XIV Международный семинар
ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ
Москва, МГУ, 20–24 июня 2022 г

А. А. Евдокимов

О направлениях исследования и результатах по дискретному анализу в ИМ СО РАН им. С. Л. Соболева

Метрические и комбинаторные задачи дискретного анализа

- В 2021 г. всего участников 21 : научных сотрудников 14 , аспирантов 5, ведущий инженер и ведущий программист, оба к.т.н.

  9 участников моложе 30 лет.

Лаборатория ИМ СО РАН «Дискретный анализ»

Трое аспирантов защитили диссертации к.ф.- м.н. по 01.01.09. в 2021 году

Облаухов А.К. Метрически регулярные множества в булевом кубе: конструкции и свойства. рук. Токарева Н. Н.

Куценко А.В., Самодуальные бент-функции и их метрические свойства . рук. Токарева Н. Н.

Быков И.С. Конструкции циклов с локальными ограничениями в булевом n-мерном кубе. Рук. Евдокимов А.А. Пережогин А.Л.

- А. А. Евдокимов. Дискретный анализ: направления, результаты, история развития. В книге «Очерки об Институте математики им. С.Л.Соболева» Изд-во Института математики, 2017. С. 291–317.

  К 60- летию ИМ и Международной конференции «Математика в современном мире», 14-20 августа 2017 г.

  Книга с фотографиями > 700 стр.

Юрий Иванович Журавлёв (1935 - 2022)

Основные направления наших исследований

- Дискретные функции и структуры.
- Кодирование структурированной информации и вложения дискретных метрических пространств и графов в классе отображений ограниченного искажения.
- Коды, **криптография**, комбинаторные конфигурации.
- Свойства типичных дискретных объектов, асимптотические формулы числа объектов.
- Комбинаторика слов и сложность символьных последовательностей.
- Задачи анализа, синтеза и сложности схем вычисления дискретных функций, включая модели функционирования генных сетей.

НГУ каф. Теоретическая кибернетика, ММФ, каф. Дискр анализ и иссл. операций, ФИТ

10 направлений, в том числе

- Дискретный анализ и комбинаторика
- Криптология
- Теория графов
- Теория кодирования
- Дискретные математические модели генных сетей (2012, Москва)
- + направления по исследованию операций

Криптографический Центр

Центр создан на базе Института математики им. С.Л.Соболева, лаборатории криптографии ФИТ НГУ, Международного математического центра в Академгородке, Новосибирского государственного университета.

Руководитель: Наталья Николаевна Токарева.

Tokareva N. Bent functions: results and applications to cryptography // Acad. Press. Elsevier, 2015. 220 pages.

