МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2014 № 4(26)

Свидетельство о регистрации: ПИ №ФС 77-33762
от 16 октября 2008 г.

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Адрес редакции: 634050, г. Томск, пр. Ленина, 36
E-mail: vestnik_pdm@mail.tsu.ru

В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надежности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*
Верстка *И. А. Панкратовой*

Подписано к печати 05.12.2014.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13,4. Уч.-изд. л. 15. Тираж 300 экз.

Издательство ТГУ. 634029, Томск, ул. Никитина, 4

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ И СЖАТИЯ ИНФОРМАЦИИ

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

APPLIED CODING AND DATA COMPRESSION THEORY

APPLIED GRAPH THEORY

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/26/1

УДК 512.579

О СИСТЕМАХ ОБРАЗУЮЩИХ ДИАГОНАЛЬНЫХ ПОЛИГОНОВ НАД ПОЛУГРУППАМИ ИЗОТОННЫХ И НЕПРЕРЫВНЫХ ПРЕОБРАЗОВАНИЙ

Т. В. Апраксина

Национальный исследовательский университет «МИЭТ», г. Москва, Россия

E-mail: taya.apraksina@gmail.com

Исследуются диагональные полигоны (автоматы) над полугруппами изотонных преобразований частично упорядоченного множества и непрерывных отображений топологического пространства в себя. Найдено необходимое условие цикличности диагонального правого полигона над полугруппой непрерывных отображений компакта в себя. Доказано отсутствие счётного множества образующих диагонального биполигона над полугруппой изотонных отображений множества натуральных чисел в себя. Изучаются связи между понятиями изотонности и непрерывности.

Ключевые слова: *полигон, диагональный полигон, непрерывные отображения, изотонные отображения, система образующих.*

Введение

Изотонные (то есть сохраняющие порядок) отображения $X \to Y$, где X и Y — частично упорядоченные множества, изучались многими авторами. При $X = Y$ получаем множество $O(X)$ изотонных отображений $X \to X$, которое является полугруппой относительно композиции $x(\alpha\beta) = (x\alpha)\beta$, где $x \in X$, $\alpha, \beta \in O(X)$. В случае, если рассматриваются частичные отображения $\alpha : X_1 \to X$, где $X_1 \subseteq X$, понятие изотонности может быть определено разными неэквивалентными способами [1]. Другое обобщение понятия изотонного отображения состоит в переходе от частичного порядка к квазипорядку или вообще произвольному бинарному отношению [1]. Вместе с тем можно заметить, что понятие изотонного отображения является частным случаем непрерывного отображения $X \to Y$, если X и Y наделить топологиями, естественным образом связанными с заданными на X и Y частичными порядками. Для конечных множеств X и Y это установлено в [2], а в общем случае — в п. 1 настоящей работы.

Полугруппа $C(X)$ непрерывных отображений $X \to X$ (где X — топологическое пространство) также подвергалась интенсивному изучению с алгебраической точки зрения. Этой полугруппе посвящён обстоятельный обзор [3]. Один из центральных вопросов этой теории — в каких случаях топологическое пространство X определяется с точностью до гомеоморфизма своей полугруппой $C(X)$? М. Торнтон [4] дал абстрактную характеризацию полугрупп, изоморфных полугруппе непрерывных отображений $C(X)$. Он рассмотрел гомоморфизмы этих полугрупп и показал, что любой изоморфизм между полугруппами $C(X)$ и $C(Y)$ индуцируется гомеоморфизмом или

дуальным гомеоморфизмом (это понятие определяется для некоторого класса T_0-пространств) между топологическими T_0-пространствами X и Y. Ранее Л. М. Глускин [5] доказал аналогичное утверждение для частично упорядоченных множеств с нетривиальными порядками. Б. С. Нурутдинов [6] рассматривал аналогичные вопросы определяемости топологического пространства другими полугруппами отображений, в частности полугруппами замкнутых отображений.

Далее рассматриваются полигоны над полугруппами. Хорошо известно, что полигон над полугруппой является *алгебраической моделью автомата*, где элементы множества X — состояния, а S — входные сигналы (см., например, [7]). В п. 2 и 3 изучаются полугруппы непрерывных/изотонных отображений с точки зрения их диагональных полигонов и биполигонов. Ранее автором было доказано, что для отрезка числовой прямой с обычной топологией диагональный правый полигон над полугруппой $C(X)$ непрерывных отображений $X \to X$ является циклическим. В п. 2 приводится условие на компакт X, необходимое для цикличности полигона $(C(X) \times C(X))_{C(X)}$. В п. 3 рассматривается диагональный биполигон над полугруппой $O(\mathbb{N})$ всех изотонных преобразований $\mathbb{N} \to \mathbb{N}$. Доказано отсутствие счётной системы образующих этого полигона.

1. Изотонность и непрерывность

В [2] Р. Стонг исследовал конечные топологические пространства X. Он определил U_x для $x \in X$ как пересечение всех открытых множеств, содержащих x, и отношение $\leqslant$ на X по правилу $x \leqslant y \Leftrightarrow U_x \subseteq U_y$. В случае конечного множества X пересечение любой совокупности открытых множеств открыто. Поэтому все U_x открыты. Однако данная конструкция может быть легко перенесена и на бесконечные множества X.

Пусть X — произвольное частично упорядоченное множество, не обязательно конечное. Введём на X топологию, приняв множество подмножеств вида $U_x = (-\infty, x] = \{y \in X : y \leqslant x\}$ за базу открытых множеств (тот факт, что это база топологии, проверятся непосредственно). Назовем эту топологию *порядковой топологией*. Обычно порядковая топология рассматривалась для линейно упорядоченных множеств, но и в случае частично упорядоченного множества получается топология. Легко видеть, что антисимметричность отношения $\leqslant$ равносильна тому факту, что X является T_0-пространством. Можно расссматривать квазипорядок вместо порядка, тогда от аксиомы T_0 придётся отказаться.

Утверждение 1. Пусть X, Y — частично упорядоченные множества и $\alpha : X \to Y$ — отображение. Наделим X и Y порядковыми топологиями. Тогда α изотонно в том и только в том случае, если оно непрерывно.

Доказательство. Необходимость. Пусть α изотонно. Возьмём любой элемент $y \in Y$. Так как $\{(-\infty, y] : y \in Y\}$ — база топологии в Y, то достаточно доказать, что $(-\infty, y]\alpha^{-1}$ открыто в X. Пусть $x \in (-\infty, y]\alpha^{-1}$. Тогда $x\alpha \leqslant y$. Если $x' \leqslant x$, то из изотонности α получаем, что $x'\alpha \leqslant y$, а значит, $(-\infty, x] \subseteq (-\infty, y]\alpha^{-1}$. Таким образом, $(-\infty, y]\alpha^{-1} = \bigcup\limits_{x\alpha \leqslant y} (-\infty, x]$, то есть $(-\infty, y]\alpha^{-1}$ открыто.

Достаточность. Пусть α непрерывно и $x \leqslant x'$ для некоторых $x, x' \in X$. Пусть $V = (-\infty, x'\alpha]$. Множество V открыто в Y, а так как α непрерывно, $V\alpha^{-1}$ открыто в X. Имеем $x' \in V\alpha^{-1}$. Отсюда следует, что существует элемент базы U, такой, что $x' \in U$ и $U \subseteq V\alpha^{-1}$. Имеем $U = (-\infty, u]$ для некоторого $u \in X$. Так как $x' \in U$, выполняется $x' \leqslant u$. Это влечёт $x \leqslant u$, а значит, $x \in U$. Но $U\alpha \subseteq V$. Следовательно, $x\alpha \leqslant x'\alpha$. ■

Следствие 1. Пусть X — частично упорядоченное множество, рассматриваемое как топологическое пространство с порядковой топологией. Тогда $C(X) = O(X)$.

2. Диагональные полигоны над полугруппой непрерывных отображений

Напомним понятие полигона над полугруппой. *Правым полигоном* [8] над полугруппой S называется множество X, на котором действует полугруппа S, то есть определено отображение $X \times S \to X$, $(x, s) \mapsto xs$, такое, что выполняется тождество $(xs)s' = x(ss')$ для $x \in X$, $s, s' \in S$. *Левый полигон* Y над полугруппой S определяется двойственным образом, то есть как отображение $Y \times S \to Y$, $(s, y) \mapsto sy$, причём $s(s'y) = (ss')y$ для $y \in Y$, $s, s' \in S$. Если множество X является левым полигоном над полугруппой S и правым полигоном над полугруппой T, то оно называется *биполигоном* в случае, когда выполняется условие $(sx)t = s(xt)$ при $x \in X$, $s \in S$, $t \in T$. Если S — полугруппа, то множество $S \times S$ является правым полигоном над S относительно действия $(x, y)s = (xs, ys)$ при всех $x, y, s \in S$, левым относительно действия $s(x, y) = (sx, sy)$, а также биполигоном. Назовем их *правым, левым диагональными полигонами*, а также *диагональным биполигоном* и будем обозначать $(S \times S)_S$, ${}_S(S \times S)$, ${}_S(S \times S)_S$ соответственно. Диагональный (би)полигон называется *циклическим*, если он порождается одним элементом (то есть одной парой $(a, b) \in S \times S$).

Раннее автором изучались свойства диагональных полигонов над полугруппой непрерывных отображений в случае, когда X — отрезок числовой прямой. Доказано, что диагональный правый полигон $(C(X) \times C(X))_{C(X)}$ является циклическим [9], а диагональный левый полигон ${}_{C(X)}(C(X) \times C(X))$ не является счётно порождённым [10]. В случае произвольного компакта можно получить необходимое условие цикличности диагонального полигона.

Утверждение 2. Пусть X — компакт и $|X| > 1$. Если диагональный правый полигон $(C(X) \times C(X))_{C(X)}$ циклический, то X содержит непересекающиеся подпространства X_1, X_2, гомеоморфные пространству X.

Доказательство. Предположим, что выполнены условия утверждения. Тогда существует пара $(\alpha, \beta) \in C(X) \times C(X)$, порождающая диагональный правый полигон. Если 1_X — тождественное отображение $X \to X$, то $(\alpha, \beta)\gamma = (1_X, 1_X)$ при некотором $\gamma \in C_X$. Отсюда следует, что α, β — инъективные отображения. Пусть $X_1 = X\alpha$, $X_2 = X\beta$. Очевидно, $\alpha : X \to X_1$, $\beta : X \to X_2$ — непрерывные биективные отображения, а так как X — компакт, α — гомеоморфизм между X и X_1. Аналогично получаем, что β — гомеоморфизм между X и X_2. Осталось доказать, что $X_1 \cap X_2 = \varnothing$. Пусть это не так. Тогда $x\alpha = y\beta$ при некоторых $x, y \in X$. Возьмём два различных элемента $a, b \in X$, и пусть θ_a, θ_b — константные отображения, то есть $x\theta_a = a$ и $x\theta_b = b$ при всех $x \in X$. Очевидно, что отображения θ_a, θ_b непрерывны. Следовательно, $(\alpha, \beta)\delta = (\theta_a, \theta_b)$ при некотором $\delta \in C_X$. Имеем: $a = x\theta_a = x\alpha\delta = y\beta\delta = y\theta_b = b$, что противоречит выбору элементов a и b. ■

Следует отметить, что не все компакты являются таковыми. Например, в компакте $X = \left\{0, 1, \frac{1}{2}, \frac{1}{3}, \dots\right\}$ (с обычной топологией действительных чисел) нет двух непересекающихся гомеоморфных X подпространств.

3. Диагональные биполигоны над полугруппой изотонных отображений

В работе [11] доказано, что диагональный правый полигон $(S \times S)_S$, диагональный левый полигон ${}_S(S \times S)$ и диагональный биполигон ${}_S(S \times S)_S$ являются циклическими, если $S = T(X)$, $P(X)$ или $B(X)$, где X — бесконечное множество, $T(X)$ —

полугруппа всех отображений $X \to X$, $P(X)$ — полугруппа частичных отображений, а $B(X)$ — полугруппа бинарных отношений на множестве X. Аналогичный вопрос возникает для полугруппы $O(X)$ всех *изотонных* (сохраняющих порядок) отображений $\alpha : X \to X$, где X — частично упорядоченное множество. Ранее автором были исследованы диагональные полигоны над полугруппой $O(X)$ и получены условия цикличности и конечной порожденности этих полигонов [9]. Там же доказано, что ни для какой бесконечной цепи X диагональные полигоны над полугруппой $O(X)$ не могут быть циклическими. Основной результат данной работы обобщает упомянутый результат в случае, когда X — множество натуральных чисел $\mathbb{N}$ с обычным порядком, а именно доказано, что диагональный биполигон над полугруппой изотонных отображений $O(\mathbb{N})$ не имеет счётной системы образующих.

Определение 1. Пусть α, β: $\mathbb{N} \to \mathbb{N}$ — изотонные отображения. Назовём пару (α, β) *правильной*, если выполняются следующие условия:

(i) $i\alpha \neq j\alpha$, $i\beta \neq j\beta$ при $i \neq j$;
(ii) $i\alpha \neq j\beta$ при любых i, j (т. е. $\operatorname{im}\alpha \cap \operatorname{im}\beta = \varnothing$);
(iii) для любого k существует l, такое, что $l\alpha = k$ или $l\beta = k$ (т. е. $\operatorname{im}\alpha \cup \operatorname{im}\beta = \mathbb{N}$).

Замечание 1. Если пара (α, β) принадлежит порождающему множеству (множеству образующих), но не является правильной, то существует правильная пара $(\tilde{\alpha}, \tilde{\beta})$, такая, что $(\tilde{\alpha}, \tilde{\beta})\gamma = (\alpha, \beta)$ при некотором $\gamma \in O(\mathbb{N})$. Поэтому в системе образующих пару (α, β) можно заменить на пару $(\tilde{\alpha}, \tilde{\beta})$. Далее будем считать, что система образующих состоит только из правильных пар.

Следующая лемма показывает, что в системе образующих любую пару можно заменить на правильную пару.

Лемма 1. Пусть $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ — изотонные отображения, такие, что $\operatorname{im}\alpha$, $\operatorname{im}\beta$ — бесконечные множества. Тогда существуют изотонные отображения $\tilde{\alpha}, \tilde{\beta}$, образующие правильную пару, такие, что $(\tilde{\alpha}, \tilde{\beta})\gamma = (\alpha, \beta)$ при некотором изотонном отображении γ.

Доказательство. По отображениям α, β построим множество M троек (p, t, ε) для некоторых $p, t \in \mathbb{N}$ следующим образом: $M = \{(p, t, 0) : t\alpha = p\} \cup \{(p, t, 1) : t\beta = p\}$. Множество M упорядочим лексикографически: $(p, t, \varepsilon) < (p', t', \varepsilon')$, если и только если $p < p'$, или $p = p'$, $t < t'$, или $p = p'$, $t = t'$, $\varepsilon < \varepsilon'$.

Докажем, что для каждого $p_0 \in \mathbb{N}$ существует лишь конечное число троек $(p_0, t, \varepsilon) \in$ $\in M$. Действительно, если таких троек бесконечно много, то либо троек вида $(p_0, t, 0)$, либо троек вида $(p_0, t, 1)$ бесконечно много. В первом случае $|\operatorname{im}\alpha| < \infty$, во втором случае $|\operatorname{im}\beta| < \infty$ — то и другое противоречит условию леммы. Так как число троек $(p_0, t, \varepsilon) \in M$ конечно для каждого $p_0 \in \mathbb{N}$, множество M упорядочено по типу натурального ряда. Для тройки $(p, t, \varepsilon) \in M$ пусть $N(p, t, \varepsilon)$ обозначает номер этой тройки по порядку в M. Очевидно, для любого $t \in \mathbb{N}$ имеем $(t\alpha, t, 0), (t\beta, t, 1) \in M$. Это позволяет определить отображения $\tilde{\alpha}, \tilde{\beta} : \mathbb{N} \to \mathbb{N}$ по формулам $t\tilde{\alpha} = N(t\alpha, t, 0)$, $t\tilde{\beta} = N(t\beta, t, 1)$. Проверим, что $\tilde{\alpha}, \tilde{\beta}$ — изотонные инъективные отображения. Ясно, что достаточно осуществить проверку для $\tilde{\alpha}$. Пусть $t < t'$. Тогда $t\alpha \leqslant t'\alpha$. Если $t\alpha < t'\alpha$, то $(t\alpha, t, 0) < (t'\alpha, t', 0)$, а значит, $N(t\alpha, t, 0) < N(t'\alpha, t', 0)$, то есть $t\tilde{\alpha} < t'\tilde{\alpha}$. Если $t\alpha = t'\alpha$, то $(t\alpha, t, 0) < (t'\alpha, t', 0)$, откуда $N(t\alpha, t, 0) < N(t'\alpha, t', 0)$, то есть $t\tilde{\alpha} < t'\tilde{\alpha}$.

Проверим, что $(\tilde{\alpha}, \tilde{\beta})$ — правильная пара. Условие (i) следует из инъективности отображений $\tilde{\alpha}, \tilde{\beta}$. Проверим выполнение условия (ii). Пусть $i\tilde{\alpha} = j\tilde{\beta}$. Тогда $N(i\alpha, i, 0) = N(j\beta, j, 1)$. Но это невозможно, так как $(i\alpha, i, 0) \neq (j\beta, j, 1)$. Пусть $k \in \mathbb{N}$. Рассмотрим тройку с номером k. Если это тройка $(p, t, 0)$, то $t\alpha = p$, то есть $(p, t, 0) = (t\alpha, t, 0)$, а значит, $t\tilde{\alpha} = N(t\alpha, t, 0) = k$. Если тройка с номером k имеет вид

$(p,t,1)$, то аналогично получаем, что $t\tilde{\beta}=k$. Таким образом, $k\in\operatorname{im}\alpha\cup\operatorname{im}\beta$, то есть выполнено условие (iii). Теперь построим отображение $\gamma:\mathbb{N}\to\mathbb{N}$. Пусть $s\in\mathbb{N}$ и (p,t,ε) — s-я по порядку тройка из M, то есть $s=N(p,t,\varepsilon)$. Тогда полагаем $s\gamma=p$. Ясно, что таким образом отображение γ определено корректно. Докажем, что γ изотонно. Пусть $s<s'$. При этом $s=N(p,t,\varepsilon)$, $s'=N(p',t',\varepsilon')$. Имеем $(p,t,\varepsilon)<(p',t',\varepsilon')$. Отсюда получается, что $p\leqslant p'$. Так как $p=s\gamma$ и $p'=s'\gamma$, то выполняется $s\gamma\leqslant s'\gamma$. Этим доказана изотонность отображения γ.

Осталось доказать, что $\tilde{\alpha}\gamma=\alpha$ и $\tilde{\beta}\gamma=\beta$. Пусть $t\in\mathbb{N}$, тогда $t\tilde{\alpha}=N(t\alpha,t,0)$. Отсюда $t\tilde{\alpha}\gamma=N(t\alpha,t,0)\gamma=t\alpha$. Таким образом, $\tilde{\alpha}\gamma=\alpha$. Аналогично доказывается, что $\tilde{\beta}\gamma=\beta$. ■

Приведём пример, иллюстрирующий лемму 1.

Пример 1. Пусть $\alpha=\begin{pmatrix}1&2&3&4&5&6&\cdots\\2&5&5&7&8&9&\cdots\end{pmatrix}$, $\beta=\begin{pmatrix}1&2&3&4&5&\cdots\\4&4&4&7&8&\cdots\end{pmatrix}$.

Тогда α даёт следующие тройки для множества M: $(2,1,0)$, $(5,2,0)$, $(5,3,0)$, $(7,4,0)$, $(8,5,0)$, $(9,6,0)$, …; β даёт $(4,1,1)$, $(4,2,1)$, $(4,3,1)$, $(7,4,1)$, $(8,5,1)$, …

Перенумеруем их и упорядочим: $\underbrace{(2,1,0)}_{1}$, $\underbrace{(4,1,1)}_{2}$, $\underbrace{(4,2,1)}_{3}$, $\underbrace{(4,3,1)}_{4}$, $\underbrace{(5,2,0)}_{5}$, $\underbrace{(5,3,0)}_{6}$, $\underbrace{(7,4,0)}_{7}$, $\underbrace{(7,4,1)}_{8}$, …

Следовательно,

$$\tilde{\alpha}=\begin{pmatrix}1&2&3&4&5&\cdots\\1&5&6&7&9&\cdots\end{pmatrix},\quad \tilde{\beta}=\begin{pmatrix}1&2&3&4&\cdots\\2&3&4&8&\cdots\end{pmatrix},\quad \gamma=\begin{pmatrix}1&2&3&4&5&6&7&\cdots\\2&4&4&4&5&5&7&\cdots\end{pmatrix}.$$

Положим теперь, что правильные пары изотонных преобразований $\alpha,\beta:\mathbb{N}\to\mathbb{N}$ взаимно однозначно соответствуют последовательностям $\varepsilon=(\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots)$ из нулей и единиц, в которых бесконечно много как нулей, так и единиц. Действительно, для каждого $k\in\mathbb{N}$ пусть $k\alpha$ — позиция, которую в последовательности ε занимает k-й по счёту нуль, а $k\beta$ — позиция k-й по счёту единицы. Нетрудно проверить, что тогда α,β являются изотонными преобразованиями, составляющими правильную пару. Последовательность ε восстанавливается по правильной паре (α,β) однозначно:

$$\varepsilon_i=\begin{cases}0, & \text{если } i\in\operatorname{im}\alpha,\\ 1, & \text{если } i\in\operatorname{im}\beta.\end{cases}$$

Например, если $\alpha=\begin{pmatrix}1&2&3&4&5&\cdots\\1&5&6&7&9&\cdots\end{pmatrix}$, $\beta=\begin{pmatrix}1&2&3&4&5&\cdots\\2&3&4&8&10&\cdots\end{pmatrix}$, то

$$\varepsilon=1000111010\ldots$$

Пусть $\varepsilon=(\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots)$ — последовательность из нулей и единиц.

Определение 2. *Позицией* элемента ε_i назовём индекс i и будем писать $\operatorname{pos}(\varepsilon_i)=i$.

Определение 3. *Элементарным прореживанием* последовательности нулей и единиц называется одновременное удаление i-й по счёту единицы и i-го по счёту нуля (для какого-либо i), *прореживанием* — применение элементарных прореживаний конечное или бесконечное число раз.

Далее будем писать $\varepsilon_i = 0_m$, если ε_i — m-й по счёту нуль в последовательности ε. Аналогично этому m-ю по счёту единицу в ε будем обозначать 1_m. Например, последовательность $\varepsilon = 0010110110011$ можно записать так: $\varepsilon = 0_1 0_2 1_1 0_3 1_2 1_3 0_4 1_4 1_5 0_5 0_6 1_6 1_7$. Пусть дана последовательность ε из нулей и единиц, в которой бесконечно много нулей и бесконечно много единиц. Операцию прореживания последовательности ε можно проиллюстрировать следующим образом. Если $t_1 < t_2 < t_3 \ldots$ — возрастающая последовательность натуральных чисел, то возьмём в ε те единицы и нули, которые имеют номера $t_1, t_2, t_3, \ldots$, сохраняя их порядок в ε. Полученная последовательность η будет последовательностью, полученной из ε прореживанием. Например, если $t_1 = 1$, $t_2 = 3$, $t_3 = 6$, $t_4 = 7$, $\ldots$, то прореживание ε даёт $\eta = 0101011\ldots$

Лемма 2. Пусть ε, η — последовательности из нулей и единиц, соответствующие правильным парам (α, β) и (α', β'), причём $\alpha' = \gamma\alpha\delta$, $\beta' = \gamma\beta\delta$ при некоторых $\gamma, \delta \in O(\mathbb{N})$. Тогда последовательность η можно получить из последовательности ε прореживанием.

Доказательство. Так как $\alpha' = \gamma\alpha\delta$ инъективно, то γ также инъективно. Пусть $i\gamma = t_i$ $(i = 1, 2, 3, \ldots)$. Очевидно, $t_1 < t_2 < \ldots$ Так как $\gamma\alpha\delta$ и $\gamma\beta\delta$ образуют правильную пару, то

1) $\operatorname{im}(\gamma\alpha) \cap \operatorname{im}(\gamma\beta) = \varnothing$;
2) δ инъективно на множестве $\operatorname{im}(\gamma\alpha) \cup \operatorname{im}(\gamma\beta)$.

Следовательно, $i\gamma\alpha = \operatorname{pos}(0_{t_i})$, $i\gamma\beta = \operatorname{pos}(1_{t_i})$. Таким образом, в последовательности ε выделяются нули и единицы с номерами $t_1, t_2, t_3, \ldots$ Отображение δ переведёт эту последовательность взаимно однозначно. ■

С помощью лемм 1 и 2 рассуждениями, близкими к диагональному методу Кантора, доказывается следующая теорема.

Теорема 1. Диагональный биполигон ${}_{O(\mathbb{N})}(O(\mathbb{N}) \times O(\mathbb{N}))_{O(\mathbb{N})}$ не имеет счётного множества образующих.

Доказательство. Предположим, что $M = \{(\alpha_1, \beta_1), (\alpha_2, \beta_2), (\alpha_3, \beta_3), \ldots\}$ — счётное множество образующих диагонального биполигона ${}_{O(\mathbb{N})}(O(\mathbb{N}) \times O(\mathbb{N}))_{O(\mathbb{N})}$. Выберем среди них такие пары, для которых $\operatorname{im}\alpha_i, \operatorname{im}\beta_i$ — бесконечные множества. Получаем множество M'. Множество M' конечно или счётно: $M' = \{(\alpha'_1, \beta'_1), (\alpha'_2, \beta'_2), (\alpha'_3, \beta'_3), \ldots\}$. Ввиду леммы 1 можно считать, что все $(\alpha'_i, \beta'_i) \in M$ — правильные пары. Пусть $\varepsilon^{(i)} (i = 1, 2, 3, \ldots)$ — соответствующие этим парам последовательности из нулей и единиц. Положим $A = \{\varepsilon^{(1)}, \varepsilon^{(2)}, \ldots\}$. Тогда A конечно или счётно. Пусть $B = A \times \mathbb{N}$. Ясно, что B — счётное множество. Имеем $B = \{b_1, b_2, b_3, \ldots\}$. Построим последовательность $p_1, p_2, p_3, \ldots$ натуральных чисел рекурсивно. Пусть $b_i = (\varepsilon, m)$. Число p_1 выберем таким, чтобы $p_1 > 1$ и $p_1 > a$, где a — количество нулей 0_i, таких, что $i \geqslant m$ и $\operatorname{pos} 0_i < \operatorname{pos} 1_m$. Если в последовательности ε имеет место $\operatorname{pos} 0_m > \operatorname{pos} 1_m$, то $a = 0$ и можно положить $p_1 = 2$.

Пусть числа $p_1, p_2, \ldots, p_{k-1}$ уже построены, причем $p_i > i$ при $i = 1, 2, \ldots, k-1$. Рассмотрим b_k. Пусть $b_k = (\varepsilon, m)$. Сначала выбираем, если это возможно, p_1 нулей, лежащих от 0_m до 1_m: $0_{t_1} = 0_m$, 0_{t_2}, 0_{t_3}, $\ldots$, $0_{t_{p_1}}$. Автоматически будут выбраны единицы $1_{t_1} = 0_m$, 1_{t_2}, 1_{t_3}, $\ldots$, $1_{t_{p_1}}$. Ясно, что существует лишь конечное число способов выбора нулей $0_{t_1} = 0_m$, $\ldots$, $0_{t_{p_1}}$. Далее выбираем, если это возможно, p_2 нулей между 1_{t_1} и 1_{t_2}: $0_{t_{p_1+1}}$, $0_{t_{p_1+2}}$, $\ldots$, $0_{t_{p_1+p_2}}$. Это также можно сделать лишь конечным количеством способов. Пусть выбраны нули $0_{t_{p_1+\ldots+p_{i-1}+1}}, \ldots, 0_{t_{p_1+\ldots+p_{i-1}+p_i}}$, предшествующие элемен-

ту 1_{t_i}. Так как $p_1 + \ldots + p_i > i$, то определено t_{i+1}, и если $i < k-1$, то можно выбрать следующую последовательность из нулей p_{i+1} между 1_{t_i} и $1_{t_{i+1}}$.

Последние выбранные нули — это $0_{t_{p_1+\ldots+p_{k-2}+1}}, \ldots, 0_{t_{p_1+\ldots+p_{k-2}+p_{k-1}}}$, они предшествуют элементу $1_{t_{k-1}}$. Так как $p_1+\ldots+p_{k-1} > k-1$, то t_k также определено. Обозначим через c максимальное количество нулей между $1_{t_{k-1}}$ и 1_{t_k} при всевозможных выборах нулей и единиц вышеописанным способом. Ввиду конечности количества способов выбора имеем $c \neq \infty$. Полагаем $p_k = \max\{c+1, k+1\}$. Итак, последовательность $p_1, p_2, p_3, \ldots$ построена. Пусть $\eta = 0^{p_1}10^{p_2}10^{p_3}1\ldots$ (здесь 0^p обозначает $\underbrace{0\ldots0}_{p}$). Докажем, что последовательность η не может быть получена из какой-либо последовательности $\varepsilon^{(i)} \in A$ с помощью прореживания. Действительно, пусть η получается из $\varepsilon^{(i)}$ путем прореживания, то есть выделения нулей и единиц с номерами $t_1, t_2, ...$, где $t_1 < t_2 < \ldots$ Тогда существует такое k, что $(\varepsilon^{(i)}, t_1) = b_k$. Имеем $(\operatorname{pos} 1_{k-1}) < (\operatorname{pos} 0_{p_1+\ldots+p_k}) < (\operatorname{pos} 1_{t_k})$. Из условия $p_k = \max\{c+1, k+1\}$ имеем $p_k \geqslant c+1$. Значит, между $1_{t_{k-1}}$ и 1_{t_k} всего нулей меньше чем p_k. Получили противоречие. Следовательно, последовательность η не получится из $\varepsilon^{(i)}$ прореживанием. Последовательность η соответствует некоторой правильной паре (φ, ψ) через образующие: $\varphi = \gamma\alpha_i\delta$, $\psi = \gamma\beta_i\delta$ для некоторых $\gamma, \delta \in O(\mathbb{N})$. Так как $\operatorname{im}\varphi$ и $\operatorname{im}\psi$ бесконечны, то же верно для α_i, β_i. Следовательно, $(\alpha_i, \beta_i) \in M'$. Если ε' — соответствующая этой паре последовательность из нулей и единиц, то $\varepsilon' \in A$, то есть $\varepsilon' = \varepsilon^{(i)}$ при некотором $i \in \mathbb{N}$. По лемме 2 получаем, что η полуается из $\varepsilon^{(i)}$ прореживанием. Полученное противоречие завершает доказательство теоремы. ■

Следствиями из теоремы 1 являются аналогичные утверждения для диагональных левого и правого полигонов.

Следствие 2. Диагональный левый полигон ${}_{O(\mathbb{N})}(O(\mathbb{N})\times O(\mathbb{N}))$ не имеет конечной или счётной системы образующих.

Следствие 3. Диагональный правый полигон $(O(\mathbb{N}) \times O(\mathbb{N}))_{O(\mathbb{N})}$ не имеет конечной или счётной системы образующих.

Заключение

При исследовании диагональных полигонов над полугруппами изотонных преобразований частично упорядоченного множества доказано отсутствие их счётнопорождённости в случае множества натуральных чисел для левого, правого и биполигонов. Найдены условия цикличности правого диагонального полигона над полугруппой непрерывных отображений в случае компакта.

ЛИТЕРАТУРА

1. *Ярошевич В. А.* О свойствах полугрупп частичных изотонных преобразований квазиупорядоченных множеств // Вестник МГАДА. 2011. Вып. 3(9). С. 139–144.
2. *Stong R. E.* Finite topological spaces // Trans. Amer. Math. Soc. 1996. No. 123. P. 325–340.
3. *Magill K. D. Jr.* A survey of semigroups of continuous selfmaps // Semigroup Forum. 1975/1976. V. 11. P. 189–282.
4. *Thornton M. C.* Semigroups of isotone selfmaps on partially ordered sets // J. London Math. Soc. 1976. V. 14. No. 3. P. 545–553.
5. *Глускин Л. М.* Полугруппы изотонных преобразований // Успехи матем. наук. 1961. № 16:5(101). С. 157–162.
6. *Нурутдинов Б. С.* Топологии пространств, описываемые полугруппами отображений // Вестник МГУ. Сер. Математика, Механика. 1973. № 4. С. 24–29.

7. *Плоткин Б. И., Гринглаз Л. Я., Гварамия А. А.* Элементы алгебраической теории автоматов. М.: Высшая школа, 1994.
8. *Kilp M., Knauer U., and Mikhalev A. V.* Monoids, acts and categories. Berlin; New York: de Gruyter, 2000.
9. *Апраксина Т. В.* Диагональные полигоны над полугруппами изотонных преобразований // Чебышевский сб. 2011. № 12:1. С. 10–16.
10. *Апраксина Т. В.* Цикличность и конечнопорожденность диагональных полигонов над полугруппами преобразований // Мат. вестн. педвузов и ун-тов Волго-Вятск. региона. 2012. № 14. С. 51–58.
11. *Gallagher P. and Ruškuc N.* Generation of diagonal acts of some semigroups of transformations and relations // Bull. Austral. Math. Soc. 2005. V. 72. P. 139–146.

2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/2

УДК 519.1:511.2

СРАВНЕНИЯ ДЛЯ ЧИСЕЛ ПОЛНЫХ ОТОБРАЖЕНИЙ[1]

Л. Н. Бондаренко*, М. Л. Шарапова**

*Пензенский государственный университет, г. Пенза, Россия

**Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: leobond5@mail.ru

Для чисел стандартных полных отображений и для чисел стандартных сильных полных отображений получены сравнения по модулю простого числа. Доказательства основаны на рассмотрении свойств некоторых статистик и чисел Эйлера на соответствующих множествах перестановок. Получены аналогичные результаты для этих множеств с учётом знака их элементов.

Ключевые слова: *полные отображения, перестановка, статистика, числа Эйлера, смещение перестановки.*

Введение

Все перестановки симметрической группы S_{n-1} над алфавитом $\{1,\dots,n-1\}$, вычитание из которых единичной перестановки $\varepsilon \in S_{n-1}$ приводит к перестановке из S_{n-1}, определяют множество $CM(\mathbb{Z}_n)$ стандартных полных отображений. Если сложение $\varepsilon \in S_{n-1}$ с перестановкой из $CM(\mathbb{Z}_n)$ также приводит к перестановке из S_{n-1}, то все такие перестановки задают множество $SCM(\mathbb{Z}_n)$ стандартных сильных полных отображений [1]. Рассматриваемое сложение (вычитание) перестановок выполняется посимвольно по $\bmod n$, т. е. на аддитивной группе $\mathbb{Z}_n$, отождествляемой с множеством $\{0,1,\dots,n-1\}$; такие операции с перестановками находят применение, в частности, в криптографии.

В работе [1] показано, что задачи вычисления чисел $\#CM(\mathbb{Z}_n)$ и $\#SCM(\mathbb{Z}_n)$ не являются #P-полными, но являются трудными вычислительными проблемами.

В [2] доказан ряд утверждений о делимости перманента $P_n = \operatorname{per}(\omega^{km})_{k,m=0}^{n-1}$, где $\omega = \exp(2\pi i/n)$ — корень n-й степени из единицы, а $(n \times n)$-матрица Шура $(\omega^{km})_{k,m=0}^{n-1}$ встречается в теории чисел, теории кодирования, комбинаторном анализе и т. п. В [3] вычисление чисел P_n сведено к нахождению мощности множества $CM(\mathbb{Z}_n)$ с учётом знака его элементов.

В настоящей работе получены некоторые сравнения для $\#CM(\mathbb{Z}_n)$ и $\#SCM(\mathbb{Z}_n)$, а также для мощностей множеств $CM(\mathbb{Z}_n)$ и $SCM(\mathbb{Z}_n)$ с учётом знака их элементов. Эти результаты связаны с нахождением сравнений по простым модулям для чисел Эйлера на соответствующих множествах перестановок.

1. Свойства некоторых статистик и отображений

При делении с остатком мощности некоторого множества на заданное число можно разбить это множество на части, для которых этот вопрос решается проще, а затем использовать полученные результаты. Этот подход удобно применять для достаточно сложных по структуре множеств перестановок, определяя понятие статистики как неотрицательной целочисленной функции, заданной для каждой перестановки рассматриваемого множества.

[1]Работа поддержана грантом РФФИ № 14-01-00273.

Например, статистика $\mathrm{des}(\sigma) = \#\{i : 1 \leqslant i \leqslant n-1,\ \sigma_i > \sigma_{i+1},\ \sigma_n = 0\}$ при фиксированном $n \geqslant 2$ описывает число спусков перестановки $\sigma = \sigma_1 \dots \sigma_{n-1} \in S_{n-1}$, т. е. спуск учитывается также на последнем символе перестановки, и индуцирует производящий многочлен Эйлера

$$A_{n-1}(t) = \sum_{\sigma \in S_{n-1}} t^{\mathrm{des}(\sigma)} = \sum_{k=1}^{n-1} A_{n-1,k}\, t^k, \tag{1}$$

коэффициенты которого $A_{n-1,k} = \#\{\sigma : \sigma \in S_{n-1},\ \mathrm{des}(\sigma) = k\}$ называются числами Эйлера [4]. Так как $\#S_{n-1} = A_{n-1}(1)$, остаток от деления $\#S_{n-1}$ на n можно найти, используя остатки от деления чисел $A_{n-1,k}$, $k = 1, \dots, n-1$, на n.

При исследовании делимости мощностей некоторых множеств перестановок полезно ввести некоторые отображения.

Зададим биекцию $\mathbf{c} : S_{n-1} \to S_{n-1}$, определяющую дополнение $\overline{\sigma} = \mathbf{c}\sigma$ к перестановке $\sigma = \sigma_1\sigma_2 \dots \sigma_{n-1} \in S_{n-1}$, с помощью равенств $\mathbf{c}\sigma_i = n - \sigma_i$, $1 \leqslant i \leqslant n-1$.

Непосредственно из этого определения следует, что отображение $\mathbf{c}$ есть инволюция, а $\sigma + \overline{\sigma} = 0$, причём элементарное равенство $\mathrm{des}(\sigma) + \mathrm{des}(\overline{\sigma}) = n$ влечёт соотношение $t^n A_{n-1}(t^{-1}) = A_{n-1}(t)$, т. е. $A_{n-1,k} = A_{n-1,n-k}$, $k = 1, \dots, n-1$.

Статистика $\mathrm{des}(\sigma^*)$ для расширения $\sigma^* = \sigma_1 \dots \sigma_{n-1}0 \in S_n$ перестановки $\sigma \in S_{n-1}$ обладает свойством $\mathrm{des}(\sigma^*) = \mathrm{des}(\sigma) + 1$, и справедливо простое равенство

$$\mathrm{des}(\sigma) = \frac{1}{n} \sum_{i=0}^{n-1} (\sigma_{i+1} - \sigma_i),\ \sigma_0 = \sigma_n = 0, \tag{2}$$

где разности под знаком суммы вычисляются по модулю n.

На симметрической группе S_n в [5] применяются биекции $\mathbf{t} : S_n \to S_n$ и $\mathbf{u} : S_n \to S_n$, задаваемые для перестановки $\pi = \pi_1 \dots \pi_n \in S_n$ над алфавитом $\{0, 1, \dots n-1\}$ соотношениями $\mathbf{t}\,\pi{=}\pi_2 \dots \pi_n\pi_1$ и $\mathbf{u}\,\pi_i = \pi_i + 1 \bmod n$, $1 \leqslant i \leqslant n$.

Преобразования переноса $\mathbf{t}$ и единичного сдвига $\mathbf{u}$ позволяют ввести отношение эквивалентности на S_n: перестановки $\sigma, \tau \in S_n$ называются эквивалентными, если найдутся такие целые числа k и m, что $\mathbf{t}^k\mathbf{u}^m\sigma = \tau$. Мощность фактор-множества по этому отношению эквивалентности вычисляется по формуле

$$\frac{1}{n^2} \sum_{d|n} \varphi^2\,(n/d)\,(n/d)^d\,d!, \tag{3}$$

где $\varphi(n)$ — функция Эйлера [5].

Определение 1. Биекцию $\mathbf{d} : S_{n-1} \to S_{n-1}$, задающую смещение перестановки $\sigma = \sigma_1 \dots \sigma_{n-1} \in S_{n-1}$, опишем выражениями

$$(\mathbf{d}\,\sigma)^* = \mathbf{t}\,\mathbf{u}^{-\sigma_1}\sigma^*,$$

а порядком $d(\sigma)$ перестановки $\sigma \in S_{n-1}$ (относительно операции $\mathbf{d}$) назовём наименьшее положительное целое k, для которого $\mathbf{d}^k\sigma = \sigma$.

Определение 1 позволяет аналогично работе [5] ввести отношение эквивалентности на S_{n-1}: перестановки $\sigma, \tau \in S_{n-1}$ назовём эквивалентными, если найдётся такое целое число k, что $\mathbf{d}^k\sigma = \tau$; мощность соответствующего фактор-множества по этому отношению эквивалентности вычисляется также по формуле (3). Поэтому $d(\sigma)|n$, а мощность каждого класса эквивалентности, содержащего перестановку $\sigma \in S_{n-1}$, совпадает с порядком $d(\sigma)$.

Лемма 1. Для $\sigma \in S_{n-1}$ справедливо равенство $\mathrm{des}(\mathbf{d}\,\sigma) = \mathrm{des}(\sigma)$.

Доказательство. Записывая, согласно определению 1, смещение $\mathbf{d}$ перестановки $\sigma = \sigma_1 \dots \sigma_{n-1} \in S_{n-1}$ в виде $\mathbf{d}\,\sigma = (\sigma_2 - \sigma_1) \dots (\sigma_{n-1} - \sigma_1)(n - \sigma_1)$, где разности вычисляются по модулю n, и применяя соотношение (2), получаем требуемое. ■

Статистика $\operatorname{inv}(\pi) = \#\{(i,j) : 1 \leqslant i < j \leqslant n, \pi_i > \pi_j\}$ задаёт число инверсий перестановки $\pi \in S_n$ [4], причём $\operatorname{inv}(\sigma^*) = \operatorname{inv}(\sigma) + n - 1$. С помощью этой статистики определяется знак $\operatorname{sgn}(\sigma) = (-1)^{\operatorname{inv}(\sigma)}$ перестановки $\sigma \in S_{n-1}$.

Лемма 2. Если n нечётно, то $\operatorname{sgn}(\mathbf{d}\,\sigma) = \operatorname{sgn}(\sigma)$, $\sigma \in S_{n-1}$.

Доказательство. Для перестановки $\pi \in S_n$ с $\pi_i = 0$, где $1 \leqslant i \leqslant n$, легко устанавливается равенство $\operatorname{inv}(\mathbf{u}^{-1}\pi) = \operatorname{inv}(\pi) + n - 2i + 1$, применение которого совместно с определением 1 даёт требуемый результат. ■

Леммы 1 и 2 показывают, что по введённому отношению эквивалентности перестановки каждого класса эквивалентности на S_{n-1} характеризуются одинаковым числом спусков и при нечётном n имеют одинаковый знак.

Использование знака перестановок на S_{n-1} позволяет определить производящий многочлен

$$B_{n-1}(t) = \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma)\, t^{\operatorname{des}(\sigma)} = \sum_{k=1}^{n-1} B_{n-1,k}\, t^k, \tag{4}$$

коэффициенты которого $B_{n-1,k}$, $k = 1, \dots, n-1$, также назовём числами Эйлера, но с учётом знака элементов множества S_{n-1}.

Пусть множество $R_n = \{r\varepsilon : r \in \{1, \dots, n-1\}, (r,n) = 1, \varepsilon \in S_{n-1}\}$ образовано умножением чисел r из приведённой системы вычетов по модулю n на единичную перестановку $\varepsilon \in S_{n-1}$ (умножение выполняется посимвольно по модулю n и $\#R_n = \varphi(n)$). Тогда имеет место следующее утверждение.

Лемма 3. Если $r\varepsilon \in R_n$, то $\operatorname{des}(r\varepsilon) = r$, а для простого нечётного числа $n = p$ справедливо равенство $\operatorname{sgn}(r\varepsilon) = \left(\dfrac{r}{p}\right)$, где $\left(\dfrac{r}{p}\right)$ — символ Лежандра.

Доказательство. Соотношение $\operatorname{des}(r\varepsilon) = r$ устанавливается с помощью формулы (2), а равенство $\operatorname{sgn}(r\varepsilon) = \left(\dfrac{r}{p}\right)$ получено И. И. Золотаревым (см. [6]). ■

Отметим, что применение операции композиции перестановок позволяет найти выражение для знака $r\varepsilon \in R_n$ и при составном n.

2. Сравнения для чисел Эйлера на S_{n-1}

Известная теорема Вильсона [7] утверждает, что $(p-1)! \equiv -1 \pmod p$, где p — простое число. Так как $A_{p-1}(1) = \#S_{p-1} = (p-1)!$, новое доказательство этой теоремы может быть получено с помощью явного выражения для чисел Эйлера $A_{p-1,k}$, $k = 1, \dots, p-1$.

Для чисел $A_{n,k}$, $k = 1, \dots, n$, методом математической индукции нетрудно доказать следующее известное рекуррентное соотношение [8]:

$$A_{0,k} = \delta_{0k},\ A_{n,k} = kA_{n-1,k} + (n-k+1)A_{n-1,k-1},\ k \in \mathbb{Z},\ n \geqslant 1, \tag{5}$$

в котором δ_{ij} — символ Кронекера.

Действительно, если (5) верно для $\sigma \in S_{n-1}$ над алфавитом $\{1, \dots, n-1\}$, то для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-1}$ с $\operatorname{des}(\sigma) = k$ символ 0 можно вставить k способами, а из $\sigma \in S_{n-1}$ с $\operatorname{des}(\sigma) = k-1$ — $(n-k+1)$ способами.

С помощью формулы (5) находится рекуррентное соотношение

$$A_0(t) = 1,\ A_n(t) = ntA_{n-1}(t) + t(1-t)A'_{n-1}(t),\ n \geqslant 1, \tag{6}$$

и известная формула Ворпицкого [8]

$$t^n = \sum_{k=1}^{n} A_{n,k} \binom{t+k-1}{n},$$

а её обращение в смысле Мебиуса приводит к выражению для чисел Эйлера

$$A_{n,k} = \sum_{i=0}^{k-1} (-1)^i \binom{n+1}{i} (k-i)^n. \tag{7}$$

В частности, имеем $A_{n,1} = A_{n,n} = 1$.

Малая теорема Ферма [7] и формула (7) сразу дают следующее утверждение, из которого легко выводится теорема Вильсона.

Теорема 1. Для простого p имеем $A_{p-1,k} \equiv 1 \pmod{p},\ k = 1, \ldots, p-1$.

Доказательство. Приведём косвенное получение сравнений теоремы 1 без использования выражения (7) для чисел Эйлера. При $n = p$ приведённая система вычетов состоит из чисел $r = 1, \ldots, p-1$, порядок $d(r\varepsilon) = 1$, а для перестановок $\sigma \in S_{p-1} \setminus R_p$ порядок $d(\sigma) = p$. Поэтому применение лемм 1 и 3 дает требуемый результат. ■

Отметим, что из равенства $\#S_{n-1} = (n-1)!$ при составном n непосредственно находим $\#S_{n-1} \equiv 0 \pmod{n}$. Мощность множества S_{n-1} с учётом знака его элементов равна нулю, т. е. $B_{n-1}(1) = 0$, $n > 2$. Покажем, что и для множества S_n с учётом знака его элементов существуют аналоги выражений (5) и (6).

Теорема 2. Числа Эйлера $B_{n,k}$, $k = 1, \ldots, n$, с учётом знака элементов множества S_n удовлетворяют следующему рекуррентному соотношению:

$$\begin{gathered} B_{0,k} = \delta_{0k},\ B_{1,k} = \delta_{1k}, \\ B_{n,k} = kB_{n-2,k} + (n-2k+1)B_{n-2,k-1} - (n-k+1)B_{n-2,k-2},\ k \in \mathbb{Z},\ n \geqslant 2, \end{gathered} \tag{8}$$

справедливы также рекуррентная формула

$$B_0(t) = 1,\ B_1(t) = t,\ B_n(t) = t(1-t)((n-1)B_{n-2}(t) + (1-t)B'_{n-2}(t)),\ n \geqslant 2 \tag{9}$$

и следующее выражение:

$$B_n(t) = A_{[(n+1)/2]}(t)(1-t)^{[n/2]},\ n \geqslant 0, \tag{10}$$

где $[\cdot]$ — целая часть числа, а $A_{[(n+1)/2]}(t)$ — многочлены Эйлера. В частности, имеем $|B_{n,1}| = |B_{n,n}| = 1$.

Доказательство. При установлении справедливости (8) методом математической индукции базис тривиален. Пусть (8) верно для S_{n-2} над алфавитом $\{2, \ldots, n-1\}$. Тогда для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-2}$ с $\operatorname{des}(\sigma) = k$ пара символов 01 вставляется k способами без изменения знака перестановок, так как число транспозиций чётно. Для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-2}$ с $\operatorname{des}(\sigma) = k-1$ пара символов 01 вставляется $(n-k)$ способами без изменения знака перестановок, а пара символов 10 вставляется $(k-1)$ раз с изменением знака перестановок. Для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-2}$ с $\operatorname{des}(\sigma) = k-2$ пара символов 10 вставляется

$(n-k+1)$ способами с изменением знака перестановок. Остальные вставки символов 0 и 1 разбиваются на пары, имеющие противоположные знаки.

Формула (9) проверяется с помощью (4) и (8), а из неё раздельно для чётных и нечётных n получается и соотношение (10). ■

Таким образом, явные выражения для чисел $B_{n,k}$, $k=1,\dots,n$, можно получить, например, с помощью соотношений (7) и (10).

Значительно легче аналог теоремы 1 для чисел Эйлера $B_{p-1,k}$, $k=1,\dots,p-1$, с учётом знака элементов множества S_{p-1} получить косвенно.

Теорема 3. Для простого p имеем $B_{p-1,k} \equiv \left(\dfrac{k}{p}\right) \pmod p$, $k=1,\dots,p-1$.

Доказательство. Как и при доказательстве теоремы 1 для $n=p$, заметим, что приведённая система вычетов состоит из чисел $r=1,\dots,p-1$, порядок $d(r\varepsilon)=1$, а для перестановок $\sigma \in S_{p-1} \setminus R_p$ порядок $d(\sigma)=p$. Поэтому применение лемм 1, 2 и 3 даёт требуемый результат. ■

Так как $\sum\limits_{k=1}^{p-1}\left(\dfrac{k}{p}\right)=0$ [7], тривиальным следствием теоремы 3 является сравнение $B_{p-1}(1)\equiv 0 \pmod p$, перекрываемое равенством $B_{n-1}(1)=0$.

3. Сравнения для чисел Эйлера на $\overline{CM}(\mathbb{Z}_n)$

Введём множество перестановок $\overline{CM}(\mathbb{Z}_n)$.

Определение 2. Перестановки $\sigma, \widetilde{\sigma} \in S_{n-1}$ назовём сопряжёнными относительно $\overline{\varepsilon} \in S_{n-1}$, если $\sigma + \widetilde{\sigma} = \overline{\varepsilon}$, а ε — единичная перестановка.

Все перестановки, удовлетворяющие определению 2, образуют множество $\overline{CM}(\mathbb{Z}_n)$. Следуя определению 2, можно задать перестановки, сопряжённые относительно любой $\tau \in S_{n-1}$, в частности, множество $CM(\mathbb{Z}_n)$ всех стандартных полных отображений [1] является множеством всех перестановок, сопряжённых относительно $\varepsilon \in S_{n-1}$, причём справедливость равенства $\#CM(\mathbb{Z}_n) = \#\overline{CM}(\mathbb{Z}_n)$ очевидна.

Числа Эйлера $\widetilde{A}_{n-1,k}$, $k=1,\dots,n-1$, на множестве $\overline{CM}(\mathbb{Z}_n)$ определим как коэффициенты многочлена $\widetilde{A}_{n-1}(t)$ вида (1), построенного на множестве перестановок $\overline{CM}(\mathbb{Z}_n)$. Аналогично числами Эйлера $\{\widetilde{B}_{n-1,k}\}_{k=1}^{n-1}$ на множестве $\overline{CM}(\mathbb{Z}_n)$ с учётом знака его элементов будем называть коэффициенты многочлена $\widetilde{B}_{n-1}(t)$ вида (4), но построенного на множестве перестановок $\overline{CM}(\mathbb{Z}_n)$ с учётом знака его элементов.

При чётном n не существует сопряжённых перестановок $\sigma, \widetilde{\sigma} \in S_{n-1}$ относительно $\overline{\varepsilon} \in S_{n-1}$. Действительно, предполагая противное и суммируя все символы перестановок левой части равенства $\sigma + \widetilde{\sigma} = \overline{\varepsilon}$, а также все символы правой части, легко получить противоречие. Поэтому в этом случае $\#CM(\mathbb{Z}_n)=0$ и $\widetilde{A}_{n-1}(t)=\widetilde{B}_{n-1}(t)=0$.

При нечётном n находим $\#CM(\mathbb{Z}_n) \equiv 1 \pmod 2$, так как в этом случае существует только одна самосопряжённая относительно $\overline{\varepsilon} \in S_{n-1}$ перестановка σ, определяемая равенством $2\sigma = \overline{\varepsilon}$.

Лемма 4. Если $\sigma \in \overline{CM}(\mathbb{Z}_n)$, n — нечётное, то $\operatorname{des}(\sigma) + \operatorname{des}(\widetilde{\sigma}) = n-1$.

