Московский Государственный Университет
имени М.В. Ломоносова
Российская Академия Наук
Международная Академия Технологических Наук
Российская Академия Естественных Наук

Интеллектуальные Системы.

Теория и приложения

ТОМ **28** ВЫПУСК 2 * **2024**

МОСКВА

УДК 519.95; 007:159.955 ISSN 2411–4448
ББК 32.81 Издаётся 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 имени М.В. Ломоносова, Научного Совета по комплексной проблеме «Кибернетика» РАН, Отделения «Математическое моделирование технологических процессов» МАТН.
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.

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

Адрес редакции: 119991, Москва, ГСП-1, Ленинские Горы, д. 1, 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. Общие проблемы теории интеллектуальных систем

Колдоба Е.В. Численное решение многопараметрического уравнения состояния Бенедикта-Вебба-Рубина 5

Часть 2. Специальные вопросы теории интеллектуальных систем

Фомченко А.В., Парфенов Д.В. Жадный алгоритм формирования решающих ансамблей 13

Носов М.В. Степени разделяющих многочленов для классов Поста 24

Часть 3. Математические модели

Калашников М.Э. Изучение базисов предполных классов линейных 2-адических автоматов 34

Родин С.Б. О свойстве аддитивного сдвига для линейной реализуемости автоматов 52

Часть 4. Семинары кафедры МаТИС

Доклады семинара «Теория автоматов» - 2023 год 68

Доклады семинара «Теория автоматов» - 2024 год 78

Часть 1
Общие проблемы теории интеллектуальных систем

Численное решение многопараметрического уравнения состояния Бенедикта-Вебба-Рубина

Е. В. Колдоба[1]

При решении нелинейного уравнения Бенедикта-Вебба-Рубина обычно используют метод Ньютона. В некоторых областях давлений и температур уравнение может иметь много корней, чтобы найти нужный корень необходимо аккуратно подставлять начальные значения для метода Ньютона. Для этого предлагается использовать формулы, задающие плотности газовой и жидкой фазы на равновесном фазовом переходе «газ-жидкость», которые можно настраивать на решаемое уравнение. Такой подход позволяет построить термодинамически согласованную модель удобную для численного решения, которая повышает надежность расчетов.

Ключевые слова: численные алгоритмы, многопараметрическое уравнение состояния, уравнение Бенедикта-Вебба-Рубина.

1. Введение

В последнее время возрос интерес к численному решению многопараметрических уравнений состояния высокой точности, нахождению нужного определенного корня уравнения. Например, в современных гидродинамических симуляторах, моделирующих месторождения нефти и газа, широко используется метод Педерсен [1] для вычисления вязкости газового, жидкого и закритического состояния флюида, в котором необходимо находить нужный корень уравнения Бенедикта-Вебба-Рубина. Метод Педерсен использует принцип соответственных состояний: вязкость многокомпонентного раствора (состав которого может непрерывно меняться) вычисляется через вязкость чистого (эталонного) вещества, например, метана. Метод себя хорошо зарекомендовал, однако, в некоторых случаях при решении наблюдаются нефизические скачки вязкости и даже отрицательные значения вязкости. Исследование таких случаев выявило несколько причин ошибок, одна из которых состоит в некорректном вычислении корня уравнения Бенедикта-Вебба-Рубина для эталонного вещества. В работе рассмотрен физический подход для задания начального приближения при вычисления нужного корня методом Ньютона для

[1] *Колдоба Елена Валентиновна* — доцент каф. вычислительная механика мех.-мат. ф-та МГУ, e-mail: elenakoldoba@mail.ru.

Koldoba Elena Valentinovna — Associate Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Computational Mechanics.

решения уравнения состояния высокой точности. Рассматривается вопрос термодинамического согласования формул и уравнения состояния.

2. Уравнение состояния Бенедикта-Вебба-Рубина для метана

Уравнения Бенедикта-Вебба-Рубина (БВР) - это многопараметрическое термическое уравнение состояния высокой точности, выражающее зависимость давления от температуры и плотности: $P = f(T, \rho)$. Оно описывает свойства и жидкой и газовой фаз, а также закритического состояния. Алгебраическое уравнение БВР имеет много модификаций [2-3], содержит от 15 до 40 членов, часть из которых экспоненциальные остальные степенные.

Уравнение БВР в форме, предложенной McCarty [3], выглядит следующим образом:

$$p = \sum_{n=1}^{9} a_n(T)\rho^n + exp(-0.0096\rho^2) \sum_{n=10}^{15} a_n(T)\rho^{2n-17}$$

здесь используются следующие единицы измерения величин: давление в атмосферах, температура в градусах Кельвина, плотность в молях на литр: $[p] = 1\ atm,\ [\rho] = 1mol/l,\ [T] = 1^oK$.

a_1	RT	a_9	N_{19}/T^2
a_2	$N_1T + N_2T^{1/2} + N_3 + N_4/T + N_5/T^2$	a_{10}	$N_{20}/T^2 + N_{21}/T^3$
a_3	$N_6T + N_7 + N_8/T + N_9/T^2$	a_{11}	$N_{22}/T^2 + N_{23}/T^4$
a_4	$N_{10}T + N_{11} + N_{12}T$	a_{12}	$N_{24}/T^2 + N_{25}/T^3$
a_5	N_{13}	a_{13}	$N_{26}/T^2 + N_{27}/T^4$
a_6	$N_{14}/T + N_{15}/T^2$	a_{14}	$N_{28}/T^2 + N_{29}/T^3$
a_7	N_{16}/T	a_{15}	$N_{30}/T^2 + N_{31}/T^3+$
a_8	$N_{17}/T + N_{18}/T^2$		$+N_{32}/T^4$

Table 1. Функции a_i [3].

При решении УРС в гидродинамических симуляторах на каждом шаге по времени и по пространству для заданных давлении P и температуре T следует определить плотность ρ газового, жидкого или

N_1	$-1.8439486666 \cdot 10^{-2}$	N_{17}	$5.7974531455 \cdot 10^{-6}$
N_2	1.0510162064	N_{18}	$-7.1648329297 \cdot 10^{-3}$
N_3	$-1.6057820303 \cdot 10^{1}$	N_{19}	$1.2577853784 \cdot 10^{-4}$
N_4	$8.4844027562 \cdot 10^{2}$	N_{20}	$2.2240102466 \cdot 10^{4}$
N_5	$-4.2738409106 \cdot 10^{4}$	N_{21}	$-1.4800512328 \cdot 10^{6}$
N_6	$7.6565285254 \cdot 10^{-4}$	N_{22}	$5.0498054887 \cdot 10^{1}$
N_7	$-4.8360724197 \cdot 10^{-1}$	N_{23}	$1.6428375992 \cdot 10^{6}$
N_8	$8.5195473835 \cdot 10^{1}$	N_{24}	$2.1325387196 \cdot 10^{-1}$
N_9	$-1.6607434721 \cdot 10^{4}$	N_{25}	$3.7791273422 \cdot 10^{1}$
N_{10}	$-3.7521074532 \cdot 10^{-5}$	N_{26}	$-1.1857016815 \cdot 10^{-5}$
N_{11}	$2.8616309259 \cdot 10^{-2}$	N_{27}	$-3.1630780767 \cdot 10^{1}$
N_{12}	-2.8685295973	N_{28}	$-4.1006782941 \cdot 10^{-6}$
N_{13}	$1.1906973942 \cdot 10^{-4}$	N_{29}	$1.4870043284 \cdot 10^{-3}$
N_{14}	$-8.5315715699 \cdot 10^{-3}$	N_{30}	$3.1512261532 \cdot 10^{-9}$
N_{15}	3.8365063841	N_{31}	$-2.1670774745 \cdot 10^{-6}$
N_{16}	$2.4986828379 \cdot 10^{-5}$	N_{32}	$12.4000551079 \cdot 10^{-5}$

Table 2. Коэффициенты функций N_i для метана [3]

закритического состояния флюида. Например, при вычислении вязкости газовой фазы по методу Педерсен, необходимо найти именно «газовый» корень уравнения состояния, иначе ошибка вычислений может составить несколько порядков. Уравнение решается методом Ньютона.

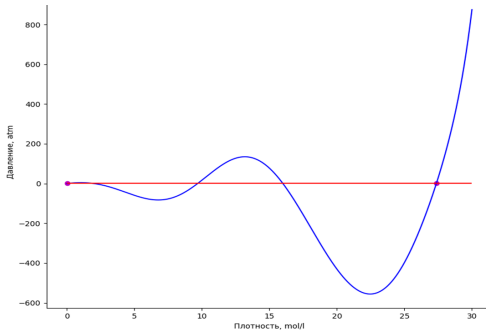

Figure 1. Изотерма уравнения БВР $P = f(\rho)$ при $T = 100^oK$,

При температурах выше критической решить уравнение просто: функция $P = f(T, \rho)$ монотонная и корень один. Сложность решения уравнения возникает при температурах ниже критических $T < T_c$. когда количество корней возрастает, так при $T = 100^oK$ их может быть уже пять (см. Рис.1), но только два из них имеют физический смысл - газовый (G) и жидкий (L), находящиеся соответственно на газовой и жидкой

ветвях уравнения состояния, и только один из них является искомым решением уравнения. Нахождение нужного корня прежде всего зависит в этом случае от правильно заданного начального приближения ρ_0. В данной работе предлагается использовать для этого формулы, задающие плотности газовой ρ_{sG} и жидкой ρ_{sL} фаз в точках фазового перехода (P_s, T) (индекс "s" указывает, что значение величины берется на фазовом переходе).

Формулы, задающие плотности жидкой $\rho_{sL}(T)$ и газовой $\rho_{sG}(T)$ фазы на кривой фазового перехода (кривая насыщения) имеют вид [4]:

$$\rho_{sL}(T) = \rho_c \exp\left(n_1\theta^{0.354} + n_2\theta^{0.5} + n_3\theta^{2.5}\right) \tag{1}$$

где $\theta = 1 - T/T_c$, $n_1 = 1.9906389$, $n_2 = -0.78756197$, $n_3 = 0.036976723$.

$$\rho_{sG}(T) = \rho_c \exp\left(n_1\theta^{0.354} + n_2\theta^{5/6} + n_3\theta^{3/2} + n_4\theta^{5/2} + n_5\theta^{25/6} + n_6\theta^{47/6}\right) \tag{2}$$

где $n_1 = -1.880284$, $n_2 = -2.8526531$, $n_3 = -3.000648$, $n_4 = -5.251169$, $n_5 = -13.191859$, $n_6 = -37.553961$.

Было проведено исследование термодинамической согласованности формул (1-2) с уравнением БВР. В широком диапазоне температур по уравнению БВР находилось давления насыщения $P_s(T)$ фазового перехода "жидкость-газ" и вычислялись значения плотностей жидкой ρ_{sL} и газовой ρ_{sG} фаз, которые сравнивались со значениями, полученными по формулам (1-2). Результаты совпали с хорошей точностью: погрешность меньше 1 процента (см. Рис.2).

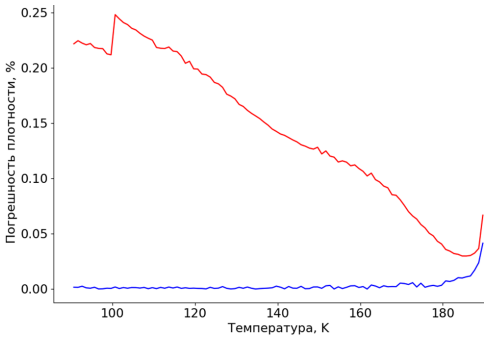

Figure 2. Сравнение плотности жидкой и газовой фазы на фазовом переходе, вычисленных по БВР и формулам (1), (2).

Если наблюдается рассогласованность формул с уравнением БВР, то для формулы (1-2) можно подстроить, введя поправочный коэффициент.

Однако, даже при правильно заданном начальном приближении при нахождении корня методом Ньютона возможны "перескоки" с газовой

ветви уравнения на другие ветви, не имеющие физического смысла, что приводит к нахождению неправильного корня и к значительным ошибкам. В этом случае в качестве искомой плотности ρ, например, для вычисление вязкости, предлагается брать значение ρ_{sL} или ρ_{sG} соответственно для нужной нам фазы, что дает некоторую ошибку, но не столь большую, как в случае "перескока".

Пример 1

Найти плотность газовой фазы ρ_G при давлении P = 10 atm и температуре T = 150 K, т.е. необходимо найти корень уравнения БВР на отрезке уравнения, задающего плотности газовой фазы. Начальное приближение, полученное по формуле (2): $\rho_{sG} = 1.02 mol/l$, подставляем его в уравнение БВР, получаем $P_s = 1.02 mol/l$. Метод Ньютона стартует из точки (P_s, ρ_{sG}). Ответ: $\rho_G = 0.98 mol/l$.

Пример 2

Найти плотность жидкой фазы ρ_L при P = 40 atm и T = 150 K, т.е. необходимо найти корень уравнения БВР на отрезке уравнения, задающего плотности жидкой фазы. Начальное приближение берется по формуле (1): $\rho_{sL} = 22.3 mol/l$. Ответ: $\rho_L = 22.7 mol/l$.

Пример 3

Найти газовый корень ρ_G при P = 40 atm и T = 190 K. Начальное приближение по формуле (2): $\rho_{sG} = 0.12 mol/l$. Ответ:: плотность газа $\rho_{sG} = -19.6 < 0$.

Найденный корень в примере 3 - отрицательный, он не является физическим решением. Хотя начальное приближение было взято на газовой ветви по формуле (2), при решении методом Ньютона произошел "перескок" с газовой ветви уравнения на другую. Если для задачи требуется в этом случае значение плотности газовой фазы, то в качестве приближенного решения можно брать начальное значение $\rho_{sG} = 0.12 mol/l$.

3. Заключение

Предлагаемые начальные приближения для метода Ньютона делают более надежным численный алгоритм для нахождения нужного корня уравнения состояния высокой точности Бенедикта-Вебба-Рубина. Для решения уравнений состояния высокой точности необходимо проверять термодинамическое согласоване формул и решаемого уравнения. Кроме того, плотности, заданные формулам (1-2) могут использоваться для решения задач гидродинамики в случае отсутствия точного численного решения как приблизительное значени, что актуально, например, для модели Педерсен.

Список литературы

[1] Pedersen, K.S. and Fredenslund, Aa., "An improved corresponding states model for the prediction of oil and gas viscosities and thermal conductivities", *Chem. Eng. Sci.*, **42** (1987), 182—186.

[2] Benedict M., Webb G. B., Rubin L. C., "An Empirical Equation for Thermodynamic Properties of Light Hydrocarbons and Their Mixtures: I. Methane, Ethane, Propane, and n-Butane", *Journal of Chemical Physics*, **8**:4 (1940), 334-345.

[3] McCarty, R.D., "A modified Benedict-Webb-Rubin equation of state for methane using recent experimental data", *Cryogenics*, **14** (1974), 276—280.

[4] Kleinrahm R. and Wagner W., "Measurement and Correlation of the Equilibrium Liquid and Vapour Densities and the Vapour Pressure along the Coexistence Curve of Methane", *Journal of Chemical Thermodynamics*, **18**:8 (1986), 739—760.

Numerical solution of the multiparameter Benedict-Webb-Rubin equation of state with high accuracy

Koldoba E.V.

When solving the nonlinear Benedict-Webb-Rubin equation, Newton's method is usually used. In some areas of pressure and temperature, the equation has many roots; to find the root we need, we must carefully set the initial values for Newton's method. To do this, it is proposed to use formulas that specify the densities of the gas and liquid phases at the equilibrium gas-liquid phase transition, which can be adjusted to the equation being solved. This approach makes it possible to construct a thermodynamically consistent model convenient for numerical solution, which increases the reliability of calculations.

Keywords: numerical algorithms, multiparameter equation of state, Benedict-Webb-Rubin equation.

References

[1] Pedersen, K.S. and Fredenslund, Aa., "An improved corresponding states model for the prediction of oil and gas viscosities and thermal conductivities", *Chem. Eng. Sci.*, **42** (1987), 182—186.

[2] Benedict M., Webb G. B., Rubin L. C., "An Empirical Equation for Thermodynamic Properties of Light Hydrocarbons and Their Mixtures: I. Methane, Ethane, Propane, and n-Butane", *Journal of Chemical Physics*, **8**:4 (1940), 334-345.

[3] McCarty, R.D., "A modified Benedict-Webb-Rubin equation of state for methane using recent experimental data", *Cryogenics*, **14** (1974), 276—280.

[4] Kleinrahm R. and Wagner W., "Measurement and Correlation of the Equilibrium Liquid and Vapour Densities and the Vapour Pressure along the Coexistence Curve of Methane", *Journal of Chemical Thermodynamics*, **18**:8 (1986), 739—760.

Часть 2
Специальные вопросы теории интеллектуальных систем

Жадный алгоритм формирования решающих ансамблей

А. В. Фомченко[1] Д. В. Парфенов[2]

Рассмотрен подход к совершенствованию методов решения задач машинного обучения на основе ансамблей алгоритмов на примере задачи классификации. Предложен метод выбора слабых решателей на основе жадного алгоритма и построения избирательного ансамбля. Этот подход является достаточно общим и может найти применение в системах поддержки принятия решений и в других экспертных системах.

Ключевые слова: машинное обучение, слабые решатели, решающие ансамбли, бустинг

1. Постановка задачи

Задача обучения по прецедентам $\langle X, Y, y^*, X', Y' \rangle$, где X – пространство объектов; Y – множество ответов; $y^* : X \to Y$ – неизвестная целевая зависимость; X' – обучающая выборка; Y' – вектор ответов на обучающих объектах, заключается в том, чтобы построить алгоритм $r : X \to Y$, аппроксимирующий целевую зависимость с заданной точностью α. Это значит, что вероятность верного ответа $P(r(x) = y) \geq \alpha$, то есть вектор результатов алгоритма должен совпадать с вектором ответов не менее чем на $\alpha \cdot 100\%$ [1].

2. Особенности ансамблевого подхода

Одним из методов построения эффективного решателя является ансамблирование, предполагающее использование нескольких слабых решающих правил (далее для краткости решателей) для формирования сильного правила требуемого качества. Такой метод имеет следующие преимущества:

1) Ансамбль способен обеспечить значительно лучший результат для разнородных данных по сравнению с отдельными его частями;

[1] *Фомченко Александр Валерьевич* — аспирант каф. высшей математики Института искусственного интеллекта РТУ МИРЭА, e-mail: fomchenko@mirea.ru.

Fomchenko Aleksandr Valerevich — Ph.D. student, Russian Technological University (MIREA), Institute of Artificial Intelligence, Department of Higher Mathematics.

[2] *Парфенов Денис Васильевич* — к.т.н., доцент каф. высшей математики Института искусственного интеллекта РТУ МИРЭА, e-mail: parfenov@mirea.ru.

Parfenov Denis Vasilevich, Ph.D. — associate professor, Russian Technological University (MIREA), Institute of Artificial Intelligence, Department of Higher Mathematics.

2) Ансамблированный решатель гораздо проще дообучать на новых данных в случае необходимости, поскольку дообучение можно проводить локально;

3) Решатель хорошо поддаётся декомпозиции в силу способа его построения, что облегчает его анализ и расширяет возможности параллельной программной реализации;

4) Есть возможность вычислительной оптимизации для принятия решения через выбор части ансамбля или даже только одного слабого решающего алгоритма ситуативно [2].

При построении ансамбля одновременно используют конечное множество предварительно обученных решателей, выходные сигналы которых объединяются в более качественный ответ. Возникает ряд вспомогательных проблем, которые рассмотрим детальнее.

Проблема 1: агрегирование результатов.
Одним из простейших способов объединения является метод голосования, где результат выбирается простым большинством по совокупности ответов всех слабых решателей. Развитием этой идеи служит использование весовых коэффициентов для каждого решателя в голосовании, но возникает задача отыскания оптимальных весов. Общий подход состоит в обучении еще одного дополнительного алгоритма, входами которого будут прогнозы всех алгоритмов ансамбля, выходом – итоговый прогноз. После завершения этапа обучения для каждого решателя определяется коэффициент его компетентности на совокупности данных [1]. Также популярно применение алгоритма бустинга – процедуры последовательного построения композиции алгоритмов машинного обучения, когда каждый следующий алгоритм стремится компенсировать недостатки композиции всех предыдущих алгоритмов [3].

Проблема 2: обеспечение разнообразия ансамбля.
Гарантия различия индивидуальных слабых решателей является фундаментальной задачей при построении ансамблей [4]. Очевидно, агрегация схожих решателей в ансамбле затрудняет существенное повышение качества решения задачи. При этом индивидуальные слабые решатели обучаются для решения одной задачи по одной обучающей выборке и, как следствие, достаточно сильно коррелированы.

Проблема 3: обоснованный выбор количества решателей в ансамбле.
Начиная с некоторого момента, увеличение их количества перестает значимо способствовать улучшению точности решения задачи, но приводит к существенному росту требуемых вычислительных ресурсов [5].

3. Применение жадного алгоритма для генерации ансамбля

Рассмотрим предлагаемый жадный алгоритм построения ансамбля на примере задачи классификации и то, как он справляется с описанными проблемами.

