О сложности А-выразимости элементарного базиса для А-замыкания в классах линейных автоматов над конечными полями.

И. Ю. Ильин[1]

В предыдущей работе нами был получены оценки сложности реализации элементарного базиса в классе одноместных линейных автоматов, сохраняющих нулевую последовательность. В данной работе мы получили верхнюю оценку сложности реализации элементарного базиса через операции А-замыкания в классе линейных автоматов над конечным полем [4].

Ключевые слова: линейные автоматы, А-замыкание, А-выразимость, временная сложность алгоритма.

Мы продолжаем исследовать сложность реализации функций в различных классах линейных автоматов. В предыдущей работе нами были получены оценки сложности реализации элементарного базиса в классе линейных автоматов, сохраняющих нулевую последовательность. В данной работе мы будем решать задачу сложности реализации элементарного базиса для А-замыкания в классе линейных автоматов над конечным полем E_k [4], предварительно получив результаты для поля E_2. Для упрощения приведем используемые нами обозначения, определения и теоремы, подробные доказательства которых читатель сможет найти в работах [1] [2] [5].

§1. Оценка сложности τ-приближения функций элементарного базиса в классе линейных автоматов над полем E_2.

Мы рассматриваем множество линейных автоматов L_2 над E_2 с операциями композиции:

1. Подстановки.
2. Переименования переменных.
3. Отождествления переменных.
4. Обратной связи.

[1] *Ильин Иван Юрьевич* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: vanyail@yandex.ru.

Ilin Ivan Yurievich— graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Обозначим $K(M)$ – замыкание множества M по операциям перечисленным операциям.

Введем множества T_a, $a \in E_2$ следующим образом:

$T_a = \{f | f \in L_2, f$ сохраняет a в начальный момент времени. $\}$ [1]

Переменная x_j функции $f(x_1, ..., x_n) = \sum_1^n \mu_i x_i + \mu_0, \mu_i \in E_2'(\xi)$ называется непосредственной, если $\mu_j(0) = 1$.

Введем ещё два множества:

$V_1 = \{f | f \in L_2, f$ имеет не более одной непосредственной переменной$\}$.

$V_2 = \{f | f \in L_2, f$ имеет нечетное число непосредственных переменных$\}$.

Обозначим $U(f) = \{\mu_i, i = 1, ..., n\}$.

Введем множество

$$M(\xi) = \{f | f \in L_2, \forall \mu \in U(f), \mu + \mu(0) = a_2\xi^2 + a_3\xi^3 + ...\}.$$

Множества $T_0, T_1, V_1, V_2, M(\xi)$ являются К-замкнутыми и предполными в L_2 [1].

Пусть $M \subseteq L_2, f \in L_2, \tau \in \mathbf{Z}_+$. Тогда функция $f = f(x_1, ..., x_n)$ является τ-выразимой через M, если существует функция $g(x_1, ...x_n) \in K(M)$ такая, что

$$\forall \alpha_i, \alpha_i = a_{0i}a_{2i}...a_{\tau i}, i = 1, 2, ..., n$$

$$f(\alpha_1, ..., \alpha_n) = g(\alpha_1, ..., \alpha_n).$$

Функция f называется A-выразимой через M, если $\forall \tau \in \mathbb{Z}_+$ функция f τ-выразима из M [5].

Пусть $M \subseteq L_2$ тогда A-замыканием M называется множество $A(M) = \{f | f \in L_2, f$ - A-выразима из $M\}$.

Множества $T_0, T_1, V_1, V_2, M(\xi)$ являются A-замкнутыми, далее будем обозначать $J_a = \{T_0, T_1, V_1, V_2, M(\xi)\}$.

Лемма 1. *Пусть множество $M \subseteq L_2$, M не содержится целиком ни в одном из множеств $\Theta \in J_a$. Пусть n - максимальная арность функций из M. Тогда мы можем получить константы γ_0, γ_1 такие, что $\gamma_0(0) = 0, \gamma_1(0) = 1$, используя $O(n)$ операций сложения и умножения, а также 1 операцию обратной связи.*

Доказательство. Так как M целиком не содержится в V_1, V_2, то существует функция $f(x_1, ..., x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0$ имеющая четное количество непосредственных переменных. Рассмотрим функцию

$$g(x) = f(x, x, ..., x) = \sum_{i=1}^n \mu_i x + \mu_0 = \mu x + \mu_0,$$

которую мы получаем за $O(n)$ операций сложения. В силу того, что у функции f четное количество непосредственных переменных, $\mu(0) = 0$, а значит к функции g применима обратная связь. $F_b(g(x)) = \gamma$ – константа.

Предположим, что $\gamma(0) = 0$, тогда $\gamma \in T_0$. В M выберем функцию h не принадлежащую T_0 и подставим в неё константу γ: $h(\gamma, \gamma, ..., \gamma) = \gamma_1$, для чего используем $O(n)$ операций сложения и умножения.

Схожим образом поступим, если $\gamma(0) = 1$, в этом случае $\gamma \in T_1$. В M выберем функцию h' не принадлежащую T_1 и подставим в неё константу γ: $h'(\gamma, \gamma, ..., \gamma) = \gamma_0$, для чего используем $O(n)$ операций сложения и умножения.

А значит, мы получаем две константы γ_0, γ_1 такие, что $\gamma_0(0) = 0$, $\gamma_1(0) = 1$. $\square$

Лемма 2. *Пусть множество $M \subseteq L_2$, M не содержится целиком ни в одном из множеств $\Theta \in J_a$, n - максимальная арность функций из M. Пусть также нами уже были получены две константы γ_0, γ_1 из леммы 1. Тогда мы можем получить функцию $\hat{f}(x_1, x_2, x_3)$, 2^s-эквивалентную $x_1 + x_2 + x_3$ за $O(s + n)$ операций.*

