

# Декомпозиция линейных автоматов над кольцом вычетов в сдвиговые регистры \*

Арнольд Шойинг (Arnold Scheuing)

*Институт информатики и прикладной математики, Бернский университет, CH-3012 Берн, Швейцария*

## Аннотация

Линейный автомат  $\mathfrak{A}$  над факторкольцом  $\mathbb{Z}_n$ ,  $n \in \mathbb{N}$ , в общем случае неразложим на параллельно соединённые сдвиговые регистры. Мы смогли сформулировать необходимые и достаточные условия для такого разложения, используя теорию об артиновых локальных кольцах  $R$  и  $R[x]$ -модульной структуре  $\mathfrak{A}$ .

## 1 Введение

Структура конечного, детерминированного линейного автомата (далее КА) интересна не только с точки зрения информатики, но и с точки зрения теории систем. Сфера применений КА, называемых также линейными последовательными схемами (LCS) включает в себя обнаружение и исправление ошибок, генераторы случайных чисел, криптологию (мотивация автора), а также конечномерные линейные системы с постоянными коэффициентами и дискретным или непрерывным временем. До тех пор пока коэффициенты такого автомата или системы являются элементами поля  $F$ , структура хорошо известна и тщательно изучалась последние двадцать лет [4] с помощью линейной алгебры: пространство состояний  $E$  автомата  $\mathfrak{A}$  — это конечномерное векторное пространство  $E$  над  $F$ , а функция перехода может быть рассмотрена как эндоморфизм в  $E$  или как матрица  $A$  над  $F$ , если базис в  $E$  зафиксирован.

Для нахождения более "простого" эквивалентного  $\mathfrak{A}$  КА можно использовать взаимнооднозначное соответствие между КА, эквивалентными  $\mathfrak{A}$ , и матрицами, подобными  $A$ . Есть существенные причины для выбора рациональной канонической формы  $A$  как наиболее "простой" потому что она соответствует разложению  $A$  на параллельные сдвиговые регистры.

На рисунке 1 мы показываем три представления КА относительно данного базиса  $B$  в  $E$ . Рисунок 1(а) соответствует сдвиговому регистру (его технической реализации) с 3-мерным пространством состояний, каждое из которых обладает компонентами  $(s_1, s_2, s_3)$ . В теории систем  $s_i$  и  $a_i$  называются, соответственно, элементами задержки и умножения. Каждый такт элемент из  $s_3$  переходит в  $s_2$ , из  $s_2$  — в  $s_1$  и сумма  $a_0s_1 + a_1s_2 + a_2s_3$  (в поле  $F$ ) попадает в  $s_3$ . На рисунке 1(б) изображено представление линейной функции  $f$  в форме матрицы  $3 \times 3$ . Эта специальная форма называется сопровождающей матрицей. Если полином  $x^3 - a_2x^2 - a_1x - a_0$  является несократимым в  $F[x]$ , тогда КА нельзя разложить. Рисунок 1(в) указывает  $F[x]$ -модуль ранга 3, например, базис  $B$  имеет три элемента:  $e$ ,  $f(e)$ ,  $f^2(e)$ , и

$$f^3(e) = a_0e + a_1f(e) + a_2f^2(e).$$

---

\*Результаты приведённые в данной работе являются частью докторской диссертации автора, которой руководил профессор Урс Вюрглер (Urs Würgler) из Бернского университета.

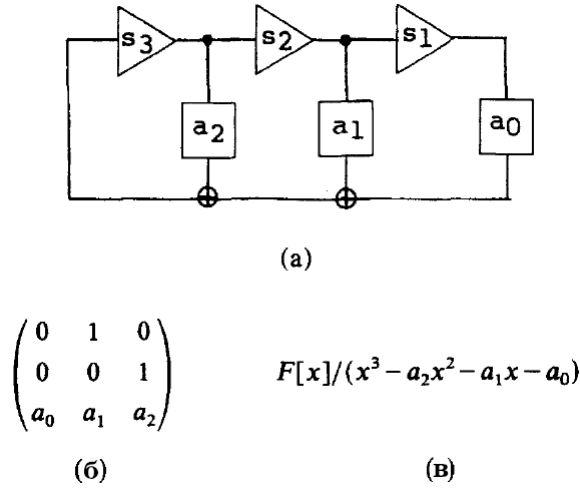


Рис. 1: Соответствующие представления ( $a_0, a_1, a_2 \in F$ ). (а) Сдвиговый регистр. (б) Сопровождающая матрица. (в) Циклический  $F[x]$ -модуль ранга 3.

Взаимооднозначное соответствие между этими структурами используется на всём протяжении данной работы: диаграммы КА и сдвиговые регистры для визуализации технической реализации, матрицы для расчётов в примерах, а модули для развития теории.

Известно, что КА с коэффициентами над полем может быть всегда реализован с помощью параллельного соединения сдвиговых регистров [9]. Но в применениях, указанных выше, нас также интересуют системы над кольцами  $\mathbb{Z} \bmod 2^r$  ( $r \in \mathbb{N}$ ). Например, в криптологии процесс автоматизированного шифрования и расшифрования связан с диапазоном значений  $2^r$  регистра с  $r$  бинарными разрядами.

Хорошее исследование расширения теории линейных систем от полей до колец за последние десять лет можно найти в работе [12]. Принцип двойственности для линейных систем над факторкольцами рассматривалась в работах [2, 8]. Представление матричных дробей для линейных систем над коммутативными кольцами также было изучено в работе [5].

