Математическая логика и логическое программирование

mk.cs.msu.ru → Лекционные курсы
→ Математическая логика и логическое программирование (3-й поток)

Блок 54

Логика Хоара
Автоматизация проверки правильности программ

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2023/2024, осенний семестр

Логика Хоара

Для проверки проверки частичной корректности
модельных императивных программ
можно адаптировать метод семантических таблиц:
ввести понятие вывода (дерева, построенного по правилам вывода)
и свести проверку корректности к построению успешного вывода

Правила вывода будут выглядеть так:[1]

$$\frac{\Phi}{\Psi}, \quad \frac{\Phi}{\Psi, \Omega}, \quad \frac{\Phi}{\varphi} \quad \text{или} \quad \frac{\Phi}{\varphi, \Omega, \psi},$$

где Φ, Ψ, Ω — триплеты Хоара и φ, ψ — формулы логики предикатов

Содержательное прочтение:
если в $\mathcal{I}$ истинны все триплеты и формулы под чертой
то в $\mathcal{I}$ истинен триплет Φ

1 Hoare C.A.R. An axiomatic basis for computer programming. 1969

Логика Хоара

Вот эти правила:

$$R_{\emptyset}: \frac{\{\varphi\}\emptyset\{\varphi\}}{\mathbb{t}} \qquad R_{:=}: \frac{\{\varphi\{\mathrm{x}/t\}\}\mathrm{x} := t;\{\varphi\}}{\mathbb{t}}$$

(подстановка $\{\mathrm{x}/t\}$ правильна для φ)

$$R_{\textbf{if}}: \frac{\{\varphi\}\textbf{if } C \textbf{ then } \pi_1 \textbf{ else } \pi_2 \textbf{ fi}\{\psi\}}{\{\varphi \,\&\, C\}\pi_1\{\psi\}, \{\varphi \,\&\, \neg C\}\pi_2\{\psi\}}$$

$$R_{\textbf{while}}: \frac{\{\varphi\}\textbf{while } C \textbf{ do } \pi \textbf{ od}\{\varphi \,\&\, \neg C\}}{\{\varphi \,\&\, C\}\pi\{\varphi\}}$$

$$R_{seq}: \frac{\{\varphi\}\pi_1\ \pi_2\{\psi\}}{\{\varphi\}\pi_1\{\chi\}, \{\chi\}\pi_2\{\psi\}}$$

$$R_{inf}: \frac{\{\varphi\}\pi\{\psi\}}{\varphi \to \varphi', \{\varphi'\}\pi\{\psi'\}, \psi' \to \psi}$$

Логика Хоара

Лемма (о корректности правил вывода Хоара)

Для любой интерпретации $\mathcal{I}$ и любого из правил

$$R_{\emptyset},\ R_{:=},\ R_{\textbf{if}},\ R_{\textbf{while}},\ R_{seq},\ R_{while}$$

$$\left(\frac{\Phi}{\Psi},\quad \frac{\Phi}{\Psi,\Omega},\quad \frac{\Phi}{\varphi},\quad \frac{\Phi}{\varphi,\Psi,\psi}\right)$$

верно следующее: если $\mathcal{I} \models \Psi$, $\mathcal{I} \models \Omega$, $\mathcal{I} \models \varphi$ и $\mathcal{I} \models \psi$, то $\mathcal{I} \models \Phi$

Доказательство.

Подробно рассмотрим только правило $R_{:=}$: $\dfrac{\{\varphi\{\mathrm{x}/t\}\}\mathrm{x} := t;\{\varphi\}}{\mathbb{t}}$

Пусть σ — произвольное состояние данных, такое что $\mathcal{I} \models \varphi\{\mathrm{x}/t\}\sigma$

Шаг вычисления для программы «$\mathrm{x} := t;$» устроен так:

$$\langle \mathrm{x} := t; \mid \sigma\rangle \xrightarrow{\mathcal{I}} \langle \emptyset \mid \sigma\{x \leftarrow t\sigma\}\rangle$$

Так как $\mathcal{I} \models \varphi\{\mathrm{x}/t\}\sigma$, то верно и $\mathcal{I} \models \varphi(\sigma\{x \leftarrow t\sigma\})$

Следовательно, $\mathcal{I} \models \{\varphi\{\mathrm{x}/t\}\}\mathrm{x} := t;\{\varphi\}$

Корректность остальных правил обосновывается по той же схеме ▼

Логика Хоара

Вывод триплета $\{\varphi\}\pi\{\psi\}$ — это дерево следующего вида:

- вершины размечены триплетами и формулами
- корень помечен триплетом $\{\varphi\}\pi\{\psi\}$
- дети вершины определяются относительно правил логики Хоара так же, как и в дереве табличного вывода относительно правил табличного вывода
- все листья помечены формулами

Успешный вывод триплета $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$ — это конечный вывод, все листья которого помечены формулами, истинными в $\mathcal{I}$

Логика Хоара

Теорема (о корректности логики Хоара)
Если существует успешный вывод триплета $\{\varphi\}\pi\{\psi\}$ в интерпретации $\mathcal{I}$, то $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$

Доказательство.

