Математическая логика и логическое программирование

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

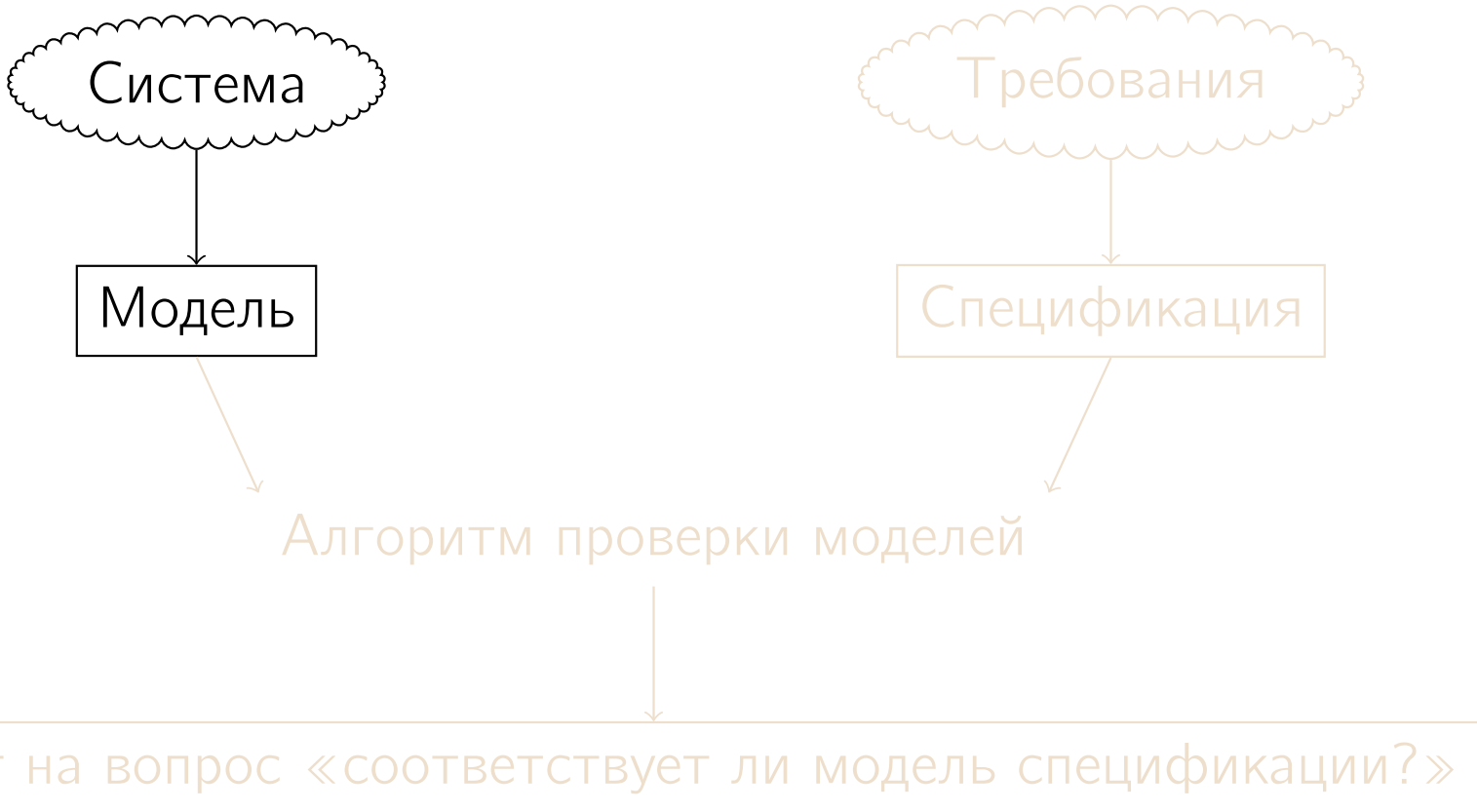
Блок 51

Модели Крипке

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

ВМК МГУ, 2025, сентябрь–декабрь

Вступление (краткая схема проверки моделей)