В разделе 5 мы приводим пример КА над  $\mathbb{Z}_4$ , который и не является, и не разложим на сдвиговые регистры. Следовательно, возникает вопрос, при каких условиях КА над  $\mathbb{Z}_n$  может быть реализован как параллельное соединение сдвиговых регистров. Похожая проблема изучалась в работах [6, 7], путём использования биекции  $\beta : \mathbb{Z}_{p^r} \approx \prod_1^r \mathbb{Z}_p$  для декомпозиции КА  $\mathfrak{A}$  над  $\mathbb{Z}_{p^r}$  в каскад из  $r$  автоматов  $\mathfrak{A}_i$  над  $\mathbb{Z}_p$ . Но поскольку  $\beta$  не является гомоморфизмом колец,  $\mathfrak{A}_i$  соединены с помощью нелинейной логики без задержек, которая ограничивает дальнейший анализ посредством коммутативной алгебры.

Данная работа состоит из следующих разделов: в разделе 2 мы покажем, что  $\mathbb{Z}_n$ -свободные  $\mathbb{Z}_n[x]$ -модули являются подходящими математическими объектами для изучения структуры КА над полем  $\mathbb{Z}_n$  (рисунок 1). В разделе 3 мы докажем что проблема может быть сведена к КА над  $\mathbb{Z}_p$  без потери общности; с другой стороны, рекурсивный критерий в последнем разделе предлагает не ограничивать наше внимание на конечных и локальных кольцах  $\mathbb{Z}_{p^r}$ , а рассматривать более общие (коммутативные) артиновы локальные кольца  $R$  (с 1). Следовательно, в разделе 3 мы соберём все необходимые утверждения относительно артиновых локальных колец и модулей над ними. В разделе 4 мы покажем, что наш  $R[x]$ -модуль всегда имеет **примарное (primary)** разложение. Основные результаты находятся в разделах 5 и 6, где мы приводим необходимые и

достаточные условия для циклического разложения пространства состояний; другими словами, условия для того, чтобы КА был эквивалентен прямой сумме сдвиговых регистров. Общий случай мы рассматриваем в разделе 5, а специальный с кольцом главных идеалов — в разделе 6.

## 2 Модульная структура конечного автомата

Начнём с более точного описания конечного автомата (КА).

**Определение 2.1** Конечный детерминированный линейный автомат (без входных или выходных функций) над кольцом  $R$  — это пара  $(E, f)$ , где пространство состояний  $E$  является свободным  $R$ -модулем конечной размерности (скажем  $n$ ), а функция перехода  $f$  — это линейное отображение из  $E$  в  $E$ . Каждое  $e \in E$  является состоянием КА, функция перехода отображает состояние  $e$  в новое  $f(e)$ . Мы можем использовать простую нотацию без начального состояния, потому что нас интересует структура КА в целом.

Множество функций переходов над  $E$  — это кольцо эндоморфизмов  $\text{End}_R(E) = \{f : E \rightarrow E \mid f \text{ линейна}\}$ .  $\text{End}_R(E)$  также является  $R$ -модулем. Этот факт может быть выражен с помощью гомоморфизма колец на следующей коммутативной диаграмме.

$$\begin{array}{ccc} R & \xrightarrow{\psi} & \text{End}_R(E) \\ \downarrow & \searrow \hat{\psi} & \\ R[x] & & \end{array}$$

Для  $r \in R$ ,  $\psi(r)$  — это скалярное произведение для  $r$  из  $E$ . Так как  $f$  линейна над  $E$ , мы можем расширить  $\psi$  на  $R[x]$  как гомоморфизм колец с помощью задания  $\hat{\psi}(x) := f$ . Теперь  $E$  становится  $R[x]$ -модулем.

Путём параллельного соединения различных КА над одним и тем же кольцом мы можем построить более крупный автомат. Но ещё больший интерес представляет возможность разложения данного (сложного) автомата на мельчайшие, несократимые части — сдвиговые регистры.

**Определение 2.2** КА  $(E, f)$  над кольцом  $R$  называется *сдвиговым регистром*, если  $E$  циклическое, как  $R[x]$ -модуль. Другими словами, если существует такое начальное состояние  $e \in E$ , что его орбита:

$$e, f(e), f^2(e), \dots, f^{n-1}(e)$$

охватывает  $E$ .

Под «параллельным соединением КА  $(E_i, f_i)$ » мы подразумеваем техническую реализацию (см. рисунок 2(б)), но оно попросту означает прямую сумму КА  $(\bigoplus E_i, \bigoplus f_i)$ . Высказывание «КА реализован как параллельное соединение сдвиговых регистров» является интуитивным способом выразить то, что  $E$  — это прямая сумма  $R[x]$ -циклических  $R$ -свободных подмодулей.

Для формулировки первой теоремы необходима следующая нотация:

- $M_n(R)$  — множество всех  $n \times n$ -матриц над  $R$ ,
- $GL_n(R)$  — подмножество всех регулярных матриц из  $M_n(R)$ ,

- $M_n(R)/GL_n(R)$  — множество всех классов подобия матриц ( $A \in M_n(R)$  подобна  $T^{-1}AT$  для всех  $T \in GL_n(R)$ ),
- $Mod_n(Rp[x])$  — класс всех  $R$ -свободных  $R[x]$ -модулей  $E$  ранга  $n$  (т.е.  $\dim_R(E) = n$ ),
- $Iso(Mod_n(R[x]))$  — множество классов изоморфизма таких модулей.