Основные шаги алгоритма:

1) Создание множества n различных слабых решателей и их обучение на исходной совокупности данных $A = \langle X', Y' \rangle$.

2) Проверка каждого решателя на выборке A, выбор одного из них с наилучшим результатом. Пусть он обеспечил правильные ответы на некоторой выборке $B \in A$.

3) Дальнейшее дообучение выбранного слабого решателя на выборке B с целью улучшения его надёжности, что важно для противостояния шумам и погрешностям в реальных данных. При этом решатель специализируется на качественной работе с определённым подклассом данных.

4) Переход к шагу 2 на усеченной выборке $A = A - B$, если не выполнено хотя бы одно из двух условий:

   а) Достигнута заданная точность (мощность новой выборки составляет заданную малую часть от мощности изначальной $|A| < (1 - \alpha)\ |\langle X', Y' \rangle|$). Это означает, что далее гарантированно будут происходить еще меньшие отсечения от основной выборки, и оставшиеся решатели нет смысла включать в ансамбль. Это нормальное завершение алгоритма.

   б) Исчерпано множество слабых решателей. Это свидетельствует о недостаточности ансамбля для решения задачи с заданной точностью и необходимости его пополнения, либо усиления разнообразия.

Рассмотрим алгоритм построения ансамбля подробнее. При создании и обучении слабых решателей важно, чтобы они давали различные результаты на одном наборе данных. Если ответы двух решателей совпадают сильнее заданной для задачи величины α, то нет смысла применять оба в ансамбле. Действительно, алгоритм использует ровно один лучший решатель на каждом шаге, что вычислительно экономично. По этой же причине на шаге 3 алгоритма применяется дообучение, а не обучение с самого начала. Этим обеспечиваются как разнородность сравниваемых решателей, так и экономия вычислительных ресурсов.

В самом начале создается набор из n слабых решателей, удовлетворяющих требованию разнообразия ансамбля. Один из методов такой генерации – манипуляции с входными переменными и параметрами обучения [6]. За счёт этого решатели при обучении могут сходиться к разным результатам. Однако это не гарантируется для всех решателей, какие-то могут сходиться к близким, и даже одинаковым параметрам. Такие случаи на шаге 1 алгоритма отфильтровываются для увеличения производительности обучения. Другой подход – генерация уникальных обучающих подмножеств для каждого слабого решателя [6]. Здесь возникает сложность их обоснованного выбора.

После создания набора решателей из него итеративно выбираются наиболее подходящие для итогового ансамбля. Изначальное множество данных A сокращается на каждой итерации, поэтому цикл может завершиться только двумя способами: либо множество данных для обучения сократится до объема $(1 - \alpha)$ от изначального, либо закончится набор самих решателей. Первый случай является успешным завершением алгоритма.

После нахождения и обучения минимально достаточного набора решателей требуется их объединить с помощью агрегирующего решающего правила. Для формирования ансамбля можно использовать голосование с использованием весов, описанное выше. Вес для каждого решателя задается соотношением множества его правильных ответов на обучающей выборке ко всей обучающей выборке. Таким образом, веса автоматически получаются нормированными. Однако при этом никак качественно не учитывается область применимости того или другого слабого решателя. Альтернативный подход – использование отдельного селективного решателя для выбора одного наиболее подходящего по ситуации слабого решателя из ансамбля. Селективный решатель обучается после построения всех решателей в ансамбле. Итоговый алгоритм описывается блок-схемой, приведённой на Рисунке 1.

Такой метод решает всю совокупность проблем, описанных выше:

1) Разнородные данные обрабатываются так, что для каждой выборки с особыми свойствами в ходе цикла берётся один решатель, лучше работающий на ней. Таким образом попутно осуществляется кластеризация обучающих данных с позиций их проекции на решатели, что сильно упрощает анализ алгоритма.

2) Разнообразие ансамбля обеспечивается шагом 3 алгоритма, где за счёт дообучения на отдельных непересекающихся выборках данных решатели будут значительно отличаться, даже если исходно их поведение было похожим. Кроме того, изначальная генерация n слабых решателей уже подразумевает их некоторое разнообразие.

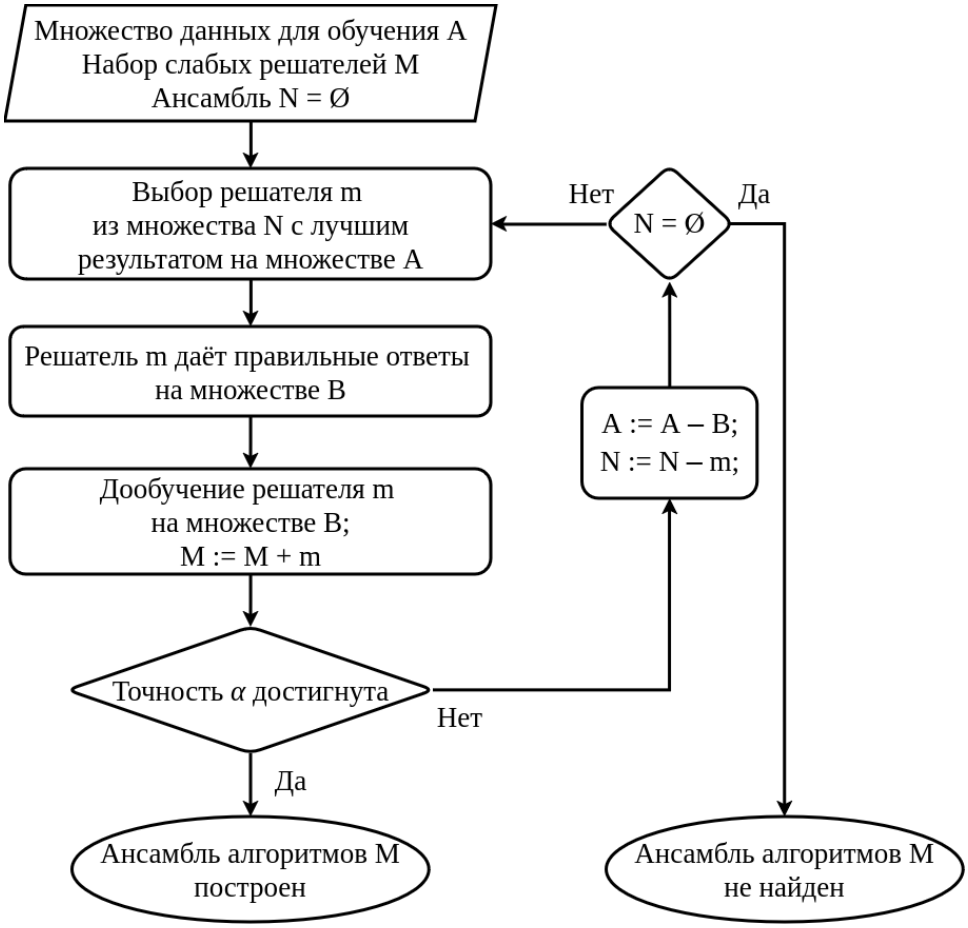

Рисунок 1. Блок-схема алгоритма построения ансамбля решателей.

3) Количество решателей в ансамбле оптимально подбирается самим алгоритмом. Однако, важна возможность их выбора из исходно достаточно большой и разнородной совокупности. Вообще говоря, чем больше n, тем лучше может оказаться результат ценой увеличения затрат на создание ансамбля. При этом сложность всего ансамблевого решателя не только не увеличивается с ростом n, но и способна снижаться за счёт более удачного выбора его компонент на каждом шаге 2 и, таким образом, сокращения их числа в ансамбле.

Существуют другие жадные алгоритмы для решения задач классификации данных, в том числе разнородных. Так, например, в статье [7] описано итеративное применение одиночных классификаторов на обучающей выборке и учёт в итоговом решении вклада только тех классификаторов,

ошибка которых не превосходит заданный порог. Однако в этом алгоритме не применяется дополнительное дообучение выбранных алгоритмов на данных, где они себя проявляют (шаг 3 алгоритма). В работе [8] приведен алгоритм set covering machine для построения решающих списков. Решающий список закономерностей представляет собой частный случай алгоритмической композиции с голосованием по старшинству. На каждой итерации алгоритма выбирается правило, допускающее наименьшее количество ошибок. В этом алгоритме также нет дообучения, кроме того, есть ограничение на максимальную допустимую долю ошибок на обучающей выборке, подбираемое экспериментально.

4. Экспериментальное сравнение с другими алгоритмами

В наших экспериментах в качестве решателей используются свёрточные нейронные сети прямого распространения, в частности, потому что для них относительно легко обеспечить разнообразие ансамбля, выбирая веса перед обучением случайным образом. Выборкой данных служит разнородная совокупность из 100000 объектов 5 классов; данные в ней распределены по классам равномерно. Использовался один и тот же набор однотипных трёхслойных нейросетей по 5 нейронов в каждом слое. Далее в тексте такие нейросети будут называться малыми. В качестве решателей взяты:

1) Одна нейросеть 6 слоёв по 15 нейронов. Такой размер выбран исходя из приближенного равенства общего числа нейронов в ней и в 6 нейросетях из ансамбля пункта 2).

2) Ансамбль с голосованием – 6 малых нейросетей.

3) Ансамбль с избирательной нейросетью. Избирательная сеть такая же по размерам, как и малая.

4) Ансамбль, сформированный из 10 малых нейросетей со случайной инициализацией весов с применением жадного алгоритма. Для ансамбля использовалась селективная нейросеть такого же размера, как и малая.

Точность алгоритма (вероятность принятия правильного решения) приведена в Таблице 1. В экспериментах жадный алгоритм формирования ансамбля завершался по достижении заданной точности $\alpha = 95\%$. При увеличении α до 100% алгоритм продолжил работу до 5 нейросетей и достиг точности 0.9628. Предлагаемый метод экспериментально

Таблица 1. Сравнение точности алгоритмов.

Метод	Параметры	Точность
Нейросеть	1 нейросеть (90 нейронов)	0.8651
Ансамбль с голосованием	6 нейросетей (суммарно 90 нейронов)	0.7457
Ансамбль с селективной нейросетью	5 нейросетей + селективная (суммарно 90 нейронов)	0.9171
Применение жадного алгоритма	Изначально 10 нейросетей, в результате выбраны 4 + селективная (суммарно 75 нейронов)	0.9513

Таблица 2. Сравнение алгоритмов по площади ROC-AUC.

Метод	Параметры	ROC-AUC
Нейросеть	1 нейросеть (90 нейронов)	0.848
Ансамбль с голосованием	6 нейросетей (суммарно 90 нейронов)	0.864
Ансамбль с селективной нейросетью	5 нейросетей + селективная (суммарно 90 нейронов)	0.935
Применение жадного алгоритма	Изначально 10 нейросетей, в результате выбрано 2 + селективная (суммарно 45 нейронов)	0.966

превосходит сравниваемые, имеющие даже превосходящую сложность. В Таблице 2 представлен результат для бинарной классификации из 100000 объектов теми же алгоритмами. В качестве метрики выбрана площадь под кривой ошибок (ROC-AUC, см. Рисунок 2). В случае безошибочного распознавания площадь под кривой равна единице. Если же использование решателя не отличается от случайного угадывания, значение площади под кривой стремится к 0.5. Использование этой метрики позволяет дать наглядную оценку для случая разнородных данных [9].

Таким образом, представленный метод не уступает ближайшему сопернику – ансамблю с избирательной нейросетью и дополнительным шагом кластеризации. Важно подчеркнуть существенное отличие предложенного подхода от избирательной нейросети. Дело в том, что такая нейросеть представляет собой «чёрный ящик» – нельзя точно сказать, почему был выбран конкретный решатель или совокупность результатов нескольких слабых решателей. Из этого следует дополнительная сложность донастройки ансамбля в случае небольшого изменения исходных

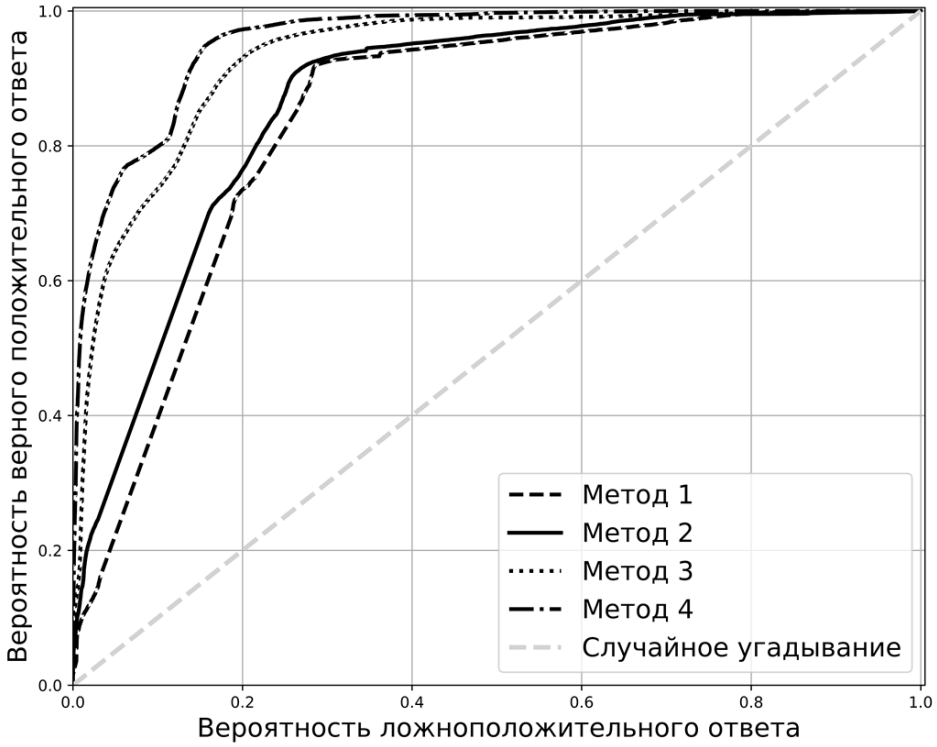

Рисунок 2. ROC-кривые четырёх методов.

данных, а также неприменимость подхода с избирательной нейросетью в задачах, где нужна доказательность решения.

Выводы:

1) В результате тестирования предложенный подход продемонстрировал превосходящую эффективность по обоим применявшимся критериям в сравнении с рассмотренными альтернативами.

2) Новый метод универсален, хорошо модифицируем и применим для решения широкого класса задач интеллектуального анализа данных. Возможно использование решателей различного типа в рамках одного гетерогенного ансамбля.

3) Рассмотренный алгоритм имеет доказательное построение и лишён подстроечных гиперпараметров, что облегчает его анализ, программную реализацию и обучение.

4) В нем количество отобранных для ансамбля слабых решателей мало зависит от их количества в изначальном наборе. Оно определяется лишь качеством первичных решателей, их способностью дообучаться на сокращённом наборе данных и требуемой точностью. Даже при большом изначальном количестве решателей в результате получается компактный и эффективный ансамбль.

5) Данный подход прекрасно приспособлен к распараллеливанию вычислений как на стадии обучения, так и при использовании.

6) Его применение является вычислительно экономным в силу использования выбираемого селективным решателем каждый раз одного слабого решателя для выработки полноценного итогового решения. Это возможно благодаря специализации решателей в процессе их дообучения.

Литература

[1] Воронцов К.В., *Математические методы обучения по прецедентам (теория обучения машин)*, `http://www.machinelearning.ru/wiki/index.php`, 2023.

[2] Rokach L., *Artificial Intelligence Review*, **33**:1-2 (2009), 1-39.

[3] Кашницкий Ю.С., Игнатов Д.И., "Ансамблевый метод машинного обучения, основанный на рекомендации классификаторов", *Интеллектуальные системы. Теория и приложения*, **19**:4 (2015), 37-55.

[4] Kuncheva L.I., *Combining Pattern Classifiers: Methods and Algorithms*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2014, 360 pp.

[5] Кривенко М.П., Васильев В.Г., *Методы классификации данных большой размерности*, ИПИ РАН, М., 2013, 203 pp.

[6] Мангалова Е.С., Агафонов Е.Д., "О проблеме генерации разнообразия ансамблей индивидуальных моделей в задаче идентификации", *Тр. XII Всерос. совещания по проблемам управления ВСПУ-2014*, 2014, 3214-3223

[7] Alsova O.K., Stubarev I.M., "Inhomogeneous ensemble algorithm for classifying different types of data", *News of Samara scientific center of Russian Academy of Sciences*, 2017, 118-123

[8] Marchand M., Shawe-Taylor J., "Learning with the set covering machine", *Proc. 18th International Conf. on Machine Learning*, Morgan Kaufmann, San Francisco, CA, 2001, 345-352

[9] Zweig M., Campbell G., "Receiver-operating characteristic (ROC) plots: a fundamental evaluation tool in clinical medicine", *Clinical Chemistry 1993*, **39**:4 (1993), 561-577

A greedy algorithm for building learning ensembles
Fomchenko A.V., Parfenov D.V.

An approach to improving methods for solving machine-learning problems based on ensembles of algorithms is considered using classification problem as an example. A method based on a greedy algorithm for choosing weak learners and building the selective ensemble is proposed. This approach is general and applicable in decision support systems and other expert systems.

Keywords: machine learning, weak learners, ensembling, boosting

References

[1] Vorontsov K.V., *Mathematical methods of teaching by precedents (machine learning theory)*, `http://www.machinelearning.ru/wiki/index.php`, 2023 (In Russian)

[2] Rokach L., *Artificial Intelligence Review*, **33**:1-2 (2009), 1-39

[3] Kashnitsky Yu.S., Ignatov D.I., "Ensemble machine learning method based on classifier recommendation", *Intelligent Systems. Theory and Applications*, **19**:4 (2015), 37-55 (In Russian)

[4] Kuncheva L.I., *Combining Pattern Classifiers: Methods and Algorithms*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2014, 360 pp.

[5] Krivenko M.P., Vasilev V.G., *Methods for classifying high-dimensional data*, IPI RAN, M., 2013 (In Russian), 203 pp.

[6] Mangalova E.S., Agafonov E.D., "On the problem of generating diversity of ensembles of individual models in the identification problem", *Proc. of the XII All-Russian meetings on management issues, VSPU-2014*, 2014, 3214-3223 (In Russian)

[7] Alsova O.K., Stubarev I.M., "Inhomogeneous ensemble algorithm for classifying different types of data", *News of Samara scientific center of Russian Academy of Sciences*, 2017, 118-123

[8] Marchand M., Shawe-Taylor J., "Learning with the set covering machine", *Proc. 18th International Conf. on Machine Learning*, Morgan Kaufmann, San Francisco, CA, 2001, 345-352

[9] Zweig M., Campbell G., "Receiver-operating characteristic (ROC) plots: a fundamental evaluation tool in clinical medicine", *Clinical Chemistry 1993*, **39**:4 (1993), 561-577

Степени разделющих многочленов для классов Поста

М. В. Носов[1]

В работе получены оценки степеней многочленов с действительными коэффициентами, разделяющих нули и единицы булевских функциий для классов Поста.

Ключевые слова: классы Поста, разделяющий многочлен.

Пусть B^n– n-мерный единичный куб, $R[x]$ – множество многочленов от n переменных с действительными коэффициентами, $x = (x_1, \ldots, x_n)$, P_2 – множество булевых функций. Скажем, что многочлен $f(x), f(x) \in R[x]$ разделяет нули и единицы булевой функции $F(x)$, если

$$F(\alpha) = 1 \Leftrightarrow f(\alpha) \geq 0, \quad F(\alpha) = 0 \Leftrightarrow f(\alpha) < 0, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in B^n.$$

Такой многочлен $f(x)$ будем называть разделяющим многочленом функции $F(x)$ и обозначать $f \sim F$.Пусть K подмножество множества булевых функций, $K(n)$ подмножество функций множества K, функции из $K(n)$ зависят от n аргументов. Введём обозначение

$$degK(n) = \max_{F, F \in K(n)} \min_{f, f \sim F} degf(x).$$

Укажем $degK(n)$ для всех классов Поста K [1].

Приведём утверждения из [2,3], на которых основаны дальнейшие выводы.

1.Для любой булевой функции от n аргументов степень разделяющего многочлена не превышает n.

2.Пусть $F \in P_2$, B^k– k-мерная грань B^n, пусть $F|_{B^k} \in L$, тогда степень разделяющего многочлена не меньше k. Из этого утверждения следуют два факта.

2.1. Только для двух булевых функций $x_1 \bigoplus \ldots \bigoplus x_n$ и $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1$ степень разделяющего многочлена n.

2.2. Пусть $F \in P_2$, пусть Π^k– k-мерный параллелепипед, вершинами которого являются вершины B^n, пусть на соседних вершинах Π^k функция F принимает разные значения, тогда степень разделяющего многочлена для F не меньше k.

3.$degM(n) = [\frac{n}{2}]$, где $M-$ класс монотонных функций.

[1] *Носов Михаил Васильевич* — с.н.с. каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: mvnosov@rambler.ru.

Nosov Michail Vasilevich-senior researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Далее перечислим оценки для классов Поста, при необходимости приведём соответствующие доказательства (в обозначениях и нумерации будем придерживаться "Сводной таблицы замкнутых классов" [1]).