Рассмотрим произвольный успешный вывод D для $\{\varphi\}\pi\{\psi\}$ в $\mathcal{I}$

Во всех листьях D записаны формулы, истинные в $\mathcal{I}$

Применив лемму о корректности правил вывода конечное число раз, получим истинность триплета $\{\varphi\}\pi\{\psi\}$ в $\mathcal{I}$ ▼

Логика Хоара

Пример: алгоритм Эвклида

$\pi =$ **while** $\neg(\mathtt{x} = \mathtt{y})$ **do if** $\mathtt{x} > \mathtt{y}$ **then** $\mathtt{x} := \mathtt{x} - \mathtt{y}$; **else** $\mathtt{y} := \mathtt{y} - \mathtt{x}$; **fi od**

Докажем, что в результате выполнения π в интерпретации $Ar_{\mathbb{Z}}$ в $\mathtt{x}$ записывается **наибольший общий делитель** (НОД) положительных чисел, заданных в $\mathtt{x}$ и $\mathtt{y}$ перед выполнением

Предусловие φ: чи́сла $\mathtt{x}$ и $\mathtt{y}$ положительны, и $\mathtt{z}$ — переменная, обозначающая НОД $\mathtt{x}$ и $\mathtt{y}$ в начале выполнения программы

$$\begin{aligned} \mathtt{u}|\mathtt{v} = & \quad \exists \mathtt{w}\,(\mathtt{v} = \mathtt{u} \cdot \mathtt{w}) \\ \gcd(\mathtt{u},\mathtt{v},\mathtt{w}) = & \quad (\mathtt{w}|\mathtt{u}) \,\&\, (\mathtt{w}|\mathtt{v}) \,\&\, \forall \mathtt{r}\,((\mathtt{r}|\mathtt{u}) \,\&\, (\mathtt{r}|\mathtt{v}) \to (\mathtt{w} \geq \mathtt{r})) \\ \varphi = & \quad \mathtt{x} > 0 \,\&\, \mathtt{y} > 0 \,\&\, \gcd(\mathtt{x},\mathtt{y},\mathtt{z}) \end{aligned}$$

Постусловие ψ: в $\mathtt{x}$ записан требуемый НОД

$$\psi = (\mathtt{x} = \mathtt{z})$$

Для обоснования правильности π достаточно построить успешный табличный вывод для триплета $\{\varphi\}\pi\{\psi\}$

Логика Хоара

$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z)\}$
while $\neg(x = y)$ **do if** $x > y$ **then** $x := x - y$; **else** $y := y - x$; **fi od**
$\{x = z\}$

χ_1: $x > 0 \,\&\, x > 0 \,\&\, \gcd(x, y, z) \to x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z)$

χ_2: $x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z) \,\&\, \neg\neg(x = y) \to x = z$

$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z)\}$
while $\neg(x = y)$ **do if** $x > y$ **then** $x := x - y$; **else** $y := y - x$; **fi od**
$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z) \,\&\, \neg\neg(x = y)\}$

$$R_{inf}: \frac{\{\varphi\}\pi\{\psi\}}{\varphi \to \varphi', \{\varphi'\}\pi\{\psi'\}, \psi' \to \psi}$$

$$\mathcal{I} \models \chi_1$$
$$\mathcal{I} \models \chi_2$$

Логика Хоара

$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z)\}$
while $\neg(x = y)$ **do if** $x > y$ **then** $x := x - y$; **else** $y := y - x$; **fi od**
$\{x = z\}$

χ_1: $x > 0 \,\&\, x > 0 \,\&\, \gcd(x, y, z) \to x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z)$

