27.10.10 Лекция 5

Предикатное программирование

Однозначность предикатов
Однозначность предикатов рекурсивного кольца
Теорема об однозначности предикатов
4. Система правил доказательства корректности программы
Правила для однозначной спецификации
Правила для общего случая
Правила декомпозиции доказательства для однозначной спецификации
Правила декомпозиции доказательства для общего случая
Задачи верификации и синтеза
5. Построение языка предикатного программирования. Методы доказательства корректности предикатных программ
Язык P1: подстановка определения предиката на место вызова
Язык P2: оператор суперпозиции и параллельный оператор общего вида
Язык P2: другое обобщение оператора суперпозиции
Язык P3: выражения

Пусть рекурсивный предикат $D(z: u)$ принадлежит кольцу (3.36), т.е. $D = A_j$ для некоторого j. Логическая семантика предиката D определяется следующим образом:

$$LS(D(z: u)) \cong (z, u) \in pr(j, \bigcup_{m \geq 0} G^m) \qquad (3.40)$$

Систему (3.36) определений кольца предикатов запишем в векторном виде: $A \equiv K(A)$, где $A = (A_1, A_2, \ldots, A_n)$, $K = (K_1, K_2, \ldots, K_n)$. Определим цепь векторов предикатов $\{A^m\}_{m \geq 0}$:

$$A^0 \equiv \Phi,\ A^{m+1} \equiv K(A^m),\ m \geq 0, \qquad (3.41)$$

где $\Phi \cong (F, F, \ldots, F)$ — вектор тотально ложных предикатов. Цепь $\{A^m\}_{m \geq 0}$ соответствует цепи (3.39) вектор-графиков $\{G^m\}_{m \geq 0}$, поскольку $G^m = (Gr(A^m{}_1), Gr(A^m{}_2), \ldots, Gr(A^m{}_n))$.

$$G^0 = \varnothing,\ G^{m+1} = V(G^m),\ m \geq 0 \qquad (3.39)$$

$$A_i(x_i: y_i) \equiv K_i(x_i: y_i);\ i = 1 \ldots n;\ n > 0, \qquad (3.36)$$

Рекурсивное кольцо предикатов представим в виде:

$$A \equiv K(A_1, A_2, \ldots, A_n, E_1, E_2, \ldots, E_s) \qquad (3.42)$$

$E_1, E_2, \ldots, E_s$, $s > 0$, —предикаты, используемые в правых частях определений (3.36), но не принадлежащих данному кольцу.

Лемма 3.16. Пусть предикаты $E_1, E_2, \ldots, E_s$, используемые в системе (3.42), обладают свойством согласованности. Тогда рекурсивные предикаты $A_1, A_2, \ldots, A_n$ кольца (3.42) обладают свойством согласованности.

3. Язык исчисления вычислимых предикатов (продолжение 3)

Однозначность предикатов

Лемма 3.17. Оператор суперпозиции (3.16), параллельный оператор (3.19) или условный оператор (3.20) является однозначным, если вызываемые в операторе предикаты B и C являются однозначными.

Лемма 3.18. Пусть имеется рекурсивное кольцо предикатов (3.42). Кроме рекурсивных предикатов $A_1, A_2,\dots,A_n$ в правых частях определений кольца предикатов используются предикаты $E_1, E_2,\dots, E_s$. Предположим, что предикаты $E_1, E_2,\dots, E_s$ являются однозначными. Если аргумент определения кольца имеет предикатный тип, то предикат, являющийся значением аргумента, считается однозначным. Тогда рекурсивные предикаты $A_1, A_2,\dots,A_n$ кольца (3.42) являются однозначными.

Доказательство. Из-за ограничений на сложные формы рекурсии предикат, являющийся значением аргумента, не может входить в кольцо предикатов. Поэтому можно считать, что такой предикат находится среди $E_1, E_2,\dots, E_s$.

$$A \equiv K(A_1, A_2,\dots, A_n, E_1, E_2,\dots, E_s) \qquad (3.42)$$

Пусть $D(u: v)$ —рекурсивный предикат кольца, т.е. $D = A_j$ для некоторого j. Допустим, истинны $D(u: v1)$ и $D(u: v2)$. Необходимо доказать, что $v1 = v2$. В соответствии с леммой 3.13 существует m, при котором $D^m(u: v1)$ и $D^m(u: v2)$ — истинны. Поэтому достаточно доказать, каждый элемент A^m цепи $\{A^m\}_{m\geq0}$, определенной в (3.41), является вектором однозначных предикатов. Доказательство проводится индукцией по m.

Элемент A^0 является вектором однозначных предикатов, поскольку тотально ложный предикат F является однозначным. Допустим, по индуктивному предположению, A^{m-1} является вектором однозначных предикатов. Докажем это свойство для A^m. В правой части каждого определения из A^m используется оператор суперпозиции, параллельный оператор или условный оператор. Вызываемые предикаты в правой части: $A^{m-1}{}_1, A^{m-1}{}_2, \ldots, A^{m-1}{}_n$ и $E_1, E_2, \ldots, E_s$ —однозначны. Однозначность компонент A^m следует из леммы 3.17. □

Базисные предикаты $ConsPred$ и $ConsArray$ не являются однозначными. В двух разных исполнениях вызова $ConsPred(x, B: A)$ (при совпадающих x и B) в качестве значения переменной A будут получены разные имена.

Лемма 3.19. Вызов C(…), где C — переменная предикатного типа, является однозначным, если для каждого вызова конструктора ConsPred(x, B: A) или ConsArray(x, B: A) предикат B является однозначным.

Теорема 3.2. Допустим, всякий базисный предикат языка CCP, кроме ConsPred и ConsArray, является однозначным. Пусть имеется программа на языке CCP, и ее исполнение реализуется вызовом предиката D(u: v), причем в наборе v нет переменных предикатного типа. Тогда предикат D является однозначным.

Доказательство. Сначала доказательство проводится для программы, в которой нет переменных предикатного типа.