Криптография и информационная безопасность

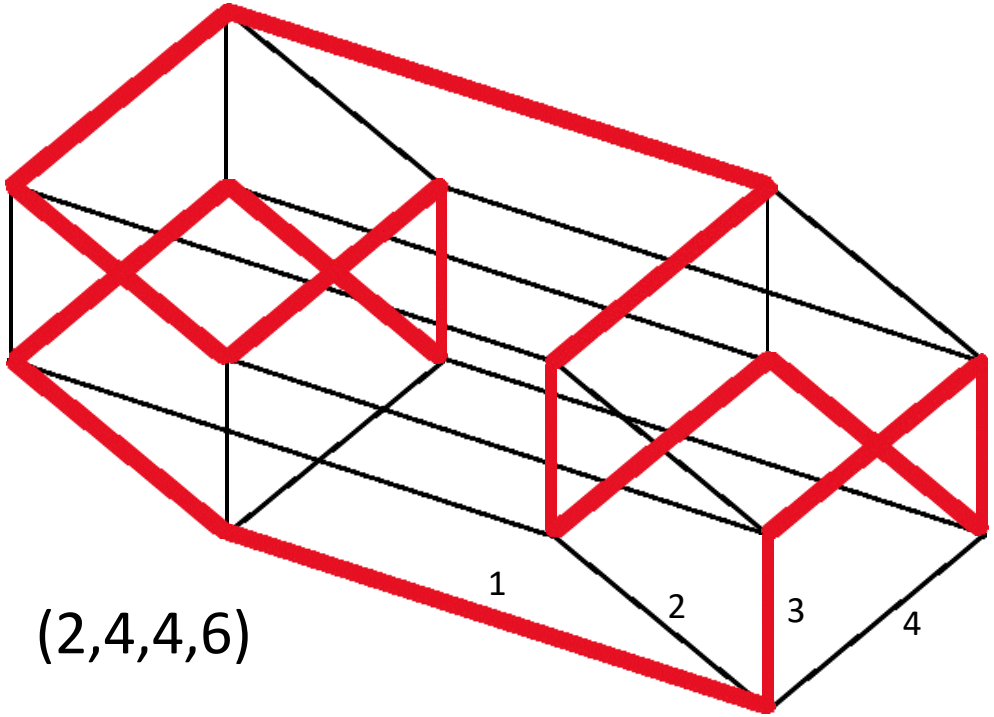
1) криптографические булевы функции, коды и метрически регулярные множества:
2) блочные шифры и S-блоки;
3) устойчивость современных шифров к различным типам криптоанализа:
4) SAT-решатели для криптоанализа:
5) квантовые вычисления и криптография:
6) технологии блокчейн и их приложения;

Важнейшие научные результаты ИМ СО РАН 2021г.

Направление

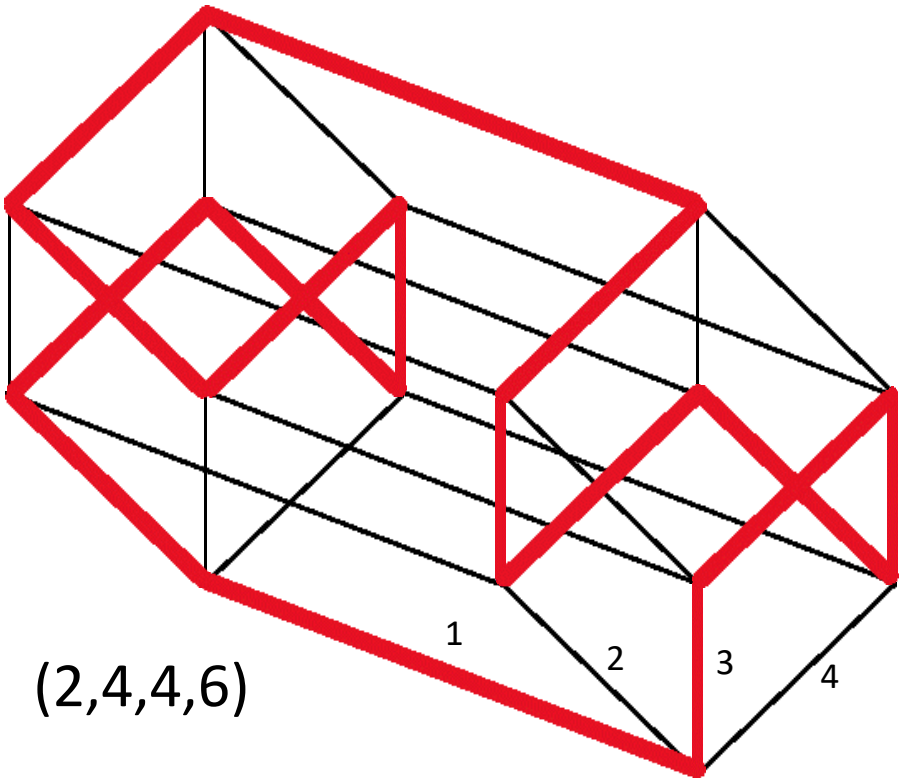
Дискретная математика, информатика и математическая кибернетика

Описано множество кортежей, являющихся спектрами гамильтоновых циклов в n-кубе.
(Пережогин А.Л. совместно с Малых А.Е.)



