МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

На правах рукописи

Кяжин Сергей Николаевич

Характеристики локальной примитивности матриц и орграфов, определяющие свойства систем защиты информации

Специальность 05.13.19 — методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2018

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский ядерный университет «МИФИ»

Научный руководитель — *Фомичев Владимир Михайлович*,
доктор физико-математических наук, профессор

Официальные оппоненты — *Агибалов Геннадий Петрович*,
доктор технических наук, профессор,
Национальный исследовательский Томский государственный университет, профессор кафедры защиты информации и криптографии

Симонов Валерий Михайлович,
доктор физико-математических наук, старший научный сотрудник, Центр информационных технологий и систем органов исполнительной власти, заместитель директора по научной работе

Варфоломеев Александр Алексеевич,
кандидат физико-математических наук, доцент,
Московский государственный технический университет имени Н.Э. Баумана (НИУ), доцент кафедры «Информационная безопасность»

Защита диссертации состоится 16 мая 2018 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.05.01 Московского государственного университета имени М. В. Ломоносова по адресу: 119234, Москва, ГСП-1, Ленинские горы, д.1, главное здание МГУ, механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на сайте ИАС «ИСТИНА»: https://istina.msu.ru/dissertations/102446195/

Автореферат разослан «___» _____ 2018 г.

Ученый секретарь
диссертационного совета,
кандидат физико-математических наук М.А. Кривчиков

Общая характеристика работы

Актуальность темы исследования. Применение информационных технологий во всех сферах общественных отношений порождает новые информационные угрозы. Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента РФ №646 от 5 декабря 2016 года, характеризует состояние научных исследований в области информационной безопасности как недостаточно эффективное (п. 18). Одним из основных направлений обеспечения информационной безопасности является проведение научных исследований в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности (п. 27).

Важную роль при создании средств защиты информации, а также при анализе уровня защищённости информационных систем играют математические модели и методы. В основе исследований математических моделей и методов, использующихся при синтезе или анализе методов и средств защиты информации, лежат свойства отображений. К. Шеннон[1], проводя исследование свойств отображений, важных для систем защиты информации, определил строго не формализуемые свойства преобразования:

а) перемешивание — свойство, выражающееся в существенном усложнении взаимосвязи статистических и аналитических характеристик элементов значения преобразования по сравнению с подобными взаимосвязями элементов аргумента преобразования;

б) рассеивание — свойство, состоящее в том, что каждый элемент аргумента преобразования влияет на большое число элементов значения преобразования.

Работа Шеннона породила многообразные подходы к анализу данных свойств. В основе одного из них лежит следующее свойство. Преобразование g множества X^n, где X — произвольное множество, n — натуральное число, заданное системой координатных функций $\{g_1(x_1,\ldots,x_n),\ldots,g_n(x_1,\ldots,x_n)\}$, называется

[1] Shannon C. E. Communication theory of secrecy systems // Bell System Technical Journal. — 1949. — Vol. 28. — P. 656-715.

совершенным[2], если каждая координатная функция существенно зависит от всех переменных. Если преобразование не является совершенным, то уровень защиты системы понижается, поскольку упрощается вскрытие секретных параметров безопасности системы путём решения системы уравнений (например, с помощью методов последовательного опробования). Кроме того, многие совершенные преобразования обладают свойством распространения искажений, что позволяет их использовать в системах аутентификации.

Ориентированным графом (орграфом) Γ называется пара множеств (V,E), где V — произвольное множество, $E \subseteq V^2$. Под перемешивающими свойствами преобразования[2] понимаются свойства множества $\{S(g_1),\ldots,S(g_n)\}$, где $S(g_j)$ — множество номеров существенных переменных функции $g_j(x_1,\ldots,x_n)$, $j=1,\ldots,n$. Свойства данного множества можно описать с помощью n-вершинного перемешивающего орграфа $\Gamma(g)$, где пара вершин (i,j) образует дугу в графе, если и только если $i \in S(g_j)$. Матрица $A(g)$ смежности вершин графа $\Gamma(g)$ называется перемешивающей матрицей. Преобразование g является совершенным тогда и только тогда, когда матрица $A(g)$ положительная (орграф $\Gamma(g)$ полный).

Для многих композиций преобразований сложность точного вычисления множеств существенной зависимости координатных функций высока, поэтому целесообразно использовать оценочный матрично-графовый подход[3]. Неотрицательная матрица A называется примитивной, если существует такое число γ, что для любого $t \geq \gamma$ матрица A^t является положительной. Наименьшее такое γ называется экспонентом матрицы A и обозначается $\exp A$. Орграф Γ называется примитивным, если существует такое число γ, что для любого $t \geq \gamma$ существует путь длины t из любой вершины графа в любую. Наименьшее такое γ называется экспонентом графа Γ и обозначается $\exp\Gamma$. Орграф Γ и матрица смежности его вершин одновременно примитивны или не примитивны, в случае примитивности их

[2] Фомичев В. М. Методы дискретной математики в криптологии. — М.: Диалог-МИФИ, 2010. — 424 с.
[3] Фомичев В. М., Мельников Д. А. Криптографические методы защиты информации. Часть 1. Математические аспекты / Под ред. В. М. Фомичева. — М.: Издательство ЮРАЙТ, 2016. — 209 с.

экспоненты равны[4]. Использование величины экспонента γ перемешивающего орграфа (перемешивающей матрицы) позволяет сократить вычислительную сложность определения глубины композиции преобразований, при которой достигается свойство совершенности. Если экспонент γ известен, то для преобразований g^t при $t<\gamma$ можно не проверять существенную зависимость каждой координатной функции от всех переменных.

Таким образом, анализ перемешивающих свойств преобразования с помощью матрично-графового подхода — важный этап анализа системы защиты информации.

Требование положительности всех элементов перемешивающей матрицы не всегда является необходимым. Например, для генераторов псевдослучайных последовательностей, построенных на основе регистров сдвига, значения координатных функций, определяющих знаки выходной последовательности, зависят от части переменных. В связи с этим возникает актуальная задача обобщения понятия примитивности матрицы (графа) и исследования соответствующих свойств и характеристик.

Степень разработанности темы исследования. Важными задачами для матрично-графового подхода являются распознавание примитивности перемешивающих матриц (графов) и определение их экспонентов. Данными вопросами занимались такие отечественные и зарубежные учёные, как В. Н. Сачков[5,6], В. Е. Тараканов[6], В. М. Фомичев[4,7,8], А. В. Князев[9], Г. Виландт[10], А. Далмейдж, Н. Мендельсон[11] и другие. Известны универсальный критерий примитивности орграфа Г, универсальные и частные оценки экспонентов орграфов.

---

[4] Фомичев В. М. Оценки экспонентов примитивных графов // Прикладная дискретная математика. — 2011. — №2 (12). — С. 101-112.

[5] Сачков В. Н., Ошкин И. Б. Экспоненты классов неотрицательных матриц // Дискретная математика. — 1993. — Т. 5, №2. — С. 150-159.

[6] Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. — М.: ТВП, 2000. — 448 с.

[7] Фомичев В. М. Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. — 2016. — №3 (33). — С. 78-84.

[8] Фомичев В. М. Оценка экспонента некоторых графов с помощью чисел Фробениуса для трех аргументов // Прикладная дискретная математика. — 2014. — №2 (24). — С. 88-96.

[9] Князев А. В. Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов: диссертация доктора физ.-мат. наук: 01.01.09. — Москва, 2002. — 203 с.

[10] Wielandt H. Unzerlegbare nicht negative Matrizen // Mathematische Zeitschrift. — 1950. — №52. — P. 642-648.

[11] Dulmage A. L., Mendelsohn N. S. Gaps in the exponent set of primitive matrices // Illinois Journal of Mathematics. — 1964. — Vol. 8. — P. 642-656.