Доказательство. Существует функция $f'(x_1, ..., x_n)$, принадлежащая $M \setminus V_1$. Без ограничения общности, x_1, x_2 - непосредственные переменные. Подставим константу γ_0 вместо всех переменных, кроме x_1, x_2,

$$f'(x_1, x_2, \gamma_0 ..., \gamma_0) = \mu_1 x_1 + \mu_2 x_2 + \gamma'$$

за $O(n)$ операций сложения и умножения. Переменные x_1, x_2 - непосредственные, а значит $\mu_1(0) = \mu_2(0) = 1$. Получим функции

$$f_{\gamma_0, x_1}(x_1) = f'(\gamma_0, x_1, \gamma_0 ..., \gamma_0),$$

$$f_{x_2, \gamma_0}(x_2) = f'(x_2, \gamma_0, \gamma_0 ..., \gamma_0),$$

$$f''(x_1, x_2) = f'(f_{\gamma_0, x_1}(x_1), f_{x_2, \gamma_0}(x_2), \gamma_0 ..., \gamma_0),$$

$$f''(x_1, x_2) = \mu_1 \mu_2 x_1 + \mu_1 \mu_2 x_2 + \gamma''.$$

Для этого мы используем $O(n)$ операции сложения и умножения, $\mu = \mu_1 \mu_2$ в нулевой момент принимает значение $\mu(0) = \mu_1(0)\mu_2(0) = 1$. Следовательно, μ имеет вид $1 + \xi\hat{\mu}$, где $\hat{\mu} \in E'_2(\xi)$. Получим функцию

$$f_1(x_1, x_2) = f''(f''(x_1, x_2), \gamma_0) = \mu^2 x_1 + \mu^2 x_2 + \gamma^{(1)}$$

за $O(1)$ операций сложения и умножения.

Предположим, что мы уже получили функцию $f_{s-1}(x_1, x_2)$. Построим теперь функцию $f_s(x_1, x_2)$:

$$f_s(x_1, x_2) = f_{s-1}(f_{s-1}(x_1, x_2), \gamma_0) =$$

$$= \mu^{2^{s-1}} \mu^{2^{s-1}} x_1 + \mu^{2^{s-1}} \mu^{2^{s-1}} x_2 + \gamma^{(s-1)} \mu^{2^{s-1}} =$$

$$= \mu^{2^s} x_1 + \mu^{2^s} x_2 + \gamma^{(s-1)} \mu^{2^{s-1}}$$
$$= \mu^{2^s} x_1 + \mu^{2^s} x_2 + \gamma^{(s)}$$

На каждой итерации такого процесса мы будем использовать $O(1)$ операций сложения и умножения, значит, всего на построение $f_s(x_1, x_2)$ потребуется $O(s)$ операций сложения и умножения.

Подставим функцию f_s в себя следующим образом:

$$f_s(x_1, f_s(x_1, x_3)) = \mu^{2^s} x_1 + \mu^{2^{s+1}} x_2 + \mu^{2^{s+1}} x_3 + \gamma^{(s)} + \mu^{2^s} \gamma^{(s)} =$$

$$= (1 + \xi^{2^s} \bar{\mu}) x_1 + (1 + \xi^{2^s} \tilde{\mu}) x_2 + (1 + \xi^{2^s} \mu') x_3 + \xi^{2^s} \hat{\gamma},$$

используя $O(1)$ операций сложения и умножения. Отсюда видно, что эта функция 2^s-эквивалентна $x_1 + x_2 + x_3$ и была построена за $O(s + n)$ операций сложения и умножения. Поскольку мы можем построить подобную функцию для любых s, то таким образом мы получили функцию $\hat{f}(x_1, x_2, x_3)$, 2^s-эквивалентную функции $x_1 + x_2 + x_3$. □

Заметим, что принимая $\tau = s$ в лемме 2, мы получаем функцию $\hat{f}(x_1, x_2, x_3)$, τ-эквивалентную функции $x_1 + x_2 + x_3$.

Лемма 3. *Пусть множество $M \subseteq L_2$, M не содержится целиком ни в одном из множеств $\Theta \in J_a$, n - максимальная арность функций из M. Пусть мы уже получили константы γ_0, γ_1 из леммы 1 и функцию $x_1 + x_2 + x_3$. Тогда мы можем получить функции, τ-эквивалентые задержке, сумматору $x_1 + x_2$, константе 0, используя $O(n + \tau)$ операций сложения и умножения.*

Доказательство. Из множества M выберем функцию $h(x_1, ..., x_r)$ не принадлежащую $M(\xi)$. Существует $\mu \in U(h)$ такая, что

$$\mu + \mu(0) = \xi + \xi^2 a_2 + ...$$

Будем считать, что

$$h(x_1, ..., x_r) = \mu x_1 + \mu_2 x_2 + ... + \mu_r \xi_r + \gamma.$$

Получим функцию $h_1(x) = h(x, \gamma_0, ..., \gamma_0) = \mu x + \gamma$ за $O(n)$ операций сложения.

Для того чтобы получить оценки количества операций сложения и умножения, повторим индуктивное доказательство, представленное в работе [1]. Если $\mu(0) = 1$, то получим из функции $h_1(x)$ и сумматора $x_1 + x_2 + x_3$ следующую функцию:

$$h_2(x) = h_1(x) + x + \gamma_0 = \mu x + \gamma + x + \gamma_0 = \xi \mu' x + \gamma'.$$

Если $\gamma'(0) = 1$, то прибавив к $h_2(x)$ константы γ_0, γ_1 получим

$$h_2(x) + \gamma_0 + \gamma_1 = \xi\mu' x + \tilde{\gamma}', \tilde{\gamma}'(0) = 0.$$

Таким образом мы можем считать, что в $h_2(x)$ константа $\gamma'(0) = 0$. Значит, $\gamma' = 0 + b_1\xi + b_2\xi^2 + ...$. Если $b_1 = 0$, то все доказано. Пусть $b_1 = 1$.

$$h_2(\gamma_0) = \xi\mu'\xi\tilde{\gamma} + \gamma' = \xi + b_2'\xi^2 + b_3'\xi^3 + ...$$
$$h_2(\gamma_1) = \xi\mu'\tilde{\tilde{\gamma}} + \gamma' = b_2''\xi^2 + b_3''\xi^3 + ...$$
$$\hat{h}_2(x) = h_2(x) + h_2(\gamma_0) + h_2(\gamma_1) = \xi\mu' x + \xi^2\mu'', \mu'(0) = 1.$$

Функция $\hat{h}_2(x)$, таким образом, 2-эквивалентна задержке. Теперь докажем для $\tau > 2$.

