Московский Государственный Университет
им. М.В. Ломоносова
Российская Академия Наук
Академия Технологических Наук России
Российская Академия Естественных Наук

Интеллектуальные Системы.

Теория и приложения

ТОМ **22** ВЫПУСК 1 * **2018**
МОСКВА

ISSN 2411–4448

УДК 519.95; 007:159.955
ББК 32.81

Издается с 1996 г.*

В журнале «Интеллектуальные системы. Теория и приложения» публикуются научные достижения в области теории и приложений интеллектуальных систем, новых информационных технологий и компьютерных наук.

Издание журнала осуществляется под эгидой МГУ им. М. В. Ломоносова, Научного Совета по комплексной проблеме «Кибернетика» РАН, Отделения «Математическое моделирование технологических процессов» АТН РФ, Секции «Информатики и кибернетики» РАЕН.

Учредитель журнала: ООО «Интеллектуальные системы».

Журнал входит в список изданий, включенных ВАК РФ в реестр публикаций материалов по кандидатским и докторским диссертациям по математике и механике.

Спонсором издания является:

ООО «Два Облака»
Разработка корпоративных информационных систем
http://www.dvaoblaka.ru

Индекс подписки на журнал: 64559 в каталоге НТИ «Роспечать».

Адрес редакции: 119899, Россия, Москва, Воробьевы Горы, МГУ, ГЗ, механико-математический факультет, комн. 12-01.
Адрес издателя: 115230, Россия, Москва, Хлебозаводский проезд, д. 7, стр. 9, офис 9. Тел. +7 (495) 939-46-37, e-mail: mail@intsysjournal.org

*) Прежнее название журнала: «Интеллектуальные системы».

ОГЛАВЛЕНИЕ

Часть 1.
Специальные вопросы теории интеллектуальных систем

О классе нейронных функций с двоично-рациональными параметрами

Агафонова М.В.

В работе рассматривается класс нейронных кусочно-параллельных функций с двоично-рациональными коэффициентами. Доказано что для любой функции из класса кусочно-параллельных функций существует функция из класса кусочно-параллельных функций с двоично-рациональными коэффициентами, приближающая ее с наперед заданной точностью. Также, для рассматриваемого класса функций показано, что существуют базисы, состоящие из заданного (произвольного) числа элементов, в частности, найдена Шефферова функция.

Ключевые слова: класс кусочно-параллельных функций, класс нейронных функций с двоично-рациональными коэффициентами, операции суперпозиции, Шефферова функция, базисы.

1. Введение.

В данной работе рассматривается класс кусочно-параллельных функций с двоично-рациональными коэффициентами (BPP), являющийся аппроксимирующим для рассмотренного в работе [1] класса кусочно-параллельных функций (PP). Основной темой исследования работы [1] является изучение, так называемых нейронных схем. Под понятием нейронная схема понимается математический объект, представляющий из себя набор функциональных элементов, определенных строением модели исследуемой нейронной сети, а также функциональные схемы, полученные из них операциями суперпозиции. Где под суперпозицией понимаются операции: добавления фиктивного входа, изъятия фиктивного входа, склеивания входов, переименования входов без склеивания, последовательного соединения [1]. Стоит отметить, что данное построение происходит по аналогии с построением автоматных схем [2].

Особый же интерес в работе [1] представляет доказательство совпадения множеств функций, реализуемых нейронными схемами, с некоторы-

ми классами кусочно-линейных функций, изучение которых в дальнейшем и ведется. Так, например, устанавливается эквивалентность между множеством функций, реализуемых нейронными схемами без памяти, и множеством кусочно-линейных функций (PL), эквивалентность множества функций, реализуемых нейронными схемами модели Мак-Каллока-Питтса[3], множеству кусочно-параллельных функций (PP).

Изучение класса кусочно-линейных функций (PL) получило развитие в работе [4]. В настоящей же работе, находит свое развитие изучение подкласса кусочно-параллельных функций PP. Рассматриваемый класс, являющийся замыканием [5] множества B, $B = \{\frac{1}{2}x, -x, x+y, \theta(x)\}$, будем называть классом кусочно-параллельных функций с двоично-рациональными коэффициентами, и обозначать BPP. Интерес изучения класса BPP состоит в том, что он является конечно-порожденным, в отличие от ранее рассматриваемых классов в работах[1], [4]. В настоящей работе показано, что для любой функции из класса PP существует функция из класса BPP, приближающая ее с наперед заданной точностью. Далее, абстрагируясь от смысловой интерпретации этих функций, рассматриваются задачи типичные для всех функциональных систем [6]. Устанавливается существование Шефферовой функции[5]. Такой функцией является: $F(x,y,z) = x - \frac{1}{2}y - \frac{1}{2}\theta'(z) + \frac{1}{2}$, где $\theta'(z) = \begin{cases} 1 & \text{при } z > 0 \\ 0 & \text{при } z \leq 0 \end{cases}$.

Доказано существования в классе BPP базиса из k элементов для произвольного натурального числа k.

2. Основные определения.

Определение1. Множество кусочно-параллельных функций, определяется следующим выражением:

$PP = \{f | f = f_c + f_l, f_c \in PC, f_l \in L\}$, где PC – множество всех кусочно-постоянных функций, L – множество всех линейных функций [1]

Рассмотрим множество функций $B = \{\frac{1}{2}x, -x, x+y, \theta(x)\}$, в котором $x \in \mathbb{R}, y \in \mathbb{R}$. В множестве B содержатся функции: умножитель на двоично-рациональную константу $f_1(x) = \frac{1}{2}x$, отрицание $f_2(x) = -x$, сумматор $f_3(x,y) = x + y$, функция Хэвисайда $\theta(x) = \begin{cases} 1 & \text{при } x \geq 0 \\ 0 & \text{при } x < 0 \end{cases}$.

Определение 2. Замыкание функций, принадлежащих множеству $B = \{\frac{1}{2}x, -x, x+y, \theta(x)\}$, по операциям суперпозиции [1],[4] назовем множе-

ством кусочно-параллельных функций с двоично-рациональными коэффициентами и обозначим BPP.

$$[B] = BPP.$$

Данное замыкание содержит все целые и двоично-рациональные константы. Так константа $\frac{1}{2}$ может быть получена подстановкой: $\frac{1}{2}(\theta(\theta(x))$. Константа 1 получается из f_3 подстановкой: $f_3(\frac{1}{2}, \frac{1}{2}) = 1$. Все положительные целые числа можно получить также из f_3 : $f_3(1, n-1) = 1 + (n-1)$. Произведя затем, подстановки вида:$f_2(n) = -n$, получим все целочисленные константы. Двоично-рациональные константы могут быть получены при помощи подстановок функций $f_1(\frac{1}{2^{k-1}}) = \frac{1}{2}(\frac{1}{2^{k-1}}) = \frac{1}{2^k}$ и $f_3(\frac{1}{2^k}, \frac{m-1}{2^k}) = \frac{m}{2^k}$.

3. Теорема о приближении с наперед заданной точностью функций, принадлежащих классу PP, функциями класса BPP.

Определение 3. Пусть $g(x_1, x_2, \ldots, x_n) \in$ PP, $f(x_1, x_2, \ldots, x_n) \in$ BPP. Функция $f(x_1, x_2, \ldots, x_n)$ приближает функцию $g(x_1, x_2, \ldots, x_n)$ на множестве $A = [0,1]^n$ с точностью ε,если $\forall\ n\ \exists\ A^{'} \subseteq [0,1]^n$ такое что $|A^{'}| > 1 - \varepsilon$ и $\forall (x_1, x_2, \ldots, x_n) \in A^{'} : |f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n)| < \varepsilon$.

Теорема 1. *$\forall g(x_1, x_2, \ldots, x_n) \in PP\ \forall\ \varepsilon\ \exists\ f(x_1, x_2, \ldots, x_n) \in BPP$, которая приближает g на множестве $A = [0,1]^n$ с точностью ε.*

Доказательство: Сначала определим $A^{'} \subseteq [0,1]^n$.
Функцией $g(x_1, x_2, \ldots, x_n) \in$PP, порождается k гиперплоскостей $l_1, \ldots, l_k$ разбивающих R^n на классы эквивалентности $R_1, \ldots, R_s, (k, s \in \mathbb{N})$. Обозначим через $k^{'}(k^{'} \in 1, \ldots, k)$ – количество гиперплоскостей $l_1, \ldots, l_{k'}$, пересекающих рассматриваемый единичный гиперкуб A.

При $k^{'} = 0, \forall n$, положим $A^{'} = A$. Построим множество $A^{'}$ при $k^{'} = 1$, и затем обобщим для любого $k^{'} \in \{1, \ldots, k\}$. Рассмотрим случаи $n = 1, n = 2$ и потом индуктивно построим $A^{'}$ для произвольного n.

Случай $k^{'} = 1, n = 1$. То есть множество A представляет собой отрезок $[0,1]$, имеется одна разделяющая гиперплоскость, допустим проходящая через точку $B \in [0,1], B \in \mathbb{R}$. Если B лежит внутри интервала $(0,1)$, то приблизим B двоично-рациональными числами $B^{'}$ и $B^{''}$ слева и с права соответственно, такими, что $|B - B^{'}| \leq \frac{\delta}{2}, |B - B^{''}| \leq \frac{\delta}{2}$. (рис. 1). Тогда

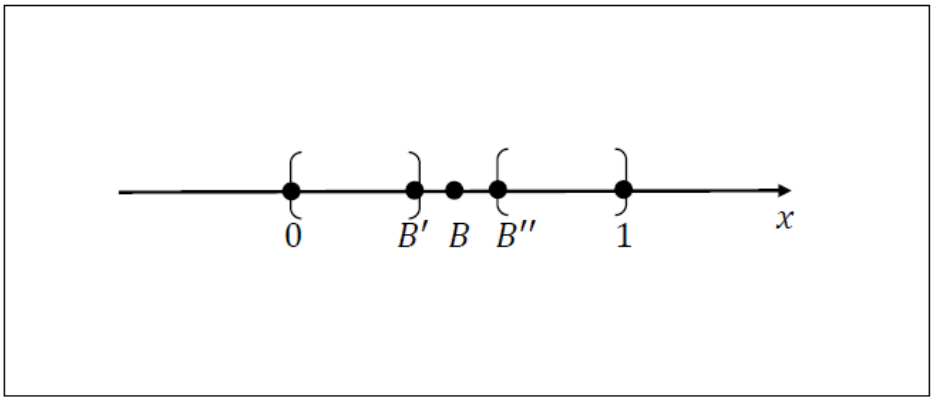

Рис. 1.

в качестве $A^{'}$ рассмотрим объединение множеств $[0, B^{'}] \cup [B^{''}, 1]$. Заметим, что для любого наперед заданного $\varepsilon > 0$ при $\delta < \varepsilon$, $|A^{'}| > 1 - \varepsilon$. Следовательно положим $A^{'} = [0, B^{'}] \cup [B^{''}, 1]$. Если точка B лежит на одном из концов отрезка $[0, 1]$, т.е. ее координатами будут целые числа либо 0, либо 1 соответственно. Поскольку, классу BPP принадлежит множество всех целочисленных констант, можно принять $B^{'} = 0 (B^{'} = 1), B^{''} = 0 (B^{''} = 1)$ и так как $|B - B^{'}| = 0, |B - B^{''}| = 0$, положить $A^{'} = A$. И следовательно свести этот случай к случаю $k = 0$. Стоит отметить, что так же можно поступить и когда B принимает любые двоично-рациональные координаты внутри отрезка $[0, 1]$.

Случай $k^{'} = 1, n = 2$, представляет больший интерес. Множество A в этом случае – это квадрат с единичной стороной. Разделяющая множество A гиперплоскость l, на A представляет отрезок прямой, лежащий внутри этого квадрата. Обозначим его BC. (рис.2). Случай, если отрезок лежит на одной из сторон, аналогичен предыдущему случаю, когда точка B совпадала с одним из концов отрезка. Диагональ квадрата обозначим OD. Длина отрезка $BC \leq OD$, в зависимости от его расположения (равенство достигается при совпадении BC с OD). Приблизим точки $B, C \in \mathbb{R}$ точками $B^{'}, B^{''}$ и $C^{'}, C^{''}$ соответственно. Причем $B^{'}, B^{''}, C^{'}, C^{''} \in \{\frac{m}{2^k}, m, k \in \mathbb{N}\}$, $|B - B^{'}| \leq \frac{\delta}{2}, |B - B^{''}| \leq \frac{\delta}{2}, |C - C^{'}| \leq \frac{\delta}{2}, |C - C^{''}| \leq \frac{\delta}{2}$. В зависимости от расположения BC, получим трапецию $B^{'}B^{''}C^{'}C^{''}$ с высотой $B^{'}E < B^{'}B^{''} = \delta$ и основаниями $B^{'}C^{'} = B^{'}C^{''} < OD$ или прямоугольник со сторонами $B^{'}B^{''} = C^{'}C^{''} = \delta$ и $B^{'}C^{'} = B^{'}C^{''} = BC$. Диагональ OD также достроим до прямоугольника $O^{'}O^{''}D^{'}D^{''}$ как показано на рисунке 2. $O^{'}O^{''} = D^{'}D^{''} = \delta, O^{'}D^{'} = O^{''}D^{''} = OD$.Заметим,

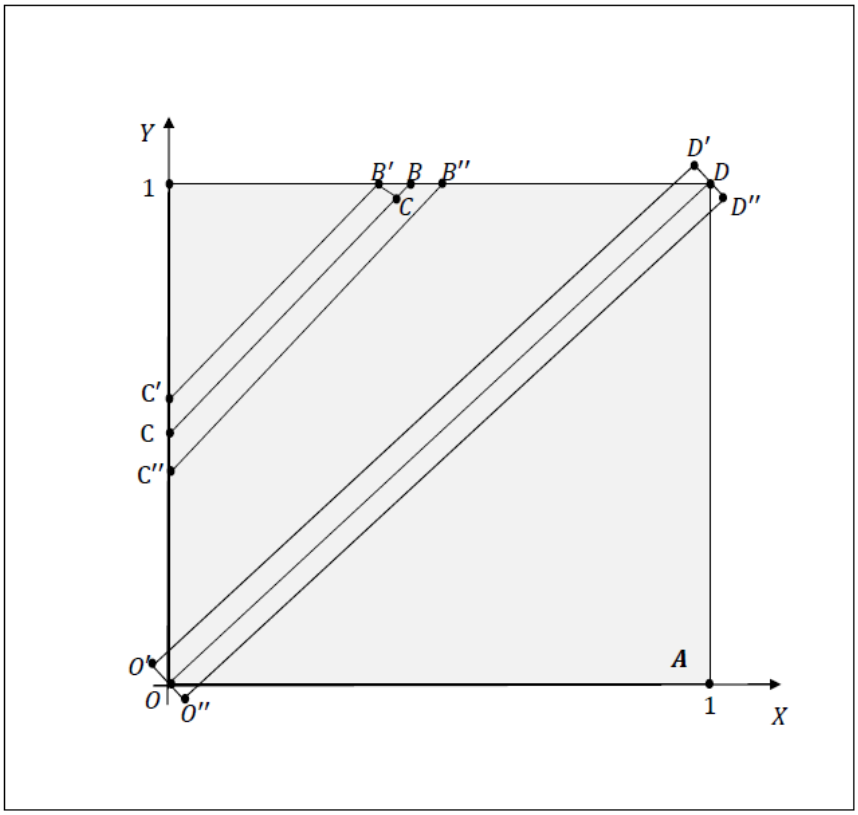

Рис. 2.

что $|O^{'}D^{'}| = \sqrt{2}$. Из соотношения BC≤OD, следует, что

$$S_{B'B''C'C''} \leq S_{O'O''D'D''} = |O^{'}D^{'}| \cdot |O^{'}O^{''}| = \sqrt{2}\delta < \varepsilon.$$

Следовательно при $\delta < \frac{\varepsilon}{\sqrt{2}}$ множество $A^{'} = A \backslash S_{B'B''C'C''}, |A^{'}| > 1 - \varepsilon$.

Теперь обобщим этот случай для произвольного n (при $k' = 1$). Сечение n-мерного куба, будет иметь размерность $(n-1)$. Его пересечение с гранью n-мерного куба будет иметь размерность $(n-2)$. Гиперплоскость l будет проходить через одно из таких сечений. Рассмотрим внутри n – мерного куба A $(n-1)$-мерный многогранник с $(n-2)$-мерными сторонами представляющий это сечение соответствующее l. Причем каждая грань единичного n-мерного куба A представляет собой также единичный $(n-1)$-мерный куб. Например для $n = 3$ сечение, соответствующее l будет иметь вид многоугольника стороны которого являются отрезка-

ми лежащими на гранях A, в свою очередь являющихся кубами меньшей размерности т.е. квадратами для $n = 3$. Для построения $A^{'}$ для n-мерного куба A, необходимо оценить объем Δ максимально возможного $(n-1)$-мерного сечения в A, затем приблизить его сечениями $\Delta^{'}, \Delta^{''}$ имеющими двоично рациональные координаты и такими, что:

$$|x_i - x_i^{'}| < \frac{\delta}{2}, |x_i - x_i^{''}| < \frac{\delta}{2}, \forall x_i \in \Delta, \forall x_i^{'} \in \Delta^{'}, \forall x_i^{''} \in \Delta^{''}.$$

Оценим объем Δ максимально возможного $(n-1)$-мерного сечения в n-мерном кубе A, отталкиваясь от идеи, что это будет $(n-1)$-мерный многогранник, со сторонами лежащими в $(n-1)$-мерных единичных кубах. Объём этого многогранника, будет меньше или равен объему $(n-1)$-мерного куба, с максимально возможными гранями лежащими в $(n-1)$-мерных кубах, являющихся гранями A. Максимально возможные грани в кубе можно оценить его диагональю равной $\sqrt{n}$.

$$S_\Delta \leq (\sqrt{n})^{n-1}, n \geq 2.$$

Учитывая , приближения $\Delta^{'}, \Delta^{''}$, заметим, что $S_{\Delta^{'},\Delta^{''}}$ равна произведению высоты, в качестве которой мы возьмем δ, на основание, т.е. S_Δ,следовательно получим оценку для$S_{\Delta^{'},\Delta^{''}}$:

$$S_{\Delta^{'},\Delta^{''}} \leq (\sqrt{n})^{n-1}\delta < \varepsilon.$$

Следовательно, для $n \geq 2$, при $\delta < \frac{\varepsilon}{(\sqrt{n})^{n-1}}$, множество $A^{'} = A \backslash S_{\Delta^{'},\Delta^{''}}, |A'| > 1 - \varepsilon$.

Наконец обобщим результат для произвольного $k^{'}$. Тогда в качестве $A^{'}$ рассмотрим множество $A \backslash k^{'} S_{\Delta^{'},\Delta^{''}}$, тогда $|A^{'}| > |A| - k^{'}|S_{\Delta^{'},\Delta^{''}}| = 1 - k^{'}(\sqrt{n})^{n-1}) \cdot \delta$, и при $\delta < \frac{\varepsilon}{k \cdot (\sqrt{n})^{n-1})}, |A^{'}| > 1 - \varepsilon$. Отдельно стоит отметить, что в случае, $k^{'} > 1$ возможно, что концы отрезка для $n = 2$ и грани многогранника в случае $n > 2$ представляющего l, не будут лежать на гранях A. В этом случае продолжим многогранник по плоскости сечения соответствующего l (отрезок продолжим по прямой на которой он лежит) до пересечения с гранями A. Очевидно это только увеличит его объём и следовательно, найденная оценка сохранится.

Теперь построим такую функцию $f(x_1, x_2, \ldots, x_n) \in BPP$,что $\forall (x_1, x_2, \ldots, x_n) \in A^{'} : |f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n)| < \varepsilon$. Пусть на некотором классе $R_i, i \in \{1, \ldots, s\}$, имеет место равенство:

$$g(x_1, x_2, \ldots, x_n) = c_n x_n + c_{n-1} x_{n-1} + \cdots + c_0, c_i \in \mathbb{R}.$$

Тогда рассмотрим пересечение: $R_i \cap A'$. Это множество задается пересечением гиперплоскостей. Определим на нем функцию:

$$f(x_1, x_2, \ldots, x_n) = d_n x_n + d_{n-1} x_{n-1} + \cdots + d_0, d_i \in \{\frac{m}{2^k}, m, k \in \mathbb{N}\}, 0 \leq x_i \leq 1,$$

приближающую $g(x_1, x_2, \ldots, x_n)$. Пусть $|c_i - d_i| < \frac{\varepsilon}{n+1} = \delta^{'}, \forall i$. Так как $0 \leq x_i \leq 1$:

$$|c_i x_i - d_i x_i| \leq |c_i - d_i||x_i| \leq 1 \frac{\varepsilon}{n+1} \leq \frac{\varepsilon}{n+1}.$$

Следовательно

$$|c_n x_n + c_{n-1} x_{n-1} + \cdots + c_0 - d_n x_n - d_{n-1} x_{n-1} - \cdots - d_0| \leq$$

$$|c_n x_n - d_n x_n| + |c_{n-1} x_{n-1} - d_{n-1} x_{n-1}| + \cdots + |c_0 - d_0| \leq$$

$$\frac{\varepsilon}{n+1} + \frac{\varepsilon}{n+1} \cdots + \frac{\varepsilon}{n+1} \leq \varepsilon$$

Следовательно при $\delta^{'} \leq \frac{\varepsilon}{n+1}$, выполняется неравенство:

$$|f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n)| < \varepsilon$$

Теорема доказана.

4. Существование в классе функций BPP базиса размерности равной любому наперед заданному натуральному числу k.

Сам класс BPP, представляет множество кусочно-линейных функций от n переменных, с двоично-рациональными коэффициентами и возможными разрывами 1го рода. В соответствии с леммой о нелинейной глубине[1], все функции класса BPP представляются в виде:

$$(*) f(x_1, x_2, \ldots, x_n) = \frac{k_1}{2^{m_1}} x_1 + \frac{k_2}{2^{m_2}} x_2 + \cdots + \frac{k_i}{2^{m_i}} x_i +$$

$$+ \frac{k_{i+1}}{2^{m_{i+1}}} \theta(\omega_1) + \cdots + \frac{k_j}{2^{m_j}} \theta(\omega_s) + \frac{k_0}{2^{m_0}}$$

где, $0 \leq i \leq N, i \leq j \leq N$,
$k_1, k_2, \ldots k_N \in \mathbb{Z}, (N \leq n)$,

$m_1, m_2, \dots m_N \in \mathbb{N}, (N \le n)$,
$0 \le l \le s$,
$0 \le s \le n - i$,

$$\theta(\omega_l) = \theta(\frac{k_{l0}^{'}}{2^{m_0^{'}}} + \frac{k_{l1}^{'}}{2^{m_1^{'}}} x_1 + \frac{k_{l2}^{'}}{2^{m_2^{'}}} x_2 + \dots + \frac{k_{li'}^{'}}{2^{m_{i'}^{'}}} x_{i'} + \frac{k_{li+1}^{'}}{2^{m_{i+1}^{'}}} x_{i+1}^{l} + \frac{k_{li+2}^{'}}{2^{m_{i+2}^{'}}} x_{i+2}^{l} +$$
$$\dots + \frac{k_{l'}}{2^{m_{j'-1}^{'}}} x_{j'-1}^{l} + \frac{k_{j'}}{2^{m_{j'}^{'}}} \theta(\omega_{l1}) + \dots + \frac{k_{t'}}{2^{m_{t'}^{'}}} \theta(\omega_{ls'}))$$

$$\theta(\omega_{li'}) = \theta(\frac{k_{li'0}^{'}}{2^{m_0^{'}}} + \frac{k_{li'1}^{'}}{2^{m_1^{'}}} x_1 + \frac{k_{li'2}^{'}}{2^{m_2^{'}}} x_2 + \dots + \frac{k_{li'i}^{'}}{2^{m_i^{'}}} x_i + \frac{k_{li'i+1}^{'}}{2^{m_{i+1}^{'}}} x_{i+1}^{li'} + \frac{k_{li'i+2}^{'}}{2^{m_{i+2}^{'}}} x_{i+2}^{li'} +$$
$$\dots + \frac{k_{li'j'-1}^{'}}{2^{m_{j'-1}^{'}}} x_{i'})$$

$k_{l0}^{'}, k_{l1}^{'}, \dots, k_{t}^{'} \in \mathbb{Z}, (N \le n)$
$k_{li'0}^{'}, k_{li'1}^{'}, \dots, k_{li'j'-1}^{'} \in \mathbb{Z}, (N \le n)$
$m_1^{'}, m_2^{'}, \dots, , m_t^{'} \in \mathbb{N}, (N \le n), 0 \le t \le s, 0 \le j^{'} - 1 \le n, 0 \le i^{'} \le i$,
$i + \sum_l (j^{'} - 1 - i^{'}) + \sum_{l'} (j^{'} - 1 - i^{'}) = n$

4.1. Шефферова функция для класса BPP.

Теорема 2. *В классе BPP, функция* $F(x, y, z) = x - \frac{1}{2}y - \frac{1}{2}\theta^{'}(z) + \frac{1}{2}$, *где* $\theta^{'}(z) = \begin{cases} 1 & \text{при } z > 0 \\ 0 & \text{при } z \le 0 \end{cases}$. , *является шефферовой.*

.

Доказательство: Сначала получим константу $\frac{1}{2}$. Для этого рассмотрим суперпозицию:

$F_1(x, y, z) = F(F(x, y, z), y, z) = x - \frac{1}{2}y - \frac{1}{2}\theta^{'}(z) + \frac{1}{2} - \frac{1}{2}y - \frac{1}{2}\theta^{'}(z) + \frac{1}{2} = x - y - \theta^{'}(z) + 1$. Отождествим переменные x и y: $F_2(z) = F_1(x, x, z) = x - x - \theta^{'}(z) + 1 = -\theta^{'}(z) + 1 = 1 - \theta^{'}(z)$.

Далее применим операцию суперпозиции для F и $F_2(z)$:

$F_3 = F(F_2(z), F_2(z), F_2(z)) = 1 - \theta^{'}(z) - \frac{1}{2}(1 - \theta^{'}(z)) - \frac{1}{2}\theta^{'}(1 - \theta^{'}(z)) + \frac{1}{2} = 1 - \theta^{'}(z) - \frac{1}{2} + \frac{1}{2}\theta^{'}(z) - \frac{1}{2}\theta^{'}(1 - \theta^{'}(z)) + \frac{1}{2} = 1 - \theta^{'}(z) + \frac{1}{2}\theta^{'}(z) - \frac{1}{2}\theta^{'}(1 - \theta^{'}(z))$.

Рассмотрим чему равно $\theta^{'}(1 - \theta^{'}(z))$. Так как $\theta^{'}(1 - \theta^{'}(z)) = \begin{cases} 0 & \text{при } z > 0 \\ 1 & \text{при } z \le 0 \end{cases}$.

и одновременно $1 - \theta^{'}(z) = \begin{cases} 0 & \text{при } z > 0 \\ 1 & \text{при } z \le 0 \end{cases}$, значит $\theta^{'}(1 - \theta^{'}(z)) = 1 - \theta^{'}(z)$. И следовательно $F_3 = 1 - \theta^{'}(z) + \frac{1}{2}\theta^{'}(z) - \frac{1}{2}(1 - \theta^{'}(z)) = 1 - \theta^{'}(z) + \frac{1}{2}\theta^{'}(z) - \frac{1}{2} + \frac{1}{2}\theta^{'}(z) = \frac{1}{2}$.

Теперь получим константу ноль. Для этого, подставим в функцию F_1 вместо переменной z, константу $\frac{1}{2}$: $F_4(x, y) = F_1(x, y, \frac{1}{2}) = x - y -$

$\theta'(\frac{1}{2})+1 = x-y-1+1 = x-y$. Отожествляя переменные x и y, получим тождественный ноль. $F_4(x,x) = x - x = 0$.

Из $F_4(x,y)$ при помощи константы ноль получим функцию $-x$:

$F_5(y) = F_4(0,y) = 0 - y = -y$

$F_5(x) = -x$.

Затем из $F_4(x,y)$ и $F_5(y)$ суперпозицией выведем $x+y$:

$F_6(x,y) = F_4(x, F_5(y)) = x - (-y) = x + y$.

Теперь получим функцию $\frac{1}{2}x$. Для начала, получим константу 1. $F_6(\frac{1}{2},\frac{1}{2}) = \frac{1}{2}+\frac{1}{2} = 1$. Рассмотрим суперпозицию функций $F(x,y,z), F_5(x)$ и констант $0, 1$:

$$F(0, F_5(x), 1) = 0 - \frac{1}{2}(-x) - \frac{1}{2}\theta'(1) + \frac{1}{2} = \frac{1}{2}x - \frac{1}{2} + \frac{1}{2} = \frac{1}{2}x.$$

И последнее, выведем $\theta(x)$.

$\theta(x) = 1 - \theta'(-x)$.

Теорема доказана.

4.2. Построение базиса мощности k.

Теорема 3. *В классе кусочно-параллельных функций с двоично-рациональными коэффициентами BPP для любого наперед заданного $k \in \mathbb{N}$, существует базис из k элементов.*

. *Доказательство:* Приведем такие множества функций, составляющих базис BPP при $k < 5$.

Для $k = 4$ - базисом BPP является множество $B = \{\frac{1}{2}x, -x, x + y, \theta(x)\}$, по определению.

Докажем, что множество B действительно является базисом, в том смысле, что оно не избыточно. Т.е. нельзя выразить ни какую из входящих в него функций через остальные функции из B. Для этого поочередно будем исключать каждую функцию множества B и рассматривать, как будет меняться все множество функций составляющих класс BPP, используя общий вид функций принадлежащих классу BPP $(*)$. Если из B исключить $f_1 = \frac{1}{2}x$, то очевидно мы получим функции вида:
$(**) f(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_i + \cdots + \theta(\omega_1) + \cdots + \theta(\omega_s)$

$\theta(\omega_l) = \theta(x_1+x_2+\cdots+x_{i'}+x^l_{i+1}+x^l_{i+2}+\cdots+x^l_{j'-1}+\theta(\omega_{l1})+\cdots+\theta(\omega_{ls'}))$

$\theta(\omega_{li'}) = \theta(x_1 + x_2 + \cdots + x_{i'} + x^{li'}_{i+1} + x^{li'}_{i+2} + \cdots + x^{'}_{j'-1})$, т.е. множество линейных функций от n переменных с целыми коэффициентами и

возможными разрывами 1го рода. Очевидно $\frac{1}{2}x$ не может быть представлена в виде $(**)$. Если из B исключить $f_2 = -x$, то мы получим функции вида:

$(***) f(x_1, x_2, \ldots, x_n) = \frac{k_1}{2^{m_1}}x_1 + \frac{k_2}{2^{m_2}}x_2 + \cdots + \frac{k_i}{2^{m_i}}x_i + \frac{k_{i+1}}{2^{m_{i+1}}}\theta(\omega_1) + \cdots + \frac{k_j}{2^{m_j}}\theta(\omega_s) + \frac{k_0}{2^{m_0}}$.

Где $k_0, k_1, \ldots, k_i, k_{i+1}, \ldots, k_j \in \mathbb{N},$, т.к. коэффициент $\frac{k_i}{2^{m_i}}$ при x_i получается суперпозицией положительных функций $\frac{1}{2}x$ и $x + y$. И, следовательно, мы получаем класс линейных функций от n переменных, с положительными двоично-рациональными коэффициентами и возможными разрывами 1го рода. Функция $f_1 = -x$ не пренадлежит этому классу, т.к не может быть выражена через функции вида $(***)$.

Если из B исключить $f_3 = x + y$, то мы получим функции вида:

$f_1 = \frac{1}{2^m}x$,

$f_2 = \theta(\frac{1}{2^m}x)$,

$m_1, m_2, \ldots m_N \in \mathbb{N}, (N \leq n)$, т.е. функции зависящие от одной переменной.

Если из B исключить $f_4 = \theta(x)$, то очевидно мы получим функции вида:

$$f(x_1, x_2, \ldots, x_n) = \frac{k_1}{2^{m_1}}x_1 + \frac{k_2}{2^{m_2}}x_2 + \cdots + \frac{k_i}{2^{m_i}}x_i$$

Т.е. множество линейных непрерывных функций от n переменных, с двоично-рациональными коэффициентами. Получить разрывную функцию из непрерывных, используя операции суперпозиции и переименования, очевидно невозможно.

Следовательно множество B являющееся базисом для BPP, действительно не избыточно при $|B| = 4$.

Для $k = 3$ - базисом BPP является множество $\{-x, x + \frac{1}{2}y, \theta(x)\}$.

Для доказательства этого, выведем из данного множества функций, множество функций B. Операцией суперпозиции функции $F_1(x, y) = x + \frac{1}{2}y$ получим функцию $x+y$: $F_2(x, y) = F_1(F_1(x, y), y) = x+\frac{1}{2}y+\frac{1}{2}y = x+y$ Далее получим функцию $\frac{1}{2}x$:

$$F_2(F_1(x, y), -x) = x + \frac{1}{2}y - x = \frac{1}{2}y = \frac{1}{2}x.$$

В тоже время, ни одна функция не может быть удалена из данного, множества, что доказывается аналогично случаю $n = 4$.

Для $f_1 = x+\frac{1}{2}y$, это следует из того, что она необходима для образования функций: $f(x, y) = x + y$ и $f(x) = \frac{1}{2}x$.

Для $k = 2$ - базисом BPP является множество $\{x - \frac{1}{2}y, \theta(x)\}$.

Докажем этот факт аналогично предыдущему. Сначала получим функцию $\frac{1}{2}x$ дважды применяя операцию суперпозиции к функции $F_1(x,y) = x - \frac{1}{2}$:

$F_2(x,y) = F_1(x, x - \frac{1}{2}y) = x - \frac{1}{2}(x - \frac{1}{2}y) = \frac{1}{2}(x + \frac{1}{2}y)$

$F_2(x - \frac{1}{2}y, y) = \frac{1}{2}(x - \frac{1}{2}y + \frac{1}{2}y) = \frac{1}{2}x.$

Затем получим функцию $x + y$:

$F_3(x,y) = F_1(x - \frac{1}{2}y, y) = x - \frac{1}{2}y - \frac{1}{2}y = x - y.$

$F_4(x,y) = F_1(x - y, y) = x - y - y = x - 2y.$

$F_5(x,y) = F_1(x, F_4(x,y)) = x - \frac{1}{2}(x - 2y) = x - \frac{1}{2}x + y = \frac{1}{2}x + y.$

$F_5(x, F_5(x,y)) = \frac{1}{2}x + \frac{1}{2}x + y = x + y.$

И в заключение суперпозицией функций $F_3(x,y), F_4(x,y)$ и $x + y$ и последующим отожествлением x и y получим функцию $-x$:

$F_3(F_4(x,y), x + y) = x - 2y - x + y = -y = -x$

Так как $F_1(x,y) = x - \frac{1}{2}y$ образует только непрерывные функции, $f(x) = \theta(x)$ необходима для образования BPP, включающего в себя так же разрывные функции. В то же время функции $f(x) = \theta(x)$ не достаточно для образования базиса в BPP, так как, например, с помощью нее не возможно получить двухместную функцию суммы $f(x) = x + y$, принадлежащую BPP.

Для $k = 1$ - базисом BPP является $\{x - \frac{1}{2}y - \frac{1}{2}\theta'(z) + \frac{1}{2}\}$, где $\theta'(z) = \begin{cases} 1 & \text{при } z > 0 \\ 0 & \text{при } z \leq 0 \end{cases}$, т.к. функция $F(x,y,z) = x - \frac{1}{2}y - \frac{1}{2}\theta'(z) + \frac{1}{2}$ является шефферовой в данном классе.

Теперь для $k \geq 5$ будем строить базис BPP в виде:

$$\{\frac{1}{2}x, -x, p_1x + y, p_2x + y, \ldots, p_{k-3}x + y, \theta(x)\},$$

где НОД$(p_1, p_2, \ldots, p_{k-3}) = 1$, а НОД $(\bar{P}_i) \neq 1$,НОД$(\bar{P}_i) \neq 2m, \forall i, \bar{P}_i = (p_1, p_2, \ldots, p_{i-1}, p_{i+1}, \ldots, p_{k-3}), \forall m \in \mathbb{N}$.

Сначала докажем, что данная система функций порождает класс функций BPP. Для этого нам достаточно получить функцию $x + y$.
Рассмотрим числа $p_1, p_2, \ldots, p_{k-3}$. Так как НОД$(p_1, p_2, \ldots, p_{k-3}) = 1$, следовательно можно применив расширенный алгоритм Евклида найти такие числа $a_1, a_2, \ldots, a_{k-3} \in \mathbb{Z}$, что

$$a_1p_1 +_2 p_2 + \cdots + a_{k-3}p_{k-3} = 1$$

Произведя $|a_1|$ раз операцию суперпозиции функции $F_1(x,y) = p_1x + y$ вида $F_1(x, F_1(x,y))$, получим функцию $F_1^2(x,y) = a_1p_1x + y$, затем произведем a_2 раз операцию суперпозиции функции $F_2(x,y) = p_2x + y$ вида

$F_1(x, F_1(x, y))$, получим функцию $F_2^2(x, y) = a_2p_2x + y$ и так получим $k-3$ функции, вида $F_i^2(x, y) = a_ip_ix + y$, где $i = 1, \overline{k-3}$. Далее произведем суперпозицию $F_+^1(x, y) = F_2^1(x, F_2^2(x, y)) = a_1p_1x + a_2p_2x + y$. И так последовательно будем проводить суперпозиции вида:

$F_+^i(x, y) = F_+^{i-1}(x, F_1^{i+1}(x, y))$, для всех $k-3$ функций $F_i^2(x, y)$. В итоге получим функцию $F_+(x, y) = F_+^{k-4}(x, y) = a_1p_1x + a_2p_2x + \cdots + a_{k-3}p_{k-3}x + y = (a_1p_1 + a_2p_2 + \cdots + a_{k-3}p_{k-3})x + y = x + y$.