Обобщение понятия экспонента впервые было дано Р. Бруалди и Б. Лиу[12] в 1990 году, оно относилось к примитивным графам. Локальным экспонентом вершины i орграфа Г названо такое наименьшее натуральное γ, что для любого $t \geq \gamma$ в Г имеется путь длины t из i в любую вершину. Позже было дано соответствующее определение локальной примитивности орграфа, получена универсальная оценка локального экспонента. Результаты работ[12,13,14,15] по локальной примитивности согласно данному определению касаются примитивных орграфов или используют обобщения понятия примитивности и экспонента, которые не ориентированы на использование в рамках матрично-графового подхода к анализу перемешивающих свойств преобразований, используемых в системах защиты информации.

Несмотря на указанные результаты, актуальной остаётся задача исследования свойств и характеристик локальной примитивности, в особенности в отношении непримитивных орграфов.

Цель работы — развитие математического аппарата исследования локальной примитивности матриц и орграфов (в том числе непримитивных), определяющих свойства систем защиты информации.

Для достижения поставленной цели в диссертации решены следующие **задачи**.

1. Получены свойства примитивных матриц, связанные с количеством положительных элементов в матрице.

2. Получен критерий примитивности сплетения орграфов.

3. Для различных классов орграфов получены условия локальной примитивности и оценки локальных экспонентов.

4. Описано строение локально примитивных орграфов, разработаны принципы оптимизации оценок экспонентов и локальных экспонентов орграфов.

5. Получены условия локальной примитивности и оценки локальных экспонентов перемешивающих графов преобразований множества состояний

[12] Brualdi R., Liu B. Generalized exponents of primitive directed graphs // Journal of Graph Theory. — 1990. — №14. — P. 483-499.
[13] Shen J., Neufeld S. Local exponents of primitive digraphs // Linear Algebra and its Applications. — 1998. — №268. — P. 117-129.
[14] Liu B. Generalized exponents of Boolean matrices // Linear Algebra and its Applications. — 2003. — №373. — P. 169-182.
[15] Huang Y., Liu B. Generalized *r*-exponents of primitive digraphs // Taiwanese Journal of Mathematics. — 2011. — Vol. 15, №5. — P. 1999-2012.

генераторов псевдослучайных последовательностей с равномерным и неравномерным движением информации (двухкаскадный генератор на основе последовательного соединения регистров сдвига, генератор «1–2 шагов», генератор с перемежающимся шагом, генератор типа A5/1).

Положения, выносимые на защиту. На защиту выносятся следующие основные результаты.

1. Критерий примитивности сплетения орграфов.

2. Условия локальной примитивности и оценки локального экспонента для различных классов орграфов в зависимости от особенностей строения орграфа.

3. Принципы оптимизации оценок экспонентов и локальных экспонентов орграфов, учитывающие свойства множеств контуров орграфа.

4. Полученные с использованием теоретических результатов условия локальной примитивности и оценки локальных экспонентов для перемешивающих графов преобразований множества состояний генераторов псевдослучайных последовательностей с равномерным и неравномерным движением (двухкаскадные генераторы на основе последовательного соединения регистров сдвига, генераторы «1–2 шагов», генераторы с перемежающимся шагом, генераторы типа A5/1).

Соответствие диссертации паспорту специальности. Диссертация соответствует паспорту специальности 05.13.19 в части п. 1 «Теория и методология обеспечения информационной безопасности и защиты информации», п. 9 «Модели и методы оценки защищённости информации и информационной безопасности объекта», п. 13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Теоретическая значимость работы. Разработанный автором математический аппарат существенно расширяет предметную область исследований локальной примитивности в части непримитивных матриц и графов.

Практическая значимость работы. Результаты работы расширяют область применения матрично-графового подхода к анализу перемешивающих свойств преобразований, используемых в системах защиты информации; применение

полученных автором результатов позволяет более точно оценивать перемешивающие свойства преобразований.

Методология исследования. Методы теории групп (полугрупп), комбинаторики и теории графов.

Достоверность результатов обеспечивается строгим математическим доказательством утверждений и подтверждается их согласованностью с данными, полученными в ходе вычислительных экспериментов. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Научная новизна работы характеризуется следующими новыми результатами автора.

1. Получен критерий примитивности сплетения ориентированных графов.
2. Для различных классов орграфов получены условия локальной примитивности и оценки локального экспонента.
3. Впервые описано строение орграфов, обладающих свойством локальной примитивности.
4. На основе анализа множества контуров графа разработаны принципы оптимизации оценок экспонентов и локальных экспонентов орграфов.
5. Получены условия локальной примитивности и оценки локальных экспонентов перемешивающих графов преобразований множества состояний генераторов псевдослучайных последовательностей с равномерным и неравномерным движением информации.

Публикации по теме диссертации. Основное содержание диссертации и результаты проведённого исследования изложены в 14 опубликованных научных работах, в том числе в 5 работах — в журналах, индексируемых системами Scopus, RSCI.

Апробация результатов. Основные результаты исследования докладывались на следующих научных семинарах и всероссийских конференциях:

- XI Всероссийская конференция «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT’12 (3–7 сентября 2012 г., г. Иркутск);

- XII Всероссийская конференция «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT’13 (2–7 сентября 2013 г., г. Томск);

- XIII Всероссийская конференция «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT’14 (8–13 сентября 2014 г., г. Екатеринбург);

- XIV Всероссийская конференция «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT’15 (7–12 сентября 2015 г., г. Новосибирск);

- XV Всероссийская конференция «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT’16 (5–10 сентября 2016 г., г. Новосибирск);

- XVI Всероссийская конференция «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT’17 (4–9 сентября 2017 г., г. Красноярск);

- XIX Всероссийская конференция «Проблемы информационной безопасности в системе высшей школы» (30–31 января 2012 г., г. Москва);

- научный семинар «Математические методы криптографического анализа» кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова (2015 г.);

- научно-практический семинар Центра специальных разработок Министерства обороны Российской Федерации (2015, 2017 гг.).

Структура и объём работы. Представленная работа состоит из введения, четырёх глав, заключения, списка сокращений и условных обозначений, списка литературы, списка иллюстративного материала и двух приложений. Диссертация изложена на 125 страницах, содержит 22 иллюстрации и 8 таблиц. Список литературы включает 48 наименований.

Основное содержание работы

Во **введении** обосновывается актуальность темы исследования и определяется степень её разработанности, формулируются цель, задачи исследования.

В **главе 1** получены алгебраические и весовые свойства примитивных матриц и орграфов, доказан критерий примитивности сплетения орграфов, который можно использовать при исследовании перемешивающих свойств преобразований, реализуемых генераторами псевдослучайных последовательностей с самоуправлением (например, генератором A5/1).

Пусть M_n^0 — множество неотрицательных матриц порядка n над полем действительных чисел, $M_n^{0,1}$ — множество 0,1-матриц порядка n. Матрица $A \in M_n^0$ называется положительной (*s*-положительной, *c*-положительной), если она не содержит нулевых элементов (строк, столбцов).

Носителем неотрицательной матрицы $A=(a_{i,j})$ называется 0,1-матрица $\nu(A)=(\nu a_{i,j})$, где $\nu a_{i,j}=1$, если $a_{i,j}>0$, $\nu a_{i,j}=0$, если $a_{i,j}=0$. На множестве $M_n^{0,1}$ рассмотрим операции $\pm$ и $*$, где $A \pm B=\nu(A+B)$, $A*B=\nu(AB)$. Множество $N(A)=\{\nu(A^k),\ k=0,1,\ldots\}$ образует циклическую полугруппу относительно операции $*$.

Периодом вершины орграфа называется наибольший общий делитель длин всех контуров, содержащих данную вершину. Если орграф сильно связен (матрица смежности его вершин неразложима), то все его вершины имеют одинаковый период, называемый также к-периодом орграфа (матрицы).