Доказательство. Применение формулы (2) к сопряжённым относительно $\overline{\varepsilon} \in S_{n-1}$ перестановкам $\sigma, \widetilde{\sigma} \in S_{n-1}$ сразу дает требуемое. ■

Отметим, что множество $\widetilde{R}_n = R_n \cap \overline{CM}(\mathbb{Z}_n)$ не содержит $\overline{\varepsilon} \in S_{n-1}$. Поэтому по первой части леммы 3 имеем $\widetilde{A}_{n-1,n-1} = \widetilde{B}_{n-1,n-1} = 0$, а по лемме 4 получаем равенство

$t^{n-1}\widetilde{A}_{n-1}(t^{-1}) = \widetilde{A}_{n-1}(t)$, т. е. $\widetilde{A}_{n-1,k} = \widetilde{A}_{n-1,n-k-1}$, $k = 1, \ldots, n-2$, и имеют место равенства $\deg\widetilde{A}_{n-1}(t) = \deg\widetilde{B}_{n-1}(t) = n-2$.

Если $n > 1$ имеет разложение $n = \prod\limits_{p|n} p^{\mathrm{ord}_p(n)}$ на простые множители, то аналогично формуле для функции Эйлера $\varphi(n)$ находится выражение

$$\#\widetilde{R}_n = n\prod_{p|n}\left(1 - \frac{2}{p}\right), \tag{11}$$

которое также показывает, что $\#\widetilde{R}_n = 0$ при чётном n. Формула (11) базируется на подсчёте количества представлений числа $n-1$ суммой двух натуральных слагаемых r и s, взаимно простых с n.

Из предыдущих рассмотрений следует, что основные свойства чисел $A_{p-1,k}$ наследуются числами $\widetilde{A}_{p-1,k}$. Поэтому аналогично теореме 1 доказывается

Теорема 4. Если простое $p > 2$, то $\widetilde{A}_{p-1,k} \equiv 1 \pmod p$ для $k = 1, \ldots, p-2$; $\widetilde{A}_{p-1,p-1} = 0$.

Следствие 1. Если простое $p > 2$, то $\#CM(\mathbb{Z}_p) \equiv -2 \pmod p$.

Числа $\#CM(\mathbb{Z}_n)$ при нечётных $n = 1, 3, \ldots, 25$ приведены в [9]. Вычисления при составном n показывают, что $n|\#CM(\mathbb{Z}_n)$, но рассматриваемый подход даёт только следующее частное утверждение.

Теорема 5. $p|\#CM(\mathbb{Z}_{p^s})$ при простом $p > 2$ и $s > 1$.

Доказательство. По формуле (11) имеем $p|\#\widetilde{R}_{p^s}$, а для перестановок $\sigma \in \overline{CM}(\mathbb{Z}_{p^s}) \setminus \widetilde{R}_{p^s}$ имеем $p|d(\sigma)$. ■

Если на множестве $\overline{CM}(\mathbb{Z}_n)$ наряду с сопряжением относительно $\overline{\varepsilon} \in S_{n-1}$ рассматривать и обращение перестановки, то $\left(\widetilde{\sigma^{-1}}\right)^{-1} = \widetilde{(\widetilde{\sigma})^{-1}}$ [3], а $\overline{CM}(\mathbb{Z}_n)$ разбивается на шестёрки перестановок вида $\left\{\sigma, \widetilde{\sigma}, \sigma^{-1}, \widetilde{\sigma^{-1}}, (\widetilde{\sigma})^{-1}, \left(\widetilde{\sigma^{-1}}\right)^{-1}\right\}$, причём в некоторых шестёрках могут встречаться и одинаковые члены. Можно показать, что при $n = 6m+5$ имеются только шестёрки различных перестановок и одна тройка, содержащая самосопряжённую перестановку, т. е. $\#CM(\mathbb{Z}_{6m+5}) \equiv 3 \pmod 6$.

В работе [2] для перманентов матрицы Шура P_n получены следующие результаты:

а) $P_p \equiv p! \pmod{p^3}$ для простого $p > 3$;

б) $P_p \equiv 0 \pmod q$ для нечётных простых чисел p и q, связанных равенством $p = 2q^s + 1$ при $s \geqslant 1$;

в) если $p^s|n$ при простом p и $s \geqslant 1$, то $p^{\frac{(p^s-1)n}{(p-1)p^s}}\Big|P_n$.

Числа P_n при нечётных $n = 1, 3, \ldots, 33$ приведены в [10], причём имеет место равенство $\widetilde{B}_{n-1}(1) = (-1)^{(n-1)/2}n^{-1}P_n$ [3]. Так как основные свойства чисел $B_{p-1,k}$ наследуются числами $\widetilde{B}_{p-1,k}$, с помощью теоремы 3 получаем следующее утверждение.

Теорема 6. Если простое $p > 2$, то $\widetilde{B}_{p-1,k} \equiv \left(\frac{k}{p}\right) \pmod p$ для $k = 1, \ldots, p-2$; $\widetilde{B}_{p-1,p-1} = 0$.

Следствие 2. Если простое $p > 2$, то $\widetilde{B}_{p-1}(1) \equiv (-1)^{(p+1)/2} \pmod p$.

Доказательство. Так как $\sum\limits_{k=1}^{p-1}\left(\frac{k}{p}\right) = 0$ и $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ [7], легко находим требуемый результат. ■

Таким образом, для перманента матрицы Шура при простом $p > 2$ также имеет место сравнение $p^{-1}P_p \equiv -1 \pmod p$.

4. Сравнения для чисел Эйлера на $SCM(\mathbb{Z}_n)$

Множество всех стандартных сильных полных отображений $SCM(\mathbb{Z}_n)$ [1] задаётся равенством $SCM(\mathbb{Z}_n) = CM(\mathbb{Z}_n) \cap \overline{CM}(\mathbb{Z}_n)$.

Числа Эйлера $\widehat{A}_{n-1,k}$, $k = 1, \ldots, n-1$, на множестве перестановок $SCM(\mathbb{Z}_n)$ определим как коэффициенты многочлена $\widehat{A}_{n-1}(t)$ вида (1), построенного на множестве $SCM(\mathbb{Z}_n)$, а числами Эйлера $\widehat{B}_{n-1,k}$, $k = 1, \ldots, n-1$, на множестве перестановок $SCM(\mathbb{Z}_n)$ с учётом знака его элементов будем называть коэффициенты многочлена $\widehat{B}_{n-1}(t)$ вида (4), но построенного на множестве $SCM(\mathbb{Z}_n)$ с учётом знака его элементов.

Так как множество $\widehat{R}_n = R_n \cap SCM(\mathbb{Z}_n)$ не содержит как $\overline{\varepsilon} \in S_{n-1}$, так и $\varepsilon \in S_{n-1}$, по лемме 3 находим $\widehat{A}_{n-1,1} = \widehat{A}_{n-1,n-1} = 0$ и $\widehat{B}_{n-1,1} = \widehat{B}_{n-1,n-1} = 0$. Очевидно, что при чётном n выполняются равенства $\#SCM(\mathbb{Z}_n) = 0$ и $\widehat{A}_{n-1}(t) = \widehat{B}_{n-1}(t) = 0$; можно показать их выполнение и при n, кратном трём.

Из определения множества перестановок $SCM(\mathbb{Z}_n)$ следует, что при $\sigma \in SCM(\mathbb{Z}_n)$ также и $\overline{\sigma} \in SCM(\mathbb{Z}_n)$. Поэтому в силу равенства $\mathrm{des}(\sigma) + \mathrm{des}(\overline{\sigma}) = n$ получаем соотношение $t^n \widehat{A}_{n-1}(t^{-1}) = \widehat{A}_{n-1}(t)$, т. е. $\widehat{A}_{n-1,k} = \widehat{A}_{n-1,n-k}$, $k = 2, \ldots, n-2$, и имеют место равенства $\deg \widehat{A}_{n-1}(t) = \deg \widehat{B}_{n-1}(t) = n-2$.

Аналогично формуле (11) при нечётном $n > 1$ находится выражение

$$\#\widehat{R}_n = n \prod_{p|n} \left(1 - \frac{3}{p}\right), \tag{12}$$

которое также показывает, что $\#\widehat{R}_n = 0$ при n, кратном трём.

На множестве $SCM(\mathbb{Z}_n)$ аналогично теореме 4 доказывается

Теорема 7. Если простое число $p > 3$, то справедливы следующие соотношения: $\widehat{A}_{p-1,1} = 0$; $\widehat{A}_{p-1,k} \equiv 1 \pmod p$, $k = 2, \ldots, p-2$; $\widehat{A}_{p-1,p-1} = 0$.

Следствие 3. Если простое $p > 3$, то $\#SCM(\mathbb{Z}_p) \equiv -3 \pmod p$.

Вычисления при составном n показывают, что $n|\#SCM(\mathbb{Z}_p)$, но рассматриваемый подход даёт только следующее частное утверждение, аналогичное теореме 5 (в доказательстве вместо формулы (11) применяется (12)).

Теорема 8. $p|\#SCM(\mathbb{Z}_{p^s})$ при простом $p > 3$ и $s > 1$.

В качестве аналога теоремы 6 отметим также следующий результат.

Теорема 9. Если простое число $p > 3$, то справедливы следующие соотношения: $\widehat{B}_{p-1,1} = 0$; $\widehat{B}_{p-1,k} \equiv \left(\dfrac{k}{p}\right) \pmod p$, $k = 2, \ldots, p-2$; $\widehat{B}_{p-1,p-1} = 0$.

Следствие 4. Если простое $p > 3$, то $\widehat{B}_{p-1}(1) \equiv (-1)^{(p+1)/2} - 1 \pmod p$.

Доказательство. Так как $\sum\limits_{k=1}^{p-1} \left(\dfrac{k}{p}\right) = 0$ и $\left(\dfrac{1}{p}\right) = 1$, $\left(\dfrac{-1}{p}\right) = (-1)^{(p-1)/2}$ [7], легко находим требуемый результат. ■

Следствия 1 и 3 можно рассматривать как аналоги теоремы Вильсона для чисел стандартных полных отображений $\#CM(\mathbb{Z}_p)$ и чисел стандартных сильных полных отображений $\#SCM(\mathbb{Z}_p)$, но многие вопросы делимости этих чисел при составном n остаются открытыми.

Авторы благодарны рецензенту за внимательное прочтение статьи и ценные замечания.

ЛИТЕРАТУРА

1. *Hsiang J., Hsu D. F., and Shieh Y. P.* On the hardness of counting problems of complete mappings // Discrete Mathematics. 2004. V. 277. P. 87–100.
2. *Graham R. L.and Lehmer D. H.* On the permanent of Schur's matrix // J. Australian Math. Soc. 1976. V. 21 (Series A). Part 4. P. 487–497.
3. *Бондаренко Л. Н.* Перманенты и «аддитивные» задачи перечисления перестановок // Материалы VII Междунар. семинара «Дискретная математика и ее приложения» (29 января–2 февраля 2001 г.). Ч. III. М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. С. 335–338.
4. *Стенли Р.* Перечислительная комбинаторика. Т. 1. М.: Мир, 1990. 440 с.
5. *Moser W. O. J.* A (modest) generalization of theorems of Wilson and Fermat // Canadian Math. Bul. 1990. V. 33 (2). P. 253–256.
6. *Мельников И. Г., Славутский И. Ш.* О двух забытых доказательствах закона взаимности // Труды института истории естествознания и техники. Т. 28. История физико-математических наук. М., 1959. С. 201–218.
7. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
8. *Бондаренко Л. Н., Шарапова М. Л.* Применение обобщенной формулы Родрига в комбинаторном анализе // Изв. вузов. Поволжский регион. Физ.-мат. науки. 2011. № 4 (20). С. 44–58.
9. `http://oeis.org/A003111` — Sloane N. J. A. The on-line encyclopedia of integer sequences.
10. `http://oeis.org/A003112` — Sloane N. J. A. The on-line encyclopedia of integer sequences.

2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/3

УДК 512.548.2

ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ В КОНЕЧНОМЕРНОЙ АЛГЕБРЕ НАД ПОЛЕМ[1]

С. Ю. Катышев

ООО «Центр сертификационных исследований», г. Москва, Россия

E-mail: sairos87@mail.ru

Описывается алгоритм, сводящий с полиномиальной сложностью задачу дискретного логарифмирования в конечномерной алгебре к задаче дискретного логарифмирования над конечным полем.

Ключевые слова: *открытое распределение ключей, неассоциативные группоиды, конечномерные алгебры, дискретное логарифмирование.*

Введение

В работе [1] предложены варианты обобщения хорошо известного алгоритма Диффи — Хеллмана [2], использующего циклические группы для реализации протокола открытого распределения ключей, на случай, когда вместо группы используется неассоциативный группоид. Опишем один из вариантов предложенных обобщений.

Для элемента g конечного группоида $(\Omega, *)$ и заданного $r \in \mathbb{N}$ определим *правую r-ю степень* равенством

$$g^{[r]} = \underbrace{(\ldots((g * g) * g)\ldots)}_{r \text{ сомножителей}}.$$

Назовём g *элементом с перестановочными правыми степенями*, или *ППС-элементом*, если

$$\forall m, n \in \mathbb{N} \quad \left(g^{[m][n]} = g^{[n][m]}\right).$$

Если это тождество выполняется для всех элементов $g \in \Omega$, то будем называть $(\Omega, *)$ *ППС-группоидом.*

Алгоритм открытого распределения ключей. Выбрав (несекретный) ППС-элемент g группоида Ω, абоненты A и B независимо друг от друга выбирают произвольные числа $r_A, r_B \in \mathbb{N}$ соответственно и обмениваются элементами $g^{[r_A]}$ и $g^{[r_B]}$. Затем формируют общий секретный ключ $g^{[r_A][r_B]} = g^{[r_B][r_A]}$.

Сложность восстановления наблюдателем секретного ключа по открытой информации g, $g^{[r_A]}$, $g^{[r_B]}$ не превосходит сложности *задачи правого дискретного логарифмирования в группоиде*, т. е. сложности решения уравнения

$$g^{[x]} = h.$$

В качестве ППС-группоида могут быть выбраны конечномерные алгебры над конечным полем, обладающие свойством перестановочности степеней.

В связи с этим представляется интересным решение задачи правого дискретного логарифмирования в неассоциативной конечномерной алгебре над полем.

В работе описывается алгоритм, с полиномиальной сложностью сводящий задачу дискретного логарифмирования в конечномерной алгебре к задаче дискретного логарифмирования над конечным полем.

[1]Работа выполнена при поддержке гранта Президента РФ НШ-6260.2012.10 и Академии криптографии РФ.

1. Основные определения и предварительные результаты

Пусть $(P,+,\cdot)$ — поле из q элементов с единицей e.

P-алгеброй, или алгеброй над полем P, называют P-модуль Ω с билинейным отображением $*:\Omega\times\Omega\to\Omega$, называемым *операцией умножения* [3]. Условие билинейности операции $*$ означает выполнение законов дистрибутивности справа и слева и условия

$$\forall u,v\in\Omega, a\in P\ \ ((u*v)a=u*(va)=(ua)*v=a(u*v)).$$

Размерностью P-алгебры называют размерность $\dim\Omega=\dim_P\Omega$ пространства ${}_P\Omega$.

Пусть $\mathbf{e}=(e_1,\dots,e_n)$ — базис конечномерной алгебры ${}_P\Omega$. Тогда операция $*$ определяется заданием произведений

$$e_i*e_j=\sum_{k=1}^{n}e_k a_{ij}^{(k)}, \tag{1}$$

поскольку из (1) и условия билинейности $*$ имеем

$$\left(\sum_{i=1}^{n}e_iu_i\right)*\left(\sum_{j=1}^{n}e_jv_j\right)=\sum_{k=1}^{n}e_k\left(\sum_{i,j=1}^{n}u_ia_{ij}^{(k)}v_j\right).$$

Элементы $a_{ij}^{(k)}$ из (1) называют *структурными константами* P-алгебры, набор матриц $A_k=(a_{ij}^k)_{n\times n}$, $k=1,\dots,n$, — *матрицами структурных констант.*

Рассмотрим представление P-алгебры в базисе $\mathbf{e}$. Пусть $\vec{u},\vec{v}\in P^n$ — строки координат элементов $u,v\in\Omega$ в базисе $\mathbf{e}$; тогда строка координат произведения $u*v$ удовлетворяет равенству

$$\overrightarrow{u*v}=(\vec{u}\,A_1v^{\downarrow},\dots,\vec{u}\,A_nv^{\downarrow}). \tag{2}$$

Для удобства изложения будем рассматривать P-алгебру Ω как её представление P^n в некотором базисе $\mathbf{e}$ с операцией (2). P-алгебру P^n с матрицами структурных констант $A_1,\dots,A_n$ и умножением, определённым равенством (2), будем обозначать $\mathscr{G}(A_1,\dots,A_n)$.

Рассмотрим свойства операции умножения в P-алгебре $\mathscr{G}(A_1,\dots,A_n)$, где $A_k=$ $=(a_{ij}^{(k)})_{n\times n}$, $k=1,\dots,n$.

Равенство (2) можно записать также следующим образом:

$$\begin{aligned}&\vec{u}*\vec{v}=\vec{u}\cdot R(\vec{v}),\quad R(\vec{v})=\left(A_1v^{\downarrow}\dots A_nv^{\downarrow}\right),\\&\vec{u}*\vec{v}=\vec{v}\cdot L(\vec{u}),\quad L(\vec{u})=\left(A_1^Tu^{\downarrow}\dots A_n^Tu^{\downarrow}\right).\end{aligned} \tag{3}$$

Тогда справедливо

Утверждение 1. Для произвольного элемента $\vec{u}$ P-алгебры $\mathscr{G}(A_1,\dots,A_n)$, для любого натурального k верны равенства

$$\vec{u}^{[k+1]}=\vec{u}\,R(\vec{u})^k,\quad {}^{[k+1]}\vec{u}=\vec{u}\,L(\vec{u})^k. \tag{4}$$

На основании равенств (4) можно предложить алгоритм вычисления степени $\vec{u}^{[k]}$, аналогичный бинарному алгоритму вычисления степени элемента абелевой группы [4], имеющий сложность, полиномиально зависящую от $\log k$.

P-алгебры $(\Omega, *, +)$ и $(\Omega, \star, +)$ называют *изоморфными*, если существует невырожденное линейное преобразование ψ пространства ${}_P\Omega$ со свойством

$$\forall u, v \in \Omega \quad (\psi(u) \star \psi(v) = \psi(u * v)).$$

Будем называть элемент u *реверсивным* (справа), если для некоторого натурального t выполнено $u^{[t+1]} = u$.

Утверждение 2. Если элемент $\vec{u} = (u_1, \dots u_n)$ P-алгебры $\mathscr{G}(A_1, \dots, A_n)$ реверсивен и существует набор $c_1, \dots, c_n$ элементов поля P, такой, что

$$c_1 A_1 + \ldots + c_n A_n = 0, \tag{5}$$

то выполнено соотношение $c_1 u_1 + \ldots + c_n u_n = 0$.

Лемма 1. Если вектор $\vec{\omega} = (\omega_1, \dots, \omega_n)$ равен произведению векторов $\vec{\alpha} * \vec{\beta}$, то при условии (5) для его координат выполнено соотношение

$$c_1\omega_1 + \ldots + c_n\omega_n = 0. \tag{6}$$

Доказательство. Верна цепочка равенств
$c_1\omega_1 + \ldots + c_n\omega_n = c_1\ \vec{\alpha}\ A_1\beta^{\downarrow} + \ldots + c_n\ \vec{\alpha}\ A_n\beta^{\downarrow} = \vec{\alpha}\ (c_1A_1 + \ldots + c_nA_n)\beta^{\downarrow} = 0$. ■

Доказательство утверждения 2. Для реверсивного элемента $\vec{u}$ существует $k > 1$, такое, что $\vec{u} = \vec{u}^{[k]} = \vec{u}^{[k-1]} * \vec{u}$. Теперь утверждение 2 следует из леммы 1. ■

Пусть $\mathscr{G}' = \{\vec{w} = (w_1, \dots, w_n) \in P^n : c_1w_1 + \ldots + c_nw_n = 0\}$. Заметим, что $\mathscr{G}'$ — подалгебра алгебры $\mathscr{G}(A_1, \dots, A_n)$, причём ввиду утверждения 2 $\mathscr{G}'$ содержит все реверсивные элементы. Будем называть $\mathscr{G}'$ *подалгеброй, определённой тождеством* (6).

Утверждение 3. Пусть $\mathscr{G}(A_1, \dots, A_n)$ — алгебра над полем P и существует ненулевой набор $c_1, \dots, c_{n-1}$ элементов поля P, такой, что $A_n = c_1A_1 + \ldots + c_{n-1}A_{n-1}$. Тогда подалгебра $\mathscr{G}'$ алгебры $\mathscr{G}$, определённая тождеством $\omega_n = c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1}$, изоморфна P-алгебре $\mathscr{G}(B_1, \dots, B_{n-1})$, где матрицы $B_k = (b_{ij}^k)_{(n-1)\times(n-1)}$ для $k = 1$, $\dots, n-1$ определены соотношениями

$$b_{ij}^k = a_{ij}^k + c_j a_{in}^k + c_i a_{nj}^k + c_i c_j a_{nn}^k, \quad i, j = 1, \dots, n-1. \tag{7}$$

Доказательство. Зададим отображение $\varphi : \mathscr{G}' \to \mathscr{G}(B_1, \dots, B_{n-1})$ следующим образом: $\varphi((\omega_1, \dots, \omega_n)) = (\omega_1, \dots, \omega_{n-1})$. Очевидно, φ биективно. Покажем, что φ — гомоморфизм. По определению φ

$$\forall\ \vec{u}, \vec{v} \in \mathscr{G}'\ \left(\varphi(\vec{u} * \vec{v}) = (\vec{u}\ A_1v^{\downarrow}, \dots, \vec{u}\ A_{n-1}v^{\downarrow})\right).$$

Для $k = 1, \dots, n-1$ рассмотрим k-ю координату:

$$\vec{u}\ A_kv^{\downarrow} = \left((u_1, \dots u_{n-1}, \sum_{i=1}^{n-1} c_iu_i)A_k(v_1, \dots v_{n-1}, \sum_{i=1}^{n-1} c_iv_i)^T\right) =$$

$$= \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} u_iv_ja_{ij}^k + \sum_{i=1}^{n-1} u_i\left(\sum_{j=1}^{n-1} c_jv_j\right)a_{in}^k + \sum_{j=1}^{n-1}\left(\sum_{i=1}^{n-1} c_iu_i\right)v_ja_{nj}^k + \left(\sum_{i=1}^{n-1} c_iu_i\right)\left(\sum_{j=1}^{n-1} c_jv_j\right)a_{nn}^k.$$

Сгруппировав суммы, получаем равенство

$$\vec{u}\ A_kv^{\downarrow} = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} u_iv_j(a_{ij}^k + c_ja_{in}^k + c_ia_{nj}^k + c_ic_ja_{nn}^k) = \varphi(\vec{u})B_k\varphi(\vec{v})^T.$$

Таким образом, $\varphi(\vec{u} * \vec{v}) = \left(\varphi(\vec{u})B_1\varphi(\vec{v})^T, \ldots, \varphi(\vec{u})B_{n-1}\varphi(\vec{v})^T\right) = \varphi(\vec{u}) \star \varphi(\vec{v})$, где $\star$ — операция в $\mathscr{G}(B_1, \ldots, B_{n-1})$. ■

Следующий результат иногда позволяет решить задачу проверки перестановочности степеней и дискретного логарифмирования в алгебре меньшей размерности.

Теорема 1. В алгебре $\mathscr{G}(A_1, \ldots, A_n)$ существует подалгебра $\mathscr{G}'$, содержащая все реверсивные элементы и изоморфная некоторой алгебре $\mathscr{G}(B_1, \ldots, B_t)$, $t \leqslant n$, такой, что система матриц $B_1, \ldots, B_t$ линейно независима.

Доказательство. Индукция по $k = n - \operatorname{rank}\{A_1, \ldots, A_n\}$ с применением утверждения 3. ■

Алгебру $\mathscr{G}(B_1, \ldots, B_t)$ из теоремы 1 будем называть *приведённым видом алгебры* $\mathscr{G}(A_1, \ldots, A_n)$.

Пусть $\vec{u}$ — произвольный элемент алгебры $\mathscr{G}(A_1, \ldots, A_n)$. Для произвольного $k \in \mathbb{N}$ положим $\vec{u}^{[k]} = (u_1^r(k), \ldots, u_n^r(k))$. Тогда последовательность векторов

$$\vec{u}^{\mathbb{N}} = (\vec{u}, \vec{u}^{[2]}, \ldots, \vec{u}^{[k]}, \ldots) \tag{8}$$

можно рассматривать как вектор $\vec{u}^{\mathbb{N}} = (u_1^r, \ldots, u_n^r)$ из n координатных последовательностей

$$u_i^r = (u_i^r(1) = u_i, u_i^r(2), \ldots, u_i^r(k), \ldots), \quad i = 1, \ldots, n. \tag{9}$$

Через $\vec{u}^{[\mathbb{N}]}$ обозначим множество всех различных элементов вида $\vec{u}^{[r]}$, $r \in \mathbb{N}$.

Следующее утверждение показывает, что задачи логарифмирования и определения потенциала элемента алгебры иногда могут быть перенесены в алгебру ещё меньшей размерности.

Утверждение 4. Пусть $\vec{u}$ — элемент P-алгебры $\mathscr{G}(A_1, \ldots, A_n)$. Тогда для некоторой P-алгебры $\mathscr{G}(B_1, \ldots, B_t)$, $t \leqslant n$, существует инъективное отображение $\varphi : \vec{u}^{[\mathbb{N}]} \to \to \mathscr{G}(B_1, \ldots, B_t)$, обладающее следующими свойствами:

1) система координатных последовательностей $\{\varphi(\vec{u})_i^r : i = 1, \ldots, t\}$ линейно независима;
2) для любого натурального k верно равенство $\varphi(u^{[k]}) = (\varphi(u))^{[k]}$.

Лемма 2. Пусть $\vec{u} \in \mathscr{G}(A_1, \ldots, A_n)$ и существует ненулевой набор $c_1, \ldots, c_{n-1}$ элементов поля P, такой, что система последовательностей $\{u_1^r, \ldots, u_n^r\}$ удовлетворяет соотношению

$$u_n^r = c_1u_1^r + \ldots + c_{n-1}u_{n-1}^r. \tag{10}$$

Рассмотрим алгебру $\mathscr{G}(B_1, \ldots, B_{n-1})$ с операцией $\star$, где матрицы структурных констант B_i определены соотношением (7). Тогда отображение $\psi : \vec{u}^{[\mathbb{N}]} \to \mathscr{G}(B_1, \ldots, B_{n-1})$, $\psi((v_1, \ldots, v_n)) = (v_1, \ldots, v_{n-1})$ есть инъективное отображение со свойством

$$\psi(u^{[*r]}) = (\psi(u))^{[\star r]}. \tag{11}$$

Доказательство. В силу соотношения (10) ψ инъективно. Докажем равенство (11) методом математической индукции. При $r = 1$ равенство очевидно. Пусть при $r = m$ утверждение верно, докажем его при $r = m + 1$. Пусть $v = u^{[*m]}$, тогда по определению ψ

$$\psi(\vec{u}^{[*m+1]}) = \psi(\vec{v} * \vec{u}) = (\vec{v}\ A_1u^{\downarrow}, \ldots, \vec{v}\ A_{n-1}u^{\downarrow}).$$

В силу (10) $u_n = \sum\limits_{i=1}^{n-1} c_i u_i$ и $v_n = \sum\limits_{i=1}^{n-1} c_i v_i$. Для $k = 1, \ldots, n-1$ рассмотрим k-ю координату вектора $\vec{u}^{[*(m+1)]}$:

$$\vec{v}\ A_k u^{\downarrow} = \left((v_1, \ldots v_{n-1}, \sum_{i=1}^{n-1} c_i v_i) A_k (u_1, \ldots u_{n-1}, \sum_{i=1}^{n-1} c_i u_i)^T \right) =$$

$$= \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} v_i u_j a_{ij}^k + \sum_{i=1}^{n-1} v_i \left(\sum_{j=1}^{n-1} c_j u_j \right) a_{in}^k + \sum_{j=1}^{n-1} \left(\sum_{i=1}^{n-1} c_i v_i \right) u_j a_{nj}^k + \left(\sum_{i=1}^{n-1} c_i v_i \right) \left(\sum_{j=1}^{n-1} c_j u_j \right) a_{nn}^k.$$

Сгруппировав суммы, получаем равенство

$$\vec{v}\ A_k u^{\downarrow} = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} v_i u_j (a_{ij}^k + c_j a_{in}^k + c_i a_{nj}^k + c_i c_j a_{nn}^k) = \psi(\vec{v}) B_k \psi(\vec{u})^T.$$

Тогда $\psi\left(\vec{u}^{[*(m+1)]}\right) = \left(\psi(\vec{v})B_1\psi(\vec{u})^T, \ldots, \psi(\vec{v})B_{n-1}\psi(\vec{u})^T\right) = \psi(\vec{v}) \star \psi(\vec{u}) =$
$= (\psi(u))^{[\star(m+1)]}$. ■

Доказательство утверждения 4. Индукция с применением леммы 2 по параметру $k = n - \operatorname{rank}\{\varphi(\vec{u})_i^r : i = 1, \ldots, n\}$. ■

Алгебру $\mathscr{G}(B_1, \ldots, B_t)$ из утверждения 4 будем называть *приведённой алгеброй для элемента* $\vec{u}$.

Замечание 1. Для нахождения линейной зависимости между координатными последовательностями степеней элемента $\vec{u}$ достаточно найти линейную зависимость между столбцами матрицы, составленной из строк $\vec{u}$, $\vec{u}^{[2]}$, …, $\vec{u}^{[n]}$.

2. Дискретное логарифмирование

Для любого унитарного многочлена $F(x) \in P[x]$ и любого $n \in \mathbb{N}$ обозначим через $L_{P^n}(F)$ семейство всех линейных рекуррентных последовательностей (ЛРП) над пространством ${}_P P^n$ с характеристическим многочленом $F(x)$ [5, 6].

Утверждение 5. Последовательности $\vec{u}^{\mathbb{N}}$ из (8) и u_i^r, $i = 1, \ldots, n$, из (9) суть ЛРП с характеристическим многочленом, равным характеристическому многочлену $\chi_{R(\vec{u})}(x)$ матрицы $R(\vec{u})$ из (3): $u^{\mathbb{N}} \in L_{P^n}(\chi_{R(\vec{u})})$; $u_i^r \in L_P(\chi_{R(\vec{u})})$, $i = 1, \ldots, n$.

Доказательство проводится стандартным способом, с использованием соотношений (4) и теоремы Гамильтона — Кэли (см., например, [6, Example 1.6]). ■

Пусть Q — поле разложения многочлена $\chi_{R(\vec{u})}(x)$ над P и

$$\chi_{R(\vec{u})}(x) = (x - \alpha_1)^{k_1} \cdot \ldots \cdot (x - \alpha_t)^{k_t} \tag{12}$$

— каноническое разложение этого многочлена над Q. Тогда существует представление координатных последовательностей u_i^r через соответствующие биномиальные последовательности [5, 6]:

Следствие 1. Для любого $i \in \{1, \ldots, n\}$ существует вектор-столбец $d_i^{r\downarrow} \in Q^{(n)}$, такой, что

$$u_i^r(k) = \left(\alpha_1^{k-1}, C_{k-1}^1 \alpha_1^{k-1}, \ldots, C_{k-1}^{k_1-1}\alpha_1^{k-1},\ \alpha_2^{k-1}, \ldots, C_{k-1}^{k_2-1}\alpha_2^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) d_i^{r\downarrow}. \tag{13}$$

Для краткости будем использовать запись

$$u_i^r(k) = \left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) d_i^{r\downarrow}, \quad i \in \{1, \ldots, n\}.$$

Следствие 2. При условии (12) существует матрица $D \in Q_{n,n}$, такая, что для любого натурального k правая степень элемента $\vec{u}$ представляется в виде

$$\vec{u}^{[k]} = \left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) D. \tag{14}$$

При этом следующие утверждения равносильны:

a) система координатных последовательностей $u_1^r, \ldots, u_n^r$ последовательности $\vec{u}^{\mathbb{N}}$ линейно независима;

b) матрица D обратима.

Доказательство. Ввиду (13) матрица $D = (d_1^{r\downarrow}, \ldots, d_n^{r\downarrow}) \in Q_{n,n}$ удовлетворяет условию (14).

$(a) \Rightarrow (b)$. Если D — вырожденная матрица, то $Dc^\downarrow = 0^\downarrow$ для некоторого $c^\downarrow \in Q^{(n)} \setminus \{0^\downarrow\}$, и ввиду (14) $(u_1^r, \ldots, u_n^r)c^\downarrow = 0$, что противоречит условию (a).

$(b) \Rightarrow (a)$. Если система координатных последовательностей $u_1^r, \ldots, u_n^r$ линейно зависима, то $(u_1^r, \ldots, u_n^r)c^\downarrow = 0$ для некоторого $c^\downarrow \in Q^{(n)} \setminus \{0^\downarrow\}$. Тогда ввиду (14) для вектора $c'^\downarrow = Dc^\downarrow \neq 0^\downarrow$ выполнено равенство $\left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right) c'^\downarrow = 0^\downarrow$. Противоречие, так как система биномиальных последовательностей линейно независима. ■

Следствие 3. В условиях следствия 2 если матрица D обратима, то $\chi_{R(\vec{u})}$ есть минимальный многочлен последовательности $u^{\mathbb{N}}$.

Доказательство. Пусть $G(x) \in P[x]$ — минимальный многочлен ЛРП $u^{\mathbb{N}}$. Тогда $G(x)|\chi_{R(\vec{u})}(x)$, и если $G(x) \neq \chi_{R(\vec{u})}(x)$, то $\deg G(x) = m < n$. В таком случае система из n координатных последовательностей $u_1^r, \ldots, u_n^r$ принадлежит подпространству $L_P(G)$ размерности m и является линейно зависимой. Ввиду (14) это означает, что линейно независимая система из n биномиальных последовательностей $\left(\alpha_1^{k-1}, \ldots, C_{k-1}^{k_t-1}\alpha_t^{k-1}\right)$ при умножении на матрицу D становится линейно зависимой, что противоречит обратимости матрицы D. ■

На основании равенства (14) можно предложить метод дискретного логарифмирования. Пусть $\mathscr{G}(A_1, \ldots, A_n)$ — произвольная алгебра над некоторым полем P. Для элементов $\vec{u}, \vec{v} \in \mathscr{G}(A_1, \ldots, A_n)$ решается уравнение $\vec{u}^{[n]} = \vec{v}$.

Ввиду утверждения 4 можем считать, что рассматриваемая алгебра является приведённой алгеброй для элемента $\vec{u}$, то есть система координатных последовательностей $\{u_1^r, \ldots, u_n^r\}$ линейно независима.

Пусть Q — расширение поля P, являющееся полем разложения характеристического многочлена $\chi_R(x)$ матрицы $R = (A_1u^\downarrow, \ldots, A_nu^\downarrow)$. Элементы $\alpha_1, \ldots, \alpha_t$ — корни многочлена $\chi_R(x)$, k_i — кратность корня α_i, $i = 1, \ldots, t$.

Замечание 2. Задача нахождения корней многочлена, очевидно, сводится к разложению многочлена на неприводимые сомножители (над полем разложения). Разложение многочлена степени n на множители имеет полиномиальную трудоёмкость относительно величины $n \log |P|$, то есть относительно размера задачи $(\log |P^n|)$. Подробный обзор методов разложения многочлена на множители можно найти в [4].

Последовательность степеней элемента P-алгебры представляется в виде (14), причём матрица D обратима, так как система координатных последовательностей $\{u_i(k) : k = 1, \ldots, n\}$ линейно независима.

Для нахождения матрицы D можно решать систему, составленную из равенств (14), для различных степеней $k \in \{1, \ldots, n\}$. Однозначность нахождения матрицы D следует из линейной независимости системы биномиальных последовательностей в правой части равенства (14). Сложность вычисления матрицы D_r полиномиальна относительно размера матрицы, её можно оценить величиной $\mathrm{O}(n^3)$.

При умножении обеих частей равенства (14) на матрицу D^{-1} справа получаем

$$\vec{v}\ D^{-1} = \vec{u}^{[x]}\ D^{-1} = \left(\alpha_1^{x-1}, C_{x-1}^1\alpha_1^{x-1}, \ldots, C_{x-1}^{k_1-1}\alpha_1^{x-1},\ \alpha_2^{x-1}, \ldots, C_{x-1}^{k_2-1}\alpha_2^{x-1}, \ldots, C_{x-1}^{k_t-1}\alpha_t^{x-1}\right).$$

Пусть $\vec{v}\ D^{-1} = (w_1, \ldots, w_n)$, тогда нахождение решения уравнения (14) равносильно решению системы уравнений

$$\begin{cases} \alpha_1^{x-1} = w_1, \\ C_{x-1}^1\alpha_1^{x-1} = w_2, \\ \ldots \\ C_{x-1}^{k_1-1}\alpha_1^{x-1} = w_{k_1}, \\ \alpha_2^{x-1} = w_{k_1+1}, \\ \ldots \\ C_{x-1}^{k_t-1}\alpha_t^{x-1} = w_n. \end{cases}$$

Нетрудно показать, что решение данной системы уравнений не сложнее однократного логарифмирования в поле Q по основанию примитивного элемента.

В качестве вывода сформулируем результат.

Теорема 2. Задача дискретного логарифмирования на P-алгебре Ω размерности n с полиномиальной сложностью сводится к задаче дискретного логарифмирования в поле Q, являющемся расширением степени l поля P, где $l < n$.

Сложность задачи дискретного логарифмирования в конечном поле имеет субэкспоненциальную оценку. Подробный обзор методов дискретного логарифмирования в конечном поле можно найти, например, в [4].

ЛИТЕРАТУРА

1. *Катышев С. Ю., Марков В. Т., Нечаев А. А.* Использование неассоциативных группоидов для открытого распределения ключей // Дискретная математика. 2014. Т. 46. № 3. С. 51–59.
2. *Diffie W. and Hellman M. E.* New directories in cryptography // IEEE Trans. Inf. Theory. 1976. V. 22. P. 644–654.
3. *Пирс Р.* Ассоциативные алгебры: пер. с англ. М.: Мир, 1986. 543 с.
4. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. 2-е изд. М.: МЦНМО, 2007. 326 с.
5. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. В 2-х т. М.: Гелиос, 2003. 336 + 416 с.
6. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear recurring sequences over rings and modules // J. Math. Sci. 1995. V. 76. No. 6. P. 2793–2915.

2014 Теоретические основы прикладной дискретной математики № 4(26)
DOI 10.17223/20710410/26/4
УДК 519.7

ВЗАИМОСВЯЗЬ КОЭФФИЦИЕНТОВ ПОЛИНОМА НАД ПОЛЕМ И ВЕСА БУЛЕВОЙ ФУНКЦИИ

А. С. Кузьмин, В. И. Ноздрунов

Лаборатория ТВП, г. Москва, Россия

E-mail: vlad_vin@mail.ru

Работа посвящена изучению зависимости коэффициентов многочлена одного переменного, задающего над полем из 2^n элементов булеву функцию, от веса исследуемой функции. Получены точные формулы зависимости коэффициентов многочлена от первых двух коэффициентов веса в двоичном представлении и ограничения на линейные многообразия функций из рассматриваемых специальных классов.

Ключевые слова: *булева функция, бент-функция, многочлен над полем, вес функции, подпространство, многообразия.*

Введение

В 70-х годах прошлого века был введён класс функций, находящихся на наибольшем расстоянии, с точки зрения метрики Хемминга, от класса аффинных функций; такие функции названы О. С. Ротхаузом бент-функциями [1]. В дальнейшем в работе [2] А. Йоссефом и Г. Гонгом построен класс функций, которые находятся на наибольшем расстоянии от мономиальных функций — класс гипер-бент-функций.

Несмотря на многочисленные исследования в этой области, пока не получено полного описания данных классов функций. Этим объясняется актуальность изучения свойств бент-функций и гипер-бент-функций и поиска новых методов их анализа.

При изложении результатов удобно использовать представление булевых функций от n переменных в виде многочленов над полем $\mathrm{GF}(2^n)$. Пусть $P = \mathrm{GF}(2)$ — поле из двух элементов, $Q = \mathrm{GF}(2^n)$ — расширение поля P степени n. Булевы функции $f(x_0, x_1, \ldots, x_{n-1})$ от n переменных можно рассматривать как функции вида $F : Q \to P$. Для простоты будем считать, что $f(0, 0, \ldots, 0) = 0$.

Обозначим через $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ базис поля $\mathrm{GF}(2^n)$ как векторного пространства над полем $\mathrm{GF}(2)$, а через $\omega_0, \omega_1, \ldots, \omega_{n-1}$ — базис поля $\mathrm{GF}(2^n)$ над полем $\mathrm{GF}(2)$, двойственный к базису $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$, т. е.

$$\mathrm{tr}_1^n(\varepsilon_j \omega_k) = \begin{cases} 1, & \text{если } j = k, \\ 0, & \text{если } j \neq k, \end{cases}$$

где $\mathrm{tr}_1^n(x) = \sum\limits_{k=0}^{n-1} x^{2^k}$ — функция «след» из поля $\mathrm{GF}(2^n)$ в поле $\mathrm{GF}(2)$.

Тогда для любого набора булевых величин $x_0, x_1, \ldots, x_{n-1}$ однозначно определён элемент $x \in \mathrm{GF}(2^n)$:

$$x = \sum_{k=0}^{n-1} x_k \varepsilon_k.$$

При этом, в силу двойственности базисов, справедливо соотношение $x_k = \mathrm{tr}_1^n(\omega_k x)$. Таким образом, для булевой функции $f(x_0, x_1, \ldots, x_{n-1})$ имеет место равенство

$$f(x_0, x_1, \ldots, x_{n-1}) = f(\mathrm{tr}_1^n(\omega_0 x), \mathrm{tr}_1^n(\omega_1 x), \ldots, \mathrm{tr}_1^n(\omega_{n-1} x)),$$

задающее эту функцию в виде полинома над полем $\mathrm{GF}(2^n)$ в базисе $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$.

Обозначим $F(x) = f(\mathrm{tr}_1^n(\omega_0 x), \mathrm{tr}_1^n(\omega_1 x), \ldots, \mathrm{tr}_1^n(\omega_{n-1} x))$. Так как функция F представляется в виде многочлена над полем, то

$$F(x) = \sum_{k=1}^{2^n-1} c_k x^k, \ x \in Q. \tag{1}$$

Здесь коэффициенты c_k принадлежат полю $\mathrm{GF}(2^n)$. Заметим, что $c_0 = 0$, так как $F(0) = 0$, поэтому в формуле (1) сумма начинается с $k = 1$.

Поскольку многочлен $F(x)$ принимает только два значения 0 или 1, то он может быть представлен в виде

$$F(x) = \mathrm{tr}_1^n(\Phi(x)),$$

где $\Phi(x)$ — некоторый полином над полем $\mathrm{GF}(2^n)$. В работе [3] показано, что существует представление функции $F(x)$, в котором многочлен $\Phi(x)$ имеет вид

$$\Phi(x) = \sum_{k \in M} c'_k \xi_k x^k, \ c'_k \in Q_k, \ k \in M. \tag{2}$$

Здесь M — набор минимальных представителей всех различных циклотомических классов по модулю $2^n - 1$ [4, с. 108], $Q_k = \mathrm{GF}(2^r)$, где значение r определяется условиями $r = \min\left\{t : t > 0, \dfrac{2^n-1}{(2^n-1,k)} \big| (2^t - 1)\right\}$, а ξ_k — фиксированный элемент поля $\mathrm{GF}(2^n)$, след которого в подполе $\mathrm{GF}(2^r)$ равен 1.

Замечание 1. Из формул (1) и (2), а также из формулы $F(x) = \mathrm{tr}_1^n(\Phi(x))$ следует, что $c_k = c'_k \xi_k$, если $k \in M$. Отсюда следует также, что если $c'_k \xi_k = 0$, то $c_t = 0$ для всех таких t, что t и k лежат в одном циклотомическом классе.

1. Зависимости коэффициентов в представлении в виде многочлена над конечным полем от веса булевой функции

Рассмотрим задачу установления зависимости коэффициентов многочлена $F(x)$ от параметров двоичного разложения веса самой функции $||F|| = n_0 + 2n_1 + 4n_2 + \cdots$, где $n_i \in \{0, 1\}$. Под весом понимается сумма значений функции по всем аргументам, т. е. $||F|| = \sum\limits_{x \in Q} F(x)$, где суммирование ведётся в действительной области.

Утверждение 1. Коэффициент $c_{2^n-1} = 0$ тогда и только тогда, когда $n_0 = 0$.

Доказательство. Очевидно, что $n_0 = \sum\limits_{x \in Q} F(x)$, где суммирование ведётся в поле Q характеристики 2. Тогда

$$n_0 = \sum_{x \in Q} \sum_{k=1}^{2^n-1} c_k x^k.$$

Любой обратимый элемент x поля Q можно представить в виде θ^t для подходящего $t \in \{0, 1, \ldots, 2^n - 2\}$, где θ — примитивный элемент поля Q. Учитывая, что $c_0 = 0$, получаем

$$n_0 = \sum_{t=0}^{2^n-2} \sum_{k=1}^{2^n-1} c_k (\theta^t)^k.$$

Поменяем порядок суммирования и выделим слагаемое, соответствующее $k = 2^n - 1$:

$$n_0 = \sum_{k=1}^{2^n-2} c_k \sum_{t=0}^{2^n-2} (\theta^k)^t + c_{2^n-1} \sum_{t=0}^{2^n-2} (\theta^{2^n-1})^t.$$

Порядок θ равен 2^n-1, следовательно, вторая сумма при коэффициенте c_{2^n-1} есть суммирование единиц 2^n-1 раз; значит, она равна 1. Теперь, применяя формулу для вычисления суммы геометрической прогрессии, получаем равенство

$$n_0 = \sum_{k=1}^{2^n-2} c_k \frac{\theta^{k(2^n-1)}-1}{\theta^k-1} + c_{2^n-1} = c_{2^n-1}.$$

Таким образом, имеем, что $n_0 = 0$ тогда и только тогда, когда $c_{2^n-1} = 0$. ■

Лемма 1 [5]. Пусть $a_i \in \{0,1\}$, $i \in \{1,2,\ldots,n\}$ и $\sum\limits_{i=1}^{n} a_i = k = n_0 + 2n_1 + 4n_2 + \ldots$, где суммирование ведётся в области целых чисел. Тогда

$$n_1 = \sum_{1 \leqslant j < s \leqslant n} a_j a_s \pmod 2.$$

Теорема 1. Пусть $F : Q \to P$, $F(0) = 0$ и $||F|| = n_0 + 2n_1 + 4n_2 + \ldots$ Тогда

$$n_1 = c_{2^n-1}^2 + \sum_{k=1}^{2^{n-1}-1} c_k c_{2^n-1-k}. \tag{3}$$

Доказательство. Зафиксируем примитивный элемент θ поля Q и аналогично тому, как было сделано в лемме 1, представим элементы поля Q через элемент θ. Пусть x и y — элементы поля Q, $x = \theta^k$, $y = \theta^l$, где k, l — натуральные числа. Будем считать, что $x < y$ тогда и только тогда, когда $k < l$. Согласно лемме 1, имеем

$$n_1 = \sum_{x_1, x_2 \in Q \,:\, x_1 < x_2} F(x_1)F(x_2) = \sum_{x_1 < x_2} \left(\sum_{k=0}^{2^n-1} c_k x_1^k \sum_{l=0}^{2^n-1} c_l x_2^l \right).$$

Так как $F(0) = 0$, то $c_0 = 0$ и справедливо соотношение

$$n_1 = \sum_{0 \leqslant s < t \leqslant 2^n-2} \left(\sum_{k=1}^{2^n-1} c_k (\theta^s)^k \sum_{l=1}^{2^n-1} c_l (\theta^t)^l \right).$$

Далее, поменяв порядок суммирования, будем иметь

$$n_1 = \sum_{k,l=1}^{2^n-1} \sum_{0 \leqslant s < t \leqslant 2^n-2} c_k c_l \theta^{sk+tl} =$$

$$= \sum_{k,l=1}^{2^n-1} c_k c_l \left(\sum_{s=0, 1 \leqslant t \leqslant 2^n-2} \theta^{tl} + \theta^k \sum_{s=1,2 \leqslant t \leqslant 2^n-2} \theta^{tl} + \ldots + \sum_{s=2^n-3, t=2^n-2} \theta^{sk}\theta^{tl} \right).$$

Применим формулу геометрической прогрессии, выделив отдельно слагаемое, соответствующее $l = 2^n-1$, так как при нём $\theta^l = 1$:

$$n_1 = \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} c_k c_l \left(\frac{\theta^l(\theta^{(2^n-2)l}-1)}{\theta^l-1} + \ldots + \theta^{(2^n-3)k}\theta^{(2^n-2)l} \right) +$$

$$+ \sum_{k=1, (l=2^n-1)}^{2^n-1} c_k c_l \left(\sum_{1 \leqslant t \leqslant 2^n-2} 1 + \theta^k \sum_{2 \leqslant t \leqslant 2^n-2} 1 + \ldots + \theta^{(2^n-3)k} \right) =$$

$$= \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} c_k c_l \frac{1}{\theta^l-1} \sum_{i=1}^{2^n-2} \theta^{il}\theta^{(i-1)k} \left(\theta^{(2^n-1-i)l} - 1 \right) +$$

$$+ \sum_{k=1, (l=2^n-1)}^{2^n-1} c_k c_l \left((2^n-2) + \theta^k(2^n-3) + \ldots + \theta^{(2^n-3)k} \right).$$

Пусть

$$A = \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} c_k c_l \frac{1}{\theta^l - 1} \sum_{i=1}^{2^n-2} \theta^{il} \theta^{(i-1)k} \left(\theta^{(2^n-1-i)l} - 1\right),$$

$$B = \sum_{k=1,\ (l=2^n-1)}^{2^n-1} c_k c_l \left((2^n-2) + \theta^k(2^n-3) + \ldots + \theta^{(2^n-3)k}\right).$$

Для A имеем

$$A = \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} \frac{c_k c_l}{\theta^l - 1} \sum_{i=1}^{2^n-2} \left(\theta^{l(i+2^n-1-i)+ik}\theta^{-k} - \theta^{(l+k)i}\theta^{-k}\right) =$$

$$= \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} \sum_{i=1}^{2^n-2} \theta^{ik} - \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} \sum_{i=1}^{2^n-2} \theta^{(l+k)i}.$$

Снова посчитаем суммы по отдельности, первую обозначим A_1, а вторую — A_2:

$$A_1 = \sum_{k,\ l=1}^{2^n-2} \frac{c_k c_l}{\theta^l - 1} \frac{\theta^{(2^n-2)k} - 1}{\theta^k - 1} + \sum_{l=1,(k=2^n-1)}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} \sum_{i=1}^{2^n-2} 1. \tag{4}$$

В силу того, что порядок θ равен $2^n - 1$, имеем $\theta^{(2^n-2)k} = \theta^{-k}$, отсюда следует, что $\dfrac{\theta^{(2^n-2)k} - 1}{\theta^k - 1} = \dfrac{1}{\theta^k}$. Заметим, что вторая сумма в равенстве (4) содержит множитель $(2^n - 2)$, а так как характеристика поля равна 2, то она равна нулю. В итоге

$$A_1 = \sum_{k,l=1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k}.$$

Теперь посчитаем A_2, выделим слагаемое, соответствующее $k = 2^n - 1$:

$$A_2 = \sum_{k,l=1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} \sum_{i=1}^{2^n-2} \theta^{(l+k)i} + \sum_{l=1,(k=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^l - 1} \sum_{i=1}^{2^n-2} \theta^{il} =$$

$$= \sum_{k,l=1:l+k=2^n-1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} \sum_{i=1}^{2^n-2} 1 + \sum_{k,l=1:l+k\neq 2^n-1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} \sum_{i=1}^{2^n-2} \theta^{(l+k)i} +$$

$$+ \sum_{l=1,(k=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^l - 1} \frac{\theta^l(\theta^{-l} - 1)}{\theta^l - 1}.$$

Первая из трёх сумм равна нулю, так как $\sum\limits_{i=1}^{2^n-2} 1 = 2^n - 2 \equiv 0 \pmod 2$, и поэтому

$$A_2 = \sum_{k,l=1:l+k\neq 2^n-1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} \frac{\theta^{l+k}(\theta^{-(l+k)} - 1)}{\theta^{l+k} - 1} + \sum_{l=1,(k=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^l - 1} \frac{\theta^l(1-\theta^l)}{\theta^l(\theta^l-1)} =$$

$$= \sum_{k,l=1:l+k\neq 2^n-1}^{2^n-2} \frac{c_k c_l}{(\theta^l - 1)\theta^k} + \sum_{l=1,(k=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^l - 1}.$$

Осталось вычислить сумму B:

$$B = \sum_{k=1,(l=2^n-1)}^{2^n-1} c_k c_l \sum_{i=1}^{2^n-3} \theta^{ik}(2^n - 2 - i) =$$

$$= \sum_{k=1,(l=2^n-1)}^{2^n-1} c_k c_l (2^n-2) \sum_{i=1}^{2^n-3} \theta^{ik} - \sum_{k=1,(l=2^n-1)}^{2^n-1} c_k c_l \sum_{i=1}^{2^n-3} i\theta^{ik}.$$

Заметим, что первая сумма обращается в нуль, значит,

$$B=\sum_{k=1,(l=2^n-1)}^{2^n-2}c_kc_l\theta^k\sum_{i=1}^{2^n-3}i(\theta^k)^{i-1}+\sum_{k=2^n-1,l=2^n-1}c_kc_l\sum_{i=1}^{2^n-3}i=$$

$$=\sum_{k=1,(l=2^n-1)}^{2^n-2}c_kc_l\theta^k\left(\sum_{i=1}^{2^n-3}x^i\right)'_{x=\theta^k}+c_{2^n-1}^2\sum_{i=1}^{2^n-3}i=\sum_{k=1,(l=2^n-1)}^{2^n-2}c_kc_l\theta^k\left(\frac{x^{2^n-2}-x}{x-1}\right)'_{x=\theta^k}+c_{2^n-1}^2=$$

$$=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2}c_kc_l\theta^k\left(\frac{((2^n-2)x^{2^n-3}-1)(x-1)-x^{2^n-2}+x}{(x-1)^2}\right)_{x=\theta^k}=$$

$$=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2}c_kc_l\theta^k\frac{-\theta^k+1-\theta^{-k}+\theta^k}{(\theta^k-1)^2}=$$

$$=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2}c_kc_l\frac{\theta^k-1}{(\theta^k-1)^2}=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^k-1}.$$

Собирая все подсчитанные суммы вместе, получаем

$$n_1=\sum_{k,l=1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}+\sum_{k,l=1(l+k\neq2^n-1)}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}+\sum_{l=1,(k=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^l-1}+c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^k-1}.$$

Первую сумму можно разбить на две области суммирования по $l+k=2^n-1$ и $l+k\neq$ $\neq 2^n-1$:

$$n_1=\sum_{k,l=1,(l+k=2^n-1)}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}+\sum_{k,l=1,(l+k\neq2^n-1)}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}+\sum_{k,l=1(l+k\neq2^n-1)}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}+$$
$$+\sum_{l=1,(k=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^l-1}+c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^k-1}.$$

Заметим, что $\sum\limits_{l=1}^{2^n-2}\frac{c_kc_l}{\theta^l-1}=\sum\limits_{k=1}^{2^n-2}\frac{c_kc_l}{\theta^k-1}$. Тогда $n_1=\sum\limits_{k,l=1,(l+k=2^n-1)}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}+c_{2^n-1}^2$. Выразив l через k из равенства $l+k=2^n-1$, получаем

$$n_1=c_{2^n-1}^2+\sum_{k=1}^{2^n-2}\frac{c_kc_{2^n-1-k}}{(\theta^{2^n-1-k}-1)\theta^k}=c_{2^n-1}^2+\sum_{k=1}^{2^n-2}\frac{c_kc_{2^n-1-k}}{1-\theta^k}=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{(2^n-2)/2}\frac{c_kc_{2^n-1-k}}{1-\theta^k}+\sum_{k=(2^n-2)/2+1}^{2^n-2}\frac{c_kc_{2^n-1-k}}{1-\theta^k}=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{(2^n-2)/2}\frac{c_kc_{2^n-1-k}}{1-\theta^k}+\sum_{k=1}^{(2^n-2)/2}\frac{c_kc_{2^n-1-k}}{1-\theta^{-k}}=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{(2^n-2)/2}\frac{c_kc_{2^n-1-k}}{1-\theta^k}+\sum_{k=1}^{(2^n-2)/2}\frac{c_kc_{2^n-1-k}}{\theta^k-1}\theta^k=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{2^{n-1}-1}\frac{c_kc_{2^n-1-k}(1-\theta^k)}{1-\theta^k}=c_{2^n-1}^2+\sum_{k=1}^{2^{n-1}-1}c_kc_{2^n-1-k}.$$

Теорема доказана. ■

Следствие 1. Пусть $F:Q\to P$, $F(0)=0$, F — бент-функция и $||F||=n_0+$ $+2n_1+4n_2+\ldots$ Тогда в равенстве (1) $c_{2^n-1}=0$ при $n\geqslant 4$, а при $n\geqslant 6$ выполняется $c_{2^n-1-2^l}=0$ для всех $l\in\{0,1,\ldots,n-1\}$.

