

05 Марта 2010

Инсерционное моделирование 1

Лекция 3

**Система верификации документированных программ.
Транзиционные системы.**

<http://apsystem.org.ua/lectures.html>

Контрольные задания

1-й модуль (до 1 апреля)

1. Верифицировать программу поиска наименьшего и наибольшего числа в массиве.
2. Верифицировать программу вычисления наибольшего общего делителя двух чисел

Решения посылать по адресу: let@cyfra.net

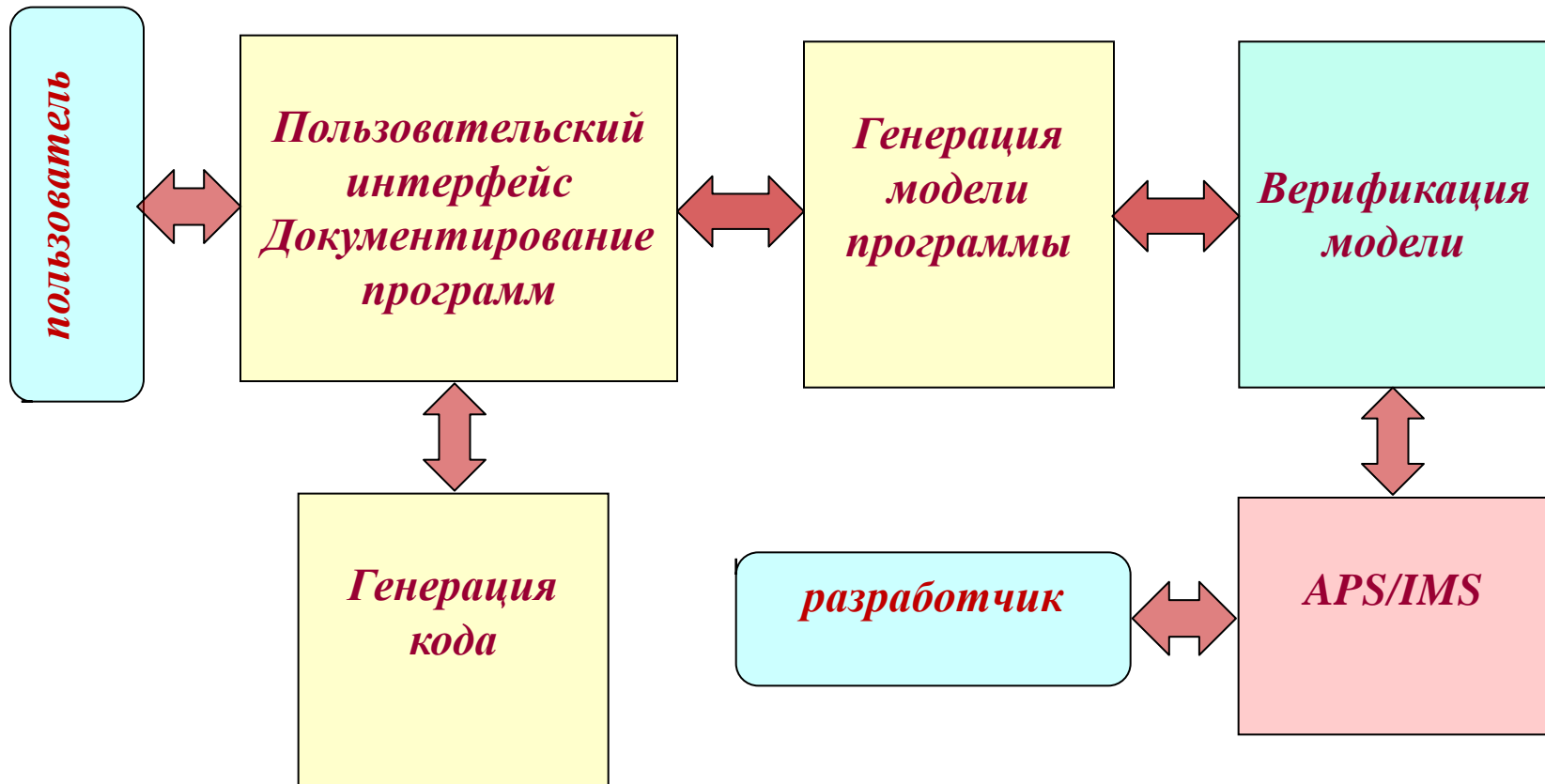
Полезная ссылка:

В.А.Непомнящий, О.М.Рякин

Прикладные методы верификации программ

М. «Радио и связь»

Проект системы верификации документированных программ



APS/IMS

1-system (APLAN)

2-applications (APLAN)

aps/ims (C++)

2-applications/5-verification of programs/10-generate model

input.ap: запрос к системе инсерционного моделирования,
построить и верифицировать модель факториала.

Транзиционные системы

Ординарные транзитивные системы

Другой термин: дискретные динамические системы

$$\langle S, T \rangle, T \subseteq S^2$$

$$s \rightarrow s'$$

S – пространство состояний

T – отношение переходов



Движение в фазовом пространстве,
(для заданного временного интервала, разностные системы)

Изменение состояния
хардверной системы

Изменение состояния
софтверной системы

Транзитивное замыкание, достижимость

Размеченные транзиторные системы

$$\langle S, A, T \rangle, \quad T \subseteq S \times A \times S$$

D.Park (1981)

$$S \xrightarrow{a} S'$$

A – множество меток
символы,
события,
действия

Черный ящик

состояния скрыты
действия наблюдаемы

Непрерывные динамические системы:

действия – длительность перехода

Автоматы:

входные символы, вход/выход

Программы:

операторы, условия, условные операторы

Исчисления:

состояния – формулы (множества формул),
действия – правила вывода, предикатные
трансформеры, верифицирующие условия.

**Взаимодействующие распределенные
системы:**

передача (прием) сообщений

Базы данных

запросы, ответы

Смешанные системы

$$\langle S, A, T \rangle, T \subseteq S \times A \times S \cup S^2$$

$$S \xrightarrow{a} S' \quad \text{наблюдаемые переходы}$$

$$S \longrightarrow S' \quad \text{скрытые переходы}$$

абстракция и конкретизация

Атрибутные транзиторные системы

$$\langle S, A, U, T, \varphi \rangle, \varphi: S \rightarrow U$$

Автоматы Мура

$$U = D^R$$

Программы над памятью

атрибуты

$$U = (D_{\xi}^{R_{\xi}})_{\xi \in \Xi}$$

Типизированная память

$$D = \{0, 1\}$$

Системы Крипке (модальная логика)

(Не размеченные переходы)

Настроенные системы

$$S_0, S_{\Delta}, S_{\perp} \subseteq S$$

S_0 **начальные состояния**
 S_{Δ} **заключительные состояния**
 S_{\perp} **неопределенные состояния (можно доопределять)**

Трассовая эквивалентность

История: $s_1 \xrightarrow{a_1} s_2 \xrightarrow{a_2} \dots \xrightarrow{a_n} \dots$

Трасса: $a_1 a_2 \dots a_n \dots$

Трасса для атрибутивной системы:

$$\varphi(s_1) \xrightarrow{a_1} \varphi(s_2) \xrightarrow{a_2} \dots \xrightarrow{a_n} \dots$$

$L(s)$ трассы из S

$$s \sim_T t \Leftrightarrow L(s) = L(t)$$

$L_{\Delta}^0(S)$ трассы из S_0 в S_{Δ}

$$S \sim_T S' \Leftrightarrow L(S_{\Delta}^0) = L((S')_{\Delta}^0)$$

Недетерминизм

Система детерминирована:

$$s \xrightarrow{a} s' \wedge s \xrightarrow{a} s'' \Rightarrow s' = s''$$

настройки не пересекаются