Докажем не избыточность этого множества. Необходимость функций $\frac{1}{2}x, -x, \theta(x)$ доказывается аналогично случаю $k = 4$. Все функции $p_1x + y, p_2x + y, \ldots, p_{k-3}x + y$ являются необходимыми, в силу того, что числа $p_1, p_2, \ldots, p_{k-3}$ попарно не взаимно-просты, т.е., НОД$(\bar{P}_i) \neq 1$,а также - НОД$(\bar{P}_i) \neq 2m$. Рассмотрим множество функций $B' = B\backslash p_ix + y$. Пусть НОД$(\bar{P}_i)) = c$, тогда из алгоритма Евклида, будет следовать, что при суперпозиции функций принадлежащих множеству B мы получим сумму вида: $f_+(x, y) = cx + y$, где $c \neq 1$. Причем, так как НОД$(\bar{P}_i) \neq 2m$, т.е. $c \neq 2m$, единицу не возможно получить применяя m раз суперпозицию $f_+(\frac{1}{2}x, y)$.

Теорема доказана.

Например, для $k = 6$, базис BPP составляет множество функций $\frac{1}{2}x, -x, 231x + y, 165x + y, 105x + y, 385x + y, \theta(x)$.

Автор выражает искреннюю признательность Часовских А.А. за постановку задачи, а также за обсуждение результатов работы за ценные советы и замечания.

Список литературы

[1] Половников В. С. Об оптимизации структурной реализации нейронных сетей. Диссертация на соискание ученой степени кандидата физико-математических наук — Москва, 2006.

[2] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов . — М.: Изд-во Наука, 1985.

[3] Хайкин. С. Нейронные сети: полный курс // 2-е издание. Вильямс, 2006. // Вестн. Моск. ун-та. Матем. Механ. — 2016. — № 4. — С. 12–17.

[4] Кан А. Н. Вопросы выразимости в классе нейронных функций //Интеллектуальные системы — том 19, — Выпуск 1. — 2015.

[5] Яблонский С. В. Введение в дискретную математику. . — М.: Изд-во Наука, 1986.

[6] Кудрявцев В. Б. Функциональные системы. . — М.: Изд-во МГУ, 1982.

On a class of neural functions with binary-rational parameters

Agafonova M. V.

The paper deals with a class of neural piecewise-parallel functions with binary-rational coefficients. It is proved that for any function in the class of piecewise-parallel functions there exists a function in the class of piecewise-parallel functions with binary-rational coefficients that approximates it with a predetermined accuracy. Also, for the class of functions under consideration, it is shown that there exist bases consisting of arbitrary number of elements, in particular, a Scheffer function is found.

Keywords: class of piecewise-parallel functions, class of neural functions with binary-rational coefficients, superposition operations, Scheffer function, bases.

Исследование квазигрупп, получаемых с помощью правильных семейств булевых функций порядка 2

Пивень Н.А.

Ключевые слова: Квазигруппа, латинский квадрат, параметрическое задание, полиномиальная полнота, правильные семейства функций.

В работе анализируются всевозможные латинские квадраты порядка 4, порождаемые с помощью правильных семейств функций. Оказывается, что все такие квадраты задают квазигруппы, не являющиеся полиномиально полными. Предлагается обобщение конструкции, связанной с правильными семействами. В результате удается в 4 раза увеличить число порождаемых латинских квадратов и получить значительное число полиномиально полных квазигрупп.

1. Введение

В наши дни разрабатываются различные способы защиты информации, использующие квазигруппы и связанные с ними латинские квадраты. Это обусловлено например тем, что К. Шеннон показал, что шифры, построенные на латинских квадратах, обладают свойством “совершенной секретности” ([1]). Примеры использования квазигрупп для решения различных задач криптографии можно найти в работах [2, 3, 4, 5].

С точки зрения криптографических приложений важную роль играет свойство полиномиальной полноты квазигрупп, так как задача распознавания разрешимости системы уравнений в полиномиально полной алгебре NP-полна ([6]). В работе [7] В. А. Артамоновым с соавторами в частности был получен критерий полиномиальной полноты квазигрупп порядка 4. Интересные результаты о полиномиальной полноте квазигрупп в более общем случае можно найти в работах [8, 9, 10].

В случае конечных квазигрупп квазигрупповая операция может быть задана таблицей Кэли, являющейся латинским квадратом. В. А. Носовым в работе [11] был предложен эффективный способ задания больших семейств латинских квадратов с помощью так называемых правильных семейств функций. Мы анализируем всевозможные латинские квадраты порядка 4, задаваемые правильными семействами функций. Оказывается, что, во-первых, таким образом порождается 60 из 576 квазигрупп, и, во-вторых, ни одна порождаемая квазигруппа не является полиномиально полной. Для устранения этого недостатка предлагается усиление конструкции В. А. Носова, названное перестановочной конструкцией. При ее использовании удается породить 240 латинских квадратов, 112 из которых задают полиномиально полные квазигруппы.

Дальнейшее изложение имеет следующую структуру. В разделе 2 даются основные определения. В разделе 3 анализируются латинские квадраты порядка 4, порождаемые правильными семействами функций. В разделе 5 вводится перестановочная конструкция и доказывается ее корректность. В разделе 6 анализируются латинские квадраты порядка 4, задаваемые перестановочной конструкцией. В приложении приводится список классов изоморизма построенных латинских квадратов.

Автор выражает благодарность А. Е. Панкратьеву и А. В. Галатенко за постановку задачи и внимание к работе.

2. Основные понятия

Определение 1. Конечной квазигруппой (Q, f_Q) называется множество Q, $|Q| < \infty$, на котором определена бинарная операция f_Q такая, что для любых элементов $a, b \in Q$ уравнения $f_Q(a, x) = b$ и $f_Q(y, a) = b$ однозначно разрешимы в Q.

В дальнейшем мы будем опускать слово “конечная”.

Определение 2. Латинским квадратом порядка n называется матрица размера $n \times n$, заполненная элементами некоторого n-элементного множества таким образом, что в каждой её строке и в каждом столбце все элементы различны.

Квазигрупповую операцию можно задавать табличным способом: для множества элементов $\{q_1, \ldots, q_m\}$, составляющих квазигруппу Q, выписывается квадратная таблица $m \times m$, такая что на пересечении i-ой строки и j-го столбца стоит $f_Q(q_i, q_j)$. Заметим, что построенная таким образом таблица, в связи с существованием и единственностью решения

уравнений $f_Q(a,x) = b$ и $f_Q(y,a) = b$, является латинским квадратом, который мы и называем латинским квадратом, связанным с квазигруппой.

Определение 3. Две квазигруппы (Q, f_Q) и (Q, f'_Q) называются изоморфными, если существует биекция $\varphi : Q \to Q$ такая, что для любых $a, b \in Q$ выполнено равенство $f'_Q(\varphi(a), \varphi(b)) = \varphi(f_Q(a,b))$. Функция φ называется изоморфизмом квазигрупп (Q, f_Q) и (Q, f'_Q).

Определение 4. Две квазигруппы (Q, f_Q) и (Q, f'_Q) называются изотопными, если существуют такие перестановки α, β и γ на множестве Q, что для любых $a, b \in Q$ справедливо равенство $f'_Q(a,b) = \gamma^{-1}(f_Q(\alpha(a), \beta(b)))$.

Понятие изотопности естественным образом переносится на латинские квадраты. Несложно увидеть, что матрица, изотопная латинскому квадрату, сама является латинским квадратом.

Пусть $n \in \mathbb{N} \cup \{0\}$, $\mathcal{O}_n$ — множество всех n-местных функций на множестве Q, $\mathcal{O} = \bigcup\limits_{n=0}^{\infty} \mathcal{O}_n$. На множестве $\mathcal{O}$ стандартным образом вводятся операции суперпозиции и замыкания ([12]). Замыкание множества $F \subseteq \mathcal{O}$ обозначается через $[F]$.

Определение 5. Квазигруппа (Q, f_Q) называется полиномиально полной, если $[\{f_Q\} \cup \mathcal{O}_0] = \mathcal{O}$.

Определение 6. Квазигруппа (Q, f_Q) называется простой, если операция f_Q не сохраняет ни одного нетривиального отношения эквивалентности на множестве Q.

Определение 7. Квазигруппа (Q, f_Q) называется аффинной, если на множестве Q может быть введена структура абелевой группы $(Q, +)$, такая что существуют автоморфизмы α, β группы $(Q, +)$, элемент $c \in Q$, и для любых $a, b \in Q$ справедливо равенство $f_Q(a,b) = \alpha(a) + \beta(b) + c$.

Несложно увидеть, что простота и аффинность сохраняются при изоморфизме.

Известно ([13]), что квазигруппа является полиномиально полной если и только если она простая и не аффинная. В случае $|Q| = 4$ в работе [7] установлено, что квазигруппа полиномиально полна тогда и только тогда, когда соответствующий латинский квадрат обладает следующими двумя свойствами:

I. среди строк и столбцов квадрата есть перестановка с 3-циклом (что обеспечивает простоту);

II. цикловая структура строк не является одной из этих трех (что обеспечивает не аффинность):

   1) четыре 3-цикла;

   2) два 4-цикла и две строки по два 2-цикла;

   3) одна тождественная перестановка и три строки по два 2-цикла.

Определение 8. Семейство булевых функций $\mathrm{F}=\{f_i\}_{i=1}^n$, $f_i = f_i(x_1, \ldots, x_n)$, называется правильным, если для любых различных значений аргументов $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ найдется такой индекс $\alpha \in \{1, \ldots, n\}$, что $x'_\alpha \neq x''_\alpha$, $f_\alpha(x'_1, \ldots, x'_n) = f_\alpha(x''_1, \ldots, x''_n)$

Правильные семейства функций были введены В. А. Носовым в работе [11] для построения латинских квадратов порядка 2^n. Занумеруем элементы множества Q, $|Q| = 2^n$, числами от 0 до $2^n - 1$. Таким образом, каждому элементу $a \in Q$ можно сопоставить n-битный вектор $(a_1, \ldots, a_n)$, задающий двоичную запись номера. В результате квазигрупповая операция f_Q может быть представлена в векторной форме: записи $z = f_Q(x, y)$ и

$$\begin{aligned} z_1 &= f_Q^1(x_1, \ldots, x_n, y_1, \ldots, y_n), \\ &\vdots \\ z_n &= f_Q^n(x_1, \ldots, x_n, y_1, \ldots, y_n), \end{aligned}$$

где $f_Q^1, \ldots, f_Q^n$ — булевы функции, являющиеся компонентами вектор-функции, порожденной f_Q, эквивалентны.

Пусть $f_1, \ldots, f_n$ — булевы функции от n переменных, $\pi_1, \ldots, \pi_n$ — булевы функции от двух переменных. Рассмотрим следующее семейство функций от $2n$ переменных:

$$\begin{aligned} g_1 &= x_1 \oplus y_1 \oplus f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ &\vdots \\ g_n &= x_n \oplus y_n \oplus f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \end{aligned} \tag{1}$$

где операция $\oplus$ означает сложение по модулю 2. В работе [11] показано, что семейство $G = \{g_1, \ldots, g_n\}$ задает латинский квадрат для любых функций $\pi_1, \ldots, \pi_n$ тогда и только тогда, когда семейство $F = \{f_1, \ldots, f_n\}$ правильное.

3. Латинские квадраты порядка 4, задаваемые правильными семействами

Рассмотрим латинские квадраты порядка 4, задаваемые всевозможными правильными семействами функций порядка 2 с помощью конструкции В. А. Носова. Известно ([14]), что в этом случае одна из функций правильного семейства является константой, а вторая фиктивно зависит от одноименной переменной.

Теорема 1. *С помощью правильных семейств порядка 2 порождается 60 различных латинских квадратов порядка 4, входящих в 8 различных классов изоморфизма. При этом все задаваемые квазигруппы не обладают свойством полиномиальной полноты.*

Доказательство. В силу структуры правильных семейств порядка 2, формулы для задания латинских квадратов принимают вид

$$\begin{aligned} z_1 &= x_1 \oplus y_1 \oplus f_1(\pi_2(x_2, y_2)) \\ z_2 &= x_2 \oplus y_2 \oplus f_2(\pi_1(x_1, y_1)). \end{aligned}$$

При этом возможны следующие случаи.

1) Обе функции f_1, f_2 являются константами. Несложно увидеть, что здесь возникает 4 различных латинских квадрата.

2) Ровно одна из функций f_1, f_2 являетсяя константой. Заметим, что выбор номера константной функции и выбор значения константы может быть выполнен четырьмя способами. Без ограничения общности рассмотрим случай, когда f_1 отлична от константы и f_2 тождественно равна 0. Значит, f_1 является тождественной функцией, либо отрицанием. Так как отрицание может быть опущено на переменную, множество латинских квадратов, задаваемых семейством, в котором $f_1(x) = x$, и семейством, в котором $f_1(x) = \overline{x}$, совпадают, и без ограничения общности можно считать, что $f_1(x) = x$. Заметим, что получаемые в этом случае латинские квадраты будут отличаться от латинских квадратов, учтенных в прошлом пункте, тогда и только тогда, когда функция π_2 отлична от константы. Таких функций 14. Очевидно, что различные функции π_2 задают различные латинские квадраты. Значит, общее число новых латинских квадратов, полученных в этом пункте, равно $14 \cdot 4 = 56$.

Таким образом, общее число латинских квадратов, порожденных правильными семействами порядка 2, равно $56 + 4 = 60$.

Заметим, что из приведенных выше рассуждений в частности следует, что число различных правильных семейств порядка 2 равно 12.

Все 60 латинских квадратов были перечислены явно, используя приведенные выше рассуждения. В работе мы ограничимся анализом классов изоморфизма. Представители классов и результаты анализа содержатся в таблице 1 в Приложении. Полиномиальная полнота устанавливалась в соответствии с упомянутым критерием из работы [7]. В четвертом столбце таблицы указан номер нарушенного необходимого условия полноты. □

4. Перестановочная конструкция

Усилим конструкцию, связанную с правильными семействами, следующим образом. Пусть $n \in \mathbb{N}$, $F = \{f_1, \ldots, f_n\}$ — правильное семейство булевых функций, $\alpha, \beta, \gamma \in S_n$ — перестановки на множестве $\{1, \ldots, n\}$. Наложим перестановки α, β, γ на индексы переменных x и y и номера функций g в представлении (1):

$$\begin{array}{rcl} g_{\gamma(1)} & = & x_{\alpha(1)} \oplus y_{\beta(1)} \oplus f_1(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})), \\ & \vdots & \\ g_{\gamma(n)} & = & x_{\alpha(n)} \oplus y_{\beta(n)} \oplus f_n(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})). \end{array} \quad (2)$$

Заметим, что исходное задание (1) получается из формул (2) при выборе тождественных перестановок в качестве α, β и γ.

Теорема 2. *При любых перестановках $\alpha, \beta, \gamma \in S_n$ и любых функциях от двух переменных $\pi_1, \ldots, \pi_n$ система функций $g_1, \ldots, g_n$ задает латинский квадрат.*

Доказательство. Так как любая перестановка может быть разложена в произведение транспозиций, наложение перестановок α, β и γ на систему (1) может быть сведено к цепочке наложения транспозиций, причем, как несложно увидеть, транспозиции, соответствующие разным перестановкам, коммутируют. Докажем утверждение теоремы индукцией по длине цепочек транспозиций.

Базис индукции: если длина всех цепочек равна 0, система (2) принимает вид (1), и утверждение теоремы следует из правильности семейства F.

Индуктивный переход: пусть утверждение верно для перестановок α', β', γ'. Покажем, что в этом случае к любой из этих перестановок можно применить произвольную транспозицию без нарушения условия теоремы. Достаточно доказать три утверждения.

1) Пусть α_0 — транспозиция, переставляющая переменные с номерами s и t, $s < t$, $\pi_1, \ldots, \pi_n$ — произвольные функции от двух переменных, $\alpha = \alpha_0 \cdot \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$. Тогда система (2) задает латинский квадрат.

2) Пусть β_0 — транспозиция, переставляющая переменные с номерами s и t, $s < t$, $\pi_1, \ldots, \pi_n$ — произвольные функции от двух переменных, $\alpha = \alpha'$, $\beta = \beta_0 \cdot \beta'$, $\gamma = \gamma'$. Тогда система (2) задает латинский квадрат.

3) Пусть γ_0 — транспозиция, переставляющая функции с номерами s и t, $s < t$, $\pi_1, \ldots, \pi_n$ — произвольные функции от двух переменных, $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma_0 \cdot \gamma'$. Тогда система (2) задает латинский квадрат.

Для доказательства первого утверждения рассмотрим латинский квадрат LS, порожденный перестановками α', β', γ'. Дополнительно применим перестановку α_0. Порожденную новой системой матрицу обозначим LS'. Несложно заметить, что действие перестановки α_0 — это замена всех вхождений s-того разряда в номере строки на t-тый и наоборот. Это эквивалентно перестановке строк LS, при которой меняются местами строки с номерами вида $(a_1, \ldots, a_{s-1}, 0, a_{s+1}, \ldots, a_{t-1}, 1, a_{t+1}, \ldots, a_n)$ и $(a_1, \ldots, a_{s-1}, 1, a_{s+1}, \ldots, a_{t-1}, 0, a_{t+1}, \ldots, a_n)$. Следовательно матрица LS' получается применением изотопии к латинскому квадрату LS, то есть является латинским квадратом.

Второе утверждение доказывается аналогично, с заменой строк на столбцы.

Для доказательства третьего утверждения достаточно заметить, что транспозиция γ_0 действует как “перекодировка” элементов, меняя местами элементы, двоичное представление которых отличается только в позициях s и t. Следовательно, получающаяся матрица вновь изотопна исходному латинскому квадрату и, значит, сама является латинским квадратом.

В силу произвольности выбора функций $\pi_1, \ldots, \pi_n$ доказательство индуктивного перехода завершено. □

Расходы памяти на хранение перестановок α, β, γ невелики — они составляют $3n] \log n[$, что мало по сранению с памятью, требующейся для задания булевой функции от n переменных. В то же время возникающие новые латинские квадраты могут оказаться более предпочтительными с точки зрения приложений. В частности, в случае $n = 2$, как будет показано в следующем разделе, конструкция (2) позволяет получить значительное число полиномиально полных квазигрупп.

5. Латинские квадраты порядка 4, задаваемые перестановочной конструкцией

Теорема 3. *Перестановочная конструкция при $n = 2$ порождает 240 различных латинских квадрата, лежащих в 29 различных классах изоморфизма. При этом 112 полученных латинских квадрата задают полиномиально полные квазигруппы, лежащие в 14 различных классах изоморфизма.*

Доказательство. Порождаемые латинские квадраты были перечислены явно: к каждому из 60 функциональных заданий латинских квадратов, найденных в теореме 1, применялось по 8 перестановок (произвольных комбинаций транспозиций x_1 и x_2, y_1 и y_2, z_1 и z_2). В результате возникло 480 латинских квадратов, 240 из которых оказались попарно различными. В работе мы ограничимся анализом классов изоморфизма. Представители классов выписаны в Приложении. Результаты анализа содержатся в таблице 2 Приложения. Полиномиальная полнота устанавливалась в соответствии с критерием из работы [7]. В третьем столбце таблицы указано нарушенное необходимое условие полноты или поставлен прочерк, если квазигруппа полиномиально полна. □

6. Заключение

В работе проведено исследование латинских квадратов порядка 4, получаемых с помощью правильных семейств булевых функций порядка 2. Установлено, что все соответствующие квазигруппы не являются полиномиально полными. Предложено усиление конструкции правильных семейств, названное перестановочной конструкцией. Показано, что среди квазигрупп, связанных с новыми латинскими квадратами, имеется значительное число полиномиально полных.

Список литературы

[1] C. Shannon, “Communication theory of secrecy systems Bell System Techn. J., 28:4 (1949), 656–715

[2] М.М. Глухов, “О применениях квазигрупп в криптографии Прикладная дискретная математика, 2008, № 2, 28–32

[3] S. Markovski, D. Gligoroski, V. Bakeva, “Quasigroup String Processing: Part 1 Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci., XX: 1–2 (1999), 13–28

[4] S. Markovski, V. Kusacatov, “Quasigroup String Processing: Part 2 Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci., XXI: 1–2 (2000), 15–32

[5] V. Shcherbacov, “Quasigroup based crypto-algorithms arXiv:201.3016v1

[6] G. Horváth, C.L. Nehaniv, Cs. Szabó, “An assertion concerning functionally complete algebras and NP-completeness Theoret. Comput. Sci., 407 (2008), 591–595

[7] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, “On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts Quasigroups and Related Systems, 21:2 (2013), 117–130

[8] V.A. Artamonov, S. Chakrabarti, S.K. Pal, “Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations Discrete Applied Mathematics, 2016, 5–17

[9] V.A. Artamonov, S. Chakrabarti, S.K. Pal, “Characterizations of highly non-associative quasigroups and associative triples Quasigroups and Related Systems, 25 (2017), 1–19

[10] А.В. Галатенко, А.Е. Панкратьев, С.Б. Родин, “О полиномиально полных квазигруппах простого порядка Интеллектуальные системы. Теория и приложения, 20:3 (2016), 194–198

[11] В.А. Носов, “О построении классов латински хквадратов в булевой базе данных Интеллектуальные системы, 4:3–4 (1999), 307–320

[12] С.В. Яблонский, “Введение в дискретную математику Москва, Высшая школа, 2010

[13] J. Hagemann, C. Herrmann, “Arithmetically locally equational classes and representations of partial functions Colloq.Math.Sci. J. Bolyai., 29, 1982, 345–360

[14] V.A. Nosov, A.E. Pankratiev, “A generalization of the Feistel cipher Международная конференция “Мальцевские чтения”. Тезисы докладов., Новосибирск, 2015, 59

Приложение

Таблица 1

Номер	Мощность класса	Представитель класса	Нарушение полноты
1	4	0 1 2 3 1 0 3 2 2 3 0 1 3 2 1 0	I
2	8	0 3 2 1 3 2 1 0 2 1 0 3 1 0 3 2	I
3	8	2 3 0 1 1 2 3 0 0 1 2 3 3 0 1 2	I
4	8	0 3 2 1 1 2 3 0 2 1 0 3 3 0 1 2	I
5	8	2 1 0 3 3 2 1 0 0 3 2 1 1 0 3 2	I

Продолжение на следующей странице

Таблица 1, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
6	8	0 1 2 3 3 2 1 0 2 3 0 1 1 0 3 2	I
7	8	2 1 0 3 1 2 3 0 0 3 2 1 3 0 1 2	I
8	8	0 1 2 3 1 2 3 0 2 3 0 1 3 0 1 2	I

Таблица 1: Результаты анализа классов изоморфизма латинских квадратов, порожденных с помощью конструкции В. А. Носова правильными семействами булевых функций порядка 2

Таблица 2

Номер	Мощность класса	Представитель класса	Нарушение полноты
1	4	0 1 2 3 1 0 3 2 2 3 0 1 3 2 1 0	I
2	8	0 3 2 1 3 2 1 0 2 1 0 3 1 0 3 2	I
3	8	2 3 0 1 1 2 3 0 0 1 2 3 3 0 1 2	I

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
4	12	0 3 2 1 1 2 3 0 2 1 0 3 3 0 1 2	I
5	8	2 1 0 3 3 2 1 0 0 3 2 1 1 0 3 2	I
6	12	0 1 2 3 3 2 1 0 2 3 0 1 1 0 3 2	I
7	12	2 1 0 3 1 2 3 0 0 3 2 1 3 0 1 2	I
8	8	0 1 2 3 1 2 3 0 2 3 0 1 3 0 1 2	I
9	8	0 3 1 2 3 1 2 0 1 2 0 3 2 0 3 1	—
10	8	1 3 0 2 2 1 3 0 0 2 1 3 3 0 2 1	—
11	8	0 3 1 2 2 1 3 0 1 2 0 3 3 0 2 1	II.1

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
12	8	1 2 0 3 3 1 2 0 0 3 1 2 2 0 3 1	—
13	8	0 2 1 3 3 1 2 0 1 3 0 2 2 0 3 1	—
14	8	1 2 0 3 2 1 3 0 0 3 1 2 3 0 2 1	II.1
15	8	1 3 0 2 3 0 2 1 0 2 1 3 2 1 3 0	—
16	8	1 3 0 2 2 0 3 1 0 2 1 3 3 1 2 0	—
17	8	1 2 0 3 3 0 2 1 0 3 1 2 2 1 3 0	II.1
18	8	0 2 3 1 3 1 2 0 2 0 1 3 1 3 0 2	—
19	8	2 0 3 1 1 3 2 0 0 2 1 3 3 1 0 2	—

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
20	8	0 2 3 1 1 3 2 0 2 0 1 3 3 1 0 2	II.1
21	8	2 0 1 3 3 1 2 0 0 2 3 1 1 3 0 2	—
22	8	0 2 1 3 3 1 2 0 2 0 3 1 1 3 0 2	I
23	8	2 0 3 1 3 1 0 2 0 2 1 3 1 3 2 0	—
24	8	2 0 3 1 1 3 0 2 0 2 1 3 3 1 2 0	I
25	8	0 1 3 2 3 2 1 0 1 0 2 3 2 3 0 1	—
26	8	1 0 3 2 2 3 1 0 0 1 2 3 3 2 0 1	—
27	8	1 0 2 3 3 2 1 0 0 1 3 2 2 3 0 1	—

Продолжение на следующей странице

Таблица 2, продолжение

Номер	Мощность класса	Представитель класса	Нарушение полноты
28	8	0 1 2 3 3 2 1 0 1 0 3 2 2 3 0 1	II.3
29	8	1 0 3 2 3 2 0 1 0 1 2 3 2 3 1 0	—

Таблица 2: Результаты анализа классов изоморфизма латинских квадратов, порожденных с помощью перестановочной конструкции правильными семействами булевых функций порядка 2

Investigations of quasigroups generated by proper families of boolean functions of order 2
Piven N.A.

Keywords: Quasigroup, Latin square, parametric assignment, polynomial completeness, proper families of functions

We analyze all Latin squares of order 4 generated by proper families of Boolean functions. It turns out that all these Latin squares define polynomially incomplete quasigroups. We propose a generalization of the construction based on proper families. As a result, the number of generated Latin squares grows four times, and an essential number of the corresponding quasigroups becomes polynomially complete.

Часть 2.
Математические модели

Об автоматных функциях с магазинной памятью

Иванов И.Е.

Известно, что автоматы с магазинной памятью сохраняют множество периодических последовательностей. Ранее автор привёл верхние и нижние оценки на максимальный период выходной последовательности автономного автомата с магазинной памятью в зависимости от характеристик автомата. В данной работе приводятся оценки на максимальный период выходной последовательности для общего случая. Период выходный последовательности был изучен главным образом как функция от периода входной последовательности.

Ключевые слова: автомат с магазинной памятью, детерминированная функция, периодические последовательности.

1. Введение

Теория автоматов как конечных, так и бесконечных начала активно развиваться в 50-е годы прошлого века. Разумеется, упоминания были и раньше. Машины Тьюринга были введены А.Тьюрингом в 1936 году [35]. Несколько позже в работе Мак-Каллока и Питтса [30] появилось понятие конечного автомата.

Развитие теории автоматов было стимулировано развитием теории формальных грамматик, основной задачей которой было построение математической модели для описания естественных языков. Основополагающими работами данной тематики можно считать работы американского ученого Н.Хомского [36], [37], в которых и были сформулированы современные подходы теории формальных грамматик. Их основным результатом можно считать построение иерархии Хомского, то есть классификации формальных грамматик по правилам вывода.

Оказалось, что каждому классу иерархии соотвествует свой тип распознавателя. Для регулярных языков распознавателем является конечный автомат [21]. Конечные автоматы как распознаватели языков изуча-

лись очень широко и довольно скоро стали самостоятельным объектом исследований. Была доказана эквивалентность классов детерминированных и недетерминированных конечных автоматов [34], алгоритмически решена проблема эквивалентности автоматов [32]. Для регулярных языков были алгоритмически решены следующие проблемы: проблема принадлежности слова языку, проблема пустоты языка, проблема бесконечности языка. Была доказана замкнутость регулярных языков относительно операций объединения, пересечения и дополнения. Обзор по этим результатам можно найти в [1], [10].

Понятие регулярности было обобщено для бесконечных последовательностей (ω-языки). Мак-Нотон показал, что и в этом случае акцептором является конечный автомат [31]. Обзор по результатам для ω-языков, распознаваемых конечными автоматами, можно найти в [33], [50].

Многие задачи для конечных автоматов в рамках теории формальных языков были решены. Было доказано существование алгоритмов по большинству языковых проблем, например:

- Существует алгоритм проверки принадлежности слова регулярному языку.
- Существует алгоритм проверки регулярного языка на пустоту.
- Существует алгоритм проверки регулярного языка на бесконечность.
- Существует алгоритм проверки эквивалентности двух регулярных языков.
- Существует алгоритм проверки вхождения одного языка в другой (как подмножество).

Более детально с этой областью формальных языков можно ознакомиться в [1], [10].

Класс регулярных языков является самым изученным в иерархии Хомского. Оказалось, что если расширить принятое в теории формальных грамматик определение детерминированного автомата, добавив к нему выход, то можно не только построить всю теорию регулярных языков, но и получить новую функциональную систему, изучение которой само по себе представляет интерес.

В 1960-х годах возникают задачи распознавания полноты для конечных автоматов: требуется найти алгоритм, позволяющий по любой системе автоматов установить, является ли она полной или нет. Для булевых функций, то есть автоматов без памяти, данная задача была решена Э.Постом [43]. Для функций с задержками В.Б. Кудрявцев установил критерии полноты [25]. Вместе с тем была показана континуальность предполных классов автоматных функций [26]. М.И. Кратко в общем случае доказал алгоритмическую неразрешимость распознавания полноты для конечных автоматов относительно операции суперпозиции и обратной связи [24].

В дальнейшем задача полноты для автоматных функций была широко изучена в различных вариациях. При этом можно выделить несколько основных подходов.

Первый связан с определением понятия равенства автоматов. Были исследованы следующие вариации:

- A-полнота [8], [9];
- Клини-полнота [12];
- ϵ-полнота [49];
- полнота с учетом недостижимых состояний [53];
- N - полнота [2].

Все эти задачи оказались алгоритмически неразрешимыми.

Следующий подход связан с изучением полноты в некоторых подклассах автоматов. В.Б. Кудрявцев для функций с задержками описал все предполные классы и нашел алгоритм распознавания полноты [25]. А.А. Часовских в классе линейных автоматов также описал все предполные классы и нашел алгоритм распознавания полноты конечных систем относительно операции композиции [54].

Третий подход связан с ограничениями на исследуемые системы автоматов. А.А. Летичевский привёл алгоритм решения задачи о полноте относительно операций композиции для автоматов Медведева (конечных систем автоматных функций, выдающих свое состояние) при наличии всех булевых функций [28]. В 1986 В.А. Буевич показал алгоритмическую разрешимость задачи A-полноты для систем, содержащих все булевы функции [9]. В 1992 Д.Н. Бабин показал существование алгоритма распознавания полноты относительно суперпозиции и обратной

связи для систем, содержащих все булевы функции [3]. Также он осуществил классификацию добавок из замкнутых классов булевых функций по свойству алгоритмической разрешимости распознавания полноты и показал, что обеспечивающих алгоритмическую разрешимость добавок конечное число [4].

Задача распознавания полноты конечных систем относительно операций суперпозиции не имеет смысла, так как любая конечная система относительно суперпозиции не является полной. Поэтому относительно суперпозиции разумно изучать полноту бесконечных систем. Д.Н. Бабиным было доказано, что система, состоящая из всех одноместных конечных автоматов и всех булевых функций, полна. Это означает, что арность множества автоматных функций равна двум (аналог 13-ой проблемы Гильберта для автоматных функций) [5]. В задаче выразимости констант при наличии всех булевых функций преуспел А.А. Летуновский. Им детально были изучены периодические свойства конечных автоматов. В работе [29] полностью описаны периоды выходных последовательностей, которые может генерировать произвольный автомат из замыкания конечной системы автоматов.

Развитием функционального подхода в теории автоматов в основном занималась советская школа теории автоматов. С основными результатами можно ознакомиться в [27].

Следующим классом языков в иерархии Хомского является класс контекстно-свободных языков. Для них распознавателем является автомат с магазинной памятью. Важность магазинов (известных также под названием стеков) в процессах обработки языков была осознана в начале 1950-х годов. Эттингер[40] и Шютценберже [38] первыми формализовали понятие автомата с магазинной памятью. Эквивалентность автоматов с магазинной памятью и контекстно-свободных грамматик была показана Хомским[37] и Эви[39]. Очень скоро стало понятно, что класс контекстно-свободных языков устроен сложнее класса регулярных. В работах [6], [15] появились примеры алгоритмически неразрешаемых проблем, а именно:

- Не существует алгоритма, позволяющего установить равенство двух контекстно-свободных языков.
- Не существует алгоритма проверки, что один контекстно-свободный язык лежит в другом.
- Не существует алгоритма проверки, что пересечение двух контекстно-свободных языков является пустым.

- Не существует алгоритма проверки контекстно-свободного языка на регулярность.

Оказалось, что многие техники работы с конечными автоматами и регулярными языками для автоматов с магазинной памятью не работают. В частности, было показано, что класс языков, распознаваемых детерминированными автоматами с магазинной памятью, не равен классу всех контекстно-свободных языков, а является его собственным подмножеством [11] [38].

Так как для большинства нетривиальных языковых задач были получены отрицательные результаты в виде отсутствия алгоритмов, то были предприняты попытки найти подклассы, в которых эти задачи имели бы решения. Пожалуй, самой известной и трудоёмкой задачей является проблема эквивалентности детерминированных контекстно-свободных языков, которая была решена лишь в 1997 году французским математиком Сенизерже (Senizergues) [46]. За почти полвека этой проблемой занимались многие математики, и были получены положительные решения этой проблемы в различных подклассах [23], [16], [52], [20], [51], [7], [42], [44], [48], [41], [45].

Заметим, что для всех исследуемых выше подклассов детерминированных автоматов с магазинной памятью проблема регулярности, то есть эквивалентности конечному автомату, разрешима [47]. Тем не менее, для всех этих подклассов проблема включения одного языка в другой алгоритмически неразрешима.

Несмотря на существование алгоритмов для задач проверки на регулярность и эквивалентность, до сих пор во многих классах не понятна сложность этих задач. С одними из последних результатов в этой области можно ознакомиться в [13], [14].

Основной целью работы является изучение свойств автоматов с магазинной памятью как преобразователей последовательностей. Изучение детерминированных автоматных функций в теории конечных автоматов позволяет строить продуктивные методы их анализа [27]. Периодические свойства конечных автоматов — это фундамент, на основе которого выполнено множество построений. В случае же автомата с магазинной памятью периодические свойства почти не были изучены. Данная работа и предыдущие работы автора [17], [18], [19] — это попытка разобраться в этом вопросе.

Основными результатами данной работы можно считать следующие:

- Приведена оценка на максимальную длину периода выходной последовательности в зависимости от характеристик автомата.
- В случае однобуквенного алфавита удалось существенно понизить полученную верхнюю оценку. Была дана асимптотически достижимая оценка для автономного случая.
- В случае произвольного алфавита магазина удалось показать, что существенно понизить полученную верхнюю оценку нельзя. Были построены примеры автономных автоматов с магазинной памятью, генерирующих периодические последовательности с длиной периода, экспоненциально зависящей от характеристик автомата.
- Было доказано, что найдется такой автомат с магазинной памятью с однобуквенным магазином, который способен преобразовывать входную последовательность, увеличивая ее период квадратичным образом.
- Если же в магазине автомата с магазинной памятью разрешить иметь хотя бы два символа, то найдется такой автомат, который сможет преобразовывать входную последовательность, увеличивая ее период полиномиально.

Далее работа состоит из 7 разделов, включая введение, заключение и список литературы. Во втором разделе приводятся основные определения и постановка задачи. Следующие две части посвящены изучению автономных автоматов с магазинной памятью. В третьем разделе изучается случай, когда алфавит магазина содержит больше двух символов, а в четвёртом — случай однобуквенного магазина. В пятом разделе работы рассматривается автомат с магазинной памятью со входом. Далее следуют заключение и список литературы.

2. Определения

Инициальным детерминированным автоматом с магазинной памятью будем называть "девятку"

$$P = (A, Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0),$$

где A — входной алфавит, Q — конечное множество состояний, B — выходной алфавит, Γ — алфавит памяти (алфавит ленты магазина), $\varphi : A \times Q \times (\Gamma \cup \lambda) \to Q$ — функция переходов, $\psi : A \times Q \times (\Gamma \cup \lambda) \to B$ — функция выхода, $\eta : A \times Q \times (\Gamma \cup \lambda) \to \Gamma^*$ — функция памяти, $q_0 \in Q$ — начальное состояние, $\gamma_0 \in \Gamma^*$ — начальная запись в магазине.