**Теорема 2.3** *Существует биекция:*

$$\chi : M_n(R)/GL_n(R) \rightarrow Iso(Mod_n(R[x]))$$

**Доказательство.** **Определение  $\chi$ :** Пусть  $[A] \in M_n(R)/GL_n(R)$  и  $A \in M_n(R)$  — представители (Definition of  $\chi$ : Let ... be a representant.). Далее, пусть  $E$  — свободный  $R$ -модуль ранга  $n$ . Выберем базис в  $E$  и определим  $x \cdot e := A \cdot e$  ( $\forall e \in E$ ). Таким образом  $E$  становится  $R[x]$ -модулем  $E_A$ . Определим  $\chi[A] := [E_A]$  — класс изоморфизма  $E_A$ .  $\chi$  определено корректно, потому что для подобных матриц  $A \sim A'$ , модули изоморфны:  $E_A \cong E_{A'}$ , следовательно,  $[E_A] = [E_{A'}]$ .

Определение  $\chi'$ : Пусть  $[F] \in Iso(Mod_n(R[x]))$  и  $F \in Mod_n(R[x])$  — представители (Definition of  $\chi$ : Let ... be a representant.). Выберем  $R$ -базис в  $F$ , тогда (линейное) преобразование  $x$  может быть выражено с помощью матрицы  $A$ . Если мы зададим  $\chi'[F] := [A]$ , то оно также корректно определено и очевидно является обратной функцией к  $\chi$ .  $\square$

### 3 Артиновы локальные кольца и конечнопорождённые модули

В первой части этого раздела мы применим китайскую теорему об остатках для упрощения задачи с КА над  $\mathbb{Z}_n$  до КА над  $\mathbb{Z}_{p^r}$  ( $p$  — простое,  $r \in \mathbb{N}$ ). Мы помним, что кольцо  $\mathbb{Z}_n$  изоморфно произведению колец  $\prod_{i=1}^m \mathbb{Z}_{p_i^{r_i}}$ , так как  $n$  единственным образом разлагается на простые множители  $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$ . Из этого изоморфизма вытекает следующая теорема.

**Теорема 3.1** Пусть  $R_1, R_2, \dots, R_m$  — (коммутативные) кольца (с единицей),  $R := \prod_{i=1}^m R_i$ ,  $E$  —  $R$ -модуль и определим  $E_i := E \otimes R_i$ . Тогда кольцо  $End_R(E)$  изоморфно  $\bigoplus_{i=1}^m End_{R_i}(E_i)$ .

**Доказательство.** Пусть  $f_i := f \otimes 1_{E_i} \in End_{R_i}(E_i)$ . Мы можем определить гомоморфизм колец  $\phi : End_R(E) \rightarrow \bigoplus_{i=1}^m End_{R_i}(E_i)$  как  $\phi(f) := (f_1, f_2, \dots, f_m)$ .

Если  $\phi$  — мономорфизм: для  $f \in \ker(\phi) \Rightarrow f_i = f \otimes 1_{E_i} = 0 (\forall i) \Rightarrow f(E) \cong \prod_i (f(E) \otimes R_i) = 0 \Rightarrow f =$  **(ОПЕЧАТКА: в оригинальной статье формула обрывается).**

Если  $\phi$  — эпиморфизм: мы выбираем произвольное  $f_i \in End_{R_i}(E_i)$ . Принимая во внимание диаграмму:

$$\begin{array}{ccc} E & \xrightarrow{\prod_i f_i (1_E \otimes \pi_i)} & \prod_i E_i = \prod_i (E \otimes R_i) \cong E \otimes \prod_i R_i \cong E, \\ \downarrow 1_E \otimes \pi_i & & \downarrow \pi_i \\ E_i & \xrightarrow{f_i} & E_i \end{array}$$

получаем, что  $\phi(\prod_i f_i (1_E \otimes \pi_i)) = (f_1, f_2, \dots, f_m)$ .  $\square$

**Следствие 3.2** КА над  $\mathbb{Z}_n$  может быть всегда реализован с помощью параллельного соединения КА над  $\mathbb{Z}_{p^r}$ .

**Пример 3.3** КА над  $\mathbb{Z}_6$ , изображенный на рисунке 2(a), изоморфен автомату на рисунке 2(b). Соответствующий модуль выглядит следующим образом:

$$E \cong \mathbb{Z}_6[x]/(x^3 - 2x^2 - 3x - 4) \cong \mathbb{Z}_2[x]/(x^3 + x) \oplus \mathbb{Z}_3[x]/(x^3 + x^2 - 1).$$

Во второй части данного раздела мы хотим собрать воедино необходимые факты об артиновых локальных кольцах и о модулях над ними.

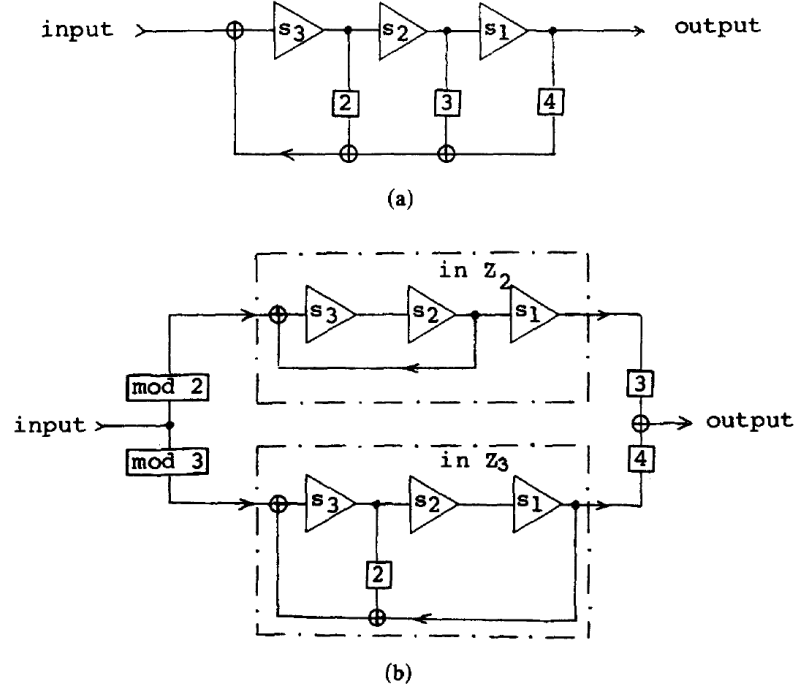


Рис. 2: Эквивалентные КА над  $\mathbb{Z}_6$  (со входом и выходом)

**Определение 3.4** Кольцо  $R$  является артиновым, если оно нётерово и имеет размерность 0 (любой простой идеал максимален, см. [1]).