Модели Крипке

Чтобы лучше понять, как (*и почему именно так*) устроена модель вычислительной системы, используемая в проверке моделей, рассмотрим **для примера** такую систему

Система состоит из кофейного автомата и покупателя

Кофейный автомат имеет приёмник монет и кнопки «чай» и «кофе» и запрограммирован на такое поведение:

- В режиме ожидания приёмник монет открыт
- После приёма монеты
  - приёмник закрывается, ожидается нажатие на одну из кнопок,
  - после нажатия на кнопку соответствующий напиток выдаётся покупателю, монета удаляется из приёмника и автомат переходит в режим ожидания

Покупатель в зависимости от своего желания может кидать монеты в приёмник и нажимать на кнопки

Модели Крипке

Поведение кофейного автомата можно представить себе так

В каждый момент времени он находится в некотором состоянии:
«ожидает монету», «ожидает нажатия кнопки»,
«выдаёт чай», «выдаёт кофе»

Иногда автомат переходит из одного состояния в другое
согласно внешним обстоятельствам и своей программе

Некоторое состояние (начальное) отвечает запуску программы

Чтобы проверить правильность работы автомата, достаточно
выделить набор *простых* свойств состояний (атомарных высказываний)
и проанализировать изменение этих свойств с течением времени:
«приёмник открыт», «в приёмнике есть монета»,
«выдаётся чай», «выдаётся кофе»

Модели Крипке

Для множества X записью 2^X будем обозначать
множество всех подмножеств X

В качестве модели системы будем использовать модель Крипке (МК)
над множеством атомарных высказываний (АВ) $\mathcal{AP}$ —
систему $M = (S, S_0, \to, L)$, где:

- S — множество состояний
- S_0 — множество начальных состояний, $S_0 \subseteq S$
- $\to \subseteq S \times S$ — тотальное отношение переходов
- $L : S \to 2^{\mathcal{AP}}$ — функция разметки

Тотальность отношения переходов означает, что
для любого состояния s существует состояние s', такое что $s \to s'$

МК будем называть конечной,
если конечны множества её состояний и АВ

Модели Крипке

МК представляет собой размеченный ориентированный граф, вершинами которого являются состояния, а дугами — переходы, и поэтому будем использовать для МК терминологию теории графов

Путь в МК будем называть начальным, если он исходит из начального состояния

Бесконечный начальный путь будем называть вычислением МК

Вычисления МК отвечают (*потенциально*) бесконечным сценариям выполнения моделируемой системы

Модели Крипке

Пример: МК кофейного автомата

Атомарные высказывания:

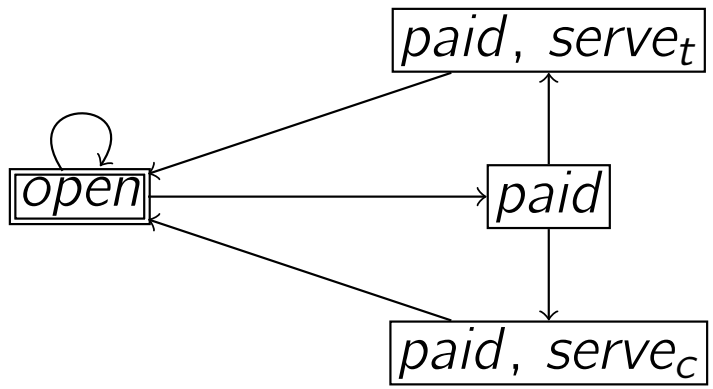
$open$ = «приёмник открыт»

$paid$ = «в приёмнике есть монета»

$serve_t$ = «выдаётся чай»

$serve_c$ = «выдаётся кофе»

Модель Крипке:



□ — состояние

▣ — начальное состояние

Высказывания, размечающие состояние,
записаны внутри этого состояния

Модель Крипке программы

Математически строгий анализ императивной программы π
(и программ других парадигм в рамках операционной семантики),
как правило, основан на понятиях, которые уже появлялись в лекциях:

- Состояние управления:
  то, какую часть программы осталось выполнить
- Состояние данных: то, как устроены данные,
  преобразуемые программой на каждом шаге
  (например, оценки переменных или запросы)
- Состояние вычисления,
  включающее в себя состояние данных и состояние управления
- Отношение $\rightarrow_\pi$ шага вычисления программы π

Модель Крипке программы

Программе π отвечает МК $(S, S_0, \mapsto, L)$ над $\mathcal{AP}$, где:

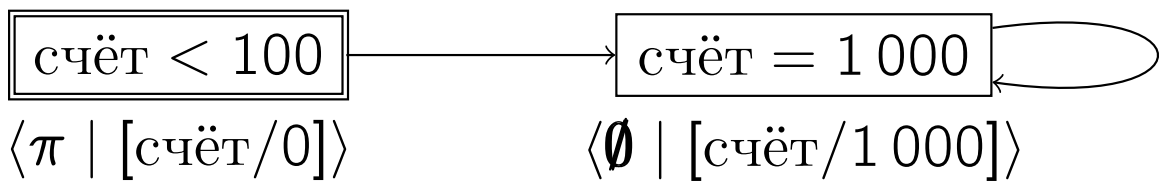
- S — множество всех состояний вычисления π
- S_0 — состояния, с которых начинаются вычисления π на интересующих входных данных
- $\mapsto = \rightarrow_\pi$ с поправкой на требуемую тотальность: если из состояния s не исходит ни одного перехода, то в $\mapsto$ «насильно» добавляется переход $s \mapsto s$
- $\mathcal{AP}$ суть интересующие свойства состояний вычисления, например:
  - «$\mathrm{x} = 2$», «$\mathrm{x} > 2$», «$\mathrm{x} > \mathrm{y}$»
  - «Состояние управления — это пустая команда»
  - «Предикатный символ левой подцели — P»
- $L(s)$ состоит из всех AB, истинных для s согласно естественной трактовке их записи

Модель Крипке программы

Пример

$$\pi = \text{счёт} := \text{счёт} + 1\,000;$$

Достижимый фрагмент МК этой модельной императивной программы для интерпретации $Ar_{\mathbb{Z}}$, начальной оценки $[\text{счёт}/0]$ и АВ «$\text{счёт} < 100$» и «$\text{счёт} = 1\,000$»:



Модель Крипке программы

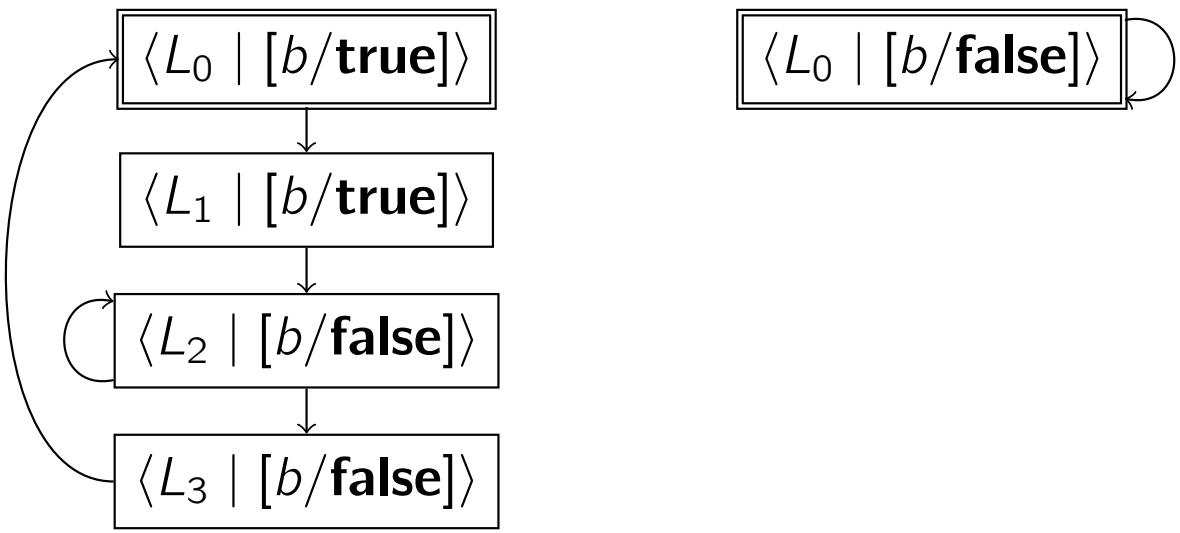
Другой пример

Пусть в сетевом принтере содержится булев регистр $\mathtt{b}$,
обозначающий *занятость* принтера,
и доступ к нему осуществляется при помощи такой программы π:

$$\textbf{while } (\textbf{true}) \{ \quad L_0 : \textbf{while } (!\mathtt{b}); \quad L_1 : \mathtt{b} = \textbf{false}; \\ L_2 : \mathit{EXCHANGE} \quad L_3 : \mathtt{b} = \textbf{true}; \quad \}$$

(*EXCHANGE* — подпрограмма обмена данными для печати)

Фрагмент МК для π, достижимый из начальных состояний
с произвольным начальным значением $\mathtt{b}$, может быть устроен так
(*для простоты считаем, что метка состояния — это оно само*):



Модель Крипке программы в окружении

Программа в распределённой системе может
взаимодействовать со своим **окружением** при помощи
разделяемых переменных, сообщений, сигналов, ...

Такое взаимодействие выражается в том,
что состояние вычисления программы
может измениться под воздействием окружения

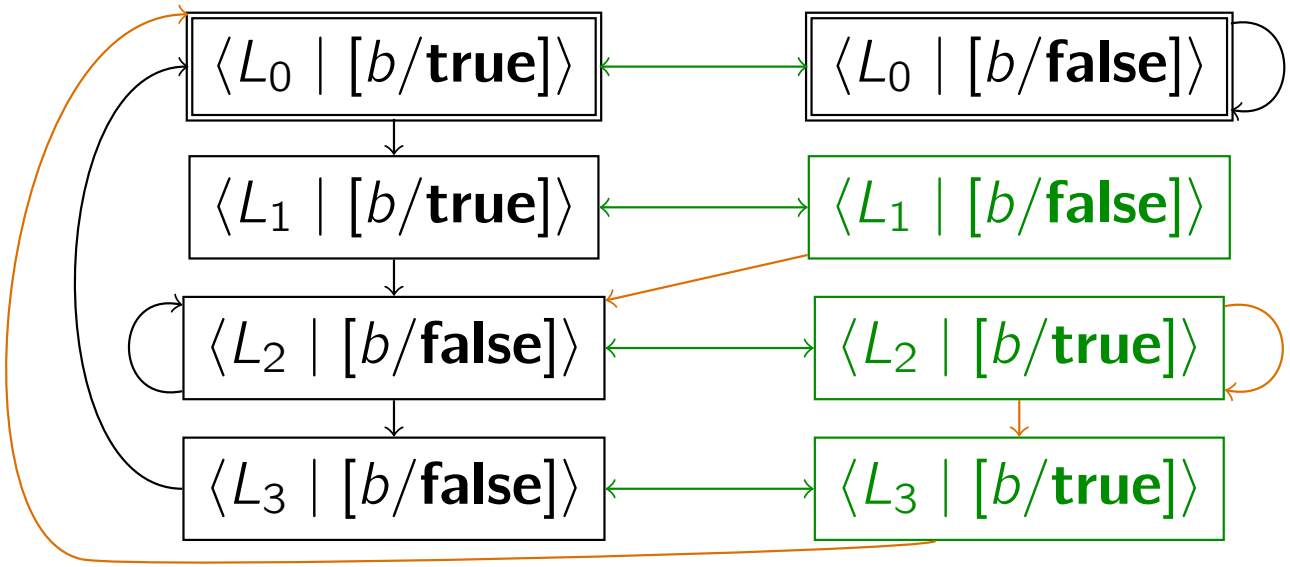
МК программы в окружении — это МК программы,
в которую добавлены переходы, отвечающие возможностям окружения