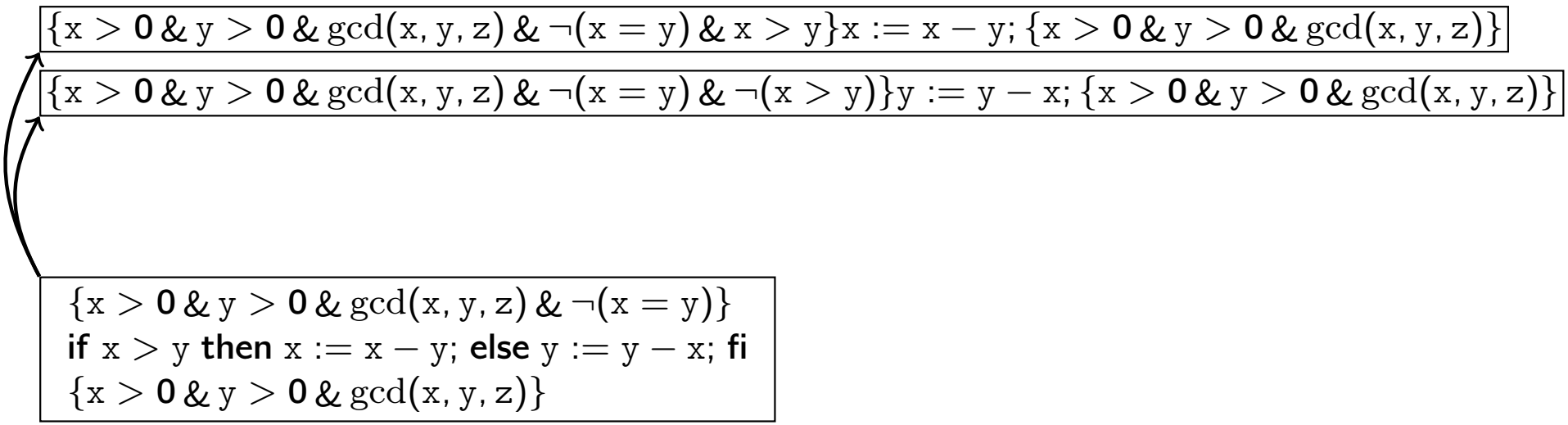
χ_2: $x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z) \,\&\, \neg\neg(x = y) \to x = z$

$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z)\}$
while $\neg(x = y)$ **do if** $x > y$ **then** $x := x - y$; **else** $y := y - x$; **fi od**
$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z) \,\&\, \neg\neg(x = y)\}$

$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z) \,\&\, \neg(x = y)\}$
if $x > y$ **then** $x := x - y$; **else** $y := y - x$; **fi**
$\{x > 0 \,\&\, y > 0 \,\&\, \gcd(x, y, z)\}$

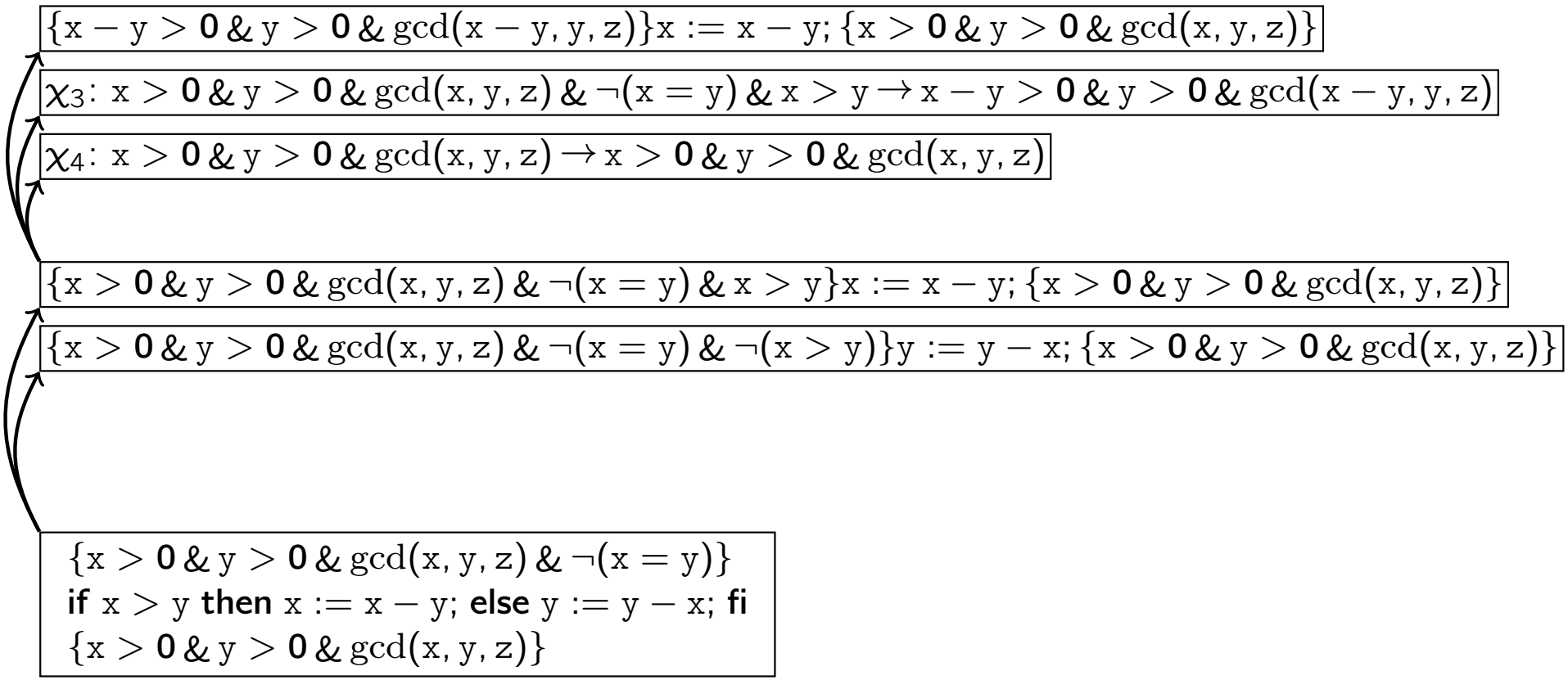
$$R_{\textbf{while}}\colon \frac{\{\varphi\}\textbf{while } C \textbf{ do } \pi \textbf{ od}\{\varphi \,\&\, \neg C\}}{\{\varphi \,\&\, C\}\pi\{\varphi\}}$$