Функционирование P можно определить с помощью системы канонических уравнений, которые задают в каждый момент времени t состояние автомата $q(t)$, записанное в магазине слово $\gamma(t)$ и выход автомата $b(t)$ при подаче на вход $a(t)$:

$$\begin{cases} q(0) = q_0, \\ \gamma(0) = \gamma_0, \\ z(t) = LS(\gamma(t)), \\ q(t+1) = \varphi(a(t), q(t), z(t)), \\ \gamma(t+1) = S(\gamma(t))\eta(a(t), q(t), z(t)), \\ b(t) = \psi(a(t), q(t), z(t)), \end{cases}$$

где $LS : \Gamma^* \to \Gamma \cup \{\lambda\}$ возвращает последний символ при подаче непустого слова и $LS(\lambda) = \lambda$, а $S : \Gamma^* \to \Gamma^*$ стирает последний символ входного слова и $S(\lambda) = \lambda$.

Инициальный автомат с магазинной памятью определяет детерминированную функцию $f : A^* \to B^*$. Обозначим через $\mathcal{M}(A, B)$ множество детерминированных функций, порождаемых автоматами с магазинной памятью. Отметим, что $\mathcal{M}(A, B)$ содержит множество ограниченно-детерминированных функций.

Обозначим $n = |Q|$, $m = |\Gamma|$, $k = \max\limits_{(q,z) \in Q \times \Gamma \cup \{\lambda\}} |\eta(q, z)|$ и будем говорить, что $P \in \mathcal{M}(n, m, k)$. Здесь n — число состояний, m — арность (или ширина) магазина, k — максимально возможная длина записи в магазин за один такт.

Будем говорить, что $P_0 = (Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0)$, — инициальный автомат с магазинной памятью без входа, если он удовлетворяет системе канонических уравнений:

$$\begin{cases} q(0) = q_0, \\ \gamma(0) = \gamma_0, \\ z(t) = LS(\gamma(t)), \\ q(t+1) = \varphi(q(t), z(t)), \\ \gamma(t+1) = S(\gamma(t))\eta(q(t), z(t)), \\ b(t) = \psi(q(t), z(t)). \end{cases}$$

Будем говорить, что автомат с магазинной памятью без входа P_0 лежит в $\mathcal{M}_0(n, m, k)$, если $n = |Q|$, $m = |\Gamma|$, $k = \max\limits_{(q,z)\in Q\times\Gamma\cup\{\lambda\}} |\eta(q, z)|$. Для автомата с магазинной памятью без входа обозначим $L(P)$ минимальную длину периода периодической последовательности, которую он генерирует. Нас будет интересовать максимальная длина периода в классе автоматов $\mathcal{M}_0(n, m, k)$, а именно:

$$L(n, m, k) = \max_{P\in\mathcal{M}_0(n,m,k)} L(P).$$

Для оценки длины периода автономного автомата с магазинной памятью удобно пользоваться следующими функциями: $\omega(q, \gamma) : Q \times \Gamma^* \to \mathbb{N} \cup \{\infty\}$ и $\pi(q, \gamma) : Q \times \Gamma^* \to Q$, которые формально определим следующим образом. Пусть автомат находится в состоянии q, а в магазине лежит слово γ. Если существует такое минимальное положительное количество тактов τ работы автомата, что магазин становится пустым, а автомат переходит в состояние q', то положим, что $\omega(q, \gamma) = \tau$, а $\pi(q, \gamma) = q'$, иначе $\omega(q, \gamma) = \infty$, а значение $\pi(q, \gamma)$ не определено.

Для автомата с магазинной памятью со входом P и слова α из A^+ обозначим $L(P, \alpha)$ — период выходной последовательности при подаче последовательности α^∞ на вход автомату с магазинной памятью P.

Данная работа посвящена исследованию свойств функций $L(n, m, k)$ и $L(P, \alpha)$.

3. Периодическиеские свойства автономных автоматов с магазинной памятью при $|\Gamma| > 1$

3.1. Периодичность выходной последовательности

Известно, что автоматы автономные с магазинной памятью генерируют периодические последовательности [22]. Приведем свое доказательство этого факта в принятых обозначениях.

Теорема 1 ([22]). *Автономный автомат с магазинной памятью* $P = (Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0)$ *генерирует периодическую выходную последовательность.*

Доказательство. Не ограничивая общности, можно считать, что автомат имеет самую общую функцию выхода, то есть $B = Q \times \Gamma \cup \{\lambda\}$ и $\psi(q, z) = (q, z)$. Рассмотрим последовательности $q(t), \gamma(t), z(t)$, заданные каноническими уравнениями. Для целого $h > 0$ определим $M(h) = \{t \mid |\gamma(t)| \leq h\}$.

Если найдётся такое h_0, что $|M(h_0)| = \infty$, то это означет, что найдутся такие t_1 и t_2 из $M(h_0)$, что $q(t_1) = q(t_2)$ и $\gamma(t_1) = \gamma(t_2)$, что и доказывает периодичность выходной последовательности в силу детерминированности канонических уравнений.

Пусть теперь для любого h выполнено, что $|M(h)| < \infty$. Заметим, что $M(h+1) \supseteq M(h)$. Значит, начиная с некоторого номера H, будет выполнено, что $|M(h)| > 0$ при $h > H$ и, следовательно, корректно определена последовательность $t_h = \max M(h)$. В последовательности t_h найдутся такие $t_{h_1} < t_{h_2}$, что $q(t_{h_1}) = q(t_{h_2})$ и $z(t_{h_1}) = z(t_{h_2})$. Из определения последовательности t_h следует, что функционирование автомата, начиная с моментов t_h, зависит лишь от верхнего символа магазина и состояния автомата. Тогда из детерминированности канонических уравнений получаем, что для любого неотрицательного целого τ выполнено $q(t_{h_1} + \tau) = q(t_{h_2} + \tau)$ и $z(t_{h_1} + \tau) = z(t_{h_2} + \tau)$, откуда и следует периодичность последовательностей $q(t)$ и $z(t)$ и выходной последовательности. □

3.2. Верхняя оценка

Теорема 2. *При* $k > 1$

$$L(n, m, k) \leq \frac{n(k^{nm+1} - 1)}{k - 1}.$$

Доказательство. Рассмотрим произвольный автономный автомат с магазинной памятью $P = (Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0)$ из $\mathcal{M}_0(n, m, k)$ и докажем оценку для $L(P)$. Не ограничивая общность рассуждения, можно считать, что у выходной последовательности отсутствует предпериод и что автомат имеет самую общую функцию выхода, то есть $B = Q \times \Gamma \cup \{\lambda\}$ и $\psi(q, z) = (q, z)$. Пусть последовательности $q(t), \gamma(t), z(t)$ заданы каноническими уравнениями автомата P.

Рассмотрим несколько случаев.

Пусть автомат P достигает дна магазина бесконечное число раз, то есть любой записанный символ будет удален из магазина. В этом случае для всех достижимых пар из $Q \times \Gamma^*$ определены функции ω и π. Нас будут интересовать значения функций на однобуквенных словах. Причем для каждого правила записи в магазин $\eta(q, z) = \alpha(1)...\alpha(\ell)$ можно записать, что

$$\omega(q, z) = 1 + \omega(q_\ell, \alpha(\ell)) + \omega(q_{\ell-1}, \alpha(\ell - 1)) + ... + \omega(q_1, \alpha(1)),$$

где $q_\ell = \varphi(q, z)$, и $q_i = \pi(q_{i+1}, \alpha(i + 1))$.

Таким образом, можно составить систему линейных уравнений на значения $w(q, z)$. Пусть вектор $\vec{\omega} = (\omega_1, ..., \omega_{nm})$ — решение этой системы, причем упорядоченное по возрастанию. Очевидно, что $\omega_1 = 1$, $\omega_i \leq 1 + k\omega_{i-1}$ при $i > 1$. Из этих соотношений следует, что

$$\omega_i \leq \sum_{j=0}^{i-1} k^j.$$

Значит, для длины периода выполнено

$$L(P) \leq \sum_{q \in Q} \omega(q, \lambda) \leq n(1 + k\omega_1) \leq n \sum_{i=0}^{nm} k^i \leq \frac{n(k^{nm+1} - 1)}{k - 1}.$$

Рассмотрим следующий случай. Пусть последовательность $|\gamma(t)|$ ограничена и $|\gamma(t)| > 0$. Рассмотрим $\ell = \min\limits_{0<t\leq L(P)} |\gamma(t)|$. Обозначим $\gamma' = \gamma(t_0)$ и $q' = q(t_0)$, где t_0 таково, что $|\gamma(t_0)| = l$. Не ограничивая общности рассуждения, можно считать, что $\gamma_0 = \gamma'$ и $q_0 = q'$. Рассмотрим автомат P', который получится из автомата P заменой начального слова в магазине на $LS(\gamma')$. Очевидно, что P и P' геренируют одни и те же периодические последовательности. Теперь изменим поведение автомата P' следующим образом. Тот такт работы, когда у автомата P'

в магазине находится однобуквенное слово $LS(\gamma')$, а сам автомат находится в состоянии q', разобьем на два такта: в первый такт мы стираем $LS(\gamma')$ и остаемся в том же состоянии q', а во втором такте пишем в магазин нужное слово и переходим в следующее состояние. Таким образом, полученный автомат удовлетворяет предыдущему случаю, а длина периода последовательности, которую он генерирует на 1 больше, чем у автомата P. Таким образом, оценка верна и в данном случае.

Рассмотрим последний случай. Пусть последовательность $|\gamma(t)|$ не ограничена. Пусть $\ell = \min\limits_{0<t\leq L(P)} |\gamma(t)|$. Обозначим $\gamma' = \gamma(t_0)$ и $q' = q(t_0)$, где t_0 таково, что $|\gamma(t_0)| = l$. Не ограничивая общности рассуждения, можно считать, что $\gamma_0 = \gamma'$ и $q_0 = q'$. Рассмотрим автомат P', который получится из автомата P заменой начального слова в магазине на $LS(\gamma')$. Очевидно, что P и P' геренируют одни и те же периодические последовательности. Теперь изменим поведение автомата P' следующим образом. Добавим состояние q''. Автомат P' из состояния q' переходит в q'', в котором опустошается магазин. При пустом магазине в состоянии q'' P' ведет себя так же, как автомат P, когда находится в состоянии q' и видит символ $LS(\gamma')$ магазина. Полученный автомат удовлетворяет первому рассматриваемому случаю. Учитывая, что $\omega(q'', z) = 1$, видим, что добавленное состояние не увеличивает оценку, что и завершает доказательство.

□

Пример 1.

Рассмотрим автомат $P_1 = (Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0)$, где $Q = \{q\}$, $B = \{0, 1\}$, $\Gamma = \{1, 2, ..., m\}$, $q_0 = q$, $\gamma_0 = \lambda$. Функция переходов тривиальна. Функция выхода выдает 1, если магазин пуст; в остальных случаях — 0. Функцию памяти определим следующим образом:

$$\eta(q, z) = \begin{cases} 1^k, \text{ если } z = \lambda, \\ (i+1)^k, \text{ если } z = i < m, \\ \lambda, \text{ если } z = m, \end{cases}$$

где натуральное число $k > 1$. Для данного автомата выпишем систему:

$$\begin{cases} \omega(q,\lambda) = 1 + k\omega(q,1), \\ \omega(q,1) = 1 + k\omega(q,2), \\ ... \\ \omega(q,i) = 1 + k\omega(q,i+1), \\ ... \\ \omega(q,m-1) = 1 + k\omega(q,m), \\ \omega(q,m) = 1. \end{cases}$$

Длиной периода в данном автомате можно считать количество тактов работы автомата между пустыми состояниями магазина, то есть $\omega(q,\lambda)$. Из системы видно, что

$$\omega(q,\lambda) = \sum_{i=0}^{m} k^i.$$

Этот пример показывает достижимость оценки сверху из теоремы для случая $|Q| = 1$, то есть из него следует, что для автомата с одним состоянием верхняя и нижняя оценки совпадают, то есть верна следующая теорема.

Теорема 3. *При $k > 1$*

$$L(1,m,k) = \frac{(k^{m+1}-1)}{k-1}.$$

3.3. Нижняя оценка

Лемма 1. *Пусть дана система уравнений*

$$\begin{cases} x_0 = a + bx_1, \\ x_1 = a + bx_2, \\ ... \\ x_{m-1} = a + bx_m, \\ x_m = c, \end{cases}$$

где a, b, c — некоторые действительные параметры, причем $b \neq 1$. Тогда

$$x_0 = a\frac{b^m - 1}{b-1} + b^m c.$$

Доказательство.

$$x_0 = a + bx_1 = a + b(a + bx_2) = a + ab + b^2x_2 = a + ab + ab^2 + b^3x_3 =$$

$$= ... = a(1 + b + b^2 + ... + b^{m-1}) + b^m x_m.$$

Отсюда и получаем, что

$$x_0 = a\frac{b^m - 1}{b - 1} + b^m c,$$

что и требовалось доказать. □

Пример 2.

Пусть автономный автомат с магазинной памятью

$$P_m = (Q, B, \Gamma, \varphi, \eta, \psi, q_n, \lambda) \in \mathcal{M}_0(n, m, k),$$

где $B = \{0, 1\}$, $Q = \{q_1, ..., q_n\}$, $\Gamma = \{1, ..., m\}$, $m > 1$,

$$\psi(q, z) = \begin{cases} 1, \text{ если } q = q_1, \ z = \lambda, \\ 0, \text{ иначе,} \end{cases}$$

$$\varphi(q, z) = \begin{cases} q_{i+1}, \text{ если } q = q_i, \ i \neq n, \ z = m - 1, \\ q_{i-1}, \text{ если } q = q_i, \ i \neq 0, \ z = m, \\ q, \text{ иначе,} \end{cases}$$

$$\eta(q, z) = \begin{cases} (z + 1)^k, \text{ если } z < m - 1, \\ m1^{k-1}, \text{ если } q \neq q_n, \ z = m - 1, \\ \lambda, \text{ иначе.,} \end{cases}$$

На рисунке 1 приведем диаграмму этого автомата. Переходы автомата описываются следующим шаблоном z/η, то есть из данного состояния q, при значении верхнего символа магазина z, автомат записывает на выходную ленту $\psi(q, z)$, а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка. Начальное состояние помечено символом " $*$ " и через запятую указана начальная запись в магазине. Для удобства записи формул будем считать, что пустому значению λ соотвествует значение $z = 0$.

Из уравнений следует, что

$$\omega(q, z) = 1 + k\omega(q, z + 1), \ z < m - 1.$$

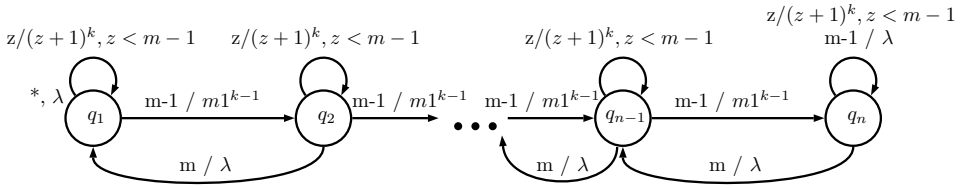

Рис. 1. Диаграмма автомата P_m.

Очевидно, что $\omega(q_n, m-1) = 1$. При $i \neq n$ имеем:

$$\omega(q_i, m) = 1 + \omega(q_{i+1}, m1^{k-1}) = 1 + (k-1)\omega(q_{i+1}, 1) + \omega(q_{i+1}, m).$$

Пусть ω_0 — длина периода последовательности, сгенерированной автоматом с магазинной памятью. Тогда $\omega_0 = 1 + k\omega(q_1, 1)$. Обозначая $\omega_{i,j} = \omega(q_i, j)$ получаем следующую систему линейных уравнений при $m > 2$ (случай $m = 2$ будет рассмотрен отдельно):

$$\begin{cases} \omega_{n,m-1} = 1, \\ \omega_{n,m-2} = 1 + k\omega_{n,m-1}, \\ \ldots \\ \omega_{n,i} = 1 + k\omega_{n,i+1}, \\ \ldots \\ \omega_{n,1} = 1 + k\omega_{n,2}, \\ \omega_{n-1,m-1} = 2 + (k-1)\omega_{n,1}, \\ \ldots \\ \omega_{j,m-2} = 1 + k\omega_{j,m-1}, \\ \ldots \\ \omega_{j,i} = 1 + k\omega_{j,i+1}, \\ \ldots \\ \omega_{j,1} = 1 + k\omega_{j,2}, \\ \omega_{j-1,m-1} = 2 + (k-1)\omega_{j,1}, \\ \ldots \\ \omega_{1,1} = 1 + k\omega_{1,2}, \\ \omega_0 = 1 + k\omega_{1,1}. \end{cases}$$

Применяя лемму 1 к уравнениям вида $w_{i,j} = 1 + kw_{i,j+1}$ при каждом фиксированном i и $j = 1, ..., m-2$, удается получить следующую систему уравнений:

$$\begin{cases} \omega_{n,m-1} = 1, \\ \omega_{n,1} = \frac{k^{m-2}-1}{k-1} + \omega_{n,m-1}k^{m-2}, \\ \omega_{n-1,m-1} = 2 + (k-1)\omega_{n,1}, \\ ... \\ \omega_{i,1} = \frac{k^{m-2}-1}{k-1} + \omega_{i,m-1}k^{m-2}, \\ \omega_{i-1,m-1} = 2 + (k-1)\omega_{i,1}, \\ ... \\ \omega_{2,1} = \frac{k^{m-2}-1}{k-1} + \omega_{2,m-1}k^{m-2}, \\ \omega_{1,m-1} = 2 + (k-1)\omega_{2,1}, \\ \omega_0 = \frac{k^{m-1}-1}{k-1} + k^{m-1}\omega_{1,m-1}. \end{cases}$$

Преобразовывая дальше, получаем:

$$\begin{cases} \omega_{n,m-1} = 1, \\ \omega_{n-1,m-1} = 1 + k^{m-2} + \omega_{n,m-1}(k^{m-1} - k^{m-2}), \\ ... \\ \omega_{i-1,m-1} = 1 + k^{m-2} + \omega_{i,m-1}(k^{m-1} - k^{m-2}), \\ ... \\ \omega_{1,m-1} = 1 + k^{m-2} + \omega_{2,m-1}(k^{m-1} - k^{m-2}), \\ \omega_0 = \frac{k^{m-1}-1}{k-1} + k^{m-1}\omega_{1,m-1}. \end{cases}$$

К полученной системе снова применим лемму 1. Получаем, что

$$\begin{cases} \omega_{1,m-1} = (1 + k^{m-2})\frac{(k^{m-1}-k^{m-2})^{n-1}-1}{k^{m-1}-k^{m-2}-1} + (k^{m-1} - k^{m-2})^{n-1}, \\ \omega_0 = \frac{k^{m-1}-1}{k-1} + k^{m-1}\omega_{1,m-1}. \end{cases}$$

Откуда находим период выходной последовательности:

$$\omega_0 = \frac{k^{m-1}-1}{k-1} + k^{m-1}((1+k^{m-2})\frac{(k^{m-1}-k^{m-2})^{n-1}-1}{k^{m-1}-k^{m-2}-1} + (k^{m-1}-k^{m-2})^{n-1}).$$

Теперь перейдем к рассмотрению случая, когда $m = 2$. В этом случае получается следующая система уравнений:

$$\begin{cases} \omega_{n,1} = 1, \\ \omega_{n-1,1} = 2 + (k-1)\omega_{n,1}, \\ ... \\ \omega_{i-1,1} = 2 + (k-1)\omega_{i,1}, \\ ... \\ \omega_{1,m-1} = 2 + (k-1)\omega_{2,1}, \\ \omega_0 = 1 + k\omega_{1,m-1}. \end{cases}$$

Применяя лемму 1 и преобразовывая, получаем, что

$$\omega_0 = \begin{cases} 4n-1, \text{ если } k = 2, \\ 1 + \frac{k}{k-2}((k-1)^n + (k-1)^{n-1} - 2), \text{ если } k > 2. \end{cases}$$

Объединяя обе формулы и учитывая, что $L(P_m) = \omega_0$, получаем итоговую:

$$L(P_m) = \begin{cases} 4n-1, \text{ если } m = 2,\ k = 2, \\ \frac{k^{m-1}-1}{k-1} + k^{m-1}((1+k^{m-2})\frac{(k^{m-1}-k^{m-2})^{n-1}-1}{k^{m-1}-k^{m-2}-1} + (k^{m-1}-k^{m-2})^{n-1}), \text{ иначе.} \end{cases}$$

К сожалению, данный пример автомата для случая $k = 2,\ m = 2$ вырождается, то есть длина периода в этом случае существенно отличается. Поэтому рассмотрим следующий пример.

Пример 3.

Пусть автономный автомат с магазинной памятью

$$P(n') = (Q, B, \Gamma, \varphi, \eta, \psi, q_s^1, \lambda) \in \mathcal{M}_0(n, m, k),$$

где $n' \in \mathbb{N}$ — параметр, $B = \{0,1\}$, $Q = \bigsqcup_{i=1}^{n'} Q_i$, где $Q_i = \{q_s^i, q_{s1}^i, q_{s2}^i, q_1^i, q_2^i, ..., q_8^i\}$, $\Gamma = \{1,2\}$,

$$\psi(q,z) = \begin{cases} 1, \text{ если } q = q_s^1,\ z = \lambda, \\ 0, \text{ иначе,} \end{cases}$$

$$\varphi(q,z)=\begin{cases} q_s^i,\ \text{если } q=q_{s2}^{i+1},\ z=2,\ i<n', \\ q_s^i,\ \text{если } q=q_8^{i-1},\ i>1, \\ q_{s1}^i,\ \text{если } q=q_s^i,\ z=1, \\ q_{s2}^i,\ \text{если } q=q_s^i,\ z=2, \\ q_1^i,\ \text{если } q=q_s^i,\ z=\lambda, \\ q_2^i,\ \text{если } q=q_1^i, \\ q_3^i,\ \text{если } q=q_2^i, \\ q_3^i,\ \text{если } q=q_{s1}^i,\ z=1, \\ q_4^i,\ \text{если } q=q_3^i, \\ q_5^i,\ \text{если } q=q_4^i, \\ q_5^i,\ \text{если } q=q_{s2}^i,\ z=1, \\ q_6^i,\ \text{если } q=q_5^i, \\ q_7^i,\ \text{если } q=q_6^i, \\ q_7^i,\ \text{если } q=q_{s1}^i,\ z=2,\ i<n', \\ q_8^i,\ \text{если } q=q_7^i,\ i<n', \\ q_s^{n'},\ \text{если } q=q_{s1}^{n'},\ z=2, \\ q_s^{n'},\ \text{если } q=q_7^{n'}, \end{cases}$$

$$\eta(q,z) = \begin{cases} \lambda, \text{ если } q = q_{s2}^{i+1},\ z = 2,\ i < n', \\ 11, \text{ если } q = q_8^{i-1},\ i > 1, \\ \lambda, \text{ если } q = q_s^i,\ z = 1, \\ \lambda, \text{ если } q = q_s^i,\ z = 2, \\ 1x, \text{ если } q = q_s^i,\ z = \lambda, \\ 1x, \text{ если } q = q_1^i, \\ 1x, \text{ если } q = q_2^i, \\ 1x, \text{ если } q = q_{s1}^i,\ z = 1, \\ 2x, \text{ если } q = q_3^i, \\ 2x, \text{ если } q = q_4^i, \\ 2x, \text{ если } q = q_{s2}^i,\ z = 1, \\ 1x, \text{ если } q = q_5^i, \\ 2x, \text{ если } q = q_6^i, \\ 2x, \text{ если } q = q_{s1}^i,\ z = 2,\ i < n', \\ 2x, \text{ если } q = q_7^i,\ i < n', \\ \lambda, \text{ если } q = q_{s1}^{n'},\ z = 2, \\ 1, \text{ если } q = q_7^{n'}. \end{cases}$$

На рисунке 2 приведем диаграмму этого автомата. Переходы автомата описываются следующим шаблоном z/η, то есть из данного состояния, при значении верхнего символа магазина z, автомат записывает на выходную ленту $\psi(q,z)$, а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка. Начальное состояние помечено символом " $*$ " и через запятую указана начальная запись в магазине. Для удобства записи формул будем считать, что пустому значению λ соотвествует значение $z = 0$.

Данный автомат имитирует работу автомата из предыдущего примера с n' состояниями, $k = 2$, $m = 4$. Обозначим его P'. Поскольку в текущем случае $\Gamma = \{1, 2\}$, то чтобы имитировать автомат мы будем использовать кодировку, приведенную в таблице 1.

Каждому состоянию P' соотвествует множество состояний Q_i. Текущий автомат устроен таким образом, что в состоянии q_s^i в магазине будет записан корректный код. И каждому переход из состояния q_i в q_j автомата P' соовествует переход из состояний q_s^i в q_s^j текущего автомата с

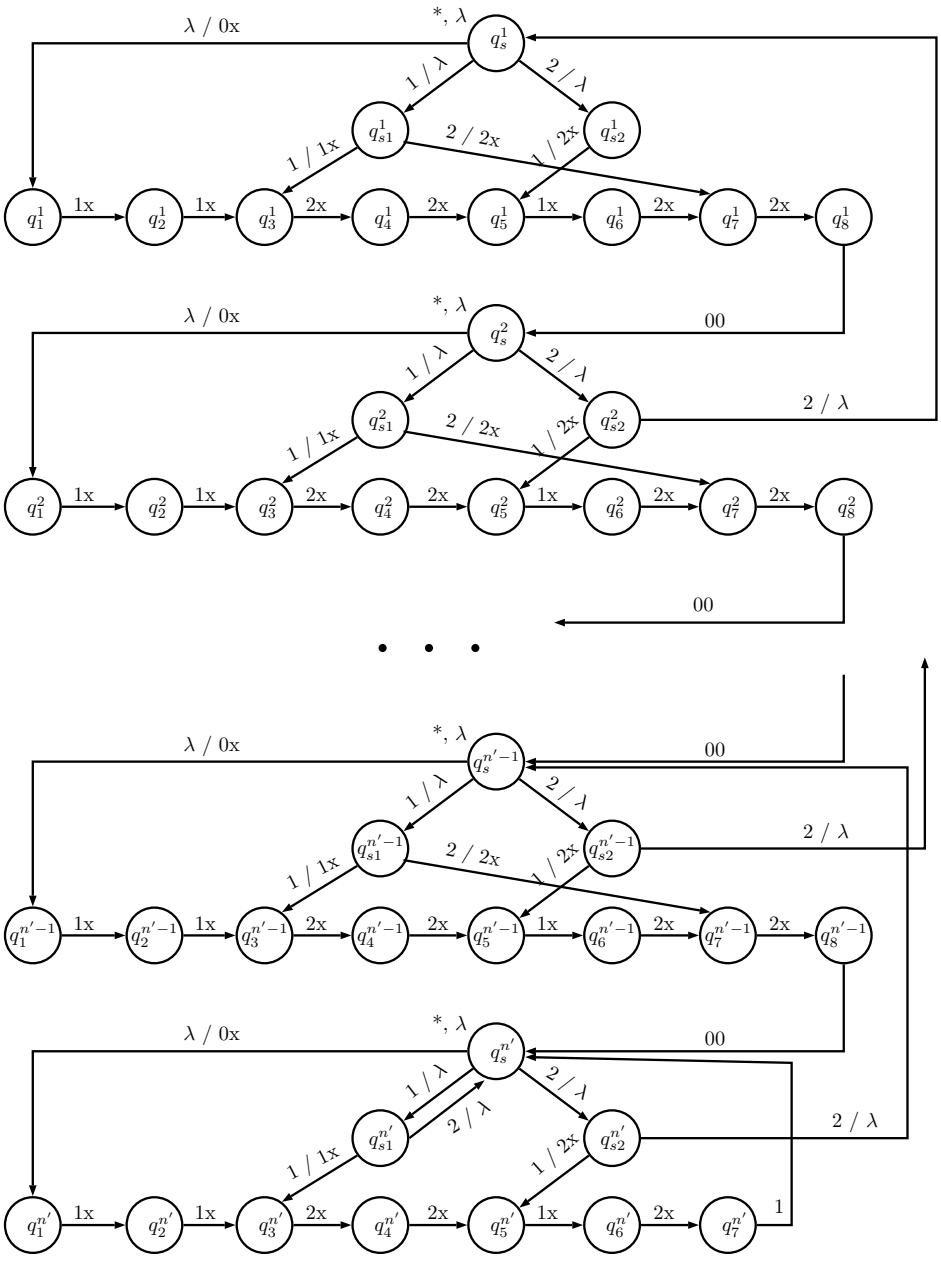

Рис. 2. Диаграмма автомата $P(n')$.

#1	11
#2	12
#3	21
#4	22

Таблица 1. Используемая кодировка символов.

:

аналогичной трансформацией магазина. Заметим, что в текущем случае на этот переход может потребоваться более одного такта.

Теперь, когда стало понятно из каких соображений строился автомат, строго подсчитаем длину периода выходящей последовательности.

Из уравнений автомата получаем:

$$\omega(q_s^{n'}, \#3) = 2,$$

$$\omega(q_s^{n'}, \#2) = 5 + \omega(q_s^{n'}, \#3\#3) = 5 + 2\omega(q_s^{n'}, \#3) = 9,$$

$$\omega(q_s^{n'}, \#1) = 7 + \omega(q_s^{n'}, \#2\#3\#3) = 7 + 2\omega(q_s^{n'}, \#3) + \omega(q_s^{n'}, \#2) = 20.$$

Пусть $1 < i < n'$. Тогда

$$\omega(q_s^i, \#3) = 4 + \omega(q_s^{i+1}, \#4\#1) = 4 + \omega(q_s^{i+1}, \#4) + \omega(q_s^{i+1}, \#1) =$$

$$= 6 + \omega(q_s^{i+1}, \#1)$$

и

$$\omega(q_s^i, \#2) = 6 + \omega(q_s^{i+1}, \#3\#4\#1) =$$

$$= 6 + \omega(q_s^{i+1}, \#1) + \omega(q_s^{i+1}, \#4) + \omega(q_s^i, \#3) =$$

$$= 14 + 2\omega(q_s^{i+1}, \#1).$$

Откуда получаем, что

$$\omega(q_s^i, \#1) = 8 + \omega(q_s^{i+1}, \#2\#3\#4\#1) = 30 + 4\omega(q_s^{i+1}, \#1).$$

Из полученных выше уравнений составим следующую систему:

$$\begin{cases} \omega(q_s^{n'}, \#1) = 20, \\ \omega(q_s^{n'-1}, \#1) = 30 + 4\omega(q_s^{n'}, \#1), \\ ... \\ \omega(q_s^{i-1}, \#1) = 30 + 4\omega(q_s^{i}, \#1), \\ ... \\ \omega(q_s^{1}, \#1) = 30 + 4\omega(q_s^{2}, \#1). \end{cases}$$

Воспользовавшись леммой, получаем, что

$$\omega(q_s^1, \#1) = 30 \cdot 4^{n'-1} - 10.$$

Теперь найдем длину периода

$$\tau = \omega(q_s^1, \lambda) = 9 + \omega(q_s^2, \#1\#2\#3\#4\#1) =$$

$$9 + \omega(q_s^1, \#1\#2\#3) + \omega(q_s^2, \#4\#1) = 11 + \omega(q_s^1, \#1\#2\#3) +$$

$$+\omega(q_s^2, \#1) = 11 + \omega(q_s^1, \#1) + \omega(q_s^1, \#2) + \omega(q_s^1, \#3) + \omega(q_s^2, \#1) =$$

$$= 11 + \omega(q_s^1, \#1) + (14 + 2\omega(q_s^2, \#1)) + (6 + \omega(q_s^{i+1}, \#1)) + \omega(q_s^2, \#1) =$$

$$= 31 + \omega(q_s^1, \#1) + 4\omega(q_s^2, \#1) = 1 + 2\omega(q_s^1, \#1) = 15 \cdot 4^{n'} - 19.$$

Подставляя $n' = \frac{n-1}{9}$, получаем

$$\tau = 15 \cdot 4^{\frac{n-1}{9}} - 19.$$

Из примеров следует, что доказана следующая теорема:

Теорема 4. *При $m > 1$, $k > 1$*

$$L(n, m, k) \geq \begin{cases} 15 \cdot 4^{\frac{n-1}{9}} - 19, & \textit{при } m = 2,\ k = 2, \\ (\frac{k-1}{k})^{n-1} k^{(m-1)n}, & \textit{иначе.} \end{cases}$$

Замечание. При доказательстве нижней оценки было существенно использовано то, что алфавит магазина содержит больше одного символа. В следующем разделе отдельно рассматривается случай однобуквенного магазина.

4. Периодические свойства автономных автоматов с однобуквенным магазином

Для получения оценок на $L(n,1,k)$ введем дополнительные ограничения на рассматриваемые автоматы. Пусть P — автономный автомат с магазинной памятью с однобуквенным магазином. Будем считать, что P генерирует периодическую последовательность без предпериода и все состояния достижимые и встречаются бесконечное число раз в последовательности $q(t)$, заданной каноническими уравнениями. Заметим, что если в последовательности $\gamma(t)$ пустое слово встречается лишь конечное число раз, то из-за отсутствия предпериода магазин не бывает пустым. Поэтому в этом случае P функционируют в точности как автомат без магазина, то есть конечный автомат. Разумеется, этот случай нас не интересует. Поэтому будем считать, что пустое слово в последовательности $\gamma(t)$ будет встречаться бесконечное число раз. Для удобства будем считать, что начальная запись в магазине пустая, то есть $\gamma_0 = \lambda$. Будем рассматривать наиболее общую функцию выхода $\psi(q,z) = (q,z)$, то есть $B = Q \times \Gamma \cup \{\lambda\}$. Очевидно, что наложение описанных ограничений на класс автоматов не меняют максимальную длину периода внутри класса автоматов.

Обозначим через $\mathcal{M}'_0(n,1,k)$ множество автоматов P из $\mathcal{M}'_0(n,1,k)$, для которых выполнены описанные выше ограничения, а именно:

- периодическая последовательность, сгенерированная P, не имеет предпериода;
- все состояния достижимы бесконечное число раз;
- $\gamma_0 = \lambda$;
- $B = Q \times \Gamma \cup \{\lambda\}$ и $\psi(q,z) = (q,z)$.

Очевидно, что выполнено

$$L(n,1,k) = \max_{P \in \mathcal{M}'_0(n,1,k)} L(P),$$

поэтому далее будем рассматривать автоматы только из $\mathcal{M}'_0(n,1,k)$.

Введем еще несколько определений, необходимых для дальнейших рассуждений. Для автомата P выделим множество стирающих состояний

$$S = \{q \in Q \mid \eta(q,1) = \lambda\}.$$

Если $q \in W = Q \backslash S$, то будем говорить, что состояние пишущее. В множестве пишущих состояний выделим подмножество нейтральных состояний

$$N = \{q \in Q \mid \eta(q, 1) = 1\},$$

то есть таких, при прохождении через которые непустое слово, записанное в магазине, не изменяет свою длину.

Если в автомате P найдется множество состояний $C = \{c_1, ..., c_\ell\} \subseteq Q$ такое, что выполнено $\varphi(c_i, 1) = c_{i+1}$ для $i = 1, .., l-1$ и $\varphi(c_\ell, 1) = c_1$, то будем говорить, что C является автоматным циклом. Длиной автоматного цикла C будем называть число состояний в этом цикле.

Для автомата P однозначно определены последовательности состояний и состояний магазина согласно каноническим уравнениям. Будем говорить, что автоматный цикл C достижим, если найдется такой момент времени t_1, что выполнены следующие условия:

1) $\{q(t_1), q(t_1 + 1), ..., q(t_1 + |C| - 1)\} = C$;

2) $z(t_1) = z(t_1 + 1) = ... = z(t_1 + |C| - 1) = 1$.

Каждому автоматному циклу сопоставим индекс — число, на которое изменится длина памяти магазина при одном проходе по нему. Будем называть автоматный цикл стирающим, если индекс отрицательный, то есть количество символов в магазине при одном проходе по циклу уменьшается. Если индекс автоматного цикла неотрицательный, то будем говорить, что автоматный цикл пишущий.

Будем называть конфигурацией автомата пару его состояние и состояние магазина $c(t) = (q(t), \gamma(t))$. Будем говорить, что конфигурация c_2 достижима из конфигурации c_1, и писать $c_1 \Rightarrow c_2$, если автомат с магазинной памятью из конфигурации c_1 перейдет в конфигурацию c_2 через конечное число тактов.

В некоторых случаях нас будет интересовать поведение автомата при непустом магазине. В таких случаях будем говорить, что конфигурация c_2 достижима без опустошения магазина из конфигурации c_1, и писать $c_1 \Rrightarrow c_2$, если конфигурация c_2 достижима из конфигурации c_1 и во всех промежуточных конфигурация, исключая c_1 и c_2, магазин не пуст. Заметим, что и c_1, и c_2 могут иметь пустой магазин.

4.1. Доказательство нижней оценки L(n,1,k)

Пример 4.