1.$degO_1(n) = 1$. 2.$degO_2(n) = 0$. 3.$degO_3(n) = 0$. 4.$degO_4(n) = 1$.

5.$degO_5(n) = 1$. 6.$degO_6(n) = 1$. 7.$degO_7(n) = 0$. 8.$degO_8(n) = 1$.

9.$degO_9(n) = 1$.

10.$degS_1(n) = 1$. Разделяющий многочлен для функции $\bigvee\limits_{i=1}^{n} x_i$ имеет вид $x_1 + \ldots + x_n - 0.5$.

11.$degS_3(n) = 1$. 12.$degS_5(n) = 1$. 13.$degS_6(n) = 1$.

14.$degP_1(n) = 1$. Разделяющий многочлен для функции $\bigwedge\limits_{i=1}^{n} x_i$ имеет вид $x_1 + \ldots + x_n - n$.

15.$degP_3(n) = 1$. 16.$degP_5(n) = 1$. 17.$degP_6(n) = 1$.

18.$degL_1(n) = n$. Следует из вышеприведенных фактов.

19.$degL_2(n) = n$. 20.$degL_3(n) = n$. 21.$degL_4(n) = n$, n - нечётное.

22.$degL_5(n) = n$, n - нечётное.

23.$2l - 1 \leq degD_2(4l) \leq 2l, l \geq 2$.

$2l - 1 \leq degD_2(4l + 1) \leq 2l, l \geq 2$.

$degD_2(4l + 2) = 2l + 1, l \geq 2$.

$degD_2(4l + 3) = 2l + 1, l \geq 2$.

Доказательство.

Класс D_2 содержится в классе монотонных функций, поэтому степень разделяющего полинома не превышает $[\frac{n}{2}]$. Рассмотрим четыре случая.

а) $n = 4l + 2$.

$$R = (1, 0, 1, 0, \ldots, 1, 0)$$

$$b_1 = (-1, 1, 0, 0, \ldots, 0, 0),$$

$$b_2 = (0, 0, -1, 1, \ldots, 0, 0),$$

$$\ldots\ldots\ldots$$

$$b_{2l+1} = (0, 0, 0, 0, \ldots, -1, 1)$$

Построим параллелепипед размерности $2l + 1$.

$$\Pi^{2l+1} = \{R + \delta_1 b_1 + \ldots + \delta_{2l+1} b_{2l+1} | \delta_1 \ldots, \delta_{2l+1} \in \{0, 1\}\}$$

Очевидно, что все вектора параллелепипеда несравнимы между собой, имеют длину $2l+1$, противоположный вектор к вершине параллелепипеда попадает в параллелепипед. Следовательно, на параллелепипеде можно задать линейную функцию от нечётного числа аргументов, т.е.

самодвойственную. Пусть $S_{2l+1} = \{x \in B^n || x| = 2l+1\}$ - слой куба, вектора слоя несравнимы между собой, вектор слоя переходит в вектор слоя при взятии противоположного вектора, таким образом, множество векторов слоя вне параллелепипеда можно разбить на пары: (вектор, противоположный вектор). Функцию с параллелепипеда можно продолжить на слой положив на паре разные значения. Наконец, продолжим на весь куб: на вершинах B^{4l+2} выше слоя положим значение 1, на вершинах ниже слоя положим значение 0. В результате получили самодвойственную монотонную функцию, у которой есть параллелепипед размерности $2l+1$, на котором функция линейна. Следовательно, степень разделяющего многочлена не меньше $2l+1$. Значит, $degD_2(4l+2) = 2l+1$.

б)$n = 4l+3$.

$$R = (0,1,0,1,0,\ldots,1,0)$$

$$b_1 = (1,-1,1,0,0,\ldots,0,0),$$

$$b_2 = (0,0,0,-1,1,\ldots,0,0),$$

$$b_3 = (0,0,0,0,0,-1,1,\ldots,0,0),$$

$$\ldots\ldots\ldots$$

$$b_{2l+1} = (0,0,0,0,\ldots,-1,1)$$

Построим параллелепипед размерности $2l+1$.

$$\Pi^{2l+1} = \{R + \delta_1 b_1 + \ldots + \delta_{2l+1} b_{2l+1} | \delta_1 \ldots, \delta_{2l+1} \in \{0,1\}\}$$

Пусть

$$W = \{R + 0 \cdot b_1 + \delta_2 b_2 + \ldots + \delta_{2l+1} b_{2l+1} | \delta_2 \ldots, \delta_{2l+1} \in \{0,1\}\}$$

$$U = \{R + 1 \cdot b_1 + \delta_2 b_2 + \ldots + \delta_{2l+1} b_{2l+1} | \delta_2 \ldots, \delta_{2l+1} \in \{0,1\}\}$$

Очевидно, что вектора параллелепипеда несравнимы между собой. Для $u \in U, \overline{u} \in W$, для $w \in W, \overline{w} \in U$. Определим функцию: на Π^{2l+1} зададим линейную функцию, на $S^{2l+2} \setminus U$ функция равна 1, на $S^{2l+1} \setminus W$ функция равна 0, ниже слоя S^{2l+1} равна 0, выше слоя S^{2l+2} равна 1. Построенная функция является самодвойственной монотонной. Значит, $degD_2(4l+3) = 2l+1$.

в) $n = 4l+1$.

$n = 4l+1 = 2(2l-2)+5$.

$$R = (1,1,0,0,0,0,1,0,1,\ldots,0,1)$$

$$b_1 = (-1, -1, 1, 1, 1, 0, 0, 0, 0, \ldots, 0, 0),$$

$$b_2 = (0, 0, 0, 0, 0, 1, -1, \ldots, 0, 0),$$

$$b_3 = (0, 0, 0, 0, 0, 0, 0, 1, -1, \ldots, 0, 0),$$

$$\ldots\ldots\ldots$$

$$b_{2l-1} = (0, 0, 0, 0, \ldots, 1, -1)$$

Построим параллелепипед размерности $2l - 1$.

$$\Pi^{2l-1} = \{R + \delta_1 b_1 + \ldots + \delta_{2l-1} b_{2l-1} | \delta_1 \ldots, \delta_{2l-1} \in \{0, 1\}\}$$

$$W = \{R + 0 \cdot b_1 + \delta_2 b_2 + \ldots + \delta_{2l-1} b_{2l-1} | \delta_2 \ldots, \delta_{2l-1} \in \{0, 1\}\}$$

$$U = \{R + 1 \cdot b_1 + \delta_2 b_2 + \ldots + \delta_{2l-1} b_{2l-1} | \delta_2 \ldots, \delta_{2l-1} \in \{0, 1\}\}$$

Очевидно, что вектора параллелепипеда несравнимы между собой. Для $u \in U, \overline{u} \in W$, для $w \in W, \overline{w} \in U$. Определим функцию: на Π^{2l-1} зададим линейную функцию, на $S^{2l+1} \setminus U$ функция равна 1, на $S^{2l} \setminus W$ функция равна 0, ниже слоя S^{2l} равна 0, выше слоя S^{2l+1} равна 1. Построенная функция является самодвойственной монотонной. Значит, $degD_2(4l + 1) \geq 2l - 1$.

г) $n = 4l$.

$n = 4l = 2(2l - 2) + 4$.

$$R = (1, 1, 0, 0, 0, 1, 0, 1, \ldots, 0, 1)$$

$$b_1 = (-1, -1, 1, 1, 0, 0, 0, 0, \ldots, 0, 0),$$

$$b_2 = (0, 0, 0, 0, 1, -1, \ldots, 0, 0),$$

$$b_3 = (0, 0, 0, 0, 0, 0, 1, -1, \ldots, 0, 0),$$

$$\ldots\ldots\ldots$$

$$b_{2l-1} = (0, 0, 0, 0, 0, 0, \ldots, 1, -1)$$

Построим параллелепипед размерности $2l - 1$.

$$\Pi^{2l-1} = \{R + \delta_1 b_1 + \ldots + \delta_{2l-1} b_{2l-1} | \delta_1 \ldots, \delta_{2l-1} \in \{0, 1\}\}$$

$$W = \{R + 0 \cdot b_1 + \delta_2 b_2 + \ldots + \delta_{2l-1} b_{2l-1} | \delta_2 \ldots, \delta_{2l-1} \in \{0, 1\}\}$$

$$U = \{R + 1 \cdot b_1 + \delta_2 b_2 + \ldots + \delta_{2l-1} b_{2l-1} | \delta_2 \ldots, \delta_{2l-1} \in \{0, 1\}\}$$

Очевидно, что вектора параллелепипеда несравнимы между собой. Для $u \in U, \overline{u} \in W$, для $w \in W, \overline{w} \in U$. Определим функцию: на Π^{2l-1} зададим линейную функцию, на $S^{2l} \setminus U \cup W$ функцию зададим аналогично пункту а) − разобъём на пары (вектор, противоположный вектор), положив на паре разные значения, ниже слоя S^{2l} функция равна 0, выше слоя S^{2l} функция равна 1. Построенная функция является самодвойственной монотонной. Значит, $degD_2(4l) \geq 2l-1$.

24.$degD_1(n) = n-1, n-$чётное,

$degD_1(n) = n, n-$нечётное.

Доказательство.

а)$n-$нечётное. Тогда $D_1 \ni x_1 \bigoplus \ldots \bigoplus x_n$, значит $degD_1(n) = n$.

б)$n-$чётное. Тогда $x_1 \bigoplus \ldots \bigoplus x_n \notin D_1$ и $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1 \notin D_1$, значит $degD_1(n) \leq n-1$, но $D_1 \ni x_1 \bigoplus \ldots \bigoplus x_{n-1}$, значит $degD_1(n) = n-1$.

25.$degD_3(n) = n-1, n-$чётное,

$degD_3(n) = n, n-$нечётное.

Доказательсттво аналогично предыдущему пункту.

26.$degA_1(n) = [\frac{n}{2}]$[2,3].

27.$degA_2(n) = [\frac{n}{2}]$[2,3].

28.$degA_3(n) = [\frac{n}{2}]$[2,3].

29.$degA_4(n) = [\frac{n}{2}]$[2,3].

30.$degC_1(n) = n$.

31.$degC_2(n) = n$.

Доказательство.

а)$n-$нечётное. Тогда $C_2 \ni x_1 \bigoplus \ldots \bigoplus x_n$, значит $degC_2(n) = n$.

б)$n-$чётное. Тогда $C_2 \ni x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1$, значит $degC_2(n) = n$.

32.$degC_3(n) = n$.

Доказательство.

$C_3 \ni x_1 \bigoplus \ldots \bigoplus x_n$, значит $degC_3(n) = n$.

33.$degC_4(n) = n-1, n-$чётное,

$degC_4(n) = n, n-$нечётное.

Доказательство.

а)$n-$нечётное. Тогда $C_4 \ni x_1 \bigoplus \ldots \bigoplus x_n$, значит $degC_4(n) = n$.

б)$n-$чётное. Тогда $x_1 \bigoplus \ldots \bigoplus x_n \notin C_4$ и $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1 \notin C_4$, значит $degC_4(n) \leq n-1$, но $C_4 \ni x_1 \bigoplus \ldots \bigoplus x_{n-1}$, значит $degC_4(n) = n-1$.

34. $F_1^{\mu}(n) = n-1$.

Доказательство.

а)$n-$чётное. Тогда $x_1 \bigoplus \ldots \bigoplus x_n \notin F_1^{\mu}$ и $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1 \notin F_1^{\mu}$, значит $degF_1^{\mu}(n) \leq n-1$.

б)$n-$нечётное. Очевидно, что $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1 \notin F_1^{\mu}$. Функция $x_1 \bigoplus \ldots \bigoplus x_n$ является $\alpha-$ функцией, но не удовлетворяет условию

$< a^{\mu} >$,например, на наборах $(1,1,1,\ldots,1,1,0)$ и $(0,1,,1\ldots,1,1,1)$. Значит $degF_1^{\mu}(n) \leq n-1$.

Возьмём

$$H(x) = x_n \bigvee (x_1 \bigoplus \ldots \bigoplus x_{n-1})$$

Очевидно, $H(x) \in degF_1^{\infty} \subset degF_1^{\mu}$. Ограничение $H|_{x_n=0}-$ линейная функция от $n-1$ аргументов, следовательно, разделяющий полином для $H(x)$ имеет степень не меньше $n-1$. Значит $degF_1^{\mu}(n) = n-1$, одновременно доказано $degF_1^{\infty}(n) = n-1$.

35.$[\frac{n-1}{2}] \leq degF_2^{\mu}(n) \leq [\frac{n}{2}]$.

Доказательство.

Класс $degF_2^{\mu} \subset M$, значит $degF_2^{\mu}(n) \leq [\frac{n}{2}]$.

Возьмём функцию $F(x_1,\ldots,x_n)$ следующего вида

$$F(x_1,\ldots,x_n) = x_n \bigvee H(x_1,\ldots,x_{n-1}),$$

где $H(x_1,\ldots,x_{n-1})-$монотонная функция от $n-1$ аргумента, для которого разделяющий полином $h(x_1,\ldots,x_{n-1})$ имеет степень не меньше $[\frac{n-1}{2}]$. Очевидно, что $F(x) \in degF_2^{\infty} \subset degF_2^{\mu}$. Для $F(x)$ в качестве разделяющего полинома $f(x)$ можно взять

$$f(x_1,\ldots,x_n) = x_n + \varepsilon h(x_1,\ldots,x_{n-1}),$$

где $0 < \varepsilon << 1$. Так как $F|_{x_n=0} = H$, то степень полинома понизить нельзя. Это доказательство проходит и для $F_2^{\infty}(n)$.

36.$[\frac{n-1}{2}] \leq degF_3^{\mu}(n) \leq [\frac{n}{2}]$.

Доказательство аналогичное п.35, оно же проходит для $F_3^{\infty}(n)$.

37.$degF_4^{\mu}(n) = n-1$.

Возьмём

$$H(x) = x_n \bigvee (x_1 \bigoplus \ldots \bigoplus x_{n-1})$$

Очевидно, $H(x) \in degF_4^{\infty} \subset degF_4^{\mu}$. Ограничение $H|_{x_n=0}-$ линейная функция от $n-1$ аргументов, следовательно, разделяющий полином для $H(x)$ имеет степень не меньше $n-1$. Разберёмся с двумя линейными функциями от всех аргументов.

а)$n-$ чётное. Функция $x_1 \bigoplus \ldots \bigoplus x_n$ равна 0 на всех единицах, функция $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1$, зануляется на наборах $(0,1,1,\ldots,1,1,1)$ и $(1,1,1,\ldots,1,1,0)$ без общей нулевой компоненты. Обе не лежат в $degF_4^{\mu}(n)$.

б)$n-$ нечётное. Функция $x_1 \bigoplus \ldots \bigoplus x_n$ зануляется на наборах $(0,1,1,\ldots,1,1,1)$ и $(1,1,1,\ldots,1,1,0)$ без общей нулевой компоненты,

функция $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1$ равна 0 на всех единицах. Обе не лежат в $degF_4^\mu(n)$.

Это доказательство проходит и для $F_4^\infty(n)$.

38.$degF_5^\mu(n) = n-1$.

Доказательство.

Разберёмся с двумя линейными функциями от всех аргументов.

а)$n-$ чётное. Функция $x_1 \bigoplus \ldots \bigoplus x_n$ не является $\alpha-$ функцией, функция $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1$, равна 1 на нулевом наборе. Обе не лежат в $F_5^\mu(n)$.

б)$n-$ нечётное. Функция $x_1 \bigoplus \ldots \bigoplus x_n$ равна 1 на наборах $(1,0,\ldots,0)$ и $(0,1,0,\ldots,0)$ без общей единичной компоненты, функция $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1$, равна 0 на всех единицах. Обе не лежат в $F_5^\mu(n)$.

Таким образом, $degF_5^\mu(n) \leq n-1$.

Рассмотрим два случая.

а)$n-$ чётное.

Возьмём

$$H(x) = x_n \cdot (x_1 \bigoplus \ldots \bigoplus x_{n-1})$$

Очевидно, $H(x) \in F_5^\infty \subset F_5^\mu$.Далее, $F|_{x_n=1} = x_1 \bigoplus \ldots \bigoplus x_{n-1}$, следовательно, степень разделяющего полинома не меньше $n-1$.

б)$n-$ нечётное.

Возьмём

$$H(x) = x_n \cdot (x_1 \bigoplus \ldots \bigoplus x_{n-1} \bigoplus 1)$$

Очевидно, $H(x) \in F_5^\infty \subset F_5^\mu$. Далее, $F|_{x_n=1} = x_1 \bigoplus \ldots \bigoplus x_{n-1} \bigoplus 1$, следовательно, степень разделяющего полинома не меньше $n-1$.

В итоге получаем требуемое $degF_5^\mu(n) = n-1$. Это доказательство проходит для $F_5^\infty(n)$.

39.$[\frac{n-1}{2}] \leq degF_6^\mu(n) \leq [\frac{n}{2}]$.

Доказательство.

Класс $degF_6^\mu \subset M$, значит $degF_6^\mu(n) \leq [\frac{n}{2}]$.

Возьмём функцию $F(x_1,\ldots,x_n)$ следующего вида

$$F(x_1,\ldots,x_n) = x_n \cdot H(x_1,\ldots,x_{n-1}),$$

где $H(x_1,\ldots,x_{n-1})-$монотонная функция от $n-1$ аргумента, для которого разделяющий полином $h(x_1,\ldots,x_{n-1})$ имеет степень не меньше $[\frac{n-1}{2}]$. Очевидно, что $F(x) \in degF_6^\infty \subset degF_6^\mu$. Это доказательство проходит и для $F_6^\infty(n)$.

40.$[\frac{n-1}{2}] \leq degF_7^\mu(n) \leq [\frac{n}{2}]$.

Доказательство аналогично п.39, оно же проходит и для $degF_7^\infty(n)$.

41.$degF_8^{\mu}(n) = n - 1$.

Доказательство.

Разберёмся с двумя линейными функциями от всех аргументов.

Функция $x_1 \bigoplus \ldots \bigoplus x_n$ равна 1 на наборах $(1, 0, \ldots, 0)$ и $(0, 1, 0, \ldots, 0)$ без общей единичной компоненты, функция $x_1 \bigoplus \ldots \bigoplus x_n \bigoplus 1$, равна 1 на всех нулях. Обе функции не лежат в $F_8^{\mu}(n)$.

Таким образом, $degF_8^{\mu}(n) \leq n - 1$.

Возьмём

$$H(x) = x_n \cdot (x_1 \bigoplus \ldots \bigoplus x_{n-1})$$

Очевидно, $H(x) \in F_8^{\infty} \subset F_8^{\mu}$.Далее, $F|_{x_n=1} = x_1 \bigoplus \ldots \bigoplus x_{n-1}$, следовательно, степень разделяющего полинома не меньше $n - 1$.

В итоге получаем требуемое $degF_8^{\mu}(n) = n - 1$. Это доказательство проходит для $F_8^{\infty}(n)$.

42.$degF_1^{\infty}(n) = n - 1$.

См.п.34.

43.$[\frac{n-1}{2}] \leq degF_2^{\infty}(n) \leq [\frac{n}{2}]$.

См.п.35.

44.$[\frac{n-1}{2}] \leq degF_3^{\infty}(n) \leq [\frac{n}{2}]$.

См.п.36.

45.$degF_4^{\infty}(n) = n - 1$.

См.п.37.

46.$degF_5^{\infty}(n) = n - 1$.

См.п.38.

47.$[\frac{n-1}{2}] \leq degF_6^{\infty}(n) \leq [\frac{n}{2}]$.

См.п.39.

48.$[\frac{n-1}{2}] \leq degF_7^{\infty}(n) \leq [\frac{n}{2}]$.

См.п.40.

49.$degF_8^{\infty}(n) = n - 1$.

См.п.41.

Автор благодарит Алёшина С.В. за постановку задачи, многочисленные обсуждения в процессе её решения, ценные советы и предложения.

Список литературы

[1] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. Функции алгебры логики и классы Поста. Издательство Наука, Москва, 1966, 119.

[2] Алешин С.В. Распознавание динамических образов. Издательство Московского университета, Москва, 1996, 97.

[3] Носов М.В. Оценка степеней разделяющих многочленов для монотонных и самодвойственных функций. Интеллектуальные системы. Теория и приложения. 27:2 (2023), 79-82.

Degrees of separating polynomials for Post's classes
Nosov M.V.

In this paper, estimates of the degrees of polynomials with real coefficients separating zeros and ones of Boolean functions for Post's classes are obtained. Post's classes, separating polynomial.

References

[1] Yablonsky S.V.,Gavrilov G.,P.,Kudryavtsev V.B., *Functions of the algebra of logic and Post's classes.*, Nauka, Moscow, 1966 (In Russian), 119 c.

[2] Aleshin S.V., *Dynamic image recognition.*, Moscow University Press, Moscow, 1996 (In Russian), 97 c.

[3] Nosov M.V., "Estimates of the degrees of separating polynomials for monotone and self-dual functions.", *Intelligent systems. Theory and Applications*, **27**:2 (2023), 79–82 (In Russian)

Часть 3
Математические модели

Изучение базисов предполных классов линейных 2-адических автоматов

М. Э. Калашников[1]

В настоящей работе проводится изучение предполных классов в классе линейных 2-адических автоматов. Решается задача исследования конечной порожденности предполных классов и поиск их базисов.