Рассмотрим случай, когда программа не содержит рекурсивно определяемых предикатов. Если предикат D — базисный, то его однозначность гарантируется условием теоремы. Пусть предикат D имеет определение в виде оператора суперпозиции, параллельного оператора или условного оператора. В соответствии с леммой 3.17 достаточно установить однозначность предикатов B и C, вызываемых в правой части определения. Если эти предикаты — базисные, то их однозначность является условием теоремы. Если один из них — определяемый, то его полное замкнутое определение — программа меньшего размера. Далее по индукции.

Имеется рекурсивных дерево колец (теорема 3.1). Для колец, являющихся листьями, однозначность следует из леммы 3.18. Применяется индукция по длине пути в дереве колец. Доказательство легко обобщается для случая, когда в программе имеются переменные предикатного типа, а их значения — однозначные предикаты.

Допустим, в программе П имеются переменные предикатного типа. Обозначим через SUBS(П) набор предикатов, являющийся объединением множеств заместителей для всех переменных предикатного типа в программе П. Для набора предикатов M из П обозначим через П[M] минимальную программу, являющуюся частью П и содержащую определения предикатов набора M. Пусть $П_0 = П$, $П_{j+1} = П_j[SUBS(П_j)]$, $j=0, 1, 2, \ldots$. В теореме 3.1 доказано, что для некоторого k программа $П_k \neq \varnothing$, а $П_{k+1} = \varnothing$. Программа $П_k$ не содержит переменных предикатного типа. Однозначность предикатов программы $П_k$ доказана выше. Тогда предикаты $B_1, B_2, \ldots, B_n$, входящие в $SUBS(П_{k-1})$, являются однозначными. В соответствии с леммой 3.19 любой вызов вида C(…) в программе $П_{k-1}$, где C — переменная предикатного типа, является однозначным. Доказательство теоремы, представленное выше, обобщается для программы $П_{k-1}$, поскольку согласно принятым ограничениям вызов вида C(…) не может участвовать в рекурсии. Доказательство теоремы для произвольной программы $П_i$, $i = k-1, \ldots, 0$, проводится по индукции. □

4. Система правил доказательства корректности операторов

4.1. Правила для однозначной спецификации

Предикат $B(x, y)$ корректен относительно $[P_B(x), Q_B(x, y)]$, если:

$$P(x) \Rightarrow [L_k(x, y) \Rightarrow Q(x, y)] \ \& \ \exists y. L_k(x, y) \qquad (2.5)$$

$$P(x) \Rightarrow [LS(B(x, y)) \Rightarrow Q(x, y)] \ \& \ \exists y. LS(B(x, y) \qquad (4.1)$$

$$Corr(B, P, Q) \cong (4.1)$$

Правила для корректного оператора

Лемма 4.3. Пусть имеется оператор B со спецификацией в виде тройки Хоара $\{P_B(x)\}\ B\ \{Q_B(x, y)\}$. Предполагается, что оператор B является корректным Тогда истинны следующие правила вывода:

Правило E1. $P_B(x) \vdash \exists y. Q_B(x, y)$

Правило E2. $P_B(x) \vdash \exists y. LS(B(x, y))$

Правило E3. $P_B(x) \vdash LS(B(x, y)) \Rightarrow Q_B(x, y)$

Теорема 2.1 тождества спецификации и программы

$$P(x)\ \{\ S\ (x, y)\ \blacklozenge_k\ \}\ Q(x, y) \qquad (2.1)$$

Оператор $S(x, y)$ является однозначным, а спецификация $[P(x), Q(x, y)]$ — тотальной. Пусть истина формула:

$$P(x)\ \&\ Q(x, y) \Rightarrow LS(S(x, y)) \qquad (4.6)$$

Тогда программа (2.1) является корректной.

Лемма 2.8. В условиях теоремы 2.1 истинна ф-ла:

$$P(x) \Rightarrow (LS(S(x, y)) \equiv Q(x, y))$$

Лемма 2.9. Допустим, программа (2.1) является корректной, а ее спецификация — однозначной. Тогда истинна формула (4.6), т.е. $LS(S(x, y))$ выводима из спецификации.

Правила для параллельного оператора

$$\{P(x)\}\ A \parallel B\ \{Q(x, y, z)\} \qquad (4.17)$$

$$\{P_A(x)\}\ A\ \{Q_A(x, y)\}, \qquad \{P_B(x)\}\ B\ \{Q_B(x, z)\}$$

Правило LP1. $P(x) \vdash P_B(x)\ \&\ P_C(x)$

Правило LP2. $P(x)\ \&\ Q(x, y, z) \vdash Q_A(x, y)$.

Правило LP3. $P(x)\ \&\ Q(x, y, z) \vdash Q_B(x, z)$.

Лемма 4.10. Пусть спецификация параллельного оператора (4.17) реализуема, операторы A и B однозначны в области предусловий и корректны, а их спецификации —однозначны. Если правила **LP1**, **LP2** и **LP3** истинны, то параллельный оператор (4.17) является корректным.

Доказательство. Операторы A и B —однозначны ⇒ оператор (4.17) однозначный. Поскольку спецификация оператора (4.17) реализуема, в соответствии с теоремой 2.1 достаточно доказать:

$$P(x)\ \&\ Q(x, y, z) \Rightarrow LS(A \parallel B)(x, y, z)$$

$$LS(A \parallel B)(x, y, z) \cong LS(A)(x, y)\ \&\ LS(B)(x, z) \qquad (4.2)$$

Пусть истинны $P(x)$ и $Q(x, y, z)$. Докажем истинность $LS(A)(x, y)$ и $LS(B)(x, z)$. Из истинности предусловия $P(x)$ по правилу **LP1** следует истинность $P_A(x)$ и $P_B(x)$. По правилам **LP2** и **LP3** становятся истинными $Q_A(x, y)$ и $Q_B(x, z)$. Для предикатов A и B выполняются условия леммы 2.9. Поэтому истинны формулы:

$$P_A(x)\ \&\ Q_A(x, y) \Rightarrow LS(A)(x, y) \qquad P_B(x)\ \&\ Q_B(x, z) \Rightarrow LS(B)(x, z)$$

