О сложности реализации элементарного базиса в классе одноместных линейных автоматов, сохраняющих нулевую последовательность.

И. Ю. Ильин[1]

Сейчас нам известны некоторые факты о полноте конечных множеств линейно-автоматных функций, найдены все предполные классы по операциям суперпозиции и композиции, выведены критерии полноты в терминах предполных классов. В данной работе доказаны оценки количества операций для выразимости задержки и нейтрального элемента в случая одноместных линейных автоматов, сохраняющих нулевую последовательность.

Ключевые слова: линейные автоматы, оценки сложности.

Необходимые для нашей работы определения можно найти в работах [1] и [2], однако, в целях упрощения, представляется правильным повторить их, чтобы исключить избыточные обращения к источникам.

Мы рассмотриваем множество рациональных дробей $E_2^{'}(\xi) = \{\frac{u}{v} | u, v \in E_2[\xi], v(0) = 1\}$ с операциями:

1. Сложения: $\mu_1, \mu_2 \in E_2^{'}(\xi) : \mu_1 + \mu_2$
2. Умножения: $\mu_1, \mu_2 \in E_2^{'}(\xi) : \mu_1 \mu_2$
3. Обратной связи: $\mu_1, \mu_2 \in E_2^{'}(\xi), \mu_2(0) = 0 : F_b(\mu_1, \mu_2) = \frac{\mu_1}{1+\mu_2}$.

Обозначим $K^{(1)}(M)$ - замыкание множества M по операциям сложения, умножения и обратной связи, а $S^{(1)}(M)$ - замыкание множества M только по операциям сложения и умножения.

Множество $M \subseteq E_2^{'}(\xi)$ - полно, если $K^{(1)}(M) = E_2^{'}(\xi)$

Назовем множество $\{1, \xi\}$ элементарным базисом в $E_2^{'}(\xi)$ по операциям $K^{(1)}$.

Введем последовательность p_i: $p_1 = \xi, p_2 = 1+\xi, ...$ состоящую из всех неприводимых многочленов.

Введем множества $R_i^{(1)}$ и $M_i^{(1)}$ следующим образом:

$R_0^{(1)} = \{\mu | \mu = \frac{u}{v}; u, v \in E_2[\xi], (u, v) = 1 : \deg(u) < \deg(v)\ \}$.

$R_i^{(1)} = \{\mu | \mu = \frac{u}{v}; u, v \in E_2[\xi], (u, v) = 1, up_i\}$.

$M_0^{(1)} = \{\mu | \mu = \frac{u}{v}; u, v \in E_2[\xi], (u, v) = 1 :$ если $u(0) = 0$, тогда $\deg(u) < \deg(v)$, а если $u(0) = 1$, тогда $\deg(u) = \deg(v)\ \}$.

[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.

$M_i^{(1)} = \{\mu | \mu = \frac{u}{v}; u, v \in E_2[\xi], (u, v) = 1$ такие, что если $u(0) = 1 =>$ $1 + \frac{u}{v} = \frac{u+v}{v} = \frac{\xi p_i u'}{v}$, а если $u(0) = 0 => \frac{u}{v} = \frac{\xi p_i u'}{v}\}$.

$J^{(1)} = \{M_i^{(1)}, R_i^{(1)}, i = 0, 1, 2, ...\}$. В работе [1] показано, что множества $R_i^{(1)}$ и $M_i^{(1)}$ составляют приведенную критериальную систему предполных классов в $E_2'(\xi)$ относительно операций $K^{(1)}$.

Перед тем как сформулировать итоговую теорему, докажем вспомогательные леммы и утверждения.

Лемма 1. *Пусть* $K^{(1)}(M) = E_2'(\xi)$, *где* $M = \{\frac{u_i}{v_i} | u_i,\ v_i \in E_2[\xi],$ $v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$.

Обозначим $k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$.

Тогда из M *можно получить рациональные дроби* $\mu, \mu\xi$, $\mu \neq 0$, *используя* $O(nk^2)$ *операций сложения и умножения,* $\deg(\mu) \leq 2^k k$.