Ключевые слова: конечный автомат, p-адическое число, линейный 2-адический автомат, операции композиции, обратная связь, проблема полноты, базис.

Введение.

В настоящее время ведется активная работа по изучению свойств класса конечных автоматов и широкого многообразия его подклассов. Так, в работах [2], [3], [4] решается задача K-полноты для линейных автоматов над конечными полями.

Одним из важных подклассов в множестве конечных автоматов являются p-адические автоматы, изучение которых ведется с работы [5]. В этих работах для изучения автоматов использовался аппарат p-адических чисел. В работе [1] была решена задача K-полноты для класса линейных 2-адических автоматов. Были описаны все предполные классы и показана алгоритмическая разрешимость задачи проверки полноты конечных множеств в этом классе.

В настоящей работе проводится дальнейшее изучение предполных классов в классе линейных 2-адических автоматов. Ставится задача исследования конечной порожденности предполных классов и нахождения их базисов.

1. Постановка задачи.

В данной работе изучаются линейные 2-адические автоматы, вычисляющие линейные функции на кольце целых 2-адических чисел $\mathbb{Z}_2$, коэффициенты которых лежат в подкольце $\mathbb{Z}_{(2)} = \mathbb{Z}_2 \cap \mathbb{Q}$.

[1] *Калашников Максим Эдуардович* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: maxkalash98@gmail.com.

Kalashnikov Maksim Eduardovich — postgraduate, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Определение 1. *Конечный инициальный автомат из P с входным алфавитом E_2^n и выходным алфавитом E_2 называется линейным 2-адическим автоматом, если для определяемого им отображения $f(x_1, \ldots, x_n)$ найдутся такие числа $r_0, r_1, \ldots, r_n \in \mathbb{Z}_{(2)}$, что для любых $\alpha_1, \ldots, \alpha_n$ из $\mathbb{Z}$ выполнено:*

$$f(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} r_i \alpha_i + r_0$$

В этом случае мы говорим, что для функции f имеется разложение:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} r_i x_i + r_0 \tag{1}$$

Всюду в работе будут использоваться следующие обозначения и соглашения. Запись Fb_x обозначает операцию применения обратной связи к переменной x. Запись $\lceil x \rceil$ обозначает наименьшее целое число, не меньшее x. Последовательность $P = \{p_i\}_{i=1}^{\infty}$ содержит все простые числа кроме 2. Мы говорим, что дробь делится на число p, если её числитель делится на p, а знаменатель не делится. В обозначениях равенства 1 положим $U(f) = \{r_i \mid i = 1, 2, ..., n\}$. Пусть A - произвольное числовое множество, тогда введем обозначения:

$$kA = \{ka \mid a \in A\}; \quad k + A = \{k + a \mid a \in A\}; \quad \frac{A}{k} = \left\{ \frac{a}{k} \;\middle|\; a \in A \right\}.$$

Также, всюду в работе будет использоваться следующая лемма, доказанная в [1]:

Лемма 1. *Пусть для функций f и f' выполнено:*

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} r_i x_i + r_0,$$
$$f'(x_{n+1}, \ldots, x_{n+n'}) = \sum_{i=n+1}^{n+n'} r_i x_i + r'_0.$$

Через f_1, f_2, f_3 обозначим функции, получаемые, соответственно, отождествлением переменных x_{n-1} и x_n функции f, переименованием переменных функции f с $x_1, \ldots, x_n$ на $x'_1, \ldots, x'_n$, подстановкой функции f вместо переменной $x_{n+n'}$ функции f'. Если к переменной x_n функции f применима обратная связь, то через f_4 обозначим результат применения обратной связи к этой переменной. Тогда выполнены следующие

равенства:

$$f_1(x_1,\dots,x_n n-1)=\sum_{i=1}^{n-2} r_i x_i+(r_{n-1}+r_n)x_{n-1}+r_0,$$

$$f_2(x'_1,\dots,x'_n)=\sum_{i=1}^{n} r_i x'_i+r_0,$$

$$f_3(x_1,\dots,x_{n+n'-1})=\sum_{i=n+1}^{n+n'-1} r_i x_i+\sum_{i=1}^{n} r_i r_{n+n'} x_i+r'_0+r_{n+n'}r_0,$$

$$f_4(x_1,\dots,x_{n-1})=\sum_{i=1}^{n-1}\frac{r_i}{1-r_n}x_i+\frac{r_0}{1-r_n}.$$

Определим некоторые важные замкнутые классы в L_2:

Определение 2.

$$T_0=\{f\in L_2 \mid \forall x_1,..,x_n\in 2\mathbb{Z}: f(x_1,\dots,x_n)\in 2\mathbb{Z}_{(2)}\}.$$

$$T_1=\{f\in L_2 \mid \forall x_1,..,x_n\in 1+2\mathbb{Z}: f(x_1,\dots,x_n)\in 1+2\mathbb{Z}_{(2)}\}.$$

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

$V_o=\{f\in L_2 \mid f$ *имеет нечетное число непосредственных переменных* $\}$.

$$I=\{f\in L_2 \mid f=\sum_{i=1}^{n} r_i x_i+r_0 \implies \sum_{i=1}^{n}|r_i|\le 1\}.$$

$R_c(p_i)=\{f\in L_2 \mid f$ *имеет не одну существенную переменную,*
$\forall\frac{u}{v}\in U(f):(u,p_i)=p_i\}\cup$
$\{f\in L_2 \mid f$ *имеет одну существенную переменную,*
$\forall\frac{u}{v}\in U(f)\setminus\{0\}:(v,p_i)=1\},\quad p_i\in P.$

$R_d(p_i)=\{f\in L_2 \mid f$ *имеет не одну непосредственную переменную,*
$\forall\frac{u}{v}\in U(f):(u,p_i)=p_i\}\cup$
$\{f\in L_2 \mid f$ *имеет одну непосредственную переменную,* $\forall\frac{u}{v}\in U(f)\cap 2\mathbb{Z}_{(2)}:$
$(u,p_i)=p_i,\ \forall\frac{u}{v}\in U(f)\cap 1+2\mathbb{Z}_{(2)}:(v,p_i)=1\},\quad p_i\in P.$

В работе А.А. Часовских [1] была доказана следующая

Теорема 1. *Перечисленные замкнутые классы образуют критериальную систему предполных классов в* L_2

Теперь мы готовы сформулировать задачу, решаемую в данной работе:

Задача. *Для каждого предполного класса в* L_2 *требуется выяснить, является ли он конечно-порожденным, найти его базис или доказать, что его не существует.*

2. Базисы в предполных классах.

2.1. Класс T_0.

Утверждение 1.

$$f \in T_0 \iff \exists r_1, .., r_n \in \mathbb{Z}_{(2)}, \exists r_0 \in 2\mathbb{Z}_{(2)} : \forall x_1, .., x_n : \\ f(x_1, .., x_n) = \sum_{i=1}^{n} r_i x_i + r_0.$$

Доказательство. Необходимость. Известно, что функция f лежит в L_2. Для неё справедливо разложение $f = \sum_{i=1}^{n} r_i x_i + r_0$ для некоторых $r_0, r_1, \ldots, r_n \in \mathbb{Z}_{(2)}$. Подставляя в функцию $\alpha_1, \ldots, \alpha_n \in 2\mathbb{Z}_{(2)}$, получим, что $\sum_{i=1}^{n} r_i \alpha_i + r_0$ должно лежать в $2\mathbb{Z}_{(2)}$. Но $\sum_{i=1}^{n} r_i \alpha_i \in 2\mathbb{Z}_{(2)}$. Следовательно, r_0 должно лежать в $2\mathbb{Z}_{(2)}$.

Необходимость доказана.

Достаточность легко проверить подстановкой $\alpha_1, \ldots, \alpha_n \in 2\mathbb{Z}_{(2)}$ в приведённое разложение. □

Теорема 2. *Множество* $M = \{x_1 + x_2,\ 2\}$ *является базисом в* T_0.

Доказательство. Для начала получим инвертор $-x$:

$$x_1 + x_2 \in M \implies x_1 + x_2 + x_3 \in K(M) \implies x_1 + 2x_2 \in K(M) \\ \overset{\mathrm{Fb}_{x_2}}{\Longrightarrow} \quad \frac{x_1}{1-2} = -x_1 \in K(M).$$

Используя сумматор и инвертор можем получить

$$kx \in K(M) \quad \forall k \in \mathbb{Z}.$$

Далее, имеем:

$$\forall u \in \mathbb{Z}\ \forall v \in 1 + 2\mathbb{Z}\ \ ux_1 + (1-v)x_2 \in K(M) \\ \overset{\mathrm{Fb}_{x_2}}{\Longrightarrow} \quad \frac{ux_1}{1-(1-v)} = \frac{u}{v}x_1 \in K(M).$$

Таким образом, $\forall r \in \mathbb{Z}_{(2)} \;\; r = \frac{u}{v} : rx \in K(M)$.

В обозначениях утверждения 1 для произвольной функции $f \in T_0$ имеем:

$$\sum_{i=1}^{n} r_i x_i + r'_0 x \in K(M) \implies \text{(подставляя константу 2 вместо переменной } x\text{)}$$

$$\sum_{i=1}^{n} r_i x_i + r_0 \in K(M)$$

Таким образом показано, что $T_0 \subseteq K(M)$. T_0 – замкнутый класс и $M \subseteq T_0$, получаем $K(M) \subseteq T_0$ Следовательно, $T_0 = K(M)$. Учитывая, что $K(\{x_1 + x_2\})$ сохраняет нулевые последовательности, а $K(\{2\})$ содержит лишь функции без существенных переменных, получаем, что M является базисом в T_0. □

2.2. Класс T_1.

Утверждение 2.

$$f \in T_1 \iff \textit{либо } f = \sum_{i=1}^{2n} r_i x_i + \sum_{i=1}^{n'} r'_i x'_i + r_0 \tag{2}$$

$$\textit{для } \exists r_0, r_1, \ldots, r_{2n+1} \in 1 + 2\mathbb{Z}_{(2)} \;\; u \;\exists r'_1, \ldots, r'_{n'} \in 2\mathbb{Z}_{(2)},$$

$$\textit{либо } f = \sum_{i=1}^{2n+1} r_i x_i + \sum_{i=1}^{n'} r'_i x'_i + r'_0 \tag{3}$$

$$\textit{для } \exists r_1, \ldots, r_{2n+1} \in 1 + 2\mathbb{Z}_{(2)} \;\; u \;\exists r'_0, r'_1, \ldots, r'_n \in 2\mathbb{Z}_{(2)}.$$

Доказательство. Необходимость. Известно, что функция f лежит в L_2. Для неё справедливо разложение $f = \sum_{i=1}^{m} \tilde{r}_i \tilde{x}_i + r_0$ для некоторых $r_0, \tilde{r}_1, \ldots, \tilde{r}_n \in \mathbb{Z}_{(2)}$. Подставляя в функцию $\alpha_1, \ldots, \alpha_n \in 1 + 2\mathbb{Z}_{(2)}$, получим, что сумма $\sum_{i=1}^{m} r_i \alpha_i + r_0$ должна лежать в $1 + 2\mathbb{Z}_{(2)}$. Слагаемые с коэффициентами из $2\mathbb{Z}_{(2)}$ не влияют на принадлежность всей суммы $1+2\mathbb{Z}_{(2)}$. Обозначим их количество через n' и вычтем из суммы. Переобозначив оставшиеся коэффициенты через $\hat{r}_j$, получим, что $\sum_{i=1}^{m'} \hat{r}_i \alpha_i + r_0$ должно лежать в $1 + 2\mathbb{Z}_{(2)}$. Рассмотрим два случая:

Случай 1 : $r_0 \in 1+2\mathbb{Z}_{(2)}$. Тогда, для нечетности всей суммы, m' должно быть четным, то есть верно разложение (2)

Случай 2 : $r_0 \in 2\mathbb{Z}_{(2)}$. Тогда, для нечетности всей суммы, m' должно быть нечетным, то есть верно разложение (3)

Необходимость доказана.

Достаточность легко проверить подстановкой $\alpha_1, \ldots, \alpha_n \in 1 + 2\mathbb{Z}$ в приведённые разложения. □

Теорема 3. *В классе T_1 существует базис $\{x_1 + x_2 + x_3,\ 1\}$.*

Доказательство. Верна следующая цепочка рассуждений:

$$\begin{aligned} x_1 + x_2 + x_3 \in T_1 &\implies x_1 + 2x_2 \in K(M) \overset{\mathrm{Fb}_{x_2}}{\implies} -x \in K(M) \\ &\implies (1 + 2k)x_1 - 2lx_2 \in K(M) \quad \forall k, l \in \mathbb{Z} \\ &\overset{\mathrm{Fb}_{x_2}}{\implies} \forall r \in 1 + 2\mathbb{Z}_{(2)}, r = \frac{2k+1}{2l+1} : rx \in K(M). \end{aligned}$$

С помощью сумматора, умножения на $r \in 1 + 2\mathbb{Z}_{(2)}$ и подстановки 1 можем получить произвольную функцию вида $\sum_{i=1}^{m_1} r_i x_i + \sum_{i=1}^{m_2} r'_i$ с нечетным числом $(m_1 + m_2)$ слагаемых, коэффициенты и свободные члены которой лежат в $1 + 2\mathbb{Z}_{(2)}$.

В обозначениях утверждения 2 для произвольной функции $f \in T_1$ имеется два случая:

$$\begin{aligned} \text{Функция имеет вид (2)} \implies f &= \sum_{i=1}^{2n} r_i x_i + \sum_{i=1}^{n'} r'_i x'_i + r_0 = \\ &= \sum_{i=1}^{2n} r_i x_i + \sum_{i=1}^{n'} (2r'_i - 1)x'_i + \sum_{i=1}^{n'} (1 - r'_i)x'_i + r_0. \end{aligned}$$

$$\begin{aligned} \text{Функция имеет вид (3)} \implies f &= \sum_{i=1}^{2n+1} r_i x_i + \sum_{i=1}^{n'} r'_i x'_i + r'_0 = \\ &= \sum_{i=1}^{2n+1} r_i x_i + \sum_{i=1}^{n'} (2r'_i - 1)x'_i + \sum_{i=1}^{n'} (1 - r'_i)x'_i + (2r_0 - 1) + (1 - r_0). \end{aligned}$$

Вспоминая, что $r_i \in 1 + 2\mathbb{Z}_{(2)}$ и $r'_i \in 2\mathbb{Z}_{(2)}$, можем видеть, что в обоих случаях функция f представляется в виде суммы нечетного числа слагаемых с коэффициентами и свободными членами из $1 + 2\mathbb{Z}_{(2)}$, следовательно $T_1 \subseteq K(M)$. T_1 – замкнутый класс и $M \subseteq T_1$, получаем $K(M) \subseteq T_1$. Следовательно, $T_1 = K(M)$. Учитывая, что $K(\{x_1 + x_2 + x_3\})$ сохраняет нулевые последовательности, а $K(\{1\})$ содержит лишь функции без существенных переменных, получаем, что M является базисом в T_0. □

2.3. Класс V_1.

Утверждение 3.

$$f \in V_1 \iff f = rx + \sum_{i=1}^{n} 2r_i x_i + r_0 \text{ для } \exists r, r_0, r_1, \ldots, r_n \in \mathbb{Z}_{(2)}$$

Доказательство. Необходимость. Известно, что функция f лежит в L_2. Для неё справедливо разложение $f = \sum_{i=1}^{m} \tilde{r}_i \tilde{x}_i + r_0$ для некоторых $r_0, \tilde{r}_1, \ldots, \tilde{r}_n \in \mathbb{Z}_{(2)}$. Известно, что у неё не более одной непосредственной переменной. Обозначим эту переменную через x. Тогда коэффициенты при остальных переменных должны делиться на 2. Что и требовалось. Необходимость доказана.

Достаточность же очевидна из приведеного разложения. □

Теорема 4. *Класс V_1 имеет базис $\{x_1 + 2x_2,\ 0,\ x + 1\}$.*

Доказательство. Верна следующая цепочка рассуждений:

$$\begin{aligned}
x_1 + 2x_2 \in M &\overset{\mathrm{Fb}_{x_2}}{\Longrightarrow} -x \in K(M);\\
x_1 + 2x_2 \in M &\Longrightarrow x_1 + 2kx_1 = (2k+1)x_1 \in K(M);\\
(2k+1)x_1 - 2lx_2 \in K(M) &\overset{\mathrm{Fb}_{x_2}}{\Longrightarrow} \frac{2k+1}{2l+1}x \in K(M) \Longrightarrow\\
&\Longrightarrow rx \in K(M),\ \forall r \in 1 + 2\mathbb{Z}_{(2)};\\
0 \in M, x_1 + 2x_2 \in M &\Longrightarrow 2x \in K(M);\\
rx \in K(M), 2x \in K(M) &\Longrightarrow \tilde{r}x \in K(M),\ \forall \tilde{r} \in \mathbb{Z}_{(2)};\\
x + 1, rx \in K(M),\ \forall r \in 1 + 2\mathbb{Z}_{(2)} &\Longrightarrow r(\frac{x}{r} + 1) = x + r \in K(M) \Longrightarrow\\
\Longrightarrow x + r + \cdots + r \in K(M) &\Longrightarrow x + \hat{r} \in K(M),\ \forall \hat{r} \in \mathbb{Z}_{(2)}.
\end{aligned}$$

В обозначениях утверждения 3 для произвольной функции $f \in V_1$ имеем:

$$rx + \sum_{i=1}^{n} 2r_i x_i + r_0 \in K(M)$$

Таким образом показано, что $V_1 \subseteq K(M)$. V_1 – замкнутый класс и $M \subseteq V_1$, значит $K(M) \subseteq V_1$ Следовательно, $V_1 = K(M)$. Учитывая, что $K(\{x_1 + 2x_2, 0\})$ сохраняет 0 в начальный момент времени, $K(\{x_1 + 2x_2, 1\})$ сохраняет 1 в начальный момент времени, $K(\{0, 1\})$ содержит лишь функции без существенных переменных, окончательно имеем, что M является базисом в V_1. □

2.4. Класс V_o.

Утверждение 4.

$$f \in V_o \iff f = \sum_{i=1}^{2n+1} r_i x_i + \sum_{i=1}^{n} 2r'_i x'_i + r_0$$
$$\text{для } \exists r_0, r'_1, \ldots, r'_n \in \mathbb{Z}_{(2)} \ u \ \exists r_1, \ldots, r_{2n+1} \in (1 + 2\mathbb{Z}_{(2)}) \setminus \{0\}.$$

Доказательство. Необходимость. Известно, что функция f лежит в L_2. Для неё справедливо разложение $f = \sum_{i=1}^{m} \tilde{r}_i \tilde{x}_i + r_0$ для некоторых $r_0, \tilde{r}_1, \ldots, \tilde{r}_n \in \mathbb{Z}_{(2)}$. Известно, что у неё нечетное число непосредственных переменных. Обозначим их через x_i. Тогда коэффициенты при них должны быть нечетными. Остальные же переменные обозначим через x'_j; коэффициенты при них должны делиться на 2. Что и требовалось. Необходимость доказана.