Предположим теперь, что

$$h_\tau(x) = (\xi^{\tau-1} + \xi^\tau\mu_{\tau-1})x + \xi^\tau\gamma_{\tau-1}.$$

Подставим $\hat{h}_2(x)$ в $h_\tau(x)$ и получим

$$h_\tau'(x) = (\xi^\tau + \xi^{\tau+1}\mu_\tau')x + \xi^\tau\gamma_\tau.$$

Если $\gamma_\tau(0) = 0$, то мы уже получили $h_{t+1}(x)$, Предположим, что $\gamma_\tau(0) \neq 0$, тогда подставим в сумматор $x_1 + x_2 + x_3$ функции $h_\tau'(x)$, $h_\tau'(\gamma_0), h_\tau'(\gamma_1)$ и получим,

$$h_\tau'(x) + h_\tau'(\gamma_0) + h_\tau'(\gamma_1) = (\xi^\tau + \xi^{\tau+1}\mu_\tau'')x + \xi^{\tau+1}\gamma_\tau' = h_{\tau+1}(x)$$

Заметим, что функция $h_{\tau+1}(x)$ будет τ-эквивалентна нулю. Следовательно, мы можем получить сумматор от двух переменных, подставив $h_{\tau+1}(x)$ на место любой переменной в сумматоре $x_1 + x_2 + x_3$. Суммируя функции $h_{i,c} = h_i(\gamma_1) + h_i(\gamma_0)$, мы можем получить константу с началом из $i - 1$ нуля, $h_{i,c}(i) = 1$ и произвольным концом.

Снова рассмотрим функцию $\hat{h}_2(x)$ и переобозначим её как $f_1(x)$:

$$\hat{h}_2(x) = \xi\mu' x + \xi^2\mu'' = \xi x + \xi^2\mu''' x + \gamma_{1,1} = f_1(x), \mu'(0) = 1.$$

Функция $f_1(x)$ является 2-эквивалентной задержке с нулевым начальным состоянием. Получим теперь функцию $f_2(x)$:

$$f_1(x) = (\xi + \xi^2\mu''')x + \gamma_{1,1}, \mu'''(0) = a.$$
$$f_1(x) + (1 + \mu'''(0))h_3(x) = (\xi + \xi^3\mu^{(3)})x + \xi^2\gamma_{2,1}.$$
$$f_1(x) + (1 + \mu'''(0))h_3(x) + (1 + \gamma_{2,1}(0))h_3(\gamma_1) = (\xi + \xi^3\mu^{(3)})x + \xi^3\gamma_{2,2} = f_2(x).$$

Видно, что для получения $f_2(x)$ мы потратили $O(1)$ операций сложения и умножения. Функция $f_2(x)$ является 3-эквивалентной задержке с нулевым начальным состоянием. Продолжая данный процесс, получая $f_4, f_5, ...$ до времени τ, получим функцию $f_\tau(x)$, τ-эквивалентную задержке с нулевым начальным состоянием. На каждой итерации мы будем использовать $O(1)$ операций сложения и умножения, а значит всего, для получения $f_\tau(x)$, мы используем $O(n+\tau)$ операций сложения и умножения. □

Теорема 1. *1. Пусть множество $M \subseteq L_2$. M является A-замкнутым тогда и только тогда, когда M не содержится целиком ни в одном из множеств $\Theta \in J_a$.*

2. Пусть n - максимальная арность функций из M. Тогда за $O(\tau+n)$ операций сложения и умножения, а также одну операцию обратной связи мы можем получить функции τ-эквивалентные единице, задержке, сумматору от двух переменных.

Доказательство. Доказательство первого утверждения теоремы читатель может найти в работе [1]. Докажем второе утверждение.

В леммах 1,2,3 мы научились получать функции τ- эквивалентные задержке с нулевым начальным состоянием, константы γ_0,γ_1, где $\gamma_0(0) = 0$,$\gamma_1(0) = 1$, функцию $x_1 + x_2 + x_3$, сумматор $x_1 + x_2$, константу 0, задержку ξx за $O(n + \tau)$ операций сложения и умножения и одну операцию обратной связи. Получим функцию τ-эквивалентную единице.

Выпишем константу γ_1 до такта τ в виде ряда: $1 + a_1\xi + a_2\xi^2 + ... + a_\tau\xi^\tau + ...$

Получим константы $\gamma_1\xi^i, i = 1, ..., \tau$. Теперь прибавим к константе γ_1 константу $\gamma_1\xi$, если коэффициент $a_1 = 0$, и запишем это в таком виде:

$$\gamma_{1,1} = \gamma_1 + b_1\xi\gamma_1 = 1 + \xi + (b_1a_1 + a_2)\xi^2 + (b_1a_2 + a_3)\xi^3 + ...,$$

$$\text{где } b_1 = 1, \text{ если } a_1 = 0, \text{ и } b_1 = 0, \text{ если } a_1 = 1.$$

Перепишем

$$\gamma_{1,1} = 1 + \xi + a_{2,1}\xi^2 + a_{3,1}\xi^3 + ...,$$

Теперь предположим, что мы уже получили $\gamma_{1,p}$, получим теперь $\gamma_{1,p+1}$:

$$\gamma_{1,p+1} = \gamma_{1,p} + b_{p+1}\xi^{p+1}\gamma_1 = 1 + \xi + ... + \xi^{p+1} + (b_{p+1}a_{p+1,p} + a_{p+2,p})\xi^{p+2} + ...,$$

$$\text{где } b_{p+1} = 1, \text{ если } a_{p+1,p} = 0, \text{ и } b_{p+1} = 0, \text{ если } a_{p+1,p} = 1.$$

Перепишем

$$\gamma_{1,p+1} = 1 + \xi + ... + \xi^{p+1} + a_{p+2,p+1}\xi^{p+2} + ...$$

Отсюда видно, что на итерации τ константа $\gamma_{1,\tau}$ будет τ-эквивалентна единице. На каждой итерации мы используем $O(1)$ операций сложения, так как тактов всего τ, то мы используем для получения функции τ-эквивалентной единице $O(\tau)$ операций сложения и умножения. Подставляя оценки из предыдущих лемм, мы получим, что в общей сложности используется не более 1 операций обратной связи и $O(\tau+n)$ операций сложения и умножения. $\square$

На этом доказательстве мы закончим исследование сложности τ-выразимости элементарного базиса в классе линейных автоматов над полем E_2 и перейдем к линейным автоматам над полем E_k.

