РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Журнал основан
в январе 1965 г.

ISSN: 0555-2923

Выходит
4 раза в год

Том 56, 2020

Вып. 4

Октябрь–Ноябрь–Декабрь

Москва

СОДЕРЖАНИЕ

Теория информации

Теория кодирования

Большие системы

Теория автоматов

Кодирование источников

Защита информации

Письма в редакцию

CONTENTS

Information Theory

Coding Theory

Large Systems

Automata Theory

Source Coding

Information Protection

Errata

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.723

© 2020 г. **М. Ковачевич**

ПЕРЕДАЧА СИГНАЛОВ РЕЛЯТИВИСТСКИМ НАБЛЮДАТЕЛЯМ: ТАМ, ГДЕ ВСТРЕЧАЮТСЯ ЭЙНШТЕЙН, ШЕННОН И РИМАН[1]

Описывается сценарий связи, включающий в себя серию событий, инициируемых передатчиком и наблюдаемых приемником, испытывающим релятивистское замедление времени. Предполагается, что сообщение, выбранное передатчиком, кодируется согласно хронометражу событий и должно быть безошибочно восстановлено приемником независимо от разницы в шкалах времени в двух системах отсчета. Показано, что максимальная доля пространства всех k-событийных сигналов, которые могут быть выбраны в качестве кода, обеспечивающего безошибочную передачу информации в этой постановке, равна $\zeta(k)^{-1}$, где ζ – дзета-функция Римана.

Ключевые слова: замедление времени, дрейф часов, канал синхронизации, теория Шеннона, передача данных, исправление ошибок, код с нулевой ошибкой, дзета-функция Римана.

DOI: `10.31857/S0555292320040014`

§ 1. Введение

Теория информации [1, 2] – одно из главных научных достижений второй половины XX века – была разработана Шенноном как формальная основа для изучения передачи и обработки информации в классической области. В настоящей статье вводится и изучается задача, которая выводит теорию информации в релятивистский контекст и, в частности, призвана проиллюстрировать влияние замедления времени [3, 4] на фундаментальные пределы передачи информации.

1.1. Описание модели. Рассмотрим следующую модель передачи между двумя участниками: Алиса инициирует k событий в моменты времени $\widetilde{t}_1, \widetilde{t}_2, \ldots, \widetilde{t}_k$, которые выбираются из множества целых чисел $\{1, 2, \ldots, N\}$ согласно показаниям часов в ее системе отсчета, т.е. $\widetilde{t}_i \in \{1, 2, \ldots, N\}$, $1 \leqslant \widetilde{t}_1 < \widetilde{t}_2 < \ldots < \widetilde{t}_k \leqslant N$, и эти события обнаруживаются Бобом в моменты времени $\alpha\widetilde{t}_1, \alpha\widetilde{t}_2, \ldots, \alpha\widetilde{t}_k$ согласно его собственным часам. Множитель α, моделирующий разницу в скорости хода часов в двух системах отсчета, заранее не известен ни одной стороне. (Предполагается, что обе стороны синхронизованы в том смысле, что они согласовали нулевой момент времени; этого можно добиться, инициируя дополнительное событие в момент времени $\widetilde{t} = 0$ в системе отсчета Алисы, при обнаружении которого Боб также устанавливает свои часы на $\widetilde{t} = 0$.) Нам будет удобнее описывать сигналы, указывая интервалы между последовательными событиями, а не время, прошедшее от момента $\widetilde{t} = 0$

---

[1] Работа выполнена при финансовой поддержке научно-исследовательской и инновационной программы “Горизонт 2020” Европейского союза (грант № 856967) и Министерства образования, науки и технологического развития республики Сербия (номер проекта 451-03-68/2020-14/200156).

до каждого из событий. В этих обозначениях множество всех возможных сигналов, который может передавать Алиса, имеет вид

$$T_{N,k} = \left\{ (t_1, \ldots, t_k) \in \mathbb{N}^k : \sum_{i=1}^{k} t_i \leqslant N \right\}, \tag{1}$$

где $\mathbb{N} = \{1, 2, \ldots\}$ – множество натуральных чисел.

Восстановление “переданного k-вектора” $\boldsymbol{t} = (t_1, t_2, \ldots, t_k)$ по “полученному k-вектору” $\alpha\boldsymbol{t}$ тривиально, если коэффициент замедления времени α известен и фиксирован, и поскольку k-вектор $\boldsymbol{t}$ выбирается произвольным образом из $\binom{N}{k}$ возможных, таким способом можно сообщить Бобу $\log_2\binom{N}{k}$ битов информации. Однако при нашем предположении, что коэффициент α априори не известен, не все возможные векторы $\boldsymbol{t}$ можно использовать для надежной передачи информации, поскольку некоторые из них неразличимы на приемном конце. Например, при $k = 2$, если бы Боб наблюдал события в моменты времени (2,1; 4,2), то он не смог бы однозначно определить, какая из возможностей имеет место: $\boldsymbol{t} = (1; 2)$ или $\boldsymbol{t} = (2; 4)$. В этом случае обоим участникам следует заранее ограничить множество разрешенных сигналов $\boldsymbol{t}$ на некоторое собственное подмножество множества $T_{N,k}$ (код) таким образом, чтобы Боб всегда мог правильно распознать переданный k-вектор независимо от значения α. Другими словами, в описанном сценарии замедление времени действует как искажение сигнала, и естественным образом возникает следующий вопрос: сколько битов информации можно надежно передать приемнику при только что описанном простом способе передачи?

Применяя теоретико-информационный подход, мы будем моделировать искажение сигнала, т.е. неизвестный коэффициент α, как абсолютно непрерывную случайную величину с плотностью вероятности $p_\alpha(\cdot)$, носителем которой является либо интервал $[1, \overline{\alpha}]$ для некоторой константы $\overline{\alpha} \in (1, \infty)$, либо $[1, \infty)$. Более общая, на первый взгляд, модель, где носителем $p_\alpha(\cdot)$ является $\left[\underline{\alpha}, \overline{\alpha}\right]$, с точки зрения передачи информации эквивалентна случаю $\left[1, \overline{\alpha}/\underline{\alpha}\right]$, так что нижнюю границу интервала без ограничения общности можно считать равной 1.

Замечание 1. Предполагаемая в этой модели разница в скорости хода часов может быть вызвана различными физическими эффектами: движение Алисы и Боба относительно друг друга, разница гравитационного потенциала между ними, погрешности часов и т.д. Заметим, что наши результаты применимы ко всем моделям с линейной заменой шкалы времени $\boldsymbol{t} \mapsto \alpha\boldsymbol{t}$ и не зависят от физических причин, вызывающих такую замену.

1.2. Коды с нулевой ошибкой. Будем говорить, что два сигнала на входе $\boldsymbol{t}', \boldsymbol{t}'' \in T_{N,k}$ являются *неразличимыми*, если на приемном конце можно перепутать один с другим в том смысле, что соответствующие множества сигналов на выходе $\{\alpha'\boldsymbol{t}'\}$ и $\{\alpha''\boldsymbol{t}''\}$ имеют бесконечное пересечение (здесь значения α' и α'' пробегают носитель функции $p_\alpha(\cdot)$). Подмножество $S \subseteq T_{N,k}$ называется *кодом с нулевой ошибкой* [5], если любые два различных элемента из S различимы. Элементы кода называются кодовыми словами. Таким образом, код с нулевой ошибкой представляет собой множество сигналов, которые можно однозначно распознать на приемном конце. Другими словами, на основе принятого сигнала Боб сможет определить кодовое слово, породившее этот сигнал, и тем самым восстановить передаваемую информацию с вероятностью 1.

Код с нулевой ошибкой $S \subseteq T_{N,k}$ будем называть оптимальным, если он имеет наибольшую возможную мощность среди всех таких кодов в $T_{N,k}$. Эту максимальную мощность трудно установить в общем случае для произвольных значений параметров N и k, поэтому будет целесообразно сосредоточиться на ее асимптотике. Для этого определим максимальную асимптотическую *плотность* кодов в пространстве k-событийных сигналов:

$$\delta_{\overline{\alpha}}(k) = \lim_{N\to\infty} \max_{S\subseteq T_{N,k}} \frac{|S|}{\binom{N}{k}}, \tag{2}$$

где максимум берется по всем кодам с нулевой ошибкой $S \subseteq T_{N,k}$, а $\overline{\alpha} \in (1,\infty]$ – верхняя граница носителя функции $p_\alpha(\cdot)$. (Из дальнейшего анализа будет видно, что зависимость мощности оптимальных кодов от $p_\alpha(\cdot)$ определяется только значением $\overline{\alpha}$, что обосновывает обозначение в (2).) Нашей целью является описание величины $\delta_{\overline{\alpha}}(k)$ для любых k и $\overline{\alpha}$.

§ 2. Оптимальные множества сигналов и их плотность

Вначале рассмотрим случай неограниченной неопределенности коэффициента растяжения времени, что означает, что носителем функции плотности вероятности $p_\alpha(\cdot)$ является вся полупрямая $[1,\infty)$. Растяжение времени искажает сигнал, представленный точкой $\boldsymbol{t} \in T(N,k)$, умножая эту точку на случайный множитель α, или, что то же самое, сдвигая эту точку $\boldsymbol{t}$ на случайное расстояние вдоль ее “луча обзора”, выходящего из начала координат (см. рисунок). Поскольку любые две точки, лежащие на одном луче обзора, выходящем из начала координат, неразличимы (так как $\Pr\{\alpha \geqslant \alpha_0\} > 0$ для любого фиксированного α_0), никакие две такие точки не могут принадлежать одному коду с нулевой ошибкой. Поэтому оптимальный код получается при выборе ровно одной точки на каждом луче обзора, причем проще всего выбирать самую первую точку на каждом луче. Точки $\boldsymbol{t}$ на решетке $\mathbb{N}^k$, которые первыми встречаются при движении по лучам, выходящим из начала координат, – это те, которые удовлетворяют условию $\text{НОД}(\boldsymbol{t}) \equiv \text{НОД}(t_1,\ldots,t_k) = 1$, где через НОД обозначен наибольший общий делитель. Это показывает, что оптимальным кодом с нулевой ошибкой в данной модели является множество

$$C_{N,k} = \Big\{\boldsymbol{t} \in T_{N,k} :\ \text{НОД}(\boldsymbol{t}) = 1\Big\}. \tag{3}$$

В случае, когда носителем функции $p_\alpha(\cdot)$ является конечный интервал $[1,\overline{\alpha}]$, код можно построить с помощью следующей жадной процедуры на каждом луче обзора, выходящем из начала координат: выберем первую точку $\boldsymbol{t}$ на луче (т.е. ту, для которой $\text{НОД}(\boldsymbol{t}) = 1$) в качестве кодового слова и выбросим все точки множества $\big\{\alpha\boldsymbol{t} :\ \alpha \in [1,\overline{\alpha})\big\}$, так как они неразличимы с $\boldsymbol{t}$, затем выберем следующую ближайшую точку на этом луче $\lceil\overline{\alpha}\rceil\boldsymbol{t}$ в качестве кодового слова и выбросим все точки множества $\big\{\alpha\lceil\overline{\alpha}\rceil\boldsymbol{t} :\ \alpha \in [1,\overline{\alpha})\big\}$ и т.д. В результате этой итеративной процедуры получаем следующее множество:

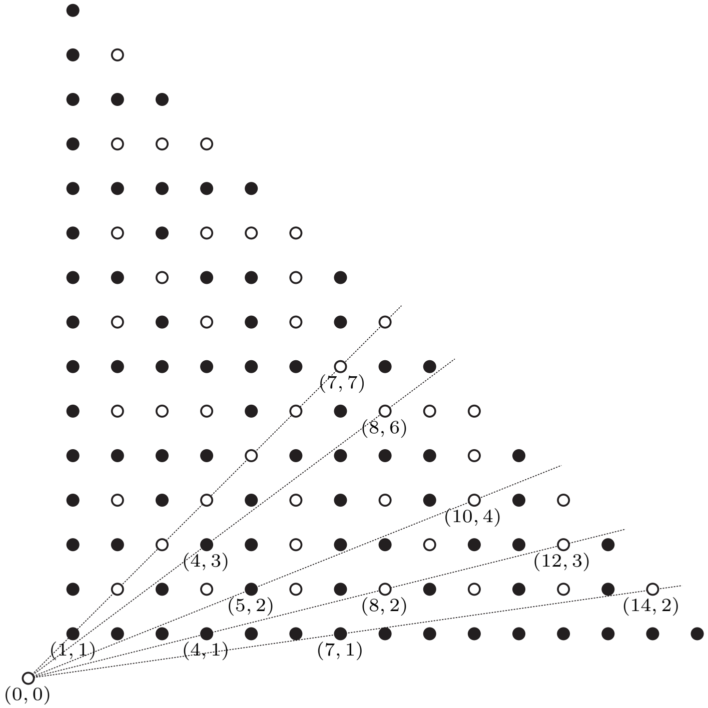
$$D_{N,k} = \left(\biguplus_{n=1}^{\infty} d_n C_{N,k}\right) \cap T_{N,k}, \tag{4}$$

где $(d_n)_{n=1}^{\infty}$ – последовательность, заданная рекуррентным соотношением

$$d_n = \lceil\overline{\alpha} d_{n-1}\rceil, \qquad d_1 = 1, \tag{5}$$

через $d_n C_{N,k}$ обозначено множество $\big\{d_n\boldsymbol{t} :\ \boldsymbol{t} \in C_{N,k}\big\}$, а знак $\biguplus$ подчеркивает, что объединяемые множества попарно не пересекаются. Для простоты в этих обозначениях мы не указываем зависимость d_n от $\overline{\alpha}$ в явном виде. Отметим, что для $\overline{\alpha} \in \mathbb{N}$, $\overline{\alpha} \geqslant 2$, рекуррентное соотношение (5) упрощается до

$$d_n = \overline{\alpha}^{n-1}. \tag{6}$$



Пространство $T_{16,2}$, описывающее сигналы, состоящие из $k = 2$ событий, которые могут возникнуть в один из $N = 16$ моментов времени, и код $C_{16,2}$, состоящий из всех точек $\boldsymbol{t} = (t_1, t_2) \in T_{16,2}$, удовлетворяющих условию НОД$(t_1, t_2) = 1$. Кодовые слова кода $C_{16,2}$ показаны черными точками. Для иллюстрации также показано несколько “лучей обзора”, выходящих из начала координат

Из построения очевидно, что $D_{N,k}$ действительно является кодом с нулевой ошибкой: единственная возможность, при которой два различных кодовых слова $d_n\boldsymbol{t}$ и $d_{n+1}\boldsymbol{t}$ породят один и тот же сигнал на приемном конце, – это случай, когда α принимает значение $\overline{\alpha}$ (и при этом $\overline{\alpha} \in \mathbb{N}$). В следующей теореме будет показано, что код $D_{N,k}$ на самом деле оптимален, и на основе этого наблюдения мы получим характеризацию максимальной асимптотической плотности $\delta_{\overline{\alpha}}(k)$. Чтобы это утверждение было также верно и для тривиального случая $\overline{\alpha} = 1$, по определению положим $d_n = n$ для $\overline{\alpha} = 1$, что обосновывается соображениями непрерывности (переходя к пределу при $\overline{\alpha} \to 1$ в (5)).

Напомним определение дзета-функции Римана [6]:

$$\zeta(k) = \sum_{n=1}^{\infty} n^{-k}. \tag{7}$$

Теорема 1. *Зафиксируем* $k \in \mathbb{N}$, $k \geqslant 2$, *и* $\overline{\alpha} \in [1, \infty)$, *и пусть* $(d_n)_{n=1}^{\infty}$ *– последовательность, определенная в* (5). *Тогда*

$$\delta_{\overline{\alpha}}(k) = \zeta(k)^{-1} \sum_{n=1}^{\infty} d_n^{-k}. \tag{8}$$

При $\overline{\alpha} = \infty$ *имеем*

$$\delta_{\infty}(k) = \zeta(k)^{-1}. \tag{9}$$

Доказательство. Оптимальность кода $D_{N,k}$ непосредственно вытекает из результата Шеннона [5, теорема 3], который утверждает, что код с нулевой ошибкой $S \subseteq T$ оптимален, если существует отображение $f\colon T \to S$, обладающее тем свойством, что $f(\boldsymbol{t}') \neq f(\boldsymbol{t}'')$ для любых двух различимых сигналов $\boldsymbol{t}', \boldsymbol{t}'' \in T$. Требуемая функция $f\colon T_{N,k} \to D_{N,k}$ в нашем случае задается с помощью отображения всех точек множества $\bigl\{\alpha d_n \boldsymbol{t} \,:\, \alpha \in [1, \overline{\alpha})\bigr\} \cap T_{N,k}$ в $d_n \boldsymbol{t}$ для всех $\boldsymbol{t} \in T_{N,k}$, таких что НОД$(\boldsymbol{t}) = 1$, и всех $n \geqslant 1$. Поскольку любые две различимые точки множества $T_{N,k}$ принадлежат различным множествам вида $\bigl\{\alpha d_n \boldsymbol{t} \,:\, \alpha \in [1, \overline{\alpha})\bigr\}$ (т.е. либо у них различные n, либо различные $\boldsymbol{t}$, либо и то, и другое), их образы при отображении f различны. Поэтому из вышеуказанного результата Шеннона следует, что код $D_{N,k}$ оптимален, откуда

$$\delta_{\overline{\alpha}}(k) = \lim_{N\to\infty} \frac{|D_{N,k}|}{\dbinom{N}{k}}. \tag{10}$$

Теперь обратимся к соотношению (4) и заметим, что все подкоды $\bigl(d_n C_{N,k}\bigr) \cap T_{N,k}$ можно представить в виде

$$\bigl(d_n C_{N,k}\bigr) \cap T_{N,k} = \Bigl\{\boldsymbol{t} \in T_{N,k} \,:\, \text{НОД}(\boldsymbol{t}) = d_n\Bigr\} = d_n C_{\lfloor N/d_n \rfloor, k}. \tag{11}$$

Тем самым, их асимптотическая плотность равна

$$\begin{aligned} \lim_{N\to\infty} \frac{\bigl|\bigl(d_n C_{N,k}\bigr) \cap T_{N,k}\bigr|}{|T_{N,k}|} &= \lim_{N\to\infty} \frac{\bigl|C_{\lfloor N/d_n \rfloor, k}\bigr|}{\dbinom{N}{k}} = \lim_{N'\to\infty} \frac{|C_{N',k}|}{\dbinom{d_n N'}{k}} = \\ &= \lim_{N'\to\infty} \frac{|C_{N',k}|}{d_n^k \dbinom{N'}{k}} = d_n^{-k} \delta_\infty(k), \end{aligned} \tag{12}$$

где был использован тот факт, что код $C_{N,k}$ из (3) является оптимальным для случая $\overline{\alpha} = \infty$ и поэтому

$$\delta_\infty(k) = \lim_{N\to\infty} \frac{|C_{N,k}|}{\dbinom{N}{k}}. \tag{13}$$

Теперь из (4), (10) и (12) вытекает

$$\delta_{\overline{\alpha}}(k) = \delta_\infty(k) \sum_{n=1}^{\infty} d_n^{-k}. \tag{14}$$

Тем самым, доказательство соотношения (8) сведено к доказательству равенства (9). Плотность $\delta_\infty(k)$ можно найти из соотношений (3), (13) и известного факта [7], что вероятность того, что k случайно выбранных положительных чисел взаимно просты, равна $\zeta(k)^{-1}$, но здесь мы также приведем и прямое доказательство. Для этого сперва заметим, что $\delta_1(k) = 1$ для любого k. Это так, поскольку условие $\overline{\alpha} = 1$ означает, что коэффициент замедления времени точно известен на приемном конце, и поэтому оптимальный код для этого случая тривиальным образом равен множеству всех возможных сигналов на входе $T_{N,k}$, плотность которого равна 1. Теперь из равенства (14) и того факта, что $d_n = n$ при $\overline{\alpha} = 1$, получаем

$$1 = \delta_\infty(k) \sum_{n=1}^{\infty} n^{-k} = \delta_\infty(k)\zeta(k), \tag{15}$$

что и завершает доказательство теоремы. ▲

Для целочисленных значений $\overline{\alpha}$ полученную плотность можно выразить явно в силу равенства (6). А именно, для $\overline{\alpha} \in \mathbb{N}$, $\overline{\alpha} \geqslant 2$, получаем

$$\delta_{\overline{\alpha}}(k) = \frac{\overline{\alpha}^k}{\zeta(k)\bigl(\overline{\alpha}^k - 1\bigr)}. \tag{16}$$

Как мы видели, в случае, когда о коэффициенте α ничего не известно, соотношение (9) получается как важный специальный случай соотношения (8) (или, скорее, как предельный случай при $\overline{\alpha} \to \infty$). В частности, наибольшая асимптотическая плотность множества двухсобытийных сигналов, различимых приемником, время которого замедляется, равна

$$\delta_\infty(2) = \frac{6}{\pi^2}. \tag{17}$$

Вообще, для любого четного $k = 2m$ имеем

$$\delta_\infty(2m) = \frac{(-1)^{m+1} 2 (2m)!}{(2\pi)^{2m} B_{2m}}, \tag{18}$$

где B_k – числа Бернулли [8, § 1.5].

Замечание 2. Модель, тесно связанная с представленной в настоящей статье, где вместо релятивистского замедления времени сигналы искажались благодаря ошибке синхронизации, известной как дрейф часов, рассматривалась в [9,10]. Оптимальные коды с нулевой ошибкой для этой модели были описаны в [10], хотя оценка их мощности не была проведена. Следует отметить, что понятие "неразличимости" было определено в [10] как условие, что рассматриваемые сигналы не могут приводить к одинаковым сигналам на приемном конце. Это определение немного отличается от нашего, в котором требуется, чтобы появление двух входных сигналов, которые можно перепутать на приемном конце, было событием с нулевой вероятностью. Дальнейшая характеризация оптимальных кодов в [10] аналогична (4), но с последовательностью $(b_n)_{n=1}^\infty$ вместо $(d_n)_{n=1}^\infty$, где

$$b_n = \lfloor \overline{\alpha} b_{n-1} + 1 \rfloor, \qquad b_1 = 1. \tag{19}$$

В частности, для $\overline{\alpha} \in \mathbb{N}$

$$b_n = 1 + \overline{\alpha} + \overline{\alpha}^2 + \ldots + \overline{\alpha}^{n-1} = \frac{\overline{\alpha}^n - 1}{\overline{\alpha} - 1}. \tag{20}$$

Таким же способом, как и в доказательстве теоремы 1, можно показать, что наибольшая асимптотическая плотность кодов, определенных в [10], равна

$$\zeta(k)^{-1} \sum_{n=1}^\infty b_n^{-k}. \tag{21}$$

Заметим, что $b_n \geqslant d_n$ для всех $n \geqslant 1$. В частности, при $\overline{\alpha} \in \mathbb{N}$, $\overline{\alpha} \geqslant 2$, неравенство является строгим для любых $n \geqslant 2$, поэтому плотность (21) строго меньше, чем плотность $\delta_{\overline{\alpha}}(k)$ из (8). Однако это не всегда так; для иррациональных $\overline{\alpha}$ имеем $b_n = d_n$ для любых $n \geqslant 1$, так что эти две плотности равны.

§ 3. Заключительные замечания

Оценка количества информации и установление фундаментальных границ на передачу информации – два основных направления в теории информации. Области исследования, в которых изучаются такие вопросы для различных физических систем, имеют долгую историю в науке, особенно в квантовой теории информации. В настоящей статье описан сценарий, в котором передача информации рассматривается в релятивистском контексте, и представлен результат, количественно оценивающий границы на передачу в этой модели. Полученное решение, хотя и довольно простое, интересно тем, что оно устанавливает связь между теорией информации Шеннона, специальной теорией относительности и теорией чисел. Тем самым, представляет интерес дальнейшее изучение этой задачи и других, связанных с ней, в частности, исследование гораздо более трудного случая нелинейного изменения шкалы времени, которое может возникать, например, когда наблюдатели движутся с ускорением.

Автор выражает благодарность рецензенту за несколько весьма ценных замечаний и поправок к первоначальному варианту статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Shannon C.E.* A Mathematical Theory of Communication // Bell Syst. Tech. J. 1948. V. 27. № 3. P. 379–423.
2. *Csiszár I., Körner J.* Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge: Cambridge Univ. Press, 2011.
3. *Einstein A.* Zur Elektrodynamik bewegter Körper // Ann. Phys. 1905. V. 322. № 10. P. 891–921.
4. *Mermin N.D.* It's about Time: Understanding Einstein's Relativity. Princeton: Princeton Univ. Press, 2005.
5. *Shannon C.E.* The Zero Error Capacity of a Noisy Channel // IRE Trans. Inform. Theory. 1956. V. 2. № 3. P. 8–19.
6. *Riemann B.* Über die Anzahl der Primzahlen unter einer gegebenen Größe // Monatsber. Königl. Preufs. Akad. Wiss. Berlin, 1859. Berlin: Königlichen Akad. der Wissenschaften, 1960. P. 671–680.
7. *Nymann J.E.* On the Probability that k Positive Integers are Relatively Prime // J. Number Theory. 1972. V. 4. № 5. P. 469–473.
8. *Edwards H.M.* Riemann's Zeta Function. Mineola, NY: Dover, 2001.
9. *Yeung R.W., Cai N., Ho S.-W., Wagner A.B.* Reliable Communication in the Absence of a Common Clock // IEEE Trans. Inform. Theory. 2009. V. 55. № 2. P. 700–712.
10. *Shaviv D., Özgür A., Arbabian A.* Communication with Crystal-free Radios // IEEE Trans. Commun. 2018. V. 66. № 10. P. 4513–4520.

Ковачевич Младен
Факультет технических наук,
Университет г. Нови-Сад, Сербия
`kmladen@uns.ac.rs`

Поступила в редакцию
22.09.2020
После доработки
21.10.2020
Принята к публикации
28.10.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.725

© 2020 г. **И.Ю. Могильных, Ф.И. Соловьева**

О БАЗИСАХ КОДОВ БЧХ С КОНСТРУКТИВНЫМ РАССТОЯНИЕМ 3 И ИХ РАСШИРЕНИЙ[1]

Рассматриваются коды БЧХ в узком смысле длины $p^m - 1$ над $\mathbb{F}_p$, $m \geqslant 3$. Доказано, что такой код с конструктивным расстоянием $\delta = 3$ и его расширение при $p \geqslant 5$ не порождаются множеством своих кодовых слов минимального ненулевого веса. Установлено, что расширенные коды БЧХ с конструктивным расстоянием $\delta = 3$ при $p \geqslant 3$ порождаются множеством слов веса 5, причем базисные векторы могут быть выбраны среди аффинных орбит некоторых кодовых слов.

Ключевые слова: код БЧХ, циклический код, аффинно-инвариантный код, базис минимального веса, аффинный порождающий элемент.

DOI: `10.31857/S0555292320040026`

§ 1. Введение

Вопрос существования базиса, состоящего из векторов минимального или небольшого веса линейного кода, как компактного способа хранения информации, задающего код большой мощности, представляет интерес с точки зрения теории кодирования [1, § 3.2], а также теории тестов [2–4].

Так как циклический МДР-код достигает границы Синглтона, его порождающий многочлен имеет минимальный вес. Следовательно, существует базис из кодовых слов минимального веса для такого кода. К этим кодам относятся коды Рида–Соломона, а также некоторые другие связанные с ними коды [5, гл. 11, теоремы 9, 10].

Известно [5, теорема 10, гл. 13], что всякий код Рида–Маллера порождается словами минимального веса. Также базис, состоящий из векторов минимального веса, существует для q-ичных кодов Хэмминга вследствие их единственности для заданных параметров и леммы Глаголева (см. данный результат в работе [6] и аналогичный результат для q-ичного случая в [7]). Итеративная конструкция базисов из кодовых слов минимального веса для двоичного кода Хэмминга была получена в работе [8]. Отметим, что этот результат может быть обобщен на случай расширенных двоичных кодов Хэмминга и q-ичных кодов Хэмминга (со сходной схемой доказательства на основе конструкции Шонхайма). В [2] было доказано, что расширенные двоичные коды БЧХ в узком смысле достаточно большой длины порождаются множеством слов минимального веса.

С другой стороны, в работе [9] установлено, что совокупность слов минимального веса двоичного примитивного кода БЧХ с конструктивным расстоянием $2^{m-2} - 1$ совпадает с множеством слов минимального веса выколотого кода Рида–Маллера $RM(2, m)$.

---

[1] Работа выполнена при поддержке Министерства науки и высшего образования РФ (соглашение № 075-02-2020-1479/1).

В силу большей симметрии проблему существования базиса из кодовых слов минимального веса естественно рассматривать для расширенных кодов, к примеру, выдерживающих аффинные преобразования поля. Кодовое слово c аффинно-инвариантного кода называется *аффинным порождающим элементом* (single orbit affine generator, см. [4]), если орбита вектора c действия аффинной группы поля $\mathbb{F}_{p^m}$ содержит базис кода. Очевидно, аффинным порождающим элементом аффинно-инвариантного кода будет вектор, полученный расширением вектора, отвечающего порождающему многочлену выколотого циклического кода. Естественной представляется задача поиска аффинного порождающего элемента минимально возможного веса.

В [3] приводятся результаты, мотивирующие поиск аффинных порождающих элементов небольшого веса с позиций локальных тестирований. В работе [4] доказано, что двоичный расширенный код БЧХ в узком смысле с конструктивным расстоянием 5 имеет аффинный порождающий элемент минимального веса. В работе [10] авторами настоящей статьи были получены аффинные порождающие элементы минимального веса аффинно-инвариантных кодов, отвечающих функции Голда.

В данной статье исследуется вопрос существования аффинного порождающего элемента минимально возможного веса расширенного кода БЧХ над $\mathbb{F}_p$, $p \neq 2$. Отметим, что его структура для недвоичных кодов БЧХ с конструктивным расстоянием 3 существенно отличается от такового в двоичном случае (для двоичных расширенных кодов Хэмминга результат был получен в [4, следствие 8]).

В §2 приводятся основные понятия и утверждения. В §3 доказывается несуществование базисов, состоящих из векторов минимального веса для расширенных кодов БЧХ с конструктивным расстоянием 3 над $\mathbb{F}_p$ для любого простого p, $p \neq 2, 3$. В §4 вводится понятие ранга кодового слова аффинно-инвариантного кода. Доказано, что ранг аффинного порождающего элемента веса 5 расширенного кода БЧХ с конструктивным расстоянием 3 равен 3. Ранг введен по аналогии с рангом кодового слова циклического кода [5, гл. 9, §11], предложенным для определения минимального расстояния некоторых циклических кодов. Полученное ограничение на ранг неявно использовано при нахождении подходящего аффинного порождающего элемента в теореме 4. Отметим, что при $p = 3$ аффинный порождающий элемент имеет минимальный вес, поскольку кодовое расстояние кода равно 5, а при $p > 3$ имеет предминимальный вес, равный 5.

§2. Циклические и аффинно-инвариантные коды

Основные определения и обозначения см. в [5]. Линейный код называется *циклическим*, если циклический сдвиг любого его кодового слова является кодовым словом. В дальнейшем будем рассматривать лишь циклические коды длины $p^m - 1$ над простым полем $\mathbb{F}_p$. Для всякого ненулевого элемента β поля Галуа $\mathbb{F}_{p^m}$ справедливо $\beta^{p^m-1} = 1$. Элемент поля $\mathbb{F}_{p^m}$ называется *примитивным*, если его порядок равен $p^m - 1$. Координаты векторного пространства $\mathbb{F}_p^{p^m-1}$ перенумеруем числами $0, \ldots, p^m - 2$ и отождествим координату с номером i с элементом α^i, где $i \in \{0, \ldots, p^m - 2\}$ и α – примитивный элемент поля $\mathbb{F}_{p^m}$. *Циклотомическим классом элемента* $i \in \{0, \ldots, p^m - 2\}$ *по модулю* $p^m - 1$ называется множество

$$\mathrm{cl}(i) = \bigl\{ip^j \pmod{p^m - 1} : j \in \{0, \ldots, m - 1\}\bigr\}.$$

Со всяким вектором $c = (c_0, \ldots, c_{p^m-2})$ в пространстве $\mathbb{F}_p^{p^m-1}$ отождествим многочлен $c(x) = \sum\limits_{i=0}^{p^m-2} c_i x^i$. Элемент поля $\mathbb{F}_{p^m}$ называется *нулем* p-ичного циклического кода длины $p^m - 1$, если он является корнем каждого его кодового многочлена. Известно, что множество нулей всякого циклического кода состоит из степеней примитивного элемента, пробегающих объединение некоторых циклотомических классов. Если $i_1, \ldots, i_\ell$ – представители некоторых циклотомических классов, то через $C_{i_1,\ldots,i_\ell}$ обозначим соответствующий циклический код

$$\{c(x) : c(\alpha^j) = 0, \ j \in \mathrm{cl}(i_1) \cup \ldots \cup \mathrm{cl}(i_\ell)\}.$$

Согласно теореме о границе БЧХ, если найдется $\delta - 1$ подряд идущих степеней примитивного элемента α, являющихся нулями циклического кода, то кодовое расстояние в коде не меньше δ. Кодом с таким свойством является $C_{1,\ldots,\delta-1}$, именуемый *кодом БЧХ в узком смысле с конструктивным расстоянием* δ.

Для вектора $c = (c_0, \ldots, c_{p^m-2})$ длины $p^m - 1$ обозначим его расширение через $\bar{c}$, т.е.

$$\bar{c} = \left(c_0, \ldots, c_{p^m-2}, -\sum_{i=0}^{p^m-2} c_i\right).$$

Расширенный код $\{\bar{c} : c \in C\}$ обозначим через $\overline{C}$. В дальнейшем считаем, что добавляемая при расширении координата занумерована нулем поля Галуа $\mathbb{F}_{p^m}$. Таким образом, на координатных позициях векторного пространства $\mathbb{F}_p^{p^m}$ действует *аффинная группа поля* $\mathbb{F}_{p^m}$, состоящая из перестановок, которые могут быть описаны парами (γ, σ), а именно: $(\gamma, \sigma)(\beta) = \gamma\beta + \sigma$, где $\gamma, \sigma \in \mathbb{F}_{p^m}$, $\gamma \neq 0$, относительно операции композиции. Код длины p^m над $\mathbb{F}_p$ называется *аффинно-инвариантным*, если аффинная группа поля $\mathbb{F}_{p^m}$ оставляет на месте множество кодовых слов этого кода.

Пусть $i \in \{0, \ldots, p^m - 1\}$. Через I обозначим вектор, представляющий число i в p-ичной системе счисления, т.е. $i = \sum\limits_{s=0}^{m-1} I_s p^s$. Пусть J и I – записи чисел j и i, соответственно, в p-ичной системе счисления. Обозначим $j \prec i$, если $J_s \leqslant I_s$ для всех $s \in \{0, \ldots, m-1\}$. Следующая теорема характеризует аффинно-инвариантные коды.

Теорема 1 [11]. *Пусть C – циклический код длины $p^m - 1$. Если α^i – нуль кода C и для всякого ненулевого j, $j \prec i$, элемент α^j является нулем кода C, тогда код $\overline{C}$ является аффинно-инвариантным. Верно и обратное.*

Следствие 1. *Расширенный код БЧХ $\overline{C_{1,2,\ldots,\delta-1}}$ для всякого $\delta \geqslant 2$, а также код $\overline{C_{1,2,p^2+1}}$ являются аффинно-инвариантными.*

В дальнейшем нам понадобится следующий факт.

Предложение. *Пусть конструктивное расстояние кода БЧХ в узком смысле совпадает с кодовым расстоянием d. Тогда расширение этого кода имеет кодовое расстояние $d + 1$.*

Доказательство. Предположим, что $\bar{c}$ – кодовое слово веса d расширенного кода БЧХ $\overline{C_{1,\ldots,d-1}}$. Тогда $c = (c_0, \ldots, c_{p^m-2})$ – кодовое слово веса d кода $C_{1,\ldots,d-1}$, а $\{i_1, \ldots, i_d\}$ – множество позиций ненулевых символов слова c, такое что

$$\sum_{j=1}^{d} c_{i_j} = 0.$$

Так как $c \in C_{1,\ldots,d-1}$, то

$$\sum_{j=1}^{d} c_{i_j} \alpha^{\ell i_j} = 0$$

для всех $\ell \in \{1, \ldots, d-1\}$. Учитывая, что матрица системы относительно неизвестных $c_{i_1}, \ldots, c_{i_d}$ является матрицей Вандермонда, и следовательно, невырождена, имеем $c_{i_1} = c_{i_2} = \ldots = c_{i_d} = 0$, противоречие. ▲

Кодовое расстояние кодов БЧХ и других кодов с двумя нулями было получено в работе [12]. При $p = 3$ имеем $C_{1,2} = C_{1,2,3}$, откуда в силу границы БЧХ кодовое расстояние $C_{1,2}$ равно 4. Отсюда получаем

Следствие 2. *Кодовое расстояние кода БЧХ* $C_{1,2}$ *равно* 3 *при всех простых* p, $p \neq 3$, *и равно* 4 *при* $p = 3$. *Расширения этих кодов имеют кодовые расстояния* 4 *и* 5 *соответственно.*

§ 3. Несуществование базисов кодов $C_{1,2}$ и $\overline{C_{1,2}}$ из слов минимального веса

Лемма 1. *Пусть* $c \in C_2$ *– такое кодовое слово, что для всякого* i, *для которого* $c_i \neq 0$, *имеет место* $\alpha^i \in \mathbb{F}_p$. *Тогда* $c \in C_{2,p^2+1}$.

Доказательство. Так как $c \in C_2$, то

$$\sum_{i \in \{0,\ldots,p^m-2\}\colon c_i \neq 0} c_i \alpha^{2i} = 0.$$

По условию леммы для всякого i, для которого $c_i \neq 0$, имеет место $\alpha^i \in \mathbb{F}_p$, откуда $\alpha^{ip^2} = \alpha^i$. Следовательно,

$$\sum_{i \in \{0,\ldots,p^m-2\}\colon c_i \neq 0} c_i \alpha^{(p^2+1)i} = \sum_{i \in \{0,\ldots,p^m-2\}\colon c_i \neq 0} c_i \alpha^{2i} = 0,$$

другими словами, α^{p^2+1} является корнем $c(x)$, который, в свою очередь, принадлежит C_{2,p^2+1}. ▲

Теорема 2. *Множество кодовых слов кода* $C_{1,2}$ *веса* 3 *содержится в* $C_{1,2,p^2+1}$.

Доказательство. Без ограничения общности имеем $c(x) = 1 + ax^i + bx^j$, $c(x) \in C_{1,2}$, где a, b – ненулевые элементы поля Галуа $\mathbb{F}_p$. По определению кода БЧХ выполнены проверочные соотношения

$$1 + a\alpha^i + b\alpha^j = 0, \qquad (1)$$

$$1 + a\alpha^{2i} + b\alpha^{2j} = 0. \qquad (2)$$

Покажем, что α^{p^2+1} является корнем многочлена $c(x)$, т.е.

$$1 + a\alpha^{(p^2+1)i} + b\alpha^{(p^2+1)j} \qquad (3)$$

равно нулю. Возможны следующие случаи.

Случай 1. Пусть $b = -a$. Используя это равенство и подставляя выражение для α^j из (1) в (2), получаем $a - 1 - 2a\alpha^i = 0$. Таким образом, α^i и, следовательно, α^j принадлежат $\mathbb{F}_p$. Отсюда и из леммы 1 получаем требуемое.

Случай 2. Пусть $a + b \neq 0$. Обозначим $a + b$ через $-f^{-1}$. Преобразуем (1) и (2), используя замену

$$\alpha^i = by_i + f, \quad \alpha^j = ay_j + f. \qquad (4)$$

Из (1) после преобразований имеем $y_i = -y_j$. Отсюда с учетом (2) и $a + b = -f^{-1}$ получаем

$$y_i^2 ab(a+b) = f - 1. \qquad (5)$$

Преобразуем выражение (3), произведя замену (4) и принимая во внимание равенства $y_i = -y_j$, $a^{p^2} = a$ и $b^{p^2} = b$:

$$\begin{aligned}
&1 + a\alpha^{(p^2+1)i} + b\alpha^{(p^2+1)j} = \\
&= 1 + a(by_i + f)^{p^2}(by_i + f) + b(-ay_i + f)^{p^2}(-ay_i + f) = \\
&= 1 + a(by_i^{p^2} + f)(by_i + f) + b(-ay_i^{p^2} + f)(-ay_i + f) = \\
&= 1 + ab(a + b)y_i^{p^2+1} + f^2(a + b).
\end{aligned}$$

Из полученного выражения согласно обозначению $a + b = -f^{-1}$ получаем

$$y_i^{p^2+1}ab(a + b) + 1 - f.$$

Однако $(p^2 + 1)/2 = (p - 1)(p + 1)/2 + 1$, и так как из (5) следует, что $y_i^2 \in \mathbb{F}_p$, то

$$(y_i^2)^{(p^2+1)/2} = y_i^2.$$

Таким образом, приходим к выводу, что выражение (3) преобразуется в $y_i^2ab(a+b)+$ $+1 - f$. Из (5) следует, что α^{p^2+1} является корнем $c(x)$. ▲

Следствие 3. *Для любого простого p, не равного 2 или 3, код $C_{1,2}$ и расширенный код $\overline{C_{1,2}}$ не порождаются множествами кодовых слов минимального ненулевого веса.*

Доказательство. В силу следствия 2 минимальные расстояния кодов $C_{1,2}$ и $\overline{C_{1,2}}$ равны 3 и 4 соответственно. Число $p^2 + 1$ не принадлежит циклотомическим классам $\mathrm{cl}(1) = \{p^i : i \in \{0, \ldots, m - 1\}\}$ и $\mathrm{cl}(2) = \{2p^i : i \in \{0, \ldots, m - 1\}\}$, следовательно, $C_{1,2,p^2+1}$ является собственным подкодом кода $C_{1,2}$. Из теоремы 2 заключаем, что все слова веса 3 кода $C_{1,2}$ содержатся в $C_{1,2,p^2+1}$.

Рассмотрим расширенные коды. Пусть $\bar{c}$ – кодовое слово веса 4 кода $\overline{C_{1,2}}$, полученное добавлением общей проверки на четность к кодовому слову c кода $C_{1,2}$. Покажем, что вектор $\bar{c}$ принадлежит коду $\overline{C_{1,2,p^2+1}}$. Пусть c имеет вес 4, т.е. в позиции вектора $\bar{c}$, занумерованной нулем поля $\mathbb{F}_{p^m}$, стоит символ 0. Пусть для некоторого i в позиции вектора $\bar{c}$, занумерованной элементом α^i, стоит ненулевой символ. В силу того, что аффинная группа поля действует 2-транзитивно на координатных позициях $\bar{c}$, найдется аффинное преобразование, меняющее местами позиции, занумерованные элементами 0 и α^i. Другими словами, представитель $\overline{c'}$ аффинной орбиты кодового слова $\bar{c}$ может быть выбран таким, что c' имеет вес 3 и $\sum\limits_{i=0}^{p^m-2} c'_i \neq 0$. В силу следствия 1 коды $\overline{C_{1,2}}$ и $\overline{C_{1,2,p^2+1}}$ аффинно-инвариантны, поэтому c и c' или содержатся в этих кодах одновременно, или одновременно не содержатся. Из теоремы 2 заключаем, что векторы $\overline{c'}$ и, следовательно, $\bar{c}$ принадлежат $\overline{C_{1,2,p^2+1}}$. ▲

§ 4. Базис кода $\overline{C_{1,2}}$ веса 5

4.1. Ранг аффинного порождающего элемента. *Рангом* вектора $\bar{c} \in \mathbb{F}_p^{p^m}$ назовем размерность векторного пространства над $\mathbb{F}_p$, натянутого на носитель вектора c, т.е. $\{\alpha^i : i \in \{0, \ldots, p^m - 2\},\ c_i \neq 0\}$.

Теорема 3. *Пусть c – кодовое слово кода $C_{1,2}$ веса 4 и $\bar{c}$ – аффинный порождающий элемент кода $\overline{C_{1,2}}$. Тогда $\bar{c}$ имеет вес 5 и ранг 3.*

Доказательство. По следствию 3 аффинный порождающий элемент кода $\overline{C_{1,2}}$ имеет вес не меньше 5. Пусть слово $\bar{c}$ веса 5 является аффинным порождающим элементом кода $\overline{C_{1,2}}$. Так как вес c равен 4 и $c \in C_1$, то ранг $\bar{c}$ не превосходит 3. Если ранг $\bar{c}$ равен 1, то по лемме 1 вектор $\bar{c}$ принадлежит аффинно-инвариантному коду $\overline{C_{1,2,p^2+1}}$, являющемуся собственным подкодом кода $\overline{C_{1,2}}$. Следовательно, кодовое слово $\bar{c}$ не является аффинным порождающим элементом кода $\overline{C_{1,2}}$.

Пусть $c(x) = h + ax^i + bx^j + fx^k$ и кодовое слово $\bar{c}$ имеет ранг 2. Так как ранг $\bar{c}$ равен 2, то

$$\alpha^j = s + t\alpha^i, \quad \alpha^k = u + v\alpha^i$$

для некоторых элементов s, t, u, v поля Галуа $\mathbb{F}_p$.

Так как $c \in C_2$, то

$$\begin{aligned} &c(\alpha^2) = h + a\alpha^{2i} + b(s + t\alpha^i)^2 + f(u + v\alpha^i)^2 = \\ &\ = h + a\alpha^{2i} + bs^2 + 2bst\alpha^i + bt^2\alpha^{2i} + fu^2 + 2fuv\alpha^i + fv^2\alpha^{2i} = \\ &\ = a\alpha^{2i}(a + t^2b + v^2f) + 2\alpha^i(stb + uvf) + h + bs^2 + fu^2 = 0. \end{aligned} \tag{6}$$

Последнее равенство имеет место в случае тождества, т.е.

$$a + t^2b + v^2f = stb + uvf = h + bs^2 + fu^2 = 0, \tag{7}$$

или если $\alpha^i \in \mathbb{F}_{p^2}$.

