

Декомпозиция линейных автоматов над кольцом вычетов в сдвиговые регистры *

Арнольд Шойинг (Arnold Scheuing)

Институт информатики и прикладной математики, Бернский университет, СН-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 3×3 . 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.

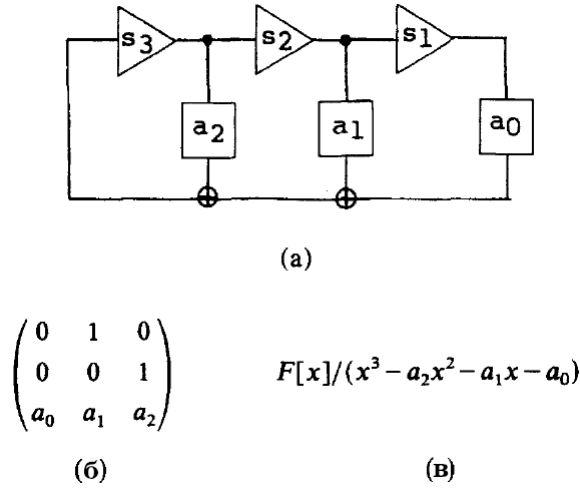


Рис. 1: Соответствующие представления ($a_0, a_1, a_2 \in F$). (а) Сдвиговый регистр. (б) Сопровождающая матрица. (в) Циклический $F[x]$ -модуль ранга 3.

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 β 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** 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 ψ 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 $T \in GL_n(R)$),
- $Mod_n(R[x])$ — 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 χ :** Пусть $[A] \in M_n(R)/GL_n(R)$ $A \in M_n(R)$ — **представители**. 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 . χ определено корректно, потому что для подобных матриц $A \sim A'$, модули изоморфны: $E_A \cong E_{A'}$, следовательно, $[E_A] = [E_{A'}]$.

Определение χ' : Пусть $[F] \in Iso(Mod_n(R[x]))$ $F \in Mod_n(R[x])$ — **представители**. 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 χ . \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 ϕ — мономорфизм: для $f \in \ker(\phi) \Rightarrow f_i = f \otimes 1_{E_i} = 0 (\forall i) \Rightarrow f(E) \cong \prod_i (f(E) \otimes R_i) = 0 \Rightarrow f = 0$ (**ОПЕЧАТКА: в оригинальной статье формула обрывается**).

Если ϕ — 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(а), изоморфен автомату на рисунке 2(б). 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.

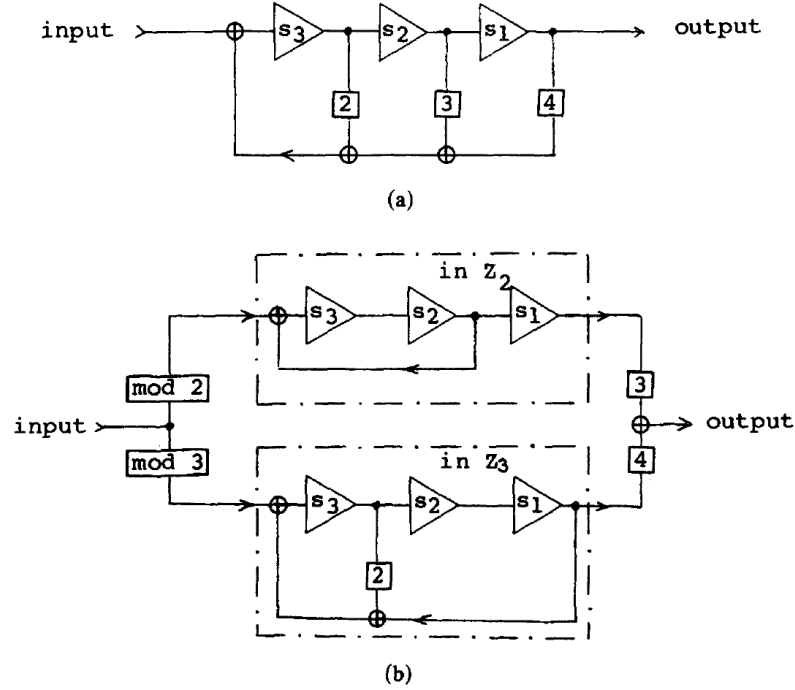


Рис. 2: Эквивалентные КА над \mathbb{Z}_6 (со входом и выходом)

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:

- (а) 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 $\pi : R \rightarrow R/Rad(R)$, мы будем использовать следующую нотацию на всём протяжении работы: $\overline{R} = R/Rad(R)$, **поле остатков**, $\bar{r} = \pi(r) (\forall r \in R)$, $\overline{M[x]} = \pi(M[x]) = 0$.

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 ϕ_i должен быть обратим (см. лемму 3.6). Без потери общности, обратимый ϕ_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, $F \cap G = L_S(g_1, \dots, g_p)$ и $F + G = L_S(g_1, \dots, g_p, f_{q+1}, \dots, f_m)$ оба свободны. \square

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

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).