Логика Хоара



$$R_{\textbf{if}}\colon \frac{\{\varphi\}\textbf{if } C \textbf{ then } \pi_1 \textbf{ else } \pi_2 \textbf{ fi}\{\psi\}}{\{\varphi \,\&\, C\}\pi_1\{\psi\}, \{\varphi \,\&\, \neg C\}\pi_2\{\psi\}}$$

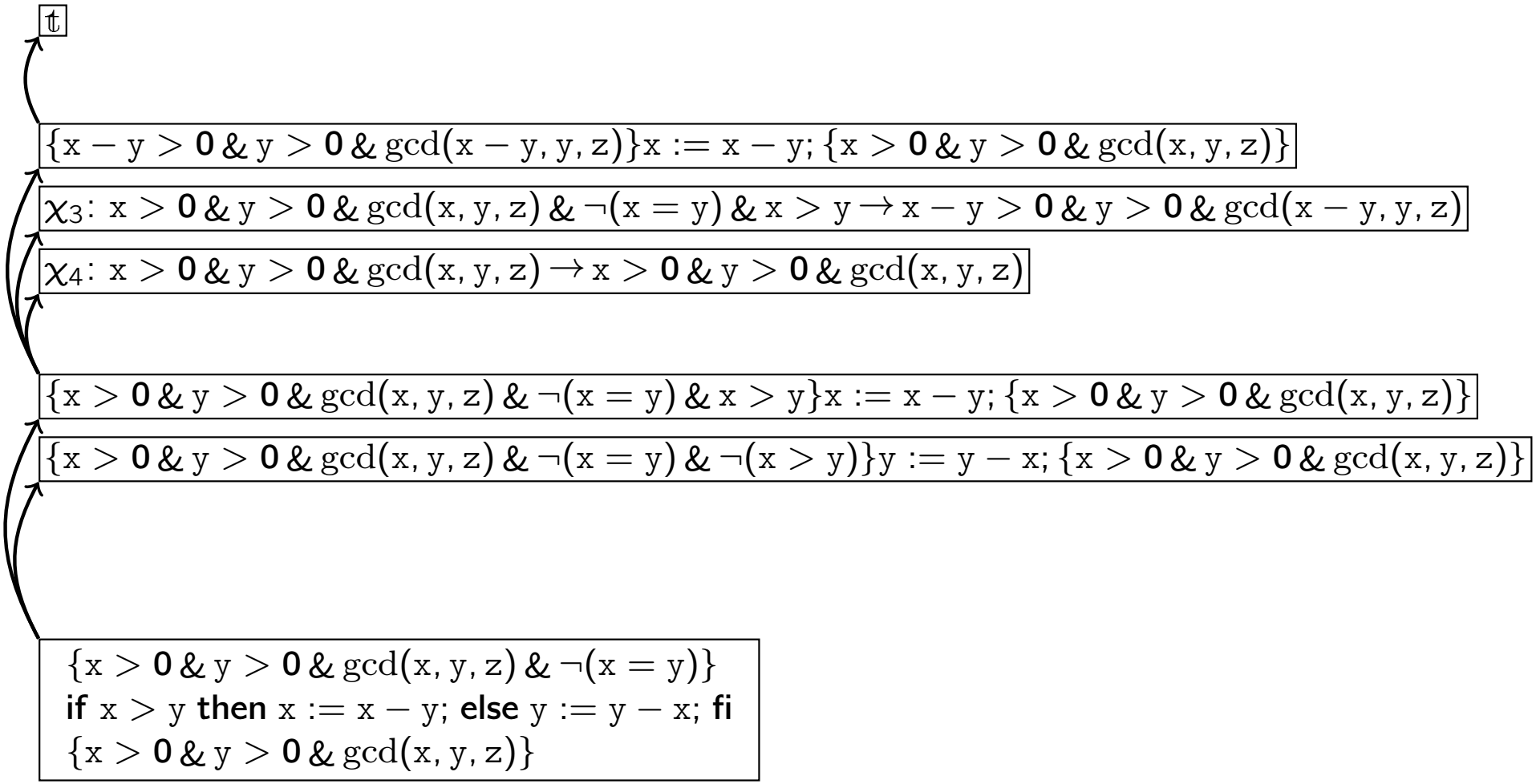