Доказательство. Обозначим $F_i(z) = \mu_i(\xi)v_i(z) + u_i(z)$ - многочлены от z с коэффициентами из $E_2'(\xi)$. Каждый из этих многочленов строится за $O(1)$ операций умножения и сложения, таким образом, для построения всех многочленов мы потратим $O(n)$ операций сложения и умножения. Теперь найдем НОД этих многочленов.

Шаг 1. Возьмем $F_i(z)$ с минимальной степенью $\deg(F_i(z)) = p$. Уменьшим степень каждого $F_j(z), i \neq j$ на 1 по следующему правилу: Перепишем $F_j(z)$, вынесем старшую степень z^s вперед. $F_j(z) = z^s(\mu_j'(\xi)a_{j,s} + b_{j,s}) + ...$, где s - $\deg(F_j(z))$. $F_i(z) = z^p(\mu_i'(\xi)a_{i,k} + b_{i,k})$. Сократим сташую степень в $F_j(z)$: $F_j(z)$: $:= F_j(z)(\mu_i'(\xi)a_{i,k} + b_{i,k}) + z^{s-p}(\mu_j'(\xi)a_{j,s} + b_{j,s})F_i(z)$. Степень по ξ не выше чем $\deg(\mu_i') + \deg(\mu_i')$. Коэффициент перед z с наибольшей степенью переобозначим как μ_j'. Количество операций для получения всех коэффициентов многочлена F_j - $O(k)$, так как степень F_j не больше чем k. Поскольку мы проводим операцию уменьшения степени для всех F_j, то общее количество операций - $O(nk)$.

Шаг 2. Теперь будем повторять шаг 1 не более чем k раз, поскольку k - максимальная степень изначального $F_j(z)$.

Согласно работе [1] НОД многочленов $F_j(z)$ равен $\xi + z$. Таким образом не более чем за $O(nk^2)$ операций мы получим $\mu(\xi)(\xi + z)$, где μ - итоговый коэффициент перед НОД, который получаем в результате применения алгоритма, степень многочлена-коэффициента увеличивается не более чем в два раза от максимальной степени коэффициентов на предыдущем шаге, таким образом получаем оценку $2^k k$ на степень μ. □

Лемма 2. $M = \{\frac{u_i}{v_i} | u_i,\ v_i \in E_2[\xi],\ v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$.
$k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$, $K^{(1)}(M) = E_2'(\xi)$. *Пусть по доказанной ранее лемме 1 были получены дроби* $\mu, \xi\mu$, *где* $\mu = \frac{u}{v}, \mu \neq 0$. *Тогда*

за $k\lceil \log k \rceil$ *операций сложения и умножения и 1 операцию обратной связи мы можем получить* $\xi\hat{\mu}, \hat{\mu}$, *где* $\hat{\mu} = \frac{\hat{u}}{\hat{v}}$ *такие, что* $\deg(\hat{u}) \geq \deg(\hat{v})$. *Степень итоговой дроби* $\hat{\mu}$ *не превосходит* $4k^2 2^k$.

Доказательство. В случае, если $deg(u) \geq deg(v)$, доказывать нечего. Предположим, что $\deg(u) < \deg(v)$. Так как M - полно, то существует дробь $\mu_R \in M \setminus R_0^{(1)}, \mu_R = \frac{u_R}{v_R}, \deg(u_R) \geq \deg(v_R), \deg(\mu_R) \leq k$.

Случай 1. Если $\deg(u_R) > \deg(v_R)$, то искомые дроби $\hat{\mu}, \xi\hat{\mu}$ мы можем получить за $\deg(\mu)$ операций. Напомним, что в предыдущей лемме мы доказали, что степень $\deg(\mu)$ не превосходит $k2^k$, тогда количество операций для получения самого $\hat{\mu}$ оценим как $k + \lceil \log k \rceil$, т.к. количество операций для получения $\mu_R^{k2^k}$ не превосходит $k + \lceil \log k \rceil$. Степень итоговой дроби $\hat{\mu}$ - не превосходит $2\deg(\mu_R)k2^k$.

Предположим теперь, что $\deg u_R = \deg v_R$.