Доказательство. Рассмотрим функцию $G(x) = F(x) + L_a(x)$, где $\{L_a(x) : a \in Q\}$ — множество линейных булевых функций от n переменных. Функцию $G(x)$ можно представить в виде $G(x) = \sum\limits_{k=1}^{2^n-1} g_k x^k$; линейная функция имеет вид $L_a(x) = \sum\limits_{s=0}^{n-1} a^{2^s} x^{2^s}$. Тогда имеем равенство

$$\sum_{k=1}^{2^n-1} g_k x^k = \sum_{k=1}^{2^n-1} c_k x^k + \sum_{s=0}^{n-1} a^{2^s} x^{2^s} = \sum_{k=1,k\neq 2^s,s\in\{0,1,\ldots,n-1\}}^{2^n-1} c_k x^k + \sum_{s=0}^{n-1} \left(a^{2^s} + c_{2^s}\right) x^{2^s}.$$

Известно [6, с. 236], что вес бент-функции от n переменных описывается значениями $2^{n-1} + \varepsilon\, 2^{n/2-1}$, где $\varepsilon \in \{-1, 1\}$. Тогда $c_{2^n-1} = 0$, а при $n/2 - 1 \geqslant 2$ (т. е. при $n \geqslant 6$) коэффициент n_1 в двоичном разложении веса функции F равен 0. Имеем

$$\begin{aligned}\sum_{k=1}^{2^{n-1}-1} g_k g_{2^n-1-k} &= \sum_{k=1,k\neq 2^s,s\in\{0,1,\ldots,n-1\}}^{2^{n-1}-1} c_k c_{2^n-1-k} + \sum_{s=0}^{n-1} \left(c_{2^s} + a^{2^s}\right) c_{2^n-1-2^s} = \\ &= \sum_{k=1}^{2^{n-1}-1} c_k c_{2^n-1-k} + \sum_{s=0}^{n-1} a^{2^s} c_{2^n-1-2^s}.\end{aligned} \tag{5}$$

Так как F и G — бент-функции, то, используя (3), получаем равенства

$$\sum_{k=1}^{2^{n-1}-1} g_k g_{2^n-1-k} = 0, \quad \sum_{k=1}^{2^{n-1}-1} c_k c_{2^n-1-k} = 0.$$

В результате из (5) следует, что $\sum\limits_{s=0}^{n-1} a^{2^s} c_{2^n-1-2^s} = 0$ для всех $a \in Q$. Таким образом, имеем многочлен степени 2^{n-1} относительно a. Он не может иметь в поле больше чем 2^{n-1} корней, а в наших условиях он имеет 2^n корней, значит, $c_{2^n-1-2^s} = 0$ для всех $s \in \{0, 1, \ldots, n-1\}$. ■

Следствие 2. Пусть $F : Q \to P$, $F(0) = 0$, F — гипер-бент-функция и $||F|| = n_0 + 2n_1 + 4n_2 + \ldots$ Тогда при $n \geqslant 4$ имеет место $c_{2^n-1} = 0$, а при $n \geqslant 6$ выполняется $c_{2^n-1-v2^l} = 0$ для всех $l \in \{0, 1, \ldots, n-1\}$ и для всех v, таких, что $(v, 2^n - 1) = 1$.

Доказательство. Рассмотрим функцию $G(x) = F(x) + L_a^{(v)}(x)$, где $L_a^{(v)}(x)$ — собственная мономиальная функция [7] и $(v, 2^n - 1) = 1$; $G(x)$ при этом является гипер-бент-функцией. Тогда имеем равенство

$$G(x) = \sum_{k=1}^{2^n-1} c_k x^k + \sum_{s=0}^{n-1} a^{2^s} x^{v2^s}.$$

Заметим, что гипер-бент-функция является бент-функцией. При $n \geqslant 6$ аналогично следствию 1 получаем, что $\sum\limits_{s=0}^{n-1} a^{2^s} c_{2^n-1-v2^s} = 0$ для всех $a \in Q$. Отсюда следует, что $c_{2^n-1-v2^l} = 0$ для всех $l \in \{0, 1, \ldots, n-1\}$ и для всех v со свойством $(v, 2^n - 1) = 1$. ■

Для получения соотношения для третьего разряда в двоичном разложении веса функции используется следующая лемма.

Лемма 2 [5]. Пусть $a_i \in \{0, 1\}$, $\sum\limits_{i=1}^{n} a_i = k = n_0 + 2n_1 + 4n_2 + \ldots$, где $n_j \in \{0, 1\}$; при этом $k \geqslant 4$. Тогда $n_2 = \sum\limits_{1\leqslant t<l<h<f\leqslant n} a_k a_l a_h a_f$, где сумма берётся по модулю 2.

При вычислении следующего разряда в разложении веса пока не удалось получить такого же красивого и компактного результата, как в теореме 1. Представим результат вычислений, сами расчёты приведены в Приложении.

Теорема 2. Пусть $F : Q \to P$, $F(0) = 0$ и $||F|| = n_0 + 2n_1 + 4n_2 + \dots$ Тогда

$$
\begin{aligned}
n_2 = (c_{2^n-1})^4 &+ \sum_{f,h,l,k\neq 2^n-1} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{f,h,l,k+l\neq 2^n-1} \frac{c_k c_l c_h c_f \theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)})+\\
&+ \sum_{\substack{f,h,k\neq 2^n-1\\ l=2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^h\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{f,h,l+h,k\neq 2^n-1} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{f,h,l+h,k+l+h\neq 2^n-1} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^{k+l+h}-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3(k+l+h)})+\\
&+ \sum_{\substack{f,h,k\neq 2^n-1\\ l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^k\theta^h}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}(1-\theta^{3(k+l)})+\\
&+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}}+\\
&+ \sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}} + \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k})+\\
&+ \sum_{\substack{f,l,k\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}+\\
&+ \sum_{\substack{f,l,k+l\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_k c_l c_h c_f \theta^l(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}+\\
&+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l=2^n-1}} \frac{c_k c_l c_h c_f \theta^k(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^h\theta^{3k}}+\\
&+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f\neq 2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}+\\
&+ \sum_{\substack{f,k+l+h+f\neq 2^n-1\\ h+f,l+h+f\neq 2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3(l+h+f+k)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^{l+h+f+k}-1)\theta^h\theta^{2l}\theta^{3k}}+\\
&+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{h+k}\theta^{2f}(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^{3k}} + \sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_k c_l c_h c_f \theta^f(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}+\\
&+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_k c_l c_h c_f \theta^f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}}+
\end{aligned}
$$

$$+\sum_{\substack{f,l,k\neq 2^n-1\\ h+f=2^n-1}}\frac{c_kc_lc_hc_f\theta^f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}}+\sum_{\substack{f,k\neq 2^n-1\\ h+f,l=2^n-1}}\frac{c_kc_lc_hc_f\theta^f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k})+$$

$$+\sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^k-1)\theta^{2l}\theta^{3k}}+$$

$$+\sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2h}\theta^k(1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{3k}}+$$

$$+\sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f(1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{2l}\theta^{3k}}+\sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2h}(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^{2k}}+$$

$$+\sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\,\frac{1-\theta^{3(l+h+k)}}{\theta^{3(l+k)}(\theta^{l+h+k}-1)^2}+$$

$$+\sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f\theta^{l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\,\frac{1-\theta^{3(l+h+k)}}{\theta^{2(l+k)}(\theta^{l+h+k}-1)^2}+$$

$$+\sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^l\theta^{3k}}+\sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}}\frac{c_kc_lc_hc_f\theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k}+$$

$$+\sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}}\,\frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}}+\sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}}\frac{c_kc_lc_hc_f\theta^l}{(\theta^h-1)^2(\theta^l-1)}\,\frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}}+$$

$$+\sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}}\frac{c_kc_lc_hc_f\theta^k}{(\theta^h-1)^2}\,\frac{1-\theta^{3k}}{(\theta^k-1)^2\theta^{3k}}+\sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^l-1)^3}\,\frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2}+$$

$$+\sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}}\frac{c_kc_lc_hc_f\theta^k}{(\theta^l-1)^3}\,\frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2}+\sum_{\substack{l,k\neq 2^n-1\\ f,h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^l-1)^3}\,\frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)}+$$

$$+\sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^l-1)(\theta^{l+k}-1)}\,\frac{1-\theta^{3(l+k)}}{\theta^k(\theta^{l+k}-1)^2}+\sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^k-1)^4}(1-\theta^{3k}).$$

Доказательство приводится в Приложении.

2. Структурные характеристики бент-функций и гипер-бент-функций

В качестве структурных характеристик рассматриваются вес функции и веса её ограничений на различных подпространствах и многообразиях. Пусть $n = 2\lambda$, где $\lambda \in \mathbb{N}$. Фиксируя какие-либо переменные или значения линейных комбинаций переменных функции $f(x_0, x_1, \ldots, x_{n-1})$ значениями 0 или 1, получаем вес соответствующей ей функции $F(x)$ на подпространстве или многообразии. При определённой фиксации $n - s$ переменных, где s делит n, получаем подполе $\mathrm{GF}(2^s)$. Тогда для функции $g(x_{i_1}, \ldots, x_{i_s})$, которая получается из функции f фиксацией $n - s$ переменных, существуют аналогичные приведённым во введении представления в виде полинома от одного переменного над полем. При этом должна существовать зависимость между коэффициентами полиномов, заданных над полем $\mathrm{GF}(2^n)$ и полем $\mathrm{GF}(2^\lambda)$.

Для установления этой зависимости необходимо описать значения веса функции $f(x_0, x_1, \ldots, x_{n-1})$ на различных подпространствах. Обозначим (α, x) скалярное произведение векторов $\alpha \in V_n$ и $x \in V_n$; $f|_T$ — ограничение функции f на пространстве или многообразии T.

Лемма 3. Пусть $\alpha \in V_n \setminus \{\mathbf{0}\}$. Тогда вес функции $f(x_0, x_1, \ldots, x_{n-1}) \cdot (\alpha, x)$ равен весу $f|_W$, где $W = \{x \in V_n : (\alpha, x) = 1\}$.

Для дальнейшего изложения результатов приведём вспомогательное утверждение.

Утверждение 2. Пусть $k \geqslant 2$ и $f_i(x)$ — булевы функции от n переменных, $i = 1, \ldots, k$. Тогда

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} \sum_{t=1}^{k} (-1)^{t-1} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant k} ||f_{i_1} + \ldots + f_{i_t}||.$$

Доказательство. Докажем утверждение методом математической индукции по параметру $k \geqslant 2$. База индукции при $k = 2$ получается из известной формулы

$$||f + g|| = ||f|| + ||g|| - 2||f \cdot g||.$$

Шаг индукции. Пусть утверждение верно при $k \leqslant m-1$, покажем, что оно верно и для $k = m$. Имеет место равенство $||f_1 \cdot \ldots \cdot f_k|| = ||(f_1 \cdot f_k) \cdot \ldots \cdot (f_{k-1} \cdot f_k)||$. Обозначим $g_i = (f_i \cdot f_k)$, $i = 1, \ldots, k-1$. Тогда по предположению индукции

$$||g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-2}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||g_{i_1} + \ldots + g_{i_t}|| =$$

$$= \frac{1}{2^{k-2}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_k(f_{i_1} + \ldots + f_{i_t})||.$$

Теперь снова воспользуемся формулой $||f \cdot g|| = \frac{1}{2}\left(||f|| + ||g|| - ||f + g||\right)$. Получаем равенство

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_k|| +$$

$$+ \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_{i_1} + \ldots + f_{i_t}|| +$$

$$+ \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_k + f_{i_1} + \ldots + f_{i_t}||.$$

Первую из трёх сумм свернём по биному Ньютона, а в третьей преобразуем индексы суммирования:

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} ||f_k|| + \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t < k} ||f_{i_1} + \ldots + f_{i_t}|| +$$

$$+ \frac{1}{2^{k-1}} \sum_{t=2}^{k} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t = k} ||f_{i_1} + \ldots + f_{i_t}||.$$

Объединяя все слагаемые в одну сумму, получаем

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} \sum_{t=1}^{k} (-1)^{t-1} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant k} ||f_{i_1} + \ldots + f_{i_t}||.$$

Утверждение доказано. ■

Известно [6, с. 236], что вес бент-функции f от n переменных описывается значениями $||f|| = 2^{n-1} + \varepsilon 2^{n/2-1}$, где $\varepsilon \in \{1, -1\}$. Известно также, что сумма линейной и бент-функции снова является бент-функцией. Из этого следует, что $||f+g|| = 2^{n-1} + \varepsilon' 2^{n/2-1}$, где g — произвольная линейная функция; $\varepsilon' \in \{1, -1\}$.

Теорема 3. Пусть f — бент-функция, $k \geqslant 2$, $g_1, \ldots, g_{k-1}$ — линейные функции, такие, что для любого $t \in \{1, \ldots, k-1\}$ и для любых $1 \leqslant i_1 < \ldots < i_t \leqslant k-1$ сумма $g_{i_1} + \ldots + g_{i_t}$ тождественно не равна 0. Пусть также вес функции f равен $||f|| = 2^{n-1} + \varepsilon_0 \cdot 2^{n/2-1}$, вес функции $f + g_{i_1} + \ldots + g_{i_t}$ равен $||f + g_{i_1} + \ldots + g_{i_t}|| = 2^{n-1} + \varepsilon_{i_1,\ldots,i_t} \cdot 2^{n/2-1}$, где $t \in \{1, \ldots, k-1\}$, $\varepsilon_0, \varepsilon_{i_1,\ldots,i_t} \in \{1, -1\}$. Тогда

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = 2^{n-k} + \frac{2^{n/2}}{2^k} \left[\varepsilon_0 + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} \varepsilon_{i_1,\ldots,i_t} \right]. \qquad (6)$$

Доказательство. Используя утверждение 2 и выделяя слагаемые, содержащие функцию f, получаем

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-1}} \left(||f|| + \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||g_{i_1} + \ldots + g_{i_t}|| + \right.$$
$$\left. + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||g_{i_1} + \ldots + g_{i_t} + f|| \right).$$

Сумма линейных функций является линейной функцией и её вес равен 2^{n-1}. Подставляя значения весов функций, получаем равенство

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-1}} \left(2^{n-1} + \varepsilon_0 2^{n/2-1} + 2^{n-1} \sum_{t=1}^{k-1} (-1)^{t-1} C_{k-1}^t + \right.$$
$$\left. + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} \left(2^{n-1} + \varepsilon_{i_1,\ldots,i_t} 2^{n/2-1} \right) \right).$$

Заметим, что

$$2^{n-1} \sum_{t=1}^{k-1} (-1)^{t-1} C_{k-1}^t = -2^{n-1} \sum_{t=1}^{k-1} (-1)^t C_{k-1}^t = -2^{n-1} \left((1-1)^{k-1} - 1 \right) = 2^{n-1}.$$

Возвращаясь к исходному равенству, получаем

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-1}} \left(2^{n-1} + \varepsilon_0 2^{n/2-1} + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} \varepsilon_{i_1,\ldots,i_t} 2^{n/2-1} \right).$$

Теорема доказана. ■

Замечание 2. При $k < n/2$ получаем, что вес ограничения функции f на многообразиях и подпространствах размерности больше $n/2$ кратен 2. Однако это верно и при $k = n/2$. Для этого достаточно показать, что выражение в скобках в равенстве (6) сравнимо с нулем по модулю 2. Обозначим данную сумму по модулю 2 через S:

$$S = 1 + \sum_{t=1}^{k-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} 1 \pmod 2.$$

Внутренняя сумма равна биномиальному коэффициенту C_{k-1}^t. Чётные биномиальные коэффициенты сравнимы с нулем по модулю 2, а количество нечётных биномиальных коэффициентов чётно, при этом 1 в начале формулы равна недостающему коэффициенту при $t = 0$. Таким образом, получаем, что $S = 0 \pmod 2$.

Заметим, что так как гипер-бент-функция, в частности, является бент-функцией, то теорема верна и для гипер-бент-функций.

Рассмотрим два примера бент-функций и покажем, что при определённых фиксациях переменных можно получить более сильные по сравнению с теоремой 3 результаты.

1) $f(x_1, \ldots, x_{2\lambda}) = \sum\limits_{i=1}^{\lambda} x_{2i-1}x_{2i}$. Функции такого вида являются совершенно нелинейными, а следовательно, бент-функциями [4]. Заметим, что при фиксации любой переменной x_{2j} единицей получаем, что переменная x_{2j-1} входит линейно, а значит, получаемая подфункция сбалансирована. Аналогично происходит при фиксации $x_{2j-1} = 1$. При фиксации переменной x_{2j} (или переменной x_{2j-1}) нулём получаем, что подфункция не зависит от переменной x_{2j-1} (или от x_{2j} соответственно). Таким образом, вес функции f чётен на всех подпространствах степени больше первой и функция равновероятна на всех многообразиях степени больше первой, получаемых при фиксации хотя бы одной переменной $x_j = 1$.

2) $f(x_1, \ldots, x_{2\lambda}) = \sum\limits_{i=1}^{\lambda} x_i x_{i+\lambda} + h(x_1, \ldots, x_\lambda)$. Функция f является бент-функцией для любой функции h [6]. При фиксации любой из переменных x_t, $t \in \{1, \ldots, \lambda\}$, единицей получаем, что переменная $x_{t+\lambda}$ входит линейно и, следовательно, получаемая при данной фиксации подфункция сбалансирована. При фиксации любой из переменных x_t, $t \in \{1, \ldots, \lambda\}$, нулём получаем, что подфункция не зависит от переменной $x_{t+\lambda}$.

Таким образом, функция f равновероятна на 2^λ многообразиях степени выше первой, которые получаются выбором и фиксацией переменных x_j, $j \in \{1, \ldots, \lambda\}$, единицей. Вес функции f чётен на всех подпространствах, получаемых при фиксации хотя бы одной переменной x_t, $t \in \{1, \ldots, \lambda\}$, нулём.

ЛИТЕРАТУРА

1. *Rothaus O. S.* On bent functions // J. Combinatorial Theory. 1976. V. 20(A). P. 300–305.
2. *Youssef A. and Gong G.* Hyper-bent functions // LNCS. 2001. V. 2045. P. 406–419.
3. *Логачев О. А., Сальников А. А., Ященко В. В.* О свойствах сумм Вейля на конечных полях и конечных абелевых группах // Дискретная математика. 1999. Т. 11. № 2. С. 66–85.
4. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. *Rueppel R. A.* Analysis and Design of Stream Ciphers. Berlin: Springer, 1986. 244 p.
6. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
7. *Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б.* Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18. № 1. С. 9–29.

ПРИЛОЖЕНИЕ

Доказательство теоремы 2

Сначала докажем вспомогательную лемму.

Лемма 4. Пусть $s, t \in \mathbb{N}$ и $s \leqslant t$. Тогда

$$\sum_{i=s}^{t} ix^{i-1} = \frac{tx^{t+1} - (t+1)x^t - (s-1)x^s + sx^{s-1}}{(x-1)^2}.$$

Доказательство. Заметим, что $\sum\limits_{i=s}^{t} ix^{i-1} = \left(\sum\limits_{i=s}^{t} x^i\right)'$. Используя формулу геометрической прогрессии, получим

$$\left(\sum_{i=s}^{t} x^i\right)' = \left(x^s \frac{x^{t-s-1} - 1}{x - 1}\right)' = \left(\frac{x^{t+1} - x^s}{x - 1}\right)'.$$

Возьмём производную: $\left(\frac{x^{t+1}-x^s}{x-1}\right)' = \frac{(t+1)x^{t+1} - sx^s - (t+1)x^t + sx^{s-1} - x^{t+1} + x^s}{(x-1)^2}$. После приведения подобных слагаемых получим требуемую формулу. ■

Доказательство теоремы 2.

$$n_2 = \sum_{\substack{x_1,x_2,x_3,x_4 \in Q: \\ x_1<x_2<x_3<x_4}} F(x_1)F(x_2)F(x_3)F(x_4) = \sum_{x_1<x_2<x_3<x_4} \left(\sum_{k=1}^{2^n-1} c_k {x_1}^k \sum_{l=1}^{2^n-1} c_l {x_2}^l \sum_{h=1}^{2^n-1} c_h {x_3}^h \sum_{f=1}^{2^n-1} c_f {x_4}^f \right).$$

Представим элементы x_1, x_2, x_3, x_4 через примитивный элемент θ поля Q и поменяем порядки суммирования:

$$n_2 = \sum_{0\leqslant s<t<p<v\leqslant 2^n-2} \left(\sum_{k,l,h,f=1}^{2^n-1} c_k c_l c_h c_f (\theta^s)^k (\theta^t)^l (\theta^p)^h (\theta^v)^f \right) = \sum_{k,l,h,f=1}^{2^n-1} c_k c_l c_h c_f \sum_{0\leqslant s<t<p<v\leqslant 2^n-2} \theta^{sk}\theta^{tl}\theta^{ph}\theta^{vf} =$$
$$= \sum_{k,l,h,f=1}^{2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \left(\theta^{ph} \sum_{v=p+1}^{2^n-2} \theta^{vf} \right) \right] \right).$$

Далее многократно будем применять лемму 4 и, чтобы избежать деления на ноль, будем выделять слагаемые, для которых в показателе θ присутствует $2^n - 1$, так как $\theta^{2^n-1} = 1$:

$$n_2 = \sum_{\substack{k,l,h,f=1 \\ f\neq 2^n-1}}^{2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{ph} \frac{\theta^{(p+1)f}(\theta^{(2^n-2-p)f}-1)}{\theta^f-1} \right] \right) +$$
$$+ \sum_{\substack{k,l,h=1 \\ f=2^n-1}}^{2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{ph}(2^n-2-p) \right] \right).$$

Всюду далее для сокращения формы записи вместо $\sum\limits_{\substack{k,l,h,f=1 \\ f\neq 2^n-1}}^{2^n-1}$ будем писать $\sum\limits_{f\neq 2^n-1}$; продолжим:

$$n_2 = \sum_{f\neq 2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \frac{\theta^{ph} - \theta^f \cdot \theta^{p(h+f)}}{\theta^f - 1} \right] \right) +$$
$$+ \sum_{f=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{ph} p \right] \right) = \sum_{f\neq 2^n-1} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{ph} \right] \right) +$$
$$+ \sum_{f\neq 2^n-1} \frac{c_k c_l c_h c_f \theta^f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{p(h+f)} \right] \right) + \sum_{f=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} p\theta^{ph} \right] \right).$$

Обозначим суммы:

$$A = \sum_{f\neq 2^n-1} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{ph} \right] \right);$$
$$B = \sum_{f\neq 2^n-1} \frac{c_k c_l c_h c_f \theta^f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{p(h+f)} \right] \right);$$
$$D = \sum_{f=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \left(\theta^{sk} \sum_{t=s+1}^{2^n-4} \left[\theta^{tl} \sum_{p=t+1}^{2^n-3} p\theta^{ph} \right] \right).$$

Посчитаем их отдельно:

$$A = \sum_{f\neq 2^n-1} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl} \sum_{p=t+1}^{2^n-3} \theta^{ph} = \sum_{f,h\neq 2^n-1} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl}\theta^{(t+1)h} \frac{\theta^{(2^n-3-t)h} - 1}{\theta^h - 1} +$$
$$+ \sum_{\substack{f\neq 2^n-1 \\ h=2^n-1}} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl}(2^n-3-t) = \sum_{f,h\neq 2^n-1} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl} \frac{\theta^{-h} - \theta^{th}\theta^h}{\theta^h - 1} +$$

$$+\sum_{\substack{f\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}(t+1)\theta^{tl}=\sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}+$$

$$+\sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)}\theta^h\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{t(l+h)}+\sum_{\substack{f\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}(t+1)\theta^{tl}.$$

Обозначим первую после последнего знака равенства сумму A_1, вторую — A_2, третью — A_3:

$$A_1=\sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}=\sum_{f,h,l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}\frac{\theta^{-2l}-\theta^{ls}\theta^l}{\theta^l-1}+$$

$$+\sum_{\substack{f,h\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}(2^n-4-s)=\sum_{f,h,l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h\theta^{2l}}\sum_{s=0}^{2^n-5}\theta^{sk}+$$

$$+\sum_{f,h,l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h}\theta^l\sum_{s=0}^{2^n-5}\theta^{s(k+l)}+\sum_{\substack{f,h\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}s\theta^{sk}=$$

$$=\sum_{f,h,l,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h\theta^{2l}}\frac{\theta^{(2^n-4)k}-1}{\theta^k-1}+\sum_{\substack{f,h,l\neq 2^n-1\\ k=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h\theta^{2l}}(\underbrace{2^n-4}_{=0})+$$

$$+\sum_{f,h,l,k+l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h}\theta^l\frac{\theta^{(2^n-4)(k+l)}-1}{\theta^{k+l}-1}+0+$$

$$+\sum_{\substack{f,h\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}s\theta^{(s-1)k}\theta^k=\sum_{f,h,l,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+$$

$$+\sum_{f,h,l,k+l\neq 2^n-1}\frac{c_kc_lc_hc_f\theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)})+$$

$$+\sum_{\substack{f,h\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f\theta^k}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}s(\theta^k)^{(s-1)}.$$

С помощью леммы 4 вычислим сумму $\sum\limits_{s=0}^{2^n-5}s(\theta^k)^{s-1}$ при $k\neq 2^n-1$, так как при $k=2^n-1$ она равна нулю:

$$\sum_{s=0}^{2^n-4}s(\theta^k)^{s-1}=\left(\sum_{s=1}^{2^n-4}x^s\right)'_{x=\theta^k}=\frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)^2}.$$

Получаем, что

$$A_1=\sum_{f,h,l,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+$$

$$+\sum_{f,h,l,k+l\neq 2^n-1}\frac{c_kc_lc_hc_f\theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)})+$$

$$+\sum_{\substack{f,h,k\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f\theta^k}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^h\theta^{3k}}(1-\theta^{3k}).$$

Вычисление суммы A_2 повторяет вычисление A_1. Поэтому с учётом замены $l\mapsto l+h$ имеем

$$A_2=\sum_{f,h,l+h,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+$$

$$+\sum_{f,h,l+h,k+l+h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^{k+l+h}-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3(k+l+h)})+$$

$$+\sum_{\substack{f,h,k\neq 2^n-1\\ l+h=2^n-1}}\frac{c_kc_lc_hc_f\theta^k\theta^h}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^{3k}}(1-\theta^{3k}).$$

Теперь вычислим $A_3=\sum\limits_{\substack{f\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum\limits_{s=0}^{2^n-5}\theta^{sk}\sum\limits_{t=s+1}^{2^n-4}(t+1)\theta^{tl}$. Для этого воспользуемся леммой 4 и посчитаем сумму $\sum\limits_{t=s+1}^{2^n-4}(t+1)\theta^{tl}$ при $l\neq 2^n-1$:

$$\sum_{t=s+1}^{2^n-4}(t+1)\theta^{tl}=\left(\sum_{t=s+1}^{2^n-4}x^{t+1}\right)'_{x=\theta^l}=\frac{(s+1)\theta^{l(s+2)}-s\theta^{l(s+1)}-\theta^{-l}}{(\theta^l-1)^2}.$$

Подставляя полученное выражение в A_3, имеем

$$A_3=\sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\frac{(s+1)\theta^{l(s+2)}-s\theta^{l(s+1)}-\theta^{-l}}{(\theta^l-1)^2}+\sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+2}^{2^n-3}t=$$

$$=\sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2}\sum_{s=0}^{2^n-5}(s+1)\theta^{s(l+k)}\theta^{2l}+\sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2}\sum_{s=0}^{2^n-5}s\theta^{s(l+k)}\theta^{l}+$$

$$+\sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\theta^{-l}+\sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+2}^{2^n-3}t.$$

Обозначим последние четыре суммы $A_{3.1}$, $A_{3.2}$, $A_{3.3}$, $A_{3.4}$ соответственно; вычислим их:

$$A_{3.1}=\sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2}\sum_{s=0}^{2^n-5}(s+1)\theta^{s(l+k)}\theta^{2l}=$$

$$=\sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2l}}{(\theta^f-1)(\theta^l-1)^2}\left(\sum_{s=0}^{2^n-5}(s+1)x^s\right)'_{x=\theta^{l+k}}+\sum_{\substack{f,l\neq 2^n-1\\ h,l+k=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2l}}{(\theta^f-1)(\theta^l-1)^2}\sum_{s=1}^{2^n-5}s.$$

С учетом равенства $\sum\limits_{s=0}^{2^n-5}(s+1)x^s=\left(\sum\limits_{s=1}^{2^n-4}x^s\right)'$ имеем

$$A_{3.1}=\sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}(1-\theta^{3(k+l)}).$$

Рассмотрим $A_{3.2}$:

$$A_{3.2}=\sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2}\sum_{s=0}^{2^n-5}s(\theta^{l+k})^{s-1}\theta^l\theta^{l+k}=\sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2}\left(\sum_{s=1}^{2^n-5}x^s\right)'_{x=\theta^{l+k}}+0=$$

$$=\sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2}\frac{1-\theta^{-3(l+k)}}{(\theta^{l+k}-1)^2}=\sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}}.$$

Теперь вычислим $A_{3.3}$:

$$A_{3.3}=\sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\theta^{-l}=\sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2\theta^l}\frac{\theta^{(2^n-4)k}-1}{\theta^k-1}+0=$$

$$=\sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\frac{1-\theta^{3k}}{\theta^{3k}}.$$

Осталось вычислить $A_{3.4}$:

$$A_{3.4}=\sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+2}^{2^n-3}t=\sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)}\sum_{t=2}^{2^n-3}t\sum_{s=0}^{t-2}\theta^{sk}=$$

$$=\sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)}\sum_{t=2}^{2^n-3}t\frac{\theta^{(t-1)k}-1}{\theta^k-1}+\sum_{\substack{f\neq 2^n-1\\ h,l,k=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)}\sum_{t=2}^{2^n-3}\underbrace{t(t-1)}_{=0}=$$

$$=\sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)}\sum_{t=2}^{2^n-3}t(\theta^k)^{t-1}+\sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)}\underbrace{\sum_{t=2}^{2^n-3}t}_{=0}=$$

$$=\sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)}\left(\sum_{t=2}^{2^n-3}x^t\right)'_{x=\theta^k}.$$

Для завершения вычисления $A_{3.4}$ осталось применить лемму 4 и вычислить

$$\left(\sum_{t=2}^{2^n-3} x^t\right)'_{x=\theta^k} = \frac{1+\theta^{3k}}{\theta^k(\theta^k-1)^2}.$$

В итоге получаем $A_{3.4} = \sum\limits_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \dfrac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k})$.

Собирая все суммы вместе, получаем

$$A = A_1+A_2+A_3 = \sum_{f,h,l,k\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k}) +$$
$$+ \sum_{f,h,l,k+l\neq 2^n-1} \frac{c_kc_lc_hc_f\theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)}) +$$
$$+ \sum_{\substack{f,h,k\neq 2^n-1\\ l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^h\theta^{3k}}(1-\theta^{3k}) +$$
$$+ \sum_{f,h,l+h,k\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k}) +$$
$$+ \sum_{f,h,l+h,k+l+h\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^{k+l+h}-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3(k+l+h)}) +$$
$$+ \sum_{\substack{f,h,k\neq 2^n-1\\ l+h=2^n-1}} \frac{c_kc_lc_hc_f\theta^k\cdot\theta^h}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^{3k}}(1-\theta^{3k}) + \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}(1-\theta^{3(k+l)}) +$$
$$+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}} +$$
$$+ \sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}} + \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k}).$$

Сравнивая суммы A и B, можно заметить, что B получается из A заменой $h\mapsto h+f$ и умножением на θ^f. Поэтому сразу выпишем B:

$$B = \sum_{\substack{f,l,k\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}} +$$
$$+ \sum_{\substack{f,l,k+l\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f\theta^l(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}} + \sum_{\substack{f,h+f,k\neq 2^n-1\\ l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^h\theta^{3k}} +$$
$$+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}} +$$
$$+ \sum_{\substack{f,k+l+h+f\neq 2^n-1\\ h+f,l+h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3(l+h+f+k)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^{l+h+f+k}-1)\theta^h\theta^{2l}\theta^{3k}} +$$
$$+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{h+k}\theta^{2f}(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^{3k}} + \sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}} +$$
$$+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}} + \sum_{\substack{f,l,k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}} +$$
$$+ \sum_{\substack{f,k\neq 2^n-1\\ h+f,l=2^n-1}} \frac{c_kc_lc_hc_f\theta^f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k}).$$

Осталось посчитать последнюю сумму:

$$D = \sum_{f=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3} p\theta^{ph}\right]\right) = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} c_kc_lc_hc_f\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\sum_{p=t+1}^{2^n-3} p(\theta^h)^{p-1}\theta^h +$$

$$+\sum_{f,h=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\sum_{p=t+1}^{2^n-3} p = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} c_k c_l c_h c_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\theta^h \left(\sum_{p=t+1}^{2^n-3} x^p\right)'_{x=\theta^h} +$$

$$+\sum_{f,h=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\sum_{p=t+1}^{2^n-3} p.$$

Обозначим последние две суммы D_1 и D_2 соответственно. Для вычисления D_1 сначала посчитаем следующую сумму:

$$\left(\sum_{p=t+1}^{2^n-3} x^p\right)'_{x=\theta^h} = \frac{t\theta^{h(t+1)} - (t+1)\theta^{th} - \theta^{-h}}{(\theta^h-1)^2}.$$

Вернёмся к D_1:

$$D_1 = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} c_k c_l c_h c_f \theta^h \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\frac{t\theta^{h(t+1)} - (t+1)\theta^{th} - \theta^{-h}}{(\theta^h-1)^2} =$$

$$= \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\left(t\theta^{t(l+h)}\theta^h - (t+1)\theta^{t(h+l)} - \theta^{tl}\theta^{-h}\right) =$$

$$= \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4} t\theta^{t(l+h)} + \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}(t+1)\theta^{t(h+l)} +$$

$$+\sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}.$$

Обозначим получившиеся суммы $D_{1.1}$, $D_{1.2}$ и $D_{1.3}$ соответственно. Тогда

$$D_{1.1} = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4} t\theta^{(t-1)(l+h)}\theta^{l+h} =$$

$$= \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\theta^{l+h}\left(\sum_{t=s+1}^{2^n-4} x^t\right)'_{x=\theta^{l+h}} + \sum_{\substack{h\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4} t.$$

С использованием леммы 4 выпишем значение

$$\left(\sum_{t=s+1}^{2^n-4} x^t\right)'_{x=\theta^{l+h}} = \frac{\theta^{-3(l+h)} - s\theta^{(l+h)(s+1)} - (s+1)\theta^{(l+h)s}}{(\theta^{l+h}-1)^2}.$$

Подставляя это выражение в $D_{1.1}$, получаем

$$D_{1.1} = \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^{l+h}}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\frac{\theta^{-3(l+h)} - s\theta^{(l+h)(s+1)} - (s+1)\theta^{(l+h)s}}{(\theta^{l+h}-1)^2} +$$

$$+\sum_{\substack{h\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2}\sum_{t=1}^{2^n-4} t\sum_{s=0}^{t-1}\theta^{sk} = \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2(\theta^{l+h}-1)^2\theta^{2(l+h)}}\sum_{s=0}^{2^n-5}\theta^{sk} +$$

$$+\sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^l}{(\theta^h-1)^2(\theta^{l+h}-1)^2}\sum_{s=0}^{2^n-5} s\theta^{(l+h+k)s}\theta^{l+h} + \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^l}{(\theta^h-1)^2(\theta^{l+h}-1)^2}\sum_{s=0}^{2^n-5}(s+1)\theta^{(l+h+k)s} +$$

$$+\sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2}\sum_{t=1}^{2^n-4} t\frac{\theta^{kt}-1}{\theta^k-1} + \sum_{\substack{h\neq 2^n-1\\ f,l+h,k=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2}\underbrace{\sum_{t=1}^{2^n-4} t\cdot t}_{=0} =$$

$$= \sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^{l+h}-1)^2\theta^{2l}}\frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)} +$$

$$+\sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{4h}\theta^{2l}}{(\theta^h-1)^2(\theta^{l+h}-1)^2}\sum_{s=0}^{2^n-5} s\theta^{(l+h+k)(s-1)}\theta^{l+h+k} +$$

$$+\sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^l}{(\theta^h-1)^2(\theta^{l+h}-1)^2}\left(\sum_{s=0}^{2^n-5} x^{s+1}\right)'_{x=\theta^{l+h+k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2(\theta^k-1)}\sum_{t=1}^{2^n-4} t\theta^{k(t-1)}\theta^k =$$

$$= \sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^k-1)\theta^{2l}\theta^{3k}} + \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^k(1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{3k}} +$$

$$+ \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{2l}\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^{2k}}.$$

Теперь посчитаем $D_{1.2}$:

$$D_{1.2} = \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \left(\sum_{t=s+2}^{2^n-3} x^t\right)'_{x=\theta^{h+l}} + \sum_{\substack{h\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+2}^{2^n-3} t.$$

По лемме 4 имеем $\left(\sum\limits_{t=s+2}^{2^n-3} x^t\right)'_{x=\theta^{h+l}} = \dfrac{(s+1)\theta^{(h+l)(s+2)} - s\theta^{(h+l)(s+1)} - \theta^{-(h+l)}}{(\theta^{h+l}-1)^2}$. Вернёмся к вычислению $D_{1.2}$:

$$D_{1.2} = \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \frac{(s+1)\theta^{(h+l)(s+2)} - s\theta^{(h+l)(s+1)} - \theta^{-(h+l)}}{(\theta^{h+l}-1)^2} +$$

$$+ \sum_{\substack{h\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2} \sum_{t=2}^{2^n-3} t \sum_{s=0}^{t-2} \theta^{sk}.$$

Заметим, что вторая сумма была посчитана в $A_{3.4}$. Продолжим преобразования:

$$D_{1.2} = \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \sum_{s=0}^{2^n-5} (s+1)\theta^{(h+l+k)s}\theta^{2(h+l)} +$$

$$+ \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \sum_{s=0}^{2^n-5} s\theta^{(h+l+k)s}\theta^{(h+l)} +$$

$$+ \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk}\theta^{-(h+l)} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k} =$$

$$= \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \left(\sum_{s=1}^{2^n-4} x^s\right)'_{x=\theta^{h+l+k}} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^l}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \left(\sum_{s=1}^{2^n-5} x^s\right)'_{x=\theta^{h+l+k}} \theta^{h+l+k} +$$

$$+ \sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^l\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k} =$$

$$= \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \frac{1-\theta^{3(l+h+k)}}{\theta^{3(l+h+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^l}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \frac{1-\theta^{3(l+h+k)}}{\theta^{2(l+h+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^l\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k}.$$

Далее вычислим сумму $D_{1.3}$:

$$D_{1.3} = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl} = \sum_{\substack{h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \frac{\theta^{(2^n-3)l} - \theta^{l(s+1)}}{\theta^l-1} +$$

$$+ \sum_{\substack{h\neq 2^n-1\\ f,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} 1 = \sum_{\substack{h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}} \sum_{s=0}^{2^n-5} \theta^{sk} +$$

$$+ \sum_{\substack{h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^h-1)^2(\theta^l-1)} \sum_{s=0}^{2^n-5} \theta^{s(l+k)} + \sum_{\substack{h\neq 2^n-1\\ f,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} s\theta^{(s-1)k}\theta^k =$$

$$= \sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}} \frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}} + \sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^h-1)^2(\theta^l-1)} \frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}} +$$

$$+ \sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^h-1)^2} \left(\sum_{s=1}^{2^n-5} x^s\right)'_{x=\theta^k} = \sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}} \frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}} +$$

$$+ \sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^h-1)^2(\theta^l-1)} \frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^h-1)^2} \frac{1-\theta^{3k}}{(\theta^k-1)^2\theta^{3k}}.$$

Осталось вычислить D_2:

$$D_2 = \sum_{f,h=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl} \sum_{p=t+1}^{2^n-3} p = \sum_{f,h=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{p=s+2}^{2^n-3} p \sum_{t=s+1}^{p-1} \theta^{tl} =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{p=s+2}^{2^n-3} p\theta^{(s+1)l} \frac{\theta^{(p-1-s)l}-1}{\theta^l-1} + \sum_{f,h,l=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{p=s+2}^{2^n-3} p(p-1-s) =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{\theta^l-1} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{p=s+2}^{2^n-3} p\theta^{(p-1)l}\theta^l + \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{\theta^l-1} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{p=s+2}^{2^n-3} p\theta^{ls}\theta^l +$$

$$+ \sum_{f,h,l=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{p=s+2}^{2^n-3} (p(p-1)+ps) = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5} \theta^{sk} \left(\sum_{p=s+2}^{2^n-3} x^p\right)'_{x=\theta^l} +$$

$$+ \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5} \theta^{s(l+k)} \sum_{p=s+2}^{2^n-3} p + \sum_{f,h,l=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} s\theta^{sk} \sum_{p=s+2}^{2^n-3} p.$$

Обозначим три последние суммы $D_{2.1}$, $D_{2.2.}$ и $D_{2.3}$. Заметим, что $D_{2.1}$ вычисляется аналогично $D_{1.2}$:

$$D_{2.1} = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5} \theta^{sk} \left(\sum_{p=s+2}^{2^n-3} x^p\right)'_{x=\theta^l} =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5} \theta^{sk} \frac{(s+1)\theta^{l(s+2)} - s\theta^{l(s+1)} - \theta^{-l}}{(\theta^l-1)^2} =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3l}}{(\theta^l-1)^3} \sum_{s=0}^{2^n-5} (s+1)\theta^{s(k+l)} + \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}}{(\theta^l-1)^3} \sum_{s=0}^{2^n-5} s\theta^{(s-1)(k+l)}\theta^{l+k} +$$

$$+ \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^l-1)^3} \sum_{s=0}^{2^n-5} \theta^{sk}\theta^{-l} = \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3l}}{(\theta^l-1)^3} \frac{1-\theta^{3(k+l)}}{\theta^{3(k+l)}(\theta^{k+l}-1)^2} +$$

$$+ \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3l}\theta^k}{(\theta^l-1)^3} \frac{1-\theta^{3(k+l)}}{\theta^{3(k+l)}(\theta^{k+l}-1)^2} + \sum_{\substack{l,k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)^3} \frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)}.$$

Вычислим $D_{2.2}$:

$$D_{2.2} = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5} \theta^{s(l+k)} \sum_{p=s+2}^{2^n-3} p = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{p=2}^{2^n-3} p \sum_{s=0}^{p-2} \theta^{s(l+k)} =$$

$$= \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{p=2}^{2^n-3} p\frac{\theta^{(l+k)(p-1)}-1}{\theta^{l+k}-1} + \sum_{\substack{l\neq 2^n-1\\ f,h,l+k=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{\theta^l-1} \sum_{p=2}^{2^n-3} \underbrace{p(p-1)}_{=0} =$$

$$= \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^l-1)(\theta^{l+k}-1)} \sum_{p=2}^{2^n-3} p\theta^{(p-1)(l+k)} = \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^l-1)(\theta^{l+k}-1)} \left(\sum_{p=2}^{2^n-3} x^p\right)'_{x=\theta^{l+k}} =$$

$$= \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^l-1)(\theta^{l+k}-1)} \frac{1-\theta^{3(l+k)}}{\theta^{l+k}(\theta^{l+k}-1)^2}.$$

Осталось вычислить $D_{2.3}$:

$$D_{2.3} = \sum_{f,h,l=2^n-1} c_k c_l c_h c_f \sum_{s=1}^{2^n-5} s\theta^{sk} \sum_{p=s+2}^{2^n-3} p = \sum_{f,h,l=2^n-1} c_k c_l c_h c_f \theta^k \sum_{p=3}^{2^n-3} p \sum_{s=1}^{p-2} s\theta^{(s-1)k} =$$

$$= \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} c_k c_l c_h c_f \theta^k \sum_{p=3}^{2^n-3} p \left(\sum_{s=1}^{p-2} x^s\right)'_{x=\theta^k} + \sum_{f,h,l,k=2^n-1} c_k c_l c_h c_f \theta^k \underbrace{\sum_{p=3}^{2^n-3} p \sum_{s=1}^{p-2} s}_{=1}.$$

Заметим, что $\left(\sum\limits_{s=1}^{p-2} x^s\right)'_{x=\theta^k} = \dfrac{px^{p-1}-(p-1)x^{p-2}-1}{(x-1)^2}$. Тогда

$$D_{2.3} = \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} c_k c_l c_h c_f \theta^k \sum_{p=3}^{2^n-3} p \frac{p\theta^{k(p-1)}-(p-1)\theta^{k(p-2)}-1}{(\theta^k-1)^2} + (c_{2^n-1})^4 =$$

$$= \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^k-1)^2} \sum_{p=3}^{2^n-3} p^2 \theta^{k(p-1)} + (c_{2^n-1})^4 = \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^k-1)^2} \left(\sum_{p=3}^{2^n-3} x^p\right)'_{x=\theta^k} + (c_{2^n-1})^4 =$$

$$= \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^k-1)^2} \frac{1-\theta^{3k}}{\theta^k(\theta^k-1)^2} + (c_{2^n-1})^4 = \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^k-1)^4}(1-\theta^{3k}) + (c_{2^n-1})^4.$$

В итоге получаем

$$D = \sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^k-1)\theta^{2l}\theta^{3k}} + \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^k(1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{3k}} +$$

$$+ \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{2l}\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^{2k}} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \frac{1-\theta^{3(l+h+k)}}{\theta^{3(l+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \frac{1-\theta^{3(l+h+k)}}{\theta^{2(l+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^{l}\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^{h}(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^{k}} +$$

$$+ \sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}} \frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}} + \sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{l}}{(\theta^h-1)^2(\theta^l-1)} \frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}} +$$

$$+ \sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}} \frac{c_k c_l c_h c_f \theta^{k}}{(\theta^h-1)^2} \frac{1-\theta^{3k}}{(\theta^k-1)^2\theta^{3k}} + \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)^3} \frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2} +$$

$$+ \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{k}}{(\theta^l-1)^3} \frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2} + \sum_{\substack{l,k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)^3} \frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)} +$$

$$+ \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)(\theta^{l+k}-1)} \frac{1-\theta^{3(l+k)}}{\theta^{k}(\theta^{l+k}-1)^2} + \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^k-1)^4}(1-\theta^{3k}) + (c_{2^n-1})^4.$$

Выражение $A + B + D$ даёт требуемый результат. ■

2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/5

УДК 519.213

РЕКУРРЕНТНОЕ ПОСТРОЕНИЕ ДИСКРЕТНЫХ ВЕРОЯТНОСТНЫХ РАСПРЕДЕЛЕНИЙ СЛУЧАЙНЫХ МНОЖЕСТВ СОБЫТИЙ

Д. В. Семенова, Н. А. Лукьянова

Институт математики и фундаментальной информатики Сибирского федерального университета, г. Красноярск, Россия

E-mail: dariasdv@gmail.com, nata00sfu@gmail.com

Исследуется класс дискретных вероятностных распределений II рода случайных множеств событий. В качестве инструмента построения таких распределений предлагается использовать ассоциативные функции. Излагается новый подход к определению дискретного вероятностного распределения II рода случайного множества на конечном множестве из N событий на основе полученного рекуррентного соотношения и заданной ассоциативной функции. Преимущество предлагаемого подхода заключается в том, что для определения вероятностного распределения вместо полного набора 2^N вероятностей достаточно знать N вероятностей событий и вид ассоциативной функции. Данный подход продемонстрирован на примере трёх ассоциативных функций. Приводятся теоремы, устанавливающие вид и условия легитимности полученных вероятностных распределений случайных множеств событий.

Ключевые слова: *случайное множество событий, дискретное вероятностное распределение, ассоциативная функция.*

Введение

Теория случайных множеств рассматривается как естественное обобщение теории случайных векторов, которые играют ключевую роль в многомерном статистическом анализе. Случайные множества данных можно рассматривать как неточные/неполные наблюдения, которые часто встречаются в современном технологическом обществе [1]. Центральным объектом нашего исследования является специфическое случайное множество, а именно — случайное конечное множество событий. Случайные множества событий позволяют выявить общие статистические закономерности распределения событий в различных системах объектов нечисловой природы. Вероятностное распределение случайного множества событий — это удобный математический аппарат для описания всех способов взаимодействия элементов моделируемой этим множеством системы между собой. В работе исследуется проблема построения вероятностных распределений случайных множеств событий и предлагается метод решения этой проблемы с помощью аппарата ассоциативных функций.

В п. 1 приводятся основные сведения о ключевых объектах исследования — случайных множествах событий и вероятностных распределениях, их характеризующих, и инструменте исследования — аппарате ассоциативных функций. В п. 2 излагается суть предлагаемого рекуррентного подхода построения дискретного вероятностного распределения II рода случайных множеств событий на основе заданной ассоциативной функции, определяется вид соответствующего рекуррентного соотношения. В п. 3 предложенный подход демонстрируется на трёх известных ассоциативных функциях. Приводятся теоремы, устанавливающие вид и условия легитимности полученных вероятностных распределений.

1. Основные понятия и обозначения

1.1. Случайное множество событий

Наряду со случайными величинами в теории вероятностей и её приложениях рассматривают случайные объекты произвольной природы, например случайные точки, векторы, функции, поля, множества и наборы множеств. Для описания такого типа объектов используется понятие случайного элемента [2].

Определение 1. Пусть $(\Omega, \mathcal{F}, \mathbf{P})$ — вероятностное пространство, $(U, \mathcal{A})$ — измеримое пространство, где U — произвольное множество, а $\mathcal{A}$ — некоторая σ-алгебра его подмножеств. Будем говорить, что функция $K = K(w)$, определённая на Ω и принимающая значения в U, есть $\mathcal{F}/\mathcal{A}$-измеримая функция, или случайный элемент (со значениями в U), если для любого $A \in \mathcal{A}$ верно $\{\omega : K(\omega) \in A\} \in \mathcal{F}$.