Логика Хоара



$$R_{inf}\colon \frac{\{\varphi\}\pi\{\psi\}}{\varphi \to \varphi', \{\varphi'\}\pi\{\psi'\}, \psi' \to \psi}$$

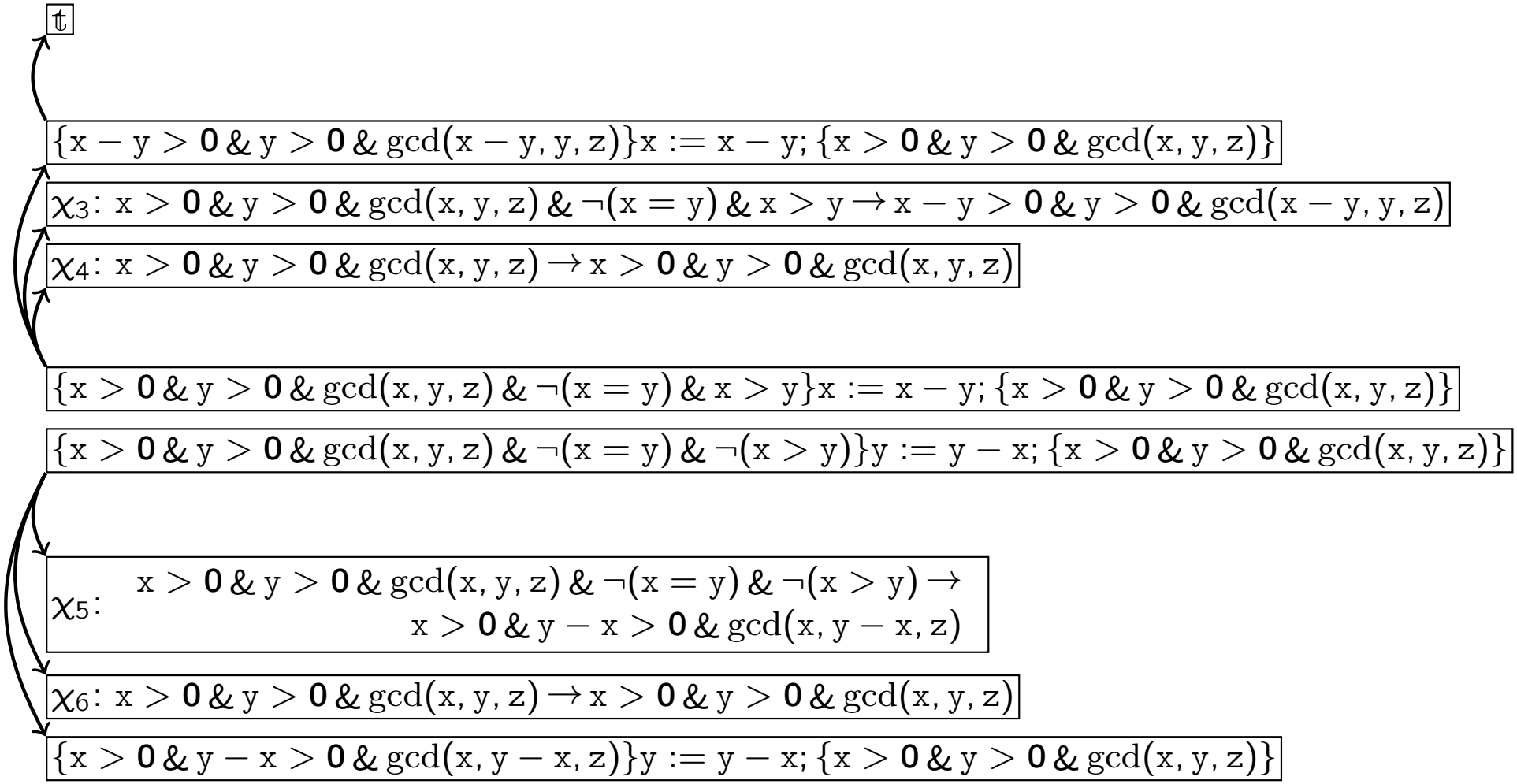
$$\mathcal{I} \models \chi_3$$
$$\mathcal{I} \models \chi_4$$

