

достаточен для представления произвольного алгоритма и поэтому не ограничивает общности излагаемого метода.

Пусть для программы $Prgm$ задана внешняя спецификация в виде предусловия $P(x_1, \dots, x_n)$ и постусловия $Q(x_1, \dots, x_n)$, относительно которой требуется доказать частичную корректность, т. е. истинность тройки Хоара $\{P\}Prgm\{Q\}$. Очевидно, что при выполнении программы для различных исходных данных возможны различные последовательности операторов, начинающиеся оператором START и оканчивающиеся оператором STOP. Назовем такие последовательности *трассами вычислений*. Истинность тройки Хоара $\{P\}Prgm\{Q\}$ имеет место, если истинны тройки Хоара $\{P_j\}T_j\{Q\}$ для всех трасс T_j , т. е.

$$\{P\}Prgm\{Q\} : \forall j (\{P_j\}T_j\{Q\}),$$

где P_j — предикат «вычисления выполняются по j -й трассе T_j »; T_j — трасса вычислений, соответствующая P_j .

Трассы вычислений осуществляют разбиение предусловия P таким образом, что

$$P = \bigvee P_j; \quad \forall i, j ((j_1 \neq j_2) \Rightarrow P_{j_1} \wedge P_{j_2} = false).$$

Сложность анализа $\{P\}Prgm\{Q\}$ разбиением на трассы состоит в том, что при наличии циклических вычислений в программе он не может быть выполнен непосредственным перебором всех трасс. Выход состоит во включении в программу дополнительных индуктивных утверждений так, чтобы любой циклический путь проходил по крайней мере через одно такое утверждение. В этом случае достаточно проанализировать только одно прохождение по каждому циклу, т. е. существенно уменьшить количество анализируемых трасс вычислений.

Индуктивное утверждение, приписанное циклу, принято называть *инвариантом цикла*¹. Оно «разрезает» циклические пути на два: путь через тело цикла и путь к выходу из цикла. Инвариант цикла может приписываться точке входа в цикл или любой другой точке цикла, которая лежит на каждой трассе через цикл.

Таким образом, аннотированная программа, используемая в методе индуктивных утверждений, должна кроме внешней спецификации (предусловия и постусловия) иметь для каждого цикла инвариант цикла. Условимся считать, что программа аннотируется выбором контрольных точек на входе, выходе программы и на каждом пути через цикл. С каждой контрольной точкой t_i ассо-

¹ Название не вполне удачное, так как инвариант цикла — утверждение, характеризующее фактические (а не ожидаемые!) вычисления в цикле в соответствии с общей концепцией инвариантов. Индуктивное утверждение цикла совпадает с инвариантом цикла при отсутствии ошибок.