Отметим, что в случае, когда U — конечное множество, можно ограничиться понятием алгебры подмножеств 2^U.

Зафиксируем некоторый конечный набор событий $\mathfrak{X} \subset \mathcal{F}$. Случайный элемент, значения которого являются подмножествами конечного множества $\mathfrak{X}$, т. е. элементами $2^{\mathfrak{X}}$, будем называть случайным множеством событий [1], заданным на конечном множестве $\mathfrak{X} \subset \mathcal{F}$.

Определение 2. Случайное множество событий K на конечном множестве событий $\mathfrak{X} \subset \mathcal{F}$ определяется как отображение $K : \Omega \to 2^{\mathfrak{X}}$, измеримое относительно пары алгебр $\left(\mathcal{F}, 2^{2^{\mathfrak{X}}}\right)$ в том смысле, что для всякого $X \in 2^{2^{\mathfrak{X}}}$ существует прообраз $K^{-1}(X) \in \mathcal{F}$, такой, что $\mathbf{P}(X) = \mathbf{P}(K^{-1}(X))$.

Выражение $K(\omega) = \{x \in \mathfrak{X} : \omega \in x\}$ может быть истолковано как «случайное множество наступивших событий», поскольку элементарному исходу эксперимента $\omega \in \Omega$ ставится в соответствие некоторое подмножество событий $X \subseteq \mathfrak{X}$, которое содержит все те события, которые наступили в данном испытании.

1.2. Два основных способа представления вероятностного распределения случайного множества событий

Случайное множество событий K, заданное на конечном множестве событий $\mathfrak{X}$, определяется своим дискретным вероятностным распределением. Если мощность рассматриваемого множества событий $|\mathfrak{X}| = N < \infty$, то имеется 2^N видов вероятностных зависимостей между событиями этого множества, т. е. ровно столько, сколько у этого множества подмножеств. Дискретное вероятностное распределение (далее просто вероятностное распределение) случайного множества событий K, заданного на конечном множестве избранных событий $\mathfrak{X} \subset \mathcal{F}$, — это набор 2^N значений вероятностной меры $\mathbf{P}$ на событиях из $2^{\mathfrak{X}}$. Как известно, такое распределение можно задать шестью эквивалентными способами [3–5]. В настоящей работе исследуются только два из них.

PI. Вероятностное распределение I рода случайного множества событий K на $\mathfrak{X}$ — это набор $\{p(X), X \subseteq \mathfrak{X}\}$ из 2^N вероятностей вида

$$p(X) = \mathbf{P}(K = X) = \mathbf{P}\left(\left(\bigcap_{x \in X} x\right) \bigcap \left(\bigcap_{x \in X^c} x^c\right)\right),$$

где $X^c = \mathfrak{X} \setminus X$; $x^c = \Omega \setminus x$.

Вероятностное распределение I рода всегда легитимно, т. е. обладает свойствами

$$0 \leqslant p(X) \leqslant 1, \quad X \subseteq \mathfrak{X}; \tag{1}$$

$$\sum_{X \subseteq \mathfrak{X}} p(X) = 1. \tag{2}$$

PII. Вероятностное распределение II рода случайного множества событий K на $\mathfrak{X}$ — набор $\{p_X, X \subseteq \mathfrak{X}\}$ из 2^N вероятностей вида

$$p_X = \mathbf{P}(X \subseteq K) = \mathbf{P}\left(\bigcap_{x \in X} x\right), \quad X \subseteq \mathfrak{X}.$$

Вероятностное распределение II рода $\{p_X, X \subseteq \mathfrak{X}\}$ случайного множества событий K на $\mathfrak{X}$ удовлетворяет системе из 2^N неравенств Фреше — Хёфдинга

$$0 \leqslant p_X^- \leqslant p_X \leqslant p_X^+ \leqslant 1,$$

где $p_X^- = \max\left\{0, 1 - \sum\limits_{x \in X}(1 - p_x)\right\}$ — нижняя граница Фреше — Хёфдинга; $p_X^+ = \min\limits_{x \in X} p_x$ — верхняя граница Фреше — Хёфдинга.

Замечание 1. В теории случайных событий [3 – 7] обозначение $\varnothing$ используется для $\mathfrak{X}^c = \Omega \setminus \mathfrak{X}$. Событие $\varnothing = \bigcap\limits_{x \in \mathfrak{X}} x^c$ означает, что не наступило ни одно событие из $\mathfrak{X}$. В вероятностном распределении II рода всегда $p_\varnothing = 1$.

Замечание 2. Только распределение I рода обладает привычным для распределения вероятности свойством нормировки (2), которое очевидно следует из того, что соответствующие события $\left(\bigcap\limits_{x \in X} x\right) \bigcap \left(\bigcap\limits_{x \in X^c} x^c\right)$ образуют разбиение пространства элементарных событий Ω. А поскольку события $\bigcap\limits_{x \in X} x$ образуют не разбиение, а всего лишь покрытие Ω, то соотношение нормировки для вероятностного распределения II рода не выполняется, сумма вероятностей этих событий всегда больше единицы.

Вероятностные распределения I и II рода связаны взаимно-обратными формулами обращения Мёбиуса [3]

$$p_X = \sum_{Y \in 2^{\mathfrak{X}}: X \subseteq Y} p(Y); \tag{3}$$

$$p(X) = \sum_{Y \in 2^{\mathfrak{X}}: X \subseteq Y} (-1)^{|Y| - |X|} p_Y \tag{4}$$

для всех $X \in 2^{\mathfrak{X}}$.

Если задано вероятностное распределение I рода $\{p(X), X \subseteq \mathfrak{X}\}$, то по формуле (3) всегда можно получить вероятностное распределение II рода $\{p_X, X \subseteq \mathfrak{X}\}$. Однако преобразование (4) заданного набора из 2^N чисел $\{p_X, X \subseteq \mathfrak{X}\}$, удовлетворяющих границам Фреше — Хёфдинга, может привести к вероятностному распределению I рода с отрицательными значениями. Этот факт демонстрирует следующий пример.

Пример 1. Рассмотрим случайное множество, заданное на триплете событий $\mathfrak{X} = \{x, y, z\}$. Пусть известно его вероятностное распределение II рода

$$\{p_\varnothing, p_x, p_y, p_z, p_{xy}, p_{xz}, p_{yz}, p_{xyz}\} = \{1,\ 0{,}375,\ 0{,}75,\ 0{,}625,\ 0{,}243,\ 0{,}19,\ 0{,}429,\ 0{,}118\}. \tag{5}$$

Заметим, что все вероятности из (5) удовлетворяют границам Фреше — Хёфдинга. Например, для $p_{xz} = \mathbf{P}(x \cap z) = 0{,}19$ имеем

$$\max\{p_x + p_z - 1, 0\} \leqslant p_{xz} \leqslant \min\{p_x, p_z\} \Rightarrow 0 \leqslant p_{xz} \leqslant 0{,}375.$$

Применение формул (4) приводит к вероятностному распределению I рода

$$p(x) = \mathbf{P}\left(x \cap y^c \cap z^c\right) = p_x - p_{xy} - p_{xz} + p_{xyz} = 0{,}375 - 0{,}243 - 0{,}19 + 0{,}118 = 0{,}06;$$
$$p(y) = \mathbf{P}\left(x^c \cap y \cap z^c\right) = p_y - p_{xy} - p_{yz} + p_{xyz} = 0{,}75 - 0{,}243 - 0{,}429 + 0{,}118 = 0{,}196;$$
$$p(z) = \mathbf{P}\left(x^c \cap y^c \cap z\right) = p_z - p_{xz} - p_{yz} + p_{xyz} = 0{,}625 - 0{,}19 - 0{,}429 + 0{,}118 = 0{,}124;$$
$$p(xy) = \mathbf{P}\left(x \cap y \cap z^c\right) = p_{xy} - p_{xyz} = 0{,}243 - 0{,}118 = 0{,}125;$$
$$p(xz) = \mathbf{P}\left(x \cap y^c \cap z\right) = p_{xz} - p_{xyz} = 0{,}19 - 0{,}118 = 0{,}072;$$
$$p(yz) = \mathbf{P}\left(x^c \cap y \cap z\right) = p_{yz} - p_{xyz} = 0{,}429 - 0{,}118 = 0{,}311;$$
$$p(xyz) = \mathbf{P}\left(x \cap y \cap z\right) = p_{xyz} = 0{,}118;$$
$$p(\varnothing) = \mathbf{P}\left(x^c \cap y^c \cap z^c\right) = 1 - p_x - p_y - p_z + p_{xy} + p_{xz} + p_{yz} - p_{xyz} = -0{,}006.$$

Такое распределение нелегитимно, так как $p(\varnothing) < 0$.

Определение 3. Будем говорить, что случайное множество событий K обладает легитимным вероятностным распределением II рода, если соответствующее вероятностное распределение I рода, полученное по формулам обращения Мёбиуса (4), является легитимным.

В общем случае количество параметров, задающих вероятностные распределения случайного множества событий, зависит от мощности $\mathfrak{X}$, поскольку каждое множество из N событий характеризуется набором из 2^N вероятностей. Одной из главных проблем исследования случайных множеств событий является задача описания их вероятностных распределений через меньшее число параметров. Например, для определения вероятностного распределения равномерного случайного множества необходимо знать только один параметр $N = |\mathfrak{X}|$. В [5] исследован класс m-зависимых распределений случайного множества событий, которые определяются через фиксированные вероятности p_X, когда $|X| \leqslant m < N$. Общей идеей современных подходов [5 – 7] является выражение вероятности пересечений множества событий функционально через вероятности самих событий, что приводит к уменьшению числа параметров, необходимых для построения самих вероятностных распределений случайных множеств событий. В работе предлагается рекуррентный подход построения вероятностных распределений случайных множеств событий, использующий ассоциативные функции, которые связывают вероятности пересечения множества событий $\mathbf{P}\left(\bigcap\limits_{x\in X} x\right)$ с вероятностями самих событий $\mathbf{P}(x)$, $x \in X$, $X \subseteq \mathfrak{X}$.

1.3. Ассоциативные функции

Определение 4. Ассоциативная функция в теории случайных множеств событий $AF : [0,1]^2 \to [0,1]$ определяется как двуместная функция, удовлетворяющая следующим свойствам:

- A1) граничные условия: $AF(a,0) = AF(0,a) = 0$, $AF(a,1) = AF(1,a) = a$ для всех $a \in [0,1]$;
- A2) монотонность: для всех $a_1, a_2, b_1, b_2 \in [0,1]$, таких, что $a_1 \leqslant a_2$, $b_1 \leqslant b_2$, справедливо $AF(a_1,b_1) \leqslant AF(a_2,b_2)$;
- A3) коммутативность: $AF(a,b) = AF(b,a)$ для всех $a, b \in [0,1]$;
- A4) ассоциативность: $AF(AF(a,b),c) = AF(a,AF(b,c))$ для всех $a,b,c \in [0,1]$;
- A5) условие липшиц-непрерывности: $AF(c,b) - AF(a,b) \leqslant c - a$, $a \leqslant c$, $a,b,c \in [0,1]$.

Геометрически график ассоциативной функции — это поверхность (рис. 1), которая «натянута» на четырёхугольник с вершинами $(0,0,0)$, $(0,1,0)$, $(1,0,0)$ и $(1,1,1)$.

На рис. 1 стороны четырёхугольника выделены жирными линиями и соответствуют граничным условиям A1. Согласно свойству A2, ассоциативная функция возрастает по вертикали и по горизонтали [8, 9], а по свойству A3 она симметрична относительно плоскости $a = b$. Свойства A1–A3, A5 гарантируют, что значение функции $AF(a, b)$ обладает свойствами вероятности. Свойство A4 позволяет рекуррентно перейти к n-местной функции.

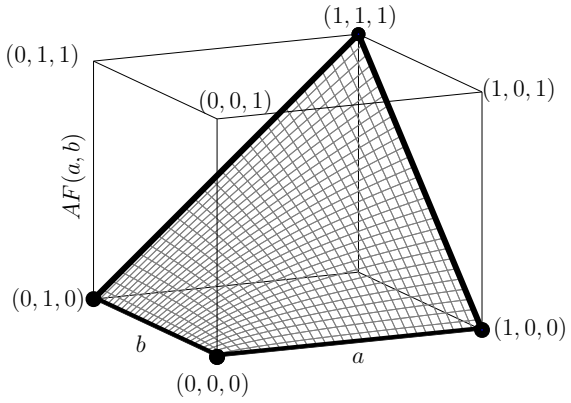

Рис. 1. График произвольной ассоциативной функции

Заметим, что свойства ассоциативной функции A1–A4 соответствуют свойствам треугольной нормы (t-нормы). Понятие t-нормы введено и используется в теории вероятностных метрических пространств [10, 11]. В настоящее время t-нормы получили широкое применение в нечёткой логике в качестве операции конъюнкции. Они представляют интерес для нечёткой логики, потому что сохраняют основные свойства связки «и», которые выполняются одновременно, а именно коммутативность, монотонность, ассоциативность и ограниченность, и, таким образом, служат естественным обобщением классической конъюнкции для многозначных систем рассуждений [8, 12, 13]. Классом бинарных операций, которые связаны с t-нормами, являются копулы [9], введённые А. Скляром в 1959 г. Модели на основе копул чрезвычайно значимы для моделирования многомерных наблюдений, ведь копула содержит всю информацию о природе зависимости между случайными величинами, которой нет в маргинальных распределениях, но не содержит информации о маргинальных распределениях. В результате информация о маргиналах и информация о зависимости между ними отделяются копулой друг от друга [9]. Таким образом, модели с использованием копул определяют функцию совместного распределения случайных величин в виде двух частей, что позволяет отдельно рассматривать одномерные маргинальные распределения и функцию, отвечающую за их зависимость [9]. В нашем случае использование копул позволяет представить вероятность пересечения множества событий через вероятности событий и функцию AF, отражающую их взаимосвязь. Некоторые семейства t-норм известны как семейства копул под различными именами. В [8] доказано, что свойство A5 даёт условия, при которых t-норма является копулой. С другой стороны, любая коммутативная и ассоциативная копула является t-нормой. Известно [8, 9, 13], что любая копула удовлетворяет границам Фреше — Хёфдинга, которые, как следствие, справедливы и для ассоциативных функций (рис. 2).

Таким образом, с учётом [8, 9, 13] и вышеизложенного определение 4 можно выразить так: ассоциативная функция — непрерывная t-норма, удовлетворяющая условию

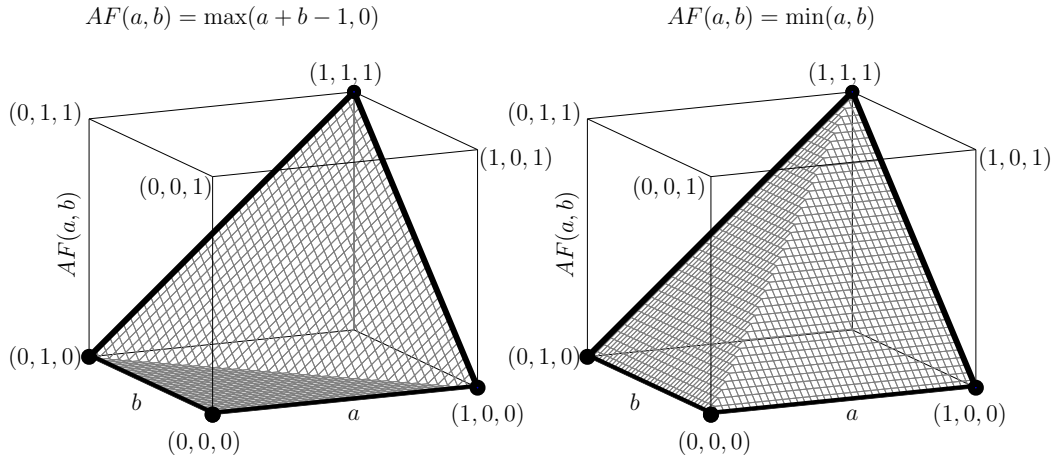

Рис. 2. Нижняя и верхняя границы Фреше — Хёфдинга для ассоциативных функций

Липшица, или, что то же самое, ассоциативная и коммутативная копула. Именно такая трактовка понятия ассоциативной функции используется далее.

2. Рекуррентное построение вероятностных распределений случайных множеств событий ассоциативными функциями

Применим аппарат ассоциативных функций к вероятностным распределениям случайных множеств событий. В качестве аргументов ассоциативной функции предлагается рассматривать вероятности событий, их число совпадает с мощностью базового множества. Таким образом, ассоциативные функции связывают вероятности пересечения множества событий $p_X = \mathbf{P}\left(\bigcap\limits_{x\in X} x\right)$ с вероятностями самих событий $p_x = \mathbf{P}(x)$, $x \in X$, $X \subseteq \mathfrak{X}$. Перейдём к изложению подхода.

Вход:

— множество событий $\mathfrak{X}$, $|\mathfrak{X}| = N$;
— N вероятностей событий p_x, $x \in \mathfrak{X}$;
— ассоциативная функция $AF(a,b)$.

Выход: вероятностное распределение II рода $\{p_X, X \subseteq \mathfrak{X}\}$ случайного множества событий K на $\mathfrak{X}$.

Основная идея: исходя из известных вероятностей событий $p_x = \mathbf{P}(x)$, $x \in \mathfrak{X}$, формирование вероятностей пересечения множеств событий p_X осуществлять последовательно согласно рекуррентной формуле

$$p_X = \mathbf{P}\left(\bigcap_{x\in X} x\right) = AF\left(p_x, \mathbf{P}\left(\bigcap_{y\in X\setminus\{x\}} y\right)\right), \qquad X \subseteq \mathfrak{X}, \qquad |X| > 1. \tag{6}$$

Например,

$$p_{xy} = \mathbf{P}(x \cap y) = AF(p_x, p_y),$$
$$p_{xyz} = \mathbf{P}(x \cap y \cap z) = AF(p_x, AF(p_y, p_z)) = AF(p_x, \mathbf{P}(y \cap z)),$$

и далее аналогичным образом. Напомним, что вероятность II рода для пустого множества событий всегда известна и равна 1.

Формула (6) позволяет построить вероятностное распределение II рода случайного множества событий, где в качестве входных параметров выступают N вероятностей событий и вид ассоциативной функции. В результате формируются $2^N - N - 1$ вероятностей II рода, удовлетворяющих границам Фреше — Хёфдинга, которых не хватало до полного набора. Однако полученные распределения могут быть нелигитимными в смысле определения 3. Следовательно, для каждого семейства ассоциативных функций необходимо определять условия легитимности построенных распределений.

3. Демонстрация рекуррентного построения вероятностных распределений случайных множеств событий

Проиллюстрируем предложенный рекуррентный подход на трех ассоциативных функциях, изученных в работах [8, 9, 12, 13]:

— $AF(a,b) = a \cdot b$;
— $AF(a,b) = \min\{a,b\}$;
— $AF(a,b) = \max\{a+b-1,0\}$.

Покажем для каждой из них, к какому вероятностному распределению случайного множества событий она приводит. Исследуем легитимность этого распределения.

Теорема 1. Пусть заданы вероятности событий $p_x = \mathbf{P}(x) > 0$, $x \in \mathfrak{X}$. Тогда ассоциативная функция

$$AF(a,b) = a \cdot b \tag{7}$$

определяет независимо-точечное случайное множество событий с легитимным вероятностным распределением II рода.

Доказательство. Доказательство теоремы следует непосредственно из определения независимо-точечного случайного множества [5, 14]. Исходя из этого определения, значениями независимо-точечного случайного множества K служат подмножества $X \subseteq \mathfrak{X}$ наступивших событий, независимых в совокупности. Поскольку события из $\mathfrak{X}$ независимы в совокупности, то для всех $X \subseteq \mathfrak{X}$ справедливо

$$p_X = \mathbf{P}\left(\bigcap_{x\in X} x\right) = \prod_{x\in X} \mathbf{P}(x) = \prod_{x\in X} p_x. \tag{8}$$

С другой стороны, для $X \subseteq \mathfrak{X}$ по формуле (6) получаем

$$p_X = AF\left(p_x, \mathbf{P}\left(\bigcap_{y\in X\setminus\{x\}} y\right)\right) = \prod_{x\in X} p_x. \tag{9}$$

Из (8) и (9) следует, что ассоциативная функция (7) определяет независимо-точечное случайное множество событий.

Известно [5, 14], что для независимо-точечного случайного множества событий распределение вероятностей I рода имеет вид

$$p(X) = \prod_{x\in X} \mathbf{P}(x) \prod_{x\in X^c} \mathbf{P}(x^c) = \prod_{x\in X} p_x \prod_{x\in X^c} (1-p_x), \quad X \subseteq \mathfrak{X},$$

и это распределение всегда легитимное.

Таким образом, формула (6) с ассоциативной функцией (7) всегда позволяет построить одно легитимное распределение, которое определяет независимо-точечное случайное множество событий. ■

Теорема 2. Пусть заданы вероятности событий $p_x = \mathbf{P}(x) > 0$, $x \in \mathfrak{X}$. Тогда ассоциативная функция

$$AF(a,b) = \min\{a,b\} \tag{10}$$

определяет случайное множество вложенных событий с легитимным вероятностным распределением II рода.

Доказательство. Упорядочим события в $\mathfrak{X} = \{x_1, x_2, \ldots, x_N\}$ в порядке возрастания их вероятностей $p_{x_1} \leqslant p_{x_2} \leqslant \ldots \leqslant p_{x_N}$. Применение формулы (6) даёт

$$\begin{aligned} p_{x_i x_j} &= \mathbf{P}\left(x_i \cap x_j\right) = \min\left\{p_{x_i}, p_{x_j}\right\} = p_{x_i},\ i < j, \\ p_{x_i x_j x_k} &= \mathbf{P}\left(x_i \cap x_j \cap x_k\right) = \min\left\{p_{x_i}, p_{x_j}, p_{x_k}\right\} = p_{x_i},\ i < j < k. \end{aligned} \tag{11}$$

Из (11) следует, что $x_i \subseteq x_j \subseteq x_k$. Действительно, если $x \subseteq y$, то $\mathbf{P}(x \cap y) = \mathbf{P}(x)$; если $x \subseteq y$ и $y \subseteq z$, то $x \subseteq y \subseteq z$ и $\mathbf{P}(x \cap y \cap z) = \mathbf{P}(x)$.

Рассмотрим упорядоченный набор индексов $I \subseteq \{1, 2, \ldots, N\}$, соответствующий некоторому подмножеству $X \subseteq \mathfrak{X}$, элементы которого упорядочены в порядке возрастания вероятностей событий. Тогда формула (6) примет вид

$$p_X = \mathbf{P}\left(\bigcap_{i\in I} x_i\right) = \min_{i\in I}\{p_{x_i}\} = p_{x_m},\ \text{где } m = \min_{i\in I} i. \tag{12}$$

Формула (12) определяет вероятностное распределение случайного множества K, заданного на множестве $\mathfrak{X} \subset \mathcal{F}$ из N вложенных друг в друга событий $x_1 \subseteq x_2 \subseteq \ldots \subseteq x_N$.

Обратимся теперь к вопросу легитимности полученного вероятностного распределения II рода случайного множества вложенных событий (12). По формулам обращения Мёбиуса (4) перейдём к вероятностному распределению I рода и получим $N+1$ ненулевую вероятность

$$\begin{gathered} p(\mathfrak{X}) = \mathbf{P}\left(\bigcap_{i\in\{1,\ldots,N\}} x_i\right) = p_{x_1};\quad p(\mathfrak{X}\setminus\{x_1\}) = \mathbf{P}\left(\bigcap_{i\in\{2,\ldots,N\}} x_i\right) = p_{x_2} - p_{x_1}; \\ p(\mathfrak{X}\setminus\{x_1,x_2\}) = \mathbf{P}\left(\bigcap_{i\in\{3,\ldots,N\}} x_i\right) = p_{x_3} - p_{x_2}; \\ \ldots \\ p(\mathfrak{X}\setminus\{x_1,x_2,\ldots,x_{k-1}\}) = \mathbf{P}\left(\bigcap_{i\in\{k,\ldots,N\}} x_i\right) = p_{x_k} - p_{x_{k-1}}; \\ \ldots \\ p(x_{N-1}x_N) = \mathbf{P}\left(x_{N-1}\cap x_N\right) = p_{x_{N-1}} - p_{x_{N-2}};\quad p(x_N) = \mathbf{P}\left(x_N\right) = p_{x_N} - p_{x_{N-1}}; \\ p(\varnothing) = \mathbf{P}\left(\bigcap_{i\in\{1,\ldots,N\}} x_i^c\right) = 1 - p_{x_N}. \end{gathered} \tag{13}$$

Остальные $2^N - N - 1$ вероятности равны нулю.

Из (13) видно, что полученное распределение I рода удовлетворяет условиям (1) и (2), следовательно, формула (6) с ассоциативной функцией (10) всегда позволяет построить одно легитимное распределение, которое определяет случайное множество вложенных событий. ■

Теорема 3. Пусть заданы вероятности событий $p_x = \mathbf{P}(x) > 0$, $x \in \mathfrak{X}$. Ассоциативная функция

$$AF(a,b) = \max\{a+b-1, 0\} \tag{14}$$

определяет

1) случайное множество с непересекающейся структурой зависимостей с легитимным вероятностным распределением, если вероятности событий $p_x = \mathbf{P}(x)$, $x \in \mathfrak{X}$, удовлетворяют неравенству

$$\sum_{x\in\mathfrak{X}} p_x \leqslant 1; \tag{15}$$

2) случайное множество событий с легитимным вероятностным распределением, если вероятности событий $p_x = \mathbf{P}(x)$, $x \in \mathfrak{X}$, удовлетворяют неравенствам

$$|\mathfrak{X}| - 1 \leqslant \sum_{x\in\mathfrak{X}} p_x \leqslant |\mathfrak{X}|. \tag{16}$$

Доказательство. В [12, 13] получен вид n-местной функции

$$AF(a_1, \ldots, a_n) = \max\left\{\sum_{i=1}^{n} a_i - n + 1, 0\right\}.$$

Для всех $X \subseteq \mathfrak{X}$, $|X| > 1$, из (6) и (3) следует

$$p_X = AF\left(p_x, \mathbf{P}\left(\bigcap_{y\in X\setminus\{x\}} y\right)\right) = \max\left\{\sum_{x\in X} p_x - |X| + 1, 0\right\}. \tag{17}$$

Рассмотрим следующие ситуации.

1) Пусть в (17) все вероятности p_X равны нулю, т. е. $\max\left\{\sum\limits_{x\in X} p_x - |X| + 1, 0\right\} = 0$ для всех $X \subseteq \mathfrak{X}$, таких, что $|X| > 1$. По формулам обращения Мёбиуса (4) перейдём к вероятностному распределению I рода:

$$\begin{gathered} p(x) = p_x \text{ для всех } x \in \mathfrak{X}, \\ p(X) = 0 \text{ для всех } X \subseteq \mathfrak{X}, \text{ таких, что } |X| > 1, \\ p(\varnothing) = 1 - \sum_{x\in\mathfrak{X}} p_x. \end{gathered} \tag{18}$$

Очевидно, что полученное распределение (18) удовлетворяет свойству (1), если $p(\varnothing) \geqslant 0$. Следовательно, распределение будет легитимным тогда и только тогда, когда $\sum\limits_{x\in\mathfrak{X}} p_x \leqslant 1$.

2) Пусть в (17) все $p_X \neq 0$, $X \subseteq \mathfrak{X}$, $|X| > 1$. Тогда из (17) и условия (1) следует $0 < \sum\limits_{x\in X} p_x - |X| + 1 \leqslant 1$ или, что эквивалентно, $|X| - 1 < \sum\limits_{x\in X} p_x \leqslant |X|$.

По формулам обращения Мёбиуса (4), используя принципы сет-суммирования [3], получим легитимное вероятностное распределение I рода:

$$\begin{gathered} p(X) = 0 \text{ для всех } X \subset \mathfrak{X} \text{ мощности } |X| < |\mathfrak{X}| - 1, \\ p(\mathfrak{X} \setminus \{x\}) = 1 - p_x \text{ для всех } x \in \mathfrak{X}, \\ p(\mathfrak{X}) = \sum_{x\in\mathfrak{X}} p_x - |\mathfrak{X}| + 1. \end{gathered} \tag{19}$$

Таким образом, ассоциативная функция (14) определяет случайное множество событий с легитимным вероятностным распределением (19), если вероятности событий $p_x = \mathbf{P}(x)$, $x \in \mathfrak{X}$, удовлетворяют системе из $2^{|\mathfrak{X}|} - 1$ неравенств

$$|X| - 1 < \sum_{x \in X} p_x \leqslant |X|, \ X \subseteq \mathfrak{X}. \tag{20}$$

Покажем, что если выполняется неравенство (16), то справедлива вся система (20). Действительно, пусть $|\mathfrak{X}| - 1 \leqslant \sum\limits_{x \in \mathfrak{X}} p_x \leqslant |\mathfrak{X}|$. Оценка сверху $\sum\limits_{x \in X} p_x \leqslant |X|$ для всех $X \subseteq \mathfrak{X}$ следует из свойства вероятности $p_x \leqslant 1$. Оценка снизу для $X \subset \mathfrak{X}$ получается следующим образом:

$$\sum_{x \in \mathfrak{X}} p_x = \sum_{x \in X} p_x + \sum_{y \in \mathfrak{X} \setminus X} p_y \geqslant |\mathfrak{X}| - 1 \Rightarrow \sum_{x \in X} p_x \geqslant |\mathfrak{X}| - 1 - \sum_{y \in \mathfrak{X} \setminus X} p_y \Rightarrow$$
$$\Rightarrow \sum_{x \in X} p_x \geqslant |\mathfrak{X}| - 1 - (|\mathfrak{X}| - |X|) \Rightarrow \sum_{x \in X} p_x \geqslant |X| - 1.$$

Из (20) также следует, что для получения легитимного распределения требуется, чтобы все p_X были больше нуля, за исключением, может быть, $p_{\mathfrak{X}}$. Действительно, пусть для некоторого X, такого, что $1 < |X| < |\mathfrak{X}|$, вероятность p_X равна нулю, а все остальные вероятности, полученные с помощью ассоциативной функции (14), отличны от нуля. Из (17) и (20) следует, что $\sum\limits_{x \in X} p_x = |X| - 1$. Добавим к множеству X любое событие y из $\mathfrak{X} \setminus X$. Тогда для множества $X \cup \{y\}$ из (20) получаем

$$|X| \leqslant \sum_{x \in X} p_x + p_y \leqslant |X| + 1 \Rightarrow |X| \leqslant |X| - 1 + p_y \leqslant |X| + 1 \Rightarrow 1 \leqslant p_y \leqslant 2,$$

что противоречит свойству вероятности $0 \leqslant p_y \leqslant 1$.

Рассмотрим ситуацию, когда $\sum\limits_{x \in \mathfrak{X}} p_x = |\mathfrak{X}| - 1$, т. е. $p_{\mathfrak{X}} = 0$. Из (20) следует, что все $p_X > 0$ для $X \subset \mathfrak{X}$. По формулам обращения Мёбиуса (4), используя принципы сет-суммирования [3], получим легитимное вероятностное распределение I рода:

$$p(X) = 0 \text{ для всех } X \subset \mathfrak{X} \text{ мощности } |X| < |\mathfrak{X}| - 1,$$
$$p(\mathfrak{X} \setminus \{x\}) = \sum_{y \in \mathfrak{X} \setminus \{x\}} p_y - |\mathfrak{X}| + 2 \text{ для всех } x \in \mathfrak{X}, \quad p(\mathfrak{X}) = 0.$$

Теорема доказана. ■

Из теоремы 3 можно сделать следующий вывод: рекуррентное построение легитимного вероятностного распределения случайного множества событий с использованием ассоциативной функции (14) возможно только при выполнении определённых ограничений на входные вероятности событий. При этом возникают только три вида результирующих случайных множеств событий с соответствующими вероятностными распределениями:

1) случайное множество непересекающихся событий, если выполнено условие (15);
2) случайное множество событий, принимающее значения с ненулевой вероятностью лишь на подмножествах мощности $|\mathfrak{X}| - 1$ и $|\mathfrak{X}|$, если $|\mathfrak{X}| - 1 < \sum\limits_{x \in \mathfrak{X}} p_x \leqslant |\mathfrak{X}|$;
3) случайное множество событий, принимающее значения с ненулевой вероятностью лишь на подмножествах мощности $|\mathfrak{X}| - 1$, если $\sum\limits_{x \in \mathfrak{X}} p_x = |\mathfrak{X}| - 1$.

Заключение

Предложен новый подход к определению дискретного вероятностного распределения II рода случайного множества на конечном множестве из N событий на основе заданной ассоциативной функции. Преимущество предлагаемого подхода заключается в том, что для определения вероятностного распределения вместо полного набора 2^N вероятностей достаточно знать N вероятностей событий и вид ассоциативной функции. Данный подход продемонстрирован на примере трёх ассоциативных функций. Рассмотренные в работе функции хорошо известны и широко применяются как в нечёткой логике [8, 12, 13], так и в теории вероятностей [9 – 11]. Рекуррентное построение дискретного вероятностного распределения на основе данных ассоциативных функций привело к известным вероятностным распределениям случайных множеств событий с независимо-точечной (8), вложенной (13) и непересекающейся (18) структурой зависимостей, что подтверждает корректность предложенного подхода. Случайные множества с такими структурами зависимостей играют ключевую роль в теории случайных множеств событий, поскольку описывают «крайние» ситуации [15]. Стоит отметить, что предложенный рекуррентный подход с использованием ассоциативных функций (7) и (10) приводит всегда к одному из соответствующих легитимных вероятностных распределений случайного множества событий, в то время как рекуррентное построение легитимного вероятностного распределения случайного множества событий с использованием ассоциативной функции (14) возможно только при выполнении определённых ограничений на входные вероятности событий. При этом возникают только три вида результирующих случайных множеств событий с соответствующими вероятностными распределениями.

Перспективными представляются дальнейшие исследования характеристик построенных вероятностных распределений случайных множеств событий в зависимости от аргументов ассоциативных функций (7), (10), (14), а также изучение новых классов вероятностных распределений, построенных с использованием известных однопараметрических семейств ассоциативных функций, например Али — Михаэля — Хака, Франка и др. [8].

ЛИТЕРАТУРА

1. *Nguyen H. T.* An Introduction to Random Sets. Boca Raton: Taylor & Francis Group, LLC, 2006. 240 p.
2. *Ширяев А. Н.* Вероятность-1. М.: МЦНМО, 2004. 519 с.
3. *Воробьев О. Ю., Воробьев А. О.* Суммирование сет-аддитивных функций и формула обращения Мёбиуса // Доклады РАН. 2009. Т. 336. № 4. С. 417–420.
4. *Semenova D. V.* On new notion of quasi-entropies of eventological distribution // Proc. Second IASTED Intern. Multi-Conf. Automation Control and Inform. Technology. Novosibirsk: ACTA PRESS, 2005. P. 380–385.
5. *Vorobyev O. Yu. and Lukyanova N. A.* Properties of the entropy of multiplicative-truncated approximations of eventological distributions // J. Siberian Federal University. Math. & Physics. 2011. V. 4. No. 1. P. 50–60.
6. *Semenova D. V. and Lukyanova N. A.* Random set decomposition of joint distribution of random variables of mixed type // Proc. IAM. 2012. V. 1. No. 2. P. 50–60.
7. *Semenova D. V. and Shangareeva L. Yu.* Associative Ali-Mikhail-Haq's random set // Proc. scientific-applied conf. «Statistics and its Applications». Tashkent: National University of Uzbekistan, 2013. P. 88–94.

8. *Alsina S., Frank M., and Schveizer B.* Associative Functions: Triangular Norms and Copulas. Singapore: World Scientific Publishing Co. Pte. Ltd., 2006. 237 p.
9. *Nelsen R. B.* An Introduction to Copulas (second edition). N.Y.: Springer Science+Business Media, Inc., 2006. 270 p.
10. *Menger K.* Statistical metrics // Proc. Nat. Acad. Sci. USA. 1942. No. 8. P. 535–537.
11. *Schweizer B. and Sklar A.* Probabilistic Metric Spaces. N.Y.: North Holland, 1983. 275 p.
12. *Klement E. P., Mesiar R., and Pap E.* Triangular Norms. Boston: Kluwer Academic Pub., 2000. 220 p.
13. Logical, Algebraic, Analytic, and Probabilistic Aspects of Triangular Norms / eds. E. P. Klement and R. Mesiar. Amsterdam: Elsevier, 2005. 481 p.
14. *Орлов А. И.* Нечисловая статистика. М.: МЗ-Пресс, 2004. 513 с.
15. *Goldenok E. E., Lukyanova N. A., and Semenova D. V.* Applications of wide dependence theory in eventological scoring // Proc. IASTED Intern. Conf. Automation Control and Inform. Technology, Control, Diagnostics, and Automation. Novosibirsk: ACTA Press Anaheim|Calgary|Zurich, 2010. P. 316–322.

2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/6

УДК 519.7

О РАЗЛОЖЕНИИ ДУАЛЬНОЙ БЕНТ-ФУНКЦИИ В СУММУ ДВУХ БЕНТ-ФУНКЦИЙ[1]

Н. Н. Токарева

Институт математики им. С. Л. Соболева, г. Новосибирск, Россия

E-mail: tokareva@math.nsc.ru

Установлено, что бент-функции и функции, дуальные к ним, разложимы или не разложимы в сумму двух бент-функций одновременно.

Ключевые слова: *бент-функция, дуальная функция.*

Введение

Бент-функции — булевы функции с экстремальными нелинейными свойствами — интенсивно исследуются в связи с многими приложениями в криптографии, теории кодирования, дискретной математике [1]. Одним из нерешённых вопросов этой области остаётся вопрос об оценках числа таких функций.

В работе [2] предложен новый подход к этой проблеме и выдвинута гипотеза: *произвольная булева функция от n переменных степени $\leqslant n/2$ может быть представлена в виде суммы двух бент-функций от n переменных* (n *чётно,* $n \geqslant 2$). При малых $n = 2, 4, 6$ гипотеза проверена в [2], при $n = 8$ доказано [3], что каждая функция степени не выше трёх представима в виде суммы не более четырех бент-функций. Для произвольного n доказан [4] ослабленный вариант гипотезы. Авторы [5] доказали, что в виде суммы двух бент-функций может быть представлена любая квадратичная булева функция, любая бент-функция Мак-Фарланда, произвольная функция частичного расщепления. В работе [6] отмечается связь гипотезы с открытыми вопросами о метрических свойствах класса бент-функций.

В данной работе продолжено исследование разложимости произвольной булевой функции от чётного числа переменных в сумму двух бент-функций. Доказано, что бент-функции и функции, дуальные к ним, разложимы или не разложимы в сумму двух бент-функций одновременно.

1. Основные определения

Пусть $x = (x_1, \ldots, x_n)$ — двоичный вектор. Вектор x *предшествует* вектору y, если для всех $i = 1, \ldots, n$ выполняется $x_i \leqslant y_i$. Будем обозначать предшествование так: $x \preccurlyeq y$. Через $\mathrm{wt}(x)$ обозначим *вес* вектора x, т. е. число его ненулевых координат.

Напомним, что произвольная булева функция f от n переменных однозначно представляется с помощью *алгебраической нормальной формы* (АНФ):

$$f(x) = \sum_y f_y\, x_1^{y_1} \cdot \ldots \cdot x_n^{y_n}, \text{ где } f_y = \sum_{z \preccurlyeq y} f(z). \tag{1}$$

Здесь и далее под знаком суммы мы опускаем области значений векторов y, z, предполагая, что каждый вектор принимает все значения из множества $\mathbb{Z}_2^n$, возможно, с некоторыми ограничениями, как во втором случае: все такие z, что $z \preccurlyeq y$.

[1]Работа выполнена при финансовой поддержке РФФИ № 14-01-00507.

Степенью булевой функции называется число множителей в самом длинном слагаемом, присутствующем в её АНФ.

Преобразованием Уолша — Адамара булевой функции f от n переменных называется целочисленная функция W_f, заданная на множестве $\mathbb{Z}_2^n$ равенством

$$W_f(y) = \sum_x (-1)^{\langle x,y\rangle \oplus f(x)},$$

где $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$.

Булева функция f от чётного числа переменных n называется *бент-функцией*, если $W_f(x) = \pm 2^{n/2}$ для любого вектора x. *Дуальной функцией* к бент-функции f называется булева функция $\widetilde{f}$ от n переменных, определяющая знаки коэффициентов Уолша — Адамара функции f, т. е. $\widetilde{f}$ для каждого x определяется равенством

$$W_f(x) = (-1)^{\widetilde{f}(x)}\, 2^{n/2}.$$

Несложно показать, что дуальная функция — всегда бент-функция, более того, $\widetilde{\widetilde{f}} = f$.

Согласно [1], выполняется

Утверждение 1. Степень бент-функции от $n \geqslant 4$ переменных не превышает $n/2$.

Известен следующий факт [7, лемма 5.17]:

Утверждение 2. Пусть f — бент-функция от n переменных, $n \geqslant 4$. Тогда

$$\sum_{x \preccurlyeq y} f(x) = 2^{\mathrm{wt}(y)-1} - 2^{n/2-1} + 2^{\mathrm{wt}(y)-n/2} \sum_{x \preccurlyeq y \oplus 1} \widetilde{f}(x).$$

Бент-функции и функции, дуальные к ним, нередко исследуются вместе. Так, в работе [8] получен ряд результатов, направленных на характеризацию *самодуальных* бент-функций, т. е. таких, что $\widetilde{f} = f$. За исключением самодуальных функций, весь класс бент-функций разбивается на пары функций, связанных отношением дуальности. Интересно, что бент-функции из одной такой пары не обязательно имеют похожие свойства. Например, дуальные функции к бент-функциям Касами не являются мономиальными [9], а возможно (но пока это не доказано), и не эквивалентны им. Поэтому, если удаётся исследовать какое-либо свойство одновременно для бент-функций и функций, дуальных к ним, то «пространство исследования» сокращается в 2 раза (за исключением самодуальных функций). Далее покажем, что таким свойством как раз является разложимость функции в сумму двух бент-функций.

2. Разложение дуальных бент-функций

Теорема 1. Бент-функция от n переменных, $n \geqslant 4$, разложима в сумму двух бент-функций от n переменных тогда и только тогда, когда таким свойством обладает дуальная к ней бент-функция.

Доказательство. Пусть g — бент-функция от n переменных, такая, что $g = f \oplus h$, где f, h — бент-функции. Тогда для каждого ненулевого коэффициента g_y АНФ функции g справедливо представление $g_y = f_y \oplus h_y$, где y — произвольный вектор. Можем рассматривать лишь векторы веса не больше $n/2$, т. е. $\mathrm{wt}(y) \leqslant n/2$, поскольку в соответствии с утверждением 1 все коэффициенты g_y, f_y, h_y равны нулю, если $\mathrm{wt}(y) > n/2$. Согласно представлению (1), имеем

$$g_y = \sum_{x \preccurlyeq y} g(x) = \left(\sum_{x \preccurlyeq y} f(x)\right) \oplus \left(\sum_{x \preccurlyeq y} h(x)\right).$$

Используя равенство $a \oplus b = a + b - 2ab$, можем перейти в правой части к знакам обычного сложения и вычитания. По утверждению 2 выполняется равенство

$$\sum_{x \preccurlyeq y} g(x) = 2^{\mathrm{wt}(y)-1} - 2^{n/2-1} + 2^{\mathrm{wt}(y)-n/2} \sum_{x \preccurlyeq y \oplus 1} \widetilde{g}(x).$$

Используя его и аналогичные равенства для функций f, h, получаем

$$2^{\mathrm{wt}(y)-n/2} \left(\sum_{x \preccurlyeq y} \widetilde{g}(x) - \sum_{x \preccurlyeq y} \widetilde{f}(x) - \sum_{x \preccurlyeq y} \widetilde{h}(x) \right) = 2^{\mathrm{wt}(y)-1} - 2^{n/2-1} - 2 f_y h_y.$$

Домножим равенство на $2^{n/2-\mathrm{wt}(y)}$. Тогда

$$\sum_{x \preccurlyeq y} \widetilde{g}(x) - \sum_{x \preccurlyeq y} \widetilde{f}(x) - \sum_{x \preccurlyeq y} \widetilde{h}(x) = 2^{n/2-1} - 2^{n-\mathrm{wt}(y)-1} - 2^{n/2-\mathrm{wt}(y)+1} f_y h_y.$$

Заметим, что выражение в правой части чётное, поскольку $\mathrm{wt}(y) \leqslant n/2$ и $n \geqslant 4$. Поэтому, рассматривая равенство по модулю два, получаем

$$\sum_{x \preccurlyeq y} \widetilde{g}(x) = \sum_{x \preccurlyeq y} \widetilde{f}(x) \oplus \sum_{x \preccurlyeq y} \widetilde{h}(x),$$

т. е. $\widetilde{g}_y = \widetilde{f}_y \oplus \widetilde{h}_y$ для произвольного вектора y веса $\leqslant n/2$. Напомним, что для векторов большего веса это равенство автоматически выполняется. Таким образом, $\widetilde{g} = \widetilde{f} \oplus \widetilde{h}$. Очевидно, что в обратную сторону теорема доказывается аналогично. ■

Следствие 1. Пусть g, f, h — бент-функции от n переменных, $n \geqslant 4$. Тогда если $g \oplus f \oplus h = 0$, то справедливо $\widetilde{g} \oplus \widetilde{f} \oplus \widetilde{h} = 0$.

Следствие 1 говорит о том, что, зная разложение бент-функции в сумму двух других, можно простым способом перейти к разложению дуальной бент-функции.

Следствие 2. Число различных разложений бент-функции g в сумму двух бент-функций равно числу аналогичных разложений дуальной бент-функции $\widetilde{g}$.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N. N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. Math. Comm. 2011. V. 5. No. 4. P. 609–621.
3. *Tokareva N. N.* Every cubic Boolean function in 8 variables is the sum of not more than 4 bent functions // Прикладная дискретная математика. Приложение. 2014. № 7. С. 38–39.
4. *Токарева Н. Н.* О разложении булевой функции в сумму бент-функций // Прикладная дискретная математика. Приложение. 2012. № 5. С. 30.
5. *Qu L. and Li C.* When a Boolean function can be expressed as the sum of two bent functions // Cryptology ePrint Archive. 2014/048.
6. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. 2014. № 3. С. 28–39.
7. *Cusick T. W. and Stănică P.* Cryptographic Boolean Functions and Applications. San Diego: Acad. Press, 2009. 245 p.
8. *Carlet C., Danielsen L.-E., Parker M. G., and Solé P.* Self-dual bent functions // Int. J. Inform. and Coding Theory. 2010. V. 1. No. 4. P. 384–399.
9. *Langevin Ph. and Leander G.* Monomial bent functions and Stickelberger's theorem // Finite Fields and Their Applications. 2008. V. 14. No. 3. P. 727–742.

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ И СЖАТИЯ ИНФОРМАЦИИ

DOI 10.17223/20710410/26/7

УДК 517.19

ОЦЕНКА СТОЙКОСТИ КОДОВОГО ЗАШУМЛЕНИЯ К l-КРАТНОМУ ЧАСТИЧНОМУ НАБЛЮДЕНИЮ В СЕТИ

И. И. Винничук, Ю. В. Косолапов

Южный федеральный университет, г. Ростов-на-Дону, Россия

E-mail: ilonavinnichuk144@gmail.com

Рассматривается сеть передачи данных с линейным кодированием в узлах. Предполагается, что наблюдатель подслушивает данные, передаваемые по некоторым рёбрам сети, а информация, поступающая на вход сети, защищается с помощью кодового зашумления. В рамках этой модели решается задача анализа стойкости кодового зашумления при многократном подслушивании в сети данных, соответствующих одному информационному слову. Получена формула вычисления стойкости после l перехватов для $l \geqslant 1$. Для одной сети в качестве примера рассмотрено применение полученной формулы при анализе стойкости кодового зашумления, основанного на коде Рида — Маллера $\mathcal{R}(1,3)$.

Ключевые слова: *сетевое кодирование, частичное наблюдение, кодовое зашумление, анализ стойкости.*

Введение

В работе рассматривается передача данных по сети связи, в узлах которой над принятыми данными выполняются линейные операции. Такие сети отличаются от традиционных сетей, где узлы могут только принимать, временно хранить и передавать данные другим узлам [1]. В работах [2 – 4] показано, что с помощью методов сетевого кодирования можно увеличить пропускную способность сети. В частности, в [4] показано, как повысить производительность сети без радикальных изменений в инфраструктуре сети передачи данных. Отметим, что пропускная способность сети может быть увеличена в случае, когда получателей не менее двух.

Как и в случае каналов связи, в сетях связи также возникает задача защиты конфиденциальности передаваемых данных от несанкционированного ознакомления (наблюдения). Кроме естественных методов защиты, основанных на применении криптографических преобразований, в последнее время активно исследуются методы, специфичные для сетей [5, 6]. Эти методы основаны на том, что потенциальному наблюдателю доступны не все передаваемые по сети данные, а только их часть. Такой подход оправдан по той причине, что сеть, как правило, географически распределена и контролирование всех каналов сети для наблюдателя в большинстве случаев может оказаться неприемлемым или невозможным. Учитывая частичную доступность данных наблюдателю, одним из подходящих способов защиты является метод кодового зашумления, использованный в [7] для защиты данных от частичного наблюдения в канале.

По частично наблюдаемым данным подслушивающий может построить множество возможных информационных блоков (претендентов), которым соответствуют наблю-

даемые данные. Чем больше мощность этого множества претендентов, тем больше неопределённость наблюдателя относительного информационного блока и соответственно тем лучше защита. Часто, в силу особенности структуры, передаваемое сообщение (состоящее из набора информационных блоков) содержит повторяющиеся блоки. Эта особенность даёт возможность наблюдателю провести атаку многократного подслушивания с целью уменьшить мощность множества претендентов. В частности, наблюдатель может провести атаку многократного частичного подслушивания в сети. В случае применения метода кодового зашумления задача наблюдателя по сокращению множества претендентов усложняется за счёт того, что одному информационному блоку, в силу особенностей метода, соответствуют разные кодовые блоки.

Модель многократного частичного подслушивания в канале рассмотрена, например, в [8], где получена зависимость неопределённости наблюдателя от множеств наблюдаемых координат, когда данные перед отправкой в канал преобразуются с помощью метода кодового зашумления. В настоящей работе ставится задача оценки неопределённости наблюдателя в рамках модели многократного наблюдения частичных данных в сети с линейными преобразованиями в узлах, когда информационные блоки на входе сети кодируются с помощью метода кодового зашумления.

Работа организована следующим образом. В п. 1.1 и 1.2 приведены необходимые сведения о линейном сетевом кодировании и методе кодового зашумления соответственно. В п. 1.3 строится модель многократного перехвата в сети и вводится мера неопределённости наблюдателя после многократного перехвата. Оценке этой меры посвящён п. 2, где в п. 2.1 эта мера оценивается в случае однократного перехвата, а в п. 2.2 этот результат обобщается на случай многократного перехвата. В п. 2.3 приводится пример вычисления меры неопределённости для одной сети и кода Рида — Маллера $\mathcal{R}(1,3)$.

1. Предварительные сведения и результаты

1.1. Сетевое кодирование

Приведём необходимые сведения из теории сетевого кодирования. Пусть $\mathbb{F}_q$ — конечное поле. Сеть связи $\mathcal{N}$, состоящая из одного источника S, t получателей и промежуточных узлов, представляется в виде конечного связанного направленного графа. Стоит отметить, что для повышения пропускной способности сети необходимо выполнение условия $t \geqslant 2$ [2], однако результат, полученный в настоящей работе, может быть применён и для сетей, где $t = 1$. Поэтому здесь и далее с целью общности полагается, что t — произвольное натуральное число. Множества всех узлов и рёбер сети $\mathcal{N}$ обозначим соответственно $\mathcal{V}$ и $\mathcal{E}$; $v(\mathcal{N}) = |\mathcal{V}|$, $e(\mathcal{N}) = |\mathcal{E}|$. Узлы сети будем обозначать прописными латинскими буквами, а рёбра — строчными. Для узла U множества входных и выходных рёбер обозначим $\mathrm{In}(U)$ и $\mathrm{Out}(U)$ соответственно. Будем полагать, что источник S имеет n мнимых входных ребер, множество которых обозначим $\mathrm{Im}(S)$, $|\mathrm{Im}(S)| = n$, и по мнимым входным рёбрам в источник S загружается вектор данных $\mathbf{x} \in \mathbb{F}_q^n$, который необходимо передать по сети: по каждому мнимому ребру загружается одна компонента вектора $\mathbf{x}$. Предполагается, что в сети $\mathcal{N}$ нет помех.

