МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2020 № 47

Зарегистрирован в Федеральной службе по надзору
в сфере связи и массовых коммуникаций

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

Подписной индекс в объединённом каталоге «Пресса России» 38696

УЧРЕДИТЕЛЬ
Томский государственный университет

Адрес редакции и издателя: 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 надёжности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

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

Подписано к печати 10.03.2020. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 14,78. Тираж 300 экз.
Заказ № 4265. Цена свободная. Дата выхода в свет 20.03.2020.

Отпечатано на оборудовании
Издательского Дома Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

CONTENTS

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.14 + 519.23

СТРУКТУРА КОЛЛЕКТИВА БЛИЖАЙШИХ СОСЕДЕЙ В СЕМЕЙСТВЕ РАЗБИЕНИЙ КОНЕЧНОГО МНОЖЕСТВА

С. В. Дронов

Алтайский государственный университет, г. Барнаул, Россия

Рассмотрены разбиения конечного множества на дизъюнктные подмножества, ближайшие к заданному (основному) разбиению в специальной кластерной метрике. Для фиксированного основного разбиения найдены вид ближайших к нему разбиений и их количество. На основе этого предложен статистический критерий для определения значимости отличий двух разбиений. Приводится пример обработки медицинских данных с помощью этого критерия.

Ключевые слова: *разбиения конечных множеств, кластерная метрика, статистическая значимость различия разбиений.*

DOI 10.17223/20710410/47/1

A STRUCTURE OF THE NEAREST NEIGHBORS COLLECTIVE IN A FAMILY OF PARTITIONS OF A FINITE SET

S. V. Dronov

Altai State University, Barnaul, Russia

E-mail: dsv@math.asu.ru

In this paper, we study partitions of a finite set of some objects into disjoint subsets closest to a given (main) partition. The distance between two partitions is taken equal to the sum of squares of numbers of the elements of sets that make up each of the partitions minus twice the sum of squares of the values of the sets forming the intersection of the partitions. For a fixed main partition, all the closest partitions and their number are found. The closest neighbors are always obtained by picking out one of the objects into a new set or by merging two single-element sets of the main partition (Theorem 1). The nearest neighbor here is $2(m-1)$ from the main partition, where m is the number of objects of the minimum non-singleton of the main partition, if one exists. Otherwise, this distance equals 2. Theorem 2 describes a situation where the number of elements of partitions must be the same. This happens, for example, when both partitions are constructed by the method of k -means for the same k. Here, to construct the nearest neighbor, one of the objects moves between the smallest sets of the main partition. Wherein, at least one of them must contain at least two objects. The corollaries of both theorems, obtained by accurately calculating the possible number of operations of the described type, give the exact quantities of nearest neighbors of the main partition, depending on its structure. We propose an application of the

obtained results to the construction of a statistical criterion for the significance of the difference between two partitions. An example of medical data processing using this criterion is given.

Keywords: *partitions of finite sets, cluster metric, statistical significance of differences of partitions.*

1. Основная задача работы

При рассмотрении разных способов разбиения конечного множества на части возникает ряд комбинаторных проблем [1; 2, Example 11.7]. На семействе всех возможных разбиений данного множества имеется естественная структура решётки, подробно изученная в [3]. Исследование одновременно нескольких разбиений множества на непустые части может потребоваться, например, в задачах анализа данных, в частности, подобное разбиение всегда появляется в результате применения некоторого алгоритма кластерного анализа. При применении к изучаемому множеству разных кластерных алгоритмов, равно как и при попытках разделения этого множества на группы по степени близости различных наборов характеризующих его элементы признаков, мы приходим, вообще говоря, к разным разбиениям. Сравнение получившихся разбиений может привести к заключению о степени различия применявшихся алгоритмов или о силе взаимного влияния и связей двух наборов признаков.

Рассмотрим множество U, состоящее из конечного числа n объектов. Набор непустых его подмножеств $A = \{a_1, \ldots, a_k\}$ будем называть разбиением U, если эти подмножества попарно дизъюнктны, а их объединение совпадает со всем множеством U. Сделанные предположения означают, в частности, что для каждого $x \in U$ найдется единственное множество $a_{i(x)}$ из набора A, для которого справедливо $x \in a_{i(x)}$.

Заметим, что любое кластерное разбиение множества U удовлетворяет данному определению. Мы не употребляем термин «кластерное разбиение» для изучаемых далее наборов множеств только потому, что при построении этих множеств не предполагается близости элементов каждого из них в каком-либо смысле, что является обязательным для кластеров. Хотя, конечно, можно считать признаком близости двух элементов сам факт попадания их в одно и то же множество разбиения.

Задача оценки степени различия разных разбиений одного и того же конечного множества имеет довольно широкий спектр приложений. При решении подобных задач можно использовать такие характеристики, как расстояние Кульбака — Лейблера (см., например, [4, гл. 14]) или взаимная информация разбиений [5, с. 104–105]. Хотя эти характеристики и не являются метриками на семействе разбиений, но с помощью специальных приёмов (симметризации и т. п.) на их основе можно построить метрики. Несколько в стороне лежат методы, основанные на так называемых редакционных расстояниях, схожих с расстоянием Левенштейна [6]. Здесь принадлежность элементов множества разным элементам разбиения кодируется с помощью набора букв, в котором элементам одного множества присваиваются одинаковые буквы, а далее рассчитывается количество замен букв, путём совершения которых набор букв одного разбиения может быть самым быстрым способом переведён в буквы другого разбиения. Алгоритмы для вычисления таких расстояний можно найти в [7]. К подобным метрикам можно также отнести расстояния Джаро и Джаро — Винклера (см. [8]). Общие подходы к определению метрик на семействе разбиений рассматриваются в [9]. Там же обсуждаются и вероятностные интерпретации различных метрик, в том числе и основной метрики настоящей работы.

Для оценки степени близости разбиений A и B одного и того же множества далее будем использовать кластерную метрику d [10]:

$$d(A,B) = \sum_{x\in U} |a_{i(x)} \Delta b_{j(x)}|. \tag{1}$$

Здесь символом Δ обозначена симметрическая разность множеств

$$a\Delta b = (a \setminus b) \cup (b \setminus a),$$

под $b_{j(x)}$ понимается то из множеств набора B, в котором оказывается x, а через $|c|$ обозначается число элементов конечного множества c.

В силу дискретного характера рассматриваемой задачи понятно, что множество всех возможных значений метрики d на семействе разбиений U конечно. В [10] замечено, что наибольшее возможное её значение равно $n(n-1)$ и достигается лишь в том случае, когда одно из разбиений каждый элемент U объявляет отдельным множеством, а второе является одноэлементным набором. В [10] для этих двух разбиений введены следующие обозначения:

$$\underline{U} = \{\{x_1\}, \ldots, \{x_n\}\}, \quad \overline{U} = \{U\}.$$

Из определения (1) ясно, что значениями d могут служить только целые неотрицательные числа. Основной целью работы является изучение возможных минимальных ненулевых значений данной метрики, которую иногда будем называть просто расстоянием, в случае, когда одно из разбиений фиксировано, а также выяснение всех возможных вариантов строения второго разбиения, которое удалено от первого на такое минимальное расстояние.

2. Несколько предварительных и технических результатов

В [10] приведена и более простая в применении формула, чем (1):

$$d(A,B) = \sum_{i,j} |a_i \cap b_j| \cdot |a_i \Delta b_j|.$$

Здесь сумма берётся по всем возможным парам a_i, b_j, которые можно составить из множеств двух изучаемых наборов.

Если имеются два разбиения $A = \{a_1, \ldots, a_k\}$, $B = \{b_1, \ldots, b_m\}$ множества U, то набор множеств

$$\{a_i \cap b_j : i = 1, \ldots, k,\ j = 1, \ldots, m\},$$

из которого исключены все пустые пересечения, также является разбиением U. Полученный таким образом набор обозначим AB и назовём пересечением разбиений A и B. Для произвольного набора конечных множеств $A = \{a_1, \ldots, a_k\}$ пусть

$$\mathrm{sq}(A) = \sum_{i=1}^{k} |a_j|^2.$$

В [11] для вычисления расстояния d получена следующая формула:

$$d(A,B) = \mathrm{sq}(A) + \mathrm{sq}(B) - 2\mathrm{sq}(AB). \tag{2}$$

Оказывается, что изучение значений, которые может принимать сумма квадратов натуральных чисел, для нашей задачи весьма важно.

Лемма 1 (о максимуме суммы квадратов). Пусть натуральные числа n, f, z_1, $\ldots$, z_f таковы, что $z_1 + \ldots + z_f = n$, $f \leqslant n$. Тогда величина

$$S(f, z_1, \ldots, z_f) = \sum_{i=1}^{f} z_i^2$$

при каждом фиксированном f достигает своего максимума тогда и только тогда, когда все z_i, кроме, возможно, одного из них, равны 1. Этот максимум равен

$$M(f) = (n - f + 1)^2 + f - 1$$

и монотонно убывает с ростом f.

Доказательство. Пусть, скажем, $z_i > z_j$. Тогда в силу неравенства

$$(z_i + 1)^2 + (z_j - 1)^2 > z_i^2 + z_j^2$$

величина $S(f, z_1, \ldots, z_f)$ строго возрастает при перемещении единицы в сторону большего слагаемого. Таким образом, если число слагаемых менять нельзя, то максимальное значение S достигается, например, когда $z_1 = n-f+1$, $z_2 = 1, \ldots, z_f = 1$. Проверка монотонности $M(f)$ при $1 \leqslant f \leqslant n$ элементарна. ■

Условимся писать $A \subset B$ и говорить, что разбиение B содержит разбиение A, если любое из множеств, составляющих разбиение A, является подмножеством какого-то множества из B. Тогда для каждого из множеств $a \in A$ может быть выбрана часть разбиения B, являющаяся разбиением a. В частности, $AB \subset B$, $AB \subset A$. Нам понадобятся следующие два простых следствия (2):

Лемма 2. Если $A \subset B$, то $d(A, B) = \mathrm{sq}(B) - \mathrm{sq}(A)$.

Лемма 3. $d(A, B) = d(A, AB) + d(AB, B)$.

Утверждение леммы 3 можно интерпретировать как расположение пересечения двух разбиений на прямолинейном отрезке, соединяющем разбиения A и B в метрическом пространстве разбиений. Некоторое развитие такого подхода, приводящее к выводу о том, что метрика (1) согласована с частичным порядком по включению на семействе всех разбиений, реализовано в [12].

Лемма 4. Пусть разбиение B получено из разбиения $A = \{a_1, \ldots, a_k\}$ перенесением одного элемента $x \in U$ из a_t в a_s. Тогда

$$d(A, B) = 2(|a_t| + |a_s| - 1).$$

Доказательство. Применим (2):

$$d(A, B) = \mathrm{sq}(A) + \left(\mathrm{sq}(A) - |a_t|^2 - |a_s|^2 + (|a_t| - 1)^2 + (|a_s| + 1)^2\right) - \\ -2\left(\mathrm{sq}(A) - |a_t|^2 + (|a_t| - 1)^2 + 1\right).$$

После этого осталось лишь раскрыть скобки. ■

При рассмотрении таких A, B, как в лемме 4, множество a_t условимся называть донором, а a_s — реципиентом элемента x.

Рассмотрим набор неотрицательных целых чисел $g_1, \ldots, g_N$. Пусть среди них имеется ровно n ненулевых. Обозначив эти n чисел $q_1, \ldots, q_n$, положим

$$Q(g_1, \ldots, g_N) = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} q_i q_j, \ n \geqslant 2,$$

а при $n \leqslant 1$ будем считать, что $Q(g_1, \ldots, g_N) = 0$.

Лемма 5. Если в наборе целых неотрицательных чисел $g_1, \ldots, g_N$ имеется ровно n ненулевых, $n \geqslant 2$, то

$$1 + Q(g_1, \ldots, g_N) \geqslant \sum_{i=1}^{N} g_i. \tag{3}$$

Доказательство. Пусть список $q_1, \ldots, q_n$ содержит все ненулевые числа набора. Заметив, что $Q(g_1, \ldots, g_N) = Q(q_1, \ldots, q_n)$ и $\sum\limits_{i=1}^{N} g_i = \sum\limits_{i=1}^{n} q_i$, будем действовать индукцией по n. При $n = 2$ неравенство

$$1 + q_1 q_2 \geqslant q_1 + q_2 \tag{4}$$

очевидно, если $q_1 = 1$. Предположив, что $1 + kq_2 \geqslant k + q_2$, получаем

$$1 + (k+1)q_2 = 1 + kq_2 + q_2 \geqslant k + q_2 + 1 = (k+1) + q_2,$$

что доказывает справедливость (4). Теперь предположим, что (3) выполнено при некотором $n = k$. Тогда

$$1 + Q(q_1, \ldots, q_{k+1}) = 1 + Q(q_1, \ldots, q_k) + q_{k+1} \sum_{j=1}^{k} q_j \geqslant \sum_{j=1}^{k} q_j + q_{k+1},$$

что завершает доказательство (3). ■

Далее будем считать, что разбиение A состоит из множеств $a_1, \ldots, a_k$, а разбиение B — из множеств $b_1, \ldots, b_m$. Введём в рассмотрение $g_{i,j} = |a_i \cap b_j|$. Тогда

$$|a_i| = \sum_{j=1}^{m} g_{i,j},\ i = 1, \ldots, k;\ |b_j| = \sum_{i=1}^{k} g_{i,j},\ j = 1, \ldots, m. \tag{5}$$

Среди $g_{i,j}$ могут содержаться нули, но в каждой из сумм (5) есть по крайней мере одно ненулевое слагаемое. Обозначим количества таких слагаемых в этих суммах через $N(a_i), N(b_j)$ соответственно.

Лемма 6. Если A и B различны, то $d(A, B) \geqslant 2$.

Доказательство. Используя (2), запишем

$$d(A, B) = (\mathrm{sq}(A) - \mathrm{sq}(AB)) + (\mathrm{sq}(B) - \mathrm{sq}(AB)),$$

причём обе разности неотрицательны по лемме 2. Следовательно, хотя бы одна из них не равна нулю. Пусть это вторая разность. Тогда из

$$\mathrm{sq}(B) - \mathrm{sq}(AB) = \sum_{j=1}^{m} \left(\left(\sum_{i=1}^{k} g_{i,j} \right)^2 - \sum_{i=1}^{k} g_{i,j}^2 \right)$$

вытекает, что хотя бы одно из слагаемых в выписанной сумме положительно. Но, согласно лемме 1, это означает, что одно из $N(b_j)$ не меньше 2. Взяв в соответствующей сумме (5) два ненулевых слагаемых, скажем g_1, g_2, видим, что

$$d(A, B) \geqslant \left(\sum_{i=1}^{k} g_{i,j} \right)^2 - \sum_{i=1}^{k} g_{i,j}^2 = 2Q(g_{1,j}, \ldots, g_{1,k}) \geqslant 2g_1 g_2 \geqslant 2.$$

Лемма 6 доказана. ■

Рассмотрим произвольное разбиение A множества U. Для $x \in U$ через $\mathbf{A}(x)$ обозначим семейство всех разбиений, полученных из A перемещением x из $a_{i(x)}$ в другое множество из A или выделением x в новое одноэлементное множество.