Логика Хоара



$$R_{:=}\colon \frac{\{\varphi\{x/t\}\}x := t; \{\varphi\}}{\mathbb{t}}$$

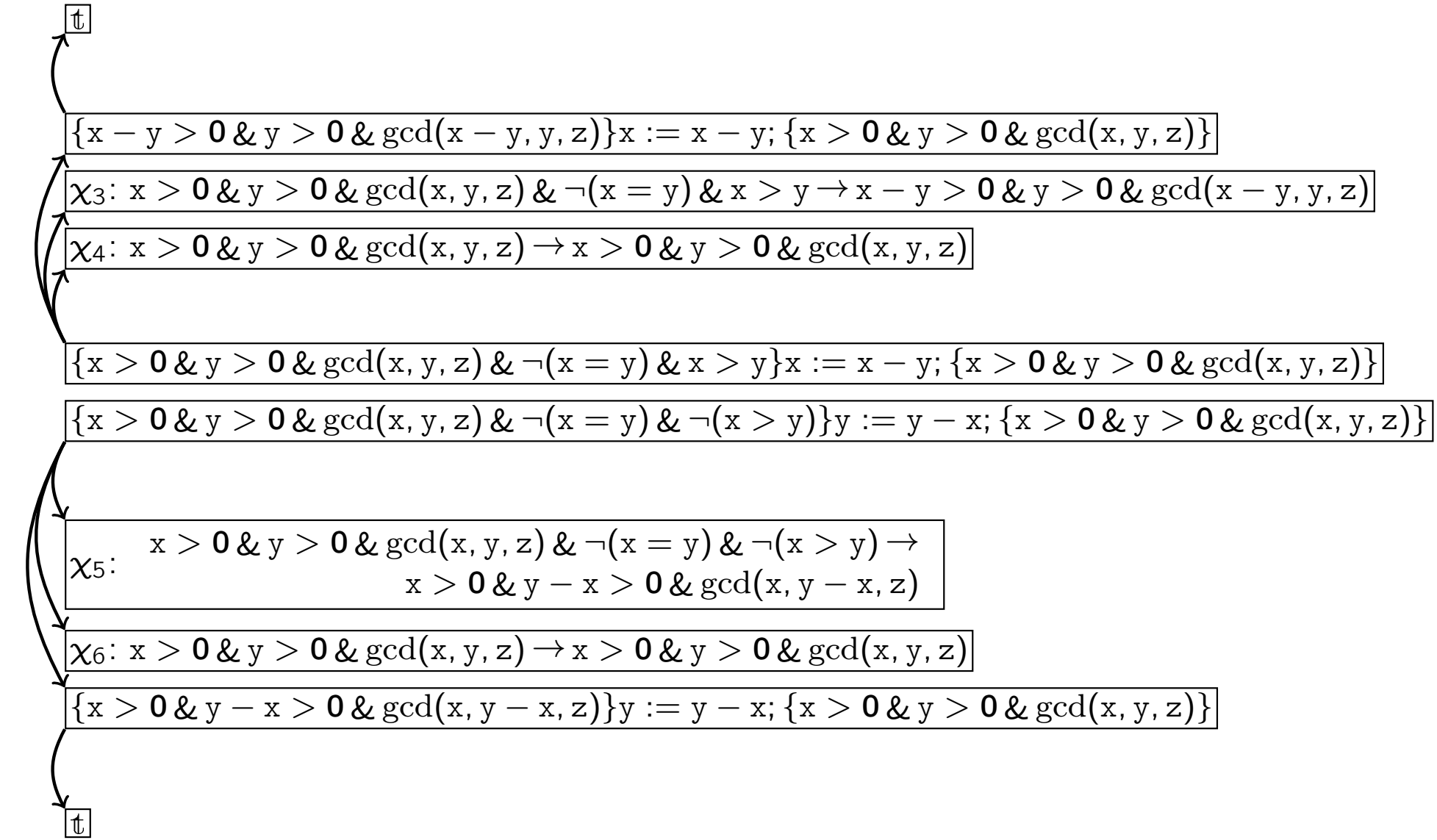
Логика Хоара



$$R_{inf}\colon \frac{\{\varphi\}\pi\{\psi\}}{\varphi \to \varphi', \{\varphi'\}\pi\{\psi'\}, \psi' \to \psi}$$