Кольцо  $R$  является локальным, если оно нётерово и имеет ровно один максимальный идеал  $M$ . Нотация:  $(R, M)$ .

**Пример 3.5**  $(\mathbb{Z}_{p^r}, (p))$  и  $(\mathbb{Z}_{p^r}[x]/(x^S), (p, x))$  — это артиновы локальные кольца.

**Лемма 3.6** Артиновы локальные кольца  $(R, M)$ , обладают следующими свойствами:

- (a)  $M$  является единственным простым идеалом;
- (б) нильрадикал  $Rad(R)$  совпадает с  $M$  и сам является нильпотентным; наименьшее  $z \in \mathbb{N}$ , при котором  $M^z = (0)$ , называется нильпотентностью  $M$ ;
- (в) каждый элемент  $R$  либо обратим, либо нильпотентен.

Снэппер (Snapper) [11] называет такие кольца «совершенно простыми кольцами».

Учитывая важность канонического отображения  $\pi : R \rightarrow R/\text{Rad}(R)$ , мы будем использовать следующую нотацию на всём протяжении работы:  $\bar{R} = R/\text{Rad}(R)$ , **поле остатков (residue field)**,  $\bar{r} = \pi(r)(\forall r \in R)$ ,  $\bar{M}[x] = \pi(M[x]) = 0$ .

**Примечание 3.7** В данной работе мы будем рассматривать только конечнопорождённые модули, не повторяя этот факт каждый раз.

Причина, по которой мы не можем следовать такому же разложению, как для автомата над полем  $F$  (т.е. как модули над областью главных идеалов  $F[x]$ ), состоит в том, что подмодуль свободного модуля не обязательно является свободным. Но у нас есть следующая фундаментальная теорема.

**Теорема 3.8** (а) В локальном кольце  $(S, M)$  все конечнопорождённые модули свободны.

(б) Пусть  $(S, M)$  — артиново локальное кольцо,  $F \subset E$  — оба конечнопорождённые свободные  $S$ -модули. Тогда  $E \cong F \oplus E/F$ .

(в) Пусть  $(S, M)$  артиново локальное кольцо,  $F, G \subset E$  — три конечнопорождённых свободных  $S$ -модуля. Тогда  $F \cap G$  и  $F + G$  являются свободными.

**Доказательство.** (а) См. [10].

(б) Пусть  $\{e_1, \dots, e_n\}$  и  $\{f_1, \dots, f_m\}$  — базисы в  $E$  и  $F$ , соответственно. Поскольку  $F \cap E \Rightarrow f_1 = \sum \phi_i e_i$  и поскольку  $\{f_1, \dots, f_m\}$  линейно независимы, как минимум один из  $\phi_i$  должен быть обратим (см. лемму 3.6). Без потери общности, обратимый  $\phi_i$  подразумевает  $e_1 = (\phi_1^{-1})(f_1 - \sum_{i < 1} \phi_i e_i)$ . Поэтому  $\{f_1, e_2, \dots, e_n\}$  — это базис в  $E$ . По индукции получаем, что  $\{f_1, f_2, \dots, f_m, e_{m+1}, \dots, e_n\}$  является базисом в  $E$ , следовательно,  $E \cong F \oplus L_R(e_{m+1}, \dots, e_n)$ .

(в)  $G \rightarrow F \oplus E/F$  и оба слагаемых свободные (см. часть (б)). Пусть  $\{g_1, \dots, g_p\}$  — базис в  $G$ , а  $\{f_1, f_2, \dots, f_m, e_{m+1}, \dots, e_n\}$  — базис в  $E = F \oplus E/F$ . Поскольку  $g_i \in E$ , мы можем заключить аналогично части (б), что  $\{g_1, \dots, g_p, f_{q+1}, \dots, f_m, g_{q+1}, \dots, g_p, e_{n-m-p+q}, \dots, e_n\}$  является базисом в  $E$ . Следовательно,  $F \cap G = L_S(g_1, \dots, g_q)$  и  $F + G = L_S(g_1, \dots, g_p, f_{q+1}, \dots, f_m)$  свободны.  $\square$

Напомним, что для несократимого полинома  $\alpha \in R[x]$ , **отображение (projection)**  $\bar{\alpha} \in \bar{R}[x]$  не обязательно будет несократимым. Если оно является таковым, то мы называем  $\alpha$  фундаментально несократимым.

**Лемма 3.9** Вот некоторые важные типы идеалов в  $R[x]$  для артинова локального  $(R, M)$ :

(а)  $M[x] := \{\sum_i r_i x^i \in R[x] | r_i \in M\} \subset R[x]$  является единственным **нулевым (nil)** простым идеалом в  $R[x]$ ;

(б) Все ненулевые простые идеалы имеют вид  $M[x] + (\alpha)$ , где  $\alpha \in R[x]$  приведённый и фундаментально несократимый. Поскольку  $\bar{R}$  поле, эти идеалы также являются максимальными;

(в) Ненулевой идеал в  $R[x]$  представим в виде  $N + (\beta)$ , где  $\beta$  — приведённый многочлен и  $N \subset M[x]$ . Порождающие  $N$  могут быть всегда выбраны так, что их степень будет меньше, чем  $\beta$ .