Лемма 7. Пусть A и B — два различных разбиения U. Тогда найдётся такой $x \in U$ и такое разбиение $A' \in \mathbf{A}(x)$, что $d(A, A') \leqslant d(A, B)$.

Доказательство. Сделаем сначала два допущения:

1) среди множеств первого разбиения нашлись два, a_1 и a_2, такие, что $N(a_1), N(a_2) \geqslant 2$;
2) $\mathrm{sq}(B) - \mathrm{sq}(AB) \neq 0$.

Тогда, как показано в доказательстве леммы 6, $\mathrm{sq}(B) - \mathrm{sq}(AB) \geqslant 2$, откуда

$$d(A, B) = \mathrm{sq}(A) - \mathrm{sq}(AB) + \mathrm{sq}(B) - \mathrm{sq}(AB) \geqslant \mathrm{sq}(A) - \mathrm{sq}(AB) + 2. \tag{6}$$

Дважды применяя лемму 5, получаем

$$d(A, B) \geqslant 2Q(g_{1,1}, \ldots, g_{1,m}) + 2Q(g_{2,1}, \ldots, g_{2,m}) + 2 \geqslant 2(|a_1| + |a_2| - 1),$$

что завершает доказательство в сделанных допущениях, поскольку правая часть последнего неравенства равна расстоянию между A и разбиением, полученным из него перенесением любого из элементов a_1 в a_2 или наоборот.

Пусть нарушается первое из допущений. Если все $N(a_i) = 1$, то каждое множество из A пересекается ровно с одним множеством из B, что означает $A \subset B$. Тут каждое множество из B может быть разбито на какие-то множества из A. При этом хотя бы в одном таком разбиении должно найтись не менее двух элементов, так как иначе $A = B$. Пусть $b_1 \supset a_1 \cup a_2$. Тогда

$$d(A, B) \geqslant |b_1|^2 - |a_1|^2 - |a_2|^2 \geqslant 2|a_1| \cdot |a_2| \geqslant 2|a_1| > 2(|a_1| - 1),$$

что, согласно лемме 4, означает возможность построить A', отделяя один из элементов a_1 в новое одноэлементное множество. Если и a_1, и a_2 оказались одноэлементными, требуемый эффект достигается объединением их в одно двухэлементное множество (в этом случае $d(A, A') = 2$ и $d(A, B)$, согласно лемме 6, не меньше этого значения).

Если только $N(a_1) \geqslant 2$, отделим в новое одноэлементное множество один из элементов a_1, результат приняв за A'. При этом из леммы 5 вытекает

$$d(A, B) \geqslant 2Q(g_{1,1}, \ldots, g_{1,m}) \geqslant 2(|a_1| - 1) = d(A, A').$$

Наконец, предположим, что $\mathrm{sq}(B) - \mathrm{sq}(AB) = 0$. Привлекая лемму 2, приходим к выводу, что тогда $B = AB$, т. е. $B \subset A$. На этот раз каждое из множеств A образуется объединением некоторых из $b_1, \ldots, b_m$, причём, чтобы не допустить совпадения разбиений, хотя бы одно a_i должно содержать не менее двух таких множеств. Тогда $N(a_i) \geqslant 2$, а этот случай только что был рассмотрен. ■

3. Ближайшее разбиение

Сначала займёмся поиском ближайшего к A среди тех разбиений B, для которых $A \not\subset B$. Из этого условия, в частности, следует, что $d(A, AB) \neq 0$. Поэтому для рассматриваемого случая из леммы 3 вытекает строгое неравенство $d(A, B) > d(A, AB)$. Заменим любое найденное B на AB. При этом расстояние уменьшится, следовательно, нужное B обязательно таково, что $B \subset A$. Таким образом, для его построения следует разбить какие-то из множеств, составляющих A, на дизъюнктные части. Лемма 7 показывает, что ближайшее разбиение всегда получается перемещением одного элемента. При этом, согласно лемме 4, множества, между которыми перемещается этот единственный элемент, должны содержать минимально возможные количества элементов.

Таким образом, реципиент должен быть пустым, а вот донор не может содержать менее двух элементов. Заметим, что требуемого донора не существует только в случае, когда $A = \underline{U}$, а для такого разбиения, очевидно, нет ни одного B с нужным условием. Согласно лемме 4, расстояние между найденным и исходным разбиением равно

$$d_0 = 2(n_A - 1), \tag{7}$$

где n_A — минимальное число элементов множеств A, большее 1.

Перейдём к поиску ближайшего разбиения с условием $B \supset A$. Из проведённого рассуждения понятно, что A должно получаться отделением одного элемента от некоторого множества из B, если только это возможно. Итак, если в A имеется хотя бы одно одноэлементное множество, то B получается объединением этого множества с тем из остальных множеств A, которое имело наименьшее число элементов. Если это множество также было одноэлементным, то искомое разбиение по лемме 4 удалено от исходного на расстояние 2, иначе, с учётом (7) и того, что новый донор содержит $n_A + 1$ элемент, на величину $2n_A$, что больше, чем d_0 при $n_A > 2$, поэтому не является минимальным. Тем не менее значение d_0 в (7) может быть равным 2, как и при объединении двух одноэлементных множеств, в случае, когда $n_A = 2$.

Если в A нет ни одного одноэлементного множества, то любое разбиение $B \supset A$ будет заведомо дальше от A, чем построенное «внутреннее» разбиение. Действительно, построение требуемого B должно будет сопровождаться перемещением более чем одного элемента, тогда как ранее перемещался единственный $x \in U$. Вывод следует из леммы 7.

Пусть $M(k; A)$ — количество тех множеств в разбиении A, которые состоят ровно из k элементов. Резюмируем проведённые рассуждения.

Теорема 1. Пусть $M(1; A) \geqslant 2$. Если $M(2; A) = 0$, то ближайшее к A разбиение B получается заменой двух любых одноэлементных множеств на их объединение. Если $M(2; A) \geqslant 1$, то, кроме описанного способа, можно разбить любое двухэлементное множество A на два одноэлементных. Во всех указанных вариантах $d(A, B) = 2$.

Пусть $M(1; A) \leqslant 1$, a — любое из минимальных по числу элементов неодноэлементных множеств A. Тогда ближайшее к A разбиение B получается выделением одного из элементов a в новое множество и $d(A, B) = 2(n_A - 1)$, где n_A — число элементов a. С помощью этой процедуры могут быть построены все разбиения, ближайшие к A.

Заметим, что ближайшее к A разбиение обязательно либо строго содержится в нём, либо содержит его. Это вновь подтверждает заключение [12] о том, что метрика d согласована со структурой решётки на семействе всех разбиений.

Подсчёт количества ближайших разбиений происходит параллельно алгоритму их формирования. Следует только учесть, что отделение любого из элементов двухэлементного множества всегда даёт один и тот же результат, тогда как для множества из большего числа элементов число разных результатов отделения равно числу элементов множества.

Следствие 1. Число $l(A)$ разбиений, ближайших к разбиению A, вычисляется следующим образом:

$$l(A) = \begin{cases} C^2_{M(1;A)} + M(2; A), & M(1; A) \geqslant 2; \\ n_A M(n_A; A), & M(1; A) \leqslant 1, M(2; A) = 0; \\ M(2; A), & M(1; A) \leqslant 1, M(2; A) \neq 0. \end{cases}$$

В некоторых исследованиях в качестве допустимых могут рассматриваться только те разбиения, которые содержат фиксированное число множеств. Так бывает, например, в случае, когда каждое из рассматриваемых разбиений исследователь получает при помощи алгоритма k-средних, который часто применяется в приложениях и постоянно совершенствуется [13]. При таком предположении полученный результат нуждается в пересмотре — каждое из найденных ближайших разбиений имеет иное количество составляющих его множеств, чем исходное. Но леммы 4 и 7 позволяют произвести требуемый пересмотр довольно легко: для построения ближайшего к данному разбиению необходимо переместить один элемент между двумя множествами исходного разбиения с минимальными количествами элементов. Запрещённым оказывается лишь случай, когда реципиент оказывается пустым. Сформулируем результат.

Упорядочим множества, составляющие разбиение A, по возрастанию числа их элементов. Каждому множеству присвоим ранг, считая, что множества, имеющие одинаковое число элементов, получают одинаковые ранги. Через k_j будем обозначать количество элементов в множестве с рангом j. С учётом введённых ранее обозначений количество множеств разбиения A, имеющих ранг j, равно $M(k_j; A)$.

Теорема 2. Пусть $A \neq \underline{U}, \overline{U}$. Если $k_1 = 1$ или $M(k_1; A) = 1$, то произвольное B, ближайшее к A среди разбиений, состоящее из такого же числа множеств, образуется перенесением одного элемента из множества ранга 2 в произвольное множество ранга 1. При этом

$$d(A, B) = 2(k_2 + k_1 - 1). \tag{8}$$

Иначе ближайшее разбиение требуемого типа образуется перемещением одного элемента между произвольными двумя множествами ранга 1, причём

$$d(A, B) = 2(2k_1 - 1). \tag{9}$$

Ясно, что для разбиений $\underline{U}, \overline{U}$ задача не имеет решений. Поскольку в (8) $k_2 \geqslant 2$, а расстояние (9) возникает лишь при $k_1 \geqslant 2$, то из теоремы следует, что $d(A, B) \geqslant 4$. Это совпадает с результатом, полученным ранее в [10].

Следствие 2. Пусть $A \neq \underline{U}, \overline{U}$. Число разбиений $l_k(A)$, удаленных от заданного разбиения A на минимальное расстояние и имеющее то же число множеств k, может быть вычислено следующим образом:

$$l_k(A) = \begin{cases} k_2 M(k_2; A) M(k_1; A), & k_1 = 1 \text{ или } M(k_1; A) = 1; \\ k_1^2 C^2_{M(k_1;A)}, & k_1 \neq 1,\ M(k_1; A) \geqslant 2. \end{cases}$$

4. Обсуждение. Пример применения

Способ получения ближайшего к некоторому фиксированному разбиению, а также полученные в п. 3 количества ближайших разбиений можно рассматривать как первый шаг к построению статистического критерия для определения значимости отличий друг от друга разных разбиений. Такой критерий можно использовать для решения многих практических задач.

Предположим, задано некоторое разбиение A, которое назовём основным. Например, оно было получено методами, которым мы доверяем, или предложено квалифицированными экспертами. Пусть в результате применения новых методов к тем же данным получено другое разбиение B. Если различия разбиений A и B оказываются статистически незначимыми, то это может являться основанием для внедрения новых методов в исследовательскую практику.

Можно предложить применение подобного рассуждения и для нового решения задач сокращения размерности в задачах кластерного анализа. Если исключение одного или нескольких формирующих показателей не приводит к существенному изменению итогового разбиения, то эти показатели можно исключить без существенных потерь информации.

Допустим, что для основного разбиения найдены все значения, принимаемые $d(A, C)$ для всех возможных разбиений C, а также повторности каждого из этих значений. Это означает, что каждое возможное значение расстояния d встречается известное число n_d раз. Известно [14], что число разбиений множества из n элементов на непустые подмножества задаётся числом Белла, которое равно сумме чисел Стирлинга второго рода:

$$B_n = \sum_{m=1}^{n} S(n, m).$$

Тогда в предположении, что разбиение B могло оказаться произвольным, вероятность получить более удалённое от A разбиение равна

$$Q(B) = \frac{1}{B_n} \sum_{d>d(A,B)} n_d, \tag{10}$$

и именно это число следует рассматривать как меру значимости различия рассматриваемых двух разбиений (или вероятность того, что они близки).

Если число множеств в разбиении B может быть только тем же, что и в разбиении A, то следует составить таблицу всех возможных расстояний и их повторностей только для таких разбиений. При этом полное число допустимых разбиений равно $S(n, k)$, если основное разбиение состоит из k множеств.

Для примера рассмотрим множество из пяти пациентов с достоверно установленными тремя диагнозами (тромбоз глубоких вен, тромбоэмболия легочной артерии и их сочетание). Второй строкой в табл. 1 задано основное разбиение A множества пациентов.

Таблица 1

Диагнозы и генотип

Пациенты	A	B	C	D	E
Диагноз	1	2	1	3	2
Генотип	1	3	2	2	3

Изучим разбиение множества этих же пациентов, задаваемое их генотипом по гену F5 (фактор Лейден, свертываемость крови); обозначим: 1 — отсутствие патологического гена в обеих аллелях (нормозигота), 2 — наличие патологии в одной аллели (гетерозигота), 3 — патологический ген в обеих аллелях (гомозигота). Данные приведены в третьей строке табл. 1. Расстояние d между двумя этими разбиениями равно 4. Все возможные расстояния от основного разбиения и их повторности приведены в табл. 2.

Таблица 2

Расстояния и повторности

d	0	2	4	6	8	10	12	16	Всего
n_d	1	2	7	14	15	4	8	1	52

Отсюда формула (10) приводит к $Q(B) = 42/52 \approx 0{,}81$, что означает довольно высокую вероятность схожести двух разбиений. Это даёт повод для заключения о существенной сцепленности генотипа и диагноза. Если вместо изучения трёх возможных генотипов второе разбиение свести к констатации наличия или отсутствия патологии в генотипе, тем самым объединив множества, элементы которых соответствуют 2 и 3 в третьей строке табл. 1, то получается $d = 8$, откуда $Q(B) = 13/52 = 0{,}25$, что приводит к выводу о гораздо меньшей надёжности такой «более грубой» формы представления данных.

Конечно, уверенный вывод обычно делают, если соответствующая вероятность не менее 0,95 или не более 0,05, но в примере для наглядности взята выборка слишком малого объёма, по которой надёжные выводы сделать заведомо невозможно.

Заключение

В работе изучена структура метрического пространства на семействе всех разбиений конечного множества. Для каждого из возможных разбиений полностью описано строение разбиений, удалённых от фиксированного разбиения на минимальное расстояние в специальной кластерной метрике. Рассчитано количество таких ближайших соседей для произвольного конкретного разбиения. В качестве приложения результатов предложен новый статистический критерий для установления значимости различий двух разбиений одного и того же множества.

Автор выражает благодарность рецензенту за ценные замечания и указание ряда альтернативных способов оценки различия двух разбиений, ранее автору неизвестных.