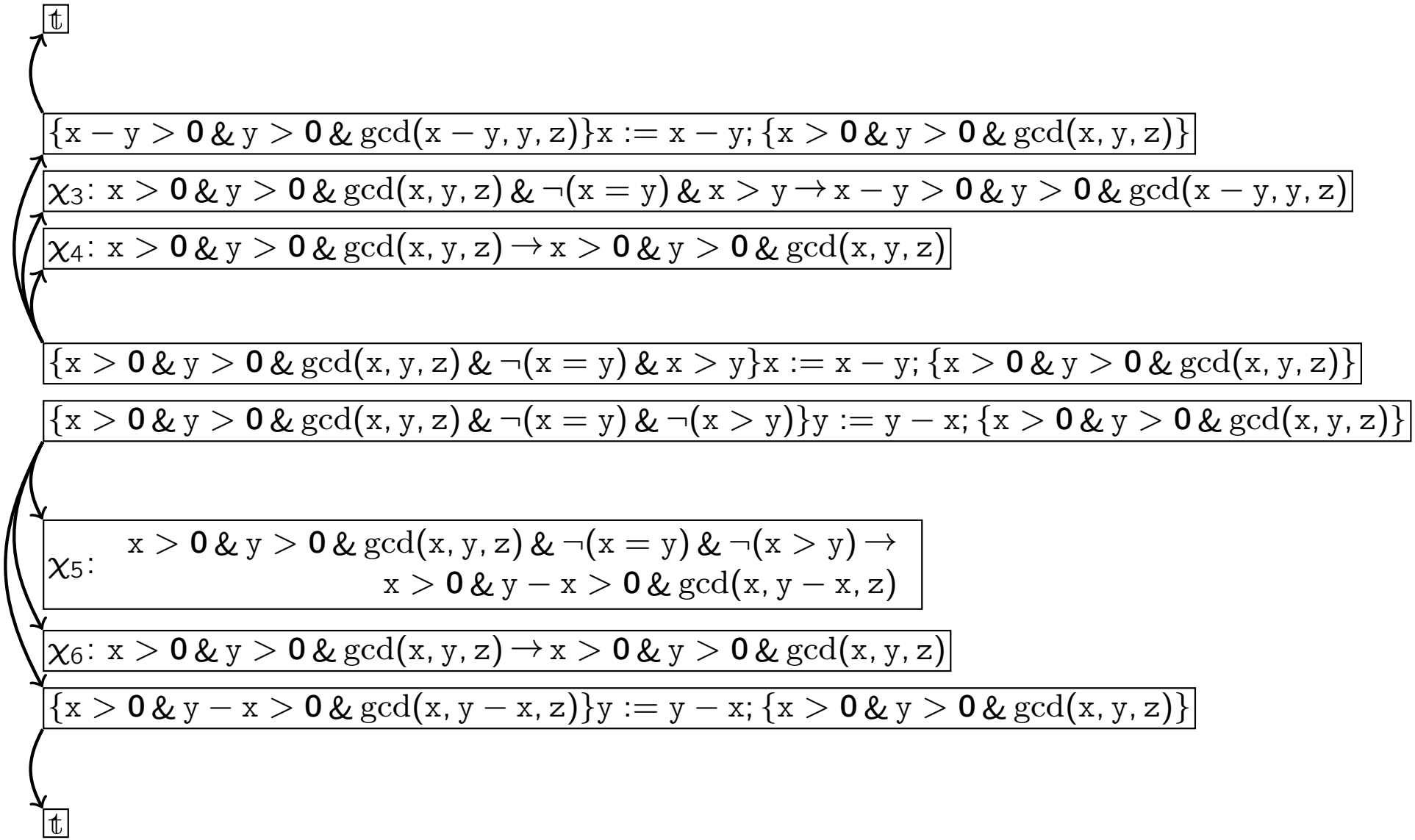
$$\mathcal{I} \models \chi_5$$
$$\mathcal{I} \models \chi_6$$

Логика Хоара



$$R_{:=}\colon \frac{\{\varphi\{x/t\}\}x := t;\{\varphi\}}{\mathbb{t}}$$

Логика Хоара



Частичная корректность программы доказана

Полнота логики Хоара

Согласно теореме о корректности логики Хоара,
правильность программы можно обосновать, построив
успешный табличный вывод подходящего триплета Хоара

А правда ли, что корректность **любой** правильной программы
может быть обоснована построением
успешного табличного вывода подходящего триплета?

На самом деле это не один вопрос, а два принципиально разных:

1. Все ли свойства правильности программ
   могут быть записаны в виде формул логики предикатов?
2. Для любого ли истинного триплета существует успешный вывод?