Покажем, что $c(x) \in C_{1,2,p^2+1}$. Учитывая, что элементы s, t, u, v принадлежат простому полю $\mathbb{F}_p$, имеем

$$\begin{aligned} &c(\alpha^{p^2+1}) = h + a\alpha^{i(p^2+1)} + b(s + t\alpha^i)^{p^2+1} + f(u + v\alpha^i)^{p^2+1} = \\ &\ = a\alpha^{(p^2+1)i}(a + t^2b + v^2f) + (\alpha^{ip^2} + \alpha^i)(stb + uvf) + h + bs^2 + fu^2. \end{aligned}$$

Из этого выражения для $c(\alpha^{p^2+1})$ заключаем, что если выполнено условие (7), то $c(\alpha^{p^2+1}) = 0$. Если $\alpha^i \in \mathbb{F}_{p^2}$, то $\alpha^{ip^2} = \alpha^i$, и выражение для $c(\alpha^{p^2+1})$ совпадает с выражением для $c(\alpha^2)$ из (6), а следовательно, кодовое слово $\bar{c}$ из $\overline{C_{1,2,p^2+1}}$ не является аффинным порождающим элементом кода $\overline{C_{1,2}}$. ▲

4.2. Явный вид аффинного порождающего элемента. В следующей лемме найдем подходящий для дальнейших рассмотрений кодовый многочлен кода $C_{1,2}$.

Лемма 2. *Пусть α – примитивный элемент поля Галуа $\mathbb{F}_{p^m}$, $p, m \geqslant 3$. Тогда циклический код $C_{1,2}$ длины $p^m - 1$ содержит многочлен*

$$c(x) = 2 + x^i + x^j - 2x^k,$$

где i, j, k удовлетворяют условиям

$$\alpha^i = \alpha + 2^{-1}\alpha^2, \quad \alpha^j = -\alpha + 2^{-1}\alpha^2, \quad \alpha^k = 1 + 2^{-1}\alpha^2. \tag{8}$$

Доказательство. Справедливы следующие равенства:

$$\begin{aligned} &c(\alpha) = 2 + \alpha^i + \alpha^j - 2\alpha^k = 2 + \alpha + 2^{-1}\alpha^2 - \alpha + 2^{-1}\alpha^2 - 2 - \alpha^2 = 0, \\ &c(\alpha^2) = 2 + \alpha^{2i} + \alpha^{2j} - 2\alpha^{2k} = \\ &\ = 2 + \alpha^2 + 2^{-2}\alpha^4 + \alpha^3 + \alpha^2 + 2^{-2}\alpha^4 - \alpha^3 - 2 - 2^{-1}\alpha^4 - 2\alpha^2 = 0. \end{aligned}$$

Так как $c(\alpha) = c(\alpha^2) = 0$, то $c(x) \in C_{1,2}$. ▲

Обозначим многочлен

$$2 + (x + 2^{-1}x^2)^{sp^\ell+t} + (-x + 2^{-1}x^2)^{sp^\ell+t} - 2(1 + 2^{-1}x^2)^{sp^\ell+t}$$

через $P_{\ell,s,t}(x)$. Если i,j,k удовлетворяют (8) для $\alpha\in\mathbb{F}_{p^m}$ и $c(x)$ – многочлен, указанный в лемме 2, то $c(\alpha^{sp^\ell+t})=P_{\ell,s,t}(\alpha)$.

Лемма 3. *Многочлен $P_{\ell,s,t}(x)$ не является тождественно нулевым при любых $s,t\in\{1,2\}$ и любых $\ell\in\{1,2,\ldots,m-1\}$, а также при $\ell=s=0$, $t\in\{3,\ldots,p-1\}$.*

Доказательство. Коэффициент при x^2 произвольного многочлена $P_{\ell,s,t}(x)$ при указанных в формулировке ограничениях на ℓ,s,t является ненулевым. Действительно, при раскрытии скобок в слагаемых многочлена $P_{\ell,s,t}(x)$ только в последнем слагаемом имеем коэффициент при x^2, равный $-(sp^\ell+t)$. ▲

Теорема 4. *Для любого простого $p\geqslant 3$ и любого $m\geqslant 3$ существует примитивный элемент α поля Галуа $\mathbb{F}_{p^m}$, такой что слово $\bar c$, где*

$$c(x)=2+x^i+x^j-2x^k$$

и i,j,k удовлетворяют условиям (8), является аффинным порождающим элементом кода $\overline{C_{1,2}}$ длины $n=p^m$.

Доказательство. Согласно лемме 2 вектор $\bar c$ принадлежит коду $\overline{C_{1,2}}$. Докажем, что существует примитивный элемент α поля $\mathbb{F}_{p^m}$, такой что аффинная орбита слова $\bar c$ порождает код $\overline{C_{1,2}}$, а координатные позиции кода $C_{1,2}$ перенумерованы степенями элемента α.

Пусть $\bar D$ – расширенный циклический код, являющийся линейной оболочкой аффинной орбиты вектора $\bar c$, и $\bar D\subsetneq\overline{C_{1,2}}$. Докажем, что множества нулей кодов $C_{1,2}$ и D совпадают.

Пусть α^r – нуль многочлена $c(x)$, где r – минимальное число относительно порядка $\prec$, такое что $r\notin\mathrm{cl}(1)\cup\mathrm{cl}(2)$. По определению циклотомического класса без ограничения общности r можно полагать не делящимся на p. Рассмотрим вектор R, являющийся p-ичным представлением числа r. Согласно теореме 1 возможны два случая: либо вектор $R=(t,0,\ldots,0)$ имеет вес 1, где $t\in\{3,\ldots,p-1\}$, либо $R=(t,0,\ldots,0,s,0,\ldots,0)$ имеет вес 2, т.е. $r=sp^\ell+t$, где $s,t\in\{1,2\}$, $\ell\in\{1,\ldots,m-1\}$. Предположим, что во втором случае ℓ больше, чем $\lfloor m/2\rfloor$, где $\alpha^{sp^\ell+t}$ – корень многочлена $c(x)$. Тогда

$$\alpha^{(sp^\ell+t)p^{m-\ell}}=\alpha^{tp^{m-\ell}+s}$$

является корнем $c(x)$, поскольку $sp^\ell+t$ и $tp^{m-\ell}+s$ принадлежат одному и тому же циклотомическому классу. Следовательно, во втором случае достаточно рассмотреть $\ell\in\{1,\ldots,\lfloor m/2\rfloor\}$.

Покажем, что найдется примитивный элемент α, не являющийся корнем многочлена

$$P_{\ell,s,t}(x)=c(x^{sp^\ell+t})$$

для любых s,t,ℓ, таких что $s=\ell=0$, $t\in\{3,\ldots,p-1\}$ или $t,s\in\{1,2\}$, $\ell\in\{1,\ldots,\lfloor m/2\rfloor\}$.

Для этого рассмотрим многочлен

$$Q(x)=\left(\prod_{t=3}^{p-1}P_{0,0,t}(x)\right)\left(\prod_{\ell=1}^{\lfloor m/2\rfloor}\prod_{1\leqslant s,t\leqslant 2}P_{\ell,s,t}(x)\right).\tag{9}$$

Так как по лемме 3 многочлены $P_{\ell,s,t}$ не являются тождественно нулевыми, то и многочлен Q не тождественно нулевой. Убедимся, что степень $\deg(Q)$ многочлена Q меньше числа всех примитивных элементов поля $\mathbb{F}_{p^m}$.

Из определения многочлена $P_{\ell,s,t}$ имеем

$$\deg(P_{\ell,s,t}) \leqslant 2sp^{\ell} + 2t.$$

Отсюда и из (9) получаем

$$\deg(Q) \leqslant (p+2)(p-3) + 12\frac{p^{\lfloor m/2 \rfloor+1} - p}{p-1} + 6m. \tag{10}$$

Покажем, что $\deg(Q) < \varphi(p^m - 1)$ начиная с некоторого достаточно большого m, где $\varphi(p^m - 1)$ – число всех примитивных элементов поля Галуа $\mathbb{F}_{p^m}$. Учитывая хорошо известное неравенство для функции Эйлера φ

$$\varphi(n) > \frac{n}{\ln n} \cdot \frac{\ln 2}{2},$$

при $n = p^m - 1$ получаем

$$\varphi(p^m - 1) > \frac{p^m - 1}{\ln(p^m - 1)} \cdot \frac{\ln 2}{2}. \tag{11}$$

Сравнивая нижнюю оценку (11) для $\varphi(p^m - 1)$ с верхней оценкой (10) степени $\deg(Q)$ многочлена $Q(x)$, нетрудно видеть, что

$$\varphi(p^m - 1) > \deg(Q) \tag{12}$$

начиная с некоторого достаточно большого m. Следовательно, найдется примитивный элемент α в $\mathbb{F}_{p^m}$, такой что $Q(\alpha) \neq 0$, и значит, $D = C_{1,2}$.

В частности, (12) выполняется для всех простых $p \geqslant 101$ и любого $m \geqslant 3$. Для каждого простого $p < 101$ и $m \geqslant 3$, для которых (12) не выполняется, с помощью компьютера был найден примитивный элемент α, такой что $Q(\alpha) \neq 0$.

Следовательно, $D = C_{1,2}$, и кодовое слово $\bar{c}$ является аффинным порождающим элементом кода $\overline{C_{1,2}}$ длины $n = p^m$ для любого $m \geqslant 3$. ▲

Задача нахождения аффинного порождающего элемента наименьшего возможного веса оказалась достаточно трудной для расширенных кодов БЧХ и далека от своего полного решения для всех значений конструктивного расстояния. Открытой и сложной проблемой представляется поиск аффинного порождающего элемента для двоичных расширенных циклических кодов из различных APN-мономов [13] (напомним что в [10] получено решение этой задачи для функции Голда), а также расширенного двоичного кода БЧХ $\overline{C_{1,3,5}}$. В работе [14] установлено, что класс циклических кодов, получаемых из APN-мономов над троичными полями, имеет максимальное кодовое расстояние 4. В этой связи задача существования базиса из кодовых слов минимального веса может быть естественным образом сформулирована, например, для троичных аффинно-инвариантных кодов $\overline{C_{1,4}}$ длины 3^m при нечетных m.

Авторы выражают свою благодарность рецензенту за ряд замечаний и предложений, позволивших улучшить изложение статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Charpin P.* Open Problems on Cyclic Codes // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. V. 1. Ch. 11. P. 965–1063.
2. *Kaufman T., Litsyn S.* Almost Orthogonal Linear Codes Are Locally Testable // Proc. 2005 46th Annu. IEEE Symp. on Foundations of Computer Science (FOCS'05). Pittsburgh, PA, USA. October 23–25, 2005. P. 317–326.

3. *Kaufman T., Sudan M.* Algebraic Property Testing: The Role of Invariance // Proc. 40th Annu. ACM Symp. on Theory of Computing (STOC'08). Victoria, BC, Canada. May 17–20, 2008. New York: ACM, 2008. P. 403–412.
4. *Grigorescu E., Kaufman T.* Explicit Low-Weight Bases for BCH Codes // IEEE Trans. Inform. Theory. 2011. V. 58. № 2. P. 78–81.
5. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
6. *Курляндчик Я.М.* О логарифмической асимптотике длины максимального цикла разброса $r > 2$ // Дискретный анализ. Новосибирск: Инст. матем. СО АН СССР, 1971. Вып. 19. С. 48–55.
7. *Simonis J.* On Generator Matrices of Codes // IEEE Trans. Inform. Theory. 1992. V. 38. № 2. P. 516–516.
8. *Соловьева Ф.И.* О факторизации кодообразующих д.н.ф. // Методы дискретного анализа в исследовании функциональных схем. Новосибирск: Инст. матем. СО АН СССР, 1988. Вып. 47. С. 66–88.
9. *Augot D., Charpin P., Sendrier N.* Studying the Locator Polynomials of Minimum Weight Codewords of BCH Codes // IEEE Trans. Inform. Theory. 1992. V. 38. № 3. P. 960–973.
10. *Mogilnykh I.Yu., Solov'eva F.I.* On Explicit Minimum Weight Bases for Extended Cyclic Codes Related to Gold Functions // Des. Codes Cryptogr. 2018. V. 86. № 11. P. 2619–2627.
11. *Kasami T., Lin S., Peterson W.W.* Some Results on Cyclic Codes Which Are Invariant under the Affine Group and Their Applications // Inform. Control. 1967. V. 11. № 5–6. P. 475–496.
12. *Charpin P., Tietäväinen A., Zinoviev V.* On the Minimum Distances of Non-binary Cyclic Codes // Des. Codes Cryptogr. 1999. V. 17. № 1–3. P. 81–85.
13. *Carlet C., Charpin P., Zinoviev V.* Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems // Des. Codes Cryptogr. 1998. V. 15. № 2. P. 125–156.
14. *Ding C., Helleseth T.* Optimal Ternary Cyclic Codes from Monomials // IEEE Trans. Inform. Theory. 2013. V. 59. № 9. P. 5898–5904.

Могильных Иван Юрьевич
Региональный научно-образовательный математический центр,
Томский государственный университет
Институт математики им. С.Л. Соболева СО РАН
Новосибирский Государственный университет
`ivmog@math.nsc.ru`
Соловьева Фаина Ивановна
Институт математики им. С.Л. Соболева СО РАН
Новосибирский государственный университет
`sol@math.nsc.ru`

Поступила в редакцию
10.07.2020
После доработки
26.10.2020
Принята к публикации
27.10.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 2020 Вып. 4

УДК 621.391 : 519.725

© 2020 г. **А.В. Харин, К.Н. Заверткин, А.А. Овинников**

ОБНАРУЖЕНИЕ ЦИКЛОВ ДЛИНЫ 10 В ГРАФЕ ТАННЕРА КВАЗИЦИКЛИЧЕСКОГО МПП-КОДА ПО РЕЗУЛЬТАТАМ АНАЛИЗА ПРОТОГРАФА[1]

Завершено описание процедуры топологического расширения двудольного графа без параллельных ветвей в плоскости изменения структуры циклов длины до 10 включительно. На основании предыдущих работ дополнен набор теорем, определяющих правила преобразования циклов и маршрутов в результате перехода от протографа к графу Таннера. Предложена процедура определения наличия цикла длины 10 в расширенном графе путем анализа протографа.

Ключевые слова: граф Таннера, протограф, расширенный граф, объединение циклов, базовое уравнение, метрика связанности цикла, МПП-код.

DOI: `10.31857/S0555292320040038`

§ 1. Введение

На сегодняшний день коды с малой плотностью проверок (МПП-коды) занимают одну из лидирующих позиций в технике передачи и хранения данных. При этом наибольшее практическое значение имеет подкласс квазициклических (КЦ) МПП-кодов в силу ряда особенностей [1], обеспечивающих существенные преимущества как при аппаратной, так и программной реализации. Анализ зарубежных источников [2–4] показал, что можно классифицировать все структурированные МПП-коды в порядке уменьшения числа степеней свободы, имеющихся при синтезе проверочных матриц. Рассмотрим три основные категории, представленные на рис. 1, которые, в свою очередь, разбиваются на множество более мелких, имеющих в рамках данной статьи меньшее значение. Наибольшей общностью обладают многореберные (MET – multi-edge type) МПП-коды [2], покрывающие все современные прикладные решения в целевой области. Крайне важным подмножеством многореберных (МР) МПП-кодов являются коды, основанные на протографах (ПГ) [3]. Проверочные матрицы таких кодов получаются за счет расширения небольшого протографа (базового графа) квадратными матрицами фиксированного размера (обычно используются матрицы перестановок). Расширение можно представить следующим образом: протограф копируется несколько раз, а далее переставляются ребра, имеющие одинаковые номера (мы полагаем, что ребра протографа занумерованы). И наконец, КЦ МПП-коды относятся к подмножеству протографов, для которого любая из перестановочных матриц является циклической. При этом в зависимости от типа кодов изменяется ограничение на максимальный вес w циркулянта в классах регулярных и нерегулярных конструкций.

Результаты, полученные в настоящей статье, относятся к КЦ МПП-кодам первого типа, где $w = 1$.

---

[1] Исследование выполнено за счет гранта Российского научного фонда (проект № 17-79-20302).

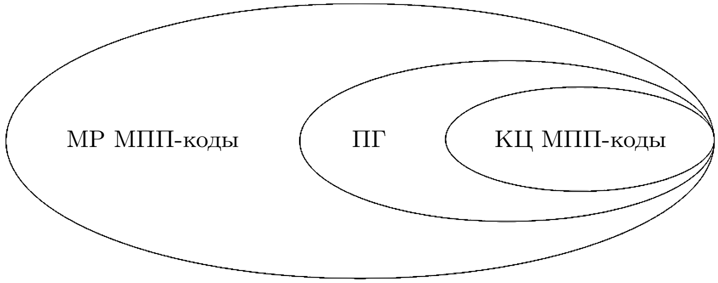


Рис. 1. Классификация структурированных МПП-кодов

Все структурированные МПП-коды могут быть описаны с помощью некоторого базового графа, который с помощью процедуры расширения преобразуется в граф Таннера. Его параметры обычно оптимизируются с целью получения заданных показателей качества. Среди косвенных критериев выделяют максимизацию локального обхвата графа Таннера [5] либо метрик связанности коротких циклов (МСЦ) [6]. Для решения таких оптимизационных задач необходимо уметь быстро обнаруживать циклы различной длины и по необходимости проводить расчет МСЦ. В предшествующей работе [1] была рассмотрена процедура обнаружения циклов длины 8 в графе Таннера КЦ МПП-кода по результатам анализа протографа. Схожие принципы будут отражены и в рамках текущего повествования с некоторыми специфическими особенностями, характерными для циклов большей длины. Дальнейшее увеличение размера исследуемого объекта сопряжено с рядом трудностей и в некоторых случаях полностью лишено смысла. Для полносвязных двудольных протографов величина максимального обхвата ограничена значением 12 согласно работе [7]. Если КЦ МПП-код является нерегулярным или регулярным с наличием ненулевых циркулянтов, то увеличение обхвата сопряжено в первую очередь с устранением балансных циклов [8], что выходит за рамки настоящей статьи. Вопрос топологического расширения базового графа для циклов длины 8 и 10 был рассмотрен в публикации [9], где авторы выдвинули гипотезу о существовании не обнаруживаемого алгоритмом PEG цикла в расширенном графе. Однако их предположение о том, что объединение циклов в базовом графе должно содержать как минимум одно общее ребро является в общем случае ошибочным, что будет доказано рядом теорем ниже. Настоящая статья является логическим продолжением публикации [1] и завершает тему анализа коротких маршрутов в КЦ МПП-кодах.

§ 2. Общие теоретические сведения

Определим необходимые понятия, используемые в дальнейшем как фундамент теоретического исследования.

Пусть ненаправленный двудольный граф КЦ МПП-кода $G = (V, C, E)$ определяется множествами кодовых V и проверочных C вершин, таких что $V \cap C = \varnothing$, а также подмножеством пар $\{(v, c),\ v \in V,\ c \in C\}$, соответствующих ребрам $e = (v, c) \in E$. Степени кодовых и проверочных вершин обозначаются через d_v, $v \in V$, и d_c, $c \in C$. В силу того, что в дальнейшем интерес будут представлять только значения d_v, можно ввести упрощенное обозначение вида $d_{v_i} = d_i$. Маршрут w^g длины g в графе G представляется последовательностью вершин вида $v_0, c_0, v_1, c_1, \ldots, v_{(g-1)}, c_{(g-1)}, v_g$. При этом если $v_0 = v_g$, то маршрут называется замкнутым. Маршрут не содержит обратных проходов, если любая тройка вершин имеет вид v_i, c_j, v_k или c_i, v_j, c_k, $i \neq k$. В дальнейшем будем рассматривать только замкнутые маршруты без обратных проходов, и будем называть их просто маршрутами. Циклом s^g длины g называется такой маршрут, в котором все промежуточные вершины за исключением $v_0 = v_g$

отличаются друг от друга. Обхватом графа G считается длина g_0 кратчайшего цикла s_0. В классе двудольных графов g_0 не может быть меньше $g_{\min} = 4$. Общее количество кодовых и проверочных вершин определяется формулами $n = |V|$, $m = |C|$. Класс КЦ МПП-кодов предполагает отсутствие кратных ребер в соответствующих двудольных графах.

Рассмотрим следующую конструкцию. Пусть C_q – циклическая подгруппа симметричной группы S_q над множеством целых чисел $Z_q = \{0, 1, \ldots, q-1\}$ мощности q с единственной операцией – циклической перестановкой. Элементы S_q – это перестановки на множестве из q элементов. Рассмотрим циркулянт p_a в C_q, который соответствует циклическому сдвигу на a элементов вправо, где a – величина сдвига циркулянта.

Пусть G_b и G – топологически связанные двудольные графы, причем второй получается из первого следующим образом: копируем q раз каждую кодовую и проверочную вершину в G_b, где $v_b \in V_b$, $c_b \in C_b$. Полученные q копий

$$v = \{v_b^0, v_b^1, \ldots, v_b^{q-1}\} \in V \quad \text{и} \quad c = \{c_b^0, c_b^1, \ldots, c_b^{q-1}\} \in C$$

подвергаются циклической перестановке $p_a \in C_q$ для каждой копии e_b в e. Далее граф G_b будет называться базовым или протографом, а G – расширенным графом. Число вершин в G определяется соотношениями $m = m_b q$ и $n = n_b q$.

Известно [7], что представленное топологическое преобразование графов приводит к тому, что интегральный сдвиг для маршрута в G_b определяется согласно формуле

$$P^{g_b} = \sum_{k=0}^{g_b/2-1} (a_{i_k, j_k} - a_{i_{k+1}, j_k}) \mod (q). \tag{1}$$

В предыдущей работе [1] была представлена теорема 1, описывающая необходимое и достаточное условие существования циклов в расширенном графе, в основе которой лежит выражение (1). Дальнейшие рассуждения построены на том факте, что маршруты в базовом рассматриваются как объединения пар коротких циклов s_i и s_j, обладающих как минимум одной общей вершиной. При этом объединение характеризуется следующим набором параметров:

- g_i и g_j – длины пересекающихся циклов;
- n_{cv} – число общих вершин между s_i и s_j;
- n_{ce} – число общих ребер между s_i и s_j;
- n_{cr} – взаимное направление обхода, которое принимает значение, равное нулю, при совпадении обходов циклов по общему ребру (общим ребрам), а в противном случае $n_{\text{cr}} = 1$.

Важное значение при анализе графов Таннера КЦ МПП-кодов имеет метрика связанности циклов (МСЦ), которая показывает число ребер, связывающих проверочные вершины графа с кодовыми узлами текущего цикла и определяемая формулой (см. [6])

$$\gamma = \sum_{k=0}^{g/2-1} (d_k - 2). \tag{2}$$

Оценка МСЦ применительно к маршрутам в базовом графе несколько видоизменяется, что будет показано далее.

В последующих параграфах рассмотрены маршруты целевой длины $g_x = 10$ и образующие их подграфы – элементы протографов, состоящие из объединений циклов

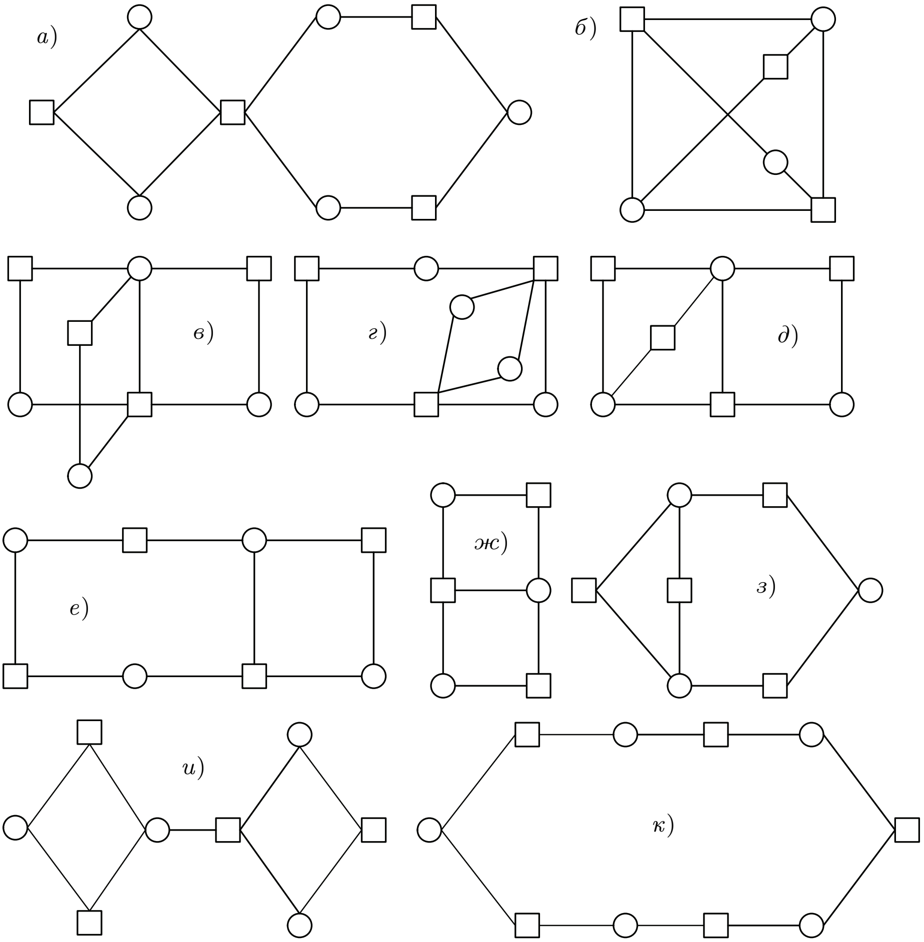


Рис. 2. Конфигурации подграфов, в которых возможно существование маршрутов длины g_x

минимальной длины, а также аналитика изменения значений МСЦ при расширении базового графа.

§ 3. Условия образования циклов

Теорема 1. *Циклы* s^{g_x} *в расширенном графе* G *образуются из маршрутов* w^{g_x} *в базовом графе* G_b, *таких что определяемые ими подграфы изоморфны одному из десяти графов, представленных на рис.* 2.

Доказательство. Пусть цикл имеет вид $s^{g_x} = (u_1, u_2, \dots, u_{g_x}, u_1)$, где $u \in \in C \cup V$. Тогда маршрут в протографе, из которого образовался цикл, имеет вид $w^{g_x} = (f(u_1), f(u_2), \dots, f(u_{g_x}), f(u_1))$, где $f(v_b^i) = v_b$, $f(c_b^j) = c_b$ для всех $v_b \in V_b$, $c_b \in C_b$, $i, j \in [1, q]$.

Тогда маршрут w^{g_x} определяет в графе G_b подграф T с множеством вершин $\{f(u_1), f(u_2), \dots, f(u_{g_x})\}$ и множеством ребер

$$\{(f(u_1), f(u_2)), (f(u_2), f(u_3)), \dots, (f(u_{g_x}), f(u_1))\}.$$

Теперь можно сформулировать следующие предложения.

Предложение 1. *Подграф T изоморфен факторграфу графа S по разбиению P, а именно $T \cong S/P$, где S – цикл с вершинами $\{u_1, u_2, \ldots, u_{g_x}\}$ и ребрами $\{(u_1, u_2), (u_2, u_3), \ldots, (u_{g_x}, u_1)\}$, а P – разбиение I на части вида $\{j \in I \mid f(u_j) = f(u_i)\}$, $i \in I$, $I = \{1, 2, \ldots, g_x\}$.*

Предложение 2. *Для всяких $J \in P$, $u_i, u_j \in J$ разность $i - j$ четна, но отлична от двух и $2g - 2$.*

Для $g_x = 10$ из предложения 2 следует, что J либо одноэлементно, либо является одной из пар (u_1, u_5), (u_2, u_6), (u_3, u_7), (u_4, u_8), (u_5, u_9), (u_6, u_{10}), (u_1, u_7), (u_2, u_8), (u_3, u_9) или (u_4, u_{10}).

Пусть $\mathcal{P}$ – множество всех разбиений множества J, указанного в предложении 2. Назовем $P, Q \in \mathcal{P}$ эквивалентными, $P \sim Q$, если $Q = \{\{a(u_j) \mid u_j \in J\} \mid J \in P\}$, где a – автоморфизм цикла S. Тогда справедливо следующее

Предложение 3. *Если $P \sim Q$, $P, Q \in \mathcal{P}$, то $S/P \cong S/Q$. Если P эквивалентно Q, то факторграф графа S по разбиению P изоморфен факторграфу графа S по разбиению Q.*

Учитывая возможные значения J и предложение 3, существует десять вариантов для P:

$$\begin{aligned}
&\{(u_1, u_5), u_2, u_3, u_4, u_6, u_7, u_8, u_9, u_{10}\},\\
&\{(u_1, u_5), (u_2, u_8), (u_3, u_7), (u_4, u_{10}), u_6, u_9\},\\
&\{(u_1, u_5), (u_4, u_8), u_2, u_3, u_6, u_7, u_9, u_{10}\},\\
&\{(u_1, u_5), (u_3, u_7), u_2, u_4, u_6, u_8, u_9, u_{10}\},\\
&\{(u_1, u_5), (u_2, u_6), (u_4, u_8), u_3, u_7, u_9, u_{10}\},\\
&\{(u_1, u_5), (u_2, u_6), u_3, u_4, u_7, u_8, u_9, u_{10}\},\\
&\{(u_1, u_5), (u_2, u_6), (u_3, u_7), (u_4, u_8), u_9, u_{10}\},\\
&\{(u_1, u_5), (u_2, u_6), (u_3, u_7), u_4, u_8, u_9, u_{10}\},\\
&\{(u_1, u_7), (u_2, u_6), u_3, u_4, u_5, u_8, u_9, u_{10}\},\\
&\{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9, u_{10}\}.
\end{aligned} \tag{3}$$

Тогда S/P для этих вариантов P будет соответствовать подграфам а), б), в), г), д), е), ж), з), и) и к). ▲

В силу того, что подграф к) является одиночным циклом в базовом графе, его учет является относительно тривиальной задачей и может быть выполнен на основе любого алгоритма нумерации циклов.

Теорема 2. *Базовое уравнение для любого маршрута w^{g_x} в протографе может быть выражено через БУ циклов s^4 или s^6, имеющихся в подграфе, определяемом маршрутом w^{g_x}.*

Доказательство полностью аналогично доказательству теоремы 3 из [1]. Поэтому далее приведем только описания маршрутов и циклов для каждого из возможных подграфов и определим связь между их БУ.

Рассмотрим первый из возможных подграфов (рис. 3). В данном подграфе существуют два маршрута длины g_x

$$\begin{aligned}
&w_1^{g_x} = v_1, c_1, v_4, c_3, v_5, c_4, v_3, c_1, v_2, c_2, v_1,\\
&w_2^{g_x} = v_1, c_1, v_3, c_4, v_5, c_3, v_4, c_1, v_2, c_2, v_1
\end{aligned}$$

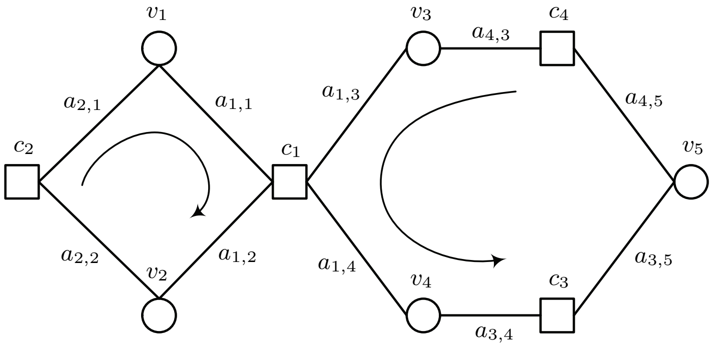


Рис. 3. Графическое изображение подграфа а)

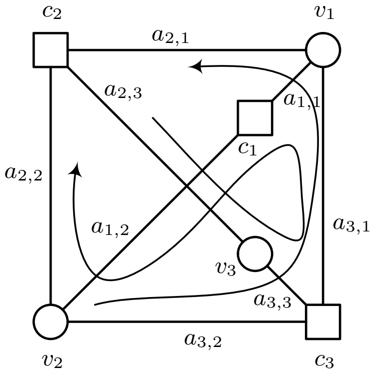


Рис. 4. Графическое изображение подграфа б)

и циклы $s_1^4 = v_1, c_1, v_2, c_2, v_1$ и $s_2^6 = v_3, c_1, v_4, c_3, v_5, c_4, v_3$. При этом их БУ связаны следующими выражениями:

$$\begin{aligned} P_1^{g_x} &= P_1^4 + P_2^6, \\ P_2^{g_x} &= P_1^4 - P_2^6. \end{aligned} \tag{4}$$

Далее рассмотрим второй из возможных подграфов (рис. 4). В нем существуют три маршрута длины g_x

$$\begin{aligned} w_1^{g_x} &= v_1, c_2, v_2, c_3, v_1, c_1, v_2, c_2, v_3, c_3, v_1, \\ w_2^{g_x} &= v_1, c_1, v_2, c_2, v_1, c_3, v_2, c_2, v_3, c_3, v_1, \\ w_3^{g_x} &= v_1, c_1, v_2, c_2, v_1, c_3, v_3, c_2, v_2, c_3, v_1 \end{aligned}$$

и циклы $s_1^4 = v_1, c_2, v_2, c_3, v_1$, $s_2^6 = v_1, c_3, v_3, c_2, v_2, c_1, v_1$ и $s_3^6 = v_1, c_1, v_2, c_3, v_3, c_2, v_1$. При этом БУ для маршрутов $w_1^{g_x}$ и $w_2^{g_x}$ могут быть выражены через (4), а БУ для $w_3^{g_x}$ определяется выражением

$$P_3^{g_x} = P_3^6. \tag{5}$$

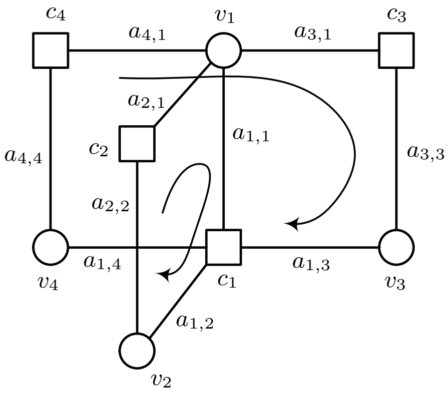


Рис. 5. Графическое изображение подграфа в)

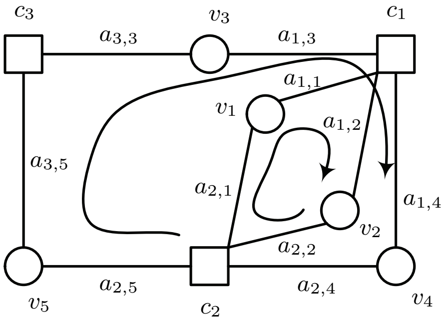


Рис. 6. Графическое изображение подграфа г)

Далее рассмотрим третий из возможных подграфов (рис. 5). В нем существуют шесть маршрутов длины g_x

$$
\begin{aligned}
&w_1^{g_x} = v_1, c_1, v_2, c_2, v_1, c_3, v_3, c_1, v_4, c_4, v_1,\\
&w_2^{g_x} = v_1, c_1, v_2, c_2, v_1, c_4, v_4, c_1, v_3, c_3, v_1,\\
&w_3^{g_x} = v_1, c_1, v_4, c_4, v_1, c_3, v_3, c_1, v_2, c_2, v_1,\\
&w_4^{g_x} = v_1, c_1, v_4, c_4, v_1, c_2, v_2, c_1, v_3, c_3, v_1,\\
&w_5^{g_x} = v_1, c_1, v_3, c_3, v_1, c_2, v_2, c_1, v_4, c_4, v_1,\\
&w_6^{g_x} = v_1, c_1, v_3, c_3, v_1, c_4, v_4, c_1, v_2, c_2, v_1
\end{aligned}
$$

и циклы $s_1^4 = v_1, c_1, v_2, c_2, v_1$, $s_2^6 = v_1, c_3, v_3, c_1, v_4, c_4, v_1$, $s_3^4 = v_1, c_1, v_4, c_4, v_1$, $s_4^6 = v_1, c_3, v_3, c_1, v_2, c_2, v_1$, $s_5^4 = v_1, c_1, v_3, c_3, v_1$ и $s_6^6 = v_1, c_2, v_2, c_1, v_4, c_4, v_1$. При этом их БУ связаны следующими выражениями:

$$
\begin{aligned}
&P_i^{g_x} = P_i^4 + P_{i+1}^6,\\
&P_{i+1}^{g_x} = P_i^4 - P_{i+1}^6
\end{aligned}
\tag{6}
$$

для $i = 1, 3, 5$.

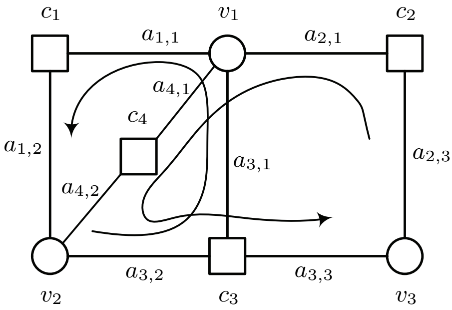


Рис. 7. Графическое изображение подграфа д)

Далее рассмотрим четвертый из возможных подграфов (рис. 6). В нем существуют шесть маршрутов длины g_x

$$w_1^{g_x} = v_1, c_1, v_4, c_2, v_5, c_3, v_3, c_1, v_2, c_2, v_1,$$
$$w_2^{g_x} = v_1, c_1, v_3, c_3, v_5, c_2, v_4, c_1, v_2, c_2, v_1,$$
$$w_3^{g_x} = v_1, c_1, v_2, c_2, v_5, c_3, v_3, c_1, v_4, c_2, v_1,$$
$$w_4^{g_x} = v_1, c_1, v_3, c_3, v_5, c_2, v_2, c_1, v_4, c_2, v_1,$$
$$w_5^{g_x} = v_1, c_2, v_2, c_1, v_4, c_2, v_5, c_3, v_3, c_1, v_1,$$
$$w_6^{g_x} = v_1, c_1, v_3, c_3, v_5, c_2, v_2, c_1, v_4, c_2, v_1$$

и циклы $s_1^4 = v_1, c_1, v_2, c_2, v_1$, $s_2^6 = v_3, c_1, v_4, c_2, v_5, c_3, v_3$, $s_3^4 = v_1, c_1, v_4, c_2, v_1$, $s_4^6 = v_3, c_1, v_2, c_2, v_5, c_3, v_3$, $s_5^4 = v_2, c_1, v_4, c_2, v_2$ и $s_6^6 = v_3, c_1, v_1, c_2, v_5, c_3, v_3$. При этом их БУ связаны выражением (6) для $i = 1, 3, 5$.

Далее рассмотрим пятый из возможных подграфов (рис. 7). В нем существуют четыре маршрута длины g_x

$$w_1^{g_x} = v_1, c_1, v_2, c_3, v_1, c_4, v_2, c_3, v_3, c_2, v_1,$$
$$w_2^{g_x} = v_1, c_1, v_2, c_3, v_1, c_2, v_3, c_3, v_2, c_4, v_1,$$
$$w_3^{g_x} = v_1, c_4, v_2, c_3, v_1, c_1, v_2, c_3, v_3, c_2, v_1,$$
$$w_4^{g_x} = v_1, c_4, v_2, c_3, v_1, c_2, v_3, c_3, v_2, c_1, v_1$$

и циклы $s_1^4 = v_1, c_1, v_2, c_3, v_1$, $s_2^6 = v_1, c_4, v_2, c_3, v_3, c_2, v_1$, $s_3^4 = v_1, c_4, v_2, c_3, v_1$, $s_4^6 = v_1, c_1, v_2, c_3, v_3, c_2, v_1$. При этом их БУ связаны выражением (6) для $i = 1, 3$.

Далее рассмотрим шестой из возможных подграфов (рис. 8). В нем существует один маршрут длины g_x

$$w_1^{g_x} = v_1, c_1, v_2, c_2, v_3, c_3, v_4, c_4, v_2, c_2, v_1$$

и циклы $s_1^4 = v_1, c_1, v_2, c_2, v_1$ и $s_2^6 = v_2, c_2, v_3, c_3, v_4, c_4, v_2$. При этом их БУ связаны выражением

$$P_1^{g_x} = P_1^4 + P_2^6. \tag{7}$$

Далее рассмотрим седьмой из возможных подграфов (рис. 9). В нем существует один маршрут длины g_x

$$w_1^{g_x} = v_1, c_1, v_3, c_2, v_1, c_3, v_2, c_1, v_3, c_2, v_1$$

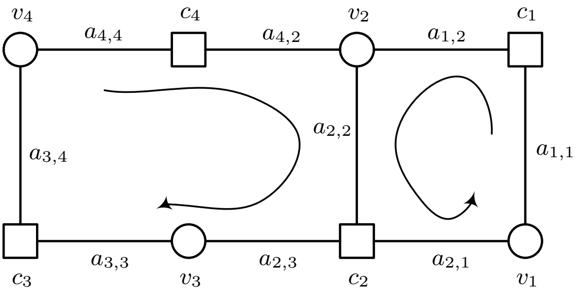


Рис. 8. Графическое изображение подграфа е)

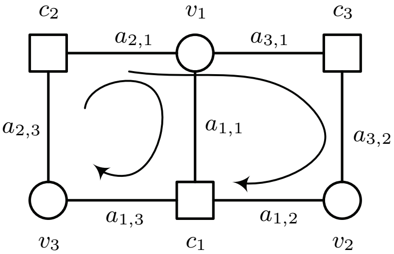


Рис. 9. Графическое изображение подграфа ж)

и циклы $s_1^4 = v_1, c_1, v_3, c_2, v_1$ и $s_2^6 = v_1, c_3, v_2, c_1, v_3, c_2, v_1$. При этом их БУ связаны выражением (7).

Далее рассмотрим восьмой из возможных подграфов (рис. 10). В нем существуют два маршрута длины g_x

$$w_1^{g_x} = v_1, c_1, v_2, c_2, v_1, c_1, v_2, c_4, v_3, c_3, v_1,$$
$$w_2^{g_x} = v_1, c_1, v_2, c_2, v_1, c_3, v_3, c_4, v_2, c_2, v_1$$

и циклы $s_1^4 = v_1, c_1, v_2, c_2, v_1$, $s_2^6 = v_1, c_1, v_2, c_4, v_3, c_3, v_1$ и $s_3^6 = v_1, c_3, v_3, c_4, v_2, c_2, v_1$. При этом их БУ связаны выражениями

$$\begin{aligned} P_1^{g_x} &= P_1^4 + P_2^6, \\ P_2^{g_x} &= P_1^4 + P_3^6. \end{aligned} \tag{8}$$

И наконец, рассмотрим заключительный подграф (рис. 11). В нем существуют два маршрута длины g_x

$$w_1^{g_x} = v_1, c_1, v_2, c_3, v_3, c_4, v_4, c_3, v_2, c_2, v_1,$$
$$w_2^{g_x} = v_1, c_1, v_2, c_3, v_4, c_4, v_3, c_3, v_2, c_2, v_1$$

и циклы $s_1^4 = v_1, c_1, v_2, c_2, v_1$ и $s_2^4 = v_3, c_3, v_4, c_4, v_3$. При этом их БУ связаны выражениями

$$\begin{aligned} P_1^{g_x} &= P_1^4 + P_2^4, \\ P_2^{g_x} &= P_1^4 - P_2^4. \end{aligned} \tag{9}$$

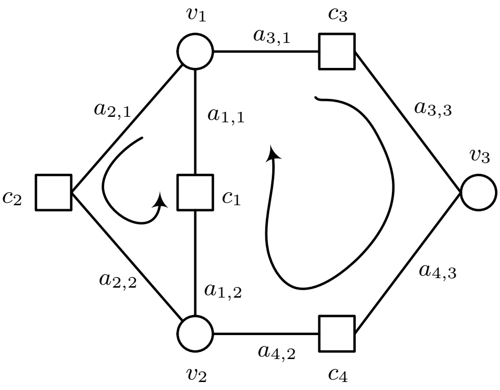


Рис. 10. Графическое изображение подграфа з)

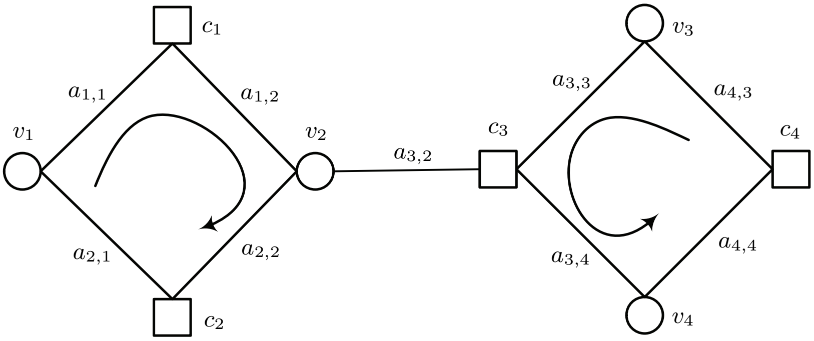


Рис. 11. Графическое изображение подграфа и)

Из всего вышесказанного следует, что БУ любого маршрута длины g_x может быть выражено через БУ циклов длины 4 или 6, которые существуют в подграфе, формируемом маршрутом. ▲

Теорема 3. *Условие образования цикла длины g_x в расширенном графе из маршрута в протографе может быть выражено через базовые уравнения циклов длины 4 и 6, существующих в подграфе, определяемом маршрутом.*

Доказательство аналогично доказательству теоремы 4 из [1], поэтому далее приведем системы условий для маршрутов в каждом подграфе.

Итак, преобразование маршрутов в протографе а) в цикл при расширении графа происходит при выполнении системы условий следующего вида:

$$\begin{cases} (P_1^4 \pm P_2^6) \mod (q) = 0, \\ P_1^4 \mod (q) \neq 0, \\ P_2^6 \mod (q) \neq 0. \end{cases}$$

Аналогичная система условий может быть составлена для маршрутов, существующих в подграфе и) с той лишь разницей, что оба компонентных цикла являются циклами длины 4:

$$\begin{cases}(P_1^4 \pm P_2^4) \mod (q) = 0,\\ P_1^4 \mod (q) \neq 0,\\ P_2^4 \mod (q) \neq 0.\end{cases}$$

Для подграфов е) и ж), где существует по одному возможному маршруту, система условий будет иметь вид

$$\begin{cases}(P_1^4 + P_2^6) \mod (q) = 0,\\ P_1^4 \mod (q) \neq 0,\\ P_2^6 \mod (q) \neq 0.\end{cases}$$

Точно также выглядит система условий для циклов, образующихся из маршрута w_1^{gx} в подграфе з). Для циклов, образующихся из маршрута w_2^{gx} в том же подграфе, с учетом используемых обозначений циклов из теоремы 2 система условий будет иметь вид

$$\begin{cases}(P_1^4 + P_3^6) \mod (q) = 0,\\ P_1^4 \mod (q) \neq 0,\\ P_3^6 \mod (q) \neq 0.\end{cases}$$

Маршруты, существующие в оставшихся подграфах, помимо циклов, через БУ которых выражаются БУ самих маршрутов, содержат в себе и другие циклы. Рассмотрим их подробнее.

