

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

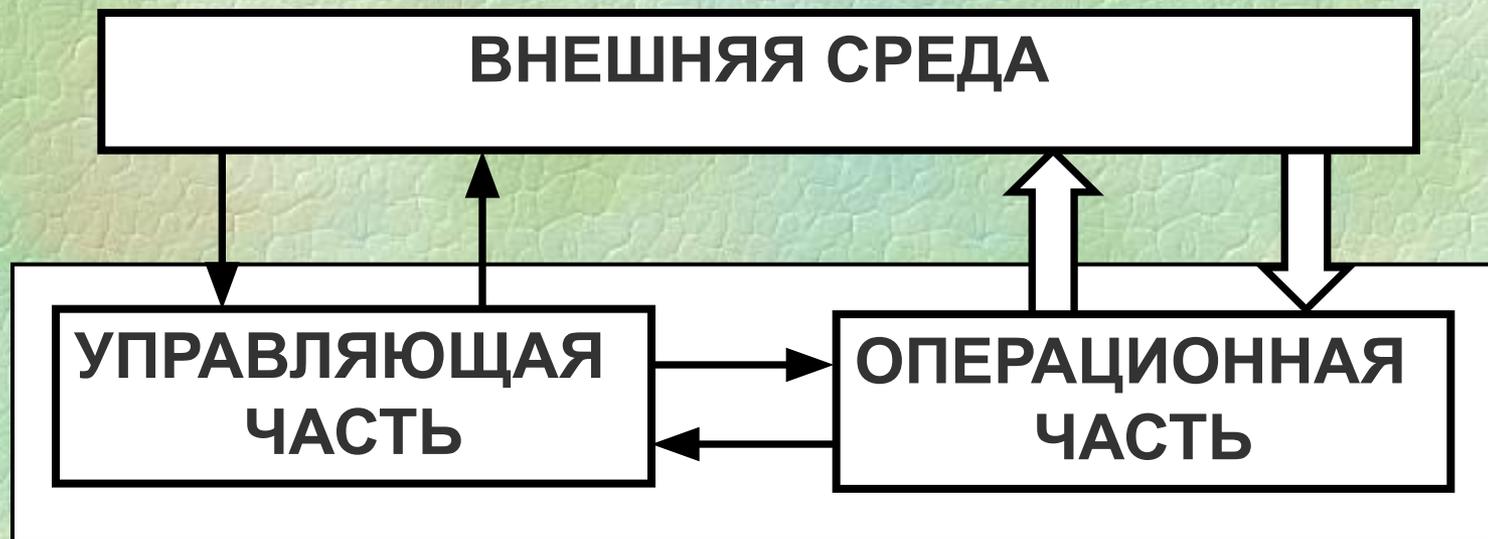
Под **реактивными системами** понимаются системы, постоянно взаимодействующие со своим окружением.

