ПРИМЕР ДОКАЗАТЕЛЬСТВА ПРАВИЛЬНОСТИ ПРОГРАММЫ

Рассмотрим программу $\mathbf{C_0}$ целочисленного деления двух натуральных чисел **x** и **y**:

a:=0; b:= x; while b≥y do b:= b–y; a:= a+1 od

Докажем, что **{x≥0 & y≥0}** $\mathbf{C_0}$ **{a·y+b=x & 0≤b<y)**, т.е., если **x**, **y** – неотрицательные целые числа и программа $\mathbf{C_0}$ завершается, то **a** – целое частное от деления **x** на **y** и **b** – остаток от деления.

ПРИМЕР ДОКАЗАТЕЛЬСТВА ПРАВИЛЬНОСТИ ПРОГРАММЫ

По аксиоме A1 имеем:

$\{0 \cdot y + x = x \ \&\ x \geq 0\}\ a := 0\ \{a \cdot y + x = x \ \&\ x \geq 0\}$ (1)

$\{a \cdot y + x = x \ \&\ x \geq 0\}\ b := x\ \{a \cdot y + b = x \ \&\ b \geq 0\}$ (2)

Далее, из (1) и (2) по R2 получаем:

$\{0 \cdot y + x = x \ \&\ x \geq 0\}\ a := 0;\ b := x\ \{a \cdot y + b = x \ \&\ b \geq 0\}$ (3)

Так как справедливо следующее утверждение:

$x \geq 0 \ \&\ y \geq 0 \rightarrow 0 \cdot y + x = x \ \&\ x \geq 0,$ (4)

то из (3) и (4) по R5 получаем:

$\{x \geq 0 \ \&\ y \geq 0\}\ a := 0;\ b := x\ \{a \cdot y + b = x \ \&\ b \geq 0\}$ (5)

По аксиоме A1 имеем:

$\{(a+1) \cdot y + b - y = x \ \&\ b - y \geq 0\}\ b := b - y\ \{(a+1) \cdot y + b = x \ \&\ b \geq 0\}$ (6)

$\{(a+1) \cdot y + b = x \ \&\ b \geq 0\}\ a := a + 1\ \{a \cdot y + b = x \ \&\ b \geq 0\}$ (7)

Далее, из (6) и (7) по R2 получаем:

$\{(a+1) \cdot y + b - y = x \ \&\ b - y \geq 0\}\ b := b - y;\ a := a + 1\ \{a \cdot y + b = x \ \&\ b \geq 0\}$ (8)

ПРИМЕР ДОКАЗАТЕЛЬСТВА ПРАВИЛЬНОСТИ ПРОГРАММЫ

Так как справедливо следующее утверждение:

$a \cdot y + b = x \;\&\; b \geq 0 \;\&\; b \geq y \rightarrow (a+1) \cdot y + b - y = x \;\&\; b - y \geq 0$, (9)

то из (8) и (9) по R5 получаем:

$\{a \cdot y + b = x \;\&\; b \geq 0 \;\&\; b \geq y\}$ b := b–y; a := a+1 $\{a \cdot y + b = x \;\&\; b \geq 0\}$ (10)

Отсюда по R4 получаем:

$\{a \cdot y + b = x \;\&\; b \geq 0\}$ while b≥y do b := b–y; a := a+1 od

$\{a^* y + b = x \;\&\; b \geq 0 \;\&\; b < y\}$ (11)

Наконец, из (5) и (11) по R2 получаем искомое утверждение.

Отметим, что при использовании правила R5 предполагалась истинность предположений вида **A → B** (в примере предположения (4) и (9)). Доказательство истинности этих предположений в данном примере тривиально (имеются тождественные утверждения), тогда как в общем случае необходимо доказательство истинности этих утверждений для конкретных интерпретаций языка **L**.

ИНВАРИАНТЫ ЦИКЛА

Приведенное в примере доказательство утомительно и трудно для анализа вследствие того, что в нем осуществляется большое количество малых шагов. Всё доказательство базируется на том, что утверждение (10) справедливо. Установив, что должно иметь место утверждение **P ≡ a·y+b=x & b≥0**, доказательство существенно упрощается. Утверждение **P** является в этом случае **инвариантом цикла**

while b≥y do b := b–y; a := a+1 od

Поскольку утверждение (5) справедливо, то это означает, что программа **a:=0; b:=x** устанавливает **P**. Далее, поскольку утверждение (11) также истинно, то это означает, что программа **while b≥y do b := b–y; a := a+1 od** сохраняет **P**.

Простым путем включения этой информации в программу **C** является аннотация **C** желаемыми утверждениями.

АННОТИРОВАННАЯ ПРОГРАММА

Для строгого доказательства правильности программ требуется достаточно большое количество шагов.