(2,4,4,6)

Спектром гамильтонова цикла (кода Грея) в булевом **n- кубе** называется кортеж из n чисел, где i-ое число равно количеству ребер i-го направления в цикле. Известны необходимые условия существования гамильтонова цикла с фиксированным спектром: **все числа в спектре четные и сумма любых k из них не меньше 2^k.**



(2,4,4,6)

Доказано, что эти необходимые условия являются достаточными. Это окончательное решение широко известной задачи, в частности, сформулированной Д. Кнутом в 2009 г. в 4-м томе «Искусство программирования». Ранее при перечислении классов эквивалентности кодов Грея задача была решена для $n < 7$, а в [1] для $n = 7$ и 8. В 2012 году В.Н. Потапов получил условно асимптотическое решение. В [2] Пережогиным дано полное решение для любой размерности.

1. Малых А. Е., Пережогин А. Л. Конструктивный подход к перечислению спектров кодов Грея в булевых кубах малых размерностей // *Вестник НГУ. Серия: Информационные технологии*,**15**:4 (2017), С. 32–42.
2. Perezhogin A.L. On the spectrum of Hamiltonian cycles in the n-cube. *Journal of Combinatorial Theory*, *Series B* 151 (2021), P. 435–464.

Методы конструирования

1. Т. Бакош в книге A d a m A. Truth Functions and the Problem of their Realization by Two-Terminal. Graphs// Akad.emiai Kiad.o,1968. c.28 -37. **Равномерный спектр, индукция n --> n+2.**

2. Евдокимов А. А. О нумерации подмножеств конечного множества // Методы дискретного анализа в решении комбинаторных задач. 1980. Т.34. С. 8–26. **Гиперкуб как n-мерный тор.**

3. Goddyn L., Gvozdjak P. Binary Gray codes with long bit runs // Electron. J. Comb. 2003. Vol.10, R.27. **Обобщение - потоковая конструкция.**

4. Потапов В.Н. Построение гамильтоновых циклов с заданным спектром направлений рёбер в булевом n-мерном кубе // Дискрет. анализ и исслед. опер. 2012. Т. 19, № 2. С.75–83. **Асимптотическая конструкция.**

гиперкуб как тор $C_2^n = C_2 \times \ldots \times C_2$

- В торических и потоковых конструкциях кодов Грея работает представление n-куба как к-мерного тора с соответствующей метрикой (Хемминга или Ли). Рёбра булева n-куба можно считать циклами длины 2. а в общем случае это гамильтоновы циклы в подкубах при разложении n-куба в декартово произведение.

- Любой цикл (и гамильтонов) в гиперкубе размерности n можно закодировать круговым словом в алфавите ортов **<** 1, 2, 3,… n >. Например, цикл на **рис 1** запишется кодовым словом
- 1 2 4 **2 3 4 2 4 1 4 3 4** 2 3 4 3.

Свойством несамопересекаемости цикла будет отсутствие в нём подслов (отрезков), в которые все буквы входят четное число раз.Например, в выделенном подслове буква **1** входит один раз, а остальные чётное число раз. «Кодирование последовательностями переходов с запретами подслов» широко используется в компьютерном анализе цепей и циклов, в частности, в проблеме «Змея в ящике».

Я не раз отмечал, что в проблеме «Змея в ящике» (близкой к кодам Грея) правильнее ассоциировать задачу конструуирования змеи не с упаковкой цепи в коробку, а с траекториями в n-мерных торических решётках. На этом пути был найден порядок величины максимальной длины змеи $L(n) > Const \cdot 2^n$, и конструкция цепных (n,d)-кодов для $d > 2$.