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

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

t – ПЕРЕМЕННАЯ, СО ЗНАЧЕНИЯМИ ИЗ Z

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

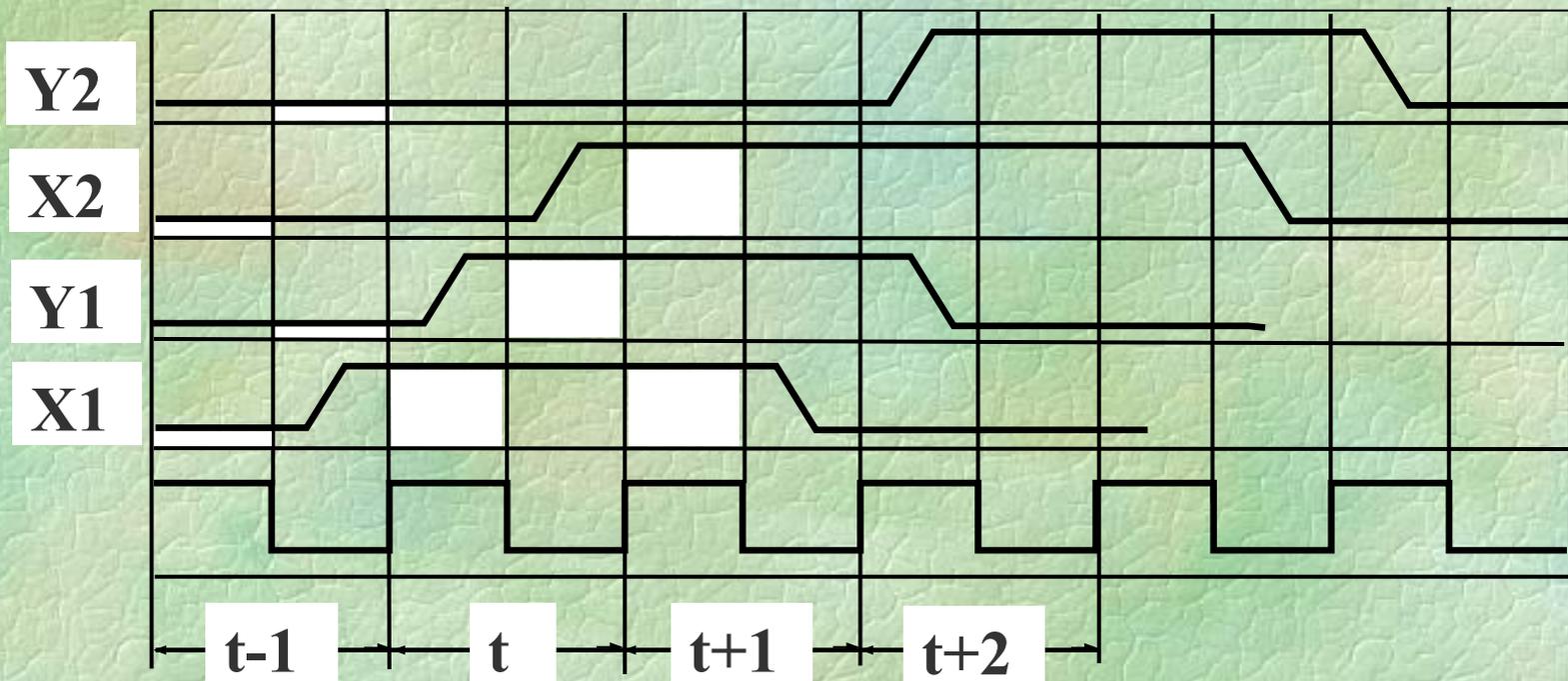
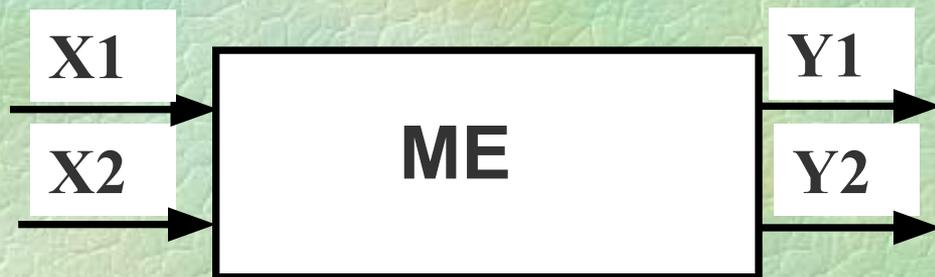
ЯЗЫК L