Маршруты, образующиеся в подграфе б), помимо циклов, через которые выражаются их БУ в соответствии с теоремой 2, содержат в себе циклы длины 4: $s_2^4 = v_1, c_1, v_2, c_3, v_1$, $s_3^4 = v_1, c_2, v_3, c_3, v_1$, $s_4^4 = v_1, c_1, v_2, c_2, v_1$ и $s_5^4 = v_2, c_2, v_3, c_3, v_2$. Используя данные обозначения циклов и обозначения из теоремы 2, можно показать, что

$$\begin{aligned}&w_1^{gx} \supset s_1^4, s_2^6, s_2^4, s_3^4,\\ &w_2^{gx} \supset s_1^4, s_2^6, s_4^4, s_5^4,\\ &w_3^{gx} \supset s_2^4, s_3^4, s_4^4, s_5^4.\end{aligned}$$

В таком случае, при расширении протографа происходит преобразование маршрутов w_1^{gx} и w_2^{gx} в равновеликие циклы, если выполняется одна из систем условий:

$$\begin{cases}(P_1^4 + P_1^6) \mod (q) = 0,\\ P_1^4 \mod (q) \neq 0,\\ P_1^6 \mod (q) \neq 0,\\ P_2^4 \mod (q) \neq 0,\\ P_3^4 \mod (q) \neq 0,\end{cases} \qquad \begin{cases}(P_1^4 - P_1^6) \mod (q) = 0,\\ P_1^4 \mod (q) \neq 0,\\ P_1^6 \mod (q) \neq 0,\\ P_4^4 \mod (q) \neq 0,\\ P_5^4 \mod (q) \neq 0.\end{cases}$$

Преобразование маршрута w_3^{gx} в равновеликий цикл при расширении протографа происходит, если выполняется следующая система условий:

$$\begin{cases}P_2^6 \mod (q) = 0,\\ P_2^4 \mod (q) \neq 0,\\ P_3^4 \mod (q) \neq 0,\\ P_4^4 \mod (q) \neq 0,\\ P_5^4 \mod (q) \neq 0.\end{cases}$$

Маршруты, образующиеся в подграфе в), содержат по четыре дополнительных цикла. Используя нумерацию циклов из описания подграфа в) в теореме 2, можно показать, что

$$\begin{aligned}
&w_1^{g_x} \supset s_1^4, s_2^6, s_3^4, s_4^6,\\
&w_2^{g_x} \supset s_1^4, s_2^6, s_5^4, s_6^6,\\
&w_3^{g_x} \supset s_3^4, s_4^6, s_1^4, s_2^6,\\
&w_4^{g_x} \supset s_3^4, s_4^6, s_5^4, s_6^6,\\
&w_5^{g_x} \supset s_5^4, s_6^6, s_3^4, s_4^6,\\
&w_6^{g_x} \supset s_5^4, s_6^6, s_1^4, s_2^6.
\end{aligned}$$

В таком случае, при расширении протографа происходит преобразование маршрута w^{g_x} в равновеликий цикл, если выполняется система условий

$$\begin{cases}(P_i^4 + P_{i+1}^6) \mod (q) = 0,\\ P_i^4 \mod (q) \neq 0,\\ P_{i+1}^6 \mod (q) \neq 0,\\ P_k^4 \mod (q) \neq 0,\\ P_{k+1}^6 \mod (q) \neq 0,\end{cases} \tag{10}$$

где $i = 1, 3, 5$, $k = 3, 1, 3$, или

$$\begin{cases}(P_i^4 - P_{i+1}^6) \mod (q) = 0,\\ P_i^4 \mod (q) \neq 0,\\ P_{i+1}^6 \mod (q) \neq 0,\\ P_k^4 \mod (q) \neq 0,\\ P_{k+1}^6 \mod (q) \neq 0,\end{cases} \tag{11}$$

где $i = 1, 3, 5$, $k = 5, 5, 1$.

Маршруты, образующиеся в подграфе г), содержат по четыре дополнительных цикла. Используя нумерацию циклов из описания подграфа г) в теореме 2, можно показать, что

$$\begin{aligned}
&w_1^{g_x} \supset s_1^4, s_2^6, s_3^4, s_4^6,\\
&w_2^{g_x} \supset s_1^4, s_2^6, s_5^4, s_6^6,\\
&w_3^{g_x} \supset s_3^4, s_4^6, s_1^4, s_2^6,\\
&w_4^{g_x} \supset s_3^4, s_4^6, s_5^4, s_6^6,\\
&w_5^{g_x} \supset s_5^4, s_6^6, s_1^4, s_2^6,\\
&w_6^{g_x} \supset s_5^4, s_6^6, s_3^4, s_4^6.
\end{aligned}$$

В таком случае, при расширении протографа происходит преобразование маршрута w^{g_x} в равновеликий цикл, если выполняется система условий (10), где $i = 1, 3, 5$, $k = 3, 1, 1$, или (11), где $i = 1, 3, 5$, $k = 5, 5, 3$.

Маршруты, образующиеся в подграфе д), помимо циклов, через которые выражаются их БУ в соответствии с теоремой 2, содержат в себе циклы длины 4: $s_5^4 = v_1, c_1, v_2, c_4, v_1$ и $s_6^4 = v_1, c_3, v_3, c_2, v_1$. Используя данные обозначения циклов и обозначения из теоремы 2, можно показать, что

$$\begin{aligned}
&w_1^{g_x} \supset s_1^4, s_2^6, s_3^4, s_4^6,\\
&w_2^{g_x} \supset s_1^4, s_2^6, s_5^4, s_6^4,\\
&w_3^{g_x} \supset s_1^4, s_2^6, s_3^4, s_4^6,\\
&w_4^{g_x} \supset s_3^4, s_4^6, s_5^4, s_6^4.
\end{aligned}$$

В таком случае, при расширении протографа происходит преобразование маршрута w^{g_x} в равновеликий цикл, если выполняется система условий (10), где $i = 1, 3$, $k = 3, 3$, или (11), где $i = 1, 3$, $k = 5, 5$.

Таким образом, утверждение теоремы является верным для всех существующих маршрутов. ▲

Теорема 4. *Значение МСЦ для циклов s^{g_x}, за исключением циклов, образуемых из маршрутов, существующих в подграфе и), в расширенном графе может быть выражено через метрики связанности циклов длины 4 и 6, существующих в подграфе, определяемом маршрутом, из которого образован цикл s^{g_x}.*

Доказательство. Следуя логике рассуждений из доказательства теоремы 5 в [1], можно показать следующее.

В случае подграфов а), б), е) и ж) МСЦ циклов длины g_x, образованных соответствующими им маршрутами, могут быть вычислены согласно следующему выражению:

$$\gamma^{g_x} = \gamma_1^4 + \gamma_2^6. \tag{12}$$

В случае подграфов в) и г) МСЦ циклов длины g_x, образованных соответствующими им маршрутами, могут быть вычислены согласно следующему выражению:

$$\gamma^{g_x} = \gamma_1^4 + \gamma_2^6 = \gamma_3^4 + \gamma_4^6 = \gamma_5^4 + \gamma_6^6. \tag{13}$$

В случае подграфа д) МСЦ циклов длины g_x, образованных соответствующими им маршрутами, могут быть вычислены согласно следующему выражению:

$$\gamma^{g_x} = \gamma_1^4 + \gamma_2^6 = \gamma_3^4 + \gamma_4^6. \tag{14}$$

В случае подграфа з) МСЦ циклов длины g_x, образованных соответствующими им маршрутами, могут быть вычислены согласно следующему выражению:

$$\gamma^{g_x} = \gamma_1^4 + \gamma_2^6 = \gamma_1^4 + \gamma_3^6, \tag{15}$$

или

$$\begin{aligned}
\gamma_1^{g_x} &= \gamma_1^4 + \gamma_2^6,\\
\gamma_2^{g_x} &= \gamma_1^4 + \gamma_3^6,
\end{aligned} \tag{16}$$

если в подграфе все кодовые вершины заменить проверочными и наоборот.

Таким образом, утверждение теоремы является верным для всех типов подграфов при целевой длине цикла, равной g_x. ▲

Отдельно рассмотрим значения МСЦ для циклов, образующихся из подграфа и). Они вычисляются в соответствии с выражением

$$\gamma^{g_x} = (d_1 - 2) + 2(d_2 - 2) + (d_3 - 2) + (d_4 - 2).$$

Таблица 1

Параметры n_{cv} и n_{ce} для подграфов

Подграф	а)	б)	в)	г)	д)	е)	ж)	з)
n_{cv}	1	4	2	2	3	2	4	3
n_{ce}	0	2	0	0	1	1	3	2

При этом метрики компонентных циклов длины 4, существующих в подграфе, могут быть выражены уравнениями

$$\gamma_1^4 = (d_1 - 2) + (d_2 - 2),$$
$$\gamma_2^4 = (d_3 - 2) + (d_4 - 2).$$

Тогда будет справедливо следующее выражение:

$$\gamma^{g_x} = \gamma_1^4 + \gamma_2^4 + (d_{\text{ce}} - 2),$$

где d_{ce} – степень кодовой вершины, с которой связано соединяющее циклы ребро.

Если в подграфе заменить типы вершин на противоположные, то выражения для вычисления МСЦ не изменятся.

Таким образом, значение МСЦ для циклов длины g_x, образующихся из маршрутов, существующих в подграфе и), может быть частично выражено через МСЦ коротких циклов с учетом свойств соединяющего их ребра, что позволяет рассчитать МСЦ для циклов длины g_x только на основе информации о протографе, и это также выполняется для всех остальных циклов длины g_x.

§ 4. Процедура определения наличия циклов длины g_x в расширенном графе путем анализа протографа

Полученные выше условия позволяют построить процедуру определения наличия циклов длины g_x в расширенном графе путем анализа циклов, существующих в протографе.

Сравнение алгоритмов обнаружения коротких циклов с прямым поиском маршрутов по вычислительной сложности говорит не в пользу последнего. Поэтому целесообразно взять за основу именно первый вариант. Любой из восьми возможных подграфов (исключая подграф и)), в котором существуют маршруты длины g_x, может быть представлен как объединение двух циклов длины 4 и 6 с некоторым количеством общих вершин n_{cv} и ребер n_{ce}. В табл. 1 приведено соответствие между подграфами, в которых существуют маршруты длины g_x, и параметрами n_{cv} и n_{ce} объединения двух циклов длины 4 и 6.

Подграф и) может быть представлен как объединение двух циклов длины 4 без общих вершин, связанных ребром.

Таким образом, сравнив записи двух циклов длины 4 и 6 и определив наличие общих вершин и ребер, мы можем однозначно определить наличие и тип подграфа согласно теореме 1. Надо обратить внимание на то, что подграфы в) и г) обладают одинаковыми параметрами n_{cv} и n_{ce}, однако алгоритм анализа совпадает для этих подграфов, поэтому необходимость в их различении отсутствует. Обнаружение подграфов и) выполняется с помощью отдельной процедуры, в ходе которой проверяется наличие соединяющих ребер для всех возможных пар циклов длины 4. Также можно заметить, что для описания протографа и выражения БУ маршрута используется одна и та же пара циклов. Все это позволяет нам предложить процедуру определения наличия циклов длины g_x в расширенном графе, который включает в себя следующие шаги:

1) Выполнить поиск одиночных циклов длины g_x, 4 и 6 в протографе;
2) Составить и решить БУ для одиночных циклов длины g_x, найденных в п. 1. Если хотя бы одно связанное с циклом РБУ равно нулю, то процедура завершается, иначе переходим к следующему шагу;
3) Попарно проверить все циклы длины 4 на наличие соединяющих их ребер и обнаружить объединения типа и);
4) Составить и решить систему условий по всем объектам из п. 3, рассчитав РБУ для входящих в условия циклов длины 4;
5) Если хотя бы одна из систем условий выполнена, то процедура завершается, иначе переходим к следующему шагу;
6) Попарно сравнить все циклы длины 4 и 6 и обнаружить их объединения;
7) Определить тип подграфа по табл. 1 для каждого из обнаруженных объединений;
8) Составить и решить систему условий по всем объектам из п. 7, рассчитав РБУ для входящих в условия циклов длины 4 и 6;
9) Цикл длины g_x считается обнаруженным, если хотя бы одна из систем условий выполнена, иначе циклы целевой длины отсутствуют.

С помощью предложенной процедуры мы можем обнаружить циклы длины g_x без выполнения затратной процедуры расширения протографа.

§ 5. Заключение

В результате анализа маршрутов в базовом графе КЦ МПП-кода разработана процедура, определяющая наличие цикла длины $g_x = 10$ в расширенном графе. Сформулирован и доказан набор теорем 1–4, которые обосновывают предлагаемую процедуру. В совокупности с работой [1] показано, что для получения необходимой информации о циклах и их МСЦ в расширенном графе достаточно провести анализ одиночных циклов длины от $g_{\min}$ до g_x, а также их объединений в парах $(g_{\min}, g_{\min})$ и $(g_{\min}, g_{\min} + 2)$ для достижения обхвата графа Таннера вплоть до значения 12 включительно. Таким образом, полностью описан процесс топологического расширения двудольного графа без параллельных ветвей в плоскости изменения структуры циклов длины $g_x < 12$. Дальнейшее увеличение обхвата связано в первую очередь с устранением балансных циклов [8], что возможно лишь на этапе синтеза базового графа.

Далее планируется применить предлагаемый подход для получения регулярных полносвязанных двудольных графов минимально возможной длины при фиксированном числе проверочных вершин в рамках полнопереборного алгоритма с элементами предсказания. Кроме того, значительная область для фундаментальных исследований открывается при переходе к более широкому классу МПП-кодов, основанному на протографах, где кратность ребер может быть произвольной.

Авторы выражают особую благодарность А.Н. Воропаеву за помощь в доработке теоремы 1, а также рецензенту за внимательное прочтение рукописи и ценные замечания, позволившие улучшить качество итоговой статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Харин А.В., Заверткин К.Н., Овинников А.А.* Обнаружение циклов длины 8 в графе Таннера квазициклического МПП-кода по результатам анализа протографа // Пробл. передачи информ. 2020. Т. 56. № 2. С. 82–94.
2. *Richardson T., Urbanke R.* Multi-Edge Type LDPC Codes. Tech. Rep. LTHC-REPORT-2004-001. Communication Theories Lab. (LTHC), EPFL, Switzerland. 2004. Available at `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.106.7310`.

3. *Thorpe J.* Low Density Parity Check (LDPC) Codes Constructed from Protographs. The Interplanetary Network Progress Report № 42-154. Jet Propulsion Lab., California Inst. of Technology. 2003. Available at `https://ipnpr.jpl.nasa.gov/progress_report/42-154/154C.pdf`.
4. *Fan J.L.* Array Codes as Low-Density Parity-Check Codes // Proc. 2nd Int. Symp. on Turbo Codes and Related Topics. Brest, France. Sept. 4–7, 2000. P. 543–546.
5. *Hu X.-Y., Eleftheriou E., Arnold D.M.* Regular and Irregular Progressive Edge-Growth Tanner Graphs // IEEE Trans. Inform. Theory. 2005. V. 51. № 1. P. 386–398.
6. *Tian T., Jones C.R., Villasenor J.D., Wesel R.D.* Selective Avoidance of Cycles in Irregular LDPC Code Construction // IEEE Trans. Commun. 2004. V. 52. № 8. P. 1242–1247.
7. *Fossorier M.P.C.* Quasi-cyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices // IEEE Trans. Inform. Theory. 2004. V. 50. № 8. P. 1788–1793.
8. *Xiao G., Nan Z.* Analysis of Balanced Cycles of QC-LDPC Codes // Proc. 8th Int. Conf. on Wireless and Optical Communication Networks (WOCN'2011). Paris, France. May 24–26, 2011. P. 1–5.
9. *Diouf M., Declercq D., Fossorier M., Quya S., Vasić B.* Improved PEG Construction of Large Girth QC-LDPC Codes // Proc. 9th Int. Symp. on Turbo Codes & Iterative Information Processing (ISTC'2016). Brest, France. Sept. 5–9, 2016. P. 146–150.
10. *Karimi M., Banihashemi A.H.* On the Girth of Quasi Cyclic Protograph LDPC Codes // IEEE Trans. Inform. Theory. 2013. V. 59. № 7. P. 4542–4552.

Харин Алексей Владимирович
Заверткин Константин Николаевич
Овинников Алексей Анатольевич
Рязанский государственный радиотехнический
университет им. В.Ф. Уткина,
факультет радиотехники и телекоммуникаций,
кафедра телекоммуникаций и основ радиотехники
`kharin.a.v@tor.rsreu.ru`
`zavertkin.k.n@tor.rsreu.ru`
`ovinnikov.a.a@tor.rsreu.ru`

Поступила в редакцию
27.08.2020
После доработки
23.11.2020
Принята к публикации
23.11.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.17

© 2020 г. **С. Чжоу, Ч. Сунь, Ц. Пань**

ДОСТАТОЧНОЕ УСЛОВИЕ СУЩЕСТВОВАНИЯ В ГРАФАХ ДРОБНЫХ (g, f)-ФАКТОРОВ С ОГРАНИЧЕНИЯМИ[1]

В NFV-сети доступность планирования ресурсов может быть выражена наличием дробного фактора в соответствующем графе. Исследования о существовании специальных дробных факторов в структуре сети могут помочь построить NFV-сеть с эффективным распределением ресурсов. Рассмотрим некоторую функцию $h\colon E(G) \to [0,1]$. Обозначим $d_G^h(x) = \sum\limits_{e \ni x} h(e)$. Назовем граф F_h с множеством вершин $V(G)$ и множеством ребер E_h дробным (g, f)-фактором графа G с индикаторной функцией h, если неравенство $g(x) \leqslant d_G^h(x) \leqslant f(x)$ выполняется для любого $x \in V(G)$, где $E_h = \{e : e \in E(G),\ h(e) > 0\}$. Скажем, что G обладает свойством $E(m, n)$ относительно дробного (g, f)-фактора, если для любых двух множеств независимых ребер M и N, таких что $|M| = m$, $|N| = n$ и $M \cap N = \varnothing$, граф G допускает дробный (g, f)-фактор F_h, такой что $h(e) = 1$ для всякого $e \in M$ и $h(e) = 0$ для всякого $e \in N$. Понятие $E(m, n)$-свойства относительно дробного (g, f)-фактора отвечает структуре NFV-сети, где определенные каналы заняты или повреждены в некоторые моменты времени. Рассматривается проблема планирования ресурсов в NFV-сетях, используя теорию графов. Приводится условие, основанное на объединении окрестностей вершин, при котором граф обладает $E(1, n)$-свойством относительно дробного (g, f)-фактора. Кроме того, показывается, что нижняя оценка в данном условии является наилучшей возможной в некотором смысле.

Ключевые слова: NFV-сеть; граф; объединение окрестностей; дробный (g, f)-фактор; дробные (g, f)-факторы с ограничениями.

DOI: `10.31857/S055529232004004X`

§ 1. Введение

Построение сервисной цепочки для новой сети традиционным способом требует покупки и настройки специальных аппаратных устройств и их физического соединения в определенной последовательности. Расходы на построение и поддержание такой системы могут быть высоки, а соответствующее аппаратное решение всегда избыточно, что выливается в трату аппаратных ресурсов в непиковые часы. Виртуализация сетевых функций (NFV – network function virtualization) – смена парадигмы, достигнутая инженерами на примере Vodafone, China Mobile и AT&T, – ставит своей целью решение вышеозначенных проблем путем упрощения и ускорения продвижения сетевых сервисов. Европейский институт телекоммуникационных стандартов (ETSI) опубликовал в 2012 г. серию отчетов об NFV, в которых описывались область применения, задачи и возможности, развитие индустрии и архитектурное моделирование. Виртуальные сетевые функции могут быть созданы по необходимости без

---

[1] Работа выполнена при частичной финансовой поддержке проекта “Шесть вершин таланта” провинции Цзянсу, Китай (номер гранта JY-022).

установки новых устройств. Это позволяет операторам сети обновлять, создавать и удалять сервисные цепочки недорогим и гибким способом. Одной из главных проблем в сервисе NFV является возможность планирования ресурсов, которая эквивалентна наличию дробного (g, f)-фактора со свойством $E(m, n)$. Это создает мотивацию для исследования соответствующей теоретической проблемы с использованием теории графов.

В данной статье рассматриваются простые и конечные графы. Терминологию и обозначения, которые не вводятся здесь явно, можно найти в монографии [1]. Пусть $G = (V(G), E(G))$ – некоторый граф, где $V(G)$ обозначает множество вершин, а $E(G)$ – множество ребер графа G. Множества вершин и ребер графа G соответствуют множествам узлов и каналов в NFV-сети. Для вершины x из G обозначим через $N_G(x)$ окрестность x в G, а через $d_G(x) = |N_G(x)|$ – степень x в G. Будем использовать обозначение $N_G[x]$ для $N_G(x) \cup \{x\}$. Введем также $\delta(G)$ – минимальную степень G и $i(G)$ – число изолированных вершин G. Для подмножества вершин X из G обозначим через $G[X]$ подграф G, индуцированный X, и будем использовать обозначение $G - X$ для $G[V(G) \setminus X]$. Подмножество вершин X из G является независимым множеством G, если никакие две вершины из X не смежны в G. Для подмножества $E' \subseteq E(G)$ граф, полученный из G удалением ребер, принадлежащих E', обозначается через $G - E'$. Для всякого $X \subseteq V(G)$ введем

$$\varphi(X) = \sum_{x \in X} \varphi(x)$$

для любой функции φ, определенной на $V(G)$, и положим $\varphi(\varnothing) = 0$. Соединение $G \vee H$ обозначает граф с множеством вершин $V(G) \cup V(H)$ и множеством ребер

$$E(G \vee H) = E(G) \cup E(H) \cup \{xy : \, x \in V(G), \, y \in V(H)\}.$$

Пусть $g, f \colon V(G) \to Z$ – некоторые функции, удовлетворяющие неравенству $0 \leqslant g(x) \leqslant f(x)$ для любого $x \in V(G)$. Остовный подграф F графа G назовем (g, f)-фактором, если $g(x) \leqslant d_F(x) \leqslant f(x)$ для любого $x \in V(G)$. Далее, (g, f)-фактор является $[a, b]$-фактором, если $g(x) = a$ и $f(x) = b$ для всякого $x \in V(G)$. Скажем, что (g, f)-фактор является f-фактором, если $g(x) = f(x)$ для любого $x \in V(G)$. Если $f(x) \equiv k$, то f-фактор называется k-фактором. 1-фактор называется также совершенным паросочетанием.

Пусть $h \colon E(G) \to [0, 1]$ – некоторая функция. Будем писать

$$d^h_G(x) = \sum_{e \ni x} h(e).$$

Назовем граф F_h с множеством вершин $V(G)$ и множеством ребер E_h дробным (g, f)-фактором G с индикаторной функцией h, если $g(x) \leqslant d^h_G(x) \leqslant f(x)$ для любого $x \in V(G)$, где $E_h = \{e : \ e \in E(G), \ h(e) > 0\}$. Если $g(x) = f(x)$ для всякого $x \in V(G)$, то дробный (g, f)-фактор является дробным f-фактором. Дробный f-фактор называется дробным k-фактором, если $f(x) = k$ для любого $x \in V(G)$. Дробный 1-фактор называется также совершенным дробным паросочетанием.

Подмножество E' множества $E(G)$ называется множеством независимых ребер, если никакие два ребра E' не инцидентны одной вершине. Скажем, что G обладает свойством $E(m, n)$ относительно дробного (g, f)-фактора, если для любых двух независимых множеств ребер M и N с $|M| = m$, $|N| = n$ и $M \cap N = \varnothing$ граф G допускает дробный (g, f)-фактор F_h, где $h(e) = 1$ для любого $e \in M$ и $h(e) = 0$ для любого $e \in N$. Если $g(x) = f(x)$ для всякого $x \in V(G)$, то свойство $E(m, n)$ относительно дробного (g, f)-фактора является свойством $E(m, n)$ относительно дробного f-фактора. Если $f(x) \equiv k$, то свойство $E(m, n)$ относительно дробного f-фактора является свойством $E(m,n)$ относительно дробного k-фактора. В частности, свойство $E(m,n)$ относительно 1-фактора называется также свойством $E(m,n)$ относительно совершенного дробного паросочетания, и мы говорим, что G – дробный $E(m,n)$. Похожим образом можно определить свойство $E(m,n)$ относительно (g,f)-фактора, свойство $E(m,n)$ относительно f-фактора, свойство $E(m,n)$ относительно k-фактора и свойство $E(m,n)$ относительно совершенного паросочетания.

Описание графов, допускающих дробные (g,f)-факторы, было получено в работе [2]. Новое доказательство было представлено в [3].

Теорема 1 [2,3]. *Пусть G – некоторый граф, и пусть g,f – две целочисленные функции, определенные на $V(G)$, такие что $0 \leqslant g(x) \leqslant f(x)$ для всех $x \in V(G)$. Тогда G допускает дробный (g,f)-фактор, если и только если*

$$\gamma_G(S,T) = f(S) + d_{G-S}(T) - g(T) \geqslant 0$$

для любого $S \subseteq V(G)$, где $T = \{x : x \in V(G) \setminus S,\ d_{G-S}(x) \leqslant g(x)\}$.

Авторы работы [4] расширили теорему 1 и представили описание графов, допускающих дробный (g,f)-фактор, со свойством $E(1,0)$. Эта теорема будет использована позже при доказательстве основного результата.

Теорема 2 [4]. *Пусть G – некоторый граф, и пусть g,f – две целочисленные функции, определенные на $V(G)$, такие что $0 \leqslant g(x) \leqslant f(x)$ для всех $x \in V(G)$. Тогда G допускает дробный (g,f)-фактор со свойством $E(1,0)$, если и только если*

$$\gamma_G(S,T) = f(S) + d_{G-S}(T) - g(T) \geqslant \varepsilon(S,T)$$

для любого $S \subseteq V(G)$, где $T = \{x : x \in V(G) \setminus S,\ d_{G-S}(x) \leqslant g(x)\}$, а $\varepsilon(S,T)$ определено следующим образом:

$$\varepsilon(S,T) = \begin{cases} 2, & \text{если } S \text{ не является независимым множеством,} \\ 1, & \text{если } S \text{ является независимым множеством и есть ребро,} \\ & \text{соединяющее } S \text{ и } V(G) \setminus (S \cup T)\text{, или есть ребро } e = uv\text{, соеди-} \\ & \text{няющее } S \text{ и } T\text{, такое что } d_{G-S}(v) = g(v) \text{ для любого } v \in T, \\ 0 & \text{в противном случае.} \end{cases}$$

В работе [5] для графов, допускающих k-факторы, было выведено условие на окрестности.

Теорема 3 [5]. *Пусть $k \geqslant 2$ – целое число, а G – связный граф порядка p, где $p \geqslant 9k - 1 - 4\sqrt{2(k-1)^2 + 2}$. Предположим, что kp четно и $\delta(G) \geqslant k$. Если G удовлетворяет условию*

$$|N_G(u) \cup N_G(v)| \geqslant \frac{p+k-2}{2}$$

для любой пары несмежных вершин $u, v \in V(G)$, то G допускает k-фактор.

Авторы работы [6] обобщили теорему 3 и получили условие на окрестности для графов, допускающих дробные k-факторы.

Теорема 4 [6]. *Пусть $k \geqslant 1$ – целое число, и пусть G является связным графом порядка p, где $p \geqslant 9k - 1 - 4\sqrt{2(k-1)^2 + 2}$, а $\delta(G) \geqslant k$. Если G удовлетворяет условию*

$$|N_G(u) \cup N_G(v)| \geqslant \max\left\{\frac{p}{2}, \frac{p+k-2}{2}\right\}$$

для любой пары несмежных вершин u, v из G, то G допускает дробный k-фактор.

В работах многих авторов были получены и другие результаты о факторах [7–17] и дробных факторах [18–29] графов. Отметим, что дробный (g, f)-фактор G с индикаторной функцией h является (g, f)-фактором графа G, если $h(e) \in \{0, 1\}$ для любого $e \in E(G)$; (g, f)-фактор называется просто k-фактором, а дробный (g, f)-фактор называется просто дробным k-фактором, если $g(x) = f(x) = k$ для любого $x \in V(G)$. Тем самым, понятие дробного (g, f)-фактора (соответственно, дробного k-фактора) является обобщением понятия (g, f)-фактора (соответственно, k-фактора). Более того, нетрудно видеть, что понятие свойства $E(m, n)$ относительно дробного (g, f)-фактора является обобщением понятия дробного (g, f)-фактора. Поэтому мы естественным образом обобщим теоремы 3, 4 и выведем условие на окрестности для графов, обладающих свойством $E(1, n)$ относительно дробного (g, f)-фактора.

Теорема 5. *Пусть a, b, r, n – неотрицательные целые числа, такие что $2 \leqslant a \leqslant b - r$. Рассмотрим граф G порядка p, где*

$$p \geqslant \frac{2(a + b)(a + b + n - 1) + 2}{a + r},$$

а функции $g, f\colon V(G) \to Z$ таковы, что $a \leqslant g(x) \leqslant f(x) - r \leqslant b - r$ для любого $x \in V(G)$. Если G удовлетворяет условиям

$$\delta(G) \geqslant \frac{(b + 1)(b - r + 2) - b + a}{a + r}$$

и

$$|N_G(u) \cup N_G(v)| \geqslant \frac{(b - r)p + 2}{a + b}$$

для каждой пары u, v из G, то G обладает свойством $E(1, n)$ относительно дробного (g, f)-фактора.

Граф G называется дробным (g, f)-покрытым графом, если для любого $e \in E(G)$ существует дробный (g, f)-фактор F_h, удовлетворяющий условию $h(e) = 1$. Если в теореме 5 положить $n = 0$, то получаем

Следствие 1. *Пусть a, b, r – неотрицательные целые числа, такие что $2 \leqslant a \leqslant b - r$. Рассмотрим граф G порядка p, где*

$$p \geqslant \frac{2(a + b)(a + b - 1) + 2}{a + r},$$

а функции $g, f\colon V(G) \to Z$ таковы, что $a \leqslant g(x) \leqslant f(x) - r \leqslant b - r$ для любого $x \in V(G)$. Если G удовлетворяет условиям

$$\delta(G) \geqslant \frac{(b + 1)(b - r + 2) - b + a}{a + r}$$

и

$$|N_G(u) \cup N_G(v)| \geqslant \frac{(b - r)p + 2}{a + b}$$

для каждой пары несмежных вершин u, v из G, то G является дробным (g, f)-покрытым графом.

Следствие 1 похоже на следствие 2 недавней работы [22], однако следствие 1 дает потенциально лучший результат, поскольку оно использует размер объединения окрестностей, а не максимум из степеней вершин.

Если $g(x) \equiv f(x) \equiv k$ в теореме 5, то получаем следующий результат.

Следствие 2. *Пусть n и $k \geqslant 2$ – неотрицательные целые числа, и пусть G – граф порядка p, где $p \geqslant 4(2k+n-1)+\dfrac{2}{k}$. Если G удовлетворяет условиям*

$$\delta(G) \geqslant k+3+\frac{2}{k}$$

и

$$|N_G(u) \cup N_G(v)| \geqslant \frac{kp+2}{2k}$$

для каждой пары несмежных вершин u, v из G, то G обладает свойством $E(1,n)$ относительно дробного k-фактора.

§ 2. Доказательство теоремы 5

Предположим, что G удовлетворяет условиям теоремы 5, но не обладает свойством $E(1,n)$ относительно дробного (g,f)-фактора. Тогда существует множество независимых ребер $\{e_1, e_2, \ldots, e_n\}$ и ребро e из G, такие что граф G не допускает (g,f)-фактора F_h с $h(e_i)=0$ для $1 \leqslant i \leqslant n$ и $h(e)=1$. Обозначим $N=\{e_1,e_2,\ldots,e_n\}$ и $H=G-N$, где N – множество независимых ребер графа G. Ясно, что H не обладает свойством $E(1,0)$ относительно дробного (g,f)-фактора. В силу теоремы 2 существует подмножество вершин $S \subseteq V(H)$, удовлетворяющее соотношению

$$\gamma_H(S,T)=f(S)+d_{H-S}(T)-g(T) \leqslant \varepsilon(S,T)-1, \tag{1}$$

где $T=\{x:\ x \in V(H) \setminus S,\ d_{H-S}(x) \leqslant g(x)\}$.

Предложение 1. *Справедлива оценка $|T| \geqslant 2$.*

Доказательство. Если $|T|=0$, то согласно (1) получаем

$$\begin{aligned}&\varepsilon(S,T)-1 \geqslant \gamma_H(S,T)=f(S)+d_{H-S}(T)-g(T) \geqslant f(S) \geqslant\\ &\quad\geqslant (a+r)|S| \geqslant |S| \geqslant \varepsilon(S,T),\end{aligned}$$

что приводит к противоречию. Далее будем предполагать, что $|T|=1$. Положим $T=\{t\}$. Тогда из соотношений $H=G-N$ и

$$\delta(G) \geqslant \frac{(b+1)(b-r+2)-b+a}{a+r}$$

следует, что

$$\begin{aligned}&\gamma_H(S,T)=f(S)+d_{H-S}(T)-g(T)=f(S)+d_{H-S}(t)-g(t) \geqslant\\ &\quad\geqslant (a+r)|S|+d_{G-S}(t)-1-(b-r) \geqslant (a+r)|S|+d_G(t)-|S|-1-(b-r) \geqslant\\ &\quad\geqslant (a+r-1)|S|+\delta(G)-(b-r+1) \geqslant\\ &\quad\geqslant (a+r-1)|S|+\frac{(b+1)(b-r+2)-b+a}{a+r}-(b-r+1)=\\ &\quad=(a+r-1)|S|+\frac{(b-a-r)(b-r+1)+a+b+2-r}{a+r}>\\ &\quad>(a+r-1)|S| \geqslant |S| \geqslant \varepsilon(S,T),\end{aligned}$$

что противоречит неравенству (1). Стало быть, $|T| \geqslant 2$. ▲

Предложение 2. *Справедливо неравенство*

$$(b-r)|T|>(a+r)|S|-2.$$

Доказательство. Если $(b-r)|T| \leqslant (a+r)|S|-2$, то из (1) и $\varepsilon(S,T) \leqslant 2$ следует, что

$$\begin{aligned}&\varepsilon(S,T)-1 \geqslant \gamma_H(S,T) = f(S)+d_{H-S}(T)-g(T) \geqslant f(S)-g(T) \geqslant\\ &\quad \geqslant (a+r)|S|-(b-r)|T| \geqslant (b-r)|T|+2-(b-r)|T| = 2 \geqslant \varepsilon(S,T),\end{aligned}$$

что приводит к противоречию. ▲

Предложение 3. *Справедливо неравенство*

$$|S| < \frac{(b-r)p+2}{a+b}.$$

Доказательство. С учетом предложения 2 и того, что $|S|+|T| \leqslant p$, получаем оценку

$$(b-r)p \geqslant (b-r)(|S|+|T|) > (b-r)|S|+(a+r)|S|-2 = (a+b)|S|-2,$$

из которой следует, что

$$|S| < \frac{(b-r)p+2}{a+b}. \quad ▲$$

Предложение 4. *Для всякого $x \in T$ верно неравенство*

$$d_{G-S}(x) \leqslant d_{H-S}(x)+1 \leqslant g(x)+1 \leqslant b-r+1.$$

Доказательство. Заметим, что $N = \{e_1, e_2, \dots, e_n\}$ является множеством независимых ребер G и $H = G-N$. Значит,

$$d_{G-S}(x) \leqslant d_{H-S}(x)+1$$

для любого $x \in T$. Таким образом, по определению T имеем

$$d_{G-S}(x) \leqslant d_{H-S}(x)+1 \leqslant g(x)+1 \leqslant b-r+1$$

для всякого $x \in T$. ▲

Предложение 5. *Справедливо неравенство*

$$d_{H-S}(T) \geqslant d_{G-S}(T) - \min\{2n, |T|\}.$$

Доказательство. Введем обозначения

$$D = V(G) \setminus (S \cup T)$$

и

$$E_G(T) = \{e:\ e = xy \in E(G),\ x, y \in T\}.$$

Пусть $s \leqslant n$ – два целых неотрицательных числа. Заметим, что N является множеством независимых ребер G. Положим $N = \{e_1, e_2, \dots, e_n\}$, где $e_i = u_i v_i$ для $1 \leqslant i \leqslant n$. Запишем $N \cap E_G(T) = \{u_1 v_1, \dots, u_r v_r\}$ и $N \cap E_G(T, D) = \{u_{r+1} v_{r+1}, \dots, u_s v_s\}$. Очевидно,

$$2|N \cap E_G(T)| + |N \cap E_G(T,D)| = 2r + (s-r) = r+s$$

и

$$|T| \geqslant 2r + (s-r) = r+s.$$

Таким образом, приходим к неравенству

$$2|N \cap E_G(T)| + |N \cap E_G(T, D)| \leqslant |T|.$$

Легко видеть, что $2|N \cap E_G(T)| + |N \cap E_G(T, D)| \leqslant \min\{2n, |T|\}$. Стало быть, мы получаем, что

$$\begin{aligned} &d_{H-S}(T) = d_{G-N-S}(T) = d_{G-S}(T) - (2|N \cap E_G(T)| + |N \cap E_G(T, D)|) \geqslant \\ &\geqslant d_{G-S}(T) - \min\{2n, |T|\}. \quad \blacktriangle \end{aligned}$$

Отметим, что $T \neq \varnothing$ по предложению 1. Таким образом, можно определить

$$h_1 = \min\{d_{G-S}(x) : \, x \in T\}$$

и

$$\rho = |\{x : \, x \in T, \, d_{G-S}(x) = 0\}|.$$

Пусть $x_1 \in T$, где $d_{G-S}(x_1) = h_1$. Если $T \setminus N_T[x_1] \neq \varnothing$, то зададим

$$h_2 = \min\{d_{G-S}(x) : \, x \in T \setminus N_T[x_1]\}$$

и выберем $x_2 \in T$ так, что $d_{G-S}(x_2) = h_2$.

С учетом предложения 4 и определений h_1, h_2 и T легко видеть, что

$$0 \leqslant h_1 \leqslant h_2 \leqslant b - r + 1.$$

Далее рассмотрим три случая.

Случай 1: $\rho \geqslant 2$.

В этом случае существуют по меньшей мере две вершины $x, y \in T$, такие что $d_{G-S}(x) = d_{G-S}(y) = 0$ и $xy \notin E(G)$. Согласно предложению 3 и предположению теоремы 5 получаем

$$\frac{(b-r)p+2}{a+b} \leqslant |N_G(x) \cup N_G(y)| \leqslant d_{G-S}(x) + d_{G-S}(y) + |S| = |S| < \frac{(b-r)p+2}{a+b},$$

что является противоречием.

Случай 2: $\rho = 1$.

Заметим, что $d_{G-S}(x_1) = h_1$ и $d_{G-S}(x_2) = h_2$. Очевидно, $h_1 = 0$ и $|N_T[x_1]| = 1$. Из предложения 1 и равенства $\rho = 1$ следует, что $T \setminus N_T[x_1] \neq \varnothing$ и $1 \leqslant h_2 \leqslant b - r + 1$. Очевидно, что $x_1 x_2 \notin E(G)$. Тогда с учетом предположения теоремы 5 имеем

$$\frac{(b-r)p+2}{a+b} \leqslant |N_G(x_1) \cup N_G(x_2)| \leqslant d_{G-S}(x_1) + d_{G-S}(x_2) + |S| = h_2 + |S|,$$

откуда следует неравенство

$$|S| \geqslant \frac{(b-r)p+2}{a+b} - h_2. \tag{2}$$

Случай 2.1: $h_2 = b - r + 1$.

Предложение 6. *Верно следующее неравенство*:

$$\frac{2(a+b)(a+b+n-1)+2}{a+r} > \frac{(a+b)((a+r+1)(b-r+1)+2) - 2(a+r)}{(a+r)(b-r)}.$$

Доказательство. Из неравенств $2 \leqslant a \leqslant b-r$ и $n \geqslant 0$ следует, что

$$\begin{aligned}
&(b-r)(2(a+b)(a+b+n-1)+2)-\\
&\ -((a+b)((a+r+1)(b-r+1)+2)-2(a+r))=\\
&\ =2(a+b)(a+b+n-1)(b-r)-(a+b)(a+r+1)(b-r+1)=\\
&\ =(a+b)(b-r)(a+2b+2n-r-3)-(a+b)(a+r+1)\geqslant\\
&\ \geqslant 2(a+b)(a+2b+2n-r-3)-(a+b)(a+r+1)\geqslant\\
&\ \geqslant 2(a+b)(a+2(2+r)-r-3)-(a+b)(a+r+1)=(a+b)(a+r+1)>0,
\end{aligned}$$

откуда вытекает требуемая оценка. ▲

Заметим, что

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r} > \frac{(a+b)((a+r+1)(b-r+1)+2)-2(a+r)}{(a+r)(b-r)}$$

по предложению 6. В свете соотношений (1), (2) и предложения 5 получаем

$$\begin{aligned}
&\varepsilon(S,T)-1 \geqslant \gamma_H(S,T)=f(S)+d_{H-S}(T)-g(T)\geqslant\\
&\ \geqslant f(S)+d_{G-S}(T)-\min\{2n,|T|\}-g(T)\geqslant\\
&\ \geqslant (a+r)|S|+h_2(|T|-1)-|T|-(b-r)|T|=\\
&\ =(a+r)|S|-(b-r+1-h_2)|T|-h_2\geqslant\\
&\ \geqslant (a+r)\left(\frac{(b-r)p+2}{a+b}-h_2\right)-h_2=\\
&\ =(a+r)\left(\frac{(b-r)p+2}{a+b}-(b-r+1)\right)-(b-r+1)=\\
&\ =\left(\frac{(a+r)(b-r)p+2(a+r)}{a+b}-(a+r)(b-r+1)\right)-(b-r+1)>\\
&\ >\frac{(a+b)((a+r+1)(b-r+1)+2)-2(a+r)+2(a+r)}{a+b}-\\
&\ -(a+r+1)(b-r+1)=2\geqslant\varepsilon(S,T),
\end{aligned}$$

что приводит к противоречию.

Случай 2.2: $1 \leqslant h_2 \leqslant b-r$.

С учетом (2), предложения 5 и соотношений $|S|+|T| \leqslant p$ и

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r}$$

имеем

$$\begin{aligned}
&\gamma_H(S,T)=f(S)+d_{H-S}(T)-g(T)\geqslant\\
&\ \geqslant f(S)+d_{G-S}(T)-\min\{2n,|T|\}-g(T)\geqslant\\
&\ \geqslant (a+r)|S|+h_2(|T|-1)-2n-(b-r)|T|=\\
&\ =(a+r)|S|-(b-r-h_2)|T|-h_2-2n\geqslant\\
&\ \geqslant (a+r)|S|-(b-r-h_2)(p-|S|)-h_2-2n=\\
&\ =(a+b-h_2)|S|-(b-r-h_2)p-h_2-2n\geqslant\\
&\ \geqslant (a+b-h_2)\left(\frac{(b-r)p+2}{a+b}-h_2\right)-(b-r-h_2)p-h_2-2n,
\end{aligned}$$

т.е.

$$\gamma_H(S,T) \geqslant (a+b-h_2)\left(\frac{(b-r)p+2}{a+b} - h_2\right) - (b-r-h_2)p - h_2 - 2n. \tag{3}$$

Положим

$$\varphi(h_2) = (a+b-h_2)\left(\frac{(b-r)p+2}{a+b} - h_2\right) - (b-r-h_2)p - h_2 - 2n.$$

Поскольку

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r} > \frac{(a+b)(a+b-1)+2}{a+r}$$

и $1 \leqslant h_2 \leqslant b-r$, получаем

$$\begin{aligned}\varphi'(h_2) &= -\frac{(b-r)p+2}{a+b} + h_2 - a - b + h_2 + p - 1 = \\ &= \frac{(a+r)p-2}{a+b} + 2h_2 - a - b - 1 \geqslant \frac{(a+r)p-2}{a+b} - a - b + 1 > \\ &> \frac{(a+b)(a+b-1)+2-2}{a+b} - a - b + 1 = 0.\end{aligned}$$

Очевидно, что $\varphi(h_2)$ достигает своего минимального значения в точке $h_2 = 1$. Тогда, учитывая неравенства (3) и

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r} > \frac{(a+b)(a+b+2n)+2}{a+r},$$

получаем

$$\begin{aligned}&\gamma_H(S,T) \geqslant \varphi(h_2) \geqslant \varphi(1) = \\ &= (a+b-1)\left(\frac{(b-r)p+2}{a+b} - 1\right) - (b-r-1)p - 1 - 2n = \\ &= \frac{(a+r)p-2}{a+b} - a - b - 2n + 2 > \\ &> \frac{(a+b)(a+b+2n)+2-2}{a+b} - a - b - 2n + 2 = 2 \geqslant \varepsilon(S,T),\end{aligned}$$

что противоречит (1).

Случай 3: $\rho = 0$.

Случай 3.1: $T = N_T[x_1]$.