Посылки этих формул истинны ⇒ истинны $LS(A)(x, y)$ и $LS(B)(x, z)$. □

Правила для оператора суперпозиции

$$\{P(x)\}\ A;\ B\ \{Q(x, y)\} \qquad (4.18)$$

$$\{P_A(x)\}\ A\ \{Q_A(x, z)\}, \qquad \{P_B(z)\}\ B\ \{Q_B(z, y)\}$$

Правило LS1. $P(x) \vdash P_A(x)$

Правило LS2. $P(x)\ \&\ Q(x, y)\ \&\ Q_A(x, z) \vdash P_B(z)\ \&\ Q_B(z, y)$

Лемма 4.11. Пусть спецификация оператора суперпозиции (4.18) реализуема, операторы A и B однозначны в области предусловий и корректны, а их спецификации — однозначны. Если правила **LS1** и **LS2** истинны, то оператор суперпозиции (4.18) является корректным.

Доказательство. Поскольку операторы A и B —однозначны, то и оператор суперпозиции (4.18) является однозначным. В соответствии с теоремой 2.1 для доказательства леммы достаточно доказать истинность формулы:

$$P(x)\ \&\ Q(x, y) \Rightarrow LS(A; B)(x, y)$$

$$LS(A; B)(x, y) \cong \exists z.(LS(A)(x, z)\ \&\ LS(B)(z, y)) \qquad (4.1)$$

Пусть истинны $P(x)$ и $Q(x, y)$. Докажем истинность $\exists z.(LS(A)(x, z) \mathbin{\&} LS(B)(z, y))$. Из истинности предусловия $P(x)$ по правилу **LS1** следует истинность $P_A(x)$. Из корректности оператора A по правилу **E2** следует истинность формулы $\exists z.\ LS(A)(x, z)$. Допустим для некоторого z_0 истинно $LS(A)(x, z_0)$. Для оператора A истинны условия леммы 2.8. Поэтому истинно $Q_A(x, z_0)$. В соответствии с правилом **LS2** истинна формула $P_B(z_0) \mathbin{\&} Q_B(z_0, y)$. В соответствии с леммой 2.9 истинна формула

$$P_B(z) \mathbin{\&} Q_B(z, y) \Rightarrow LS(B)(z, y)$$

Тогда истинна $LS(B)(z_0, y)$. В итоге, будет истинна формула $\exists z.(LS(A)(x, z) \mathbin{\&} LS(B)(z, y))$. □

Правила для условного оператора

$$\{P(x)\}\ \textbf{if}\ \textbf{(}C)\ A\ \textbf{else}\ B\ \{Q(x, y)\} \qquad (4.19)$$

$$\{P_A(x)\}\ A\ \{Q_A(x, y)\}, \qquad \{P_B(x)\}\ B\ \{Q_B(x, y)\}$$

Правило LC1. $P(x)\ \&\ Q(x, y)\ \&\ C \vdash P_A(x)\ \&\ Q_A(x, y)$

Правило LC2. $P(x)\ \&\ Q(x, y)\ \&\ \neg C \vdash P_B(x)\ \&\ Q_B(x, y)$

Лемма 2.12. Пусть спецификация условного оператора (4.19) реализуема, операторы A и B однозначны в области предусловий и корректны, а их спецификации — однозначны. Если правила **LC1** и **LC2** истинны, то условный оператор (4.19) является корректным.

Доказательство. Поскольку операторы A и B —однозначны, то и условный оператор (4.19) является однозначным. В соответствии с теоремой 2.1 для доказательства леммы достаточно доказать:

$$P(x)\ \&\ Q(x, y) \Rightarrow LS(\ \textbf{if}\ \textbf{(}C)\ A\ \textbf{else}\ B\ )\ (x, y)$$

$$LS(\textbf{if}\ \textbf{(}C)\ A\ \textbf{else}\ B)(x, y) \cong (C \Rightarrow LS(A)(x, y))\ \&\ (\neg C \Rightarrow LS(B)(x, y)) \quad (4.3)$$

Пусть истинны $P(x)$ и $Q(x, y)$. Докажем истинность формулы $C \Rightarrow LS(A)(x, y)$. Пусть истинно C. Докажем истинность $LS(A)(x, y)$. Можно применить правило **LC1**, поскольку истинны $P(x)$, $Q(x, y)$ и C. Получим истинность формулы $P_A(x) \& Q_A(x, y)$. В соответствии с леммой 2.9 истинна формула

$$P_A(x) \& Q_A(x, y) \Rightarrow LS(A)(x, y)$$

Поскольку истинна посылка, то истинно $LS(A)(x, y)$. Следовательно, доказана истинность формулы $C \Rightarrow LS(A)(x, y)$. Истинность формулы $\neg C \Rightarrow LS(B)(x, y)$ доказывается аналогично. □

4. Система правил доказательства корректности программы 4.2. Правила для общего случая

Правила для параллельного оператора

$$\{P(x)\}\ A \parallel B\ \{Q(x, y, z)\} \qquad (4.11)$$

$$\{P_A(x)\}\ A\ \{Q_A(x, y)\}, \qquad \{P_B(x)\}\ B\ \{Q_B(x, z)\}$$

Правило RP1. $P(x) \vdash P_A(x) \,\&\, P_B(x)$

Правило RP2. $Q_A(x, y), Q_B(x, z) \vdash Q(x, y, z)$

Лемма 4.4. Пусть предусловие $P(x)$ истинно. Допустим, операторы A и B корректны. Если правила RP1 и RP2 истинны (т.е. правая часть доказуема из левой части для каждого правила), то параллельный оператор (4.11) является корректным.

Доказательство. В соответствии с формулой (4.1) достаточно доказать реализуемость $LS(A \parallel B)$ и выводимость постусловия $Q(x, y, z)$ из $LS(A \parallel B)$.

$$\mathbf{LS(A \parallel B)(x, y, z) \cong LS(A)(x, y) \,\&\, LS(B)(x, z).}$$

Из истинности предусловия $P(x)$ по правилу **RP1** следует истинность $P_A(x)$ и $P_B(x)$. Далее, по правилу **E2** становятся истинными формулы $\exists y.\ LS(A)(x, y)$ и $\exists z.\ LS(B)(x, z)$. Их конъюнкция определяет реализуемость $LS(A \,||\, B)(x, y, z)$.

