ЛОГИКА ХОАРА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Супринович И. Ю.

Миськевич В. И. – канд. филос. наук, доцент

В последние десятилетия компьютеры стали занимать больше места в каждой сфере нашей жизни. В связи с этим возникла необходимость тщательной проверки компьютерных программ на правильность, ведь всё чаще и чаще компьютерам доверяют человеческие жизни. Это привело к возникновению различных методов, используемых для доказательства корректности компьютерных программ, одним из которых является логика Хоара.

Логика Хоара – формальная система с набором логических правил, используемая для строгого доказательства корректности компьютерных программ. Она основывается на идее того, что пользователь обязуется соблюдать подробное описание программы. Описание состоит из предусловия и постусловия. Предусловие – это предикат, описывающий условие, которое требуется программе для правильного выполнения; пользователь обязан следовать этим условиям, если ему надо получить правильный результат. Постусловие – это предикат, описывающий результат правильного выполнения программы; пользователь может рассчитывать на правильное выполнение программы, если выполнит предусловие.

Программа может быть частично корректной по отношению к её описанию. Если предположить, что предусловие верно как раз перед выполнением программы, и если затем программа завершается, то постусловие верно. Программа также может быть абсолютно корректной. Абсолютная корректность подобна частичной за исключением одного факта: абсолютная корректность гарантирует завершение программы, в отличие от частичной корректности.

Следует отметить, что если пользователь использует программу без выполнения её предусловия, то она может повести себя как угодно и при этом остаться корректной. Поэтому, если требуется, чтобы программа была устойчива к ошибкам, предусловие должно включать в себя возможность ошибочного ввода, а постусловие – описание того, что может произойти в случае неправильного ввода.

Логика Хоара использует Тройки Хоара для рассуждения о корректности программы. Тройка Хоара имеет вид {Pre} S {Post}, где Pre – предусловие, Post – постусловие, а S – одно или несколько выражений, которые являются реализацией программы. Тройка {Pre} S {Post} в случае абсолютной корректности означает, что если Pre является истинным и выполнит S, то после этого S завершится в таком состоянии, где Post истинно.

Рассмотрим в качестве примера тройку {x=-7} x:=x*2 {x<0}. Очевидно, что эта тройка абсолютно корректная, ведь если подставить -7 в выражение x:=x*2, действительно окажется, что x<0. Несмотря на то, что эта тройка корректная, она не является самой точной. Она будет более точной, если мы напишем в постусловии x<0&&x>-30. Сильнейшим постусловием будет x=-14. Таким образом, сильнейшее постусловие sp(S, Pre) – это предикат, определяющий все те состояния, в которые попадёт S из начальных состояний, удовлетворяющих до начала выполнения программы условию Pre.

Также существует такое понятие, как слабейшее предусловие. Слабейшее предусловие wp(S, Post) – это предикат, определяющий все те начальные состояния, из которых программа S после её завершения попадёт в состояния, удовлетворяющие Post. Попробуем определить wp(x:=x+3, x>z+5-x*y), т.е. такие значения x до начала работы программы, чтобы после прохождение через x:=x+3 мы получили x>z+5-x*y. Для этого мы просто подставляем x:=x+3 в x>z+5-x*y: wp(x:=x+3, x>z+5-x*y)={x>z+2-x*y-3y}.

Для доказательства частичной корректности программ можно использовать как слабейшее предусловие, так и сильнейшее постусловие. Пусть задана сама программа S, предусловие Pre и постусловие Post. Пусть также мы смогли построить сильнейшее постусловие этой программы. Вспомним, что тройка Хоара {Pre} S {Post} означает, что если Pre истинно до начала выполнения S, и S завершается, то после завершения S утверждение Post станет истинным. Тогда можно сформулировать теорему о корректности программ обработки данных: программа S частично корректна тогда и только тогда, когда sp{S, Pre} целиком лежит в Post.

Аналогичным образом можно сформулировать теорему о корректности программ обработки данных в случае со слабейшим предусловием: пусть задана сама программа S, предусловие Pre и постусловие Post и мы смогли определить слабейшее предусловие программы. Вспомним, что тройка Хоара {Pre} S {Post} означает, что если Pre истинно до начала выполнения S, и S завершается, то после завершения S утверждение Post станет истинным. Тогда программа S частично корректна тогда и только тогда, когда wp{S, Post} целиком лежит в Pre.

Таким образом, логика Хоара применяется для доказательства частичной корректности программ.

Список использованных источников:

1. Hoare Logic. – [Электронный ресурс]. – Режим доступа: https://www.cs.cmu.edu/~aldrich/courses/654-sp09/notes/3-hoare-notes.pdf. – Дата доступа: 19.03.2016.