Случай 2. $u_R(0) = 0$, то $\tilde{\mu} = Fb(\mu_R, \mu_R) = \frac{\mu_R}{1+\mu_R} = \mu_R \frac{v_R}{u_R + v_R}, \deg(v_R) > \deg(v_R + u_R) => \tilde{\mu} = \frac{\tilde{u_R}}{\tilde{v_R}}, \deg(\tilde{u}) > \deg(\tilde{v})$. Таким образом мы получили дробь, к которой можем применить доказательство из случая 1, $\deg(\tilde{\mu}) \leq 2\deg\mu_R$.

Случай 3. Если $u_R(0) = 1, \exists \mu_m \in M \setminus M_0^{(1)}, \mu_m = \frac{u_m}{v_m}$. Если $\deg(u_m) > \deg(v_m)$, то сводим к случаю 1. Если $\deg(u_m) = \deg(v_m)$ и $u_m(0) = 0$, то сводим к случаю 2. Если $\deg(u_m) < \deg(v_m) => u_m(0) = 1$. $\mu_R + \mu_m = \mu' = \frac{u'}{v'}$, $\deg(u') = \deg(v') : \mu_R + \mu_m = \frac{u_R v_m + v_R u_m}{v_R v_m}$. $\deg(u_R v_m + v_R u_m) = \deg(u_R v_m) = \deg(v_R u_m)$. $u'(0) = 1$, а значит имеем случай 2, $deg(\mu_R + \mu_m) \leq 2k$. По итогу мы используем не более 1 операций обратной связи и $k + \lceil \log k \rceil$ операций умножения и сложения. Степень итоговой дроби не превосходит $4k^2 2^k$. □

Лемма 3. $M = \{\frac{u_i}{v_i}, u_i,\ v_i \in E_2[\xi],\ v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$.
$k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$, $K^{(1)}(M) = E_2'(\xi)$.
Пусть $\mu,\ \xi\mu \in K^{(1)}(M),\ \mu = \frac{u}{v} \neq 0, \deg(u) \geq \deg(v),\ \deg(\mu) \leq 4k^2 2^k$. *Тогда существует такое* $T \in \mathbb{N}$, *что* $\forall i, j \geq T : \xi^i \mu^j \in K^{(1)}(M)$, *дробь* $\xi^i \mu^j$ *может быть получена не более чем за* $O(max(i - j, 0)k^2 2^k + j)$ *операций сложения и умножения.*

Доказательство. Пусть $j \geq i$. Тогда перемножая $\xi\mu$ i-раз, мы получим $\xi^i \mu^i$. Домножим $\xi^i \mu^i$ на μ^{j-i} (перемноженное $j - i$ раз), получим $\xi^i \mu^j$, затрачивая не более j операций.

Теперь предположим, что $j < i$ и перепишем дробь μ следующим образом:

$$\mu = \frac{u}{v} = \frac{a_0 + a_1\xi + ...a_{p-1}\xi^{p-1} + \xi^p}{1 + b_1\xi + ...b_{k-1}\xi^{s-1} + \xi^s}, p \geq s, p \leq 4k^2 2^k.$$

Получим все степени μ^i до p, потратив на это $O(k^2 2^k)$ операций умножения, степень μ полагаем не превосходящей $4k^2 2^k$ (степень μ из прошлой леммы). Теперь формально домножим выражение $a_0 + a_1\xi + ...a_{p-1}\xi^{p-1} + \xi^p + \mu(1 + b_1\xi + ...b_{k-1}\xi^{s-1} + \xi^s) = 0$ на μ^{p-1}.

Получим $a_0\mu^{p-1} + a_1\xi\mu^{p-1} + ...a_{p-1}\xi^{p-1}\mu^{p-1} + \xi^p\mu^{p-1} + \mu^p(1 + b_1\xi + ...b_{k-1}\xi^{s-1} + \xi^s) = 0$, и перепишем в следующем виде:

$$a_0\mu^{p-1} + a_1\xi\mu^{p-1} + ...a_{p-1}\xi^{p-1}\mu^{p-1} + \mu^p(1 + b_1\xi + ...b_{k-1}\xi^{s-1} + \xi^s) = \xi^p\mu^{p-1}$$

Заметим теперь, что общее количество членов в левой части этого выражения не превышает $8k^2 2^k$, а общее количество операций для получения $\xi^p\mu^{p-1}$ - $O(k^2 2^k)$.

