построенной теории доказуемы все конечно реализуемые формулы и только они.*

ТЕОРЕМА 2 (о неполноте и непротиворечивости теории для вычислителя с бесконечной памятью). *В построенной формальной теории все доказуемые формулы абсолютно реализуемы. Множество абсолютно реализуемых формул не является рекурсивно-перечислимым.*

РАСПРЕДЕЛЕННЫЕ И ВЕРОЯТНОСТНЫЕ СВОЙСТВА ПРОГРАММ

Бордаченкова Е.А., Москва

Предлагается аппарат для анализа программ в предположении, что начальные значения программных переменных выбираются в соответствии с известным распределением вероятностей.

Используются обозначения: S - программа с множеством состояний памяти V, α, β, γ - предикаты на V, μ_k, ν - меры на V, μ, η - переменные, принимающие значения в множестве мер на V, φ, ψ - предикаты на множестве мер на V.

Рассмотрим свойство

$$\{\varphi(\mu(\alpha_1), \ldots, \mu(\alpha_n))\}\, S\, \{\psi(\mu(\gamma_1), \ldots, \mu(\gamma_k))\}. \qquad (1)$$

ОПРЕДЕЛЕНИЕ. Пусть μ_0 - произвольное значение переменной μ, для которого формула

$$\varphi(\mu(\alpha_1), \ldots, \mu(\alpha_n)) \wedge (\mu(\mathrm{wlp}(S, л)) = 0)$$

принимает значение "истина". Пусть для любого α мера ν определяется следующим образом: $\nu(\alpha) = \mu_0(\mathrm{wp}(S, \alpha))$. Если для значения ν переменной μ формула $\psi(\mu(\gamma_1), \ldots, \mu(\gamma_k))$ принимает значение "истина", будем говорить, что справедливо распределенное свойство (1).

Можно показать, что функция ν, участвующая в определении, является мерой и определена для любого α на V.

Приведем правила доказательства распределенных свойств.

1. Распределенное свойство (1) выполняется тогда и только тогда, когда справедлива импликация

$$\varphi(\mu(\alpha_1),\ldots,\mu(\alpha_n)) \wedge (\mu(\mathrm{wlp}(S,\Lambda)) = 0) \supset$$

$$\supset \psi(\mu(\mathrm{wp}(S,\gamma_1)),\ldots,\mu(\mathrm{wp}(S,\gamma_k))).$$

2. Пусть выполнено распределенное свойство (1), тогда

а) если $\varphi_1(\mu(\beta_1),\ldots,\mu(\beta_l)) \supset \varphi(\mu(\alpha_1),\ldots,\mu(\alpha_n))$, то справедливо $\{\varphi_1(\mu(\beta_1),\ldots,\mu(\beta_l))\}\ S\ \{\psi(\mu(\gamma_1),\ldots,\mu(\gamma_k))\}$;

б) если $\psi(\mu(\gamma_1),\ldots,\mu(\gamma_k)) \supset \psi_1(\mu(\beta_1),\ldots,\mu(\beta_l))$, то справедливо $\{\varphi(\mu(\alpha_1),\ldots,\mu(\alpha_n))\}\ S\ \{\psi_1(\mu(\beta_1),\ldots,\mu(\beta_l))\}$.

3. Если выполнены свойства $\{\varphi_1\}\ S\ \{\psi_1\}$ и $\{\varphi_2\}\ S\ \{\psi_2\}$, то выполняется распределенное свойство $\{\varphi_1 \wedge \varphi_2\}\ S\ \{\psi_1 \wedge \psi_2\}$.

4. Распределенное свойство $\{\varphi(\mu(\alpha_1(a,\ldots,z)),\ldots,)\}z := f(a,\ldots,z)\{\psi(\mu(\gamma_1(a,\ldots,z)),\ldots)\}$ справедливо тогда и только тогда, когда истинна импликация

$$\varphi(\mu(\alpha_1)(a,\ldots,z)),\ldots) \wedge (\mu(\mathrm{wlp}(z:=f(a,\ldots$$

$$\ldots,z),\Lambda)) = 0) \supset \psi(\mu(\gamma_1(a,\ldots,f(a,\ldots,z))),\ldots).$$

5. Распределенное свойство $\{\varphi\}\ S;\ Q\{\psi\}$ справедливо тогда и только тогда, когда существует предикат ξ, определенный на множестве мер на V, такой, что справедливы свойства $\{\varphi\}\ S\ \{\xi\}$ и $\{\xi\}\ Q\ \{\psi\}$.