Линейный сетевой код размерности n задается с помощью линейных локального и глобального кодирующих отображений, а именно: для узла U и канала $e \in \mathrm{Out}(U)$ локальным кодирующим отображением называется отображение вида $\widetilde{k}_e : \mathbb{F}_q^{|\mathrm{In}(U)|} \to \mathbb{F}_q$, а глобальным кодирующим отображением для узла $U \neq S$ и канала $e \in \mathrm{Out}(U)$ — отображение вида

$$\widetilde{f}_e : \mathbb{F}_q^n \to \mathbb{F}_q,$$

однозначно определяемое с помощью упорядоченного множества $\{\widetilde{f}_d(x)) : d \in \mathrm{In}(U)\}$ и локального отображения $\widetilde{k}_e$ для этого ребра e [9]. Так как сеть линейная, для узла U каждому локальному отображению $\widetilde{k}_e$, $e \in \mathrm{Out}(U)$, можно сопоставить вектор-столбец $\widetilde{\mathbf{k}}_e \in \mathbb{F}_q^{|\mathrm{In}(U)|}$, определяющий это отображение. Тогда узлу U соответствует $(|\mathrm{In}(U)| \times |\mathrm{Out}(U)|)$-матрица локальных сетевых линейных преобразований, составленная из столбцов $\widetilde{\mathbf{k}}_e$:

$$K_U = [\widetilde{\mathbf{k}}_e]_{e \in \mathrm{Out}(U)}. \tag{1}$$

Матрица (1) для U позволяет по значениям на входных рёбрах узла U вычислить значения на его выходных рёбрах. Линейному отображению $\widetilde{f}_e$ также можно однозначно сопоставить вектор-столбец $\widetilde{\mathbf{f}}_e \in \mathbb{F}_q^n$ высоты n, определяющий это отображение:

$$\widetilde{\mathbf{f}}_e = [f_{e,1}, \ldots, f_{e,n}]^{\mathrm{T}}, \tag{2}$$

где символом $\mathbf{a}^{\mathrm{T}}$ обозначаем транспонирование вектора $\mathbf{a}$. Отметим, что для источника S набор $(\widetilde{\mathbf{f}}_e)_{e \in \mathrm{Im}(S)}$ должен образовывать базис векторного пространства $\mathbb{F}_q^n$. Глобальное отображение $\widetilde{f}_e$ позволяет по вектору входных данных длины n определить элемент поля $\mathbb{F}_q$, передаваемый по ребру e. Другими словами, по известному входному вектору $\mathbf{x}$, загружаемому по мнимым рёбрам в источник S сети $\mathcal{N}$, для каждого ребра $e \in \mathcal{E}$ можно определить передаваемое по этому ребру значение, используя глобальное отображение (2) для этого ребра. Таким образом, по вектору $\mathbf{x}$ можно построить вектор значений, передаваемых по рёбрам сети $\mathcal{N}$, вида

$$\mathcal{F}(\mathbf{x}) = (\widetilde{f}_e(\mathbf{x}))_{e \in \mathcal{E}}. \tag{3}$$

Отметим, что координаты вектора (3) помечены рёбрами сети.

1.2. Кодовое зашумление

Предположим, что имеется наблюдатель, который может подслушивать значения, передаваемые по $\mu \leqslant e(\mathcal{N})$ рёбрам сети $\mathcal{N}$. Пусть для защиты от такого наблюдения применяется метод кодового зашумления [7]. Опишем этот метод. Пусть $\mathcal{C}$ — линейный $(n, n-k)$-код с порождающей матрицей $G = G_{(n-k)\times n}$ и проверочной матрицей $H = H_{k\times n}$. Построим матрицу $\widetilde{G} = \widetilde{G}_{n\times n}$ вида

$$\widetilde{G} = \begin{pmatrix} G^* \\ G \end{pmatrix},$$

где $G^* = G^*_{k\times n}$ и $\mathrm{rank}(\widetilde{G}) = n$. Для кодирования информационного блока $\mathbf{s} \in \mathbb{F}_q^k$ случайным образом выбирается вектор $\mathbf{v} \in \mathbb{F}_q^{n-k}$ и выполняется операция

$$(\mathbf{s}||\mathbf{v})\widetilde{G} = \mathbf{s}G^* + \mathbf{v}G = \mathbf{x}. \tag{4}$$

Правило кодирования задаёт отображение

$$\mathbf{s} \mapsto C_{\mathbf{s}} = \mathbf{s}G^* + \mathcal{C},$$

которое каждому информационному блоку $\mathbf{s} \in \mathbb{F}_q^k$ ставит в соответствие фактор-класс $C_{\mathbf{s}}$ из фактор-множества $\mathbb{F}_q^n/\mathcal{C}$. Заметим, что за счёт случайного аргумента $\mathbf{v}$ в (4) один и тот же информационный блок $\mathbf{s}$ в разные моменты времени может быть закодирован, в общем случае, в разные кодовые векторы. Напомним, что кодовый

вектор $\mathbf{x}$, полученный по правилу (4), по мнимым рёбрам загружается в источник S сети $\mathcal{N}$.

Так как, по предположению, в сети $\mathcal{N}$ нет помех, каждый из t легитимных получателей примет исходный вектор $\mathbf{x}$. Согласно [10], матрицу H всегда можно выбрать так, что для любого информационного блока $\mathbf{s} \in \mathbb{F}_q^k$ и любого $\mathbf{x} \in C_{\mathbf{s}}$ справедливо равенство

$$\mathbf{x}H^{\mathrm{T}} = \mathbf{s}.$$

В соответствии с [10] код $\mathcal{C}$ будем называть базовым кодом, а код, построенный по $\mathcal{C}$, — факторным кодом и обозначать $(\mathbb{F}_q^n/\mathcal{C})$.

1.3. Модель l-кратного наблюдения

Пусть $\mathcal{C}$ — базовый $(n, n-k)$-код, $(\mathbb{F}_q^n/\mathcal{C})$ — соответствующий факторный код, $\mathbf{s} \in \mathbb{F}_q^k$ — информационный блок, $\mathbf{x}(1), \ldots, \mathbf{x}(l)$ — кодовые слова факторного кода $(\mathbb{F}_q^n/\mathcal{C})$, соответствующие информационному блоку $\mathbf{s}$ в моменты времени $1, \ldots, l$, $l \geqslant 1$. Случайный вектор, моделирующий множество информационных векторов, обозначим $\mathbf{S}$, а через $\mathbf{X}_i$ — случайный вектор, моделирующий кодовые векторы в момент времени i, $i \in \{1, \ldots, l\}$. Пусть $\mathcal{T}_i$ — множество рёбер, наблюдаемое в момент времени i, $i \in \{1, \ldots, l\}$, $\mathcal{T}_i \subseteq \mathcal{E}$, $|\mathcal{T}_i| = \mu_i$. Отметим, что множество $\{\mathcal{T}_i : i = 1, \ldots, l\}$ может содержать любые рёбра сети, в том числе и рёбра, по которым компоненты кодовых слов передаются в чистом виде, например мнимые рёбра. Тогда наблюдателю доступны для исследования частичные векторы значений $\mathcal{F}_{\mathcal{T}_1}(\mathbf{x}(1)), \ldots, \mathcal{F}_{\mathcal{T}_l}(\mathbf{x}(l))$, где в векторе $\mathcal{F}_{\mathcal{T}_i}(\mathbf{x}(i))$ длины μ_i координаты помечены рёбрами из $\mathcal{T}_i$ и для каждого $e \in \mathcal{T}_i$ координата с соответствующей меткой имеет значение $\widetilde{f}_e(\mathbf{x}(i))$, $i \in \{1, \ldots, l\}$ (см. (3)). Пусть для $i \in \{1, \ldots, l\}$ случайный вектор $\mathbf{Y}_{\mathcal{T}_i}(i)$ моделирует распределение соответствующего вектора значений вида $\mathcal{F}_{\mathcal{T}_i}(\mathbf{x}(i))$. Неопределённость наблюдателя при l-кратном подслушивании, соответствующем набору $\mathcal{T}_1, \ldots, \mathcal{T}_l$, определим естественным образом как условную энтропию

$$\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l} = \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)). \tag{5}$$

В общем случае предполагается, что в сети существует наблюдатель, который может произвольно выбирать набор $\mathcal{T}_1, \ldots, \mathcal{T}_l$, $|\mathcal{T}_i| = \mu_i$, $i = 1, \ldots, l$. Поэтому введём обозначение для минимально возможной неопределённости наблюдателя при заданном наборе $(\mu_1, \ldots, \mu_l)$:

$$\Delta(\mu_1, \ldots, \mu_l) = \min_{\mathcal{T}_i \subset \mathcal{E}, |\mathcal{T}_i| = \mu_i, i \in \{1,\ldots,l\}} \{\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l}\}. \tag{6}$$

В случае, когда $\mu_1 = \ldots = \mu_l = \mu$, величину $\Delta(\mu_1, \ldots, \mu_l)$ будем обозначать $\Delta^{(l)}(\mu)$.

2. Оценка меры неопределённости при l-кратном наблюдении

Предполагается, что наблюдателю известен факторный код, проверочная матрица базового кода и матрицы сетевых линейных преобразований вида (1) и (2). В случае, когда для всех μ_i, $i \in \{1, \ldots, l\}$, выполняется равенство $\Delta(\mu_i) = k$, будем говорить, что обеспечена совершенная защита. Если же это равенство не выполняется для некоторых $j \in \{1, \ldots, l\}$, то наблюдатель может попытаться выбрать подмножества наблюдаемых рёбер так, чтобы максимально уменьшить множество претендентов. Отметим, что существенным отличием от перехвата в канале является то, что наблюдатель наблюдает не координаты векторов в чистом виде, а их линейные комбинации.

2.1. Случай $l = 1$

Пусть информационный вектор $\mathbf{s} \in \mathbb{F}_q^k$ кодируется с помощью факторного кода $(\mathbb{F}_q^n/\mathcal{C})$ в вектор $\mathbf{x} = (x_1, \ldots, x_n)$. При передаче по сети вектора $\mathbf{x}$ по рёбрам графа передаются компоненты x_j, $j \in \{1, \ldots, n\}$, и их линейные комбинации. Пусть $\mathcal{T}$ — множество наблюдаемых рёбер, $|\mathcal{T}| = \mu$, H_1 — матрица вида

$$H_1 = \left[\widetilde{\mathbf{f}}_{e_1}, \ldots, \widetilde{\mathbf{f}}_{e_\mu}\right],$$

где $e_i \in \mathcal{T}$, $i = 1, \ldots, \mu$. Другими словами, H_1 — матрица, состоящая из столбцов линейных преобразований вида (2) над координатами вектора $\mathbf{x}$, $r = \operatorname{rank}(H_1)$. Тогда после подслушивания наблюдателю доступен вектор $\mathbf{y}$ вида

$$\mathbf{y} = \mathcal{F}_{\mathcal{T}}(\mathbf{x}) = \mathbf{x}H_1.$$

Отметим, что наблюдателю известна матрица H_1 линейного преобразования координат и результат преобразования $\mathbf{y}$, а вектор $\mathbf{x}$ неизвестен. Без потери общности можно полагать, что ранг матрицы H_1 равен μ, т. е. $r = \mu$. В противном случае подслушивание наблюдателя будет неоптимальным, так как какое-то из перехватываемых рёбер будет иметь значение, выражаемое линейно через другие перехватываемые значения. Поэтому как минимум одно из перехватываемых рёбер будет лишним. Таким образом, наблюдателю доступен для исследования вектор $\mathbf{y} \in \mathbb{F}_q^\mu$, составленный из наблюдаемых значений, передаваемых по μ рёбрам. Пусть $\mathcal{K}$ — $(n, n-r)$-код с проверочной матрицей H_1^{T}. Для полноты изложения приведём простую лемму.

Лемма 1. Пусть $\mathcal{K}$, $\mathcal{C}$ — подпространства $\mathbb{F}_q^n$, $\widehat{\mathcal{C}} = \mathcal{K} \cap \mathcal{C}$. Если смежные классы $\mathfrak{a}$ из $\mathbb{F}_q^n/\mathcal{C}$ и $\mathfrak{b}$ из $\mathbb{F}_q^n/\mathcal{K}$ пересекаются, то $|\mathfrak{a} \cap \mathfrak{b}| = q^{\dim(\widehat{C})}$.

Доказательство. Так как $\widehat{\mathcal{C}} \subset \mathcal{C}$ и $\widehat{\mathcal{C}} \subset \mathcal{K}$, то можно построить разбиения подпространств $\mathcal{C}$ и $\mathcal{K}$: $\mathcal{C}/\widehat{\mathcal{C}}$, $\mathcal{K}/\widehat{\mathcal{C}}$. Смежные классы $\mathfrak{a} \in \mathcal{C}/\widehat{\mathcal{C}}$ и $\mathfrak{b} \in \mathcal{K}/\widehat{\mathcal{C}}$ представим в следующем виде:

$$\mathfrak{a} = \bigcup_{\widetilde{a}} \{\widetilde{a} + \widehat{\mathcal{C}}\}, \quad \mathfrak{b} = \bigcup_{\widetilde{b}} \{\widetilde{b} + \widehat{\mathcal{C}}\},$$

где $\widetilde{a} \in \mathcal{C} \setminus \widehat{\mathcal{C}}$; $\widetilde{b} \in \mathcal{K} \setminus \widehat{\mathcal{C}}$. Так как смежный класс $\mathfrak{a}$ из $\mathbb{F}_q^n/\mathcal{C}$ пересекается со смежным классом $\mathfrak{b}$ из $\mathbb{F}_q^n/\mathcal{K}$, то существуют $\widetilde{a} \in \mathcal{C}\setminus\widehat{\mathcal{C}}$, $\widetilde{b} \in \mathcal{K}\setminus\widehat{\mathcal{C}}$, $\widehat{c}_1, \widehat{c}_2 \in \widehat{\mathcal{C}}$, такие, что $\widetilde{a}+\widehat{c}_1 = \widetilde{b}+\widehat{c}_2$. Тогда для всех $\widehat{c} \in \widehat{\mathcal{C}}$ справедливо равенство $\widetilde{a} + \widehat{c}_1 + \widehat{c} = \widetilde{b} + \widehat{c}_2 + \widehat{c}$. Следовательно, $|\mathfrak{a} \cap \mathfrak{b}| = q^{\dim(\widehat{C})}$. ■

Следствие 1. Пусть $\mathcal{K}$, $\mathcal{C}$ — подпространства $\mathbb{F}_q^n$, $\widehat{\mathcal{C}} = \mathcal{K} \cap \mathcal{C}$. Тогда каждый смежный класс из $\mathbb{F}_q^n/\mathcal{K}$ пересекается с $q^{\dim(\mathcal{K})-\dim(\widehat{\mathcal{C}})}$ смежными классами из $\mathbb{F}_q^n/\mathcal{C}$.

Теорема 1. Пусть $\mathcal{T}$ — множество наблюдаемых рёбер, $|\mathcal{T}| = \mu$, H_1 — соответствующая множеству $\mathcal{T}$ матрица линейных преобразований вида (2.1), $\mathcal{K}$ — линейный код с проверочной матрицей H_1, $\mathcal{C}$ — базовый код факторного кода $(\mathbb{F}^n/\mathcal{C})$. Тогда

$$\Delta_{\mathcal{T}} = \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}}) = \dim(\mathcal{K}) - \dim(\mathcal{K} \cap \mathcal{C}). \tag{7}$$

Доказательство. Воспользуемся определением энтропии:

$$\mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}}) = \sum_{\mathbf{y}\in\mathbb{F}^\mu} p(\mathbf{y}) H(\mathbf{S}|\mathbf{y}) = -\sum_{\mathbf{y}\in\mathbb{F}^\mu} \sum_{\mathbf{s}\in\mathbb{F}^k} p(\mathbf{y}) p(\mathbf{s}|\mathbf{y}) \log p(\mathbf{s}|\mathbf{y}),$$

$$\mathrm{H}(\mathbf{S}|\mathbf{y}) = \sum_{\mathbf{s}\in\mathbb{F}^k} p(\mathbf{s}|\mathbf{y}) I(\mathbf{s}|\mathbf{y}) = -\sum_{\mathbf{s}\in\mathbb{F}^k} p(\mathbf{s}|\mathbf{y}) \log p(\mathbf{s}|\mathbf{y}).$$

Пусть $\mathbf{y}$ — конкретный вектор наблюдаемых значений, а $\mathbf{s}$ — конкретный информационный вектор. Представим $p(\mathbf{s}|\mathbf{y})$ в виде

$$p(\mathbf{s}|\mathbf{y}) = \frac{p(\mathbf{s},\mathbf{y})}{p(\mathbf{y})} = \frac{p(\mathbf{y}|\mathbf{s})p(\mathbf{s})}{p(\mathbf{y})}.$$

Так как все информационные блоки появляются с одинаковой вероятностью, $p(\mathbf{s}) = 1/q^k$. Найдём $p(\mathbf{y}|\mathbf{s})$:

$$p(\mathbf{y}|\mathbf{s}) = \sum_{\mathbf{x}\in C_\mathbf{s}} p(\mathbf{x}|\mathbf{s})p(\mathbf{y}|\mathbf{x}) = \frac{1}{q^{(n-k)}} \sum_{\mathbf{x}\in C_\mathbf{s}\cap K_\mathbf{y}} p(\mathbf{y}|\mathbf{x}) = \frac{|C_\mathbf{s}\cap K_\mathbf{y}|}{q^{(n-k)}},$$

где $K_\mathbf{y}$ — смежный класс из $\mathbb{F}^n/\mathcal{K}$, соответствующий синдрому $\mathbf{y}$. Так как $\operatorname{rank}(H_1) = r$ и $\mathbf{y} = \mathbf{x}H_1$, легко проверить, что $p(\mathbf{y}) = 1/q^r$. В итоге получим

$$\mathrm{H}(\mathbf{S}|\mathbf{y}) = -\sum_{\mathbf{s}\in S} p(\mathbf{s}|\mathbf{y}) \log p(\mathbf{s}|\mathbf{y}) = -\sum_{s\in S} q^{r-n}|C_\mathbf{s}\cap K_\mathbf{y}| \log_q(q^{r-n}|C_\mathbf{s}\cap K_\mathbf{y}|).$$

По лемме 1 $|C(\mathbf{s})\cap K(\mathbf{y})| = |\mathcal{C}\cap\mathcal{K}| = q^{\dim(\mathcal{C}\cap\mathcal{K})}$, поэтому

$$\begin{aligned}\mathrm{H}(\mathbf{S}|\mathbf{y}) &= -\sum_{\mathbf{s}\in\mathbb{F}^k} q^{r-n}q^{\dim(\mathcal{C}\cap\mathcal{K})}((r-n)+\dim(\mathcal{C}\cap\mathcal{K})) = \\ &= -\sum_{\mathbf{s}\in\mathbb{F}^k} q^{r-n+\dim(\mathcal{C}\cap\mathcal{K})}(r-n+\dim(\mathcal{C}\cap\mathcal{K})).\end{aligned}$$

По следствию 1 имеем, что для заданного вектора наблюдаемых значений $\mathbf{y}$ имеется $q^{n-r-\dim(\mathcal{C}\cap\mathcal{K})}$ кандидатов на информационный блок. Поэтому

$$\begin{aligned}\mathrm{H}(\mathbf{S}|\mathbf{y}) &= -q^{r-n+\dim(\mathcal{C}\cap\mathcal{K})}q^{n-r-\dim(\mathcal{C}\cap\mathcal{K})}(r-n+\dim(\mathcal{C}\cap\mathcal{K})) = \\ &= n-r-\dim(\mathcal{C}\cap\mathcal{K}) = \dim(\mathcal{K})-\dim(\mathcal{K}\cap\mathcal{C}).\end{aligned}$$

Так как $\mathrm{H}(\mathbf{S}|\mathbf{y})$ не зависит от $\mathbf{y}$, то $\mathrm{H}(\mathbf{S}|\mathbf{Y}_\mathcal{T}) = \dim(\mathcal{K}) - \dim(\mathcal{K}\cap\mathcal{C})$. ■

Полученный в теореме 1 результат можно обобщить на случай, когда множество $\mathcal{T}$ неизвестно, а известно только то, что наблюдатель может выбирать произвольное множество мощности μ. В этом случае, с точки зрения защиты, необходимо знать гарантированный уровень неопределённости при заданном μ. Пусть $\mathcal{H}(\mu)$ — множество всех $(n\times\mu)$-матриц линейных преобразований, которые можно построить по μ ребрам сети; $\mathcal{K}(\mu)$ — множество всех линейных кодов, для каждого из которых найдется проверочная матрица из $\mathcal{H}(\mu)$. Тогда из (6) получим

$$\Delta(\mu) = \min_{K\in\mathcal{K}(\mu)}\{\dim(K) - \dim(K\cap\mathcal{C})\}.$$

2.2. Случай $l > 1$

Далее для удобства набор кодовых векторов $\mathbf{x}(1),\ldots,\mathbf{x}(l)\in\mathbb{F}_q^n$, соответствующий одному информационному блоку $\mathbf{s}\in\mathbb{F}_q^k$, назовём однородной выборкой объёма l.

Теорема 2. Пусть наблюдателю доступна однородная выборка объёма l, $\mathcal{T}_i$ — подмножество подслушиваемых рёбер в момент времени i, $|\mathcal{T}_i| = \mu_i$, H_i — соответствующая множеству $\mathcal{T}_i$ матрица линейных преобразований:

$$H_i = \left[\widetilde{\mathbf{f}}_{e_{i,1}},\ldots,\widetilde{\mathbf{f}}_{e_{i,\mu_i}}\right].$$

Здесь $e_{i,j} \in \mathcal{T}_i$, $j \in \{1, \ldots, \mu_i\}$; $\widetilde{\mathbf{f}}_{e_{i,j}}$ — глобальное кодирующее отображение для ребра $e_{i,j} \in \mathcal{T}_i$, $i \in \{1, \ldots, l\}$; $\mathcal{C}$ — базовый код факторного кода $\mathbb{F}^n/\mathcal{C}$. Тогда

$$\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l} = k + \dim(\mathcal{L}(M_1) \cap \mathcal{L}(M_2)) - \sum_{i=1}^{l} \dim(\mathcal{C}^\perp \cap \mathcal{L}(H_i^{\mathrm{T}})), \tag{8}$$

где

$$M_1 = \begin{pmatrix} H_1^{\mathrm{T}} & 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & H_l^{\mathrm{T}} \end{pmatrix}; \quad M_2 = \begin{pmatrix} H & -H & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ H & 0 & 0 & \ldots & 0 & -H \end{pmatrix};$$

$\mathcal{L}(A)$ — линейная оболочка, натянутая на строки матрицы A.

Доказательство. После l-го подслушивания наблюдателю доступны векторы $\mathbf{y}(i)$ следующего вида:

$$\mathbf{y}(i) = \mathcal{F}_{\mathcal{T}_i}(\mathbf{x}(i)) = \mathbf{x}(i)H_i, \quad i = 1, \ldots, l. \tag{9}$$

Из формулы (5) получим

$$\begin{gathered} \Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l} = \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) = \mathrm{H}(\mathbf{S}|\mathbf{X}_1, \ldots, \mathbf{X}_l, \mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) + \\ + \mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l|\mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) - \mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l|\mathbf{S}, \mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) = \\ = \mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l|\mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) - \mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l|\mathbf{S}, \mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)). \end{gathered}$$

Вычислим каждое из слагаемых в последнем равенстве. Пусть $(\mathbf{x}(1), \ldots, \mathbf{x}(l))$ — какая-то реализация для набора случайных векторов $\mathbf{X}_1, \ldots, \mathbf{X}_l$. По условию теоремы векторы $\mathbf{x}(1)$, …, $\mathbf{x}(l)$ соответствуют одному информационному блоку, т. е. принадлежат одному смежному классу. Поэтому выполняются следующие равенства:

$$H\left[\mathbf{x}^{\mathrm{T}}(1) - \mathbf{x}^{\mathrm{T}}(i)\right] = 0, \quad i \in \{2, \ldots, l\}. \tag{10}$$

Перепишем равенства (9) и (10) вместе в матричном виде:

$$M\left[\mathbf{x}(1), \ldots, \mathbf{x}(l)\right]^{\mathrm{T}} = [\mathbf{y}(1), \ldots, \mathbf{y}(l), \underbrace{0, \ldots, 0}_{l-1}]^{\mathrm{T}}, \tag{11}$$

где $M = \begin{pmatrix} M_1 \\ \hline M_2 \end{pmatrix}$. Мощность множества решений системы (11) равна $q^{ln-\mathrm{rank}(M)}$. Таким образом, $\mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l|\mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) = ln - \mathrm{rank}(M)$, где

$$\mathrm{rank}(M) = \sum_{i=1}^{l} \mathrm{rank}(H_i^{\mathrm{T}}) + (l-1)\,\mathrm{rank}(H) - \dim(\mathcal{L}(M_1) \cap \mathcal{L}(M_2)).$$

Вычислим $\mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l|\mathbf{S}, \mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l))$. Так как при фиксированном $\mathbf{s}$ случайные векторы $\mathbf{X}_i$ и $\mathbf{Y}_j$, $i \neq j$, независимы, получим

$$\mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l|\mathbf{S}, \mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) = \sum_{i=1}^{l} \mathrm{H}(\mathbf{X}_i|\mathbf{S}, \mathbf{Y}_{\mathcal{T}_i}(i)). \tag{12}$$

Отметим, что для $i \in \{1, \ldots, l\}$

$$\mathrm{H}(\mathbf{X}_i|\mathbf{S}, \mathbf{Y}_{\mathcal{T}_i}(i)) = \mathrm{H}(\mathbf{X}_i|\mathbf{Y}_{\mathcal{T}_i}(i)) - \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}_i}(i)) =$$

$$= \dim(\mathcal{L}^\perp(H_i^{\mathrm{T}})) - (\dim(\mathcal{L}^\perp(H_i^{\mathrm{T}})) - \dim(\mathcal{L}^\perp(H_i^{\mathrm{T}}) \cap \mathcal{C})) = \dim(\mathcal{L}^\perp(H_i^{\mathrm{T}}) \cap \mathcal{C}) = n - \mathrm{rank}\begin{pmatrix} H \\ \hline H_i^{\mathrm{T}} \end{pmatrix}.$$

Следовательно, принимая во внимание (12), получаем

$$\mathrm{H}(\mathbf{X}_1,\dots,\mathbf{X}_l|\mathbf{S},\mathbf{Y}_{\mathcal{T}_1}(1),\dots,\mathbf{Y}_{\mathcal{T}_l}(l)) = \sum_{i=1}^{l}\left(n-\operatorname{rank}\begin{pmatrix}H\\H_i^{\mathrm{T}}\end{pmatrix}\right) =$$
$$= ln - l\cdot\operatorname{rank}(H) - \sum_{i=1}^{l}\left[\operatorname{rank}(H_i^{\mathrm{T}}) - \dim(\mathcal{C}^{\perp}\cap\mathcal{L}_{H_i^{\mathrm{T}}})\right].$$

Собирая полученные выражения, запишем

$$\mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}_1}(1),\dots,\mathbf{Y}_{\mathcal{T}_l}(l)) = \operatorname{rank}(H) + \dim(\mathcal{L}(M_1)\cap\mathcal{L}(M_2)) - \sum_{i=1}^{l}\dim(\mathcal{C}^{\perp}\cap\mathcal{L}(H_i^{\mathrm{T}})).$$

Теорема доказана. ■

Отметим, что порядок подслушивания множеств $\mathcal{T}_i$ не влияет на значение неопределённости $\Delta_{\mathcal{T}_1,\dots,\mathcal{T}_l}$. Ценным с практической точки зрения следствием представляется тот факт, что если матрицы сетевых линейных преобразований совпадают, то никакое повторное наблюдение не принесёт дополнительной информации.

Следствие 2. Если $\mathcal{L}(H_i^{\mathrm{T}}) = \mathcal{L}(H_1^{\mathrm{T}})$ для всех $i\in\{1,\dots,l\}$, то $\Delta_{\mathcal{T}_1} = \Delta_{\mathcal{T}_1,\dots,\mathcal{T}_l}$.

Доказательство. Вычислим $\Delta_{\mathcal{T}_1,\dots,\mathcal{T}_l}$:

$$\Delta_{\mathcal{T}_1,\dots,\mathcal{T}_l} = k + (l-1)\dim(\mathcal{L}(H_1^{\mathrm{T}})\cap\mathcal{L}(H)) - l\dim(\mathcal{L}(H_1^{\mathrm{T}})\cap\mathcal{L}(H)) =$$
$$= k - \dim(\mathcal{L}(H_1^{\mathrm{T}})\cap\mathcal{L}(H)).$$

С другой стороны, согласно (7),

$$\Delta_{\mathcal{T}_1} = \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})) - \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})\cap\mathcal{L}^{\perp}(H)) =$$
$$= \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})) - [\dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})) + \dim(\mathcal{L}^{\perp}(H)) - \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})\cup\mathcal{L}^{\perp}(H)) =$$
$$= \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})\cup\mathcal{L}^{\perp}(H)) - \dim(\mathcal{L}^{\perp}(H)) =$$
$$= n - \dim(\mathcal{L}(H_1^{\mathrm{T}})\cap\mathcal{L}(H)) - [n-k] = k - \dim(\mathcal{L}(H_1^{\mathrm{T}})\cap\mathcal{L}(H)) = \Delta_{\mathcal{T}_1,\dots,\mathcal{T}_l}.$$

Следствие доказано. ■

Следствие 2, в частности, может позволить подстраивать защиту информации в сети в тех ситуациях, когда наблюдатель не может по своему усмотрению выбирать множества подслушиваемых рёбер.

Из следствия 2 получаем, что если наблюдатель подслушивает рёбра из множества $\mathcal{T}$ мощности μ, то $\Delta_{\mathcal{T}} = k - \dim(\mathcal{L}(H_1^{\mathrm{T}})\cap\mathcal{L}(H))$. Если, как и раньше, $\operatorname{rank}(H_1) = \mu$, то минимальное значение величины $\Delta_{\mathcal{T}}$ равно $\Delta^{\mu,\min} = k - \min\{k,\mu\}$, а максимальное — $\Delta^{\mu,\max} = k - \max\{0,\mu-(n-k)\}$. Используя $\Delta^{\mu,\min}$ и $\Delta^{\mu,\max}$, можно получить грубую оценку $\bar{l}(\mu)$ количества перехватов в сети, после которых мера неопределённости $\Delta^{(l)}(\mu)$ будет равна нулю. Для этого воспользуемся формулой (1.23) из [11, с. 38] и получим

$$\left\lceil\left(1-\log_{|\mathbb{F}_q^k|-1}\left(q^{\Delta^{\mu,\min}}-1\right)\right)^{-1}\right\rceil \leqslant \bar{l}(\mu) - 1 \leqslant \left\lceil\left(1-\log_{|\mathbb{F}_q^k|-1}\left(q^{\Delta^{\mu,\max}}-1\right)\right)^{-1}\right\rceil. \quad (13)$$

2.3. Пример вычисления меры неопределённости

Рассмотрим сеть, изображенную на рис. 1. Пусть $(\mathbb{F}_2^8/\mathcal{C})$ — факторный код, где $\mathcal{C}$ — самодуальный код Рида — Маллера с проверочной матрицей

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Пусть в сети на вход источника S по мнимым рёбрам загружается кодовое слово $\mathbf{x} = (x_1, \ldots, x_8)$ факторного кода $(\mathbb{F}_2^8/\mathcal{C})$; в узлах C, F, I и L выполняется суммирование (в поле $\mathbb{F}_2$) приходящих по входным рёбрам битов.

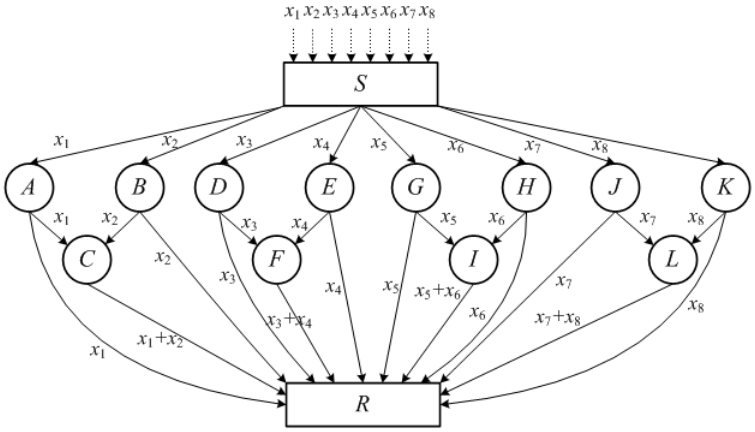

Рис. 1. Сеть с кодированием в узлах C, F, I, L

Для данной сети вычислена неопределенность $\Delta^{(l)}(\mu)$ наблюдателя для l-кратного подслушивания в зависимости от μ. Результаты вычислений, приведённые в таблице, показывают, что при $\mu = 1$ повторный перехват при любом l не позволяет снизить неопределённость меньше 4. То есть в этом случае обеспечивается совершенная защита даже при l-кратном подслушивании при любом l. В то же время при $\mu = 2$ необходимо и достаточно четырёх повторных перехватов для полного снятия неопределённости. Примером такой последовательности перехватываемых рёбер может быть последовательность $(\{CR, FR\}, \{CR, IR\}, \{CR, LR\}, \{IR, LR\})$.

Результаты вычисления $\Delta^{(l)}(\mu)$

		μ			
		1	**2**	**3**	**4**
l	**1**	4	3	1	0
	2	4	2	0	0
	3	4	1	0	0
	4	4	0	0	0

Воспользуемся оценкой (13) для этого примера. Непосредственные вычисления показывают, что при $\mu = 1$ значение величины $\bar{l}(\mu)$ лежит в границах от ∞ до ∞ (значение дроби $1/0$ здесь и далеее полагается равным ∞), что соответствует точному результату, согласно которому совершенная защита при l-кратном подслушивании обеспечивается при всех l. В то же время при $\mu = 2$ получим $3 \leqslant \bar{l}(\mu) \leqslant \infty$; из таблицы

видно, что полностью неопределённость снимается при $l = 4$. При $\mu = 3$ нижняя оценка $\overline{l}(\mu) = 2$ совпадает с точным значением l, при котором неопредёленность снимается полностью.

Отметим, что, помимо грубой оценки (13) для $\Delta^{(l)}(\mu)$, представляет интерес аналитическое уточнение формулы вычисления меры неопредёленности $\Delta(\mu_1, \ldots, \mu_l)$ для конкретных базовых и сетевых кодов, так как по полученной в работе формуле (8) эта мера может быть вычислена только алгоритмически перебором всех возможных наборов подмножеств подслушиваемых рёбер. В [12] получена формула вычисления меры стойкости кодового зашумления в случае, когда данные многократно передаются по каналу, а не по линейной сети. Там же эту формулу удалось аналитически уточнить только в частных случаях для базового кода Хэмминга и некоторых кодов Рида — Маллера. Уточнение формулы (8) представляется задачей не менее трудной, чем уточнение аналогичной формулы, полученной в [12], так как канал можно рассматривать как тривиальный случай линейной сети.

ЛИТЕРАТУРА

1. *Габидулин Э. М., Пилипчук Н. И., Колыбельников А. И. и др.*Сетевое кодирование // Труды МФТИ. 2009. Т. 1. № 2. С. 3–25.
2. *Yeung R. W. and Zhang Z.* Distributed source coding for satellite communications // IEEE Trans. Inform. Theory. 1999. V. 1. No. 45. P. 1111–1120.
3. *Ahlswede R., Cai N., Li S. R., and Yeung R. W.* Network information flow // IEEE Trans. Inform. Theory. 2000. V. 46. No. 6. P. 1204–1216.
4. *Бараш Л. С.* Сетевое кодирование // Компьютерное обозрение. 2009. Т. 5. № 671. С. 20–31.
5. *Rouayheb S. E. and Soljanin E.* On wiretap networks II // Proc. 2007 IEEE Intern. Symp. (ISIT-2007). Nice, France, 24–29 June 2007. P. 551–555.
6. *Rouayheb S. E., Soljanin E., and Sprinston A.* Secure network coding for wiretap networks of type II // IEEE Trans. Inform. Theory. 2012. V. 58. No. 3. P. 1361–1371.
7. *Ozarov H. and Wyner A. D.* Wire-Tap Channel II // BLTj. 1984. V. 63. No. 10. P. 2135–2157.
8. *Винничук И. И., Газарян Ю. О., Косолапов Ю. В.* Стойкость кодового зашумления в рамках модели многократного частичного наблюдения кодовых сообщений // Материалы XII Междунар. науч.-практич. конф. «Информационная безопасность». Таганрог: Известия ЮФУ, 2012. С. 258–263.
9. *Yeung R. W., Li S. R., Cai N., et al.* Network coding theory, foundation and trends // Communic. Inform. Theory. 2005. V. 2. No. 4. C. 241–381.
10. *Деундяк В. М., Косолапов Ю. В.* Математическая модель канала с перехватом второго типа // Изв. вузов. Северо-Кавказский регион, сер. Естественные науки. 2008. Т. 3. № 145. С. 3–8.
11. *Шанкин Г. П.* Ценность информации. Вопросы теории и приложений. М.: Филоматис, 2004. 128 с.
12. *Деундяк В. М., Косолапов Ю. В.* Об одном методе снятия неопределенности в канале с помехами в случае применения кодового зашумления // Известия ЮФУ. Технические науки. 2014. Т. 2. № 151. С. 197–208.

2014 Прикладная теория кодирования и сжатия информации № 4(26)

DOI 10.17223/20710410/26/8

УДК 519.72

О РАДИУСЕ ПОКРЫТИЯ ЛИНЕЙНЫХ КОДОВ, ПОРОЖДЁННЫХ АФФИННЫМИ ГЕОМЕТРИЯМИ НАД ПОЛЕМ ИЗ ЧЕТЫРЁХ ЭЛЕМЕНТОВ

М. Э. Коваленко

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: kovalenkomaryana@gmail.com

Рассматриваются линейные коды, порождённые аффинными геометриями над полем из четырёх элементов. Для данных кодов приводятся некоторые свойства и вычисляется точное значение радиуса покрытия равное 4.

Ключевые слова: *линейные коды, конечные аффинные геометрии, радиус покрытия, покрывающие коды.*

Введение и основные определения

Аффинная геометрия $\mathbb{EG}(n, p^s)$ представляет собой аффинное пространство $\mathbb{F}_{p^s}^n$, т. е. точки — это векторы из $\mathbb{F}_{p^s}^n$; прямые — одномерные подпространства $\mathbb{F}_{p^s}^n$ и их смежные классы (по операции сложения векторов); d-мерные плоскости — d-мерные подпространства $\mathbb{F}_{p^s}^n$ и их смежные классы. В работе используется ряд терминов, связанных с конечными геометриями, их можно найти, например, в [1].

Определение 1. *Матрицей инцидентности* аффинной геометрии называется матрица, строки и столбцы которой сопоставлены прямым и точкам аффинной геометрии соответственно, а элемент в пересечении строки b и столбца p равен 1, если точка p лежит на прямой b, и 0 иначе.

Рассмотрим строки матрицы инцидентности $\mathbb{EG}(h, 4)$ как двоичные векторы. Они порождают линейное подпространство $\mathbb{C}_h \subset \mathbb{F}_2^{4^h}$. По определению $\mathbb{C}_h$ является двоичным линейным кодом длины 4^h.

Расстоянием (*Хэмминга*) между двумя векторами из $\mathbb{F}_2^{4^h}$ называется количество координат, в которых они отличаются. Для каждого вектора пространства $\mathbb{F}_2^{4^h}$, не лежащего в $\mathbb{C}_h$, можно выбрать минимальное расстояние среди всех расстояний от него до каждого из векторов $\mathbb{C}_h$. Максимум из всех этих расстояний называется *радиусом покрытия* линейного кода. Обозначим его $r(\mathbb{C}_h)$. Для векторов $\mathbb{C}_h$ выберем минимальное расстояние между двумя различными векторами, это расстояние называется *кодовым*. Более подробно с приведёнными понятиями можно ознакомиться в [1, 2].

В работе исследуется вопрос нахождения точного значения радиуса покрытия кода $\mathbb{C}_h$, а именно доказывается, что при любой размерности кода радиус его покрытия равен 4.

Вопрос нахождения радиуса покрытия кода является одной из версий классической задачи покрытия: *даны n и r; какое наименьшее число шаров радиуса r в метрике Хэмминга можно разместить в n-мерном пространстве так, чтобы каждый вектор пространства принадлежал хотя бы одному из них.* С большей частью результатов, посвящённых покрывающим кодам, можно ознакомиться в [2].

Приведём некоторые свойства кодов $\mathbb{C}_h$, необходимые для дальнейшей работы.

Лемма 1. В коде $\mathbb{C}_h$ нет векторов нечётного веса и векторов веса 2.

Доказательство. Первая часть леммы очевидна, поскольку в силу строения порождающей матрицы базис подпространства составляют векторы веса 4. Докажем вторую часть.

Предположим, что в коде лежит вектор веса 2. Выберем соответствующую ему пару точек из $\mathbb{F}_4^h$, а у этих двух точек — координату, по которой они отличаются. Пусть это координата y_i, и у первой точки $y_{i,1} = \alpha$, а у второй $y_{i,2} = \beta$. Тогда красим гиперплоскость $\{y_i = \alpha\}$ в красный цвет, а $\{y_i = \beta\}$ — в синий. Из оставшихся двух гиперплоскостей ещё одну красим в синий и одну в красный. Итак, по фиксированной координате покрасили половину точек в красный, половину в синий цвет.

Любая прямая или целиком лежит в одной из этих плоскостей, или пересекает все четыре, а значит, содержит чётное число точек каждого цвета. Таким образом, прибавление векторов, соответствующих прямым, не изменит чётности количества точек каждого цвета, входящих в набор, то есть не существует линейной комбинации векторов, соответствующих прямым пространства $\mathbb{F}_4^h$, которая даёт выбранную пару точек, что противоречит предположению. ■

Замечание 1. Поскольку в выбранном коде лежит нулевой вектор и не лежат векторы веса 2, то кодовое расстояние данного кода равно 4.

1. Совокупность всех подмножеств $\mathbb{F}_4^h$ как векторное пространство над $\mathbb{F}_2$

Рассмотрим совокупность всех подмножеств множества $\mathbb{F}_4^h$ как векторное пространство над $\mathbb{F}_2$ с операцией симметрической разности. При этом под суммой прямых, точек и других подмножеств будем понимать сумму в смысле указанного векторного пространства. Такая операция устроена простым образом: точка из $\mathbb{F}_4^h$ принадлежит множеству, являющемуся результатом суммирования, тогда и только тогда, когда она принадлежит нечётному количеству множеств-слагаемых. В терминах такого пространства можно задавать вопросы, свойственные произвольным векторным пространствам: как выглядят порождающие системы векторов, какова размерность линейной оболочки данного набора векторов, можно ли один вектор выразить через другие (т. е. представить линейной комбинацией) и так далее. Обозначим это векторное пространство $\mathcal{A}(h)$ и $x_i(a)$ — i-ю координату элемента $a \in A \in \mathcal{A}(h)$ или, что то же самое, $a \in \mathbb{F}_4^h$. В пространстве $\mathcal{A}(h)$ выберем базис из одноточечных множеств e_j: $x_i(e_j) = \delta_{ij}$.

Пространство $\mathcal{A}(h)$ изоморфно пространству двоичных векторов размерности 4^h. Здесь и далее подразумевается, что поле $\mathbb{F}_4$ реализовано в виде фактор-алгебры $\mathbb{F}_2[x]/(x^2 + x + 1)$.

Далее выберем в $\mathcal{A}(h)$ все подмножества с чётным числом элементов, такие, что покоординатная сумма всех элементов каждого подмножества равна 0: $\mathcal{A}_0(h) = \{A \in \in \mathcal{A}(h) : |A| \equiv 0 \pmod 2 \ \& \ \forall i \sum\limits_{a \in A} x_i(a) = 0\}$. Под суммой здесь понимается сумма над $\mathbb{F}_4$; считается, что пустое множество удовлетворяет необходимому условию.

Лемма 2. Множество $\mathcal{A}_0(h)$ является подпространством $\mathcal{A}(h)$.

Доказательство. Очевидно, что операция симметрической разности сохраняет чётность количества точек в множестве. Рассмотрим $A_1 \triangle A_2$, где $A_1, A_2 \in \mathcal{A}_0(h)$; тогда $\sum\limits_{a \in A_1 \triangle A_2} x_i(a) = \sum\limits_{a \in A_1} x_i(a) + \sum\limits_{a \in A_2} x_i(a) = 0+0 = 0$, так как $\mathcal{A}(h)$ — пространство над полем характеристики 2. Таким образом, симметрическая разность двух элементов из $\mathcal{A}_0(h)$ также является элементом из $\mathcal{A}_0(h)$. ■

Каждый из элементов $a \in \mathbb{F}_4^h$, $a = (x^1 + Xy^1, \ldots, x^h + Xy^h)$, представим в виде $a = (x^1, y^1, \ldots, x^h, y^h)$, и всего множеств $A \subseteq \mathbb{F}_4^h$ ровно $2^{|\mathbb{F}_4^h|}$. Тогда множеств, у кото-

рых $\sum\limits_{a\in A} x^1(a) = 0$, ровно половина (у второй половины сумма равна 1), т. е. $2^{|\mathbb{F}_4^h|}/2$. Далее: тех множеств, у которых одновременно $\sum\limits_{a\in A} x^1(a) = 0$ и $\sum\limits_{a\in A} y^1(a) = 0$, ровно $2^{|\mathbb{F}_4^h|}/2^2$. Все пары x^i, y^j можно рассматривать независимо друг от друга; таким образом, продолжая подобные рассуждения, получим, что $|A| = 2^{|\mathbb{F}_4^h|}/2^{2h}$, где A — любое подмножество $\mathcal{A}(h)$, у которого покоординатная сумма всех элементов равна нулю. Заметим, что подмножеств с чётным числом элементов столько же, сколько и подмножеств с нечётным числом элементов, а значит, фактически вычислено $|\mathcal{A}_0(h)|$.

Введём обозначение $\mathbb{N}^* = \mathbb{N}\setminus\{1\}$.

Лемма 3. Для любого $h \in \mathbb{N}^*$ верно $|\mathcal{A}_0(h)| = 2^{2^{2h}-2h-1}$.

Поскольку $\mathcal{A}_0(h)$ — подпространство над полем характеристики 2, то можно посчитать его размерность.

Следствие 1. Для любого $h \in \mathbb{N}^*$ верно $\dim \mathcal{A}_0(h) = 2^{2h} - 2h - 1$.

Обозначим $\mathcal{A}_0^4(h) = \{A \in \mathcal{A}(h) : |A| = 4 \ \& \ \forall i \sum\limits_{a\in A} x_i(a) = 0\}$ — множество всех подмножеств из четырёх элементов, таких, что покоординатная сумма всех элементов подмножества равна 0; $\mathbb{B}_0(h)$ — все прямые. Здесь и далее будем использовать обозначение $\mathbb{B}_0(h)$ как для совокупности подмножеств над $\mathbb{F}_2$, так и для совокупности прямых в $\mathbb{F}_4^h$. Заметим, что $\langle\mathbb{B}_0(h)\rangle$ является подпространством $\langle\mathcal{A}_0^4(h)\rangle$.

Лемма 4. Для любого $h \in \mathbb{N}^*$ выполняется $\langle\mathcal{A}_0^4(h)\rangle = \mathcal{A}_0(h)$.

Доказательство. Построим выражение любого множества $\mathcal{A}_0(h)$ через множества $\mathcal{A}_0^4(h)$, для этого рассмотрим элемент $A \in \mathcal{A}_0(h)$, $A \neq \varnothing$, $|A| \geqslant 4$, поскольку множества из двух элементов удовлетворяют условию принадлежности $\mathcal{A}_0(h)$, только если состоят из двух одинаковых точек. Выберем любые три точки $a, b, c \in A$ и рассмотрим $A' = A \triangle \{a, b, c, a+b+c\}$, где $x_i(a+b+c) = x_i(a)+x_i(b)+x_i(c)$ — сумма над $\mathbb{F}_4$. Заметим, что A выражается множествами $\mathcal{A}_0^4(h)$, если и только если выражается A' и при этом $|A'| < |A|$. Получился спуск по весу; продолжаем этот спуск к A'', A''', …, $A^{(n)}$ до тех пор, пока не получим $|A^{(n)}| \leqslant 4$. Тем самым построено выражение любого множества $\mathcal{A}_0(h)$ через множества $\mathcal{A}_0^4(h)$, поскольку $A^{(n)}$ лежит в $\mathcal{A}_0^4(h)$. ■

Таким образом, в $\mathcal{A}_0^4(h)$ можно выбрать порождающую систему из $2^{2h} - 2h - 1$ множеств.

Лемма 5. Если одна четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ порождается прямыми $\mathbb{B}_0(h)$, то все четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ порождаются прямыми $\mathbb{B}_0(h)$, где $h \in \mathbb{N}^*$.

Замечание 2. Лемму также можно сформулировать следующим образом: или все четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ порождаются прямыми $\mathbb{B}_0(h)$, или никакая четвёрка $\mathcal{A}_0^4(h) \setminus \setminus \mathbb{B}_0(h)$ не выражается через прямые $\mathbb{B}_0(h)$, где $h \in \mathbb{N}^*$.

Доказательство. Пусть какое-либо множество A из $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ выражается через прямые $\mathbb{B}_0(h)$. Рассмотрим любую четвёрку из $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ и шесть прямых, проходящих через пары точек выбранной четвёрки. В силу строения четвёрок эти прямые можно разбить на три пары параллельных прямых, которые будем называть *образующими* A.

Выберем аффинное преобразование, переводящее три точки рассматриваемой четвёрки в точки $(0, \ldots, 0)$, $(1, 0, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$. Тогда оставшаяся точка перейдёт в точку $(1, 1, 0, \ldots, 0)$ в силу того, что при аффинном преобразовании сохраняется параллельность прямых. Таким образом, выбранная четвёрка перейдет во множество $\{(0, \ldots, 0), (0, 1, 0, \ldots, 0), (1, 0, 0, \ldots, 0), (1, 1, 0, \ldots, 0)\}$. Поскольку любую четвёрку

$\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ можно эквивалентными аффинными преобразованиями перевести в четвёрку $\{(0,\dots,0),(0,1,0,\dots,0),(1,0,0,\dots,0),(1,1,0,\dots,0)\}$, то из того, что какая-либо четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ выражается через прямые $\mathbb{B}_0(h)$, следует, что любая другая четвёрка выражается через прямые $\mathbb{B}_0(h)$. ■

Далее покажем, что на расстоянии 0 до $\mathbb{B}_0(h)$ в $\mathbb{F}_4^h$ не могут лежать четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$; здесь и далее $h \in \mathbb{N}^*$. Из лемм 4 и 5 можно сделать важный вывод:

Следствие 2. В $\mathcal{A}_0(h)$ не существует базиса из прямых $\mathbb{B}_0(h)$, если и только если никакая четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не порождается прямыми $\mathbb{B}_0(h)$.

В работе [3] приводится точное значение размерности пространства $\langle \mathbb{B}_0(h) \rangle$.

Теорема 1 (о базисе $\mathbb{B}_0(h)$) [3]. В $\mathbb{B}_0(h)$ существует базис из $2^{2h} - h^2 - h - 1$ элементов, т. е. в $\mathbb{F}_4^h$

$$\dim \langle \mathbb{B}_0(h) \rangle = 2^{2h} - h^2 - h - 1.$$

Таким образом, любая достаточно большая система прямых $\mathbb{B}_0(h)$ линейно зависима в $\mathbb{F}_4^h$. Тогда по теореме о базисе $\mathbb{B}_0(h)$ и следствию 1 в $\mathcal{A}_0(h)$ не существует базиса из прямых $\mathbb{B}_0(h)$, а значит, по следствию 2 никакая четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не выражается через прямые $\mathbb{B}_0(h)$. Следовательно, множества $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не могут лежать на расстоянии 0 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$.

Более того, по лемме 1 множества $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не могут лежать и на расстоянии 2 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$. Тогда любая четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ обязана лежать на расстоянии 4 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$. Проверим, что никакие другие четвёрки не лежат на расстоянии больше 2 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$.

Введём для $\mathbb{F}_4^h$ следующие обозначения для различных множеств по четыре точки: $\mathbb{B}_1$ содержит все четырёхточечные множества, пересекающиеся с какой-нибудь прямой ровно по трём точкам; $\mathbb{S}_i$ — множество четвёрок, никакие три точки которых не лежат на одной прямой, и среди трёх пар образующих их прямых ровно в i, $i > 0$, парах есть пересечение.

Заметим, что эти множества не пересекаются, а вместе с $\mathcal{A}_0^4(h)$ они исчерпывают все четырёхточечные множества $\mathbb{F}_4^h$. Для любой четвёрки из множества $\mathbb{B}_1$ выберем прямую, пересекающуюся с ней по трём точкам, а для $\mathbb{S}_i$, $i > 0$, выберем пересекающуюся пару прямых из трёх образующих пар (хотя бы одна обязательно найдется) — линейная комбинация указанных прямых и выбранной четвёрки оставляет множество из двух точек. То есть четвёрки из множеств $\mathbb{B}_1$ или $\mathbb{S}_i$, $i > 0$, лежат на расстоянии не больше 2 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$. Таким образом, доказана следующая теорема:

Теорема 2. Для любого натурального $h \neq 1$ любое множество $F \in \mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ лежит на расстоянии 4 до $\langle \mathbb{B}_0(h) \rangle$. При этом никакие другие четвёрки не лежат на расстоянии больше 2 до $\langle \mathbb{B}_0(h) \rangle$.

Итак, показано, что для векторов из $\mathbb{F}_2^{4^h}$, соответствующих четвёркам $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, с ростом h сохраняется расстояние от них до кода.

2. Радиус покрытия $r(\mathbb{C}_h)$

Заметим, что по аффинной геометрии $\mathbb{EG}(h,4)$ можно построить систему Штейнера $S(2,4,4^h)$. *Системой Штейнера* $S(t,k,v)$ называется пара $(V,\mathcal{B})$, где V — множество из v элементов, а $\mathcal{B}$ — семейство k-элементных подмножеств V, называемых *блоками*, таких, что любое t-элементное подмножество V лежит ровно в одном блоке. С основными результатами по системам Штейнера с указанными параметрами можно ознакомиться, например, в [4].