Евдокимов А. А., Цепные коды и Snake-in-the-Box Problem, Учён. зап. Казан. гос. ун-та. **156**, № 3, Казань, 2014, 55–65

Нерешённая задача

Пусть L(*n*) - наибольшая длина слова в *n*-буквенном алфавите, в любое подслово-отрезок которого длины не меньшей двух хотя бы две буквы входят нечетное число раз. Существует ли предел ?

$$\lim_{n \to \infty} l(n)/2^n ?$$

А.А.Евдокимов

(Задача есть на сайте кафедры Дискретной математики ММФ МГУ)

Коды типа Грея, их вариации и обобщения продолжают интенсивно исследоваться и в связи с приложениями. Главное: конструкции алгоритмы реализациии и их сложность . Литература широко представлена, например, в статье.

Пережогин А. Л., Быков И. С.. Обзор конструкций и свойств кодов Грея. Сборник Математические вопросы кибернетики. 2022

Нерешённая задача

- Для каких n существует двоичный код Грэя, у которого номера позиций, в которых происходят любые (n-1) последовательных изменений разрядов, все различны?

  А.А.Евдокимов

(Этот вопрос есть на сайте кафедры дискретной математики ММФ МГУ)

Количество кодов Грея

- Фрэнк Харари. 1964. Комбинаторные задачи перечисления графов. С 107-140. (в книге «Прикладная комбинаторная математика», сборник переводов статей под редакцией М. Деза. 1968). Ссылка дана на статью

- G i l b e r t E. N. Gray codes and paths on the n-cube //The bell system technical journal.1958. V. 37, No 3.—P. 815–826.

Количество кодов Грея

n	Hn	hn
2	2	1
3	12	1
4	2688	9
5	1813091520	237675
6	*23 знака*	*18 знаков*

Число гамильтоновых циклов

F e d e r T., S u b i C. Nearly Tight Bounds on the Number of Hamiltonian Circuits of the Hypercube and Generalizations // Inform. Process.Lett. 2009. V. 109, No 5. P. 267–272.

$$\left(\frac{n\log 2}{e\log\log n}(1-o(1))\right)^{2^n} \le H_n \le \frac{1}{2}(n!)^{\frac{2^n}{2n}}((n-1)!)^{\frac{2^n}{2(n-1)}}$$

В важнейших научных результатах ИМ СО РАН 2021г. Федоряева Татьяна Ивановна.

На основе типичных свойств метрических шаров, содержащихся в графе, найден радиус почти всех n-вершинных графов фиксированного диаметра k. Описана структура и спектр центра почти всех таких графов. **Найдены векторы разнообразия шаров.**

T. I. Fedoryaeva. On radius and typical properties of n-vertex graphs of given diameter // Siber. Electr. Math. Reports. **18**:1 (2021), 345–357.
T. I. Fedoryaeva. Center and its spectrum of almost all n-vertex graphs of given diameter // Siber. Electr. Math. Reports, **18**:1 (2021), 511–529.

Полученные Татьяной Ивановной Федоряевой результаты о структурных свойствах типичных графов произвольного диаметра значительно расширяют наши представления о метрической структуре типичных графов.

Подробнее в её докладе завтра.

Т. И. Федоряева. Строение вектора разнообразия шаров типичного графа заданного диаметра,

Сиб. электрон. матем. изв. **13** (2016), 375–387

Раздувающиеся шары в графе

- Изучались векторы разнообразия шаров (i-я компонента вектора равна числу различных шаров радиуса i) обыкновенных связных графов. Решена проблема характеризации векторов разнообразия шаров графов малого диаметра.
- А. А. Евдокимов, Т. И. Федоряева, О проблеме характеризации векторов разнообразия шаров, *Дискрет. анализ и исслед. операций*, **21**:1 (2014), 44–53