Доказательство очевидно; подробности можно найти в работе [11].

## 4 Примарное (primary) разложение

Для начала подготовим факты и определения, связанные с идеалами. Пусть  $J$  — идеал в кольце  $S$ . Радикал в  $J$  — это  $\text{Rad}(J) = \{s \in S \mid \exists n \in \mathbb{N} : s^n \in J\}$ . Напомним, что  $\text{Rad}(R) := \text{Rad}(0)$ .  $J$  называется **примарным (primary)**, если для  $st \in J, t \notin J \Rightarrow s \in \text{Rad}(J)$ .

Пусть  $E$  — это  $S$ -модуль, тогда аннигиляторный идеал в  $E$  определяется как  $\text{Ann}_S(E) := \{s \in S \mid se = 0 (\forall e \in E)\}$ .

**Определение 4.1**  $S$ -модуль называется **примарным (primary)**, если  $(0)$  — это **примарный (primary)** подмодуль  $E$ . То есть  $se = 0$  (при  $s \in S, 0 \neq e \in E$ ) означает, что  $s \in \text{Rad}(\text{Ann}_S(E))$ . (Если элемент  $s$  уничтожает один элемент из  $E$ , то **потентность (potency)**  $s$  уничтожает всё в  $E$ .) Идеалы  $J$  и  $I$  в  $S$  называются **взаимно простыми (coprime)**, если  $I + J = S$ .

**Лемма 4.2** Пусть  $(R, M)$  — артиново локальное кольцо и  $I, J$  — **примарные (primary)** идеалы в  $R[x]$ . Тогда:

(а)  $J, I$  взаимно простые  $\Leftrightarrow \text{Rad}(J), \text{Rad}(I)$  взаимно простые;

(б) Пусть  $J$  и  $I$  **ненулевые (nonnil)**:  $\text{Rad}(J) = \text{Rad}(I) \Rightarrow J$  и  $I$  взаимно простые.

**Доказательство** (а) ( $\Leftarrow$ ): Очевидно, так как  $\text{Rad}(J) \subset J$  и  $\text{Rad}(I) \subset I$ .

( $\Rightarrow$ ): Выберем  $p \in \text{Rad}(J), q \in \text{Rad}(I)$  такими, что  $p + q = 1$ . Теперь существуют такие  $n, m \in \mathbb{N}$ , для которых выполняется  $p^m \in J$  и  $q^n \in I$ , что:

$$1 = 1^{m+n-1} = (p + q)^{m+n-1} = \sum_{k=1}^{m+n-1} \binom{m+n-1}{k} p^k \cdot q^{m+n-k-1} = p^m(\dots) + q^n(\dots) \in J + I,$$

что подразумевает  $1 \in I + J$ .

(б) Из леммы 3.9 мы знаем что  $\text{Rad}(J) = M[x] + (\alpha), \text{Rad}(I) = M[x] + (\beta)$ , где подходящие  $\alpha, \beta \in R[x]$  нормированы, а  $\overline{\alpha}, \overline{\beta} \in \overline{R}[x]$  взаимно просты. Следовательно,  $1 \in (\overline{\alpha}) + (\overline{\beta})$ , и  $1 + \nu \in (\alpha) + (\beta)$  для некоторого  $\nu \in M[x]$ . Таким образом,  $\text{Rad}(J)$  и  $\text{Rad}(I)$  взаимно простые и, учитывая часть (а),  $J$  и  $I$  взаимно простые.  $\square$

**Лемма 4.3** Пусть  $R$  — нётерово кольцо, и  $E$  —  $R$ -свободный  $R[x]$ -модуль.  $E$  является **примарным (primary)** тогда и только тогда, когда  $\text{Ann}_{R[x]}(E)$  является **примарным (primary)**.

**Доказательство** Пусть  $A := \text{Ann}_{R[x]}(E)$ .

( $\Rightarrow$ ): Допустим  $\alpha\beta \in A, \beta \notin A$ , подразумевая, что существует  $0 \neq e \in E$ , для которого  $\beta e \neq 0$ . Но  $(\alpha\beta)e = 0 = \alpha(\beta e)$  и  $E$  **примарный (primary)**, следовательно,  $\alpha \in \text{Rad}(A)$ .

( $\Leftarrow$ ) Пусть  $0 \neq e \in E, \alpha e = 0$ . Мы знаем, что

$$((\alpha) + A) \cdot ((\alpha) \cap A) \subset (\alpha) \cdot A \subset (\alpha) \cap A.$$

*Случай 1:*  $(\alpha) \cdot A = (\alpha) \cap A$ . Для нётеровых колец это означает, что  $(\alpha) + A = R[x]$ . Следовательно, существуют такие  $\beta \in R[x]$  и  $\gamma \in A$ , что  $\beta\alpha + \gamma = 1$ . Возникает противоречие:  $1 \cdot e = \beta(\alpha e) + \gamma e = \beta 0 + 0$ .

Случай 2:  $(\alpha) \cdot A \neq (\alpha) \cap A$ . Существует  $\beta \in (\alpha) \cap A, \beta \notin (\alpha) \cdot A$  такое, что  $\beta = \alpha\gamma \in A, \gamma \notin A$ , следовательно,  $\alpha \in \text{Rad}(A)$ .  $\square$

Нас интересуют артиновы локальные кольца, а они по определению являются нётеровыми, поэтому мы можем применить следующую важную теорему.