ЛИТЕРАТУРА

1. *Brualdi R. A.* Introductory Combinatorics. 5th ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2017. 624 p.
2. *Bender E. A. and Williamson S. G.* Foundations of Combinatorics with Applications. Mineola, NY: Dover Publ., 2006. 480 p. `www.math.ucsd.edu/~ebender/CombText/ch-11.pdf`
3. *Birkhoff G.* Lattice Theory. 3rd ed. Providence, Rhode Island: AMS, 1991. 420 p.
4. *Press W. H., Teukolsky S. A., Vetterling W. T., and Flannery B. P.* Numerical Recipes: The Art of Scientific Computing. 3rd ed. Cambridge University Press, 2007. 1235 p.
5. *Яглом А. М., Яглом И. М.* Вероятность и информация. 3-е изд. М.: Наука, 1973. 513 с.
6. *Левенштейн В. И.* Двоичные коды с исправлением выпадений, вставок и замещений символов // ДАН СССР. 1965. Т. 163. Вып. 4. С. 845–848.
7. *Гасфилд Д.* Строки, деревья и последовательности в алгоритмах. Информатика и вычислительная биология. СПб.: Невский Диалект БВХ-Петербург, 2003. 654 с.
8. *Cohen W. W., Rawikumar P., and Fienberg S. E.* A comparison of string distance metrics for name-matching tasks // Proc. IIWEB'03, Acapulco, Mexico: AAAI Press, 2003. P. 73–78.
9. *Каграманян А. Г., Машталир В. П., Скляр Е. В., Шляхов В. В.* Метрические свойства разбиений множеств произвольной природы // Докл. НАН Украины. 2007. Т. 6. С. 35–39.
10. *Дронов С. В.* Одна кластерная метрика и устойчивость кластерных алгоритмов // Известия АлтГУ. 2011. Т. 69. № 1/2. С. 32–35.
11. *Dronov S. V. and Evdokimov E. A.* Post-hoc cluster analysis of connection between forming characteristics // Model Assisted Statistics Appl. 2018. V. 13. No. 2. P. 183–192.
12. *Дронов С. В.* Кратчайшие маршруты семейства кластерных разбиений // Труды семинара по геометрии и математическому моделированию. 2017. № 3. С. 4–12.
13. *Gribel D. and Vidal T.* HG-means: A scalable hybrid metaheuristic for minimum sum-of-squares clustering // Pattern Recognition. 2019. V. 88. No. 1. P. 569–583.

14. *Riordan J.* Introduction to Combinatorial Analysis. Mineola, NY: Dover Publ., 2006. 256 p.

REFERENCES

1. *Brualdi R. A.* Introductory Combinatorics. 5th ed. Upper Saddle River, NJ, Pearson Prentice Hall, 2017. 624 p.
2. Foundations of Combinatorics with Applications. Mineola, NY, Dover Publ., 2006. 480 p. www.math.ucsd.edu/~ebender/CombText/ch-11.pdf
3. *Birkhoff G.* Lattice Theory. 3rd ed. Providence, Rhode Island, AMS, 1991. 420 p.
4. *Press W. H., Teukolsky S. A., Vetterling W. T., and Flannery B. P.* Numerical Recipes: The Art of Scientific Computing. 3rd ed. Cambridge University Press, 2007. 1235 p.
5. *Yaglom A. M. and Yaglom I. M.* Veroyatnost i Informatsiya [Probability and Information], 3rd ed. Moscow, Nauka Publ., 1973. 513 p. (in Russian)
6. *Levenshteyn V. I.* Dvoichnyye kody s ispravleniyem vypadeniy, vstavok i zameshcheniy simvolov [Binary codes for correcting dropouts, inserts, and symbol substitutions]. Reports of the USSR Academy of Sciences, 1965, vol. 163, no. 4, pp. 845–848. (in Russian)
7. *Gasfild D.* Stroki, Derevia i Posledovatelnosti v Algoritmakh. Informatika i Vychislitelnaya Biologiya [Lines, Trees, and Sequences in Algorithms. Computer Science and Computational Biology]. St. Petersburg, Nevskiy Dialekt BVKh-Peterburg, 2003. 654 p. (in Russian)
8. *Cohen W. W., Rawikumar P., and Fienberg S. E.* A comparison of string distance metrics for name-matching tasks. Proc. IIWEB'03, Acapulco, Mexico, AAAI Press, 2003, pp. 73–78.
9. *Kagramanyan A. G., Mashtalir V. P., Sklyar E. V., and Shlyakhov V. V.* Metricheskiye svoystva razbiyeniy mnozhestv proizvolnoy prirody [Metric properties of partitions of sets of arbitrary nature]. Reports of the Academy of Sciences of Ukraine, 2007, vol. 6, pp. 35–39. (in Russian)
10. *Dronov S. V.* Odna klasternaya metrika i ustoychivost klasternykh algoritmov [One cluster metric and the stability of cluster algorythms]. Izvestiya AltGU, 2011, vol. 69, no. 1/2, pp. 32–35. (in Russian)
11. *Dronov S. V. and Evdokimov E. A.* Post-hoc cluster analysis of connection between forming characteristics. Model Assisted Statistics Appl., 2018, vol. 13, no. 2, pp. 183–192.
12. *Dronov S. V.* Kratchayshie marshruty semeystva klasternykh razbieniy [The shortest routes in the family of the cluster partitions]. Workshop on Geometry and Mathematical Modeling, 2017, no. 3, pp. 4–12. (in Russian)
13. *Gribel D. and Vidal T.* HG-means: A scalable hybrid metaheuristic for minimum sum-of-squares clustering. Pattern Recognition, 2019, vol. 88, no. 1, pp. 569 – 583.
14. *Riordan J.* Introduction to Combinatorial Analysis. Mineola, NY, Dover Publ., 2006. 256 p.

UDC 519.7 DOI 10.17223/20710410/47/2

A NOTE ON THE PROPERTIES OF ASSOCIATED BOOLEAN FUNCTIONS OF QUADRATIC APN FUNCTIONS[1]

A. A. Gorodilova

Sobolev Institute of Mathematics, Novosibirsk, Russia
Novosibirsk State University, Novosibirsk, Russia

E-mail: gorodilova@math.nsc.ru

Let F be a quadratic APN function in n variables. The associated Boolean function γ_F in $2n$ variables ($\gamma_F(a,b)=1$ if $a\neq \mathbf{0}$ and equation $F(x)+F(x+a)=b$ has solutions) has the form $\gamma_F(a,b)=\Phi_F(a)\cdot b+\varphi_F(a)+1$ for appropriate functions $\Phi_F:\mathbb{F}_2^n\to\mathbb{F}_2^n$ and $\varphi_F:\mathbb{F}_2^n\to\mathbb{F}_2$. We summarize the known results and prove new ones regarding properties of Φ_F and φ_F. For instance, we prove that degree of Φ_F is either n or less or equal to $n-2$. Based on computation experiments, we formulate a conjecture that degree of any component function of Φ_F is $n-2$. We show that this conjecture is based on two other conjectures of independent interest.

Keywords: *a quadratic APN function, the associated Boolean function, degree of a function.*

Introduction

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. Let $\mathbf{0}$ denote the zero vector of $\mathbb{F}_2^n$ and $\mathbf{1}$ denote the vector with all 1s. By «+» we denote the coordinate-wise sum modulo 2 for vectors from $\mathbb{F}_2^n$. Let $x\cdot y=x_1y_1+\ldots+x_ny_n$ denote the *inner product* of vectors $x=(x_1,\ldots,x_n), y=(y_1,\ldots,y_n)\in\mathbb{F}_2^n$; $x\preceq y$ if $x_i\leqslant y_i$ for all $i=1,\ldots,n$; and $\mathrm{wt}(x)=\sum\limits_{i=1}^{n}x_i$ denote the *Hamming weight* of $x\in\mathbb{F}_2^n$. A set $M\subseteq\mathbb{F}_2^n$ forms a *linear subspace* if $x+y\in M$ for any $x,y\in M$; the *dimension* of M, $\dim(M)$, is the maximal number of linearly independent over $\mathbb{F}_2$ vectors from M. We consider *vectorial Boolean functions* $F:\mathbb{F}_2^n\to\mathbb{F}_2^m$, $F=(f_1,\ldots,f_m)$, where $f_i:\mathbb{F}_2^n\to\mathbb{F}_2$, $i=1,\ldots,m$, is a *coordinate* function of F. The *algebraic normal form* (ANF) of F is the following unique representation: $F(x)=\sum\limits_{I\in\mathcal{P}(N)}a_I\left(\prod\limits_{i\in I}x_i\right)$, where $\mathcal{P}(N)$ is the power set of $N=\{1,\ldots,n\}$ and $a_I\in\mathbb{F}_2^m$. The *algebraic degree* of F is degree of its ANF: $\deg(F)=\max\{|I|:\ a_I\neq\mathbf{0},\ I\in\mathcal{P}(N)\}$. Function of algebraic degree at most 1 are called *affine* (they are *linear* in case of $F(\mathbf{0})=\mathbf{0}$). Functions of algebraic degree 2 are called *quadratic*. The *Walsh transform* $W_f:\mathbb{F}_2^n\to\mathbb{Z}$ of a Boolean function $f:\mathbb{F}_2^n\to\mathbb{F}_2$ is defined as $W_f(u)=\sum\limits_{x\in\mathbb{F}_2^n}(-1)^{f(x)+u\cdot x}$. For F the *Walsh spectrum* consists of all *Walsh coefficients* $W_{F_v}(u)$, $u\in\mathbb{F}_2^n$, $v\in\mathbb{F}_2^m$, $v\neq\mathbf{0}$, where $F_v=v\cdot F$ is a *component* Boolean function of F.

A function F from $\mathbb{F}_2^n$ to itself is called *almost perfect nonlinear* (APN) (according to K. Nyberg [1]) if for any $a,b\in\mathbb{F}_2^n$, $a\neq\mathbf{0}$, equation $F(x)+F(x+a)=b$ has at most two solutions. APN functions are of special interest for using as S-boxes in block ciphers

[1]The work was funded by RFBR (projects no. 18-31-00479, 18-07-01394); by the program of fundamental scientific researches of the SB RAS no. I.5.1, project no. 0314-2019-0017; Regional Mathematical Center NSU and Laboratory of cryptography JetBrains Research.

due to their optimal differential characteristics. Despite the fact that APN functions are intensively studied (see, for example, the book of L. Budaghyan [2], surveys of A. Pott [3], M. M. Glukhov [4], and M. E. Tuzhilin [5]), there are a lot of open problems on finding new constructions, classifications, etc.

In [6], C. Carlet, P. Charpin, and V. Zinoviev introduced the *associated Boolean function* $\gamma_F : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ for a given vectorial Boolean function F from $\mathbb{F}_2^n$ to itself; $\gamma_F(a, b) = 1$ if and only if $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions.

Two functions are called *differentially equivalent* [7] (or γ-equivalent according to K. Boura et al. [8]), if their associated Boolean functions coincide. The problem of describing the differential equivalence class of an APN function remains open even for quadratic case. That is why we are interested in obtaining some properties of γ_F. We will focus on quadratic APN functions.

Let F be a quadratic APN function. Then the set $B_a(F) = \{F(x) + F(x + a) : x \in \mathbb{F}_2^n\}$ is a linear subspace of dimension $n - 1$ or its complement for a nonzero $a \in \mathbb{F}_2^n$. Using this fact, γ_F can be uniquely represented in the form

$$\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1,$$

where $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$ are defined from $B_a(F) = \{y \in \mathbb{F}_2^n : \ \Phi_F(a) \cdot y = \varphi_F(a)\}$ for all $a \neq \mathbf{0}$; and $\Phi_F(\mathbf{0}) = \mathbf{0}$, $\varphi_F(\mathbf{0}) = 1$. Note that $B_a(F)$ is a linear subspace if and only if $\varphi_F(a) = 0$. It is easy to see that $(F(x) + F(x + a) + F(a) + F(\mathbf{0})) \cdot \Phi_F(a) = \mathbf{0}$ for all $x \in \mathbb{F}_2^n$ by definition.

In this paper we study the properties of functions Φ_F and φ_F.

1. Properties of φ_F and Φ_F

In this section we summarize known results and present new ones about properties of Φ_F and φ_F. As it usually happens the cases of even and odd number of variables are different.

1.1. The image set of Φ_F

According to [9], let us denote $A_v^F = \{a \in \mathbb{F}_2^n : \Phi_F(a) = v\}$.

Theorem 1 [6, 9]. Let F be a quadratic APN function in n variables.

1) If n is odd, then Φ_F is a permutation.
2) If n is even, then the preimage Φ_F of any nonzero vector is a linear subspace of even dimension together with the zero vector.

Note that state 1 in Theorem 1 means also that γ_F is a bent function of Maiorana—McFarland type (readers may find details regarding bent functions in [10]).

Corollary 1. Let F be a quadratic APN function. Then Φ_F takes an odd number of distinct nonzero values.

Proof. By definition of Φ_F, we have $\Phi_F(\mathbf{0}) = \mathbf{0}$.

If n is odd, then Φ_F is a permutation [6]. Hence, the proposition holds.

Let n be even. It is known [9] that the preimage set $A_v^F = \{x \in \mathbb{F}_2^n : \Phi_F(x) = v\}$ for any nonzero $v \in \mathbb{F}_2^n$ represents a linear subspace of even dimension together with the zero vector. Let $\Phi_F \in \{\mathbf{0}, v_1, \ldots, v_m\}$, where v_i, $i = 1, \ldots, m$, are pairwise distinct nonzero vectors. We need to prove that m is odd. We have

$$2^n - 1 = |A_{v_1}^F| + \ldots + |A_{v_m}^F| = 2^{\lambda_1} - 1 + \ldots + 2^{\lambda_m} - 1 = 2^{\lambda_1} + \ldots + 2^{\lambda_m} - m,$$

where λ_i, $i = 1, \ldots, m$, are nonzero even numbers. Since $2^n - 1$ is odd, then m is also odd. ■

1.2. The degree of φ_F

Proposition 1. Let F be a quadratic APN function in n variables, n is even. Then $\deg(\varphi_F) = n$, or, equivalently, $\mathrm{wt}(\varphi_F)$ is odd.

Proof. It is known [9] that $A_v^F \cup \{\mathbf{0}\}$ is a linear subspace of even dimension if n is even for any nonzero $v \in \mathbb{F}_2^n$. Also [9], there exists $c_v \in \mathbb{F}_2^n$ such that $\varphi_F|_{A_v^F} = c_v \cdot x|_{A_v^F}$. Hence, $\mathrm{wt}(\varphi_F|_{A_v^F})$ is an even number equal to 0 or $2^{\dim(A_v^F \cup \{\mathbf{0}\})-1}$ for any nonzero v and $\varphi_F(\mathbf{0}) = 1$ by definition. Thus, $\mathrm{wt}(\varphi_F)$ is odd. It is widely known that $\mathrm{wt}(f)$ is odd if and only if $\deg(f) = n$ for any Boolean function in n variables. ■

The case of odd n remains open. Based on our computational experiments for all known quadratic APN functions of not more than 11 variables, we can formulate the following

Conjecture 1. Let F be a quadratic APN function in n variables, n is odd. Then $\deg(\varphi_F) < n$, or, equivalently, $\mathrm{wt}(\varphi_F)$ is even.

1.3. The degree of Φ_F

Theorem 2 [7]. Let F be a quadratic APN function in n variables, $n \geqslant 3$, n is odd. Then $\deg(\Phi_F) \leqslant n - 2$.

The following theorem contains a similar bound for even n.

Theorem 3. Let F be a quadratic APN function in n variables, $n \geqslant 4$, n is even. Then each coordinate function of Φ_F is represented as $(\Phi_F)_i(x) = f_i(x) + \lambda_i\big(x_2 \dots x_n + + x_1x_3 \dots x_n + \dots + x_1x_2 \dots x_{n-1} + x_1 \dots x_n\big)$, where $\deg(f_i) \leqslant n - 2$ and $\lambda_i \in \mathbb{F}_2$.