Пусть автономный автомат с магазинной памятью

$$P(s) = (Q, B, \Gamma, \varphi, \psi, \eta, r_h, \lambda) \in \mathcal{M}_0(n, 1, k),$$

где $0 < s < n$, $B = \{0, 1\}$, $Q = \{q_1, ..., q_{n-s}, r_1, ..., r_s\}$, $\Gamma = \{1\}$, $h = (((k-1)(n-s+1)+2) \mod s) + 1$

$$\psi(q, z) = \begin{cases} 1, \text{ если } q = q_h, \ z = \lambda, \\ 0, \text{ иначе,} \end{cases}$$

$$\varphi(q, z) = \begin{cases} q_{i+1}, \text{ если } q = q_i, \ i \neq n-s, \\ r_1, \text{ если } q = q_{n-s}, \\ r_{i+1}, \text{ если } q = r_i, \ z = 1, \\ q_1, \text{ если } q = r_h, \ z = \lambda, \\ q_{1+[\frac{(h-1-i) \mod s}{k-1}]}, \text{ если } q = r_i, \ i \neq h, \ z = \lambda, \\ q, \text{ иначе,} \end{cases}$$

$$\eta(q, z) = \begin{cases} 1^k, \text{ если } q = q_i, \\ 1^k, \text{ если } q = r_h, \ z = \lambda, \\ 1^{k-1-((h-1-i) \mod s) \mod (k-1)}, \text{ если } q = r_i, \ i \neq h, \ z = \lambda, \\ \lambda, \text{ иначе.} \end{cases}$$

На рисунке 3 приведем диаграмму этого автомата для $n = 8$, $k = 3$ и $s = 5$. Переходы автомата описываются следующим шаблоном z/η, то есть из данного состояния, при значении верхнего символа магазина z, автомат записывает на выходную ленту $\psi(q, z)$, а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка. Начальное состояние помечено " $*$ " и через запятую указана начальная запись в магазине.

Опишем функционирование описанного выше автомата $P(s)$ и поясним его канонические уравнения. Автомат начинает работу из состояния r_h и с пустым магазином. Далее автомат максимально заполняет магазин, проходя по состояниям $q_1, ..., q_{n-s}$ до тех пор, пока не попадает в стирающий цикл $r_1, ..., r_s$. В состоянии r_1 в магазине записано $(k-1)(n-s+1)+1$ символов. Так как дальше при каждом заполнении магазина мы будем уменьшать на единицу количество записываемых символов, то состояния, в которых, магазин становится пустым, будут

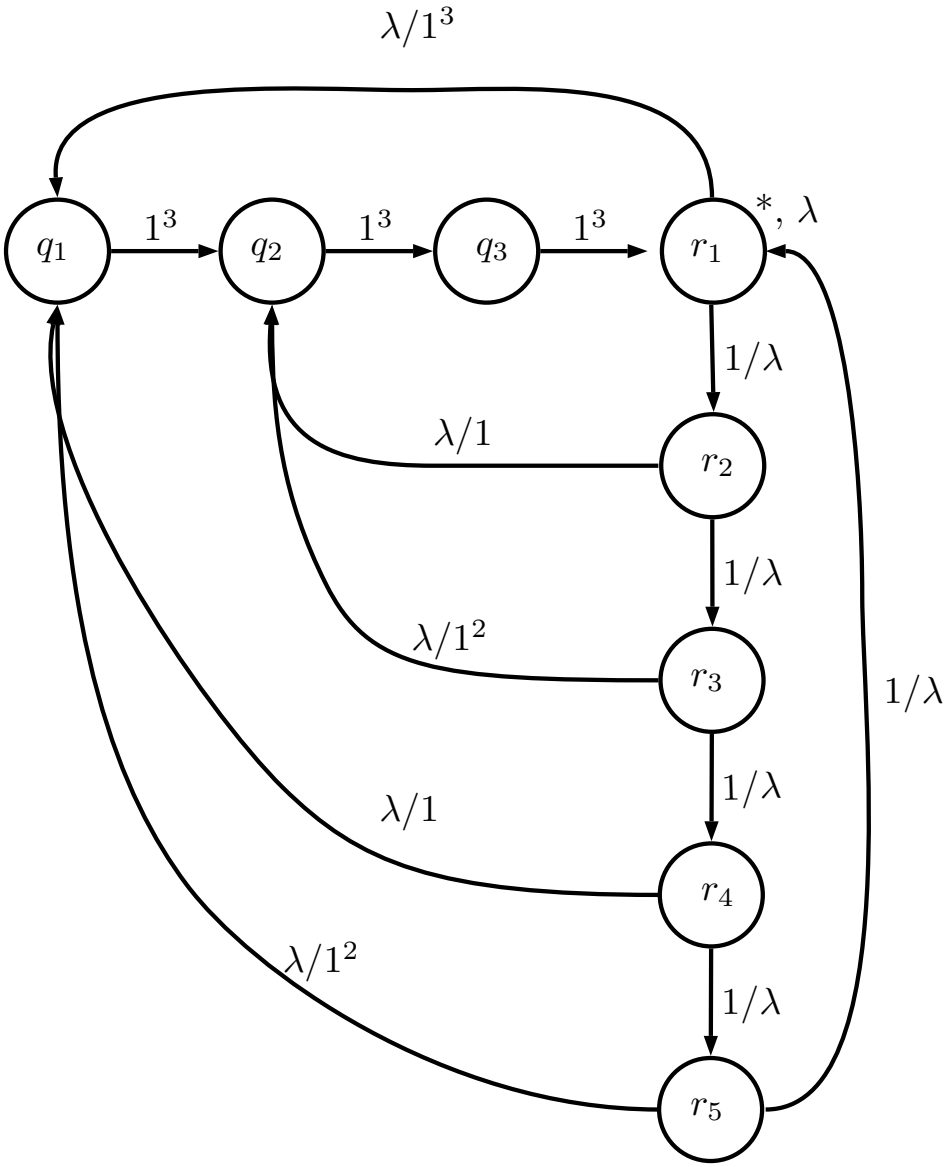

Рис. 3. Диаграмма автомата $P(s)$ при $n = 8$, $k = 3$ и $s = 5$.

меняться последовательно. То есть если мы стартовали из состоянии r_{i+1} при пустом магазине, то, заполнив и опустошив магазин, автомат окажется в состоянии r_i. Исходя из этого, мы и получаем формулу для номера начального состояния. Мы подберем r_h таким, чтобы, заполняя магазин максимально возможным количеством символов, после стирания их попасть в состояние r_{h-1}. Отсюда получаем, что

$$h = (((k-1)(n-s+1)+2) \mod s) + 1.$$

Следующим требующем объяснения моментом в описании уравнений автомата является его поведение при опустошении магазина, то есть в состоянииии r_i и $z = \lambda$. По сказанному выше в состоянии r_h автомат пишет максимально возможное количество символов в магазин. Значит, из этого состояния при пустом магазине автомат должен перейти в состояние q_1 и записать при этом слово длины k в магазин. При следующем опустошении магазина мы окажемся в состоянии r_{h-1}. Из этого состояния начинается заполнение магазина. Причем автомат должен записать на единицу меньше символов в магазин. Следовательно, из состояния r_{h-1} автомат перейдет в состояние q_1, и в магазин будет записано слово длины $k-1$. Продолжая опустошать магазин, автомат будет писать на 1 символ меньше и переходить в состояние q_1 до тех пор, пока не придётся записать один символ. После этого мы уже не сможем перейти в состояние q_1, так как зациклимся. Следовательно, мы должны будем перейти в состояние q_2 и записать в магазин $k-1$ символ по той же причине. И далее при переходе из стирающего цикла мы будем писать от $k-1$ до 1 символа в магазин, после чего будем менять состояние перехода.

Подсчитаем длину периода $L(P(s))$. Удобно считать стирающие такты и записывающие по отдельности:

$$L(P(s)) = \tau_{\text{записи}} + \tau_{\text{стирания}},$$

где

$$\tau_{\text{стирания}} = \sum_{i=0}^{s-1}((n-s+1)(k-1)+1-i) = s(k-1)(n-s+1)+s-\frac{s(s-1)}{2},$$

$$\tau_{\text{записи}} = s(n-s+1) - \sum_{i=0}^{s-2}[\frac{i}{k-1}].$$

Таким образом, длина периода сгенерированной им последовательности равна

$$L(P(s)) = sk(n-s+1) + s - \frac{s(s-1)}{2} - \sum_{i=0}^{s-2}[\frac{i}{k-1}].$$

Лемма 2. *Для натуральных s, $k > 1$ выполнено*

$$\frac{s^2}{2(k-1)} - \frac{3s}{2} \leq \sum_{i=0}^{s-2}[\frac{i}{k-1}] \leq \frac{s^2}{2(k-1)} + \frac{3s}{2}.$$

Доказательство. Пусть $f(s) = \sum\limits_{i=0}^{s-1}[\frac{i}{k-1}]$. Тогда

$$f(s) = (k-1)\sum_{i=0}^{[\frac{s}{k-1}]-1} i + [\frac{s}{k-1}](s \mod (k-1)) =$$

$$= (k-1)\frac{[\frac{s}{k-1}]([\frac{s}{k-1}]-1)}{2} + [\frac{s}{k-1}](s \mod (k-1)).$$

Отсюда получаем, что

$$f(s) \leq (k-1)\frac{\frac{s}{k-1}(\frac{s}{k-1}-1)}{2} = \frac{s^2}{2(k-1)} - \frac{s}{2}$$

и

$$f(s) \geq (k-1)\frac{(\frac{s}{k-1}+1)\frac{s}{k-1}}{2} + s = \frac{s^2}{2(k-1)} + \frac{3s}{2}.$$

Так как

$$\sum_{i=0}^{s-2}[\frac{i}{k-1}] = f(s) - [\frac{s-1}{k-1}],$$

то

$$\frac{s^2}{2(k-1)} - \frac{3s}{2} \leq \sum_{i=0}^{s-2}[\frac{i}{k-1}] \leq \frac{s^2}{2(k-1)} + \frac{3s}{2},$$

что и требовалось доказать.

□

Применяя лемму, получаем, что

$$L(P(s)) \geq sk(n-s+1)+s-\frac{s(s-1)}{2}-\frac{s^2}{2(k-1)}-\frac{3s}{2} = sk(n-s+1)-\frac{ks^2}{2(k-1)}.$$

Полагая $P = P(s)$ при $s = [\frac{k-1}{2k-1}n]$, получаем, что

$$L(P) \geq [\frac{k-1}{2k-1}n]k(n-[\frac{k-1}{2k-1}n]+1) - \frac{k([\frac{k-1}{2k-1}n])^2}{2(k-1)} \geq$$

$$\geq (\frac{k-1}{2k-1}n-1)k(n-\frac{k-1}{2k-1}n+1) - \frac{k(\frac{k-1}{2k-1}n)^2}{2(k-1)} =$$

$$= \frac{k(k-1)}{4k-2}n^2 - \frac{1}{2k-1}n - 1.$$

Данный пример доказывает нижние оценки на $L(n,1,k)$.

Теорема 5. *При $k > 1$ и $n \to \infty$*

$$L(n,1,k) \geq \frac{k(k-1)}{4k-2}n^2(1+o(1)).$$

Теорема 6. *При $n > 1$ и $k \to \infty$*

$$L(n,1,k) \geq \frac{n^2}{4}k(1+o(1)).$$

4.2. Доказательство верхней оценки L(n,1,k)

Сформулируем и докажем несколько вспомогательных утверждений.

Лемма 3. *Пусть P — автомат с магазинной памятью из $\mathcal{M}'_0(n,1,k)$. Тогда существует автомат с магазинной памятью P' из $\mathcal{M}'_0(n,1,k)$, который в процессе функционирования не бывает с пустым магазином два такта подряд, и периоды выходных последовательностей автоматов P и P' отличаются не более чем на n.*

Доказательство. Пусть автомат P при очередном такте стирает последний символ из магазина, оказываясь в некотором состоянии q, и далее проходит еще несколько состояний, не делая записей в магазин. После чего попадает в состояние q_1, в котором пишет непустое слово 1^ℓ и переходит в состояние q_2. Тогда можно трансформировать автомат P так,

чтобы из состояния q автомат сразу переходил в q_2 и писал при этом в магазин 1^ℓ. Делая такую трансформацию для всех аналогичных состояний, получаем автомат P', который удовлетворяет условием леммы, так как внутри одного периода автомат может быть с пустым магазином не более n раз. □

4.2.1. Простая верхняя оценка

Теперь непосредственно приступим к доказательству верхней оценки на $L(n, 1, k)$.

Лемма 4. *Пусть P — автомат с магазинной памятью из $\mathcal{M}'_0(n, 1, k)$. Тогда*

$$L(P) \leq n(h_{max} + 1),$$

где $h_{max} = \max\limits_t |\gamma(t)|$ — максимальное количество символов, которое может быть записано в магазине.

Доказательство. Заметим, что из определения класса $\mathcal{M}'_0(n, 1, k)$ следует, что h_{max} всегда существует, то есть $h_{max} < \infty$. Внутри одного периода автомат может находиться в состоянии q только с разными состояниями магазина от пустого до содержащего h_{max} символов. Суммируя по всем состояниям, получаем требуемую оценку. □

Утверждение 1. *При $k > 1$*

$$L(n, 1, k) \leq (k - 1)n^2 + 2n.$$

Доказательство. Так как среди n состояний должно быть хотя бы одно стирающее, то $n-1$ пишущее состояние не может записать больше $n(k-1)+1$, то есть $h_{max} \leq n(k-1)+1$. Подставляя эту оценку в предыдущую лемму, получаем требуемое. □

4.2.2. Случай пишущего автоматного цикла

Лемма 5. *Пусть P — автомат с магазинной памятью из $\mathcal{M}'_0(n, 1, k)$. Если в P есть достижимый пишущий автоматный цикл, то период сгенерированной P последовательности равен длине этого цикла.*

Доказательство. Если в P есть достижимый пишущий цикл, то автомат не может его покинуть, так как магазин уже никогда не будет пустым в силу неотрицательности индекса. Значит, период будет равен длине цикла. □

Замечание. В силу доказанной леммы далее не имеет смысл рассматривать автоматы с достижимыми пишущими циклами. Будем считать, что если в автомате есть достижимый цикл, то он стирающий.

4.2.3. Случай без автоматных циклов

В этом разделе будет дана оценка на максимальную длину периода выходной последовательсти для автомата без стирающих циклов.

Лемма 6. *Пусть P — автомат с магазинной памятью из $\mathcal{M}'_0(n,1,k)$. Если P не имеет автоматных циклов, то период сгенерированной P последовательности не превосходит $\frac{k-1}{k}n^2+2n$.*

Доказательство. Оценим h_{max}. Так как в P нет автоматных циклов, то h_{max} не может быть большим. Максимально возможное значение h_{max} можно получить следующем образом. Необходимо в автомате иметь максимально возможное число w пишущих по k символов состояний так, чтобы оставшихся $s=n-w$ состояний хватило, чтобы стереть то, что было записано. Все стирания должы быть сделаны в разных состояниях, так как стирающих циклов нет. Отсюда получаем следующее условие:

$$h_{max} \le (w+1)(k-1)+1 = s.$$

Решая, получаем, что

$$h_{max} \le s = \frac{k-1}{k}n+1.$$

Подставляя h_{max} в полученную выше оценку, получаем требуемое. □

Обозначим $L_0(n,k)=\frac{k-1}{2k}n^2+5n$.

Утверждение 2. *Пусть P — автомат с магазинной памятью из класса $\mathcal{M}'_0(n,1,k)$. Если P не имеет автоматных циклов или имеет только недостижимые пищущие автоматные циклы, то период сгенерированной P последовательности не превосходит $L_0(n,k)$.*

Доказательство. При функционировании автомата P найдется последовательность тактов от t_1 до t_2, когда из пустого магазина автомат заполняет магазин до уровня в h_{max} символов, то есть $\gamma(t_1)=\lambda$, $\gamma(t_2)=1^{h_{max}}$ и $\gamma(t)\neq\lambda$ при $t_1<t\le t_2$. Очевидно, что каждое состояние $q(t)$ при $t_1<t\le t_2$ не может встречаться в одном периоде больше, чем

$|\gamma(t)|+1$ раз в силу определения h_{max}. Пусть $h_{max} = 1 + h_0 + h_1(k-1)$, где $0 \le h_0 < k-1$. Нетрудно видеть, что в отрезке от t_1+1 до t_2 найдутся такие t_i, что будет выполнено $|\gamma(t_i)| \le (k-1)i+1$ при $i = 1, ..., h_1$ и $q(t_i) \in W$. Учитывая это, получаем, что

$$L(P) \le (h_{max}+1)(n-h_1) + \sum_{i=1}^{h_1}(2+i(k-1)) =$$

$$= (h_{max}+1)n - \sum_{i=1}^{h_1}(h_{max} - 2 - i(k-1)) =$$

$$= (h_{max}+1)n - \sum_{i=1}^{h_1}(h_0 + (h_1 - i)(k-1) - 1) =$$

$$= (h_{max}+1)n + h_1 - h_0 h_1 - \frac{(k-1)h_1(h_1-1)}{2} =$$

$$= (h_{max}+1)n + \frac{h_1(k+2-h_0-h_{max})}{2} \le (h_{max}+1)n + \frac{h_{max}(k+2-h_{max})}{2(k-1)}.$$

Каждому состоянию q сопоставим число $h(q)$, равное максимальному числу символов в магазине, которое может быть при достижении этого состояния. Заметим, что оценку удалось улучшить за счет уточнения функции $h(q)$ для некоторых пишущих состоятий q пользуясь тем, что автомат за один такт может писать ограниченное количество символов. Теперь сделаем аналогичное уточнение при стирании магазина, то есть для стирающих состояний.

Покажем, что в P для любого натурального d такого, что $1 \le d < h_{max}$, найдется такое стирающее q, что $h(q) = d$. Рассмотрим последовательность тактов от t_2 до t_3, когда автомат стирает магазин от h_{max} до пустого, то есть $\gamma(t_2) = 1^{h_{max}}$, $\gamma(t_3) = \lambda$ и $\gamma(t) \ne \lambda$ при $t_2 < t < t_3$. В этом отрезке найдется такой номер t', что $q(t') = q_0 \in S$ и $|\gamma(t')| = d$. Если $h(q_0) = d$, то заканчиваем процедуру поиска. Если $h(q_0) > d$, то это означает, что найдется момент времени t_4 такой, что $q(t_4) = q_0$ и $|\gamma(t_4)| > d$. Тогда пусть t_5 таково, что $\gamma(t_5) = \lambda$ и при $t_4 < t < t_5$ $\gamma(t_5) \ne \lambda$. На этом новом отрезке выберем аналогичным образом t'' такое, что $q(t'') = q_1 \in S$ и $|\gamma(t')| = d$ и так далее. Возможны два результата работы этой процедуры: мы найдем такое q_i, что $h(q_i) = d$ или последовательность $q_0, q_1, ..., q_\ell$ зациклится. Если последовательность зациклилась, то это означает, что

в автомате есть стирающий автоматный цикл, что противоречит условию. Значит, данная процедура всегда приводит к нахождению требуемого состояния.

Таким образом, мы можем понизить верхнюю оценку еще на $\frac{h_{max}(h_{max}-1)}{2}$, то есть получаем, что выполнено:

$$L(P) \leq (h_{max}+1)n + \frac{h_{max}(k+2-h_{max})}{2(k-1)} - \frac{h_{max}(h_{max}-1)}{2}.$$

Максимизируя выражение по h_{max} при условии, что $0 \leq h_{max} \leq \frac{(k-1)n}{k} + 1$, получаем, что $L(P) \leq \frac{k-1}{2k}n^2 + 5n$, что и требовалось доказать.

□

Пример 5.

Для $n \geq 3$ и $k \geq 2$ рассмотрим автономный автомат с магазинной памятью $P_0 = (Q, B, \Gamma, \varphi, \psi, \eta, r_s, \lambda) \in \mathcal{M}_0(n, 1, k)$, где $s = n - 1 - [\frac{n-3}{k}]$, $x = s - 1 - (k-1)(n-s-1)$, $B = \{0, 1\}$, $Q = \{q_1, ..., q_{n-s}, r_1, r_2 ..., r_s\}$, $\Gamma = \{1\}$,

$$\psi(q, z) = \begin{cases} 1, \text{ если } q = r_2, \ z = \lambda, \\ 0, \text{ иначе,} \end{cases}$$

$$\varphi(q, z) = \begin{cases} q_{i+1}, \text{ если } q = q_i, \ i \neq n-s, \\ r_1, \text{ если } q = q_{n-s}, \\ r_{i+1}, \text{ если } q = r_i, \ i \neq s, \ z = 1, \\ q_{n-s}, \text{ если } q = r_s, \ z = \lambda, \\ q_1, \text{ если } q = r_{s-1}, \ z = \lambda, \\ q_{n-s-[\frac{i-1}{k-1}]}, \text{ если } q = r_i, \ 1 < i < s-1, \ z = \lambda, \\ q, \text{ иначе,} \end{cases}$$

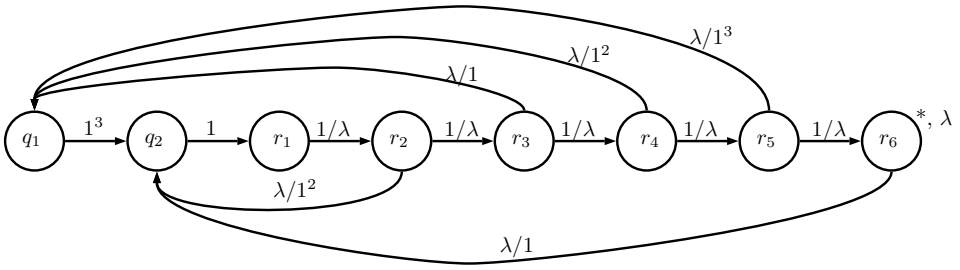

Рис. 4. Диаграмма автомата P_0 при $n = 8$, $k = 3$.

$$\eta(q,z) = \begin{cases} 1^k, \text{ если } q = q_i,\ i \neq n-s, \\ 1, \text{ если } q = q_{n-s}, \\ \lambda, \text{ если } q = r_i,\ z = 1, \\ 1, \text{ если } q = r_s,\ z = \lambda, \\ 1^x, \text{ если } q = r_{s-1},\ z = \lambda, \\ 1^{k-1}, \text{ если } q = r_i,\ z = \lambda,\ i \mod (k-1) = 0, \\ 1^{i \mod (k-1)}, \text{ если } q = r_i,\ z = \lambda,\ i \mod (k-1) \neq 0, \\ \lambda, \text{ иначе.} \end{cases}$$

На рисунке 4 приведем диаграмму этого автомата для $n = 8$ и $k = 3$. Переходы автомата описываются следующим шаблоном z/η, то есть из данного состояния, при значении верхнего символа магазина z, автомат записывает на выходную ленту $\psi(q,z)$, а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка. Начальное состояние помечено " $*$ " и через запятую указана начальная запись в магазине.

Опишем функционирование описанного выше автомата P_0 и поясним его канонические уравнения. Состояния автомата поделены на две группы: $\{q_1, ..., q_{n-s}\}$ — состояния, в которых происходит наполнение магазина, и состояния $\{r_1, ..., r_s\}$, в которых происходит опустошение магазина. Автомат начинает свою работу из состояния r_s с пустым магазином. Далее автомат переходит в первую группу состояний, где происходит запись в магазин, после заполнения автомат переходит во вторую группу состояний, а именно: в состояние q_1 с одним записанным символом в магазине. Далее происходит опустошение. После чего подобные итерации повторяются с той лишь разницей, что каждую последующую итерацию

количество записанных в магазин символов увеличивается на 1 вплоть до значения $s-1$. После стирания $s-1$ символа автомат опять попадает в состояние r_s.

Аналогично предыдущему примеру получаем, что

$$L(P_0) = \frac{(s-1)s}{2} + (s-1)(n-s) + x - \sum_{i=0}^{s-2-x} [\frac{i}{k-1}].$$

Оценим $L(P_0)$, пользуясь леммой из предыдущего примера, и упростим выражение:

$$L(P_0) \geq \frac{(s-1)s}{2} + (s-1)(n-s) + x - \frac{(s-x)^2}{2(k-1)} - \frac{3(s-x)}{2} \geq sn - \frac{s^2 k}{2(k-1)} - s.$$

Далее подставим оценки на s:

$$L(P_0) \geq n(n-2-\frac{n-3}{k}) - \frac{(n-1-\frac{n-3}{k})^2 k}{2(k-1)} + (n-1-\frac{n-3}{k}) \geq \frac{k-1}{2k} n^2 - 3n - 2.$$

Замечание. Нижняя оценка, полученная в примере, асимптотически совпадает с доказанной верхней оценкой при $n \to \infty$.

4.2.4. Дополнительные определения

Перейдем к рассмотрению основного случая, когда в автомате с магазинной памятью есть стирающие автоматные циклы.

Пусть в автомате P из $\mathcal{M}'_0(n,1,k)$ есть хотя бы один автоматный цикл. Выберем любой и обозначим C. Тогда для $q \in C$ определим множество состояний $W(q) \subseteq Q \backslash C$, из которых можно попасть в стирающий цикл через q:

$W(q) = \{q' \in Q \backslash C \mid \exists t_1, t_2 : \ q(t_1) = q', \ q(t_2) = q, \forall t : \ t_1 \leq t < t_2, \ \gamma(t) \neq \lambda, \ q(t) \notin C\}$.

Заметим, что для различных $q_1 \in C$ и $q_2 \in C$ выполнено $W(q_1) \cap W(q_2) = \emptyset$. Для всех состояний из $W(q)$ будем говорить, что q является точкой входа в автоматный цикл.

Для стирающего цикла C определим множество состояний $W(C)$, которые попадают в автоматный цикл C:

$$W(C) = \bigcup_{q \in C} W(q).$$

Заметим, что для двух стирающих циклов C_1 и C_2 выполнено $W(C_1) \cap W(C_2) = \emptyset$.

Назовем окресностью стирающего цикла множество состояний $U(C) = C \cup W(C)$. Обозначим U_0 — множество состояний, которые не лежат ни в какой окресности стирающего цикла. Для автомата только со стирающими автоматными циклами $C_1, ..., C_d$ имеем следующее разложение:

$$Q = \bigsqcup_{i=1}^{d} U(C_i) \sqcup U_0.$$

Пусть P — автомат из $\mathcal{M}'_0(n, 1, k)$ с периодом выхода τ. Пусть $q(t)$ — последовательность состояний автомата и $\gamma(t)$ — последовательность слов, записанных в магазине, заданы каноническими уравнениями. Так как эти последовательности периодические, рассмотрим их лишь на номерах от 0 до τ. Пусть $t_1, ..., t_{d+1}$ — множество номеров на этом отрезке, когда магазин пуст. Не ограничивая общности, будем считать, что $0 = t_1 < t_2 < ... < t_d < t_{d+1} = \tau$. Рассмотрим полуинтервал $(t_i, t_{i+1}]$, на котором функционирует автомат P. На этой последовательности тактов автомат порождает подпоследовательности состояний $\{q(t)\}_{t_i+1}^{t_{i+1}}$ и слов $\{\gamma(t)\}_{t_i+1}^{t_{i+1}}$, записанных в магазин. Эту пару подпоследовательностей назовем этапом функционирования автомата и будем обозначать I_i. Обозначим длину этапа $|I_i|$ — количество тактов работы автомата в этапе. Для P однозначно определено представление периода в виде упорядоченного множества этапов $(I_1, I_2, ..., I_d)$. Обозначим это отображение $I(P)$. Описание функционирование автомата как последовательности этапов важно, так как имеет довольно интересные свойства, описываемые в следующей лемме.

Лемма 7. *Пусть P — автомат из $\mathcal{M}'_0(n, 1, k)$ и для него выполнено $I(P) = (I_1, ..., I_d)$. Тогда выполнены следующие утверждения:*

1) *Для любой перестановки σ на d элементах найдется автомат P_σ из $\mathcal{M}'_0(n, 1, k)$ такой, что его период будет описываться последовательностью этапов $I(P_\sigma) = (I_{\sigma(1)}, ..., I_{\sigma(d)})$.*

2) *Для любого подмножества этапов $I_{j_1}, ..., I_{j_h}$ найдется автомат P' из $\mathcal{M}'_0(n, 1, k)$ такой, что $I(P') = (I_{j_1}, ..., I_{j_h})$.*

Доказательство. Нетрудно видеть, что оба автомата P_σ и P' получаются из автомата P изменением его поведения на пустом магазине. □

4.2.5. Случай одного стирающего цикла

Пусть в автомате P из $\mathcal{M}'_0(n,1,k)$ есть ровно один стирающий цикл C длины ℓ со стирающим индексом $-s$. Обозначим $C_W = C \cap W$ — все пишущие состояния автоматного цикла, а $C_S = C \cap S$ — все его стирающие состояния. Пусть $C_{S_0} = \{q \in C_S |\ \exists h > \ell : (q, 1^h) \Rrightarrow (q, \lambda)\}$, а $C_{S_1} = C_S \backslash C_{S_0}$. Нетрудно видеть, что $|C_{S_0}| = s$.

Для каждого состояния q из стирающего цикла C определим функцию стирания $f_C(q,h) : C \times \mathbb{N} \to \mathbb{N}$ — минимальное количество тактов необходимое для достижение пустого магазина из состояния q с записанном в магазине словом длины h. Нетрудно видеть, что если ℓ — длина стрирающего цикла, а s — абсолютное значение стирающего индекса C, то

$$h + \lfloor \frac{h}{s} \rfloor (\ell - s) \le f_C(q,h) \le h + \lceil \frac{h}{s} \rceil (\ell - s) =: f_C^{max}(h).$$

Лемма 8. *В текущих обозначениях при* $\ell \neq n$

$$\sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) = \begin{cases} h_{max} l - \frac{s(s-1)}{2}, & \textit{если } s \le h_{max} - (k-1), \\ \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + h_{max}(\ell - s), & \textit{иначе}, \end{cases},$$

где $s' = \min(s, h_{max} - (k-1))$.

Доказательство. Если $s \le h_{max} - (k-1)$, то

$$\sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) = \sum_{i=0}^{s-1} f_C^{max}(h_{max} - i) =$$

$$= \sum_{i=0}^{s-1} \left(h_{max} - i + \lceil \frac{h_{max} - i}{s} \rceil (\ell - s) \right) =$$

$$= h_{max} s - \frac{s(s-1)}{2} + (\ell - s) \sum_{i=0}^{s-1} \lceil \frac{h_{max} - i}{s} \rceil =$$

$$= h_{max} s - \frac{s(s-1)}{2} + (\ell - s) \sum_{i=0}^{s-1} \frac{h_{max} - i}{s} + \frac{(l-s)(s-1)}{2} =$$

$$= h_{max} s - \frac{s(s-1)}{2} + h_{max}(\ell - s) = h_{max} \ell - \frac{s(s-1)}{2}.$$

Если $s > h_{max} - (k-1)$, то

$$\sum_{i=0}^{s'-1} f_C^{max}(h_{max}-i) = \sum_{i=0}^{h_{max}-k} f_C^{max}(h_{max}-i) =$$

$$= \sum_{i=k}^{h_{max}} f_C^{max}(i) = \sum_{i=k}^{h_{max}} \left(i + \lceil \frac{i}{s} \rceil (\ell - s) \right) =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) \sum_{i=k}^{h_{max}} \lceil \frac{i}{s} \rceil =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) \left(\sum_{i=k}^{h_{max}-k+1} \lceil \frac{i}{s} \rceil + \sum_{i=h_{max}-k+2}^{h_{max}} \lceil \frac{i}{s} \rceil \right) =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) \left(\sum_{i=k}^{h_{max}-k+1} 1 + \sum_{i=h_{max}-k+2}^{h_{max}} 2 \right) =$$

$$= \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + (\ell - s) h_{max},$$

что и требовалось доказать.

□

Лемма 9. *Пусть P — автомат из $\mathcal{M}'_0(n,1,k)$ и пусть P удовлетворяет следующим условиям:*

1) *в P есть единственный автоматный цикл C с отрицательным стирающем индексом;*

2) *вне этого цикла стирающих состояний нет, то есть $S \subseteq C$.*

Тогда найдется такой автомат из P' из $\mathcal{M}'_0(n,1,k)$, удовлетворяющий тем же условиям, такой, что все состояния вне стирающего цикла при непустом магазине пишут ровно k символов в магазин, при этом выполнено

$$L(P) \leq L(P') + n.$$

Доказательство. Рассмотрим непустое $W(q_*)$ для некоторого $q_* \in C$. Рассмотрим все этапы, которые начинаются с состояния из $W(q_*)$. Любой такой этап можно разделить на две части: это заполнение магазина,

когда текущее состояние не из стирающего цикла, и стирание магазина, когда автомат вошел в стирающий цикл. Заметим, что длина второй части зависит только от количества символов записанных в магазин. Проведем следующую трансформацию автомата. Во всех состояниях q из $W(q_*)$ сделаем $\eta(q,1) = 1^k$, а также изменим переходы и запись в магазин по пустым состояниям стирающего цикла так, чтобы изменения коснулись только рассматриваемых этапов и для каждого рассматриваемого этапа количество символов, записанное в магазин, при первом попадании в стирающий цикл (то есть в q_*) не изменилось. Заметим, что при данной трансформации стирающая часть этапа будем иметь такую же длину, как и раньше. Может так оказаться, что количество тактов, которое автомат заполнял магазин уменьшилось. Если после трансформации среди состояний из $W(q_*)$ возникли недостижимые, то все такие состояния добавим в стирающий цикл как нейтральные сразу после q_*. Таким образом, каждый рассматриваемый этап может уменьшиться не более чем на 1.

Проводя подобные трансформации для всех непустых $W(q)$, построим требуемый автомат P'. Так как количество этапов не превосходит n, то будет верна оценка

$$L(P) \leq L(P') + n,$$

что и требовалось доказать.

□

Обозначим $L_1(n,k) = \frac{k(k-1)}{4k-2}n^2 + (8k+32)n$.

Утверждение 3. *Пусть P — автомат из $\mathcal{M}'_0(n,1,k)$ и пусть P удовлетворяет следующим условиям:*

1) *в P есть единственный автоматный цикл C с отрицательным стирающем индексом;*

2) *вне этого цикла стирающих состояний нет, то есть $S \subseteq C$.*

Тогда

$$L(P) \leq L_1(n,k).$$

Доказательство. Последовательно применяя леммы 3 и 9, далее можно рассматривать автомат P' такой, что при пустом магазине автомат P' должен писать в магазин и для которого при $q \notin C$ выполнено $\eta(q,1) = 1^k$, при этом будет верно, что

$$L(P) \leq L(P') + 2n.$$

Так как начальное слово, записанное в магазине, пустое, то все функционировние автомата устроено следующим образом. Из стирающего цикла при пустом магазине автомат заполняет магазин одним из двух способов: либо он выходит из стирающего цикла и заполняет магазин до тех пор, пока не попадает в стирающий цикл снова, либо, не выходя, переходит в другое состояние стирающего цилка. В стирающем цикле автомат опустошает магазин и так далее повторяется до зацикливания, то есть пока автомат не окажется опять в начальном состоянии с пустым магазином.

Пусть ℓ — длина стирающего цикла C. Пусть $s = |C_{S_0}|$ и $r = |C_{S_1}|$.

Пусть $I(P') = (I_1, I_2, ..., I_{r+s})$ — упорядоченное множество этапов автомата P' таково, что последнее состояние первых s этапов из C_{S_0}. Оценим отдельно $\sum\limits_{i=1}^{s} |I_i|$ и $\sum\limits_{i=s+1}^{s+r} |I_i|$.

Начнем с $\sum\limits_{i=s+1}^{s+r} |I_i|$. Эти этапы характерны тем, что в них автомат не проходит по всем состояним стирающего цикла. И максимальное количество символов в магазине не более чем r. С другой стороны, можно считать, что автомат сразу находится в стирающем цикле на протяжении всего этапа. Отсюда получаем оценку

$$\sum_{i=s+1}^{s+r} |I_i| \leq L_0(\ell - s, k) \leq \frac{k-1}{2k}(\ell - s)^2 + 5(\ell - s).$$

Теперь оценим $\sum\limits_{i=1}^{s} |I_i|$. Заметим, для всех этапов из рассматриваемого подмножества, в которых автомат не покидает стирающий цикл, можно оценить сверху сумму их длин как $(k+1)n$. Рассмотрим остальные этапы. Для них отдельно оценим такты записи и такты стирания. Пусть $\tau_{\text{записи}}$ — количество тактов, которые начинаются либо вне стирающего цикла, либо из стирающего цикла, но с пустым магазином, а $\tau_{\text{стирания}}$ — все остальные такты работы автомата.

Рассмотрим случай, когда найдется $q_* \in C$ такое, что $W(q_*) = Q \backslash C$. Заметим, что автомат P' не сможет записать больше, чем $h_{max} = (n - \ell + 1)(k-1) + 1$ символ в магазин. Учитывая, что внутри одного периода автомат не может оказаться в одном и том же состоянии с одинаковым содержимым магазина, получаем:

$$\tau_{\text{стирания}} \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i),$$

где $s' = \min(s, h_{max} - (k-1))$ — количество оставшихся этапов.

Теперь оценим $\tau_{\text{записи}}$. При максимальном заполнении магазина автомат пройдет по всем пишущим состояниям. Из стирающего цикла автомат не может перейти в одно и то же состояние более $k-1$ раза, кроме, тех состояний, в которые можно попасть только из стирающего цикла. В такие состояния автомат можем попасть не более k раз. Отсюда получаем, что

$$\tau_{\text{записи}} \leq (n - \ell + 1)s' - \sum_{i=0}^{s'-2} [\frac{i}{k-1}].$$

Откуда получаем, что

$$\sum_{i=1}^{s} |I_i| \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) + (n - \ell + 1)s - \sum_{i=0}^{s'-2} [\frac{i}{k-1}] + (k+1)n.$$

Пусть теперь $W(q) \neq Q \backslash C$ для всех $q \in C$. Заметим, что если $s \leq (n-k)(k-1)+1$, то полученные оценки остаются в силе, так как, собирая состояния $Q \backslash C$ в одном $W(q)$ достигается большая длина этапов. Если же $s > (n-k)(k-1)+1$, то можно считать, что все непустые $W(q)$ для $q \in C$ содержат по одному состоянию, кроме одного, в котором лежат все остальные состояния. Этапы, которые начинаются с состояния из $W(q)$, где $|W(q)| = 1$ можно суммарно оценить сверху $2kn$, так как до входа в стирающий цикл не будет записано более $2k-1$ символов в магазин. Таким образом можно считать, что в случае, когда $W(q) \neq Q \backslash C$ для всех $q \in C$ оценка увеличится не более чем на $2kn$.