**Теорема 4.4** В нётеровом кольце  $R$  каждый идеал имеет примарное (primary) разложение на примарные (primary, лексический повтор в оригинале) идеалы  $Q_i$  (с точностью до порядка (unique up to order))

$$J = \bigcap_{i=1}^m Q_i, \quad Q_i \not\subset \bigcap_{j \neq i} Q_j \quad (i = 1, \dots, m)$$

и все  $\text{Rad}(Q_i)$  различны.

Если все  $Q_i$  попарно взаимно просты, тогда

$$J \cong \prod_{i=1}^m Q_i.$$

Доказательство первой части можно найти в работе [3]. Второй — в [13].

**Теорема 4.5** (Примарное (primary) разложение модулей). Пусть  $(R, M)$  — артиново локальное кольцо,  $E \in \text{Mod}_n(R[x])$ . Тогда существуют примарные (primary)  $L_i \in \text{Mod}_{n_i}(R[x]), L_i \subset E$ , и эндоморфизмы  $f_i = f|_{L_i}$  такие, что

$$E \cong \bigoplus_{i=1}^m L_i \quad \text{и} \quad \text{Ann}_{R[x]}(E) \cong \prod_{i=1}^m \text{Ann}_{R[x]}(L_i).$$

**Доказательство** Применяя теорему 4.4 мы получаем примарное (primary) разложение  $\text{Ann}_{R[x]}(E) = \bigcap_i Q_i$ , где все  $Q_i$  примарные (primary). Поскольку  $E$  имеет конечный ранг, все  $Q_i$  не нулевые (nonnil). Лемма 4.2 гарантирует, что все  $Q_i$  попарно взаимно просты, следовательно,  $\text{Ann}_{R[x]}(E) \cong \prod_i Q_i$ .

Пусть  $L_i := \prod_{j \neq i} Q_j \cdot E, K_i := \prod_{j=1}^i Q_j \cdot E$ . Мы хотим показать, что  $E = L_1 \oplus L_2 \oplus \dots \oplus L_i \oplus K_i$  для  $i = 0, \dots, m$  с помощью индукции. Естественно,  $L_0 = \text{Ann}(E)E = 0, K_0 = E$ , и  $K_m = 0$ . Покажем, что  $K_{i-1} = L_i \oplus K_i$ :

$$L_i + K_i = \left( \prod_{j \neq i} Q_j + \prod_{j=1}^i Q_j \right) E = \prod_{j=1}^{i-1} Q_j \left( Q_i + \prod_{j=i+1}^m Q_j \right) E = \prod_{j=i}^m (Q_i + Q_j) K_{i-1} = K_{i-1},$$

поскольку все  $Q_j$  взаимно простые. Аналогичным образом,  $L_i \cap K_i = \prod_{j=1}^m Q_j E = \text{Ann}(E)E = 0$ .

Каждый  $L_i$   $R$ -свободен, потому что он является  $R$ -проективным (R-projective) (как прямое слагаемое  $R$ -свободного модуля), следовательно,  $R$ -свободным по теореме 3.8. По лемме 4.3  $L_i$  является примарным (primary), так как  $\text{Ann}(L_i) = Q_i$ .  $\square$

**Пример 4.6** Пусть  $R = \mathbb{Z}_4, E = e_1 R \oplus e_2 R$ . КА на рисунке 3(а) соответствует матрице переходов  $A = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix}$ .



$A^2 + A = 0$  подразумевает  $\text{Ann}(E) = (x^2 + x)$  с **примарным(primary)** разложением  $(x)(x + 1)$ . Следовательно,

$$\begin{aligned} L_1 &= (x)E = (3e_1 + 3e_2)\mathbb{Z}_4, & f_1 &= f|_{L_1} = (3), \\ L_2 &= (x + 1)E = (e_2)\mathbb{Z}_4, & f_2 &= f|_{L_2} = (0). \end{aligned}$$

Относительно нового базиса  $\{3e_1 + 3e_2, e_2\}$  мы имеем матрицу переходов  $A = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$  и конечный автомат на рисунке 3(b).

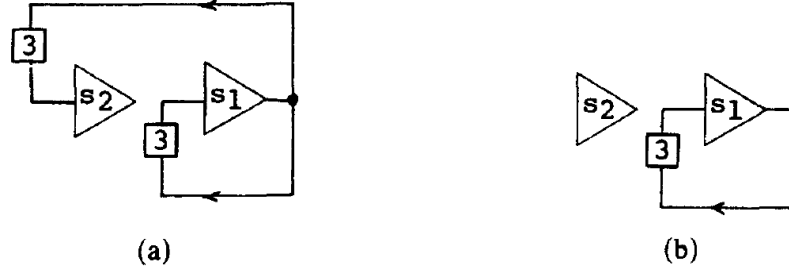


Рис. 3: Два эквивалентных КА: упрощение путём **примарного (primary)** разложения

## 5 Циклическое разложение

В силу теоремы 4.5 мы можем предположить без потери общности, что начнём с локального артинова кольца  $(R, M)$  и **примарного(primary)**  $E \in \text{Mod}_n(R[x])$ . В общем случае разложение  $E$  на циклические  $R[x]$ -модули не представляется возможным. Приведём следующий пример.

**Пример 5.1** Пусть  $R = \mathbb{Z}_4$ ,  $E = e_1R \oplus e_2R$ . Два КА на рисунке 4 эквивалентны. Они соответствуют матрицам  $A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$ ,  $A' = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ .

Перебирая все преобразования  $GL_2(\mathbb{Z}_4)$ , мы можем убедиться в том, что  $\{A, A'\}$  — это **класс подобия (similarity-class)**  $A$ . И ни  $A$ , ни  $A'$  не являются **представлениями (representations)** циклических модулей.