Достаточность же очевидна из приведеного разложения. □

Теорема 5. *Класс V_o имеет базис $\{x_1 + x_2 + x_3,\ x + 1\}$.*

Доказательство. Положим $V_o^{(0)} = \{f \in V_o | r_0 = 0\}$ – множество однородных функций из V_o. Из утверждений 4 и 2 легко видеть, что $V_o^{(0)} \subset T_1$, поэтому, аналогично случаю T_1, с помощью функции $x_1 + x_2 + x_3$, можем получить произвольную функцию из $V_o^{(0)}$. Кроме того, с помощью функции $x + 1$, можем получить добавление произвольной константы из $\mathbb{Z}_{(2)}$:

$$\forall r \in 1 + 2\mathbb{Z}_{(2)} : r = \frac{2u+1}{2v+1}, \quad u, v \in \mathbb{Z}_{(2)} : rx, \frac{1}{r}x \in K(M) \implies$$
$$\implies \forall r \in 1 + 2\mathbb{Z}_{(2)} : r(\frac{x}{r} + 1) = x + r \in K(M) \implies$$
$$\implies x + r + \cdots + r \in K(M) \implies \forall \hat{r} \in \mathbb{Z}_{(2)} : \ x + \hat{r} \in K(M)$$

Таким образом показано, что $V_o \subseteq K(M)$. V_o – замкнутый класс и $M \subseteq V_o$, получаем $K(M) \subseteq V_o$ Следовательно, $V_o = K(M)$. Учитывая, что $K(\{x_1 + x_2 + x_3\}) \subset T_1 \cap V_o$, а $K(\{x+1\})$ содержит только функции с не более чем одной существенной переменной, получаем, что M является базисом в V_o. □

2.5. Класс I

Теорема 6. *Класс I имеет базис $\{\frac{1}{3}x_1 + \frac{1}{3}x_2 + \frac{1}{3}x_3,\ -x,\ x + 1,\ 0\}$.*

Доказательство. Для начала получим все однородные функции из I. Возьмем произвольное нечетное натуральное число V и положим $T = \lceil \log_3 V \rceil$.

$$\sum_{i=1}^{3^T} \frac{x_i}{3^T} \in K(M) \implies \sum_{i=1}^{V} \frac{x_i}{3^T} + \frac{3^T - V}{3^T} x_{V+1} \in K(M)$$

$$\overset{\mathrm{Fb}_{x_V}}{\Longrightarrow} \text{ (} 3^T - V \text{ - четное число)} \frac{1}{1 - \frac{3^T - V}{3^T}} \sum_{i=1}^{V} \frac{x_i}{3^T} = \sum_{i=1}^{V} \frac{\frac{x_i}{3^T}}{\frac{V}{3^T}} = \sum_{i=1}^{V} \frac{x_i}{V} \in K(M).$$

Пусть $f = \frac{u_1}{v_1} x_1 + \cdots + \frac{u_n}{v_n} x_n$ - произвольная однородная функция из I. $\sum_{i=1}^{n} \frac{|u_i|}{|v_i|} \leq 1$. Положим $V = v_1 \cdot \ldots \cdot v_n \implies f_0 = \sum_{i=1}^{V} \frac{x_i}{V} \in K(M)$. Без ограничения общности (так как $-x \in M$) можно считать, что $u_i > 0,\ v_i > 0$, тогда:

$$\sum_{i=1}^{n} \frac{u_i}{v_i} \leq 1 \implies \sum_{i=1}^{n} \frac{u_i}{v_i} V \leq V$$

Далее, мы можем разбить слагаемые f_0 на группы, соответствующие переменным функции f, подставив вместо ненужных переменных $0 \in M$. Затем отождествить переменные внутри каждой из групп:

$$f_0 = \sum_{i=1}^{V} \frac{x_i}{V} \in K(M) \Rightarrow \sum_{i=1}^{\frac{u_1}{v_1} V} \frac{x_1}{V} + \cdots + \sum_{i=1}^{\frac{u_n}{v_n} V} \frac{x_n}{V} = \frac{u_1}{v_1} x_1 + \cdots + \frac{u_n}{v_n} x_n = f \in K(M)$$

Осталось получить функцию, осуществляющую добавление произвольного свободного члена. Для этого достаточно показать, что для произвольного нечетного натурального v выполняется $x + \frac{1}{v} \in K(M)$. Рассмотрим три возможных случая:

Случай 1 : $(v, 3) = 1$

Положим $T = \lceil \log_3 V \rceil$; $\quad \sum_{i=1}^{3^T} \frac{x_i}{3^T} + 1 \in K(M) \implies$

$$\implies \sum_{i=1}^{v} \frac{x_i}{3^T} + \frac{3^T - v}{3^T} x_{v+1} + 1 \in K(M) \overset{\text{Fb}_{x_{v+1}}}{\Longrightarrow}$$

$$\overset{\text{Fb}_{x_{v+1}}}{\Longrightarrow} \sum_{i=1}^{v} \frac{\frac{x_i}{3^T}}{\frac{v}{3^T}} + \frac{3^T}{v} = x + \frac{3^T}{v} \in K(M).$$

$(v, 3^T) = 1 \implies \exists a \in \mathbb{Z},\ \exists b \in \mathbb{N} : av + b3^T = 1 \implies a + b\frac{3^T}{v} = \frac{1}{v}$

$\implies$ Добавляя или вычитая a раз единицу и добавляя b раз $\frac{3^T}{v}$,

получим окончательно: $x + \frac{1}{v} \in K(M)$.

Случай 2 : $v = 3^T$

Положим p - некоторое простое число, $p > 3^T$; $\sum_{i=1}^{p} \frac{x_i}{p} + 1 \in K(M) \implies$

$$\implies \sum_{i=1}^{3^T} \frac{x_i}{p} + \frac{p - 3^T}{p} x_{3^T+1} + 1 \in K(M) \overset{\text{Fb}_{x_{3^T+1}}}{\Longrightarrow}$$

$$\overset{\text{Fb}_{x_{3^T+1}}}{\Longrightarrow} \sum_{i=1}^{3^T} \frac{\frac{x_i}{p}}{\frac{3^T}{p}} + \frac{p}{3^T} = x + \frac{p}{3^T} \in K(M)$$

$(3^T, p) = 1 \implies \exists a \in \mathbb{Z},\ \exists b \in \mathbb{N} : a3^T + bp = 1 \implies a + b\frac{p}{3^T} = \frac{1}{3^T}$

$\implies$ Добавляя или вычитая a раз единицу и добавляя b раз $\frac{p}{3^T}$,

получим окончательно: $x + \frac{1}{3^T} \in K(M)$.

Случай 3 : $v = 3^T v', (v', 3) = 1$

$(3^T, v') = 1 \implies \exists a \in \mathbb{Z},\ \exists b \in \mathbb{N} : a3^T + bv' = 1 \implies \frac{a}{v'} + \frac{b}{3^T} = \frac{1}{3^T v'}$

$\implies$ Добавляя или вычитая a раз $\frac{1}{v'}$ и добавляя b раз $\frac{1}{3^T}$,

получим окончательно: $x + \frac{1}{v} \in K(M)$.

Таким образом показано, что $I \subseteq K(M)$. I – замкнутый класс и $M \subseteq I$, получаем $K(M) \subseteq I$. Следовательно, $I = K(M)$. Покажем, что M – базис. Для этого проверим подножества M.

$K(\{-x,\ x+1,\ 0\})$ содержит только функции не более чем с одной существенной переменной.

$K(\{\frac{1}{3}x_1+\frac{1}{3}x_2+\frac{1}{3}x_3,\ x+1,\ 0\})$ содержит только функции из I с положительными коэффициентами в разложении (1). Доказательство можно провести индукцией по построению: для отождествления, переименования и подстановки переменных утверждение очевидно, а при применении обратной связи все коэффициенты будут умножены на множитель $\frac{1}{1-r}$, который является положительным так как $0 < r < 1$.

$K(\{\frac{1}{3}x_1+\frac{1}{3}x_2+\frac{1}{3}x_3,\ -x,\ 0\})$ сохраняет нулевые последовательности.

$K(\{\frac{1}{3}x_1+\frac{1}{3}x_2+\frac{1}{3}x_3,\ -x,\ x+1\})$ содержится в $V_o \cap I$.

Таким образом, доказано, что M является базисом в I. □

2.6. Класс $R_c(p_i)$.

Утверждение 5.

$$f \in R_c(p_i) \iff \textit{либо } f = rx + r_0 \tag{4}$$
$$\textit{для } \exists r_0 \in \mathbb{Z}_{(2)},\ \exists r \in \mathbb{Z}_{(2)} \setminus \left(\frac{\mathbb{Z}_{(2)}}{p_i} \cup p_i\mathbb{Z}_{(2)}\right),$$
$$\textit{либо } f = \sum_{j=1}^{n} p_i r_j x_j + r_0 \tag{5}$$
$$\textit{для } \exists r_0 \in \mathbb{Z}_{(2)},\ \exists r_1, \ldots, r_n \in \mathbb{Z}_{(2)} \setminus \frac{\mathbb{Z}_{(2)}}{p_i}, n \geq 2.$$

Доказательство. Необходимость. Известно, что функция f лежит в L_2. Для неё справедливо разложение $f = \sum_{i=1}^{m} \tilde{r}_i\tilde{x}_i + r_0$ для некоторых $r_0, \tilde{r}_1, \ldots, \tilde{r}_n \in \mathbb{Z}_{(2)}$. Если у нее только одна существенная переменная, обозначим её через x и знаменатель коэффициента при ней не должен делиться на p_i, следовательно справедливо либо разложение (4) при наличии нескольких непосредственных переменных, либо разложение (5), при наличии лишь одной непосредственной переменной. Если же существенных переменных несколько, все коэффициенты при них должны делиться на p_i, то есть верно разложение (5).

Достаточность же очевидна из вида приведенных разложений. □

Определение 3. *В обозначениях утверждения 5 введем два множества:*

$$R_1(p_i) = \{f \in R_c(p_i) \mid f \textit{ имеет вид } (4)\}$$
$$R_p(p_i) = \{f \in R_c(p_i) \mid f \textit{ имеет вид } (5)\}$$

Легко видеть, что верно следующее

Замечание. *$R_1(p_i)$ и $R_p(p_i)$ являются замкнутыми классами, причем:*

$$R_1(p_i) \cup R_p(p_i) = R_c(p_i); \quad R_1(p_i) \cap R_p(p_i) = \{f \in R_c(p_i) \mid f \equiv \text{const}\}$$

Лемма 2. *Если для построения $f \in R_c(p_i)$ используется функция из $R_p(p_i)$, тогда $f \in R_p(p_i)$.*

Доказательство. Пусть $f \in R_p(p_i)$. Легко видеть, что операции суперпозиции и обратной связи не выводят за пределы класса $R_p(p_i)$. Рассмотрим функцию $g = rx + r_0 \in R_1(p_i)$. При подстановке g вместо одной из переменных f получим функцию из $R_p(p_i)$. При подстановке f вместо переменной x функции g тоже получим функцию из $R_p(p_i)$. Применяя индукцию по построению, получаем утверждение леммы. □

Лемма 3. *Пусть M – порождающее множество для $R_c(p_i)$. Тогда для всякого натурального n_0 :* $\exists n \in \mathbb{N}, n \geq n_0$:
$\exists r_1, \ldots, r_n \in \mathbb{Z}_{(2)} \setminus \left(\frac{\mathbb{Z}_{(2)}}{p_i} \cup 2\mathbb{Z}_{(2)} \cup p_i\mathbb{Z}_{(2)}\right)$, $\exists f_0 \in R_p(p_i)$:

$$f = \sum_{j=1}^{n} p_i r_j x_j + f_0(x'_1, \ldots, x'_m) \in M.$$

Другими словами, в произвольном порождающем множестве найдется функция, у которой как минимум n переменых с коэффициентами, не делящимися на p_i^2 и 2.

Доказательство. Предположим обратное. Пусть существует $n_0 \in \mathbb{N}$ такое, что $\forall n \geq n_0$ в M нет функции с обозначенными условиями. Тогда $px_1 + \cdots + px_{n_0} \notin K(M)$. Действительно, в $R_c(p_i)$ нет функций, которые бы позволи делить коэффициенты на 2 и на p_i. При этом, при подстановке одной функции из $M \cap R_p(p_i)$ в другую, в новой функции коэффициенты при добавленных переменных будут делится на p_i^2. Использование же функций из $M \cap R_1(p_i)$ не увеличит количество переменных в сумме. Таким образом, $px_1 + \cdots + px_{n_0} \notin K(M)$, но $px_1 + \cdots + px_{n_0} \in R_c(p_i)$. Получили противоречие. □

Таким образом, верно следующее

Следствие 1. *Класс $R_c(p_i)$ не имеет конечного порождающего множества.*

Теорема 7. *Класс $R_c(p_i)$ не имеет базиса.*

Доказательство. Для доказательства теоремы покажем, что для произвольного порождающего множества M найдется функция $f \in M$ такая, что $M \setminus \{f\}$ тоже является порождающим для $R_c(p_i)$. Возьмем произвольную функцию f_1, существование которой гарантируется леммой 3. Она имеет вид:

$$f_1 = \sum_{j=1}^{n} p_i s_j x_j + f_0(x'_1, \ldots, x'_m)$$

Также по лемме 3 найдется функция f_2 для которой верно, что $k > m + n$:

$$f_2 = \sum_{j=1}^{k} p_i r_j x_j + \tilde{f}_0(x'_1, \ldots, x'_m)$$

Подставив в функцию f_2 нули на место переменных $x'_1, \ldots, x'_m$ получим функцию $\tilde{f}_2 = \sum_{j=1}^{k} p_i r_j x_j$. Учитывая, что $r_j \in \mathbb{Z}_{(2)} \setminus (\frac{\mathbb{Z}_{(2)}}{p_i} \cup 2\mathbb{Z}_{(2)} \cup p_i\mathbb{Z}_{(2)})$, имеем $\frac{x}{r_j} \in K(M)$. Кроме того, по лемме 2 для построения этих функций могут быть использованы только функции из $M \cap R_1(p_i)$. Таким образом, можем получить функции $f_+ = p_i x_1 + \cdots + p_i x_k$ и $f_{p_i} = p_i x$. Также, из $M \cap R_1(p_i)$, так как M - порождающее множество, можем получить $f_{r_0} = x + r_0$ для $\forall r_0 \in \mathbb{Z}_{(2)}$.

Построим теперь функцию f_1. Так как $f_0 \in R_p(p_i)$:

$$f_1 = \sum_{j=1}^{n} p_i s_j x_j + \sum_{j=1}^{m} p_i s'_j x'_j + r_0, \quad s'_j \in \mathbb{Z}_{(2)} \setminus \frac{\mathbb{Z}_{(2)}}{p_i}$$

С помощью функций из $R_1(p_i)$ и f_{p_i} можем построить функции $s_j x$ и $s'_j x$. Подставив их в функцию f_+ и применив f_{r_0}, получим окончательно функцию f_1, причем для её построения использовались только f_2 и функции из $K(R_1(p_i) \cap M)$. Таким образом, $M \setminus \{f_1\}$ является порождающим для $R_c(p_i)$. □

2.7. Класс $R_d(p_i)$.

Утверждение 6.

$$f \in R_c(p_i) \iff \textit{либо } f = rx + \sum_{j=1}^{n} 2p_i r_j x_j + r_0 \tag{6}$$

$$\textit{для } \exists r_0 \in \mathbb{Z}_{(2)},\ \exists r, r_1, \ldots, r_n \in \mathbb{Z}_{(2)} \setminus \frac{\mathbb{Z}_{(2)}}{p_i},\ (r, p_i) = 1,$$

$$\textit{либо } f = \sum_{j=1}^{n} p_i r_j x_j + r_0 \tag{7}$$

$$\textit{для } \exists r_0 \in \mathbb{Z}_{(2)},\ \exists r_1, \ldots, r_n \in \mathbb{Z}_{(2)} \setminus \frac{\mathbb{Z}_{(2)}}{p_i}.$$

Доказательство. Необходимость. Известно, что функция f лежит в L_2. Для неё справедливо разложение $f = \sum_{i=1}^{m} \tilde{r}_i \tilde{x}_i + r_0$ для некоторых $r_0, \tilde{r}_1, \ldots, \tilde{r}_n \in \mathbb{Z}_{(2)}$. Если у нее только одна непосредственная переменная, обозначим её x и знаменатель коэффициента при ней не должен делиться на p_i, остальные же переменные должны делиться на $2p_i$, следовательно справедливо разложение (6). Если же непосредственных переменных несколько, все коэффициенты при них должны делиться на p_i, то есть верно разложение (7).

Достаточность же очевидна из приведеного разложения. □

Определение 4. *В обозначениях утверждения 6 введем два множества:*

$$R_2(p_i) = \{f \in R_f(p_i) \mid f \text{ имеет вид (6)}\}$$
$$R_p(p_i) = \{f \in R_f(p_i) \mid f \text{ имеет вид (7)}\}$$

Легко видеть, что верно следующее

Замечание. *$R_2(p_i)$ и $R_p(p_i)$ являются замкнутыми классами.*

Лемма 4. *Класс $R_d(p_i)$ имеет порождающее множество:*

$$\{p_i x_1 + .. + p_i x_n,\ -x,\ x_1 + 2p_i x_2,\ 3x,\ 5x,\ \ldots,\ (2p_i - 1)x,\ x + \frac{1}{p_i^T},\ \frac{x}{p_j} \mid$$
$$n \in \mathbb{N}, T \in \mathbb{Z}_+, p_j \in P,\ p_j \not\equiv \pm 1 \pmod{2p_i}, p_j \neq p_i\}.$$

Доказательство. Верна следующая цепочка рассуждений

$$-x \in M,\ \ x_1 + 2p_i k x_2 \in K(M) \overset{\mathrm{Fb}_{x_2}}{\Longrightarrow} \frac{x}{1 + 2p_i \tilde{k}}\ \ \forall k \in \mathbb{Z};$$
$$\forall l \in \{3, 5, \ldots, 2p_i - 1\}\ lx \in M,\ \ (x + 2p_i k x) \in K(M) \implies$$
$$\implies kx \in K(M) \forall k \in 1 + 2\mathbb{Z};$$
$$\forall p_j \not\equiv \pm 1(\mod 2p_i),\ p_j \neq p_i : \ \frac{x}{p_j} \in M \text{ и полученное выше} \implies$$
$$\implies rx \in K(M)\ \ \forall r \in \left(1 + 2\mathbb{Z}_{(2)}\right) \setminus \frac{\mathbb{Z}_{(2)}}{p_i};$$
$$x_1 + \sum_{j=1}^{n} 2p_i x_j \in K(M) \implies rx + \sum_{l=1}^{n} 2p_i r_l x_l \in K(M);$$
$$p_i x_1 + \cdots + p_i x_n \in M \implies \sum_{l=1}^{n} p_i r_l x_l \in K(M);$$
$$\forall T \in \mathbb{Z}_+ : r\left(\frac{x}{r} + \frac{1}{p_i^T}\right) = x + \frac{r}{p_i^T} \in K(M),\ (r, p_i) = 1,\ (r, 2) = 1 \implies$$
$$\implies \text{(прибавляя нужное число раз) } \forall r_0 \in \mathbb{Z}_{(2)} x + r_0 \in K(M). \qquad \square$$

Лемма 5. *Пусть M – порождающее множество для $R_c(p_i)$. Тогда для всякого натурального n_0 : $\exists n \in \mathbb{N}, n \geq n_0 : \exists r, r_1, \ldots, r_n \in \mathbb{Z}_{(2)} \setminus \left(\frac{\mathbb{Z}_{(2)}}{p_i} \cup 2\mathbb{Z}_{(2)} \cup p_i\mathbb{Z}_{(2)}\right)$, $\exists f_0, g_0 \in R_p(p_i), g(0) = 0$:*

$$f = \sum_{j=1}^{n} p_i r_j x_j + f_0(x'_1, \ldots, x'_m) \in M,$$

$$g = g_0(x_1, \ldots, x_k) + \frac{r}{p_i^n} \in M$$

Доказательство. Существование f доказывается аналогично лемме 3. В $R_d(p_i)$ не существует функций, позволяющих делить коэффициенты на p_i и на 2. Если t_0 - максимальная степень p_i в знаменателе свободных членов в M, то мы не сможем получить функцию $x + \frac{1}{p_i^{t_0+1}}$, откуда следует утверждение о существовании функции $g \in M$. □

Следствие 2. *Класс $R_d(p_i)$ не имеет конечного порождающего множества.*

Теорема 8. *Класс $R_d(p_i)$ не имеет базиса.*

Доказательство. Для начала выразим из M функции $M_0 = \{-x,\ x-1$ $x_1 + 2p_i x_2,\ 3x, 5x,\ \ldots,\ (2p_i - 1)x\}$. Для этого потребуется конечное число функций из M; в дальнейшем мы не будем трогать эти функции.

Теперь получим функции $\frac{x}{p_0}$ для всякого простого p_0, такого что $p_0 \not\equiv \pm 1(\mod p_i)$. Покажем, что для их построения не требуются функции вида (7). Вспомним, как выглядят функции вида (6) и (7):

$$f = rx + \sum_{j=1}^{n} 2p_i r_j x_j + r_0 \qquad (6)$$

$$f = \sum_{j=1}^{n} p_i r_j x_j + r_0 \qquad (7)$$

При применении операций композиции к функциям вида (7), их вид не поменяется. При подстановке функции вида (7) вместо переменной x функции вида (6) получится функция вида (7). При подстановке функции вида (7) вместо переменной x_j функции вида (6) получится функция вида (6), однако коэффициент r не изменится.

Применение обратной связи к непосредственной переменной x_j функции вида (6) умножит коэффициент при переменной x на $\frac{k}{1+2lp}$ для некоторых $k \in 1 + 2\mathbb{Z}, l \in \mathbb{Z}$. Но $krx + 2lx_1 \in K(M_0)$, следовательно и $\frac{k}{1+2lp} rx \in K(M_0)$. А значит, применение операции подстановки функции вида (7) вместо переменной x_j функции вида (6), с точки зрения

влияния на коэффициент при переменной x, может быть заменено на применение ряда операций композиции к функциям из M_0. Что и требовалось. Таким образом, было построено множество:

$$M_1 = \{-x, x-1, x_1+2p_ix_2,\ 3x, 5x,\ \ldots, (2p_i-1)x, \frac{x}{p_j} \mid p_j \not\equiv \pm 1 \ (\mod 2p_i)\}$$

Причем, для его построения из множества $M \cap R_p(p_i)$ потребовалось лишь конечное множество функций. Назовем его R_0. Из доказательства леммы 4:

$$\forall r \in \mathbb{Z}_{(2)} \setminus \left(\frac{\mathbb{Z}_{(2)}}{p_i} \cup 2\mathbb{Z}_{(2)} \cup p_i\mathbb{Z}_{(2)}\right): \quad rx \in K(M_1), \quad \frac{x}{r} \in K(M_1)$$

Возьмем произвольную функцию f, существование которой гарантируется леммой 5 и которая не принадлежит R_0. Она имеет вид:

$$f = \sum_{j=1}^{n} p_i s_j x_j + f'(x'_1, \ldots, x'_m)$$

Пусть t_0 – степень p_i в знаменателе свободного члена f' . Также по лемме 3 найдется функция:

$$f_1 = \sum_{j=1}^{k} p_i r_j x_j + f'_1(x'_1, \ldots, x'_m)$$

Для неё верно, что $k \geq m + n + 1$. И найдется функция $g = g_0(x_1, \ldots, x_k) + \frac{r_g}{p_i^l}$ для которой верно, что $l \geq t_0 + 1$.