Однако знание желаемых инвариантов позволяет существенно упростить понимание процесса доказательства.

Так, например, аннотируя программу с утверждениями

$$\{x \geq 0 \;\&\; y \geq 0\}\ a:=x;\ b:=y;\ z:=1;\ \underline{\textbf{while}}\ b \neq 0\ \underline{\textbf{do}}\ b:=b-1;\ z:=z*a\ \underline{\textbf{od}}\ \{z=x^y\}$$

следующим образом:

$$\{x \geq 0 \;\&\; y \geq 0\}\ a:=x;\ b:=y;\ z:=1;$$
$$\underline{\textbf{while}}\ b \neq 0\ \underline{\textbf{do}}\ \{z*a^b=x^y\}\ b:=b-1;\ z:=z*a\ \underline{\textbf{od}}\ \{z=x^y\}$$

нетрудно видеть, что она истинна при стандартной интерпретации над целыми числами.

АННОТИРОВАННАЯ ПРОГРАММА

Рассмотрение программы в терминах установки и сохранения инвариантов имеет также непосредственное приложение к анализу программ и их разработке.

Например, наблюдение, что цикл **while even(b) do b:=b/2; a:=a*a od** сохраняет инвариант $z*a^b=x^y$, ведет к следующему улучшению программы:

{x≥0 & y ≥0} a:=x; b:=y; z:=1

while b≠0 do {$z*a^b=x^y$}

while even(b) do {$z*a^b=x^y$}

b:=b/2; a:=a*a od

b:=b–1; z:=z*a od {$z=x^y$}

Эта программа, эквивалентная предыдущей программе, значительно более эффективна с точки зрения времени выполнения.

ИНВАРИАНТЫ ЦИКЛА

В общем случае, без изменения истинности программы можно осуществлять вставку в текст программы любого фрагмента программы, не изменяющего инвариант, устанавливаемый операторами, предшествующими этому фрагменту.

ЗАВЕРШИМОСТЬ ПРОГРАММ

Следует учитывать, что доказательства правильности программ не зависят от того, завершаются они или нет.

Доказательство того факта, что **{P} C {Q}** является истинным, не гарантирует, что программа завершится.

Отметим также, что завершимость программы зависит от ее интерпретации.

Таким образом, встает вопрос о том, является ли программа завершимой или нет.

Очевидно, что единственным оператором языка **L**, который может принести к незавершимости программы, является команда цикла **while B do C od**. Для анализа завершимости этого цикла можно использовать инварианты цикла.

ЗАВЕРШИМОСТЬ ПРОГРАММ

Пусть **E** – некоторое целочисленное выражение.

Предположим, что справедливо утверждение: $\mathbf{P \,\&\, B \rightarrow (E>0)}$ (1)

и для любого выражения $\mathbf{E_0}$, принимающего целочисленные значения, справедливо: $\mathbf{\{0<E=E_0\}\ C\ \{0 \le E<E_0\}}$ (2)

Это означает, что утверждение $\mathbf{E \ge 0}$ также, как и **P** является инвариантом цикла, т.е. выражение **E** остается неотрицательным в течении итерационного процесса. Кроме того, условие (2) означает, что каждое выполнение программы **C** уменьшает значение выражения **E**. Таким образом, из справедливости (1) и (2), а также $\mathbf{\{P \,\&\, B\}\ C\ \{P\}}$ непосредственно следует вывод о конечности итерационного процесса, так как целочисленное выражение **E** не может уменьшаться бесконечное число раз и оставаться положительным, как требует условие (1).

ПРИМЕР ПРОВЕРКИ ЗАВЕРШИМОСТИ ПРОГРАММЫ

В качестве примера рассмотрим программу $\mathbf{C_0}$ целочисленного деления натуральных чисел **x** и **y**:

{x≥0 & y>0} a:=0; b:=x; while b≥y do {b+y>0} b:=b–y; a:=a+1 od {b+y>0}

Искомым выражением **E** здесь является **b+y**, а инвариантом цикла утверждение **b+y≥0**.

Докажем вначале справедливость утверждения (1) для данной программы. Возьмем для этой цели в качестве **P** утверждение **y>0**, являющееся инвариантом цикла.

Доказательство того, что **y>0** является инвариантом, тривиально, т.к. **y>0** перед выполнением программы и нигде в программе не изменяется.

При стандартной интерпретации на области целых чисел получаем, что утверждение **y>0 & b≥y → b+y>0** справедливо.