Полнота логики Хоара

Ответ на оба вопроса существенно зависит от сигнатуры,
в которой записываются предусловия и постусловия

Если эта сигнатура слишком «скудная», то:

- Её может быть недостаточно
  для записи свойств правильности программы
- При применении правил
  $$R_{seq} : \frac{\{\varphi\}\pi_1\ \pi_2\{\psi\}}{\{\varphi\}\pi_1\{\chi\}, \{\chi\}\pi_2\{\psi\}} \qquad R_{inf} : \frac{\{\varphi\}\pi\{\psi\}}{\varphi \to \varphi', \{\varphi'\}\pi\{\psi'\}, \psi' \to \psi}$$
  может и не найтись подходящих формул φ', ψ', χ,
  позволяющих достроить вывод до успешного

При этом чем «богаче» сигнатура, тем труднее анализировать
истинность формул и подбирать «подходящие» формулы при
построении вывода

Автоматизация проверки правильности программ

А если сигнатура достаточно «богата», то можно ли реализовать программу, автоматически доказывающую корректность программ?

Как и в вопросе про полноту, это на самом деле не один вопрос, а два:

1. Можно ли автоматизировать запись триплетов Хоара, отвечающих свойствам правильности программ?
2. Можно ли автоматизировать построение успешного вывода для заданного триплета Хоара?

Ответ на первый вопрос однозначен — **нет**:
один из главных недостатков формальной верификации состоит в том, что формальная спецификация программы, как правило, создаётся вручную специально обученным экспертом

Автоматизация проверки правильности программ

С автоматизацией построения успешного вывода
для заданного триплета Хоара дела обстоят чуть лучше

Слабейшим предусловием для программы π и постусловия ψ
в интерпретации $\mathcal{I}$ называется формула $wpr(\pi, \psi, \mathcal{I})$, такая что

- $\mathcal{I} \models \{wpr(\pi, \psi, \mathcal{I})\}\pi\{\psi\}$ и
- для любой формулы φ, такой что $\mathcal{I} \models \{\varphi\}\pi\{\psi\}$,
  верно соотношение $\mathcal{I} \models \varphi \to wpr(\pi, \psi, \mathcal{I})$

Слабейших предусловий на самом деле может быть много,
но они имеют одинаковый смысл в $\mathcal{I}$,
так что для простоты иногда будем считать, что оно единственно

Теорема. $\mathcal{I} \models \{\varphi\}\pi\{\psi\} \Leftrightarrow$
$\mathcal{I} \models \{wpr(\pi, \psi, \mathcal{I})\}\pi\{\psi\}$ **и** $\mathcal{I} \models \varphi \to wpr(\pi, \psi, \mathcal{I})$

Доказательство. Следует из определения слабейшего предусловия ▼

Автоматизация проверки правильности программ

Теорема (о слабейшем предусловии)

- $wpr(\emptyset, \psi, \mathcal{I}) = \psi$
- $wpr(\mathrm{x} := t;, \psi, \mathcal{I}) = \psi\{\mathrm{x}/t\}$,
  если подстановка $\{\mathrm{x}/t\}$ **правильна для** ψ
- $wpr(\textbf{if } C \textbf{ then } \pi_1 \textbf{ else } \pi_2 \textbf{ fi}, \psi, \mathcal{I}) =$
  $C \,\&\, wpr(\pi_1, \psi, \mathcal{I}) \vee \neg C \,\&\, wpr(\pi_2, \psi, \mathcal{I})$
- $wpr(\pi_1\ \pi_2, \psi, \mathcal{I}) = wpr(\pi_1, wpr(\pi_2, \psi, \mathcal{I}), \mathcal{I})$

Доказательство опустим, чтобы сэкономить время

Таким образом,

- проверка корректности программы сводится к вычислению слабейшего предусловия и проверки истинности заданной формулы
- для программ **без циклов** слабейшее предусловие не зависит от выбора интерпретации и вычисляется очень просто

Автоматизация проверки правильности программ

А как вычислить слабейшее предусловие для цикла?

Устройство слабейшего предусловия тесно связано с устройством правил доказательства корректности программ:
вычисление этого предусловия — настолько же (не)простая задача, насколько и применение правила для построения успешного вывода

Чтобы применить правило

$$R_{\textbf{while}} : \frac{\{\varphi\}\textbf{while } C \textbf{ do } \pi \textbf{ od}\{\varphi \,\&\, \neg C\}}{\{\varphi \,\&\, C\}\pi\{\varphi\}},$$

требуется предварительно найти формулу φ, реализующую свойство состояний данных, сохраняющееся при выполнении каждого витка цикла

Эта формула φ называется инвариантом цикла и явно или неявно используется практически всегда при анализе циклов

Автоматическая генерация инвариантов циклов — это **ключевая проблема** автоматизации проверки правильности программ