Аналогично теореме 8 из функции f_1 получим $f_+ = p_ix_1 + \cdots + p_ix_{m+n+1}$ и $f_p = p_ix$.

Подставим на входы всех переменных функции g нули и подставим результат в функцию $\frac{x}{r_g}$. Получим константу $\frac{1}{p^l}$.

Построим теперь функцию f. Так как $f' \in R_p(p_i)$,

$$f = \sum_{j=1}^{n} p_i s_j x_j + + \sum_{j=1}^{m} p_i s'_j x'_j + \frac{s'_0}{p^{t_0}}, \quad s'_j \in \mathbb{Z}_{(2)} \setminus \frac{\mathbb{Z}_{(2)}}{p_i}$$

С помощью функций из $K(M_0)$ можем построить функции s_jx и s'_jx. Также уже построили $\frac{1}{p^l}$ Подставив их в функцию f_+, получим окончательно функцию f, причем для её построения использовались только f_1, g и функции из $K(M_2)$. Таким образом, $M \setminus \{f_1\}$ является порождающим для $R_d(p_i)$.

□

Заключение.

В работе исследованы базисы в предполных классах L_2. Для предполных классов T_0, T_1, V_o, V_1, I были найдены базисы. Для двух бесконечных серий предполных классов $R_c(p_i)$ и $R_d(p_i)$ было продемонстрировано отсутствие конечных порождающих систем, равно как и отсутствие базисов.

Автор выражает благодарность профессору А.А. Часовских за помощь в постановке задачи и содействие в подготовке статьи.

Список литературы

[1] А. А. Часовских, "О полноте в классе линейных 2-адических автоматов", *Интеллектуальные системы. Теория и приложения*, **20**:4 (2016), 209–227.

[2] А. А. Часовских, "Об алгоритмической разрешимости проблемы полноты для линейных автоматов", *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 1986, № 3, 82–84.

[3] А. А. Часовских, "Проблема полноты для класса линейно-автоматных функций", *Дискрет. матем.*, **27**:2 (2015), 134–151; *Discrete Math. Appl.*, **26**:2 (2016), 89–104.

[4] А. А. Часовских, "Проблема полноты в классах линейных автоматов", *Интеллектуальные системы. Теория и приложения*, **22**:2 (2018), 151–153.

[5] А. Г. Лунц, "Конечные p-адические автоматы", *Докл. АН СССР*, **150**:4 (1963), 755–758.

Study of bases in precomplete classes of the set of linear 2-adic automata

Kalashnikov M.E.

The present paper considers precomplete classes in the class of linear 2-adic automata. The paper provides the study of bases for each precomplete class.

Keywords: finite automaton, p-adic number, linear 2-adic automaton, compositional operations, feedback, completeness problem, basis.

References

[1] Chasovskikh A. A., "Completeness problem in the class of linear 2-adic automata", *Intelligent systems*, **20**:4 (2016), 209–227 (In Russian).

[2] Chasovskikh A. A., "Algorithmic solvability of the completeness problem for linear automata", *Vestnik Moskov. Univ. Ser. I Mat. Mekh.*, 1986, № 3, 82–84 (In Russian).

[3] Chasovskikh A. A., "Completeness problem for the class of linear automata functions", *Discrete Math. Appl.*, **26**:2 (2016), 89–104 (In Russian).

[4] Chasovskikh A. A., "Completeness problem in the classes of linear automata", *Intelligent systems*, **22**:2 (2018), 151–153 (In Russian).

[5] Lunts A. G., "Finite p-adic automata", *Dokl. Akad. Nauk SSSR*, **150**:4 (1963), 755–758 (In Russian).

О свойстве аддитивного сдвига для линейной реализуемости автоматов

С. Б. Родин[1]

Одним из необходимых условий для линейной реализуемости автомата является выполнения условия «аддитивного сдвига» на порождающих внутренней полугруппы автомата. «Аддитивный сдвиг» задается отображением на множестве состояний автомата. В данной работе изучаются такие отображения. Приведены свойства, которыми должно обладать отображение, чтобы задавать «аддитивный сдвиг». Так же показано, что такие отображения линейно реализуемы посредством неизбыточных кодирований и приведен явный вид получаемого оператора.

Ключевые слова: теория автоматов, переходные системы, подстановка, кодирование, сложность, булев оператор

1. Введение

На практике часто приходится решать задачу перехода от автоматного описания функционирования на язык схем. Например, при логическом синтезе чипов на первом этапе функционирование чипа описывается как конечный автомат. Переход к описанию на языке схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $E_2 = \{0, 1\}$. В результате кодирования возникает булев оператор. При этом автомат может обладать тем свойством, что каждое кодирование порождает оператор, отличный от оператора, порождаемого любым другим кодированием [1].

Возникаемый в результате кодирования булев оператор можно рассматривать как набор булевых функций. Сложность такого оператора можно определить как максимальную сложность получающихся булевых функций. Как известно [2], каждой булевой функции единственным образом соответствует полином Жегалкина. В статье [3] было предложено определить сложность как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, т. е. как максимальную степень полиномов. Тогда простейшими с точки зрения такой сложности являются такие операторы, что соответствующие полиномы Жегалкина имеют первую степень, или линейные булевы функции. Интересно

[1] *Родин Сергей Борисович* — старший научный сотрудник каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: sergei_rodin@mail.ru.

Rodin Sergei Borisovich — Senior research scientist, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

заметить, что максимальность мощности множества возникаемых для автомата посредством кодирований операторов [1] не гарантирует существование «простой», в указанном выше смысле, реализации автомата [4].

В статье [3] был доказан критерий линейной реализуемости нумерованной переходной системы $V = (E_2, E_n, \varphi)$ [5] посредством неизбыточного кодирования F. Данный критерий был сформулирован в терминах порождающих внутренней полугруппы переходной системы [6]. Обозначим через p_0 отображение на n-элементном множестве [7], индуцированное входным символом 0, а через p_1 отображение на n-элементном множестве, индуцированное входным символом 1. Для линейной реализуемости переходной системы необходимыми и достаточными условиями являются, во-первых линейная реализуемость отображений p_0 и p_1, во-вторых выполнения свойства «аддитивного сдвига» на отображениях p_0 и p_1 [3]. В работах [8] и [9] изучался вопрос линейной реализуемости отображений. Данная работа посвящена изучению отображений, задающих «аддитивный сдвиг». В частности, будут сформулированы свойства, которыми должны обладать отображения, задающие «аддитивный сдвиг», а также доказана линейная реализуемость таких отображений с указанием кодирования.

2. Основные понятия и определения

Основным объектом изучения являются отображения на множестве E_n, задающие аддитивный сдвиг, где $n = 2^k$. Так же будет рассмотрен вопрос реализации таких отображений булевыми операторами [2].

2.1. Булев оператор и его сложность

Сначала введем понятия, связанные с булевым оператором, и определим его сложность.

Определение 1. *Пусть $\phi : E_2^m \to E_2^k$ — булев оператор. Его можно рассматривать как набор k булевых функций [2], зависящих от m переменных, а именно, если $\phi(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = (\beta_0, \beta_1, \ldots, \beta_{k-1})$, то $f_j(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \beta_j$, где $0 \le j \le k-1$. Обозначим этот набор через $\mathcal{F}_\phi = \{f_0, f_1, \ldots, f_{k-1}\}$.*

Пример 1. *Рассмотрим оператор ϕ, заданный таблицей*

x_0	x_1	x_2	y_0	y_1	y_2
0	*0*	*0*	*0*	*0*	*1*
0	*0*	*1*	*0*	*1*	*0*
0	*1*	*0*	*0*	*0*	*0*
0	*1*	*1*	*1*	*0*	*0*
1	*0*	*0*	*1*	*0*	*1*
1	*0*	*1*	*1*	*0*	*1*
1	*1*	*0*	*1*	*1*	*1*
1	*1*	*1*	*0*	*1*	*1*

Тогда последние три столбца y_0, y_1, y_2 *можно рассматривать как булевы функции* f_0, f_1, f_2. *Эти функции имеют следующий вид*

$$\begin{aligned} f_0(x_0, x_1, x_2) =& x_0 + x_1 \cdot x_2 \\ f_1(x_0, x_1, x_2) =& x_2 + x_0 \cdot x_1 + x_1 \cdot x_2 \\ f_2(x_0, x_1, x_2) =& 1 + x_1 + x_2 + x_0 \cdot x_1 + x_1 \cdot x_2 \end{aligned}$$

Определение 2. *Пусть* $\mathcal{F} = \{f_0, f_1, \ldots, f_{k-1}\}$ *— набор булевых функций, зависящих от* m *переменных. Данный набор определяет булев оператор* $\phi_{\mathcal{F}} : E_2^m \to E_2^k$ *по правилу*

$$\begin{aligned} \phi_{\mathcal{F}}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) =& (f_0(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}), \\ & f_1(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}), \\ & \ldots \\ & f_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})), \end{aligned}$$

где $\alpha_i \in E_2$.

Пример 2. *Пусть дана пара функций* $f_0(x_0, x_1, x_2) = x_0 + x_1 \cdot x_2$

x_0	x_1	x_2	f_0
0	*0*	*0*	*0*
0	*0*	*1*	*0*
0	*1*	*0*	*0*
0	*1*	*1*	*1*
1	*0*	*0*	*1*
1	*0*	*1*	*1*
1	*1*	*0*	*1*
1	*1*	*1*	*0*

и $f_1(x_0, x_1, x_2) = x_0 \cdot x_1 + x_1 \cdot x_2 + x_2$

x_0	x_1	x_2	f_1
0	*0*	*0*	*0*
0	*0*	*1*	*1*
0	*1*	*0*	*0*
0	*1*	*1*	*0*
1	*0*	*0*	*0*
1	*0*	*1*	*1*
1	*1*	*0*	*1*
1	*1*	*1*	*1*

Данные функции определяют булев оператор оператор ϕ, задаваемый таблицей

x_0	x_1	x_2	y_0	y_1
0	*0*	*0*	*0*	*0*
0	*0*	*1*	*0*	*1*
0	*1*	*0*	*0*	*0*
0	*1*	*1*	*1*	*0*
1	*0*	*0*	*1*	*0*
1	*0*	*1*	*1*	*1*
1	*1*	*0*	*1*	*1*
1	*1*	*1*	*0*	*1*

Определение 3. *Пусть $\phi : E_2^m \to E_2^k$ — булев оператор. Сложностью оператора назовем максимальную степень полиномов Жегалкина функций $\mathcal{F}_\phi$ или $L_{deg}(\phi) = max_{f_i \in \mathcal{F}_\phi}\{deg f_i\}$*

Заметим, что сложность оператора из примеров 1 и 2 равна 2.

В предыдущих определениях предполагалось, что операторы определены на всех элементах множества E_2^m. Однако, в дальнейшем будут возникать частично-определенные операторы, т. е. операторы, определенные на подмножестве множества E_2^m. Определим понятие доопределения частично-определенного оператора.

Определение 4. *Оператор $\widehat{\phi} : E_2^m \to E_2^k$, $m, k \in N$ назовем доопределением оператора $\phi : R \to {E_2}^k$, где $R \subseteq E_2^m$, если для каждого $(\alpha_1, \ldots, \alpha_m) \in R$ верно*

$$\phi(\alpha_1, ..., \alpha_m) = \widehat{\phi}(\alpha_1, ..., \alpha_m).$$

Пример 3. *Рассмотрим частично-определенный оператор ϕ*

x_0	x_1	x_2	y_0	y_1
0	*0*	*0*	*0*	*0*
0	*0*	*1*	*0*	*1*
0	*1*	*0*	*0*	*0*
1	*0*	*0*	*1*	*0*
1	*1*	*0*	*1*	*1*

Примером доопределения является оператор $\widehat{\phi}$

x_0	x_1	x_2	y_0	y_1
0	*0*	*0*	*0*	*0*
0	*0*	*1*	*0*	*1*
0	*1*	*0*	*0*	*0*
0	*1*	*1*	*0*	*1*
1	*0*	*0*	*1*	*0*
1	*0*	*1*	*1*	*1*
1	*1*	*0*	*1*	*1*
1	*1*	*1*	*1*	*0*

2.2. Реализуемость отображения посредством кодирования

От отображения к булеву оператору можно перейти с помощью кодирования. Сначала определим кодирование, а затем как с помощью кодирование получается булев оператор.

Определение 5. *Кодированием множества* $E_n = \{0, \ldots, n-1\}$ *назовем взаимно-однозначное отображение (вложение)* $F : \{0, \ldots, n-1\} \to E_2^m$, *где* $m \geq]\log_2 n[$.

Пример 4. *В качестве примера кодирования можно рассмотреть следующее отображение* E_8 *в* E_2^3*:*

q	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$F(q)$	*001*	*010*	*000*	*100*	*101*	*101*	*111*	*011*

Выделим из всех кодирований «стандартное» кодирование.

Определение 6. *Кодирование* $F_0 : \{0, \ldots, n-1\} \to E_2^k$ *назовем стандартным, если код элемента есть его двоичное представление.*

Пример 5. *В качестве примера стандартного кодирования можно рассмотреть следующее отображение* E_8 *в* E_2^3*:*

q	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$F_0(q)$	*000*	*001*	*010*	*011*	*100*	*101*	*110*	*111*

Каждому кодированию F можно сопоставить подстановку s_F на множестве $Q = \{0, \ldots, n-1\}$ по правилу $s_F(i) = F_0^{-1}(F(i))$.

Кодированию F из примера 4 соответствует подстановка

$$s_F = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 0 & 4 & 5 & 6 & 7 & 3 \end{pmatrix}$$

Каждой подстановке $s : E_n \to E_n$ сопоставим кодирование F_s по правилу $F_s(i) = F_0(s(i))$.

Пример 6. *Пусть задана подстановка*

$$s = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 0 & 4 & 5 & 6 & 7 & 3 \end{pmatrix}$$

Данной подстановке соответствует кодирование

q	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$F(q)$	*001*	*010*	*000*	*100*	*101*	*110*	*111*	*011*

Заметим, что для неизбыточного F верно, кодирование $F_{s_F} = F$, для подстановки s верно $s_{F_s} = s$.

Определение 7. *Пусть $s : E_n \to E_n$ — отображение множества $E_n = \{0, \ldots, n-1\}$ в себя. Кодирование $F : E_n \to E_2^l$ множества E_n сопоставляет отображению s булев оператор $\phi_s^F : R \to R$, где $R \subseteq E_2^k$, по правилу*

$$\phi_s^F(\alpha_1, ..., \alpha_{l-1}) = F(s(F^{-1}(\alpha_1, ..., \alpha_{l-1}))),$$

где $\alpha_1, ..., \alpha_{l-1} \in E_2$.

Пример 7. *Пусть задано отображение*

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 5 & 6 & 7 & 2 & 3 & 4 \end{pmatrix}$$

Рассмотрим кодирование

q	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$F(q)$	*0000*	*0001*	*0010*	*0100*	*1000*	*0011*	*0101*	*1111*

Построим булев оператор по отображению p с использованием кодирования F. Запишем отображение p в табличном виде.

i	$p(i)$
0	0
1	1
2	5
3	6
4	7
5	2
6	3
7	4

Заменим в таблице элементы множества E_8 на их коды, определяемые кодированием F. В результате получится определяет следующий частично определенный булев оператор ϕ

x_0	x_1	x_2	x_3	y_0	y_1	y_2	y_3
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	0	1	0	1
0	1	0	1	0	1	0	0
1	0	0	0	1	1	1	1
1	1	1	1	1	0	0	0

Определение 8. *Отображение $s : E_n \to E_n$ называется линейно реализуемым посредством кодирования F, если для оператора ϕ_s^F существует такое доопределение $\widehat{\phi}_s^F$, что набор $\mathcal{F}_{\widehat{\phi}_s^F}$ состоит из линейных булевых функций.*

Пример 8. *Заметим,что оператор ϕ из примера 7*

x_0	x_1	x_2	x_3	y_0	y_1	y_2	y_3
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	0	1	0	1
0	1	0	1	0	1	0	0
1	0	0	0	1	1	1	1
1	1	1	1	1	0	0	0

может быть доопределен до оператора $\widehat{\phi}$, таким образом что $\mathcal{F}_{\widehat{\phi}}^F$ состоит из линейных булевых функций. Жирным шрифтом выделены наборы, на которых оператор ϕ не определен и значения оператора $\widehat{\phi}$ на этих наборах.

x_0	x_1	x_2	x_3	y_0	y_1	y_2	y_3
0	*0*	*0*	*0*	*0*	*0*	*0*	*0*
0	*0*	*0*	*1*	*0*	*0*	*0*	*1*
0	*0*	*1*	*0*	*0*	*0*	*1*	*1*
0	*0*	*1*	*1*	*0*	*0*	*1*	*0*
0	*1*	*0*	*0*	*0*	*1*	*0*	*1*
0	*1*	*0*	*1*	*0*	*1*	*0*	*0*
0	**1**	**1**	**0**	**0**	**1**	**1**	**0**
0	**1**	**1**	**1**	**0**	**1**	**1**	**1**
1	*0*	*0*	*0*	*1*	*1*	*1*	*1*
1	**0**	**0**	**1**	**1**	**1**	**1**	**0**
1	**0**	**1**	**0**	**1**	**1**	**0**	**0**
1	**0**	**1**	**1**	**1**	**1**	**0**	**1**
1	**1**	**0**	**0**	**1**	**0**	**1**	**0**
1	**1**	**0**	**1**	**1**	**0**	**1**	**1**
1	**1**	**1**	**0**	**1**	**0**	**0**	**1**
1	*1*	*1*	*1*	*1*	*0*	*0*	*0*

Причем множество $\mathcal{F}^F_{\widehat{\phi}}$ *состоит из функций*

$$\begin{aligned} y_0 &= x_0 \\ y_1 &= x_0 + x_1 \\ y_2 &= x_0 + x_2 \\ y_3 &= x_0 + x_1 + x_2 + x_3 \end{aligned}$$

Следовательно подстановка p *из примера 7 является линейной реализуемой посредством кодирования* F*.*

2.3. Отображения, задающие аддитивный сдвиг

Если $n = 2^k$, то отображения множества $E_n = \{0, \ldots, n-1\}$ в себя могут быть представлены [2] как многочлены над полем Галуа F_n [10].

Обозначим через $H_+ \subset P_n$ множество подстановок, соответствующих многочленам вида $x + c$ над полем Галуа F_n, где $c \in E_n$ — константа.

Пример 9. *Приведем пример множеств* H_+ *для* $n = 8$*. Обозначим отображение, соответствующее многочлену* f *над полем Галуа, через* h_f*.*

$$H_+ = \{h_x = e, h_{x+1} = (0\,1)(2\,3)(4\,5)(6\,7), h_{x+2} = (0\,2)(1\,3)(4\,6)(5\,7),$$

$$h_{x+3} = (0\,3)(1\,2)(4\,7)(5\,6), h_{x+4} = (0\,4)(1\,5)(2\,6)(3\,7), h_{x+5} = (0\,5)(1\,4)(2\,7)(3\,6),$$

$$h_{x+6} = (0\,6)(1\,7)(2\,4)(3\,5), h_{x+7} = (0\,7)(1\,6)(2\,5)(3\,4)\},$$

Замечание. *Умножение отображений осуществляется «слева направо», т.е. если заданы отображения p_1 и p_2, то значение их произведения на элементе i определяется равенством $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.*

Определение 9. *Отображение $h : E_n \to E_n$ определяет аддитивный сдвиг, если существует такое взаимнооднозначное отображение $s : E_n \to E_n$, что $h \in H_+^s = s^{-1} \cdot H_+ \cdot s$.*

3. Основные результаты

Лемма 1. *Пусть задано отображение $h : E_n \to E_n$, отличное от тождественного, такое, что верно*

- *если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$*
- *$h(q) \neq q$, $\forall q \in E_n$*
- *$h(h(q)) = q$, $\forall q \in E_n$*

тогда существует такое разбиение множества $E_n = Q_1 \sqcup Q_2 \sqcup \ldots \sqcup Q_m$, что верно

- *$m = \frac{n}{2}$*
- *$Q_i \bigcap Q_j = \emptyset$, если $i \neq j$*
- *$|Q_i| = 2$, $\forall i \in \{1, \ldots, m\}$*
- *$h(Q_i) = Q_i$, $\forall i \in \{1, \ldots, m\}$*

Доказательство. Построим указанное разбиение множества E_n явным образом по индукции.

База индукции. Обозначим через Q_1 множество $\{0, h(0)\}$.