§2. Оценка сложности τ-приближения функций элементарного базиса в классе линейных автоматов над полем E_k.

В данной главе под обозначением E_k мы будем понимать конечное поле, где $k = p^m, p$ - простое, $m \in \mathbb{N}$. [4]

Аналогично со случаем в E_2, определим следующие множества согласно работам [2] [1]:

$T_a = \{f | f \in L_k, f$ сохраняет $a \in E_k$ в начальный момент времени. $\}$

$V_1 = \{f | f \in L_k, f$ имеет не более одной непосредственной переменной$\}$.

$V_0 = \{f(x_1, ..., x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0 | \sum_{i=1}^n \mu_i(0) = 1 (\text{mod } p)\}$.

$U(f) = \{\mu_i, i = 1, ..., n\}$.

$M_1(\xi) = \{f | f \in L_k, \forall \mu \in U(f), \mu - \mu(0) \in \xi^2 E'_k(\xi)\}$.

$\hat{P}_1, \hat{P}_2, ..., \hat{P}_s$ - все максимальные собственные подполя в E_k.

$P_j = \{f | f \in L_k, \forall i, i = 1, ..., n\ \mu_i(0) \in \hat{P}_j\}$.

$J_k^A = \{T_a, V_0, V_1, M_1, P_j | a \in E_k,\ i \in \{1, ..., s\}\}$.

Определения τ-эквивалентности и A-полноты аналогичны случаю с автоматами над E_2.

Перечисленные выше классы J_k^A являются A-замкнутыми и предполными в L_k [1].

Аналогично со случаем L_2 мы сформулируем следующую лемму:

Лемма 4. *Пусть множество $M \subseteq L_k$, M не содержится целиком ни в одном из множеств $\Theta \in J_k^A$. Пусть также n - максимальная арность функций из M. Тогда мы можем получить константу $\gamma, \gamma(0) = a, a \in E_k$, используя $O(k+n)$ операций сложения и умножения, а также 1 операцию обратной связи.*

Доказательство. Так как M не содержится в V_1, то, без ограничения общности, будем считать, что у нас есть функция $f(x_1, ..., x_n) = \sum_{i=1}^n \mu_i x_i +$

μ_0 имеющая непосредственные переменные x_1, x_2. Тогда рассмотрим функцию $g(x_1, x_2, x) = f(x_1, x_2, x, ..., x) = \mu_1 x_1 + \mu_2 x_2 + \mu' x + \mu_0$, которую мы получаем за $O(n)$ операций сложения. Обозначим $\mu_i(0) = a_i, i = 1, 2$.

Так как k - порядок поля E_k, то мы можем возвести a_i в степень $k-1$, чтобы получить $a_i^{k-1} = 1$ [4]. Получим функции

$$g_1(x_1, x) = g(x_1, x, x), g_2(x_2, x) = g_2(x, x_2, x).$$

Подставим g_1, g_2 в себя $k-2$ раз:

$$h_1 = g_1(g_1(g_1(...(x_1, x)...x), x), x),$$

$$h_2 = g_2(g_2(g_2(...(x_2, x)...x), x), x).$$

Мы используем для этого $O(k)$ операций сложения и умножения, а затем подставим полученные функции в $g(x_1, x_2, x_3)$:

$$g(h_1(x_1, x), h_2(x_2, x), x) = \mu_1^{k-1} x_1 + \mu_2^{k-1} x_2 + \hat{\mu} x + \hat{\mu_0} = h(x_1, x_2, x).$$

$$\mu_1^{k-1}(0) = (\mu_1(0))^{k-1} = 1, \mu_2^{k-1}(0) = 1.$$

p-раз подставим в себя функцию h следующим образом:

$$H(x_1, ...x_{p+1}, x) = h(h(...(h(x_1, x_2, x), ..., x_p, x), x_{p+1}, x) =$$
$$= \tilde{\mu}_1 x_1 + \tilde{\mu}_2 x_2 + ... + \tilde{\mu}_{p+1} x_{p+1} + \tilde{\mu} x + \tilde{\mu}_0.$$

Таким образом, за $O(p)$ операций мы получили, что $\tilde{\mu}_i(0) = 1, i = 1, ..., p-1, \tilde{\mu}_0(0) = p\hat{\mu}(0) = 0$, причем переменная x не является непосредственной.

Теперь возьмем функцию $u(x_1, ..., x_{n'}) \in M \setminus V_0$.

$G(x) = u(x, x, ..., x) = \sum_{i=1}^{n'} \mu_i' x + \mu_0' = \mu x + \mu_0'$, получаем $G(x)$ за $O(n')$ операций сложения. $\mu(0) \neq 1$, $n' \leq n$.

Если $\mu(0) = 0$, то мы можем применить оператор обратной связи к $G(x)$, получим $Fb_x(G(x)) = \gamma$, где γ - константа.

Пусть $\mu(0) = a, a \neq 0$. Элемент a порождает подполе E' в E_k. $E_p \subseteq E'$.

Рассмотрим случай $p = 2$. Имеем $z^{k-1} - 1 = 0$, $z = 1$ - корень данного уравнения, $a^{k-1} - 1 = 0$. Следовательно, мы можем переписать уравнение в виде $(z+1)(z^{k-2} + ...) = 0$. Если количество слагаемых во второй части уравнения - чётное, то вторая часть уравнения делится на $z+1$. Будем выделять $z+1$ из второй части уравнения до того момента, когда количество слагаемых в нём не станет нечётным, получим уравнение $(z+1)^s(\sum_{i=0}^r a_i z^i) = 0$, $\sum_{i=0}^r a_i a^i = 0, a_i \in \{0, 1\}, \sum_{i=0}^r a_i = 1$. Так как всего элементов в поле не более k, то на получение степеней μ^i мы используем не более $O(k)$ операций сложения и умножения. Из леммы 5 мы можем получить 3-сложение (текущая лемма не требуется для доказательства леммы 5). Используя 3-сложение и полученные степени a^i, получим дробь $\mu \sum_{i=0}^{r} a_i \mu^i$, для этого мы будем применять 3-сложение не более $O(k)$ раз. Таким образом мы получаем функцию $\hat{H}(x)$ такую, что $\hat{H}(0) = 0$, а значит к ней применима обратная связь. Применяя к $\hat{H}(x)$ обратную связь получим константу γ за $O(k+n)$ операций сложения и умножения и одну операцию обратной связи.

