Семинар «Образный компьютер»

ДОКАЗАТЕЛЬНОЕ ПРОЕКТИРОВАНИЕ РЕАКТИВНЫХ АЛГОРИТМОВ

Чеботарев
Анатолий Николаевич

Институт кибернетики им.В.М.Глушкова

НАН Украины

ancheb@gmail.com

24.05.2011

РЕАКТИВНЫЕ СИСТЕМЫ

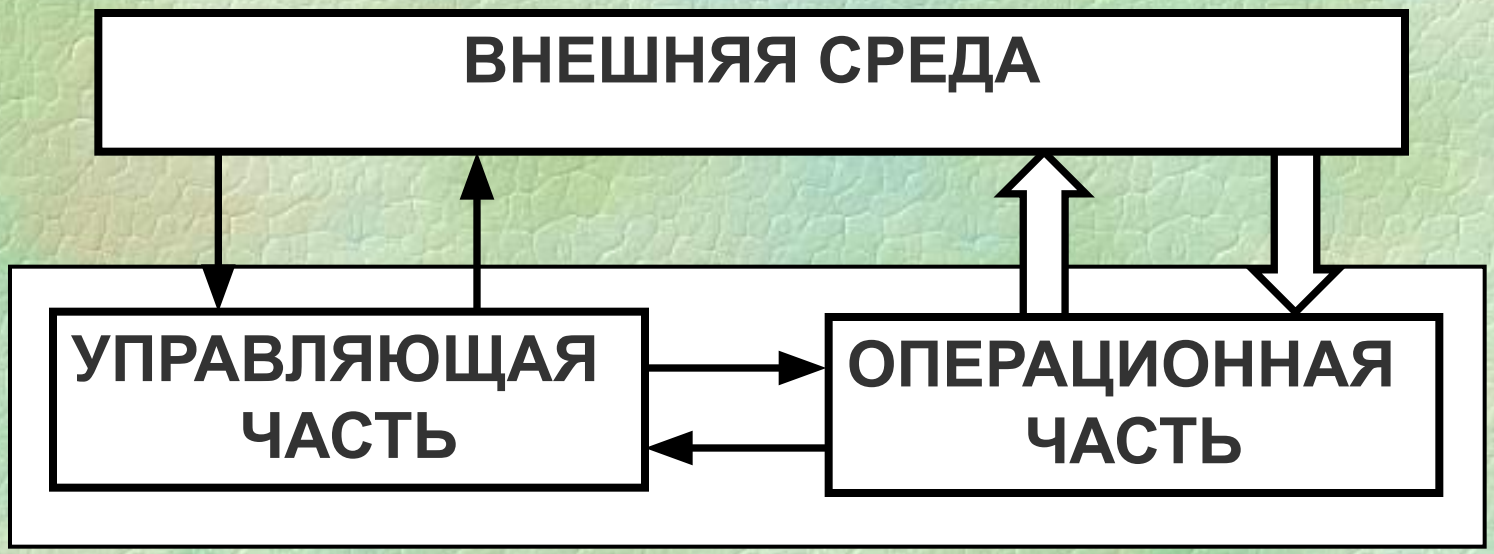
Под **реактивными системами** понимаются системы, постоянно взаимодействующие со своим окружением.

Примеры таких систем

- системы управления технологическими процессами,
- телекоммуникационные сети,
- системы управления летательными аппаратами и др.

Функционирование таких систем состоит в выработке реакции на сигналы, поступающие из окружающей среды.

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ РЕАКТИВНОГО АЛГОРИТМА



ПОДХОД К ПРОЕКТИРОВАНИЮ

При проектировании систем управления потенциально опасными объектами необходимо гарантировать точное соответствие алгоритма управления всем требованиям к функционированию системы.

В основе подхода лежит спецификация функциональных требований к системе в языке логики предикатов и формальный переход от спецификации к процедурному представлению алгоритма функционирования проектируемой системы.

ОСНОВНЫЕ ПОДХОДЫ К КОРРЕКТНОМУ ПРОЕКТИРОВАНИЮ РЕАКТИВНЫХ АЛГОРИТМОВ

ФОРМАЛЬНАЯ ВЕРИФИКАЦИЯ доказывает, что полученный алгоритм обладает некоторыми свойствами, однако не гарантирует, что он в точности соответствует своему назначению.