Модель Крипке программы в окружении

Пример

$$\textbf{while}\ (\textbf{true})\ \{ \quad L_0 : \textbf{while}\ (!\mathtt{b});\quad L_1 : \mathtt{b} = \textbf{false};$$
$$L_2 : \mathit{EXCHANGE}\quad L_3 : \mathtt{b} = \textbf{true};\quad \}$$

МК для программы доступа к сетевому принтеру
в окружении, способном произвольно изменять значение регистра $\mathtt{b}$,
может быть устроена так:



Параллельная композиция моделей Крипке

Наиболее популярный способ композиции МК параллельно выполняющихся программ — это асинхронная композиция (согласно семантике чередующихся вычислений; *interleaving*)

Это способ композиции устроен так:

- Состояние композиции компонентов представляет собой набор локальных частей их состояний и *включённую один раз* общую (разделяемую) часть
- Переход в композиции отвечает
  - произвольному выбору одного из компонентов и перехода в нём и
  - выполнению этого перехода с изменением локальной части состояния компонента и общей части состояния согласно устройству МК компонента системы

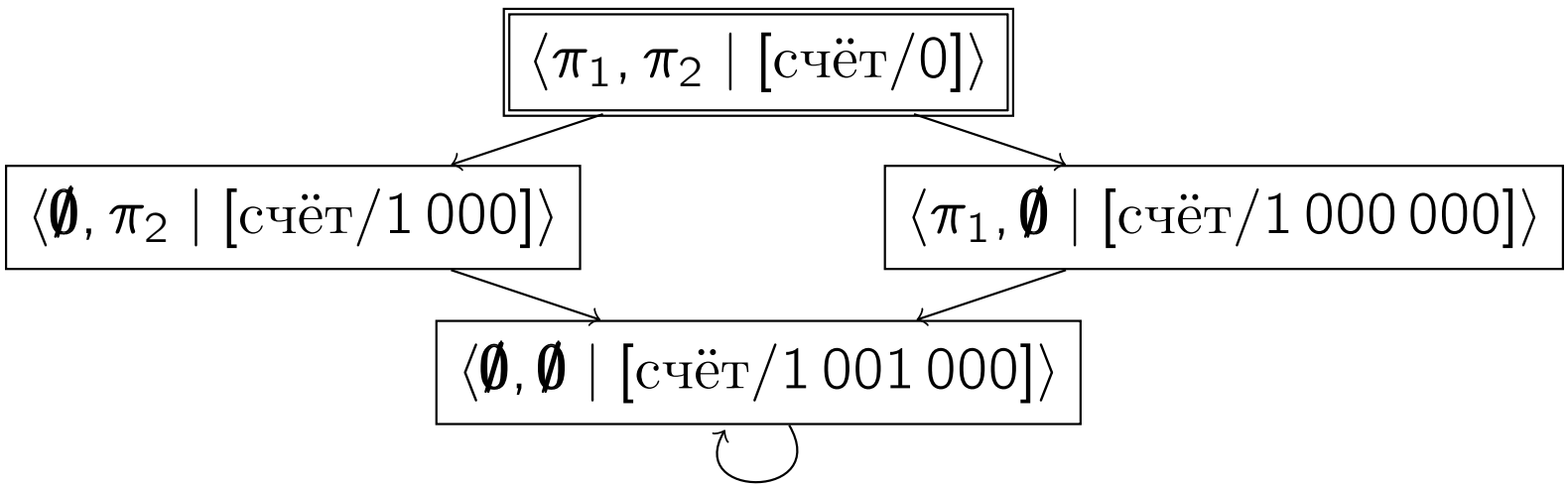
В вычислении построенной так композиции произвольно чередуется выполнение переходов компонентов системы