Рис. 4: Контрпример: КА над  $\mathbb{Z}_4$ , который неразложим на сдвиговые регистры

Поэтому мы определяем более слабое условие, чем прямая сумма. Пусть  $L_i$  — это  $R[x]$ -подмодули  $E$  ( $i = 1, \dots, k$ ) такие, что  $\sum_{i=1}^k L_i = E$ .

**Определение 5.2** Сумма  $E = \sum_{i=1}^k L_i$  называется прямой суммой по модулю  $M$ , если  $\bar{E} \cong \bigoplus_{i=1}^k \bar{L}_i$ , и обозначается как  $_{M\sum_{i=1}^k L_i}$ .

Легко заметить, что  $E = _{M\sum_{i=1}^k L_i}$ , если  $(L_i + ME) \cap \sum_{j \neq i} L_j \subset ME$ . Напомним, что  $R[x]$ -модуль  $E$  называется циклическим, если  $E$  может быть порождён одним элементом; тогда мы имеем  $E \cong R[x]/Ann(E)$ .

**Лемма 5.3** Для указанных выше  $(R, M)$  и  $E$  существуют нормированные и неприводимые  $\alpha_i \in \bar{R}[x]$  и  $s_i \in \mathbb{N}$  ( $i = 1, \dots, k$ ) такие, что  $\bar{E} \cong \bigoplus_{i=1}^k L'_i$  и  $L'_i \cong \bar{R}[x]/(\alpha_i^{s_i})$ .

**Доказательство** Поскольку  $e$  является  $R[x]$ -модулем, мы можем применить структурную теорему для конечнопорождённых модулей над областью главных идеалов (principal ideal domain)  $\bar{R}[x] = R[x]/M[x] = (R/M)[x]$  (пример в работе [3]). Из того, что  $e$  примарный (primary), получается что  $\bar{E}$  и, следовательно, все подмодули  $L'_i$  тоже примарны (primary). Примарный (primary) идеал в  $\bar{R}[x]$  — это потенциальность (potency) простого идеала  $(\bar{\alpha}_i)^{s_i}$ .  $\square$

Эти  $\bar{R}[x]$ -подмодули  $L'_i \subset \bar{E}$  могут быть подняты до (can be lifted to)  $R[x]$ -подмодулей  $L_i$  следующим образом. Пусть  $e'_i \in L'_i$  порождает  $L'_i$ , а выбор  $e_i \in \pi^{-1}(e'_i) \subset E$  произволен: тогда  $L_i := R[x] \cdot e_i$  ( $i = 1, \dots, k$ ). Каждый  $L_i$  циклический по определению, но в общем случае не  $R$ -свободный. Поскольку  $\pi((L_i + ME) \cap \sum_{j \neq i} L_j) = L'_i \cap \sum_{j \neq i} L'_j = 0$  мы доказали следующую теорему.

**Теорема 5.4** Пусть  $(R, M)$  — артиново локальное кольцо, и  $E \in Mod_n(R[x])$  — примарный модуль (is primary). Тогда существуют циклические  $R[x]$ -модули  $L_i \subset E$  ( $i = 1, \dots, k$ ) такие, что  $E = _{M\sum_{i=1}^k L_i}$  (сумма по модулю  $M$ ).

**Теорема 5.5** Для  $(R, M)$  и  $E$  указанных выше:

$$\begin{aligned} E \cong \bigoplus_{i=1}^k L_i &\Leftrightarrow L_i \text{ является } R\text{-свободным } (i = 1, \dots, k) \\ &\Leftrightarrow Ann_R[x](L_i) \text{ является главным идеалом } (i = 1, \dots, k). \end{aligned}$$

**Доказательство** (а) ( $\Rightarrow$ ):  $E$  —  $R$ -свободный модуль, а  $L_i$  — прямое слагаемое  $E$ , следовательно,  $L_i$  является  $R$ -проективным (R-projective), и тогда можно использовать теорему 3.8.

( $\Leftarrow$ ): Из теоремы 3.8 мы можем заключить, что  $L_1 \cap \sum_{i>1} L_i$  является  $R$ -свободным, а из определения суммы по модулю  $M$ , мы знаем, что

$$(L_1 + ME) \cap \sum_{i>1} L_i \subset ME \Rightarrow L_1 \cap \sum_{i>1} L_i = 0.$$

Теперь продолжим для  $\sum_{i>1} L_i$  по индукции.

(б) Пусть  $i = 1, \dots, k$  произвольно,  $e$  порождающий в  $L_i$  и  $d := d_i$ , тогда  $B := e, xe, \dots, x^{d-1}e$  —  $R$ -базис в  $L_i$ .

( $\Rightarrow$ ):  $x^d e = \sum_{j=0}^{d-1} a_j(x^j e) \in L$  подразумевает (в оригинале implying — причастие), что  $\alpha := x^d - \sum_{j=0}^{d-1} a_j x^j \in Ann(L)$  и  $\alpha$  имеет степень  $d$ . Согласно лемме 3.9,  $Ann(L) = (\alpha) + N$  при  $N \subset M[x]$ . Если  $N \neq 0$ , тогда  $\exists 0 \neq \beta \in N, \deg(\beta) < d$  (лемма 3.9), но это приводит к противоречию с тем, что базис  $B$  линейно независим.