Теперь будем получать степени выше p+1: Снова запишем выражение

$$a_0 + a_1\xi + ...a_{p-1}\xi^{p-1} + \xi^p + \mu(1 + b_1\xi + ...b_{k-1}\xi^{s-1} + \xi^s) = 0$$

но на этот раз домножим его на $\mu^{p-1}\xi$ и получим выражение

$$a_0\xi\mu^{p-1} + a_1\xi^1\mu^{p-1} + ...a_{p-1}\xi^p\mu^{p-1} + \xi^{p+1}\mu^{p-1} + \mu^p(\xi + b_1\xi^2 + ...b_{k-1}\xi^s + \xi^{s+1}) = 0.$$

Перенесем $\xi^{p+1}\mu^{p-1}$ в правую часть и получим

$$a_0\xi\mu^{p-1} + a_1\xi^1\mu^{p-1} + ...a_{p-1}\xi^p\mu^{p-1} + \mu^p(\xi + b_1\xi^2 + ...b_{k-1}\xi^s + \xi^{s+1}) = \xi^{p+1}\mu^{p-1}.$$

На получение данного выражения потратим не более $O(k^2 2^k)$ операций.

Таким образом для получения дроби $\xi^i\mu^j$; где $i, j \geq 4k^2 2^k = T$ мы потратим не более $O(max(i - j, 0)k^2 2^k + j)$ операций.

□

Лемма 4. *$M = \{\frac{u_i}{v_i}, u_i,\ v_i \in E_2[\xi],\ v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$.*
$k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$.

Пусть мы уже построили дробь $\xi^i\mu^s$, где $i, s = 4k^2 2^k$, тогда мы можем получить многочлены $\xi^j u_0$, где $j = i, ..., i + 256k^{10}2^{6k}$, $u_0 = a_0 + a_1\xi^1 + ... + a_T\xi^T$ не более чем за $O(k^9 2^{5k})$ операций, для T справедлива оценка $T \leq 16k^4 2^{2k}$.

Доказательство. Обозначим $\mu^s = \mu_0 = \frac{u_0}{v_0}$. Напомним, что $\deg(\mu) \leq (4k^2 2^k)$, поэтому $\deg(\mu_0) \leq 16k^4 2^{2k}$.

Выпишем многочлен $v_0 = b_0 + b_1\xi^1 + ... + b_T\xi^T$, $T \leq 16k^4 2^{2k}$.

По предыдущей лемме получим дроби $\xi^i\mu_0, \xi^{i+1}\mu_0, ..., \xi^{T+i}, ...,$ $\xi^{i+16k^5 2^{3k}}\mu_0, ..., \xi^{i+256k^{10}2^{6k}+T}\mu_0$ и посчитаем необходимое количество операций. Имея дробь $\xi^l\mu_0$ мы можем получить дробь $\xi^{l+1}\mu_0$ за $O(k^2 2^k)$ операций, а значит, получение всех таких дробей до $\xi^{i+256k^{10}2^{6k}+T}\mu_0$ будет иметь сложность $O(k^{11}2^{7k})$.

Затем каждую дробь $\xi^j\mu_0$ домножим на соответствующие константы b_l и просуммируем с $\xi^j\mu_0$ с:

$$\xi^j\mu_0 + b_1\xi^{j+1}\mu_0 + b_2\xi^{j+2}\mu_0 + ... + b_T\xi^{j+T}\mu_0 =$$

$$= \xi^j\mu_0(1 + b_1\xi^1 b_2\xi^2 + ... + b_T\xi^T) =$$

$$= \xi^j\mu_0 v_0 = \xi^j u_0,$$

$$\text{где } u_0 = p_{i_1}^{j_1} p_{i_2}^{j_2} ... p_{i_s}^{j_s}$$

.