ОСНОВНЫЕ ПОДХОДЫ К КОРРЕКТНОМУ ПРОЕКТИРОВАНИЮ РЕАКТИВНЫХ АЛГОРИТМОВ

СИНТЕЗ

гарантирует точное соответствие между спецификацией требований к алгоритму и ее процедурной реализацией.

ОСНОВНЫЕ ПОДХОДЫ К КОРРЕКТНОМУ ПРОЕКТИРОВАНИЮ РЕАКТИВНЫХ АЛГОРИТМОВ

ДОКАЗАТЕЛЬНОЕ ПРОЕКТИРОВАНИЕ доказывается корректность всех процедур проектирования, а также всех преобразований, выполняемых разработчиком в процессе интерактивного проектирования.

ЯЗЫКИ СПЕЦИФИКАЦИИ

$\Omega = \{p_1, \ldots, p_k\}$ – ПРЕДИКАТНЫЕ СИМВОЛЫ

t – ПЕРЕМЕННАЯ, СО ЗНАЧЕНИЯМИ ИЗ Z

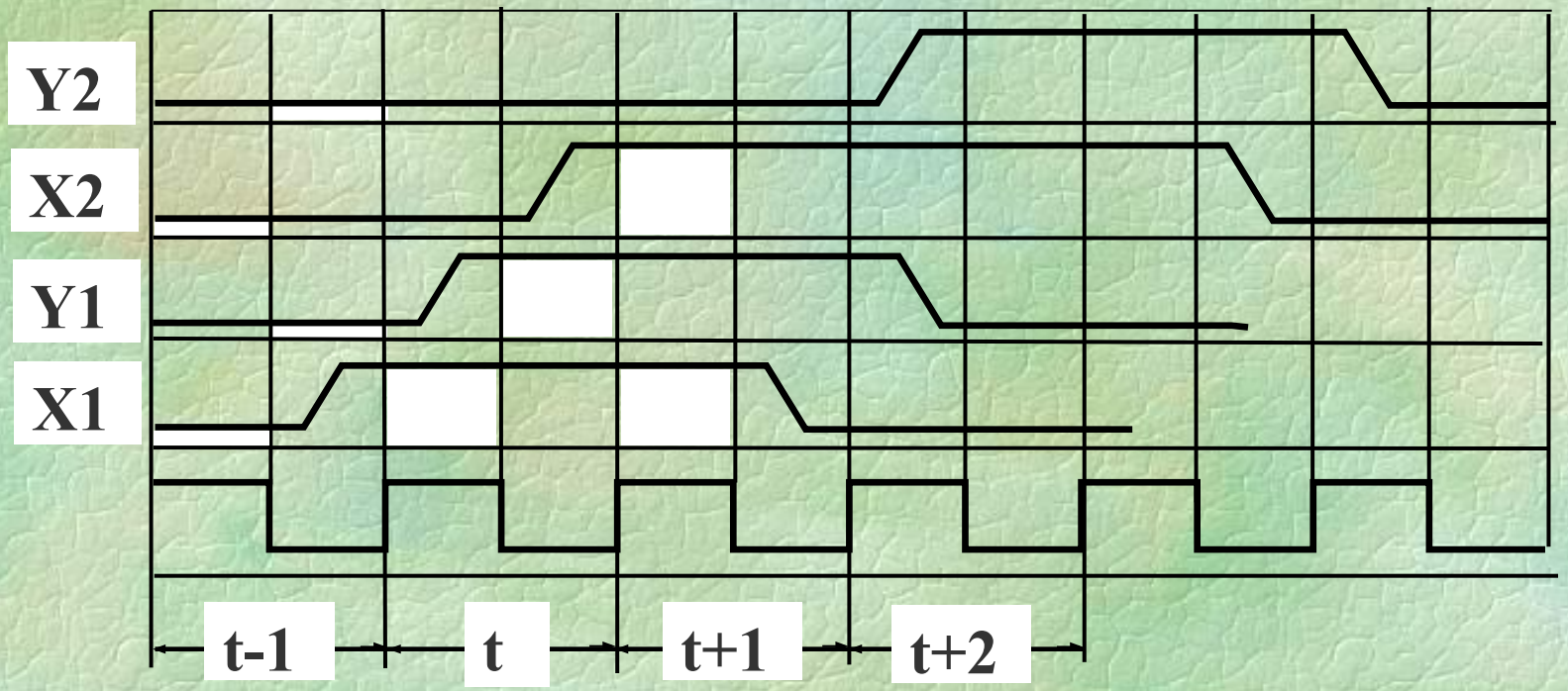
ВИД ФОРМУЛ СПЕЦИФИКАЦИИ : $\forall t\, F(t)$

ЯЗЫК L

$F(t)$ – ФОРМУЛА, ПОСТРОЕННАЯ С ПОМОЩЬЮ ЛОГИЧЕСКИХ СВЯЗОК ИЗ АТОМОВ ВИДА

$p(t + k)$, где $p \in \Omega$, $k \in Z$.