Суммируя обе оценки, получаем, что

$$L(P') \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) + (n - \ell + 1)s' - \sum_{i=0}^{s'-2} [\frac{i}{k-1}] + \frac{k-1}{2k}(\ell - s)^2 +$$

$$+5(\ell - s) + 2kn.$$

Следовательно,

$$L(P) \le \sum_{i=0}^{s'-1} f_C^{max}(h_{max}-i) + (n-\ell+1)s' - \sum_{i=0}^{s'-2}[\frac{i}{k-1}]+$$

$$+\frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) + 2kn + (k+1)n + 2n \le$$

$$\le \sum_{i=0}^{s'-1} f_C^{max}(h_{max}-i) + (n-\ell+2)s' - \frac{s'^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2+$$

$$+5(\ell-s) + \frac{s'}{2} + (3k+3)n,$$

где $h_{max} = (n-\ell+1)(k-1)+1$ и $s' = \min(s, h_{max}-(k-1))$.

При $s \le (n-\ell)(k-1)+1$, получаем:

$$L(P) \le ((n-\ell+1)(k-1)+1)\ell - \frac{s(s-1)}{2} + s(n-\ell+2) + \frac{s}{2} -$$

$$-\frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) + (3k+3)n \le$$

$$\le \max_{\substack{1 \le s \le \ell \le n, \\ s \le (n-\ell)(k-1)+1}} \left(((n-\ell+1)(k-1)+1)\ell - \frac{s(s-1)}{2} + \right.$$

$$\left. +s(n-\ell+2) - \frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) \right) + (3k+\frac{7}{2})n.$$

Максимизируя квадратичную функцию по s и ℓ получаем, что

$$L(P) \le \frac{k(k-1)}{4k-2}n^2 + 5kn + (3k+3)n = \frac{k(k-1)}{4k-2}n^2 + (8k+\frac{7}{2})n.$$

Значит, $L(P) \le L_1(n,k)$ в этом случае.

При $s > (n-\ell)(k-1)+1$ и $\ell \ne n$ получаем:

$$L(P) \le \frac{(h_{max}+k)^2}{2} + \frac{h_{max}+k}{2} + h_{max}(l-s) + s'(n-\ell+2) + \frac{s'}{2} -$$

$$-\frac{s'^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) + (3k+3)n =$$

$$= \frac{k-2}{2(k-1)}h_{max} + h_{max}(n-s) + \frac{s}{2} + \frac{k-1}{2k}(\ell - s)^2 + kh_{max} +$$

$$+\frac{7}{2}h_{max} + (k-1)(n-\ell) + 5(\ell - s) + \frac{k^2}{2} + \frac{1}{2} - 2(k-1) + (3k+3)n \leq$$

$$\leq nh_{max} - \frac{k-1}{k}\ell h_{max} + \frac{k-1}{2k}\ell^2 - \frac{2k-1}{2k(k-1)}h_{max}^2 +$$

$$+k(2h_{max}+2\ell-n)+4\ell-\frac{5}{2}h_{max}+n+3(k-1)+\frac{k^2}{2}+\frac{1}{2}+\frac{(k-1)^3}{2k}+(3k+\frac{7}{2})n \leq$$

$$\leq nh_{max}-\frac{k-1}{k}\ell h_{max}+\frac{k-1}{2k}\ell^2-\frac{2k-1}{2k(k-1)}h_{max}^2+6kn+9n+5(k-1)+k^2+\frac{1}{2}$$

Подставляя $h_{max} = (n - \ell + 1)(k-1) + 1$, получаем

$$L(P) \leq \frac{n^2}{2} - \frac{n^2}{2(k-1)} + \frac{n^2}{2k(k-1)} - \frac{1}{2(k-1)} + n -$$

$$-k(n-\ell+1) - \frac{1}{2} + 6kn + 9n + 5(k-1) + k^2 + \frac{1}{2} \leq$$

$$\leq \frac{k-1}{2k}n^2 + 6kn + 10n + 5(k-1) + k^2 \leq \frac{k-1}{2k}n^2 + 7kn + 15n \leq L_1(n,k).$$

Остается лишь заметить, что в случае $\ell = n$, будет верна оценка

$$L(P) \leq L_0(n,k) + 2n + 2kn \leq L_1(n,k),$$

что и завершает доказательство.

□

Утверждение 4. *Пусть P — автомат из $\mathcal{M}'_0(n,1,k)$ и пусть в P есть единственный автоматный цикл C с отрицательным стирающем индексом. Тогда*

$$L(P) \leq L_1(n,k).$$

Доказательство. Применяя лемму 3, далее можно рассматривать автомат P' такой, что при пустом магазине автомат P' должен писать в магазин при этом будет выполнено:

$$L(P) \leq L(P') + n.$$

Рассмотрим $I(P') = (I_1, I_2, ..., I_d)$ — упорядоченное множество этапов автомата P'. Разобьем этапы на две группы. В первую включим все этапы, предпоследнее состояние которых не лежит в стирающем цикле C, в во вторую все остальные. По лемме 7 найдутся такие автоматы P'_1 и P'_2 из $\mathcal{M}'_0(n, 1, k)$, что $I(P'_1)$ будет состоять из первой группы этапов, а $I(P'_2)$ — из второй, причем будет выполнено, что

$$L(P') = L(P'_1) + L(P'_2).$$

Пусть n_0 — количество состояний в $L(P'_1)$. Тогда можно имеет место оценка

$$L(P'_1) \leq L_0(n_0, k) \leq \frac{k-1}{2k} n_0^2 + 5n_0.$$

Теперь оценим $L(P'_2)$. В P'_2 после стирающих состояний вне стирающего цикла магазин не становится пустым. Это означает, что можно трансформировать запись в магазин, не изменив при этом длину периода. Следовательно, можно считать, что автомат удовлетворяет предыдущей лемме, то есть для него верна оценка

$$L(P'_2) \leq \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) + (n - \ell + 2)s' + \frac{s'}{2} - \frac{s'^2}{2(k-1)} +$$

$$+ \frac{k-1}{2k}(\ell - s)^2 + 5(\ell - s) + (3k + 2)n,$$

где $h_{max} \leq (n - \ell - n_0 + 1)(k - 1) + 1$ и $s' = \min(s, h_{max} - (k - 1))$.

Суммируя обе оценки, имеем

$$L(P) \leq L(P'_1) + L(P'_2) + n \leq \frac{k-1}{2k} n_0^2 + 5n_0 + \sum_{i=0}^{s'-1} f_C^{max}(h_{max} - i) +$$

$$+ (n - \ell + 2)s' + \frac{s'}{2} - \frac{s'^2}{2(k-1)} + \frac{k-1}{2k}(\ell - s)^2 + 5(\ell - s) + (3k + 3)n,$$

где $h_{max} \leq (n - \ell - n_0 + 1)(k - 1) + 1$ и $s' = \min(s, h_{max} - (k - 1))$.

При $s \leq (n-\ell-n_0)(k-1)+1$, получаем:

$$L(P) \leq \left(\frac{k-1}{2k}n_0^2+5n_0+((n-\ell-n_0+1)(k-1)+1)\ell-\frac{s(s-1)}{2}+s(n-\ell+2)-\right.$$

$$\left.-\frac{s^2}{2(k-1)}+\frac{k-1}{2k}(\ell-s)^2+5(\ell-s)\right)+(3k+\frac{7}{2})n,$$

Максимизируя по n_0, ℓ и s, получаем,что

$$L(P) \leq L_1(n,k).$$

При $s > (n-\ell-n_0)(k-1)+1$ и $\ell \neq n$ получаем:

$$L(P) \leq \frac{k-1}{2k}n_0^2+5n_0+nh_{max}-\frac{k-1}{k}\ell h_{max}+\frac{k-1}{2k}\ell^2-\frac{2k-1}{2k(k-1)}h_{max}^2+$$

$$+3(k-1)+\frac{k^2}{2}+\frac{1}{2}+\frac{(k-1)^3}{2k}+(3k+\frac{7}{2})n \leq$$

$$\leq (\frac{k-1}{2k}n_0^2+5n_0+n-\frac{k-1}{k}\ell)((n-\ell-n_0+1)(k-1)+1)+\frac{k-1}{2k}\ell^2-$$

$$-\frac{2k-1}{2k(k-1)}(n-\ell-n_0)(k-1)+(4k+\frac{7}{2})n+3k.$$

Максимизируя по n_0, ℓ , получаем,что

$$L(P) \leq L_1(n,k).$$

При $\ell = n$ получаем, что $n_0 = 0$, следовательно, будет верна оценка из предыдущего утверждения, что и завершает доказательство.

□

4.2.6. Общий случай

Теперь все готово для доказательства асимптотической верхней оценки для $L(n,1,k)$.

Теорема 7. *При* $k > 1$

$$L(n,1,k) \leq L_1(n,k).$$

Доказательство. Пусть P содержит d автоматных циклов. В случае $d = 0$ и $d = 1$ все доказано. Пусть $d \geq 1$. Заметим, что все циклы являтся стирающими, и обозначим их C_1,..., C_d. Имеет место следующее разбиение множества состояний:

$$Q = \bigsqcup_{i=0}^{d} Q_i,$$

где при $i > 0$ $Q_i = C_i \cup W(C_i)$ — множество состояний, и, а Q_0 — все оставшиеся состояния, то есть множество состояний, из которых автомат не попадает ни в один стирающий цикл. Заметим, что внутри каждого этапа I все состояния лежат в одном и том же Q_i. Следовательно, для каждого Q_i можно выделить свое подмножество этапов, для которого по лемме 7 будет существовать автомат P_i, реализующий его. Так как каждый этап автомата P воздет в $I(P_i)$, то будет выполнено, что

$$L(P) = \sum_{i=0}^{d} L(P_i).$$

По построению P_0 — автомат без стирающего цикла, а остальные P_i — автоматы с одним стирающим циклов. Следовательно, для каждого P_i будет выполнено $L(P_i) \leq L_1(|Q_i|, k)$. Значит,

$$L(P) \leq \sum_{i=0}^{d} L_1(|Q_i|, k) \leq L_1(\sum_{i=0}^{d} |Q_i|, k) = L_1(n, k),$$

что и требовалось доказать.

□

4.2.7. Дополнения: решение экстремальных задач

Лемма 10. *Пусть*

$$g(n,k) = \max_{\substack{s,\ell \\ 1 \leq s \leq \ell \leq n, \\ s \leq (n-\ell)(k-1)+1}} \Bigg(((n-\ell+1)(k-1)+1)\ell - \frac{s(s-1)}{2} + s(n-\ell+2) - \frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) \Bigg).$$

Тогда $g(n,k) \leq \frac{k(k-1)}{4k-2}n^2 + 5kn$.

Доказательство. Максимум квадратичной функции достигается либо в критической точке (где все частные производные равны нулю), либо на границе области. Обозначим максимизируемую функцию через f. Найдем критические точки:

$$\begin{cases} \frac{\partial f}{\partial s} = n - 2\ell + \frac{\ell - s}{k} - \frac{s}{k-1} - 5/2 = 0, \\ \frac{\partial f}{\partial \ell} = 3\ell - n - 2s + k(n - 2\ell + 1) - \frac{(\ell - s)}{k} + 5 = 0 \end{cases}$$

Полученная система линейных уравнений не имеет решений, поэтому продолжим поиск решений на границе заданной области.

1. Пусть $s = 1$. При $s = 1$

$$f = 5\ell + n - \frac{1}{2k-2} + \frac{(k-1)(\ell-1)^2}{2k} + \ell(k-1)(n-\ell+1) - 3.$$

1.1. Найдем критические точки

$$\frac{\partial f}{\partial \ell} = 3\ell - n + k(n - 2\ell + 1) - \frac{\ell - 1}{k} + 3 = 0.$$

Откуда находим:

$$\ell = \frac{3k - kn + k^2 n + k^2 + 1}{2k^2 - 3k + 1}.$$

Подставляя в f получаем:

$$\frac{k(k-1)}{4k-2}n^2 + \frac{kn}{2} + \frac{11n}{4(2k-1)} + \frac{11n}{4} + \frac{k}{4} + \frac{12}{k-1} - \frac{121}{8(2k-1)} - \frac{5}{8} \leq$$

$$\leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

1.2. Рассмотрим границу $\ell = 1$. Подставляя в f, получаем:

$$kn - \frac{1}{2(k-1} + 2 \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

1.3. Рассмотрим границу $\ell = n$. Подставляя в f, получаем:

$$5n + kn - \frac{1}{2k-2} + \frac{(k-1)(n-1)^2}{2k} - 3 \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

2. Пусть $s = (n - \ell)(k-1) + 1$. При $s = (n-\ell)(k-1) + 1$

$$f = \frac{5\ell}{2} + \frac{3n}{2} - \frac{1}{2(k-1)} + \frac{7k\ell}{2} - \frac{5kn}{2} - \frac{(n-1)^2}{2k} + \frac{n^2}{2} - \frac{5}{2}.$$

2.1. Найдем критические точки

$$\frac{\partial f}{\partial \ell} = \frac{7k}{2} + \frac{5}{2} = 0.$$

Критических точек нет, поэтому будем искать максимум на границе, а именно: $\ell = 1$ и $\ell = n$.

2.2. При $\ell = 1$ получаем

$$\frac{7k}{2} + \frac{3n}{2} - \frac{1}{2(k-1)} - \frac{5kn}{2} - \frac{(n-1)^2}{2k} + \frac{n^2}{2} \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

2.3. При $\ell = n$ получаем

$$5n + kn - \frac{1}{2k-2} + \frac{(k-1)(n-1)^2}{2k} - 3 \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

3. Пусть $s = \ell$. При $s = \ell$

$$f = \frac{\ell(2k - \ell - 2k\ell + 2kn + 5)}{2} - \frac{\ell^2}{2(k-1)}.$$

3.1. Найдем критические точки

$$\frac{\partial f}{\partial \ell} = k(n - 2\ell + 1) - \ell - \frac{\ell}{k-1} + 5/2 = 0.$$

Откуда находим:

$$\ell = \frac{(k-1)(2k + 2kn + 5)}{2k(2k-1)}.$$

Подставляя в f, получаем:

$$\frac{(k-1)(2k + 2kn + 5)^2}{8k(2k-1)} \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

Рассмотрим граничные значения ℓ.

3.2. Случай $\ell = 1$ уже был рассмотрен в 1.2.

3.3. При $\ell = n$ получаем

$$\frac{n(2k - n + 5)}{2} - \frac{n^2}{2(k-1)} \le \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

4. Теперь s не лежит на границе. Пусть $\ell = n$. При $\ell = n$

$$f = 5n - 3s + kn - \frac{s(s-1)}{2} - \frac{s^2}{2k-2} + \frac{(n-s)^2(k-1)}{2k}.$$

Найдем критические точки

$$\frac{\partial f}{\partial s} = \frac{n-s}{k} - n - \frac{s}{k-1} - \frac{5}{2} = 0.$$

Откуда находим:

$$s = -\frac{(k-1)(5k-2n+2kn)}{2(2k-1)} < 0.$$

Следовательно, подставим граничное значение s, а именно: $s = 1$. Подставляя, получаем:

$$5n + kn - \frac{1}{2k-2} + (\frac{(k-1)(n-1)^2}{2k} - 3 \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

Во всех случаях получили верхнюю оценку

$$\frac{k(k-1)}{4k-2}n^2 + 5kn,$$

что и требовалось доказать.

□

Лемма 11. *Пусть*

$$g(n,k) = \max_{\substack{s,\ell,n_0 \\ 1 \leq s \leq \ell \leq n, \\ s \leq (n-\ell)(k-1)+1, \\ 0 \leq n_0 \leq n-\ell}} \Bigg(\frac{k-1}{2k}n_0^2 + ((n-\ell-n_0+1)(k-1)+1)\ell -$$

$$-\frac{s(s-1)}{2} + s(n-\ell+2) - \frac{s^2}{2(k-1)} + \frac{k-1}{2k}(\ell-s)^2 + 5(\ell-s) + 5n_0\Bigg).$$

Тогда $g(n,k) \leq \frac{k(k-1)}{4k-2}n^2 + 5kn$.

Доказательство. Максимум квадратичной функции достигается либо в критической точке (где все частные производные равны нулю), либо на границе области. Обозначим максимизируемую функцию через f. Найдем критические точки:

Найдем критические точки:

$$\begin{cases} \frac{\partial f}{\partial s} = n - 2\ell + \frac{\ell-s}{k} - \frac{s}{k-1} - \frac{5}{2} = 0, \\ \frac{\partial f}{\partial \ell} = \frac{(k-1)(2\ell-2s)}{2k} - (k-1)(\ell - n + n_0 - 1) - \ell(k-1) - s + 6 = 0, \\ \frac{\partial f}{\partial n_0} = \frac{n_0(k-1)}{k} - \ell(k-1) + 5 = 0 \end{cases}$$

Решая систему, получаем:

$$\begin{cases} \ell = \frac{17k+5}{2k(k-1)}, \\ s = k(\frac{n}{2} - \frac{5}{4}) - \frac{n}{4} - \frac{k(n/4+35/8)-5/2}{k(2k-1)} - \frac{63}{8}, \\ n_0 = \frac{6}{k-1} + \frac{7}{2} \end{cases}$$

Решая систему, получаем:

$$\frac{25k}{16} + \frac{5n}{8} + \frac{48}{k-1} - \frac{5kn}{4} - \frac{(2n-5)^2}{32(2k-1)} + \frac{kn^2}{4} - \frac{25}{8k} - \frac{n^2}{8} + \frac{731}{32} \leq$$

$$\leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

Продолжим поиск решений на границе заданной области.

1. Случай, когда $n_0 = 0$, уже был полностью разобран.

2. Пусть теперь $n_0 = n - \ell$. Тогда в этом случае можно оценить

$$L(P) \leq (k+1)n + L_0(n-\ell, k) + L_0(\ell - s, k) + n \leq L_0(n,k) + (k+2)n \leq$$

$$\leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

3. Пусть теперь n_0 лежит не на границе. 3.1. Пусть $s = 1$. При $s = 1$

$$f = 5\ell + n + 5n_0 - \frac{1}{2k-2} + \frac{(k-1)(\ell-1)^2}{2k} -$$

$$-\ell(k-1)(\ell - n + n_0 - 1) + \frac{n_0^2(k-1)}{2k} - 3.$$

3.1.1. Найдем критические точки

$$\begin{cases} \frac{\partial f}{\partial \ell} = \frac{(\ell-1)(k-1)}{k} - \ell(k-1) - (k-1)(\ell - n + n_0 - 1) + 5 = 0, \\ \frac{\partial f}{\partial n_0} = \frac{n_0(k-1)}{k} - \ell(k-1) + 5 = 0 \end{cases}$$

Решая систему, получаем:

$$\begin{cases} \ell = \frac{5}{k-1} + \frac{k(n+1)-6}{k^2+2k-1}, \\ n_0 = \frac{k(k+kn-6)}{k^2+2k-1} \end{cases}$$

Подставляя в f, получаем:

$$7n + \frac{12}{k-1} - \frac{(51k)/2 - 7n + 9kn + (3kn^2)/2 - n^2/2 + 23/2}{k^2+2k-1} + \frac{n^2}{2} + 3 \leq$$

$$\leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

Продолжим поиск решений на границе заданной области.
3.1.2. Пусть $\ell = 1$. При $\ell = 1$

$$f = n + 5n_0 - \frac{1}{2k-2} + (n-n_0)(k-1) + \frac{n_0^2(k-1)}{2k} + 2$$

Найдем критические точки

$$\frac{\partial f}{\partial n_0} = \frac{n_0(k-1)}{k} - k + 6 = 0$$

Откуда находим:

$$n_0 = \frac{k(k-6)}{k-1}.$$

Подставляя в f, получаем:

$$k(n+11/2) - 13/(k-1) - k^2/2 - 21/2 \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

3.1.3. Пусть $\ell = n$. Тогда $n_0 = 0$, случай был разобран.
3.2. Пусть $s = (n-\ell)(k-1)+1$. При $s = (n-\ell)(k-1)+1$

$$f = \frac{5\ell}{2} + \frac{3n}{2} + 5n_0 - \frac{1}{2(k-1)} + \frac{7k\ell}{2} - \frac{5kn}{2} +$$
$$+\ell n_0 - \frac{n^2 - 2n + n_0^2 + 1}{2k} + \frac{n^2}{2} + \frac{n_0^2}{2} - kln_0 - \frac{5}{2}.$$

3.2.1. Найдем критические точки

$$\begin{cases} \frac{\partial f}{\partial \ell} = \frac{7k}{2} + n_0 - kn_0 + \frac{5}{2} = 0, \\ \frac{\partial f}{\partial n_0} = \frac{n_0(k-1)}{k} - \ell(k-1) + 5 = 0 \end{cases}$$

Решая систему, получаем:

$$\begin{cases} \ell = \frac{17k+5}{2k(k-1)}, \\ n_0 = \frac{7k+5}{2(k-1)} \end{cases}$$

Подставляя в f, получаем:

$$\frac{3n}{2} + \frac{95}{2(k-1)} - \frac{5kn}{2} - \frac{n^2 - 2n + 29/4}{2k} + \frac{n^2}{2} + \frac{169}{8} \leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

3.2.2. Пусть $\ell = 1$. Тогда и $s = 1$, случай был рассмотрен.
3.2.3. Пусть $\ell = n$. Тогда опять $s = 1$ и случай был рассмотрен.
3.3. Пусть $s = \ell$. При $s = \ell$

$$f = 5n_0 - \ell((k-1)(\ell - n + n_0 - 1) - 1) + \ell(n - \ell + 2) -$$
$$- \frac{\ell(\ell-1)}{2} - \frac{\ell^2}{2k-2} + \frac{n_0^2(k-1)}{2k}.$$

3.3.1 Найдем критические точки:

$$\begin{cases} \frac{\partial f}{\partial \ell} = n_0 - \ell - k(2\ell - n + n_0 - 1) - \frac{\ell}{k-1}/(k-1) + \frac{5}{2} = 0, \\ \frac{\partial f}{\partial n_0} = \frac{n_0(k-1)}{k} - \ell(k-1) + 5 = 0 \end{cases}$$

Решая систему, получаем:

$$\begin{cases} \ell = \frac{(k-1)(12k+2kn+5)}{2k^3}, \\ n_0 = n - \frac{5}{k-1} - \frac{5}{2k^2} - \frac{2n+7}{2k} + 1 \end{cases}$$

Подставляя в f, получаем:

$$\frac{(7k + 2kn - 2k^2n - 2k^2 + 5)(7k + 2kn - 2k^2n - 22k^2 + 5)}{8k^3(k-1)} \leq$$
$$\leq \frac{k(k-1)}{4k-2}n^2 + 5kn.$$

3.3.2. Пусть $\ell = 1$. Тогда и $s = 1$, случай был рассмотрен.
3.3.3. Пусть $\ell = n$. Тогда $n_0 = 0$ и случай уже был разобран.
3.4. Пусть теперь s лежит не на границе.
3.4.1. Пусть $\ell = 1$. Тогда $s = 1$ и случай уже был разобран.
3.4.2. Пусть $\ell = n$. Тогда $n_0 = 0$ и случай уже был разобран.
Во всех случаях получили верхнюю оценку

$$\frac{k(k-1)}{4k-2}n^2 + 5kn.$$

□

Лемма 12. *Пусть*

$$g(n,k) = \max_{\substack{\ell, n_0 \\ \frac{k-1}{k}n + 1 \leq \ell \leq n, \\ 0 \leq n_0 \leq n - \ell}} \left((n - \frac{k-1}{k}\ell)((n - \ell - n_0 + 1)(k-1) + 1) + \right.$$

$$+\frac{k-1}{2k}\ell^2 - \frac{2k-1}{2k(k-1)}(n-\ell-n_0)(k-1) + \frac{k-1}{2k}n_0^2 + 5n_0\Big).$$

Тогда $g(n,k) \le \frac{k-1}{2k}n^2 + kn + 3n + 23$.

Доказательство. Максимум квадратичной функции достигается либо в критической точке (где все частные производные равны нулю), либо на границе области. Обозначим максимизируемую функцию через f. Найдем критические точки:

$$\begin{cases} \frac{\partial f}{\partial n_0} = \ell - 2n + 4n_0 - k(\ell - n + 2n_0 - 2) + (n - 2n_0)/k + 4 = 0, \\ \frac{\partial f}{\partial \ell} = k + n_0 - kn_0 = 0 \end{cases}$$

Решая систему получаем, что

$$\begin{cases} \ell = n + \frac{6}{k-1} - \frac{n}{k}, \\ n_0 = \frac{1}{k-1} + 1 \end{cases}$$

Подставляя в f и упрощая, получаем:

$$\frac{k-1}{2k}n^2 + \frac{11}{(2(k-1))} + \frac{11}{2} \le \frac{k-1}{2k}n^2 + 11.$$

Продолжим поиск решений на границе заданной области.
1. Случай $n_0 = 0$ уже был рассмотрен.
2. Пусть теперь $n_0 = n - \ell$. При $n_0 = n - \ell$

$$f = 5n - 5\ell + kn - \ell(k-1) - \frac{k(2k-1)}{2(k-1)} + \frac{(k-1)\ell^2}{2k} + \frac{(k-1)(\ell-n)^2}{2k}.$$

Найдем критические точки:

$$\frac{\partial f}{\partial \ell} = 2\ell - k - n - \frac{2l-n}{k} - 4 = 0.$$

Решая уравнение, получаем:

$$\ell = k/2 + n/2 + 5/(2(k-1)) + 5/2.$$

Подставляя в f получаем:

$$3n - (13k)/4 - 27/(4(k-1)) + (kn)/2 - k^2/4 + n^2/4 - n^2/(4k) - 27/4 \le$$

$$\le n^2/4 + kn + 3n.$$

3. Пусть теперь n_0 не на границе.
3.1. Случай $\ell = n$ уже был рассмотрен, так как в этом случае $n_0 = 0$.
3.2. Пусть теперь $\ell = \frac{k-1}{k}n + 1$. Тогда

$$f = 5n_0 - \frac{1}{2(k-1)} + kn_0 - \frac{n^2}{2k} - \frac{n_0^2}{k} - kn_0^2 + \frac{n^2}{2} + 2n_0^2 - 1/2.$$

Найдем критические точки:

$$\frac{\partial f}{\partial n_0} = 4n_0 - \frac{2n_0}{k} - k(2n_0 - 1) + 5.$$

Решая уравнение, получаем:

$$n_0 = \frac{k^2 + 5k}{2k^2 - 4k + 2}.$$

Подставляя в f получаем:

$$\frac{k}{4} + \frac{23}{2(k-1)} + \frac{9}{(k-1)^2} + \frac{n^2}{2} - \frac{n^2}{2k} + \frac{5}{2} \le \frac{k-1}{2k}n^2 + 23 + k/4.$$

Во всех случаях получили, что максимум ограничен:

$$\frac{k-1}{2k}n^2 + kn + 3n + 23.$$

□

4.3. Формулировка полученных результатов

Подведем итоги этого раздела. Были доказаны нижняя и верхняя оценки на $L(n, 1, k)$. Основным результатом является доказательство следующей теоремы.

Теорема 8. *При* $k > 1$

$$\frac{k(k-1)}{4k-2}n^2 - \frac{1}{2k-1}n - 1 \le L(n, 1, k) \le \frac{k(k-1)}{4k-2}n^2 + (8k + 32)n.$$

Из нее следует, что нижняя и верхняя оценки асимптотически совпадают при $n \to \infty$, а именно:

Теорема 9. *При* $k > 1$ *и* $n \to \infty$

$$L(n, 1, k) = \frac{k(k-1)}{4k-2}n^2(1 + o(1)).$$

5. Периодические свойства автоматов со входом

5.1. Свойство сохранения периодических последовательностей

Пусть дан инициальный конечный автомат $V = (A, Q_V, B, \varphi_V, \psi_V, q_0)$, который задает ограниченно-детерминированную функцию $f_V : A^* \to B^*$, и инициальный автомат с магазинной памятью

$P = (B, Q_P, C, \Gamma, \varphi_P, \psi_P, \eta_P, r_0, \gamma_0)$, который задает детерминированное отображение $f_P : B^* \to C^*$. Тогда суперпозицией конечного автомата V и P будем называть отображение $f_{P \circ V} : A^* \to C^*$, где $f_{P \circ V}(\alpha) = f_P(f_V(\alpha))$.

Утверждение 5. *Пусть $V = (A, Q_V, B, \varphi_V, \psi_V, q_0)$ — инициальный конечный автомат,*

$P = (B, Q_P, C, \Gamma, \varphi_P, \psi_P, \eta_P, r_0, \gamma_0)$ — инициальный автомат с магазинной памятью. Тогда суперпозиция V и P $f_{P \circ V} : A^* \to C^*$ является детерминированной функцией, порожденной инициальным автоматом с магазинной памятью

$$P_V = (A, Q_V \times Q_P, C, \Gamma, \varphi, \psi, \eta, (q_0, r_0), \gamma_0),$$

где

$$\varphi(a, (q_V, q_P), z) = (\varphi_V(a, q_V), \varphi_P(\psi_V(a, q_V), q_P, z)),$$
$$\psi(a, (q_V, q_P), z) = \psi_P(\psi_V(a, q_V), q_P, z),$$
$$\eta(a, (q_V, q_P), z) = \eta_P(\psi_V(a, q_V), q_P, z).$$

Доказательство. Необходимо рассмотреть системы канонических уравнений автоматов V и P и подставить первую во вторую. □

Известно, что автоматы с магазинной памятью переводят периодические последовательности в периодические [22]. Приведем свое доказательство этого факта в принятых обозначениях.

Теорема 10 ([22])**.** *Пусть P — автомат с магазинной памятью из $\mathcal{M}(A, B)$. Тогда P переводит периодические последовательности в периодические.*

Доказательство. Для любой периодической последовательности найдется конечный автономный автомат V, который ее генерирует. Рассмотрим суперпозицию V и P. По утверждению 5 суперпозицией является

автономный автомат с магазинной памятью, который, как известно, генерирует периодическую последовательность, что и требовалось доказать. □

Обозначим $L(P, \alpha)$ — период выходной последовательности при подаче последовательности α^∞ на вход автомату с магазинной памятью P.

5.2. Верхние оценки периода выходной последовательности

Теперь сформулирует и докажем оценки в случае неавтономного автомата с магазинной памятью.

Теорема 11. *Пусть $P = (A, Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0)$— автомат с магазинной памятью из $\mathcal{M}(n, m, k)$ при $k > 1$. Тогда для любого непустого слова α из алфавита A будет выполнено*

$$L(P, \alpha) \leq \frac{|\alpha| n (k^{|\alpha| nm+1} - 1)}{k - 1}.$$

Доказательство. Пусть V — конечный автомат с $|\alpha|$ состояниями, генерирующий последовательность α^∞. Рассмотрим суперпозицию конечного автомата V и автомата с магазинной памятью P. В силу предыдушего утверждения их суперпозиция является автономным автоматом с магазинной памятью с $|\alpha||Q|$ состояниями. К полученному автомату применим теорему о длине периода выходной последовательности для автономного автомата с магазинной памятью, откуда и получаем оценку. □

Теорема 12. *Пусть $P = (A, Q, B, \Gamma, \varphi, \psi, \eta, q_0, \gamma_0)$— автомат с магазинной памятью из $\mathcal{M}(n, 1, k)$ при $k > 1$. Тогда для любого непустого слова α из алфавита A будет выполнено*

$$L(P, \alpha) \leq \frac{k(k-1)}{4k-2} |\alpha|^2 n^2 + (8k + 32)|\alpha| n.$$

Доказательство. Доказательство дословно повторяется из предыдущей теоремы. □

6. Нижние оценки периода выходной последовательности

Пример 6.

Пусть автомат с магазинной памятью $P_{\ell,1} = (A, Q, B, \Gamma, \varphi, \psi, \eta, r_1, \lambda) \in \mathcal{M}(n, 1, k)$, где $0 < \ell < n$, $A = B = \{0, 1\}$, $Q = \{q_1, ..., q_{n-\ell}, r_1, ..., r_\ell\}$, $\Gamma = \{1\}$,

$$\psi(a, q, z) = \begin{cases} 1, \text{ если } q = r_1, \ z = \lambda, \ a = 1, \\ 0, \text{ иначе,} \end{cases}$$

$$\varphi(a, q, z) = \begin{cases} q, \text{ если } a = 0, \\ q_{i+1}, \text{ если } q = q_i, \ i \neq n - \ell, \ a = 1, \\ r_1, \text{ если } q = q_{n-\ell}, \ a = 1, \\ r_{i+1}, \text{ если } q = r_i, \ i \neq \ell, \ z = 1, \ a = 1, \\ r_1, \text{ если } q = r_\ell, \ z = 1, \ a = 1, \\ q_1, \text{ если } q = r_i, \ z = \lambda, \ a = 1, \\ q, \text{ иначе,} \end{cases}$$

$$\eta(a, q, z) = \begin{cases} 1^k, \text{ если } q = q_i, \\ z, \text{ если } q = r_i, \ a = 0, \\ 1, \text{ если } q = r_i, \ i \neq \ell, \ z = 1, \ a = 1, \\ \lambda, \text{ если } q = r_\ell, \ z = 1, \ a = 1, \\ 1^k, \text{ если } q = r_i, \ z = \lambda, \ a = 1, \\ \lambda, \text{ иначе.} \end{cases}$$

На рисунке 5 приведем диаграмму этого автомата. Переходы автомата описываются следующим шаблоном $a, z/\eta$, то есть из данного состояния, при подаче входного символа a и при значении верхнего символа магазина z, автомат записывает на выходную ленту $\psi(a, q, z)$, а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка. Начальное состояние помечено символом " $*$ " и через запятую указана начальная запись в магазине.

Исследуем поведение автомата при подаче последовательности α^∞ на вход, где $\alpha = 0^{p-1}1$. Автомат начинает работу из состояния r_1 и находится в нем с пустым магазином до прихода первой единицы на вход. Далее автомат переходит в состояние q_1 и начинает заполнение магазина.

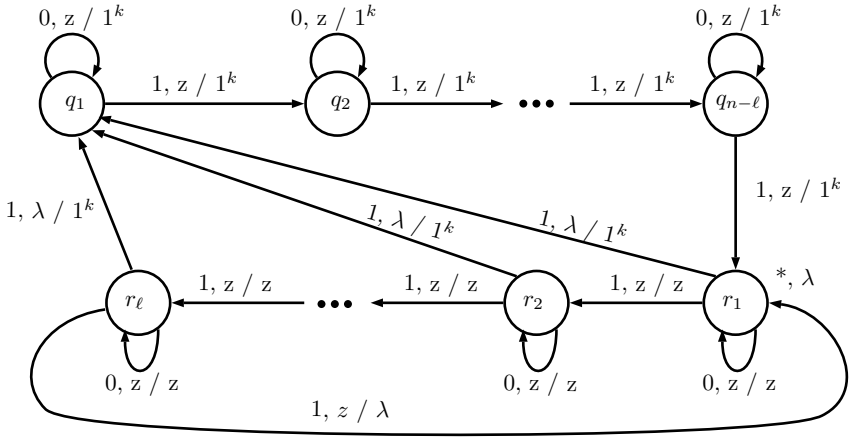

Рис. 5. Диаграмма автомата $P_{\ell,1}$.

Переход в следующее состояние осуществляется каждые $|\alpha|$ тактов при подаче единицы на вход. Таким образом автомат проходит по состояниям $q_1, ..., q_{n-\ell}$. После чего попадает в состояние r_1. При подаче нуля на вход магазин и состояние остаются неизменными, а при подаче единицы автомат переходит в следующее по циклу состояние. Так происходит до тех пор, пока автомат не достигнет состояния r_ℓ, где при подаче единицы на вход происходит стирание и переход в состояние r_1. По циклу $r_1, ..., r_\ell$ автомат ходит до опустошения магазина. Опустошается же магазин в состоянии r_1, что и будет означать зацикливание.

Теперь подсчитаем длину периода выходной последовательности.

$$L(P_{\ell,1}, \alpha) = (k + |\alpha|(n-\ell)(k-1))|\alpha|\ell + |\alpha|(n-\ell+1) =$$

$$= |\alpha|^2\ell(n-\ell)(k-1) + |\alpha|(n + (k-1)\ell + 1).$$

Рассмотренный пример доказывает следующую теорему.

Теорема 13. *При $n > 1$ и $k > 1$ найдется автомат с магазинной памятью P из $\mathcal{M}(n, 1, k)$ такой, что для входных последовательностей вида α^∞, где $\alpha = 0^{p-1}1$, $p \in \mathbb{N}$, период выходных последовательностей будет квадратично зависеть от периода входной.*

Пример 7.