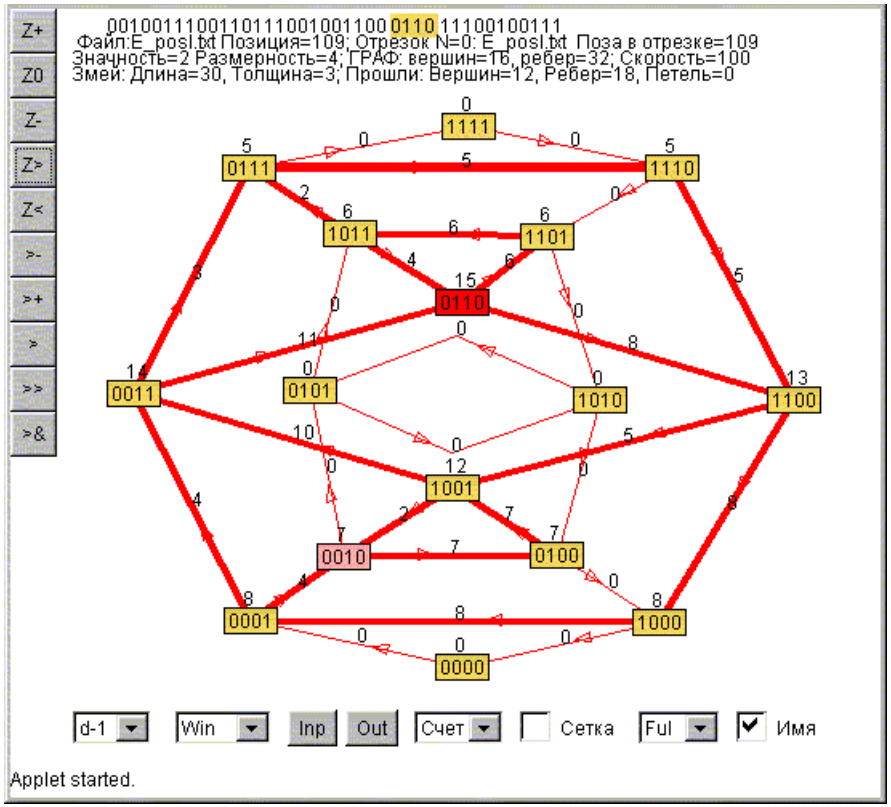
Комбинаторика слов, сложность символьных последовательностей. Графы де Брёйна

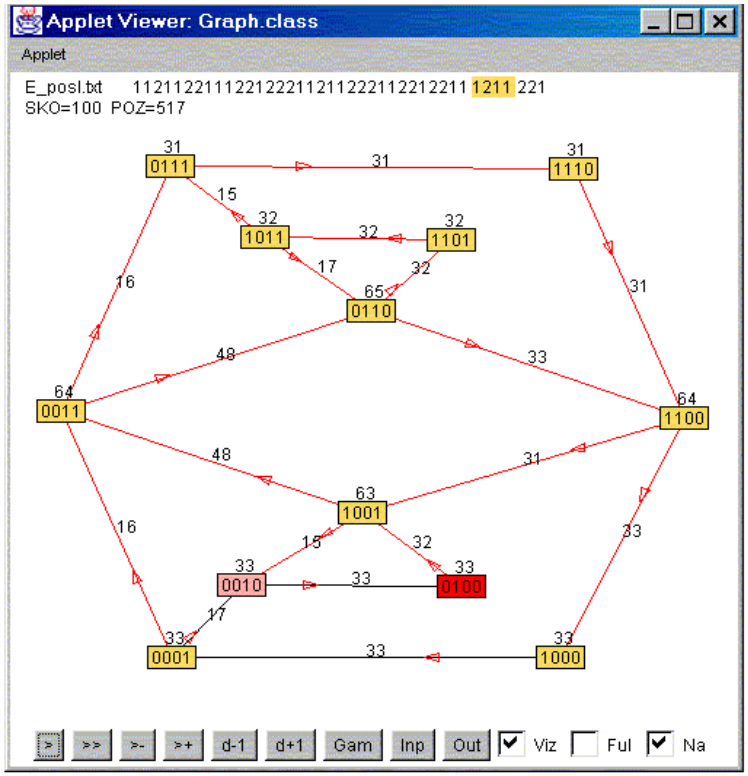
Визуализация символьных последовательностей на структурах перекрытия слов.