В этом случае имеем

$$|T| = |N_T[x_1]| \leqslant d_{G-S}(x_1) + 1 = h_1 + 1 \leqslant b - r + 2. \tag{4}$$

Отметим, что $\delta(G) \leqslant d_G(x_1) \leqslant d_{G-S}(x_1) + |S| = h_1 + |S|$. Таким образом, получаем

$$|S| \geqslant \delta(G) - h_1 \geqslant \frac{(b+1)(b-r+2)-b+a}{a+r} - h_1. \tag{5}$$

Поскольку $\rho = 0$, имеем $1 \leqslant h_1 \leqslant b-r+1$. Используя (1), (4), (5) и предложение 5, получаем

$$\varepsilon(S,T) - 1 \geqslant \gamma_H(S,T) = f(S) + d_{H-S}(T) - g(T) \geqslant$$

$$
\begin{aligned}
&\geqslant f(S) + d_{G-S}(T) - \min\{2n, |T|\} - g(T) \geqslant \\
&\geqslant (a+r)|S| + h_1|T| - |T| - (b-r)|T| = (a+r)|S| - (b-r+1-h_1)|T| \geqslant \\
&\geqslant (a+r)\left(\frac{(b+1)(b-r+2)-b+a}{a+r} - h_1\right) - (b-r+1-h_1)(b-r+2) = \\
&= r(b-r+2) - b + a + (b-a-r)h_1 - rh_1 + 2h_1 \geqslant \\
&\geqslant r(b-r+2) - b + a + b - a - r - r(b-r+1) + 2 = 2 \geqslant \varepsilon(S,T),
\end{aligned}
$$

что является противоречием.

Случай 3.2: $T \neq N_T[x_1]$.

Очевидно, существует $x_2 \in T \setminus N_T[x_1]$, такое что $d_{G-S}(x_2) = h_2$. Легко видеть, что $x_1x_2 \notin E(G)$. По предположению теоремы 5 получаем неравенство

$$
\frac{(b-r)p+2}{a+b} \leqslant |N_G(x_1) \cup N_G(x_2)| \leqslant d_{G-S}(x_1) + d_{G-S}(x_2) + |S| = h_1 + h_2 + |S|,
$$

из которого вытекает оценка

$$
|S| \geqslant \frac{(b-r)p+2}{a+b} - h_1 - h_2. \tag{6}
$$

Поскольку $\rho = 0$, имеем $1 \leqslant h_1 \leqslant h_2 \leqslant b-r+1$. Заметим, что $|N_T[x_1]| \leqslant h_1 + 1$. Рассмотрим три случая возможных значений h_1 и h_2.

Случай 3.2.1: $1 \leqslant h_1 \leqslant h_2 \leqslant b-r$.

С учетом (6), предположения 5 и неравенства $|S| + |T| \leqslant p$ получаем

$$
\begin{aligned}
&\gamma_H(S,T) = f(S) + d_{H-S}(T) - g(T) \geqslant \\
&\geqslant f(S) + d_{G-S}(T) - \min\{2n, |T|\} - g(T) \geqslant \\
&\geqslant (a+r)|S| + h_1|N_T[x_1]| + h_2(|T| - |N_T[x_1]|) - 2n - (b-r)|T| = \\
&= (a+r)|S| + (h_1-h_2)|N_T[x_1]| - (b-r-h_2)|T| - 2n \geqslant \\
&\geqslant (a+r)|S| + (h_1-h_2)(h_1+1) - (b-r-h_2)(p-|S|) - 2n = \\
&= (a+b-h_2)|S| + (h_1-h_2)(h_1+1) - (b-r-h_2)p - 2n \geqslant \\
&\geqslant (a+b-h_2)\left(\frac{(b-r)p+2}{a+b} - h_1 - h_2\right) + \\
&+ (h_1-h_2)(h_1+1) - (b-r-h_2)p - 2n.
\end{aligned}
$$

Положим

$$
\begin{aligned}
&F(h_1,h_2) = (a+b-h_2)\left(\frac{(b-r)p+2}{a+b} - h_1 - h_2\right) + (h_1-h_2)(h_1+1) - \\
&- (b-r-h_2)p - 2n.
\end{aligned}
$$

Таким образом,

$$
\gamma_H(S,T) \geqslant F(h_1,h_2). \tag{7}
$$

Из неравенств

$$
p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r} > \frac{(a+b)(a+b-1)+2}{a+r}
$$

и $1 \leqslant h_2 \leqslant b-r$ следует, что

$$\frac{\partial F(h_1,h_2)}{\partial h_2} = -\frac{(b-r)p+2}{a+b} + h_1 + h_2 - a - b + h_2 - h_1 - 1 + p =$$
$$= \frac{(a+r)p-2}{a+b} - a - b + 2h_2 - 1 > \frac{(a+b)(a+b-1)+2-2}{a+b} - a - b + 1 = 0.$$

Поэтому согласно (7) получаем неравенство

$$\gamma_H(S,T) \geqslant F(h_1,h_2) \geqslant F(h_1,h_1). \tag{8}$$

С учетом того, что

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r} > \frac{2(a+b)(a+b-2)+2}{a+r}$$

и $1 \leqslant h_1 \leqslant b-r$, выполняется следующая цепочка соотношений:

$$\frac{dF(h_1,h_1)}{dh_1} = -\frac{(b-r)p+2}{a+b} + 2h_1 - 2(a+b-h_1) + p =$$
$$= \frac{(a+r)p-2}{a+b} + 4h_1 - 2(a+b) >$$
$$> \frac{2(a+b)(a+b-2)+2-2}{a+b} + 4 - 2(a+b) = 0,$$

из которой следует неравенство

$$F(h_1,h_1) \geqslant F(1,1). \tag{9}$$

Здесь мы использовали, что $1 \leqslant h_1 \leqslant b-r$. Из (8), (9) и неравенства

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r}$$

следует, что

$$\gamma_H(S,T) \geqslant F(h_1,h_1) \geqslant F(1,1) =$$
$$= (a+b-1)\left(\frac{(b-r)p+2}{a+b} - 2\right) - (b-r-1)p - 2n =$$
$$= \frac{(a+r)p-2}{a+b} - 2(a+b-2) - 2n \geqslant$$
$$\geqslant \frac{2(a+b)(a+b+n-1)+2-2}{a+b} - 2(a+b-2) - 2n = 2 \geqslant \varepsilon(S,T).$$

Получаем противоречие с (1).

Случай 3.2.2: $1 \leqslant h_1 \leqslant b-r-1$ и $h_2 = b-r+1$.

Из (6), предложений 1 и 5, а также неравенств

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r}$$

и $2 \leqslant a \leqslant b-r$ следует, что

$$\gamma_H(S,T) = f(S) + d_{H-S}(T) - g(T) \geqslant$$
$$\geqslant f(S) + d_{G-S}(T) - \min\{2n,|T|\} - g(T) \geqslant$$

$$\begin{aligned}
&\geqslant (a+r)|S| + h_1|N_T[x_1]| + h_2(|T| - |N_T[x_1]|) - 2n - (b-r)|T| =\\
&= (a+r)|S| + (h_1 - h_2)|N_T[x_1]| - (b-r-h_2)|T| - 2n \geqslant\\
&\geqslant (a+r)|S| + (h_1 - h_2)(h_1+1) + |T| - 2n \geqslant\\
&\geqslant (a+r)\left(\frac{(b-r)p+2}{a+b} - h_1 - h_2\right) + (h_1-h_2)(h_1+1) + 2 - 2n =\\
&= (a+r)\left(\frac{(b-r)p+2}{a+b} - h_1 - (b-r+1)\right) +\\
&+ (h_1 - (b-r+1))(h_1+1) + 2 - 2n =\\
&= \frac{(b-r)(a+r)p + 2(a+r)}{a+b} - h_1(a+b-h_1) - (a+r+1)(b-r+1) + 2 - 2n \geqslant\\
&\geqslant \frac{(b-r)(2(a+b)(a+b+n-1)+2) + 2(a+r)}{a+b} - (b-r-1)(a+b-1) -\\
&- (a+r+1)(b-r+1) + 2 - 2n = (b-r)(b-r+2n-1) + 2 - 2n \geqslant\\
&\geqslant 2(2n+1) + 2 - 2n > 2 \geqslant \varepsilon(S,T).
\end{aligned}$$

Полученное соотношение противоречит (1).

Случай 3.2.3: $h_1 = b - r$ и $h_2 = b - r + 1$.

Предложение 7. *Справедливо неравенство* $|T| \geqslant b + 1$.

Доказательство. Предположим, что $|T| \leqslant b$. Отметим, что $h_1 = d_{G-S}(x_1)$. Таким образом,

$$|S| + h_1 = |S| + d_{G-S}(x_1) \geqslant d_G(x_1) \geqslant \delta(G),$$

т.е.

$$|S| \geqslant \delta(G) - h_1 \geqslant \frac{(b+1)(b-r+2) - b + a}{a+r} - (b-r). \tag{10}$$

Согласно (10), предложению 5 и неравенству $2 \leqslant a \leqslant b - r$ получаем следующую цепочку соотношений:

$$\begin{aligned}
&\gamma_H(S,T) = f(S) + d_{H-S}(T) - g(T) \geqslant\\
&\geqslant (a+r)|S| + d_{G-S}(T) - |T| - (b-r)|T| \geqslant\\
&\geqslant (a+r)|S| + h_1|T| - |T| - (b-r)|T| = (a+r)|S| - |T| \geqslant\\
&\geqslant (a+r)\left(\frac{(b+1)(b-r+2) - b + a}{a+r} - (b-r)\right) - b =\\
&= (b-r)(b+1-a-r) + a + 2 > 2 \geqslant \varepsilon(S,T),
\end{aligned}$$

которая противоречит (1), что завершает доказательство предложения 7. ▲

Используя (6), предложения 5 и 7, а также соотношения

$$p \geqslant \frac{2(a+b)(a+b+n-1)+2}{a+r}$$

и $2 \leqslant a \leqslant b - r$, можно вывести, что

$$\begin{aligned}
&\gamma_H(S,T) = f(S) + d_{H-S}(T) - g(T) \geqslant\\
&\geqslant f(S) + d_{G-S}(T) - \min\{2n, |T|\} - g(T) \geqslant\\
&\geqslant (a+r)|S| + h_1|N_T[x_1]| + h_2(|T| - |N_T[x_1]|) - 2n - (b-r)|T| =\\
&= (a+r)|S| + (h_1 - h_2)|N_T[x_1]| + (h_2 - b + r)|T| - 2n \geqslant
\end{aligned}$$

$$
\begin{aligned}
&\geqslant (a+r)\left(\frac{(b-r)p+2}{a+b}-h_1-h_2\right)+(h_1-h_2)(h_1+1)+\\
&+(h_2-b+r)(b+1)-2n=\\
&=(a+r)\left(\frac{(b-r)p+2}{a+b}-2(b-r)-1\right)-(b-r+1)+b+1-2n=\\
&=\frac{(b-r)(a+r)p+2(a+r)}{a+b}-2(b-r)(a+r)-a-2n\geqslant\\
&\geqslant\frac{(b-r)(2(a+b)(a+b+n-1)+2)+2(a+r)}{a+b}-2(b-r)(a+r)-a-2n=\\
&=2(b-r)(b-r+n-1)+2-a-2n\geqslant 2a(n+1)+2-a-2n>2\geqslant\varepsilon(S,T).
\end{aligned}
$$

Полученные соотношения противоречат (1).

Случай 3.2.4: $h_1=h_2=b-r+1$.

Из предложения 5 и $\varepsilon(S,T)\leqslant|S|$ следует цепочка соотношений

$$
\begin{aligned}
&\gamma_H(S,T)=f(S)+d_{H-S}(T)-g(T)\geqslant(a+r)|S|+d_{G-S}(T)-|T|-(b-r)|T|\geqslant\\
&\geqslant(a+r)|S|+h_1|T|-|T|-(b-r)|T|=(a+r)|S|\geqslant|S|\geqslant\varepsilon(S,T),
\end{aligned}
$$

которая противоречит (1). Это завершает доказательство теоремы 5. ▲

§ 3. Замечание

Нижняя оценка на размер объединения окрестностей в теореме 5 является наилучшей из возможных в том смысле, что нельзя заменить $\frac{(b-r)p+2}{a+b}$ выражением $\frac{(b-r)p+2}{a+b}-1$. Это можно проиллюстрировать следующим примером.

Пусть a,b,r и n – целые неотрицательные числа, удовлетворяющие условию $b-r=a\geqslant 2$. Построим граф

$$G=(a(t+n)K_2)\vee(2b(t+n)K_1)$$

порядка p, где t – достаточно большое целое число. Ясно, что $p=2(a+b)(t+n)$ и

$$
\begin{aligned}
&\frac{(b-r)p+2}{a+b}-1<|N_G(u)\cup N_G(v)|=2a(t+n)=\frac{ap}{a+b}=\\
&=\frac{(b-r)p}{a+b}<\frac{(b-r)p+2}{a+b}
\end{aligned}
$$

для любых двух вершин $u,v\in V(2b(t+n)K_1)$. Очевидно также, что

$$|N_G(u)\cup N_G(v)|=2b(t+n)+2>\frac{(b-r)p+2}{a+b}-1$$

для любой пары несмежных вершин u,v графа $a(t+n)K_2$. Положим

$$
\begin{aligned}
&S=V(a(t+n)K_2),\quad T=V(2b(t+n)K_1),\\
&N=\{e_1,e_2,\dots,e_n\}\subseteq E(a(t+n)K_2),\quad H=G-N.
\end{aligned}
$$

Тогда $|S|=2a(t+n)$, $|T|=2b(t+n)$ и $\varepsilon(S,T)=2$. Пусть g,f являются целочисленными функциями с $g(x)=a$ и $f(x)=b$ для любого $x\in V(G)$. Тогда $d_{H-S}(x)=0<g(x)$ для всякого $x\in T$. Таким образом, получаем, что

$$
\begin{aligned}
&\gamma_H(S,T)=f(S)+d_{H-S}(T)-g(T)=b|S|-a|T|=\\
&=b(2a(t+n))-a(2b(t+n))=0<2=\varepsilon(S,T).
\end{aligned}
$$

С учетом теоремы 2 граф H не обладает свойством $E(1,0)$ относительно дробного (g,f)-фактора, поэтому G не обладает свойством $E(1,n)$ относительно дробного (g,f)-фактора.

Авторы благодарят рецензентов за их конструктивные замечания по улучшению качества настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Bondy J.A., Murty U.S.R.* Graph Theory. Berlin: Springer, 2008.
2. *Anstee R.P.* An Algorithmic Proof of Tutte's f-Factor Theorem // J. Algorithms. 1985. V. 6. № 1. P. 112–131.
3. *Liu G., Zhang L.* Fractional (g,f)-Factors of Graphs // Acta Math. Sci. Ser. B (Engl. Ed.). 2001. V. 21. № 4. P. 541–545.
4. *Li Z., Yan G., Zhang X.* On Fractional (g,f)-Covered Graphs // OR Trans. (in Chinese). 2002. V. 6. № 4. P. 65–68.
5. *Iida T., Nishimura T.* Neighborhood Conditions and k-Factors // Tokyo J. Math. 1997. V. 20. № 2. P. 411–418.
6. *Zhou S., Liu H.* Neighborhood Conditions and Fractional k-Factors // Bull. Malays. Math. Sci. Soc. (2). 2009. V. 32. № 1. P. 37–45.
7. *Liu H., Lu H.* A Degree Condition for a Graph to Have (a,b)-Parity Factors // Discrete Math. 2018. V. 341. № 1. P. 244–252.
8. *Plummer M.D.* Graph Factors and Factorization: 1985–2003: A Survey // Discrete Math. 2007. V. 307. № 7–8. P. 791–821.
9. *Zhou S.* Remarks on Orthogonal Factorizations of Digraphs // Int. J. Comput. Math. 2014. V. 91. № 10. P. 2109–2117.
10. *Zhou S.* Some Results about Component Factors in Graphs // RAIRO Oper. Res. 2019. V. 53. № 3. P. 723–730.
11. *Zhou S., Sun Z.* Binding Number Conditions for $P_{\geqslant 2}$-Factor and $P_{\geqslant 3}$-Factor Uniform Graphs // Discrete Math. 2020. V. 343. № 3. Article 111715 (6 pp.).
12. *Zhou S.Z., Sun Z.R.* Some Existence Theorems on Path Factors with Given Properties in Graphs // Acta Math. Sin. (Engl. Ser.). 2020. V. 36. № 8. P. 917–928.
13. *Zhou S., Sun Z., Liu H.* Sun Toughness and $P_{\geqslant 3}$-Factors in Graphs // Contrib. Discrete Math. 2019. V. 14. № 1. P. 167–174.
14. *Sun Z., Zhou S.* A Generalization of Orthogonal Factorizations in Digraphs // Inform. Process. Lett. 2018. V. 132. P. 49–54.
15. *Zhou S., Zhang T., Xu Z.* Subgraphs with Orthogonal Factorizations in Graphs // Discrete Appl. Math. 2020. V. 286. P. 29–34.
16. *Zhou S.* Remarks on Path Factors in Graphs // RAIRO Oper. Res. 2020. V. 54. № 6. P. 1827–1834.
17. *Zhou S., Yang F., Xu L.* Two Sufficient Conditions for the Existence of Path Factors in Graphs // Sci. Iran. D: Comput. Sci. Eng. Electr. Eng. 2019. V. 26. № 6. P. 3510–3514.
18. *Cai J., Wang X., Yan G.* A Note on the Existence of Fractional f-Factors in Random Graphs // Acta Math. Appl. Sin. Engl. Ser. 2014. V. 30. № 3. P. 677–680.
19. *Gao W., Guirao J.L.G., Wu H.* Two Tight Independent Set Conditions for Fractional (g,f,m)-Deleted Graphs Systems // Qual. Theory Dyn. Syst. 2018. V. 17. № 1. P. 231–243.
20. *Gao W., Guirao J.L.G., Chen Y.J.* A Toughness Condition for Fractional (k,m)-Deleted Graphs Revisited // Acta Math. Sin. (Engl. Ser.). 2019. V. 35. № 7. P. 1227–1237.
21. *Gao W., Wang W., Dimitrov D.* Toughness Condition for a Graph to Be All Fractional (g,f,n)-Critical Deleted // Filomat. 2019. V. 33. № 9. P. 2735–2746.
22. *Lv X.* A Degree Condition for Fractional (g,f,n)-Critical Covered Graphs // AIMS Math. 2020. V. 5. № 2. P. 872–878.
23. *Wu J., Yuan J., Siddiqui M.K.* Independent Set Conditions for All Fractional (g,f,n',m)-Critical Deleted NFV Networks // J. Intell. Fuzzy Syst. 2018. V. 35. № 4. P. 4495–4502.

24. *Yuan Y., Hao R.-X.* A Degree Condition for Fractional $[a, b]$-Covered Graphs // Inform. Process. Lett. 2019. V. 143. P. 20–23.
25. *Yuan Y., Hao R.-X.* Toughness Condition for the Existence of All Fractional (a, b, k)-Critical Graphs // Discrete Math. 2019. V. 342. № 8. P. 2308–2314.
26. *Zhou S., Sun Z., Ye H.* A Toughness Condition for Fractional (k, m)-Deleted Graphs // Inform. Process. Lett. 2013. V. 113. № 8. P. 255–259.
27. *Zhou S., Liu H., Xu Y.* Binding Numbers for Fractional (a, b, k)-Critical Covered Graphs // Proc. Rom. Acad. Ser. A Math. Phys. Tech. Sci. Inf. Sci. 2020. V. 21. № 2. P. 115–121.
28. *Zhou S., Xu L., Xu Z.* Remarks on Fractional ID-k-Factor-Critical Graphs // Acta Math. Appl. Sin. Engl. Ser. 2019. V. 35. № 2. P. 458–464.
29. *Zhou S., Xu Y., Sun Z.* Degree Conditions for Fractional (a, b, k)-Critical Covered Graphs // Inform. Process. Lett. 2019. V. 152. Article 105838 (5 pp.).

Чжоу Сычжун
Школа естественных наук,
Научно-технологический университет Цзянсу,
Чжэньцзян, провинция Цзянсу, КНР
`zsz_cumt@163.com`
Сунь Чжижэнь
Школа математических наук,
Нанкинский нормальный университет, Нанкин, КНР
Пань Цюаньэжу
Школа естественных наук,
Научно-технологический университет Цзянсу,
Чжэньцзян, провинция Цзянсу, КНР

Поступила в редакцию
21.02.2020
После доработки
30.05.2020
Принята к публикации
02.06.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.176

© 2020 г. **П.А. Огарок, А.М. Райгородский**

ОБ УСТОЙЧИВОСТИ ЧИСЛА НЕЗАВИСИМОСТИ НЕКОТОРОГО ДИСТАНЦИОННОГО ГРАФА[1]

Изучается асимптотическое поведение числа независимости случайного подграфа определенного (r, s)-дистанционного графа. Представлены верхние и нижние оценки критической вероятности сохранения ребра, при которой происходит фазовый переход и в подграфе появляются большие новые независимые множества, которых в исходном графе не было.

Ключевые слова: случайный граф, дистанционный граф, число независимости.

DOI: `10.31857/S0555292320040051`

§ 1. Введение, определения и формулировка основного результата

Рассмотрим множество $[n] := \{1, 2, \ldots, n\}$ и натуральные числа r и s, $n > r > s$. Построим граф $G(n, r, s)$ следующим образом: его вершинами будут все r-элементные подмножества множества $[n]$, а ребро соединяет две вершины, мощность пересечения которых (как подмножеств) равна s.

Данное определение можно переформулировать и в линейно-алгебраических терминах. А именно, вершинами графа будут всевозможные векторы длины n из нулей и единиц, скалярный квадрат которых равен r, а ребро будет соединять две вершины, если скалярное произведение соответствующих векторов равно s.

Кроме того, вершины этого графа можно воспринимать как вершины n-мерного гиперкуба, и тогда ребра будут проводиться между вершинами на расстоянии ровно $\sqrt{2(r-s)}$. Поэтому графы $G(n, r, s)$ часто называются *дистанционными графами*.

Дистанционные графы естественным образом возникают в различных задачах дискретной математики: в задаче о раскраске метрического пространства (Нелсона – Эрдеша – Хадвигера, см. [1–4]), проблеме Борсука (см. [5–9]), задачах о числах Рамсея (см. [10, 11]), о кодах с одним запрещенным расстоянием (см. [12]) и о пересекающихся семействах множеств (см. [13–20]).

Частным случаем дистанционного графа является *кнезеровский* граф $K(n, r)$ – это граф $G(n, r, 0)$. Кнезеровские графы изучались, например, в работах [21–27].

Важным направлением исследования дистанционных графов является изучение поведения их числа независимости. *Число независимости* графа G, обыкновенно обозначаемое через $\alpha(G)$, – наибольшая мощность его *независимого множества*, т.е. такого подмножества его вершин, что никакие две вершины в нем не соединены ребром. Числа независимости дистанционных графов исследовались, например, в [28–30].

В данной статье будет исследоваться несколько другой тип случайных графов. Здесь этот граф будет обозначаться через $\widetilde{G}(n, r, s)$. Его вершинами являются те

---

[1] Работа выполнена за счет гранта Российского научного фонда (проект № 16-11-10014).

же самые r-элементные подмножества множества $[n]$, но ребра соединяют те пары вершин, мощность пересечения которых (как подмножеств) строго меньше s (а не равна, как в классическом дистанционном графе). Заметим, что кнезеровский граф $K(n,r)$ также является графом $\widetilde{G}(n,r,1)$.

Пусть множество $X \subset [n]$ состоит из s элементов. Рассмотрим семейство всех подмножеств множества $[n]$, состоящих из r элементов и содержащих X. Это семейство, мощность которого равна $\binom{n-s}{r-s}$, является независимым множеством вершин графа $\widetilde{G}(n,r,s)$. Мы будем называть это семейство *звездой* с центром в X, а само множество X – *базой* этой звезды. Отметим, что данное определение работает не только для графа $\widetilde{G}(n,r,s)$ – оно дано в теоретико-множественных терминах.

На языке графов $\widetilde{G}(n,r,s)$ очень удобно сформулировать известную теорему, которая отвечает на вопрос об асимптотическом поведении их числа независимости.

Теорема 1 (теорема Франкла). *Для заданных натуральных чисел r и s, $s < r$, существует такое $n_0 = n_0(r,s)$, что для всех $n \geqslant n_0$ все независимые множества в графе $\widetilde{G}(n,r,s)$ являются звездами или имеют мощность, по порядку величины меньшую $\binom{n-s}{r-s}$.*

Теперь определим *последовательность случайных подграфов*, построенную по последовательности графов. Пусть задана последовательность графов $G(n)$, где число вершин n-го элемента последовательности растет с ростом n, и функция *вероятности сохранения ребра $p = p(n)$*. Сохраним в каждом графе последовательности $G(n)$ каждое ребро независимо с вероятностью $p(n)$. Полученная таким образом последовательность случайных подграфов обозначается через $G_p(n)$.

Рассмотрим последовательность случайных подграфов, построенную по последовательности дистанционных графов. Как ведет себя число независимости случайного подграфа в последовательности в сравнении с числом независимости графа в исходной последовательности? В работе [31] был получен достаточно полный ответ на такой вопрос для кнезеровских графов. Более точно, была установлена истинность следующего утверждения.

Теорема 2. *Пусть $r = r(n) = o(n^{\frac{1}{3}})$, $r > 2$. Пусть также фиксировано $\varepsilon > 0$. Обозначим*

$$p_c(n,r) := \frac{(r+1)\ln n - r\ln r}{\binom{n-1}{r-1}}.$$

Тогда:

(i) *При вероятности сохранения ребра*

$$p \geqslant (1+\varepsilon)p_c(n,r)$$

в графе $K_p(n,r)$ асимптотически почти наверное (с ростом n) мощность независимого множества максимального размера равна $\binom{n-1}{r-1}$, и все такие независимые множества в нем суть звезды.

(ii) *При вероятности сохранения ребра*

$$p \leqslant (1-\varepsilon)p_c(n,r)$$

в графе $K_p(n,r)$ асимптотически почти наверное (с ростом n) мощность независимого множества максимального размера не меньше $\binom{n-1}{r-1} + 1$.

Эта теорема означает, что $p_c(n,r)$ – точная критическая вероятность сохранения ребра: если вероятность сохранения ребра в случайном подграфе кнезеровского графа больше нее, то число независимости этого подграфа совпадает с числом независимости исходного графа (и даже новых независимых множеств в подграфе не появляется), а если меньше, то оно резко растет.

Аналогичные вопросы рассматривались в работах [32–36].

Цель данной статьи – попробовать найти подобную критическую вероятность для графа $\widetilde{G}_p(n,r,s)$ (с произвольным s). Более конкретно, в статье доказаны оценки этой вероятности сверху и снизу.

Сформулируем основной результат.

Теорема 3. *Справедливы следующие утверждения*:

(i) *Для любых констант r и s, таких что $r>s$ и $r>3$, при вероятности сохранения ребра*

$$p=p_1(n)=\frac{2s\binom{r}{s}\ln n}{\binom{n-s}{r-s}}$$

в графе $\widetilde{G}_p(n,r,s)$ асимптотически почти наверное (с ростом n) мощность независимого множества максимального размера равна $\binom{n-s}{r-s}$, и все такие независимые множества в нем суть звезды.

(ii) *Для любого $\varepsilon>0$ и для любых констант r и s, таких что $r>s$, при вероятности сохранения ребра*

$$p=p_2(n)=\frac{(1-\varepsilon)(r+s)\ln n}{\binom{n-s}{r-s}}$$

в графе $\widetilde{G}_p(n,r,s)$ асимптотически почти наверное (с ростом n) мощность независимого множества максимального размера не меньше $\binom{n-s}{r-s}+1$.

Дальнейшая часть статьи устроена так. В § 2 вводятся обозначения и формулируются известные результаты, которые будут использоваться в доказательстве. В § 3 доказывается первая часть теоремы 3, а в § 4 – ее вторая часть. Доказательство построено по аналогии с работой [31]. Наконец, в § 5 приведены неформальные замечания, касающиеся предмета статьи.

§ 2. Обозначения и базовые теоремы

Во-первых, приведем известные оценки биномиальных коэффициентов и экспоненты, которые пригодятся в дальнейшем:

1. Для натуральных n и r, таких что $n>r$, верно

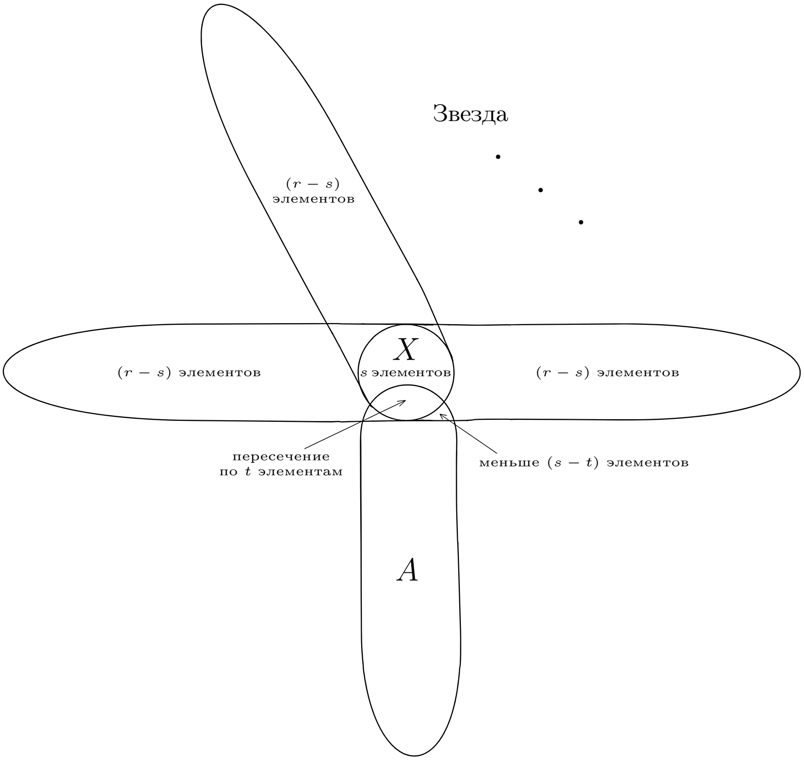
$$\left(\frac{n}{r}\right)^r\leqslant\binom{n}{r}\leqslant\frac{n^r}{r!}\leqslant\left(\frac{en}{r}\right)^r.$$

2. Для вещественного x, такого что $|x|\leqslant\frac{1}{2}$, верно

$$e^{x-x^2}\leqslant 1+x\leqslant e^x.$$

В дальнейшем для краткости записи будем обозначать число вершин графа $\widetilde{G}(n,r,s)$ через

$$V:=\binom{n}{r},$$



а число вершин максимальной звезды – через

$$N := \binom{n-s}{r-s}.$$

Заметим, что

$$V \sim \frac{n^r}{r!}$$

и

$$N \sim \frac{n^{r-s}}{(r-s)!}.$$

Пусть задана звезда S_X с базой $X \subset \{1, 2, \ldots, n\}$, а также вершина A графа $\widetilde{G}(n, r, s)$, пересекающая множество X по t, $t < s$, элементам (см. рисунок). Подсчитаем число вершин звезды S_X, соединенных с вершиной A ребром. Это число мы обозначим через M_t.

Вершина A соединена ребром с теми вершинами звезды S_X, с которыми она пересекается меньше чем по s элементам. Для того чтобы получить все вершины звезды, с которыми она соединена ребром, надо добавить к множеству X еще $r - s$ элементов так, чтобы пересечение этой добавки с множеством $A \backslash X$ имело мощность строго меньше $s - t$ (в нижеследующей формуле его мощность обозначена через u). Значит,

$$M_t = \sum_{u=0}^{s-t-1} \binom{r-t}{u} \binom{n-r-s+t}{r-s-u}.$$

Пользуясь вышеприведенными оценками на биномиальные коэффициенты, можно записать

$$M_t \sim \sum_{u=0}^{s-t-1} \frac{(r-t)^u}{u!} \frac{(n-r-s+t)^{r-s-u}}{(r-s-u)!}.$$

В этой сумме главным является первое слагаемое (при $u = 0$), равное

$$\frac{(n-r-s+t)^{r-s}}{(r-s)!} \sim \frac{n^{r-s}}{(r-s)!} \sim N.$$

В прочих слагаемых n возводится в меньшую степень, поэтому для всякого t имеем

$$M_t \sim N.$$

Наконец, приведем полезное определение, которое будет использоваться в дальнейшем. Пусть задано некоторое семейство D вершин графа $\widetilde{G}(n, r, s)$. Будем называть *степенью* семейства D максимальную (по всем звездам) мощность пересечения D со звездой.

§ 3. Верхняя оценка критической вероятности сохранения ребра

Пусть даны натуральные числа r и s, такие что $r > s$, и пусть

$$p = p(n) = \frac{2s\binom{r}{s}\ln n}{\binom{n-s}{r-s}}.$$

Докажем, что при этих условиях с вероятностью, стремящейся к 1, мощность независимого множества максимального размера в графе $\widetilde{G}_p(n, r, s)$ равна N, и все такие независимые множества суть звезды.

Для этого определим на графе $\widetilde{G}_p(n, r, s)$ случайные величины X_i, $i \in \mathbb{N}$, и Y так, что из их одновременного равенства нулю следует желаемое, и докажем, что они действительно одновременно равны нулю с вероятностью, стремящейся к 1.

А именно, пусть для каждого натурального i случайная величина X_i равна числу независимых множеств мощности N вершин графа $\widetilde{G}_p(n, r, s)$, степень которых равна $N - i$. Пусть также случайная величина Y равна числу независимых множеств мощности $N + 1$ вершин графа $\widetilde{G}_p(n, r, s)$, степень которых равна N. Можно заметить, что Y – это попросту число независимых множеств мощности $N + 1$, содержащих целую звезду. Если все X_i равны 0, то всякое независимое множество в графе $\widetilde{G}_p(n, r, s)$ мощности хотя бы N содержит целую звезду, а если вдобавок $Y = 0$, то независимых множеств мощности больше N в графе нет.

Итак, нам надо доказать, что с вероятностью, стремящейся к 1, одновременно все X_i и Y равны нулю. В нижеследующих пунктах мы по очереди с ними разберемся.

3.1. Доказательство того, что $\boldsymbol{Y = 0}$. Для доказательства того, что асимптотически почти наверное $Y = 0$, мы убедимся в том, что математическое ожидание $\mathbf{E}(Y)$ стремится к 0 при $n \to \infty$, и воспользуемся неравенством Маркова: $\mathbf{P}(Y > 0) \leqslant \mathbf{E}(Y)$, т.е. $\mathbf{P}(Y > 0) \to 0$ при $n \to \infty$, что и требуется.

Вычислим $\mathbf{E}(Y)$. Для того чтобы получить независимое множество мощности $N + 1$, содержащее целую звезду, надо выбрать базу этой звезды (обозначим ее через X, она имеет мощность s), построить по этой базе звезду и добавить еще одну вершину A, которая в графе $\widetilde{G}_p(n, r, s)$ не соединена ни с одной из вершин звезды.

Базу мы выбираем $\binom{n}{s}$ способами, новую вершину – $(V-N)$ способами. Если последняя пересекает базу по $t<s$ элементам, то в графе $\widetilde{G}(n,r,s)$ она соединена в точности с M_t вершинами звезды. Все эти ребра должны быть удалены в графе $\widetilde{G}_p(n,r,s)$. Значит, поскольку $M_t=(1+o(1))N$ для любого $t<s$, то

$$\mathbf{E}(Y)=\binom{n}{s}(V-N)(1-p)^{(1+o(1))N}.$$

Согласно ранее приведенным оценкам

$$\mathbf{E}(Y)\leqslant\left(\frac{en}{s}\right)^s\left(\frac{en}{r}\right)^r e^{-(1+o(1))pN}\leqslant$$

$$\leqslant e^{(r+s)(1+\ln n)-s\ln s-r\ln r-2(1+o(1))s\binom{r}{s}\ln n}=O\Big(n^{(r+s)-2(1+o(1))s\binom{r}{s}}\Big)=o(1).$$

Итак, $\mathbf{E}(Y)\to 0$ при $n\to\infty$, что и требовалось.

3.2. Доказательство того, что $X_i=0$. Для доказательства того, что асимптотически почти наверное все $X_i=0$, рассмотрим три случая: очень маленькое i, маленькое i и большое i.

Случай 1: очень маленькое i. Выберем малое положительное ε (например, можно считать, что $\varepsilon=1/10$). Оно будет использоваться в этом и следующем случаях.

Пусть $i\leqslant\varepsilon N$. Оценим сверху вероятность того, что какая-то из случайных величин X_i больше 0, суммой вероятностей

$$\sum_{i=1}^{\varepsilon N}\mathbf{P}(X_i>0).$$

Оценим каждое слагаемое в этой сумме членом убывающей геометрической прогрессии, а затем оценим всю прогрессию удвоенным первым членом.

Зафиксируем i и оценим $\mathbf{P}(X_i>0)$. В данном диапазоне значений i простая оценка этой вероятности по неравенству Маркова через математическое ожидание X_i не приводит к успеху, поэтому воспользуемся более сложной техникой. А именно, для всякого $j\geqslant i$ введем на графе $\widetilde{G}_p(n,r,s)$ случайную величину $X_{i,j}$, равную числу максимальных (к которым нельзя добавить никакую вершину) независимых множеств вершин мощности $N-i+j$, степень которых равна $N-i$. Теперь же воспользуемся неравенством Маркова и получим оценку

$$\mathbf{P}(X_i>0)\leqslant\sum_{j\geqslant i}\mathbf{E}(X_{i,j}).$$

Каждое слагаемое в этой сумме мы также оценим членом убывающей геометрической прогрессии, а затем оценим всю прогрессию удвоенным первым членом.

Оценим $\mathbf{E}(X_{i,j})$. Напомним, что мы хотим получить максимальное независимое множество вершин мощности $N-i+j$, степень которого равна $N-i$. Для этого нужно выбрать базу X той звезды S_X, с которой будет достигаться пересечение по $N-i$ вершинам, затем те i вершин этой звезды S_X, которые не войдут в наше множество, и наконец, те j вершин не из S_X, которые войдут в наше множество. Обозначим первое из этих семейств через A_1, а второе – через A_2. При этом также необходимо, чтобы всякая вершина из A_1 была соединена в графе $\widetilde{G}_p(n,r,s)$ хотя бы с одной вершиной из A_2, а ребер между вершинами из $S_X\setminus A_1$ и вершинами из A_2 в этом графе не было, потому что иначе построенное множество будет не независимым или не максимальным независимым.

Пусть задана вершина не из звезды S_X, которая (как множество) пересекает базу X этой звезды по $t < s$ элементам. Тогда эта вершина соединена ровно с M_t вершинами звезды S_X. Значит, число ребер в графе $\widetilde{G}(n,r,s)$, ведущих из множества A_2 в множество $S_X \setminus A_1$, не меньше $j(M_t - i)$ для некоторого t, которое является максимальной мощностью пересечения вершины из A_2 и базы X звезды S_X. В графе $\widetilde{G}(n,r,s)$ вершина из A_1 имеет не более j соседей в A_2, т.е. вероятность того, что в графе $\widetilde{G}_p(n,r,s)$ у этой вершины остался там сосед, не превосходит jp.

Объединяя вышесказанное и пользуясь тем, что $M_t = (1+o(1))N$ для всех $t < s$, получаем оценку

$$\mathbf{E}(X_{i,j}) \leqslant \binom{n}{s}\binom{N}{i}\binom{V-N}{j}(1-p)^{j((1+o(1))N-i)}(jp)^i.$$

Для того чтобы оценить эту величину членом убывающей геометрической прогрессии, оценим сверху отношение верхних оценок для $\mathbf{E}(X_{i,j+1})$ и $\mathbf{E}(X_{i,j})$. Оно не больше

$$\frac{V-N-j}{j+1}(1-p)^{(1+o(1))N-i}\Bigl(1+\frac{1}{j}\Bigr)^i.$$

При $i \leqslant \varepsilon N$ и $j \geqslant i$ эта величина не превосходит

$$Ve^{-p((1+o(1))N-i)}e \leqslant e\left(\frac{en}{r}\right)^r e^{-(1-\varepsilon)(1+o(1))Np} =$$
$$= e\left(\frac{en}{r}\right)^r e^{-2(1+o(1))(1-\varepsilon)s\binom{r}{s}\ln n} = O\Bigl(n^r n^{-2(1+o(1))(1-\varepsilon)s\binom{r}{s}}\Bigr) = o(1).$$

Итак, при достаточно больших n действительно можно оценить

$$\mathbf{P}(X_i > 0) \leqslant \sum_{j \geqslant i}\mathbf{E}(X_{i,j}) \leqslant 2\,\mathbf{E}(X_{i,i}) \leqslant$$
$$\leqslant 2\binom{n}{s}\binom{N}{i}\binom{V-N}{i}(1-p)^{i((1+o(1))N-i)}(ip)^i \leqslant$$
$$\leqslant 2\left(\frac{en}{s}\right)^s\left(\frac{eN}{i}\right)^i\left(\frac{e(V-N)}{i}\right)^i e^{-pi((1+o(1))N-i)}\left(\frac{2is\binom{r}{s}\ln n}{N}\right)^i.$$

Сокращая все лишнее, получаем, что эта величина равна

$$2\left(\frac{en}{s}\right)^s e^{2i}\left(2s\binom{r}{s}\ln n\right)^i\left(\frac{V-N}{i}\right)^i e^{-pi((1+o(1))N-i)}.$$

Подставим $p = \frac{2s\binom{r}{s}\ln n}{N}$ и оценим $i \leqslant \varepsilon N$:

$$e^{-pi((1+o(1))N-i)} = n^{-2is\binom{r}{s}\frac{((1+o(1))N-i)}{N}} \leqslant n^{-2is\binom{r}{s}((1+o(1))-\varepsilon)} \leqslant n^{-(1+o(1))is\binom{r}{s}}.$$

Значит,

$$\mathbf{P}(X_i > 0) \leqslant 2\left(\frac{en}{s}\right)^s e^{2i}\left(2s\binom{r}{s}\ln n\right)^i\left(\frac{V-N}{i}\right)^i n^{-i(1+o(1))s\binom{r}{s}} \leqslant$$
$$\leqslant 2\left(\frac{en}{s}\right)^s e^{2i}\left(2s\binom{r}{s}\ln n\right)^i V^i n^{-i(1+o(1))s\binom{r}{s}} \leqslant$$

$$\leqslant 2\left(\frac{en}{s}\right)^s \left(2e^2 s\binom{r}{s}\ln n\left(\frac{en}{r}\right)^r n^{-(1+o(1))s\binom{r}{s}}\right)^i \leqslant$$

$$\leqslant 2\left(2n^s e^{2+r+s} s\binom{r}{s}\ln n\, n^r n^{-(1+o(1))s\binom{r}{s}}\right)^i =$$

$$= 2\left(2e^{2+r+s} s\binom{r}{s}\ln n\, n^{r+s-(1+o(1))s\binom{r}{s}}\right)^i = o(1).$$

Следовательно, снова при достаточно больших n получаем оценку

$$\sum_{i=1}^{\varepsilon N}\mathbf{P}(X_i > 0) \leqslant 2\left(2e^{2+r+s} s\binom{r}{s}\ln n\, n^{r+s-(1+o(1))s\binom{r}{s}}\right)^i \leqslant$$

$$\leqslant 8\left(2e^{2+r+s} s\binom{r}{s}\ln n\, n^{r+s-(1+o(1))s\binom{r}{s}}\right) = o(1).$$

Значит, с вероятностью, стремящейся к 1, все X_i при $1 \leqslant i \leqslant \varepsilon N$ равны 0.

Случай 2: маленькое *i*. Пусть $\varepsilon N \leqslant i \leqslant N\left(1 - \frac{2}{3\binom{r}{s}}\right)$ (ε определено в предыдущем случае).

Вероятность того, что какое-то из X_i больше 0, оценим сверху суммой вероятностей

$$\sum_{i=\varepsilon N}^{N\left(1-\frac{2}{3\binom{r}{s}}\right)} \mathbf{P}(X_i > 0).$$

Оценим единообразно каждое слагаемое в этой сумме и воспользуемся тем, что всего слагаемых не более N.

Зафиксируем i и оценим $\mathbf{P}(X_i > 0)$. Для этого воспользуемся неравенством Маркова и оценим $\mathbf{P}(X_i > 0) \leqslant \mathbf{E}(X_i)$. Напомним, что мы хотим получить максимальное независимое множество вершин мощности N, степень которого равна $N - i$. Для этого нужно выбрать базу X той звезды S_X, с которой будет достигаться пересечение по $N - i$ вершинам, а затем те i вершин этой звезды S_X, которые не войдут в наше множество. Обозначим это семейство через A.

Пусть задана вершина из семейства A, которая (как множество) пересекает базу X этой звезды по $t < s$ элементам. Тогда эта вершина соединена ровно с M_t вершинами звезды S_X. Значит, она будет соединена не менее чем с $(N - i) - (N - M_t)$ вершинами из семейства A. Согласно ранее приведенным оценкам $M_t = (1 + o(1))N$ для любого t. Значит, количество ребер графа $\widetilde{G}(n, r, s)$ внутри семейства A не меньше $(1 + o(1))(N - i)i$. Значит,

$$\mathbf{E}(X_i) \leqslant \binom{n}{s}\binom{N}{i}\binom{V-N}{i}(1-p)^{(1+o(1))(N-i)i} \leqslant$$

$$\leqslant \binom{n}{s}\left(\frac{eN}{i}\right)^i\left(\frac{eV}{i}\right)^i e^{-(1+o(1))p(N-i)i}.$$

Собирая все вместе, получаем, что эта величина равна

$$\binom{n}{s}\left(\frac{e^2 VN}{i^2}e^{-(1+o(1))p(N-i)}\right)^i.$$

Подставим $p = \frac{2s\binom{r}{s}\ln n}{N}$ и оценим $N - i \geqslant \frac{2}{3\binom{r}{s}}N$:

$$\mathbf{E}(X_i) \leqslant \binom{n}{s}\left(\frac{e^2VN}{i^2}\left(n^{-2(1+o(1))s\binom{r}{s}}\right)^{\frac{2}{3\binom{r}{s}}}\right)^i.$$

Заметим, что $V = N\frac{n(n-1)\dots(n-s+1)}{r(r-1)\dots(r-s+1)}$, т.е. что $V \leqslant N\frac{n^s}{(r-s)^s}$. Значит,

$$\mathbf{E}(X_i) \leqslant \binom{n}{s}\left(\frac{e^2N^2}{i^2}\frac{n^s}{(r-s)^s}\left(n^{-2(1+o(1))s\binom{r}{s}}\right)^{\frac{2}{3\binom{r}{s}}}\right)^i.$$

Теперь оценим $i \geqslant \varepsilon N$ и получим, что

$$\mathbf{E}(X_i) = O\left(\binom{n}{s}\left(n^{s-2(1+o(1))s\binom{r}{s}\frac{2}{3\binom{r}{s}}}\right)^{\varepsilon N}\right) = O\left(\binom{n}{s}n^{-(1+o(1))\frac{s}{3}\varepsilon N}\right) =$$
$$= O\left(n^{s-(1+o(1))\frac{s}{3}\varepsilon N}\right) = o(1).$$

Грубо оценим количество членов в сумме через N, и при достаточно больших n получим оценку

$$\sum_{i=\varepsilon N}^{N\left(1-\frac{2}{3\binom{r}{s}}\right)} \mathbf{P}(X_i > 0) = O\left(Nn^{s-(1+o(1))\frac{\varepsilon}{3}N}\right) = o(1).$$

Значит, с вероятностью, стремящейся к 1, все X_i при $\varepsilon N \leqslant i \leqslant N\left(1 - \frac{2}{3\binom{r}{s}}\right)$ равны 0.

