1 Transitive closure of a binary relation, it's existence

Предложение (Транзитивное замыкание)

Дано отношение r на множестве A, оно является транзитивным замыканием, т.е.

$$r^* = \bigcup\{r^n | n \geq 1\}$$

Доказательство

Во-первых, отметим, что r^* транзитивно. Действительно, пусть $(a,b),(b,c) \in r^*$. Тогда для некоторых $n, m \geq 1$, $(a,b) \in r^n$ и $(b,c) \in r^m$. Но тогда $(a,c) \in r^n \circ r^m = r^{n+m} \subseteq r^*$. Так как $r^1 = r$, то $r \subseteq r^*$. Доказательство минимальности r^* проведём по индукции: покажем, что $r^n \subseteq r'$ для любого транзитивного r' содержащего r. Основание индукции - $n = 1$ очевидно. Теперь предположим, что $r^{n-1} \subseteq r'$ и $(a,c) \in r^n \stackrel{def}{=} r^{n-1} \circ r$. По определению композиции существует некоторое b такое, что $(a,b) \in r^{n-1}$ и $(b,c) \in r$. Тогда $(a,b),(b,c) \in r'$, и так как r' транзитивно, то $(a,c) \in r'$.

2 Church numbers: addition and multiplication

Сложение, умножение

Если определить сложение и умножение как

- $PLUS = \lambda mnfx.m\ f\ (n\ f\ x)$
- $MULT = \lambda mnfx.m\ (n\ f)\ x$

то

- $PLUS\ \underline{n}\ \underline{m} = \underline{n+m}$
- $MULT\ \underline{n}\ \underline{m} = \underline{n \cdot m}$

3 Hoare triples, axiomatic semantics for a programming language. Correctness and completeness of axiomatic semantic

Математическая природа π

Любая программа π может рассматриваться как **математический** объект, к которому могут быть применены все математические методы.

Итак, мы можем переформулировать проблему корректности программы, используя понятия математической логики. Но сначала разделим программы на два класса:

- **завершающиеся** (такие как компилятор, конвертер любых данных и т. д.)
- **не завершающиеся** (такие как ОС, IDE и т. д.)

Далее будем говорить только о *завершающихся* программах.

Проблема: формальная корректность

Дана программа π, и некоторое множество входных данных, соответствующее формуле ϕ (**предусловие**), будут ли выходные данные соответствовать формуле ψ (**постусловие**)?

Отметим, что здесь мы *формализовали* технические требования к программе, используя *формулы* логики предикатов. В сокращённых обозначениях проблема корректности записывается как:

$$\{\phi\}\pi\{\psi\}$$

и называется **тройка Хоара** или **условие частичной корректности**.

Аксиоматическая семантика

Дан язык программирования l, его **аксиоматическая семантика** - это множество аксиом и правил вывода, действующих на формулы и тройки Хоара и адекватных семантике l.

Аксиомы и правила для основных операторов

- $\{(\phi)^x_e\}x := e\{\phi\}$ - аксиома присваивания
- $\frac{\{\phi\}\sigma\{\chi\} \quad \{\chi\}\tau\{\psi\}}{\{\phi\}\sigma;\tau\{\psi\}}$ - правило композиции
- $\frac{\{\phi\wedge\chi\}\sigma\{\psi\} \quad \{\phi\wedge\neg\chi\}\tau\{\psi\}}{\{\phi\}if\ \chi\ then\ \sigma\ else\ \tau\{\psi\}}$ - условное правило
- $\frac{\{\phi\wedge\chi\}\sigma\{\phi\}}{\{\phi\}while\ \chi\ do\ \sigma\ \{\phi\wedge\neg\chi\}}$ - итеративное правило, здесь ϕ - **инвариант** цикла.

Правило следствия

Существует специальное правило, операндами которого могут быть не только тройки Хоара, но и обычные формулы:

$$\frac{\phi \to \phi' \quad \{\phi'\}\sigma\{\psi'\} \quad \psi' \to \psi}{\{\phi\}\sigma\{\psi\}}$$

Это правило помогает извлекать формальные математические вопросы, не зависящие от каких-либо объектов языка программирования, из программы и спецификации. Этот процесс известен как **генерация условий корректности**.