Proof. Let $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linear function. Then it is easy to see that

$$\gamma_{F+L}(a,b) = \gamma_F(a, b+L(a)) = (b+L(a))\cdot\Phi_F(a)+\varphi_F(a)+1 = b\cdot\Phi_F(a)+\varphi_F(a)+L(a)\cdot\Phi_F(a)+1.$$

Hence, $\Phi_{F+L} = \Phi_F$ and $\varphi_{F+L} = \varphi_F + L \cdot \Phi_F$. By Proposition 1, $\deg(\varphi_F) = \deg(\varphi_{F+L}) = n$, since $F+L$ is also a quadratic APN function. Thus, $\deg(L\cdot\Phi_F) < n$ for any linear function L.

Suppose that $\deg(\Phi_F) = n$. This means that there exists a coordinate function $(\Phi_F)_i$ of degree n. Let us represent

$$(\Phi_F)_i(x) = f_i(x) + a_1x_2 \dots x_n + a_2x_1x_3 \dots x_n + \dots + a_nx_1x_2 \dots x_{n-1} + x_1 \dots x_n,$$

where $\deg(f_i) \leqslant n - 2$ and $a_1, \dots, a_n \in \mathbb{F}_2$.

— If $a_j = 0$, then $\deg(L \cdot \Phi_F) = n$ for $L = (0, \dots, 0, x_j, 0, \dots, 0)$, where x_j is the i-th coordinate function of L. Hence, we get a contradiction.
— If $a_j = 1$ for all j, then it is easy to see that we will always have $\deg(L \cdot \Phi_F) < n$ for any linear function L.

Suppose that $\deg(\Phi_F) = n - 1$. Similarly,

$$(\Phi_F)_i(x) = f_i(x) + a_1x_2 \dots x_n + a_2x_1x_3 \dots x_n + \dots + a_nx_1x_2 \dots x_{n-1},$$

where at least one coefficient is equal to 1, say a_j. Then $\deg(L \cdot \Phi_F) = n$ for $L = (0, \dots, 0, x_j, 0, \dots, 0)$, where x_j is the i-th coordinate function of L. Hence, we get a contradiction.

Thus, $(\Phi_F)_i$ is of degree not more than $n - 2$ or all monomials of degree $n - 1$ and n are included in the ANF of $(\Phi_F)_i$. ■

Remark 1. For all known quadratic APN functions in not more than 11 variables, we computationally verified that

— for even n, the case $\deg((\Phi_F)_i) = n$ is not realized;

— any component function of Φ_F has degree exactly $n-2$.

Based on our computational experiments we can formulate the following

Conjecture 2. Let F be a quadratic APN function in n variables, $n \geqslant 3$. Then $\deg(v \cdot \Phi_F) = n-2$ for any nonzero $v \in \mathbb{F}_2^n$.

2. Does the equality $\deg(\Phi_F) = n-2$ hold?

In this section we study the following question: "Is conjecture 2 true or not?".

For example, consider an APN Gold function $F(x) = x^{2^k+1}$, $\gcd(n,k) = 1$ (the function is given as a function over the finite field of order 2^n). Its associated Boolean function is known [6]: $\gamma_F(a,b) = \mathrm{tr}((a^{2^k+1})^{-1}b) + \mathrm{tr}(1) + 1$ (here tr is the absolute trace function in the finite field of order 2^n). So, we have $\Phi_F(a) = (a^{2^k+1})^{-1}$, $\Phi_F(0) = 0$, and as it is easy to see $\deg(\Phi_F) = n-2$ (since it is well-known that the degree of a function $F(x) = x^d$ is equal to the 2-weight of the integer d modulo 2^n).

We wonder whether conjecture 2 is true or not for arbitrary n. Let us focus on the case of odd n since in this case we have the bound of Theorem 2. For even case, the consideration could be rather similar but with assumption that $\deg(\Phi_F)$ is not equal to n, that is only a conjecture up to now.

S t e p 1. Let F be a quadratic APN function of n variables, n is odd, $n \geqslant 5$; v be a nonzero vector from $\mathbb{F}_2^n$. We need to prove that $\deg(v \cdot \Phi_F) = n-2$ for any nonzero $v \in \mathbb{F}_2^n$.

We use the following widely known equality for counting the ANF coefficients of a Boolean function f in n variables:

$$g_f(a) = \Big(2^{\mathrm{wt}(a)-1} - 2^{\mathrm{wt}(a)-n-1} \sum_{b \preceq (a+\mathbf{1})} W_f(b)\Big) \bmod 2. \tag{1}$$

We need to show that there exists a vector a^v with $\mathrm{wt}(a^v) = n-2$ such that $g_{v\cdot\Phi_F}(a^v) = 1$. Equivalently, that there exist coordinates i, j, $1 \leqslant i \neq j \leqslant n$, such that

$$\sum_{b \preceq (a^v+\mathbf{1})} W_{v\cdot\Phi_F}(b) = W_{v\cdot\Phi_F}(\mathbf{0}) + W_{v\cdot\Phi_F}(e^i) + W_{v\cdot\Phi_F}(e^j) + W_{v\cdot\Phi_F}(e^i+e^j)$$

is not divided by 16 according to (1). Here e^i is the vector with 1 in the i-th coordinate and 0s in other coordinates. Let us introduce the following sets:

$$M^i = \{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0,\ x \cdot e^i = 0\},$$
$$M^j = \{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0,\ x \cdot e^j = 0\},$$
$$M^{ij} = \{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0,\ x \cdot (e^i+e^j) = 0\}.$$

Then, we have

$$\sum_{b \preceq (a^v+\mathbf{1})} W_{v\cdot\Phi_F}(b) = 4|M^i| - 2^n + 4|M^j| - 2^n + 4|M^{ij}| - 2^n =$$
$$= 4(|M^i| + |M^j| + |M^{ij}|) - 3\cdot 2^n = 4(2^{n-1} + 2|M_0^{ij}|) - 3\cdot 2^n = 8|M_0^{ij}| - 2^{n-1},$$

where $M_0^{ij} = \{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0,\ x \cdot e^i = 0,\ x \cdot e^j = 0\}$.

S t e p 2. Thus, we need to prove that there exist coordinates i, j, $1 \leqslant i \neq j \leqslant n$, such that $|M_0^{ij}|$ is odd (since we consider $n \geqslant 5$). From [7, prop. 7], we know that $M = \{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0\} = \bigcup_{\ell \in I} A_\ell$, where A_ℓ is a linear subspace of dimension 2,

and $A_\ell \cap A_k = \{\mathbf{0}\}$, $\ell, k \in I$, $\ell \neq k$. Since Φ_F is a permutation, then $|M| = 2^{n-1}$ and $|I| = (2^{n-1}-1)/3$.

Let us consider an arbitrary $A_\ell = \{\mathbf{0}, x^\ell, y^\ell, x^\ell + y^\ell\}$. Then for any distinct coordinates i, j of $x^\ell, y^\ell, x^\ell + y^\ell$ we have the following situations (without permutations of rows):

	ij		ij		ij		ij		ij
x^ℓ	00		00		00		00		01
y^ℓ	00	or	01	or	10	or	11	or	10
$x^\ell + y^\ell$	00		01		10		11		11

Hence, the number of $x^\ell, y^\ell, x^\ell + y^\ell$ together with $\mathbf{0}$ that belong to the set M_0^{ij} is equal to $1+3\cdot N_3^{ij}+1\cdot N_1^{ij}+0\cdot N_0^{ij}$, where $N_3^{ij}+N_1^{ij}+N_0^{ij} = |I| = (2^{n-1}-1)/3$, and N_k^{ij}, $k = 0, 1, 3$, is the number of A_ℓ, $\ell \in I$, having exactly k vectors with both coordinates i and j equal to 0. Thus, $|M_0^{ij}|$ is odd if and only if N_0^{ij} is odd.

S t e p 3. Now, we need to prove that there exist coordinates i, j, $1 \leqslant i \neq j \leqslant n$, such that N_0^{ij} is odd. We found the following interesting property (computationally verified for $n = 5$) that we formulate as a conjecture.

Conjecture 3. Let $M = \bigcup\limits_{\ell \in I} A_\ell$, where A_ℓ is a linear subspace of dimension 2, and $A_\ell \cap A_k = \{\mathbf{0}\}$, $\ell, k \in I$, $\ell \neq k$, $|I| = (2^{n-1}-1)/3$. Then the set M is a hyperplane $\{x \in \mathbb{F}_2^n : x_m = 0\}$ for some coordinate m if and only if the number of subspaces A_ℓ without elements having both coordinates i and j equal to 0 is even for any distinct coordinates i, j.

S t e p 4. If Conjecture 3 is true, then we need to prove that $M = \{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0\}$ cannot be a hyperplane $\{x \in \mathbb{F}_2^n : x_m = 0\}$ for some coordinate m.

Conjecture 4. Let F be a quadratic APN function in n variables, $n \geqslant 5$. Then $\{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0\}$ is not a linear subspace.

We computationally verified this property for all known quadratic APN functions for $n = 5, \ldots, 11$ and formulate the conjecture.

Thus, by proving Conjectures 3 and 4, we can prove the starting Conjecture 2. Unfortunately, each of them remains open up to now.

Conclusion

The following question is open: what properties must a Boolean function satisfy in order to be the associated function for some vectorial function? Even a partial answer to the question provides a potential method to find new APN functions if we can choose "admissible" Boolean functions as γ_F. For example, using the algorithm from [8] for reconstructing APN functions from its associated functions. Another reason why we study the properties of associated functions is that they may lead to new results in the differential equivalence classification of APN functions.

REFERENCES

1. *Nyberg K.* Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, LNCS, 1994, vol. 765, pp. 55–64.
2. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer International Publishing, 2014. 168 p.
3. *Pott A.* Almost perfect and planar functions. Designs, Codes and Cryptography, 2016, vol. 78, pp. 141–195.
4. *Glukhov M. M.* O priblizhenii diskretnykh funktsiy lineynymi funktsiyami [On the approximation of discrete functions by linear functions]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, no. 4, pp. 29–50. (in Russian)

5. *Tuzhilin M. E.* Pochti sovershennye nelineynye funktsii [APN-functions]. Prikladnaya Diskretnaya Matematika, 2009, no. 3 (5), pp. 14–20. (in Russian)
6. *Carlet C., Charpin P., and Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography, 1998, vol. 15, iss. 2, pp. 125–156.
7. *Gorodilova A.* On the differential equivalence of APN functions. Cryptography and Communications, 2019, vol. 11, iss. 4, pp. 793–813.
8. *Boura C., Canteaut A., Jean J., and Suder V.* Two notions of differential equivalence on Sboxes. Designs, Codes and Cryptography, 2019, vol. 87, iss. 2–3, pp. 185–202.
9. *Gorodilova A.* Lineynyy spektr kvadratichnykh APN-funktsiy [The linear spectrum of quadratic APN functions]. Prikladnaya Diskretnaya Matematika, 2016, no 4(34), pp. 5–16. (in Russian)
10. *Tokareva N.* Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015. 230 p.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

УДК 519.718

АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫЕ ПО НЕНАДЁЖНОСТИ СХЕМЫ В БАЗИСЕ, СОСТОЯЩЕМ ИЗ ФУНКЦИИ ВЕББА, В P_3 ПРИ НЕИСПРАВНОСТЯХ ТИПА 2 НА ВЫХОДАХ ЭЛЕМЕНТОВ[1]

О. Ю. Барсукова*, М. А. Алехина**

*Пензенский государственный университет, г. Пенза, Россия

**Пензенский государственный технологический университет, г. Пенза, Россия

Рассматривается реализация функций трёхзначной логики схемами из ненадёжных функциональных элементов в полном базисе, состоящем из функции Вебба. Предполагается, что элементы схемы переходят в неисправные состояния независимо друг от друга, подвержены однотипным константным неисправностям типа 2 на выходах. Доказано, что любую функцию трёхзначной логики можно реализовать схемой, функционирующей с ненадёжностью асимптотически не больше 3ε при $\varepsilon \to 0$. Найден класс функций (он содержит почти все функции трёхзначной логики), каждую из которых нельзя реализовать схемой, ненадёжность которой асимптотически меньше 3ε при $\varepsilon \to 0$. Таким образом, доказано, что почти любую функцию трёхзначной логики можно реализовать асимптотически оптимальной по надёжности схемой, функционирующей с ненадёжностью асимптотически равной 3ε при $\varepsilon \to 0$.

Ключевые слова: *функции трёхзначной логики, ненадёжные функциональные элементы, надёжность и ненадёжность схемы, синтез схем из ненадёжных элементов, неисправности на выходах элементов.*

DOI 10.17223/20710410/47/3

ASYMPTOTICALLY OPTIMAL IN UNRELIABILITY CIRCUITS IN THE BASIS CONSISTING OF THE WEBB FUNCTION IN P_3 UNDER FAULTS OF TYPE 2 AT THE OUTPUTS OF ELEMENTS

O. Yu. Barsukova*, M. A. Alekhina**

*Penza State University, Penza, Russia

**Penza State Technological University, Penza, Russia

E-mail: oksana.barsukova.71@gmail.com, alekhina@penzgtu.ru

We consider the realization of ternary logic functions by circuits from unreliable elements in full basis consisting of the Webb function. We assume that elements of the circuit pass to fault states independently of each other, and they are exposed to single-type constant faults of type 2 at the outputs. It is proved that any function of ternary

[1]Работа поддержана грантом РФФИ № 17-01-00451а.

logic can be realized by an asymptotically optimal in reliability circuit functioning with unreliability which is asymptotically no more 3*varepsilon* with $\varepsilon \to 0$. A class of functions is found (it contains almost all ternary logic functions), each of which cannot be implemented by a circuit whose unreliability is asymptotically less 3ε with $\varepsilon \to 0$. Thus, it is proved that almost any function of ternary logic can be implemented by an asymptotically optimal on reliability circuit operating with unreliability which is asymptotically equal to 3ε with $\varepsilon \to 0$.

Keywords: *ternary logic functions, unreliable functional elements, reliability and unreliability of circuit, synthesis of circuits from unreliable elements, faults at outputs of elements.*

Введение

В современной технике и математике в подавляющем большинстве случаев используется двузначная логика. Это исторически сложившееся положение предопределено её сравнительной простотой и сделало её применение предпочтительным (в сравнении с другими логическими системами) с технической и экономической точек зрения. Однако сложность решаемых задач, а следовательно и технических устройств, постоянно возрастает. Многозначная логика предоставляет более широкие возможности для разработки различных алгоритмов во многих областях. Она позволяет уменьшить как вычислительную сложность, так и размеры, число соединений в различных арифметико-логических устройствах, повысить плотность размещения элементов на схемах, найти альтернативные методы решения задач. Уже сейчас многозначная логика с успехом применяется при решении многих задач и во множестве технических разработок. Среди них различные арифметические устройства, системы искусственного интеллекта и обработки данных, обработка сложных цифровых сигналов и т. д.

Среди работ по многозначным логикам отметим работу [1], в которой функционирование реальных электронных схем описано с помощью функций трёхзначной логики, построен функционально полный в P_3 базис, на компромиссной основе согласованы математические и технические требования и интересы и рассмотрены некоторые аспекты синтеза электронных схем в этом базисе. Знакомство с [1] положило начало исследованиям по синтезу схем из ненадёжных элементов в том или ином полном конечном базисе как в P_3 [2], так и вообще в P_k ($k \geqslant 3$).