Случай 3: большое *i*. Пусть $i > N\left(1 - \frac{2}{3\binom{r}{s}}\right)$. Вероятность того, что какое-то из X_i больше 0, оценим сверху суммой вероятностей

$$\sum_{i>N\left(1-\frac{2}{3\binom{r}{s}}\right)} \mathbf{P}(X_i > 0).$$

Каждое слагаемое в этой сумме оценим по неравенству Маркова и докажем, что

$$\sum_{i>N\left(1-\frac{2}{3\binom{r}{s}}\right)} \mathbf{E}(X_i) = o(1).$$

Рассмотрим множество A вершин графа $\widetilde{G}(n, r, s)$ мощности N и степени d. В подграфе, индуцированном этим множеством, минимальная степень вершины не меньше $N - \binom{r}{s}d$.

Для оценки математического ожидания $\mathbf{E}(X_i)$ нам нужны те множества A, для которых $d = N - i \leqslant \left(\frac{2}{3\binom{r}{s}}\right)N$. Число ребер внутри таких множеств A не меньше

$$\frac{N}{2}\left(N - \binom{r}{s}\left(\frac{2}{3\binom{r}{s}}\right)N\right) = \frac{N^2}{6}.$$

Значит,

$$\sum_{i>N\left(1-\frac{2}{3\binom{r}{s}}\right)} \mathbf{E}(X_i) \leqslant \binom{V}{N}(1-p)^{\frac{N^2}{6}} \leqslant \left(\frac{eV}{N}\right)^N n^{-(1+o(1))s\binom{r}{s}\frac{N}{3}}.$$

Оценивая $V \leqslant \frac{n^s}{(r-s)^s}N$, получаем, что

$$\sum_{i>N\left(1-\frac{2}{3\binom{r}{s}}\right)} \mathbf{E}(X_i) = O\left(n^{sN} n^{-\frac{\binom{r}{s}}{3}sN}\right) = o(1)$$

при $r > 3$.

Значит, при $r > 3$ с вероятностью, стремящейся к 1, все X_i при $i > N\left(1 - \frac{2}{3\binom{r}{s}}\right)$ равны 0.

§ 4. Нижняя оценка критической вероятности сохранения ребра

Пусть снова Y – количество независимых множеств вершин графа $\widetilde{G}_p(n,r,s)$ мощности $N+1$, содержащих целую звезду. Пусть вероятность сохранения ребра равна

$$p = p(n) = \frac{(1-\varepsilon)(r+s)\ln n}{\binom{n-s}{r-s}},$$

где для удобства доказательства $\frac{1}{2} > \varepsilon > 0$.

Покажем, что $Y > 0$ с вероятностью, стремящейся к 1, т.е. число независимости графа $\widetilde{G}_p(n,r,s)$ не меньше $N+1$.

Как было показано ранее,

$$\mathbf{E}(Y) = \binom{n}{s}(V-N)(1-p)^{(1+o(1))N}.$$

Заметим, что

$$V - N = \left(\frac{n(n-1)\dots(n-s+1)}{r(r-1)\dots(r-s+1)} - 1\right)N \geqslant \left(\frac{(n-s+1)^s}{r^s} - 1\right)N =$$
$$= \Omega\left(n^s \cdot N\right) = \Omega\left(n^r\right).$$

Отсюда следует, что

$$\mathbf{E}(Y) = \Omega\left(n^s n^r (1-p)^{(1+o(1))N}\right) = \Omega\left(n^{r+s} e^{(-p-p^2)(1+o(1))N}\right) =$$
$$= \Omega\left(n^{r+s} n^{-(1-\varepsilon)(1+o(1))(r+s)}\right) = \Omega\left(n^{(1+o(1))(r+s)\varepsilon}\right) \to \infty$$

при $n \to \infty$.

Заметим, что

$$\mathbf{P}(Y=0) = \mathbf{P}(Y \leqslant 0) = \mathbf{P}(Y - \mathbf{E}(Y) \leqslant -\mathbf{E}(Y)) \leqslant \mathbf{P}(|Y - \mathbf{E}(Y)| \leqslant \mathbf{E}(Y)).$$

Таким образом, согласно неравенству Чебышева

$$\mathbf{P}(Y \leqslant 0) \leqslant \frac{\mathbf{D}(Y)}{(\mathbf{E}(Y))^2}.$$

Значит, для доказательства того, что $Y > 0$ с вероятностью, стремящейся к 1, осталось показать, что $\mathbf{D}(Y) = o((\mathbf{E}(Y))^2)$, т.е. что $\mathbf{E}(Y(Y-1)) = (1+o(1))(\mathbf{E}(Y))^2$.

Для доказательства воспользуемся стандартной техникой подсчета второго момента. Пусть индекс i пробегает все семейства мощности $N+1$ вершин графа $\widetilde{G}_p(n,r,s)$. Пусть случайная величина I_i является индикатором того, что соответствующее семейство содержит целую звезду. Тогда

$$Y = \sum_i I_i.$$

В силу линейности математического ожидания и свойств индикаторов имеем

$$\mathbf{E}(Y(Y-1)) = \sum_{i \neq j} \mathbf{E}(I_i I_j) = \sum_{P,Q,A,B} \mathbf{P}(S_P \cup \{A\} \text{ и } S_Q \cup \{B\} \text{ независимы}).$$

Здесь суммирование ведется по всем четверкам (P, Q, A, B), где P и Q – подмножества мощности s множества $[n]$, S_P и S_Q – построенные на них звезды, A и B – подмножества мощности r множества $[n]$, пересекающие, соответственно, P и Q меньше чем по s элементам, и $(P, A) \neq (Q, B)$. Действительно, для того чтобы выбрать семейство вершин мощности $N+1$, содержащее целую звезду, надо выбрать саму эту звезду и еще одну вершину, не соединенную ни с одной вершиной звезды, – ровно это и записано в соответствующей сумме.

Теперь заметим, что данная сумма состоит из двух сумм:

$$\sum_{P \neq Q} \mathbf{P}(S_P \cup \{A\} \text{ и } S_Q \cup \{B\} \text{ независимы}) +$$
$$+ \sum_{P=Q,\, A \neq B} \mathbf{P}(S_P \cup \{A\} \text{ и } S_Q \cup \{B\} \text{ независимы}).$$

Кроме того,

$$\sum_{P \neq Q} \mathbf{P}(S_P \cup \{A\} \text{ и } S_Q \cup \{B\} \text{ независимы}) \leqslant$$
$$\leqslant \binom{n}{s}^2 (V-N)^2 (1-p)^{2(1+o(1))N} = (1+o(1))(\mathbf{E}(Y))^2$$

и

$$\sum_{P=Q,\, A \neq B} \mathbf{P}(S_P \cup \{A\} \text{ и } S_Q \cup \{B\} \text{ независимы}) \leqslant$$
$$\leqslant \binom{n}{s} (V-N)^2 (1-p)^{2(1+o(1))N} = o((\mathbf{E}(Y))^2).$$

Итого получаем, что

$$\mathbf{E}(Y(Y-1)) = (1+o(1))(\mathbf{E}(Y))^2,$$

что и требовалось.

§ 5. Заключение

Верхняя оценка критической вероятности

$$p = p(n) = \frac{2s\binom{r}{s}\ln n}{\binom{n-s}{r-s}}$$

выглядит достаточно искусственно. Приступая к доказательству, авторы были уверены, что аналогично работе [31] она будет выглядеть как

$$p = p(n) = \frac{(1+\varepsilon)(r+s)\ln n}{\binom{n-s}{r-s}}$$

для малого положительного ε. Однако для такой вероятности сохранения ребра доказать ничего не получилось – это связано с особенностями принятого метода доказательства. Более конкретно, в третьем случае (“большое i”) нужно оценить число ребер в подграфе графа $\widetilde{G}(n, r, s)$, индуцированном множествами вершин с фиксированными параметрами. Если в работе [31] (т.е. при $s = 1$) хватало достаточно слабой оценки на вероятность сохранения ребра, то в общем случае ее уже не хватает. Если изначальное предположение о природе точной верхней оценки верно, то для его доказательства нужен новый метод.

Также для дальнейшего исследования остается вопрос, что происходит при непостоянных r и s. В работе [31] аналогичные результаты были доказаны для $r = o(n^{\frac{1}{3}})$, и скорее всего, результаты этой статьи также можно обобщить на случай, когда r и s – (медленно) растущие функции.

СПИСОК ЛИТЕРАТУРЫ

1. *Боголюбский Л.И., Райгородский А.М.* Замечание о нижних оценках хроматических чисел пространств малой размерности с метриками ℓ_1 и ℓ_2 // Матем. заметки. 2019. V. 105. № 2. P. 187–213.
2. *Székely L.A.* Erdős on Unit Distances and the Szemerédi–Trotter Theorems // Paul Erdős and His Mathematics, II (Proc. Conf. Held in Budapest, Hungary. July 4–11, 1999). Bolyai Soc. Math. Stud. V. 11. Berlin: Springer; Budapest: János Bolyai Math. Soc., 2002. P. 649–666.
3. *Захаров Д.А., Райгородский А.М.* Клико-хроматические числа графов пересечений // Матем. заметки. 2019. V. 105. № 1. P. 142–144.
4. *Balogh J., Cherkashin D., Kiselev S.* Coloring General Kneser Graphs and Hypergraphs via High-Discrepancy Hypergraphs // Europ. J. Combin. 2019. V. 79. P. 228–236.
5. *Raigorodskii A.M.* Cliques and Cycles in Distance Graphs and Graphs of Diameters // Discrete Geometry and Algebraic Combinatorics (AMS Special Session on Discrete Geometry and Algebraic Combinatorics. San Diego, CA, USA. January 11, 2013). Providence, RI: Amer. Math. Soc., 2014. P. 93–109.
6. *Boltyanski V.G., Martini H., Soltan P.S.* Excursions into Combinatorial Geometry. Berlin: Springer, 1997.
7. *Райгородский А.М.* Вокруг гипотезы Борсука // Геометрия и механика. Современная математика. Фундаментальные направления. Т. 23. М: РУДН, 2007. С. 147–164.
8. *Райгородский А.М., Черкашин Д.Д.* Экстремальные задачи в раскрасках гиперграфов // УМН. 2020. Т. 75. № 1 (451). С. 95–154.
9. *Просанов Р.И.* Контрпримеры к гипотезе Борсука, имеющие большой обхват // Матем. заметки. 2019. V. 105. № 6. P. 890–898.

10. *Graham R.L., Rothschild B.L., Spencer J.H.* Ramsey Theory. New York: John Wiley & Sons, 1990.
11. *Купавский А.Б., Сагдеев А.А.* Теория Рамсея в пространстве с чебышевской метрикой // УМН. 2020. Т. 75. № 5 (455). С. 191–192.
12. *Пушняков Ф.А.* О количествах ребер в порожденных подграфах некоторых дистанционных графов // Матем. заметки. 2019. V. 105. № 4. P. 592–602.
13. *Sagdeev A.A., Raigorodskii A.M.* On a Frankl–Wilson Theorem and Its Geometric Corollaries // Acta Math. Univ. Comenian. (N.S.). 2019. V. 88. № 3. P. 1029–1033.
14. *Сагдеев А.А.* Об одной теореме Франкла – Уилсона // Пробл. передачи информ. 2019. Т. 55. № 4. С. 86–106.
15. *Kupavskii A.* Degree Versions of Theorems on Intersecting Families via Stability // J. Combin. Theory Ser. A. 2019. V. 168. P. 272–287.
16. *Ihringer F., Kupavskii A.* Regular Intersecting Families // Discrete Appl. Math. 2019. V. 270. P. 142–152.
17. *Frankl P., Kupavskii A.* Partition-free Families of Sets // Proc. Lond. Math. Soc. (3). 2019. V. 119. № 2. P. 440–468.
18. *Frankl P., Kupavskii A.* Two Problems on Matchings in Set Families—In the Footsteps of Erdős and Kleitman // J. Combin. Theory Ser. B. 2019. V. 138. P. 286–313.
19. *Kupavskii A., Pach J., Tomon I.* On the Size of K-Cross-free Families // Combinatorica. 2019. V. 39. № 1. P. 153–164.
20. *Ипатов М.М., Кошелев М.М., Райгородский А.М.* Модулярность некоторых дистанционных графов // Докл. РАН. 2020. Т. 490. № 1. С. 71–73.
21. *Kiselev S., Kupavskii A.* Sharp Bounds for the Chromatic Number of Random Kneser Graphs // Acta Math. Univ. Comenian. (N.S.). 2019. V. 88. № 3. P. 861–865.
22. *Alishahi M., Hajiabolhassan H.* Chromatic Number of Random Kneser Hypergraphs // J. Combin. Theory Ser. A. 2018. V. 154. P. 1–20.
23. *Пядеркин М.М., Райгородский А.М.* О случайных подграфах кнезеровского графа и его обобщений // ДАН. 2016. Т. 470. № 4. С. 384–386.
24. *Бобу А.В., Куприянов А.Э., Райгородский А.М.* Об одном обобщении кнезеровских графов // Матем. заметки. 2020. Т. 107. № 3. С. 351–365.
25. *Pyaderkin M.M.* On the Chromatic Number of Random Subgraphs of a Certain Distance Graph // Discrete Appl. Math. 2019. V. 267. P. 209–214.
26. *Raigorodskii A.M., Koshelev M.M.* New Bounds on Clique-Chromatic Numbers of Johnson Graphs // Discrete Appl. Math. 2020. V. 283. P. 724–729.
27. *Райгородский А.М., Кошелев М.М.* Новые оценки клико-хроматических чисел графов Джонсона // Докл. РАН. 2020. Т. 490. № 1. С. 78–80.
28. *Райгородский А.М., Шишунов Е.Д.* О числах независимости дистанционных графов с вершинами в $\{-1,0,1\}^n$ // ДАН. 2019. V. 488. № 5. P. 486–487.
29. *Райгородский А.М., Шишунов Е.Д.* О числах независимости некоторых дистанционных графов с вершинами в $\{-1,0,1\}^n$ // ДАН. 2019. V. 485. № 3. P. 269–271.
30. *Пушняков Ф.А., Райгородский А.М.* Оценка числа ребер в особых подграфах некоторого дистанционного графа // Матем. заметки. 2020. Т. 107. № 2. С. 286–298.
31. *Bollobás B., Narayanan B.P., Raigorodskii A.M.* On the Stability of the Erdős–Ko–Rado Theorem // J. Combin. Theory Ser. A. 2016. V. 137. P. 64–78.
32. *Tran T., Das S.* A Simple Removal Lemma for Large Nearly-Intersecting Families // Ext. Abstr. 8th European Conf. on Combinatorics, Graph Theory and Applications (EuroComb'2015). Bergen, Norway. Aug. 31 – Sept. 4, 2015. Electron. Notes Discrete Math. 2015. V. 49. P. 93–99.
33. *Balogh J., Bollobás B., Narayanan B.P.* Transference for the Erdős–Ko–Rado Theorem // Forum Math. Sigma. 2015. V. 3. Article e23 (18 pp).
34. *Пядеркин М.М.* О пороговой вероятности для устойчивости независимых множеств в дистанционном графе // Матем. заметки. 2019. Т. 106. № 2. С. 280–294.

35. *Das S., Tran T.* Removal and Stability for Erdős–Ko–Rado // SIAM J. Discrete Math. 2016. V. 30. № 2. P. 1102–1114.
36. *Devlin P., Kahn J.* On “Stability” in the Erdős–Ko–Rado Theorem // SIAM J. Discrete Math. 2016. V. 30. № 2. P. 1283–1289.

Огарок Петр Алексеевич
Московский физико-технический институт
(государственный университет),
факультет инноваций и высоких технологий,
кафедра дискретной математики
`ogarokpeter@yandex.ru`
Райгородский Андрей Михайлович
Московский физико-технический институт
(государственный университет),
Физтех-школа прикладной математики и информатики;
лаборатория продвинутой комбинаторики и сетевых приложений
Московский государственный университет им. М.В. Ломоносова,
механико-математический факультет,
кафедра математической статистики и случайных процессов
Кавказский математический центр
Адыгейского государственного университета
Бурятский государственный университет,
институт математики и информатики
`mraigor@yandex.ru`

Поступила в редакцию
09.03.2020
После доработки
29.10.2020
Принята к публикации
29.10.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.714.5

© 2020 г. **И.В. Чередник**

ОСОБЕННОСТИ p-ЛИНЕЙНОГО РАЗЛОЖЕНИЯ p-ЛИНЕЙНЫХ ФУНКЦИЙ В ТЕРМИНАХ ОПЕРАЦИИ СДВИГ-КОМПОЗИЦИИ

Исследуется операция сдвиг-композиции дискретных функций, которая возникает при гомоморфизмах конечных регистров сдвига. Доказано, что при простом p в классе всех функций, линейных по крайним переменным, для p-линейных функций совпадают понятия приводимости и p-линейной приводимости. Кроме того, показано, что линейная функция, неприводимая в классе всех линейных функций, не имеет p-линейных делителей, биективных по крайней правой переменной, а в некоторых случаях и вовсе не имеет p-линейных делителей.

Ключевые слова: регистр сдвига, гомоморфизмы регистров сдвига, сдвиг-композиция, конечные поля, p-линейные функции, разложение матричных многочленов, скрученные многочлены, скрученные линейные рекуррентные последовательности.

DOI: `10.31857/S0555292320040063`

§ 1. Введение

Пусть $\mathbb{F}_q$ – конечное поле из $q = p^t$ элементов, $F_q(n) = \{f \mid f\colon \mathbb{F}_q^n \to \mathbb{F}_q\}$ – множество всех $\mathbb{F}_q$-значных функций от n переменных, $F_q = \bigcup\limits_{n\geqslant 0} F_q(n)$.

В работах отечественных криптографов К.Г. Таболова, А.Я. Прососова, В.А. Башева, В.И. Солодовникова и др. была введена и исследована (преимущественно в терминах гомоморфизмов регистров сдвига) операция сдвиг-композиции ($\lhd$-умножения) на множестве всех функций F_q:

$$\forall f \in F_q(n+1)\ \forall g \in F_q(m+1)$$
$$(f \lhd g)(x_0,\ldots,x_{n+m}) = f\big(g(x_0,\ldots,x_m),\ldots,g(x_n,\ldots,x_{n+m})\big).$$

В работах перечисленных выше авторов в разной степени общности и направленности достаточно подробно исследована связь между представлением функции h в виде $h = f \lhd g$ и существованием гомоморфизма регистра сдвига, внутреннее функционирование которого определяется функцией h, на регистр сдвига, внутреннее функционирование которого определяется функцией f (функция g из разложения $h = f \lhd g$ определяет характер гомоморфизма регистров сдвига). Все основные достижения в данной области единым образом изложены в монографии [1], мы лишь кратко перечислим результаты, полученные в направлении декомпозиции функций относительно операции $\lhd$-умножения.

В работе [2] описаны все возможные представления произвольной функции $h \in F_q$ в виде $h = l \lhd g$, где l – линейная над $\mathbb{F}_q$ функция. Это достижение позволяет указать все возможные гомоморфизмы произвольного регистра сдвига на регистры сдвига с линейной обратной связью.

В работе [3] описаны все возможные представления произвольной функции $h \in F_q$ в виде $h = f \lhd l$, где l – линейная над $\mathbb{F}_q$ функция. Кроме того, изучена возможность представления произвольной функции $h \in F_q$ в виде $f = l_1 \lhd g \lhd l_2$, где l_1, l_2 – линейные над $\mathbb{F}_q$ функции.

В работе [4] в терминах операции сдвиг-композиции исследуется возможность левого линейного разложения системы функций. Как оказалось, подобные разложения кроме стандартных приложений, связанных с гомоморфизмами регистров сдвига (см. [1]), обнаруживают очень интересное применение в вычислении представления произвольной функции $h \in F_q$ в виде $h = f \lhd g$, где f – p-линейная функция (линейная над $\mathbb{F}_p$). Здесь стоит отметить, что предложенный в работе [4] метод позволяет эффективно выделять максимальный левый p-линейный $\lhd$-делитель у произвольной p-нелинейной функции, но не пригоден для построения нетривиального p-линейного $\lhd$-разложения p-линейной функции. Последняя задача по существу является переформулировкой классической проблемы факторизации многочленов над кольцом матриц и, очевидно, крайне сложна.

В данной статье мы представляем два нетривиальных результата о p-линейных разложениях p-линейных функций, которые кроме теоретической ценности описания возможных гомоморфизмов регистров сдвига также имеют большое значение при исследовании факторизации многочленов над кольцом матриц и, соответственно, при построении практически значимых классов скрученных линейных рекуррентных последовательностей (см. [5]).

§ 2. Постановка задачи

1. Следуя терминологии работ [1,2,6,7], регистром сдвига длины n над полем $\mathbb{F}_q$ с функцией обратной связи $\varphi \in F_q(n+1)$ и выходной функцией $\psi \in F_q(n+1)$ будем называть автомат

$$R(\varphi, \psi) = (\mathbb{F}_q, \mathbb{F}_q^n, \mathbb{F}_q, h, f),$$

у которого функции переходов и выходов определяются равенствами

$$h((x_1, \dots, x_n), x) = (x_2, \dots, x_n, \varphi(x_1, \dots, x_n, x)),$$
$$f((x_1, \dots, x_n), x) = \psi(x_1, x_2, \dots, x_n, \varphi(x_1, \dots, x_n, x)).$$

Нетрудно видеть, что биективность функции обратной связи φ по первой переменной равносильна регулярности регистра сдвига $R(\varphi, \psi)$ – при любом входном символе частичная функция переходов h_x автомата $R(\varphi, \psi)$ является биекцией. Кроме того, биективность каждой из функций φ и ψ по последней переменной является необходимым и достаточным условием для обратимости автомата $R(\varphi, \psi)$. В связи с отмеченными особенностями при реализации регистров сдвига на практике преимущественно используются функции обратной связи, биективные по первой и (или) последней переменным, и выходные функции, биективные по последней переменной (см. [1, 2, 7]). Здесь стоит отметить, что наиболее простыми в реализации и, соответственно, наиболее распространенными на практике функциями, биективными по какой-либо переменной, являются функции, линейные по указанной переменной.

Множество всех $\mathbb{F}_q$-значных функций, биективных по первой (последней) переменной, будем обозначать через ${}^*F_q$ (F_q^*), а множество всех $\mathbb{F}_q$-значных функций, линейных по первой (последней) переменной, – через ${}^+F_q$ (F_q^+). При этом естественными будут производные обозначения

$${}^*F_q^* = {}^*F_q \cap F_q^*, \quad {}^*F_q^+ = {}^*F_q \cap F_q^+, \quad {}^+F_q^* = {}^+F_q \cap F_q^*, \quad {}^+F_q^+ = {}^+F_q \cap F_q^+.$$

2. Как известно (см. [8]), каждая функция $f(x_0,\ldots,x_n)\in F_q$ единственным образом представляется приведенным многочленом из $\mathbb{F}_q[x_0,x_1,\ldots]$:

$$f(x_0,\ldots,x_n)=\sum_{i_0,\ldots,i_n\in\overline{0,q-1}} c_{i_0\ldots i_n}x_0^{i_0}\ldots x_n^{i_n}.$$

При проведении некоторых исследований относительно функций из F_q часто бывает удобным вести изложение на языке соответствующих приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\ldots]$, которые в отличие от функций определяются от общего набора переменных $x_0,x_1,\ldots$

Множество всех приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\ldots]$ относительно операций сложения и умножения с последующим приведением результата по модулю идеала $(x_i^q-x_i\mid i\in\mathbb{N}_0)$ образует коммутативное кольцо с единицей. Кроме того, на множестве всех приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\ldots]$ корректно определить операцию сдвиг-композиции ($\lhd$-умножения):

$$f(x_0,\ldots,x_n)\lhd g(x_0,\ldots,x_m)\overset{\text{def}}{=}$$
$$\overset{\text{def}}{=} f\big(g(x_0,\ldots,x_m),\ldots,g(x_n,\ldots,x_{n+m})\big)\mod (x_i^q-x_i\mid i\in\mathbb{N}_0).$$

Нетрудно видеть, что множество всех приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\ldots]$ относительно операции $\lhd$-умножения образует полугруппу с нейтральным элементом x_0.

3. Как известно, существует несколько подходов к определению степени нелинейности отображения над конечным полем $\mathbb{F}_q$ (см. [9, 10]). Наиболее простой состоит в том, что под степенью нелинейности функции $f\in F_q$ понимается степень соответствующего приведенного многочлена из $\mathbb{F}_q[x_0,x_1,\ldots]$. При таком подходе линейными называют функции, приведенные многочлены которых имеют вид

$$\beta_0x_0+\ldots+\beta_nx_n\in\mathbb{F}_q[x_0,x_1,\ldots].$$

Однако в случае $q=p^t$ на практике зачастую гораздо более плодотворным оказывается другой подход к определению степени нелинейности, который учитывает более общую линейность отображения $f\in F_q$ над подполем $\mathbb{F}_p$.

Если функция $f(x_0,\ldots,x_n)\in F_q$ задана приведенным многочленом

$$f(x_0,\ldots,x_n)=\sum_{i_0,\ldots,i_n\in\overline{0,q-1}} c_{i_0\ldots i_n}x_0^{i_0}\ldots x_n^{i_n},$$

то *индексом p-нелинейности функции* f называют величину

$$\operatorname{ind}_p f=\max\big\{\|i_0\|_p+\ldots+\|i_n\|_p : i_0,\ldots,i_n=\overline{0,q-1},\ c_{i_0\ldots i_n}\neq 0\big\},\tag{1}$$

где $\|j\|_p=j_0+j_1+\ldots+j_{t-1}$ – p-ичный вес числа $j=j_0+pj_1+\ldots+p^{t-1}j_{t-1}\in\overline{0,q-1}$.

С другой стороны, если зафиксировать некоторый базис $\alpha_1,\ldots,\alpha_t$ пространства $\mathbb{F}_q$ над $\mathbb{F}_p$, то каждый аргумент x_i функции $f(x_0,\ldots,x_n)$ можно представить в виде

$$x_i=\alpha_1x_{i1}+\ldots+\alpha_tx_{it},\quad x_{ij}\in\mathbb{F}_p,$$

а саму функцию $f(x_0,\ldots,x_n)$ отождествить с набором p-значных *координатных* функций

$$f_1(x_{01},\ldots,x_{0t},\ldots,x_{n1},\ldots,x_{n,t}),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f_t(x_{01},\ldots,x_{0t},\ldots,x_{n1},\ldots,x_{n,t}),$$

который удовлетворяет соотношению $f = \alpha_1 f_1 + \ldots + \alpha_t f_t$. В таком случае индекс p-нелинейности функции f согласно [9] можно вычислить по формуле

$$\operatorname{ind}_p f = \max\{\deg f_1, \ldots, \deg f_t\}. \tag{2}$$

Здесь стоит отметить, что в случае простого p индекс p-нелинейности функции $f \in F_q$ совпадает с ее аддитивным показателем нелинейности $\operatorname{dl} f$. Изящное аксиоматическое изложение аддитивного подхода к измерению степени нелинейности, а также сравнение данного подхода с классическим, можно найти в работах [10, 11]. Так, в работе [10] доказано, что при простом p аддитивный показатель $\operatorname{dl} f$ степени нелинейности функции $f \in F_p$ совпадает с классическим показателем $\deg f$, а для произвольной функции $f \in F_q$ ее аддитивный показатель нелинейности можно вычислять различными способами в зависимости от представления функции f:

$$\operatorname{dl} f = \max\{\operatorname{dl} f_1, \ldots, \operatorname{dl} f_t\} = \max\{\deg f_1, \ldots, \deg f_t\} = \operatorname{ind}_p f.$$

Функцию $f \in F_q$ будем называть *p-линейной*, если $\operatorname{ind}_p f = 1$ и $f(0, \ldots, 0) = 0$. Согласно (1) функция $f(x_0, \ldots, x_n) \in F_q$ является p-линейной в том и только том случае, когда она представляется приведенным многочленом вида

$$\big(\beta_{01}x_0 + \ldots + \beta_{0t}x_0^{p^{t-1}}\big) + \ldots + \big(\beta_{n1}x_n + \ldots + \beta_{nt}x_n^{p^{t-1}}\big) \in \mathbb{F}_q[x_0, x_1, \ldots],$$

при этом ее координатные функции $f_1, \ldots, f_t$ ввиду (2) представляются многочленами вида

$$\begin{array}{l}
a_{01}^{(1)}x_{01} + \ldots + a_{0t}^{(1)}x_{0t} + \ldots + a_{n1}^{(1)}x_{n1} + \ldots + a_{n,t}^{(1)}x_{n,t} \in \mathbb{F}_p[x_{01}, \ldots, x_{0t}, x_{11}, \ldots],\\
\dotfill\\
a_{01}^{(t)}x_{01} + \ldots + a_{0t}^{(t)}x_{0t} + \ldots + a_{n1}^{(t)}x_{n1} + \ldots + a_{n,t}^{(t)}x_{n,t} \in \mathbb{F}_p[x_{01}, \ldots, x_{0t}, x_{11}, \ldots].
\end{array}$$

Множество всех p-линейных функций из F_q будем обозначать через L_q^p. Заметим, что в данной терминологии классические линейные функции из F_q являются q-линейными, т.е. $L_q = L_q^q$. Напомним, что многочлены вида $\beta_1 x + \ldots + \beta_t x^{p^{t-1}} \in \mathbb{F}_q[x]$ описывают все линейные преобразования пространства $\mathbb{F}_q$ над полем $\mathbb{F}_p$ и называются *p-линеаризованными* многочленами (см. [8]). Соответственно, все p-линеаризованные многочлены вида

$$\big(\beta_{01}x_0 + \ldots + \beta_{0t}x_0^{p^{t-1}}\big) + \ldots + \big(\beta_{n1}x_n + \ldots + \beta_{n,t}x_n^{p^{t-1}}\big) \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$$

описывают все отображения пространства $\mathbb{F}_q^{n+1}$ в $\mathbb{F}_q$, линейные над $\mathbb{F}_p$.

4. Множество $L_q[x_0, x_1, \ldots]$ всех линейных, но не аффинных многочленов над $\mathbb{F}_q$

$$\beta_0 x_0 + \ldots + \beta_n x_n \in \mathbb{F}_q[x_0, x_1, \ldots]$$

относительно операций сложения и $\lhd$-умножения образует коммутативное кольцо, а отображение

$$\beta_0 x_0 + \ldots + \beta_n x_n \mapsto \beta_0 x^0 + \ldots + \beta_n x^n$$

является изоморфизмом колец $(L_q[x_0, x_1, \ldots], +, \lhd) \cong (\mathbb{F}_q[x], +, \cdot)$ (см. [1, 2, 7]).

Рассмотрим теперь множество $L_q^p[x_0, x_1, \ldots]$ всех p-линеаризованных многочленов из $\mathbb{F}_q[x_0, x_1, \ldots]$. Множество всех p-линеаризованных многочленов из $\mathbb{F}_q[x]$ относительно операций сложения и композиции образует кольцо, изоморфное кольцу $\operatorname{End}_{\mathbb{F}_p} \mathbb{F}_q$ всех линейных преобразований пространства $\mathbb{F}_q$ над $\mathbb{F}_p$. Указанный изоморфизм

$$\beta_1 x + \ldots + \beta_t x^{p^{t-1}} \mapsto B$$

естественным образом индуцирует отображение

$$\bigl(\beta_{01}x_0 + \ldots + \beta_{0t}x_0^{p^{t-1}}\bigr) + \ldots + \bigl(\beta_{n1}x_n + \ldots + \beta_{n,t}x_n^{p^{t-1}}\bigr) \mapsto B_0 + \ldots + B_n X^n,$$

являющееся изоморфизмом колец $(L_q^p[x_0, x_1, \ldots], +, \lhd) \cong ((\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot\,)$. Отметим, что кольцо $((\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot\,)$ известно как кольцо *скрученных* многочленов и является базовым объектом исследований в теории скрученных линейных рекуррентных последовательностей (см. [5, 12]).

Элементы кольца $\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q$ наиболее естественно представлять матрицами размера $t \times t$ над полем $\mathbb{F}_p$. Поэтому всюду далее в данной статье мы будем рассматривать кольцо скрученных многочленов $((\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot\,)$ в матричном представлении $((\mathbb{F}_p)_{t\times t}[X], +, \cdot\,)$, подразумевая при этом известный изоморфизм

$$((\mathbb{F}_p)_{t\times t}[X], +, \cdot\,) \cong ((\mathbb{F}_p[x])_{t\times t}, +, \cdot\,).$$

5. Будем говорить, что *функция g делит справа функцию h*, если существует функция f, для которой выполняется равенство $h = f \lhd g$; при этом будем говорить, что *функция f делит функцию h слева.* Произвольная $h \in F_q$ делится слева и справа на обратимые элементы моноида $(F_q, \lhd)$:

$$h = g \lhd (g^{-1} \lhd h), \quad h = (h \lhd g^{-1}) \lhd g,$$

подобные разложения будем называть *несобственными.* Если функция h допускает собственное разложение $h = f \lhd g$, то будем говорить, что h *приводима*, а функции f и g будем называть *собственными левым и правым делителями функции h.*

Следуя [3], определим один параметр, который естественным образом характеризует размер функции. Если функция $f(x_0, \ldots, x_n)$ зависит существенным образом только от переменных $x_{i_0}, \ldots, x_{i_k}$, $0 \leqslant i_0 < \ldots < i_k \leqslant n$, то величину $\mathrm{len}\, f = i_k - i_0$ будем называть *длиной функции f*. Длины постоянных функций по определению полагаем равными $-\infty$. Введенный параметр удачно согласуется с операцией сдвиг-композиции:

$$\mathrm{len}(f \lhd g) \leqslant \mathrm{len}\, f + \mathrm{len}\, g;$$

более того, при естественных с практической точки зрения ограничениях $f \in {}^*F_q^*$ или $g \in {}^*F_q^*$ указанное неравенство обращается в равенство (см. [3, утверждение 3]).

Разложение $h = f \lhd g$, в котором $\mathrm{len}\, f < \mathrm{len}\, h$ и $\mathrm{len}\, g < \mathrm{len}\, h$, будем называть *существенным*, при этом функции f и g будем называть *существенными левым и правым делителями функции h.*

С практической точки зрения исследования гомоморфизмов регистров сдвига существенность соответствующих разложений (см. [2, теорема 1]) означает, что гомоморфный образ регистра сдвига является регистром сдвига меньшей длины. Здесь стоит отметить также, что наличие собственных разложений еще не гарантирует возможность их применения при решении практической задачи построения гомоморфизма регистра сдвига на регистр сдвига меньшей длины. Так, например, над полем $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ линейная функция $x_0 + x_1$ допускает собственное разложение

$$x_0 + x_1 = \bigl(x_0 + (\alpha + 1)x_1 + \alpha x_1^2\bigr) \lhd \bigl(x_0 + \alpha x_1 + \alpha x_1^2\bigr),$$

в котором длины компонент разложения совпадают с длиной исходной функции.

Замечание 1. Вообще говоря, существенное разложение необязательно является собственным и, наоборот, собственное разложение не всегда существенно. Однако при рассмотрении класса ${}^*F_q^*$, который относительно операции сдвиг-композиции образует полугруппу, понятия собственного и существенного разложений совпадают, поскольку множество всех обратимых элементов моноида $({}^*F_q^*, \lhd)$ совпадает с множеством всех его элементов длины 0.

Замечание 2. Нетрудно видеть, что множество $\widehat{F}_q$ всех функций из F_q, сохраняющих константу 0, замкнуто относительно операции сдвиг-композиции и образует полугруппу. Для произвольной функции $f \in F_q$, $f(0, \ldots, 0) = c_f$ существует тесная связь между приводимостью f в F_q и приводимостью $\widehat{f} = f - c_f$ в $\widehat{F}_q$:

$$f = g \lhd h \iff \widehat{f} = (x_0 - c_f) \lhd g \lhd (x_0 + c_h) \lhd \widehat{h} = g_1 \lhd \widehat{h}, \quad g_1, \widehat{h} \in \widehat{F}_q.$$

Таким образом, исследование приводимости в моноиде $(F_q, \lhd)$ сводится к исследованию приводимости в подмоноиде $(\widehat{F}_q, \lhd)$. В дальнейшем в данной статье без ограничения общности рассматривается приводимость в рамках $\widehat{F}_q$, даже если это не оговаривается явным образом.

6. В работе [4] предложен эффективный алгоритм выделения максимального левого существенного p-линейного делителя у произвольной p-нелинейной функции h:

$$h = f \lhd g, \quad f \in L_q^p, \quad \operatorname{len} g \text{ минимально возможная.}$$

К сожалению, указанный алгоритм не пригоден даже для вычисления собственного разложения p-линейной функции – результатом применения данного метода к p-линейной функции h будет тривиальное разложение $h = h \lhd x_0$. Задача нахождения p-линейных разложений p-линейных функций по существу эквивалентна построению $\lhd$-разложений p-линеаризованных многочленов в кольце $(L_q^p[x_0, x_1, \ldots], +, \lhd)$ и фактически является переформулировкой классической проблемы о факторизации многочленов над кольцом матриц – по-видимому, на текущий момент данная проблема не имеет простого алгебраического решения.

В данной статье представлены два нетривиальных результата о p-линейных разложениях p-линейных функций, которые кроме теоретической ценности также имеют большое значение при исследовании и построении практически значимых классов скрученных линейных рекуррентных последовательностей (см. [5]). Исследование приводимости проводится в естественных практических рамках поиска существенных разложений, в которых обе компоненты линейны (биективны) по крайней правой переменной.

Операция сдвиг-композиции обладает определенной симметричностью, а потому для краткости формулирования результатов и удобства проведения соответствующих доказательств мы будем рассматривать множества ${}^*F_q$ и ${}^+F_q$, хотя естественно, что все утверждения остаются верными и для множеств F_q^* и F_q^+.

§ 3. p-линейная приводимость линейных функций

Как было отмечено выше, множество всех линейных многочленов $L_q[x_0, x_1, \ldots]$ относительно операций сложения и сдвиг-композиции образует кольцо, изоморфное кольцу многочленов $\mathbb{F}_q[x]$. Таким образом, исследование приводимости классической линейной функции в классе L_q эквивалентно известной проблеме факторизации многочленов над конечным полем $\mathbb{F}_q$ (см., например, [8]).

Поскольку $L_q \subsetneq L_q^p$, то очевидно, что для классической линейной функции понятие p-линейной приводимости в классе L_q^p является более широким по сравнению с линейной приводимостью в классе L_q. Для удобства и наглядности исследование

p-линейной приводимости классических линейных функций будем проводить в матричном представлении, подразумевая ранее отмеченные изоморфизмы

$$(L_q^p[x_0, x_1, \ldots], \lhd, +) \cong ((\operatorname{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot\,) \cong ((\mathbb{F}_p)_{t\times t}[X], +, \cdot\,) \cong ((\mathbb{F}_p[x])_{t\times t}, +, \cdot\,).$$

В матричной терминологии исследование p-линейной приводимости классической линейной функции $h \in L_q$ фактически означает исследование приводимости соответствующего многочлена $h(x) \in \mathbb{F}_q[x]$ в кольце многочленов $(\mathbb{F}_p)_{t\times t}[X]$.

Напомним, как устроено естественное вложение $\mathbb{F}_q[x] \to (\mathbb{F}_p)_{t\times t}[X]$. Выберем произвольный неприводимый над $\mathbb{F}_p$ многочлен $\chi(x) \in \mathbb{F}_p[x]$ степени t. Как известно, многочлен $\chi(x)$ имеет в поле $\mathbb{F}_q$ корень α и $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. При выборе произвольной матрицы $S \in (\mathbb{F}_p)_{t\times t}$ с характеристическим многочленом $\chi(x)$ корректно определить отображение

$$r_0 + r_1\alpha + \ldots + r_{t-1}\alpha^{t-1} \mapsto r_0E + r_1S + \ldots + r_{t-1}S^{t-1}, \tag{3}$$

являющееся изоморфизмом полей

$$\mathbb{F}_q = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p(S) = \{r_0E + r_1S + \ldots + r_{t-1}S^{t-1} : r_0, r_1, \ldots, r_{t-1} \in \mathbb{F}_p\}.$$

Данный изоморфизм полей естественным образом продолжается до изоморфизма колец многочленов $\mathbb{F}_p(\alpha)[x] \cong \mathbb{F}_p(S)[X]$, при котором многочлену

$$h(x) = h_0 + \ldots + h_{n-1}x^{n-1} + h_nx^n \in \mathbb{F}_p(\alpha)[x], \quad h_i = \sum_{j=0}^{t-1} r_{ij}\alpha^j, \quad 0 \leqslant i \leqslant n,$$

ставится в соответствие многочлен

$$H(X) = H_0 + \ldots + H_{n-1}X^{n-1} + H_nX^n \in \mathbb{F}_p(S)[X], \quad H_i = \sum_{j=0}^{t-1} r_{ij}S^j, \quad 0 \leqslant i \leqslant n.$$

Таким образом, установлено вложение $\mathbb{F}_q[x] \to (\mathbb{F}_p)_{t\times t}[X]$ (здесь стоит отметить, что данное вложение не является единственным, но все подобные вложения сопряжены).

Теперь можно сформулировать и доказать центральный результат данного параграфа.

Теорема 1. *Пусть многочлен $h(x) \in \mathbb{F}_q[x]$ неприводим над $\mathbb{F}_q$. Тогда $H(X)$ не имеет собственных унитарных делителей в кольце $(\mathbb{F}_p)_{t\times t}[X]$. Если к тому же $h(x) \notin \mathbb{F}_{p^l}[x]$ при всех $l < t$, то $H(X)$ вообще не имеет собственных делителей в $(\mathbb{F}_p)_{t\times t}[X]$.*

Доказательство. Для удобства будем полагать, что $h(x) \in \mathbb{F}_q[x]$ – унитарный многочлен степени n. При проведении доказательства будем использовать вложение $\mathbb{F}_q[x] \to (\mathbb{F}_p)_{t\times t}[X]$, которое определялось ранее с помощью отображения (3).

Неприводимый многочлен $\chi(x) \in \mathbb{F}_p[x]$ в расширении $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ имеет t различных корней $\alpha, \ldots, \alpha^{p^{t-1}}$, и как известно из курса линейной алгебры, существует обратимая матрица $C \in (\mathbb{F}_q)_{t\times t}$, такая что $C^{-1}SC = \operatorname{diag}(\alpha, \ldots, \alpha^{p^{t-1}})$. На самом деле сопряжение указанной матрицей C приводит к диагональному виду все матрицы из $\mathbb{F}_p(S)$:

$$\begin{aligned}
&C^{-1}(r_0E + r_1S + \ldots + r_{t-1}S^{t-1})C = \ldots = \\
&= \operatorname{diag}\bigl(r_0 + r_1\alpha + \ldots + r_{t-1}\alpha^{t-1}, \ldots, r_0 + r_1\alpha^{p^{t-1}} + \ldots + r_{t-1}(\alpha^{p^{t-1}})^{t-1}\bigr) = \\
&= \operatorname{diag}\bigl(\beta, \ldots, \beta^{p^{t-1}}\bigr) \in (\mathbb{F}_q)_{t\times t}.
\end{aligned}$$

Предположим, что многочлен $H(X)$ допускает в кольце $(\mathbb{F}_p)_{t\times t}[X]$ собственное разложение:

$$H(X) = F(X)\cdot G(X), \quad \det F(x) \neq 1, \quad \det G(x) \neq 1.$$

Тогда при сопряжении обеих частей данного равенства матрицей C получим соотношение

$$\begin{aligned}
&F_1(X)\cdot G_1(X) = (C^{-1}F(X)C)\cdot(C^{-1}G(X)C) = C^{-1}h(X)C = \\
&= C^{-1}\left(\left(\sum_{j=0}^{t-1} r_{0j}S^j\right) + \ldots + \left(\sum_{j=0}^{t-1} r_{n-1j}S^j\right)X^{n-1} + X^n\right)C = \\
&= \left(\sum_{j=0}^{t-1} r_{0j}, \operatorname{diag}\bigl(\alpha^j, \ldots, \alpha^{p^{t-1}j}\bigr)\right) + \ldots + \\
&+ \left(\sum_{j=0}^{t-1} r_{n-1j}\operatorname{diag}\bigl(\alpha^j, \ldots, \alpha^{p^{t-1}j}\bigr)\right)X^{n-1} + X^n = \\
&= \operatorname{diag}\Bigl(h_0 + \ldots + h_{n-1}x^{n-1} + x^n, \ldots, h_0^{p^{t-1}} + \ldots + h_{n-1}^{p^{t-1}}x^{n-1} + x^n\Bigr) = \\
&= \operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{t-1})}(x)\Bigr).
\end{aligned}$$

Если $l \in \mathbb{N}$ – наименьшее со свойством $h(x) \in \mathbb{F}_{p^l}[x]$, то $t = lm$ и $(m,n) = 1$. Кроме того, $h^{(p^{l+s})} = h^{(p^s)}$, $s \in \mathbb{N}_0$, и следовательно,

$$\operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{t-1})}(x)\Bigr) = \operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{l-1})}(x), \ldots, h(x), \ldots, h^{(p^{l-1})}(x)\Bigr).$$

Теперь в равенстве

$$F_1(x)\cdot G_1(x) = \operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{l-1})}(x), \ldots, h(x), \ldots, h^{(p^{l-1})}(x)\Bigr)$$

вычислим определители обеих частей:

$$\det F_1(x)\cdot\det G_1(x) = h(x)^m\cdot\ldots\cdot h^{(p^{l-1})}(x)^m.$$

Из единственности канонического разложения следует, что

$$\det G_1(x) = h(x)^{m_0}\cdot\ldots\cdot h^{(p^{l-1})}(x)^{m_{l-1}}.$$

Поскольку $\det G_1(x) = \det G(x) \in \mathbb{F}_p[x]$, а $h(x), \ldots, h^{(p^{l-1})}(x) \in \mathbb{F}_{p^l}[x]$ – все многочлены, сопряженные с $h(x)$ над $\mathbb{F}_p$, то на самом деле $m_0 = \ldots = m_{l-1}$:

$$\det G_1(x) = \Bigl(h(x)\cdot\ldots\cdot h^{(p^{l-1})}(x)\Bigr)^{m_0}, \quad \deg\bigl(\det G_1(x)\bigr) = nlm_0.$$

Если $G(X)$ – унитарный многочлен степени k, то $G_1(X) = C^{-1}G(X)C$ – унитарный многочлен той же степени k, и следовательно, $\det G_1(x)$ – унитарный многочлен степени kt. В таком случае справедливы равенства

$$\deg\bigl(\det G_1(x)\bigr) = kt = klm = nlm_0,$$

из которых ввиду взаимной простоты $(m,n) = 1$ следует, что $n \mid k$. Таким образом, $\deg G(X) = k = n = \deg H(X)$, и соответственно, $G(X) = H(X)$.