$F(t)$ – 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)}

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

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

$F = \forall t F(t)$

ЯЗЫК L^*

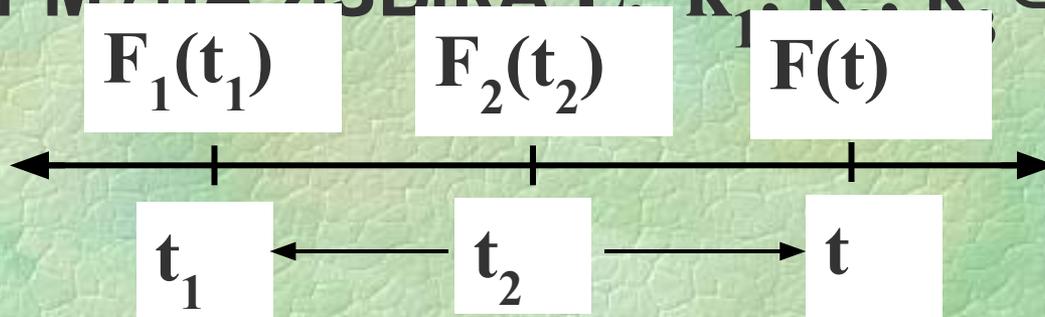
ДОБАВЛЯЕТСЯ КОНСТРУКЦИЯ

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

$F_2(t_2),$

$F_1(t_1)$ – ФОРМУЛА ЯЗЫКА L^* ,

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



СВЕРХСЛОВА

АЛФАВИТ $\Sigma = \{ \langle 00\dots 0 \rangle, \dots, \langle 11\dots 1 \rangle \}$

Σ^* – МНОЖЕСТВО ВСЕХ СЛОВ В АЛФАВИТЕ Σ

ПУСТЬ $\sigma_i \in \Sigma$ ($i \in \mathbb{Z}$)

$\dots\sigma_{-2}\sigma_{-1}\sigma_0\sigma_1\sigma_2\dots$ – ДВУСТОРОННЕЕ

СВЕРХСЛОВО ($\Sigma^{\mathbb{Z}}$)

$\sigma_1\sigma_2\dots$ – СВЕРХСЛОВО (Σ^{ω})

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

СВЕРХСЛОВА

ПУСТЬ $k \in \mathbb{Z}$ И $u \in \Sigma^{\mathbb{Z}}$

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

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

АВТОМАТЫ

$(X-Y)$ – АВТОМАТ $A = \langle X, Y, Q, \chi_A \rangle$, ГДЕ
 $\chi_A: Q \times X \times Y \rightarrow Q$ – ФУНКЦИЯ ПЕРЕХОДОВ,

$$\Sigma = X \times Y$$

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

СВЕРХСЛОВА И АВТОМАТЫ.

$l = \sigma_1 \sigma_2 \dots$ *ДОПУСТИМО* В СОСТОЯНИИ q

АВТОМАТА A , ЕСЛИ СУЩЕСТВУЕТ ТАКОЕ

СВЕРХСЛОВО $q_0 q_1 q_2 \dots$, ГДЕ $q_0 = q$, ЧТО ДЛЯ

ЛЮБОГО $i = 0, 1, 2, \dots$ $\delta_A(q_i, \sigma_{i+1}) = q_{i+1}$.

АВТОМАТЫ

ПУСТЬ $Q = \{q_1, \dots, q_n\}$ –

МНОЖЕСТВО СОСТОЯНИЙ АВТОМАТА A .

СЕМЕЙСТВО МНОЖЕСТВ (S_1, \dots, S_n) , ГДЕ S_i –

МНОЖЕСТВО ВСЕХ СВЕРХСЛОВ,

ДОПУСТИМЫХ В СОСТОЯНИИ q_i ($i = 1, 2, \dots, n$),

НАЗЫВАЕТСЯ **ПОВЕДЕНИЕМ** АВТОМАТА A .

ФОРМУЛЫ И АВТОМАТЫ

ИНТЕРПРЕТАЦИЯ ЯЗЫКА

ПУСТЬ $\Omega = \{p_1, \dots, p_k\}$

$p_1 \dots 0110100 \dots$

· ·

· ·

$p_k \dots 1001110 \dots$

$\Sigma = \{ \langle 00 \dots 0 \rangle, \dots, \langle 11 \dots 1 \rangle \}$

M_F – МНОЖЕСТВО ВСЕХ МОДЕЛЕЙ ДЛЯ F,

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

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

$\mathfrak{R}_F = \{ S_u \mid u \in M_F \} = \{ S_1, \dots, S_n \}$

ФОРМУЛЫ И АВТОМАТЫ

ФОРМУЛА $F = \forall t F(t)$ СПЕЦИФИЦИРУЕТ
АВТОМАТ A , ПОВЕДЕНИЕ КОТОРОГО
СОВПАДАЕТ С $\mathcal{R}_F = \{S_1, \dots, S_n\}$.

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!