Докажем выводимость постусловия $Q(x, y, z)$ из $LS(A)(x, y)\ \&\ LS(B)(x, z)$. Допустим, истинна $LS(A)(x, y)\ \&\ LS(B)(x, z)$. Применим правило **E3** для $P_A(x)$ и $P_B(x)$, истинность которых определена выше. Получаем истинность формул $LS(A)(x, y) \Rightarrow Q_A(x, y)$ и $LS(B)(x, z) \Rightarrow Q_B(x, z)$. Как следствие, будут истинны $Q_A(x, y)$ и $Q_B(x, z)$. Применяя правило **RP2**, получаем истинность постусловия $Q(x, y, z)$. □

Правила для оператора суперпозиции

$\{P(x)\}\ A;\ B\ \{Q(x, y)\}$ (4.12)

$\{P_A(x)\}\ A\ \{Q_A(x, z)\},\ \ \{P_B(z)\}\ B\ \{Q_B(z, y)\}$

Правило RS1. $P(x)\ \vdash P_A(x)\ \&\ \forall z\ (Q_A(x, z) \Rightarrow P_B(z))$

Правило RS2. $P(x)\ \&\ \exists z\ (Q_A(x, z)\ \&\ Q_B(z, y)) \vdash Q(x, y)$

Лемма 4.5. Пусть предусловие $P(x)$ истинно. Допустим, операторы A и B корректны. Если правила **RS1** и **RS2** истинны, то оператор суперпозиции (4.12) является корректным.

Доказательство. В соответствии с формулой (4.1) достаточно доказать реализуемость $LS(A; B)(x, y)$ и выводимость постусловия $Q(x, y)$ из $LS(A; B)(x, y)$.

$$LS(A; B)(x, y) \cong \exists z.(LS(A)(x, z)\ \&\ LS(B)(z, y))\ .$$

Из истинности предусловия $P(x)$ по правилу **RS1** следует истинность формул $P_A(x)$ и $\forall z\ (Q_A(x, z) \Rightarrow P_B(z))$. Из истинности $P_A(x)$ и правила **E2** следует истинность формулы $\exists z.\ LS(A)(x, z)$. Допустим для некоторого z_0 формула $LS(A)(x, z_0)$ истинна. Из истинности $P_A(x)$ и правила **E3** следует истинность $LS(A)(x, z_0) \Rightarrow Q_A(x, z_0)$. Как следствие, истинно $Q_A(x, z_0)$. Далее, из истинности формулы $\forall z\ (Q_A(x, z) \Rightarrow P_B(z))$ следует истинность $P_B(z_0)$. По правилу **E2** истинна формула $\exists y\ LS(B)(z_0, y)$. Далее, истинна конъюнкция

$LS(A)(x,z_0)\ \&\ \exists y\ LS(B)(z_0, y)$, и затем — формула

$\exists y.\ \exists z.\ (LS(A)(x, z)\ \&\ LS(B)(z, y))$, т.е. доказана реализуемость $LS(A; B)(x, y)$.

Докажем выводимость постусловия $Q(x, y)$ из $LS(A; B)(x, y)$. Пусть $LS(A; B)(x, y)$ истинно, т.е. истинна формула $\exists z.(LS(A)(x, z) \,\&\, LS(B)(z, y))$. Пусть формула истинна для некоторого z_1. По правилу **E3** истинна формула $LS(A)(x, z_1) \Rightarrow Q_A(x, z_1)$ и далее — $Q_A(x, z_1)$. Истинность $Q_A(x, z_1)$ и $\forall z\, (Q_A(x, z) \Rightarrow P_B(z))$ влечет истинность $P_B(z_1)$. По правилу **E3** истинно $LS(B)(z_1, y) \Rightarrow Q_B(z_1, y)$. Поскольку $LS(B)(z_1, y)$ истинно, то истинно $Q_B(z_1, y)$. Таким образом, истинна правая часть правила **RS2**, а значит и левая, т.е. истинно постусловие $Q(x, y)$. □

Правила для условного оператора

$\{P(x)\}$ **if** (C) A **else** B $\{Q(x, y)\}$ (4.13)

$\{P_A(x)\}\ A\ \{Q_A(x, y)\}$, $\{P_B(x)\}\ B\ \{Q_B(x, y)\}$

Правило RC1. $P(x)\ \&\ C \vdash P_A(x)$

Правило RC2. $P(x)\ \&\ \neg C \vdash P_B(x)$

Правило RC3. $P(x)\ \&\ C\ \&\ Q_A(x, y) \vdash Q(x, y)$

Правило RC4. $P(x)\ \&\ \neg C\ \&\ Q_B(x, y) \vdash Q(x, y)$

Лемма 4.6. Пусть предусловие $P(x)$ истинно. Допустим, операторы A и B корректны. Если правила **RC1**, **RC2**, **RC3** и **RC4** истинны, то условный оператор (4.13) является корректным.

Доказательство. Для оператора (4.13) необходимо доказать формулу (2.10). В ней дважды встречается подформула $LS($**if** (C) A **else** $B)(x, y)$, определяемая в виде:

$$(C \Rightarrow LS(A)(x, y))\ \&\ (\neg C \Rightarrow LS(B)(x, y)) \qquad (4.14)$$

Достаточно доказать реализуемость формулы (4.14) и выводимость постусловия $Q(x, y)$ из (4.14).

Допустим, что условие C истинно. Из истинности предусловия $P(x)$ по правилу **RC1** следует истинность $P_A(x)$. По правилу **E2** истинна формула $\exists y.\ LS(A)(x, y)$. Далее будет истинной формула $\exists y.\ (C \Rightarrow LS(A)(x, y))$. Из истинности C следует истинность формулы $\neg C \Rightarrow LS(B)(x, y)$, и следовательно, формулы $\exists y.\ [(C \Rightarrow LS(A)(x, y))\ \&\ (\neg C \Rightarrow LS(B)(x, y))]$. Это обеспечивает реализуемость формулы (4.14) в случае истинности C. Реализуемость (4.14) в случае ложности C доказывается аналогичным образом.