Для кодов, порождённых матрицами инцидентности систем Штейнера $S(2,4,v)$, в [5] приводится верхняя оценка радиуса покрытия.

Теорема 3 [5]. Пусть $\mathbb{C}$ — код, порождённый матрицей инцидентности $S(2,4,v)$. Тогда $r(\mathbb{C}) \leqslant \sqrt{v}$.

Для кодов, рассматриваемых в данной работе, верхнюю оценку теоремы 3 удаётся улучшить. Для этого докажем несколько утверждений.

Лемма 6. Если в $\mathbb{F}_4^h$ множество из R точек лежит на расстоянии R от $\langle \mathbb{B}_0(h) \rangle$, то любое его S-элементное подмножество лежит на расстоянии S от $\langle \mathbb{B}_0(h) \rangle$.

Доказательство. Очевидно, что расстояние больше S ни для какого S-элементного подмножества достигаться не может. Предположим, для какого-то S-элементного подмножества можно построить линейную комбинацию прямых, такую, что на ней достигается расстояние меньше S. Тогда дополнение этого подмножества из $R-S$ элементов лежит от $\langle \mathbb{B}_0(h) \rangle$ на расстоянии не больше $R-S$. Но тогда для всего R-элементного множества есть линейная комбинация, на которой достигается расстояние меньше R. Противоречие. ■

Теорема 4. Расстояние в $\mathbb{F}_4^h$ от любого R-элементного подмножества, $R > 4$, до $\langle \mathbb{B}_0(h) \rangle$ не превосходит 4.

Доказательство. Поскольку $R > 4$, то в выбранном множестве есть как минимум пять различных точек $\{a, b, c, d_1, d_2\}$. Предположим, что расстояние от этого множества до $\langle \mathbb{B}_0(h) \rangle$ не меньше 5.

Рассмотрим два подмножества $\{a, b, c, d_1\}$ и $\{a, b, c, d_2\}$; по лемме 6 расстояние от них до $\langle \mathbb{B}_0(h) \rangle$ равно 4. Из теоремы 2 известно, что на расстоянии 4 от $\langle \mathbb{B}_0(h) \rangle$ могут лежать только четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, а значит, $a + b + c + d_1 = a + b + c + d_2 = 0$. Следовательно, $d_1 = d_2$. Противоречие. ■

Переформулируя эту теорему для кода $\mathbb{C}_h$, получим уточнение верхней оценки его радиуса покрытия.

Следствие 3. Пусть $\mathbb{C}_h$ — код, порождённый строками матрицы инцидентности $\mathbb{EG}(h,4)$. Тогда $r(\mathbb{C}_h) \leqslant 4$.

Доказательство. Предположим, что существует вектор в $\mathbb{F}_2^{4^h}$, который лежит от $\mathbb{C}_h$ на расстоянии больше 4. Поскольку 0 лежит в коде, то можно считать, что вес выбранного вектора больше или равен 5. Рассмотрим соответствующее этому вектору множество элементов $\mathbb{F}_4^h$, по предположению в нем не менее 5 элементов. По теореме 4 расстояние от этого множества до $\langle \mathbb{B}_0(h) \rangle$ не превосходит 4, поэтому существует линейная комбинация прямых, а значит, и линейная комбинация векторов в $\mathbb{F}_2^{4^h}$, лежащая на расстоянии не больше 4 до выбранного множества и соответствующего вектора. Противоречие. ■

Интерес к кодам, порождённым матрицами инцидентности систем Штейнера $S(2,4,v)$, связан с исследованием ранга и аффинного ранга носителей спектра булевых функций [5]. Открытым остаётся вопрос, выполняется ли уточнённая верхняя оценка радиуса покрытия из следствия 3 для кодов, порождённых системами Штейнера $S(2,4,v)$ с параметрами, отличными от $\mathbb{EG}(h,4)$.

Вернёмся к исследованию ранга выбранных кодов: в теореме 2 фактически показано, что на векторах $\mathbb{F}_2^{4^h}$, соответствующих четвёркам $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, достигается верхняя оценка из следствия 3. Таким образом, доказана следующая

Теорема 5 (о радиусе покрытия). Пусть $h \in \mathbb{N}^*$ и $\mathbb{C}_h$ — код, порождённый строками матрицы инцидентности $\mathbb{EG}(h, 4)$. Тогда $r(\mathbb{C}_h) = 4$.

ЛИТЕРАТУРА

1. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Cohen G., Honkala I., Litsyn S., and Lobstein A.* Covering Codes. North Holland: Elsevier, 1997.
3. *Коваленко М. Э., Урбанович Т. А.* О ранге матриц инцидентности точек и прямых конечных аффинных и проективных геометрий над полем из четырех элементов // Проблемы передачи информации. 2014. Т. 50. Вып. 1. С. 102–112.
4. *Reid C. and Rosa A.* Steiner systems $S(2, 4, v)$ — a survey // Electronic J. Combinatorics. 2010. `http://www.combinatorics.org/ojs/index.php/eljc/article/view/DS18`
5. *Таранников Ю. В.* О рангах подмножеств пространства двоичных векторов, допускающих встраивание системы Штейнера $S(2, 4, v)$ // Прикладная дискретная математика. 2014. № 1. С. 73–76.

2014 Прикладная теория кодирования и сжатия информации № 4(26)

DOI 10.17223/20710410/26/9

УДК 004.627

ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ ВНУТРИКАДРОВОГО ПРЕДСКАЗАНИЯ В H.265/HEVC[1]

Р. И. Черняк

Национальный исследовательский Томский государственный университет, Томский государственный университет систем управления и радиоэлектроники, г. Томск, Россия

E-mail: roman.chernyak@elecard.ru

Рассмотрена одна из двух основных составляющих сжатия видеоинформации в новом стандарте H.265/HEVC — внутрикадровое кодирование. Проведена серия экспериментов, результаты которых позволяют оценить практическую эффективность используемых в HEVC решений.

Ключевые слова: *сжатие видео, внутрикадровое предсказание, H.265/HEVC, кодирование режимов предсказания.*

Введение

В связи с бурным ростом телекоммуникаций в современном мире всё более актуальной становится задача компактного представления информации; особенно остро она стоит в видеоиндустрии. Согласно статистике, доля видеоконтента составила 51 % всего мобильного трафика в 2012 г. и будет увеличиваться в дальнейшем [1]. В связи с этим в апреле 2013 г. группой экспертов по видеокодированию ITU-T Video Coding Experts Group совместно с экспертной группой по движущимся изображениям Moving Picture Experts Group предложен новый стандарт сжатия видеоданных H.265/HEVC [2]. В стандарт включено множество алгоритмических улучшений, которые позволили добиться существенного увеличения степени сжатия при прежнем качестве. В работе [3] приведён подробный анализ преимуществ нового стандарта H.265 по сравнению с уже устаревшими на сегодня стандартами H.263 [4] и MPEG-4 [5] и с текущим индустриальным стандартом H.264/AVC [6].

1. Краткое описание H.265/HEVC

В рамках данного стандарта кодирование видеоданных проходит последовательно по отдельным кадрам. Каждый кадр разбивается на блоки, называемые *Coding Units* — блоками кодирования; последующее кодирование происходит поблочно. При кодировании каждого блока кодер выполняет процедуру *предсказания* этого блока. Под предсказанием понимается нахождение блока, наиболее похожего на данный. В зависимости от настроек кодер может осуществлять межкадровое (интер-) или внутрикадровое (интра-) предсказание. В первом случае происходит поиск похожего участка в соседних кадрах, во втором — используется специальная процедура построения блока в рамках текущего кадра. Наличие двух способов поиска предсказанного блока обусловлено двумя типами избыточности в видеоматериале: временной и пространственной. Для устранения временной избыточности используется механизм межкадрового предсказания,

[1]Работа выполнена в рамках комплексного проекта «Предоставление услуг мультимедийного вещания в сетях общего пользования Интернет, основанных на технологиях пиринговых сетей и адаптивной передачи потоков данных» при финансовой поддержке Министерства образования и науки Российской Федерации.

пространственной — внутрикадрового. При кодировании для каждого кадра определяется тип допустимых в нём предсказаний. Всего возможны три вида кадров: I (Intra), P (Predicted) и B (Bidirectional). Для I-кадра возможны только интрапредсказания, для P и B — как интра, так и интер. Различие между P- и B-кадрами состоит в том, что P-кадры могут быть предсказаны только от хронологически предшествующих им кадров, а B-кадры — как от предшествующих, так и от следующих за ними. Для обеспечения такой возможности входящие кадры внутри кодера переупорядочиваются.

HEVC допускает 35 различных режимов внутрикадрового предсказания, среди которых два «плоских» — 0 (INTRA_PLANAR) и 1 (INTRA_DC) и 33 угловых — 2, ..., 34 (INTRA_ANGULAR2, ..., INTRA_ANGULAR34).

2. Эксперименты

Проведена серия экспериментов на входных видеоданных различных длительностей и разрешений с тем, чтобы собрать статистические данные о частоте применения тех или иных режимов интрапредсказаний. Помимо этого, собраны статистики «попадания» режима в массив MPM (Most Probable Modes) наиболее вероятных режимов из трёх элементов MPM[0], MPM[1], MPM[2]. Эксперименты проводились на видеоданных, закодированных эталонным кодером, свободно доступном на ресурсе [7]. В качестве исходного материала использовались некоторые из видеопоследовательностей, рекомендованных экспертными группами VCEG и MPEG для тестирования утилит видеокодирования. Согласно [8], все тестовые данные разделены на классы в зависимости от их разрешений и характера представленного контента, где классам A–D соответствуют снятые на видеокамеру сцены «реальной жизни» в разрешениях от WQXGA до WQVGA, а классу E — видеоконференции с разрешением HD.

Видеоданные кодировались со следующими стандартными конфигурационными файлами: `intra_main`, `lowdelay_main`, `lowdelay_P_main`, `randomaccess_main`.

Конфигурация `intra_main` предполагает для всех кадров последовательности кодирование типа интра. Конфигурации `lowdelay_main` и `lowdelay_P_main` предполагают кодирование типа интра только для первого кадра последовательности, а остальных — в режимах P или B. Конфигурация `randomaccess_main` предполагает использование периодических последовательностей из I- и B-кадров вида $IBB\ldots BI$.

2.1. Traffic

Тестовое видео Traffic относится к классу A — материалов с наиболее высоким разрешением. Для него характерно интенсивное движение объектов на неподвижном фоне.

Для данной последовательности распределения режимов внутрикадрового предсказания меняются несущественно при разных конфигурациях кодирования. Двумя наиболее частыми режимами, вне зависимости от конфигурации, стали режимы 0 и 1, следом за ними, чередуясь, с близкими результатами идут режимы 10 и 26.

Рассматривая статистики попадания режимов интрапредсказания в массив MPM для видеопоследовательности Traffic, можно сделать следующие выводы. Во всех четырёх случаях наиболее часты ситуации «MPM[0]» и «вне MPM». При этом самый благополучный с точки зрения эффективности кодирования случай имел место на конфигурации `intra_main` — доля нулевого элемента в MPM при этом максимальна.

2.2. People On Street

Видеопоследовательность People On Street также относится к классу A и имеет разрешение 2560×1600 пикселей. Для неё, как и для последовательности Traffic, характерно интенсивное движение объектов на неподвижном фоне.

Для данной видеопоследовательности проявилась бóльшая зависимость распределения режимов в зависимости от конфигурации кодирования. Во всех случаях тремя наиболее применимыми стали режимы $0, 1$ и 26 в порядке убывания частоты. Следующие за ними режимы встречаются существенно реже, и их порядок меняется в зависимости от конфигурации.

Во всех конфигурациях наиболее частой стала ситуация «вне MPM». При этом на конфигурациях `lowdelay_main` и `lowdelay_P_main` её доля близка к половине всех случаев. Далее, с большим отставанием, идёт ситуация попадания режима в MPM[0].

2.3. Kimono

Видеопоследовательность Kimono относится к классу B и имеет разрешение FullHD (1920×1080 пикселей). Для нее характерно движение как объекта, так и видеокамеры вслед за объектом, что влечёт изменение фона. Интенсивность движения в обоих случаях умеренная. Результаты эксперимента показывают, что для данного видеоматериала характерно большое количество нулевого режима интрапредсказания во всех конфигурациях. Следом за ним неизменно идут режимы 1 и 26. Частоты остальных режимов выражены менее существенно и незначительно изменяются при изменении конфигурации.

Степень попадания режимов в нулевой элемент массива MPM для данного видео довольно высока — около 40 %; непопадание режима в MPM относительно редко — около 30 %.

2.4. Cactus

Видеопоследовательность Cactus также имеет разрешение FullHD и относится к тестовому классу B. Для неё характерно умеренное движение объектов при неподвижном фоне. Как и прежде, режимы 0, 1 и 26 наиболее применимы для всех конфигураций. Частоты появления других режимов существенно меньше и незначительно изменяются при разных конфигурациях.

Для данного видео частоты наиболее и наименее благоприятных случаев попадания режимов в MPM примерно равны — около 34 %. При изменении конфигураций они изменяются несущественно.

2.5. Basketball Drill

Данная видеопоследовательность имеет разрешение 832×480 пикселей и относится к классу C. Для неё характерно интенсивное движение на неподвижном однородном фоне с ярко выраженными угловыми текстурами.

Помимо типичных INTRA_PLANAR и INTRA_DC, для данного видео характерно большое количество режимов 18 и 19 во всех конфигурациях. Это объясняется характером материала — неподвижный фон может быть хорошо предсказан в направлениях 18 и 19. В результате доля вертикального режима 26 меньше, чем доля угловых режимов 18–20.

С точки зрения попаданий режимов в массив MPM для данного материала имеет место различие между конфигурацией `intra_main` и остальными. В первом случае доли попадания и непопадания в нулевой элемент массива MPM примерно равны. Во втором — ситуация «вне MPM» существенно более частая. Такое различие объясня-

ется тем, что в случае межкадровых предсказаний доля интрарежимов относительно невелика. Иными словами, кодер чаще принимает решение закодировать тот или иной блок, используя межкадровые, а не внутрикадровые связи. В случае недоступности соседнего блока в MPM попадут наиболее вероятные в общем случае режимы — 0, 1 и 26, которые, согласно результатам эксперимента, являются неоптимальными для данной видеопоследовательности.

2.6. Blowing Bubbles

Видеопоследовательность Blowing Bubbles относится к классу D и имеет разрешение 416×240 пикселей. Она содержит интенсивное движение объектов и умеренное движение фона; для неё характерно типичное распределение режимов внутрикадрового предсказания — режимы 0, 1 и 26 являются наиболее частыми, существенно опережая остальные.

Анализируя статистики попадания режимов в MPM, можно увидеть, что во всех конфигурациях наиболее частым сценарием является непопадание режима в MPM. Его доля близка к половине всех случаев. Следом с большим отставанием идёт сценарий попадания режима в MPM[0].

2.7. Four People

Видеопоследовательность Four People имеет размеры 1280×720, относится к классу E и представляет собой видеоконференцию с участием четырёх человек; характеризуется умеренным движением на неподвижном фоне. На всех конфигурациях тройка наиболее частых режимов выглядит одинаково — 0, 1, 26.

Несмотря на то, что статистики распределения режимов внутрикадрового предсказания на данном видео меняются несущественно при изменении конфигураций кодирования, данные о попадании режимов в массив MPM различаются. Наиболее благоприятная ситуация — попадание режима в MPM[0] — происходит наиболее часто при конфигурации `intra_main`. Её доля в этом случае составляет около 36 %, а доля ситуации «вне MPM» — 60,5 %. Наименее благоприятная ситуация достигается при конфигурации `lowdelay_P_main`. В этом случае частоты сценариев попадания режима в MPM[0] и непопадания равны соответственно 30,4 и 43 %. Такое различие объясняется особенностями алгоритма, в котором при отсутствии соседнего блока используется наиболее вероятный.

2.8. Резюме

Анализируя результаты экспериментов, можно выделить следующие общие закономерности.

Наиболее частым, независимо от характера контента и конфигурации кодирования, является режим INTRA_PLANAR. Его доля изменяется от 13,38 % на последовательности Basketball Drill при конфигурации `intra_main` до 43,19 % на последовательности Kimono при конфигурации `lowdelay_P_main`. При этом из всех разностей частот соседних режимов разность, соответствующая режиму INTRA_PLANAR, максимальна и существенно превышает все остальные.

Распределение остальных режимов меняется в зависимости от последовательности. В большинстве случаев на втором и третьем местах идут режимы INTRA_DC и INTRA_ANGULAR_26 соответственно. Как правило, режим INTRA_DC используется чаще, однако на последовательностях People On Street при конфигурации `lowdelay_P_main` и Four People при конфигурациях `intra_main` и `lowdelay_main` их частоты примерно совпадают.

Отдельно следует выделить видеопоследовательность Basketball Drill. Вследствие специфического характера контента кодер более эффективно кодирует фон, используя действительное направление его текстур. Из результатов экспериментов видно, что угловые режимы интрапредсказания 18–20 применяются намного чаще, чем в других последовательностях. Такая ситуация обусловлена тем, что режимы 18–20 наиболее точно описывают направление изменения фоновых текстур в кадрах последовательности. В бóльшей степени это выражено при конфигурации `intra_main`, поскольку в этом случае используются только внутрикадровые предсказания и, следовательно, индуцированные ими эффекты проявляются наиболее ярко. Нетипичный характер контента также изменяет распределение режимов 0 и 1: частота наиболее применимого режима INTRA_PLANAR и её отрыв от следующего режима на данной последовательности минимальны; частота режима INTRA_DC находится на третьем месте после режима INTRA_ANGULAR_18.

В целом, для усреднённых по конфигурациям типичных видеопоследовательностей в множестве наиболее применимых режимов, помимо INTRA_PLANAR и INTRA_DC, характерно наличие вертикального и горизонтального угловых режимов — INTRA_ANGULAR_26 и INTRA_ANGULAR_10. Этот факт обусловливается большим количеством вертикально и горизонтально направленных текстур в кадрах типичных видеопоследовательностей.

Рассмотрим статистики попадания режимов интрапредсказания в разные позиции массива MPM.

Из результатов экспериментов видно, что наиболее частыми ситуациями являются попадание режима в нулевой элемент массива и непопадание в массив вовсе. Распределения при этом меняются довольно существенно как между последовательностями, так и внутри одной последовательности между конфигурациями. Частота попадания режима в элемент MPM[0] варьируется от 26,6 % на видео Kimono при конфигурации `intra_main` до 48,7 % на видео Blowing Bubbles при конфигурации `randomaccess_main`. Частота непопадания режима в массив изменяется от 26,5 % на последовательности Blowing Bubbles при конфигурации `randomaccess_main` до 44,1 % на последовательности Kimono при конфигурации `lowdelay_P_main`. Попадания режимов в MPM[1] и MPM[2] происходят с близкими частотами; при этом во всех экспериментах доля попаданий режима в MPM[1] несколько выше, чем в MPM[2]. Наибольшая частота попаданий в MPM[1] составляет 21,4 % для последовательности Kimono при конфигурации `intra_main`.

Следует отметить, что во всех экспериментах массив MPM, содержащий частоты попадания режимов, оказался упорядочен по убыванию. Такая ситуация объясняется особенностями алгоритма построения MPM. Действительно, для внутрикадрового предсказания характерна высокая степень корреляции соседних блоков между собой, а, согласно алгоритму, режимы соседних блоков попадают в нулевой и первый элементы массива MPM. Второй элемент определяется, исходя из статистических данных, по остаточному принципу. Отметим также, что в случае недоступности соседних блоков MPM определяется режимами $0, 1, 26$, которые, согласно проведённым экспериментам, в общем случае являются наиболее вероятными.

Заключение

В ходе проведённого исследования собраны статистические данные о внутрикадровом предсказании в новейшем стандарте сжатия видеоданных H.265/HEVC. Полученные результаты позволяют сделать вывод о том, что используемая методика в малой

степени учитывает характер сжимаемого материала, из-за чего возможны ситуации неэффективного кодирования передаваемых данных. Ещё одним отрицательным следствием текущего подхода является большое количество ситуаций непопадания режима внутрикадрового предсказания в массив наиболее вероятных режимов. Поскольку попадание в тот или иной элемент массива непосредственно определяет затраты на передачу режима, актуальной является задача построения такой процедуры кодирования, при которой три наиболее вероятных режима чаще всего попадали бы в массив, а ситуации непопадания были бы минимальны. В HEVC это свойство часто нарушается — во всех экспериментах элементы MPM[1] и MPM[2] встречались реже, чем ситуация непопадания режима в MPM. Более гибкий подход к выбору массива наиболее вероятных режимов, возможно, учитывающий характер видеоматериала, может стать предметом дальнейшего развития данного направления видеокодирования.

Следует отметить, что полученные в рамках данного исследования статистики учитывают логику принятия решений кодером, основанную на стандарте HEVC. Иными словами, при принятии решения о кодировании очередного блока тем или иным режимом кодер принимает во внимание различную стоимость этого кодирования с учётом построенного массива наиболее вероятных режимов для данного блока. Таким образом, полученные статистики являются скорее не объективными характеристиками тестовых видеопоследовательностей, а лишь иллюстрацией используемой в настоящее время практики внутрикадрового кодирования. Представляет интерес получение объективных статистических данных, с учётом которых текущий подход может быть улучшен.

ЛИТЕРАТУРА

1. `http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html` — Cisco Visual Networking Index: Global Data Traffic Forecast Update, 2012–2017. White Paper, February, 2013.
2. ITU-T Rec. H.265 and ISO/IEC 23008-2: High efficiency video coding. ITU-T and ISO/IEC JTC 1. Version 1. 2014.
3. *Ohm J-R., Sullivan G. J., Schwarz H., et al.*Comparison of the coding efficiency of video coding standards-including high efficiency video coding (HEVC) // IEEE Trans. Circuits and Systems for Video Technology. 2012. V. 22. No 12. P. 1669–1684.
4. ITU-T Rec. H.263: Video Coding for Low Bitrate Communication. ITU-T. Version 1 — 1995, version 2 — 1998, version 3 — 2000.
5. ISO/IEC 14496-2 (MPEG-4 Visual): Coding of Audio-Visual Objects. P. 2: Visual. ISO/IEC JTC 1. Version 1 — 1999, version 2 — 2000, version 3 — 2004.
6. ITU-T Rec. H.264 and ISO/IEC 14496-10 (AVC): Advanced Video Coding for Generic Audiovisual Services. ITU-T and ISO/IEC JTC 1. Version 1 — 2003, version 2 — 2004, versions 3, 4 — 2005, versions 5, 6 — 2006, versions 7, 8 — 2007, versions 9, 10, 11 — 2009, versions 12, 13 — 2010, versions 14, 15 — 2011, version 16 — 2012.
7. `http://hevc.hhi.fraunhofer.de/` High Efficiency Video Coding (HEVC). 2014.
8. JCTVC-K1100: Common test conditions and software reference configurations // Joint Collaborative Team on Video Coding (JCT-VC) of ITU-T SG16 WP3 and ISO/IEC JTC1/SC29/WG11. 11th Meeting: Shanghai, CN, 10–19 October 2012.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

DOI 10.17223/20710410/26/10

УДК 519.7

ФУНКЦИОНИРОВАНИЕ ДИСКРЕТНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЫ ЦИРКУЛЯНТНОГО ТИПА С ПОРОГОВЫМИ ФУНКЦИЯМИ В ВЕРШИНАХ

И. С. Быков

Новосибирский государственный университет, г. Новосибирск, Россия

E-mail: patrick.no10@gmail.com

Рассматриваются дискретные динамические системы, заданные на графе-циркулянте, функционирование которых определяется пороговыми функциями. Получены общие свойства графа функционирования системы. В случае значности системы $p = 2$ проведена классификация всех состояний системы в зависимости от длин серий нулей и единиц. Как результат, получены некоторые свойства циклов функционирования и нижняя оценка количества компонент связности. Для произвольного значения p сформулирован критерий существования неподвижных точек, определены их вид и количество.

Ключевые слова: *дискретные динамические системы, граф функционирования, граф-циркулянт, пороговые функции, циклы графа функционирования, неподвижные точки.*

Введение

Динамические системы в целом и дискретные динамические системы в частности моделируют различные явления и объекты. С помощью теории динамических систем можно охарактеризовать процесс, который описывает система, тем самым спрогнозировать поведение объекта (явления) в будущем. Например, можно определить, к каким последствиям приведёт какой-либо процесс: к негативным или же, напротив, к позитивным. Одним из объектов, которые моделируют дискретные динамические системы, являются генные сети.

1. Постановка задачи

1.1. Граф функционирования

Дискретной динамической системой называется пара (Ω, A), где Ω — множество состояний системы, а A — отображение, действующее на множестве состояний:

$$A : \Omega \to \Omega.$$

Функционированием дискретной динамической системы с начальным состоянием $\omega \in \Omega$ назовём бесконечную последовательность ω, $A^1(\omega)$, $A^2(\omega)$, $A^3(\omega)$, ..., где $A^1(\omega) = A(\omega)$; $A^{i+1}(\omega) = A(A^i(\omega))$ для $i \in \mathbb{Z}_+$.

Графом функционирования (или *графом состояний*) дискретной динамической системы называют ориентированный граф $H = G(V, D)$ с петлями, где

$$V = \Omega;\ D = \{(\omega_1, \omega_2) : \omega_1, \omega_2 \in \Omega,\ A(\omega_1) = \omega_2\}.$$

Согласно [1], каждая компонента связности графа функционирования представляет собой единственный контур (возможно, петлю), к которому присоединены деревья, ориентированные к корню.

Любой контур этого графа будем называть *циклом фунционирования*. Для любого состояния ω из цикла функционирования длины r верно $A^r(\omega) = \omega$. Любую вершину с петлёй будем называть *неподвижной точкой*. Другими словами, если ω — неподвижная точка, то $A(\omega) = \omega$. Висячую вершину графа функционирования будем называть *истоком*, т. е. если ω — исток, то для любого $\omega' \in \Omega$ имеем $A(\omega') \neq \omega$.

Задача анализа функционирования дискретных динамических систем состоит в определении качественных характеристик графа функционирования по заданным множеству всех состояний Ω и отображению перехода A. К качественным характеристикам графа состояния относятся, например, следующие:

1) характеристики компонент связности (циклов функционирования);
2) характеристики неподвижных точек;
3) максимальная длина цикла графа функционирования;
4) максимальная длина цепи в графе функционирования;
5) характеристики истоков.

1.2. Динамическая система циркулянтного типа

Рассматриваются динамические системы, заданные на графе-циркулянте [2, 3].

Граф-циркулянт — ориентированный граф $G_{n,k}$ $(1 \leqslant k \leqslant n)$ с множеством вершин $V = \{0, 1, \ldots, n-1\}$ и множеством рёбер $D = \{(i,j) : i,j \in V,\ (i-j) \bmod n \leqslant k\}$.

Определим множество всех состояний Ω и отображение перехода A.

Каждой вершине i графа-циркулянта сопоставим значение x_i из множества $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. *Состоянием* назовем кортеж, составленный из значений всех вершин графа-циркулянта: $(x_0, x_1, \ldots, x_{n-1})$, т. е. $|\Omega| = p^n$. Если состояние имеет вид $(x, x, \ldots, x)$, то будем обозначать его $(\tilde{x})$.

Определим отображение A, действующее на Ω следующим образом:

$$A((x_0, x_1, \ldots, x_{n-1})) = (y_0, y_1, \ldots, y_{n-1}),$$

где y_i вычисляется по правилу

$$y_i = \begin{cases} x_i + 1, & \text{если } \sum\limits_{j=1}^{k} x_{i+j} < T \text{ и } x_i < p-1, \\ x_i - 1, & \text{если } \sum\limits_{j=1}^{k} x_{i+j} \geqslant T \text{ и } x_i > 0, \\ x_i & \text{иначе.} \end{cases} \tag{1}$$

Здесь и далее все операции в индексах выполняются по модулю n.

В этом случае также говорят, что y_i принимает значение *симметричной пороговой функции* с пороговым значением $T \in \mathbb{Z}$. Аргументами этой функции являются значения вершин, дуги из которых входят в i-ю.

Такая постановка была рассмотрена ранее [2–4] при пороговых значениях $T = 1$ и k. В этих случаях действие отображения A совпадает с действиями аддитивного и мультипликативного (при $p = 2$) автомата соответственно.

Введём отношение эквивалентности на множестве всех состояний Ω. Будем говорить, что $X \sim X'$, если X' получено из X циклическим сдвигом. Таким образом, всё множество Ω разбивается на классы эквивалентности. В силу симметричности графа-

циркулянта и пороговой функции все состояния одного класса эквивалентности обладают одинаковыми характеристиками функционирования. Поэтому без ограничения общности при рассмотрении функционирования системы можно считать, что для любого начального состояния $X = (x_0, x_1, \ldots, x_{n-1})$ имеем $x_0 \neq x_{n-1}$ (если $X \neq (\tilde{x})$).

Набор параметров дискретной динамической системы p, n, k, T полностью задаёт множество состояний Ω и отображение перехода A, а значит, и граф функционирования. Граф функционирования системы с таким набором параметров будем обозначать $H_p(n, k, T)$. На рис. 1 приведён пример такого графа.

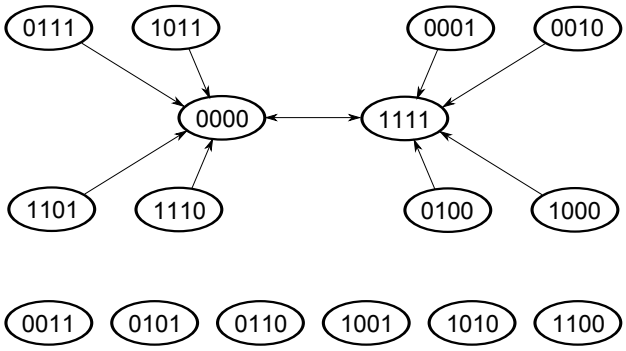

Рис. 1. Пример графа функционирования $H_2(4, 3, 2)$

В работе исследуется функционирование дискретной динамической системы $H_p(n, k, T)$. В частности, рассматриваются циклы функционирования и неподвижные точки системы.

2. Общие свойства графа функционирования

Одним из параметров систем рассматриваемого вида является пороговое значение $T \in \mathbb{Z}$. Следующая лемма характеризует граф функционирования в зависимости от значеня параметра T.

Лемма 1.

1) Если $T \leqslant 0$, то $A((x_0, \ldots, x_{n-1})) = (\max(0, x_0 - 1), \ldots, \max(0, x_{n-1} - 1))$.
2) Если $T > (p-1)k$, то $A((x_0, \ldots, x_{n-1})) = (\min(p-1, x_0+1), \ldots, \min(p-1, x_{n-1}+1))$.
3) Если $0 < T \leqslant (p-1)k$, то граф функционирования содержит цикл

$$(\lceil T/k \rceil - 1, \lceil T/k \rceil - 1, \ldots, \lceil T/k \rceil - 1) \leftrightarrow (\lceil T/k \rceil, \lceil T/k \rceil, \ldots, \lceil T/k \rceil).$$

Доказательство. Пункты 1 и 2 следуют из определения отображения A. Докажем пункт 3. Пусть $0 < T \leqslant (p-1)k$.

Положим $X = (x_0, x_1, \ldots, x_{n-1}) = (\lceil T/k \rceil - 1, \lceil T/k \rceil - 1, \ldots, \lceil T/k \rceil - 1)$. Тогда для любого $i \in \{0, \ldots, n-1\}$ верно $\sum\limits_{j=1}^{k} x_{i+j} = k(\lceil T/k \rceil - 1) = k\lceil T/k \rceil - k < T$. Значит, выполнено $y_i = x_i + 1$, т. е. $A(X) = (\lceil T/k \rceil, \lceil T/k \rceil, \ldots, \lceil T/k \rceil)$.

Аналогично, если $X = (x_0, x_1, \ldots, x_{n-1}) = (\lceil T/k \rceil, \lceil T/k \rceil, \ldots, \lceil T/k \rceil)$, то для любого $i \in \{0, \ldots, n-1\}$ верно $\sum\limits_{j=1}^{k} x_{i+j} = k\lceil T/k \rceil \geqslant T$. Значит, выполнено $y_i = x_i - 1$, откуда $A(X) = (\lceil T/k \rceil - 1, \lceil T/k \rceil - 1, \ldots, \lceil T/k \rceil - 1)$. ■

Следствие 1. Пусть $p = 2$. Тогда

1) если $T \leqslant 0$, то $A(X) = (\tilde{0})$ для любого $X \in \Omega$;

2) если $T > k$, то $A(X) = (\tilde{1})$ для любого $X \in \Omega$;
3) если $0 < T \leqslant k$, то граф функционирования содержит цикл $(\tilde{0}) \leftrightarrow (\tilde{1})$.

Лемма 2. $H_p(n,k,T) \cong H_p(n,k,(p-1)k - T + 1)$.

Доказательство. Обозначим $\hat{T} = (p-1)k - T + 1$. Введём функцию $\varphi : \Omega \to \Omega$ следующим образом: $\varphi(X) = ((p-1) - x_0,\ (p-1) - x_1, \ldots,\ (p-1) - x_{n-1})$. Докажем, что φ — изоморфизм графов $H_p(n,k,T)$ и $H_p(n,k,\hat{T})$. Очевидно, что φ — биективное отображение (так как $\varphi(\varphi(X)) = X$).

Пусть A_1, A_2 — отображения, задающие графы функционирования $H_p(n,k,T)$ и $H_p(n,k,\hat{T})$ соответственно. Обозначим $X = (x_0, x_1, \ldots, x_{n-1})$, $A_1(X) = (y_0, y_1, \ldots, y_{n-1})$, $A_2(\varphi(X)) = (\hat{y}_0, \hat{y}_1, \ldots, \hat{y}_{n-1})$. Покажем, что $\varphi(A_1(X)) = A_2(\varphi(X))$. Возможны четыре случая:

1) $y_i = 0$. Следовательно, $\sum\limits_{j=1}^{k} x_{i+j} \geqslant T \Rightarrow \sum\limits_{j=1}^{k} (p-1) - x_{i+j} \leqslant (p-1)k - T < \hat{T}$. Поскольку значение x_i равно 0 или 1, то $\hat{y}_i = p - 1$.
2) $y_i = p - 1$. Следовательно, $\sum\limits_{j=1}^{k} x_{i+j} < T \Rightarrow \sum\limits_{j=1}^{k} (p-1) - x_{i+j} > (p-1)k - T \geqslant \hat{T}$. Поскольку значение x_i равно $p-2$ или $p-1$, то $\hat{y}_i = 0$.
3) $0 < y_i < p - 1$, $x_i = y_i - 1$. Следовательно,
$$\sum_{j=1}^{k} x_{i+j} < T \Rightarrow \sum_{j=1}^{k} (p-1) - x_{i+j} > (p-1)k - T \geqslant \hat{T},$$
откуда $\hat{y}_i = p - y_i - 1$.
4) $0 < y_i < p - 1$, $x_i = y_i + 1$. Следовательно,
$$\sum_{j=1}^{k} x_{i+j} \geqslant T \Rightarrow \sum_{j=1}^{k} (p-1) - x_{i+j} \leqslant (p-1)k - T < \hat{T},$$
откуда $\hat{y}_i = p - y_i - 1$.

Заметим, что если $y_i = x_i$, то значение y_i равно $p - 1$ либо 0.

Таким образом, $\varphi(A_1(X)) = A_2(\varphi(X))$ для всех $X \in \Omega$, откуда следует, что φ — изоморфизм. ■

Следствие 2. При $p = 2$ имеем $H_2(n,k,T) \cong H_2(n,k,k - T + 1)$.

В силу лемм 1 и 2 при изучении качественных характеристик графов функционирования достаточно рассматривать пороговые значения

$$1 \leqslant T \leqslant \left\lfloor \frac{(p-1)k + 1}{2} \right\rfloor,$$

в частности, при $p = 2$

$$1 \leqslant T \leqslant \left\lfloor \frac{k+1}{2} \right\rfloor.$$

3. Циклы функционирования

Рассмотрим случай $p = 2$. При этом $|\Omega| = 2^n$, а пороговая функция задаётся следующим образом:

$$y_i = \begin{cases} 1, & \text{если } \sum\limits_{j=1}^{k} x_{i+j} < T, \\ 0, & \text{если } \sum\limits_{j=1}^{k} x_{i+j} \geqslant T. \end{cases}$$

В силу результатов предыдущего пункта считаем, что $1 \leqslant T \leqslant \lfloor (k+1)/2 \rfloor$. При рассмотрении функционирования системы будем также полагать, что для любого начального состояния $X \in \Omega \setminus \{(\tilde{0}), (\tilde{1})\}$ выполнено $x_0 = 0$, $x_{n-1} = 1$.

Серией состояния X назовём максимальную по включению последовательность компонент x_i, x_{i+1}, …, x_{i+l-1}, таких, что $x_i = x_{i+1} = \cdots = x_{i+l-1}$. Число l называется длиной серии. Количество серий состояния X будем обозначать $b(X)$.

Лемма 3. $b(A(X)) \leqslant b(X)$.

Доказательство. Пусть $A(X) = Y = (y_0, y_1, \ldots, y_{n-1})$. Покажем, что если $y_i \neq y_{i+1}$, то $x_{i+1} = y_{i+1}$. Пусть $y_i = 0$, $y_{i+1} = 1$. Тогда

$$\sum_{j=1}^{k} x_{i+j} \geqslant T; \quad \sum_{j=1}^{k} x_{(i+1)+j} = \sum_{j=2}^{k+1} x_{i+j} < T.$$

Следовательно, $x_{i+1} = 1$. Аналогично для $y_i = 1$.

Получили $x_{i+1} = y_{i+1}$. Таким образом, имеем, что если y_i и y_j — начала двух различных серий в Y, то x_i и x_j лежат в различных сериях состояния X. Следовательно, количество серий в X не меньше количества серий в Y. ■

Следствие 3. Если состояния X_1 и X_2 лежат в одном цикле функционирования, то $b(X_1) = b(X_2)$.

3.1. Состояния с длинными сериями

Состояние X из $\Omega \setminus \{(\tilde{0}), (\tilde{1})\}$ будем называть *состоянием с длинными сериями*, если длина каждой серии из нулей не меньше $k - T + 1$, а длина каждой серии из единиц не меньше T.

На множестве состояний с длинными сериями определим инъективную кодирующую функцию ψ:

$$\psi((\underbrace{0\ldots0}_{s_0}\underbrace{0\ldots0}_{k-T+1}\underbrace{1\ldots1}_{s_1}\underbrace{1\ldots1}_{T}\ldots\underbrace{0\ldots0}_{s_{b-2}}\underbrace{0\ldots0}_{k-T+1}\underbrace{1\ldots1}_{s_{b-1}}\underbrace{1\ldots1}_{T})) = (s_0, s_1, \ldots, s_{b-2}, s_{b-1}).$$

Лемма 4. Пусть состояние с длинными сериями X кодируется вектором $(s_0, s_1, \ldots, s_{b-1})$. Тогда состояние $A(X)$ (или некоторое эквивалентное ему) кодируется вектором $(s_1, s_2, \ldots, s_{b-2}, s_{b-1}, s_0)$.

Доказательство. Пусть X — состояние с длинными сериями, которое кодируется согласно условию леммы. Рассмотрим X и $A(X)$:

$$X = \ldots\underbrace{1\ldots1}_{T}\underbrace{0\ldots0}_{s_{2i}}\ \underbrace{0\ldots0}_{k-T+1}\underbrace{1\ldots1}_{s_{2i+1}}\ \underbrace{1\ldots1}_{T}\underbrace{0\ldots0}_{s_{2i+2}}\ \underbrace{0\ldots0}_{k-T+1}\underbrace{1\ldots1}_{s_{2i+3}}\underbrace{1\ldots1}_{T}\ \ldots$$

$$A(X) = \ldots\underbrace{1\ldots1}_{T}\underbrace{1\ldots1}_{s_{2i}}\ \underbrace{0\ldots0}_{k-T+1}\underbrace{0\ldots0}_{s_{2i+1}}\ \underbrace{1\ldots1}_{T}\underbrace{1\ldots1}_{s_{2i+2}}\ \underbrace{0\ldots0}_{k-T+1}\underbrace{0\ldots0}_{s_{2i+3}}\underbrace{1\ldots1}_{T}\ \ldots$$

Очевидно, что $A(X)$ — состояние с длинными сериями. Нетрудно видеть, что $A(X)$ (или некоторое эквивалентное ему) кодируется вектором $(s_1, s_2, \ldots, s_{b-2}, s_{b-1}, s_0)$. ■

Следствие 4. Любое состояние с длинными сериями лежит в цикле графа функционирования, который состоит только из состояний с длинными сериями.

Доказательство. Из леммы 4 следует, что если состояние X кодируется вектором $(s_0, s_1, \ldots, s_{b-1})$, то состояние $A^2(X)$ или некоторое эквивалентное ему кодируется вектором $(s_2, s_3, \ldots, s_{b-1}, s_0, s_1)$. Это означает, что $X \sim A^2(X)$, откуда следует, что X

лежит в цикле графа функционирования. В силу леммы 4 очевидно, что все состояния этого цикла — состояния с длинными сериями. ■

Заметим, что максимальная длина цикла, состоящего из состояний с длинными сериями, равна $2n$. Она достигается, когда X и $A(X)$ не эквивалентны и $(n, k+1) = 1$. В общем случае для циклов, состоящих из состояний с длинными сериями, длина цикла нацело делит $2n$.

Так как каждый цикл функционирования содержит состояния не более чем из двух классов эквивалентности, подсчитав количество этих классов эквивалентности для состояний с длинными сериями, можно получить оценку снизу количества циклов функционирования (а значит, и компонент связности).

Утверждение 1. Число компонент связности в графе $H_2(n, k, T)$ не меньше, чем

$$1 + \sum_{i=1}^{\lfloor n/(k+1) \rfloor} \widetilde{P}(n - (k-1)i, 2i),$$

где $\widetilde{P}(a, b)$ — число циклических разбиений a на b слагаемых.

Доказательство. Пусть X — состояние с длинными сериями, $\psi(X) = (s_0, s_1, \ldots, s_{b-1})$. Сумма компонент этого вектора равна $(n - (k-1)b/2)$.

По лемме 4 и следствию 4 каждому циклическому слову соответствует хотя бы один цикл, а значит, хотя бы одна компонента связности. Отсюда следует, что количество компонент связности, состояния цикла которых содержат b серий, не меньше

$$\tilde{P}\left(n - (k-1)b/2, b\right).$$

Для подсчёта всех компонент связности необходимо учесть различные количества серий состояния:

$$\sum_{i=1}^{\lfloor n/(k+1) \rfloor} \tilde{P}(n - (k-1)i, 2i).$$

Верхний предел суммирования равен $\lfloor n/(k+1) \rfloor$, так как минимальная сумма длин двух соседних серий равна $k+1$.

Для завершения доказательства осталось учесть тривиальный цикл $(\tilde{0}) \leftrightarrow (\tilde{1})$. ■

Наилучшие результаты эта нижняя оценка показывает при $(n, k+1) = 1$. В этом случае учитываются все циклы, состоящие из состояний с длинными сериями, так как каждый класс эквивалентности целиком попадает в один и тот же цикл.

Подсчёт числа циклических разбиений

В полученной нижней оценке числа компонент связности фигурирует число циклических разбиений. Приведём формулу для подсчёта этого числа.

Теорема 1.

$$\tilde{P}(n, k) = \frac{1}{k} \sum_{\substack{1 \leqslant d \leqslant k, \\ \frac{k}{(k,n)} \mid d}} \binom{(d,k)n/k - 1}{(d,k)n/k - (d,k)}.$$

Доказательство. Воспользуемся леммой Бернсайда

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

где X — некоторое множество; G — подгруппа симметрической группы, действующей на множестве X; X^g — множество элементов из X, которые g оставляет на месте.

Положим X — множество упорядоченных разбиений числа n на k слагаемых, $G = \{g_1, g_2, \ldots, g_n\} \leqslant S_k$ — подгруппа перестановок сдвига, где g_i — перестановка, сдвигающая на i позиций.

Лемма 5.

$$|X^{g_i}| = \begin{cases} \binom{(i,k)n/k - 1}{(i,k)n/k - (i,k)}, & \text{если } k/(i,k) \big| n, \\ 0 & \text{иначе.} \end{cases}$$

Доказательство. Для того чтобы g_i оставляла некоторое слово длины k на месте, нужно, чтобы период этого слова делил i нацело. Поэтому если $i \nmid k$, то $|X^{g_i}| = |X^{g_{(i,k)}}|$.

Если $i|k$, но $(k/i) \nmid n$, то не существует упорядоченного разбиения, которое g_i оставляет на месте: $|X^{g_i}| = 0$.

Пусть теперь $i|k$ и $(k/i)|n$. Тогда $|X^{g_i}|$ равно числу упорядоченных разбиений числа in/k на i слагаемых, то есть

$$|X^{g_i}| = \binom{in/k - 1}{in/k - i}.$$

В итоге имеем

$$|X^{g_i}| = \begin{cases} |X^{g_{(i,k)}}|, & \text{если } i \nmid k, \\ \binom{in/k - 1}{in/k - i}, & \text{если } i|k \text{ и } (k/i)|n, \\ 0 & \text{иначе.} \end{cases}$$

Заметим, что если $i|k$, то $i = (i,k)$, из чего и следует утверждение леммы. ■

Покажем, что

$$(k/(i,k)) \,\big|\, n \iff (k/(k,n)) \,\big|\, i.$$

Действительно,

$$(k/(i,k)) \,\big|\, n \iff k \,\big|\, (i,k)n \iff (k/(n,k)) \,\big|\, ((i,k)n/(n,k)).$$

Так как $k/(n,k)$ и $n/(n,k)$ взаимно просты, то $(k/(n,k)) \,\big|\, (i,k)$, что выполнено тогда и только тогда, когда $(k/(k,n)) \,\big|\, i$. Применяя лемму Бернсайда к значениям мощностей множеств X^{g_i}, получаем

$$\tilde{P}(n,k) = |X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{k} \sum_{\substack{1 \leqslant d \leqslant k, \\ \frac{k}{(k,n)} \big| d}} \binom{(d,k)n/k - 1}{(d,k)n/k - (d,k)}.$$

Теорема доказана. ■

3.2. Состояния с короткими сериями

Состояние X будем называть *состоянием с короткими сериями*, если длина каждой серии из нулей не больше $(k - T)$, а каждой серии из единиц — не больше $(T - 1)$.

Лемма 6. Пусть состояние $X = (x_0, x_1, \ldots, x_{n-1})$ лежит в цикле графа функционирования, $Y = A(X) = (y_0, y_1, \ldots, y_{n-1})$. Тогда если $x_i \neq x_{i+1}$, то $x_i = y_i$.

Доказательство. Пусть $x_i = 1$. Рассмотрим X и Y:

$$\begin{array}{lcccc} X = & \ldots\ 0\ 0 & 1\ 1\ \ldots\ 1\ 1 & 0\ 0\ \ldots\ 0\ 0 & 1\ 1\ \ldots, \\ Y = & \ldots\ y_{i_1} & \ldots\ y_i & \ldots\ y_{i_2} & \ldots \end{array}$$

Пусть $y_i \neq x_i$. Следовательно, $y_i = 0$. Очевидно, что $y_j \leqslant y_i$ для всех $i_1 < j < i_2$. Это значит, что $y_j = 0$ для всех $i_1 < j < i_2$ и в Y серий меньше, чем в X. Но X и Y лежат в одном цикле. Противоречие с леммой 3.

Аналогично для $x_i = 0$. ■

Теорема 2. Если состояние лежит в цикле графа функционирования, то оно является либо состоянием с длинными сериями, либо состоянием с короткими сериями.

Доказательство. Предположим обратное; тогда существуют две подряд идущие серии b_1 и b_2, такие, что b_1 — короткая, а b_2 — длинная. Положим $i+1$ — индекс начала серии b_1; пусть b_1 — серия из нулей, а b_2 — серия из единиц.

Рассмотрим y_i. Так как длина серии b_1 не превосходит $k - T$, а серии b_2 — не меньше T, то $\sum\limits_{j=1}^{k} x_{i+j} \geqslant T$, откуда следует, что $y_i = 0$. Это противоречит лемме 6.

Аналогично рассматривается случай, когда b_1 — серия из единиц, а b_2 — из нулей. ■

Следствие 5. Все циклы функционирования делятся на три типа:

— тривиальный цикл $(\tilde{0}) \leftrightarrow (\tilde{1})$;
— циклы, состоящие из состояний с длинными сериями;
— циклы, состоящие из состояний с короткими сериями.

3.3. Построение циклов с короткими сериями

Состояния с короткими сериями в системах с большими параметрами можно строить из подходящих систем с меньшими параметрами, используя одну из следующих двух конструкций. Обозначим вес состояния (количество ненулевых компонент) $W(X)$.

Теорема 3. Пусть имеется q систем; X_i — состояние с длинными сериями в системе с параметрами n_i, k_i, T_i и отображением A_i. Тогда если существуют такие k и T, что для любого $0 \leqslant j \leqslant q-1$ выполняются следующие условия:

$$k = k_j + \sum_{i=0}^{q-1} n_i - n_j,$$

$$T = T_j + \sum_{i=0}^{q-1} W(X_i) - W(X_j),$$

$$W(X) = W(A_j(X_j)),$$

то состояние $X = X_0 X_1 \ldots X_{q-1}$ лежит в цикле графа функционирования системы с параметрами n, k, T, где $n = \sum\limits_{i=0}^{q-1} n_i$, и является состоянием с короткими сериями.

Доказательство. Покажем, что $A(X) = A_0(X_0)A_1(X_1)\ldots A_{q-1}(X_{q-1})$. Пусть $X_i = (x_0^i, x_1^i, \ldots, x_{n_i-1}^i)$, $A(X) = (y_0, y_1, \ldots, y_{n-1})$. Рассмотрим y_i. Без ограничения общности будем полагать, что $0 \leqslant i \leqslant n_0 - 1$. Тогда

$$y_i = 0 \Longleftrightarrow \sum_{j=i+1}^{n_0-1} x_j^0 + \sum_{j=0}^{n_1-1} x_j^1 + \ldots + \sum_{j=0}^{n_{q-1}-1} x_j^{q-1} + \sum_{j=0}^{k_0-(n_0-i-1)} x_j^0 \geqslant T \Longleftrightarrow$$

$$\Longleftrightarrow \sum_{j=i+1}^{n_0-1} x_j^0 + \sum_{j=1}^{q-1} W(X_j) + \sum_{j=0}^{k_0-(n_0-i-1)} x_j^0 \geqslant T \Longleftrightarrow \sum_{j=1}^{k_0} x_{i+j}^0 \geqslant T_0.$$

Так как все переходы равносильны, то и $y_i = 1 \iff \sum\limits_{j=1}^{k_0} x^0_{i+j} < T_0$.

Получили требуемое: $A(X) = A_0(X_0)A_1(X_1)\dots A_{q-1}(X_{q-1})$.

В силу того, что $W(X_i) = W(A_i(X_i))$, очевидно, что верно и

$$A^2(X) = A^2_0(X_0)A^2_1(X_1)\dots A^2_{q-1}(X_{q-1}).$$

Значит, найдётся такое i, что $A^i(X) = X$. Отсюда следует, что X лежит в цикле графа функционирования системы с параметрами n, k, T.

Теперь покажем, что X — состояние с короткими сериями. Длина самой длинной серии из единиц не превосходит $\max(W(X_i))$. Так как $T_i > 0$, то $T > \max(W(X_i))$.

Длина самой длинной серии из нулей не превосходит $\max(n_i - W(X_i))$; $k - T = k_0 + \sum\limits_{j=1}^{q-1}(n_j - W(X_j)) - T_0$. Так как $k_i - T_i > 0$, имеем $k - T + 1 > \max(n_i - W(X_i))$.

Получили, что все серии в X короткие. ■

Теорема 4. Пусть состояние X_0 лежит в цикле графа функционирования системы с параметрами n_0, k_0, T_0 и отображением A_0. Тогда если $W(X_0) = W(A_0(X_0))$, то состояние $X = \underbrace{X_0\ X_0\ \dots\ X_0\ X_0}_{m}$ лежит в цикле графа функционирования системы с параметрами $n = mn_0$, $k = k_0 + ln_0$, $T = T_0 + lW(X_0)$ и является состоянием с короткими сериями для всех $0 < l < m$.

Доказательство. Покажем, что $A(X) = A_0(X_0)A_0(X_0)\dots A_0(X_0)$. Пусть $A(X) = (y_0, y_1, \dots, y_{mn'-1})$, $X_0 = (x_0, x_1, \dots, x_{n_0-1})$. Рассмотрим y_i. Без ограничения общности будем полагать, что $0 \leqslant i \leqslant n_0 - 1$. Тогда

$$y_i = 0 \iff \sum_{j=1}^{k} x_{i+j} = \sum_{j=1}^{k_0} x_{i+j} + lW(X_0) \geqslant T \iff \sum_{j=1}^{k'} x_{i+j} \geqslant T_0.$$

Так как все переходы равносильны, $y_i = 1 \iff \sum\limits_{j=1}^{k_0} x_{i+j} < T_0$. Получили требуемое: $A(X) = A_0(X_0)A_0(X_0)\dots A_0(X_0)$. В силу того, что $W(X_0) = W(A_0(X_0))$, очевидно, что верно и $A^2(X) = (A_0)^2(X_0)\ (A_0)^2(X_0)\ \dots\ (A_0)^2(X_0)$. Так как X_0 лежит в цикле, за конечное число шагов вернёмся в X.