Пусть автомат с магазинной памятью $P = (A, Q, B, \Gamma, \varphi, \psi, \eta, q_2, \lambda) \in \mathcal{M}(n, m, k)$, где $A = B = \{0, 1\}$, $Q = \{q_1, q_2\}$, $\Gamma = \{1, 2, ..., m\}$,

$$\psi(a, q, z) = \begin{cases} 1, \text{ если } q = q_2, \ z = \lambda, \ a = 1, \\ 0, \text{ иначе,} \end{cases}$$

$$\varphi(a, q, z) = \begin{cases} q_2, \text{ если } q = q_1, \ z = m, \ a = 1, \\ q_1, \text{ если } q = q_2, \ z \neq m, \ a = 1, \\ q, \text{ иначе,} \end{cases}$$

$$\eta(a, q, z) = \begin{cases} (z+1)^k, \text{ если } q = q_1, \ z \neq m, \ a = 1, \\ \lambda, \text{ если } q = q_1, \ z = m, \ a = 1, \\ z^k, \text{ если } q = q_1, \ a = 0, \\ z, \text{ если } q = q_2, \ a = 0, \\ (z+1)^k, \text{ если } q = q_2, \ z \neq m, \ a = 1, \\ \lambda, \text{ иначе.} \end{cases}$$

На рисунке 6 приведем диаграмму этого автомата. Переходы автомата описываются следующим шаблоном $a, z/\eta$, то есть из данного состояния, при подаче входного символа a и при значении верхнего символа магазина z, автомат записывает на выходную ленту $\psi(a, q, z)$, а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка. Начальное состояние помечено символом " $*$ " и через запятую указана начальная запись в магазине.

Рассмотрим поведение автомата при подаче на вход последовательность α^∞, где $\alpha = 0^{p-1}1$. Рассмотрим, как будут меняться состояние автомата и магазина при подаче на вход слова α:

$(q_2, m) \Rightarrow^\alpha (q_2, \lambda)$;
$(q_2, z) \Rightarrow^\alpha (q_1, (z+1)^k), 0 \leq z < m$;
$(q_1, z) \Rightarrow^\alpha (q_1, z^{(k-1)(|\alpha|-1)}(z+1)^k), 0 < z < m$;
$(q_1, m) \Rightarrow^\alpha (q_2, m^{(k-1)(|\alpha|-1)})$.

Оказывается, что полученные уравнения можно рассматривать как уравнения автономного автомата с магазинной памятью, а, значит, мы можем воспользоваться соответствующей техникой для вычисления периода выходной последовательности.

Для оценки длины периода автономного автомата с магазинной памятью удобно пользоваться следующими функциями: $\omega(q, \gamma) : Q \times \Gamma^* \rightarrow$

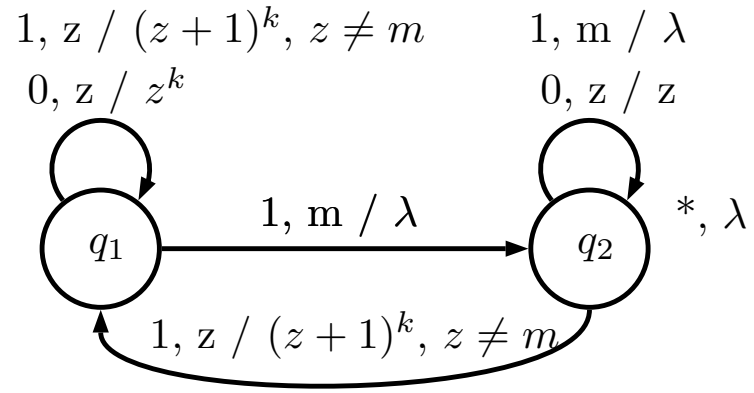

Рис. 6. Диаграмма автомата P.

$\mathbb{N} \cup \{\infty\}$ и $\pi(q, \gamma) : Q \times \Gamma^* \to Q$, которые формально определим следующим образом. Пусть автомат находится в состоянии q, а в магазине лежит слово γ. Если существует такое минимальное положительное количество тактов τ работы автомата, что магазин становится пустым, а автомат переходит в состояние q', то положим, что $\omega(q, z) = \tau$, а $\pi(q, z) = q'$, иначе $\omega(q, z) = \infty$, а значение $\pi(q, z)$ не определено.

Заметим, что

$$\omega(q_2, m) = |\alpha|.$$

$$\omega(q_2, m-1) = |\alpha| + \omega(q_1, m^k) = 2|\alpha| + \omega(q_2, m^{(k-1)|\alpha|}) =$$
$$= 2|\alpha| + (k-1)|\alpha|\omega(q_2, m) = |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, m)$$

$$\omega(q_2, m-2) = |\alpha| + \omega(q_1, (m-1)^k) = 2|\alpha| + \omega(q_1, (m-1)^{(k-1)|\alpha|} m^k) =$$

$$= 3|\alpha| + \omega(q_2, (m-1)^{(k-1)|\alpha|} m^{(k-1)|\alpha|}) =$$
$$= 3|\alpha| + (k-1)|\alpha|\omega(q_2, m) + (k-1)|\alpha|\omega(q_2, m-1) =$$
$$= |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, m-1).$$

По индукции получаем, что для $i < 1 < m$ выполнено

$$\omega(q_2, i-1) = |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, i).$$

Период будет равен

$$\omega(q_2, \lambda) = (m+1)|\alpha| + \omega(q_2, 1^{(k-1)|\alpha|}2^{(k-1)|\alpha|}...m^{(k-1)|\alpha|}) =$$
$$= |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, 1).$$

Получаем систему уравнений:

$$\begin{cases} \omega(q_2, m) = |\alpha|, \\ \omega(q_2, m-1) = |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, m), \\ \omega(q_2, m-2) = |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, m-1), \\ ... \\ \omega(q_2, i-1) = |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, i), \\ ... \\ \omega(q_2, \lambda) = |\alpha| + ((k-1)|\alpha| + 1)\omega(q_2, 1). \end{cases}$$

Решая систему, находим период выходной последовательности

$$\omega(q_2, \lambda) = ((k-1)|\alpha| + 1)^m|\alpha| + \frac{((k-1)|\alpha| + 1)^m - 1}{k-1},$$

то есть период выходной последовательности есть полином степени $m+1$ от периода входной.

Данный пример позволяет доказать следующую теорему.

Теорема 14. *Для любого многочлена $q(x)$ найдется автомат с магазинной памятью P с двумя состояниями такой, что на последовательностях α^∞, где $\alpha = 0^{p-1}1$, $p \in \mathbb{N}$ период выходной последовательности будет больше, чем $q(p)$.*

Доказательство. Рассмотрим автомат из предыдущего примера и подберем достаточно большие m и k такие, чтобы было выполнено $q(x) < ((k-1)x+1)^m x + \frac{((k-1)x+1)^m - 1}{k-1}$ при всех натуральных x. Данный автомат будет удовлетворять условиям теоремы, что и требовалось доказать. □

Пример 8.

Пусть автомат с магазинной памятью $P = (A, Q, B, \Gamma, \varphi, \psi, \eta, q_1, \lambda) \in \mathcal{M}(n, 2, k)$, где $A = B = \{0, 1\}$, $Q = \{q_1, q_2, ..., q_n, r_2, r_3, ..., r_n\}$, $\Gamma = \{*, 1\}$,

$$\psi(a, q, z) = \begin{cases} 1, \text{ если } q = q_1, \ z = \lambda, \ a = 1, \\ 0, \text{ иначе,} \end{cases}$$

$$\varphi(a,q,z)=\begin{cases} q_{i+1},\ \text{если } q=q_i,\ i<n,\ z=1,\ a=1,\\ q_n,\ \text{если } q=q_n,\ z=1,\ a=1,\\ r_i,\ \text{если } q=q_i,\ i>1,\ z=*,\ a=0,\\ q_i,\ \text{если } q=r_i,\ i>1,\ z=1,\ a=1,\\ q_{i-1},\ \text{если } q=r_i,\ i>1,\ z=*,\ a=1,\\ q_1,\ \text{если } q=r_2,\ z=\lambda,\ a=1,\\ q,\text{иначе,} \end{cases}$$

$$\eta(a,q,z)=\begin{cases} 1^k,\ \text{если } q=q_i,\ i<n,\ z=1,\ a=0,\\ *1^{k-1},\ \text{если } q=q_i,\ i<n,\ z=\lambda,\ a=1,\\ *1^{k-1},\ \text{если } q=q_i,\ i<n,\ z=1,\ a=1,\\ 1,\ \text{если } q=q_n,\ z=1,\ a=0,\\ *1^{k-1},\ \text{если } q=r_i,\ z=1,\ a=1,\\ *,\ \text{если } q=r_i,\ z=*,\ a=1,\\ *,\ \text{если } q=q_1,\ z=*,\ a=0,\\ \lambda,\ \text{если } q=q_1,\ z=*,\ a=1,\\ \lambda,\ \text{иначе.} \end{cases}$$

На рисунке 7 приведем диаграмму этого автомата. Переходы автомата описываются следующим шаблоном $a, z/\eta$, то есть из данного состояния, при подаче входного символа a и при значении верхнего символа магазина z, автомат записывает на выходную ленту $\psi(a,q,z)$, а в магазине стирает последний символ и дописывает слово η. Следующее состояние указывает стрелка. Начальное состояние помечено символом " $*$ " и через запятую указана начальная запись в магазине.

Рассмотрим поведение автомата при подаче на вход последовательность α^∞, где $\alpha = 0^{p-1}1$. Рассмотрим, как будут меняться состояние автомата и магазина при подаче на вход слова α:

$(q_1,\lambda) \Rightarrow^\alpha (q_1, *1^{k-1})$;
$(q_i,1) \Rightarrow^\alpha (q_{i+1}, 1^{(k-1)(p-1)} * 1^{k-1}),\ i<n$;
$(q_n,1) \Rightarrow^\alpha (q_n,\lambda)$;
$(q_i,1*) \Rightarrow^\alpha (q_i, *1^{k-1}),\ i>1$;
$(q_i,**) \Rightarrow^\alpha (q_{i-1}, *),\ i>1$;
$(q_1,*) \Rightarrow^\alpha (q_1,\lambda)$.

Выписанные выше уравнения не являются уравнениями для автономного автомата с магазинной памятью, так как в некоторых случаях

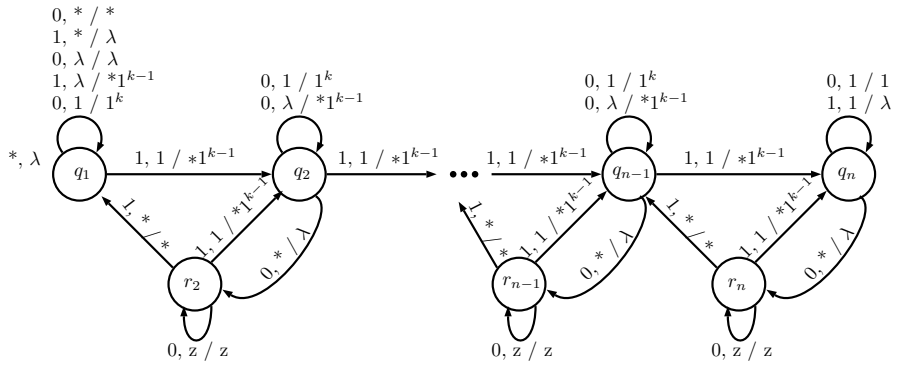

Рис. 7. Диаграмма автомата P.

имеет место зависимость от двух верхних символов магазина. Тем не менее, этих уравнений оказывется вполне достаточно, чтобы вычислить длину периода выходной последовательности.

Введем следующие обозначения:

$$\omega(q_n, *^i 1 *^{n-i}) = \omega_i + \omega(q_n, *^n),\ i = 1, ..., n.$$

Нетрудно видеть, что

$$\omega(q_n, *^n 1) = p + \omega(q_n, *^n 1),$$

то есть

$$\omega_n = p.$$

$$\omega(q_n, *^{n-1} 1 *) = p + \omega(q_n, *^n 1^{k-1}) = p + (k-1)p + \omega(q_n, *^n) = kp + \omega(q_n, *^n).$$

Откуда получаем, что

$$\omega_{n-1} = kp.$$

Обозначим $d = (k-1)p - 1$.

$$\omega(q_n, *^{n-2} 1 * *) = p + \omega(q_{n-1}, *^{n-2} 1 (k-1)) =$$

$$= 2p + \omega(q_{n-1}, *^{n-1} 1^k) = 3p + \omega(q_{n-1}, *^{n-1} 1^d * 1^{k-1} =$$

$$= 2p + kp + \omega(q_n, *^{n-1} 1^d *) = 2p + (d+1)kp + \omega(q_n, *^n).$$

Откуда получаем, что

$$\omega_{n-2} = 2p + (d+1)\omega_{n-1}.$$

По индукции получаем, что

$$\omega_i = 2p + (d+1)\omega_{i+1}$$

для $i = 1, ..., n-2$.

Обозначим $\omega_0 = 2p + (d+1)\omega_1$. Получили систему линейных уравнений:

$$\begin{cases} \omega_{n-1} = kp, \\ \omega_{n-2} = 2p + (d+1)\omega_{n-1}, \\ ... \\ \omega_i = 2p + (d+1)\omega_{i+1}, \\ ... \\ \omega_0 = 2p + (d+1)\omega_1, \end{cases}$$

Решая систему, получаем:

$$\omega_0 = 2p\frac{(d+1)^{n-1}-1}{d} + (d+1)^{n-1}kp = 2p\frac{((k-1)p)^{n-1}-1}{(k-1)p-1} + ((k-1)p)^{n-1}kp.$$

Нетрудно видеть, что для длины периода выполнено:
$L(P,\alpha) = \omega(q_1, \lambda) = p + \omega(q_1, *1^{k-1}) = 2p + \omega(q_2, *1^d * 1^{k-1}) = ... =$
$= np + \omega(q_n, (*1^d)^{n-1} * 1^{k-1}) = np + (k-1)n + \omega(q_n, (*1^d)^{n-1}*) =$
$= (n-1)p + kp + \omega(q_n, (*1^d)^{n-1}*) = (n-1)p + \omega_{n-1} + \omega(q_n, (*1^d)^{n-1}*) =$
$= (n-1)p - 2p + 2p + \omega_{n-1} + d\omega_{n-1} + \omega(q_n, (*1^d)^{n-1}*) =$
$= (n-1)p - 2p + \omega_{n-2} + \omega(q_n, (*1^d)^{n-2}*^2) =$
$= (n-1)p - 4p + \omega_{n-3} + \omega(q_n, (*1^d)^{n-3}*^3) = ... =$
$= (n-1)p - 2(n-2)p + \omega_1 + \omega(q_n, (*1^d)*^{n-1}) =$
$= (n-1)p - 2(n-1)p + \omega_0 + \omega(q_n, *^n) = \omega_0 - (n-1)p + \omega(q_n, *^n) =$
$= \omega_0 + p.$
Продолжая, получаем:

$$L(P,\alpha) = \omega_0 + p = p + 2p\frac{((k-1)p)^{n-1}-1}{(k-1)p-1} + ((k-1)p)^{n-1}kp.$$

При $k = 2$ получаем, что длина периода полиномиально зависит от длины входного периода и равна:

$$2p^n + p + 2\frac{p^n - p}{p - 1}.$$

Данный пример позволяет доказать следующую теорему.

Теорема 15. *Для любого многочлена $q(x)$ найдется автомат с магазинной памятью P из $\mathcal{M}(n, 2, 2)$ такой, что на последовательностях α^∞, где $\alpha = 0^{p-1}1$, $p \in \mathbb{N}_0$, а $\mathbb{N}_0$ — бесконечное подмножество натуральных чисел, период выходной последовательности будет больше, чем $q(p)$.*

Доказательство. Достаточно рассмотреть автомат из предыдущего примера с достаточно большим числом состояний. □

7. Заключение

В данной работе рассматривалась задача описания автоматов с магазинной как преобразователей последовательностей. Было известно, что, так же как и конечные автоматы, автоматы с магазинной памятью переводят периодические последовательности в периодические. Вокруг этого факта и выстроена работа, а именно: приведено описание зависимости периода выходной последовательности от характеристик автомата и периода входной последовательности. Оказалось, что наличие потенциально бесконечной памяти в виде магазина принципиально усложняет эту задачу.

Большая часть работы посвящена описанию автономного автомата с магазинной памятью. Была приведена экспоненциальная от характеристик автомата верхняя оценка на период выходной последовательности для автономного случая. В случае, когда в алфавите магазина есть хотя бы два символа, удалось построить пример, который показывает, что принципиально оценку понизить нельзя. Однако в случае, когда алфавит магазина содержит ровно один символ, ситуация резко упрощается. В этом случае удалось доказать верхнюю квадратичную от числа состояний оценку. Был приведен пример, в котором полученная верхняя оценка асимптотически достигается.

Оценки, полученные для автономного случая, удалось применить для получения оценок для случая автомата со входом. Оказалось, что даже в простейшем случае, когда в алфавите магазина всего один символ, автомат может преобразовывать период квадратичным образом, то есть период выходной последовательности квадратично зависит от периода входной. В этом заключается принципиальное отличие класса автоматов с магазинной памятью от класса конечных автоматов. Более того, был построен пример автомата всего с двумя состояниями, который способен преобразовывавать период входной последовательности квадратично. В общем же случае, когда в алфавите магазина разрешено использовать более одного символа, автомат способен преобразовывать периодическую последовательность полиномиально.

Помимо уже описанных результатов отдельным пунктом хотелось бы отметить, что в процессе доказательства утверждений было разработано некоторое количество алгоритмов, которые позволяют по уравнениям автомата эффективно получать длину периода выходной последовательности.

Подход к изучению периодических свойств — это первый шаг к построению теории фукнциональных систем на основе автоматов с магазинной памятью. Описание периодических свойств позволяет по-новому взглянуть на автомат с магазинной памятью. Автор верит, что предложенные им подходы могут быть плодотворно применены к решению задач, связанных с автоматами с магазинной памятью.

Автор выражает глубокую благодарность своему научному руководителю — доктору физико-математических наук, профессору Дмитрию Николаевичу Бабину за постановку задачи, постоянное внимание к работе и всестороннюю поддержку, профессору Гасанову Эльяру Эльдаровичу и Калачеву Глебу Вячеславовичу за плодотворное обсуждение работы, а также заведующему кафедрой академику Валерию Борисовичу Кудрявцеву и всему коллективу кафедры математической теории интеллектуальных систем за доброжелательную и творческую атмосферу.

Список литературы

[1] А. Ахо, Дж. Ульман Теория синтаксического анализа, перевода и компиляции, 1, Мир, 1978.

[2] Бабин Д.Н. О суперпозициях о.д.-функций ограниченного веса, Логико-алгебраические конструкции, Тверь, 1984,21-27.

[3] Бабин Д.Н., Разрешимый случай задачи о полноте автоматных функций, Дискретная математика, том 4, выпуск 4, 1992, 41-56, Наука, Москва.

[4] Бабин Д.Н., О классификации автоматных базисов Поста по разрешимости свойств полноты и A-полноты, ДАН, том 367, выпуск 4, 1999, 439-441.

[5] Бабин Д.Н., О полноте двухместных о.д.-функций относительно суперпозиции, Дискретная математика, том 1, выпуск 4, 1989, 86-91.

[6] Bar-Hillel Y., Perles M., Shamir E., On formal properties of simple phrase structure grammars. Z. Phonctik, Sprachwissensch. Kommunikationsforsch. 14, 1961, 143-172.

[7] C. Beeri, An improvement on Valiant's decision procedure for equivalence of deterministic finite-turn pushdown automata, Theoret. Comput. Sci. 3 (1976) 305-320.

[8] Буевич В.А. Об алгоритмической неразрешимости распознавания A-полноты для ограниченно-детерминированных функций, Математические заметки, выпуск 6, 1972, 687-697.

[9] Буевич В.А. Условия A-полноты для автоматов, М., изд. МГУ, 1986.

[10] Гинзбург С. (Ginsburg S.), The mathematical theory of context-free languages, McGraw-Hill, New York. (Русский перевод: Гинзбург С., Математическая теория контекстно-свободных языков, изд-во "Мир М., 1970).

[11] Гинзбург С., Грейбах С. (Ginsburg S.,Greibach S.), Deterministic context free languages, Information and Control, Volume 9, Issue 6, 1966, 620–648.

[12] Dassow J., Ein modifizierter Vollstandigkeitsbegriff in einer Algebra von Automatenabbildungen, Dissertation Doktor B, Rostock, Universitet,1978.

[13] S. Bohm, S. Goller, P. Jancar, Equivalence of deterministic one-counter automata is NL-complete, in: Proc. of STOC, ACM, 2013, pp. 131–140.

[14] S. Bohm, S. Goller, P. Jancar, Bisimulation equivalence and regularity for real-time one-counter automata, Journal of Computer and System Sciences Volume 80, Issue 4, June 2014, pp. 720–743.

[15] Гинсбург С., Роуз (Ginsburg S., Rose G.F.), Some recursively unsolvable problems in ALGOL-like languages, J. Assoc. Computing Machinety, 10, 1963, 175-195.

[16] M.A. Harrison, I.M. Havel, A. Yehudai, On equivalence of grammars through transformation trees, Theoret. Comput. Sci. 9 (1979), 173-205.

[17] Иванов И. Е. Нижняя оценка на максимальную длину периода выходной последовательности автономного автомата с магазинной памятью. Интеллектуальные системы, том 19, вып. 3, 2015, 175-193.

[18] Иванов И. Е. Улучшение нижней оценки на максимальную длину периода выходной последовательности автономного автомата с магазинной памятью Интеллектуальные системы, том 20, вып. 4, 2016, 166-183.

[19] Иванов И. Е. Оценка длины периода выходной последовательности для автономного автомата с магазинной памятью с однобуквенным магазином. Интеллектуальные системы, том 21, вып. 1, 2017, 112-148.

[20] P. Jancar, Bisimulation is decidable for one-counter processes, Proc. ICALP 97, Springer, Berlin, 1997, pp. 549-559.

[21] Клини (Kleene S.C.), Representation of events in nerve nets, в сб. Automata Studies под ред. Shannon C.E., McCarthy J., Princeton University Press, Princeton, N.J. (Русский перевод: Клини С.К., Представление событий в нервных сетях, в сб. "Автоматы ИЛ, М., 1956, 15-67.)

[22] Wolfgang Coy, Automata in Labyrinths, FCT, 1977, 65-71.

[23] A.J. Korenjac, J.E. Hopcroft, Simple deterministic languages, Proc. 7th Annu. IEEE Switching and Automata Theory Conf., 1966, pp. 36-46.

[24] Кратко М.И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов, ДАН СССР, 1964, том 155, выпуск 1, 35-37.

[25] Кудрявцев В.Б. Теорема полноты для одного класса автоматов без обратных связей. Проблемы кибернетики, 1962 год №8, 91-115.

[26] Кудрявцев В.Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами, ДАН СССР том 151, выпуск 3, 1963, 493-496.

[27] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. М.:Наука, 1985.

[28] Летичевский А.А. Условия полноты для конечных автоматов, Вычислительная математика и математическая физика, №4, 1961, 702-710.

[29] Летуновский А.А. Цикловые индексы автомата. Дискретная математика, том 25, выпуск 4, 24-29.

[30] Мак-Калок, Питтс (McCullough W.S., Pitts E.), A logical calculus of the ideas immanent in nervous activity, Bull. Math. Biophys., 5, 1943, 115-133. (Русский перевод: Маккалок У.С. Питтс Э., Логическое исчисление идей, относящихся к нервной активности, в сб. "Автоматы ИЛ, М., 1956, 362-384)

[31] McNaughton R. Testing and generating infinite sequence by a finite automation. - Information and Control, v.9, 5, 1966, 521-530.

[32] Мур (Moore E.F.) Gedanken experiments on sequential machines в сб. Automata Studies под ред. Shannon C.E., McCarthy J., Princeton University Press, Princeton, N.J. (Русский перевод: Мур Э.Ф., Умозрительные эксперименты с последовательностными машинами, в сб. "Автоматы ИЛ, М., 1956, 179-210.)

[33] Dominique Perrin, Jean-ŕEric Pin (2004): Infinite words. Pure and Applied Mathematics 141, Elsevier.

[34] Рабин, Скотт (Rabin M.O., Scott D.) Finite automata and their decition problems, IMB J. Res. Devel., 3, 1959, 114-125. (Русский перевод: Рабин М.О., Скотт. Д., Конечные автоматы и задачи их разрешения, Кибернетический сборник, вып 4, ИЛ, М., 1962, 56-91.)

[35] Тьюринг (Turing A. M.), On computable numbers, with an application to the Entscheidungs problem, Proc. London Math. Soc., ser. 2, 42, 1936, 230-265; Corrections, там же, 43, 544-546.

[36] Хомский (Chomsky N.), Three models for the description of language. IRE Transactions on Information Theory, 2:3, 1956, 113–124. (Русский перевод: Хомский Н. Три модели для описания языка, Кибернетический сборник, вып. 2, ИЛ, М., 1961, 237-266.)

[37] Хомский (Chomsky N.), Context-free grammars and pushdown storage, Quarlerly Progress Report, № 65, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambrig, Mass, 1962.

[38] Шютценберже (Schutzenberger M. P.), On contex-free languages and pushdown automata, Information and Control, 6:3, 1963, 246-264.

[39] Эви (Evey R.J.), Applications of pushdown-store machines, Proc. AFIPS Fall Joint Computer Conference, 24, 1963, 215-227.

[40] Эттингер (Oettinger A.), Automatic syntatic analysis and the pushdown store, в сб. Structure of Language and its Mathematical Concepts, Proc. 12th Symposium on Applied Mathematics, 1961, 104-129.

[41] M. Oyamaguchi, The equivalence problem for real-time d.p.d.a's, J. Assoc. Comput. Mach. 34 (1987), 731-760.

[42] M. Oyamaguchi, Y. Inagaki, N. Honda, The equivalence problem for real-time strict deterministic languages, Inform. and Control 45 (1980), 90-115.

[43] Post E. Two-Valued 1.erative Systems of Mathematical Logic. Princeton Univ. Press, Princeton, 1941.

[44] V.Yu. Romanovskii, Equivalence problem for real-time strict deterministic pd-automata, Kibernetika (5) (1980) 49-59 (English translation in Cybernet. Systems Anal. (1981), 689-700.

[45] V.Yu. Romanovskii, Equivalence problem for real-time deterministic pushdown automata, Kibernetika (2) (1986), 13-23 (English translation in Cybernet. Systems Anal. (1986), 162-175).

[46] G. Senizergues, The equivalence problem for deterministic pushdown automata is decidable, Proc. ICALP 97, Lecture Notes in Computer Science, vol. 1256, Springer, Berlin, 1997, pp. 671-681.

[47] R. E. Stearns, A Regularity Test for Pushdown Machines, INFORMATION AND CONTROL 11, 323-340 (1967).

[48] C. Stirling, Decidability of bisimulation equivalence for normed pushdown processes, Proc. CONCUR 96, Lecture Notes in Computer Science, vol. 1119, Springer, Berlin, 1996, pp. 217-232.

[49] Строгалов А.С., Метрические свойства о.д.-функций, Межвузовский сборник трудов, N 56, МЭИ, 1985, стр. 80-84.

[50] Rozenberg, Grzegorz, Salomaa, Arto (Eds.), Handbook of Formal Languages, Volume 3 Beyond Words, Ludwig Staiget, chapter 6, 339-382, Springer, 1997.

[51] L.G. Valiant, Decision procedures for families of deterministic pushdown automata, Ph.D. Thesis, University of Warwick, 1973.

[52] L.G. Valiant, M.S. Paterson, Deterministic one-counter automata, J. Comput. System Sci. 10 (1975) 340-350.

[53] Хазбун И.В., Об условиях полноты и выразимости в точной алгебре автоматов, Логико-алгебраические конструкции, Тверь 1984, стр. 35-41.

алгебре автоматов

[54] Часовских А.А., О полноте в классе линейных автоматов, Математическме вопросы кибернетики, 1995, N3, стр. 140-166.

[55] Яблонский С.В. Функциональные построения в k-значной логике, Труды математического института им. В.А. Стеклова, АН СССР, 1958, Т.51, стр. 5-142.

About automaton functions for pushdown automaton
Ivanov I.E

Realtime pushdown transducer saves the set of periodic sequences. Earlier the author found upper and lower bounds for max period of output for transducer without input as a function from parameters of transducer. There are upper and lower bounds for max period of output in general case in current paper. The max period of transducer output has been studied as function from period of input sequence.

Keywords: realtime pushdown transducer, deterministic function, periodic sequences.

О нижней оценке максимального потенциала плоских схем с несколькими выходами через площадь

Калачев Г. В.

В статье исследуется связь между площадью и максимальным потенциалом плоских схем, реализующих булевы операторы. Максимальный потенциал — мера сложности плоских схем, отражающая энергопотребление схемы в худшем случае, его также часто называется активностью. Он равен максимальному числу выходов элементов схемы, равных 1, где максимум берётся по всем входным наборам схемы. В работе показано, что для произвольного булева оператора потенциал $\widehat{U}$ не меньше, чем $\sqrt{S}/4\sqrt{2}$, где S — площадь минимальной схемы, реализующей данный оператор.

Ключевые слова: клеточные схемы, активность, потенциал, связь мер сложности, нижние оценки, булевы операторы.

1. Введение

Плоская(клеточная) схема — это схема из функциональных элементов, уложенная на плоскость так, чтобы каждому входу и выходу соответствовала некоторая сторона клетки, в которой находится элемент. Таким образом, в такой схеме могут использоваться любые функциональные элементы, у которых в сумме не более четырёх контактов. Понятие клеточных схем ввёл Кравцов С.С. в работе [1] и показал, что порядок площади плоских схем, реализующих булевы функции от n переменных, равен 2^n.

В работе рассматривается максимальная мощность, выделяемая схемой. В работе [2] была введена мера мощности плоских схем — активность, и было показано, что дешифратор нельзя реализовать плоской схемой, одновременно оптимальной по площади и активности. В работе [3] была доказана нижняя оценка максимального потенциала булевых функций через их площадь.

В данной работе мы обобщим этот результат на случай частичных булевых операторов.

2. Определения и формулировка результата.

Формальное определение плоской схемы достаточно громоздкое, поэтому приведём неформальное определение[3]. *Плоской схемой* называется такая укладка схемы из функциональных элементов на плоскость, что каждый функциональный элемент помещается в ячейку целочисленной решётки на плоскости, чтобы его входы и выходы оказались на сторонах ячейки; при этом соединяющие провода также укладываются в свободные ячейки и моделируются цепочкой клеточных элементов, реализующих тождественные функции.

Чтобы сформулировать результаты, введем несколько определений. Рассмотрим плоскую схему K с n входами и n выходами. Входы схемы K, а также выходы всех ее элементов назовем *узлами* схемы K. Множество схем, реализующих оператор f обозначим $\mathrm{Impl}(f)$.

Площадью схемы K будем называть количество её элементов, будем обозначать эту величину $S(K)$.

Площадью булева оператора $f : \mathcal{D}' \to \{0,1\}^m$ назовём величину $S(f) := \min\limits_{K \in \mathrm{Impl}(f)} S(K)$, то есть площадь минимальной схемы, реализующей оператор f.

Потенциалом схемы K *на наборе* x назовем количество узлов схемы K, принимающих значение 1, когда на вход схемы подан набор x, будем обозначать эту величину $u_K(x)$.

Максимальным потенциалом схемы K на множестве $\mathcal{D} \subset \{0,1\}^n$ назовем величину $\widehat{U}_{\mathcal{D}}(K) = \max\limits_{x \in \mathcal{D}} u_K(x)$.

Максимальным потенциалом булева оператора $f : \mathcal{D}' \to \{0,1\}^m$ на множестве $\mathcal{D}$ назовём величину $\widehat{U}_{\mathcal{D}}(f) = \min\limits_{K \in \mathrm{Impl}(f)} \widehat{U}_{\mathcal{D}}(K)$. С случае $\mathcal{D} = \{0,1\}^n$ нижний индекс $\mathcal{D}$ у меры $\widehat{U}$ будем опускать.

Теорема 1. *Для любого оператора* $f : \mathcal{D} \to \{0,1\}^m$ *выполнено*

$$\widehat{U}(f) \succcurlyeq \frac{\sqrt{S(f)}}{4\sqrt{2}}.$$

[3]Формальное определение плоской схемы можно посмотреть, например, в [3].

Замечание. Заметим, что в теореме рассматривается максимальный потенциал на множестве всех наборов $\{0,1\}^n$, а не на области определения оператора f. Однако, в случае, когда есть выход оператора f, существенно зависящий от всех переменных, то работает доказательство, полностью аналогичное доказательству из [3], только участвующие в доказательстве наборы будут принадлежать множеству $\mathcal{D}$. В этом случае верна оценка:

$$\widehat{U}_{\mathcal{D}}(f) \succcurlyeq \frac{\sqrt{S(f)}}{4\sqrt{2}}.$$

3. Доказательство

Рассмотрим произвольный оператор $f : \mathcal{D} \to \{0,1\}^m$, у которого каждый выход отличен от константы и схему K, который реализует оператор f с наименьшим максимальным потенциалом (из всех схем с одинаковым потенциалом выберем схему с наименьшим количеством узлов).

При таком способе выбора схемы K все её входы соответствуют существенным переменным оператора f на множестве $\mathcal{D}$, иначе можно было бы удалить несущественный вход, уменьшив количество узлов схемы и не увеличив её максимальный потенциал. Также простым, но важным свойством схемы K является то, что каждый её узел зависит существенно от некоторого входа схемы, иначе он равен константе, и его можно удалить, уменьшив число узлов схемы. Поскольку базис мы никак не ограничиваем, то константный узел можно удалить, заменив соответствующим образом клеточный элемент, для которого этот узел является входом. По аналогии, каждый узел, являющийся входом некоторого элемента, является существенной переменной некоторого его выхода, иначе его также можно было бы удалить, уменьшив число узлов.

Без ограничения общности будем считать, что все оператор f существенно зависит от всех n переменных. По схеме K построим граф G_K с n вершинами следующим образом.

- Вершинами графа G_K являются входы схемы K.
- Входы x_i и x_j соединены ребром, если существует узел α_{ij} схемы K такой, что функция $\phi_{\alpha_{ij}}$, реализуемая в узле α_{ij} существенно зависит от x_i и x_j.

Случай связного графа G_K. Если граф G_K связен, достроим его до графа $\overline{G}_K$

- Найдём в схеме K два наиболее удалённых друг от друга узла β_1 и β_2.
- Добавим к графу G_K две дополнительные вершины β_1 и β_2.
- Соединим вершину β_i ($i \in \{1,2\}$) ребром со всеми входами x_j, от которых ϕ_{β_i} существенно зависит.

Найдём в графе $\overline{G}_K$ кратчайший путь $\pi = [\beta_1, x_{i_1}, ..., x_{i_k}, \beta_2]$, соединяющий вершины β_1 и β_2. Без ограничения общности можно считать, что $i_1 < i_2 < ... < i_k$. Для краткости и единообразия переобозначим узлы $\alpha_{i_j i_{j+1}}$ за γ_j ($j = 1, ..., k-1$), а также положим $\gamma_0 = \beta_1$, $\gamma_k = \beta_2$. Для каждого из узлов γ_j введём набор номеров переменных $V_j = (v_j^1, ..., v_j^{m_j})$, от которых ϕ_{γ_j} зависит существенно, причём набор V_j упорядочен таким образом, что $v_j^1 = i_j$ при $j \geq 1$ и $v_j^{m_j} = i_{j+1}$ при $j \leq k-1$. Заметим, что V_j и V_{j+s} как множества не пересекаются при $s \geq 2$, поскольку иначе переменная $x_t \in V_j \cap V_{j_s}$ была бы в графе G_k соединена с вершинами x_j и x_{j+s+1}, что противоречит тому, что путь π — кратчайший.

Если $V = \{j_1, ..., j_s\}$ — набор индексов ($1 \leq j_t \leq n$), $x = (x_1, ..., x_n)$, тогда через $x[V]$ обозначим набор $(x_{j_1}, ..., x_{j_s})$. Положим $\phi_j(x[V_j]) = \phi_{\gamma_j}(x)$ — функция, полученная из ϕ_{γ_j} удалением несущественных переменных и перестановкой существенных переменных. Зафиксируем наборы $y'_j \in \{0,1\}^{|V_j|-1}$ для всех $j = 0, ..., k-1$ и $y''_j \in \{0,1\}^{|V_j|-1}$ для всех $j = 1, ..., k$ такие, что $\phi_j(0, y'_j) \neq \phi_j(1, y'_j)$ и $\phi_j(y''_j, 0) \neq \phi_j(y'', 1)$.