В предлагаемой работе рассматривается реализация функций трёхзначной логики схемами в базисе, состоящем из функции Вебба $V_3(x_1, x_2) = (\max\{x_1, x_2\} + 1) \bmod 3$, при однотипных константных неисправностях типа 2.

Задача синтеза надёжных схем в полном базисе, состоящем из функции Вебба, решена в P_3 [2] при инверсных неисправностях на выходах базисных элементов (когда на каждом входном наборе любого из базисных элементов вероятность появления неверного значения на выходе элемента одинакова). В [2] также доказаны верхняя и нижняя оценки ненадёжности схем в базисе $\{V_3(x_1, x_2)\}$, однако асимптотически эти оценки оказались различными, т. е. в [2] построены надёжные схемы, но асимптотически оптимальными по надёжности эти схемы не являются. В [3] при произвольном $k \geqslant 3$ в случае однотипных константных неисправностей типа 0 и типа $k-1$ в базисе, состоящем из функции Вебба $V_k(x_1, x_2) = (\max\{x_1, x_2\} + 1) \bmod k$, построены надёжные схемы, реализующие функции k-значной логики, получены верхние оценки ненадёжности этих схем. В случае неисправностей типа 0 на выходах элементов построенные схемы оказались не просто надёжными, а асимптотически оптимальными по надёжности.

В настоящем исследовании при однотипных константных неисправностях типа 2 на выходах элементов в базисе $\{V_3(x_1, x_2)\}$: 1) доказаны нетривиальные нижние оценки ненадёжности схем; 2) выявлен класс K функций трёхзначной логики, для которых найденные нижние оценки ненадёжности схем асимптотически равны ранее известным [3] верхним оценкам ненадёжности схем, т. е. любую функцию этого класса можно реализовать асимптотически оптимальной по надёжности схемой; 3) класс K содержит почти все функции трёхзначной логики.

Введём необходимые понятия и определения.

Пусть $n \in \mathbb{N}$, $P_3(n)$ — множество функций трёхзначной логики, каждая из которых зависит от переменных $x_1, \ldots, x_n$, т. е. функций $f(x_1, \ldots, x_n) : \{0, 1, 2\}^n \to \{0, 1, 2\}$. Обозначим через P_3 множество всех функций трёхзначной логики.

Считаем, что схема реализует функцию $f(x_1, x_2, \ldots, x_n)$, если при поступлении на входы схемы набора $\tilde{a}^n = (a_1, a_2, \ldots, a_n)$ при отсутствии неисправностей на её выходе появляется значение $f(\tilde{a}^n)$. Допустим, что все элементы схемы независимо друг от друга с вероятностью ε $(0 < \varepsilon < 1/2)$ переходят в неисправные состояния типа 2 на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему функцию трёхзначной логики, а в неисправном — константу 2.

Пусть схема S реализует функцию $f(\tilde{x}^n)$. Обозначим через $P_i(S, \tilde{a}^n)$ вероятность появления значения $i \in \{0, 1, 2\}$ на выходе схемы S при входном наборе $\tilde{a}^n$, а через $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n)$ — вероятность появления ошибки на выходе схемы S при входном наборе $\tilde{a}^n$, на котором $f(\tilde{a}^n) = \tau$. Ясно, что $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n) = P_{\tau+1}(S, \tilde{a}^n) + P_{\tau+2}(S, \tilde{a}^n)$ (в выражениях $\tau + 1$ и $\tau + 2$ сложение осуществляется по модулю 3). Например, если входной набор $\tilde{a}^n$ схемы S такой, что $f(\tilde{a}^n) = 0$ (т. е. при отсутствии неисправностей в схеме S на её выходе появляется значение 0), то вероятность ошибки на этом наборе равна $P_{f(\tilde{a}^n)\neq 0}(S, \tilde{a}^n) = P_1(S, \tilde{a}^n) + P_2(S, \tilde{a}^n)$.

Ненадёжностью схемы S будем называть число $P(S) = \max\{P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n)\}$, где максимум берется по всем входным наборам $\tilde{a}^n$ схемы S. *Надёжность* схемы S равна $1 - P(S)$.

Замечание 1. Заметим, что при неисправностях типа 2 ненадёжность базисного элемента равна ε.

Пусть $P_\varepsilon(f) = \inf P(S)$, где S — схема, реализующая $f(\tilde{x}^n)$. Схему A, реализующую f, назовём *асимптотически оптимальной по надёжности*, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

1. Верхняя оценки ненадёжности

В работе [3] получена верхняя оценка ненадёжности для схем, реализующих функции k-значной логики $(k \geqslant 3)$ при неисправностях типа $k - 1$ на выходах элементов, а именно доказано, что в базисе, состоящем из функции Вебба $V_k(x_1, x_2)=(\max\{x_1, x_2\}+1) \bmod k$, любую функцию $f \in P_k$ можно реализовать такой схемой S, что $P(S) \leqslant 3\varepsilon+c(k)\varepsilon^2$ при всех $\varepsilon \in (0, \varepsilon_0]$, где $\varepsilon_0 = 2^{-2^k}/(27k^8)$, $c(k) = 17{,}5\cdot 2^{2^k}$. Для $k = 3$ получается следующая верхняя оценка ненадёжности схем в P_3.

Теорема 1 [3]. Любую функцию $f \in P_3$ можно реализовать такой схемой S, что $P(S) < 3\varepsilon + 4480\varepsilon^2$ при всех $\varepsilon \in (0, \varepsilon_1]$, где $\varepsilon_1 = 2{,}2/10^8$.

Из теоремы 1 следует, что в полном базисе, состоящем из функции Вебба $V_3(x_1, x_2) = (\max\{x_1, x_2\} + 1) \bmod 3$, при однотипных константных неисправностях ти-

па 2 любую функцию из P_3 можно реализовать схемой, ненадёжность которой асимптотически (при $\varepsilon \to 0$) не больше 3ε.

2. Нижняя оценка ненадёжности

Для нахождения нижних оценок ненадёжности приведём ранее полученные результаты.

Лемма 1 [2]. Пусть $f(\tilde{x}^n)$ — произвольная функция, которая принимает три значения 0, 1, 2; S — любая схема, её реализующая; подсхема A схемы S содержит выход схемы S и реализует функцию $\varphi(\tilde{y}^m)$ с ненадёжностью $P(A) \leqslant 1/2$; $p_0 = \min\limits_{\tilde{b}_0^m} P_{\varphi(\tilde{b}_0^m)\neq 0}(A, \tilde{b}_0^m)$, где $\tilde{b}_0^m$ — такой входной набор схемы A, что $\varphi(\tilde{b}_0^m) = 0$; $p_1 = \min\limits_{\tilde{b}_1^m} P_{\varphi(\tilde{b}_1^m)\neq 1}(A, \tilde{b}_1^m)$, где $\tilde{b}_1^m$ — такой входной набор схемы A, что $\varphi(\tilde{b}_1^m) = 1$; $p_2 = \min\limits_{\tilde{b}_2^m} P_{\varphi(\tilde{b}_2^m)\neq 2}(A, \tilde{b}_2^m)$, где $\tilde{b}_2^m$ — такой входной набор схемы A, что $\varphi(\tilde{b}_2^m) = 2$. Тогда вероятности ошибок на выходе схемы S удовлетворяют следующим неравенствам:

$$P_{f(\tilde{a}^n)\neq 0}(S, \tilde{a}^n) \geqslant p_0, \text{ если } f(\tilde{a}^n) = 0,$$
$$P_{f(\tilde{a}^n)\neq 1}(S, \tilde{a}^n) \geqslant p_1, \text{ если } f(\tilde{a}^n) = 1,$$
$$P_{f(\tilde{a}^n)\neq 2}(S, \tilde{a}^n) \geqslant p_2, \text{ если } f(\tilde{a}^n) = 2.$$

Пусть в схеме S можно выделить подсхему D, которая имеет один вход, содержит выход схемы S и реализует либо тождественную функцию y, либо $(y+1) \bmod 3$, либо $(y+2) \bmod 3$, т. е. реализует некоторую функцию $(y+j) \bmod 3$, $j \in \{0, 1, 2\}$. Обозначим через C подсхему, получаемую из схемы S удалением подсхемы D (рис. 1).

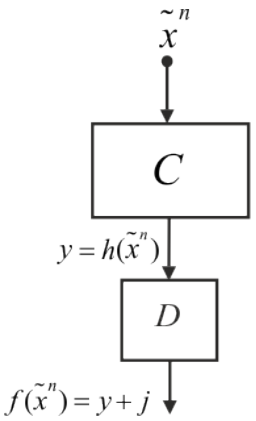


Рис. 1. Схема S

Будем говорить, что схема C *надёжнее* схемы S (и получается из схемы S удалением подсхемы D), если выполнено неравенство $P(C) < P(S)$.

Пусть $f(\tilde{x}^n)$ — функция, которая принимает три значения 0, 1, 2. Схему S, реализующую функцию $f(\tilde{x}^n)$, будем называть *bc-схемой*, если из неё нельзя получить более надёжную схему удалением подсхемы, содержащей выход схемы S и реализующей некоторую функцию $(y + j) \bmod 3$, $j \in \{0, 1, 2\}$.

Обозначим $h(\tilde{x}^n)$ функцию, которую реализует схема C (рис. 1); w_i, $i \in \{0, 1, 2\}$, — вероятность появления ошибки на выходе схемы D при поступлении на её вход значения i. Очевидно, $f(\tilde{x}^n) = (h(\tilde{x}^n) + j) \bmod 3$.

Лемма 2 [2]. Пусть схема S, ненадёжность которой равна $P(S)$, реализует функцию f и является bc-схемой. Пусть в схеме S (рис. 1) можно выделить подсхему D, имеющую один вход, содержащую выход схемы и реализующую некоторую функцию $(y + j) \bmod 3$, $j \in \{0, 1, 2\}$, с такими вероятностями ошибок w_0, w_1, w_2, что $0 < w_0 + w_1 + w_2 < 1$. Тогда верно неравенство

$$\min\left\{\frac{w_0}{w_0+w_1+w_2}, \frac{w_1}{w_0+w_1+w_2}, \frac{w_2}{w_0+w_1+w_2}\right\} \leqslant P(S).$$

Обозначим через $J_i(x)$ $(i \in \{0, 1, 2\})$ функцию, равную 2 при $x = i$ и 0 при $x \neq i$.

Лемма 3. При любом $n \in \mathbb{N}$ любую функцию $f(x_1, \ldots, x_k, \ldots, x_n)$ трёхзначной логики можно представить следующим образом:

1) при $k = 1$

$$f(x_1, x_2, \ldots, x_n) = J_0(x_1)\&f(0, x_2, \ldots x_n)\vee J_1(x_1)\&f(1, x_2, \ldots x_n)\vee J_2(x_1)\&f(2, x_2, \ldots, x_n);$$

2) при $k \in \{2, \ldots, n-1\}$

$$f(x_1, \ldots, x_{k-1}, x_k, x_{k+1}, \ldots, x_n) = J_0(x_k)\&f(x_1, \ldots, x_{k-1}, 0, x_{k+1}, \ldots, x_n)\vee$$
$$\vee J_1(x_k)\&f(x_1, \ldots, x_{k-1}, 1, x_{k+1}, \ldots, x_n) \vee J_2(x_k)\&f(x_1, \ldots, x_{k-1}, 2, x_{k+1}, \ldots, x_n);$$

3) при $k = n$

$$f(x_1, \ldots, x_{n-1}, x_n) = J_0(x_n)\&f(x_1, \ldots, x_{n-1}, 0)\vee$$
$$\vee J_1(x_n)\&f(x_1, \ldots, x_{n-1}, 1) \vee J_2(x_n)\&f(x_1, \ldots, x_{n-1}, 2).$$

Доказательство проводится непосредственной подстановкой различных значений переменной x_k в правые и левые части формул.

Обозначим через $K(n)$ множество функций трёхзначной логики, каждая из которых зависит от переменных $x_1, \ldots, x_n$ $(n \geqslant 3)$, принимает все три значения $0, 1, 2$ и не представима в виде $V_3(x_k, h(\tilde{x}^n))$, $V_3(x_k, h(\tilde{x}^n))+1$ или $V_3(x_k, h(\tilde{x}^n))+2$ $(k \in \{1, 2, \ldots, n\}$, $h(\tilde{x}^n)$ — произвольная функция трехзначной логики). Обозначим $K = \bigcup\limits_{n=3}^{\infty} K(n)$.

Замечание 2. Заметим, что в классе K не содержатся функции x_i $(i \in \mathbb{N})$, которые можно реализовать абсолютно надёжно, не используя функциональные элементы.

Теорема 2. $|K(n)| \geqslant 3^{3^n} - 3n3^{2\cdot 3^{n-1}} - 3 \cdot 2^{3^n}$.

Доказательство. Найдём число функций, представимых в виде $V_3(x_k, h(\tilde{x}^n))$. Для этого разложим функцию $V_3(x_k, h(\tilde{x}^n))$ по переменной x_k, используя лемму 3:

$$V_3(x_k, h(\tilde{x}^n)) = J_0(x_k)\&V_3(h(x_1, \ldots, 0, \ldots, x_n), 0) \vee J_1(x_k)\&V_3(h(x_1, \ldots, 1, \ldots, x_n), 1)\vee$$
$$\vee J_2(x_k) \ \& \ V_3(h(x_1, \ldots, 2, \ldots, x_n), 2) = J_0(x_k)\&\{\max[h(x_1, \ldots, 0, \ldots, x_n), 0] + 1\}\vee$$
$$\vee J_1(x_k)\&\{\max[h(x_1, \ldots, 1, \ldots, x_n), 1] + 1\} \vee J_2(x_k)\&\{\max[h(x_1, \ldots, 2, \ldots, x_n), 2] + 1\} =$$
$$= J_0(x_k)\&[h(x_1, \ldots, 0, \ldots, x_n) + 1] \vee J_1(x_k)\&\{\max[h(x_1, \ldots, 1, \ldots, x_n), 1] + 1\}.$$

Тогда число функций, представимых в виде $V_3(x_k, h(\tilde{x}^n))$, не больше $n \cdot 3^{3^{n-1}} \cdot 3^{3^{n-1}} = n3^{2\cdot 3^{n-1}}$.

Аналогично находится число функций, представимых в виде $V_3(x_k, h(\tilde{x}^n)) + 1$ или $V_3(x_k, h(\tilde{x}^n)) + 2$, их также не больше $n3^{2\cdot 3^{n-1}} + n3^{2\cdot 3^{n-1}} = 2n3^{2\cdot 3^{n-1}}$.

Теперь рассмотрим функции, принимающие не больше двух значений из множества $\{0,1,2\}$. Очевидно, их число не больше $\mathrm{C}_3^2 \cdot 2^{3^n} = 3 \cdot 2^{3^n}$.

Следовательно, число функций, не принадлежащих классу $K(n)$, не больше $3n3^{2\cdot 3^{n-1}} + 3 \cdot 2^{3^n}$. Поэтому $|K(n)| \geqslant 3^{3^n} - 3n3^{2\cdot 3^{n-1}} - 3 \cdot 2^{3^n}$. ■

Из теоремы 2 следует, что класс $K(n)$ содержит почти все функции из множества $P_3(n)$, поскольку $\lim\limits_{n\to\infty} (3n3^{2\cdot 3^{n-1}} + 3 \cdot 2^{3^n})/3^{3^n} = 0$.