То, что X — состояние с короткими сериями, доказывается аналогично предыдущей теореме. ■

4. Неподвижные точки

Вновь рассматриваем случай $p = 2$.

Частным случаем циклов функционирования являются неподвижные точки. Напомним, что X является неподвижной точкой, если $A(X) = X$. Для того чтобы $X = (x_0, x_1, \dots, x_{n-1})$ была неподвижной точкой, необходимо и достаточно:

— если $x_i = 0$, то $\sum\limits_{j=1}^{k} x_{i+j} \geqslant T$,

— если $x_i = 1$, то $\sum\limits_{j=1}^{k} x_{i+j} < T$.

Докажем критерий существования неподвижных точек в системе, а также, если они существуют, укажем их количество. Сначала докажем необходимые леммы, устанавливающие свойства неподвижных точек.

Лемма 7. Если состояние $X = (x_0, x_1, \ldots, x_{n-1})$ является неподвижной точкой системы с параметрами n, k, T, то $x_i = x_{i+k+1}$.

Доказательство. Пусть $x_i = 0$ для некоторого i. Так как X — неподвижная точка, то $\sum\limits_{j=1}^{k} x_{i+j} \geqslant T$. Так как $T > 0$, среди $1, 2, \ldots, k$ найдётся хотя бы одно j, такое, что $x_{i+j} = 1$. Выберем наименьшее такое j и обозначим его j'. Снова, в силу того, что X — неподвижная точка, верно $\sum\limits_{j=1}^{k} x_{(i+j')+j} < T$. Заметим, что в силу выбора j' выполняется $\sum\limits_{j=j'+1}^{k} x_{i+j} \geqslant T - 1$; с другой стороны, имеем

$$T > \sum_{j=1}^{k} x_{(i+j')+j} = \sum_{j=j'+1}^{k} x_{i+j} + \sum_{j=k+1}^{j'+k} x_{i+j} \Rightarrow \sum_{j=j'+1}^{k} x_{i+j} = T - 1;\ \sum_{j=k+1}^{j'+k} x_{i+j} = 0.$$

Так как $k + 1 \leqslant j' + k$, верно $x_{i+k+1} = 0 = x_i$.

Аналогично, если $x_i = 1$. ■

Следствие 6. Если состояние $X = (x_0, x_1, \ldots, x_{n-1})$ является неподвижной точкой системы с параметрами n, k, T, то $x_i = x_{i+r(k+1)}$ для любого r из $\mathbb{Z}_+$.

Лемма 8. Если состояние $X = (x_0, x_1, \ldots, x_{n-1})$ является неподвижной точкой системы с параметрами n, k, T, то $x_i = x_{i+(n,k+1)}$.

Доказательство. Пусть $k + 1 = r(n, k + 1)$ и $n = q(n, k + 1)$. Заметим, что r и q — взаимно простые числа. Докажем, что существует такое $j \geqslant 0$, что $k + 1$ делит $((n, k + 1) + jn)$ нацело. Запишем

$$\frac{(n, k + 1) + jn}{k + 1} = \frac{1 + jq}{r} = w,$$

где $w \in \mathbb{R}_+$.

По свойству взаимно простых чисел существуют $a, b \in \mathbb{Z}$, такие, что $ar + bq = 1$. Тогда $a'r + b'q = 1$ для $a' = a + qt$, $b' = b - rt$ при любом $t \in \mathbb{Z}$. В силу того, что $r \geqslant 1$ и $q \geqslant 1$, можно выбрать t так, чтобы выполнялись условия $a' > 0$, $b' < 0$. Возьмём $w = a'$ и $j = -b'$ (при таком t); получим, что $k + 1$ делит $((n, k + 1) + jn)$ нацело.

Обозначим $j' = ((n, k + 1) + jn)/(k + 1)$. Тогда $x_{i+j'(k+1)} = 0$ по следствию из леммы 7; $(i + (n, k + 1) + jn) \equiv i + (n, k + 1) \pmod{n}$. ■

Следствие 7. Если состояние $X = (x_0, x_1, \ldots, x_{n-1})$ является неподвижной точкой системы с параметрами n, k, T, то $x_i = x_{i+r(n,k+1)}$ для любого $r \in \mathbb{Z}_+$.

4.1. Критерий существования неподвижных точек

Теорема 5. Пусть система задана параметрами n, k, T. Тогда неподвижные точки в системе существуют в том и только в том случае, когда выполняется каждое из следующих трёх условий:

1) $(n, k + 1) > 1$;
2) $k + 1 - (k + 1)/(n, k + 1) \geqslant T$;
3) $(k + 1)/(n, k + 1)$ нацело делит T.

Доказательство. Необходимость. Пусть X — неподвижная точка.

1) Если $(n, k + 1) = 1$, то по лемме 8 $X = (\widetilde{0})$ или $X = (\widetilde{1})$. Противоречие, так как $(\widetilde{0})$ и $(\widetilde{1})$ не являются неподвижными точками.

2) Пусть $k+1-(k+1)/(n,k+1) < T$ и существует хотя бы одно такое i, что $x_i = 0$. Тогда по лемме 8 X имеет вид $(\dots, 0, \underbrace{\overbrace{\dots,0}^{(n,k+1)}, \overbrace{\dots,0}^{(n,k+1)}, \dots, \overbrace{\dots,0}^{(n,k+1)}}_{k+1}, \dots)$. Отсюда следует, что $\sum\limits_{j=1}^{k} x_{i+j} \leqslant k+1-(k+1)/(n,k+1) < T$, а это означает, что $x_i = 1$. Противоречие.

3) Пусть $k' = (k+1)/(n,k+1)$ не делит нацело T и существует хотя бы одно i, для которого $x_i = 0$. Тогда существуют такие t, q из $\{0,1,\dots,k'\}$, что

$$\sum_{j=i+t(n,k+1)+1}^{i+(t+1)(n,k+1)} x_{i+j} \neq \sum_{j=i+q(n,k+1)+1}^{i+(q+1)(n,k+1)} x_{i+j}.$$

Отсюда следует, что существует такое r $(1 \leqslant r < (n,k+1))$, что $x_{i_q} \neq x_{i_t}$, где $i_q = i + q(n,k+1) + r$; $i_t = i + t(n,k+1) + r$. Очевидно, что $|i_t - i_q|$ кратно $(n,k+1)$, тогда по лемме 8 имеем $x_{i_q} = x_{i_t}$. Противоречие.

Достаточность. Пусть выполнены все три условия. Построим неподвижную точку. Обозначим $T_k = T(n,k+1)/(k+1)$. Рассмотрим состояние

$$X = (\overbrace{0,\dots,0}^{(n,k+1)-T_k}, \overbrace{1,\dots,1}^{T_k}, \overbrace{0,\dots,0}^{(n,k+1)-T_k}, \dots, \overbrace{1,\dots,1}^{T_k}).$$

Легко убедиться, что X — неподвижная точка. ■

4.2. Количество неподвижных точек

Теорема 6. Пусть система задана параметрами n, k, T, которые удовлетворяют условию существования неподвижных точек. Тогда количество неподвижных точек равно $\binom{(n,k+1)}{T_k}$, где $T_k = T(n,k+1)/(k+1)$.

Доказательство. Как следует из леммы 8 и теоремы 5, неподвижная точка задаётся первыми $(n,k+1)$ компонентами, сумма которых должна быть равна T_k.

Обратно: пусть сумма первых $(n,k+1)$ компонент состояния $X = (x_0, x_1, \dots, x_{n-1})$ равна T_k, а все остальные компоненты получены повторением первых $(n,k+1)$ компонент необходимое число раз. Покажем, что X — неподвижная точка системы. В силу свойств состояния X можно провести следующие преобразования:

$$\sum_{j=1}^{k} x_{i+j} = \frac{k+1}{(n,k+1)} \sum_{j=1}^{(n,k+1)} x_{i+j} - x_{i+k+1} = \frac{k+1}{(n,k+1)} \sum_{j=1}^{(n,k+1)} x_{i+j} - x_i =$$

$$= \frac{k+1}{(n,k+1)} \sum_{j=0}^{(n,k+1)-1} x_j - x_i = T = x_i.$$

Отсюда

$$\sum_{j=1}^{k} x_{i+j} = \begin{cases} T-1, & \text{если } x_i = 1, \\ T & \text{иначе.} \end{cases}$$

Это означает, что X — неподвижная точка.

Следовательно, неподвижная точка однозначно задаётся расстановкой T_k единиц на первых $(n,k+1)$ позициях и других неподвижных точек, кроме состояний такого вида, не существует. То есть число неподвижных точек равно $\binom{(n,k+1)}{T_k}$. ■

4.3. Обобщение на случай произвольного p

Результаты о неподвижных точках в случае $p = 2$ можно обобщить на случай произвольного p. Из определения (1) следует, что если состояние X в системе с параметрами p, n, k, T является неподвижной точкой, то либо $x_i = 0$, либо $x_i = p - 1$ для любого i (в противном случае значение x_i изменится). Теперь понятно, что так как значения всех компонент в неподвижной точке делятся на $p-1$, то рассмотрение неподвижных точек при произвольном значении p эквивалентно случаю двоичной системы с параметрами $n, k, \lceil T/(p-1) \rceil$.

Теоремы о неподвижных точках можно обобщить следующим образом.

Теорема 7. Пусть система задана параметрами p, n, k, T. Тогда неподвижные точки в системе существуют в том и только в том случае, когда выполняется каждое из следующих трёх условий:

1) $(n, k+1) > 1$;
2) $k + 1 - (k+1)/(n, k+1) \geqslant \lceil T/(p-1) \rceil$;
3) $(k+1)/(n, k+1)$ нацело делит $\lceil T/(p-1) \rceil$.

Теорема 8. Пусть система задана параметрами p, n, k, T, которые удовлетворяют условию существования неподвижных точек. Тогда количество неподвижных точек равно $\binom{(n,k+1)}{T_k}$, где $T_k = \dfrac{\lceil T/(p-1) \rceil (n, k+1)}{k+1}$.

Доказательства теорем 7 и 8 аналогичны доказательствам теорем для $p = 2$.

Заключение

В ходе работы основным предметом изучения были циклы графа функционирования дискретных динамических систем заданного вида. Отдельно, как частный случай циклов функционирования, рассмотрены неподвижные точки (циклы длины 1). Для них получено полное их описание при произвольном значении p: необходимое и достаточное условие их существования, их количество и вид.

Циклы функционирования в общем случае рассматривались для систем с параметром $p = 2$. Установлено, что любой цикл функционирования либо полностью состоит из состояний с длинными сериями, либо полностью — из состояний с короткими. Для состояний с длинными сериями доказано, что любое из них лежит в цикле графа функционирования. Построены две конструкции для получения состояний с короткими сериями, лежащих в циклах, из состояний систем с меньшими значениями параметров.

В дальнейшем планируется получить полное описание всех циклов из состояний с короткими сериями и с помощью этого улучшить оценку количества компонент связности графа функционирования.

ЛИТЕРАТУРА

1. *Harary F.* The number of functional digraphs // Math. Ann. 1959. V. 139. P. 203–210.
2. *Евдокимов А. А., Лиховидова Е. О.* Дискретная модель генной сети с пороговыми функциями // Вестник ТГУ. Приложение. 2008. № 2. С. 18–21.
3. *Кутумова Е. О.* Циклы функционирования дискретной модели регуляторного контура генной сети с пороговыми функциями // Дискретный анализ и исследование операций. 2011. Т. 38. № 3. С. 65–75.
4. *Григоренко Е. Д., Евдокимов А. А., Лихошвай В. А., Лобарева И. А.* Неподвижные точки и циклы автоматных отображений, моделирующих функционирование генных сетей // Вестник Томского государственного университета. Приложение. 2005. № 14. С. 206–212.

2014 Прикладная теория графов № 4(26)

DOI 10.17223/20710410/26/11

УДК 519.178

О МЕРАХ ЦЕЛОСТНОСТИ ГРАФОВ: ОБЗОР

В. В. Быкова

Институт математики и фундаментальной информатики Сибирского федерального университета, г. Красноярск, Россия

E-mail: bykvalen@mail.ru

Дан краткий обзор по детерминированным мерам целостности графов. Приводятся известные соотношения между этими мерами и оценки, выраженные через традиционные числовые параметры графа. Меры анализируются с точки зрения сложности вычисления и положенных в их основу моделей повреждения элементов графа, учёта объёма и последствий этих повреждений. Указан ряд открытых проблем.

Ключевые слова: *графы, целостность, прочность, число рассеяния, стойкость, степень разрушения, окрестная целостность, доминирующая целостность.*

Введение

Известно, что в связном графе любые две несовпадающие вершины соединены хотя бы одной цепью. При удалении некоторого множества вершин или рёбер связность графа может быть нарушена. В зависимости от того, сколько и какие элементы удаляются, какими действиями по отношению к исходному графу сопровождаются удаления этих элементов, количественно по-разному может выглядеть результирующий граф с точки зрения числа и размера сформировавшихся компонент связности. Конечно, многое зависит и от структурных особенностей исходного графа. Для учёта и оценки всех этих факторов введено понятие целостности (или живучести) графа [23], которое является обобщением связности. Считается, что более целостным является тот граф, связность которого нарушается при удалении большего числа элементов и последствия этих удалений минимальные (например, результирующий граф имеет достаточно мощную по числу вершин компоненту связности или число компонент в результирующем графе относительно мало) [45]. Для измерения уровня целостности графа применяются количественные показатели, называемые мерами целостности.

Исследования по количественной оценке целостности графов начались в 1927 г. с введения понятий вершинной и рёберной связности и доказательств теоремы Менгера [9]. Уже предложены и изучены многие детерминированные и вероятностные меры целостности. Эти меры главным образом различаются:

— моделью повреждения графа (какие элементы исходного графа удаляются; какими действиями по отношению к исходному графу сопровождаются удаления этих элементов; что представляет собой результирующий граф);
— моделью измерения объёма повреждений, то есть числа удаляемых элементов графа (учитывать или нет, и если да, то как);
— моделью учёта последствий повреждения графа (учитывать или нет, а если да, то как, через размер наибольшей компоненты связности графа, стоимость нанесенного ущерба или полученного выигрыша и т. п.).

Все последние десятилетия и до настоящего времени проблеме исследования мер целостности графов уделяется особое внимание, поскольку она связана с вопросами анализа и синтеза отказоустойчивых сложных технических систем, включая вычислительные системы, коммуникационные и транспортные сети, трубопроводные системы [4, 26, 41]. Для таких систем отказоустойчивость, как правило, является важнейшим показателем качества функционирования [2, 4, 5, 10]. Понятие отказоустойчивости было введено А. Авиженисом [20] как свойство системы сохранять работоспособность (правильность функционирования) при наличии ошибок или отказов.

Принято выделять два уровня отказоустойчивости [2]: полная отказоустойчивость — система продолжает работать в случае отказов отдельных ее элементов без существенной потери функциональных свойств; амортизация отказов — система деградирует, то есть сохраняет работоспособность с частичной потерей функций.

Полная отказоустойчивость достигается в первую очередь введением избыточности, например, дублированием элементов системы с возможностью замены отказавшего элемента на исправный, который берет на себя соответствующие функции. Избыточность в виде аппаратных, программных, информационных и временных ресурсов является классическим подходом обеспечения отказоустойчивости, который, как правило, ведет к повышению стоимости систем [2, 4, 17]. Поэтому проектирование сложных технических систем — это, прежде всего, поиск компромисса между допустимой стоимостью и требуемой отказоустойчивостью системы. Для решения подобных задач привлекаются различные математические модели и методы оптимизации.

В задачах анализа и синтеза отказоустойчивых систем достаточно широко используются методы теории графов и комбинаторной оптимизации [2, 5, 10, 16, 38]. Техническая система представляется в виде связного графа, вершины которого соответствуют элементам системы, а рёбра — связям между элементами. Тогда отказ элемента технической системы можно интерпретировать как удаление надлежащего элемента графа, а потерю связи между элементами — как отсутствие ребра или цепи между соответствующими вершинами графа. В рамках теоретико-графового представления в работе [38] предложена модель для исследования полной отказоустойчивости. При моделировании исходной системы связным графом последний погружается в некоторый минимальный избыточный граф, который рассматривается в качестве отказоустойчивой реализации исходной системы. Минимизация избыточности — одна из основных целей при проектировании отказоустойчивых систем. В рамках этой модели получены многочисленные результаты, представленные в [1, 2, 5, 10, 11, 15, 16] и во многих других работах отечественных и зарубежных авторов. Данные результаты направлены преимущественно на синтез k-отказоустойчивых реализаций систем, где k — наибольшее число одновременных отказов элементов исходной системы.

Для исследования амортизации отказов также применяются теоретико-графовые модели и методы. Система считается полностью работоспособной, если соответствующий ей граф связный. Отказы ведут к повреждению надлежащих элементов графа. Меры целостности графа позволяют оценить частичную потерю работоспособности системы вследствие отказа её элементов или связей между ними. Данные меры применяются при решении задач анализа отказоустойчивости технических систем.

В данной работе представлен обзор по основным детерминированным мерам целостности графа. Приведены известные соотношения между этими мерами и оценки, выраженные через традиционные числовые параметры графа. Обзор выполнен по научным изданиям, представленным в списке литературы.

1. Основные понятия и обозначения

Введём понятия и обозначения теории графов, необходимые для дальнейшего изложения. Все неопределяемые ниже термины можно найти в [9]. Будем рассматривать только простые графы, то есть конечные неориентированные графы без петель и кратных рёбер.

Пусть $G = (V, E)$ — простой связный граф с множеством вершин V и множеством рёбер E, при этом $n = |V| \geqslant 1$ — порядок графа G. Напомним, что связный граф всегда состоит только из одной компоненты, в которой любые две несовпадающие вершины u и v соединены (u, v)-цепью. При $n > 1$ две вершины u и v графа $G = (V, E)$ смежны, если $\{u, v\} \in E$, и не смежны в противном случае. Ребро e инцидентно вершине u, если $e = \{u, v\} \in E$, и не инцидентно иначе. Множество всех вершин графа $G = (V, E)$, смежных с некоторой вершиной $v \in V$, образует в G окрестность вершины v, которая обозначается через $N(v)$. Под замкнутой окрестностью вершины $v \in V$ в G понимается множество $N[v] = N(v) \cup \{v\}$. Пусть $S \subseteq V$. Тогда множество вершин $N(S) = \left(\bigcup\limits_{v \in S} N(v)\right) \setminus S$ называется окрестностью, а множество $N[S] = N(S) \cup S$ — замкнутой окрестностью для S в графе G. Граф порядка n, в котором любые две вершины смежны, называется полным и обозначается через K_n. Безрёберный граф порядка n обозначается через O_n. Одновершинный граф O_1 (или K_1) считается тривиальным.

Граф $H = (V', E')$ называется подграфом графа $G = (V, E)$ при условии, что $V' \subseteq V$, $E' \subseteq E$. Если $V' = V$, то H называется остовным подграфом. Если в H множество вершин есть V', а множество рёбер совпадает с множеством всех рёбер графа G, оба конца которых принадлежат V', то H называется подграфом, порождённым множеством V', и обозначается через $G(V')$. Такой граф можно получить удалением из G всех вершин, не принадлежащих V', поэтому его обозначают также через $G - S$, где $S = V \setminus V'$.

Множество вершин $S \subseteq V$ разделяет несмежные вершины u и v графа $G = (V, E)$, если в графе $G - S$ вершины u и v принадлежат различным компонентам связности. Множество S при этом называют (u, v)-сепаратором и минимальным (u, v)-сепаратором, если в нём нет собственного подмножества, являющегося (u, v)-сепаратором. Сепаратор S минимальный, если в G существует такая пара вершин u и v, что S является минимальным (u, v)-сепаратором, то есть минимальным относительно по крайней мере двух вершин этого графа. Наименьший по мощности сепаратор графа G называется наименьшим. Аналогичным образом определяются разрез (или разделяющее множество рёбер), минимальный и наименьший разрез графа.

Необходимо отметить, что при удалении из графа $G = (V, E)$ некоторой вершины $v \in V$ всегда удаляются все рёбра, инцидентные этой вершине. Полученный в результате граф принято обозначать через $G - v$. Подобным образом определяется граф $G - e$: он получается из $G = (V, E)$ удалением ребра $e = \{u, v\} \in E$, при этом концевые вершины u и v этого ребра остаются в V. Удаление вершины или ребра, а также переход к подграфу — это операции, с помощью которых можно моделировать отказы элементов системы и получать из имеющегося исходного графа другие графы с меньшим числом элементов. Операция добавления ребра, наоборот, позволяет создавать из заданных графов более насыщенные рёбрами графы. Целью такого насыщения может быть увеличение устойчивости сетей к возможным дестабилизирующим факторам. Операция добавления ребра заключается в следующем: если вершины $u, v \in V$ графа $G = (V, E)$ не смежны, то в графе $G + e$ они смежны и соединены ребром $e = \{u, v\}$.

Далее используются следующие обозначения основных числовых параметров графа G: $k(G)$ — число компонент связности; $w(G)$ — порядок наибольшей (по числу вершин) компоненты связности; $\delta(G)$ — минимальная степень вершин; $\Delta(G)$ — максимальная степень вершин; $\alpha_0(G)$ и $\alpha_1(G)$ — число независимости и число паросочетания соответственно; $\beta_1(G)$ — число рёберного покрытия; $\chi(G)$ — хроматическое число; $\varphi(G)$ — кликовое число; $\gamma(G)$— число доминирования. Данные параметры трактуются так, как они определены в [9]. Под обозначением $\lceil x \rceil$ будем понимать наименьшее целое число, большее или равное x.

2. Вершинная и рёберная связность графа

Вершинная и рёберная связность графа — первые количественные показатели, с помощью которых начали измерять целостность графов.

Число вершинной связности $\varkappa(G)$ графа $G = (V, E)$ определяется следующим образом:

$$\varkappa(G) = \min_{S \subset V} \{|S| : k(G - S) > 1 \text{ или } G - S = O_1\}, \tag{1}$$

то есть это наименьшее число вершин, удаление которых приводит к несвязному или тривиальному графу. Другими словами, число $\varkappa(G)$ задает размер наименьшего сепаратора графа G. Исключение составляет лишь граф K_n, в котором нет сепараторов вообще, хотя $\varkappa(K_n) = n - 1$. Граф l-связен, если $\varkappa(G) \geqslant l$. Согласно теореме Менгера [9], $\varkappa(G) \geqslant l$ тогда и только тогда, когда любая пара несовпадающих вершин графа G соединена по крайней мере l вершинно-непересекающимися простыми цепями.

Аналогичным образом определяется число рёберной связности $\mu(G)$ графа $G = (V, E)$:

$$\mu(G) = \min_{S \subset E} \{|S| : k(G - S) > 1\},$$

то есть $\mu(G)$ — это наименьшее число рёбер, удаление которых из G приводит к несвязному графу. По определению число $\mu(G)$ определяет размер наименьшего разреза графа G. Граф рёберно-l-связен, если $\mu(G) \geqslant l$. Из рёберного варианта теоремы Менгера следует, что $\mu(G) \geqslant l$ тогда и только тогда, когда всякая пара несовпадающих вершин графа G связана не менее чем l рёберно-непересекающимися простыми цепями.

Значения числовых параметров $\varkappa(G)$ и $\mu(G)$ применительно к проблеме целостности графа можно интерпретировать так: это объём повреждений (число элементов или связей между элементами графа), после удаления которых граф утрачивает способность поддерживать связь между некоторыми парами вершин. Поэтому чем выше значения $\varkappa(G)$ и $\mu(G)$, тем более целостным является граф G. Следует отметить, что в данном случае никак не учитывается, сколько компонент содержит граф $G-S$ и каковы размеры этих компонент. При этом для всякого несвязного графа $\varkappa(G) = \mu(G) = 0$.

Меры связности $\varkappa(G)$ и $\mu(G)$ хорошо изучены в теории графов. В частности, установлено, что для любого графа $G = (V, E)$, $n = |V| \geqslant 1$, верны отношения [9]

$$0 \leqslant \varkappa(G) \leqslant \mu(G) \leqslant \delta(G) \leqslant n - 1. \tag{2}$$

Например, $\varkappa(K_n) = \mu(K_n) = \delta(K_n) = n - 1$ и $\varkappa(O_n) = \mu(O_n) = \delta(O_n) = 0$. Показано, что задача вычисления $\varkappa(G)$ и $\mu(G)$ для произвольного графа G сводится к задаче о максимальном потоке и минимальном разрезе и является разрешимой за полиномиальное время [12, 13]. Тем не менее вершинная и рёберная связность находят лишь ограниченное применение в анализе отказоустойчивости систем, поскольку в них учитывается лишь объём повреждений и игнорируются многие важные факторы, связан-

ные с последствиями повреждений. В настоящее время для учёта подобных факторов предложены и изучены другие числовые параметры графа.

3. Вершинная и рёберная целостность

Понятия вершинной и рёберной целостности были введены в 90-е годы XX столетия К. Багга, К. Барфутом, Р. Энтрингером и Г. Свортом [21 – 23]. На сегодняшний день это наиболее изученные меры целостности графа.

Под вершинной целостностью (*vertex integrity*) графа $G = (V, E)$ понимается числовой параметр $I(G)$, вычисляемый по формуле

$$I(G) = \min_{S \subseteq V} \{|S| + w(G - S)\}, \tag{3}$$

где $w(G-S)$ — порядок наибольшей компоненты связности графа $G-S$. Заметим, что формула (3) применима как для связного, так и для несвязного графа.

Согласно (3), вершинная целостность графа выражается через сумму двух слагаемых:

— число $|S|$ удаляемых вершин. Характеризует объём повреждений;
— порядок $w(G - S)$ самой крупной компоненты графа $G - S$, в границах которой взаимные связи между вершинами ещё возможны. Отражает, насколько сильно повреждён граф.

Считается, что всякая вышедшая из строя вершина $v \in S$ не может поддерживать связи с другими вершинами, поэтому она удаляется из графа G вместе с инцидентными ей рёбрами. В результате получается граф $G-v$. Одновременное повреждение всех вершин из $S \subseteq V$ приводит к подграфу $G - S$ графа G, который представляет собой работоспособную часть системы, состоящую из одного или более фрагментов. Величина $w(G - S)$ характеризует размер самого крупного фрагмента системы, который образовался после выхода из строя сразу всех вершин из S. Из (1) и (3) следует, что вершинная целостность $I(G)$ как мера целостности графа является обобщением $\varkappa(G)$, учитывающим не только объём повреждений, но и последствия повреждений в виде порядка самой крупной компоненты графа $G - S$. Ясно, что чем выше значение $I(G)$, тем более целостным или живучим является граф G.

Утверждение 1. Для любого графа $G = (V, E)$ справедливы высказывания:

а) если $v \in V$, то $I(G - v) \leqslant I(G)$;
б) если $e \in E$, то $I(G - e) \leqslant I(G)$;
в) если $u, v \in V$, то $I(G) \leqslant I(G + e)$, где $e = \{u, v\}$;
г) если H есть подграф графа G, то $I(H) \leqslant I(G)$.

Высказывания, сформулированные в утверждении 1, очевидным образом следуют из определения вершинной целостности и соответствующих операций над графами. Утверждение 1 свидетельствует, что удаление отдельных элементов графа может снижать его вершинную целостность. Например, $I(K_n) = n$ и $I(O_n) = 1$. Очевидно, что любой граф порядка n можно получить удалением из K_n некоторых, а возможно, и всех его рёбер. Поэтому в общем случае для вершинной целостности графа $G = (V, E)$ верны естественные границы: $1 \leqslant I(G) \leqslant n$, $n = |V| \geqslant 1$. Наибольшее значение вершинной целостности достигается на полном графе, а наименьшее — на безрёберном графе. Из утверждения 1 также следует, что вершинная целостность всякого остовного подграфа графа G не выше вершинной целостности графа G в целом.

Обозначим через $W(S) = |S| + w(G - S)$ значение целевой функции в (3) при заданном множестве S. Отсюда

$$I(G) = \min_{S \subseteq V} W(S)$$

и для любого $S \subseteq V$

$$I(G) \leqslant W(S) = |S| + w(G - S).$$

В частности, при $S = \varnothing$ всегда $I(G) \leqslant w(G - S) = w(G)$.

Множество S, для которого достигается минимум $W(S)$, то есть $I(G) = |S| + w(G - S)$, принято называть I-множеством. Для заданного графа может существовать несколько I-множеств. Наименьшее по мощности I-множество называется наименьшим. Очевидно, что для связного графа $G = (V, E)$ при $S = \varnothing$ или $S = V$ всегда $W(S) = n$. Кроме того, если S не является сепаратором графа G, то также $W(S) = n$. Значит, если связный граф G неполный, то минимум $W(S)$ может достигаться только на сепараторах этого графа G. Другими словами, в неполном связном графе G всякое I-множество является сепаратором G и, следовательно, содержит не менее $\varkappa(G)$ вершин.

Другое важное с вычислительной точки зрения свойство I-множества сформулировано в следующем утверждении, детали доказательства которого приведены в [37].

Утверждение 2. Для любого связного нетривиального графа $G = (V, E)$

$$I(G) = 1 + \min_{v \in V} I(G - v). \tag{4}$$

Для нетривиального графа, который не обязательно связен, формула (4) принимает вид

$$I(G) = \min \left\{ 1 + \min_{v \in V} I(G - v), w(G) \right\}.$$

Пусть $G_v = G - v$, $v \in V$. Систему $\{G_v : v \in V\}$ подграфов принято называть колодой графа $G = (V, E)$ [9]. Таким образом, утверждение 2 указывает рекуррентный способ вычисления вершинной целостности графа через его колоду.

Как отмечено выше, число вершинной связности $\varkappa(G)$ определяет размер наименьшего по мощности сепаратора графа G, а I-множества в неполном связном графе G обязательно являются сепараторами. Следовательно, справедливо неравенство

$$\varkappa(G) + 1 \leqslant I(G), \tag{5}$$

которое задаёт нижнюю оценку целостности графа. Оценка (5) выполняется для любого графа, так как, согласно (2), всегда $\varkappa(G) \leqslant \delta(G)$ и

$$\delta(G) + 1 \leqslant I(G). \tag{6}$$

Правильность (6) основана на следующих рассуждениях. Для всякого I-множества графа G верны отношения

$$w(G - S) \geqslant \delta(G - S) + 1 \geqslant \delta(G) - |S| + 1,$$

поэтому

$$I(G) = |S| + w(G - S) \geqslant \delta(G) + 1.$$

Примечательно, что нижние оценки (5), (6) вычисляются за полиномиальное время.

Используя (6), можно получить другие нижние оценки. В частности, всегда

$$\chi(G) \leqslant I(G). \tag{7}$$

Действительно, если $\chi(G) = r$, то в графе G существует порождённый подграф H, для которого $\delta(H) \geqslant r - 1$. По утверждению 1 имеем $I(G) \geqslant I(H) \geqslant \delta(H) + 1 \geqslant r = \chi(G)$, что подтверждает (7). Из известного неравенства $\varphi(G) \leqslant \chi(G)$ [9] следует оценка

$$\varphi(G) \leqslant I(G). \tag{8}$$

Заметим, что оценки (7), (8) трудновычисляемые, для их определения пока не найдены алгоритмы с полиномиальным временем работы [6]. Вследствие этого они не представляют большого интереса для анализа отказоустойчивости сетевых структур.

Одна из верхних оценок вершинной целостности графа выражается через число вершинного покрытия этого графа:

$$I(G) \leqslant \beta_0(G) + 1. \tag{9}$$

В самом деле, число вершинного покрытия графа определяется следующим образом:

$$\beta_0(G) = \min_{S \subseteq V} \{|S| : w(G - S) \leqslant 1\}.$$

Пусть S^* — наименьшее вершинное покрытие графа G порядка n. Это означает, что всякое ребро графа G инцидентно хотя бы одной вершине из S^* и $|S^*| = \beta_0(G)$. Удаление из G всех вершин, принадлежащих S^*, приводит к $(n - |S^*|)$-элементному множеству изолированных вершин. Отсюда $W(S^*) = \beta_0(G) + 1$. Поскольку $I(G) \leqslant W(S)$ для любого $S \subseteq V$, оценка (9) верна. Заметим, что она также трудновычисляемая [6].

Равенство в (5)–(9) достигается на полных, безрёберных и двудольных графах $K_{1,n-1}$ $(n \geqslant 3)$ типа «звезда».

В теории графов доказано, что для любого графа $G = (V, E)$ число независимости $\alpha_0(G)$ и число вершинного покрытия $\beta_0(G)$ связаны между собой отношением $\alpha_0(G) + \beta_0(G) = n$, $n = |V| \geqslant 1$. Значит, оценку (9) можно записать следующим образом:

$$I(G) \leqslant n + 1 - \alpha_0(G).$$

Это неравенство даёт возможность использовать известные полиномиально вычисляемые нижние оценки для $\alpha_0(G)$ [9]. Так, нижняя оценка для числа независимости графа

$$\frac{n}{1 + \Delta(G)} \leqslant \alpha_0(G)$$

приводит к верхней оценке вершинной целостности этого графа

$$I(G) \leqslant n + 1 - \frac{n}{1 + \Delta(G)}.$$

Параметр $I(G)$ имеет рёберный аналог, называемый рёберной целостностью и являющийся обобщением числа рёберной связности. Рёберная целостность (*edge integrity*) графа $G = (V, E)$ определяется формулой

$$I'(G) = \min_{S \subseteq E} \{|S| + w(G - S)\}, \tag{10}$$

где $w(G-S)$ — порядок наибольшей компоненты связности графа $G-S$, получаемого удалением из G множества рёбер $S \subseteq E$. Здесь также $I'(G) \leqslant w(G)$.

Множество рёбер S, для которого $I'(G) = |S| + w(G-S)$, называется I'-множеством, а наименьшее по мощности такое множество — наименьшим I'-множеством. Чем выше значение $I'(G)$, тем более целостным является граф G. Как и (3), формула (10) применима для связного и несвязного графа. Между тем, если граф G неполный и связный, то всякое I'-множество является разрезом этого графа и, следовательно, содержит не менее $\mu(G)$ рёбер.

Из определения рёберной целостности следует, что значение $I'(G)$ не возрастает при удалении отдельных элементов графа G, о чем свидетельствует

Утверждение 3. Для любых графов $G = (V, E)$ и $H = (V', E')$, $V' \subseteq V$, $E' \subseteq E$, всегда

$$I'(H) \leqslant I'(G).$$

Подобно тому, как $\varkappa(G) \leqslant \mu(G)$, вершинная целостность никогда не превышает рёберной целостности графа, так как операция удаления вершины способна сильнее повредить граф, чем операция удаления отдельного ребра: при удалении вершины удаляются все инцидентные ей ребра, и таких рёбер в графе порядка n может быть до $n-1$. Поэтому для любого графа $G = (V, E)$, $n = |V| \geqslant 1$, в общем случае верны неравенства

$$1 \leqslant I(G) \leqslant I'(G) \leqslant n. \tag{11}$$

Совпадение значений вершинной и рёберной целостности имеет место, например, для полных и безрёберных графов: $I(K_n) = I'(K_n) = n$ и $I(O_n) = I'(O_n) = 1$. Однако на графе $K_{1,n-1}$ ($n \geqslant 3$) типа «звезда» хорошо видна разница между значениями этих двух параметров. В графе $K_{1,n-1}$ центральная вершина является сепаратором, и при её удалении от данного графа остаются только $n-1$ изолированных вершин. Вследствие этого $I(K_{1,n-1}) = 2$. Для сравнения, удаление одного любого ребра из $K_{1,n-1}$ снижает порядок крупнейшей компоненты связности лишь на единицу, поэтому

$$I'(K_{1,n-1}) = n \geqslant 3. \tag{12}$$

Для полного двудольного графа $K_{p,q}$ ($p + q = n \geqslant 3$) имеем подобную ситуацию:

$$I(K_{p,q}) = \min\{p, q\} + 1, \quad I'(K_{p,q}) = p + q, \quad I(K_{p,q}) < I'(K_{p,q}).$$

С другой стороны, значения вершинной и рёберной целостности сопоставимы на простых цепях P_n ($n \geqslant 1$) [22]:

$$I(P_n) = \left\lceil 2\sqrt{(n+1)} \right\rceil - 2,$$
$$I'(P_n) = \left\lceil 2\sqrt{n} \right\rceil - 1. \tag{13}$$

Согласно (11), нижние оценки (5)–(8) для $I(G)$ являются также нижними оценками для $I'(G)$. Дополнительные нижние оценки представлены в следующем утверждении.

Утверждение 4. Для любого графа $G = (V, E)$, $n = |V| \geqslant 1$, верно неравенство

$$\Delta(G) + 1 \leqslant I'(G). \tag{14}$$

Если граф G связный, то

$$\left\lceil 2\sqrt{n} \right\rceil - 1 \leqslant I'(G). \tag{15}$$

Если граф G двусвязный, что означает $\mu(G) \geqslant 2$, то

$$\min\left\{\left\lceil 2\sqrt{n\mu} \right\rceil, n\right\} \leqslant I'(G). \tag{16}$$

Правильность оценок (14), (15) следует из утверждения 3 и равенств (12), (13): достаточно выбрать в G подграф типа «звезда» с центральной вершиной, отвечающей вершине наибольшей степени, и простую цепь максимальной длины. Пусть граф G порядка n имеет $\mu(G) \geqslant 2$, $S \subseteq E$ и k — число компонент связности графа $G - S$. Тогда при $k > 1$ справедливы очевидные неравенства $m(G - S) \geqslant n/k$, $|S| \geqslant k\mu/2$. Минимизация относительно k суммы правых частей этих неравенств даёт оценку (16). Более детальное доказательство утверждения 4 можно найти в [22].

Для узких классов графов обнаружено много других верхних и нижних оценок вершинной и рёберной целостности, а в ряде случаев получены и точные формулы их вычисления. Так, оценки для кубических графов представлены в работах [18, 55], тотальных графов — в [7, 57], графов типа «клетка» — в [19], деревьев и циклов — в [24, 46].

Доказано, что задачи вычисления вершинной и рёберной целостности графа NP-полные [30]. Распознавательные варианты этих задач формулируются следующим образом.

VERTEX INTEGRITY
Условие: заданы граф $G = (V, E)$ и целое число $1 \leqslant L \leqslant n = |V|$.
Вопрос: верно, что $I(G) \leqslant L$?

EDGE INTEGRITY
Условие: заданы граф $G = (V, E)$ и целое число $1 \leqslant L \leqslant n = |V|$.
Вопрос: верно, что $I'(G) \leqslant L$?

Установлено, что VERTEX INTEGRITY и EDGE INTEGRITY остаются NP-полными задачами для планарных графов [30], но полиномиально разрешимы на деревьях, «кактусах» [40], расщепляемых и интервальных графах, графах перестановок [43, 48, 56, 58]. Доказано также, что задача VERTEX INTEGRITY является NP-полной в классе хордальных графов [35]. Между тем для этой задачи в [36] установлена возможность нахождения решения за время $O(L^{3L}n)$, что свидетельствует о её FPT-разрешимости относительно L [3, 27, 28, 34]. Поиск новых нижних и верхних оценок для $I(G)$ и $I'(G)$, а также классов графов, на которых полиномиально разрешимы задачи VERTEX INTEGRITY и EDGE INTEGRITY, актуален по-прежнему. Это обусловлено высокой вычислительной сложностью нахождения точных значений вершинной и рёберной целостности произвольного графа.

Значительная вычислительная сложность свойственна и взвешенным версиям задач VERTEX INTEGRITY и EDGE INTEGRITY. Наиболее изученной из них является WEIGHTED VERTEX INTEGRITY. Пусть на множестве вершин графа $G = (V, E)$ задана весовая функция $w : V \to \mathbb{N}$ и вес подмножества $S \subseteq V$ определяется суммой

$$w(S) = \sum_{v \in S} w(v).$$

Обозначим вес графа $G = (V, E)$ через $w(G)$. Если граф G связен, то $w(G)$ — вес множества вершин V. Если граф G не связен, то $w(G)$ — вес самой «тяжелой» компоненты связности графа G, то есть $w(G) = w(H)$, где H — компонента связности, вес которой не меньше веса любой другой компоненты графа G. Тогда взвешенная вершинная целостность (*weighted vertex integrity*) определяется формулой

$$WI(G) = \min_{S \subseteq V} \{w(S) + w(G - S)\}.$$

Если веса всех вершин равны 1, то эта формула вырождается в определение вершинной целостности (3). Распознавательный вариант задачи нахождения взвешенной вершинной целостности формулируется следующим образом.

WEIGHTED VERTEX INTEGRITY
Условие: заданы граф $G = (V, E)$, весовая функция $w : V \to \mathbb{N}$ и целое число $1 \leqslant L \leqslant n = |V|$.
Вопрос: верно, что $WI(G) \leqslant L$?

Данная задача была впервые поставлена и исследована в работе [47]. Доказано, что она является NP-полной и остаётся NP-полной на таких классах графов, как деревья, планарные, двудольные, последовательно-параллельные, регулярные и хордальные графы. Позднее в [48] для интервальных графов предложен алгоритм с полиномиальным временем работы. Для многих других классов графов вопрос о вычислительной сложности WEIGHTED VERTEX INTEGRITY остаётся открытым.

4. Показатели, родственные мерам связности и целостности графа

Для анализа отказоустойчивости систем наряду с вершинной и рёберной целостностью часто применяются числовые параметры графа, сочетающие в себе элементы мер связности и целостности графа: прочность, число рассеяния, стойкость и степень разрушения [57].

Прочность (*toughness*) и число рассеяния (*scattering number*) учитывают число удаляемых вершин графа и количество компонент связности, получившихся после их удаления. Формально эти показатели для неполного связного графа $G = (V, E)$ определяются следующим образом:

$$\tau(G) = \min_{S \subseteq V} \left\{ \frac{|S|}{k(G-S)} : k(G-S) > 1 \right\}; \tag{17}$$

$$s(G) = \max_{S \subseteq V} \left\{ k(G-S) - |S| : k(G-S) > 1 \right\}, \tag{18}$$

и для полного графа $\tau(K_n) = \infty$. Сравнение (17), (18) с формулой (1) приводит к выводу: прочность и число рассеяния — это обобщения $\varkappa(G)$, учитывающие последствия повреждения исходного графа G через число компонент связности графа $G - S$. В отличие от $\varkappa(G)$, задачи вычисления $\tau(G)$ и $s(G)$ являются NP-трудными [25, 59]. Идея прочности графа принадлежит В. Хваталу [29]. Он использовал это понятие при исследовании гамильтоновых циклов в графах. Действительно, если граф G гамильтонов, то для любого его сепаратора S всегда $k(G-S) \leqslant |S|$ [14, 29]. Поэтому каждый гамильтонов граф G имеет прочность $\tau(G) \geqslant 1$.

Стойкость (*tenacity*) и степень разрушения (*rupture degree*) учитывают не только число удаляемых вершин графа и количество компонент связности, получившихся после их удаления, но и размер крупнейшей компоненты. Эти показатели для неполного связного графа G вычисляются по формулам

$$T(G) = \min_{S \subseteq V} \left\{ \frac{|S| + w(G-S)}{k(G-S)} : k(G-S) > 1 \right\}; \tag{19}$$

$$r(G) = \max_{S \subseteq V} \left\{ k(G-S) - |S| - w(G-S) : k(G-S) > 1 \right\}, \tag{20}$$

и для полного графа $T(K_n) = n$ и $r(G) = n - 1$. Формулы (19), (20) обобщают определения числа вершинной связности (1) и вершинной целостности (3). Доказано, что задачи вычисления стойкости и степени разрушения графа NP-трудные [42, 44].

Между приведёнными количественными показателями графа установлены следующие отношения.

Утверждение 5 [57]. Если $G = (V, E)$ является неполным связным графом порядка $n = |V|$, то справедливы неравенства

$$\tau(G) \geqslant \frac{2\varkappa(G)}{r(G) + n + 1},$$
$$I(G) \leqslant \frac{s(G) + n}{2} T(G),$$
$$T(G) \geqslant \frac{\tau(G) + 1}{n} I(G),$$
$$r(G) \leqslant \frac{n+1}{T(G)+1} - I(G),$$
$$r(G) \leqslant (n + 1 - I(G)) - \frac{2(2n - I(G))}{n + s(G)}.$$

Заметим, что верхние и нижние границы в указанных неравенствах достигаются на графе $K_{1,n-1}$ ($n \geqslant 3$), для которого

$$\varkappa(K_{1,n-1}) = 1, \qquad I(K_{1,n-1}) = 2,$$
$$\tau(K_{1,n-1}) = 1/(n-1), \qquad s(K_{1,n-1}) = n - 2,$$
$$T(K_{1,n-1}) = 2/(n-1), \qquad r(K_{1,n-1}) = n - 3.$$

В работах [22, 39, 52, 59] исследованы рёберные аналоги $\tau(G)$, $s(G)$, $T(G)$ и $r(G)$.

5. Окрестная целостность

Рассмотренные меры целостности базируются на простейшей модели повреждения графа $G = (V, E)$, которая определяется операциями удаления множества его вершин $S \subseteq V$ или рёбер $S \subseteq E$, а результирующий граф представляется графом $G - S$. Между тем возможны и другие модели повреждений. Например, можно применять операции сильного удаления вершин и рёбер графа, которые оказывают более мощное разрушающее воздействие на модельный граф, чем обычные операции удаления.

Под сильным удалением вершины $v \in V$ в графе $G = (V, E)$ принято понимать такую операцию удаления, когда вместе с вершиной v удаляются все вершины, образующие её окрестность (конечно, со всеми инцидентными им рёбрами). В результате получается граф $G \div v = G - N[v]$, где символом $\div$ обозначена операция сильного удаления элемента графа. Сильное удаление ребра $e = \{u, v\} \in E$ приводит к графу $G \div e = G - u - v$, то есть в данном случае удаляется не только само ребро, но и концевые вершины этого ребра. Такая модель разрушения применяется в анализе отказоустойчивости особых сетей связи. В подобных сетях операция сильного удаления вершины интерпретируется следующим образом: при отказе некоторого узла все примыкающие к нему узлы считаются «преданными» и поэтому становятся бесполезными для остальной части сети. Операция сильного удаления ребра означает, что при отказе канала связи между отдельными двумя узлами становятся также бесполезными сами эти узлы и инцидентные с ними каналы связи. Меры целостности, использующие такую модель разрушения, называются окрестными [8, 31, 32].

Вершинной окрестной целостностью (*vertex neighbor integrity*) графа $G = (V, E)$ называется величина

$$VNI(G) = \min_{S \subseteq V} \{|S| + w(G \div S)\},$$

где $w(G \div S)$ — порядок наибольшей компоненты связности графа $G \div S$, который получается из G сильным удалением всех вершин, входящих в $S \subseteq V$. Множество S, для которого $VNI(G) = |S| + w(G \div S)$, называется VNI-множеством, или вершинной стратегией разрушения графа G.

Рёберная окрестная целостность (*edge neighbor integrity*) графа $G = (V, E)$ определяется аналогичным образом:

$$ENI(G) = \min_{S \subseteq E}\{|S| + w(G \div S)\},$$

где $w(G \div S)$ — порядок наибольшей компоненты связности графа $G \div S$, являющегося результатом сильного удаления из G множества рёбер $S \subseteq E$. Множество S, для которого $ENI(G) = |S| + w(G \div S)$, называется ENI-множеством, или рёберной стратегией разрушения графа G.

Установлено, что задачи вычисления $VNI(G)$ и $ENI(G)$ являются NP-трудными [31, 32]. Поэтому усилия многих исследователей были направлены на получение нижних и верхних оценок. В следующем утверждении представлены наиболее значимые из них.

Утверждение 6 [32]. Для любого графа $G = (V, E)$ верны оценки

$$\begin{gathered} VNI(G) \leqslant ENI(G), \\ ENI(G) \leqslant I(G) \leqslant I'(G), \\ \lceil I(G)/2 \rceil \leqslant ENI(G), \\ ENI(G) \leqslant \beta_1(G). \end{gathered}$$

Например, для графа $K_{1,n-1}$ $(n \geqslant 3)$ справедливы равенства

$$I(K_{1,n-1}) = 2,\ I'(K_{1,n-1}) = n,\ VNI(K_{1,n-1}) = 1,\ ENI(K_{1,n-1}) = 2,\ \beta_1(K_{1,n-1}) = n - 1,$$

а для полного графа K_n $(n \geqslant 2)$

$$I(K_n) = I'(K_n) = n, \quad VNI(K_n) = 1, \quad ENI(K_n) = \lceil n/2 \rceil, \quad \beta_1(K_n) = \lceil n/2 \rceil,$$

которые отвечают оценкам утверждения 6.

6. Доминирующая целостность

Примечательно, что в формулах вычисления рассмотренных выше мер целостности множество удаляемых элементов S — произвольное подмножество вершин или рёбер графа. Однако можно потребовать, чтобы множество S удовлетворяло определённым свойствам, например являлось доминирующим. Именно такая модель повреждения графа использована в работах [49 – 51, 53, 54] по исследованию доминирующей вершинной целостности.

Напомним, что отношение доминирования определено только для вершин графа [9, 33]. Подмножество $S \subseteq V$ графа $G = (V, E)$ называется доминирующим, если для любой вершины $u \in V \setminus S$ существует вершина $v \in S$, такая, что $e = \{u, v\} \in E$. Это означает, что каждая вершина графа находится на расстоянии не более единицы от доминирующего множества. Иначе говоря, каждая вершина графа или входит в доминирующее множество, или смежна хотя бы с одной вершиной из него. Наименьшее по мощности доминирующее множество называется наименьшим. Число вершин

в наименьшем доминирующем множестве графа G определяет число доминирования, которое обозначается через $\gamma(G)$.

Применительно к техническим системам доминирование представляет собой отношение непосредственной подчинённости между элементами системы. Оно даёт возможность выделить множество элементов, которые жизненно важны и управляют другими элементами. Отказ (или удаление) доминирующего множества элементов приводит к хаосу в системе, потому что не только процесс управления будет парализован, но и связь между остальными элементами будет сведена к минимуму. Чтобы можно было учитывать эти обстоятельства, авторы работы [49] в 2009 г. ввели понятие доминирующей целостности.

Доминирующая целостность (*domination integrity*) графа $G = (V, E)$ обозначается через $DI(G)$ и определяется формулой

$$DI(G) = \min_{S \subseteq V|} \{|S| + w(G - S) : S \text{ — доминирующее множество}\},$$

где $w(G-S)$ — порядок наибольшей компоненты связности графа $G-S$. Множество S, для которого $DI(G) = |S| + w(G - S)$, называется DI-множеством. Очевидно, что

$$\gamma(G) + 1 \leqslant DI(G).$$

В частности, для безрёберного графа O_n $(n \geqslant 1)$ имеем $\gamma(O_n) = n$ и $DI(O_n) = n$; для полного графа K_n $(n \geqslant 1)$ справедливы равенства $\gamma(K_n) = 1$ и $DI(K_n) = n$, а для графа $K_{1,n-1}$ $(n \geqslant 3)$ всегда $\gamma(K_{1,n-1}) = 1$ и $DI(K_{1,n-1}) = 2$. Заметим, что операция сильного удаления доминирующего множества разрушает граф полностью, так как приводит к удалению множества вершин $N[S] = V$, вследствие чего результирующий граф становится пустым.

Научных изданий, посвящённых доминирующей целостности графов, пока немного. В работах [49 – 51] исследована доминирующая целостность путей, циклов, биномиальных и полных k-деревьев. В работах [53, 54] доминирующая целостность изучена в контексте операций расширения графа путём дублирования вершин и рёбер. Целью подобных расширений является повышение доминирующей целостности анализируемого графа.

Заключение

Для количественной оценки целостности графов уже предложены и изучены многие меры, выраженные через числовые параметры графа. Задачи вычисления известных на сегодняшний день детерминированных мер целостности и соответствующих им экстремальных множеств графа носят комбинаторный характер и являются, как правило, NP-трудными. Исследования проблемы целостности графов ведутся по следующим основным направлениям:

— совершенствование существующих и разработка новых моделей повреждения, и как следствие, создание и изучение новых мер целостности;
— введение взвешенных версий известных мер;
— анализ задач вычисления мер целостности и соответствующих им экстремальных множеств графа в рамках классической и параметрической теории сложности вычислений, выявление полиномиально разрешимых случаев для этих задач;
— установление нижних и верхних оценок мер целостности через традиционные числовые параметры графа, такие, как число вершинного покрытия, хроматическое число и другие;

— характеризация классов графов, удовлетворяющих заданному уровню целостности;
— получение формул вычисления мер целостности для узких классов графов.

Разработка и применение вычислительных систем в критических областях, а также стремительное развитие различных видов связи стимулируют поиск новых моделей, методов и средств создания отказоустойчивых систем. Актуальны модели повреждений графа, отражающие иерархичность построения систем и управления ими. Для некоторых известных мер целостности по-прежнему открыты вопросы вычислительной сложности применительно к некоторым классам графов. Востребованы алгоритмы вычисления точных и приближённых значений для существующих мер целостности.