Через e_i обозначим двоичный вектор длины n, в котором i-й координата равна 1, а остальные равны 0. Поскольку $V_j \cap V_{j+s} = \varnothing$ при $s \geq 2$, существуют наборы $u_s^{t\prime}$, $u_s^{t\prime\prime} \in \{0,1\}^n$ ($s, t \in \{0,1\}$) такие, что

$$u_0^{t\prime}[V_j] = (y'_j, 0), \quad u_0^{t\prime\prime}[V_j] = (0, y''_j), \text{ где } t \equiv j \mod 2,$$

$$u_1^{t\prime} = u_0^{t\prime} \oplus \bigoplus_{j \equiv t (mod\ 2)} e_{i_{j+1}}, \quad u_1^{t\prime\prime} = u_0^{t\prime\prime} \oplus \bigoplus_{j \equiv t (mod\ 2)} e_{i_j}.$$

Для каждого допустимого значения индекса j при $t = j \mod 2$ выполнено

$$\phi_{\gamma_j}(u_0^{t\prime}) = \phi_j(y'_j, 0) \neq \phi_j(y'_j, 1) = \phi_{\gamma_j}(u_0^{t\prime} \oplus e_{i_{j+1}}),$$

$$\phi_{\gamma_j}(u_0^{t\prime\prime}) = \phi_j(0, y''_j) \neq \phi_j(1, y''_j) = \phi_{\gamma_j}(u_0^{t\prime\prime} \oplus e_{i_j}).$$

Поскольку сложение по модулю 2 с вектором e_i изменяет лишь i-ю координату вектора, то существуют цепи c'_j и c''_j, соединяющие узел γ_j со входами $x_{i_{j+1}}$ и x_{i_j} соответственно такие, что $\phi_\gamma(u_0^{t\prime}) \neq \phi_\gamma(u_0^{t\prime} \oplus e_{i_{j+1}})$

для всех узлов $\gamma \in c'_j$ и $\phi_\gamma(u_0^{t\,\prime\prime}) \neq \phi_\gamma(u_0^{t\,\prime\prime} \oplus e_{i_j})$ для всех узлов $\gamma \in c''_j$. Кроме того, для любого узла γ цепи c'_j функция ϕ_γ зависит существенно от переменной $x_{i_{j+1}}$ и не зависит от переменной x_{i_s} при $|s-(j+1)| \geq 2$, иначе в графе $\overline{G}_K$ вершина $x_{i_{j+1}}$ была бы соединена с x_s, и путь π не был бы кратчайшим. А это означает, что $\phi_\gamma(u_1^{t\,\prime}) = \phi_\gamma(u_0^{t\,\prime} + e_{i_{j+1}}) \neq \phi_\gamma(u_0^{t\,\prime})$, и что цепи c'_j и c'_{s-1} не пересекаются. Аналогично $\phi_\gamma(u_0^{t\,\prime\prime}) \neq \phi_\gamma(u_1^{t\,\prime\prime})$ для любого узла γ цепи c''_j и цепи c''_j и c''_s не пересекаются при $|s-j| \geq 2$.

Теперь мы можем оценить сумму потенциалов схемы K на наборах $u_0^{t\,\prime}$, $u_1^{t\,\prime}$, $u_0^{t\,\prime\prime}$ и $u_1^{t\,\prime\prime}$

$$u_K(u_0^{t\,\prime}) + u_K(u_1^{t\,\prime}) \geq \sum_{j \equiv t (mod\ 2)} \sum_{\gamma \in c'_j} \Big(\phi_\gamma(u_0^{t\,\prime}) + \phi_\gamma(u_1^{t\,\prime}) \Big) = \sum_{j \equiv t (mod\ 2)} |c'_j|,$$

$$u_K(u_0^{0\,\prime}) + u_K(u_1^{0\,\prime}) + u_K(u_0^{1\,\prime}) + u_K(u_1^{1\,\prime}) \geq$$

$$\geq \sum_{j \equiv 0 (mod\ 2)} |c'_j| + \sum_{j \equiv 1 (mod\ 2)} |c'_j| = \sum_{j=0}^{k-1} |c'_j|.$$

По аналогии имеем

$$u_K(u_0^{0\,\prime\prime}) + u_K(u_1^{0\,\prime\prime}) + u_K(u_0^{1\,\prime\prime}) + u_K(u_1^{1\,\prime\prime}) \geq \sum_{j=1}^{k} |c''_j|.$$

Отсюда с использованием неравенства треугольника получим

$$\sum_{s \in \{0,1\}} \sum_{t \in \{0,1\}} (u_K(u_s^{t\,\prime}) + u_K(u_s^{t\,\prime\prime})) \geq |c'_0| + \sum_{j=1}^{k-1} (|c'_j| + |c''_j|) + |c''_k| \geq$$

$$\geq \rho_K(\gamma_0, x_{i_1}) + 1 + \sum_{j=1}^{k-1} \big(\rho_K(x_{i_j}, x_{i_{j+1}}) + 2 \big) + \rho_K(x_{i_k}, \gamma_k) + 1 \geq$$

$$\geq \rho_K(\gamma_0, \gamma_k) + 2k = \rho_K(\beta_1, \beta_2) + 2k.$$

Нетрудно убедиться, что максимальная площадь целочисленного множества с диаметром d в манхеттеновской метрике не превосходит $(d+1)^2/2$. Поскольку β_1 и β_2 — пара наиболее удалённых друг от друга узлов схемы, то расстояние между ними не меньше диаметра схемы, значит

$$\rho_K(\beta_1, \beta_2) + 2k \geq \sqrt{2S(K)} - 1 + 2k > \sqrt{2S(K)}.$$

Отсюда получаем требуемую оценку

$$\widehat{U}(f) = \widehat{U}(K) \geq \max_{s\in\{0,1\}} \max_{t\in\{0,1\}} \max(u_K(u_s^{t\prime}), u_K(u_s^{t\prime\prime})) \geq$$
$$\geq \frac{1}{8}\Big(\sum_{s\in\{0,1\}} \sum_{t\in\{0,1\}} \big(u_K(u_s^{t\prime}) + u_K(u_s^{t\prime\prime})\big)\Big) \geq$$
$$\geq \frac{\rho_K(\beta_1,\beta_2)+2k}{8} > \frac{\sqrt{2S(f)}}{8} = \frac{\sqrt{S(f)}}{4\sqrt{2}}.$$

Случай несвязного графа G_K. Пусть граф G_K имеет ℓ компонент связности, и V_i — множество вершин G_K в i-й компоненте связности. Каждому V_i соответствует множество узлов N_i схемы K, зависящих от переменных из V_i. Множества N_i и N_j не пересекаются при $i \neq j$, поскольку иначе был бы узел, существенно зависящий одновременно от переменных из V_i и V_j, значит в G_K множества V_i и V_j были бы в одной компоненте связности. Множество узлов N_i задаёт подсхему K_i схемы K с множеством входов V_i. Каждый элемент схемы K входит в некоторую подсхему K_i, иначе его выход был бы равен константе, и его можно было бы удалить. Значит $S(K_1) + ... + S(K_\ell) \geq S(K)$. Поскольку множества входных переменных подсхем K_i не пересекаются, то максимальный потенциал схемы K складывается из максимальных потенциалов подсхем $K_1, ..., K_\ell$, а именно

$$\widehat{U}(K) = \max_{x\in\{0,1\}^n} u_K(x) = \max\Big\{\sum_{i=1}^{\ell} u_{K_i}(x_i) \;\Big|\; x_1, ..., x_\ell \in \{0,1\}^{|V_i|}\Big\} =$$
$$= \sum_{i=1}^{\ell} \max_{x_i\in\{0,1\}^{|V_i|}} u_{K_i}(x_i) = \sum_{i=1}^{\ell} \widehat{U}(K_i).$$

Для каждой подсхемы K_i граф G_{K_i} соответствует компоненте связности G_K с множеством вершин V_i, и по доказанному случаю $\widehat{U}(K_i) \geq \sqrt{S(K_i)}/4\sqrt{2}$. Значит

$$\widehat{U}(K) = \sum_{i=1}^{\ell} \widehat{U}(K_i) \geq \frac{1}{4\sqrt{2}} \sum_{i=1}^{\ell} \sqrt{S(K_i)} \geq \frac{1}{4\sqrt{2}} \sqrt{\sum_{i=1}^{\ell} S(K_i)} \geq \frac{\sqrt{S(K)}}{4\sqrt{2}}.$$

Теорема доказана.

Список литературы

[1] Кравцов С.С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. Вып. 19. М.: Наука, 1967. 285–293.

[2] Калачев Г.В. Порядок мощности плоских схем, реализующих булевы функции // Дискретн. матем. 2014. **26**, № 1. 49—74.

[3] Калачев Г.В. Оценки мощности плоских схем, реализующих монотонные функции // Интеллектуальные системы. Теория и приложения. 2017. **21**, № 2. 163—192.

On the lower bound for the maximum potential of plain circuits with several outputs through the area

Kalachev G. V.

In this paper we consider the relationship between the area and the maximum potential of plain circuits realizing Boolean operators. The maximal potential is a complexity measure of plain circuits, reflecting the power consumption of the circuit in the worst case, it is also often called activity. It is equal to the maximum number of outputs of circuit elements equal to 1, where the maximum is taken over all input sets of the circuit.It was porved that for arbitrary Boolean operator f, its maximal potential $\widehat{U}$ is greater or equal than $\sqrt{S}/4\sqrt{2}$ where S is the area of the minimal plain circuit realizing f.

Keywords: plain circuits, activity, potential, retations between complexity measures, lower bounds, Boolean operators.

Часть 3.
Материалы семинара «Теория автоматов»

Доклады семинара «Теория автоматов»

В первом квартале 2018 года на научном семинаре «Теория автоматов» под руководством академика Валерия Борисовича Кудрявцева состоялись 3 доклада.

28 февраля 2018 года

От двузначной к k-значной логике

с.н.с. Жук Д. Н.

Традиционно считается, что при переходе от двузначного к многозначному случаю свойства решетки замкнутых классов функций координально меняются. В докладе будет показано, что несмотря на различия, эти решётки во многом похожи, а очень многие свойства, которые следуют из решетки Поста, могут быть обобщены на многозначный случай. Одним из таких примеров является решение задачи удовлетворения ограничениям для многозначного случая - показано, что самый общий полиномиальный алгоритм является во многом лишь комбинацией методов, давно известных для двузначного случая.

7 марта 2018 года

От булевых схем к доказательству теорем

доцент Боков Г. В.

Вопрос о сложности доказательств теорем в формальных системах возникает во многих областях. С точки зрения вычислительной сложности точные нижние оценки сложности доказательств служат средством отделения классов вычислительной сложности. В современных SAT- и SMT-решателях анализ лежащих в их основе систем доказательств позволяет оценить производительность и ограниченность решателей. Центральное место в вопросе сложности доказательств отводится доказательству теорем классического исчисления высказываний. Несмотря на то, что за последние десятилетия удалось разработать много разнообразных техник для доказательства верхних и нижних оценок в различных пропозициональных системах, успеха в получении нижних оценок для классических систем доказательств достичь так и не удалось. Тем не менее, среди специалистов в области сложности доказательств сложилась

прочная уверенность в том, что существует тесная связь между прогрессом в получении нижних оценок сложности булевых схем и прогрессом в получении нижних оценок размера пропозициональных доказательств. В докладе будет рассказано о связи между булевыми схемами и системами доказательств теорем, о том, как идеи и методы, применяемые для оценки сложности схем, применяются для оценки сложности доказательств теорем.

14 марта 2018 года

Об обобщении теоремы Мура

доцент Пантелеев П. А.

Диагностические эксперименты с конечными автоматами впервые были описаны в классической работе Э. Мура, и с тех пор применяются при решении практических и теоретических задач, возникающих в таких областях как тестирование программ, диагностика неисправностей цифровых схем, а также при верификации коммуникационных протоколов. Если имеется полное описание некоторого конечного автомата Мили, но про его начальное состояние известно лишь то, что оно принадлежит некоторому фиксированному подмножеству состояний, то простой диагностический эксперимент для этого подмножества состоит в подаче на автомат такой входной последовательности, что по реакции автомата на нее можно однозначно сказать с каким начальным состоянием мы имели дело. В докладе будет рассказано об оценках длины для таких экспериментов и показана связь данной задачи с комбинаторными проблемами, возникающими в теории гиперграфов.

От булевых схем к доказательству теорем

Боков Г. В.

Вопрос о сложности доказательств теорем в формальных системах возникает во многих областях. С точки зрения вычислительной сложности точные нижние оценки сложности доказательств служат средством отделения классов вычислительной сложности. В современных SAT- и SMT-решателях анализ лежащих в их основе систем доказательств позволяет оценить производительность и ограниченность решателей. Центральное место в вопросе сложности доказательств отводится доказательству теорем классического исчисления высказываний. Несмотря на то, что за последние десятилетия удалось разработать много разнообразных техник для доказательства верхних и нижних оценок в различных пропозициональных системах, успеха в получении нижних оценок для классических систем доказательств достичь так и не удалось. Тем не менее, среди специалистов в области сложности доказательств сложилась прочная уверенность в том, что существует тесная связь между прогрессом в получении нижних оценок сложности булевых схем и прогрессом в получении нижних оценок размера пропозициональных доказательств. В работе будет рассказано о связи между булевыми схемами и системами доказательств теорем, о том, как идеи и методы, применяемые для оценки сложности схем, применяются для оценки сложности доказательств теорем.

Ключевые слова: Системы пропозициональных доказательств, сложность доказательств, булевы схемы, сложность схем, классы сложности.

Одной из центральных проблем теории сложности вычислений является вопрос о существовании полиномиальной разрешающей процедуры для классического пропозиционального исчисления. Её важность обусловлена взаимосвязью с задачей о равенстве классов сложности **P** и **NP** [Coo71], решение которой позволит получить ответ о сложности многих комбинаторных проблем [Kar72]. Сама проблема тесно связана с изучением сложности минимального пропозиционального вывода классических тавтологий [CR74].

Отправной точкой в изучении сложности пропозиционального вывода является работа Кука и Рекхау 1979 года [CR79], в которой они формализовали систему пропозициональных доказательств, как полиномиально вычислимую функцию, область значений которой совпадает с множеством всех пропозициональных тавтологий. В этой работе Кук и Рекхау установили фундаментальную взаимосвязь между сложностью пропозиционального выводы и классами сложности вычислений: существование *полиномиальной системы доказательств* пропозициональных формул, в которой каждая истинная формула имеет доказательство, сложность которого не превосходит некоторого полинома $p(n)$ от длины формулы n, равносильно тому, что класс **NP** замкнут относительно дополнений, т.е. **NP** = **coNP**. Данная взаимосвязь послужила основой так называемой *программы Кука-Рекхау*: так как класс **P** замкнут относительно дополнений, то для того, чтобы отделить его от класса **NP**, достаточно доказать отсутствие полиномиальной системы доказательств для классических тавтологий. Этот подход связан с получением суперполиномиальных нижних оценок сложности вывода.

На сегодняшний день суперполиномиальные нижние оценки известны только для слабых систем пропозициональных доказательств [Urq95, Raz96, UF96, Pud98, BP98]. Первая из таких оценок была получена еще в конце 60-х годов Цейтиным [Tse68] для подсистем резолюции. Первым же значительным с точки зрения программы Кука-Рекхау результатом является суперполиномиальная нижняя оценка для резолюции, найденная в 1985 году Хэйкеном [Hak85]. Начиная с конца 90-х годов подобные оценки были получены и для многих других систем доказательств: системы Фреге ограниченной глубины [Ajt94, BIK$^+$92, BIP93, KPW95], исчисление полиномов [CEI96, Raz98], системы Nullstellensatz [BIK$^+$96], системы линейных уравнений [BPR97, Pud97]. Для всех этих систем были получены экспоненциальные нижние оценки на длину вывода для конкретных последовательностей тавтологий, представляющих собой естественную интерпретацию известных комбинаторных утверждений. Наиболее полный обзор последних результатов в этой области можно найти в [Seg07].

В то же время, для сильных систем доказательств, таких как системы Фреге и расширенные системы Фреге [Kra95a], известны лишь линейные нижние оценки для длины вывода и квадратичные нижние оценки для размера вывода [Bus95, BG98]. Вопрос о существовании суперполиномиальных нижних оценок для таких систем до сих пор остается открытым. В первую очередь это связано с тем, что все известные методы доказательства нижних оценок (мощностной принцип, метод подстано-

вок [Kra97a], интерполяционные теоремы [Kra97b], соотношения между длиной и шириной опровержений в методе резолюции [BSW01], псевдослучайные генераторы [ABR$^+$04, Kra01, Kra04] и др.), которые хорошо зарекомендовали себя для слабых систем доказательств, оказались непригодными для систем Фреге [KP98]. Например, принцип Дирихле, как и другие комбинаторные принципы, использующие мощностные соображения, не может иметь сложного доказательства в системах Фреге [Bus87], поэтому любые комбинаторные принципы, требующие суперполиномиальных доказательств, должны быть очень сложными [BBP95]. В некоторых случаях вопрос о существовании нижних оценок удалось свести к оценке числа раундов интерактивной игры, но получить при этом нетривиальные нижние оценки не удалось [PB95, Pud00, Kra15].

Важность изучения сложности пропозиционального вывода не ограничивается только применением в области сложности вычислений в качестве средства отделения классов сложности. Здесь можно отметить полезную взаимосвязь между длиной вывода в сильных системах пропозициональных доказательств, подобных системам Фреге и их расширениям, и выполнимостью формул в ограниченной арифметике [Kra95b]. Также понимание устройства оптимального пропозиционального вывода необходимо для создания эффективных SAT-решателей и систем автоматического доказательства теорем [PS10, Bus12].

Одна из неожиданных и вместе с тем удивительных взаимосвязей была обнаружена между сложностью доказательства теорем и сложность булевых схем. Известно, что системы Фреге не зависят от выбора аксиом и правил вывода. Все такие системы полиномиально эквивалентны [CR79]. Однако системы Фреге можно охарактеризовать по классам формул, участвующих в выводах. И в этом случае не все системы Фреге будут полиномиально эквивалентны друг другу. Например, системы формул в конъюнктивных нормальных формах вместе с методом резолюции являются системами Фреге над формулами глубины 2. Для таких систем Фреге доказана экспоненциальная нижняя оценка длины вывода [Hak85]. Рассмотрение стандартных классов булевых схем

$$\mathbf{AC} \subset \mathbf{AC}^0[p] \subset \mathbf{TC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{P}/\mathrm{poly}$$

привело к появлению соответствующей иерархии систем Фреге. В этой иерархии **AC**-системам Фреге соответствуют системы Фреге над формулами ограниченной глубины, $\mathbf{NC}^1$-системы Фреге — это обычные системы Фреге, а $\mathbf{P}/\mathrm{poly}$-системы Фреге — это расширенные системы Фреге и системы Фреге с подстановкой.

На сегодняшний день экспоненциальные нижние оценки сложности булевых схем для конкретных функций были получены только для класса $\mathbf{AC}^0[p]$ [Raz87, Smo87]. Для систем Фреге экспоненциальные нижние оценки сложности вывода найдены только для **AC**-систем Фреге [Ajt94, BIK$^+$92, BIP93, KPW95]. Все попытки применить метод Разборова и Смоленского для $\mathbf{AC}^0[p]$-схем к система Фреге до сих успехом не увенчались. Несмотря на это, среди специалистов по сложности доказательств сложилась твердая уверенность, что прогресс в получении нижних оценок сложности булевых схем послужит толчком к получению нижних оценок размера пропозициональных доказательств. Хотя данная связь между булевыми схемами и системами доказательств часто постулируется [BP98], формального обоснования она до сих пор так и не получила [BBC16]. В тоже время, данный подход послужил толчком к появлению новых, интересных и открытых до сих пор проблем [Pud08].

Список литературы

[Ajt94] *Ajtai M.* The complexity of the pigeonhole-principle // Combinatorica, vol. 14, no. 4, 1994, pp. 417–433.

[ABR$^+$04] *Alekhnovich M., Ben-Sasson E., Razborov A. A., and Wigderson A.* Pseudorandom generators in propositional proof complexity // SIAM Journal on Computing, vol. 34, no. 1, 2004, pp. 67–88.

[BIK$^+$92] *Beame P. W., Impagliazzo R., Krajíček J., Pitassi T., Pudlák P., and Woods A.* Exponential lower bounds for the pigeonhole principle // In Proc. 24th ACM Symposium on Theory of Computing, 1992, pp. 200–220.

[BIK$^+$96] *Beame P. W., Impagliazzo R., Krajíček J., Pitassi T., and Pudlák P.* Lower bounds on Hilbert's Nullstellensatz and propositional proofs // Proc. London Mathematical Society, vol. 73, no. 3, 1996, pp. 1–26.

[BIP93] *Beame P. W., Impagliazzo R., and Pitassi T.* Exponential lower bounds for the pigeonhole principle // Computational Complexity, vol. 3, no. 2, 1993, pp. 97–140.

[BP98] *Beame P., Pitassi T.* Propositional proof complexity: Past, present, and future // Bulletin of the European Association for Theoretical Computer Science, The Computational Complexity Column, vol. 65, 1998, pp. 66–89.

[BSW01] *Ben-Sasson E. and Wigderson A.* Short proofs are narrow — resolution made simple // Journal of the ACM, vol. 48, no. 2, 2001, pp. 149–169.

[BBC16] *Beyersdorff O., Bonacina I. and Chew L.* Lower Bounds: From Circuits to QBF Proof Systems // ITCS '16 Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, 2016, pp. 249–260.

[BG98] *Bonet M. L., Galesi N.* Linear Lower Bounds and Simulations in Frege Systems with Substitutions // CLS, Lecture Notes in Computer Science, Selected Papers of 11-th Computer Science Logic, vol. 1414, 1998, pp. 115–128.

[BPR97] *Bonet M. L., Pitassi T., and Raz R.* Lower bounds for cutting planes proofs with small coefficients // The Journal of Symbolic Logic, vol. 62, no. 3, 1997, pp. 708–728.

[BBP95] *Bonet M. L., Buss S. R., Pitassi T.* Are there hard examples for Frege systems // Feasible Mathematics II, 1995, pp. 30–56.

[Bus87] *Buss S. R.* The propositional pigeonhole principle has polynomial size Frege proofs // J. Symbolic Logic, vol. 52, 1987, pp. 916–927.

[Bus95] *Buss S. R.* Some remarks on lengths of propositional proofs // Archive for Mathematical Logic, vol. 34, no. 6, 1995, pp. 377–394.

[Bus12] *Buss S. R.* Towards NP–P via proof complexity and search // Annals of Pure and Applied Logic, vol. 163, 2012, pp. 906—917.

[CEI96] *Clegg M., Edmonds J., and Impagliazzo R.* Using the Groebner basis algorithm to find proofs of unsatisfiability // In Proc. 28th ACM Symposium on Theory of Computing, 1996, pp. 174–183.

[Coo71] *Cook S. A.* The complexity of theorem-proving procedures // Proceedings of the third annual ACM symposium on Theory of computing, 1971, pp. 151–158.

[CR74] *Cook S. A., Reckhow R. A.* On the lengths of proofs in the propositional calculus // Proceedings of the sixth annual ACM symposium on Theory of computing, 1974, pp. 135–148.

[CR79] *Cook S. A., Reckhow R. A.* The relative efficiency of propositional proof systems // J. Symbolic Logic, vol. 44, 1979, pp. 36–50.

[Hak85] *Haken A.* The intractability of resolution // Theoretical Computer Science, v. 39, 1985, pp. 297–308.

[Kar72] *Karp R. M.* Reducibility among combinatorial problems // Complexity of Computer Computations, R.E. Miller and J.W. Thatcher, ed., New York (Plenum Press), 1972, pp. 85–103.

[Kra95a] *Krajíček J.* On Frege and Extended Frege Proof Systems // Feasible Mathematics II, Series "Progress in Computer Science and Applied Logic", vol. 13, 1995, pp. 284-319.

[Kra95b] *Krajíček J.* Bounded Arithmetic, Propositional Logic, and Complexity Theory // Vol. 60 of Encyclopedia of Mathematics and Its Applications, Cambridge University Press, Cambridge, 1995.

[Kra97a] *Krajíček J.* On methods for proving lower bounds in propositional logic // Logic and Scientific Methods: Proc. of the Tenth International Congress on Logic, Methodology and Philosophy of Science, vol. 259, 1997, pp. 69–83.

[Kra97b] *Krajíček J.* Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic // The Journal of Symbolic Logic, vol. 62, no. 2, 1997, pp. 457–486.

[Kra01] *Krajíček J.* Tautologies from pseudo-random generators // Bulletin of Symbolic Logic, vol. 7, no. 2, 2001, pp. 197–212.

[Kra04] *Krajíček J.* Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds // The Journal of Symbolic Logic, vol. 69, no. 1, 2004, pp. 265–286.

[Kra15] *Krajíček J.* A reduction of proof complexity to computational complexity for $AC^0[p]$ frege systems // Proceedings of the American Mathematical Society, vol. 143, no. 11, 2015, pp. 4951–4965.

[KP98] *Krajíček J., Pudlák P.* Some Consequences of Cryptoproof diagramical Conjectures for S^1_2 and EF // Information and Computation, vol. 140, issue 1, 1998, pp. 82–94.

[KPW95] *Krajíček J., Pudlák P., and Woods A.* Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle // Random Structures and Algorithms, vol. 7, no. 1, 1995, pp. 15–39.

[PS10] *Pitassi T. and Santhanam R.* Effectively polynomial simulations // In Proc. 1st Innovations in Computer Science, 2010.

[Pud97] *Pudlák P.* Lower bounds for resolution and cutting planes proofs and monotone computations // The Journal of Symbolic Logic, vol. 62, no. 3, 1997, pp. 981–998.

[Pud98] *Pudlák P.* The lengths of proofs // Chapter VIII in S. R. Buss (ed.): Handbook of Proof Theory, 1998, pp. 547–637.

[Pud00] *Pudlák P.* Proofs as Games // The American Mathematical Monthly, vol. 107, no. 6, 2000, pp. 541–550.

[Pud08] *Pudlák P.* Twelve Problems in Proof Complexity // Computer Science —- Theory and Applications, CSR 2008, Lecture Notes in Computer Science, vol 5010, 2008, pp. 13–27.

[PB95] *Pudlák P. and Buss S. R.* How to lie without being (easily) convicted and the lengths of proofs in propositional calculus // Computer Science Logic: 8th Workshop, CSL '94 Kazimierz, Poland, September 25–30, 1994 Selected Papers, 1995, pp. 151–162.

[Raz96] *Razborov A. A.* Lower bounds for propositional proofs and independence results in bounded arithmetic // Proceedings of the 23rd ICALP, Lecture Notes in Computer Science, vol. 1099, 1996, pp. 48–62.

[Raz87] *Razborov A. A.* Lower bounds for the size of circuits of bounded depth with basis $\{\&, \oplus\}$ // Math. Notes Acad. Sci. USSR, vol. 41, no. 4, 1987, pp. 333—338.

[Raz98] *Razborov A. A.* Lower bounds for the polynomial calculus // Computational Complexity, vol. 7, no. 4, 1998, pp. 291–324.

[Seg07] *Segerlind N.* The complexity of propositional proofs // The Bulletin of Symbolic Logic, vol. 13, no. 4, 2007, pp. 417–481.

[Smo87] *Smolensky R.* Algebraic methods in the theory of lower bounds for Boolean circuit complexity // In Proc. of 19th ACM STOC, 1987, pp. 77—82.

[Tse68] *Tseitin G. C.* On the complexity of derivations in propositional calculus // In A. O. Slisenko, editor, Studies in Mathematics and Mathematical Logic, Part II, 1968, pp. 115–125.

[Urq95] *Urquhart A.* The Complexity of Propositional Proofs // Bulletin of Symbolic Logic, vol. 1, 1995, pp. 425–467.

[UF96] *Urquhart A., Fu X.* Simplified lower bounds for propositional proofs // Notre Dame Journal of Formal Logic, vol. 73, no. 4, 1996, pp. 523–544.

From Boolean circuits to theorem proving

Bokov G. V.

The question how difficult it is to prove given theorems in given formal systems arises in many areas. In computational complexity, lower bounds to the size of proofs offer an approach towards the separation of complexity classes. Analysis of proof systems underlying recent SAT solvers provides the main theoretical framework towards understanding the power and limitations of solving. The main part of research in proof complexity has concentrated on proof systems for classical propositional logic. Despite the fact that propositional proof complexity has made enormous progress over the past three decades in showing tight lower and upper bounds for many proof systems, some of strong classical proof systems have resisted all attempts for lower bounds for decades. Nevertheless, a general and long-standing belief in the proof complexity community asserts that there is a close connection between progress in lower bounds for Boolean circuits and progress in proof size lower bounds for strong propositional proof systems. In the paper we show how relates Boolean circuits and proof systems with respect to complexity, i.e. how ideas and techniques from Boolean circuit complexity applies to propositional proof complexity.

Keywords: Propositional proof systems, proof complexity, Boolean circuits, circuit complexity, complexity classes.

От двузначной к k-значной логике

Жук Д.Н.

Традиционно считается, что при переходе от двузначного к многозначному случаю свойства решетки замкнутых классов функций координально меняются. В докладе будет показано, что несмотря на различия, эти решётки во многом похожи, а очень многие свойства, которые следуют из решетки Поста, могут быть обобщены на многозначный случай. Одним из таких примеров является решение задачи удовлетворения ограничениям для многозначного случая - показано, что самый общий полиномиальный алгоритм является во многом лишь комбинацией методов, давно известных для двузначного случая.

Ключевые слова: Булевы функции, k-значные функции, отношения, соответствие Галуа, задачи удовлетворения ограничениям.

1. Введение

Принято считать, что двузначный случай от k-значного отличается в первую очередь тем, что в двузначном случае все замкнутых классы функций описаны Э.Постом [28, 29], а в k-значном случае замкнутых классов континуум [3], а многочисленные результаты (например, [5, 17, 16, 8, 11, 22]) лишь подтверждают, что решётка замкнутых классов k-значной логики очень сложна.

Мы покажем, что несмотря на сложность, замкнутые классы функций k-значной логики во многом похожи на замкнутые классы двузначной логики, а многие свойства решетки Поста обобщаются на k-значный случай. Главным отличием является то, что k-значный случай одновременно может совмещать разные свойства, такие как монотонность и линейность, что невозможно в двузначном случае. Сначала мы покажем, как обобщаются на k-значный случай различные свойства и функции, являющиеся ключевыми при построении решетки Поста. Затем мы продемонстрируем, что полиноминальный алгоритм решения задачи удовле-

творения ограничениям по сути является комбинацией методов, известных для двузначного случая.

2. Функции двузначной и k-значной логики

Функциями двузначной логики P_2 называются отображения вида

$$\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\} \to \{0,1\}.$$

Положим $E_k = \{0, 1, \ldots, k-1\}$. *Функциями* k*-значной логики* P_2 называются отображения вида

$$E_k \times E_k \times \cdots \times E_k \to E_k.$$

Обычным образом на функциях k-значной логики определяется оператор замыкания относительно операций суперпозиции. Замкнутый класс функций называется *клоном*, если он содержит селекторы.

3. Предполные классы

Теорема 1. *[28, 29] В* P_2 *есть 5 предполных классов:*

- *Класс функций сохраняющих 0* (T_0)*;*
- *Класс функций сохраняющих 1* (T_1)*;*
- *Класс самодвойственных функций* (S)*;*
- *Класс монотонных функций* (M)*;*
- *Класс линейных функцйи* (L)*.*

Если перейти от двузначного случая к трехзначному, то там будут следующие предполные классы.

Теорема 2. *[4] В* P_3 *есть 18 предполных классов:*

1) *Классы сохранения множеств* $T_0, T_1, T_2, T_{0,1}, T_{0,2}, T_{1,2}$.
2) *Класс самодвойственных функций* S*, то есть, сохраняющие отношение* $\left(\begin{smallmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{smallmatrix}\right)$.
3) *Класс линейных функций.*

4) *Классы монотонных функций* $M_{0<1<2}, M_{1<0<2}, M_{0<2<1}$.

5) *Класс сохранения разбиения* $T_{0\sim1}, T_{0\sim2}, T_{1\sim2}$.

6) *Центральные предполные классы, то есть сохраняющие одно из отношений* $\left(\begin{smallmatrix}0&1&2&0&0&1&2\\0&1&2&1&2&0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1&2&1&1&0&2\\0&1&2&0&2&1&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1&2&2&2&0&1\\0&1&2&0&1&2&2\end{smallmatrix}\right)$.

7) *Предполный класс Слупецкого: множество всех несущественных функций.*

Их этих теорем видно, что предполные классы P_3 отличаются от предполных классов P_3 только классами сохранения разбиений, центральными предполными классами и предполным классом Слупецкого. При этом классы сохранения разбиений являются всего лишь способом сведения к двузначному случаю, а центральные классы во многом похожи на классы монотонных функций: сравните $\left(\begin{smallmatrix}0&1&2&0&0&1&2\\0&1&2&1&2&0&0\end{smallmatrix}\right)$ и $\left(\begin{smallmatrix}0&1&2&0&0&1\\0&1&2&1&2&2\end{smallmatrix}\right)$. Таким образом принципиально новым является только предполный класс Слупецкого, и в дальнейшем мы покажем, что именно этот класс является главной отличительной особенностью P_k.

Если же перейти от трехзначного случая к k-значному , то никаких новых семейств предполных классов не появится, но существенно усложнится семейство предполных классов типа Слупецкого [30, 22].

4. Решетка замкнутых классов

Как было отмечено выше, все замкнутые классы двузначной логики были описаны Э.Постом [28, 29], причём решетку по вложению можно красиво изобразить на плоскости (рис. 1).

В то же время, для $k > 2$ имеется континуум предполных классов.

Теорема 3. *[3] уществует континуум замкнутых классов функций k-значной логики для $k > 2$.*

Тем не менее, вопреки сложившемуся мнению, континуальная мощность не является критичным моментом, что подтверждается работой автора [7, 35], в которой он построил все замкнутые классы самодвойственных функций трехзначной логики (континуальное семейство).

Если сравнить рисунки 1 и 2, то станет понятно, что между этими решётками много общего. Детальное же изучение [7, 35] покажет, что многие классы в решетке замкнутых классов самодвойственных функций являются обобщениями замкнутых классов, найденных Э.Постом в [28, 29].

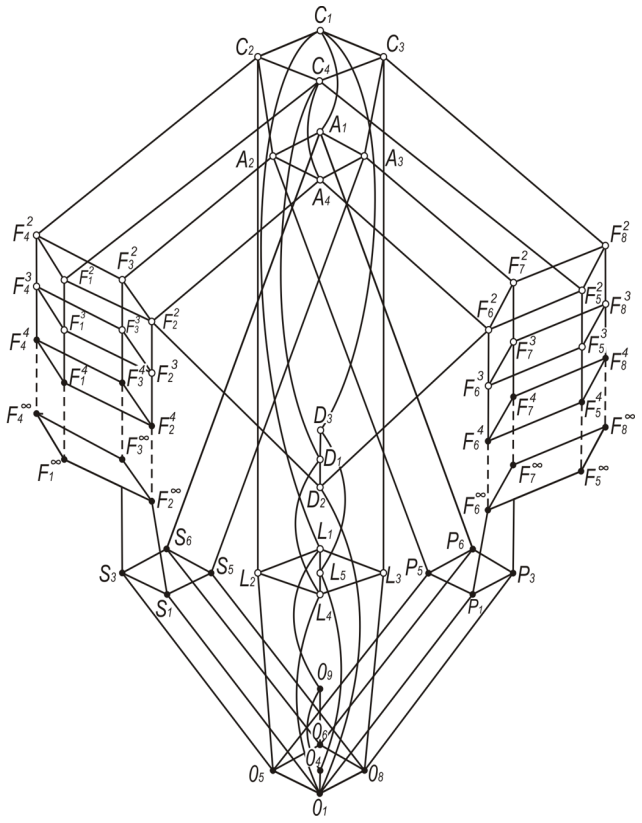

Рис. 1. Решетка Поста замкнутых классов P_2.

5. Соответствие Галуа

В этом разделе мы сформулируем, пожалуй, самое удивительное свойство замкнутых классов функций k-значной логики, которое является общим для двузначного и k-значного случая. Отображение $E_k^h \to \{0,1\}$ называется предикатом арности h. В работе мы не различаем предикаты и отношения, то есть вместо $\rho(a_1,\ldots,a_h)=1$ мы пишем $(a_1,\ldots,a_h)\in\rho$. Предикаты (отношения) мы изображаем в виде матриц, где столбцам соответствуют наборы, на которых предикат принимает значение 1.

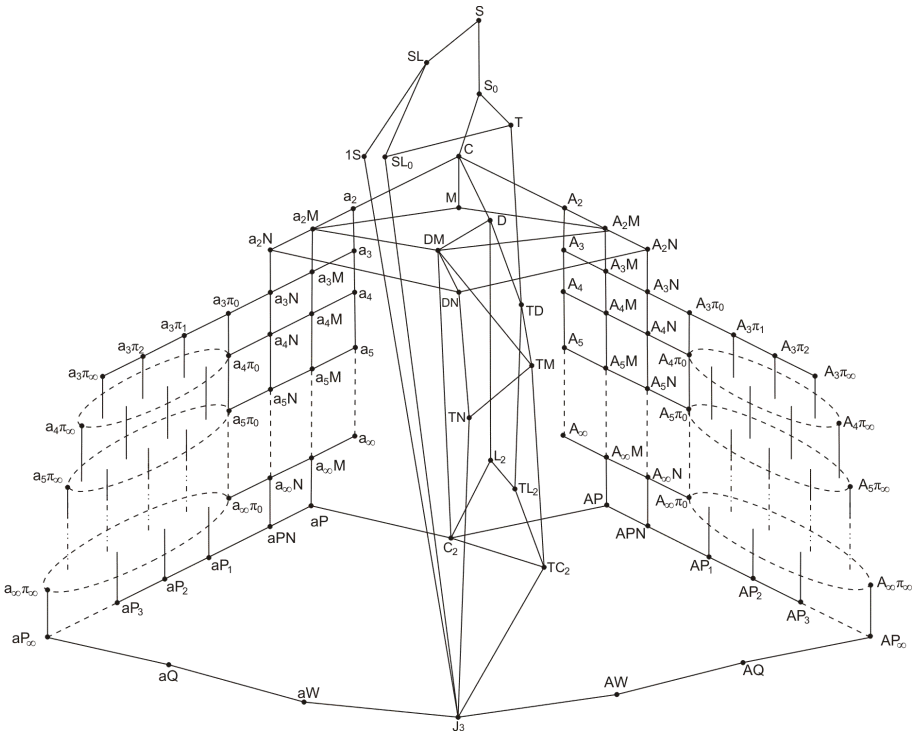

Рис. 2. Решетка замкнутых классов самодвойственных функций P_3.