Если $h(x) \notin \mathbb{F}_{p^l}[x]$ при всех $l < t$, то многочлен $h(x) \cdot \ldots \cdot h^{(p^{t-1})}(x)$ является неприводимым над $\mathbb{F}_p$ многочленом (степени nt), что противоречит системе условий

$$\det F_1(x) \cdot \det G_1(x) = h(x) \cdot \ldots \cdot h^{(p^{t-1})}(x), \quad \det F_1(x) \neq 1, \quad \det G_1(x) \neq 1. \quad \blacktriangle$$

Напомним, что произвольная p-линейная функция $f(x_0, \ldots, x_n) \in L_q^p$ задается соответствующим p-линеаризованным многочленом

$$\left(\beta_{01}x_0 + \ldots + \beta_{0t}x_0^{p^{t-1}}\right) + \ldots + \left(\beta_{n1}x_n + \ldots + \beta_{n,t}x_n^{p^{t-1}}\right),$$

которому при изоморфизме $(L_q^p[x_0, x_1, \ldots], \lhd, +) \cong ((\mathbb{F}_p)_{t\times t}[X], +, \cdot)$ сопоставляется многочлен $B_0 + \ldots + B_nX^n$. При этом, очевидно, линейным по крайней правой переменной функциям из L_q^p соответствуют унитарные многочлены из $(\mathbb{F}_p)_{t\times t}[X]$.

Следствие 1. *Пусть $h \in L_q$ – функция, неприводимая в классе L_q. Тогда h не допускает собственного (и следовательно, существенного) разложения в сдвиг-композицию p-линейных функций, одна из которых линейна по крайней правой переменной.*

Если к тому же $h \notin L_{p^l}$ при всех $l < t$, то $h(x)$ вообще не допускает собственного разложения в сдвиг-композицию p-линейных функций.

В заключение параграфа приведем несколько примеров, наглядно демонстрирующих качественное расширение понятия p-линейной приводимости по сравнению с классической линейной приводимостью. Для простоты изложения в примерах предварительно будет рассмотрено матричное представление.

Пример 1. Рассмотрим неприводимый над полем $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ многочлен $h(x) = 1 + x + x^3$. Согласно доказанной теореме 1 многочлен $H(X) = E + X + X^3$ не имеет унитарных делителей в кольце $(\mathbb{F}_2)_{2\times 2}[X]$. Однако $H(X)$ допускает собственное разложение в кольце $(\mathbb{F}_2)_{2\times 2}[X]$:

$$\begin{aligned}
H(X) &= E + X + X^3 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}X + \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}X^3 = \\
&= \begin{pmatrix}1+x+x^3 & 0\\ 0 & 1+x+x^3\end{pmatrix} = \begin{pmatrix}1 & x\\ x^2 & 1+x\end{pmatrix} \cdot \begin{pmatrix}1+x & x\\ x^2 & 1\end{pmatrix} = \\
&= \left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}X + \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}X^2\right) \cdot \left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}X + \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}X^2\right).
\end{aligned}$$

Таким образом, линейная функция $x_0 + x_1 + x_3$, неприводимая в классе L_4, допускает над $\mathbb{F}_4$ существенное и собственное 2-линейное разложение

$$\begin{aligned}
&x_0 + x_1 + x_3 = \left(x_0 + (\alpha+1)x_1 + (\alpha+1)x_1^2 + x_2 + (\alpha+1)x_2^2\right) \lhd \\
&\quad \lhd \left(x_0 + \alpha x_1 + (\alpha+1)x_1^2 + x_2 + (\alpha+1)x_2^2\right).
\end{aligned}$$

Пример 2. Многочлен $h(x) = 1 + x^2 + x^4$ над полем $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ раскладывается на линейные множители:

$$h(x) = (\alpha + x)^2 \cdot ((\alpha+1) + x)^2.$$

При этом для многочлена $H(X) = E + X^2 + X^4$ в кольце $(\mathbb{F}_2)_{2\times 2}[X]$ можно указать разложение

$$H(X) = \left(E + \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}X + X^2\right) \cdot \left(E + \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}X + X^2\right),$$

в котором каждый сомножитель не имеет корней в $(\mathbb{F}_2)_{2\times 2}$, и следовательно, не имеет унитарных делителей в $(\mathbb{F}_2)_{2\times 2}[X]$.

Таким образом, для линейной функции $x_0+x_2+x_4$ над полем $\mathbb{F}_4$ в дополнение к каноническому линейному разложению

$$x_0+x_2+x_4=(\alpha x_0+x_1)\lhd(\alpha x_0+x_1)\lhd\big((\alpha+1)x_0+x_1\big)\lhd\big((\alpha+1)x_0+x_1\big)$$

можно указать нетривиальное 2-линейное разложение

$$x_0+x_2+x_4=(x_0+x_1^2+x_2)\lhd(x_0+x_1^2+x_2),$$

в котором каждая из компонент не имеет 2-линейных делителей, линейных по крайней правой переменной.

Пример 3. Многочлен $h(x)=1+x+x^3+x^4$ над полем $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$ раскладывается на линейные множители:

$$h(x)=(1+x)^2\cdot(\alpha+x)\cdot((\alpha+1)+x).$$

При этом для многочлена $H(X)=E+X+X^3+X^4$ в кольце $(\mathbb{F}_2)_{2\times2}[X]$ можно указать дополнительные разложения:

$$H(X)=\left(E+\begin{pmatrix}1&0\\0&0\end{pmatrix}X+X^2\right)\cdot\left(E+\begin{pmatrix}0&0\\0&1\end{pmatrix}X+X^2\right)=$$
$$=\begin{pmatrix}1+x+x^2&0\\0&1+x^2\end{pmatrix}\cdot\begin{pmatrix}1+x^2&0\\0&1+x+x^2\end{pmatrix},$$
$$H(X)=\left(E+\begin{pmatrix}1&0\\1&0\end{pmatrix}X+X^2\right)\cdot\left(E+\begin{pmatrix}0&0\\1&1\end{pmatrix}X+X^2\right)=$$
$$=\begin{pmatrix}1+x+x^2&0\\x&1+x^2\end{pmatrix}\cdot\begin{pmatrix}1+x^2&0\\x&1+x+x^2\end{pmatrix},$$

в которых каждый из сомножителей не имеет корней в $(\mathbb{F}_2)_{2\times2}$, и следовательно, не имеет унитарных делителей в $(\mathbb{F}_2)_{2\times2}[X]$.

Таким образом, над полем $\mathbb{F}_4$ линейная функция $x_0+x_1+x_3+x_4$ в дополнение к каноническому линейному разложению

$$x_0+x_1+x_3+x_4=(x_0+x_1)\lhd(x_0+x_1)\lhd(\alpha x_0+x_1)\lhd\big((\alpha+1)x_0+x_1\big)$$

обладает нетривиальными 2-линейными разложениями

$$x_0+x_1+x_3+x_4=\big(x_0+(\alpha+1)x_1+\alpha x_1^2+x_2\big)\lhd\big(x_0+\alpha x_1+\alpha x_1^2+x_2\big),$$
$$x_0+x_1+x_3+x_4=\big(x_0+\alpha x_1+x_1^2+x_2\big)\lhd\big(x_0+(\alpha+1)x_1+x_1^2+x_2\big),$$

в которых каждая из компонент не имеет 2-линейных делителей, линейных по крайней правой переменной.

§ 4. Приводимость p-линейных функций

В работе [3] доказывается несколько практически значимых результатов о степени нелинейности сдвиг-композиции функций. Наиболее интересными, на наш взгляд, являются следующие утверждения.

Теорема 2 [3, теорема 10]. *Если p – простое число, то для композиции $f\lhd g$ произвольных функций $f\in F_p$ и $g\in {}^{+}F_p$ справедливы следующие утверждения:*

1. $\deg(f\lhd g)=1$ *тогда и только тогда, когда* $\deg f=\deg g=1$;
2. $\deg(f\lhd g)=2$ *тогда и только тогда, когда либо* $\deg f=1$ *и* $\deg g=2$, *либо* $\deg f=2$ *и* $\deg g=1$.

Здесь стоит отметить, что ядром доказательства теоремы 2 является следующая лемма, которая и сама по себе представляет интерес.

Лемма 1 [3, лемма 12]. *При простом p для любого $f \in F_p$, $\deg f \geqslant 2$, и любого $g \in {}^{+}F_p$ выполняется неравенство*

$$\deg(f \lhd g) \geqslant \deg g + 1.$$

В работе [3] приведены примеры, показывающие невозможность продолжения результатов теоремы 2 и леммы 1 на случай непростого поля $\mathbb{F}_q$ при использовании классического подхода к определению степени нелинейности. В данном параграфе исследуется возможность распространения результатов теоремы 2 и леммы 1 на случай непростого поля $\mathbb{F}_q$ при использовании индекса p-нелинейности, определенного выше (см. (1) и (2)).

Как показывает следующий пример, результат леммы 1 не допускает обобщения на случай непростого поля $\mathbb{F}_q$ даже при использовании параметра ind_p вместо deg.

Пример 4. Пусть $q = p^3$. Зафиксируем произвольный базис $\alpha_1, \alpha_2, \alpha_3$ поля $\mathbb{F}_q$ над $\mathbb{F}_p$. Рассмотрим функцию $f \in {}^{+}F_q^{+}$, определяемую в базисе $\alpha_1, \alpha_2, \alpha_3$ набором координатных функций

$$\begin{aligned} f_1 &= x_{01} + x_{12}x_{k+1,2} + x_{13}x_{k+1,3} + x_{k+2,1},\\ f_2 &= x_{02} + x_{k+1,2},\\ f_3 &= x_{03} + x_{k+1,3}, \end{aligned}$$

и функцию $g \in {}^{+}F_q^{+}$, которая в том же базисе $\alpha_1, \alpha_2, \alpha_3$ определяется набором координатных функций

$$\begin{aligned} g_1 &= x_{01} + x_{21} \cdot \ldots \cdot x_{2k+1,1} + x_{2k+3,1},\\ g_2 &= x_{02} + x_{11} \cdot \ldots \cdot x_{k1} + x_{2k+3,2},\\ g_3 &= x_{02} + x_{k+3,1} \cdot \ldots \cdot x_{2k+2,1} + x_{2k+3,3}. \end{aligned}$$

Согласно формулам (2) справедливы равенства

$$\begin{aligned} \operatorname{ind}_p f &= \max\{\deg f_1, \deg f_2, \deg f_3\} = 2,\\ \operatorname{ind}_p g &= \max\{\deg g_1, \deg g_2, \deg g_3\} = 2k. \end{aligned}$$

При этом нетрудно проверить, что степени координатных функций сдвиг-композиции $f \lhd g$ удовлетворяют соотношениям

$$\deg(f \lhd g)_1 = k + 1, \quad \deg(f \lhd g)_2 = k, \quad \deg(f \lhd g)_3 = k,$$

и следовательно, $\operatorname{ind}_p(f \lhd g) = k + 1$.

Рассмотренный пример наглядно демонстрирует, что величины

$$\operatorname{ind}_p f = \max\{\deg f_1, \ldots, \deg f_t\}, \quad \operatorname{ind}_p g = \max\{\deg g_1, \ldots, \deg g_t\}$$

невозможно использовать для точной оценки параметра $\operatorname{ind}_p(f \lhd g)$, поскольку значение $\operatorname{ind}_p(f \lhd g)$ зависит не от максимума степеней координатных функций f и g, а от сочетаний мономов этих координатных функций.

Кроме того, нетрудно видеть, что пример 4 опровергает возможность непосредственного продолжения результатов леммы 1 и утверждения 2 теоремы 2 (при $k = 1$) на случай непростого поля $\mathbb{F}_q$ при использовании параметра ind_p. С учетом отмеченного еще более неожиданным представляется тот факт, что утверждение 1 теоремы 2 допускает независимое обобщение на случай непростого поля $\mathbb{F}_q$.

Теорема 3. *Пусть* $q = p^t$, *где* p *– простое. Тогда для сдвиг-композиции* $f \lhd g$ *функций* $f \in {}^*F_q$ *и* $g \in {}^+F_q^*$ *равенство* $\operatorname{ind}_p(f \lhd g) = 1$ *выполняется в том и только том случае, когда* $\operatorname{ind}_p f = \operatorname{ind}_p g = 1$.

Доказательство. Содержательную часть доказательства утверждения представим в виде двух отдельных результатов, которые сами по себе представляют практический интерес.

Для удобства будем считать, что функции $f(x_0, \ldots, x_n)$ и $g(x_0, \ldots, x_m)$ имеют длины n и m соответственно.

Лемма 2. *Пусть* $q = p^t$. *Для произвольных* $f \in L_q^p$ *и* $g \in F_q$ *справедливы следующие утверждения*:

1. $\operatorname{ind}_p(f \lhd g) \leqslant \operatorname{ind}_p g$;
2. $\operatorname{ind}_p(g \lhd f) \leqslant \operatorname{ind}_p g$;
3. *Если к тому же* $f \in {}^*L_q^p$, *то* $\operatorname{ind}_p(g \lhd f) = \operatorname{ind}_p g = \operatorname{ind}_p(f \lhd g)$.

Доказательство. Доказательство утверждений 1 и 2 представляется очевидным при использовании представления функций f, g наборами координатных функций.

Докажем утверждение 3. Пусть

$$f(x_0, \ldots, x_n) = f_{00}x_0 + \ldots + f_{0,t-1}x_0^{p^{t-1}} + \ldots + f_{n0}x_n + \ldots + f_{n,t-1}x_n^{p^{t-1}},$$
$$g(x_0, \ldots, x_m) = \sum_{i_0, \ldots, i_m \in \overline{0,q-1}} c_{i_0 \ldots i_m} x_0^{i_0} \ldots x_m^{i_m}.$$

Условие $f \in {}^*L_q^p$ означает, что $\pi(x_0) = f_{00}x_0 + \ldots + f_{0,t-1}x_0^{p^{t-1}}$ – перестановочный p-линеаризованный многочлен. При этом очевидны разложения

$$f = f' \lhd \pi, \quad f = \pi \lhd f'', \quad f', f'' \in {}^+L_q^p.$$

Пусть $x_0^{j_0} \ldots x_m^{j_m}$ – наименьший относительно стандартного лексикографического порядка моном функции g со свойством

$$\operatorname{ind}_p g = \operatorname{ind}_p x_0^{j_0} \ldots x_m^{j_m} = \|j_0\|_p + \ldots + \|j_m\|_p, \quad c_{j_0 \ldots j_m} \neq 0.$$

Нетрудно понять, что приведенные многочлены функций $g \lhd f'$ и $f'' \lhd g$ также содержат одночлен $c_{j_0 \ldots j_m} x_0^{j_0} \ldots x_m^{j_m}$. Тогда с учетом утверждений 1 и 2 можно выписать следующие цепочки неравенств:

$$\operatorname{ind}_p g \leqslant \operatorname{ind}_p(g \lhd f') = \operatorname{ind}_p(g \lhd f \lhd \pi^{-1}) \leqslant \operatorname{ind}_p(g \lhd f) \leqslant \operatorname{ind}_p g,$$
$$\operatorname{ind}_p g \leqslant \operatorname{ind}_p(f'' \lhd g) = \operatorname{ind}_p(\pi^{-1} \lhd f \lhd g) \leqslant \operatorname{ind}_p(f \lhd g) \leqslant \operatorname{ind}_p g. \quad \blacktriangle$$

Легко видеть, что достаточность условия, сформулированного в теореме 3, следует из утверждения 3 доказанной леммы 2.

Для доказательства необходимости нам потребуется еще один вспомогательный результат.

Лемма 3. *Пусть* $q = p^t$, *где* p *– простое, а сдвиг-композиция функций* $f \in F_q$ *и* $g \in {}^+F_q^*$ *удовлетворяет условию* $\operatorname{ind}_p(f \lhd g) = 1$. *Тогда* $\operatorname{ind}_p f = 1$.

Доказательство. Если $\operatorname{ind}_p g = 1$, то по лемме 2 имеем $\operatorname{ind}_p f = \operatorname{ind}_p(f \lhd g) = 1$ – все доказано. Поэтому далее будем полагать, что $\operatorname{ind}_p g > 1$ и справедливо представление

$$g = x_0 + l_g(x_1, \ldots, x_{s-1}) + \varphi(x_s, \ldots, x_m),$$

в котором $\operatorname{ind}_p l_g = 1$, а функция φ существенным и p-нелинейным образом зависит от переменной x_s, $s \leqslant m$.

Доказательство проведем методом от противного. Предположим, что $\operatorname{ind}_p f > 1$. Представим функцию f в виде

$$f = l_f(x_0, \ldots, x_{r-1}) + \psi(x_r, \ldots, x_n),$$

где $\operatorname{ind}_p l_f = 1$, а функция

$$\psi(x_r, \ldots, x_n) = \sum_{i=0}^{q-1} x_r^i \psi_i(x_{r+1}, \ldots, x_n)$$

существенным и p-нелинейным образом зависит от переменной x_r, $r \leqslant n$.

Во введенных обозначениях рассмотрим соотношение $f \lhd g$ подробнее:

$$\begin{aligned} f \lhd g = {} & (l_f \lhd g)(x_0, \ldots, x_{r+m-1}) + \\ & + \sum_{i=0}^{q-1} \bigl(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\bigr)^i (\psi_i \lhd g)(x_{r+1}, \ldots, x_{n+m}), \end{aligned}$$

где

$$\tau(x_{r+1}, \ldots, x_{r+m}) = l_g(x_{r+1}, \ldots, x_{r+s-1}) + \varphi(x_{r+s}, \ldots, x_{r+m}).$$

Теперь заметим, что равенство $\operatorname{ind}_p(f \lhd g) = 1$ возможно только лишь в случае, когда функция $l_f \lhd g$ зависит p-линейным образом от переменных $x_0, \ldots, x_{r-1}$:

$$\begin{aligned} & (l_f \lhd g)\,(x_0, \ldots, x_{r+m-1}) = \\ & = l(x_0, \ldots, x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1}, \ldots, x_{r+m-1}), \quad \operatorname{ind}_p l = 1. \end{aligned}$$

Если $r = n$, то очевидно, что $\psi_i \in \mathbb{F}_q$ при всех $i \in \{0, \ldots, q-1\}$. Рассмотрим случай, когда $r < n$, и предположим, что существует такой $i \in \{1, \ldots, q-1\}$, для которого $\psi_i \notin \mathbb{F}_q$. Тогда выберем наибольшее k со свойством $\psi_k \notin \mathbb{F}_q$ и продолжим расписывать соотношение $f \lhd g$ подробнее:

$$\begin{aligned} f \lhd g = {} & l(x_0, \ldots, x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1}, \ldots, x_{r+m-1}) + \\ & + \sum_{i=0}^{k-1} \bigl(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\bigr)^i (\psi_i \lhd g)(x_{r+1}, \ldots, x_{n+m}) + \\ & + \bigl(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\bigr)^k (\psi_k \lhd g)(x_{r+1}, \ldots, x_{n+m}) + \\ & + \sum_{i=k+1}^{q-1} \bigl(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\bigr)^i \psi_i = \\ & = l(x_0, \ldots, x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1}, \ldots, x_{r+m-1}) + \\ & + \sum_{i=0}^{k-1} \bigl(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\bigr)^i (\psi_i \lhd g)(x_{r+1}, \ldots, x_{n+m}) + \end{aligned}$$

$$\begin{aligned}&+\sum_{i=0}^{k-1} x_r^i \binom{k}{i} \tau(x_{r+1},\ldots,x_{r+m})^{k-i}(\psi_k \lhd g)(x_{r+1},\ldots,x_{n+m}) +\\&+ x_r^k(\psi_k\lhd g)(x_{r+1},\ldots,x_{n+m}) + \sum_{i=0}^{q-1} x_r^i v_i(x_{r+1},\ldots,x_{r+m}).\end{aligned}$$

Из полученного представления $f \lhd g$ легко видеть, что равенство $\operatorname{ind}_p(f \lhd g) = 1$ с необходимостью влечет за собой включение

$$\varphi_k(x_{r+1},\ldots,x_{r+m-1}) + (\psi_k \lhd g)(x_{r+1},\ldots,x_{n+m}) + v_k(x_{r+1},\ldots,x_{r+m}) \in \mathbb{F}_q,$$

которое невозможно ввиду того, что

$$\begin{aligned}&\operatorname{len}\bigl(\varphi_k(x_{r+1},\ldots,x_{r+m-1}) + v_k(x_{r+1},\ldots,x_{r+m})\bigr) \leqslant m-1 <\\&< m = \operatorname{len} g \leqslant \operatorname{len}\psi_k + \operatorname{len} g = \operatorname{len}(\psi_k \lhd g)(x_{r+1},\ldots,x_{n+m}).\end{aligned}$$

Таким образом, показали, что независимо от $r \leqslant n$ для всех $i \in \{1,\ldots,q-1\}$ выполняется включение $\psi_i \in \mathbb{F}_q$, а сдвиг-композиция $f \lhd g$ на самом деле имеет вид

$$\begin{aligned}&f \lhd g = l(x_0,\ldots,x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1},\ldots,x_{r+m-1}) +\\&+ (\psi_0 \lhd g)(x_{r+1},\ldots,x_{n+m}) + \sum_{i=1}^{q-1} \psi_i\cdot\bigl(x_r + \tau(x_{r+1},\ldots,x_{r+m})\bigr)^i. \qquad (4)\end{aligned}$$

Поскольку функция f существенным и p-нелинейным образом зависит от переменной x_r, то существует такое $i \in \{1,\ldots,q-1\}$, что $\psi_i \neq 0$ и $\|i\|_p \neq 1$. Выберем наибольшее k, у которого $\psi_k \neq 0$ и $\|k\|_p$ – максимально возможный. Пусть $k = k_l p^l + \ldots + k_{t-1}p^{t-1}$, $k_l \geqslant 1$. Обозначим

$$\begin{aligned}&k^{(l)} = 0 + \ldots + 0 + k_l p^l + \ldots + k_{t-1}p^{t-1} = k,\\&k^{(l-1)} = 0 + \ldots + p^{l-1} + (k_l - 1)p^l + \ldots + k_{t-1}p^{t-1},\\&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\&k^{(0)} = p^0 + \ldots + 0 + (k_l - 1)p^l + \ldots + k_{t-1}p^{t-1},\\&k^{*} = 0 + \ldots + 0 + (k_l - 1)p^l + \ldots + k_{t-1}p^{t-1} \neq 0\end{aligned}$$

и выделим в сумме $\sum\limits_{i=1}^{q-1} \psi_i\cdot\bigl(x_r + \tau(x_{r+1},\ldots,x_{r+m})\bigr)^i$ коэффициент при $x_r^{k^*}$:

$$\begin{aligned}&\sum_{i=1}^{q-1} \psi_i\cdot\bigl(x_r + \tau(x_{r+1},\ldots,x_{r+m})\bigr)^i = \sum_{i=1}^{q-1} \psi_i\cdot(x_r+\tau)^{i_0 + p i_1 + \ldots + p^{t-1} i_{t-1}} =\\&= \sum_{i=1}^{q-1} \psi_i\cdot(x_r+\tau)^{i_0}\cdot(x_r^p+\tau^p)^{i_1}\cdot\ldots\cdot\Bigl(x_r^{p^{t-1}} + \tau^{p^{t-1}}\Bigr)^{i_{t-1}} =\\&= \psi_{k^{(l)}}\cdot\Bigl(x_r^{p^l} + \tau^{p^l}\Bigr)^{k_l}\cdot\ldots\cdot\Bigl(x_r^{p^{t-1}} + \tau^{p^{t-1}}\Bigr)^{k_{t-1}} +\\&+ \psi_{k^{(l-1)}}\cdot\Bigl(x_r^{p^{l-1}} + \tau^{p^{l-1}}\Bigr)\cdot\Bigl(x_r^{p^l} + \tau^{p^l}\Bigr)^{k_l - 1}\cdot\ldots\cdot\Bigl(x_r^{p^{t-1}} + \tau^{p^{t-1}}\Bigr)^{k_{t-1}} +\\&+ \ldots + \psi_{k^{(0)}}\cdot(x_r+\tau)\cdot\Bigl(x_r^{p^l} + \tau^{p^l}\Bigr)^{k_l - 1}\cdot\ldots\cdot\Bigl(x_r^{p^{t-1}} + \tau^{p^{t-1}}\Bigr)^{k_{t-1}} +\end{aligned}$$

$$\begin{aligned}
&+\psi_{k^*}\cdot\left(x_r^{p^l}+\tau^{p^l}\right)^{k_l-1}\cdot\ldots\cdot\left(x_r^{p^{t-1}}+\tau^{p^{t-1}}\right)^{k_{t-1}}+t(x_r,\ldots,x_{r+m})=\\
&=\psi_{k^{(l)}}\cdot\left(x_r^{k^{(l)}}+k_l x_r^{k^*}\tau^{p^l}+\ldots\right)+\psi_{k^{(l-1)}}\cdot\left(x_r^{k^{(l-1)}}+x_r^{k^*}\tau^{p^{l-1}}+\ldots\right)+\\
&+\ldots+\psi_{k^{(0)}}\cdot\left(x_r^{k^{(0)}}+x_r^{k^*}\tau^{p^0}+\ldots\right)+\psi_{k^*}\cdot\left(x_r^{k^*}+\ldots\right)+t(x_r,\ldots,x_{r+m})=\\
&=\psi_{k^{(l)}}x_r^{k^{(l)}}+\psi_{k^{(l-1)}}x_r^{k^{(l-1)}}+\ldots+\psi_{k^{(0)}}x_r^{k^{(0)}}+\\
&+\left(k_l\psi_{k^{(l)}}\cdot\tau^{p^l}+\psi_{k^{(l-1)}}\cdot\tau^{p^{l-1}}+\ldots+\psi_{k^{(0)}}\cdot\tau^{p^0}+\psi_{k^*}\right)x_r^{k^*}+v(x_r,\ldots,x_{r+m})=\\
&=\left(k_l\psi_{k^{(l)}}\cdot\tau^{p^l}+\psi_{k^{(l-1)}}\cdot\tau^{p^{l-1}}+\ldots+\psi_{k^{(0)}}\cdot\tau^{p^0}+\psi_{k^*}\right)x_r^{k^*}+w(x_r,\ldots,x_{r+m})
\end{aligned}$$

(здесь многочлены $t(x_r,\ldots,x_{r+m})$, $v(x_r,\ldots,x_{r+m})$ и $w(x_r,\ldots,x_{r+m})$ не содержат мономов с переменной x_r в степени k^*).

Теперь легко видеть, что условие $\mathrm{ind}_p(f\lhd g)=1$ накладывает на компоненты представления (4) следующее ограничение:

$$\varphi_{k^*}(x_{r+1},\ldots,x_m)+\left(k_l\psi_{k^{(l)}}x_0^{p^l}+\ldots+\psi_{k^{(0)}}x_0^{p^0}+\psi_{k^*}\right)\lhd\tau(x_{r+1},\ldots,x_{r+m})\in\mathbb{F}_q.$$

Однако данное включение невозможно ввиду того, что $k_l\psi_{k^{(l)}}\neq 0$ и $\tau\in F_q^*$, а следовательно, композиция

$$\left(k_l\psi_{k^{(l)}}x_0^{p^l}+\ldots+\psi_{k^{(0)}}x_0^{p^0}+\psi_{k^*}\right)\lhd\tau(x_{r+1},\ldots,x_{r+m})$$

существенным образом зависит от x_{r+m}.

Таким образом, $\psi_i\in\mathbb{F}_q$ для всех $i\in\{1,\ldots,q-1\}$ и неравенство $\psi_i\neq 0$ возможно только при $\|i\|_p=1$ – пришли к противоречию с тем, что функция ψ существенным и p-нелинейным образом зависит от переменной x_r. ▲

Теперь можно доказать необходимость условия, сформулированного в теореме 3.

Так как p – простое, то согласно доказанной лемме 3 из условия $\mathrm{ind}_p(f\lhd g)=1$ следует, что $\mathrm{ind}_p f=1$. А поскольку $f\in{}^*F_q$, то согласно утверждению 3 леммы 2 имеем равенство $\mathrm{ind}_p g=\mathrm{ind}_p(f\lhd g)=1$. ▲

Следствие 2. *При простом p регистр сдвига $R(\varphi,\psi)$ с p-линейной функцией обратной связи $\varphi\in{}^*(L_q^p)^+$ может допускать гомоморфизм на регистр сдвига $R(\varphi',\psi')$, $\varphi'\in{}^*F_q^+$, только если φ' – p-линейная; при этом данный гомоморфизм с необходимостью является p-линейным отображением.*

Доказательство очевидным образом следует из [2, теорема 1] и теоремы 3. ▲

Следствие 3. *Неавтономный линейный регистр сдвига с неприводимым характеристическим многочленом не допускает собственных гомоморфизмов на регулярные регистры сдвига, функции обратной связи которых линейны по входной переменной.*

Доказательство очевидным образом следует из [2, теорема 1], доказанной теоремы 3 и следствия 1. ▲

Замечание 3. Ранее отмечалось, что при простом p для произвольной функции $f\in F_q$ ее индекс p-нелинейности $\mathrm{ind}_p f$ совпадает с аддитивным показателем нелинейности $\mathrm{dl}\,f$. Следовательно, теорема 3 – центральный результат данного параграфа – допускает формулировку в терминах показателя dl, не зависящего от числа p. Таким образом, можно сделать вывод, что аддитивный показатель нелинейности при исследовании сдвиг-композиции является более органичным продолжением классического понятия нелинейности отображения deg на случай непростого поля $\mathbb{F}_q$ по сравнению с индексом p-нелинейности.

В заключение параграфа приведем ряд примеров, которые демонстрируют существенность каждого из условий теоремы 3 и леммы 3.

Пример 5. Пусть $q = p^2$ и $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Рассмотрим проекцию $\pi\colon \mathbb{F}_q \to \mathbb{F}_p$, определенную в базисе e, α по правилу

$$\pi(x_1 + x_2\alpha) = x_2.$$

Выберем произвольный нелинейный многочлен $\sigma \in \mathbb{F}_p[x_1, \ldots, x_n]$. Нетрудно понять, что функция $\varphi = \sigma \lhd \pi \in F_q$ в базисе e, α имеет координатные функции

$$\varphi_1(x_{11}, x_{12}, \ldots, x_{n1}, x_{n2}) = \sigma(x_{12}, \ldots, x_{n2}), \quad \varphi_2(x_{11}, x_{12}, \ldots, x_{n1}, x_{n2}) = 0,$$

и следовательно, выполняется равенство $\operatorname{ind}_p \varphi = \deg \sigma > 1$.

Сдвиг-композиция

$$\pi \lhd \big(x_0 + \varphi(x_1, \ldots, x_n) + x_{n+1}\big) = \pi(x_0) + \pi(x_{n+1})$$

доказывает существенность условия $f \in {}^*F_q$ в теореме 3.

Пример 6. В обозначениях примера 5 сдвиг-композиция

$$\begin{aligned}&\big(x_0 + \varphi(x_1, \ldots, x_n)\big) \lhd \big(x_0 - \varphi(x_1, \ldots, x_n)\big) = \\ &= x_0 - \sigma(x_{12}, \ldots, x_{n2}) + \sigma \lhd \pi\big(x_1 - \varphi(x_2, \ldots, x_{n+1})\big) = \\ &= x_0 - \sigma(x_{12}, \ldots, x_{n2}) + \sigma(x_{12}, \ldots, x_{n2}) = x_0\end{aligned}$$

подтверждает существенность условия $g \in F_q^*$ в лемме 3 и теореме 3.

Кроме того, данный пример показывает, что при составном q обратимые элементы множества ${}^+F_q$ могут иметь произвольные длину и степень нелинейности (см. следствие 2 в работе [3]).

Пример 7. Условие $g \in {}^+F_q$ в лемме 3 и теореме 3 нельзя заменить даже на близкое $g \in {}^*F_q$. Для любого $q > 2$ существует перестановочный полином $f(x_0) \in F_q$, $\operatorname{ind}_p f > 1$. Нетрудно понять, что обратный перестановочный полином $g(x_0)$ также удовлетворяет условию $\operatorname{ind}_p g > 1$. При этом справедливо равенство $f \lhd g = x_0$.

СПИСОК ЛИТЕРАТУРЫ

1. *Солодовников В.И.* Регистры сдвига и криптоалгоритмы на их основе: теоретико-автоматные свойства и их приложения. Saarbrücken: Lambert Acad. Publ., 2017.
2. *Солодовников В.И.* Гомоморфизмы регистров сдвига в линейные автоматы // Дискрет. матем. 2008. Т. 20. № 4. С. 89–101.
3. *Чередник И.В.* Линейное разложение дискретных функций в терминах операции сдвиг-композиции // Матем. вопр. криптогр. 2020. Т. 11. № 1. С. 115–143.
4. *Чередник И.В.* Линейное разложение системы дискретных функций в терминах операции сдвиг-композиции // Матем. вопр. криптогр. (в печати).
5. *Гольтваница М.А.* Методы построения скрученных линейных рекуррентных последовательностей максимального периода, базирующиеся на факторизации многочленов Галуа в кольце матричных многочленов // Матем. вопр. криптогр. 2019. Т. 10. № 4. С. 25–51.
6. *Башев В.А.* Теоретико-групповая характеризация неавтономных линейных регистров сдвига // Тр. по дискр. матем. Т. 8. М.: Физматлит, 2004. С. 52–68.
7. *Солодовников В.И.* Гомоморфизмы двоичных регистров сдвига // Дискрет. матем. 2005. Т. 17. № 1. С. 73–88.
8. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988.
9. *Кузьмин А.С., Нечаев А.А., Шишкин В.А.* Бент- и гипербент-функции над конечным полем // Тр. по дискр. матем. Т. 10. М.: Физматлит, 2007. С. 97–122.

10. *Черемушкин А.В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикл. дискр. матем. 2010. № 2 (8). С. 22–33.
11. *Черемушкин А.В.* Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка // Прикл. дискр. матем. 2013. № 2 (20). С. 26–38.
12. *Гольтваница М.А., Зайцев С.Н., Нечаев А.А.* Скрученные линейные рекурренты максимального периода над кольцами Галуа // Фундамент. и прикл. матем. 2012. Т. 17. № 3. С. 5–23.

Чередник Игорь Владимирович
МИРЭА – Российский технологический университет
(РТУ МИРЭА), Москва
`p.n.v.k.s@mail.ru`

Поступила в редакцию
04.06.2020
После доработки
07.11.2020
Принята к публикации
08.11.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.728

© 2020 г. **Л.А. Шоломов**

ПОЛИНОМИАЛЬНОЕ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНОЕ КОДИРОВАНИЕ НЕДООПРЕДЕЛЕННЫХ БЕРНУЛЛИЕВСКИХ ИСТОЧНИКОВ ОБЩЕГО ВИДА

Недоопределенный источник Бернулли порождает независимо с некоторыми вероятностями символы заданного недоопределенного алфавита. Каждому недоопределенному символу соответствует некоторое множество основных (полностью определенных) символов, любым из которых он может быть замещен (доопределен). Недоопределенный источник характеризуется энтропией, которая вводится неявно как минимум некоторой функции и играет роль, подобную роли энтропии Шеннона для полностью определенных источников. Кодирование недоопределенного источника должно обеспечить для всякой порождаемой им последовательности воспроизведение какого-либо ее доопределения. Кодирование асимптотически оптимально, если средняя длина кода асимптотически равна энтропии источника. Оно универсально, если не зависит от вероятностей символов источника. В статье описан метод асимптотически оптимального универсального кодирования недоопределенных источников Бернулли, для которого процедуры кодирования и декодирования реализуемы РАМ-программами почти линейной сложности.

Ключевые слова: недоопределенный источник, доопределение, энтропия недоопределенного источника, квазиэнтропия слова, комбинаторная энтропия класса, кодирование недоопределенного источника, универсальное кодирование, полиномиальный алгоритм.

DOI: `10.31857/S0555292320040075`

§ 1. Определения, постановка задачи и результат

С недоопределенными данными имеют дело во многих областях информатики – в задачах распознавания, хранения и обработки данных, управления, логического синтеза и др. Поэтому целесообразно отдельно исследовать свойства недоопределенных данных, разработать методы и алгоритмы эффективного обращения с ними. Некоторые результаты в этом направлении представлены в [1]. Настоящая статья посвящена теоретически эффективному сжатию недоопределенных данных.

Задан конечный алфавит $A_0 = \{a_i,\ i \in M\}$, $M = \{0, 1, \ldots, m-1\}$, *основных* символов. Каждому непустому $T \subseteq M$ соответствует символ a_T, называемый *недоопределенным. Доопределением символа* a_T считается всякий основной символ a_i, $i \in T$. Символ a_M, доопределимый любым основным символом, называется *неопределенным* и обозначается через $*$. Основные символы a_i можно также рассматривать как недоопределенные символы, соответствующие одноэлементным подмножествам $\{i\} \subseteq M$. Под *доопределением слова* v в алфавите A понимается любое слово в алфавите A_0, полученное из v заменой каждого символа каким-либо его доопределением.

Выделена система $\mathcal{T}$ некоторых непустых подмножеств T множества M, и с ней связан *недоопределенный алфавит* $A = A_{\mathcal{T}} = \{a_T,\ T \in \mathcal{T}\}$. Положим $k = \#A = \#\mathcal{T}$, где $\#$ означает мощность множества. В случае $A = A_0$ недоопределенный алфавит A называется *полностью определенным*, а при $A = A_0 \cup \{*\}$ – *частично определенным*. Будем рассматривать бернуллиевский источник X, порождающий (независимо) символы $a_T \in A$ с вероятностями p_T, $\sum\limits_{T \in \mathcal{T}} p_T = 1$. Он обозначается через (A, P), где $P = (p_T,\ T \in \mathcal{T})$, и называется *недоопределенным источником*. Если алфавит A полностью (частично) определен, будем говорить о полностью (частично) определенном источнике.

Задавшись набором вероятностей $Q = (q_i, i \in M)$, $\sum\limits_{i \in M} q_i = 1$, основных символов, введем функцию

$$\mathcal{H}(P, Q) = -\sum_{T \in \mathcal{T}} p_T \log \sum_{i \in T} q_i \tag{1}$$

(здесь и далее все логарифмы двоичные). *Энтропией источника* X назовем величину

$$\mathcal{H}(X) = \mathcal{H}(P) = \min_Q \mathcal{H}(P, Q). \tag{2}$$

Для полностью определенного источника в силу соотношения

$$\min_Q \left\{ -\sum_{i \in M} p_i \log q_i \right\} = -\sum_{i \in M} p_i \log p_i$$

она совпадает с энтропией Шеннона, а для частично определенного источника $X = (A_0 \cup \{*\}, P)$, $P = ((p_i,\ i \in M), p_*)$, представима [1] в виде

$$\mathcal{H}(X) = (1 - p_*) \log(1 - p_*) - \sum_{i \in M} p_i \log p_i \tag{3}$$

и достигается в (2) на наборе $Q = \left(\dfrac{p_0}{1 - p_*}, \ldots, \dfrac{p_{m-1}}{1 - p_*} \right)$.

Функция $\mathcal{H}(P)$ была введена (из эвристических соображений) в [2] в качестве меры неопределенности задач с несколькими ответами. Ее свойства изучены в работе [1]. Некоторые из них совпадают со свойствами энтропии Шеннона, некоторые получаются их модификацией, некоторые являются новыми.

Очевидно, что $\mathcal{H}(X) \geqslant 0$. Нас будет интересовать случай, когда энтропия источника $X = (A, P)$ строго положительна. Необходимым и достаточным для положительности энтропии является условие (см. [1], а также пункт 1° леммы 1 настоящей статьи)

$$\bigcap_{T\colon p_T > 0} T = \varnothing.$$

Будем рассматривать двоичное разделимое блоковое кодирование K недоопределенного источника X, использующее блоки длины n. Кодирование K должно обеспечить для всякого слова $v \in A^n$ возможность восстановления по его коду $K(v)$ какого-либо доопределения слова v. Кодирование источника (A, P) называется *универсальным* (при заданных A и n), если оно не зависит от набора вероятностей P.

Задачу кодирования недоопределенного источника можно рассматривать как специальный случай задачи кодирования с заданным критерием верности [3, 4], когда исходные сообщения в алфавите A должны быть воспроизведены в алфавите A_0, а искажение при воспроизведении символа a_i вместо a_T считается равным 0 при $i \in T$ и равным ∞ при $i \notin T$. Введенная выше энтропия $\mathcal{H}(X)$ оказалась эквивалентной [1] скорости как функции искажения (в другой терминологии – W-энтропии [5]) для этого случая. Более подробно связь кодирования недоопределенных данных и кодирования с заданным критерием верности рассмотрена в [6].

Качество кодирования K будем характеризовать *средней длиной кода*

$$\overline{\ell}_K^{(n)} = \frac{1}{n} \sum_{v \in A^n} p(v)|K(v)|, \tag{4}$$

приходящейся на символ источника. Здесь $p(v) = p_{T_1} \dots p_{T_n}$ – вероятность порождения источником X слова $v = a_{T_1} \dots a_{T_n}$, $|K(v)|$ – длина кодового слова для v.

В теории сложности принято считать процедуру эффективной, если ее сложность (число элементарных операций) не превосходит полинома от размера задачи. В качестве модели вычислений будем использовать РАМ-программу [7] с подходящим набором операций.

Основным результатом статьи является

Теорема. *Для любого недоопределенного источника X с положительной энтропией $\mathcal{H}(X)$ справедливы следующие утверждения*:

1) *При любом способе кодирования K справедливо неравенство*

$$\overline{\ell}_K^{(n)} \geqslant \mathcal{H}(X);$$

2) *Имеется метод K универсального кодирования с оценкой*

$$\overline{\ell}_K^{(n)} \leqslant \mathcal{H}(X) + O\left(\frac{\log\log n}{\log^{1/2} n}\right),$$

для которого кодирование и декодирование реализуемы РАМ-программами сложности $n^{1+o(1)}$.

Возможность асимптотически оптимального универсального кодирования недоопределенного источника общего вида была установлена в [8] методом случайного кодирования. В [9] для решения этой задачи предложена модификация метода арифметического кодирования, использующая случайные последовательности, которая также неэффективна.

В работе [10] описан метод асимптотически оптимального универсального кодирования частично определенных источников, реализуемый РАМ-программами почти линейной сложности. Но он требует многократного вычисления (для различных фрагментов кодируемых слов) энтропии и минимизирующего правую часть в (2) набора Q. В случае частично определенных источников это не вызывает трудностей, поскольку их энтропия и минимизирующий набор выразимы в явном виде (3). Недоопределенные источники общего вида требуют применения приближенных методов. При этом возникают определенные технические трудности, связанные с оценкой необходимой точности и трудоемкости ее достижения. Отметим, что в [11, Добавление] описана сходящаяся итеративная процедура вычисления минимизирующего набора, но скорость ее сходимости не установлена, и это не позволяет использовать ее для оценки трудоемкости кодирования.

В предлагаемой статье развит подход, дающий возможность избежать вычисления энтропии и минимизирующего набора и решить задачу кодирования недоопределенных источников общего вида с теми же оценками средней длины кода и сложности, что и в [10] для частично определенных источников.

Последующая часть статьи посвящена доказательству утверждения 2) теоремы. Доказательство утверждения 1) содержится в [1]. В курсе лекций [12] оценка утверждения 1) распространена на недоопределенные стационарные источники.

Приведем некоторые другие результаты, имеющие отношение к настоящей статье.

Код слова можно воспринимать как (двоичную) программу вычисления слова некоторым алгоритмом (см. классическую работу Колмогорова [13]). Если слово двоичное, то занумеровав его разряды двоичными числами, придем к булевой функции, выражающей зависимость разрядов слова от их двоичных номеров, и в качестве кода слова можно использовать двоичную запись программы вычисления этой функции. Конструктивный подход, связывающий задачи вычисления булевых функций с задачами их специального (локального) кодирования, предложен в [14].

Ряд методов исследования и сжатия недоопределенных данных возник при решении задач реализации недоопределенных булевых функций различными вычислительными средствами. Их обсуждение (с указанием авторства) имеется в работе [15], содержащей решение задачи асимптотически наилучшей реализации булевых функций с заданными числами нулевых, единичных и неопределенных значений. Свойства энтропии $\mathcal{H}(P)$ были впервые изучены в связи с задачей реализации систем недоопределенных булевых функций [11].

Метод кодирования недоопределенных слов, представленный в настоящей статье, использует некоторые подходы, разработанные при синтезе схем. Идея кодирования слова путем разбиения на короткие подслова и совместного кодирования подслов является модификацией идеи Шеннона из метода синтеза контактных схем [16]. Важную роль играет техника Нечипорука [17,18] работы с частично определенными данными, изложенная им применительно к задачам реализации булевых функций и матриц некоторыми типами схем.

Одними из центральных вопросов для настоящей статьи являются вопросы сложности кодирования. В известных исследованиях по схемной реализации недоопределенных функций вопросы трудоемкости методов построения схем фактически не рассматривались. Некоторое исключение составляет работа [19], в которой изложен почти квадратичный по трудоемкости метод построения асимптотически наилучших двоичных программ вычисления частичных булевых функций с заданной областью определения.