Теорема (корректность аксиоматической семантики SPL)

Для любой тройки Хоара $\{\phi\}\pi\{\psi\}$, если существует её дерево вывода, все листья которого, являющиеся формулами, тождественно истинны, то

$$\models \{\phi\}\pi\{\psi\}$$

Доказательство

Как всегда, докажем эту теорему индукцией по высоте дерева вывода. Сначала необходимо проверить, что аксиома присваивания всегда истинна, затем проверить все остальные правила вывода. Проверим, что $\models \{(\phi)^x_e\}x := e\{\phi\}$. Рассмотрим некоторое состояние s, такое, что $s \models (\phi)^x_e$. Тогда, если заменить каждое вхождение e в $(\phi)^x_e$ значением $e[s]$, истинность формулы сохранится. Таким образом, $s^x_e \models \phi$, потому что в этой формуле все вхождения x заменены значениями $e[s]$. Предположим, что

$\models \{\phi\}\pi\{\chi\}$ и $\models \{\chi\}\rho\{\psi\}$. Необходимо проверить, что $\models \{\phi\}\pi;\rho\{\psi\}$. Действительно, возьмём некоторое состояние $s_0 \models \phi$ такое, что $< \pi;\rho > (s)$ определено: если $s_1 =< \pi > s_0$, то $s_1 \models \chi$, следовательно, если $s_2 =< \rho > (s_1)$, то $s_2 \models \psi$. Но $s_2 =< \pi;\rho > (s_0) \models \psi$, ч.т.д. Остальные случаи доказываются аналогично.$\Box$

Теорема (полнота аксиоматической семантики SPL)

В аксиоматической семантике для любой аннотированной тройки Хоара $\{\phi\}\ \pi\ \{\psi\}$ существует вывод $\{AC\ (\pi,\ \psi)\}\ \pi\ \{\psi\}$. Все листья этого дерева вывода не являются формулами $VC\ (\pi,\ \psi)$ или являются тождественно истинными формулами.

Доказательство

Индукция по структуре π. Основание индукции - очевидно из определения аксиоматической семантики.

Шаг индукции. Случай последовательного оператора:

$$\frac{\{AC(\alpha, AC(\beta,\psi))\}\alpha\{AC(\beta,\psi)\}\{AC(\beta,\psi)\}\beta\{\psi\}}{\{AC(\alpha, AC(\beta,\psi))\}\alpha;\ \beta\{\psi\}}$$

По предположению индукции обе тройки Хоара над чертой доказуемы, поэтому тройка Хоара под чертой также доказуема.

Случай условного оператора:

$$\frac{\frac{\chi\wedge((\chi\wedge AC(\alpha,\psi))\vee(\neg\chi\wedge AC(\beta,\psi)))\rightarrow AC(\alpha,\psi)\{AC(\alpha,\psi)\}\alpha\{\psi\}}{\{\chi\wedge((\chi\wedge AC(\alpha,\psi))\vee(\neg\chi\wedge AC(\beta,\psi)))\}\alpha\{\psi\}...}}{\{(\chi \wedge AC(\alpha,\psi)) \vee (\neg\chi \wedge AC(\beta,\psi))\}\ if\ (\chi)\alpha\ else\ \beta\{\psi\}}$$

По предположению индукции верхняя тройка Хоара доказуема, поэтому нижняя тройка Хоара также доказуема. Отметим, что формулы вида $\chi\wedge((\chi\wedge AC(\alpha,\psi))\vee(\neg\chi\wedge AC(\beta,\psi))) \rightarrow AC(\alpha,\psi)$ являются тождественно истинными.

Случай цикла while:

$$\frac{\frac{\frac{I\wedge\chi\rightarrow AC(\alpha,I)\{AC(\alpha,I)\}\alpha\{I\}}{\{I\wedge\chi\}\alpha\{I\}}}{\{I\}\alpha\{I\wedge\neg\chi\}I\wedge\neg\chi\rightarrow\psi}}{\{I\}\ while\ (\chi)\alpha\{\psi\}}$$