( $\Leftarrow$ ): Без потери общности,  $Ann(L_i)$  порождён элементом  $\alpha \in R[x]$  с ненулевым старшим коэффициентом. Очевидно, что  $\deg(\alpha) = d$ . Поскольку  $Ann(L_i)$  не содержит многочленов меньшей степени, в  $B$  не существует зависимостей между элементами, следовательно,  $B$  является базисом.  $\square$

**Пример 5.6** Пусть  $R = \mathbb{Z}_4$ ,  $E = \bigoplus_{i=1}^4 e_i \cdot \mathbb{Z}_4$ . Автомат на рисунке 5 соответствует матрице переходов

$$A = \begin{pmatrix} 0 & 1 & 0 & 2 \\ 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 0 & 1 & 0 \end{pmatrix}.$$

$$\text{Ann}(E) = ((x^2 - 1)(x^2 - 2x - 1), 4(x^2 - 1)).$$

Следуя выводу и нотации теоремы 5.4, мы получаем  $\bar{R}[x] = \mathbb{Z}_2[x]$ ,  $\bar{E} = \bigoplus_{i=1}^4 \bar{e}_i \mathbb{Z}_2$  и  $\text{Ann}_{\mathbb{Z}_2[x]}(\bar{E}) = (x^2 + 1)$ .  $L'_1 = L_{\mathbb{Z}_2}(\bar{e}_1, \bar{e}_2)$ , аналогично,  $L'_2 = L_{\mathbb{Z}_2}(\bar{e}_3, \bar{e}_4)$ . Теперь выберем  $\hat{e}_1 := e_1 + 2e_3$ ,  $\hat{e}_2 := 3e_3$  и найдём, что оба

$$L_1 = L_{\mathbb{Z}_8[x]}(\hat{e}_1) = L_{\mathbb{Z}_8}(\hat{e}_1, x\hat{e}_1, (4x + 4)\hat{e}_2),$$

$$L_2 = L_{\mathbb{Z}_8}(\hat{e}_2, x\hat{e}_2, (4x + 4)\hat{e}_1)$$

не являются  $\mathbb{Z}_8$ -свободными.

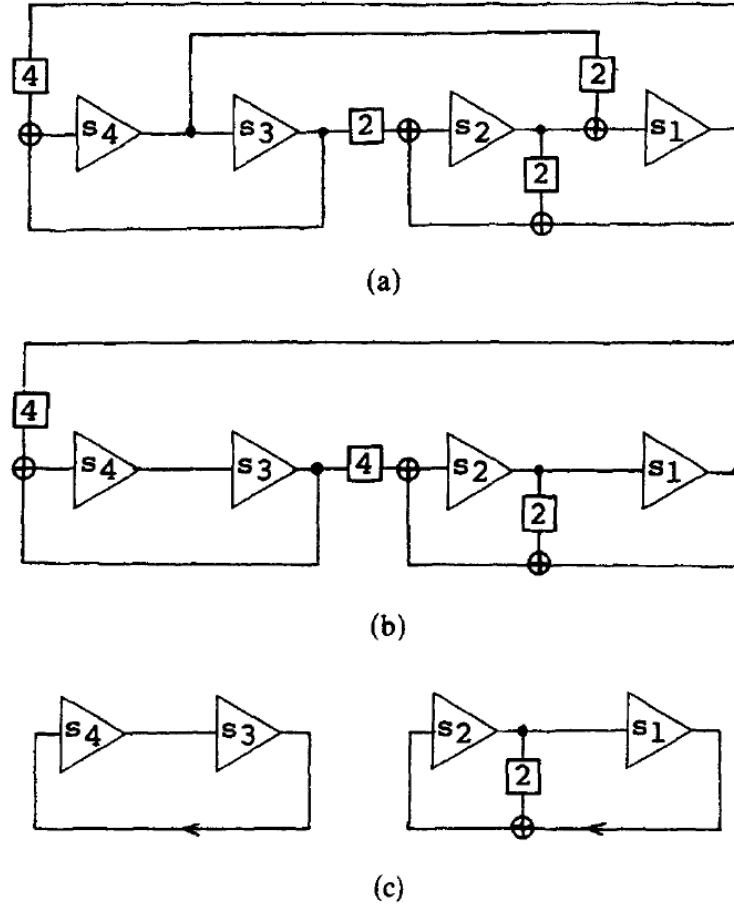


Рис. 5: Три эквивалентных КА: упрощение с помощью циклического разложения

## Список литературы

- [1] M.F. Atiyah and I.G. MacDonald, Introduction to Commutative Algebra (Addison-Wesley, Reading, MA, 1969).
- [2] W.S. Ching and B.F. Wyman, Duality and the regulation problem for linear systems over commutative rings, J. Comput. System Sci. 14 (1977) 360-368.
- [3] T. Hungerford, Algebra (Holt, Rinehart & Winston, New York, 1974).
- [4] R.E. Kalman, P.L. Falb and M.A. Arbib, Topics in Mathematical System Theory (McGraw-Hill, New York, 1969).
- [5] P. Khargonekar, On Matrix Fraction Representation for Linear Systems over Commutative Rings (Center of Math. System Theory, Univ. of Florida, 1980).
- [6] M. Magidin and A. Gill, Decomposition of linear sequential circuits over residue rings, J. Franklin Inst. 294 (1972) 167-180.
- [7] M. Magidin and A. Gill, Singular shift registers over residue class rings, Math. Systems Theory 9(4) (1976) 345-358.
- [8] G. Nandi and C. Nolte, Duality for systems over rings, Inform. Control 50. (1981) 128-132.
- [9] B. Reusch, Lineare Automaten (Bibliographisches Institut, Mannheim, 1969).
- [10] J.R. Silvester, Introduction to Algebraic K-theory (Chapman & Hall, London, 1981).
- [11] E. Snapper, Completely primary rings, Ann. of Math. 52 (1950) 666-693.
- [12] E.D. Sontag, Linear systems over commutative rings, Ricerche Automat. 7(1) (1976) 1-34.
- [13] B.L. van der Waerden, Algebra 2 (Springer, Berlin, 1967).