Рассмотрим случай $p > 2$. Умножая элемент a не более чем за $l < k$ раз, мы можем получить элемент $t \in \{2, 3, ...p-1\}$ подполя E_p [4]. Значит, подставляя $G(x)$ в себя не более чем k раз, получим функцию $G'(x) = (\mu')^l x + \mu''$, используя $O(k)$ операций сложения и умножения и одну операцию обратной связи.

Теперь подставим функцию $G'(x)$ в функцию H на место первых r' переменных, а на место остальных поставим x, где количество применений r' найдем ниже.

Получим $\hat{H}(x) = H(G'(x), ..., G'(x), x, x, ...x) = \hat{\mu}x + \tilde{\hat{\mu}}x + \hat{\mu}_0 = (\hat{\mu} + \tilde{\hat{\mu}})x + \hat{\mu}_0$. Переменная x не является непосредственной для функции $\hat{H}(x)$, т.к. $(\hat{\mu} + \tilde{\hat{\mu}})(0) = r't + (1 - r') = 0$, $r' = \frac{-1}{b-1} \in E_p$. А значит, применяя операцию обратной связи к функции $\hat{H}(x)$, получим костанту γ за $O(k+n)$ операций сложения и умножения и одну операцию обратной связи. □

Заметим, что любую другую константу γ_2 мы можем получить из функции f_a, не принадлежащей классу T_γ, подставив в функцию f_a на место всех переменных константу γ, что можно сделать не более чем за $O(n)$ операций сложения.

Теперь получим операцию сложения $p+1$ элемента, т.е. докажем следующую лемму:

Лемма 5. *Пусть множество $M \subseteq L_k$, M не содержится целиком ни в одном из множеств $\Theta \in J_k^A$. Пусть также n - максимальная арность функций из M. Тогда мы можем получить функцию τ-эквивалентную функции $x_1 + x_2 + x_3 .... + x_{p+1}$ за $O(k + \tau + n)$ операций сложения и умножения.*

Доказательство. $\exists f(x_1, ..., x_{n'}) \in M \setminus V_1$. Пусть x_1, x_2 - её непосредственные переменные. Тогда подставим переменную x в остальные переменные функции f: $f_1(x_1, x_2, x) = f(x_1, x_2, x, ..., x) = \mu_1 x_1 + \mu_2 x_2 + \mu x + \mu_0$. $\mu_1(0) \neq 0, \mu_2(0) \neq 0$, используя $O(n)$ операций сложения. Подставим функцию f_1 в себя за $O(1)$ операций умножения и сложения:

$$f_2(x_1, x_2, x) = f_1(f_1(x, x_2, x), f_1(x_1, x, x), x) = \mu_1\mu_2 x_1 + \mu_1\mu_2 x_2 + \mu' x + \mu'_0.$$

Обозначим $\mu = \mu_1\mu_2, \mu(0) \neq 0$. Распишем μ в форме ряда и переобозначим этот ряд: $\mu = a_0 + a_1\xi + ... = a_0 + \xi\hat{\mu}, \hat{\mu} \in E_k'(\xi)$. Далее за $O(k)$ операций сложения и умножения получим функцию

$$f_3(x_1, x_2, x) = \mu^{k-1}x_1 + \mu^{k-1}x_2 + \tilde{\mu}x + \tilde{\mu}_0, \mu^{k-1} = \mu_3, \mu_3(0) = 1,$$

т.к. из [4] нам известно, что

$$(a+b)^p = a^p + b^p$$
$$a^{k-1} = 1, a^k = a^{p^m} = a, \forall a \in E_k.$$

Теперь, не более чем за $O(p^t)$ операций сложения и умножения, подставляя саму в себя функцию f_3 тем же способом, что и функцию f_2, получим из функции f_3 функцию $f_4(x_1, x_2, x) = \mu_3^{p^t}x_1 + \mu_3^{p^t}x_2 + \tilde{\mu}x + \tilde{\mu_0}$. Выпишем дроби $\mu_3^p, \mu_3^{p^t}$:

$$\mu_3^p = (1 + \xi\mu_4)^p = 1^p + (\xi\mu_4)^p = 1 + a_p'\xi^p + a_{p+1}'\xi^{p+1} + ...$$
$$\mu_3^{p^t} = (1 + \xi\mu_4)^{p^t} = 1^{p^t} + (\xi\mu_4)^{p^t} = 1 + a_{p^t}'\xi^{p^t} + a_{p^t+1}'\xi^{p^t+1} + ...$$

Число t мы будем выбирать так, чтобы $\tau \leq p^t$, заметим, что при $\tau \geq 2$ мы можем выбрать t такой, что $t \leq \tau$, а значит общее количество операций сложения и умножения для получения f_4 мы можем оценить как $O(p + \tau)$. Обозначим $\mu_5 = \mu_3^{p^t}$, тогда перепишем $f_4 = \mu_5 x_1 + \mu_5 x_2 + \mu_5' x + \mu_{05}$. Теперь будем подставлять f_4 в себя p-раз следующим образом:

$$f_4(x_1, f_4(x_2, f_4(x_3, ..., x), x), x), x) =$$
$$= \mu_5 x_1 + \mu_5^2 x_2 + ...\mu_5^p x_p + \mu_5^p x_{p+1} + (\mu_5' + \mu_5'\mu + ... + \mu_5'\mu_5^{p-1})x +$$
$$+ (\mu_0'' + \mu_0''\mu + ... + \mu_0''\mu_5^{p-1}) = F(x_1, x_2, ...x_{p+1}, x).$$
$$\hat{\mu}' = \mu_0'' + \mu_0''\mu + ... + \mu_0''\mu_5^{p-1},$$
$$\hat{\mu}'' = \mu_5' + \mu_5'\mu + ... + \mu_5'\mu_5^{p-1}.$$

Вид μ_5 мы уже обсуждали ранее, все дроби $\mu_5^i, i = 1, ...p$ будут τ-эквивалентны единице. $\hat{\mu}'', \hat{\mu}'$ в свою очередь τ-эквивалентны нулю, т.к. в $\hat{\mu}'$ и в $\hat{\mu}''$ содержится p слагаемых. Следовательно, сама функция $F(x_1, x_2, ...x_{p+1}, x)$ будет τ-эквивалентна функции $x_1 + x_2 + x_3.... + x_{p+1}$, причем функцию F мы получили за $O(k+\tau)$ операций сложения и умножения. □