Как уже отмечалось, задача кодирования недоопределенных данных тесно связана с задачей кодирования с заданным критерием верности [4,20]. Близкие к сжатию недоопределенных данных постановки играют важную роль в задачах поиска информации с применением хеш-функций [21] и в задачах дерандомизации алгоритмов с использованием генераторов протыкающих множеств [22,23].

§ 2. Квазиэнтропия и комбинаторная энтропия недоопределенных данных

Дальше считаем, что алфавит A содержит символ $* = a_M$. Если его там изначально нет, добавим, приписав вероятность 0. При этом слова, содержащие символ $*$, будут иметь нулевую вероятность и не повлияют на среднюю длину кода.

Свойства энтропии $\mathcal{H}(P)$ изучены в [1]. Сформулируем и докажем те из них, которые понадобятся в настоящей статье.

Лемма 1. *Справедливы следующие утверждения*:

1°. *Функция $\mathcal{H}(P)$ неотрицательна, причем*

$$\mathcal{H}(P) = 0 \iff \bigcap_{T\colon p_T > 0} T \neq \varnothing.$$

2°. *Имеет место оценка*

$$\mathcal{H}(P) \leqslant \log m - \sum_{1 \leqslant i \leqslant m} p^{(i)} \log i,$$

где $p^{(i)} = \sum\limits_{T\colon \#T = i} p_T$ *– вероятность символов, имеющих i доопределений.*

3°. *Функция $\mathcal{H}(P)$ вогнута, т.е. для любых P, P' и θ, $0 \leqslant \theta \leqslant 1$,*

$$\mathcal{H}(\theta P + (1-\theta)P') \geqslant \theta\mathcal{H}(P) + (1-\theta)\mathcal{H}(P').$$

4°. *Если источник $X' = (A', P')$ образован из $X = (A, P)$ исключением неопределенного символа и нормировкой вероятностей, т.е. $A' = A \setminus \{*\}$, $P' = (p'_T,$ $T \in \mathcal{T} \setminus \{M\})$, $p'_T = \dfrac{p_T}{1-p_*}$, то*

$$\mathcal{H}(P) = (1-p_*)\mathcal{H}(P'). \tag{5}$$

Доказательство. 1°. Неотрицательность очевидна. Пусть минимум $\mathcal{H}(P, Q)$ в (2) достигается на наборе Q^0. Положим $T^0 = \{i \in M \mid q_i^0 > 0\}$. Если $\mathcal{H}(P) = \mathcal{H}(P, Q^0) = 0$, то для любого T с $p_T > 0$ выполнено $\sum\limits_{i \in T} q_i^0 = 1$, а потому T включает T^0, и пересечение всех таких T непусто. Обратно, если пересечение непусто, то назначив $q_i = 1$ для некоторого i из этого пересечения и $q_j = 0$ для всех $j \neq i$, получим набор Q, для которого $\mathcal{H}(P, Q) = 0$.

2°. Вычислим $\mathcal{H}(P, Q)$ на наборе $Q_0 = (1/m, \ldots, 1/m)$. Имеем

$$\mathcal{H}(P) \leqslant \mathcal{H}(P, Q_0) = -\sum_T p_T \log \frac{\#T}{m} = \log m - \sum_i \sum_{\#T = i} p_T \log i = \\ = \log m - \sum_i p^{(i)} \log i.$$

3°. Пусть минимум функции $\mathcal{H}(\theta P + (1-\theta)P', Q)$ достигается на наборе Q. Тогда

$$\mathcal{H}(\theta P + (1-\theta)P') = -\theta \sum_T p_T \log \sum_{i \in T} q_i - (1-\theta) \sum_T p'_T \log \sum_{i \in T} q_i \geqslant \\ \geqslant \theta\mathcal{H}(P) + (1-\theta)\mathcal{H}(P').$$

4°. Для любого набора вероятностей $Q = (q_i,\ i \in M)$ выполнено $\log \sum\limits_{i \in M} q_i = 0$, поэтому

$$-\sum_{T \subseteq M} p_T \log \sum_{i \in T} q_i = -(1-p_*) \sum_{T \subset M} \frac{p_T}{1-p_*} \log \sum_{i \in T} q_i.$$

Взяв минимум по Q, получаем нужное утверждение. ▲

Отметим, что выражение (3) для энтропии частично определенного источника X вытекает из пункта 4° с учетом того, что источник X' в этом случае полностью определен и его энтропия совпадает с энтропией Шеннона.

Для слова $v \in A^n$ обозначим через $r_T(v)$ число появлений в нем символа a_T, $\sum\limits_{T \in \mathcal{T}} r_T(v) = |v|$, и положим $\boldsymbol{r}(v) = (r_T(v),\ T \in \mathcal{T})$. *Квазиэнтропией слова v* назовем величину

$$h(v) = |v|\,\mathcal{H}\left(\frac{\boldsymbol{r}(v)}{|v|}\right).$$

В силу (1), (2) она может быть переписана в виде

$$h(v) = \min_Q \left\{ -\sum_{T \in \mathcal{T}} r_T(v) \log \sum_{i \in T} q_i \right\}. \tag{6}$$

Следующая лемма содержит необходимые для дальнейшего свойства квазиэнтропии слов.

Лемма 2. *Справедливы следующие утверждения*:

1°. *Имеет место неравенство* $h(v) \leqslant |v| \log m$.

2°. *Если наборы* $\boldsymbol{r}(v_1)$ *и* $\boldsymbol{r}(v_2)$ *различаются лишь в компоненте* $r_*(\cdot)$, *то* $h(v_1) = h(v_2)$.

3°. *Квазиэнтропия конкатенации* v_1v_2 *удовлетворяет неравенству* $h(v_1v_2) \geqslant h(v_1) + h(v_2)$.

4°. *Если слово* v' *образовано из слова* v *приписыванием некоторого символа, то* $h(v') \leqslant h(v) + \log|v| + 2$.

Доказательство. 1°. Из пункта 2° леммы 1 получаем неравенство $\mathcal{H}(P) \leqslant \log m$, которое умножением обеих частей на $|v|$ приводит к нужному утверждению.

2°. Обозначим через v_1' и v_2' слова, полученные из v_1 и v_2 удалением символов $*$. Имеем $|v_1'| = |v_1| - r_*(v_1) = |v_2| - r_*(v_2) = |v_2'|$ и $\boldsymbol{r}(v_1') = \boldsymbol{r}(v_2')$, а потому $h(v_1') = h(v_2')$. Из пункта 4° леммы 1 при $p_T = \dfrac{r_T(v_1)}{|v_1|}$ с учетом равенства $1 - \dfrac{r_*(v_1)}{|v_1|} = \dfrac{|v_1'|}{|v_1|}$ выводим

$$\mathcal{H}\left(\frac{\boldsymbol{r}(v_1)}{|v_1|}\right) = \frac{|v_1'|}{|v_1|}\mathcal{H}\left(\frac{\boldsymbol{r}(v_1')}{|v_1'|}\right).$$

Домножая обе части на $|v_1|$, приходим к равенству $h(v_1) = h(v_1')$. Аналогично доказывается, что $h(v_2) = h(v_2')$. Отсюда и из $h(v_1') = h(v_2')$ получаем $h(v_1) = h(v_2)$.

3°. Воспользуемся вогнутостью энтропии (пункт 3° леммы 1) при $P = \dfrac{\boldsymbol{r}(v_1)}{|v_1|}$, $P' = \dfrac{\boldsymbol{r}(v_2)}{|v_2|}$ и $\theta = \dfrac{|v_1|}{|v_1| + |v_2|}$. Имеем

$$\frac{|v_1|}{|v_1| + |v_2|}\mathcal{H}\left(\frac{\boldsymbol{r}(v_1)}{|v_1|}\right) + \frac{|v_2|}{|v_1| + |v_2|}\mathcal{H}\left(\frac{\boldsymbol{r}(v_2)}{|v_2|}\right) \leqslant \mathcal{H}\left(\frac{\boldsymbol{r}(v_1) + \boldsymbol{r}(v_2)}{|v_1| + |v_2|}\right) = \mathcal{H}\left(\frac{\boldsymbol{r}(v_1v_2)}{|v_1v_2|}\right).$$

Домножая обе части на $|v_1| + |v_2| = |v_1v_2|$, получаем $h(v_1) + h(v_2) \leqslant h(v_1v_2)$.

4°. Пусть $v' = va_{T'}$. Обозначим через $Q = (q_i,\ i \in M)$ набор, на котором в (6) достигается квазиэнтропия $h(v)$. Возьмем некоторое $s \in T'$ и образуем набор $Q' = (q_i',\ i \in M)$, положив

$$q_s' = \frac{(|v| - 1)q_s}{|v|} + \frac{1}{|v|}, \quad q_i' = \frac{(|v| - 1)q_i}{|v|}, \quad i \neq s.$$

Набор Q' удовлетворяет условию

$$\sum_{i \in M} q_i' = \frac{|v| - 1}{|v|}\sum_{i \in M} q_i + \frac{1}{|v|} = \frac{|v| - 1}{|v|} + \frac{1}{|v|} = 1.$$

С учетом этого имеем

$$\begin{aligned} h(v') &\leqslant -\sum_{T \in \mathcal{T}} r_T(v') \log \sum_{j \in T} q_j' = -\sum_{T \in \mathcal{T}} r_T(v) \log \sum_{j \in T} q_j' - \log \sum_{j \in T'} q_j' \leqslant \\ &\leqslant -\sum_{T \in \mathcal{T}} r_T(v) \log \sum_{j \in T} \frac{|v| - 1}{|v|} q_j - \log \frac{1}{|v|} = \\ &= -\sum_{T \in \mathcal{T}} r_T(v) \log \sum_{j \in T} q_j - |v| \log \frac{|v| - 1}{|v|} + \log|v| = \\ &= h(v) - |v| \log\left(1 - \frac{1}{|v|}\right) + \log|v|. \end{aligned}$$

Принимая во внимание, что при $|v| \geqslant 2$

$$-|v|\log\left(1-\frac{1}{|v|}\right) \leqslant -|v|\left(-\frac{1}{|v|}-\frac{1}{2|v|^2}\right)\log e = \left(1+\frac{1}{2|v|}\right)\log e \leqslant \frac{5}{4}\log e \leqslant 2,$$

приходим к оценке пункта 4°. ▲

Для заданного набора $\boldsymbol{r} = (r_T,\ T \in \mathcal{T})$ натуральных чисел положим

$$\ell = \sum_{T\in\mathcal{T}} r_T$$

и обозначим через $\mathcal{K}_\ell(\boldsymbol{r})$ класс всех слов длины ℓ в алфавите A, в которых символы $a_T \in A$ встречаются r_T раз (с частотой r_T/ℓ). Такие классы называют *частотными.* Все слова $v \in \mathcal{K}_\ell(\boldsymbol{r})$ имеют одинаковую квазиэнтропию $h(v) = \ell\mathcal{H}(\boldsymbol{r}/\ell)$, которую будем обозначать через $h_\ell(\boldsymbol{r})$ и называть *квазиэнтропией класса* $\mathcal{K}_\ell(\boldsymbol{r})$.

Пусть задано конечное множество V недоопределенных слов в алфавите A. Будем говорить, что некоторое *множество слов* в алфавите A_0 образует *доопределение множества* V, если в нем найдется доопределение каждого слова из V. Обозначим через $N(V)$ минимальную мощность множества, доопределяющего V. Величину $\log N(V)$ будем называть *комбинаторной энтропией* множества слов V.

Будем считать, что все слова из V имеют одинаковую длину ℓ. Для доопределения множества слов V может быть использована *градиентная процедура* (жадный алгоритм). Ее удобно описывать в терминах таблицы, строки которой соответствуют словам $v \in V$, столбцы – словам $w \in A_0^\ell$, а в клетке (v, w) содержится 1 либо 0 в зависимости от того, доопределяет w слово v или нет. Будем считать, что столбцы упорядочены в соответствии с лексикографическим упорядочением слов множества A_0^ℓ. Градиентная процедура реализуется в виде последовательности шагов, на каждом из которых в таблице, полученной после предыдущего шага, выбирается первый столбец с наибольшим числом единиц и вычеркивается вместе со строками, содержащими в нем единицы. Совокупность столбцов, выбранных к моменту, когда все строки окажутся вычеркнутыми, задает доопределяющее множество для V. Оно определено однозначно; его мощность обозначим через $N^G(V)$.

При $V = \mathcal{K}_\ell(\boldsymbol{r})$ вместо записей $N(\mathcal{K}_\ell(\boldsymbol{r}))$ и $N^G(\mathcal{K}_\ell(\boldsymbol{r}))$ будем использовать $N_\ell(\boldsymbol{r})$ и $N_\ell^G(\boldsymbol{r})$. Величина $\log N_\ell^G(\boldsymbol{r})$ оценивает сверху комбинаторную энтропию $\log N_\ell(\boldsymbol{r})$ класса $\mathcal{K}_\ell(\boldsymbol{r})$.

Всюду дальше буквами C с индексами и (или) пометками обозначаются некоторые константы, абсолютные или зависящие от мощностей m и k алфавитов A_0 и A. При необходимости они могут быть указаны явно.

Лемма 3. *Имеют место оценки*

$$h_\ell(\boldsymbol{r}) - C_1\log\ell \leqslant \log N_\ell^G(\boldsymbol{r}) \leqslant h_\ell(\boldsymbol{r}) + C_2\log\ell.$$

Доказательство. В работе [8] (см. также [1]) с использованием метода случайного кодирования получены оценки комбинаторной энтропии частотного класса $\mathcal{K}_\ell(\boldsymbol{r})$

$$h_\ell(\boldsymbol{r}) - C_1\log\ell \leqslant \log N_\ell(\boldsymbol{r}) \leqslant h_\ell(\boldsymbol{r}) + C_1'\log\ell. \tag{7}$$

Воспользуемся результатом из [24] (см. также [25]) о точности градиентного алгоритма. Применительно к данному случаю он приобретает вид

$$N_\ell^G(\boldsymbol{r}) \leqslant N_\ell(\boldsymbol{r})\left(1+\ln\frac{\#\mathcal{K}_\ell(\boldsymbol{r})}{N_\ell(\boldsymbol{r})}\right)$$

и дает

$$N_\ell^G(\boldsymbol{r}) \leqslant N_\ell(\boldsymbol{r}) \ln(\#\mathcal{K}_\ell(\boldsymbol{r})) \leqslant N_\ell(\boldsymbol{r})\, \ell \ln k.$$

Отсюда и из (7) получаем верхнюю оценку

$$\log N_\ell^G(\boldsymbol{r}) \leqslant h_\ell(\boldsymbol{r}) + C_1' \log \ell + \log \ell + \log \ln k \leqslant h_\ell(\boldsymbol{r}) + C_2 \log \ell.$$

Нижняя оценка следует из (7) и неравенства $N_\ell(\boldsymbol{r}) \leqslant N_\ell^G(\boldsymbol{r})$. ▲

Будем рассматривать также t-*ограниченную* градиентную процедуру доопределения множества V, где t – заданный натуральный параметр. Она реализуется в соответствии с предыдущим описанием и считается *результативной*, если завершается не более чем за t шагов. В противном случае, если после t шагов остались невычеркнутые строки, процедура прерывается *безрезультатно*.

Лемма 4. *Если t-ограниченная градиентная процедура доопределения класса $\mathcal{K}_\ell(\boldsymbol{r})$ завершается результативно, то*

$$h_\ell(\boldsymbol{r}) \leqslant \log t + C_1 \log \ell,$$

а если безрезультатно, то

$$h_\ell(\boldsymbol{r}) \geqslant \log t - C_2 \log \ell.$$

Доказательство. Установим первое соотношение, второе доказывается аналогично. Если процедура завершилась результативно, то справедливо неравенство $N_\ell^G(\boldsymbol{r}) \leqslant t$, а потому в силу леммы 3 выполнено $\log t \geqslant \log N_\ell^G(\boldsymbol{r}) \geqslant h_\ell(\boldsymbol{r}) - C_1 \log \ell$, откуда $h_\ell(\boldsymbol{r}) \leqslant \log t + C_1 \log \ell$. ▲

§ 3. Кодирование

Алфавиты A_0, A и длину n блоков считаем заданными.

Будем говорить, что слово w в алфавите A_0 *обобщенно доопределяет* слово u в алфавите A, если $|u| \leqslant |w|$ и начало длины $|u|$ слова w доопределяет u. Метод кодирования недоопределенных слов $v \in A^n$ использует некоторый натуральный параметр $\lambda = \lambda(n)$ и некоторое множество $\mathcal{D}$, $\mathcal{D} \subseteq A_0^\lambda$, *допустимых обобщенных доопределений*. Они будут указаны позже, а пока потребуем лишь, чтобы для каждого символа $a_i \in A_0$ в $\mathcal{D}$ имелось слово, начинающееся с a_i. Пусть $\mathcal{D} = \{w_1, w_2, \dots, w_d\}$, где $d = \#\mathcal{D}$ и слова w_s упорядочены лексикографически.

Для каждого $v \in A^n$ кодовое слово будет иметь вид $K(v) = K_0\, K_1(v)$, где подслово K_0, одинаковое для всех v, называется *справочной частью* кодового слова, а $K_1(v)$ – его *основной частью*. Опишем способ их построения.

При кодировании слова $v \in A^n$ от него последовательно отрезаются слева подслова $v_1, v_2, \dots$ максимально возможной длины, имеющие в множестве $\mathcal{D}$ обобщенные доопределения. Условие, наложенное на множество $\mathcal{D}$, гарантирует, что процедура не прервется, пока слово v не будет исчерпано. Полученные подслова v_i будем называть *фрагментами* слова v. Если число фрагментов равно $t = t(v)$, то $v = v_1 v_2 \dots v_t$.

Доопределение фрагмента v_i может быть задано парой чисел (s_i, ℓ_i), где s_i – наименьшее s, при котором слово w_s обобщенно доопределяет v_i, а ℓ_i – длина фрагмента v_i. Положим $\alpha = \lceil \log d \rceil$, $\beta = \lceil \log \lambda \rceil$, где $\lceil x \rceil$ означает наименьшее целое, не меньшее числа x, и фрагменту v_i сопоставим слово (код) $K(v_i) = \widetilde{s}_i^{(\alpha)} \widetilde{\ell}_i^{(\beta)}$, где для натуральных чисел q и γ, $\gamma \geqslant \log(q+1)$, через $\widetilde{q}^{(\gamma)}$ обозначена γ-разрядная двоичная запись числа q. Основная часть кодового слова $K(v)$ образуется путем приписывания друг к другу кодов фрагментов

$$K_1(v) = K(v_1) \dots K(v_t) = \widetilde{s}_1^{(\alpha)} \widetilde{\ell}_1^{(\beta)} \dots \widetilde{s}_t^{(\alpha)} \widetilde{\ell}_t^{(\beta)}. \tag{8}$$

Отметим, что указанное кодирование фрагментов обладает полезным свойством равномерности по выходу: фрагменты v_i могут иметь разную длину, но кодируются двоичными словами $K(v_i)$ одинаковой длины $\alpha+\beta$.

Справочная часть K_0 кодирует множество $\mathcal{D}$. Она содержит двоичные представления его параметров λ и d и двоичные представления входящих в него слов w_s. Для представления натурального числа q используется двоичное слово $\widehat{q} = q_1q_1\ldots q_rq_r01$, где $\overline{q_1\ldots q_r}$ – двоичная запись числа q минимальной длины. Такое представление чисел позволяет по слову $\widehat{q}u$, где u – некоторое двоичное слово, однозначно восстановить q и u. Очевидно, что

$$|\widehat{q}| \leqslant 2(\log q + 2). \tag{9}$$

Слово $w_s \in \mathcal{D} \subseteq A_0^{\lambda}$ будем представлять двоичным словом $\widetilde{w}_s$ длины $m\lambda$, полученным из w_s заменой символов a_i, $i = 0, 1, \ldots, m-1$, словами $0\ldots010\ldots0$ длины m, содержащими 1 в разряде i. Справочная часть имеет вид

$$K_0 = \widehat{\lambda}\widehat{d}\widetilde{w}_1\ldots\widetilde{w}_d. \tag{10}$$

Лемма 5. *При любом выборе множества $\mathcal{D}$ обобщенных доопределений описанное кодирование слов $v \in A^n$ разделимо* (*префиксно*) *и позволяет восстановить по коду $K(v)$ слова v некоторое его доопределение.*

Доказательство. Опишем способ декодирования. Пусть имеется двоичное слово, начинающееся с кодового слова $K(v) = K_0\,K_1(v)$. Отрежем от него подслова $\widehat{\lambda}$ и $\widehat{d}$ и по ним найдем параметры λ, d, α и β. Затем отрежем d подслов длины $m\lambda$. Они соответствуют словам $\widetilde{w}_s$ и позволяют найти слова w_s множества $\mathcal{D}$. Далее от оставшейся части слова будем последовательно отрезать подслова длины $\alpha+\beta$. Они являются кодами $K(v_i) = \widetilde{s}_i^{(\alpha)}\widetilde{\ell}_i^{(\beta)}$ фрагментов v_i и задают доопределения u_i этих фрагментов. Процедура завершится после того, как при некотором t длина слова $u_1\ldots u_t$ окажется равной n. Это слово доопределяет v.

Префиксность кода следует из того, что по двоичной последовательности, начинающейся с кодового слова, это слово находится однозначно. ▲

Качество кодирования зависит от выбора множества $\mathcal{D}$. Будем использовать следующий способ построения этого множества. Зададимся некоторыми натуральными параметрами $\lambda = \lambda(n)$ и $\tau = \tau(n)$, удовлетворяющими условию

$$\log\lambda = o(\tau). \tag{11}$$

При этих λ и τ к каждому частотному классу $\mathcal{K}_\lambda(\boldsymbol{r})$ применим 2^τ-ограниченную градиентную процедуру и обозначим через $\mathcal{D}_{\lambda,\tau}$ объединение полученных доопределений для всех классов $\mathcal{K}_\lambda(\boldsymbol{r})$, в применении к которым процедура завершилась результативно. В качестве $\mathcal{D}$ возьмем множество $\mathcal{D}_{\lambda,\tau}$.

Оценим мощность $d = d_{\lambda,\tau}$ множества $\mathcal{D}_{\lambda,\tau}$. Для всякого класса $\mathcal{K}_\lambda(\boldsymbol{r})$, для которого 2^τ-ограниченная градиентная процедура завершилась результативно, мощность доопределяющего множества не превосходит 2^τ. Число таких классов не больше общего числа частотных классов в A^λ, которое не превышает $\binom{\lambda+k-1}{k-1}$, где $k = \#A$. Поэтому

$$d \leqslant (\lambda+k-1)^{k-1}2^\tau \leqslant \lambda^{C_3}2^\tau. \tag{12}$$

При этом параметры $\alpha = \lceil\log d\rceil$ и $\beta = \lceil\log\lambda\rceil$ будут удовлетворять оценкам

$$\alpha \leqslant \tau + C_3\log\lambda, \quad \beta \leqslant \log\lambda + 1. \tag{13}$$

Без ограничения общности можно считать, что 2^τ не превосходит числа m^λ столбцов градиентной таблицы, а потому

$$\tau \leqslant \lambda \log m. \tag{14}$$

Приведем некоторые предварительные (не совсем строгие) соображения, объясняющие выбор $\mathcal{D}_{\lambda,\tau}$ в качестве множества допустимых обобщенных доопределений. Из леммы 4 при $t = 2^\tau$ вытекает, что квазиэнтропия фрагментов v_i слова v не превышает величины $\tau + C_1 \log \lambda$, которая в силу условия (11) асимптотически равна τ. При этом, вследствие максимальности отрезаемых фрагментов, их квазиэнтропия в типичном случае окажется асимптотически равной τ. Длина $\alpha + \beta$ кода фрагментов, асимптотически равная τ в силу (13), будет в типичном случае асимптотически минимальной, что приведет к асимптотически наилучшему кодированию источника. Далее, если назначить параметр λ удовлетворяющим условию $\lambda = o(\log n)$, то сложность построения множества $\mathcal{D}_{\lambda,\tau}$ составит $n^{o(1)}$, а кодирование и декодирование слова v при заданном явно множестве $\mathcal{D}_{\lambda,\tau}$ будут выполнимы с трудоемкостью $n^{1+o(1)}$.

§ 4. Длина кодовых слов

Лемма 6. *Длина справочной части кода удовлетворяет оценке*

$$|K_0| \leqslant \lambda^{C_4} 2^\tau. \tag{15}$$

Доказательство. Воспользуемся представлением (10). Все слова $\widetilde{w}_s$ имеют длину $m\lambda$, а потому в силу (9) и (12)

$$|K_0| \leqslant 2(\log\lambda + 2) + 2(C_3 \log\lambda + \tau + 2) + \lambda^{C_3} 2^\tau m\lambda \leqslant \lambda^{C_4} 2^\tau. \quad \blacktriangle$$

Лемма 7. *Длина основной части $K_1(v)$ кодового слова для $v \in A^n$ удовлетворяет оценке*

$$|K_1(v)| \leqslant h(v) + n\biggl(\frac{C_6 \log\lambda}{\tau - C_5 \log\lambda} + \frac{\tau + C_6 \log\lambda}{\lambda}\biggr) + \tau, \tag{16}$$

где $h(v)$ – квазиэнтропия слова v.

Доказательство. Будем говорить, что фрагмент v_i слова v имеет тип 1, если $|v_i| < \lambda$, и тип 2, если $|v_i| = \lambda$. Числа фрагментов типа 1 и типа 2 в слове v обозначим, соответственно, через t_1 и t_2. Очевидно,

$$t_2 \leqslant \frac{n}{\lambda}. \tag{17}$$

Оценим t_1. Пусть v_i – фрагмент типа 1, не являющийся заключительным в слове v, а a_T – следующий за ним символ слова v. Образуем слово $v' = v_i a_T * \ldots *$ длины λ путем приписывания к слову $v_i a_T$ подходящего числа символов $*$. Слово $v_i a_T$ в силу максимальности фрагмента v_i не имеет обобщенных доопределений в классе $\mathcal{D}_{\lambda,\tau}$, а потому слово v' не доопределимо в этом классе. Это означает, что 2^τ-ограниченная процедура доопределения в применении к частотному классу $\mathcal{K}_\lambda(\boldsymbol{r}')$, содержащему слово v', закончилась безрезультатно, а потому в силу леммы 4

$$h(v') = h_\lambda(\boldsymbol{r}') \geqslant \tau - C_2 \log\lambda.$$

Слово v' образовано из $v_i a_T$ добавлением символов $*$, и в соответствии с пунктом 2° леммы 2 выполнено

$$h(v_i a_T) = h(v') \geqslant \tau - C_2 \log\lambda.$$

Воспользовавшись пунктом 4° леммы 2, получаем

$$h(v_i) \geqslant h(v_i a_T) - \log|v_i| - 2 \geqslant \tau - (C_2+1)\log\lambda - 2 \geqslant \tau - C_5 \log\lambda.$$

Пункт 3° леммы 2 и это неравенство приводят к оценке

$$h(v) = h(v_1 \dots v_t) \geqslant \sum_{1 \leqslant i \leqslant t} h(v_i) \geqslant \sum_{i\colon i<t, |v_i|<\lambda} h(v_i) \geqslant (t_1 - 1)(\tau - C_5 \log\lambda),$$

из которой следует соотношение

$$t_1 \leqslant \frac{h(v)}{\tau - C_5 \log\lambda} + 1.$$

Оно в сочетании с (17) дает оценку числа t фрагментов v_i в слове v:

$$t = t_1 + t_2 \leqslant \frac{h(v)}{\tau - C_5 \log\lambda} + \frac{n}{\lambda} + 1. \tag{18}$$

Оценим длину $|K_1(v)|$ основной части кодового слова. Из представления (8) следует, что $|K_1(v)| = t(\alpha + \beta)$. Подставляя сюда (18) и оценку $\alpha + \beta \leqslant \tau + C' \log\lambda$, вытекающую из (13), получаем

$$|K_1(v)| \leqslant \frac{h(v)(\tau + C'\log\lambda)}{\tau - C_5 \log\lambda} + \frac{n(\tau + C'\log\lambda)}{\lambda} + \tau + C'\log\lambda. \tag{19}$$

Первое слагаемое этой суммы, которое обозначим через B, преобразуется к виду

$$B = h(v) + h(v)\frac{(C_5 + C')\log\lambda}{\tau - C_5\log\lambda}$$

и с учетом пункта 1° леммы 2 допускает оценку

$$B \leqslant h(v) + \frac{n(C_5 + C')\log m \log\lambda}{\tau - C_5 \log\lambda} \leqslant h(v) + \frac{C_6 n \log\lambda}{\tau - C_5\log\lambda}.$$

Ее подстановка в (19) приводит к (16). ▲

Из (15) и (16) вытекает оценка длины кодовых слов

$$|K(v)| \leqslant h(v) + G(n, \lambda, \tau), \tag{20}$$

где

$$G(n,\lambda,\tau) = n\left(\frac{C_6 \log\lambda}{\tau - C_5\log\lambda} + \frac{\tau + C_6\log\lambda}{\lambda}\right) + \lambda^{C_4} 2^\tau. \tag{21}$$

§ 5. Средняя длина кода

Лемма 8. *При заданных параметрах $\lambda = \lambda(n)$ и $\tau = \tau(n)$ средняя длина кода удовлетворяет оценке*

$$\overline{\ell}_K^{(n)} \leqslant \mathcal{H}(X) + \frac{G(n,\lambda,\tau)}{n},$$

где функция $G(n,\lambda,\tau)$ задается равенством (21).

Доказательство. Подстановка оценок (20) в выражение (4) средней длины кода дает

$$\overline{\ell}_K^{(n)} \leqslant \frac{1}{n} \sum_{v \in A^n} p(v) h(v) + \frac{G(n, \lambda, \tau)}{n}. \tag{22}$$

Обозначим через $p_n(\boldsymbol{r})$ вероятность порождения источником $X = (A, P)$ слов класса $\mathcal{K}_n(\boldsymbol{r})$, $\boldsymbol{r} = (r_T,\ T \in \mathcal{T})$. Вероятности $p_n(\boldsymbol{r})$ образуют полиномиальное (мультиномиальное) распределение [26]

$$p_n(\boldsymbol{r}) = \frac{n!}{\prod\limits_{T \in \mathcal{T}} r_T!} \prod_{T \in \mathcal{T}} p_T^{r_T}.$$

Оно обладает свойством

$$\sum_{\boldsymbol{r}} p_n(\boldsymbol{r}) \frac{r_T}{n} = p_T, \quad T \in \mathcal{T}, \tag{23}$$

где r_T и p_T – компоненты наборов $\boldsymbol{r}$ и P.

В выражении (22) сгруппируем слова $v \in A^n$ по их принадлежности частотным классам $\mathcal{K}_n(\boldsymbol{r})$. Поскольку слова класса $\mathcal{K}_n(\boldsymbol{r})$ имеют одинаковую квазиэнтропию $h(v) = h_n(\boldsymbol{r}) = n\mathcal{H}\Big(\frac{\boldsymbol{r}}{n}\Big)$, это дает

$$\overline{\ell}_K^{(n)} \leqslant \sum_{\boldsymbol{r}} p_n(\boldsymbol{r}) \mathcal{H}\Big(\frac{\boldsymbol{r}}{n}\Big) + \frac{G(n, \lambda, \tau)}{n}.$$

Применив к вогнутой функции $\mathcal{H}$ (пункт 3° леммы 1) неравенство Йенсена и используя (23), получаем

$$\overline{\ell}_K^{(n)} \leqslant \mathcal{H}\left(\sum_{\boldsymbol{r}} p_n(\boldsymbol{r}) \frac{\boldsymbol{r}}{n}\right) + \frac{G(n, \lambda, \tau)}{n} = \mathcal{H}(P) + \frac{G(n, \lambda, \tau)}{n}. \quad \blacktriangle$$

§ 6. Сложность кодирования и декодирования

Лемма 9. *Справедливы следующие утверждения*:

1. *Сложность построения справочной части кодового слова не превосходит величину* $\lambda^{C_7}\big((C_8)^{\lambda} + 2^{2\tau}\big)$;
2. *Сложность построения основной части кодового слова при заданной справочной части не превосходит* $n\lambda^{C_9} 2^{\tau}$;
3. *Сложность декодирования не превосходит* $(n + 2^{\tau})\lambda^{C_{10}}$.

Доказательство. 1. Сложность градиентной процедуры доопределения класса $\mathcal{K}_\lambda(\boldsymbol{r})$ полиномиальна относительно числа клеток градиентной таблицы. Числа строк и столбцов таблицы не более чем экспоненциальны по λ, а потому сложность процедуры оценивается величиной C^{λ}. То же относится и к 2^{τ}-ограниченной градиентной процедуре. Общее число классов $\mathcal{K}_\lambda(\boldsymbol{r})$ не превосходит $\lambda^{C'}$, и следовательно, на реализацию 2^{τ}-ограниченных процедур для этих классов затрачивается не более $\lambda^{C'} C^{\lambda}$ операций. При этом суммарное число слов, вошедших в доопределения классов $\mathcal{K}_\lambda(\boldsymbol{r})$, для которых 2^{τ}-ограниченная процедура завершилась результативно, не превышает $\lambda^{C'} 2^{\tau}$. Их лексикографическое упорядочивание с одновременным удалением повторяющихся слов требует не более $\lambda^{C''} 2^{2\tau}$ операций. Нетрудно понять, что суммарная трудоемкость других операций, используемых при построении справочной части, ограничена величиной $\lambda^{\widehat{C}}2^{\tau}$. Будем считать, что она учтена константой C'', и таким образом, общая сложность построения справочной части оценивается величиной $\lambda^{C'}C^{\lambda}+\lambda^{C''}2^{2\tau}$. Полагая $C_7=\max\{C',C''\}$, $C_8=C$, приходим к утверждению пункта 1.

2. При построении основной части $K_1(v)$ кодового слова вначале по справочной части K_0 восстанавливается множество $\mathcal{D}_{\lambda,\tau}$ и словам w_s этого множества приписываются двоичные номера $\widetilde{s}^{(\alpha)}$. С учетом оценки (15) нетрудно понять, что трудоемкость этого не превосходит $\lambda^{C}2^{\tau}$ при некотором C.

Далее формируется основная часть $K_1(v)$ в результате последовательности шагов i. Результатом шага i являются слово $v^{(i)}$, полученное из v удалением фрагментов $v_1,\ldots,v_i$, и слово

$$K(v_1\ldots v_i)=\widetilde{s}_1^{(\alpha)}\widetilde{\ell}_1^{(\beta)}\ldots\widetilde{s}_i^{(\alpha)}\widetilde{\ell}_i^{(\beta)}.$$

На шаге i последовательно образуются слова $v_{i,1},v_{i,2},\ldots$, где $v_{i,j}$ – начальное подслово длины j слова $v^{(i-1)}$, и для каждого из них ищется первое в порядке расположения в $\mathcal{D}$ его обобщенное доопределение w_s. Шаг i завершится после того, как при некотором $j=\ell$ окажется, что обобщенных доопределений слова $v_{i,\ell}$ словами w_s нет. Тогда полагаем $v_i=v_{i,\ell-1}$, $\ell_i=\ell-1$ и берем в качестве s_i номер слова, обобщенно доопределяющего слово $v_{i,\ell-1}$. Слово $v^{(i)}$ образуем из $v^{(i-1)}$ удалением фрагмента v_i, а слово $K(v_1\ldots v_i)$ – дописыванием к $K(v_1\ldots v_{i-1})$ слова $\widetilde{s}_i^{(\alpha)}\widetilde{\ell}_i^{(\beta)}$. Процедура завершится шагом t, после которого слово $v^{(t)}$ окажется пустым.

Основная трудоемкость этого этапа приходится на перебор пар $(v_{i,j},w_s)$ и выяснение, является ли w_s обобщенным доопределением слова $v_{i,\ell}$. При формировании фрагмента v_i используется ℓ_i+1 слов $v_{i,j}$, а потому общее число слов $v_{i,j}$, участвующих в сравнениях, не превосходит

$$\ell_1+\ldots+\ell_t+t\leqslant n+t\leqslant 2n.$$

Число слов w_s ограничено величиной $\lambda^{C_3}2^{\tau}$ (см. (12)). Поэтому общее число пар $(v_{i,j},w_s)$ не больше $2n\lambda^{C_3}2^{\tau}$. Число операций, связанных с одним сравнением, полиномиально по λ, и следовательно, на все сравнения затрачивается не более $n\lambda^{C'}2^{\tau}$ операций. Нетрудно видеть, что учет других операций не изменяет характера этой оценки, и будем считать, что она их учитывает.

Суммирование полученных оценок дает величину $\lambda^{C}2^{\tau}+n\lambda^{C'}2^{\tau}$, которая не превосходит $n\lambda^{C_9}2^{\tau}$ при некотором C_9.

3. При декодировании вначале по справочной части K_0 восстанавливается множество $\mathcal{D}_{\lambda,\tau}$ и словам w_s этого множества приписываются двоичные номера $\widetilde{s}^{(\alpha)}$. На это затрачивается $\lambda^{C}2^{\tau}$ операций. Затем основная часть разбивается на подслова $\widetilde{s}_i^{(\alpha)}\widetilde{\ell}_i^{(\beta)}$ длины $\alpha+\beta$, а они, в свою очередь, делятся на части длины α и β. Эти части задают слово w_{s_i}, обобщенно доопределяющее фрагмент v_i, и длину ℓ_i его подслова, доопределяющего v_i. Доопределение слова v образуется заменой фрагментов v_i найденными доопределениями.

Доопределение одного фрагмента v_i выполнимо с полиномиальной относительно λ сложностью. Поскольку число t фрагментов не превосходит n, на все фрагменты затрачивается не более $n\lambda^{C'}$ операций. Нетрудно видеть, что эта величина при подходящем выборе C' покрывает также сложность других операций, используемых на втором этапе. Суммарная сложность декодирования составляет $\lambda^{C}2^{\tau}+n\lambda^{C'}$. Выбирая $C_{10}=\max(C,C')$, приходим к утверждению 3 леммы. ▲

§ 7. Выбор параметров и завершение доказательства

Задавшись функцией $\varphi(n)$, удовлетворяющей условиям

$$\varphi(n)\to\infty,\quad \varphi(n)=o\bigl(\log^{1/2}(n)\bigr), \tag{24}$$

назначим параметры $\lambda=\lambda(n)$ и $\tau=\tau(n)$, положив

$$\lambda(n)=\left\lfloor\frac{\log n}{\varphi^2(n)}\right\rfloor, \tag{25}$$

$$\tau(n)=\left\lfloor\frac{(\log n\log\log n)^{1/2}}{\varphi(n)}\right\rfloor, \tag{26}$$

где через $\lfloor x\rfloor$ обозначено наибольшее целое, не большее числа x.

Лемма 10. *Если функция $\varphi(n)$ удовлетворяет условиям* (24), *то метод кодирования K при значениях* (25) *и* (26) *параметров λ и τ*

1) *обеспечивает среднюю длину кода*

$$\overline{\ell}_K^{(n)}\leqslant\mathcal{H}(X)+O\left(\varphi(n)\left(\frac{\log\log n}{\log n}\right)^{1/2}\right);$$

2) *допускает кодирование и декодирование со сложностью $n^{1+o(1)}$.*

Доказательство. 1. Из леммы 8 следует, что

$$\overline{\ell}_K^{(n)}\leqslant\mathcal{H}(X)+\frac{G(n)}{n}, \tag{27}$$

где $G(n)=G(n,\lambda(n),\tau(n))$ – результат подстановки в функцию (21) значений (25) и (26). Представим $G(n,\lambda,\tau)$ в виде $A_1+A_2+A_3$, где

$$A_1=\frac{C_6\,n\log\lambda}{\tau-C_5\log\lambda},\quad A_2=\frac{n(\tau+C_6\log\lambda)}{\lambda},\quad A_3=\lambda^{C_4}2^{\tau}.$$

Из (25) с учетом (24) следует, что $\lambda\to\infty$ и $\log\lambda\leqslant\log\log n$. Сравнение равенств (25) и (26) показывает, что $\tau\geqslant(\lambda\log\lambda)^{1/2}-1$, а потому $\log\lambda=o(\tau)$. Это означает, что выполнено условие (11) и имеют место асимптотические равенства $\tau-C_5\log\lambda\sim\tau$ и $\tau+C_6\log\lambda\sim\tau$. Принимая их во внимание, получаем

$$A_1\sim\frac{C_6 n\log\lambda}{\tau}\lesssim\frac{C_6\,n\log\log n\,\varphi(n)}{(\log n\log\log n)^{1/2}}\lesssim C_6 n\,\varphi(n)\left(\frac{\log\log n}{\log n}\right)^{1/2},$$

$$A_2\sim\frac{n\tau}{\lambda}\sim\frac{n(\log n\log\log n)^{1/2}\varphi(n)}{\log n}\sim n\,\varphi(n)\left(\frac{\log\log n}{\log n}\right)^{1/2}.$$

Из последнего соотношения следует, в частности, что $\log A_2\sim\log n$. В то же время, $\log A_3=C_4\log\lambda+\tau\sim\tau=o(\log n)$, а потому $\log A_3=o(\log A_2)$, и тем более, $A_3=o(A_2)$.

Суммируя оценки и опуская малые члены, получаем

$$D(n)\lesssim(C_6+1)n\varphi(n)\left(\frac{\log\log n}{\log n}\right)^{1/2},$$

а потому

$$\frac{D(n)}{n} = O\left(\varphi(n)\left(\frac{\log\log n}{\log n}\right)^{1/2}\right).$$

Подстановка этого соотношения в (27) дает первое утверждение леммы.

2. Параметры λ и τ, заданные равенствами (25) и (26), удовлетворяют условиям $\lambda = o(\log n)$ и $\tau = o(\log n)$. Подстановка этих соотношений в оценки сложности кодирования и декодирования из леммы 9 показывают, что каждая из этих оценок не превосходит $n^{1+o(1)}$. ▲

Основная теорема вытекает из леммы 10 при $\varphi(n) = (\log\log n)^{1/2}$.

СПИСОК ЛИТЕРАТУРЫ

1. *Шоломов Л.А.* Элементы теории недоопределенной информации // Прикл. дискр. матем. 2009. Приложение № 2 (Лекции, прочитанные на Международной конференции с элементами научной школы для молодежи “Компьютерная безопасность и криптография”. Омск, ОмГТУ. 7–12 сентября 2009 г.). С. 18–42.
2. *Бонгард М.М.* О понятии “полезная информация” // Проблемы кибернетики. Вып. 9. М.: Физматгиз, 1963. С. 71–102.
3. *Shannon C.E.* Coding Theorems for a Discrete Source with Fidelity Criterion // IRE Nat. Conv. Rec. 1959. V. 7. № 4. P. 142–163. (Русск. перевод в *Шеннон К.Э.* Работы по теории информации и кибернетике. М.: Изд-во иностр. лит., 1963. С. 587–621).
4. *Галлагер Р.* Теория информации и надежная связь. М.: Сов. радио, 1974.
5. Вероятность и математическая статистика. Энциклопедический словарь / Под ред. Ю.В. Прохорова. М: Большая российская энциклопедия, 1999.
6. *Шоломов Л.А.* О кодировании недоопределенных последовательностей с заданной точностью воспроизведения // ДАН. 2009. Т. 429. № 5. С. 605–609.
7. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
8. *Шоломов Л.А.* Сжатие частично определенной информации // Нелинейная динамика и управление. Вып. 4 / Под ред. С.В. Емельянова, С.К. Коровина. М.: Физматлит, 2004. С. 377–396.
9. *Потапов В.Н.* Арифметическое кодирование сообщений с использованием случайных последовательностей // Прикл. дискр. матем. 2008. № 2 (2). С. 131–133.
10. *Шоломов Л.А.* Теоретически эффективное асимптотически оптимальное универсальное кодирование частично определенных источников // Прикл. дискр. матем. 2020. № 47. С. 30–56.
11. *Шоломов Л.А.* Информационные свойства функционалов сложности для систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 34. М.: Наука, 1978. С. 133–150.
12. *Потапов В.Н.* Введение в теорию информации. Ижевск: НИЦ “Регулярная и хаотическая динамика”, 2014.
13. *Колмогоров А.Н.* Три подхода к определению понятия “количество информации” // Пробл. передачи информ. 1965. Т. 1. № 1. С. 3–11.
14. *Лупанов О.Б.* Об одном подходе к синтезу схем – принципе локального кодирования // Проблемы кибернетики. Вып. 14. М.: Наука, 1965. С. 31–110.
15. *Чашкин А.В.* Методы вычисления частичных булевых функций // Тр. VII Межд. конф. “Дискретные модели в теории управляющих систем” (Покровское, Моск. обл., 4–6 марта 2006 г.). М.: МАКС Пресс, 2006. С. 390–404.
16. *Shannon C.E.* The Synthesis of Two-Terminal Switching Circuits // Bell Syst. Tech. J. 1949. V. 98. № 1. P. 59–98. (Русск. перевод в *Шеннон К.Э.* Работы по теории информации и кибернетике. М.: Изд-во иностр. лит., 1963. С. 59–101.)

17. *Нечипорук Э.И.* О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР. 1965. Т. 163. № 1. С. 40–42.
18. *Нечипорук Э.И.* О топологических принципах самокорректирования // Проблемы кибернетики. Вып. 21. М.: Наука, 1969. С. 5–102.
19. *Krichevsky R.E.* Occam's Razor, Partially Specified Boolean Functions, String Matching, and Independent Sets // Inform. and Comput. 1994. V. 108. № 1. P. 158–174.
20. *Berger T.* Rate Distortion Theory: A Mathematical Basis for Data Compression. Englewood Cliffs, NJ: Prentice-Hall, 1971.
21. *Krichevsky R.* Universal Compression and Retrieval. Dordrecht: Kluwer, 1994.
22. *Andreev A.E., Clementi A.E.F., Rolim J.D.P.* Hitting Sets Derandomize BPP // Proc. 23rd Int. Colloq. on Automata, Languages and Programming (ICALP'96). Paderborn, Germany. July 8–12, 1996. Lect. Notes Comp. Sci. V. 1099. Berlin: Springer, 1996. P. 357–368.
23. *Goldreich O., Wigderson A.* Improved Derandomization of BPP Using a Hitting Set Generator // Randomization, Approximation, and Combinatorial Optimization: Algorithms and Techniques (Proc. 3rd Int. Workshop on Randomization and Approximation Techniques in Computer Science, and 2nd Int. Workshop on Approximation Algorithms for Combinatorial Optimization Problems [RANDOM-APPROX'99]. Berkeley, CA, USA. August 8–11, 1999). Lect. Notes Comp. Sci. V. 1671. Berlin: Springer, 1999. P. 131–137.
24. *Нигматуллин Р.Г.* Метод наискорейшего спуска в задачах на покрытие // Тр. симпоз. "Вопросы точности и эффективности вычислительных алгоритмов". Киев: Ин-т кибернетики АН УССР, 1969. Т. 5. С. 116–126.
25. *Нигматуллин Р.Г.* Сложность булевых функций. М.: Наука, 1991.
26. *Крамер Г.* Математические методы статистики. М.: Мир, 1975.