Евдокимов А.А., Левин А.А. Графические модели и комбинаторика генетических и математических символьных последовательностей. Вычислительные технологии. 2002, Том 7.

Евдокимов А.А. Анализ, сложность и реконструкция символьных последовательностей. Вестник ТГУ, 2005, N 14, С. 4-12

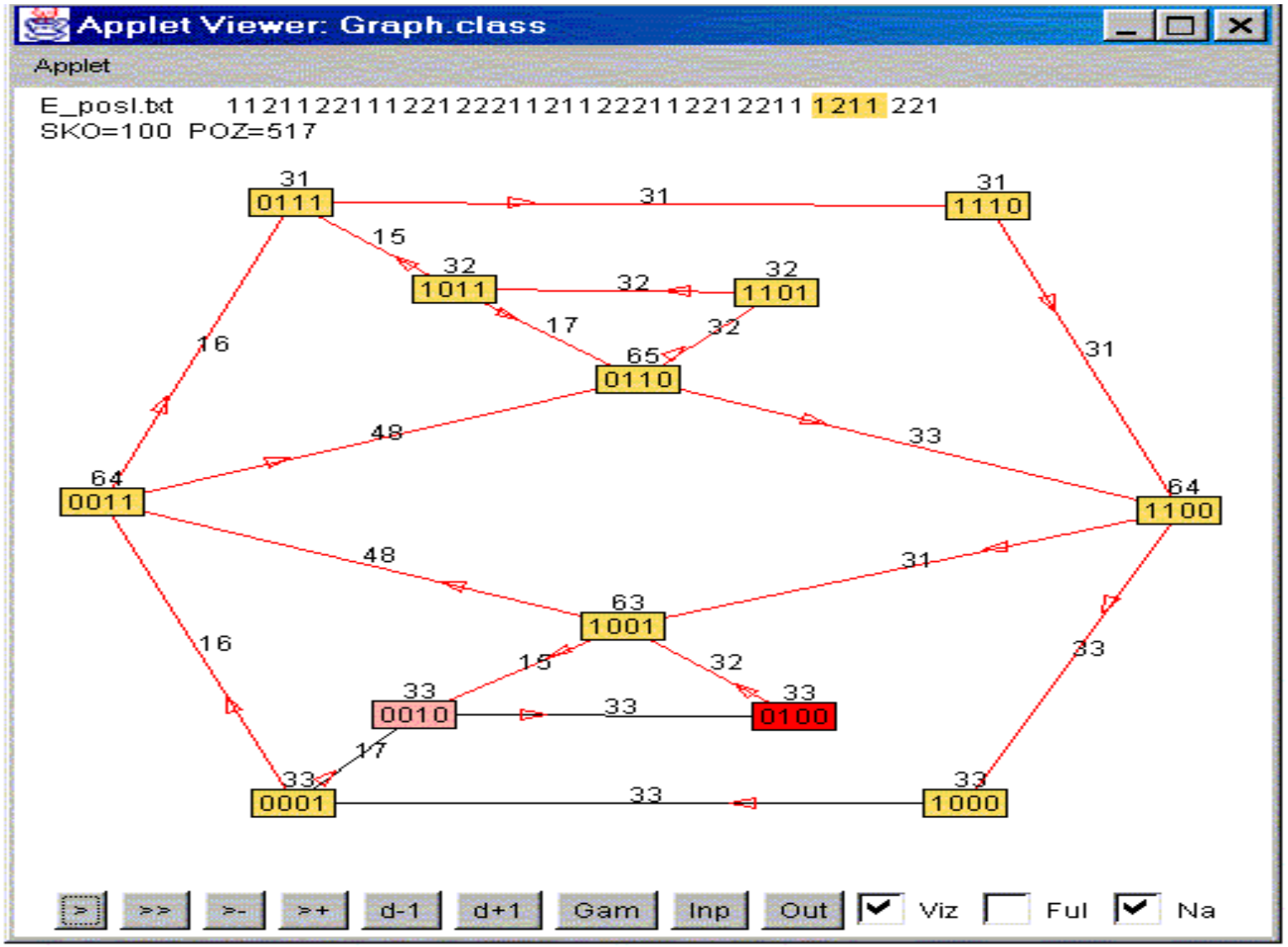
Вложение E - последовательности в графы де Брёйна (de Bruijn graphs) Dim = 4