Шаг индукции. Пусть построены множества Q_1, Q_2,. . . ,Q_l. Пусть q минимальный элемент из $E_n \setminus (Q_1 \bigcup Q_2 \bigcup \ldots \bigcup Q_l)$. Тогда через Q_{l+1} обозначим множество $\{q, h(q)\}$.

Рассмотрим множество Q_i. По построению найдется элемент $q \in E_n$ такой, что $Q_i = \{q, h(q)\}$.

В силу свойства $h(q) \neq q$, $\forall q \in E_n$, следует, что мощность множества Q_i равна 2.

В силу свойства отображения $h(h(q)) = q$, $\forall q \in E_n$, следует, что $h(Q_i) = Q_i$.

Предположим, что найдутся такие i и j, что $Q_i \bigcap Q_j \neq \emptyset$. Без ограничения общности считаем, что $i < j$. Тогда по построению в множестве Q_j лежит элемент q, не лежащий в множестве Q_i. И поскольку,

пересечение множеств не пусто, а мощность каждого множества равна 2, то $h(q) \in Q_i = \{q_1, q_2\}$. Без ограничения общности будем считать, что $h(q) = q_1$. С другой стороны в силу того, что $h(Q_i) = Q_i$, а также свойства $h(q) \neq q$, $\forall q \in E_n$, верно $h(q_2) = q_1$. Это противоречит взаимной однозначности отображения h.

В силу доказанного выше на каждом шаге индукции множество из которого выбираем минимальный элемент уменьшается ровно на 2. Следовательно, таких шагов будет сделано равно $\frac{n}{2}$. □

Теорема 1. *Пусть задано взаимнооднозначное отображение $s : E_n \to E_n$. Отображение h, отличное от тождественного, принадлежит H_+^s тогда и только тогда, когда верно*

- *если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$*
- $h(q) \neq q$, $\forall q \in E_n$
- $h(h(q)) = q$, $\forall q \in E_n$

Доказательство. Пусть отображение $h \in H_+$ и $h \neq e$. Тогда существует такое $0 \neq c \in E_n$, что $h(q) = q+c$, $\forall q \in E_n$, где сумма понимается в смысле суммы поля Галуа E_n. Пусть $h(q_1) = h(q_2)$. Это можно переписать как $q_1 + c = q_2 + c$. Прибавим c к правой и левой части. В результате получим $q_1 = q_1+c+c = q_2+c+c = q_2$. Так как $c \neq 0$, то верно, что $h(q) = q+c \neq q$, $\forall q \in E_n$. Так же заметим, что $h(h(q)) = h(q) + c = q + c + c = q$, $\forall q \in E_n$.

Таким образом утверждение верно, если s - тождественное отображение.

Теперь покажем, что при сопряжении сохраняются свойства

- если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$
- $h(q) \neq q$, $\forall q \in E_n$
- $h(h(q)) = q$, $\forall q \in E_n$

Пусть $h = s^{-1} \cdot h' \cdot s$, и $h' \in H_+$.

Пусть $h(q_1) = h(q_2)$. Это можно переписать как

$$s(h'(s^{-1}(q_1))) = s(h'(s^{-1}(q_2))).$$

В силу взаимнооднозначности s верно, что

$$h'(s^{-1}(q_1)) = h'(s^{-1}(q_2)).$$

Отсюда следует, что $s^{-1}(q_1) = s^{-1}(q_2)$, а значит и $q_1 = q_2$.

Пусть $h'(q) \neq q$, $\forall q \in E_n$, но $\exists q_0$ такое, что $h(q_0) = q_0$. Данное равенство можно переписать как

$$s(h'(s^{-1}(q_0))) = q_0.$$

Обозначим через

$$q_1 = s^{-1}(q_0),$$

а через

$$q_2 = h'(q_1).$$

Заметим, что поскольку $h' \in H_+$, то в силу доказанного выше $h(q_1) = q_2 \neq q_1$, но при этом в силу соотношений, представленных выше, $s(q_1) = q_0$ и $s(q_2) = q_0$. Что противоречит взаимнооднозначности s.

В силу доказанного выше для отображения $h' \in H_+$ имеет место равенство $h'(h'(q)) = q$, $\forall q \in E_n$.

Для произвольного $q \in E_n$ рассмотрим $h(h(q))$. Верна следующая цепочка равенств

$$h(h(q)) = s(h'(s^{-1}(s(h'(s^{-1}(q)))))) = s(h'(h'(s^{-1}(q)))) = s(s^{-1}(q)) = q.$$

Таким образом доказано, что и третье свойство сохраняется при сопряжении. Таким образом теорема доказана в одну сторону.

Пусть задано отображение $h : E_n \to E_n$ такое, что

- если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$
- $h(q) \neq q$, $\forall q \in E_n$
- $h(h(q)) = q$, $\forall q \in E_n$

Согласно лемме 1, существует разбиение множества $E_n = Q_1 \sqcup \ldots \sqcup Q_m$, такое что $h(Q_i) = Q_i$, $\forall i \in \{1, \ldots, m\}$. Обозначим, элементы множества Q_i через $q_1^{Q_i}$ и $q_2^{Q_i}$, где $q_1^{Q_i} < q_2^{Q_i}$. В силу свойств отображения h верно, $h(q_1^{Q_i}) = q_2^{Q_i}$ и $h(q_2^{Q_i}) = q_1^{Q_i}$, $\forall i \in \{1, \ldots, m\}$. Рассмотрим отображение $h' \in H_+$, отличное от тождественного. Как было показано выше оно обладает свойствами

- если $h'(q_1) = h'(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$
- $h'(q) \neq q$, $\forall q \in E_n$
- $h'(h'(q)) = q$, $\forall q \in E_n$

Согласно лемме 1, существует разбиение множества $E_n = Q'_1 \sqcup \ldots \sqcup Q'_m$, такое что $h'(Q'_i) = Q'_i$, $\forall i \in \{1, \ldots, m\}$. Обозначим, элементы множества

Q'_i через $q_1^{Q'_i}$ и $q_2^{Q'_i}$, где $q_1^{Q'_i} < q_2^{Q'_i}$. В силу свойств отображения h верно, $h'(q_1^{Q'_i}) = q_2^{Q'_i}$ и $h'(q_2^{Q'_i}) = q_1^{Q'_i}$, $\forall i \in \{1, \ldots, m\}$.

Построим отображение $s : E_n \to E_n$ по правилу

$$s(q_1^{Q'_i}) = q_1^{Q_i}, \forall i \in \{1, \ldots, m\}$$

$$s(q_2^{Q'_i}) = q_2^{Q_i}, \forall i \in \{1, \ldots, m\}$$

Заметим, что в силу $E_n = Q'_1 \sqcup \ldots \sqcup Q'_m$, отображение s определено на всем множестве E_n. Областью значений отображения s является множество $E_n = Q_1 \sqcup \ldots \sqcup Q_m$. А следовательно отображение s взаимнооднозначно.

Рассмотрим значение отображения $s^{-1} \cdot h' \cdot s$ на элементах $q_1^{Q_i}$ и $q_2^{Q_i}$. Верны равенство

$$s(h'(s^{-1}(q_1^{Q_i}))) = s(h'(q_1^{Q'_i})) = s(q_2^{Q'_i}) = q_2^{Q_i}$$

$$s(h'(s^{-1}(q_2^{Q_i}))) = s(h'(q_2^{Q'_i})) = s(q_1^{Q'_i}) = q_1^{Q_i}$$

С другой стороны верно, что

$$h(q_1^{Q_i}) = q_2^{Q_i}$$

$$h(q_2^{Q_i}) = q_1^{Q_i}.$$

Следовательно

$$s(h'(s^{-1}(q_1^{Q_i}))) = h(q_1^{Q_i})$$
$$s(h'(s^{-1}(q_2^{Q_i}))) = h(q_2^{Q_i}).$$

То есть $h = s^{-1} \cdot h' \cdot s$, где $h' \in H_+$.

□

Теорема 2. *Пусть задано взаимооднозначное отображение $s : E_n \to E_n$ и подстановка $h \in H_+^s$, тогда h линейно реализуема посредством кодирования F_s, причем верно $\mathcal{F}_h(F_s) = \{x + c_0, x + c_1, \ldots, x + c_{k-1}\}$, где $c_i \in E_2$, $i \in E_k$, $n = 2^k$.*

Доказательство. Поскольку $h \in H_+^s$, то найдется такое отображение $h_{x+c} \in H_+$, соответствующее многочлену $x + c$, что верно $h = s^{-1} \cdot h_{x+c} \cdot h$. Оператор, построенный по отображению h посредством кодирования F_s, имеет вид

$$\phi_h^{F_s}(q_0, \ldots, q_{k-1}) = F_s(h(F_s^{-1}(q_0, \ldots, q_{k-1}))) =$$

$$= F_s(s^{-1}(h_{x+c}(s(F_s^{-1}(q_0, \ldots, q_{k-1})))))).$$

В силу определения $F_s(i) = F_0(s(i))$, где $i \in E_n$ равенство может быть переписано как

$$\phi_h^{F_s}(q_0, \ldots, q_{k-1}) = F_s(s^{-1}(h_{x+c}(s(F_s^{-1}(q_0, \ldots, q_{k-1}))))) =$$

$$= F_0(s(s^{-1}(h_{x+c}(s(s^{-1}(F_0^{-1}(q_0, \ldots, q_{k-1}))))))) =$$

$$= F_0(h_{x+c}(F_0^{-1}(q_0, \ldots, q_{k-1}) = \phi_{h_{x+c}}^{F_0}(q_0, \ldots, q_{k-1}).$$

То есть построенный оператор совпадает с оператором, построенным по отображению h_{x+c} посредством кодирования F_0. В работе [3] было доказано утверждение

Утверждение. *Подстановки $h_{x+c} \in H_+$ линейно реализуемы посредством кодирования F_0 и $\mathcal{F}_{h_{x+c}}(F_0) = \{x_0 + c_0, x_1 + c_1, \ldots, x_{k-1} + c_{k-1}\}$, $(c_0, c_1, \ldots, c_{k-1}) = F_0(c)$.*

Следовательно множество функций, задающих оператор, построенный по отображению h посредством кодирования F_s, имеет вид $\mathcal{F}_h(F_s) = \{x + c_0, x + c_1, \ldots, x + c_{k-1}\}$, где $c_i \in E_2$, $i \in E_k$, $n = 2^k$. □

В заключение автор выражает благодарность Алёшину Станиславу Владимировичу и Носову Михаилу Васильевичу за многочисленные обсуждения и советы, которые позволили получить результаты, изложенные в данной работе.

Список литературы

[1] Родин С.Б., “Переходные системы с максимальной вариантностью относительно кодирования состояний”, *Интеллектуальные системы*, **4**:3-4 (1999), 335–352.

[2] Яблонский С.В., *Введение в дискретную математику*, Наука, Москва, 1979, 272 с.

[3] Родин С.Б., “Линейно реализуемые автоматы”, *Дискретная математика*, **29**:1 (2016), 59–79.

[4] Родин С.Б., “О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний”, *Интеллектуальные системы. Теория и приложения*, **20**:2 (2016), 337–347.

[5] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 с.

[6] М.А. Арбиб, “Декомпозиция автоматов и расширение полугрупп”, *Алгебраическая теория автоматов, языков и полугрупп*, «Статистика», Москва, 1975, 46–64, 335 с.

[7] А. Клиффорд, Г. Престон, *Алгебраическая теория полугрупп*. Т. 1, Мир, Москва, 1972, 288 с.

[8] Родин С.Б., “О свойствах кодирований состояний автомата”, *Интеллектуальные системы. Теория и приложения*, **21**:1 (2017), 97–111.

[9] Родин С.Б., “О свойстве линейной реализуемости отображений”, *Интеллектуальные системы. Теория и приложения*, **28**:1 (2024), 107–119.

[10] Р. Лидл, Г. Нидеррайтер, *Конечные поля*. Т. 1, Мир, Москва, 1988, 430 с.

On the additive shift property for the linear realizability of automata

Rodin S.B.

This paper studies the property of linear realizability of mapping of the finite set into itself. This property is important from linear realizability of automata, namely linear realizability of the elements of the generating set of the automaton inner semigroup is the one of the necessary conditions for linear realizability of the automaton. Previously it was shown that every mapping of the finite set into itself is linear realizable via an encoding which code length is equal the finite set cardinality. In this paper this result will be improved and it will be shown that every mapping of the finite set into itself is linear realizable via an encoding which code length is equal the finite set cardinality minus one.

Keywords: Automata theory, semiautomata, transition systems, assignment, state encoding, complexity, boolean operator

References

[1] Rodin S.B., “The most variable semiautomata with respect to the states encoding”, *Intelligent systems*, **4**:3-4 (1999), 335–352.

[2] Yablonskij S.V., *Introduction to the discrete math*, Nauka, Moscow, 1979, 272 pp.

[3] Rodin S.B., “Linearly realizable automata”, *Discrete Math*, **29**:1 (2016), 59–79.

[4] Rodin S.B., "On relation between the linearly realizable automata and the most variable automata with respect to the states encoding", *Intelligent systems. Theory and Applications*, **20**:2 (2016), 337–347.

[5] Kudryavtsev V.B., Alyoshin S.V., Podkolzin A.S., *Introduction to automata theory*, Nauka, Moscow, 1985, 320 c.

[6] M.A. Arbib, "Automaton Decompositions and Semigroup Extensions", *Algebraic theory of machines, languages and semigroups*, «Statistika», Moscow, 1975, 46–64, 335 pp.

[7] Clifford A.H., Preston G.B., *The algebraic theory of semigroups.* V. 1, Mir, Moscow, 1972, 288 pp.

[8] Rodin S.B., "On automata states encoding properties", *Intelligent systems. Theory and Applications*, **21**:1 (2017), 97–111.

[9] Rodin S.B., "On the linear realizability property of the mappings", *Intelligent systems. Theory and Applications*, **28**:1 (2024), 107–119.

[10] R. Lidl, H. Niederreiter, *Finite fields.* V. 1, Mir, Moscow, 1988, 430 pp.

Часть 4
Семинары кафедры МаТИС

Доклады семинара «Теория автоматов»

В 2023 году на научном семинаре «Теория автоматов» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 18 докладов.

8 февраля 2023 года

О порядках линейных автоматов

аспирант Муравьев Н. В.

Автоматы с совпадающим входным-выходным алфавитом образуют моноид относительно операции суперпозиции. Рассматривается задача определения порядка элемента в этом моноиде. В 2017 году было доказано, что данная задача алгоритмически неразрешима даже для обратимых конечных автоматов. В докладе будет показано, что она разрешима для класса линейных автоматов над конечными полями и полем рациональных чисел. Более того, будет доказана точная верхняя оценка порядка линейного автомата над этими полями, зависящая от размерности входного-выходного алфавита.

15 февраля 2023 года

Сложность $GF(2)$-операций над регулярными языками

аспирант Сажнева Е. А.

Классические операции в теории формальных языков — объединение и конкатенация. Цель доклада — исследование свойств операций над формальными языками, в определениях которых булева логика (дизъюнкция и конъюнкция) заменена на операции в двухэлементном поле $GF(2)$ — исключающее ИЛИ и конъюнкцию. После такой замены появляются две новые операции — $GF(2)$-конкатенация и взятие $GF(2)$-обратного языка. В докладе будет показано, что класс регулярных языков замкнут относительно этих операций. Будут приведены алгоритмы построения ДКА, распознающего $GF(2)$-конкатенацию двух регулярных языков, и ДКА, распознающего $GF(2)$-обратный язык. Кроме этого будет показано, что все построения являются оптимальными по числу состояний, а также дан ответ на вопрос о сложности данных операций в случае различных размеров алфавитов. В заключение будет кратко рассказано о последних исследованиях в области: применение $GF(2)$-операций к другим классическим моделям, а также $GF(2)$-варианты некоторых операций над языками.

1 марта 2023 года

Нерешенные проблемы в изучении микробиоты

проф. Медведев О. С.

Микробиота желудочно-кишечного тракта (ЖКТ) насчитывает примерно 10^{14} микробных клеток. В норме у взрослого человека более 90% бактерий данного биотопа относится к типам Firmicutes, Bacteroidetes, Actinobacteria и Proteobacteria, в то время как остальные типы представлены в незначительном количестве. На сегодня микробиота ЖКТ рассматривается как самостоятельный орган, который регулирует множество метаболических процессов в организме хозяина и по своей значимости не уступает любому другому жизненно важному органу. Значительная часть функций микробиоты осуществляется при помощи промежуточных и конечных продуктов обмена веществ. Возможность изучения микробного состава, его изменения при различных нозологических формах представляет несомненный практический интерес.

Разнообразие микробиоты — крайне важный параметр оценки: чем больше видов бактерий, тем выше компенсаторный потенциал всей микробиоты. При высоком видовом разнообразии, в случае исчезновения одного или нескольких видов бактерий вследствие приема антибиотиков или несбалансированного питания, их функции могут взять на себя другие бактерии, чего не отмечается при низком видовом разнообразии.

Молекулярно-генетические методы исследования являются перспективным направлением в изучении структуры сообществ микроорганизмов и особенностей их функционирования в норме и патологии. К таким методам относятся полимеразная цепная реакция (ПЦР), таргетное секвенирование, и полногеномное секвенирование. Функцию отдельных групп микроорганизмов отражают метаболиты, образуемые микробиотой при метаболизме углеводов, белков и жиров. К наиболее изученным метаболитам относят образуемые микробиотой газы (водород, метан, сероводород, углекислый газ), короткоцепочечные жирные кислоты (уксусная, пропионовая и масляная), а также триметиламин (ТМА) и его окисленный печенью продукт ТМАО. Важной и нерешенной задачей является создание математической модели, позволяющей прогнозировать микробный состав микробиоты по результатам анализа газовых и других метаболитов.

15 марта 2023 года

О характеристическом многочлене конфигурации паросочетаний графа и LP-ориентациях многогранника паросочетаний

аспирант Болотников А. И.

Для любой конфигурации гиперплоскостей можно построить частично упорядченное множество пересечений его гиперплоскостей. С использованием функции Мебиуса такого частично упорядоченного множества можно далее определить характеристический многочлен конфигурации гиперплоскостей. С помощью характеристического многочлена конфигурации гиперплоскостей можно посчитать число регионов конфигурации. Данный результат использовался, в частности, в одном из доказательств теоремы Стенли о хроматическом многочлене графа и числе ациклических ориентаций графа.

Доклад посвящен свойствам конфигурации паросочетаний графа. В докладе будет построено взаимно-однозначное соответствие между регионами конфигурации паросочетаний и LP-ориентациями многогранника паросочетаний. Также будут рассказаны результаты о характеристическом многочлене конфигурации паросочетаний некоторых семейств графов.

29 марта 2023 года

Сложность задачи о существовании сюръективного гомоморфизма на рефлексивные циклы

аспирант Корчагин Н. П.

Сюръективным гомоморфизмом графов называется сюръективное отображение вершин одного графа в вершины другого, которое сохраняет ребра. Задача о существовании сюръективного гомоморфизма на граф H — массовая задача, в которой по данному графу G требуется определить, существует ли сюръективный гомоморфизм из G на H. Сложность этой задачи долгое время оставалась неизвестной даже для очень простых графов H, таких как циклы: только недавно были получены результаты о сложности для рефлексивного цикла длины 4 и нерефлексивного цикла длины 6. В докладе будет описана сложность задачи для рефлексивных циклов длины $n = 7$, $n > 8$.

31 марта 2023 года

Булевы сети с единственной неподвижной точкой, одностоковые ориентации булева куба и правильные семейства функций

ст.н.с. Галатенко А. В., в.н.с. Носов В. А. доц. Панкратьев А. Е.

Понятие правильного семейства функций было введено В. А. Носовым в 1998 году. Оказалось, что с помощью правильных семейств функций можно порождать параметрические множества квазигрупп большой мощности. В процессе дальнейших исследований удалось установить ряд критериев правильности семейства, построить значительное число содержательных примеров, получить утверждения о сложности задачи распознавания правильности. В 2020 году К. Д. Царегородцев заметил, что в булевом случае имеется естественным образом определенное взаимно однозначное соответствие между правильными семействами и одностоковыми ориентациями ребер булева куба; в процессе доказательства было найдено еще одно критериальное свойство — существование и единственность неподвижной точки у отображения, задаваемого правильным семейством, и всех его проекций. И одностоковые ориентации (Unique Sink Orientation, USO), и булевы сети с единственной неподвижной точкой являются известными математическими объектами, которым посвящено значительное число публикаций. В первой части доклада будет сделан обзор результатов по одностоковым ориентациям и булевым сетям с неподвижной точкой и показана связь этих результатов с правильными семействами; вторая часть посвщена анализу k-значного случая при $k > 2$.

12 апреля 2023 года

Метод чередования обучаемых параметров нейронной сети

м.н.с. Хусаенов А. А.