Шоломов Лев Абрамович
ФИЦ "Информатика и управление" РАН
Институт системного анализа РАН
`levshol@mail.ru`

Поступила в редакцию
28.05.2020
После доработки
13.11.2020
Принята к публикации
23.11.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.72

© 2020 г. **Е.Е. Егорова[1], М. Фернандес[2], Г.А. Кабатянский[1], И. Мяо[3]**

СУЩЕСТВОВАНИЕ И КОНСТРУКЦИИ МУЛЬТИМЕДИЙНЫХ КОДОВ, СПОСОБНЫХ НАХОДИТЬ ПОЛНУЮ КОАЛИЦИЮ ПРИ АТАКЕ УСРЕДНЕНИЯ И ШУМЕ

Как было недавно показано в [1], не существует мультимедийных кодов цифровых водяных знаков, способных полностью восстановить коалицию недобросовестных пользователей в условиях общей линейной атаки и целенаправленного шума. Мы покажем, что такие коды существуют, если сузить класс атак до атаки усреднения. Возникающая математическая задача близка к задаче построения сигнатурных кодов для двоичного суммирующего канала с шумом.

Ключевые слова: мультимедийный код цифровых отпечатков пальцев, канал множественного доступа, целенаправленный шум, сигнатурный код, атака на основе сговора, коды без перекрытия, дизъюнктивные коды.

DOI: `10.31857/S0555292320040087`

§ 1. Введение

Математическая постановка задачи защиты цифрового контента от нелегального копирования и перераспределения возникла в конце прошлого века, см. [2–4]. Наибольшее внимание привлекла постановка задачи, известная как коды цифровых отпечатков пальцев и существующая в различных вариациях, см. [5–8]. Соответствующие модели являются дискретными, и первая непрерывная модель, мотивированная приложениями к защите мультимедийного контента (изображения, музыка), появилась в работах [9, 10] под названием мультимедийные коды отпечатков пальцев. То, что эти коды тесно связаны с сигнатурными кодами для соответствующих каналов множественного доступа, в частности, для A-канала [11], неявно появилось в работе [12], а позже – в явной форме в [13]. Затем эта связь была распространена на сигнатурные коды для взвешенного двоичного суммирующего канала [14]. Этот подход был дальше развит в [1], где было доказано, в частности, что мультимедийные коды отпечатков пальцев не способны полностью восстановить коалицию недобросовестных пользователей в условиях общей линейной атаки и целенаправленного шума. В данной статье мы покажем, что ситуация более оптимистична, если несколько ограничить атаки коалиций, а именно при атаке усреднения существуют коды, которые находят всех членов коалиции даже в присутствии целенаправленного шума. Отметим, что далее мы будем употреблять термин “цифровые водяные знаки” вместо “отпечатки пальцев”.

---

[1] Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номера проектов 20-51-50007 и 20-07-00652).

[2] Работа выполнена при частичной финансовой поддержке гранта правительства Испании TCO-RISEBLOCK (номер гранта PID2019-110224RB-I00, проект MINECO/FEDER) и гранта правительства Каталонии 2017-SGR-782.

[3] Работа выполнена при частичной финансовой поддержке Японского общества содействия развитию науки (JSPS) в рамках научного проекта JPJSBP120204802.

§ 2. Мультимедийные коды цифровых водяных знаков

Рассмотрим математическую модель защиты мультимедийного контента от нелегального перераспределения. Мультимедийный контент представляется как N-мерный вектор $\boldsymbol{x}$ над полем $\mathbb{R}$ вещественных чисел. Имеется дистрибьютор, который видоизменяет $\boldsymbol{x}$ специальным образом для каждого пользователя так, чтобы если коалиция недобросовестных пользователей подделает $\boldsymbol{x}$, то он может найти всех членов коалиции (complete traceability; см. [1]). Для этого дистрибьютор выбирает m попарно ортогональных векторов $\boldsymbol{f}_1, \dots, \boldsymbol{f}_m$ в $\mathbb{R}^N$ одинаковой длины (для простоты – длины 1), которые известны только ему – это важное предположение, которое будет использоваться в дальнейшем. Затем дистрибьютор формирует так называемые *цифровые водяные знаки* (ЦВЗ) как линейные комбинации этих векторов с двоичными коэффициентами (известен и другой вариант “модуляции” ЦВЗ, когда используются коэффициенты из $\{-1, +1\}$).

ЦВЗ $\boldsymbol{w}_j$, предназначенный j-му пользователю, имеет вид

$$\boldsymbol{w}_j = \sum_{i=1}^{m} h_{ij} \boldsymbol{f}_i, \tag{1}$$

где $h_{ij} \in \{0, 1\}$. Вложение ЦВЗ осуществляется аддитивно, т.е. дистрибьютор выдает j-му пользователю вектор

$$\boldsymbol{y}_j = \boldsymbol{x} + \boldsymbol{w}_j \tag{2}$$

как копию $\boldsymbol{x}$, где предполагается, что длина вектора $\boldsymbol{x}$ много больше длины ЦВЗ $\boldsymbol{w}_j$ (т.е. $\|\boldsymbol{x}\| \gg \|\boldsymbol{w}_j\|$, где $\|\cdot\|$ здесь и далее обозначает евклидову норму вектора), чтобы копия $\boldsymbol{y}_j$ мало отличалась от оригинала $\boldsymbol{x}$.

Пусть имеется M пользователей и среди них коалиция $A \subset [M]$ недобросовестных пользователей. *Линейная атака* состоит в том, что коалиция A генерирует поддельную копию $\boldsymbol{y}$ как линейную комбинацию имеющихся у нее копий $\boldsymbol{y}_j$ с вещественными коэффициентами $\lambda_1, \dots, \lambda_M$, такими что $\sum\limits_{j=1}^{M} \lambda_j = 1$, $\lambda_j > 0$ для всех $j \in A$ и $\lambda_j = 0$ для $j \notin A$, т.е.

$$\boldsymbol{y} = \sum_{j=1}^{M} \lambda_j \boldsymbol{y}_j = \sum_{a \in A} \lambda_a \boldsymbol{y}_a, \tag{3}$$

Так как $\sum\limits_{j=1}^{M} \lambda_j = 1$, то $\boldsymbol{y} = \boldsymbol{x} + \sum\limits_{j=1}^{M} \lambda_j \boldsymbol{w}_j$, а так как все $\lambda_j \geqslant 0$, то в силу неравенства треугольника (для нормы) имеем

$$\|\boldsymbol{y} - \boldsymbol{x}\| = \left\| \sum_{j=1}^{M} \lambda_j \boldsymbol{w}_j \right\| \leqslant \sum_{j=1}^{M} \lambda_j \|\boldsymbol{w}_j\| \leqslant \max_j \|\boldsymbol{w}_j\| \ll \|\boldsymbol{x}\|, \tag{4}$$

и следовательно, $\boldsymbol{y}$ является достаточно хорошей копией оригинала $\boldsymbol{x}$.

Так как дистрибьютор знает значение $\boldsymbol{x}$, то чтобы определить, что $\boldsymbol{y}$ – это нелегальная копия $\boldsymbol{x}$, и найти всех участников коалиции, создавших $\boldsymbol{y}$, он вычисляет скалярные произведения

$$s_k = (\boldsymbol{y} - \boldsymbol{x}, \boldsymbol{f}_k) = \left(\sum_{j=1}^{M} \lambda_j \sum_{i=1}^{M} h_{ij} \boldsymbol{f}_i, \boldsymbol{f}_k \right) = \sum_{j=1}^{M} \lambda_j h_{kj} \tag{5}$$

и формирует вектор-синдром $\boldsymbol{S} = \boldsymbol{S}(\Lambda) = (s_1, \ldots, s_m)$, где $\Lambda := (\lambda_1, \ldots, \lambda_M)$. Отметим, что для вектора Λ его носителем $\operatorname{supp}(\Lambda) := \{j : \lambda_j \neq 0\}$ является коалиция A.

Введем векторы $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M$, где $\boldsymbol{h}_j = (h_{1j}, \ldots, h_{mj})$. Тогда (5) можно переписать в виде

$$\boldsymbol{S} = \sum_{j=1}^{M} \lambda_j \boldsymbol{h}_j = \sum_{a \in A} \lambda_a \boldsymbol{h}_a. \tag{6}$$

Это уравнение, в свою очередь, можно записать как матричное уравнение

$$\boldsymbol{S} = H\Lambda^T, \tag{7}$$

где H – матрица размера $m \times M$, составленная из векторов-столбцов $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M$.

Так как векторы $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$ ортонормированные, а векторы ЦВЗ $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_M$ выражаются в базисе $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$ с двоичными коэффициентами, а именно

$$\boldsymbol{w}_j = \sum_{i=1}^{m} h_{ij} \boldsymbol{f}_i, \quad \text{где} \quad h_{ij} \in \{0, 1\},$$

то множества $\mathcal{W} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_M\}$ и $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M\}$ изометричны. При этом векторы $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$ известны дистрибьютору (и только ему), поэтому для него равносильно, работать ли с множеством ЦВЗ $\mathcal{W}$ или с множеством $\mathcal{H}$ соответствующих двоичных векторов. Поэтому далее мы будем оба множества называть мультимедийным кодом, а если по синдрому $\boldsymbol{S}$ можно однозначно найти носитель $\operatorname{supp}(\Lambda)$, т.е. коалицию A, то будем называть их *t-мультимедийным кодом со свойством полного поиска коалиций* (t-МППК-кодом).

Определение 1. Двоичный код $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M\} \subset \{0, 1\}^m$ называется *t-МППК-кодом*, если для любых двух вещественных векторов Λ и Λ', таких что

$$\sum_{j=1}^{M} \lambda_j = \sum_{j=1}^{M} \lambda'_j = 1 \quad \text{и} \quad |\operatorname{supp}(\Lambda)|, |\operatorname{supp}(\Lambda')| \leqslant t,$$

из $H\Lambda^T = H\Lambda'^T$ следует, что $\operatorname{supp}(\Lambda) = \operatorname{supp}(\Lambda')$.

Замечание 1. Заметим, что в данном определении мы не воспользовались ограничением, что все λ_j неотрицательны.

Замечание 2. Всюду далее мы предполагаем, что значение t фиксировано.

Среди всех линейных атак особо выделяется *атака усреднения*, для которой $\lambda_j = |A|^{-1}$ при $j \in A$ и $\lambda_j = 0$ в противном случае. Ранее, начиная с первых работ по этой тематике (см. [9, 10]), считалось, что “атака усреднения является наиболее справедливой для участников коалиции, чтобы избежать обнаружения” [12]. Поэтому все работы до [13] ограничивались рассмотрением только атаки усреднения. В этой статье мы покажем, что атака усреднения намного слабее общей линейной атаки, по крайней мере, в случае целенаправленного шума.

Напомним, что двоичный код $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M\} \subset \{0, 1\}^m$ называется t-сигнатурным кодом для двоичного суммирующего канала (см. [15]), если для любых двух различных кодовых подмножеств A и B, где оба подмножества мощности не более t, справедливо неравенство

$$\sum_{j \in A} \boldsymbol{h}_j \neq \sum_{j \in B} \boldsymbol{h}_j. \tag{8}$$

Код, для которого неравенство (8) выполнено для любых двух различных кодовых подмножеств A и B *одинаковой мощности* не более t, будем называть $(=,t)$*-сигнатурным кодом для суммирующего канала.* Двоичный код, обладающий свойством нахождения полной коалиции при атаке усреднения, является $(=,t)$-сигнатурным кодом для суммирующего канала. Обратное неверно ни для $(=,t)$-, ни для t-сигнатурного кода для двоичного суммирующего канала.

Обозначим через $M(m,t)$ максимально возможную мощность t-МППК-кода длины m, а через $R(m,t) := m^{-1}\log_2 M(m,t)$ – соответствующую кодовую скорость. Тогда из сделанного выше замечания об атаке усреднения и обычных соображений мощности вытекает следующий аналог границы Хэмминга:

$$C^t_{M(m,t)} \leqslant (t+1)^m. \tag{9}$$

Отметим, что из известной верхней границы для скорости сигнатурных кодов для суммирующего канала [16] следует асимптотически в два раза лучшая, чем (9), граница на скорость кода

$$\limsup_m R(m,t) \leqslant \frac{\log_2 t}{2t}(1+o(1)). \tag{10}$$

С другой стороны, в [14] была доказана следующая нижняя граница:

$$M(m,t) \geqslant 2^{\lfloor m/t \rfloor}, \tag{11}$$

из которой следует, что $R(m,t) \geqslant t^{-1}(1+o(1))$.

Повторим кратко основные аргументы из [14]. Прежде всего отметим, что если среди векторов $\boldsymbol{h}_1,\ldots,\boldsymbol{h}_M$ любые $2t$ линейно независимы над $\mathbb{R}$, то определение 1 выполнено, и более того, дистрибьютор может найти не только те j, которым соответствуют $\lambda_j \neq 0$, но и соответствующие значения λ_j (и кроме того, ограничение $\sum\limits_{j=1}^{m} \lambda_j = 1$ не требуется). Примером такого множества двоичных векторов являются столбцы проверочной матрицы двоичного кода, исправляющего t ошибок, так как любые $2t$ ее столбцов линейно независимы над полем из двух элементов, а следовательно, и над $\mathbb{R}$. Теперь, чтобы получить (11), остается взять в качестве $\boldsymbol{h}_1,\ldots,\boldsymbol{h}_M$ столбцы проверочной $(m\times M)$-матрицы неприводимого кода Гоппы (см. [17]) длины $M = 2^\ell$ и избыточности $m = \ell t$, исправляющего t ошибок.

§ 3. Мультимедийные коды цифровых водяных знаков в присутствии шума

Отметим, что ранее в литературе уже рассматривались модели мультимедийных кодов цифровых водяных знаков в присутствии шума: вероятностная модель шума (см. [18]) и модель целенаправленного шума, где нет ограничения на норму (длину) вектора ошибки, а есть только ограничение на вес Хэмминга ошибки [14].

В этой статье, следуя [1], мы рассматриваем модель, когда коалиция A не только создает ложную копию

$$\boldsymbol{y} = \boldsymbol{x} + \sum_{j\in A} \lambda_j \boldsymbol{w}_j \in \mathbb{R}^N$$

в соответствии с моделью линейной атаки, но еще и целенаправленно добавляет вектор шума $\boldsymbol{e} \in \mathbb{R}^N$, такой что $\|\boldsymbol{e}\| \leqslant \delta$, где $\|\cdot\|$ – евклидова норма на $\mathbb{R}^N$. В результате коалиция A формирует и перераспределяет копию

$$\widehat{\boldsymbol{y}} = \boldsymbol{x} + \sum_{j\in A} \lambda_j \boldsymbol{w}_j + \boldsymbol{e}. \tag{12}$$

Множество ЦВЗ $\mathcal{W} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_M\} \subset \mathbb{R}^N$ будем называть (t,δ)-*мультимедийным кодом ЦВЗ со свойством полного поиска коалиций, устойчивым к δ-шуму*, если по любой ложной копии $\widehat{\boldsymbol{y}} = \sum\limits_{j\in A} \lambda_j \boldsymbol{y}_j + \boldsymbol{e}$ можно однозначно найти коалицию A. Это условие равносильно тому, что для любых двух различных коалиций A и B, $|A|, |B| \leqslant t$, и любых двух вещественных векторов Λ и Λ', таких что

$$\sum_{j\in A} \lambda_j = \sum_{j\in B} \lambda'_j = 1,$$

справедливо неравенство

$$\left\| \sum_{j\in A} \lambda_j \boldsymbol{w}_j - \sum_{j\in B} \lambda'_j \boldsymbol{w}_j \right\| > 2\delta. \tag{13}$$

Довольно очевидно, что условие (13) слишком сильное, и таких кодов не существует, что и было показано в [1]. Приведем дополнительные к [1] аргументы, почему таких кодов нет. Положим $A = \{1, 2, \ldots, t\}$ и $B = \{1, 2, \ldots, t-1, t+1\}$. Обозначим $w = \max\limits_{j\in[t+1]} \|\boldsymbol{w}_j\|$ и выберем $\lambda_t = \lambda'_{t+1} = \lambda$ так, чтобы $0 < \lambda < \min\{\delta w^{-1}, 1\}$. Выберем положительные $\lambda_j = \lambda'_j$ для $j = 1, \ldots, t-1$ такими, что $\lambda + \sum\limits_{j=1}^{t-1} \lambda_j = 1$. Тогда

$$\sum_{j\in A} \lambda_j \boldsymbol{w}_j + \boldsymbol{e} = \sum_{j=1}^{t-1} \lambda_j \boldsymbol{w}_j = \sum_{j\in B} \lambda_j \boldsymbol{w}_j + \boldsymbol{e}',$$

где $\boldsymbol{e} = -\lambda \boldsymbol{w}_t$, $\boldsymbol{e}' = -\lambda \boldsymbol{w}_{t+1}$ и $\|\boldsymbol{e}\|, \|\boldsymbol{e}'\| \leqslant \delta$, и неравенство (13) не выполнено.

Этот анализ условия (13) показывает, что если какое-то λ_j отлично от нуля, но достаточно мало, то от него можно “избавиться”, введя взамен другое ненулевое λ_i, что и не позволяет найти коалицию целиком. Однако у атаки усреднения все λ_j равны и достаточно отделены от нуля, что позволяет надеяться, что если ограничить класс линейных атак только атакой усреднения, то существуют коды, находящие коалицию целиком; см. следующее

Определение 2. Множество $\mathcal{W} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_M\}$ будем называть (t,δ)-*мультимедийным кодом со свойством полного поиска коалиций, устойчивым к атаке усреднения и δ-шуму*, если для любых двух различных подмножеств кода $A, B \subset \mathcal{W}$, таких что $|A|, |B| \leqslant t$, справедливо неравенство

$$\left\| \frac{1}{|A|} \sum_{j\in A} \boldsymbol{w}_j - \frac{1}{|B|} \sum_{j\in B} \boldsymbol{w}_j \right\| > 2\delta. \tag{14}$$

Ниже нам будет удобнее рассматривать не код $\mathcal{W}$, а изометричный ему двоичный код $\mathcal{H}$ длины m, для которого условие (14) перепишется в виде

$$\left\| \frac{1}{|A|} \sum_{j\in A} \boldsymbol{h}_j - \frac{1}{|B|} \sum_{j\in B} \boldsymbol{h}_j \right\| > 2\delta. \tag{15}$$

Обозначим через $\mathcal{M}(m,t,\delta)$ максимальную мощность (t,δ)-мультимедийного кода со свойством полного поиска коалиций, устойчивого к атаке усреднения и δ-шуму. Определим, как обычно, соответствующую максимальную скорость

$$\mathcal{R}(m,t,\delta) := m^{-1} \log_2 \mathcal{M}(m,t,\delta).$$

Основным результатом статьи является доказательство существования соответствующих (t,δ)-мультимедийных кодов со скоростью, отделенной от нуля.

Теорема 1. *Для любых фиксированных t и δ*

$$\liminf_{m} \mathcal{R}(m,t,\delta) \geqslant \frac{\gamma_t \log_2 e}{t(1+\gamma_t \log_2 e)} > \frac{1}{t(1+e(\log_2 e)^{-1})} > \frac{0{,}346}{t}, \tag{16}$$

где $\gamma_t = (1-t^{-1})^{t-1}$.

Разобьем построение таких кодов на две подзадачи: первая, когда мощность коалиции заранее известна, вторая – построение кодов, которые позволяют найти мощность коалиции по любой ложной копии. Начнем с первой подзадачи.

Если мощность коалиции известна, то возникающая задача – это по существу задача о сигнатурном коде для *двоичного суммирующего канала с шумом* (ДСКШ). А именно, дадим

Определение 3. Двоичный код $\mathcal{C} = \{\boldsymbol{c}_1,\ldots,\boldsymbol{c}_M\}$ называется $(=,t,\Delta)$-*сигнатурным кодом для ДСКШ*, если для любых двух различных подмножеств кода $A,B \subset \mathcal{C}$, таких что $|A| = |B| \leqslant t$, справедливо неравенство

$$\|\sum_{c\in A} \boldsymbol{c} - \sum_{c'\in B} \boldsymbol{c}'\| > 2\Delta. \tag{17}$$

Очевидно, что $(=,t,\Delta)$-сигнатурный код для ДСКШ позволяет однозначно найти всю коалицию при атаке усреднения и δ-шуме, где $\delta = \Delta/t$, если мощность коалиции заранее известна и не превышает t. Заметим также, что в определении 3 условие $|A| = |B| \leqslant t$ можно без ограничения общности заменить на условие $|A| = |B| = t$.

Воспользуемся конструкцией, предложенной в [19] для построения сигнатурных кодов для двоичного суммирующего по модулю 2 канала, и переоткрытой в [20] как коды, исправляющие ошибки в канале и синдроме.

Начнем с кода $\widehat{\mathcal{H}} = \{\widehat{\boldsymbol{h}}_1,\ldots,\widehat{\boldsymbol{h}}_M\} \subset \{0,1\}^m$ длины m, слова которого – это столбцы проверочной $(m\times M)$-матрицы *линейного* двоичного кода V, исправляющего t ошибок. Закодируем слова $\widehat{\boldsymbol{h}}_1,\ldots,\widehat{\boldsymbol{h}}_M$ двоичным кодом U длины n с m информационными символами и минимальным кодовым расстоянием d (в метрике Хэмминга). Обозначим полученные векторы через $\boldsymbol{h}_1,\ldots,\boldsymbol{h}_M$ и зададим код $\mathcal{H} = \{\boldsymbol{h}_1,\ldots,\boldsymbol{h}_M\}$.

Лемма 1. *Код $\mathcal{H} = \{\boldsymbol{h}_1,\ldots,\boldsymbol{h}_M\} \subset \{0,1\}^n$ является $(=,t,\Delta)$-сигнатурным кодом для ДСКШ с $\Delta = \sqrt{d}/2$.*

Доказательство. Рассмотрим два произвольных различных подмножества A,B кода $\mathcal{H}$ одинаковой мощности не более t и соответствующие им векторы

$$\boldsymbol{h}^{(A)} = \sum_{h\in A} \boldsymbol{h} \quad \text{и} \quad \boldsymbol{h}^{(B)} = \sum_{h\in B} \boldsymbol{h}.$$

Будем обозначать через

$$\boldsymbol{a} \bmod 2 = (a_1 \bmod 2,\ldots,a_n \bmod 2) \in \{0,1\}^n$$

двоичную проекцию произвольного целочисленного вектора $\boldsymbol{a} = (a_1,\ldots,a_n)$. Так как различные суммы *по модулю* 2 из t и менее векторов $\widehat{\boldsymbol{h}}_j$ различны (и отличны от нуля), то это же справедливо и для сумм по модулю 2 векторов $\boldsymbol{h}_j$. Следовательно, $\boldsymbol{h}^{(A)} \bmod 2 \neq \boldsymbol{h}^{(B)} \bmod 2$. Так как векторы $\boldsymbol{h}^{(A)} \bmod 2$ и $\boldsymbol{h}^{(B)} \bmod 2$ принадлежат коду U (в силу линейности кода), то

$$d_H\big(\boldsymbol{h}^{(A)} \bmod 2, \boldsymbol{h}^{(B)} \bmod 2\big) \geqslant d.$$

Теперь остается применить неравенство

$$d_E(\boldsymbol{a},\boldsymbol{b}) \geqslant \sqrt{d_H(\boldsymbol{a} \bmod 2, \boldsymbol{b} \bmod 2)}, \tag{18}$$

справедливое для любых двух целочисленных векторов $\boldsymbol{a},\boldsymbol{b} \in \mathbb{R}^n$, где через d_E обозначено евклидово расстояние, а через d_H – расстояние Хэмминга.

Таким образом, код $\mathcal{H} = \{\boldsymbol{h}_1,\ldots,\boldsymbol{h}_M\}$ позволяет найти полностью коалицию недобросовестных пользователей в условиях атаки усреднения и целенаправленного шума длины не более $\delta = (2t)^{-1}\sqrt{d}$, если число таких пользователей заранее известно и не превосходит t. ▲

§ 4. Коды, определяющие мощность коалиции

Определение 4. Будем называть двоичный код C *кодом, определяющим мощность коалиции вплоть до t в условиях δ-шума*, если для любых двух его подмножеств A, B различной мощности не более t справедливо неравенство

$$\left\| \frac{1}{|A|}\sum_{c\in A}\boldsymbol{c} - \frac{1}{|B|}\sum_{c'\in B}\boldsymbol{c}' \right\| > 2\delta. \tag{19}$$

С помощью такого кода дистрибьютор сформирует итоговый код, приписывая в качестве “хвостов” к словам кода $\mathcal{H}$, построенного выше, слова кода, определяющего мощность. По “хвостам” дистрибьютор найдет мощность коалиции, а затем по коду $\mathcal{H}$ – и саму коалицию. Параметры получаемых кодов мы оценим в самом конце статьи.

Введем, как нам представляется, новое понятие в комбинаторной теории кодирования.

Определение 5. Двоичный код называется *слабым t-дизъюнктивным кодом*, если для любых t' различных кодовых слов, $1 \leqslant t' \leqslant t$, существует координата, в которой ровно одно слово равно 1.

Иначе говоря, для любого кодового подмножества A, такого что $1 \leqslant |A| \leqslant t$, существует координата i, такая что $\pi_i(A) = 1$, где $\pi_i(A) := |\{\boldsymbol{a} \in A :\ a_i = 1\}|$.

Отметим очевидную связь с дизъюнктивными кодами (см. [21, 22]). Напомним, что код называется t-дизъюнктивным кодом, если для любого кодового подмножества A мощности не более t и любого кодового слова $\boldsymbol{b} \notin A$ существует координата i, такая что $a_i = 0$ для всех $\boldsymbol{a} \in A$ и $b_i = 1$. Очевидно, что $(t-1)$-дизъюнктивный код является слабым t-дизъюнктивным кодом, так как для любых t различных кодовых слов существует t соответствующих координат i, в проекциях на которые встречаются *все* t слов веса Хэмминга 1, а для свойства слабой дизъюнктивности достаточно всего одного такого слова и одной такой координаты, но для любых t' слов, $1 \leqslant t' \leqslant t$.

Дизъюнктивные коды были переоткрыты в экстремальной комбинаторике под названием семейства множеств без t-перекрытий [23, 24]. Напомним, что семейство множеств $\mathcal{F} = \{F_1,\ldots,F_M\}$ называется семейством без t-перекрытий, если ни одно множество семейства не покрывается объединением t других множеств этого семейства.

Обобщим понятие слабого t-дизъюнктивного кода, введя, по существу, соответствующее расстояние.

Определение 6. Двоичный код называется *слабым (t,T)-дизъюнктивным кодом*, если для любого кодового подмножества A, такого что $2 \leqslant |A| \leqslant t$, существует не менее T координат i, таких что $\pi_i(A) = 1$.

В качестве примера заметим, что слабый $(2,1)$-дизъюнктивный код – это любой двоичный код, состоящий из различных слов, а слабый $(2,T)$-дизъюнктивный код – это двоичный код с минимальным кодовым расстоянием (в метрике Хэмминга) не менее T.

Обозначим через $F(t,T;L)$ максимальное число слов в слабом (t,T)-дизъюнктивном коде длины L, а через $R_F(t,T;L) = L^{-1}\log_2 F(t,T;L)$ – соответствующую максимальную скорость. Докажем следующий аналог границы Варшамова – Гилберта для слабых (t,T)-дизъюнктивных кодов.

Теорема 2. *Для фиксированных t и T*

$$\liminf_{L} R_F(t,T;L) \geqslant \frac{1}{t}\Big(1-\frac{1}{t}\Big)^{t-1}\log_2 e > \frac{\log_2 e}{et}. \tag{20}$$

Доказательство. Рассмотрим случайный двоичный код C мощности M и длины L, в котором координаты кодовых слов выбираются независимо с вероятностью $p = t^{-1}$ того, что координата равна 1. Возьмем произвольное множество A из t' слов кода C, $2 \leqslant t' \leqslant t$, и посчитаем вероятность $\mathcal{P}$ того, что для i-й координаты $\pi_i(A) = 1$. Очевидно, что

$$\mathcal{P} = \mathcal{P}(t') = t'p(1-p)^{t'-1}. \tag{21}$$

Тогда для вероятности p_{bad} того, что у A нет искомых T координат, справедливо

$$p_{\text{bad}} = p_{\text{bad}}(t') = \sum_{i=0}^{T-1} C_L^i \mathcal{P}^i (1-\mathcal{P})^{L-i} = (1-\mathcal{P})^L \sum_{i=0}^{T-1} C_L^i \left(\frac{\mathcal{P}}{1-\mathcal{P}}\right)^i. \tag{22}$$

В силу того, что $\mathcal{P} \leqslant 1/2$ и

$$\sum_{i=0}^{T-1} C_L^i < L^T$$

при $L > 1$, получаем, что $p_{\text{bad}} = p_{\text{bad}}(t') \leqslant (1-\mathcal{P})^L L^T$.

Так как имеется всего $C_M^{t'} < M^{t'}$ различных t'-подмножеств, то для вероятности P_{bad} того, что существует хотя бы одно “плохое” t'-подмножество A, т.е. такое, у которого нет T искомых координат, справедливо неравенство $P_{\text{bad}} < M^{t'} p_{\text{bad}}$. Потребуем, чтобы

$$P_{\text{bad}}(t') < M^{t'} p_{\text{bad}}(t') \leqslant (2t)^{-1}, \tag{23}$$

для чего достаточно, чтобы выполнялось неравенство

$$M = M(t') \leqslant \big(2tL^T(1-\mathcal{P}(t'))^L\big)^{-1/t'}. \tag{24}$$

Оценим теперь скорость кода $R(t') := \dfrac{1}{L}\log_2 M(t')$:

$$\begin{aligned} R(t') &\geqslant -\frac{1}{t'}(\log_2(1-\mathcal{P}(t')) + o(1) \geqslant \frac{1}{t'}\mathcal{P}(t')\log_2 e + o(1) = \\ &= t^{-1}(1-t^{-1})^{t'-1}\log_2 e + o(1), \end{aligned} \tag{25}$$

где второе неравенство следует из оценки $\ln(1+x) \leqslant x$. Так как правая часть (25) монотонно убывает по t', то выберем $t' = t$ и итоговую скорость кода

$$R := \frac{1}{t}\Big(1-\frac{1}{t}\Big)^{t-1}\log_2 e + o(1) > \frac{\log_2 e}{et} + o(1).$$

Тогда для случайного кода с данной скоростью вероятность того, что при некотором t' не выполнено требуемое условие – для любого t'-подмножества кода существует как минимум T искомых координат – не превосходит $(2t)^{-1}$ (см. (23)). Так как таких условий не более t, то следовательно, с вероятностью не меньше $1/2$ случайный код является слабым (t,T)-дизъюнктивным кодом. ▲

Перейдем теперь к доказательству того, что слабый (t,T)-дизъюнктивный код позволяет найти мощность коалиции в присутствии шума и, более того, приведем алгоритм вычисления мощности коалиции.

Рассмотрим следующие *непересекающиеся* отрезки на числовой оси:

$$S_k := \left[\frac{1}{k} - \frac{1}{2t^2}, \frac{1}{k} + \frac{1}{2t^2}\right], \quad k = 1, 2, \ldots, t.$$

Пусть C – слабый (t,T)-дизъюнктивный код, $A \subset C$ – некоторая коалиция мощности не более t и $\widehat{\boldsymbol{y}} = \boldsymbol{x} + |A|^{-1}\boldsymbol{w}^{(A)} + \boldsymbol{e}$ – ложная копия $\boldsymbol{x}$, распространяемая этой коалицией (напомним, что $\boldsymbol{w}^{(A)} := \sum\limits_{\boldsymbol{w} \in A} \boldsymbol{w}$). Так как дистрибьютор знает $\boldsymbol{x}$, то он может вычислить $\boldsymbol{z} := \widehat{\boldsymbol{y}} - \boldsymbol{x}$.

Алгоритм нахождения мощности коалиции

1. Вычислить $q_k := |\{i : z_i \in S_k\}|$.
2. Положить мощность коалиции равной максимальному k, такому что $q_k \geqslant T/2$, $k \leqslant t$.

Лемма 2. *Для любого слабого (t,T)-дизъюнктивного кода алгоритм правильно находит мощность коалиции, если длина шума*

$$\|\boldsymbol{e}\| \leqslant \delta = \frac{\sqrt{T}}{2\sqrt{2}} t^{-2}.$$

Доказательство. Из определения кода и того, что $\boldsymbol{z} := \widehat{\boldsymbol{y}} - \boldsymbol{x} = |A|^{-1}\boldsymbol{w}^{(A)} + \boldsymbol{e}$, следует, что как минимум $T/2$ координат z_i попадут в отрезок $S_{|A|}$. Действительно, из определения слабого (t,T)-дизъюнктивного кода следует, что по меньшей мере T координат вектора $|A|^{-1}\boldsymbol{w}^{(A)}$ равны $1/|A|$, и следовательно, если более $T/2$ этих координат вектора $\boldsymbol{z}$ не принадлежат отрезку $S_{|A|}$, то для квадрата длины вектора шума справедливо неравенство

$$\|\boldsymbol{e}\|^2 > \frac{T}{2}\left(\frac{1}{2t^2}\right)^2 = \delta^2,$$

что противоречит предположению $\|\boldsymbol{e}\| \leqslant \delta$.

Предположим, что есть такое k, что $|A| < k \leqslant t$ и $q_k \geqslant T/2$. Пусть координата z_i попала в отрезок S_k. Если $w_i^{(A)} \geqslant 1$, то

$$|e_i| \geqslant \frac{w_i^{(A)}}{|A|} - \left(\frac{1}{k} + \frac{1}{2t^2}\right) \geqslant \frac{1}{|A|} - \left(\frac{1}{k} + \frac{1}{2t^2}\right) \geqslant \frac{1}{t(t-1)} - \frac{1}{2t^2} > \frac{1}{2t^2}.$$

Если же $w_i^{(A)} = 0$, то

$$|e_i| \geqslant t^{-1} - (2t^2)^{-1} > \frac{1}{t^2} - \frac{1}{2t^2} > \frac{1}{2t^2}.$$

Общее число таких координат, которые могли бы привести к неправильному определению $|A|$, равно q_k. Тогда $\|\boldsymbol{e}\|^2 > q_k(2t^2)^{-2}$, а так как по предположению леммы

$\|\boldsymbol{e}\|^2 \leqslant \frac{T}{2}(2t^2)^{-2}$, то $q_k < T/2$, и следовательно, алгоритм не может выдать k как свой выход, что и требовалось доказать. ▲

§ 5. Выбор кодов

Естественно выбрать параметры d и T таким образом, чтобы обеспечиваемый леммами 1 и 2 уровень шума δ совпадал. Таким образом,

$$\delta = \frac{\sqrt{d}}{2t} = \frac{\sqrt{T}}{2\sqrt{2}t^2},$$

или, что то же самое, $T = 2dt^2$. Всюду далее и t, и δ – константы.

Напомним, что мы строим код следующим образом. Мы начинаем с t-МППК-кода мощности $M = 2^\ell$ и длины $m = \ell t$. Затем мы удлиняем слова этого кода, рассматривая их как информационные последовательности для линейного (n, m)-кода V с минимальным кодовым расстоянием d. Известная в этом случае избыточность $r_V = n - m$ кода V имеет порядок $\frac{d}{2}\log_2 n$ и достигается, если взять соответствующие двоичные коды БЧХ или Гоппы. Заметим, что это удлинение не влияет на асимптотику итоговой длины кода. Следующее удлинение (конкатенация) происходит с помощью слабого (t, T)-дизъюнктивного кода длины L. Ясно, что дистрибьютору следует выбрать длины кодов так, чтобы мощности кодов были (примерно) равными, т.е.

$$t^{-1}n \approx t^{-1}L\gamma_t \log_2 e, \quad \text{где} \quad \gamma_t = (1 - t^{-1})^{t-1}.$$

Итоговая длина кода $\widetilde{m}$ равна $n + L$, и следовательно, для скорости $\mathcal{R}(\widetilde{m}, t, \delta)$ наилучшего (t, δ)-мультимедийного кода со свойством полного поиска коалиций, устойчивого к атаке усреднения и δ-шуму, справедлива следующая асимптотическая оценка:

$$\mathcal{R}(\widetilde{m}, t, \delta) \geqslant \frac{\gamma_t \log_2 e}{t(1 + \gamma_t \log_2 e)} + o(1) > \frac{1}{t(1 + e(\log_2 e)^{-1})} + o(1) > \frac{0{,}346}{t} + o(1),$$

что и завершает доказательство теоремы 1. ▲

Таким образом, мы доказали существование мультимедийных кодов со скоростью не меньше $0{,}346t^{-1}$, способных находить целиком коалицию из не более чем t недобросовестных пользователей, которые применяют атаку усреднения и целенаправленный шум ограниченной евклидовой длины. Отметим, что главный член асимптотики скорости кода (см. выше) зависит от t, но не зависит от длины шума δ.

§ 6. Заключение

В заключение следует отметить, что рассмотренные в этой статье задачи близки к задаче о евклидовых “дизьюнктивных” кодах, см. [25, 26], которую можно получить, если неравенство (14) в определении 2 заменить на

$$\left\| \sum_{j \in A} \boldsymbol{w}_j - \sum_{j \in B} \boldsymbol{w}_j \right\| > 2\delta. \tag{26}$$

Другое отличие состоит в том, что в задаче из [25, 26] в качестве $\boldsymbol{w}_j$ рассматривались *произвольные* векторы евклидова пространства, а в данной статье – только двоичные.

Авторы считают своим приятным долгом выразить благодарность И.В. Воробьеву за полезные обсуждения.

СПИСОК ЛИТЕРАТУРЫ

1. *Fan J., Gu Y., Hachimori M., Miao Y.* Signature Codes for Weighted Binary Adder Channel and Multimedia Fingerprinting // IEEE Trans. Inform. Theory. 2020 (to appear).
2. *Wagner N.R.* Fingerprinting // Proc. 1983 IEEE Symp. on Security and Privacy. Oakland, CA, USA. April 25–27, 1983. P. 18–22.
3. *Blakley G.R., Meadows C., Purdy G.B.* Fingerprinting Long Forgiving Messages // Advances in Cryptology—CRYPTO'85 (Proc. Conf. on the Theory and Application of Cryptographic Techniques. Santa Barbara, CA, USA. August 18–22, 1985). Lect. Notes Comp. Sci. V. 218. Berlin: Springer, 1986. P. 180–189.
4. *Chor B., Fiat A., Naor M.* Tracing Traitors // Advances in Cryptology—CRYPTO'94 (Proc. 14th Annu. Int. Cryptology Conf. Santa Barbara, CA, USA. August 21–25, 1994). Lect. Notes Comp. Sci. V. 839. Berlin: Springer, 1994. P. 257–270.
5. *Hollmann H.D.L., van Lint J.H., Linnartz J.-P., Tolhuizen L.M.G.M.* On Codes with the Identifiable Parent Property // J. Combin. Theory Ser. A. 1998. V. 82. № 2. P. 121–133.
6. *Boneh D., Shaw J.* Collusion-Secure Fingerprinting for Digital Data // IEEE Trans. Inform. Theory. 1998. V. 44. № 5. P. 1897–1905.
7. *Barg A., Blakley G.R., Kabatiansky G.A.* Digital Fingerprinting Codes: Problem Statements, Constructions, Identification of Traitors // IEEE Trans. Inform. Theory. 2003. V. 49. № 4. P. 852–865.
8. *Tardos G.* Optimal Probabilistic Fingerprint Codes // Proc. 35th Annu. ACM Symp. on Theory of Computing (STOC'03). San Diego, CA, USA. June 9–11, 2003. P. 116–125.
9. *Trappe W., Wu M., Wang Z.J., Liu K.J.R.* Anti-Collusion Fingerprinting for Multimedia // IEEE Trans. Signal Process. 2003. V. 51. № 4. P. 1069–1087.
10. *Liu K.J.R., Trappe W., Wang Z.J., Wu M., Zhao H.* Multimedia Fingerprinting Forensics for Traitor Tracing. Cairo, Egypt: Hindawi, 2005.
11. *Chang S.C., Wolf J.K.* On the T-User M-Frequency Noiseless Multiple-Access Channel with and without Intensity Information // IEEE Trans. Inform. Theory. 1981. V. 27. № 1. P. 41–48.
12. *Cheng M., Miao Y.* On Anti-Collusion Codes and Detection Algorithms for Multimedia Fingerprinting // IEEE Trans. Inform. Theory. 2011. V. 57. № 7. P. 4843–4851.
13. *Egorova E., Fernandez M., Kabatiansky G., Lee M.H.* Signature Codes for the A-Channel and Collusion-Secure Multimedia Fingerprinting Codes // Proc. 2016 IEEE Int. Symp. on Information Theory (ISIT'2016). Barcelona, Spain. July 10–15, 2016. P. 3043–3047.
14. *Egorova E., Fernandez M., Kabatiansky G., Lee M.H.* Signature Codes for Weighted Noisy Adder Channel, Multimedia Fingerprinting and Compressed Sensing // Des. Codes Cryptogr. 2019. V. 87. № 2–3. P. 455–462.
15. *Györfi L., Győri S., Laczay B., Ruszinkó M.* Lectures on Multiple Access Channels. Book draft, 2005. Available at `http://www.szit.bme.hu/~gyori/AFOSR_05/book.pdf`.
16. *D'yackov A.G.* On a Search Model of False Coins // Topics in Information Theory (Proc. 2nd Colloq. on Information Theory. Keszthely, Hungary. August 25–30, 1975). Colloq. Math. Soc. János Bolyai. V. 16. Amsterdam: Horth Holland, 1977. P. 163–170.
17. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
18. *Kabatiansky G., Fernandez M., Egorova E.* Multimedia Fingerprinting Codes Resistant against Colluders and Noise // Proc. 8th IEEE Int. Workshop on Information Forensics and Security (WIFS'2016). Abu Dhabi, UAE. December 4–7, 2016. P. 1–5.
19. *Ericson T., Levenshtein V.I.* Superimposed Codes in the Hamming Space // IEEE Trans. Inform. Theory. 1994. V. 40. № 6. P. 1882–1893.
20. *Влэдуц С.Г., Кабатянский Г.А., Ломаков В.В.* Об исправлении ошибок при искажениях в канале и синдроме // Пробл. передачи информ. 2015. Т. 51. № 2. С. 50–56.

21. *Kautz W.H., Singleton R.C.* Nonrandom Binary Superimposed Codes // IEEE Trans. Inform. Theory. 1964. V. 10. № 4. P. 363–377.
22. *Дьячков А.Г., Рыков В.В.* Границы длины дизъюнктивных кодов // Пробл. передачи информ. 1982. Т. 18. № 3. С. 7–13.
23. *Erdős P., Frankl P., Füredi Z.* Families of Finite Sets in Which No Set Is Covered by the Union of Two Others // J. Combin. Theory Ser. A. 1982. V. 33. № 2. P. 158–166.
24. *Erdős P., Frankl P., Füredi Z.* Families of Finite Sets in Which No Set Is Covered by the Union of r Others // Israel J. Math. 1985. V. 51. № 1–2. P. 79–89.
25. *Ericson T., Györfi L.* Superimposed Codes in $\mathbb{R}^n$ // IEEE Trans. Inform. Theory. 1988. V. 34. № 4. P. 877–880.
26. *Füredi Z., Ruszinkó M.* An Improved Upper Bound of the Rate of Euclidean Superimposed Codes // IEEE Trans. Inform. Theory. 1999. V. 45. № 2. P. 799–802.

Егорова Елена Евгеньевна
Сколковский институт науки и технологий (Сколтех)
`egorovahelene@gmail.com`
Фернандес Марсель
Политехнический университет Каталонии,
Барселона, Испания
`marcelf@entel.upc.edu`
Кабатянский Григорий Анатольевич
Сколковский институт науки и технологий (Сколтех)
`g.kabatyansky@skoltech.ru`
Мяо Ин
Университет Цукубы, Цукуба, префектура Ибараки, Япония
`miao@sk.tsukuba.ac.jp`

Поступила в редакцию
23.10.2020
После доработки
24.11.2020
Принята к публикации
24.11.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.1

© 2020 г. **Л.А. Бассалыго**

ПОПРАВКА К СТАТЬЕ “ЗАМЕЧАНИЕ К СТАТЬЕ Н. АЛОНА И М. КАПАЛЬБО «НЕБОЛЬШИЕ ЯВНЫЕ СУПЕРКОНЦЕНТРАТОРЫ»” (ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ. 2019. Т. 55. № 3. С. 106–108)

В указанной статье обнаружена существенная ошибка.

DOI: `10.31857/S0555292320040099`

Я благодарен проф. А. Явузу Оруку (факультет информатики и электронной инженерии, Университет Мэрилэнда, Колледж-Парк, США) за указание на ошибочность данной статьи. Приношу свои извинения читателям журнала.

Бассалыго Леонид Александрович
Институт проблем передачи информации
им. А.А. Харкевича РАН
`bass@iitp.ru`

Поступила в редакцию
29.10.2020
После доработки
29.10.2020
Принята к публикации
29.10.2020

АВТОРСКИЙ УКАЗАТЕЛЬ, т. 56, 2020 г.

Адрес редакции: 127051, Москва, Б. Каретный пер., 19, стр. 1, тел. (495) 650-47-39

Оригинал-макет подготовил *Д.Ю. Ногин*
по контракту с ООО «ИКЦ «АКАДЕМКНИГА»

Москва
ООО «ИКЦ «АКАДЕМКНИГА»