Параллельная композиция моделей Крипке

Пример

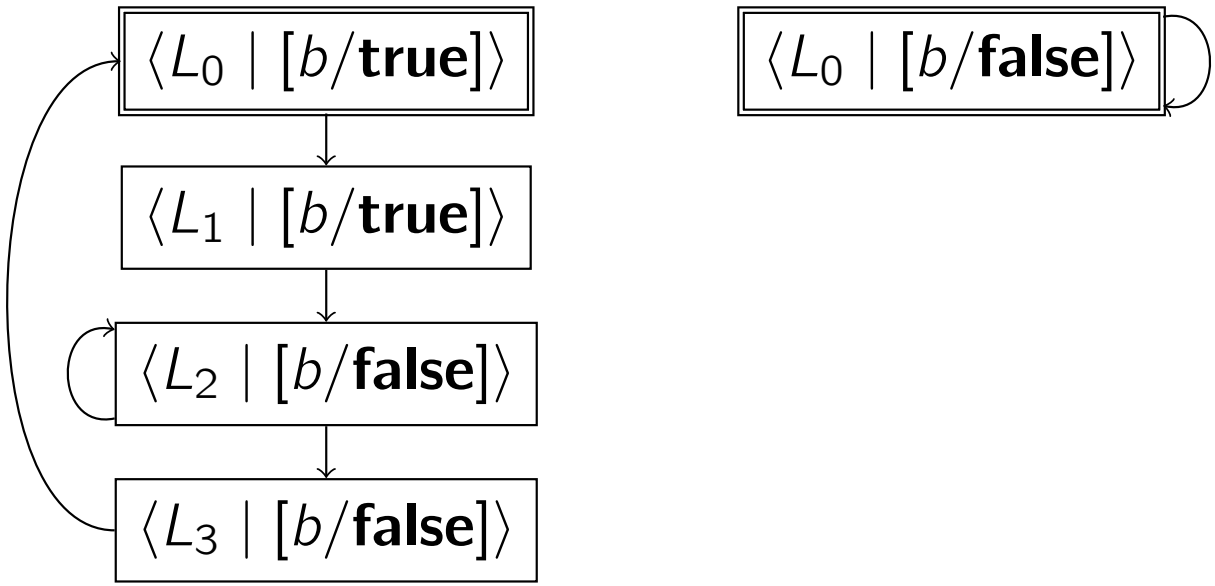
$$\pi_1 = \text{счёт} := \text{счёт} + 1\,000; \qquad \pi_2 = \text{счёт} := \text{счёт} + 1\,000\,000;$$

Достижимый фрагмент асинхронной композиции МК
этих двух модельных императивных программ
с общей переменной «счёт»
для интерпретации $Ar_{\mathbb{Z}}$ и начальной оценки $[\text{счёт}/0]$ устроен так:



Параллельная композиция моделей Крипке

Другой пример



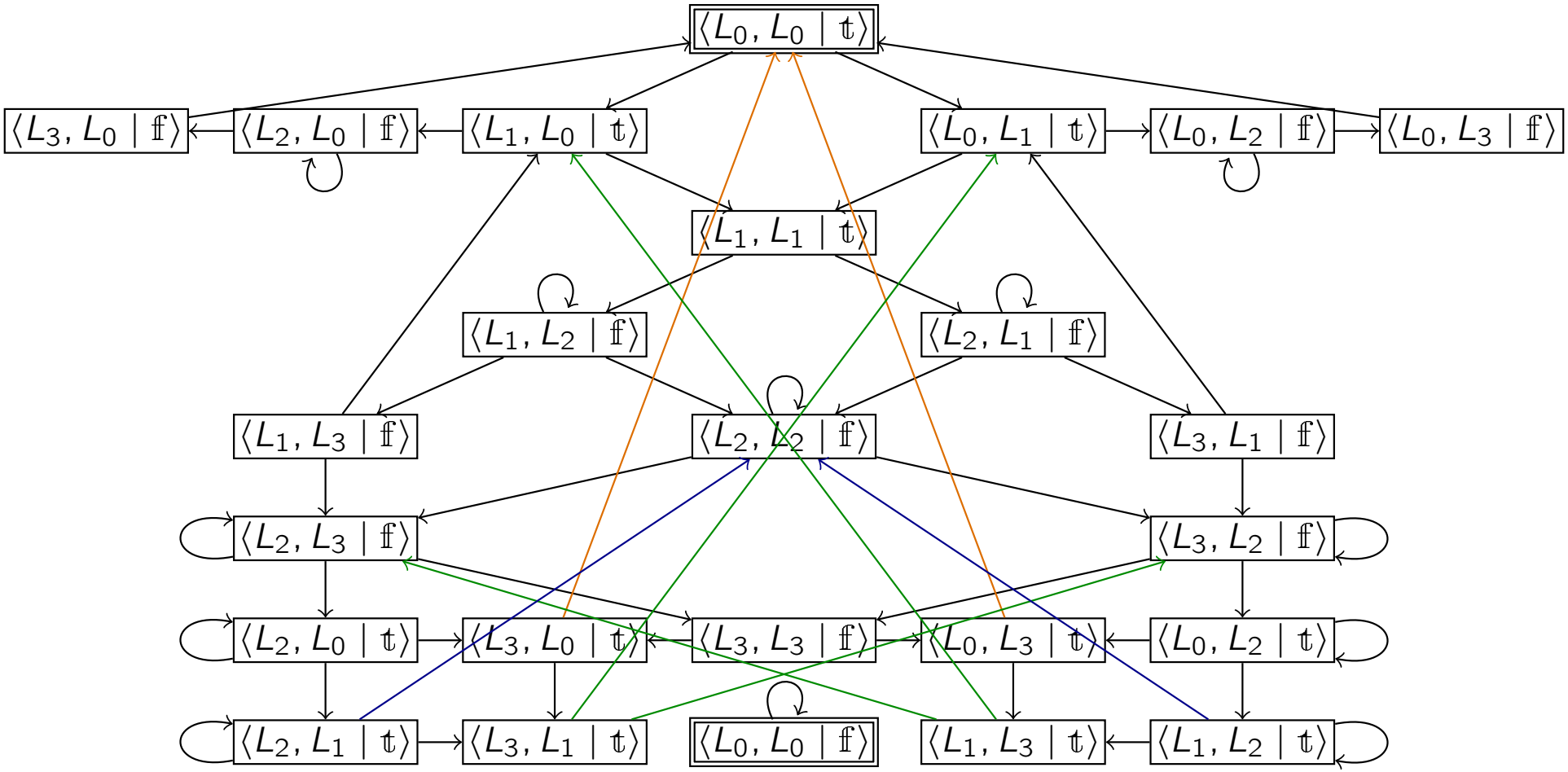
Предположим, что

- с сетевым принтером взаимодействуют две программы с одинаковыми МК (как изображено выше) и
- регистр b является общим для обеих программ

Тогда асинхронная композиция МК, отвечающая параллельному выполнению двух программ доступа к принтеру, устроена так ...

Параллельная композиция моделей Крипке

Другой пример



Согласно методу проверки моделей,
построение и анализ композиции МК производятся автоматически,
так что «нечитаемость» композиции не считается недостатком