Количество используемых операций сложения и умножения для этого суммирования не превышает $\deg(v_0)$ или $O(k^4 2^{2k})$. Так как мы проделываем этот процесс для всех j от i до $256k^{10}2^{6k}$, то итоговая оценка на количество операций сложения и умножения будет $O(k^{14}2^{10k})$. □

Лемма 5. *$M = \{\frac{u_i}{v_i}, u_i,\ v_i \in E_2[\xi],\ v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$.*
$k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$. M не содержится в θ $\forall\theta, \theta \in J^{(1)}$, следовательно, $\forall i, i \in \{2, 3, ...\}\exists\mu_i \in K^{(1)}(M), \mu_i = \frac{u_i}{v_i}, (u_i, v_i) = 1, v_i p_i$. Количество операций сложения и умножения для получения μ_i - $O(k)$, количество операций обратной связи для получения μ_i не превышает одной.

Доказательство. Случай 1. Так как M целиком не содержится в предполных классах, то существует $\mu \in M$, $\mu \notin M_i^{(1)}, R_i^{(1)}$. $\mu = \frac{u}{v}$, p_i не делит u. Если p_i делит v, то доказывать нечего. Предположим, что p_i не делит v.

Случай 1а. $\mu = \frac{\xi u'}{v}, p_i$ не делит u'.

$1 + \mu^T = \frac{v^T + (\xi u')^T}{v^T}$, существует такой $T \in \mathbb{N}$, что p_i делит $v^T + (\xi u')^T$.

Пусть $\deg(p_i) = m$, тогда $v^{2^m-1} + (\xi u')^{2^m-1} \equiv 1(\mod p_i)$. Получить μ^{2^m-1} мы можем не более чем за $2m$ операций: будем получать последовательно степени μ: μ^2, μ^4, μ^8... (это займет не более m операций), а затем перемножим нужные нам степени (это также займет не больше m операций).

Теперь, применяя обратную связь к дробям $F_b(\mu, \mu^T)$ получим выражение $\frac{\mu}{1+\mu^T} = \frac{u}{v}\frac{v^T}{v^T+(\xi u')^T}$,где знаменатель делится на p_i.

Заметим, что $m \leq k$, поэтому мы получаем оценку $O(k)$ на количество операций сложения и умножения.

Случай 1б. Если $\mu(0) = 1$, то рассмотрим дробь

$$\mu' = \mu + \mu^2 = \mu(1+\mu) = \frac{u}{v}(\frac{u+v}{v}), \mu(0) = 0, \mu'(0) = 1$$

.

$\mu \notin R_i^{(1)} => p_i$ не делит u, $\mu \in M_i^{(1)} => p_i$ не делит $u+v$

p_i не делит $u(u+v)$, а значит мы свели случай 1б к случаю 1а за 1 операцию сложения и одну операцию умножения.

Случай 2.

$\exists \mu_1 \in M \setminus M_i^{(1)}, \exists \mu_2 \in M \setminus R_i^{(1)}$.

$\mu_1 \in R_i^{(1)}, \mu_2 \in M_i^{(1)}$.

$\mu_1 + \mu_2 = \mu, \mu \notin R_i^{(1)}, \mu \notin M_i^{(1)}$, иначе бы $\mu + \mu_1 = \mu_2$ принадлежал бы $R_i^{(1)}$. $\deg(\mu)$ в данном случае не превышает $k2^k$. Таким образом за одну операцию сложения мы сводим случай 2 к случаю 1.

По итогу, для получения требуемой дроби мы тратим не более 1 операции обратной связи и $O(k)$ операций сложения и умножения.

□

Лемма 6. *$M = \{\frac{u_i}{v_i}, u_i, v_i \in E_2[\xi], v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$.*
$k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$. Если существует многочлены $\xi^i u'$,
$...\xi^{i+256k^{10}2^{6k}}u'$, такие, что степень $\deg(u') \leq 16k^4 2^{2k}$, а сам многочлен u' имеет вид $u' = p_{i_2}^{j_2} \cdot p_{i_3}^{j_3} ... \cdot p_{i_l}^{j_l}$ и такое натуральное число i_1, что $\forall i \geq i_1$ выполнено: $\xi^i u' \in K^{(1)}(M)$, то количество операций для получения ξ^i не превышает $O(k^{18}2^{10k})$.