Утверждение 1.6. Пусть неразложимая матрица $A=(a_{i,j})$ с к-периодом q имеет тип (d,τ) в полугруппе $N(A)$, где d — циклическая глубина, τ — период. Тогда $\tau=q$, и если матрица A примитивная, то $\tau=1$, $d=\exp A$.

Если неразложимая матрица A имеет тип (d,τ), то для распознавания её примитивности достаточно проверить положительность матриц из конечного множества $\{A^d,\ldots,A^{d+\tau-1}\}$.

Количество положительных элементов неотрицательной матрицы A порядка n назовём весом матрицы A и обозначим через $\|A\|$. Следующая теорема характеризует связь веса и экспонента неотрицательных матриц.

Теорема 1.1. Пусть A — неотрицательная матрица порядка $n>2$. Тогда:

а) любая матрица A веса $k\le n$ не является примитивной и для любого $k\in\{n+1,\dots,n^2-n+1\}$ существует непримитивная матрица A веса k;

б) любая матрица A веса $k\in\{n^2-n+2,\dots,n^2-1\}$ является примитивной, где $\exp A=2$, и для любого $k\in\{2n-1,\dots,n^2-n+1\}$ существует такая примитивная матрица A веса k, что $\exp A=2$;

в) для любого $k\in\{n+1,\dots,n^2-n+1\}$ существует такая примитивная матрица A веса k, что $n+2\left\lfloor\sqrt{2(n-1)}\right\rfloor\le\exp A+\|A\|\le n^2-n+3$.

Также установлено, что не для всякой примитивной матрицы вес является монотонно неубывающей функцией от её степени.

Получен критерий примитивности сплетения орграфов. Сплетением орграфа $\Gamma_1=(V_1,E_1)$ с орграфом $\Gamma_2=(V_2,E_2)$ называется орграф $\Gamma_1\circ\Gamma_2=(V,E)$, где $V=V_1\times V_2$, $E=\{((v_1,v_2),(v_1',v_2')):(v_1,v_1')\in E_1$ или $v_1=v_1',(v_2,v_2')\in E_2\}$.

Теорема 1.2. Орграф $\Gamma_1\circ\Gamma_2$ примитивен тогда и только тогда, когда выполнено хотя бы одно из условий:

а) Γ_1 примитивен; в этом случае $\exp(\Gamma_1\circ\Gamma_2)\le\exp\Gamma_1$;

б) Γ_1 сильно связен, и $E_2\ne\varnothing$.

В **главе 2** представлен математический аппарат локальной примитивности неотрицательных матриц и ориентированных графов. Данный аппарат обобщает и существенно расширяет область применения матрично-графового подхода к анализу перемешивающих свойств преобразований, используемых в системах защиты информации.

Обозначим: $\mathbb{N}$ — множество натуральных чисел, $\mathbb{N}_0=\mathbb{N}\cup\{0\}$, $\mathbb{N}_n=\{1,\dots,n\}$. Пусть $I=\{i_1,\dots,i_k\}$, $J=\{j_1,\dots,j_r\}$, $0<k,r\le n$, $\varnothing\ne I,J\subseteq\mathbb{N}_n$, $A\in M_n^{0,1}$, $A(I\times J)$ — подматрица

матрицы A размера $k\times r$, полученная путём удаления из A строк с номерами $i\notin I$ и столбцов с номерами $j\notin J$. Матрицу $A(I\times J)$ обозначим $A(J^2)$ при $I=J$, $A(*J)$ при $I=\mathbb{N}_n$, $A(I*)$ при $J=\mathbb{N}_n$.

Матрицу A назовём $I\times J$-положительной ($I\times J$-s-положительной, $I\times J$-c-положительной), если матрица $A(I\times J)$ положительна (s-положительна, c-положительна). Неотрицательную матрицу A назовём $I\times J$-примитивной (J^2-примитивной при $I=J$, $*J$-примитивной при $I=\mathbb{N}_n$, $I*$-примитивной при $J=\mathbb{N}_n$), если существует такое число $\gamma\in\mathbb{N}$, что матрица $A^t(I\times J)$ ($A^t(J^2)$, $A^t(*J)$, $A^t(I*)$) положительна при любом $t\geq\gamma$. Наименьшее такое γ назовём $I\times J$-экспонентом (J^2-экспонентом, $*J$-экспонентом, $I*$-экспонентом) матрицы A, обозначим $I\times J$-exp$A$ (J^2-exp$A$, $*J$-exp$A$, $I*$-exp$A$).

При допустимых I,J (за исключением случая $I=J=\mathbb{N}_n$) $I\times J$-примитивные матрицы будем называть локально примитивными, их $I\times J$-экспоненты — локальными экспонентами.

Утверждение 2.2. Матрица A является $I\times J$-примитивной тогда и только тогда, когда $A^t(I\times J)>0$ при $t=d,\ldots,d+\tau-1$, где (d,τ) — тип матрицы A в циклической полугруппе $N(A)$, при этом $I\times J$-exp$A$ равен такому наименьшему натуральному числу $\gamma\leq d$, что $A^t(I\times J)>0$ при любом $t\in\{\gamma,\ldots,d\}$.

Таким образом, проблема распознавания локальной примитивности матрицы алгоритмически разрешима.

Орграф Γ назовём $I\times J$-примитивным ($i\times j$-примитивным при $I=\{i\}$, $J=\{j\}$), если существует такое $\gamma\in\mathbb{N}$, что для любых $(i,j)\in I\times J$ в Γ имеются пути из i в j любой длины $t\geq\gamma$, наименьшее такое γ назовём $I\times J$-экспонентом ($i\times j$-экспонентом) орграфа Γ и обозначим $I\times J$-expΓ ($i\times j$-expΓ). Орграф Γ $I\times J$-примитивный тогда и только тогда, когда матрица A смежности его вершин $I\times J$-примитивная, $I\times J$-exp$A=I\times J$-expΓ. При допустимых I,J (за исключением случая $I=J=\mathbb{N}_n$) $I\times J$-примитивные орграфы

называются локально примитивными, их $I\times J$-экспоненты — локальными экспонентами. Обозначим для $I\times J$-примитивного графа Г: $\gamma_{I\times J}=I\times J$-exp Г.

Обозначим для орграфа Г: len$w$ — длина пути w, spc$W$ — множество длин путей из множества путей W, $l_{i,j}$ — длина кратчайшего пути из i в j; $\rho(I,J)=\min\limits_{(i,j)\in I\times J} l_{i,j}$ ($\rho(i,J)=\rho(I,J)$ при $I=\{i\}$, $\rho(I,j)=\rho(I,J)$ при $J=\{j\}$); $\theta(I,J)=\max\limits_{i\in I}\rho(i,J)$ ($\theta(I,j)=\theta(I,J)$ при $J=\{j\}$); $\tilde{U}$ — множество вершин компоненты сильной связности (кратко — ксс) U.

Пусть $W(i,j)$ ($P(i,j)$) — множество (простых) путей в орграфе Г из вершины i в вершину j.

Утверждение 2.6. а) Если орграф Г является $I\times J$-примитивным, то $W(i,j)\neq\varnothing$ для любых $(i,j)\in I\times J$.

б) Орграф Г является $I\times J$-примитивным тогда и только тогда, когда Г является $i\times j$-примитивным для любых $(i,j)\in I\times J$, при этом $\gamma_{I\times J}=\max\limits_{(i,j)\in I\times J}\gamma_{i\times j}$.

Для вершин i,j орграфа Г ксс U орграфа Г назовем i,j-связывающей (кратко i,j-ксс), если в $W(i,j)$ есть путь, проходящий через некоторую вершину ксс U.

Утверждение 2.7. Если орграф Г является $i\times j$-примитивным, то Г содержит i,j-ксс.

При исследовании локальной примитивности орграфа возможны два случая в зависимости от расположения вершин i, j в орграфе:

а) вершины i, j взаимно достижимы, то есть принадлежат общей ксс;

б) вершины i, j не принадлежат общей ксс.