В докладе представляется метод повышения качества обучения сверточных искусственных нейронных сетей (ИНС) за счет разделения параметров по их возможности расширения рецептивного поля. При обучении ResNet50 достигается увеличение точности за счет чередуемой остановки обучения в 4-х слоях, расширяющих рецептивное поле. Показано, что повышение обобщающей способности модели при использовании предложенного метода достигается за счет устранения избыточного вклада отдельных существенных (окклюзивных) элементов изображения при формировании карт признаков. В пользу указанных предположений приводятся результаты экспериментов в задаче transfer learning и

рассуждения относительно существования указанной проблемы. Демонстрируется существование подобных проблем и в прочих (не сверточных) архитектурах ИНС: например, в задаче выявления отклонений с применением автоассциативных ИНС.

19 апреля 2023 года

Сложность кванторной задачи удовлетворения ограничениям на предикатах, заданных с помощью предиката равенства

ст.н.с. Жук Д. Н.

Кванторная задача удовлетворения ограничениям — это массовая задача, где на вход подаётся утверждение с кванторами, конъюнкциями и предикатами из некоторого множества допустимых предикатов, и нужно проверить верно ли это утверждение. Даже на конечных множествах сложность этой задачи для конкретного множества допустимых предикатов остаётся открытым вопросом, поэтому на бесконечных множествах мы пока рассматриваем только предикаты специального вида. В 2007 году была опубликована полная классификация сложности для множеств допустимых предикатов, которые задаются булевыми комбинациями равенств, но в ней была обнаружена ошибка и с тех пор вопрос о полной классификации оставался открытым. Спустя 15 лет мы получили полную классификацию, причем не только для кванторной задачи удовлетворения ограничениям, но и для всевозможных ограниченных альтернаций.

26 апреля 2023 года

Современные технологии создания чипов: от дизайна к оптической литографии

ст.н.с. Родин С. Б.

Современный процесс создания чипа можно условно разделить на два этапа. На первом этапе создается дизайн вычислительного устройства. На втором этапе данный дизайн реализуется в «кремнии», в реальном физическом устройстве. Надо отметить, что дизайн создается поэтапно от абстрактного описания функционирования вычислительного устройства к схеме из функциональных элементов (или ячеек) и затем к соединению транзисторов.

Транзистор является многослойной структурой, а соединения транзисторов также размещаются на отдельном слое. В итоге дизайн передается на производство как несколько слоев, где каждый слой это множество «манхетоновских» многоугольников.

Целью данного доклада является дать представление о том, как устроены современные полупроводниковые устройства и какие технологии применяются для их создания. В первой половине будет рассказано, как устроены транзисторы, как из них формируются ячейки, и в конечном счёте чип. Во второй половине будет рассказано какие технологии используются для производства, а также какие задачи необходимо решать в процессе, чтобы на выходе получилось устройство, задуманное дизайнерами.

20 сентября 2023 года

Правильные семейства дискретных функций: эквивалентные определения и свойства

старший специалист-исследователь Царегородцев К. Д.

В последнее время растет интерес к использованию в криптографических (и теоретико-кодовых) приложениях некоммутативных и неассоциативных алгебраических структур (в частности, квазигрупп). Задание квазигруппы в виде «таблицы умножения» непрактично, поскольку размер требуемой для её хранения памяти растет крайне быстро при росте «длины» перемножаемых элементов. Одним из возможных вариантов обойти это ограничение является функциональное задание квазигрупповой операции, при котором координаты произведения $(z_1, ..., z_n)$ задаются функциями от координат сомножителей:

$$z_i = f_i(x_1, ..., x_n, y_1, ..., y_n).$$

Для функционального задания квазигрупповых операций В. А. Носовым в 1999 году было введено понятие правильного семейства (булевых) функций. Исходное определение было расширено сначала на случай абелевых групп, а затем и на более общие алгебраические структуры. В докладе мы рассмотрим исходное определение понятия правильного семейства, некоторые примеры таких семейств, а также результаты, полученные в последние годы: альтернативные характеризации правильных семейств (с более «геометрических» точек зрения), некоторые их свойства (оценки на количество правильных семейств, результаты о конкретных классах правильных семейств).

4 октября 2023 года

Компьютерное моделирование логических процессов

проф. Подколзин А. С.

В докладе рассматривается компьютерная система, моделирующая процесс решения задач человеком в таких областях, как математика, элементарные физика и химия, и ряде других. Особое внимание уделяется проблеме автоматического создания приемов решателя по теоремам предметной области.

25 октября 2023 года

Линейные автоматные системы и автоматы в лабиринтах

н.с. Волков Н. Ю.

Линейная автоматная система — это набор автоматов, взаимодействующих между собой посредством среды, параметры которой задаются целыми числами. Автоматы могут знать значения этих чисел, в случае, если они (по модулю) не превосходят обзор автоматов R, и могут постепенно менять их значения. Также числовые параметры системы могут быть связаны между собой линейными уравнениями. Тип автоматной линейной системы определяется количеством и областью значения её числовых параметров, количеством автоматов и конкретным способом их взаимодействия, а также уравнениями, связывающими параметры системы между собой.

Эта модель возникла в результате обобщения ряда задач, где различные системы автоматов в лабиринтах, фактически, производили вычисления определённых функций. В эту же модель вписываются автоматы со счётчиками и другие абстрактные вычислители. Рассматриваются вопросы вычисления функций линейными автоматными системами, моделирования одной линейной автоматной системой другой.

Вводятся понятия манёвра линейной автоматной системы и функций маневра. Вводятся обобщённые дискретные функции как пары счётнозначных функций. На таких функциях вводятся операции обобщённой суперпозиции и обобщённой рекурсии, а также оператор замыкания (замыкание Илхомова), порождённый этими операциями. Сформулирована (и доказана в ряде частных случаев) гипотеза о том, что класс функций, вычисляемых автоматными системами каждого конкретного типа, есть замыкание Илхомова класса функций манёвра, которые реализуют линейные автоматные системы данного типа.

Модель линейных автоматных систем позволяет рассматривать разные физические вычислители, описываемые одними же и теми же каноническими уравнениями, как разные геометрические образы одной и той же вычислительной системы. Также есть надежда, что озвученные в докладе подходы позволят найти новые структуры в иерархии классов вычислимых функций.

1 ноября 2023 года

Проблема полноты для функциональных систем полиномиальных и рациональных функций

доц. Алексиадис Н. Ф.

В докладе рассматривается проблема полноты для функциональных систем полиномиальных и рациональных функций, а также задачи функционального характера, порожденные ее решением (изучение структуры замкнутых и предполных классов, задача о базисах, ...). Особое внимание уделяется алгоритмически неразрешимым проблемам.

8 ноября 2023 года

Оценки энергопотребления объемных схем

м.н.с. Ефимов А. А.

Одним из разделов математической кибернетики является теория управляющих систем. Интенсивное развитие науки и вычислительной техники в XX веке породило одно из интереснейших направлений в этой области — задачу синтеза схем, вычисляющих булевы функции и операторы. Автор решает эту задачу, разрабатывая универсальные методы синтеза схем и получая фундаментальные нижние оценки сложности схем, показывающие оптимальность применяемых методов.

15 ноября 2023 года

Распознавание свойств графов автоматами

аспирант Демидова А. А.

В докладе будут представлены результаты, связанные с обходом автоматами с красками связных плоских простых неориентированных графов с целью установления их свойств. В частности, будут рассмотрены алгоритмы, в соответствии с которыми автомат, осуществляющий обход, может определить, является ли граф деревом, псевдодеревом (графом, из которого достаточно удалить одно ребро для того, чтобы он стал деревом) и графом-кактусом (графом, в котором любое ребро принадлежит

не более чем одному циклу, а любые два цикла могут иметь не более одной общей вершины). Автомату доступно некоторое количество стираемых красок, которые он наносит на рёбра в течение обхода графа. Во время обхода автомат обладает частичной информацией о вершинах, которые он посещает, и инцидентных им рёбрах. В частности, в любой момент времени автомату известно, красил ли он только что некоторое ребро, благодаря чему он может обнаруживать циклы. Определены условия, при достижении которых автомат устанавливает, что граф не относится к рассматриваемым классам, а также признаки завершения обхода деревьев, псевдодеревьев и графов-кактусов.

29 ноября 2023 года

Нижняя оценка сложности задачи поиска ближайшего соседа на прямой с помощью клеточного автомата с локаторами

проф. Гасанов Э. Э.

Рассматривается применение модели клеточного автомата с локаторами к задаче поиска ближайшего соседа на прямой. Модель клеточного автомата с локаторами подразумевает возможность каждой ячейке автомата передавать через эфир сигнал на сколь угодно большие расстояния. Ранее было показано, что такая возможность позволяет решать задачу поиска ближайшего соседа за логарифмическое время. В докладе обсуждается логарифмическая нижняя оценка для сложности этой задачи.

6 декабря 2023 года

О выразимости автоматов с операцией суперпозиции

проф. Бабин Д. Н., инженер-исследователь Летуновский А. А.

Проблема выразимости автоматов относительно суперпозиции долгое время считалась неразрешимой. В 2015 году она получила дальнейшее развитие в работах А.А Летуновского. Возник алгоритм проверки выразимости автоматов с безусловными переходами при наличии в выражающей системе автоматов «штрих Шеффера» и «задержки». Суперпозиция с такой добавкой получила название расширенной суперпозиции. Для такой суперпозиции множество всех автоматов распалось на две части: те автоматы, для которых есть алгоритм проверки выразимости, и те, для которых это неизвестно. К первой группе кроме автоматов с безусловными переходами были отнесены автоматы с простыми внутренними группами переходов и линейные автоматы. В настоящем докладе речь пойдёт о добавлении к этой группе автоматов с линейными переходами над произвольным конечным полем.

13 декабря 2023 года

Инструментарий разработки интегральных схем (ИРИС): назначение, возможности и дальнейшее развитие

м.н.с. Калачев Г. В.

ИРИС представляет собой библиотеку на языке C++, позволяющую описывать сложные конфигурируемые аппаратные схемы в рамках автоматной модели. Для этого в библиотеке имеется набор макрокоманд, формирующих встроенный в C++ язык для описания схем. Также в библиотеке имеются возможности для тестирования, оценки сложности и генерации описания на языке Verilog для последующего синтеза. В первой части доклада будет показано, как выглядит описание простых аппаратных модулей на языке ИРИС, как происходит тестирование, а также некоторые другие возможности библиотеки ИРИС. Во второй части доклада будут приведены планы по развитию ИРИС и задачи которые предстоит решить в следующем году. В частности, будет рассказано про задачу автоматической расстановки и балансировки задержек на критических путях, а также задачи, связанные с автоматизацией тестирования.

Доклады семинара «Теория автоматов»

В первом полугодии 2024 года на научном семинаре «Теория автоматов» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 15 докладов.

7 февраля 2024 года

Симметричные функции k-значной логики и универсальные алгоритмы для задачи удовлетворения ограничений

ст.н.с. Жук Д. Н.

Известно, что задача удовлетворения ограничениям на конечном множестве решается за полиномиальное время тогда и только тогда, когда множество допустимых предикатов сохраняется слабой функцией почти единогласия. При этом известные полиномиальные алгоритмы не являются универсальными, в том смысле, что работают только для конкретного фиксированного множества допустимых предикатов. С другой стороны, есть простые универсальные алгоритмы, для работы которых необходимы сохраняющие функции, имеющие намного больше симметрий, чем слабая функция почти единогласия.

На пути к построению универсального алгоритма, нам удалось доказать, что из любой слабой функции почти единогласия можно вывести функцию, симметричную на любом двухэлементном множестве. Этот чисто алгебраический результат удивителен тем, что тождества, задающие слабую функцию почти единогласия, являются самым слабым набором тождеств, который нельзя удовлетворить обычными селекторами. Оказалось, что этот слабейший набор тождеств эквивалентен симметричности на любом двухэлементном множестве.

В докладе мы обсудим как алгебраическую часть результата, так и её применение к задаче удовлетворения ограничениям.

14 февраля 2024 года

Автоматные системы

н.с. Волков Н. Ю., студент Илхомов М. М.

Предложено новое понятие автоматной системы, обобщающее все известные в дискретной математике вычислительные модели. Фактически,

автоматная система — это произвольный конечный автомат, или группа автоматов, с внешней памятью.

Введён специальный класс графов, задающих вычислительные системы. Показано, что каждая автоматная система является вычислительной системой и наоборот, каждая вычислительная система является автоматной системой. Вводятся понятия эквивалентности и сильной эквивалентности автоматных (вычислительных систем). Получен критерий сильной эквивалентности вычислительных систем.

Задача определения класса функций, вычисляемых конкретным типом (классом) автоматных систем, решена путём сведения ее к нахождению класса функций, вычисляемых автоматными системами данного типа за один такт. Этот подход позволяет найти новые базисы во множестве вычислимых (по Тьюрингу) функций.

Показано, что сложные автоматные системы, состоящие из конечного числа автоматов, сводятся к обычным автоматным системам (состоящим из одного автомата).

Для описания работы автоматных систем и решения возникших задач разработана теория парных функций, которая сама по себе может представлять значительный интерес и порождает новый класс управляющих систем, требующий изучения.

Представляется, что теория автоматных систем заполнит ряд пробелов в теории алгоритмов. Кроме того, она дает емкий язык для описания функционирования ряда хорошо известных вычислителей. Фактически, автоматные системы — это общая модель для описания всех известных и перспективных вычислителей.

21 февраля 2024 года

Статистический анализ причинно-следственных связей с использованием данных высокой размерности

аспирант Ченцов А. М.

Доклад посвящен проблеме статистических выводов о причинно-следственных зависимостях в моделях высокой размерности, связанной с неравномерной сходимостью распределения оценок. Кратко описываются подходы к идентификации причинно-следственных связей — модель потенциальных исходов Рубина и модели на ациклических ориентированных графах, применимые (в отличие от методологии рандомизированных экспериментов) к данным на основе пассивных наблюдений. Подробно разбирается решение проблемы неравномерности с помощью методов ортогонального машинного обучения, включая двойной выбор как частный случай.

6 марта 2024 года

Умножение n-значных чисел за время $O(n)$ клеточным автоматом с локаторами

проф. Гасанов Э. Э., студент Омаров Т. К.

Будет рассказан алгоритм умножения чисел, в двоичном представлении которых n бит, за время порядка n с помощью клеточных автоматов с локаторами.

Решение задачи линейного программирования клеточными автоматами с локаторами

проф. Гасанов Э. Э., студентка Музаффарова М. Ф.

Будет предложен алгоритм решения двумерной задачи целочисленного линейного программирования с помощью клеточных автоматов с локаторами. Будет показано, что время работы алгоритма — это некоторая константа, не зависящая от числа точек в исходном множестве.

13 марта 2024 года

Восстановление изображения по стертому коду с точностью до аффинной или метрической эквивалентности

ст.н.с. Алексеев Д. В.

Ранее в работах В.Н. Козлова были исследованы так называемые «правильные» коды для изометрических и аффинных преобразований. Код называется правильным для некоторого семейства преобразований, если совпадение кодов равносильно эквивалентности изображений относительно этого семейства. В докладе рассматривается задача восстановления изображения по стертому коду, т.е. коду, в котором были удалены индексы. Предложены алгоритмы, решающие (при некоторых дополнительных условиях) эту задачу за полиномиальное время.

Влияние метода подготовки обучающего материала на точность сегментации на примере нейронной сети DAUNet

ст.н.с. Алексеев Д. В., студент Шарков К. А.

Сбор и обработка реальных данных часто сопряжены с большими затратами. Синтетические данные могут стать хорошей альтернативой для обучения моделей. Также, важную роль на качество обучаемых моделей оказывает разметка данных. В докладе рассматривается задача сегментации трещин на изображениях дорожного покрытия. На первом этапе исследования было проведено обучение нейронной сети DAUNet на основе специально ухудшенной разметки. Показана зависимость метрик AIU, sODS, SOIS от качества разметки. На втором этапе исследования было проведено обучение нейронной сети DAUNet на основе синтетического обучающего материала. Показана зависимость метрик AIU, sODS, sOIS от процента содержания в обучающем материале синтетических данных.

20 марта 2024 года

О сложности решения задачи полноты для автоматов с суперпозициями

проф. Бабин Д. Н.

В традиционно изучаемых классах функциональных систем, таких как Pк и автоматы с композициями, всякий замкнутый класс расширяется до предполного, поэтому подход С.В. Яблонского к задаче полноты через предполные классы имеет смысл. Для автоматов с суперпозициями это гораздо сложнее. В докладе будет приведён пример класса, не расширяющегося до предполного.

27 марта 2024 года

Вычисление функций односторонними и двусторонними автоматами

студент Литовский В.

В докладе обсуждаются функции, вычисляемые различными видами автоматов: классическим автоматом, автоматом с остановками, двусторонним автоматом. Рассмотрены свойства кодировок, преобразующих числа во входные последовательности для автомата и обратно. Найдены классы функций, вычислимые указанными трёмя видами автоматов в этих кодировках.

3 апреля 2024 года

Математическая модель и метод верификации криптографических протоколов

доц. Миронов А. М.

В докладе будет изложена математическая модель криптографических протоколов, и будут приведён пример применения этой модели для решения задач верификации криптографических протоколов.

Криптографические протоколы — это распределенные алгоритмы, предназначенные для обеспечения передачи конфиденциальной информации в небезопасной среде. Они используются, например, в электронных платежах, электронных процедурах голосования, системах доступа к конфиденциальным данным, и т.д. Ошибки в криптографических протоколах могут привести к большому ущербу, поэтому необходимо использовать математические методы для обоснования различных свойств корректности и безопасности криптографических протоколов.

17 апреля 2024 года

Автоматизированный диагностический лечебный комплекс поддержания жизнедеятельности человека «АНГЕЛ»

доц. Староверов В. М.

Доклад посвящен деятельности, проведенной в рамках Лаборатории Бернулли МГУ им. М.В. Ломоносова. Будет рассказано о задачах, решаемых в рамках проектов по созданию комплексов тактильной диагностики и поддержки системы жизнеобеспечения Ангел. В частности, будет дан обзор языка описания медицинских протоколов и приведены результаты распознавания сенсорных образов с помощью тактильного механорецептора.

24 апреля 2024 года

Построение реалистичных палеогеографических карт методами комбинаторной оптимизации

доц. Афонин С. А.

Построение палеогеографических карт проводится на основании анализа состава горных пород (фаций). Исходными данным могут быть как точки на плоскости — координаты скважин, в которых встречаются определенные фации, — так и карта скоростей накопления осадков.

Предполагается, что одинаковые фации должны иметь близкие скорости осадконакопления. Задача реконструкции палеогеографической карты заключается в определении границ областей распространения фаций. В работе предлагается сведение задачи построения карты к задаче раскраски графов, которая, в свою очередь, решается методами целочисленного линейного программирования. Такой подход позволяет автоматически строить реалистичные карты — то есть карты, удовлетворяющей экспертным ограничениям и правилам.

15 мая 2024 года

Построение графа знаний по видео с помощью генеративного интеллекта

проф. Рыжов А. П., студентка Топорова М. С.

В докладе рассматривается разработка и исследование алгоритмов аннотирования видео и представление аннотации в виде графа знаний. Аннотирование файла — создание его краткой версии, раскрывающей его логическую структуру, наиболее существенные стороны содержания. Автоматическое аннотирование востребовано во многих областях от безопасности до научных исследований, позволяет сократить время работы многих специалистов.

О поиске ассоциативных зависимостей в медицинских данных

проф. Рыжов А. П., студентка Лужецкая А. В.

В докладе рассматривается применение алгоритма поиска ассоциативных зависимостей Apriori к результатам общего клинического анализа крови. Рассмотрен вопрос о поиске оптимального метода разбиения данных для улучшения качества правил. Протестирована гипотеза об улучшении показателей достоверности правил путем дискретизации в условиях работы с клиническими данными. Особое внимание уделено специфике применения алгоритма в сфере медицины, поскольку, в отличие от экономики, где приоритет отдается самым распространенным, «стандартным» случаям, медицина оперирует «нестандартными», то есть заболеваниями, отклонениями от нормы. Особенности структуры исследуемых данных вносят коррективы в методы дискретизации и границы допустимых значений для полученных правил.

Возможности и ограничения генеративного интеллекта в задаче синтеза изображений

проф. Рыжов А. П., студентка Егорова А. А.

Доклад посвящен анализу возможностей и ограничений генеративного искусственного интеллекта (ГИИ) в задаче синтеза изображений. Рассматриваются принципы работы ГИИ, способного генерировать новые изображения, дается краткий обзор конкретных инструментов, таких как Flair, Illustroke, PatternedAI и Stockimg, и примеры их использования. Обсуждаются ключевые проблемы ГИИ, включая сложности с генерацией связного текста, созданием и улучшением сложных изображений, пониманием количественных и пространственных понятий. Предлагается подход к преодолению этих ограничений для задачи дизайна на основе нечетких модификаторов и поиска по ним.

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://intsysmagazine.ru/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), для аспирантов ФИО научного руководителя, 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. Список на русском языке приводится в конце файла с текстом статьи, в то время как список, переведённый на английский язык, прилагается отдельным файлом.
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. Авторам бесплатно предоставляется номер журнала, в котором вышла статья. 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://intsysmagazine.ru,

и доступ к ним бесплатный. Там же будут размещены полные тексты всех публикуемых статей.

Подписано в печать: 21.06.2024
Дата выхода: 28.06.2024
Тираж: 200 экз.
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).