Доказательство. Пусть у нас есть многочлен $\xi^i u', i \geq j_1, ..., u' = p_{i_2}^{j_2} \cdot ...p_{i_l}^{j_l}$, количество операций для получения этого многочлена посчитано ранее, в леммах 2, 3.

По лемме 5 мы можем получить дробь $\mu_2 = \frac{u_2}{v_2}, (u_2, v_2) = 1, v_2 p_{i_2}$ за $O(k)$ операций. Из леммы 5 видно, что степень μ_2 не превосходит $k2^k$.

Домножим $\xi^i u'$ на $\mu_2^{j_2}$ и получим дробь $\xi^i \frac{u_2'}{v_2'} \in K^{(1)}(M)$, где p_{i_2} не делит u_2', $i \in \mathrm{N}$, $i \geq j_1$, j_2 не превосходит $\deg(u')$, а $\deg(u')$ в свою очередь не превосходит $16k^4 2^{2k}$. Следовательно, степень дроби $\frac{u_2'}{v_2'}$ не превосходит $16k^5 2^{3k}$. Из дробей $\xi^i \frac{u_2'}{v_2'}, ..., \xi^{i+16k^5 2^{3k}} \frac{u_2'}{v_2'}$, используя метод из леммы 4, мы можем получить многочлен $\xi^i u_2'$. Количество операций не будет превышать $\deg(v_2')$, а степень u_2' по итогу не будет превышать

$16k^5 2^{3k}$. Помимо многочлена $\xi^i u'_2$ нам необходимо получить степени $\xi^j u'_2$, $j = i, ..., i + 256k^{10}2^{6k}$, это потребуется в дальшейшем доказательстве. Сделать это мы можем за $O(k^{14}2^{8k})$ операций.

Аналогичным образом получим многочлены $u'_t, t = 3, .., l$, где каждый из многочленов не делится на p_{i_t} и потратим на это не более $O(lk^{14}2^{8k})$ операций.

НОД$(u', u'_2, ..., u'_l)$=1, а значит существуют многочлены $v_1, ..., v_l \in E_2[\xi]$ такие, что $v_1 u' + v_2 u'_2 + ... + v_l u'_l = 1$.

Обозначим $v_i(j)$ коэффициент перед многочленом u'_i на j-й итерации расширенного алгоритма Евклида, который мы будем применять ниже. На первом шаге которого найдем расширенный

$$\textbf{НОД}(u'\xi^i, u'_2\xi^i) = R(1)\xi^i$$
$$v_1(1)u'\xi^i + v_2(1)u'_2\xi^i = R(1)\xi^i, p(\xi, 1) = v_1(1),$$

т.е. $p(\xi, j)$ - многочлен перед первым слагаемым в результате работы расширенного алгоритма Евклида. Далее получаем

$$\textbf{НОД}(R(1)\xi^i, u'_3\xi^i) = R(2)\xi^i$$
$$p(\xi, 2)R(1)\xi^i + v_3(2)u'_3\xi^i = R(2)\xi^i$$
$$v_1(2)u'\xi^i + v_2(2)u'_2\xi^i + v_3(2)u'_3\xi^i = R(2)\xi^i$$
$$v_1(2) = v_1(1)p(\xi, 1), v_2(2) = v_2(1)p(\xi, 1)$$
$$\deg(p(\xi, j)) + deg(v_i(j)) \leq (j + 1)(16k^5 2^{3k}).$$

Видно, что итоговая степень v_i не превосходит $256k^1 02^{10k}$, и эти необходимые нам степени многочленов $\xi^j u'_s$, $j = i, ..., i + 256k^{10}2^{6k}, s = 1, ..., l$ были получены нами ранее. На последней итерации алгоритма, таким образом, будем иметь нужное нам многочлен:

$$v_1 u'\xi^i + v_2 u'_2\xi^i + ... + v_l u'_l\xi^i = \xi^i.$$

Вычисление каждого из итоговых $v_i(l)$ будет занимать не более $O(k^{10}2^{6k})$ операций. А итоговое количество операций ссложения и умножения для получения v_i будет не более $O(l(k^{10}2^{5k})$. Поскольку $l \leq (16k^4 2^{2k})$, то при уже построенных многочленах $\xi^j u'_s$, $j = i, ..., i + 256k^{10}2^{6k}, s = 1, ..., l$ сложность получения **НОД** не превосходит $O((k^{12}2^{8k}))$. Сложность построения этих многочленов мы оценивалии ранее как $O(lk^{14}2^{8k})$. Подставляя в эту оценку $l = (16k^4 2^{2k})$, получаем итоговую сложность получения ξ и в $O(k^{18}2^{10k})$.