ПРИМЕР СПЕЦИФИКАЦИИ



ПРИМЕР СПЕЦИФИКАЦИИ

{Y1(Y2) РАВЕН 1 ТОЛЬКО ТОГДА, КОГДА X1(X2) =1}

$$Y1(t) \rightarrow X1(t)\ ,\ Y2(t) \rightarrow X2(t),$$

{СТАВ РАВНЫМ 1, Y1(Y2) СОХРАНЯЕТ ЭТО ЗНАЧЕНИЕ ,

ПОКА X1(X2) = 1}

$$Y1(t–1)\ \&\ X1(t) \rightarrow Y1(t),$$

$$Y2(t–1)\ \&\ X2(t) \rightarrow Y2(t),$$

{ВЗАИМНОЕ ИСКЛЮЧЕНИЕ}

$$\neg(Y1(t)\ \&\ Y2(t)),$$

{Y1(Y2) ИЗМЕНЯЕТСЯ В 1 ОДНОВРЕМЕННО С X1(X2)}

$$X1(t) \rightarrow (Y1(t) \vee Y2(t)),$$

$$X2(t) \rightarrow (Y1(t) \vee Y2(t)).$$

$$F = \forall tF(t)$$

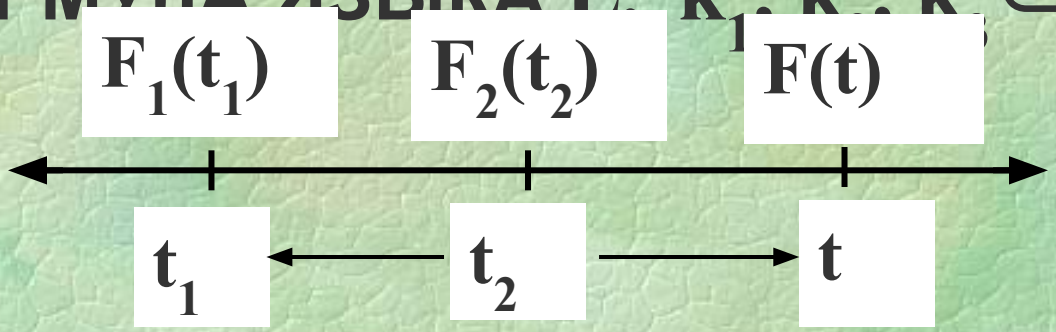
ЯЗЫК L*

ДОБАВЛЯЕТСЯ КОНСТРУКЦИЯ

$$\exists t_1(t_1 \le t+k_1)\&F_1(t_1)\&\forall t_2(t_1+k_2 \le t_2 \le t+k_3) \rightarrow F_2(t_2),$$

$F_1(t_1)$ – ФОРМУЛА ЯЗЫКА L*,

$F_2(t_2)$ – ФОРМУЛА ЯЗЫКА L, $k_1, k_2, k_3 \in Z$.



СВЕРХСЛОВА

АЛФАВИТ $\Sigma = \{<00\ldots0>, \ldots, <11\ldots1>\}$

Σ^* – МНОЖЕСТВО ВСЕХ СЛОВ В АЛФАВИТЕ Σ

ПУСТЬ $\sigma_i \in \Sigma \quad (i \in Z)$

$\ldots\sigma_{-2}\sigma_{-1}\sigma_0\sigma_1\sigma_2\ldots$ – ДВУСТОРОННЕЕ СВЕРХСЛОВО (Σ^Z)

$\sigma_1\sigma_2\ldots$ – СВЕРХСЛОВО (Σ^ω)

$\ldots\sigma_{-2}\sigma_{-1}\sigma_0$ – ОБРАТНОЕ СВЕРХСЛОВО $(\Sigma^{-\omega})$

СВЕРХСЛОВА

ПУСТЬ $k \in Z$ И $u \in \Sigma^Z$

k-префикс $u(-\infty, k) = \ldots\sigma_{k-2}\sigma_{k-1}\sigma_k$

k-суффикс $u(k+1, \infty) = \sigma_{k+1}\sigma_{k+2}\ldots$

АВТОМАТЫ

$(X–Y)$ – АВТОМАТ $A = \langle X, Y, Q, \chi_A \rangle$, ГДЕ

$\chi_A: Q \times X \times Y \to Q$ – ФУНКЦИЯ ПЕРЕХОДОВ,

$$\Sigma = X \times Y$$

Σ-АВТОМАТ $A = \langle \Sigma, Q, \delta_A \rangle$, ГДЕ $\delta_A: Q \times \Sigma \to Q$

СВЕРХСЛОВА И АВТОМАТЫ.