Справедлива теорема о нижней оценке ненадёжности схем, реализующих функции из класса K.

Теорема 3. Пусть $f \in K$. Тогда для любой схемы S, реализующей f, верно неравенство $P(S) \geqslant 3\varepsilon - 6\varepsilon^2$ при всех $\varepsilon \in (0,\ 2{,}2 \cdot 10^{-8}]$.

Доказательство. Пусть $f \in K$, S — любая схема, реализующая f. Заметим, что схема S содержит хотя бы три элемента.

Для ненадёжности $P(S)$ схемы S верно одно из двух неравенств (см. теорему 1): либо $P(S) > 3\varepsilon + 4480\varepsilon^2$ (тогда утверждение теоремы верно), либо $P(S) \leqslant 3\varepsilon + 4480\varepsilon^2$.

Пусть $P(S) \leqslant 3\varepsilon + 4480\varepsilon^2$. Без ограничения общности схему S можно считать bc-схемой (иначе будем удалять из схемы S подсхемы, реализующие либо тождественную функцию y, либо функцию $y+1$, либо функцию $y+2$, и получать более надёжные схемы, реализующие функции $(f+j) \bmod 3$, $j \in \{0,1,2\}$, до тех пор, пока не получим bc-схему S'', для которой и проведём дальнейшие рассуждения, заменив S на S'').

Выделим в схеме S подсхему S', состоящую из трёх элементов и содержащую выход схемы S (это возможно, поскольку $f \in K$). Обозначим через E_1 функциональный элемент, содержащий выход схемы S. Поскольку $f \in K$, входы элемента E_1 не могут быть соединены с полюсами, а следовательно, соединены с выходами некоторых элементов схемы S. Возможны следующие варианты:

1. Пусть входы элемента E_1 соединены с выходами двух различных элементов E_2 и E_3.

1.1. Пусть ни выход элемента E_2 не соединён со входом элемента E_3, ни выход элемента E_3 не соединён со входом элемента E_2 (рис. 2, *а*) либо пусть выход одного из элементов, например E_3, соединён со входом другого элемента E_2 (рис. 2, *б*). Пусть входной набор схемы S' таков, что при отсутствии неисправностей в схеме S' на её выходе появляется значение 1 (такой набор найдётся, поскольку $f \in K$). Вычислим вероятность появления 1 на выходе схемы S' по формуле полной вероятности и получим $(1-\varepsilon)^3 = 1 - 3\varepsilon + 3\varepsilon^2 - \varepsilon^3$.

Тогда вероятность появления ошибки на выходе подсхемы S' равна $p_1 = 3\varepsilon - 3\varepsilon^2 + \varepsilon^3$. По лемме 1 получаем неравенство $P(S) \geqslant 3\varepsilon - 3\varepsilon^2 + \varepsilon^3 \geqslant 3\varepsilon - 6\varepsilon^2$, т. е. утверждение теоремы верно.

1.2. Пусть выход одного из элементов, например E_2, соединён с каждым из двух входов другого элемента E_3 (рис. 2, *в*). Тогда схема S реализует функцию, принимающую только два значения 0 и 2, что противоречит условию $f \in K$.

2. Пусть элементы E_2 и E_3 совпадают, т. е. оба входа элемента E_1 соединены с выходом некоторого элемента E_2. Ни один из входов элемента E_2 не может быть соединён с полюсом, поскольку $f \in K$. Следовательно, оба входа элемента E_2 соединены с выходами некоторых элементов E_4 и E_5.

2.1. Пусть элементы E_4 и E_5 различны. Рассмотрим подсхему A из четырёх элементов E_1, E_2, E_4 и E_5 (рис. 3), причём возможные варианты подсхем S^* представлены на рис. 2. Вычислим вероятность правильного значения 2 на выходе подсхемы A при поступлении на входы соответствующего набора $\tilde{a}$ при отсутствии

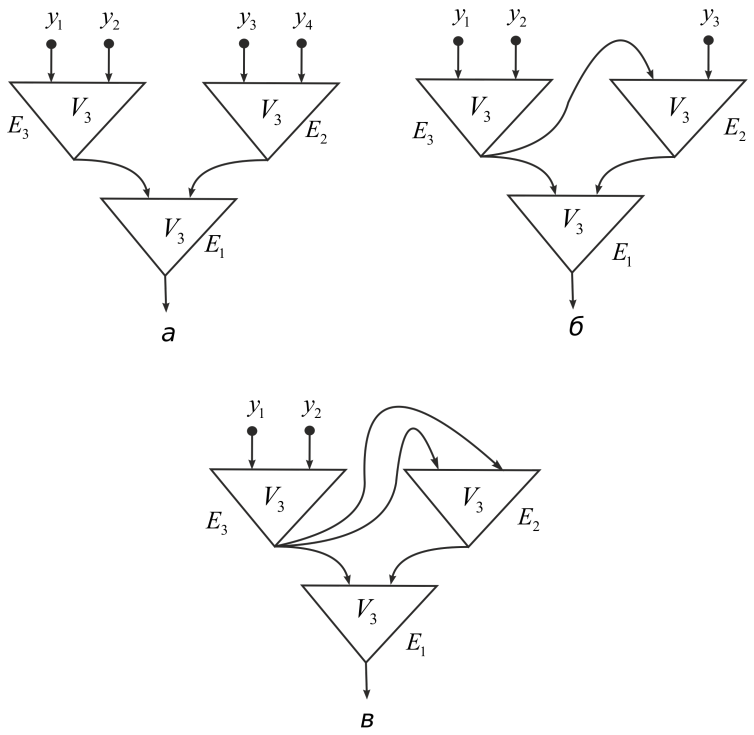


Рис. 2

неисправностей: $P_2(A, \tilde{a}) = (1 - p_1)1 + p_1\varepsilon$, где $p_1 = 3\varepsilon - 3\varepsilon^2 + \varepsilon^3$ — вероятность ошибки подсхемы из трёх элементов E_2, E_4 и E_5, найденная в п. 1 доказательства. Поэтому вероятность ошибки на выходе подсхемы A равна $1 - P_2(A, \tilde{a}) = p_1(1 - \varepsilon) = 3\varepsilon - 6\varepsilon^2 + 4\varepsilon^3 - \varepsilon^4 \geqslant 3\varepsilon - 6\varepsilon^2$. Поскольку набор $\tilde{a}$ — любой, на котором подсхема A принимает значение 2, по лемме 1 верно неравенство $P(S) \geqslant 3\varepsilon - 6\varepsilon^2$.

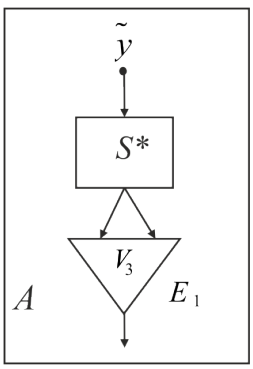


Рис. 3. Подсхема A

2.2. Пусть элементы E_4 и E_5 совпадают. Рассмотрим подсхему D из двух элементов E_1 и E_2, имеющую один вход и один выход (см. рис. 1). Вычислим вероятности ошибок на выходе этой подсхемы:

1) при поступлении на вход D значения 0 вероятность появления правильного значения 2 равна $1 - w_2 = 1 - \varepsilon + \varepsilon^2$, поэтому $w_2 = \varepsilon - \varepsilon^2$;
2) при поступлении на вход D значения 1 вероятность появления правильного значения 0 равна $1 - w_0 = 1 - \varepsilon$, поэтому $w_0 = \varepsilon$;

3) при поступлении на вход D значения 2 вероятность появления правильного значения 1 равна $1 - w_1 = (1-\varepsilon)^2$, поэтому $w_1 = 2\varepsilon - \varepsilon^2$.

Тогда $w_0 + w_1 + w_2 = 4\varepsilon - 2\varepsilon^2$ и

$$\min\left\{\frac{w_0}{w_0+w_1+w_2}, \frac{w_1}{w_0+w_1+w_2}, \frac{w_2}{w_0+w_1+w_2}\right\} = \frac{\varepsilon-\varepsilon^2}{4\varepsilon-2\varepsilon^2} = \frac{1-\varepsilon}{4-2\varepsilon}.$$

По лемме 2 при $\varepsilon \in (0,\ 2{,}2 \cdot 10^{-8}]$ верно неравенство $\dfrac{1-\varepsilon}{4-2\varepsilon} \leqslant 3\varepsilon + 4480\varepsilon^2$, что не так, поскольку $\dfrac{1-\varepsilon}{4-2\varepsilon} \geqslant (1-\varepsilon)/4 > 0{,}8/4 = 0{,}2$, а $3\varepsilon + 4480\varepsilon^2 < 0{,}1$. Полученное противоречие означает, что подсхема D не может быть подсхемой схемы S. ■

Следовательно, любая схема, реализующая функцию $f \in K$, функционирует с ненадёжностью, которая асимптотически (при $\varepsilon \to 0$) не меньше 3ε.

Таким образом, в полном базисе, состоящем из функции Вебба $V_3(x_1, x_2) = (\max\{x_1, x_2\} + 1) \bmod 3$, при неисправностях типа 2 на выходах элементов почти любую функцию можно реализовать асимптотически оптимальной по надёжности схемой, функционирующей с ненадёжностью, асимптотически (при $\varepsilon \to 0$) равной 3ε.

ЛИТЕРАТУРА

1. *Виноградов Ю. А.* О синтезе трехзначных схем // Математические вопросы кибернетики. М.: Наука, 1991. Вып. 3. С. 187–198.
2. *Барсукова О. Ю.* Синтез надежных схем, реализующих функции двузначной и трехзначной логик: дис. ... канд. физ.-мат. наук. Пенза, 2014. 87 с.
3. *Алехина М. А., Барсукова О. Ю.* О надёжности схем в базисе, состоящем из функции Вебба, в P_k при неисправностях типа 0 и типа $k-1$ на выходах элементов // Прикладная дискретная математика. 2019. № 44. С. 56–64.

REFERENCES

1. *Vinogradov Yu. A.* O sinteze trekhznachnykh skhem [About the synthesis of ternary logic circuits]. Math. Problems of Cybernetics. Moscow, Nauka Publ., 1991, vol. 3, pp. 187–198.(in Russian)
2. *Barsukova O. Yu.* Sintez nadezhnykh skhem, realizuyushchikh funktsii dvuznachnoy i trekhznachnoy logik [Synthesis of reliable schemes that implement two-valued and three-valued logics functions]. PhD Thesis, Penza, 2014. 87 p. (in Russian)
3. *Alekhina M. A. and Barsukova O. Yu.* O nadezhnosti skhem v bazise, sostoyashchem iz funktsii Vebba, v P_k pri neispravnostyakh tipa 0 i tipa $k-1$ na vykhodakh elementov [About reliability of circuits in the basis consisting of the Webb function in P_k under failures of 0 type and $k-1$ type at the outputs of elements.] Prikladnaya Diskretnaya Matematika, 2019, no. 44, pp. 56–64.

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.728

ТЕОРЕТИЧЕСКИ ЭФФЕКТИВНОЕ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНОЕ УНИВЕРСАЛЬНОЕ КОДИРОВАНИЕ ЧАСТИЧНО ОПРЕДЕЛЁННЫХ ИСТОЧНИКОВ

Л. А. Шоломов

ФИЦ «Информатика и управление» РАН, г. Москва, Россия

Частично определённый источник порождает независимо с некоторыми вероятностями символы заданного основного алфавита и неопределённый символ. Кодирование источника должно обеспечить точное воспроизведение основных символов, а неопределённые символы допускают замену (доопределение) любыми основными символами. Кодирование считается эффективным, если имеет полиномиальную оценку сложности кодирования и декодирования. Оно асимптотически оптимально, если обеспечивает среднюю длину кода, асимптотически равную энтропии источника. Кодирование универсально, если оно не зависит от вероятностей символов источника. Описан метод эффективного асимптотически оптимального универсального кодирования частично определённых источников.

Ключевые слова: *недоопределённый источник, частично определённый источник, универсальное кодирование, полиномиальный метод, энтропия источника, квазиэнтропия слова, частотный класс, комбинаторная энтропия, представительное множество.*

DOI 10.17223/20710410/47/4

THEORETICALLY EFFECTIVE ASYMPTOTICALLY OPTIMAL UNIVERSAL CODING OF PARTIALLY DEFINED SOURCES

L. A. Sholomov

Federal Research Center "Computer Science and Control" of RAS, Moscow, Russia

E-mail: levshol@mail.ru

Let $A_0 = \{a_i : i \in M\}$ be a finite alphabet of basic symbols, $A = \{a_T : T \in \mathcal{T}\}$, $\mathcal{T} \subseteq 2^M$, — an alphabet of underdetermined symbols. Any symbol a_i, $i \in T$, is considered to be a specification of the symbol a_T. The symbol a_M, denoted by $*$, is called indefinite. An underdetermined source X generates symbols $a_T \in A$ independently with probabilities p_T. The entropy of the source X is the quantity

$$\mathcal{H}(X) = \min_Q \left(- \sum_{T \in \mathcal{T}} p_T \log \sum_{i \in T} q_i \right),$$

where the minimum is taken over the set of probability vectors $Q = (q_i,\ i \in M)$, $\log x = \log_2 x$. For source X, we consider separable block coding with a block length of n. Encoding K of underdetermined words $v \in A^n$ should ensure that the code $K(v)$

of word v allow one to recover some specification of v. Coding is universal if it is independent of the probabilities p_T, $T \in \mathcal{T}$. Characteristic of coding quality is average code length

$$\bar{l}^{(n)} = \frac{1}{n} \sum_{v \in A^n} p(v)|K(v)|,$$

where $p(v) = p_{T_1} \dots p_{T_n}$ is the probability of the appearance of the word $v = a_{T_1} \dots a_{T_n}$ at the source output, $|K(v)|$ is the codeword length for v.
Earlier, the author established that for arbitrary source X and for any block coding method, the inequality $\bar{l}^{(n)} \geqslant \mathcal{H}(X)$ holds, and that there is universal block coding, for which $\bar{l}^{(n)} \leqslant \mathcal{H}(X) + \mathrm{O}\Big(\dfrac{\log n}{n}\Big)$. The upper bound here is obtained by random coding which only establishes existence of the estimation, but does not provide an appropriate algorithm. Important for applications are issues of complexity of procedures. Coding method considered theoretically effective if the complexities of coding and decoding are estimated by a some polynomial of the size n of problem. This paper presents a polynomial coding method for underdetermined sources whose alphabet has the form $A = A_0 \cup \{*\} = \{a_0, a_1, \dots, a_{m-1}, *\}$. Such sources are called partially defined. For them, entropy can be explicitly expressed:

$$\mathcal{H}(P) = (1 - p_*) \log(1 - p_*) - \sum_{i=0}^{m-1} p_i \log p_i.$$

The main content of the paper is the proof of the following result.
For a partially defined source X, there is an universal method of block coding that provides an estimate of the average length of the code

$$\bar{l}^{(n)} \leqslant \mathcal{H}(P) + \mathrm{O}\Big(\frac{\log\log n}{\log^{1/2} n}\Big)$$

and allows you to encode and decode using RAM-programs with complexity $\mathrm{O}(n^2)$. An analogue of this result is also valid for other types of undetermined sources whose entropy is explicitly representable.