Случай а). Пусть U — ксс орграфа Г с множеством вершин порядка u.

Утверждение 2.8. Если $i,j\in\tilde{U}$, то $i\times j$-примитивность ксс U и $i\times j$-примитивность орграфа Г равносильны примитивности ксс U.

Обозначим через $\gcd(a_1,\ldots,a_n)$ ($\mathrm{lcm}(a_1,\ldots,a_n)$) наибольший общий делитель (наименьшее общее кратное) натуральных чисел $a_1,\ldots,a_n$, $g(a_1,\ldots,a_n)$ — число (функция) Фробениуса, где $\gcd(a_1,\ldots,a_n)=1$, определяемое при $n>1$ как наибольшее число, не принадлежащее аддитивной полугруппе $\langle a_1,\ldots,a_n\rangle$, $g(1)=-1$.

Пусть $\hat{C}=\{C_1,\ldots,C_k\}$ — множество простых контуров длины $l_1,\ldots,l_k$ соответственно в орграфе Г. Величину $d=\gcd(l_1,\ldots,l_k)$ назовём индексом множества контуров $\hat{C}$ и обозначим $\mathrm{ind}\hat{C}$. Обозначим $\eta(\hat{C})=dg(l_1/d,\ldots,l_k/d)$. Множество простых контуров $\hat{C}$ назовём примитивным, если $\mathrm{ind}\hat{C}=1$. В примитивной ксс U имеется примитивное множество контуров.

Рассмотрим орграф $U(\hat{C})=C_1\cup\ldots\cup C_k$, являющийся частью орграфа U. В общем случае граф $U(\hat{C})$ имеет $\tau\le k$ компонент связности $U_1(\hat{C}),\ldots,U_\tau(\hat{C})$. В компоненте связности $U_t(\hat{C})$ имеется контур длины λ_t, который проходит через множество всех контуров из $\hat{C}$, принадлежащих $U_t(\hat{C})$, $t=1,\ldots,\tau$.

Утверждение 2.9. Если ксс U примитивная, то для $i,j\in\tilde{U}$ верна оценка:

$$\gamma_{i\times j}\le u(\tau-1)+\eta(\hat{C})+\rho(i,\tilde{U}(\hat{C}))+\theta(\tilde{U}(\hat{C}),j)-\sum_{t=1}^{\tau}(l_t+(t-2)\lambda_t)+1,$$

где $l_1<\ldots<l_k$, $\lambda_1\ge\ldots\ge\lambda_\tau$.

Случай б). Пусть вершина i не достижима из вершины j. Без ущерба для общности положим, что обе вершины i, j не принадлежат i,j-ксс.

Пусть $\mathbb{Z}$ — множество целых чисел, $A+B=\{a+b\colon (a,b)\in A\times B\}$, где $A,B\subseteq\mathbb{Z}$, $a+B=\{a\}+B$, $Y\subset\mathbb{Z}$. Множество Y, содержащее полную систему вычетов по модулю d, называется d-полным. Для d-полного множества Y обозначим через $\xi_d(Y)$ такое наименьшее натуральное число, что для $a=\xi_d(Y),\xi_d(Y)+1,\ldots,\xi_d(Y)+d-1$ в Y имеется число $b\le a$, сравнимое с a по модулю d. При $a\in\mathbb{Z}$, $d\in\mathbb{N}$ для множества $Y\subset\mathbb{Z}$ обозначим $Y(a,d)=\{y\in Y\colon y=a+kd,\ k\in\mathbb{N}\}$.

Лемма 2.1. Орграф Г является $i\times j$-примитивным тогда и только тогда, когда при некотором натуральном d множество $\mathrm{spc}P(i,j)$ является d-полным и при некотором целом a выполнено: $\mathrm{spc}W(i,j)\supseteq\mathrm{spc}P(i,j)+\mathbb{Z}(a,d)$. Если $P\subseteq P(i,j)$, при некотором натуральном d множество $\mathrm{spc}P$ d-полное и $\mathrm{spc}W(i,j)\supseteq\mathrm{spc}P+\mathbb{Z}(a,d)$ при некотором целом a, то орграф Г является $i\times j$-примитивным и $\gamma_{i\times j}\le\xi_d(\mathrm{spc}P)+a+d$. Эта оценка достигается, если $\mathrm{spc}W(i,j)=\mathrm{spc}P(i,j)+\mathbb{Z}(a,d)$.

С использованием леммы 2.1 получены условия $i\times j$-примитивности и оценки $i\times j$-экспонентов орграфов в различных случаях, определяемых взаимным расположением i,j-ксс.

Пусть $U_1,\ldots,U_r$ — ксс в орграфе Γ, $r\in\mathbb{N}$. Последовательность $U^{\rightarrow}=(U_1,\ldots,U_r)$ назовём ксс-цепью длины r, если $r=1$ или при $r>1$ из вершин ксс U_{s-1} достижимы вершины ксс U_s, $s=2,\ldots,r$. Индексом ксс-цепи $U^{\rightarrow}$ назовём $\mathrm{ind}U^{\rightarrow}=\gcd(d_1,\ldots,d_r)$, где d_s — наибольший общий делитель длин всех простых контуров, содержащихся в ксс U_s, $s=1,\ldots,r$.

При $r>1$ множество ксс $\hat{U}=\{U_1,\ldots,U_r\}$ назовём ксс-антицепью порядка r, если из вершин любой ксс множества $\hat{U}$ не достижимы вершины любой другой ксс в $\hat{U}$. Индексом ксс-антицепи $\hat{U}$ назовём $\mathrm{ind}\hat{U}=\mathrm{lcm}(d_1,\ldots,d_r)$.

Назовём ксс-цепь (ксс-антицепь) i,j-связывающей в Γ (кратко — i,j-ксс-цепью, i,j-ксс-антицепью соответственно), если U_s есть i,j-ксс, $s=1,\ldots,r$.

Пусть $\hat{C}=\{C_1,\ldots,C_k\}$ — непустое множество простых контуров орграфа Γ длины $l_1,\ldots,l_k$ соответственно, в Γ имеется i,j-ксс-цепь $U^{\rightarrow}=(U_1,\ldots,U_r)$ со спецификацией $(u_1,\ldots,u_r)$, содержащая множество контуров $\hat{C}$, где $\hat{C}_s$ — подмножество контуров множества $\hat{C}$, принадлежащих ксс U_s, $s=1,\ldots,r$, $1\le r\le k$. Тогда в ксс U_s имеется контур $Z(U_s,\hat{C}_s)$, обходящий все контуры множества $\hat{C}_s$, $s=1,\ldots,r$. Обозначим $u(U^{\rightarrow},\hat{C})=\sum_{s=1}^{r}\mathrm{len}Z(U_s,\hat{C}_s)$.

Подмножество путей из $P(i,j)$, проходящих через все ксс, которые содержат контуры из $\hat{C}$, обозначим $P_{\hat{C}}(i,j)$.

Теорема 2.3. Если в орграфе Γ имеется i,j-ксс-цепь $U^{\rightarrow}$, содержащая множество контуров $\hat{C}$ индекса d, и множество $\mathrm{spc}\,P_{\hat{C}}(i,j)$ является d-полным, то Γ является $i\times j$-примитивным и $\gamma_{i\times j}\le\xi_d(\mathrm{spc}\,P_{\hat{C}}(i,j))+a+d$, где $a=\eta(\hat{C})+u(U^{\rightarrow},\hat{C})$.