ЛИТЕРАТУРА

1. *Абросимов М. Б.* О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2004. № 88(5). С. 643–650.
2. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012.
3. *Быкова В. В.* FPT-алгоритмы и их классификация на основе эластичности // Прикладная дискретная математика. 2011. № 2(12). С. 40–48.
4. *Громов Ю. Ю., Драчёв В. О., Набатов К. А., Иванова О. Г.* Синтез и анализ живучести сетевых систем. М.: Машиностроение, 2007.
5. *Грязнов Н. Г., Димитриев Ю. К., Мелентьев В. А.* Оптимизация отказоустойчивого вложения диагностического графа в тороидальные структуры живучих вычислительных систем // Автоматика и телемеханика. 2003. № 4. С. 133–152.
6. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
7. *Дундар П., Айтак А.* Выражения целостности тотальных графов через некоторые характеристики графов // Матем. заметки. 2004. № 76(5). С. 714–722.
8. *Дундар П., Айтак А., Айтак В.* Вычисление индекса доступности и окрестной целостности графа // Матем. заметки. 2005. № 78(5). С. 676–686.
9. *Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И.* Лекции по теории графов. М.: Книжный дом «ЛИБРОКОМ», 2012.
10. *Каравай М. Ф.* Применение теории симметрии к анализу и синтезу отказоустойчивых систем // Автоматика и телемеханика. 1996. № 6. С. 159–173.
11. *Каравай М. Ф.* Инвариантно-групповой подход к исследованию k-отказоустойчивых структур // Автоматика и телемеханика. 2000. № 1. С. 144–156.
12. *Кормен Т., Лейзерсон Ч., Ривест Р.* Алгоритмы: построение и анализ. М.: Вильямс, 2012.
13. *Кристофидес Н.* Теория графов: алгоритмический подход. М.: Мир, 1978.
14. *Ловас Л., Пламмер М.* Прикладные задачи теории графов. Теория паросочетаний в математике, физике, химии. М.: Мир, 1998.
15. *Салий В. Н* Минимальные примитивные расширения ориентированных графов // Прикладная дискретная математика. 2008. № 1(1). С. 116–119.
16. *Салий В. Н* Оптимальные реконструкции графов // Современные проблемы дифференц. геометрии и общей алгебры. Саратов: Изд-во Сарат. ун-та, 2008. С. 59–65.
17. *Хорошевский В. Г.* Архитектура вычислительных систем. М.: МГТУ им. Н. Э. Баумана, 2008.
18. *Atici M., Crawford R., and Ernst C.* New upper bounds for the integrity of cubic graphs // Int. J. Computer Math. 2004. No. 81(11). P. 1341–1348.

19. *Atici M., Crawford R., and Ernst C.* The integrity of small cage graphs // Australasian J. Combinatorics. 2009. No. 43. P. 39–55.
20. *Avizienis A.* The design of fault tolerant computers // AFIPS Conf. Proc. NY, USA, 1967. P. 733–743.
21. *Bagga K. S., Beineke L. W., Goddard W. D., et al.* A survey of integrity // Discrete Appl. Math. 1992. No. 37/38. P. 13–28.
22. *Bagga K. S., Beineke L. W., Lipman M. J., and Pippert R. E.* Edge-integrity: a survey // Discrete Math. 1994. V. 124. P. 3–12.
23. *Barefoot C. A., Entringer R., and Swart H. C.* Vulnerability in graphs — a comparative survey // J. Combin. Math. Combin. Comput. 1987. No. 1. P. 13–22.
24. *Barefoot C. A., Entringer R., and Swart H. C.* Integrity of trees and powers of cycles // Congr. Numer. 1987. V. 58. P. 103–114.
25. *Bauer D., Hakimi S. L., and Schmeichel E.* Recognizing tough graphs is NP-hard // Discrete Appl. Math. 1990. V. 28. P. 191–195.
26. *Bodlaender H. L., Hendriks A., Grigoriev A., and Grigorieva N. V.* The valve location problem in simple network topologies // Informs. J. Computing. 2010. V. 22(3). P. 433–442.
27. *Bykova V. V.* Parameterized complexity and elasticity of the algorithms // Proc. 14th Appl. Stochastic Models and Data Analysis Int. Conf. (ASMDA2011). Rome, Italy, 2011. P. 219–225.
28. *Bykova V. V.* Analysis parameterized algorithms on the bases of elasticity to functions complexity // J. Siberian Federal University. Math. & Physics. 2011. No. 4(2). P. 195–207.
29. *Chvatal V.* Tough graphs and Hamiltonian circuits // Discrete Math. 1973. No. 5. P. 215–228.
30. *Clark L. H., Entringer R. C., and Fellows M. R.* Computational complexity of integrity // J. Combin. Math. Combin. Comput. 1987. No. 2. P. 179–191.
31. *Cozzens M. B. and Wu S. Y.* Vertex-neighbor-integrity of trees // Ars Combinator. 1996. V. 43. P. 169–180.
32. *Cozzens M. B. and Wu S. Y.* Bounds of edge-neighbor-integrity of graphs // Australasian J. Combinatorics. 1997. V. 15. P. 71–80.
33. *DeLaVia E., Pepper R., and Waller B.* Lower bounds for the domination number // Discussiones Math. Graph Theory. 2010. V. 30(3). P. 475–487.
34. *Downey R. G. and Fellows M. R.* Parameterized complexity. N.Y.: Springer Verlag, 1999.
35. *Drange P. G., Dregi M. S., and Hof P.* On the computational complexity of vertex integrity. 2014. `http://arxiv.org/abs/1403.6331v1`.
36. *Fellows M. and Stueckle S.* The immersion order, forbidden subgraphs and the complexity of network integrity // J. Combin. Math. Combin. Comput. 1989. No. 6. P. 23–32.
37. *Goddard W. and Swart H. C.* Integrity in graphs: bounds and basic // J. Combin. Math. Combin. Comput. 1990. No. 7. P. 139–151.
38. *Hayes J. P.* A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. 25(9). P. 875–884.
39. *Katona G. Y.* Toughness and edge-toughness // Discrete Math. 1997. V. 164. P. 187–196.
40. *Kratsch D., Kloks T., and Muller H.* Measuring the vulnerability for classes of intersection graphs // Discrete Appl. Math. 1997. V. 77(3). P. 259–270.
41. *Laporte G. and Pascoal M.* The pipeline and valve location problem // Eur. J. Industr. Eng. 2012. No. 6(3). P. 301–321.
42. *Li F. W. and Li X. L.* Computing the rupture degrees of graphs // Proc. 7th Int. Symp. Parallel Architectures, Algorithms and Networks, IEEE Computer Society. Los Alamitos, California, 2004. P. 368–373.

43. *Li Y., Zhang S., and Zhang Q.* Vulnerability parameters of split graphs // Int. J. Comput. Math. 2008. V. 85(1). P. 19–23.
44. *Mann D. E.* The tenacity of trees. Ph. D. Thesis. Northeastern University, 1993.
45. *Moazzami D.* Vulnerability in graphs — a comparative survey // J. Combin. Math. Combin. Comput. 1999. V. 30. P. 23–31.
46. *Moazzami D.* An algorithm for the computation of edge integrity, $I'(T)$ // Int. J. Contemp. Math. Sci. 2011. No. 6(11). P. 507–516.
47. *Ray S. and Deogun J. S.* Computational complexity of weighted integrity // J. Combin. Math. Combin. Comput. 1994. V. 16. P. 65–73.
48. *Ray S., Kannan R., Zhang D., and Jiang H.* The weighted integrity problem is polynomial for interval graphs // Ars Combinator. 2006. V. 79. P. 77–95.
49. *Sundareswaran R. and Swaminathan V.* Domination integrity in graphs // Proc. Int. Conf. Math. Exp. Physics. Prague, Narosa Publishing House, 2009. P. 46–57.
50. *Sundareswaran R. and Swaminathan V.* Domination integrity of powers of cycles // Int. J. Math. Res. 2011. No. 3(3). P. 257–265.
51. *Sundareswaran R. and Swaminathan V.* Domination integrity in trees // Bulletin Int. Math. Virtual Institute. 2012. No. 2. P. 153–161.
52. *Piazza B. L., Robertst F. S., and Stueckle S. K.* Edge-tenacious networks // Networks. 1995. V. 25. P. 7–17.
53. *Vaidya S. K. and Shah N. H.* Domination integrity of total graphs // TWMS J. App. Eng. Math. 2011. No. 4(1). P. 117–126.
54. *Vaidya S. K. and Kothari N. J.* Some new results on domination integrity of graphs // Open J. Discrete Math. 2012. No. 2(3). P. 96–98. http://dx.doi.org/10.4236/ojdm.2012.23018
55. *Vince A.* The integrity of a cubic graph // Discrete Appl. Math. 2004. V. 140(1–3). P. 223–239.
56. *Woeginger G. J.* The toughness of split graphs // Discrete Math. 1998. V. 190(1–3). P. 295–297.
57. *Ye Q.* On vulnerability of power and total graphs // WSEAS Trans. Math. 2012. No. 11. P. 1028–1038.
58. *Zhang Q. L. and Zhang S. G.* Edge vulnerability parameters of split graphs // Appl. Math. Lett. 2006. V. 19. P. 916–920.
59. *Zhang S. G., Li X. L., and Han X. L.* Computing the scattering number of graphs // Int. J. Comput. Math. 2002. V. 79(2). P. 179–187.

2014 Прикладная теория графов № 4(26)

DOI 10.17223/20710410/26/12

УДК 519.17

ИНДЕКС ВИНЕРА МАКСИМАЛЬНЫХ ВНЕШНЕПЛОСКИХ ГРАФОВ

Ю. Л. Носов

г. Липецк, Россия

E-mail: yl.nosov@yandex.ru

Рассматривается инвариант $W(G)$ связных неориентированных графов G, равный сумме расстояний между всеми парами вершин графа G. Предлагается эффективный алгоритм расчёта матрицы расстояний и индекса Винера максимальных внешнеплоских графов с большим количеством вершин. Временная сложность алгоритма $\mathrm{O}(n^2)$. Алгоритм удобен как для ручного расчёта индекса Винера небольших графов, так и для расчёта индекса Винера графов, сгенерированных компьютерной программой.

Ключевые слова: *индекс Винера, максимальный внешнеплоский граф, хордальный граф, компактное представление хордального графа.*

Введение

Рассматриваются конечные связные неориентированные графы $G(V, E)$ без петель и кратных рёбер с множеством вершин $V(G)$ и множеством рёбер $E(G)$. Числа вершин и рёбер графа обозначаются $n(G)$ и $m(G)$ соответственно (или для краткости n и m). Число вершин графа называется порядком графа, а число ребер — его размером. Длина кратчайшей по числу рёбер цепи, соединяющей вершины u и v в графе G, называется расстоянием между вершинами u и v и обозначается через $\mathrm{d}(u, v)$. Матрицей расстояний n-вершинного графа G называется квадратная матрица $D(G) = [d_{ij}]$ размера $n \times n$, каждый элемент d_{ij} которой равен расстоянию между вершинами i и j. Матрица расстояний $D(G)$ является симметричной и все её диагональные элементы равны нулю.

Все неопределяемые ниже термины можно найти в [1].

Индексом Винера $W(G)$ графа G называется инвариант, определяемый как сумма расстояний между всеми парами вершин графа G, то есть

$$W(G) = \sum_{\{u,v\}\subseteq V(G)} \mathrm{d}(u, v) = \frac{1}{2} \sum_{v\in V(G)} \sum_{u\in V(G)} \mathrm{d}(u, v).$$

В терминах матрицы расстояний индекс Винера есть полусумма всех элементов матрицы или сумма всех элементов матрицы, находящихся выше главной диагонали:

$$W(G) = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} d_{ij} = \sum_{i=1}^{n} \sum_{j=i+1}^{n} d_{ij} = \sum_{j=1}^{n} \sum_{i=1}^{j} d_{ij}.$$

Впервые этот инвариант был использован американским химиком Г. Винером в 1947 г. для установления корреляционных зависимостей между значениями W и свойствами ациклических химических соединений, молекулярные графы которых являются деревьями [2]. Индекс Винера является топологическим инвариантом, отражающим структурные свойства графа (разветвлённость, цикличность и компактность) и используется в качестве сруктурного дескриптора в многочисленных приложениях

(см., например, [3]). Наибольшее применение индекс Винера нашел в химии, где он рассматривается как мера подобия молекулярных графов и используется для создания химических соединений с заданными свойствами [4 – 8].

Работы по тематике, связанной с индексом Винера, ведутся по двум направлениям:

— исследование теоретико-графовых свойств индекса Винера;
— разработка алгоритмов для расчёта индекса Винера.

Большинство работ по исследованию теоретико-графовых свойств индекса Винера посвящено поиску зависимостей значения индекса от структурных особенностей графа, определению верхних и нижних оценок индекса Винера по значениям других инвариантов [4, 9 – 11]. В некоторых работах исследуется изменение индекса при операциях над графами (удалении или добавлении вершин) [12, 13]. Так, например, в работе [13] определено значение индекса Винера дерева при добавлении новой вершины и одного ребра, соединяющего его с одной из вершин дерева.

Обширный перечень работ по данному направлению приведён в [9]. Там же дан обзор по индексу Винера для деревьев и графов гексагональных систем, приводятся результаты по вычислению индекса Винера для графов, обсуждаются влияние структуры графов на значения индекса Винера, проблемы вырождения индекса и смежные вопросы.

Теория индекса Винера для рёберных графов $L(G)$ развита в работах [4, 10, 11]. Интерес к этому виду производных графов обусловлен тем, что его характеристики используются для характеризации «сложности» структуры исходного графа. Здесь основное внимание уделяется нахождению графов, для которых их индексы Винера и индексы их рёберных графов совпадают.

Графы со свойством $W(G) = W(L(G))$ и заданными цикломатическим числом и обхватом построены в [10, 11].

В работах по второму направлению обычно определяются простые расчётные выражения, использующие основные структурные параметры графов; разрабатываются специализированные алгоритмы расчёта индекса Винера для различных классов графов, а также «универсальные» алгоритмы расчёта индекса Винера произвольных графов, использующие матрицу расстояний. Причём, как указано в [9], определённое значение имеет и разработка простых алгоритмов расчёта индекса Винера без использования компьютера.

Особенно большой прогресс сделан в разработке расчётных выражений [5] и специализированных алгоритмов расчёта индекса Винера для различных видов деревьев, дендримеров, графов гексагональных и пентагональных систем [4, 6 – 9, 13].

Индекс Винера произвольных графов вычисляется по матрице расстояний за время $O(n^2)$. Таким образом, временная сложность алгоритма расчёта индекса Винера определяется временной сложностью алгоритма расчета матрицы расстояний, минимально возможное значение которой равно $O(n^2)$.

Расчёт матрицы расстояний можно выполнить с помощью алгоритмов Флойда — Уоршелла [14, 15], Джонсона [16] или алгоритма умножения матриц [17]. Матрицу расстояний можно получить также посредством n-кратного выполнения алгоритма, определяющего длины кратчайших путей между заданной вершиной и всеми другими вершинами, каждый раз выбирая в качестве исходной новую вершину графа. В этом случае можно воспользоваться алгоритмом Дейкстры [18], алгоритмом поиска в ширину (BFS) [1, 19] или алгоритмом Беллмана — Форда [20, 21].

Алгоритм Дейкстры имеет временную сложность $O(n^2 \log n + nm)$, алгоритм поиска в ширину — $O(n^2 + nm)$, а алгоритм Беллмана — Форда — $O(mn^2)$ (здесь имеется в виду временная сложность по расчёту длины кратчайших путей между всеми парами вершин).

Алгоритм умножения матриц имеет временную сложность $O(n^3 \log n)$, алгоритм Флойда — Уоршелла — $O(n^3)$, а алгоритм Джонсона — $O(nm + n^2 \log n)$. Алгоритм Джонсона использует в качестве подпрограмм алгоритмы Дейкстры и Беллмана — Форда. Алгоритм Беллмана — Форда применяется при наличии отрицательных весов рёбер. В случае только положительных весов рёбер используется алгоритм Дейкстры. Таким образом, в рассматриваемом случае, когда все веса рёбер равны 1, результаты работы алгоритмов Джонсона и Дейкстры совпадают.

Нетрудно заметить, что все известные в настоящее время алгоритмы расчёта матрицы расстояний произвольных графов являются полиномиальными, а их временные сложности распределены в узком диапазоне от $O(n^3 \log n)$ до $O(n^2 + nm)$. Поэтому задача поиска быстрых алгоритмов расчёта индекса Винера графов очень большого порядка является актуальной.

Интересным для приложений классом графов являются максимальные внешнеплоские графы — плоские графы, у которых все вершины принадлежат внешней грани, а все внутренние грани есть треугольники [1, 22]. Графы этого вида входят в класс хордальных графов и представляют собой триангуляции выпуклого многоугольника, применяемые в системах искусственного интеллекта для обнаружения фигур в изображениях [23].

Индекс Винера максимальных внешнеплоских графов, отражающий их структуру и разветвлённость, может быть использован для распознавания и классификации графических образов в изображениях. Таким образом, задача разработки быстрого алгоритма расчёта индекса Винера максимальных внешнеплоских графов большого порядка является актуальной.

В настоящей работе предлагается простой и быстрый алгоритм расчёта матрицы расстояний и индекса Винера максимальных внешнеплоских графов большого порядка с временной сложностью $O(n^2)$.

1. Структура максимальных внешнеплоских графов

Рассмотрим структуру и свойства максимальных внешнеплоских графов (МВП-графов) [1], которые будут использованы для разработки алгоритма расчёта индекса Винера. Сначала отметим ряд основных хорошо известных свойств (см., например, [22, 24, 25]).

Утверждение 1 [22]. Любой МВП-граф G с $n \geqslant 3$ вершинами имеет:

1) $(n-2)$ внутренних граней (каждая внутренняя грань — треугольник);
2) $(2n-3)$ рёбер, из которых $(n-3)$ — внутренние рёбра;
3) по крайней мере две вершины степени 2.

Утверждение 2 [25]. Из любого n-вершинного МВП-графа можно получить другой МВП-граф с $(n+1)$ вершинами посредством добавления одной вершины и двух рёбер, соединяющих эту вершину с двумя вершинами ребра, принадлежащего внешней грани исходного МВП-графа.

Утверждение 3. При удалении вершины степени 2 и двух инцидентных ей рёбер из n-вершинного МВП-графа образуется новый $(n-1)$-вершинный МВП-граф.

МВП-графы являются хордальными графами [24] и, следовательно, имеют не менее двух симплициальных вершин (вершин, у которых множество смежных вершин индуцирует полный подграф). В МВП-графах симплициальные вершины имеют степень 2.

По количеству симплициальных вершин все МВП-графы можно разделить на два класса. МВП-графы первого класса имеют точно две симплициальные вершины. МВП-графами второго класса являются графы, имеющие не менее трёх симплициальных вершин. В качестве примера на рис. 1, *а*–*в* представлены МВП-графы первого класса, а на рис. 1, *г* — МВП-граф второго класса. Пунктиром показаны рёбра внешней грани, незакрашенными кружками — симплициальные вершины.

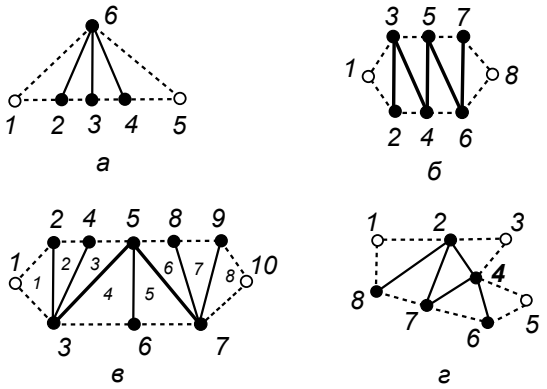

Рис. 1. МВП-графы первого класса: *а* — типа «веер», *б* — «лестница», *в* — «цепь»; *г* — второго класса

Из свойства хордальности МВП-графов следует (см., например, [24]) справедливость следующего утверждения.

Утверждение 4. Любой n-вершинный МВП-граф имеет совершенную последовательность исключения [1], т. е. последовательность вершин $v_1, v_2, \ldots, v_n$, в которой любая вершина v_i, $i = 1, \ldots, n-1$, является симплициальной вершиной в подграфе G_i, индуцированном множеством вершин $\{v_i, \ldots, v_n\}$.

Совершенная последовательность исключения МВП-графа может быть получена за линейное время с помощью алгоритмов LexBFS или MCS [26, 27].

Операция добавления вершины и двух рёбер, в литературе иногда называемая элементарным расширением [25], является основой для рекурсивной характеризации МВП-графов [25, 28].

Утверждение 5. Граф $G \neq K_3$ является МВП-графом тогда и только тогда, когда он может быть получен из графа K_3 с помощью конечной последовательности элементарных расширений.

Из утверждения 5 следует, что любой n-вершинный МВП-граф G_n получается из графа K_3 в результате последовательного k-кратного ($k = n-3$) выполнения операции элементарного расширения.

Возможность получения МВП-графа посредством конечной последовательности элементарных расширений определяет один из возможных способов нумерации вершин МВП-графа, который будем называть нумерацией в порядке построения (или естественной нумерацией).

Нумерацией в порядке построения (или *естественной нумерацией*) вершин n-вершинного МВП-графа называется такая нумерация, при которой для любого $3 \leqslant i \leqslant n$ подграф $G_i = G[\{1, 2, 3, \ldots, i\}]$, индуцированный множеством вершин $\{1, 2, 3, \ldots, i\}$, является МВП-графом.

В качестве примера на рис. 2 представлен процесс нумерации вершин МВП-графа в порядке построения.

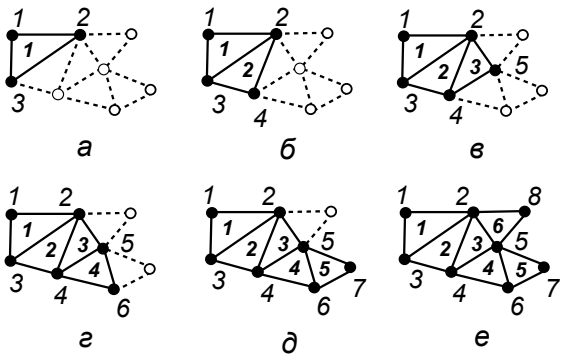

Рис. 2. Процесс нумерации вершин МВП-графа в порядке построения

Такая нумерация возникает при построении n-вершинного МВП-графа из K_3 посредством k-кратного выполнения элементарного расширения. Для этого необходимо сначала пронумеровать вершины исходного графа K_3 числами 1, 2, 3, а все остальные вершины нумеровать последовательно в порядке их добавления в граф. МВП-графы с нумерацией в порядке построения могут быть созданы с помощью компьютерной программы.

Примеры естественной нумерации в порядке построения представлены на рис. 1, *б,в*. Нумерация в порядке построения отображает структуру МВП-графа, поэтому будем её использовать для анализа метрических свойств МВП-графов и для разработки алгоритма расчёта матрицы расстояний и индекса Винера.

2. Компактное представление МВП-графов

В работе [29] для хордального графа G, имеющего симплициальную декомпозицию [24] со свойством скользящего пересечения (runnung intersection property) [30], предложено компактное представление $CP[G]$ в виде такой последовательности пар

$$CP(G) = [(R_1, S_1), (R_2, S_2), \ldots, (R_p, S_p)], \tag{1}$$

что

$$R_1 = Q_1, \quad S_1 = \varnothing, \quad R_j = Q_j \setminus S_j, \quad S_j = Q_j \cap (Q_1 \cup Q_2 \cup \ldots \cup Q_{j-1}), \quad 2 \leqslant j \leqslant p,$$

где Q_i — i-я максимальная клика; S_i — i-е минимальное разделяющее множество (сепаратор); R_i — i-е множество остатков, состоящее из симплициальных вершин.

В [29] показано, что последовательность $R_p, R_{p-1}, \ldots, R_1$ является совершенной последовательностью исключения.

В МВП-графах максимальная клика Q_1 и каждая максимальная клика Q_j состоит из трёх вершин, каждое множество S_j состоит из двух вершин, а каждое множество R_j имеет только одну симплициальную вершину.

Тогда, подставляя в формулу (1) значения составляющих Q_1, Q_j, S_j и $p = n-2$,

$$Q_1 = \{v'_1, v'_2, v'_3\}, \quad R_j = v_j, \quad Q_j = S_j \cup R_j, \quad S_j = \{x_j, y_j\}, \quad 2 \leqslant j \leqslant n-2,$$

для компактного представления МВП-графа G получим

$$CP(G) = [(\{v'_1, v'_2, v'_3\}, \varnothing), (v_2, \{x_2, y_2\}), \ldots, (v_{n-2}, \{x_{n-2}, y_{n-2}\})], \tag{2}$$

где v'_1, v'_2, v'_3 — симплициальные вершины, входящие в клику Q_1; v_j — симплициальная вершина клики Q_j; x_j, y_j — вершины из множества $(Q_1 \cup Q_2 \cup \ldots \cup Q_{j-1})$, смежные с вершиной v_j.

Таким образом, компактное представление МВП-графа G — это последовательность троек вершин, образующих максимальные клики G.

Полученное выражение (2) для n-вершинного МВП-графа G можно представить как результат последовательного применения операции элементарного расширения.

Действительно, пусть $G_1, G_2, \ldots, G_i, \ldots, G_{n-2}$ — последовательность графов, полученных в результате последовательного применения операции элементарного расширения. Тогда для этой последовательности справедливы выражения

$$G_1 = Q_1 = K_3, \quad G_j = Q_1 \cup Q_2 \cup \ldots \cup Q_j, \quad 2 \leqslant j \leqslant n-2,$$

и каждый граф G_j получается из графа G_{j-1} добавлением новой вершины v_j и двух рёбер, соединяющих её с парой вершин x_{j-1}, y_{j-1} графа G_{j-1}.

Очевидно, что для МВП-графа с нумерацией вершин в порядке построения существует компактное представление

$$CP(G) = [(\{1,2,3\}, \varnothing), (4, \{x_2, y_2\}), (5, \{x_3, y_3\}), \ldots, (n, \{x_{n-2}, y_{n-2}\})]. \tag{3}$$

Компактное предствление МВП-графа с нумерацией вершин в порядке построения вида (3) будем называть *каноническим компактным представлением* и обозначать через $CCP(G)$.

Пример 1. МВП-граф на рис. 1, *б* имеет каноническое компактное представление

$$CCP(G) = [(\{1,2,3\}, \varnothing), (4, \{2,3\}), (5, \{3,4\}), (6, \{4,5\}), (7, \{5,6\}), (8, \{6,7\})].$$

Пример 2. МВП-граф на рис. 1, *г* имеет компактное представление

$$CP(G) = [(\{1,2,8\}, \varnothing), (7, \{2,8\}), (4, \{2,7\}), (3, \{2,4\}), (6, \{4,7\}), (5, \{4,6\})].$$

В [29] показано, что компактное представление МВП-графа может быть получено из его совершенной последовательности исключения за время $O(n+m)$. Однако более целесообразно использовать алгоритм, предложенный в [31]. Алгоритм использует метод MCS и имеет временную сложность $O(n+m)$.

Каноническое компактное представление МВП-графа G получается из компактного представления $CP(G)$ посредством перенумерации вершин. Псевдокод алгоритма приводится ниже.

Алгоритм 1. Алгоритм расчёта $CCP(G)$ МВП-графа G

Вход: компактное представление $CP(G)$
Выход: каноническое компактное представление $CCP(G)$
1: $index[v'_1] := 1;\ index[v'_2] := 2;\ index[v'_3] := 3;$
2: $v'_1 := 1;\ v'_2 := 2;\ v'_3 := 3;$
3: **Для** $j = 2, \ldots, n-2$
4: $\quad index[v_j] := j + 2;\ v_j := j + 2;$
5: **Для** $j = 2, \ldots, n-2$
6: $\quad x_j := index[x_j];\ y_j := index[y_j].$

Алгоритм перенумерации достаточно прост и состоит из трёх шагов. На первом шаге создается индексный массив $index$ длины n. Затем для каждой из вершин v'_1, v'_2, v'_3 определяется индекс $index[v'_1] = 1$, $index[v'_2] = 2$, $index[v'_3] = 3$, после чего номерам вершин v'_1, v'_2, v'_3 присваиваются новые значения $v'_1 = 1, v'_2 = 2, v'_3 = 3$.

На втором шаге в цикле выполняется проход по всем другим триплетам $\{v_2, \{x_2, y_2\}\}, \ldots, \{v_{n-2}, \{x_{n-2}, y_{n-2}\}\}$ и для каждой вершины v_j, $j = 2, \ldots, n-2$, определяется индекс $index[v_j] = j + 2$, а номеру вершины присваивается новое значение $v_j = j + 2$. Количество повторений в цикле равно $n - 3$.

На третьем шаге в цикле выполняется повторный проход по триплетам и в каждой паре вершин $\{x_j, y_j\}$, $j = 2, \ldots, n-2$, вершинам x_j и y_j присваиваются новые значения номеров с помощью индексного массива по формулам $x_j = index[x_j]$ и $y_j = index[y_j]$. Таким образом, при перенумерации выполняются два цикла, в каждом из которых количество повторений равно $n - 3$. Временная сложность алгоритма перенумерации составляет $\mathrm{O}(n)$.

Отметим, что каноническое компактное представление МВП-графа может быть сгенерировано компьютерной программой в процессе создания МВП-графа.

3. Метрические свойства МВП-графов

Операция элементарного расширения (добавления вершины и двух рёбер) является очень важным звеном в построении МВП-графов. Поэтому вопрос, как изменяется индекс Винера МВП-графа при выполнении этой операции, имеет важное значение.

Теорема 1. Пусть G_n — МВП-граф с $n > 3$ вершинами $v_1, v_2, v_3, \ldots, v_n$ и индексом Винера $W(G_n)$. Тогда МВП-граф G_{n+1}, полученный добавлением вершины v_{n+1} и двух рёбер, соединяющих её с вершинами v_p и v_q ребра, принадлежащего внешней грани МВП-графа G_n, имеет индекс Винера, равный

$$W(G_{n+1}) = W(G_n) + \sum_{i=1}^{n} (\min(\mathrm{d}(v_i, v_p), \mathrm{d}(v_i, v_q)) + 1). \tag{4}$$

Доказательство. По определению индекс Винера МВП-графа G_{n+1} равен

$$W(G_{n+1}) = \sum_{i=1}^{n} \sum_{j=i+1}^{n+1} \mathrm{d}(v_i, v_j).$$

Правую часть этого выражения можно представить в виде

$$\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \mathrm{d}(v_i, v_j) + \sum_{i=1}^{n} \mathrm{d}(v_i, v_{n+1}). \tag{5}$$

Очевидно, первый член выражения (5) есть индекс Винера исходного МВП-графа, а для любой вершины $v_i \in V(G_n)$ расстояние $\mathrm{d}(v_i, v_{n+1})$ между вершинами v_i и v_{n+1} равно

$$\mathrm{d}(v_i, v_{n+1}) = \min(\mathrm{d}(v_i, v_p), \mathrm{d}(v_i, v_q)) + 1. \tag{6}$$

Подставляя значение $\mathrm{d}(v_i, v_{n+1})$ из равенства (6) в выражение (5), получим искомое выражение (4). ■

Выражения (4), (6) могут быть использованы в алгоритме расчёта индекса Винера МВП-графов.

4. Расчет индекса Винера МВП-графов

Нетрудно заметить, что для МВП-графов с естественной нумерацией вершин можно построить простой итеративный алгоритм для определения матрицы расстояний и расчёта индекса Винера. Действительно, пусть G_n — n-вершинный МВП-граф с естественной нумерацией, полученный из исходного трёхвершинного МВП-графа K_3 последовательным добавлением $n-3$ вершин. В процессе построения графа получим последовательность его подграфов вида

$$G_3 = K_3, G_4, G_5, G_6, \ldots, G_{n-1}, G_n.$$

Тогда для индекса Винера $W(G_k)$ каждого подграфа G_k будем иметь

$$W(G_k) = W(G_{k-1}) + S_k, \quad k = 4, 5, \ldots, n-1, n,$$

где S_k — приращение индекса Винера при добавлении вершины k.

В результате для индекса Винера МВП-графа G_n получим

$$W(G_n) = W(G_3) + S_4 + S_5 + \cdots + S_{n-1} + S_n. \tag{7}$$

Значение приращения индекса Винера для k-й вершины (при её добавлении) получим из выражения (3), используя матричную нотацию

$$S_k = \sum_{i=1}^{k-1} (\min(d_{ip}, d_{iq}) + 1), \tag{8}$$

где p и q — вершины подграфа G_{k-1}, смежные с вершиной k подграфа G_k; d_{ip}, d_{iq} — элементы матрицы расстояний $[d_{ij}]$.

На основании (8) предлагается алгоритм 2 расчёта матрицы расстояний и индекса Винера МВП-графа, заданного в каноническом компактном представлении. Основными исходными данными в алгоритме являются два массива, содержащие номера вершин, смежных с добавляемыми вершинами, и матрица расстояний, у которой на первой стадии расчётов инициализируются диагональные элементы и элементы подматрицы размера 3×3, соответствующей исходному трёхвершинному МВП-графу.

Расчёт выполняется последовательно для всех подграфов G_k, начиная с $k = 4$, при этом сначала определяются элементы верхней части k-го столбца подматрицы размера $k \times k$, а затем — элементы левой части k-й строки.

Докажем корректность алгоритма. Ясно, что для правильной работы алгоритма необходимо выполнение следующего условия: на каждом шаге алгоритма при добавлении вершины k к графу G_{k-1} расстояния $\mathrm{d}(v_i, v_p)$ и $\mathrm{d}(v_i, v_q)$ от любой вершины $v_i \in G_{k-1}$ до вершин v_p и v_q, смежных с вершиной k, должны быть определены на предшествующих шагах алгоритма.

Алгоритм 2. Алгоритм расчета матрицы расстояний и индекса Винера

Вход: целочисленные массивы номеров вершин $A[n]$ и $B[n]$ размера n
Выход: матрица расстояний $d[i,j]$, индекс Винера W

1: **Для** $i = 1, \ldots, n$
2: $d[i,i] := 0$; *// инициализация*
3: $d[1,2] := 1; d[1,3] := 1; d[2,1] := 1;$
4: $d[2,3] := 1; d[3,1] := 1; d[3,2] := 1; W := 3;$
5: **Для** $k = 4, \ldots, n$
6: $p := A[k]; q := B[k]; S[k] := 0;$
// Заполнение верхней части k-го столбца матрицы расстояний
7: **Для** $i = 1, \ldots, k-1$
8: $d[i,k] := \min(d[i,p], d[i,q]) + 1;$
9: $S[k] := S[k] + d[i,k];$
// Заполнение левой части k-й строки матрицы расстояний
10: **Для** $j = 1, \ldots, k-1$
11: $d[k,j] := d[j,k];$
12: $W := W + S[k]$ *// Расчёт индекса Винера*

Выполнение этого условия обеспечивается:

1) структурой алгоритма (на каждом шаге сначала производится расчёт всех элементов верхней части k-го столбца, которые затем копируются в соответствующие элементы левой части k-й строки, которая будет использована на следующем шаге);
2) использованием канонического компактного представления (следовательно, для любой вершины v_i графа G_{k-1}, к которому добавляется вершина k, выполняется неравенство $v_i < k$).

Определим временную сложность алгоритма. Алгоритм состоит из четырёх циклов. В первом цикле (операторы 1, 2) выполняется заполнение главной диагонали матрицы нулями. Все основные действия алгоритма выполняются во внешнем цикле (операторы 5–12) и двух внутренних циклах (операторы 7–9 и 10, 11). В первом внутреннем цикле производится расчёт всех элементов верхней части k-го столбца. Во втором внутреннем цикле производится заполнение всех элементов левой части k-й строки. Количество повторений в первом цикле n, в других циклах — $n^2 - n - 6$. Таким образом, временная сложность алгоритма $\mathrm{O}(n^2)$.

Общая временная сложность расчёта индекса Винера по предлагаемой методике складывается из временной сложности алгоритма расчёта индекса Винера и алгоритмов получения компактного представления и его перенумерации. Сложность алгоритма получения компактного представления равна $\mathrm{O}(n+m)$, алгоритма перенумерации — $\mathrm{O}(n)$. Для МВП-графов $m = 2n - 3$, поэтому общее количество операций алгоритма равно $n^2 + 5n - 9$, а общая временная сложность — $\mathrm{O}(n^2)$.

Ясно, что предлагаемый алгоритм превосходит по эффективности алгоритм умножения матриц, алгоритм Флойда — Уоршелла и алгоритмы Джонсона и Дейкстры, которые имеют временную сложность $\mathrm{O}(n^3 \log n)$, $\mathrm{O}(n^3)$ и $\mathrm{O}(n^2 \log n + nm)$ соответственно. Алгоритм Беллмана — Форда при расчёте индекса Винера МВП-графов имеет временную сложность $\mathrm{O}(n^3)$ (при n^3 имеется скрытая константа 2) и тоже уступает предлагаемому алгоритму по эффективности.

Из всех известных алгоритмов лучшим является алгоритм поиска в ширину (BFS), который при расчёте индекса Винера МВП-графов имеет временную сложность $O(n^2)$. Однако алгоритм BFS хуже, чем предлагаемый алгоритм, поскольку количество операций алгоритма BFS равно $(3n^2 - 3n)$, что при больших значениях n приблизительно в 3 раза больше общего количества операций предлагаемого алгоритма.

Это подтверждается результатами тестирования алгоритмов получения компактного представления (CP), расчёта индекса Винера по предлагаемой методике (W_{CP}) и с помощью алгоритма BFS (W_{BFS}). В таблице представлены средние значения времени работы алгоритмов в миллисекундах для разных значений количества вершин n. Расчёты проводились в системе `Mathematica`. Для каждого значения n с помощью компьютера генерировались случайные МВП-графы с нумерацией в порядке построения. Алгоритм BFS реализован в соответствии с [19]. Для получения компактного представления использовался алгоритм [31]. Нетрудно заметить, что при любом $n \geqslant 50$ время работы алгоритма BFS в 3 раза больше, чем суммарное время работы алгоритмов получения компактного представления и расчёта индекса Винера по предлагемой методике.

n	CP	W_{CP}	W_{BFS}
50	16	22	123
75	31	47	275
100	48	89	508
150	98	211	1158

Выводы

Для МВП-графов получено рекуррентное соотношение для вычисления индекса Винера. Разработан алгоритм расчёта индекса Винера МВП-графов, представленных в компактной форме. Алгоритм имеет минимально возможное для алгоритмов, использующих матрицу расстояний, значение временной сложности равное $O(n^2)$. Наибольшая сравнительная эффективность достигается при расчёте индекса Винера МВП-графов большого порядка. Однако простота и наглядность алгоритма позволяют использовать его и для ручных вычислений индекса Винера МВП-графов с малым количеством вершин. Дополнительным положительным свойством алгоритма является возможность его прямого (без перенумерации вершин) использования для расчёта индекса Винера МВП-графов, сгенерированных компьютерной программой.

ЛИТЕРАТУРА

1. *Евстигнеев В. А., Касьянов В. Н.* Словарь по графам в информатике. Новосибирск: ООО «Сибирское научное издательство», 2009. 300 с.
2. *Wiener H.* Structural determination of paraffin boiling points // J. Amer. Chem. Soc. 1947. V. 69. P. 17–20.
3. *Федянин Д. Н.* Об индексе Винера в последовательности социальных сетей // Тр. 52-й науч. конф. МФТИ «Соременные проблемы фундаментальных и прикладных наук». Ч. I. Радиотехника и кибернетика. Т. 2. М.: МФТИ, 2009. С. 94–97.
4. *Dobrynin A. A., Entringer R. C., and Gutman I.* Wiener index of trees: theory and applications // Acta Appl. Math. 2001. V. 66. No. 3. P. 211–249.
5. *Gutman I., Yeh Y. N., Lee S. L., and Luo Y. L.* Some recent results in the theory of the Wiener number // Indian J. Chemistry. 1993. V. 32A P. 651–661.
6. *Gutman I., Yan W., Yang B. Y., and Yeh Y. N.* Generalized Wiener indices of zigzagging pentachains // J. Math. Chem. 2007. V. 42. No. 2. P. 103–117.

7. *Gutman I., Yeh Y. N., Lee S. L., and Chen J. C.* Wiener numbers of dendrimer // Commum. Math. Chem. 1984. V. 30. No. 1. P. 103–115.
8. *Vukičević D. and Trinajstić N.* Wiener indices of benzenoid graphs // Bulletin of the Chemists and Technologists of Macedonia. 2004. V. 23. No. 2. P. 113–129.
9. *Добрынин А. А., Гутман И.* Индекс Винера для деревьев и графов гексагональных систем // Дискретный анализ и исследование операций. 1998. Сер. 2. Т. 5. № 2. С. 34–60.
10. *Добрынин А. А., Мельников Л. С.* Индекс Винера для графов и их реберных графов // Дискретный анализ и исследование операций. 2004. Сер. 2. Т. 11. № 2. С. 25–44.
11. *Добрынин А. А.* Индекс Винера для графов произвольного обхвата и их реберных графов // Сибирский журнал индустриальной математики. 2009. Т. XXII. № 4(40). С. 44–50.
12. *Šoltés L.* Transmission in graphs: a bound and vertex removing // Math. Slovaca. 1991. V. 41. No. 1. P. 11–16.
13. *El Marraki M. and Al Hagri G.* Calculation of the Wiener index for some particular trees // J. Theor. Appl. Inform. Technology (JATIT). 2010. V. 22. No. 2. P. 77–83.
14. *Floyd R. W.* Algorithm 97: Shortest Path // Comm. ACM. 1962. V. 5. No. 6. P. 345.
15. *Warshall S.* A theorem on Boolean matrices // J. ACM. 1962. V. 9. No. 1. P. 11–12.
16. *Johnson D. B.* Efficient algorithms for shortest paths in sparse networks // J. ACM. 1977. V. 24. No. 1. P. 1–13.
17. *Müller W. R., Szymanski K., Knop J. V., and Trinajstić N.* An algorithm for construction of the molecular distance matrix // J. Comput. Chem. 1987. V. 8. No. 2. P. 170–173.
18. *Dijkstra E. W.* A note on two problems in connexion with graphs // Numer. Math. 1959. V. 1. No. 1. P. 269–271.
19. *Mohar B. and Pisanski T.* How to compute the Wiener index of a graph. // J. Math. Chem. 1988. V. 3. No. 2. P. 267–277.
20. *Bellman R.* On a routing problem // Quart. Appl. Math. 1958. V. 16. No. 1. P. 87–90.
21. *Ford Jr. L. R.* Network Flow Theory // Paper P-923. Santa Monica, California: RAND Corp., 1956. P. 923.
22. *Харари Ф.* Теория графов. М.: Мир, 1973. 300 с.
23. *Felzenszwalb P. F.* Representation and detection of deformable shapes // IEEE Trans. Pattern Analys. Machine Intelligence. 2005. V. 27. No. 2. P. 208–220.
24. *Dirac G. A.* On rigid circuit graphs // Abh. Math. Sem. Univ. Hamburg. 1967. V. 25. P. 71–76.
25. *Asratian A. S. and Oksimets N.* Graphs with hamiltonian balls // Australasian J. Combinator. 1998. V. 17. No. 4. P. 185–198.
26. *Rose D., Tarjan R. E., and Lueker G.* Algorithmic aspects of vertex elimination on graphs // SIAM J. Comput. 1976. V. 5. No. 2. P. 146–160.
27. *Tarjan R. E., and Yannakakis M.* Simple linear-time algorithms to test chordality of graphs, test acyclicity of hypergraphs, and selectively reduce acyclic hypergraphs // SIAM J. Comput. 1984. V. 13. No. 3. P. 566–579.
28. *Beyer T., Jones W., and Mitchell S.* Linear algorithms for isomorphism of Maximal outerplanar graphs. // J. ACM. 1979. V. 26. No. 4. P. 603–610.
29. *Markenzon L. and Pereira P. R. C.* A compact representation for chordal graphs // Proc. of Workshop on Graphs and Combinatorial Optimization. Gargnano: CTW, 2008. P. 174–176.
30. *Blair J. R. S. and Peyton B.* An introduction to chordal graphs and clique trees // Graph Theory and Sparse Matrix Computation. N.Y.: Springer Verlag, 1993. P. 1–29.
31. *Markenzon L. and Vernet O.* Representações Computacionais de Grafos. Notas em Matemática Aplicada. V. 24. São Carlos, SP: SBMAC, 2006. 76 p.

СВЕДЕНИЯ ОБ АВТОРАХ

АПРАКСИНА Татьяна Валентиновна — аспирантка Национального исследовательского университета «МИЭТ», г. Москва, Зеленоград.
E-mail: **taya.apraksina@gmail.com**

БОНДАРЕНКО Леонид Николаевич — кандидат технических наук, доцент, доцент кафедры дискретной математики Пензенского государственного университета, г. Пенза. E-mail: **leobond5@mail.ru**

БЫКОВ Игорь Сергеевич — магистрант механико-математического факультета Новосибирского государственного университета, г. Новосибирск.
E-mail: **patrick.no10@gmail.com**

БЫКОВА Валентина Владимировна — доктор физико-математических наук, доцент, профессор Института математики и фундаментальной информатики Сибирского федерального университета, г. Красноярск. E-mail: **bykvalen@mail.ru**

ВИННИЧУК Илона Игоревна — студентка факультета математики, механики и компьютерных наук Южного федерального университета, г. Ростов-на-Дону.
E-mail: **ilonavinnichuk144@gmail.com**

КАТЫШЕВ Сергей Юрьевич — научный сотрудник ООО «Центр сертификационных исследований», г. Москва. E-mail: **sairos87@mail.ru**

КОВАЛЕНКО Марьяна Эдуардовна — аспирантка Московского государственного университета им. М. В. Ломоносова, г. Москва.
E-mail: **kovalenkomaryana@gmail.com**

КОСОЛАПОВ Юрий Владимирович — кандидат технических наук, доцент кафедры алгебры и дискретной математики Южного федерального университета, г. Ростов-на-Дону. E-mail: **itaim@mail.ru**

КУЗЬМИН Алексей Сергеевич — доктор физико-математических наук, профессор, г. Москва.

ЛУКЬЯНОВА Наталья Александровна — старший преподаватель Института математики и фундаментальной информатики Сибирского федерального университета, г. Красноярск. E-mail: **nata00sfu@gmail.com**

НОЗДРУНОВ Владислав Игоревич — сотрудник лаборатории ТВП, г. Москва. E-mail: **vlad_vin@mail.ru**

НОСОВ Юрий Леонидович — г. Липецк. E-mail: **yl.nosov@yandex.ru**

СЕМЕНОВА Дарья Владиславовна — кандидат физико-математических наук, доцент, доцент Института математики и фундаментальной информатики Сибирского федерального университета, г. Красноярск. E-mail: **dariasdv@gmail.com**

ТОКАРЕВА Наталья Николаевна — кандидат физико-математических наук, старший научный сотрудник Института математики им. С. Л. Соболева, г. Новосибирск. E-mail: **tokareva@math.nsc.ru**

ЧЕРНЯК Роман Игоревич — аспирант Национального исследовательского Томского государственного университета, младший научный сотрудник Института инноватики Томского государственного университета систем управления и радиоэлектроники, г. Томск. E-mail: **roman.chernyak@elecard.ru**

ШАРАПОВА Марина Леонидовна — старший преподаватель кафедры математического анализа механико-математического факультета Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **msharapova@list.ru**

АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ

Apraksina T. V. **ON GENERATING SETS OF DIAGONAL ACTS OVER SEMIGROUPS OF ISOTONE AND CONTINUOUS TRANSFORMATIONS.** The diagonal acts (automata) over semigroups of isotone transformations of a partially ordered set and continuous mappings of a topological space into itself are investigated. For the diagonal right act over the semigroup of continuous selfmappings of a compact, a necessary condition to be cyclic is given. For the diagonal act over a semigroup of isotone selfmappings of the set of natural numbers, the absence of a countable set of generators is proved. The connections between the continuity and the isotonness are studied.
Keywords: *act, diagonal act, isotone mapping, generating set, semigroup of continuous mappings.*

Bondarenko L. N., Sharapova M. L. **COMPARISONS FOR NUMBERS OF COMPLETE MAPPINGS.** For the numbers of standard complete mappings and for the numbers of standard strong complete mappings, comparisons modulo a prime number are obtained. The proofs of them are based on properties of some statistics and Euler's numbers on the related sets of permutations. For these sets, similar results taking into account the sign of permutations in them are also obtained.
Keywords: *complete mappings, permutation, statistic, Euler's numbers, Wilson theorem, displacement of permutation.*

Katyshev S. Yu. **DISCRETE LOGARITHM PROBLEM IN FINITE DIMENSIONAL ALGEBRAS OVER FIELD.** The open key distribution procedure by Diffie — Hellmann algorithm over non associative groupoid is studied. It is proved that the discrete logarithm problem in finite dimensional algebras is polynomially equivalent to the discrete logarithm problem in finite fields.
Keywords: *open key distribution, Diffie — Hellmann algorithm, non associative groupoids, finite dimensional algebras, discrete logarithm problem.*

Kuzmin A. S., Nozdrunov V. I. **RELATIONSHIP BETWEEN THE COEFFICIENTS OF POLYNOMIALS OVER GF(2^n) AND WEIGHTS OF BOOLEAN FUNCTIONS REPRESENTED BY THEM.** Boolean functions in n variables are represented by polynomials over GF(2^n). The relationship between the coefficients of polynomials and the weights of functions are researched. Some formulas for expressing the dependence of the first and the second bits in the binary code of the function weight on the polynomial coefficients are obtained. For weights of bent functions and for their subfunctions, some expressions are also obtained.
Keywords: *Boolean function, bent function, polynomial over a field, vector space, weight of function, subspaces.*

Semenova D. V., Lukyanova N. A. **RECURRENT FORMATION OF DISCRETE PROBABILISTIC DISTRIBUTIONS OF RANDOM SETS OF EVENTS.** The class of discrete probabilistic distributions of the II type of a random set on a set of N events is investigated. For constructing such probabilistic distributions, a recurrent formula and associative functions are offered to use. The advantage of the approach is that

for the definition of the probabilistic distribution, instead of 2^N probabilities of events, it is enough to know N probabilities and the type of the associative function. This approach is tested for some three associative functions. The theorems establishing their forms and the legitimacy conditions for obtained probabilistic distributions of random sets of events are proven.
Keywords: *random set of events, discrete probability distributions, associative function.*

Tokareva N. N. **ON DECOMPOSITION OF A DUAL BENT FUNCTION INTO SUM OF TWO BENT FUNCTIONS.** It is proven that a bent function is decomposable into the sum of two bent functions if and only if the same is true for its dual bent function.
Keywords: *bent function, dual function.*

Vinnichuk I. I., Kosolapov Y. V. **THE EVALUATION OF CODE NOISING SECURITY AGAINST THE l-FOLD PARTIAL DATA OBSERVATION IN THE NETWORK.** A communication network with linear coding in the nodes is considered. It is assumed that an adversary can overhear data transmitted through some edges of the network and code noising is used to protect incoming information. In the paper, the security of code noising against multiple eavesdropping the network data is analysed. A formula for calculating the security against l interceptions of information words is obtained. The formula is applied to the security analysis of code noising based on Reed — Muller code $\mathcal{R}(1, 3)$.
Keywords: *network coding, partial observation, code noising, analysis of security.*

Kovalenko M. E. **ON THE COVERING RADIUS OF THE LINEAR CODES GENERATED BY THE AFFINE GEOMETRIES OVER GF(4).** The covering radius for a code is defined to be a maximal distance between a space vector and the code. It is shown that the covering radius for a linear code generated by the affine geometry over GF(4) equals 4.
Keywords: *linear codes, finite affine geometries, covering radius.*

Chernyak R. I. **EXPERIMENTAL ANALYSIS OF INTRA PREDICTION IN H.265/HEVC.** In this paper, the Intra Prediction part of the newest video compression standard H.265/HEVC is experimentally tested for the effectiveness of its application to video sequences of different types.
Keywords: *digital video compression, intra prediction, H.265/HEVC, intra modes.*

Bykov I. S. **FUNCTIONING OF DISCRETE DYNAMIC CIRCULANT-TYPE SYSTEM WITH THRESHOLD FUNCTIONS.** The functioning of discrete dynamic circulant-type systems with threshold functions is studied. The general properties of the functional graph of a system are described. In binary case, all states of the system are classified according to the length of 0-series and 1-series. As a result, some properties of cycles in the functional graph and a lower estimate for the number of connected components are given. For an arbitrary value p, a criterion for the existence of stable states in the system is given, the forms and the number of these states are determined.
Keywords: *discrete dynamic systems, functional graph, circulant graph, threshold functions, cycles of functional graph, stable states.*

Bykova V. V. **MEASURES FOR GRAPH INTEGRITY: A COMPARATIVE SURVEY.** The brief overview of deterministic graph integrity measures is presented. The well-known relationships between them are given. Some estimates for these measures

expressed through the traditional numerical graph parameters are given too. A relationship between the computational complexity of the integrity measures and damage models in graphs is analyzed. Some unsolved problems are pointed.
Keywords: *graphs, vulnerability, integrity, toughness, scattering number, tenacity, rupture degree, domination integrity, network reliability, neighbour integrity.*

Nosov Y. L. **THE WIENER INDEX OF MAXIMAL OUTERPLANE GRAPHS.**
Wiener index $W(G)$ of a connected undirected graph G equals the sum of distances between all pairs of vertices in G. In this paper, an effective algorithm for calculating Wiener index of maximal outerplane graphs with a big number n of vertices is offered. The time complexity of the algorithm is $O(n^2)$. The algorithm is fit for manual calculation of Wiener index of small graphs, as well as for its calculation for computer generated graphs.
Keywords: *graph algorithm, maximal outerplane graph, Wiener index, chordal graph, compact representation of chordal graph.*

Журнал «Прикладная дискретная математика» включен в перечень ВАК рецензируемых российских журналов, в которых должны быть опубликованы основные результаты диссертаций, представляемых на соискание учёной степени кандидата и доктора наук, а также в перечень журналов, рекомендованных УМО в области информационной безопасности РФ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте journals.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также и правила подготовки рукописей статей в журнал.

Тематика публикаций журнала:

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Дискретные модели реальных процессов*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*