Вложения в графы перекрытия слов, графы де Брёйна (de Bruijn graphs).

Dir



«Портреты» и свойства Е-последовательности в двоичном алфавите на графе де Брёйна dim = 4.

Е-п. определяется совместной рекурсией

$a_1 = 0;\quad b_1 = 1;\ a_{k+1} = a_k\ 0\ b_k;\quad b_{k+1} = a_k\ 1\ b_k;\quad к = 1,2,\ldots$

Тогда $a_2 = 001$, $b_2 = 011$, $a_3 = 0010011$, $b_3 = 0011011$,

и для любого к $|a_k| = |b_k| = 2^k - 1$.

Для слов a_k выполняется свойство префиксной вложимости: $a_1 \subset a_2 \subset a_3 \subset a_4 \subset a_5 \ldots$,

и потому определена Е-п.

$$E = \lim_{n\to\infty} a_n$$

префиксами которой являются слова a_k .

15 июня 2022, однодневная конф. ИМ-65

А.А. Тараненко *Перманенты многомерных матриц, паросочетания в гиперграфах и трансверсали латинских гиперкубов.*

В важнейших результатах ИМ 2021

Найдена асимптотика числа трансверсалей в латинских гиперкубах, полученных суперпозицией (итерированием) некой бинарной квазигруппы.

Taranenko A. A. Transversals near transversals, and diagonals in iterated groups and quasigroups // Electron. J. Combin., **28**:3 (2021), #3.48, 22 p. DOI: 10.37236/9699

Доказана гипотеза Джексона о цикловом покрытии двудольных графов и найдены необходимые условия суперцикличности двудольных графов.

G(m,n,d) класс двудольных графов с долями X и Y, где |X|=m, |Y|=n, и степенью каждой вершины в X не менее d. Джексон в 1981 году доказал, что, если d не меньше m и $n < 2m-1$, то каждый граф H из G(m,n,d) содержит цикл, покрывающий X, и предположил, что это верно, если $n < 3n-5$, и граф H двусвязен.
Доказана гипотеза Джексона.

[1] ***Kostochka A.***, *Lavrov M., Luo R., Zirlin D.* Conditions for a bigraph to be super-cyclic // Electron. J. Combin., **28**:1 (2021), paper No. 1.2, 19 pp.

Также показано, что в условиях теоремы Джексона граф H не только содержит цикл длины 2m, но для каждого подмножества A из X с |A|>2 граф H содержит цикл, множество вершин которого в X есть в точности A. Назовем такие графы суперциклическими. Найдены необходимые свойства суперцикличности двудольного графа, и описано несколько классов графов, для которых эти свойства достаточны.

[2] ***A. Kostochka****, Luo R., Zirlin D.* Super-pancyclic hypergraphs and bipartite graphs // J. Combin. Theory Ser. B, **145** (2020), 450-465.

XI симпозиум «Современные тенденции в криптографии» (CTCrypt 2022) 6-9 июня, г. Новосибирск

Организаторы

Академия криптографии РФ

Математический институт им. В.А. Стеклова РАН

Технич. комитет по стандартизации «Криптографическая защита информации»

При участии

МГУ им. М.В.Ломоносова, ИМ СО РАН им. С.Л.Соболева, Бел ГУ, ФСБ России, ООО Крипто-Про ,ООО Код безопасности, АО ИнфоТеКС и ….

