|  |  |
| --- | --- |
| ДИСЦИПЛИНА | **Методы верификации и валидации характеристик программного обеспечения** |
|  | (полное наименование дисциплины без сокращений) |
| ИНСТИТУТ | **информационных технологий** |
| КАФЕДРА | **математического обеспечения и стандартизации информационных технологий** |
|  | (полное наименование кафедры) |
| ВИД УЧЕБНОГО | **Материалы для практических/семинарских занятий** |
| МАТЕРИАЛА | (в соответствии с пп.1-11) |
| ПРЕПОДАВАТЕЛЬ | **Петренко Александр Анатольевич** |
|  | (фамилия, имя, отчество) |
| СЕМЕСТР | **3, 2023-2024** |
|  | (указать семестр обучения, учебный год) |

**Формализация семантики языков программирования**

На основе изучения материала лекций по дисциплине «Методы верификации и валидации характеристик программного обеспечения» требуется выполнить следующее.

1. Выпишите сигнатуру программ P,Q и S, реализующих алгоритм Евклида (см. предыдущее практическое занятие). Расширьте эту сигнатуру предикатным символом НОД, определите аксиомы и правила вывода предметной области.
2. Докажите утверждение о единственности вычисления любой whileпрограммы в произвольном начальном состоянии.
3. Постройте вычисление программы целочисленного деления DIV для a=7 и b=3, начальные значения переменных q и r могут быть любыми.
4. Постройте вычисления программ P,Q и S, реализующих алгоритм Евклида (см. предыдущее практическое занятие), для a=14 и b=21.
5. Опишите семантику оператора недетерминированного выбора choice, используя операционный и аксиоматический подходы.
6. Опишите семантику оператора цикла repeat - until, используя операционный и аксиоматический подходы.
7. Предложите инвариант цикла для программы целочисленного деления DIV.
8. Предложите инварианты циклов для программ P,Q и S, реализующих алгоритм Евклида (см. предыдущее практическое занятие). Совпадают ли эти инварианты?

**1. Сигнатура программ P, Q и S, реализующих алгоритм Евклида**

**Сигнатура программы:**

Сигнатура включает в себя переменные и предикаты, используемые в программах.

* **Переменные**: x, y, z, a, b, c
* **Функции**: −, %, +
* **Предикаты**:
  + gcd(x, y ) — предикат, который обозначает, что значение переменных x и y равны наибольшему общему делителю.
  + =, ≠, >, ≥, < — предикаты сравнения.

**Аксиомы и правила вывода:**

1. **Аксиома эквивалентности НОД**: gcd(x, y ) ⇒ gcd(x−y, y ) если x > y. Эта аксиома определяет, что НОД остается неизменным при вычитании меньшего числа из большего.
2. **Аксиома остатка**: gcd(x, y ) ⇒ gcd(x % y, y ) если y>0 НОД остается неизменным при замене одного числа на остаток от его деления.
3. **Рекурсивное определение НОД**: gcd(x, y ) = gcd(y, x%y ) если y ≠ 0

**2. Доказательство единственности вычисления любой программы с циклом while**

Для доказательства единственности вычисления программы с циклом while нужно показать, что для любых начальных значений переменных цикл выполняется однозначно до тех пор, пока выполняется условие цикла.

Если при любом выполнении программы с циклом для заданного начального состояния результат всегда один и тот же, это доказывает единственность вычисления. Это можно сделать путем индукции на количество итераций цикла.

**3. Вычисление программы целочисленного деления DIV для a=7a = 7a=7 и b=3b = 3b=3**

Программа DIV:

q := 0;

r := a;

while r ≥ b do

q := q + 1;

r := r - b

end

**Выполнение шагов:**

1. Начальные значения: q=0 r=7.
2. Первая итерация: r=7−3=4, q=1.
3. Вторая итерация: r=4−3=1, 2q=2.
4. Завершение цикла, так как r<b.

Результат: q=2, r=1.

**4. Вычисления программ P, Q и S для a=14 и b=21**

**Программа P:**

1. x=14, y=21.
2. x ≠ yx, x < y, поэтому y=21−14=7.
3. x ≠ yx, x > y, поэтому x=14−7=7.
4. x = y, цикл завершен. НОД = 7.

**Программа Q:**

1. x=14, y=21.
2. y≠0, z=14, x=21, y=14%21=14.
3. y≠0, z=21, x=14, y=21%14=7.
4. y≠0, z=14, x=7, y=14%7=0.
5. НОД = 7.

**Программа S:**

1. x=14, y=21.
2. x≠0, y≠0, x < y, поэтому y=21%14=7.
3. x≠0, y≠0, x > y, поэтому x=14%7=0.
4. НОД = 7.

**5. Семантика оператора недетерминированного выбора (choice)**

**Операционная семантика:**

Оператор выбора предоставляет возможность выбора одного из нескольких вариантов выполнения. В операционной семантике это моделируется через множество возможных переходов в различные состояния.

**Аксиоматическая семантика:**

Оператор выбора интерпретируется как логическое ИЛИ (disjunction) между различными постусловиями.

**6. Семантика оператора цикла repeat - until**

**Операционная семантика:**

Оператор выполняет тело цикла один раз, а затем проверяет условие. Если условие истинно, выполнение прекращается, иначе тело цикла выполняется снова.

**Аксиоматическая семантика:**

Постусловие должно быть истинным, когда условие выхода истинно, а инвариант цикла выполняется перед каждой итерацией.

**7. Инвариант цикла для программы целочисленного деления DIV**

Инвариант цикла: r=a−q⋅b. Этот инвариант описывает связь между переменными r, a, q, и b на каждом шаге выполнения программы.

**8. Инварианты циклов для программ P, Q и S**

Для программ P, Q и S инварианты будут следующими:

**Программа P:**

Инвариант: gcd(x,y)=gcd(a,b).

**Программа Q:**

Инвариант: gcd(x,y)=gcd(a,b).

**Программа S:**

Инвариант: gcd(x,y)=gcd(a,b).

Все три программы имеют одинаковый инвариант, так как они реализуют один и тот же алгоритм поиска НОД.