Сформулируем ещё одну вспомогательную лемму:

Лемма 6. *Пусть множество $M \subseteq L_k$, M не содержится целиком ни в одном из множеств $\Theta \in J_k^A$. Пусть также n - максимальная арность функций из M. Пусть также нами были получены константа $\gamma, \gamma(0) = b, b \in E_k$, а также функция $x_1+x_2+x_3....+x_{p+1}$. Тогда для любых $a \in E_k$ за $O(n)$ операций мы можем получить функцию $g_a(x) = \mu_a x + \gamma'$, где $\mu_a \in E_k'(\xi), \gamma' \in E_k'(\xi)$, $\mu_a(0) = a$.*

Доказательство. Так как множество M не содержится целиком в классах $P_l, \forall l \in \{1, ..., s\}$, то $\exists \mu_{l_1}, ..., \mu'_{l_m} \in U(M)$, $\mu_i'(0) \notin E_{k,l_i}$, где $E_{k,i}$ - подполя в E_k такие, что элемент $\mu_{l_1}(0)\mu_{l_2}(0)...\mu'_{l_m}(0)$ порождает E_k по операциям сложения и умножения. Для получения этого элемента мы потратим не более $O(k)$ операций сложения и умножения. Заметим, что так как $\mu_{l_1}(0)\mu_{l_2}(0)...\mu'_{l_m}(0)$ порождает все E_k, то мы можем получить все различные элементы E_k в нулевой момент времени за $O(k)$ операций сложения и умножения. Будем далее считать, что мы получили данные элементы и добавим $O(k)$ в общую оценку сложности в теореме 2 и не будем учитывать эту оценку в данной лемме.
Значит, $\forall a \in E_k$ $\exists f(x_1, ..., x_{n'}) \in K(M)$, $\exists \mu \in U(f), \mu(0) = a$. Не ограничивая общности, будем считать, что μ - дробь перед первой переменной x_1. Подставив в f константу γ, полученную ранее, получим $f(x, \gamma, ..., \gamma) = \mu x + \gamma'$ за $O(n)$ операций сложения. □

И теперь докажем нужную нам лемму:

Лемма 7. *Пусть множество $M \subseteq L_k$, M не содержится целиком ни в одном из множеств $\Theta \in J_k^A$. Пусть также n - максимальная арность функций из M. Пусть также нами были получены константы $\gamma_a, \gamma_a(0) = a; \gamma_c, \gamma_c(0) = c; a, c \in E_k, a \neq c$, а также функция $x_1+x_2+x_3....+x_{p+1}$. Тогда мы можем получить константу $\gamma_0 \in K(M)$ такую, что $\gamma_0(0) = 0$ за $O(n+p)$ операций.*

Доказательство. Рассмотрим функцию $x_1 + x_2 + ... + x_{p+1}$. Подставим на место переменных $x_1, ...x_i$ функцию $g_b(\gamma_c)$, которую мы можем получить по лемме 6 за $O(n)$ операций сложения и умножения, на место переменных $x_{i+1}, ..., x_p$, а на место переменной x_{p+1} константу γ_c всего за $O(n+p)$ операций сложения и умножения. В итоге получим $g_b(\gamma_c) + ... + g_b(\gamma_c) + g_a(\gamma_a) + ... + \gamma_c = \gamma$. Теперь найдем такие значения i, b, что $\gamma(0) = 0$.

$$\gamma(0) = i\mu_b(0)\gamma_c(0) + (p-i)\mu_b(0)\gamma_a(0) + \gamma_c(0) + p\gamma_c'(0) = 0,$$

$$ib\gamma_c(0) + (p-i)b\gamma_a(0) + \gamma_c(0) = 0,$$

$$ib(\gamma_c(0) - \gamma_a(0)) = \gamma_c(0).$$

Получаем уравнение

$$i = \frac{\gamma_c(0)}{b(\gamma_a(0) - \gamma_c(0))}.$$

Если $\gamma_c(0) = 0$, то $i = 0$ и мы получаем необходимую нам костанту. Если $\gamma_c(0) \neq 0$, то тогда

$$b = \frac{\gamma_c(0)}{(\gamma_a(0) - \gamma_c(0))}, i = 1.$$

Количество операций для получения константы γ_0 составило $O(n + p)$. $\square$

Лемма 8. *Пусть множество $M \subseteq L_k$, M не содержится целиком ни в одном из множеств $\Theta \in J_a^k$. Пусть также n - максимальная арность функций из M. Пусть также нами были получены константа $\gamma_0(0) = 0 \in E_k$, а также функция $x_1+x_2+x_3....+x_{p+1}$. Тогда для любых $a \in E_k$ за $O(n+p)$ операций сложения и умножения мы можем получить $\mu_a x+\gamma_0$, где $\mu_a \in E_k'(\xi), \gamma \in E_k'(\xi)$, $\mu_a(0) = a, \gamma_0(0) = 0$.*

Доказательство. Будем считать, что мы уже получили функцию $\mu_a+\gamma'$, $a \in E_k$ за $O(n)$ операций. Возьмем функцию сложения $x_1 + x_2 + ... + x_{p+1}$ и подставим на место первой переменной x_1 функцию $\mu_a x + \gamma'$, на место переменных $x_2, ...x_p$ подставим константу $\mu_a\gamma_0+\gamma'$, а на место переменной x_{p+1} константу γ_0:

$$(\mu_a x + \gamma) + \sum_{i=1}^{p-1}(\mu_a\gamma_0 + \gamma) + \gamma_0 =$$

$$= \mu_a x + \sum_{i=1}^{p-1}(\mu_a\gamma_0) + \gamma_0 = \mu_a x + \gamma', \gamma'(0) = 0.$$

Таким образом мы получили необходимую нам функцию $\mu_a x + \gamma_0$, используя не более чем $O(n + p)$ операций сложения и умножения. $\square$

Теперь мы можем сформулировать нашу теорему:

Теорема 2. *Пусть множество $M \subseteq L_k$, M не содержится целиком ни в одном из множеств $\Theta \in J_k^A$. Пусть также n - максимальная арность функций из M. Тогда за $O((\tau + 1)(n + p + 1) + k + p)$ операций сложения и умножения, а также одну операцию обратной связи мы можем получить функции, τ-эквивалентные базисным функциям $\{1, x_1 + x_2, ax, \xi x | a \in E_k\}$.*

Доказательство. По лемме 4 мы научились получать функции, τ эквивалентные константам γ_a, γ_b за $O(n+k)$ операций сложения и умножения. По лемме 5 получим функцию, τ-эквивалентную функции $x_1 + x_2 + ... + x_{p+1}$ за $O(k+n+\tau)$ операций сложения и умножения. По лемме 7 получим функцию $\gamma_0, \gamma_0(0) = 0$ за $O(n+p)$ операций сложения и умножения, итого получим оценку в $O(n+k+\tau+p)$ операций сложения и умножения. Заметим, что оценка $O(k)$, полученная в лемме 6 не влияет на итоговую оценку.

Теперь будем получать задержку с нулевым начальным состоянием. Существует функция $g \in M \setminus M_1$, $g(x_1, ...x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0$. Подставим во все переменные функции, кроме x_1, полученную ранее константу γ_0. Функция g примет вид

$$g(x, \gamma_0, ..., \gamma_0) = \mu_1 x + \gamma' = h(x).$$

$$\mu_1 = a(0) + a(1)\xi + a(2)\xi^2 + ..., \text{ где } a(1) \neq 0,$$

После возведения в степень k дробь μ_1 при разложении в ряд будет выглядеть следующим образом:

$$\mu_1^k = \mu_1^{p^m} = a^{p^m}(0) + a^{p^m}(1)\xi^{p^m} + a^{p^m}(2)\xi^{2p^m} + ...$$

Заметим что так как $a^{p^m} = a$, то μ_1^k будет принимать вид

$$\mu_1^k = \mu_1^{p^m} = a(0) + a(1)\xi^{p^m} + a(2)\xi^{2p^m} + ...$$

Подставим теперь полученную выше функцию $h(x)$ и $h^k(x)$, которую мы получим за $O(k)$ операций в сумматор $x_1 + ...x_{p+1}$ следующим образом:

$$h(x) + h^k(x) + ... + h^k(x) + \gamma_r' = h'(x).$$

Константу γ_r' мы получим по лемме 8 из функции $g_r(x)$, подставляя в $g_r(x)$ константу γ_0 за $O(n+p)$ операций сложения умножения. Значение r подберем так, чтобы свободный член на нулевом такте в функции $h'(x)$ был равен нулю. Для получения самой функции $h(x)$ мы потратим не более $O(n)$ операций сложения и умножения. При подстановке в сумму - не более $O(p)$. Таким образом на данном этапе мы потратим не более $O(n + k + p)$ операций сложения и умножения.

Выпишем функцию $h'(x)$ в следующем виде:

$$h'(x) = (a(1)\xi + \xi^2\hat{\mu})x + \hat{\gamma}, \hat{\gamma}(0) = 0.$$

По доказанной ранее лемме 8, мы можем получить функцию $g'(x) = \tilde{\mu}x + \gamma_0, \tilde{\mu}(0) = (a(1))^{-1}$ за $O(n + p)$ операций сложения и умножения.

Подставим её в $h'(x)$ за $O(1)$ операций сложения и умножения:

$$h'(g'(x)) = (\xi + \xi^2\mu'')x + \gamma'', \gamma''(0) = 0.$$

Обозначим $f_1(x) = h'(g'(x))$. Предположим теперь, что мы уже получили

$$f_\tau(x) = (\xi^\tau + \xi^{\tau+1}\mu_\tau)x + \gamma_\tau, \gamma_\tau = \xi^\tau\gamma'_\tau.$$

Пусть γ_τ в моменты времени $0, ..., \tau - 1$ равна нулю, а в момент времени τ константа $\gamma_\tau(\tau) = c$. По лемме 8 получим функцию $g_{-c}(x)$ за $O(n+p)$ операций сложения и умножения. Подставим в $g_{-c}(x)$ константу γ_0 и получим константу γ_{-c} такую, что $\gamma_{-c}(0) = -c$.

Подставим γ_{-c} в $f_\tau(x)$ и получим, что в моменты времени $0, ..., \tau$ функция $f_\tau(\gamma_c)$ равна нулю. Таким образом мы получили функцию $\tau+1$-эквивалентную константе ноль. Подставив эту константу в функцию $x_1 + ...x_{p+1}$ на место переменных $x_3, ..., x_{p+1}$ получим функцию $\tau + 1$ эквивалентную сумматору $x_1 + x_2$.

Подставим теперь f_τ в $f_1(x)$. Получим функцию

$$f_\tau(f_1(x)) = (\xi^{\tau+1} + \xi^{\tau+2}\hat{\hat{\mu}})x + \hat{\hat{\gamma}}, \hat{\hat{\gamma}}(i) = 0, i \in \{0, ..., \tau - 1\}, \hat{\hat{\gamma}}(\tau) = d.$$

По лемме 8 получим функцию $g_u(x)$ за $O(n+p)$ операций сложения и умножения. Значение u найдем в ходе дальнейших вычислений. Подставим в $g_u(x)$ константу γ_0 и получим константу γ_u такую, что $\gamma_u(0) = u$. Сложим теперь $f_\tau(f_1(x))$ и $f_\tau(\gamma_u))$ и получим

$$f_\tau(f_1(x)) + f_\tau(f_1(\gamma_{-d})) = f_{\tau+1}(x).$$

$$f_{\tau+1}(x) = (\xi^{\tau+1} + \xi^{\tau+2}\hat{\hat{\mu}})x + \xi^\tau(d + c + u) + \gamma''', \gamma'''(i) = 0, i = \{0, ..., \tau\}.$$

$$u + c + d = 0, \text{ следовательно, } u = -c - d.$$

Мы получили сумматор от двух переменных и константу ноль за $O(\tau(n+p))$ операций сложения и умножения. Отсюда также видно, что на каждом такте мы можем получать константу с произвольным количеством нулей в начале и произвольным значением $u \in E_k$ за $O(n + p)$ операций сложения и умножения. Перейдем к получению задержки с нулевым начальным состоянием.