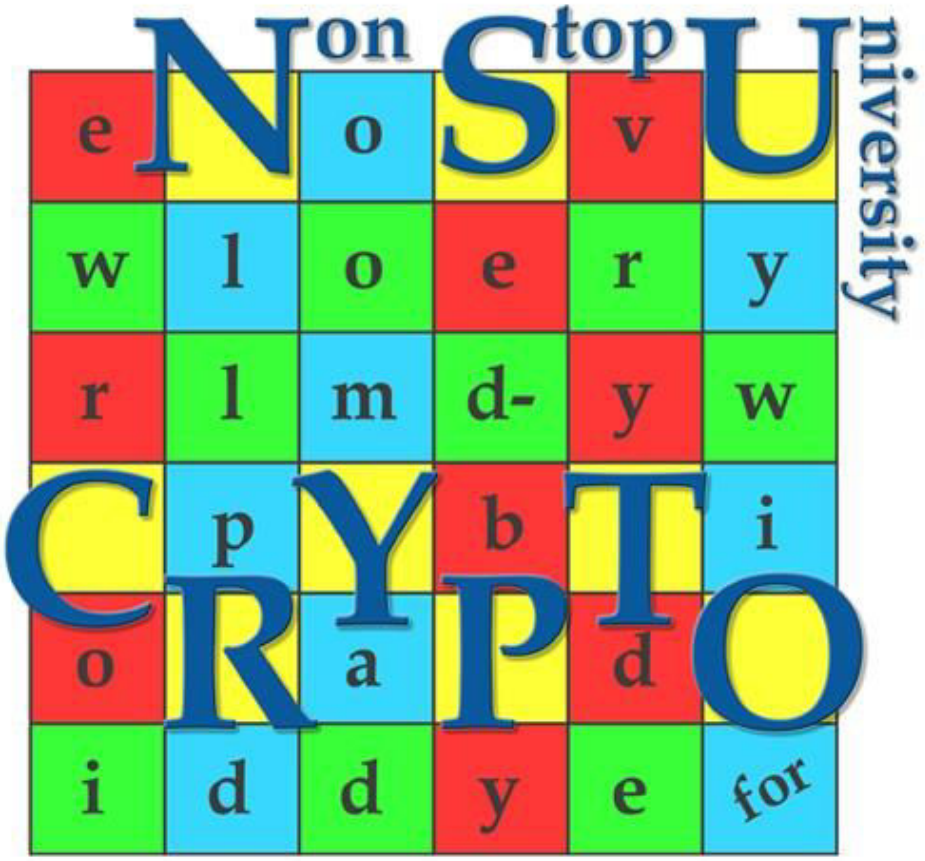
Приглашенный доклад

Криптографический центр (Новосибирск): создание, исследования, перспективы.
Наталья Токарева

Приглашенный доклад

Международная олимпиада по криптографии “Non-Stop University CRYPTO”
Анастасия Городилова, Наталья Токарева

Non-Stop University CRYPTO — единственная международная олимпиада по криптографии.



- За 2014-2021 г. активное участие в олимпиаде приняли более 3000 участников из 64 стран мира По итогам олимпиады публикуются научные статьи с разбором задач, в том числе – нерешенных.

  В 2021 в олимпиаде приняли участие746 студентов, школьников и профессионалов из 33 стран мира. Олимпиада была посвящена 100-летию криптографической службы Российской Федерации.

В олимпиаде 2021 года приняли участие **746 человек из 33 стран мира**.

Летняя школа-конференция по криптографии и информационной безопасности


СИНТЕЗ И
СЛОЖНОСТЬ
УПРАВЛЯЮЩИХ
СИСТЕМ


W = 10111001 = 10·1·1·1·0·0·1, Пред(W) = 6
W⁻¹ = 10011101 = 10·01·1·1·0·1, Сущ(W) = 5.

Спасибо за внимание