6. Распределенное свойство $\{\varphi(\mu(\alpha_1),\ldots)\}$ if β then Q fi $\{\psi(\mu(\gamma_1),\ldots)\}$ выполняется тогда и только тогда, когда для любого значения переменной η выполняется свойство $\{\varphi(\mu(\alpha_1)+\eta(\alpha_1),\ldots)\wedge(\mu(\beta)=0)\wedge(\eta(\beta)=0)\}$ Q $\{\psi(\mu(\gamma_1)+\eta(\gamma_1),\ldots)\}$. Переменная η является аналогом "свободной переменной" в системах Ч. Хоара и Э. Дейкстры.

Прежде чем сформулировать следующее правило, определим понятие распределенного инварианта. Рассматривается оператор $S \equiv$ $\equiv$ while β do Q od . Пусть π_{μ_k} - предикат, множество истинности которого состоит из единственной меры μ_k. Пусть μ_0 - произвольная мера такая, что $\mu_0(\mathrm{wlp}(S,\Lambda)) = 0$. Последовательность мер μ_1, μ_2, образованную по правилу: мера μ_k такова, что выполняется свойство $\{\pi_{\mu_{k-1}}\}$ if β then Q fi $\{\pi_{\mu_k}\}$, $k = 1,2,\ldots,$ назовем последовательностью потомков меры μ_0. Функцию $\tilde{\mu}$, определенную следующим образом: $\tilde{\mu}(\alpha) = \lim\limits_{k\to\infty} \mu_k(\alpha)$, будем называть пределом последовательности потомков. Можно доказать, что $\tilde{\mu}$ определена для всех α на V и является мерой.

ОПРЕДЕЛЕНИЕ. Предикат ξ, определенный на множестве мер, называется распределенным инвариантом цикла S, если

1) справедливо распределенное свойство

$$\{\xi\}\ \text{if}\ \beta\ \text{then Q fi}\ \{\xi\};$$

2) для любой меры μ_0, удовлетворяющей ξ, такой, что $\mu(\mathrm{wlp}(S,\Lambda)) = 0$, , предел $\tilde{\mu}$ последовательности потомков μ_0 также удовлетворяет ξ.

7. Распределенное свойство $\{\varphi\}$ while β do Q od $\{\psi\}$ справедливо тогда и только тогда, когда существует распределенный инвариант ξ такой, что $\varphi \supset \xi$ и $\xi \wedge (\mu(\beta) = 0) \supset \psi$.

Распределенные свойства программ, в пред- и постусловиях которых участвуют только вероятностные меры, будем называть вероятностными свойствами. Заметим, что отображение множества мер на V в себя, индуцируемое программой, вероятностную меру переводит в вероятностную меру.

Пусть $\{\alpha\}S\{\beta\}$ - хоаровское свойство. Оно справедливо тогда и только тогда, когда справедливо вероятностное свойство $\{\mu(\alpha) = 1\}\ S\ \{\mu(\beta) = 1\}$.

Правила доказательства вероятностных свойств легко получить из правил доказательства распределенных свойств, имея в виду, что вероятностное свойство $\{\varphi(\mu)\}\ S\{\psi(\mu)\}$ эквивалентно распределенному свойству

$$\{\varphi(\mu) \wedge (\mu(и) = 1)\}\ S\ \{\psi(\mu) \wedge (\mu(и) = 1)\}.$$

Приведем пример использования предлагаемого аппарата. Рассмотрим известную игру "Угадай наибольшее число": один игрок готовит последовательность целых чисел, длина последовательности известна заранее. Числа по одному предъявляются второму игроку. Если втсрой игрок считает, что ему предъявлено наиболь - шее число последовательности, он останавливает процесс. Второй игрок проигрывает, если он указал не на максимальное число или если он не указал ни на одно число. Рассмотрим следующую стратегию поведения второго игрока: просматривается первая половина чисел, и из нее выбирается максимальное число М. Во второй половине указывается на первое число, большее М.

Для программы, реализующей данную стратегию, с помощью предлагаемой методики доказывается, что вероятность выигрыша не меньше 1/4.