□

Лемма 7. *$M = \{\frac{u_i}{v_i}, u_i,\ v_i \in E_2[\xi],\ v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$.*
$k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$.
Если $M \not\subseteq \theta\ \forall \theta \in J^{(1)}$, то $\forall m \in \mathbb{N}, \forall u \in E_2[\xi] : \deg(u) < m, \exists \mu \in E_2'(\xi)$, что $u + \xi^m\mu \in K^{(1)}(M)$, где $\xi^m\mu = a_0\xi^m + a_1\xi^{m+1} + a_2\xi^{m+2} + ...$ Дробь $u + \xi^m\mu$ может быть получена за $O(m)$ операций.

Доказательство.

$$\mu \in M \setminus R_1^{(1)} => \mu(0) = 1,$$

$$\mu = 1 + a_1\xi + a_2\xi^2 + ... + a_i\xi^i + ...$$

$$\mu^2 = 1 + a_1\xi^2 + a_2\xi^4 + ... + a_i\xi^{2i} + ...$$

$$\mu^{2^\tau} = 1 + a_1\xi^{2^\tau} + a_2\xi^{2\cdot 2^\tau} + ... = 1 + \xi^{2^\tau}\mu'.$$

Мы можем выбрать $\tau = \lceil \log_2 m \rceil$ и таким образом для $u = 1$ получаем, что $1 + \xi^{\lceil \log 2m}\mu_1 \in K^1(M)$, применяя $\lceil \log_2 m \rceil$ операций умножения.

Выберем $\mu_1' \in M \setminus M_1^{(1)} => \mu_1' + \mu_1'(0) = \xi + b_2\xi^2 + ...$

$$\hat{\mu_1} = \begin{cases} \mu_1', & \text{если } \mu_1(0) = 0 \\ \mu_1' + (1 + \xi^n\mu_1) & \text{если } \mu_1(0) = 1 \end{cases}$$

Для $m = 1$ мы уже все доказали, докажем для $m > 1$.
$\hat{\mu} = \xi + c_2^1\xi^2 + ...$
$\hat{\mu}_s = (\hat{\mu})^s, s = 1, ..., m-1.$
$\hat{\mu}_s = \xi^s + c_{s+1}^s\xi^{s+1} + ...$
$\hat{\mu}_s = \xi^s + \xi^{s+1}\tilde{\mu}_s.$
Эти дроби мы получаем используя $O(m)$ операций.
$\xi + \xi^m\tilde{\mu} \in K^{(1)}(\{\xi^k + \xi^{k+1}\tilde{\mu} | k = 1, ..m-1\})$. Многочлен $\xi + \xi^m$ может быть получен за $O(m)$ операций.

Доказательство. Будем доказывать по индукции.
При $m = 2$ все доказано. Докажем переход индукции $m - 1 \to m$.
$\xi + \xi^{m-1}\tilde{\tilde{\mu}}_m \in K^{(1)}(M)$ по предположению индукции.
Если $\tilde{\tilde{\mu}}_m(0) = 0$, то $\tilde{\tilde{\mu}}_m = \xi\mu_m''$, а значит $\xi + \xi\mu_m'' \in K^{(1)}(M)$.
Если $\tilde{\tilde{\mu}}_m(0) = 1$, то $\xi + \xi^{m-1}\tilde{\tilde{\mu}}_m + (\xi^{m-1} + \xi^m\tilde{\mu}_{m-1}) = \xi + \xi^m\mu^*$. □