Докажем выводимость постусловия $Q(x, y)$ из формулы (2.14). Допустим, истинна формула (4.14). Пусть C истинно. Тогда истинно $LS(A)(x, y)$. По правилу **RC1** истинно $P_A(x)$. По правилу **E3** истинна формула $LS(A)(x, y) \Rightarrow Q_A(x, y)$, а значит и $Q_A(x, y)$. Таким образом, истинна правая часть правила **RC3**. Тогда истинна левая часть правила, т.е. истинно постусловие $Q(x, y)$. Доказательство истинности постусловия $Q(x, y)$ для случая, когда C ложно, проводится аналогично с использованием правила **RC4**. □

4. Система правил декомпозиции доказательства корректности операторов

4.3. Правила для однозначной спецификации

Правила для параллельного оператора

Для параллельного оператора $A(x: y) \| B(x: z)$ определим правила:

Правило FP1. $R(x, y, z) \vdash LS(A(x, y))$

Правило FP2. $R(x, y, z) \vdash LS(B(x, z))$

Лемма 7. Если истинны правила **FP1** и **FP2**, то истинна формула:

$$R(x, y, z) \Rightarrow LS(A(x: y) \| B(x: z))$$

Доказательство. Формула $LS(A(x: y) \| B(x: z))$ эквивалентна $LS(A(x: y)) \;\&\; LS(B(x: z))$. Поэтому достаточно доказать истинность двух формул:

$$R(x, y, z) \Rightarrow LS(A(x: y))$$

$$R(x, y, z) \Rightarrow LS(B(x: z))$$

Эти формулы эквивалентны правилам **FP1** и **FP2**. □

$$P(x) \;\&\; Q(x, y) \Rightarrow LS(S(x, y)) \qquad (4.6)$$

Правила для условного оператора

Для условного оператора **if (**C) A(x**:** y) **else** B(x**:** y) определим правила:

Правило FC1. $R(x, y) \,\&\, C \vdash LS(A(x{:}\ y))$

Правило FC2. $R(x, y) \,\&\, \neg C \vdash LS(B(x{:}\ y))$

Лемма 9. Если истинны правила **FC1** и **FC2**, то истинна следующая формула:

$$R(x, y) \Rightarrow LS(\textbf{if } (C)\ A(x{:}\ y)\ \textbf{else}\ B(x{:}\ y))$$

Доказательство. Формула LS(**if (**C) A(x**:** y) **else** B(x**:** y)) эквивалентна

$$(C \Rightarrow LS(A(x{:}\ y)))\ \&\ (\neg C \Rightarrow LS(B(x{:}\ y)))$$

Таким образом, требуется доказать истинность:

$$R(x, y) \Rightarrow (C \Rightarrow LS(A(x{:}\ y)))\ \&\ (\neg C \Rightarrow LS(B(x{:}\ y)))$$

Последняя формула эквивалентна конъюнкции формул:

$$R(x, y) \Rightarrow (C \Rightarrow LS(A(x{:}\ y)))$$

$$R(x, y) \Rightarrow (\neg C \Rightarrow LS(B(x{:}\ y)))$$

А эти формулы эвивалентны правилам **FC1** и **FC2**. □

Правила для оператора суперпозиции

Для оператора суперпозиции A(x: z); B(x, z: y) определим правила:

более общего вида

Правило FS1. $R(x, y) \vdash \exists z.\ LS(A(x: z))$

Правило FS2. $R(x, y)\ \&\ LS(A(x: z)) \vdash LS(B(x, z: y))$

Лемма 3. Если истинны правила **FS1** и **FS2**, то истинна следующая формула:

$$R(x, y) \Rightarrow LS(A(x: z); B(x, z: y))$$

Доказательство. Формула LS(A(x: z); B(x, z: y)) эквивалентна $\exists z.(LS(A(x: z))\ \&\ LS(B(x, z: y)))$. Пусть истинно R(x, y). Докажем истинность $\exists z.(LS(A(x: z))\ \&\ LS(B(x, z: y)))$. По правилу **FS1** истинна формула $\exists z.\ LS(A(x: z))$. Допустим для некоторого z0 истинно LS(A(x: z0)). По правилу **FS2** истинна формула LS(B(x, z0: y)). В итоге, будет истинна формула $\exists z.(LS(A(x: z))\ \&\ LS(B(x, z: y)))$. □

- позиция квантора существования
- вхождение LS(…) в левой части

Правила для нерекурсивного вызова

Пусть имеется нерекурсивный вызов предиката A(x: y) со спецификацией:

$$\{P(x)\}\ A(x\text{: } y)\ \{Q(x, y)\} \qquad (3)$$

Для нерекурсивного вызова предиката A(x: y) определим правило:

Правило FB1. $R(x, y) \vdash P(x) \,\&\, Q(x, y)$

Лемма 15. Допустим, нерекурсивный вызов предиката A(x: y) является корректным, а его спецификация (3) — однозначна. Если истинно правило **FB1**, то истинна следующая формула:

$$R(x, y) \Rightarrow LS(A(x\text{: } y))$$

Доказательство. Пусть истинно R(x, y). Докажем истинность LS(A(x: y)). Поскольку истинна правая часть правила **FB1**, то истинна формула P(x) & Q(x, y) в правой части. В соответствии с леммой 2.9 истинна формула $P(x) \,\&\, Q(x, y) \Rightarrow LS(A(x\text{: } y))$ и, следовательно, LS(A(x: y)). □

4. Система правил декомпозиции доказательства корректности операторов

4.4. Правила для общего случая

Декомпозиция для параллельного оператора

$$\{P(x)\}\ B(x{:}\ y)\ \{Q(x, y)\}$$

$$Corr(B, P, Q) \cong P(x) \Rightarrow [LS(B(x, y)) \Rightarrow Q(x, y)]\ \&\ \exists y.\ LS(B(x, y) \quad (4.1)$$

$$\{P(x)\}\ A(x{:}\ y)\ \|\ B(x{:}\ z)\ \ \{Q(x, y, z)\}$$

$$Q(x, y, z) \cong Q1(x, y)\ \&\ Q2(x, z)$$

Лемма.