ПРИМЕР ПРОВЕРКИ ЗАВЕРШИМОСТИ ПРОГРАММЫ

Докажем теперь справедливость утверждения (2) для программы, имеющего вид:

$$\{E_0=b+y>0\}\ b:=b-y;\ a:=a+1\ \{E_0>b+y\geq 0\}$$

Поскольку справедливо утверждение:

$$E_0=b+y>0\ \&\ y>0\ \&\ b\geq y \rightarrow E_0=(b-y)+2\cdot y>0\ \&\ y>0\ \&\ (b-y)+y\geq y,$$

то, по аксиоме A1 и правилу вывода R5, получаем:

$$\{E_0=b+y>0\ \&\ y>0\ \&\ b\geq y\}\ b:=b-y\ \{E_0=b+2\cdot y>0\ \&\ y>0\ \&\ b+y\geq y\}$$

Поскольку справедливы также утверждения:

$E_0=b+2\cdot y>0\ \&\ y>0 \rightarrow E_0>b+y,$

$b+y\geq y\ \&\ y>0 \rightarrow b+y\geq 0,$

то, применяя правило вывода R5, получаем:

$$\{E_0=b+y>0\ \&\ y>0\ \&\ b\geq y\}\ b:=b-y\ \{E_0>b+y\geq 0\}$$

Далее, по аксиоме A1, имеем: $\{E_0>b+y\geq 0\}\ a:=a+1\ \{E_0>b+y\geq 0\}$

Применяя теперь правило вывода R2, получаем искомый результат.

ПРИМЕР ПРОВЕРКИ ЗАВЕРШИМОСТИ ПРОГРАММЫ

Таким образом, удалось доказать и утверждение (2) для циклического участка программы.

Отсюда следует завершимость итерационного цикла, а следовательно, и всей программы.

Заметим, что неудача при попытке получить подходящее целочисленное выражение для доказательства завершимости не дает оснований для вывода о незавершимости программы для некоторых начальных значений переменных.

Незавершимость программы в этом случае также требует доказательства.

ДОКАЗАТЕЛЬСТВО НЕЗАВЕРШИМОСТИ ПРОГРАММЫ

Рассмотрим идею доказательства незавершимости на примере цикла **while B do C od**, для которого хотим доказать

$$\{P\}\ \textbf{while}\ B\ \textbf{do}\ C\ \textbf{od}\ \{P \,\&\, \neg B\}$$

Если предположить, что такой цикл не завершается, то требуется доказать, что не только **P**, но и **P & B** является инвариантом цикла, т.е. необходимо показать, что если **P & B** истинно перед выполнением **C**, то оно будет истинно и после выполнения **C**. **Отсюда следует незаверщимость цикла**.

Доказательство незавершимости позволяет также выяснить причины незавершения программы. Анализ этих причин позволяет вносить исправления в программу.

ПРИМЕР ДОКАЗАТЕЛЬСТВА НЕЗАВЕРШИМОСТИ ПРОГРАММЫ

Проиллюстрируем сказанное на примере рассмотренном ранее программы целочисленного деления.
Вместо начальных условий **x≥0 & y>0** возьмем **x≥0 & y≥0**.
В этом случав нетрудно показать, что для **y=0** утверждение **b≥y** будет инвариантом цикла **while b≥y do b:=b–y; a:=a+1 od**

Доказательство строится, как обычно, в два этапа:

1. **установка инварианта b≥y командам, предшествующими циклу;**
2. **сохранение этого инварианта командами тела цикла.**

1) Легко показать, что: **{x≥0 & y=0} a:=0; b:=x {b=x & x≥0 & y=0}**
Далее, поскольку справедливы утверждения: **b=x & x≥0 → b≥0,**
b≥0 & y=0 → b≥y & y=0, получаем по правилу вывода R5:
{x≥0 & y=0} a:=0; b:=x {b≥y & y=0}, т.е. **b≥y** истинно перед выполнением цикла.

ПРИМЕР ДОКАЗАТЕЛЬСТВА НЕЗАВЕРШИМОСТИ ПРОГРАММЫ

2) Применяя аксиому A1, получаем:

$$\{(b-y)+y \geq y \ \&\ y=0\}\ b:=b-y\ \{b+y \geq y \ \&\ y=0\}$$

Поскольку справедливо утверждение:

$$b+y \geq y \ \&\ y=0 \rightarrow b \geq y$$

то, по правилу вывода R5, получаем:

$$\{b \geq y \ \&\ y=0\}\ b:=b-y\ \{b \geq y\}$$

Далее, применяя аксиому A1, имеем:

$$\{b \geq y\}\ a:=a+1\ \{b \geq y\}$$

Далее, по правилу R2, получаем :

$$\{b \geq y \ \&\ y=0\}\ b:=b-y;\ a:=a+1\ \{b \geq y\}$$

откуда следует, что **b≥y** является инвариантом цикла, а следовательно, **цикл не завершается.**