Keywords: *underdetermined source, partially defined source, universal coding, polynomial method, source entropy, quasientropy of a word, frequency class, combinatorial entropy, representative set.*

Введение

Под недоопределёнными данными понимаются последовательности недоопределённых символов. Каждому такому символу соответствует некоторое множество символов основного алфавита, любым из которых он может быть замещен (доопределён). Считается, что последовательности порождаются источником, генерирующим символы недоопределённого алфавита A независимо с некоторыми вероятностями. Задача кодирования такого источника состоит в том, чтобы каждой порождаемой им последовательности сопоставить двоичный код, позволяющий восстановить некоторое доопределение последовательности (но не её саму). Рассматривается блоковое кодирование источника, при котором последовательности разбиваются на блоки некоторой длины n и производится кодирование блоков — слов длины n в алфавите A. Качество кодирования характеризуется средней по блокам длиной кода, приходящейся на символ источника [1]. Кодирование универсально, если оно не зависит от вероятностей символов.

С недоопределённым источником X связывается энтропия $\mathcal{H}(X)$ [2], роль которой подобна роли энтропии Шеннона для полностью определённых источников. В [3] (см. также [2]) доказано, что при любом способе кодирования недоопределённого источника X средняя длина кода не меньше $\mathcal{H}(X)$ и что существует его универсальное кодирование, обеспечивающее среднюю длину кода, асимптотически равную $\mathcal{H}(X)$. Этот результат получен с использованием метода случайного кодирования, который лишь устанавливает факт существования указанной асимптотически оптимальной оценки средней длины кода, но не обеспечивает соответствующего алгоритма и потому не позволяет утверждать что-либо нетривиальное о сложности кодирования.

Вопросы сложности процедур важны для приложений. В теории сложности принято считать процедуру эффективной, если она является детерминированной и её сложность (число элементарных операций) оценивается сверху полиномом от размера задачи. Это понятие эффективности фактически не зависит от модели вычислений, ибо для основных моделей переход от одной из них к другой связан с не более чем полиномиальным изменением числа операций. Применительно к задачам кодирования теоретическая эффективность подразумевает, что полиномиальными должны быть процедуры кодирования и декодирования. Чтобы иметь возможность говорить о степени полинома в оценке сложности, следует уточнить модель вычислений. В качестве модели будем использовать РАМ-программу [4] с подходящим набором операций. Отметим, что оценки сложности носят асимптотический характер и теоретическая эффективность ещё не означает, что процедуры являются «практически хорошими» при реальных значениях параметров.

В данной работе представлен полиномиальный (квадратичный) метод асимптотически оптимального кодирования недоопределённых источников, имеющих более частный вид. Они порождают лишь полностью определённые и неопределённые символы и названы частично определёнными. Отметим, что в приложениях чаще всего встречаются недоопределённые данные такого вида. В случае двоичного основного алфавита понятия недоопределённого и частично определённого источников совпадают.

Распространение описанного в работе эффективного метода кодирования частично определённых источников на случай недоопределённых источников общего вида затруднено тем, что в общем случае энтропия $\mathcal{H}(X)$ задана неявно как минимум некоторой функции и её явное выражение удаётся найти лишь в редких случаях, к которым относится и случай частично определённых источников. Явное выражение энтропии используется при кодировании. Метод применим и к другим типам источников с явно выразимой энтропией (например, к рассмотренным в [5]). Отметим, что в предлагаемом эффективном методе остаточный член в асимптотической оценке средней длины кода значительно хуже, чем в неэффективном методе из [3].

Приведём известные результаты, относящиеся к проблематике данной работы. Имеется тесная связь рассмотренной в работе вероятностной задачи кодирования недоопределённого источника с детерминированной задачей кодирования класса слов с заданными частотами вхождения недоопределённых символов (см. лемму 10 данной работы). В терминах [6] можно детерминированную задачу кодирования недоопределённого слова понимать как задачу построения двоичной программы вычисления некоторого его доопределения. В случае двоичных недоопределённых слов в качестве способа вычисления довольно естественно рассматривать схему из логических элементов (неветвящуюся программу [4, 7]), реализующую булеву функцию, последовательность значений которой совпадает с этим словом. Двоичное представление этой схемы можно считать кодом слова, и длина этого кода определяется сложностью схемы.

Идея воспринимать схему как код реализуемой функции восходит к К. Шеннону [8] и лежит в основе развитого им мощностного метода получения нижних оценок сложности схем. О. Б. Лупанов [9] разработал общий метод синтеза схем — принцип локального кодирования, позволивший получить асимптотически точные оценки сложности для многих классов функций и систем. В частности, этим методом Лупанов реализовал асимптотически наилучшим образом полностью определённые функции от n аргументов, принимающие N_1 единичных значений (для всех N_1, удовлетворяющих минимальному естественному ограничению). Построение асимптотически наилучших схем этот принцип связывает с кодированием функций, удовлетворяющим ряду требований. Некоторые приёмы такого кодирования использованы в данной работе.

Работа Э. И. Нечипорука [10] об асимптотически наилучшей реализации недоопределённых двоичных матриц с заданным числом булевых элементов вентильными схемами глубины 2 явилась пионерской в области синтеза недоопределённых управляющих систем. Метод этой работы с ипользованием принципа локального кодирования позволяет строить асимптотически наилучшие схемы из логических элементов для булевых функций от n аргументов, определённых на N наборах при больших значениях $N = N(n)$. В [11] предложены методы повышения степени определённости функций путём сведения к функциям от меньшего числа аргументов, определённым примерно на том же числе наборов. Это позволило решить задачу наилучшего синтеза схем в широком диапазоне значений параметра N. Окончательный результат получен в [12], где использован другой способ повышения степени определённости функций.

Детерминированной задаче кодирования двоичных частично определённых слов с заданными частотами появления символов соответствует задача схемной реализации частично определённой функции, заданной на N наборах и принимающей N_0 нулевых и N_1 единичных значений. Полное решение задачи построения асимптотически наилучших реализаций при всех значениях параметров (N, N_0, N_1), удовлетворяющих минимальному ограничению, получено А. В. Чашкиным [13]. Результаты для некоторых диапазонов значений (N, N_0, N_1) были опубликованы ранее в [14 – 16]. Вклад каждой из этих работ в решение общей задачи охарактеризован в [13]. К этой проблематике примыкает результат из [17] об асимптотически минимальной реализации вентильными схемами глубины 2 многозначных частично определённых матриц с заданными частотами символов.

В работе [18] рассмотрены функции, значениями которых являются недоопределённые символы общего вида, и описан асимптотически наилучший метод их схемной реализации (при некотором двоичном представлении символов). Другое решение той же задачи — более структурированное — имеется в [19]. Рассматриваемая в этих работах постановка задачи связана с несколько упрощённым понятием энтропии, которое использует лишь мощности доопределяющих множеств для символов и не учитывает их структуру. Это понятие согласовано с задачей протыкания системы комбинаторных кубоидов [18], но в задаче кодирования недоопределённых слов и источников даёт завышенные значения.

В перечисленных работах решается в разных постановках задача построения асимптотически наилучших по сложности схем для недоопределённых функций, но не рассматриваются вопросы сложности самих процедур построения схем. Развитые там методы включают либо вероятностные, либо неэффективные комбинаторные построения и потому не могут служить основой эффективных методов кодирования недоопределённых слов. Исключение составляет работа [20], в которой описан эффективный способ получения двоичной программы для вычисления булевой функции, заданной

на N наборах. Эта программа имеет асимптотически минимальную длину и строится со сложностью, почти квадратично зависящей от размера исходных данных.

1. Основные понятия и формулировка результата

Задан конечный алфавит $A_0 = \{a_0, a_1, \ldots, a_{m-1}\}$ *основных* символов. Каждому непустому подмножеству T множества $M = \{0, 1, \ldots, m-1\}$ соответствует символ a_T, называемый *недоопределённым*. Основные символы a_i будем также рассматривать как недоопределённые символы, соответствующие одноэлементным подмножествам $\{i\} \subseteq M$. *Доопределением символа* a_T считается всякий основной символ a_i, $i \in T$. Символ a_M, доопределимый любым основным символом, называется *неопределённым* и обозначается $*$.

Выделена система $\mathcal{T} \subseteq 2^M$ некоторых непустых множеств $T \subseteq M$ и ей сопоставлен *недоопределённый алфавит* $A = \{a_T : T \in \mathcal{T}\}$. Под *доопределением слова* $v = a_{T_1} \ldots a_{T_l} \in A^l$ понимается любое слово $w = a_{i_1} \ldots a_{i_l} \in A_0^l$, полученное из v заменой каждого символа каким-либо его доопределением.

Рассматривается источник X, порождающий символы $a_T \in A$ независимо с вероятностями p_T, $\sum\limits_{T \in \mathcal{T}} p_T = 1$. Он обозначается (A, P), где $P = (p_T,\ T \in \mathcal{T})$, и называется *недоопределённым источником*. Задавшись некоторым набором вероятностей $Q = (q_i,\ i \in M)$ основных символов, введём функцию

$$\mathcal{H}(P, Q) = -\sum_{T \in \mathcal{T}} p_T \log \sum_{i \in T} q_i \tag{1}$$

(здесь и дальше логарифмы двоичные). *Энтропией источника* X назовём величину

$$\mathcal{H}(X) = \mathcal{H}(P) = \min_{Q} \mathcal{H}(P, Q). \tag{2}$$

Для недоопределённых источников она играет роль, подобную той, какую для полностью определённых источников играет энтропия Шеннона (подробнее см. в [2]).

Дальше считаем, что вероятности p_T всех символов $a_T \in A$ строго положительны, ибо в случае $p_T = 0$ символ a_T можно исключить из рассмотрения (а множество T — из $\mathcal{T}$). Очевидно, что $\mathcal{H}(X) \geqslant 0$. Нас интересует случай, когда энтропия $\mathcal{H}(X)$ строго положительна. С учётом соглашения $p_T > 0$ необходимое и достаточное условие положительности энтропии (имеющееся, например, в [2]) приобретает вид $\bigcap\limits_{T \in \mathcal{T}} T = \varnothing$.

Рассматривается *блоковое кодирование* последовательностей, порождаемых недоопределённым источником X. Выходные последовательности источника разбиваются на куски некоторой длины n (*блоки*) и каждый блок — слово v длины n в алфавите A — заменяется его кодом $K(v)$ при некотором способе кодирования K. Считается, что кодирование является двоичным и *разделимым*. Последнее означает, что по произвольной конкатенации $K(v_1) \ldots K(v_s)$ кодовых слов образующие её слова $K(v_1)$, $\ldots$, $K(v_s)$ восстанавливаются однозначно. К кодированию K недоопределённых слов $v \in A^n$ предъявляется требование, чтобы оно обеспечивало возможность нахождения по коду $K(v)$ какого-либо доопределения слова v. Кодирование источника (A, P) называется *универсальным* (при заданной длине n блоков), если оно не зависит от набора вероятностей P.

Качество кодирования K будем характеризовать *средней длиной кода*

$$\bar{l}_K^{(n)} = \frac{1}{n} \sum_{v \in A^n} p(v)|K(v)|, \tag{3}$$

приходящейся на символ источника [1]. Здесь $p(v) = p_{T_1} \dots p_{T_n}$ — вероятность порождения источником X слова $v = a_{T_1} \dots a_{T_n}$; $|K(v)|$ — длина кодового слова для v.

В [3] получен следующий результат (см. также [2]).

Теорема 1. Для произвольного недоопределённого источника X с $\mathcal{H}(X) > 0$

1) при любом способе K блокового кодирования имеет место неравенство

$$\bar{l}_K^{(n)} \geqslant \mathcal{H}(X);$$

2) существует универсальное блоковое кодирование K, для которого

$$\bar{l}_K^{(n)} \leqslant \mathcal{H}(X) + \mathrm{O}\Big(\frac{\log n}{n}\Big).$$

Верхняя оценка теоремы 1 получена методом случайного кодирования, который лишь устанавливает факт существования указанной в теореме асимптотически оптимальной оценки средней длины кода, но не обеспечивает соответствующего алгоритма. В данной работе представлен полиномиальный метод кодирования недоопределённых источников более частного вида. Недоопределённый источник $X = (A, P)$ называется *частично определённым*, если его алфавит имеет вид $A = A_0 \cup \{*\} = \{a_0, a_1, \dots, a_{m-1}, *\}$. Ему соответствует набор вероятностей $P = (p_0, p_1, \dots, p_{m-1}, p_*)$. Для частично определённого источника энтропия (2) допускает явное выражение (см. [2], а также п. 3° леммы 1 данной работы):

$$\mathcal{H}(P) = (1 - p_*)\log(1 - p_*) - \sum_{i=0}^{m-1} p_i \log p_i.$$

При условии положительности всех p_i эта величина строго положительна тогда и только тогда, когда $m \geqslant 2$.

Основное содержание работы составляет доказательство следующего результата.

Теорема 2. Для частично определённого источника $X = (A, P)$ с положительной энтропией

1) при любом способе K блокового кодирования справедливо неравенство

$$\bar{l}_K^{(n)} \geqslant \mathcal{H}(P);$$

2) имеется метод K универсального блокового кодирования, обеспечивающий оценку средней длины кода

$$\bar{l}_K^{(n)} \leqslant \mathcal{H}(P) + \mathrm{O}\Big(\frac{\log\log n}{\log^{\frac{1}{2}} n}\Big)$$

и допускающий кодирование и декодирование РАМ-программами сложности $\mathrm{O}(n^2)$.

Замечание 1. При доказательстве верхней оценки средней длины кода остаточный член фактически получен в виде $\mathrm{O}\left(\phi(n)\Big(\frac{\log\log n}{\log n}\Big)^{1/2}\right)$, где $\phi(n)$ — произвольная растущая функция (см. лемму 11). Оценка теоремы соответствует значению $\phi(n) = (\log\log n)^{1/2}$. Её можно улучшать, беря в качестве $\phi(n)$ меньшую функцию.

Распространение теоремы 2 на общий случай недоопределённых источников затруднено тем, что доказательство использует явный вид энтропии $\mathcal{H}(X)$, который удаётся найти лишь в редких случаях.

2. Квазиэнтропия недоопределённых слов и ее свойства

Основной результат работы относится к частично определённым алфавитам (и источникам), но изложение будем вести, как правило, для недоопределённых алфавитов общего вида, учитывая возможность распространения результата работы на другие случаи. Если факт относится лишь к частично определённым данным, это будем отмечать явно.