$$Corr(A(x{:}\ y)\ \|\ B(x{:}\ z), P, Q) = Corr(A(x{:}\ y), P, Q1)\ \&\ Corr(B(x{:}\ z), P, Q2)$$

Декомпозиция для условного оператора

$$\{P(x)\}\ B(x\!: y)\ \{Q(x, y)\}$$

$$Corr(B, P, Q) \cong P(x) \Rightarrow [LS(B(x, y)) \Rightarrow Q(x, y)]\ \&\ \exists y.\ LS(B(x, y) \quad (4.1)$$

$$\{P(x)\}\ \textbf{if } (C)\ A(x\!: y)\ \textbf{else } B(x\!: y)\ \{Q(x, y)\}$$

Лемма.

$$Corr(\textbf{if } (C)\ A(x\!: y)\ \textbf{else } B(x\!: y), P, Q) =$$
$$Corr(A(x\!: y), P\ \&\ C, Q)\ \&\ Corr(B(x\!: y), P\ \&\ \neg C, Q)$$

Декомпозиция для оператора суперпозиции

Рассмотрим спецификацию оператора суперпозиции в виде тройки Хоара:

$\{P(x)\}\ A;\ B\ \{Q(x, y)\}$. (2.12)

Предположим, что оператор A коррекетн. Спецификация представлены тройками:

$$\{PA(x)\}\ A\ \{QA(x, z)\},$$

Определим правила, гарантирующие корректность оператора суперпозиции (2.12).

Правило RS17. $P(x) \vdash PA(x) \ \&\ \forall z\ (QA(x, z) \Rightarrow \exists y\ LS(B)(z, y))$.

Правило RS18. $P(x) \ \&\ \exists z\ (QA(x, z) \ \&\ LS(B)(z, y)) \vdash Q(x, y)$.

Лемма 2.5. Пусть предусловие P(x) истинно. Допустим, оператор A корректен. Если правила RS1 и RS2 истинны, то оператор суперпозиции (2.12) является корректным.

Задачи верификации и синтеза

на примере оператора суперпозиции

$A(x\colon y) \equiv$ **pre** $P(x)$ { $B(x\colon z)$; $C(z\colon y)$ } **post** $Q(x, y)$ (3)

Операторы $B(x\colon z)$ и $C(z\colon y)$ корректны относительно своих спецификаций $[P_B(x), Q_B(x, z)]$ и $[P_C(z), Q_C(z, y)]$.

Спецификация $[P(x), Q(x, y)]$ тотальна. Корректность предиката A гарантируется в случае истинности правил:

Правило LS1. $P(x) \vdash P_B(x)$

Правило LS2. $P(x) \ \& \ Q(x, y) \ \& \ Q_B(x, z) \vdash P_C(z) \ \& \ Q_C(z, y)$

Задача дедуктивной верификации

Задача программного синтеза: требуется построить программу предиката A, представленного тотальной спецификацией $[P(x), Q(x, y)]$.

Пусть для некоторых предикатов $P_B(x)$, $Q_B(x, z)$, $P_C(z)$ и $Q_C(z, y)$ доказана истинность правил **LS1** и **LS2**. Тогда синтезируем программу (3).

Корректность оператора $S(x\colon y)$ относительно однозначной и тотальной спецификации $[P(x), Q(x, y)]$:

$$P(x) \ \& \ Q(x, y) \Rightarrow LS(S(x\colon y)) \qquad (2)$$

5. Построение языка предикатного программирования. Методы доказательства корректности предикатных программ

$$P(x) \Rightarrow [\ LS(S)(x, y) \Rightarrow Q(x, y)\ ]\ \&\ \exists y.\ LS(S)(x, y) \quad (4.1)$$

$$P(x)\ \&\ Q(x, y) \Rightarrow LS(S)(x, y) \quad (4.6)$$

Система правил доказательства корректности оператора суперпозиции, параллельного оператора и условного оператора

Исчисление вычислимых предикатов — множество вычислимых формул языка исчисления предикатов — язык **CCP** (Calculus of Computable Predicates)

минимальный полный базис языка предикатного программирования

Язык предикатного программирования P (**P**redicate programming language).

Расширяющаяся последовательность языков:

CCP = P0, P1, P2, P3, P4 = P.

Язык P1: подстановка определения предиката на место вызова

Подстановка определения предиката A(x: y) ≡ K(x: y) на место вызова A(t: z) — *блок* { K(t: z) }, где x, y, t, z — наборы переменных. Происходит замена вхождений переменных и переименование локалов.

LS({ K(t: z) }) ≅ LS(K(t: z)) **(5.1)**

runBlock(s, { K(t: z) }):

runStat(s, K(t: z)) **(5.2)**

Программа П', получаемая из программы П подстановкой определения предиката на место вызова, эквивалентна программе П': исполнение любого предиката программы П' на фиксированном наборе аргументов дает тот же результат, что и в программе П.

Язык **P1:** многократное произвольное применение подстановок определений предикатов на место вызовов.

Конструкция: вызов или блок как подоператор в трех базисных операторах

Язык **P2**: оператор суперпозиции и параллельный оператор общего вида

Операторы { A(…); B(…) }; C(…) и A(…); { B(…); C(…) } являются эквивалентными

Эквивалентны { A(…) || B(…) } || C(…) и A(…) || { B(…) || C(…) }

Язык **P2:** оператор суперпозиции и параллельный оператор общего вида: $A_1(\ldots); A_2(\ldots); \ldots ; A_n(\ldots)$ и $A_1(\ldots) \mathbin{||} A_2(\ldots) \mathbin{||} \ldots \mathbin{||} A_n(\ldots)$ для $n > 1$.