$l = \sigma_1\sigma_2\ldots$ *ДОПУСТИМО* В СОСТОЯНИИ q АВТОМАТА A, ЕСЛИ СУЩЕСТВУЕТ ТАКОЕ СВЕРХСЛОВО $q_0q_1q_2\ldots$, ГДЕ $q_0 = q$, ЧТО ДЛЯ ЛЮБОГО $i = 0, 1, 2,\ldots$ $\delta_A(q_i, \sigma_{i+1}) = q_{i+1}$.

АВТОМАТЫ

ПУСТЬ $Q = \{q_1, \ldots, q_n\}$ –

МНОЖЕСТВО СОСТОЯНИЙ АВТОМАТА A.

СЕМЕЙСТВО МНОЖЕСТВ $(S_1, \ldots, S_n)$, ГДЕ S_i – МНОЖЕСТВО ВСЕХ СВЕРХСЛОВ, ДОПУСТИМЫХ В СОСТОЯНИИ q_i $(i = 1, 2, \ldots, n)$, НАЗЫВАЕТСЯ *ПОВЕДЕНИЕМ* АВТОМАТА A.

ФОРМУЛЫ И АВТОМАТЫ

ИНТЕРПРЕТАЦИЯ ЯЗЫКА

ПУСТЬ $\Omega = \{p_1, \ldots, p_k\}$

p_1 …0110100…

. .

. . $\Sigma = \{<00\ldots0>, \ldots, <11\ldots1>\}$

p_k …1001110…

M_F – МНОЖЕСТВО ВСЕХ МОДЕЛЕЙ ДЛЯ F,

W_F – МН – ВО ВСЕХ 0-СУФФИКСОВ ИЗ M_F ,

$u \in M_F \quad S_u = \{ l \in \Sigma^\omega \mid u(-\infty, 0) \cdot l \in M_F\}$

$\Re_F = \{S_u \mid u \in M_F\} = \{S_1, \ldots, S_n\}$

ФОРМУЛЫ И АВТОМАТЫ

ФОРМУЛА $F = \forall t F(t)$ СПЕЦИФИЦИРУЕТ АВТОМАТ A, ПОВЕДЕНИЕ КОТОРОГО СОВПАДАЕТ С $\Re_F = \{S_1, \ldots, S_n\}$.

ОСНОВНЫЕ ПРОЦЕДУРЫ ПРОЕКТИРОВАНИЯ

1. ПРОВЕРКА НЕПРОТИВОРЕЧИВОСТИ
2. ВЕРИФИКАЦИЯ СПЕЦИФИКАЦИИ
3. ПРЕОБРАЗОВАНИЕ СПЕЦИФИКАЦИИ ВО МНОЖЕСТВО ДИЗЪЮНКТОВ
4. ПОСТРОЕНИЕ АВТОМАТА, ПРЕДСТАВЛЕННОГО МНОЖЕСТВОМ СОСТОЯНИЙ И ФУНКЦИЯМИ ПЕРЕХОДОВ И ВЫХОДОВ
5. ДЕТЕРМИНИЗАЦИЯ АВТОМАТА

ОСОБЕННОСТИ ПОДХОДА

- ОГРАНИЧЕННЫЙ СИНТАКСИС ЯЗЫКА СПЕЦИФИКАЦИИ
- ИНТЕРПРЕТАЦИЯ ЯЗЫКА НА МНОЖЕСТВЕ ЦЕЛЫХ ЧИСЕЛ
- ИСПОЛЬЗОВАНИЕ МОДЕЛИ НЕИНИЦИАЛЬНОГО АВТОМАТА ДЛЯ ПРЕДСТАВЛЕНИЯ РЕАКТИВНОГО АЛГОРИТМА

СПАСИБО

ЗА ВНИМАНИЕ!