Пусть орграф Γ содержит i,j-ксс-антицепь $\hat{U}=\{U_1,\ldots,U_r\}$, $2\le r\le k$. Для $W(i,j)$, $P(i,j)$ верно: $W(i,j)=W_1(i,j)\cup\ldots\cup W_r(i,j)$, $P(i,j)=P_1(i,j)\cup\ldots\cup P_r(i,j)$, где $W_s(i,j)$ ($P_s(i,j)$) — подмножество путей из $W(i,j)$ ($P(i,j)$), проходящих через ксс U_s, $s=1,\ldots,r$. Обозначим: $\delta=\operatorname{ind}\hat{U}$, $H_{d_s}(P_s(i,j))$ — множество вычетов, не содержащихся во множестве $\operatorname{spc}P_s(i,j)$, $s=1,\ldots,r$, $H(P(i,j))=H_{d_1}(P_1(i,j))\times\ldots\times H_{d_r}(P_r(i,j))$, $\Theta(\hat{U})=\bigcup_{s=1}^{r}\left(\operatorname{spc}P_s(i,j)+\bigcup_{\theta=1}^{\delta/d_s}\{a_s+d_s\theta\}\right)$, где $d_s=\operatorname{ind}\hat{C}_s$, $a_s=\eta(\hat{C}_s)+\operatorname{len}Z(U_s,\hat{C}_s)$, $s=1,\ldots,r$.

Если хотя бы для одного $s\in\mathbb{N}_r$ множество $P_s(i,j)$ d_s-полное, то по теореме 2.3 орграф Γ является $i\times j$-примитивным. В противном случае множество $H(P(i,j))$ непусто. При отсутствии решений системы $\{x\equiv b_s \bmod d_s,\ s=1,\ldots,r\}$ для любого набора $(b_1,\ldots,b_r)\in H(P(i,j))$ орграф Γ $i\times j$-примитивный.

Теорема 2.4. Если $i\times j$-примитивный орграф Γ содержит i,j-ксс-антицепь $\hat{U}$, то $\gamma_{i\times j}\le\xi_\delta(\Theta(\hat{U}))$.

Рассмотрено обобщение понятия локальной примитивности матрицы. Матрицу A назовём $I\times J$-квазипримитивной, если существует такое число $\delta\in\mathbb{N}$, что матрица $A^t(I\times J)$ s-положительна для любого $t\ge\delta$. Наименьшее такое δ назовём $I\times J$-квазиэкспонентом матрицы A, обозначим через $I\times J$-$\operatorname{qexp}A$. Также $I\times J$-квазипримитивные матрицы будем называть локально квазипримитивными, а их $I\times J$-квазиэкспоненты — локальными квазиэкспонентами. При $I=J=\mathbb{N}_n$ $I\times J$-квазипримитивность матрицы равносильна s-положительности.

Орграф Γ назовём $I\times J$-квазипримитивным, если и только если $I\times J$-квазипримитивна матрица смежности его вершин, $I\times J$-квазиэкспонент орграфа равен $I\times J$-квазиэкспоненту матрицы.

Глава 3 посвящена определению принципов оптимизации оценок экспонентов и локальных экспонентов орграфов с учётом структурных свойств примитивных (локально примитивных) орграфов.

В общем случае в примитивном орграфе имеется несколько примитивных

множеств простых контуров. Обозначим через $F(\Gamma)$ ($F_p(\Gamma)$) множество всех (примитивных) множеств простых контуров примитивного орграфа Γ. $F(\Gamma)$ образует решётку относительно теоретико-множественного включения, $F_p(\Gamma)$ есть её верхняя подполурешётка. Множество минимальных элементов данной полурешётки обозначим $F_p^{\min}(\Gamma)$. Пусть $\omega(\hat{C})$ — значение оценки экспонента орграфа Γ, зависящей от множества контуров $\hat{C} \in F_p(\Gamma)$. Тогда наилучшая оценка имеет вид:

$$\exp\Gamma \le \min_{\hat{C} \in F_p(\Gamma)} \omega(\hat{C}).$$

Для получения более точной оценки следует прежде всего проанализировать множества $\hat{C} \in F_p^{\min}(\Gamma)$. Получены условия принадлежности $\hat{C}$ множеству $F_p^{\min}(\Gamma)$.

Пусть $A=(a_1,\ldots,a_k)$ — набор взаимно простых в совокупности натуральных чисел, где $1<a_1<\ldots<a_k$. Набор A назовём:

- приведённым, если в нём любое число не кратно любому другому числу;
- тупиковым, если $A=(1)$ или при $k>1$ удаление из набора любого элемента нарушает взаимную простоту чисел;
- r-примитивным, $0 \le r \le k-1$, если после удаления из A любого подмножества порядка r взаимная простота чисел из получившегося набора сохраняется.

Пусть $A=(a_1,\ldots,a_k)$ — приведённый набор натуральных чисел, 2^A — булеан множества $\{a_1,\ldots,a_k\}$, $P(A)$ — множество всех наборов взаимно простых чисел (упорядоченных подмножеств множества 2^A). Определим отношение частичного порядка на множестве 2^A: $(b_1,\ldots,b_l) \le (a_1,\ldots,a_k)$, если и только если $l \le k$ и найдётся такая бесповторная упорядоченная по возрастанию выборка $(i_1,\ldots,i_l)$ из $(1,\ldots,k)$, что b_j делит a_{i_j}, $j=1,\ldots,l$.

Тупиковый набор $B \in P(A)$ назовём минимальным в $P(A)$, если не существует другого такого набора $B' \in P(A)$, что $B' \le B$. Для любого набора B из $P(A)$ имеется хотя бы один такой минимальный тупиковый набор $\Theta(B)$, что $\Theta(B) \le B$. Тупиковый набор

$B \in P(A)$ назовём r-минимальным в $P(A)$, если не существует другого такого набора $B' \in P(A)$ длины r, что $B' \le B$.

Утверждение 3.2. Для любого приведённого набора A взаимно простых чисел $\langle P(A), \le \rangle$ есть верхняя полурешётка, в которой максимальный элемент есть A и любой минимальный элемент — минимальный тупиковый набор.

Следствие 3.1. Если $\hat{C} = \{C_1, \ldots, C_k\}$ — примитивное множество контуров в Г длины $l_1, \ldots, l_k$ соответственно, то полурешётки $F_p(\Gamma)$ и $P(A)$, где $A = (l_1, \ldots, l_k)$, изоморфны.

Отсюда $\hat{C} \in F_p^{\min}(\Gamma)$, если множество длин контуров образует минимальный тупиковый набор.

Получены критерии тупиковости и минимальности набора взаимно простых чисел. Для набора A обозначим: $A_i = \{a_1, \ldots, a_k\} \setminus \{a_i\}$, $\mu_i = \gcd(A_i)$, $i = 1, \ldots, k$.

Теорема 3.1. Набор A является тупиковым набором взаимно простых чисел тогда и только тогда, когда $\mu_1, \ldots, \mu_k$ — попарно взаимно простые числа, отличные от 1. При этом $a_i = c_i \mu_1 \ldots \mu_k / \mu_i$, где $(c_1, \ldots, c_k)$ есть 1-примитивный набор натуральных чисел, $\gcd(c_i, \mu_i) = 1$ для $i = 1, \ldots, k$.

Следствие 3.3. Тупиковый набор A взаимно простых чисел является k-минимальным тогда и только тогда, когда $\mu_1, \ldots, \mu_k$ — простые числа, $c_i = 1$, $i = 1, \ldots, k$.

Описано строение $i \times j$-примитивного орграфа. Пусть $\Gamma(i,j)$ — часть орграфа Г, соответствующая множеству путей $W(i,j)$. Если вершины i, j взаимно достижимы, то для $i \times j$-примитивного орграфа $\Gamma(i,j)$ представляет собой примитивную i,j-ксс. В противном случае $\Gamma(i,j)$ состоит из i,j-ксс, соединённых определённым образом с помощью простых путей, все вершины которых, за исключением, быть может, начальной и конечной, являются ациклическими.