$P(x)\{B_1(x\!: z_1); B_2(z_1\!: z_2);\ldots; B_j(z_{j-1}\!: z_j);\ldots; B_n(z_{n-1}\!: y)\}Q(x, y)$ (5.3)

$x, z_1, z_2, \ldots, z_{n-1}, y$ — различные непересекающиеся наборы переменных, $B_1, B_2, \ldots, B_n$ обозначают предикаты или блоки языка **P1** со спецификациями (предусловиями и постусловиями) $P_{B1}(x)$, $Q_{B1}(x, z_1)$, $P_{B2}(z_1)$, $Q_{B2}(z_1, z_2)$, …, $P_{Bn}(z_{n-1})$, $Q_{Bn}(z_{n-1}, y)$.

$LS(B_1(x{:}\ z_1);\ B_2(z_1{:}\ z_2);\ldots;\ B_j(z_{j-1}{:}\ z_j);\ldots;\ B_n(z_{n-1}{:}\ y)) \equiv$

$\exists\ z_1, z_2, \ldots, z_{n-1}.LS(B_1(x{:}\ z_1))\ \&\ LS(B_2(z_1{:}\ z_2))\ \&\ldots\&$

$\&\ LS(B_j(z_{j-1}{:}\ z_j))\ \&\ldots\&\ LS(B_n(z_{n-1}{:}\ y))$ (5.4)

runStat(s, $B_1(x{:}\ z_1);\ \ldots;\ B_n(z_{n-1}{:}\ y)$)

runCallBlock(s, B1(x: z_1)); (5.5)

runCallBlock(s, B2(z_1: z_2)); .....;

runCallBlock(s, Bj(z_{j-1}: z_j)); .....;

runCallBlock(s, Bn(z_{n-1}: y))

Параллельный оператор общего вида

$P(x)\{B_1(x\colon y_1) \parallel B_2(x\colon y_2) \parallel \ldots \parallel B_j(x\colon y_j) \parallel \ldots \parallel B_n(x\colon y_n)\}Q(x, y)$ (5.7)

x, $y = y_1, \ldots, y_n$ — различные непересекающиеся наборы переменных, $B_1, B_2, \ldots, B_n$ — предикаты или блоки языка **P1** со спецификациями $P_{B1}(x)$, $Q_{B1}(x, y_1)$, $P_{B2}(x)$, $Q_{B2}(x, y_2), \ldots,$ $P_{Bn}(x)$, $Q_{Bn}(x, y_n)$.

$$LS(B_1(x\colon y_1) \parallel B_2(x\colon y_2) \parallel \ldots \parallel B_j(x\colon y_j) \parallel \ldots \parallel B_n(x\colon y_n)) \equiv$$

$$LS(B_1(x\colon y_1)) \;\&\; LS(B_2(x\colon y_2)) \;\&\; \ldots \;\&\; LS(B_j(x\colon y_j)) \;\&\; \ldots \;\&\; LS(B_n(x\colon y_n)) \quad (5.8)$$

$$runStat(s,\ B_1(\ldots) \parallel B_2(\ldots) \parallel \ldots \parallel B_n(\ldots))$$

$$runCallBlock(s, B_1(x\colon y_1)) \parallel \quad (5.9)$$
$$runCallBlock(s, B_2(x\colon y_2)) \parallel \ldots \parallel$$
$$runCallBlock(s, B_j(x\colon y_j)) \parallel \ldots \parallel$$
$$runCallBlock(s, B_n(x\colon y_n))$$

Правило опускания скобок:

$\{A(\ldots); B(\ldots)\} \parallel C(\ldots) \rightarrow A(\ldots); B(\ldots) \parallel C(\ldots)$.

$A(x\!: y); \{B(z\!: t) \parallel C(u\!: v)\}$

Набор y пересекается с набором z и не пересекается с набором u. Тогда

$A(x\!: y); \{B(z\!: t) \parallel C(u\!: v)\} \equiv \{A(x\!: y); B(z\!: t)\} \parallel C(u\!: v) \equiv$
$\equiv A(x\!: y); B(z\!: t) \parallel C(u\!: v)$.

$\{A(x\!: y) \parallel B(z\!: t)\}; C(u\!: v) \equiv A(x\!: y) \parallel B(z\!: t); C(u\!: v)$,
если наборы y и u не пересекаются.

Язык P2: другое обобщение оператора суперпозиции

$B(x\colon z);\ C(x, z\colon y)$ — обобщение оператора суперпозиции.

$P(x)\ \{B_1(x\colon z_1);\ B_2(x, z_1\colon z_2); \ldots;\ B_j(x, z_{j-1}\colon z_j); \ldots;\ B_n(x, z_{n-1}\colon y)\}\ Q(x, y)$

(5.10)

Частный случай: $B(x\colon z);\ C(u, z\colon y)$, набор u — часть набора x

Наиболее общая форма суперпозиции:

$A(x\colon t, y) \equiv P(x)\ \{B(x\colon z, t);\ C(x, z\colon y)\}\ Q(x, t, y)$ (5.11)

наборы x и t могут быть пустыми

Спецификации: $P_B(x)$, $Q_B(x, z, t)$, $P_C(x, z)$, $Q_C(x, z, y)$.

B1(x: x1, z, t1) ≡ P_B(x) {B(x: z, t1) || x1 = x} Q_B(x, z, t1) & x1 = x

C1(x1,z,t1: y, t) ≡ P_C(x1, z) {C(x1, z: y) || t = t1} Q_C(x1,z,y) & t = t1

Поскольку B1(x: x1, z, t1); C1(x1, z, t1: t, y) ≡ B(x: z, t); C(x, z: y), то справедливо другое определение предиката A:

A(x: t, y) ≡ P(x) {B1(x: x1, z, t1); C1(x1, z, t1: t, y)} Q(x, t, y) (5.12)

LS(B(x: z, t); C(x, z: y)) ≡ ∃z. (LS(B(x: z, t)) & LS(C(z, y))) (5.13)

runCallBlock(s, B(x: z, t)); (5.14)
runCallBlock (s, C(x, z: y))