Итак, нам необходимо получить $u + \xi^m\mu$, где $\deg(u) < m, \mu \in E_2'(\xi)$.
$u = a_0 + a_1\xi + a_2\xi^2 + ...a_{m-1}\xi^{m-1}$.
Мы можем получить следующее выражение: $a_0(1 + \xi^m\mu_0^*) + a_1(\xi + \xi^m\mu_1^*) + a_2(\xi + \xi^m\mu_2^*) + a_{m-1}(\xi^{m-1} + \xi^m\mu_{m-1}^*) = a_0 + a_1\xi + a_2\xi^2 + ...a_{m-1}\xi^{m-1} + \xi^m(\mu_0^* + \mu_1^* + ... + \mu_{m-1}^*) = u + \xi^m\mu^*$.
Всего на получение $u + \xi^m\mu^*$ мы потратили не более $O(m)$ операций.
□

Теорема 1. *Пусть у нас есть множество* $M = \{\frac{u_i}{v_i}, u_i,\ v_i \in E_2[\xi], v(0) = 1, i = 1, ...n\}, n \in \mathbb{N}$. $k = \max\{\deg(\mu_1), \deg(\mu_2), ..., \deg(\mu_n)\}$. $K^{(1)}(M) = E_2'(\xi)$. *Тогда для того, чтобы из* M *получить элементарный базис* $\{1, \xi\}$ *нам необходимо не более* $O(k^{18}2^{10k}+nk^2)$ *операций сложения и умножения, а также не более 7 операций обратной связи.*

Доказательство. Для $i = 16k^4 2^{2k}$ по лемме 6 мы можем получить $\xi^i \in K^{(1)}(M)$ за $O(k^{18}2^{10k}+nk^2)$ операций сложения и умножения, количество операций обратной связи - не более 4.

Запишем произвольную дробь вида $\mu = u + \xi^i \mu'$ из $E_2'(\xi)$, где $u \in E_2[\xi], \deg(u) < i, \mu' \in E_2'(\xi)$.

По лемме 7 мы можем получить $u + \xi^i \mu''$ за $O(i)$ операций. И теперь перезапишем $\mu = (u + \xi^T \mu'') + (\xi^T \mu'' + \xi^T \mu')$.

$\xi^T \mu'' + \xi^T = \xi^T(\mu'' + \mu') = \frac{\xi^T u}{v}$.

$v \in E_2'[\xi], v(0) = 1 => \exists s \in \mathbb{N}, \exists v' \in E_2'[\xi], vv' = 1 + \xi^s$.

По модулю v не более чем $2^{16k^4 2^{2k}}$ остатков, а значит этот остаток v' мы можем получить не более чем за $O(k^4 2^{2k})$ операций.

$(1 + \xi^s)^{2^\tau} = 1 + \xi^{s2^\tau}$.

$v'(1 + \xi^s)^{2^{\tau+1}} => vv'(1 + \xi^s)^{2^{\tau+1}} = 1 + \xi^{s2^\tau}$. Выберем τ таким, чтобы $\tau \leq i$.

$\frac{\xi^i u}{v} = \frac{\xi^i uv'}{vv'} = \frac{\xi^i uv'}{1+\xi^s} = Fb(\xi^T uv, \xi^s) => \mu \in K^{(1)}(M)$.

Тем же самым способом построим дробь $\mu + \xi$. Складываем μ и $\mu + \xi$ и получаем многочлен ξ. Аналогично, мы можем получить дробь $\mu + 1$, а затем получить единицу. Для получения μ, $\mu + \xi$, $\mu + 1$ нам потребуется не более трех операций обратной связи.

Общее количество операций сложения и умножения составляет $O(k^{12}2^{6k}+nk^2)$, а общее количество операций обратной связи - не больше 7.

□

Заключение.

Таким образом получены оценки на получение простейших функций из множества рациональных дробей над полем E_2. Дальнейшее направление данной работы представляется нам довольно очевидным: вывод оценок для полных подмножеств множества линейно-автоматных функций, проверка работоспособности выведенных соотношений для дробей над произвольными числовыми полями.

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.

Comlexity of implementation of elementary basis in one-place lineary automata class that preserves zero sequence

Ilin I.Y.

For now some facts about completeness of linear automata are proven. We now know about every precomlete class on superposition operetion and composition operation, the completeness criterions are also had been formulated. In this work we have proven some facts about the complexity of this process: to receive neutral element and delay.

Keywords: linear automata, comlexity estimation.

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.