Будем говорить, что функция $f \in P_k^m$ *сохраняет предикат (отношение)* ρ, если

$$f\begin{pmatrix} a_{1,1} & a_{2,1} & \dots & a_{m,1} \\ a_{1,2} & a_{2,2} & \dots & a_{m,2} \\ \dots & \dots & \dots & \dots \\ a_{1,h} & a_{2,h} & \dots & a_{m,h} \end{pmatrix} := \begin{pmatrix} f(a_{1,1}, a_{2,1}, \dots, a_{m,1}) \\ f(a_{1,2}, a_{2,2}, \dots, a_{m,2}) \\ \dots \\ f(a_{1,h}, a_{2,h}, \dots, a_{m,h}) \end{pmatrix} \in \rho$$

для любых

$$\begin{pmatrix} a_{1,1} \\ a_{1,2} \\ \dots \\ a_{1,h} \end{pmatrix}, \begin{pmatrix} a_{2,1} \\ a_{2,2} \\ \dots \\ a_{2,h} \end{pmatrix}, \dots, \begin{pmatrix} a_{m,1} \\ a_{m,2} \\ \dots \\ a_{m,h} \end{pmatrix} \in \rho.$$

Через $Pol(\rho)$ обозначим множество всех функций $f \in P_k$, таких что f сохраняет ρ. Для множества предикатов S положим

$$Pol(S) = \bigcap_{\rho \in S} Pol(\rho).$$

Множество всех предикатов, которые сохраняются функцией $f \in P_k$, будем обозначать через $Inv(f)$. Для $M \subseteq P_k$ положим

$$Inv(M) = \bigcap_{f \in M} Inv(f).$$

Введем на множестве всех предикатов k-значной логики R_k оператор замыкания относительно позитивных примитивных формул, то есть формул следующего вида

$$\rho(x_1, \ldots, x_n) = \exists y_1 \ldots \exists y_l \; \rho_1(z_{1,1}, \ldots, z_{1,n_1}) \wedge \ldots \wedge \rho_s(z_{s,1}, \ldots, z_{s,n_s}),$$

где $z_{i,j} \in \{x_1, \ldots, x_n, y_1, \ldots, y_l\}$.

Следующая теорема из [1, 2, 22] описывает важное свойство операций Pol и Inv.

Теорема 4. *Пусть $\mathbb{L}(P_k)$ — множество всех клонов в P_k, $\mathbb{L}(R_k)$ — множество всех замкнутых множеств в R_k, содержащих пустой предикат и предикат равенства, тогда отображения*

$$Inv : \mathbb{L}(P_k) \longrightarrow \mathbb{L}(R_k),$$

$$Pol : \mathbb{L}(R_k) \longrightarrow \mathbb{L}(P_k)$$

являются биективными отображениями, которые сохраняют частичный порядок $\subseteq$, то есть

$$\forall A, B \in \mathbb{L}(P_k) : A \subseteq B \Rightarrow Inv(B) \subseteq Inv(A),$$

$$\forall S, T \in \mathbb{L}(R_k) : S \subseteq T \Rightarrow Pol(T) \subseteq Pol(S).$$

Из этой теоремы следует, что для исследования решетки замкнутых классов P_k можно изучать решетку замкнутых классов предикатов k-значной логики.

6. Критичные предикаты

Наблюдение. Рассмотрим предикат двузначной логики $\rho(x, y, z) = (x \leq y) \wedge (y \neq z)$. Нетрудно видеть, что с помощью позитивных примитивных формул из него можно вывести два предиката ρ_1 и ρ_2 следующим образом: $\rho_1(x, y) = \exists z\ (\rho(x, y, z)) = (x \leq y)$, $\rho_2(y, z) = \exists x\ (\rho(x, y, z)) = (y \neq z)$. В то же время, из ρ_1 и ρ_2 можно обратно вывести ρ следующим образом $\rho(x, y, z) = \rho_1(x, y) \wedge \rho_2(y, z)$. Это позволяет утверждать, что предикат ρ не нужен нам для исследования замкнутых классов функций, а сам предикат ρ распадается на два более простых предиката.

Предикат называется *существенным*, если он представляется в виде конъюнкции предикатов меньшей арности. Это понятие было введено в работах [6, 7, 33] и позволило не только получить простое доказательство решетки Поста замкнутых классов, но и описать все замкнутые классы самодвойственных функций трехзначной логики [7, 35].

Можно пойти дальше и ввести понятие критичного (максимального) предиката [7, 35, 18]. А именно, предикат называется *критичным*, если его нельзя разложить на предикаты меньшей арности и большие (по числу наборов) предикаты той же арности, то есть его нельзя представить в виде конъюнкции предикатов меньшей арности и больших предикатов той же арности, которые из него выводятся.

Нетрудно убедиться, что имеют место следующие утверждения.

Лемма 1. *[7, 35, 18, 36] Каждый предикат представляется в виде конъюнкции критичных предикатов, которые из него выводятся.*

Лемма 2. *[7, 35, 18, 36] Любой клон может быть задан как класс сохранения критичных предикатов.*

В работе [36] было обнаружено следующее удивительное свойство критичных предикатов двузнайной логики.

Теорема 5. *[36] Пусть ρ — критичный предикат двузначной логики. Тогда $\rho(x_1, \ldots, x_n) = L_1 \vee L_2 \vee \ldots \vee L_m$ для каких-то линейных уравнений $L_1, L_2, \ldots, L_m$.*

В качестве примеров критичных предикатов можно привести следующие предикаты, которые задают предполный класс монотонных функций, предполный класс линейных функций и счётную цепочку замкнутых классов, соответственно.

- $(x \leq y) = (x = 0) \vee (y = 1)$;

- $(x \neq y) = (x + y = 1)$;
- предикат $\{0,1\}^n \setminus \{0\}^n$ определяется как $(x_1 = 1) \vee (x_2 = 1) \vee \cdots \vee (x_n = 1)$.

При $k > 2$ такого описания получить не удалось. Более того, усилиями Станислава Моисеева на компьютере был найден следующий критичный предикат в P_3:

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

Попытки придумать красивое описание не увенчались успехом, но было обнаружено, что этот предикат сохраняется только селекторами. Чтобы избежать рассмотрения таких случаев мы определим идемпотентную слабую функцию почти единогласия.

Функция f называется *идемпотентной*, если она сохраняет все константы, то есть $f(x, x, \ldots, x) = x$. Функция f называется *слабой функцией почти единогласия*, если она удовлетворяет следующему условию:

$$f(x, \ldots, x, y) = f(x, \ldots, x, y, x) = \cdots = f(y, x, \ldots, x).$$

В качестве примеров идемпотентной слабой функции почти единогласия можно привести.

- $x \vee y$, $x \wedge y$, $\max(x, y)$
- $x + y + z$
- $xy \vee xz \vee yz$

Нетрудно видеть, что идемпотентная слабая функция почти единогласия не принадлежит ни одному предполному классу типа Слупецкого [36]. Более того, в работе [25] было показано, что это самая слабая функция, которая гарантирует, что на любом подмножестве и факторможестве есть функции отличные от селекторов, что делает рассмотрение этой функции более чем оправданным.

Оказалось, что при наличии идемпотентной слабой функции почти единогласия можно доказать результат, очень похожий на описание критичных предикатов двузначной логики.

Теорема 6. *[36] Пусть ρ – критичный предикат k-значной логики, сохраняемый идемпотентной слабой функцией почти единогласия. Тогда найдутся $A_1, \ldots, A_n \subseteq E_k$, такие что $(A_1 \times A_2 \times \cdots \times A_n) \cap \rho$ представляется в виде дизъюнкции линейных уравнений, причём только одно из них может содержать более одной переменной.*

7. Функция голосования

Одной из самых популярных функций двузначной логики, возникающей во многих задачах, является функция голосования, которая естественным образом обобщается на k-значный случай.

Функция $f \in P_k$ называется *функцией голосования*, если

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x.$$

Легко видеть, что в P_2 есть только одна функция голосования, хотя, например, в P_3 их 3^6.

Важным свойством функции голосования является следующее утверждение

Лемма 3. *[9] Любой замкнутый класс в P_k, содержащий функцию голосования, задаётся предикатами арности 1 и 2.*

Есть много других свойств функций голосования, которые легко переносятся с двузначного случая на k-значный (см. например [20, 19]).

В частности, Станиславу Моисееву удалось найти все 1 918 040 замкнутых классов трехзначной логики, содержащих функцию голосования [38]. Например, на рисунках 3 и 4 вы можете сравнить решетки замкнутых классов P_2 и P_3, содержащие функцию голосования (во втором случае на рисунок влезла только верхняя часть). Получается, что решетка в P_3 просто намного больше, но не принципиально другая.

8. Функция почти единогласия

В этом разделе мы рассмотрим функции, которые делают решетку Поста счётной. Пусть функция $f_n \in P_2$ от n переменных принимает значение 1 только тогда, когда среди значений переменных более одной единицы. Известно, что функции $f_3, f_4, f_5, \ldots$ порождают попарно различные замкнутые классы. Такие функции легко обобщаются на k-значный случай.

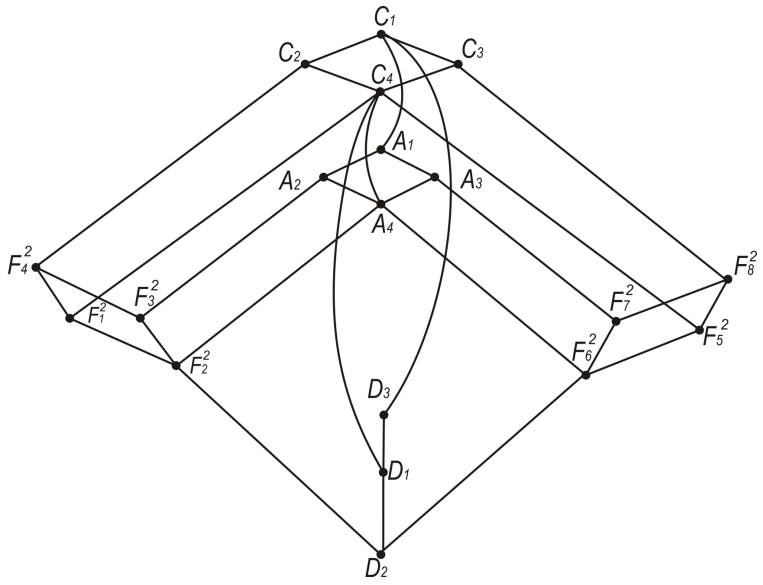

Рис. 3. Решетка замкнутых классов P_2, содержащих функцию голосования.

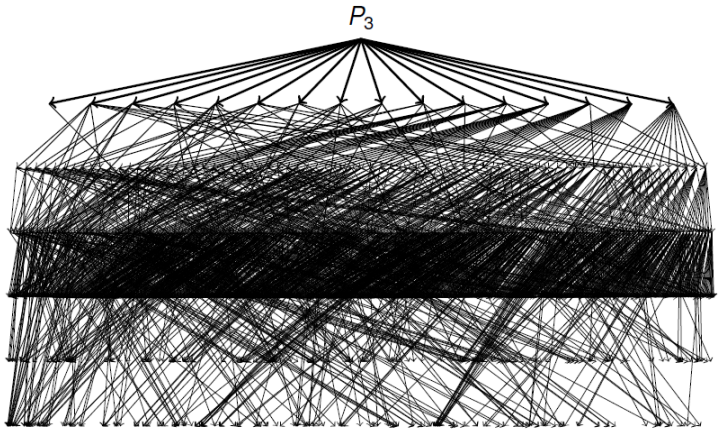

Рис. 4. Верхние слои решетки замкнутых классов P_3, содержащих функцию голосования.

Функция f называется *функцией почти единогласия*, если

$$f(x,\dots,x,y) = f(x,\dots,x,y,x) = f(y,x,\dots,x) = x.$$

Для функции почти единогласия можно доказать утверждение, аналогичное утверждению для функции почти единогласия.

Лемма 4. *[9] Любой замкнутый класс, содержащий функцию почти единогласия от n переменных, задаётся предикатами арности* $n-1$.

Функции почти единогласия активно изучались при исследовании многозначных логик, а также в универсальной алгебре [27, 26, 15, 10, 38, 21]. При этом надо понимать, что в k значном случае ситуация намного сложнее и изначально не было даже понятно, можно ли алгоритмически проверить существование функции почти единогласия в замкнутом классе [23, 24, 34]. Тем не менее, сейчас они уже достаточно хорошо изучены и мы можем доказывать утверждения, аналогичные тем, что есть в двухзначном случае. Например, верна следующая теорема.

Теорема 7. *Пусть множество функций* $F \subseteq P_k$ *от* m *переменных сохраняет все константы, а замыкание* $[F]$ *содержит функцию почти единогласия. Тогда* $[F]$ *содержит функцию почти единогласия от* $(m-1)k(k-1)/2+1$ *переменных. Оценка не может быть улучшена.*

Отметим также, что в книге [22] исследование замкнутых классов, содержащих функцию почти единогласия, приводится в качестве одной из стратегий к изучению k-значной логики.

9. Минимальные клоны

Замкнутый класс называется *минимальным клоном*, если любая его функция, отличная от селектора, порождает вместе с селекторами весь класс.

Все минимальные клоны двузначной логики могут быть получены из решётки Поста, а минимальные клоны в P_3 и P_4 найдены на компьютере.

- В P_2 всего 7 минимальных клонов: $[\{x \vee y\}]$, $[\{x \wedge y\}]$, $[\{xy \vee xz \vee yx\}]$, $[\{x+y+z\}]$, $[\{\overline{x}\}]$, $[\{x,0\}]$, $[\{x,1\}]$ [28, 29].
- В P_3 всего 84 минимальных клона (24 с точностью до внутреннего автоморфизма) (B. Csákány, 1983, [14]).
- В P_4 всего 5242 минимальных клона (Karsten Schölzel, 2012).

Найти аналогичным образом все минимальные клоны в P_5 не представляется возможным из-за слишком большого количества вариантов. Тем не менее ещё в 1983 году была получена классификация всех минимальных клонов [31].

Теорема 8. *[31] В P_k есть только 5 типов минимальных клонов:*

1) *порождённые унарной функцией,*

2) *порождённые бинарной идемпотентной функцией,*

3) *порождённые функцией голосования,*

4) *порождённые функцией минорирования ($f(x,x,y) = f(x,y,x) = f(y,x,x) = y$),*

5) *порождённые полуселекотором(semiprojection), то есть, на всех неразнозначных наборах возвращается одна переменная.*

Таким образом, единственным принципиальным отличием двузначного случая от k-значного являются полуселекторы, то есть функции, которые на любом двух элементном множестве превращаются в обычные селекторы.

10. Минимальные существенные функции

Функция называется *существенной* если она принимает все k значений и зависит существенно по крайней мере от двух переменных.

Легко убедиться, что выполняется следующая лемма.

Лемма 5. *Любой замкнутый класс P_2, содержащий существенную функцию, содержит одну из следующих функций: $x \vee y$, $x \wedge y$, $xy \vee xz \vee yz$ или $x + y + z$.*

В этом разделе обобщим этот результат на k-значный случай.

Мы говорим, что B *поглощает* A с помощью функции f если $f(B, \dots, B, A, B, \dots, B) \subseteq B$ для любой позиции A.

Ниже мы приводим некоторые примеры поглощающих множеств.

- $\{0\}$ поглощает $\{0,1\}$ с помощью $x \wedge y$.
- $\{1\}$ поглощает $\{0,1\}$ с помощью $x \vee y$.

- $\{0\}$ и $\{1\}$ поглощают $\{0,1\}$ с помощью функции голосования.

Множество функций называется *полиномиально полным*, если вместе с константами оно порождает всё P_k.

Теорема 9. *Пусть замкнутый класс $F \subseteq P_k$ содержит идемпотентную слабую функцию почти единогласия. Тогда он содержит одну из следующих функций*

1) *$f(x,y)$, такую что B поглощает E_k с помощью функции f;*

2) *$f(x,y,z)$, такую что B поглощает E_k с помощью функции f;*

3) *$f(x_1,\ldots,x_n)$, такую что $f/\sigma \cong x_1 + x_2 + \cdots + x_n (\mod p)$ для некоторого отношения эквивалентности σ на E_k;*

либо F/σ полиномиально полно для некоторого отношения эквивалентности σ на E_k.

Можно ещё упростить это утверждение, если рассмотреть только монотонные функции k-значной логики.

Легко убедиться, что выполняется следующая лемма.

Лемма 6. *Любой замкнутый класс монотонных функций в P_2, содержащий существенную функцию, содержит $x \vee y$, $x \wedge y$ или $xy \vee xz \vee yz$.*

Этот результат может быть обобщён на k-значный случай следующим образом.

Теорема 10. *Пусть замкнутый класс монотонных функций в P_k содержит идемпотентную слабую функцию почти единогласия. Тогда он содержит одну из следующих функций*

1) *$f(x,y)$, такую что $\{0,\ldots,m\}$ поглощает E_k с помощью f;*

2) *$f(x,y)$, такую что $\{m,\ldots,k-1\}$ поглощает E_k с помощью f;*

3) *$f(x,y,z)$, такую что $\{0\}$ и $\{k-1\}$ поглощают E_k с помощью f.*

11. Задача удовлетворения ограничениям

Пусть Γ – множество допустимых предикатов k-значной логики. Тогда для каждого Γ мы определяем массовую проблему.

Проблема 1. CSP(Γ).

Дано: конъюнкция предикатов, то есть формула вида

$$\rho_1(x_{i_{1,1}}, \ldots, x_{i_{1,n_1}}) \wedge \cdots \wedge \rho_s(x_{i_{s,1}}, \ldots, x_{i_{s,n_s}}),$$

где $\rho_1, \ldots, \rho_s \in \Gamma$.

Проверить выполнима ли формула.

Пример. Пусть $k = 3, \Gamma = \{x < y, x \leq y\}$. Примеры задач:

- $x_1 < x_2 \wedge x_2 < x_3 \wedge x_3 < x_4$, не имеет решений;
- $x_1 \leq x_2 \wedge x_2 \leq x_3 \wedge x_3 \leq x_1$, есть, например, решение $x_1 = x_2 = x_3 = 0$.

Для $k = 2$ полная классификация сложности задачи CSP(Γ) была получена в 1978 году [32].

Теорема 11. *[32] Пусть* Γ *— множество предикатов двузначной логики. Тогда* CSP(Γ) *решается за полиномиальное время если*

1) 0 *сохраняет* Γ*,*

2) 1 *сохраняет* Γ*,*

3) $x \vee y$ *сохраняет* Γ*,*

4) $x \wedge y$ *сохраняет* Γ*,*

5) $xy \vee yz \vee xz$ *сохраняет* Γ*,*

6) $x + y + z$ *сохраняет* Γ*.*

иначе CSP(Γ) *NP-полна.*

В дальнейшем была получена классификация для трехзначного случая [12], а в 2017 году и для k-значного [13, 37].

Теорема 12. *[13, 37] Пусть* Γ *— множество предикатов* k*-значной логики. Если есть слабая функция почти единогласия, которая сохраняет* Γ*, то* CSP(Γ) *решается за полиномиальное время; иначе* CSP(Γ) *NP-полна.*

При этом алгоритм, приведенный в [37], является во многом комбинацией методов, которые решают задачу в двузначном случае, а главное отличие заключается в том, что здесь разные пункты Теоремы 11 могут переплетаться в одной задаче.

Алгоритм для произвольного k из [37].

1) Применяем метод резолюций к бинарным проекциям всех предикатов.

2) Пытаемся разбить область значений каждой переменной на две части и решить две более простые задачи.

3) Если B поглощает область значений какой-то переменной с помощью бинарной или тернарной функции, то уменьшаем область значений до B.

4) Если существует отношение эквивалентности σ, такое что $\mathrm{Pol}(\Gamma)$ полиномиально полно, то уменьшаем область значений переменной до любого класса эквивалентности σ.

5) Иначе существуют отношения эквивалентности $\sigma_1, \ldots, \sigma_n$ такие что задача по модулю этих отношений является системой линейных уравнений в поле.

   - Решаем систему линейных уравнений в поле.
   - Для любого конкретного решения системы линейных уравнений мы можем проверить, что существует соответствующее решение исходной задачи следующим образом: ограничиваем область значений каждой переменной на решение системы и сводим задачу к задаче удовлетворения ограничений на меньшем множестве, то есть более простой.
   - Применяя предыдущий шаг, методом неопределенных коэффициентов вычисляем линейное уравнение, которое может быть добавлено к исходной задаче, чтобы множество решений не поменялось.
   - Добавляем найденное линейное уравнение к системе и повторяем процедуру.

12. Массовые проблемы

Таким образом, получается, что очень многие результаты, полученные для k-значного случая, являются лишь обобщением результатов, известных для двузначного. Поэтому остаётся открытым вопрос: есть ли какое-то принципиальное отличие между P_2 и P_k, или все отличие заключается в том, что P_k намного больше, а иногда настолько большое, что полноценное описание невозможно куда-либо записать. Чтобы ответить на этот вопрос, мы рассмотрим следующие массовые проблемы.

Проблема 2. *Дан предикат; проверить что заданный им замкнутый класс конечно порождён.*

Проблема 3. *Дано конечное множество функций; проверить что порожденный ими замкнутый класс предикатно-описуем.*

Проблема 4. *Дан предикат и конечное множество функций; проверить, что они задают один и тот же класс.*

Каждая из этих задача легко решается как для P_2, так и для других случаев, когда нам известна решетка всех замкнутых классов, даже если она континуальной мощности [7, 35]. Но разрешимы ли эти задачи в P_k? Или описания всех замкнутых классов P_k, даже необозримого для человека, не существует в принципе, так как хорошее описание должно позволять решать перечисленные задачи.

В 2017 году Мэтью Мур объявил, что Проблема 3 алгоритмически неразрешима, но пока так и не опубликовал доказательство. Если в итоге оно будет опубликовано, то это, на наш взгляд, станет первым принципиальным отличием P_2 от P_k.

Список литературы

[1] В. Г. Бондарчук, В. Г. Калужнин, В. Н. Котов, Б. А. Ромов. Теория Галуа для алгебр Поста I. *Кибернетика*, (3):1–10, 1969.

[2] В. Г. Бондарчук, В. Г. Калужнин, В. Н. Котов, Б. А. Ромов. Теория Галуа для алгебр Поста II. *Кибернетика*, (5):1–9, 1969.

[3] Ю. И. Янов, А. А. Мучник. О существовании k-значных замкнутых классов, не имеющих конечного базиса. *ДАН СССР*, 127(1):44–46, 1959.

[4] С. В. Яблонский. О функциональной полноте в трехзначном исчислении. *ДАН СССР*, 95(6):1152–1156, 1954.

[5] С. В. Яблонский. Функциональные построения в k-значной логике. *Труды математического института имени ВА Стеклова*, 51(0):5–142, 1958.

[6] Д. Н. Жук. Предикатный метод построения решетки Поста. *Дискретная математика*, 23(2):115–128, 2011.

[7] Д. Н. Жук. *Решетка замкнутых классов самодвойственных функций трехзначной логики*. Издательство МГУ, 2011.

[8] С. С. Марченков. О замкнутых классах самодвойственных функций многозначной логики. *Проблемы кибернетики*, 40:261–266, 1983.

[9] K. A. Baker, F. Pixley. Polynomial interpolation and the Chinese Remainder Theorem for algebraic systems. *Math. Zeitschrift*, 143:165–174, 1975.

[10] L. Barto. Finitely related algebras in congruence distributive varieties have near unanimity terms. *Canadian Journal of Mathematics*, 65(1):3–21, 2013.

[11] A. A. Bulatov. Finite sublattices in the lattice of clones. *Algebra and Logic*, 33(5):287–306, 1994.

[12] Andrei A. Bulatov. A dichotomy theorem for constraint satisfaction problems on a 3-element set. *J. ACM*, 53(1):66–120, January 2006.

[13] Andrei A. Bulatov. A dichotomy theorem for nonuniform csps. *CoRR*, abs/1703.03021, 2017.

[14] B. Csákány. All minimal clones on the three-element set. *Acta cybernetica*, 6:227–238, 1984.

[15] B. A. Davey, L. Heindorf, R. McKenzie. Near unanimity: an obstacle to general duality theory. *Algebra Universalis*, 33(3):428–439, 1995.

[16] J. Demetrovics, L. Hannak. The number of reducts of preprimial algebra. *Algebra Universalis*, 16(1):178–185, 1983.

[17] L. A. Kaluznin, R. Pöschel. Funktionen-und relationenalgebren. *VEB Deutscher Verlag der Wissenschaften, Berlin*, 19:79, 1979.

[18] K. A. Kearnes, Á. Szendrei. Clones of algebras with parallelogram terms. *Internat. J. Algebra Comput.*, 22, 2012.

[19] S. Kerkhoff. On the minimal majority operations on a three-element set. *Multiple-Valued Logic and Soft Computing*, 25(4-5):511–527, 2015.

[20] S. Kerkhoff, D. Zhuk. The generation of clones with majority operations. *Algebra universalis*, 72(1):71–80, 2014.

[21] Benoit Larose, Cynthia Loten, László Zádori. A polynomial-time algorithm for near-unanimity graphs. *Journal of Algorithms*, 55(2):177–191, 2005.

[22] D. Lau. *Function algebras on finite sets.* Springer, 2006.

[23] M. Maróti. On the (un) decidability of a near-unanimity term. *Algebra universalis*, 57(2):215–237, 2007.

[24] M. Maróti. The existence of a near-unanimity term in a finite algebra is decidable. *The Journal of Symbolic Logic*, 74(3):1001–1014, 2009.

[25] M. Maróti, R. Mckenzie. Existence theorems for weakly symmetric operations. *Algebra universalis*, 59(3–4):463–489, 2008.

[26] M. Maroti, L. Zadori. Reflexive digraphs with near unanimity polymorphisms. *Discrete Mathematics*, 312(15):2316 – 2328, 2012.

[27] A. Mitschke. Near unanimity identities and congruence distributivity in equational classes. *Algebra universalis*, 8(1):29–32, 1978.

[28] E. L. Post. Determination of all closed systems of truth tables. *Bull. Amer. Math. Soc.*, (26: 427), 1920.

[29] E. L. Post. *Two-Valued Iterative Systems of Mathematical Logic.* Princeton Univ. Press, Princeton, 1941.

[30] I. Rosenberg. über die funktionale vollständigkeit in den mehrwertigen logiken. *Rozpravy Československe Akad. Věd., Ser. Math. Nat. Sci.*, 80:3–93, 1970.

[31] I. Rosenberg. Minimal clones i: the five types. In *Lectures in universal algebra*, pages 405–427. Elsevier, 1986.

[32] T. J. Schaefer. The complexity of satisfiability problems. In *Proceedings of the Tenth Annual ACM Symposium on Theory of Computing*, STOC '78, pages 216–226, New York, NY, USA, 1978. ACM.

[33] D. Zhuk. The cardinality of the set of all clones containing a given minimal clone on three elements. *Algebra Universalis*, 68(3–4):295–320, 2012.

[34] D. Zhuk. The existence of a near-unanimity function is decidable. *Algebra Universalis*, 71(1):31–54, 2014.

[35] D. Zhuk. The lattice of all clones of self-dual functions in three-valued logic. *Journal of Multiple-Valued Logic and Soft Computing*, 24(1–4):251–316, 2015.

[36] D. Zhuk. Key (critical) relations preserved by a weak near-unanimity function. *Algebra Universalis*, 77(2):191–235, 2017.

[37] D. Zhuk. The proof of csp dichotomy conjecture. *CoRR*, abs/1704.01914, 2017.

[38] D. Zhuk, S. Moiseev. On the clones containing a near-unanimity function. In *43rd IEEE International Symposium on Multiple-Valued Logic (ISMVL 2013)*, pages 129–134, May 2013.

From two-valued logic to k-valued logic.
Zhuk D.N.

Traditionally, it is believed that the lattices of clones in two-valued logic and k-valued logic are totally different. In the paper we show that despite the differences they have a lot in common, and many properties that follow from the Post lattice can be generalized to the multi-valued case. As an example we show that the most general polynomial algorithm for the constraint satisfaction problem on k-element set can be viewed as a combination of methods known for two-valued case.

Keywords: Boolean functions, k-valued functions, relations, Galois connection, constraint satisfaction problem.

Об обобщении теоремы Мура

Пантелеев П.А.

Диагностические эксперименты с конечными автоматами впервые были описаны в классической работе Э. Мура, и с тех пор применяются для тестирования цифровых схем и коммуникационных протоколов. Одна из основных задач тестирования конечных автоматов состоит в определении начального состояния наблюдаемого автомата. Пусть имеется полное описание некоторого конечного автомата Мили, но про его начальное состояние известно лишь то, что оно принадлежит некоторому фиксированному подмножеству состояний. Тогда диагностическая задача состоит в нахождении начального состояния путем последовательной подачи входных символов на автомат. В данном докладе будет рассказано об оценках длины для таких последовательностей входных символов и показана связь данной задачи с комбинаторными проблемами, возникающими в теории гиперграфов.

Ключевые слова: конечный автомат, условный диагностический эксперимент, теорема Мура, гиперграф.

Диагностические эксперименты с конечными автоматами впервые были описаны в классической работе Э. Мура [1], и с тех пор нашли многочисленные применения при решении практических и теоретических задач, возникающих в таких областях как тестирование программ, диагностика неисправностей цифровых схем, а также при верификации коммуникационных протоколов [2]. В настоящей работе изучается длина простого условного диагностического эксперимента, который решает следующую задачу. Допустим, у нас есть полное описание некоторого конечного автомата Мили $\mathfrak{A}$ (например, задана его диаграмма или таблица переходов и выходов), но про его начальное состояние известно лишь то, что оно принадлежит некоторому фиксированному подмножеству состояний Q'. *Простой диагностический эксперимент для подмножества* Q' состоит в подаче на автомат $\mathfrak{A}$ такой входной последовательности, что по реакции автомата на нее можно однозначно сказать с каким начальным состоянием $q_0 \in Q'$ мы имели дело. Эксперимент называется *безусловным*, если каждая следующая входная буква, подаваемая на автомат,

не зависит от реакции автомата на уже поданные буквы. В противном случаем эксперимент называется *условным*. *Длиной* эксперимента будем назвать максимум из длин входных последовательностей, возникающих при его проведении с автоматом $\mathfrak{A}$ при всех возможных способах выбора начального состояния $q_0 \in Q'$.

Обозначим через $\ell(n,k)$ максимальную длину кратчайшего простого условного диагностического эксперимента, где максимум берется по всем автоматам с n состояниями и их k-элементным подмножествам состояний, для которых такой эксперимент существует. Обозначим также через $\tilde{\ell}(n,k)$ соответствующую величину для безусловного эксперимента. В частном случае $k=2$ диагностический эксперимент, как условный так и безусловный, по существу совпадает с отличающим словом для двух состояний, и точное значение $\ell(n,2) = \tilde{\ell}(n,2) = n-1$ было получено в упомянутой выше работе Э. Мура [1]. В общем случае данная задача впервые рассматривалась А. Гилом [3] (см. также [4, Теорема 4.5]). Им была получена верхняя оценка $\ell(n,k) \leq (k-1)n^k$. Существенный прогресс был достигнут в работе М.Н. Соколовского [5], где были получены оценки

$$\binom{n-1}{k-1} \leq \ell(n,k) \leq \sum_{i=2}^{k} \binom{n}{i}, \tag{1}$$

а также $\ell(n,n) \asymp n^2$ при $n \to \infty$. Последняя оценка была уточнена И.К. Рысцовым в работе [6], где показано, что

$$\ell(n,n) = \frac{n(n-1)}{2}. \tag{2}$$

Отметим, что пример автомата с n состояниями на котором достигается оценка (2) был построен А.А. Карацубой [7] (см. также [8]). Интересно также отметить, что оценка (2) была переоткрыта в [9], где был также предложен эффективный алгоритм, проверяющий существование простого условного диагностического эксперимента для всех состояний автомата со сложностью $O(pn\log n)$, где p — число входных символов автомата.

Несмотря на полиномиальную сложность проверки существования условного эксперимента, аналогичная проблема для безусловного эксперимента является PSPACE-полной [10, 9]. Кроме того, полиномиальный алгоритм проверки существования простого условного диагностического эксперимента для подмножества состояний Q' известен только для случая когда Q' совпадает с множеством всех состояний Q. Если $Q' \neq Q$, то, как показано в [9], данная проблема также является PSPACE-полной.

В данной работе получены оценки величины $\ell(n,k)$, уточняющие оценки (1) в случае когда мощность подмножества состояний k для которых проводится диагностический эксперимент растет не слишком быстро с ростом числа состояний автомата n. В частности показано, что $\ell(n,k) \sim \frac{n^{k-1}}{(k-1)!}$ при $k = o(n)$ и $n \to \infty$. В случае $k = 3$ удалось получить точную оценку $\ell(n,3) = \tilde{\ell}(n,3) = \binom{n}{2}$. Заметим, что оценки (1) не дают даже порядка роста величины $\ell(n,k)$ в этих случаях.

Список литературы

[1] Мур Э. Ф. Умозрительные эксперименты с последовательностными машинами [пер. с англ.] // Автоматы / Под ред. К. Э. Шеннона, Дж. Маккарти. — ИЛ, 1956.

[2] Model-Based Testing of Reactive Systems: Advanced Lectures (Lecture Notes in Computer Science) / Manfred Broy, Bengt Jonsson, Joost-Pieter Katoen et al. — Secaucus, NJ, USA : Springer-Verlag New York, Inc., 2005. — ISBN: 3540262784.

[3] Gill A. State-identification experiments in finite automata // Inform. Control. — 1961. — Vol. 4, no. 2–3. — P. 132–154.

[4] Гилл А. Введение в теорию конечных автоматов. — М. : Наука, 1966. — 272 с.

[5] Соколовский М. Н. О диагностических экспериментах с автоматами // Кибернетика. — 1971. — Т. 6. — С. 44–49.

[6] Рысцов И. К. Доказательство достижимой оценки длины условного диагностического эксперимента для конечного автомата // Кибернетика. — 1977. — Т. 3. — С. 20–22.

[7] Карацуба А. А. Решение одной задачи из теории конечных автоматов // УМН. — 1960. — Т. 15, № 3. — С. 157–159.

[8] Хиббард Т. Точные верхние границы длин минимальных экспериментов, определяющих заключительное состояние, для двух классов последовательностных машин [пер. с англ.] // Кибернетический сборник. — 1966. — Т. 2. — С. 7–23.

[9] Lee D., Yannakakis M. Testing finite-state machines: state identification and verification // Computers, IEEE Transactions on. — 1994. — Mar. — Vol. 43, no. 3. — P. 306–320.

[10] Rystsov I. K. Polynomial complete problems in automata theory // Information Processing Letters. — 1983. — Vol. 16, no. 3. — P. 147–151.

A generalization of a Moore theorem

Panteleev P.A.

Distinguishing sequences for finite automata were first introduced in the classical paper of E. Moore and since that they have many applications in testing of sequential circuits and communication protocols. One of the basic tasks in the testing of finite automata is to identify the initial state of the automaton under investigation. Suppose we have a full description of a finite deterministic Mealy automaton and we know that its initial state is in some subset of its set of states. Then the state-identification problem is to find the initial state by a sequential application of input symbols to the automaton. In this talk we discuss the bounds on the length of such input sequences and show a relation of this problem to combinatorial problems in hypergraph theory.

Keywords: Finite automaton, adaptive distinguishing sequence, Moore theorem, hypergraph.

К сведению авторов публикаций в журнале «Интеллектуальные системы. Теория и приложения»

В соответствии с требованиями ВАК РФ к изданиям, входящим в перечень ведущих рецензируемых научных журналов и изданий, в которых могут быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук, статьи в журнал «Интеллектуальные системы. Теория и приложения» предоставляются авторами в следующей форме:

1. Статьи, набранные в пакете LaTeX, предоставляются к загрузке через WEB-форму http://intsysjournal.org/generator_form .
2. К статье прилагаются файлы, содержащие название статьи на русском и английском языках, аннотацию на русском и английском языках (не более 50 слов), список ключевых слов на русском и английском языках (не более 20 слов), информация об авторах: Ф.И.О. полностью, место работы, должность, ученая степень и/или звание (если имеется), контактные телефоны (с кодом города и страны), e-mail, почтовый адрес с индексом города (домашний или служебный).
3. Список литературы оформляется в едином формате, установленном системой Российского индекса научного цитирования.
4. За публикацию статей в журнале «Интеллектуальные системы. Теория и приложения» с авторов (в том числе аспирантов высших учебных заведений) статей, рекомендованных к публикации, плата не взимается. Оттиски статей авторам не предоставляются. Журнал распространяется по подписке, экземпляры журнала рассылаются подписчикам наложенным платежом. Условия подписки публикуются в каталоге НТИ «Роспечать», индекс журнала 64559.
5. Доступ к электронной версии последнего вышедшего номера осуществляется через НЭБ «Российский индекс научного цитирования». Номера, вышедшие ранее, размещаются на сайте http://intsysjournal.org, и доступ к ним бесплатный. Там же будут размещены аннотации всех публикуемых статей.

Подписано в печать: 20.03.2018
Дата выхода: 28.03.2018
Тираж: 200 зкз.
Цена свободная
Свидетельство о регистрации СМИ: ПИ № ФС77–58444 от 25 июня 2014 г., выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций(Роскомнадзор).