Правило RS1’. P(x) ├

P_B(x) & ∀x1, z, t1 ((Q_B(x, z, t1) & x1 = x) ⇒ P_C(x1, z))

Правило RS2’. P(x) &

∃x1,z,t1 (Q_B(x1, z, t1) & x1 = x & Q_C(x1, z, y) & t = t1) ├

Q(x, t, y)

A(x: t, y) ≡ P(x) {B(x: z, t); C(x, z: y)} Q(x, t, y) (5.11)

Правило RS5. $P(x) \vdash P_B(x) \mathbin{\&} \forall z, t\ (Q_B(x, z, t) \Rightarrow P_C(x, z))$

Правило RS6. $P(x) \mathbin{\&} \exists z\ (Q_B(x, z, t) \mathbin{\&} (Q_C(x, z, y)) \vdash Q(x, t, y)$

Лемма 5.5. Пусть предусловие $P(x)$ истинно. Допустим, операторы B и C корректны. Если правила **RS5** и **RS6** истинны, то оператор суперпозиции (5.11) является корректным.

Правило LS1'. $P(x) \vdash P_B(x)$

Правило LS2'. $P(x) \mathbin{\&} Q(x, t, y) \mathbin{\&} Q_B(x, z, t1) \mathbin{\&} x1=x \vdash$

$$P_C(x1, z) \mathbin{\&} Q_C(x1, z, y) \mathbin{\&} t = t1$$

Правило LS6. $P(x) \vdash P_B(x)$

Правило LS7. $P(x) \mathbin{\&} Q(x, t, y) \mathbin{\&} Q_B(x, z, t1) \vdash$

$$P_C(x, z) \mathbin{\&} Q_C(x, z, y) \mathbin{\&} t = t1$$

Лемма 5.6. Допустим, спецификация оператора суперпозиции (5.11) реализуема, операторы B и C однозначны в области предусловий и корректны, а их спецификации — однозначны. Если правила **LS6** и **LS7** истинны, то оператор суперпозиции (5.11) является корректным.

Язык Р3: выражения

Функциональная форма. Предикат $A(t: z)$.

$$z = A(t) \cong A(t: z)$$

$|z| = A(t)$,   если z — набор

Инфиксная и постфиксная нотация как разновидность функциональной формы

$+(x, y: z)$, $-(x, y: z)$, $-(x: y)$, $<(x, y: b)$

$z = x + y$, $z = x - y$, $y = -x$, $b = x < y$.

Изображения констант:

ConsIntZero(: x)   ConsIntOne(: x)   valInt("2089" : x)

x = 0   x = 1   x = 2089

$B(x: z); C(x, z: y) \equiv z = B(x); C(x, z: y) \equiv C(x, B(x): y)$

$\{ A(x: y) \| B(z: t) \}; C(y, t: u) \equiv$

$\equiv \{ y = A(x) \| t = B(z) \}; C(y, t: u) \equiv C(A(x), B(z): u)$

$$D(x, z\textbf{:}\ u) \equiv P(x, z)\ \{C(A(x), B(z\textbf{:}\ u)\}\ Q(x, z, u) \qquad (5.15)$$

$$E(x, z\textbf{:}\ y, t) \equiv P_A(x)\ \&\ P_B(z)\{A(x\textbf{:}\ y) \parallel B(z\textbf{:}\ t)\}Q_A(x, y)\ \&\ Q_B(z, t)$$

$$D(x, z\textbf{:}\ u) \equiv P(x, z)\ \{\ E(x, z\textbf{:}\ y, t);\ C(y, t\textbf{:}\ u)\}\ Q(x, z, u) \qquad (5.16)$$

Правило RS1’.

$$P(x, z) \vdash P_A(x)\ \&\ P_B(z)\ \&\ \forall y,t\ (Q_A(x, y) \&\ Q_B(z, t) \Rightarrow P_C(y, t))$$

Правило RS2’.

$$P(x, z)\ \&\ \exists y,t.\ (Q_A(x, y)\ \&\ Q_B(z, t)\ \&\ Q_C(y, t, u)) \vdash Q(x, z, u)$$

Правило RS7. $P(x, z) \vdash P_A(x) \& P_B(z) \& P_C(A(x), B(z))$

Правило RS8. $P(x, z) \& Q_C(A(x), B(z), u) \vdash Q(x, z, u)$.

Лемма 5.7. Пусть предусловие $P(x, z)$ истинно. Допустим, операторы A, B и C корректны, операторы A и B, а также их спецификации $P_A(x)$, $Q_A(x, y)$, $P_B(z)$, $Q_B(z, t)$ —однозначны.. Если правила **RS7** и **RS8** истинны, то оператор (5.15) со спецификацией $P(x, z)$ и $Q(x, z, u)$ является корректным.

Для получения правил серии **L** применим правила **LS1** и **LS2** для оператора в правой части (5.16).

Правило LS1'. $P(x, z) \vdash P_A(x) \& P_B(z)$.

Правило LS2'.

$P(x, z) \& Q(x, z, u) \& Q_A(x, y) \& Q_B(z, t) \vdash P_C(y, t) \& Q_C(y, t, u)$.

Правило **LS8**. $P(x, z) \vdash P_A(x) \,\&\, P_B(z)$.

Правило **LS9**.

$$P(x, z) \,\&\, Q(x, z, u) \vdash P_C(A(x), B(z)) \,\&\, Q_C(A(x), B(z), u).$$

Лемма 5.8. Допустим, спецификация $P(x, z)$ и $Q(x, z, u)$ оператора (5.15) реализуема, операторы A, B и C однозначны в области предусловий и корректны, а их спецификации — однозначны. Если правила **LS8** и **LS9** истинны, то оператор (5.15) является корректным.

Понятие *выражения*.

$z = a * b;\ y = z + c \equiv y = (a * b) + c \equiv y = a * b + c$

Правила приоритетов операций

Переменные, изображения констант, вызовы функций и их представление в виде операций являются частными случаями понятия выражения.

C(x: b); **if** (b) A(x: y) **else** B(x: y) ≡

if (C(x)) A(x: y) **else** B(x: y)

В позиции условия — выражение