Оценки локального экспонента орграфа Г зависят от характеристик множества простых контуров индекса d в орграфе. В общем случае в локально примитивном орграфе имеется несколько множеств простых контуров индекса d. Множество всех множеств контуров индекса d образует верхнюю подполурешётку $F_d(\Gamma)$ решётки

F(Γ). Множество минимальных элементов полурешётки $F_d(\Gamma)$ обозначим $F_d^{\min}(\Gamma)$.

Пусть $t(\hat{C})$ — значение оценки $i\times j$-экспонента орграфа Γ, зависящей от множества контуров $\hat{C} \in F_d(\Gamma)$. Тогда наилучшая оценка имеет вид: $\gamma_{i\times j} \le \min\limits_{\hat{C}\in F_d(\Gamma)} t(\hat{C})$. Для получения более точной оценки следует прежде всего проанализировать множества $\hat{C} \in F_d^{\min}(\Gamma)$. Получены условия принадлежности $\hat{C}$ множеству $F_d^{\min}(\Gamma)$.

Набор натуральных чисел $A=(a_1,\ldots,a_k)$, $k\ge 1$, назовём d-тупиковым, если $A=(d)$ или при $k>1$ $\gcd(a_1,\ldots,a_k)=d$ и для набора B, полученного из A удалением любого элемента, наибольший общий делитель чисел не равен d. Для приведённого набора $A=(a_1,\ldots,a_k)$ обозначим через $P_d(A)$ множество таких наборов чисел (упорядоченных подмножеств множества 2^A), что наибольший общий делитель чисел из набора равен d. Назовём d-тупиковый набор $B\in P_d(A)$ минимальным, если не существует другого такого набора $B'\in P_d(A)$, что $B'\le B$.

Утверждение 3.5. Для любого приведённого набора $A=(a_1,\ldots,a_k)$, где $k\ge 1$, $\gcd(a_1,\ldots,a_k)=d$, $\langle P_d(A),\le\rangle$ есть верхняя полурешётка, в которой максимальный элемент есть A и любой минимальный элемент — минимальный d-тупиковый набор.

Следствие 3.4. Если $\hat{C}=\{C_1,\ldots,C_k\}$ — множество контуров индекса d в орграфе Γ, то полурешётки $F_d(\Gamma)$ и $P_d(A)$, где $A=(l_1,\ldots,l_k)$ — набор длин контуров $C_1,\ldots,C_k$, изоморфны.

Таким образом, для получения более точной оценки локального экспонента следует выбирать такое множество контуров $\hat{C}$, что длины контуров образуют минимальный d-тупиковый набор.

В **главе 4** полученные теоретические результаты применяются для оценки перемешивающих свойств преобразований, реализуемых генераторами псевдослучайных двоичных последовательностей на основе регистров сдвига с равномерным и неравномерным движением. Получены оценки характеристик локальной примитивности перемешивающих орграфов преобразований множества состояний генераторов.

Обозначим: h — преобразование множества состояний генератора, h_t^s — t-я координатная функция преобразования h^s, t=1,2,…, $\Gamma(h)$ — перемешивающий орграф преобразования h.

Фильтрующий генератор построен на основе двоичного регистра сдвига длины n и фильтрующей булевой функции $\varphi(x)$. В случае регистра правого сдвига с функцией обратной связи $f(x_1,\ldots,x_n)$ преобразование h задаётся следующим образом: $h(x_1,\ldots,x_n)=(f(x_1,\ldots,x_n),x_1,\ldots,x_{n-1})$. При начальном состоянии $(x_1,\ldots,x_n)$ генератора t-й знак выходной последовательности равен $y_t=\varphi(h^t(x_1,\ldots,x_n))$, t=1,2,…

Пусть $S(\varphi)=J$, $S(f)=\{s_1,\ldots,s_\mu\}$, $1\le s_1<\ldots<s_\mu=n$, $\gcd(s_1,\ldots,s_\mu)=d$. Тогда для любого $J\subseteq\mathbb{N}_n$ орграф $\Gamma(h)$ $*J$-примитивный тогда и только тогда, когда d=1.

Пусть двухкаскадный генератор построен на основе регистров правого сдвига: управляющего длины m с функцией обратной связи $f_1(x_1,\ldots,x_m)$ и генерирующего длины n с функцией обратной связи $f_2(x_{m+1},\ldots,x_{m+n})$, $m,n>1$. Преобразование h задаётся системой координатных функций $\{h_1(x_1,\ldots,x_{m+n}),\ldots,h_{m+n}(x_1,\ldots,x_{m+n})\}$, где $h_1(x_1,\ldots,x_{m+n})=f_1(x_1,\ldots,x_m)$, $h_{m+1}(x_1,\ldots,x_{m+n})=x_m\oplus f_2(x_{m+1},\ldots,x_{m+n})$, $h_k(x_1,\ldots,x_{m+n})=x_{k-1}$, k=2,…,m,m+2,…,m+n. При начальном состоянии $(x_1,\ldots,x_{m+n})$ генератора t-й знак выходной последовательности равен $y_t=h_{m+n}^t(x_1,\ldots,x_{m+n})$.

Пусть I={1,…,m}, J={m+1,…,m+n}, $S(f_1)=\{b_1,\ldots,b_\nu\}$, $S(f_2)=\{c_1,\ldots,c_\mu\}$, где $1\le b_1<\ldots<b_\nu=m$, $m+1\le c_1<\ldots<c_\mu=m+n$, $\gcd(b_1,\ldots,b_\nu)=d_1$, $\gcd(c_1-m,\ldots,c_\mu-m)=d_2$.

Утверждение 4.1. Орграф $\Gamma(h)$ является $\mathbb{N}_{m+n}\times\{m+n\}$-примитивным тогда и только тогда, когда $d_2=1$. В случае $\mathbb{N}_{m+n}\times\{m+n\}$-примитивности верна оценка:

$$\mathbb{N}_{m+n}\times\{m+n\}\text{-}\exp\Gamma(h)\le n+\max\{m,\rho_2\}+g(c_1-m,\ldots,c_\mu-m),$$

где $\rho_2=\max\limits_{l\in\mathbb{N}_\mu}\{c_l-c_{l-1}\}$, $c_0=m$, $g(c_1-m,\ldots,c_\mu-m)$ — функция Фробениуса.

Следствие 4.1. Если $c_1=m+1$, то $\Gamma(h)$ является $\mathbb{N}_{m+n}\times\{m+n\}$-примитивным и $\mathbb{N}_{m+n}\times\{m+n\}$-$\exp\Gamma(h)=n-1+\max\{m,\rho_2\}$.

Утверждение 4.2. Орграф $\Gamma(h)$ является $I\times\{m+n\}$-примитивным тогда и только тогда, когда $\gcd(d_1, d_2)=1$. В случае $I\times\{m+n\}$-примитивности верна оценка:

$$I\times\{m+n\}\text{-exp}\Gamma(h)\le m+n+\rho_1+g(b_1,\ldots,b_\nu, c_1-m,\ldots,c_\mu-m),$$

где $\rho_1=\max\limits_{l\in\mathbb{N}_\nu}\{b_l-b_{l-1}\}$, $b_0=1$.

Следствие 4.2. Орграф $\Gamma(h)$ является $I\times\{m+n\}$-примитивным, если:

а) $b_1=1$; в этом случае $I\times\{m+n\}\text{-exp}\Gamma(h)\le m+n+\rho_1-1$;

б) $c_1=m+1$; в этом случае $I\times\{m+n\}\text{-exp}\Gamma(h)=m+n-1$.