Выпишем

$$h_1(x) = (\xi + \xi^2\mu'') + \gamma'', \gamma''(0) = 0, \gamma'' = b_{1,1}\xi + b_{2,1}\xi^2 + ...$$

Прибавим к функции $h_1(x)$ константу $\gamma_{1,-b_{1,1}}$ такую, что $\gamma_{1,-b_{1,1}}(0) = 0$, $\gamma_{1,-b_{1,1}}(1) = -b_{1,1}$. Данным сложением мы обнулим значение при ξ в константе γ''.

$$h'_1(x) = (\xi + \xi^2\mu'') + \gamma'' + \gamma_{1,-b_{1,1}} = (\xi + \xi^2\mu'')x + \gamma'_1, \gamma'_1(0) = \gamma'_1(1) = 0.$$

Аналогично будем действовать с коэффициентом при степени ξ^2 в константе γ'_1. Заметим, что на уничтожение коэффициента при произвольной степени ξ в константе мы потратим $O(n+p)$ операций сложения и умножения. Теперь обнулим коэффициент в μ'' при степени ξ^2. Пусть $\mu''(0) = a'$. Тогда подставим в функцию $h_2(x)$ функцию $g_2(x) = \tilde{\mu}_2 x + \gamma_{g,2}, \tilde{\mu}_2(0) = (a')^{-1}$, полученную за $O(n+p)$ операций сложения и умножения. Затем сложим функии $h_2(g_2(x))$ и $h'_1(x)$:

$$h_2(g_2(x)) + h'(x) = \xi + \xi^3\mu_3 + \gamma_{2,0}, \gamma_{2,0}(0) = \gamma_{2,0}(1) = 0.$$

$$h_2(g_2(x)) + h'_1(x) \overset{3}{\sim} \xi x.$$

Действуя аналогично для остальных итераций, мы получим функцию τ-эквивалентную задержке с нулевым начальным состоянием за $O(\tau(n+p))$ операций сложения и умножения.

Теперь будем получать умножитель на произвольную константу. Возьмем полученный ранее по лемме 8 за $O(n+p)$ операций сложения и умножения умножитель на некоторую константу $a(0)$ и возведем его в степень k:

$$(a(0) + \xi^k\mu^k)x + \gamma, \gamma(0) = 0.$$

Эта функция может быть получена за $O(k)$ операций сложения и умножения. Подставим константу γ в задержку и получим константу γ'. Значения константы γ для тактов $1, 2....$ нам необходимо занулить до момента времени τ. Выпишем константу γ' в форме ряда:

$$\xi(\gamma(1)....) = 0\gamma(1)... = \gamma'.$$

Далее просуммируем:

$$\gamma + \gamma'(p-1) = 00\gamma''(2)...$$

Таким способом мы можем обнулить все значения γ до такта τ, используя $O(\tau p)$ операций сложения и умножения. Данным способом за τ тактов получим выражение

$$(a(0) + \xi^\tau\mu^\tau)x + \xi^\tau\gamma_\tau,$$

которое, в свою очередь, при $k \geq \tau$ будет τ-эквивалентно умножению x на константу $a(0)$. Если же $\tau > k$, будем выражение $((a_0 + \xi^k\mu^k)x + \gamma)^{k^i}$ возводить в степень k^i, где $k^i > \tau$.

Посчитаем теперь итоговое количество операций сложения и умножения. В леммах 4,5,6,7 нам потребовалось $O(p+k+n+\tau)$ операций сложения и умножения, а также одна операция обратной связи. Для получения сумматора, задежки и константы ноль мы использовали $O(\tau(n+p))$

операций сложения и умножения. Получение умножителя на константу имеет сложность $O(k+n+p\tau)$. Итого, за $O((\tau+1)(n+p+1)+k+p)$ операций сложения и умножения, а также одну операцию обратной связи мы получили функции τ-эквивалентные базису $\{x_1 + x_2, ax, \xi x | a \in E_k\}$. $\square$

Заключение.

Мы получили оценки на получение A-эквивалентного элементарного базиса для случаев E_2 и E_k. Мы получили куда более скромную оценку на количество операций, чем для случая K-замыкания над полем E_2 для линейных автоматов, сохраняющих нулевую последовательность, где оценка являлась экспоненциальной. В следующих работах представляется интересным получить нижнюю оценку на количество операций для получения A-эквивалентного элементарного базиса и проверить, можно ли улучшить верхнюю оценку.

Автор выражает благодарность своему научному руководителю А.А. Часовских.

Список литературы

[1] Часовских А. А., “О полноте в классе линейных автоматов”, *Математические вопросы кибернетики*, 1991, № 2, 140–166.

[2] Kudryavtsev V.B., Alyoshin S.V., Podkolzin A.S., *Introduction to automata theory*, «Science», Moscow, 1985, 320 с.

[3] Ильин И.Ю., *Интеллектуальные системы. Теория и приложения*, 2022, 164–173.

[4] Лидл Р., Нидеррайтер Г., *Конечные поля*, Мир, Москва, 1988, 430 с.

[5] В.А.Буевич, “Об алгоритмической неразрешимости распознавания A-полноты для ограниченно-детерминированных функций”, *Матем. заметки*, **11**:6 (1972), 687–697.

Comlexity of implementation of A-closure elementary basis in lineary automata class on finite field.

Ilin I.Y.

In the previous work we have received compexity estimation for elementary basis implementation in the class of linear automata that preserves zero-sequence. In the current work we will find the complexity estimation for elementary basis realization by A-closure operations in linear automata under finite field [4].

Keywords: linear automata, A-closure, A-expressibility, algorithm complexity.

References

[1] Часовских А. А., “О полноте в классе линейных автоматов”, *Математические вопросы кибернетики*, 1991, № 2, 140–166.

[2] Kudryavtsev V.B., Alyoshin S.V., Podkolzin A.S., *Introduction to automata theory*, «Science», Moscow, 1985, 320 с.

[3] Ильин И.Ю., *Интеллектуальные системы. Теория и приложения*, 2022, 164–173s.

[4] Лидл Р., Нидеррайтер Г., *Конечные поля*, Мир, Москва, 1988, 430 с.

[5] В.А.Буевич, “Об алгоритмической неразрешимости распознавания A-полноты для ограниченно-детерминированных функций”, *Матем. заметки*, **11**:6 (1972), 687–697.