Генератор «1–2 шагов» построен на основе управляющего и генерирующего двоичных регистров сдвига длины m и n соответственно, $m,n>2$, с функциями обратной связи $f_1(x_1,\ldots,x_m)$ и $f_2(x_{m+1},\ldots,x_{m+n})$; движение генерирующего регистра на 1–2 шага определено управляющей булевой функцией $u(x_1,\ldots,x_m)$. Подстановки, реализуемые управляющим и генерирующим регистрами, обозначим соответственно через $\varphi(x_1,\ldots,x_m)$ и $\psi(x_{m+1},\ldots,x_{m+n})$. Тогда

$$h^t(x_1,\ldots,x_{m+n})=(\varphi^t(x_1,\ldots,x_m), \psi^{\sigma(t,x_1,\ldots,x_m)}(x_{m+1},\ldots,x_{m+n})),$$

где $\sigma(t,x_1,\ldots,x_m)=\sum\limits_{l=1}^{t}((u(\varphi^l(x_1,\ldots,x_m))\oplus 1)+2u(\varphi^l(x_1,\ldots,x_m)))$, $t=1,2,\ldots$

При начальном состоянии $(x_1,\ldots,x_{m+n})$ генератора t-й знак выходной последовательности равен $y_t=h^t_{m+n}(x_1,\ldots,x_{m+n})$, $t=1,2,\ldots$

Пусть $I=\{1,\ldots,m\}$, $J=\{m+1,\ldots,m+n\}$, $S(f_1)=\{b_1,\ldots,b_\nu\}$, $S(f_2)=\{c_1,\ldots,c_\mu\}$, $1\le b_1<\ldots<b_\nu=m$, $m+1\le c_1<\ldots<c_\mu=m+n$.

Утверждение 4.4. Граф $\Gamma(h)$ является $\mathbb{N}_{m+n}\times\{m+n\}$-примитивным, при этом $\mathbb{N}_{m+n}\times\{m+n\}\text{-exp}\Gamma(h)\le\lceil n/2\rceil+\max\limits_{i\in\mathbb{N}_{m+n}}\rho(i,m+1)+\lambda(\lambda-1)$, где $\lambda=\lceil(c_1-m)/2\rceil$.

Следствие 4.3. При $S(u)=\{m\}$ $\mathbb{N}_{m+n}\times\{m+n\}\text{-exp}\Gamma(h)\le\lceil n/2\rceil+\max\{m,\rho\}+\lambda(\lambda-1)$, где $\lambda=\lceil(c_1-m)/2\rceil$, $\rho=\max\{\lceil(c_2-c_1)/2\rceil,\ldots,\lceil(c_\mu-c_{\mu-1})/2\rceil\}$.

Следствие 4.4. Орграф $\Gamma(h)$ является $I\times\{m+n\}$-примитивным; при $S(u)=\{m\}$ $I\times\{m+n\}\text{-exp}\Gamma(h)\le\lceil n/2\rceil+m+\lambda(\lambda-1)$.

Генератор с перемежающимся шагом построен на базе регистров правого сдвига: управляющего длины m и двух генерирующих длины n и r с функциями обратной связи $f_0(x_1,\ldots,x_m)$, $f_1(x_{m+1},\ldots,x_{m+n})$, $f_2(x_{m+n+1},\ldots,x_{m+n+r})$, $m,n,r>1$. В зависимости от значения управляющей функции $u(x_1,\ldots,x_m)$ сдвигается либо первый, либо второй генерирующий регистр. Подстановки, реализуемые регистрами, обозначим через $\varphi(x_1,\ldots,x_m)$, $\psi(x_{m+1},\ldots,x_{m+n})$ и $\phi(x_{m+n+1},\ldots,x_{m+n+r})$ соответственно. Тогда

$$h^t(x_1,\ldots,x_{m+n+r})=(\varphi^t(x_1,\ldots,x_m),\psi^{\sigma(t,x_1,\ldots,x_m)}(x_{m+1},\ldots,x_{m+n}),\phi^{t-\sigma(t,x_1,\ldots,x_m)}(x_{m+n+1},\ldots,x_{m+n+r})),$$

где $\sigma(t,x_1,\ldots,x_m)=\sum_{l=1}^{t}u(\varphi^l(x_1,\ldots,x_m))$, $t=1,2,\ldots$

При начальном состоянии $(x_1,\ldots,x_{m+n+r})$ генератора t-й знак выходной последовательности равен $y_t=h^t_{m+n}(x_1,\ldots,x_{m+n+r})\oplus h^t_{m+n+r}(x_1,\ldots,x_{m+n+r})$, $t=1,2,\ldots$

Пусть $I=\{1,\ldots,m\}$, $J_1=\{m+1,\ldots,m+n\}$, $J_2=\{m+n+1,\ldots,m+n+r\}$, $u(x_1,\ldots,x_m)=x_m$.

Утверждение 4.5. Орграф $\Gamma(h)$ является:

а) $I\times\{m+n,m+n+r\}$-, $(I\cup J_1)\times\{m+n\}$-, $(I\cup J_2)\times\{m+n+r\}$-примитивным,

$$I\times\{m+n,m+n+r\}\text{-}\exp\Gamma(h)=m;$$

$$\delta_1=(I\cup J_1)\times\{m+n\}\text{-}\exp\Gamma(h)=\max\{m,n-1\},\ \delta_2=(I\cup J_2)\times\{m+n+r\}\text{-}\exp\Gamma(h)=\max\{m,r-1\};$$

б) не $\mathbb{N}_{m+n+r}\times\{m+n,m+n+r\}$-примитивным, но $\mathbb{N}_{m+n+r}\times\{m+n,m+n+r\}$-квазипримитивным, при этом

$$\mathbb{N}_{m+n+r}\times\{m+n,m+n+r\}\text{-}q\exp\Gamma(h)=\max\{\min\{\delta_1,\delta_2\},n-1,r-1\}.$$

Генератор A5/1, используемый в мобильной связи GSM, построен на основе трёх двоичных линейных регистров сдвига (ЛРС) длин 19, 22 и 23. Сумма битов, снимаемых с крайних ячеек ЛРС, образует выходную последовательность.

Пусть генератор состоит из трёх двоичных регистров левого сдвига РС-1, РС-2 и РС-3 длины m, n и r с функциями обратной связи $f_1(x_1,\ldots,x_m)$, $f_2(x_{m+1},\ldots,x_{m+n})$ и $f_3(x_{m+n+1},\ldots,x_{m+n+r})$, $S(f_1)=\{b_1,\ldots,b_\nu\}$, $S(f_2)=\{c_1,\ldots,c_\mu\}$, $S(f_3)=\{d_1,\ldots,d_\sigma\}$. Каждый такт регистр РС-l сдвигается, если $u_l(x_\eta,x_\tau,x_\theta)=x_{\lambda(l)}\oplus x_\eta\,x_\tau\oplus x_\eta\,x_\theta\oplus x_\tau\,x_\theta\oplus 1=1$,

l=1,2,3, $\lambda(1)=\eta$, $\lambda(2)=\tau$, $\lambda(3)=\theta$; $1\le\eta\le m$, $\eta\notin S(f_1)$, $m+1\le\tau\le m+n$, $\tau\notin S(f_2)$, $m+n+1\le\theta\le m+n+r$, $\theta\notin S(f_3)$. Таким образом, управляющая функция суть

$$u(x_\eta, x_\tau, x_\theta)=(u_1(x_\eta, x_\tau, x_\theta), u_2(x_\eta, x_\tau, x_\theta), u_3(x_\eta, x_\tau, x_\theta)).$$

Подстановки, реализуемые регистрами, обозначим через $\varphi(x_1,\ldots,x_m)$, $\psi(x_{m+1},\ldots,x_{m+n})$ и $\phi(x_{m+n+1},\ldots,x_{m+n+r})$. Тогда $h^t(x_1,\ldots,x_{m+n+r})=$

$$(\varphi^{\sigma_1(t,x_\eta,x_\tau,x_\theta)}(x_1,\ldots,x_m), \psi^{\sigma_2(t,x_\eta,x_\tau,x_\theta)}(x_{m+1},\ldots,x_{m+n}), \phi^{\sigma_3(t,x_\eta,x_\tau,x_\theta)}(x_{m+n+1},\ldots,x_{m+n+r})),$$

где $\sigma_k(t,x_\eta,x_\tau,x_\theta)=\sum_{l=1}^{t} u_k(\varphi_\eta^l(x_1,\ldots,x_m), \psi_\tau^l(x_{m+1},\ldots,x_{m+n}), \phi_\theta^l(x_{m+n+1},\ldots,x_{m+n+r}))$, k=1,2,3, t=1,2,…

Пусть $(x_1,\ldots,x_{m+n+r})$ — начальное состояние генератора. Тогда t-й знак выходной последовательности, t=1,2,..., равен

$$y_t = h_1^t(x_1,\ldots,x_{m+n+r}) \oplus h_{m+1}^t(x_1,\ldots,x_{m+n+r}) \oplus h_{m+n+1}^t(x_1,\ldots,x_{m+n+r}).$$

Орграф $\Gamma(h)$ примитивный, при этом $\exp\Gamma(h)$ принимает:

а) наименьшее значение $1+\max\{\lceil m/\nu\rceil, \lceil n/\mu\rceil, \lceil r/\sigma\rceil\}$, если $\eta=m$, $\tau=m+n$, $\theta=m+n+r$, $\lfloor m/\nu\rfloor \le b_{k+1}-b_k \le \lceil m/\nu\rceil$, k=1,…,ν, $b_{\nu+1}=m$, $\lfloor n/\mu\rfloor \le c_{k+1}-c_k \le \lceil n/\mu\rceil$, k=1,…,μ, $c_{\mu+1}=m+n$, $\lfloor r/\sigma\rfloor \le d_{k+1}-d_k \le \lceil r/\sigma\rceil$, k=1,…,σ, $d_{\sigma+1}=m+n+r$, то есть точки съёма регистров выбраны с примерно равными промежутками;

б) наибольшее значение $\max\{m,n,r\}$, если η=1, $\tau=m+1$, $\theta=m+n+1$.

Оценка локального экспонента $*J$-$\exp\Gamma(h)$ не зависит от $J\subseteq\mathbb{N}_{m+n+r}$ и совпадает с оценкой экспонента $\Gamma(h)$. В схеме генератора A5/1 m=19, n=22, r=23, ν=4, μ=2, σ=4. Расчёты показали, что $*J$-$\exp\Gamma(h)$=21, где J={1,20,42}.

Таким образом, на примерах нескольких генераторов псевдослучайных последовательностей описано применение матрично-графового подхода для оценки перемешивающих свойств преобразований векторных пространств, используемых в системах защиты информации.

В **заключении** диссертации приводятся основные результаты работы.

Заключение

Автором получены следующие основные результаты.

1. С использованием свойств примитивных орграфов получен критерий примитивности сплетения орграфов.

2. Для различных классов орграфов получены условия локальной примитивности и оценки локального экспонента в зависимости от особенностей строения графа.

3. Разработаны принципы оптимизации оценок экспонентов и локальных экспонентов орграфов, учитывающие свойства множеств контуров орграфа.

4. Теоретические результаты применены для оценки характеристик локальной примитивности перемешивающих орграфов преобразований, используемых в системах защиты информации. Получены условия локальной примитивности и оценки локальных экспонентов для перемешивающих графов преобразований множества состояний генераторов псевдослучайных последовательностей как с равномерным, так и с неравномерным движением (двухкаскадные генераторы на основе последовательного соединения двоичных регистров сдвига, генераторы «1–2 шагов», генераторы с перемежающимся шагом, генераторы типа A5/1).

Результаты работы вносят существенный вклад в развитие математического аппарата исследования локальной примитивности матриц и орграфов (в том числе непримитивных) и позволяют расширить область применения матрично-графового подхода к исследованию перемешивающих свойств преобразований, используемых в системах защиты информации.

Благодарность. Автор выражает глубокую благодарность своему научному руководителю доктору физико-математических наук, профессору Фомичеву Владимиру Михайловичу за постановку задач, всестороннюю помощь и постоянное внимание к работе. Также автор выражает благодарность и. о. заведующего кафедрой криптологии и кибербезопасности НИЯУ МИФИ кандидату технических наук Епишкиной Анне Васильевне за творческую научную атмосферу.

Публикации автора по теме диссертации

Научные статьи, опубликованные в журналах Scopus, RSCI

1. Fomichev V. M., Kyazhin S. N. Local Primitivity of Matrices and Graphs // Journal of Applied and Industrial Mathematics. — 2017. — Vol. 11, №1. — P. 26–39. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, кроме теорем 1, 3, 4, Фомичевым В. М. поставлены задачи, намечены направления их решения и получен универсальный критерий локальной примитивности графа — теоремы 1, 3, 4).

2. Кяжин С. Н. О применении условий локальной примитивности и оценок локальных экспонентов орграфов // Прикладная дискретная математика. — 2016. — №4 (34). — С. 81–98.

3. Кяжин С. Н., Фомичев В. М. Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. — 2014. — №3 (25). — С. 68–80. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, Фомичевым В. М. поставлены задачи и намечены направления их решения).

4. Кяжин С. Н., Фомичев В. М. О примитивных наборах натуральных чисел // Прикладная дискретная математика. — 2012. — №2 (16). — С. 5–14. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, Фомичевым В. М. поставлены задачи и намечены направления их решения).

5. Фомичев В. М., Кяжин С. Н. Локальная примитивность матриц и графов // Дискретный анализ и исследование операций. — 2017. — Т. 24, №1. — С. 97–119. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, кроме теорем 1, 3, 4, Фомичевым В. М. поставлены задачи, намечены направления их решения и получен универсальный критерий локальной примитивности графа — теоремы 1, 3, 4).

Научные статьи, опубликованные в журналах, входящих в перечень изданий, рекомендованных ВАК при Минобрнауки России

6. Кяжин С. Н. Принципы оптимизации оценок экспонентов и локальных экспонентов орграфов // Вопросы защиты информации. — 2017. — №1 (116). — С. 22–26.

7. Кяжин С. Н., Фомичев В. М. Определяющие свойства примитивных наборов натуральных чисел // Безопасность информационных технологий. — 2012. — №1. — С. 37–41. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, Фомичевым В. М. поставлены задачи и намечены направления их решения).

Иные публикации

8. Кяжин С. Н. Достаточные условия локальной примитивности непримитивных орграфов // Прикладная дискретная математика. Приложение. — 2014. — №7. — С. 130–132.

9. Кяжин С. Н. О локальной примитивности графов и матриц // Прикладная дискретная математика. Приложение. — 2013. — №6. — С. 81–83.

10. Кяжин С. Н. О примитивности сплетения ориентированных графов // Сборник научных трудов Центра специальных разработок МО РФ. — 2015. — №1 (1). — С. 33–41.

11. Кяжин С. Н. Строение локально примитивных орграфов // Прикладная дискретная математика. Приложение. — 2017. — №10. — С. 87–89.

12. Кяжин С. Н., Фомичев В. М. О локальных экспонентах перемешивающих графов функций, реализуемых алгоритмами типа A5/1 // Прикладная дискретная математика. Приложение. — 2015. — №8. — С. 11–13. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, Фомичевым В. М. поставлены задачи и намечены направления их решения).

13. Кяжин С. Н., Фомичев В. М. Перемешивающие свойства двухкаскадных генераторов // Прикладная дискретная математика. Приложение. — 2016. — №9. — С. 60–62. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, Фомичевым В. М. поставлены задачи и намечены направления их решения).

14. Кяжин С. Н., Фомичев В. М. Структурные свойства примитивных наборов натуральных чисел // Прикладная дискретная математика. Приложение. — 2012. — №5. — С. 16–18. (Кяжиным С. Н. разработаны методы решения задач и получены все основные результаты работы, Фомичевым В. М. поставлены задачи и намечены направления их решения).