Для слова $v \in A^n$ обозначим через $r_T(v)$ число появлений в нем символа a_T, $\sum\limits_{T\in T} r_T(v) = |v|$, и положим $\mathbf{r}(v) = (r_T(v), T \in \mathcal{T})$. *Квазиэнтропией* слова v назовём величину $h(v) = |v|\,\mathcal{H}\Big(\dfrac{\mathbf{r}(v)}{|v|}\Big)$. С учётом (1) и (2) она может быть переписана в виде

$$h(v) = \min_{Q}\Big\{-\sum_{T\in\mathcal{T}} r_T(v)\log\sum_{i\in T} q_i\Big\}. \tag{4}$$

Отметим, что точным аналогом принятого для полностью определённых данных понятия квазиэнтропии (см., например, [21]) является $\mathcal{H}\Big(\dfrac{\mathbf{r}(v)}{|v|}\Big)$. Но величина $|v|\mathcal{H}\Big(\dfrac{\mathbf{r}(v)}{|v|}\Big)$ оказывается более удобной, поскольку измеряется в тех же единицах, что и алгоритмическая энтропия (сложность по Колмогорову [6]), а также комбинаторная (см. далее).

Сначала приведём некоторые свойства энтропии $\mathcal{H}(X)$, которые понадобятся для изучения квазиэнтропии. Более детальное рассмотрение этих (и других) свойств энтропии имеется в [2].

Лемма 1.

1°) Энтропия $\mathcal{H}(P)$ неотрицательна и не превосходит $\log m$.

2°) Функция $\mathcal{H}(P)$ вогнута, т. е. для любых P, P' и числа θ, $0 \leqslant \theta \leqslant 1$, выполнено

$$\mathcal{H}(\theta P + (1-\theta)P') \geqslant \theta\mathcal{H}(P) + (1-\theta)\mathcal{H}(P').$$

3°) Энтропии источника $X = (A, P)$ и образованного из него исключением неопределённого символа $* = a_M$ источника $X' = (A', P')$, где $A' = A \setminus \{*\}$, $P' = (p'_T, T \in \mathcal{T}\setminus\{M\})$, $p'_T = \dfrac{p_T}{1-p_*}$, связаны соотношением

$$\mathcal{H}(P) = (1-p_*)\mathcal{H}(P').$$

4°) Для частично определённого источника (A, P), где $A = \{a_0, a_1, \ldots, a_{m-1}, *\}$, $P = (p_0, p_1, \ldots, p_{m-1}, p_*)$, энтропия достигается в (2) на наборе

$$Q = \Big(\frac{p_0}{1-p_*}, \frac{p_1}{1-p_*}, \ldots, \frac{p_{m-1}}{1-p_*}\Big) \tag{5}$$

и принимает значение

$$\mathcal{H}(P) = (1-p_*)\log(1-p_*) - \sum_{i=0}^{m-1} p_i \log p_i. \tag{6}$$

Доказательство. Начнём с утверждений п. 1°. Неотрицательность энтропии очевидна. Верхнюю границу энтропии получим, вычислив $\mathcal{H}(P, Q)$ на наборе $Q = (1/m, \ldots, 1/m)$:

$$\mathcal{H}(P) \leqslant -\sum_T p_T \log\frac{|T|}{m} = \log m - \sum_T p_T \log|T| \leqslant \log m.$$

Для доказательства п. 2° рассмотрим набор Q, на котором достигается минимум функции $\mathcal{H}(\theta P + (1-\theta)P', Q)$. Имеем

$$\mathcal{H}(\theta P + (1-\theta)P') = -\theta \sum_{T\in\mathcal{T}} p_T \log \sum_{i\in T} q_i - (1-\theta) \sum_{T\in\mathcal{T}} p'_T \log \sum_{i\in T} q_i \geqslant \theta\mathcal{H}(P) + (1-\theta)\mathcal{H}(P'),$$

что и требовалось доказать.

Докажем п. 3°. Из того, что для любого набора вероятностей $Q = (q_i, i \in M)$ выполнено $\log \sum\limits_{i\in M} q_i = 0$, следует равенство

$$-\sum_{T\in\mathcal{T}} p_T \log \sum_{i\in T} q_i = -(1-p_*) \sum_{T\in\mathcal{T}\setminus\{M\}} \frac{p_T}{1-p_*} \log \sum_{i\in T} q_i.$$

Взяв минимум по Q, приходим к утверждению п. 3°.

Применим к частично определённому источнику из п. 4° утверждение п. 3°. Имеем

$$\mathcal{H}(P) = (1-p_*)\mathcal{H}(P') = (1-p_*) \min_Q \Big\{ -\sum_{i\in M} \frac{p_i}{1-p_*} \log q_i \Big\}. \tag{7}$$

Как известно, указанный минимум достигается на наборе (5). Подставляя это значение Q в (7) и преобразуя с учётом равенства $\sum\limits_{i\in M} p_i = 1 - p_*$, приходим к (6). ■

Следующая лемма 2 содержит необходимые для дальнейшего свойства квазиэнтропии слов.

Лемма 2.

1°) Квазиэнтропия $h(v)$ неотрицательна и не превосходит $n \log m$.

2°) Если слово v_2 получено из v_1 перестановкой символов, то $h(v_2) = h(v_1)$.

3°) Если $\mathbf{r}(v_2)$ отличается от $\mathbf{r}(v_1)$ лишь в компоненте $r_*(\cdot)$, то $h(v_2) = h(v_1)$.

4°) Квазиэнтропия конкатенации v_1v_2 удовлетворяет неравенству

$$h(v_1v_2) \geqslant h(v_1) + h(v_2).$$

5°) Если v_2 — продолжение слова v_1, то $h(v_2) \geqslant h(v_1)$.

6°) Если va_T — результат приписывания к слову v символа a_T, то

$$h(va_T) \leqslant h(v) + \log\big(e|v|\big).$$

7°) Квазиэнтрпия слова v в частично определённом алфавите $A = \{a_0, a_1, \ldots, a_{m-1}, *\}$ задаётся выражением

$$h(v) = \big(|v| - r_*(v)\big) \log\big(|v| - r_*(v)\big) - \sum_{i\in M} r_i(v) \log r_i(v) \tag{8}$$

и достигается в (4) на наборе

$$Q = \Big(\frac{r_0(v)}{|v| - r_*(v)}, \frac{r_1(v)}{|v| - r_*(v)}, \ldots, \frac{r_{m-1}(v)}{|v| - r_*(v)}\Big). \tag{9}$$

Доказательство. Пункт 1° следует из п. 1° леммы 1.

Пункт 2° вытекает из определения квазиэнтропии и того, что для слов v_2 и v_1 с одним и тем же составом символов имеет место $|v_2| = |v_1|$ и $\mathbf{r}(v_2) = \mathbf{r}(v_1)$.

Докажем п. 3°. Обозначим через v_1' и v_2' слова, полученные из v_1 и v_2 удалением всех символов $*$. По условиям п. 3° имеем $|v_1'| = |v_1| - r_*(v_1) = |v_2| - r_*(v_2) = |v_2'|$ и $\mathbf{r}(v_1') = \mathbf{r}(v_2')$, а потому

$$h(v_1') = h(v_2'). \tag{10}$$

Из п. 4° леммы 1 при $p_T = \dfrac{r_T(v_1)}{|v_1|}$ с учётом равенства $1 - \dfrac{r_*(v_1)}{|v_1|} = \dfrac{|v_1'|}{|v_1|}$ выводим

$$\mathcal{H}\Big(\frac{\mathbf{r}(v_1)}{|v_1|}\Big) = \frac{|v_1'|}{|v_1|}\mathcal{H}\Big(\frac{\mathbf{r}(v_1')}{|v_1'|}\Big).$$

Домножив обе части на $|v_1|$, приходим к равенству $h(v_1) = h(v_1')$. Аналогично доказывается, что $h(v_2) = h(v_2')$. Из этих равенств и (10) получаем $h(v_2) = h(v_1)$.

Для доказательства п. 4° воспользуемся вогнутостью энтропии (п. 3° леммы 1) при $P = \dfrac{\mathbf{r}(v_1)}{|v_1|}$, $P' = \dfrac{\mathbf{r}(v_2)}{|v_2|}$ и $\theta = \dfrac{|v_1|}{|v_1| + |v_2|}$.

Имеем $\dfrac{|v_1|}{|v_1| + |v_2|}\mathcal{H}\Big(\dfrac{\mathbf{r}(v_1)}{|v_1|}\Big) + \dfrac{|v_2|}{|v_1| + |v_2|}\mathcal{H}\Big(\dfrac{\mathbf{r}(v_2)}{|v_2|}\Big) \leqslant \mathcal{H}\Big(\dfrac{\mathbf{r}(v_1) + \mathbf{r}(v_2)}{|v_1| + |v_2|}\Big) = \mathcal{H}\Big(\dfrac{\mathbf{r}(v_1v_2)}{|v_1v_2|}\Big)$. Домножив обе части на $|v_1| + |v_2| = |v_1v_2|$, получаем $h(v_1) + h(v_2) \leqslant h(v_1v_2)$.

Чтобы доказать утверждение п. 5°, представим v_2 в виде $v_2 = v_1w$, после чего в соответствии с п. 4° придём к $h(v_2) \geqslant h(v_1) + h(w)$ и воспользуемся неотрицательностью квазиэнтропии $h(w)$ (п. 1°).

Докажем п. 6°. Пусть $v = a_{T_1} \dots a_{T_{|v|}}$, $v' = va_T$. Обозначим через $Q = (q_0, q_1, \dots, q_{m-1})$ набор, на котором в (4) достигается квазиэнтропия $h(v)$. Возьмём некоторое значение $s \in T$ и образуем набор $Q' = (q_0', q_1', \dots, q_{m-1}')$, где $q_s' = \dfrac{(|v| - 1)q_s}{|v|} + \dfrac{1}{|v|}$, $q_i' = \dfrac{(|v| - 1)q_i}{|v|}$ для остальных $i \in M$. Набор Q' удовлетворяет условию

$$\sum_{i \in M} q_i' = \frac{|v| - 1}{|v|}\sum_{i \in M} q_i + \frac{1}{|v|} = \frac{|v| - 1}{|v|} + \frac{1}{|v|} = 1.$$

С учётом этого имеем

$$h(v') \leqslant -\sum_{i \in M} r_{T_i}(v') \log \sum_{j \in T_i} q_j' = -\sum_{i \in M} r_{T_i}(v) \log \sum_{j \in T_i} q_j' - \log \sum_{j \in T} q_j' \leqslant$$

$$\leqslant -\sum_{i \in M} r_{T_i}(v) \log \sum_{j \in T_i} \frac{|v| - 1}{|v|} q_j - \log \frac{1}{|v|} = -\sum_{i \in M} r_{T_i}(v) \log \sum_{j \in T_i} q_j - |v| \log \frac{|v| - 1}{|v|} + \log |v| =$$

$$= h(v) - |v| \log\Big(1 - \frac{1}{|v|}\Big) + \log |v| \leqslant h(v) + \log e + \log |v| = h(v) + \log(e|v|).$$

Утверждение п. 7° вытекает из п. 4° леммы 1 при $P = \dfrac{\mathbf{r}(v)}{|v|}$ с учётом равенства $\sum\limits_{i \in M} r_i(v) = |v| - r_*(v)$. ■

Замечание 2. Выражение (8) может быть записано в виде, не зависящем от $|v|$:

$$h(v) = \Big(\sum_{i \in M} r_i(v)\Big) \log \sum_{i \in M} r_i(v) - \sum_{i \in M} r_i(v) \log r_i(v). \tag{11}$$

3. Частотные классы недоопределённых слов и их комбинаторная энтропия

Пусть задано конечное множество S недоопределённых слов в алфавите A. Скажем, что некоторое *множество слов* в алфавите A_0 *доопределяет* S, если в нём найдётся доопределение каждого слова из S. Обозначим через $N(S)$ минимальную мощность множества, доопределяющего S. Величину $\log N(S)$ будем называть *комбинаторной энтропией* множества слов S.

Для заданного набора $\mathbf{r} = (r_T, T \in \mathcal{T})$ натуральных чисел положим $l = \sum\limits_{T\in\mathcal{T}} r_T$ и обозначим через $\mathcal{K}_l(\mathbf{r})$ класс всех слов длины l в алфавите A, в которых символ $a_T \in A$ встречается r_T раз (т. е. с частотой r_T/l). Такие классы называют *частотными*. Вместо записи $N(\mathcal{K}_l(\mathbf{r}))$ будем использовать $N_l(\mathbf{r})$. Комбинаторной энтропии класса $\mathcal{K}_l(\mathbf{r})$ соответствует обозначение $\log N_l(\mathbf{r})$. Всякое доопределяющее множество для класса $\mathcal{K}_l(\mathbf{r})$ будем называть *доопределением класса* $\mathcal{K}_l(\mathbf{r})$.

Все слова $v \in \mathcal{K}_l(\mathbf{r})$ имеют одинаковую квазиэнтропию $h(v) = l\mathcal{H}(\mathbf{r}/l)$, которую будем обозначать $h_l(\mathbf{r})$ и называть *квазиэнтропией класса* $\mathcal{K}_l(\mathbf{r})$.

Следующий результат из [3] (см. также [2, 22]) показывает, что квазиэнтропия частотного класса приближает его комбинаторную энтропию с точностью $\mathrm{O}(\log l)$.

Утверждение 1. Справедливы оценки[1]

$$h_l(\mathbf{r}) - C_1 \log l \leqslant \log N_l(\mathbf{r}) \leqslant h_l(\mathbf{r}) + C_2 \log l.$$

Верхняя оценка здесь получена методом случайного кодирования, который доказывает лишь существование доопределяющего множества для класса $\mathcal{K}_l(\mathbf{r})$, обеспечивающего эту оценку, но не даёт алгоритма. Ту же оценку комбинаторной энтропии мы получим ниже конструктивным построением доопределяющего множества с использованием градиентной процедуры (называемой также жадным алгоритмом, методом наискорейшего спуска, методом вычерпывания).

При осуществлении градиентной процедуры доопределения множества слов S используется некоторое базовое множество D всюду определённых слов, из которого заимствуются доопределения слов множества S. Паре (S, D) сопоставляется таблица с элементами 0 и 1, в которой строки соответствуют словам $v \in S$, столбцы — словам $w \in D$, и на пересечении строки v и столбца w помещается 1, если w доопределяет v, и 0 в противном случае. В терминах этой таблицы градиентная процедура доопределения множества S представляет собой последовательность шагов, на каждом из которых в таблице, полученной к данному шагу, выбирается столбец с максимальным числом единиц и вычёркиваются строки, содержащие в нём единицы. Совокупность выбранных столбцов к моменту, когда все строки окажутся вычеркнутыми, соответствует доопределяющему множеству для S. При оценке его мощности используется следующее утверждение, доказанное рядом авторов как обобщение леммы Нечипорука из [10] (оно имеется, например, в [23]).

Утверждение 2. Во всякой таблице с элементами 0 и 1, имеющей b строк, d столбцов и содержащей в каждой строке не менее a единиц, градиентная процедура позволяет выделить

$$k \leqslant \frac{d}{a}\Big(\ln\frac{ba}{d} + 1\Big) + 1$$

столбцов так, что для любой строки имеется выделенный столбец, содержащий в ней 1.

[1] Всюду в работе буквой C с индексом обозначается константа, абсолютная либо зависящая от мощности алфавитов A_0 и A.

Замечание 3. Градиентная процедура выделения столбцов полиномиальна относительно площади bd таблицы.

В градиентной процедуре построения доопределяющего множества для класса $\mathcal{K}_l(\mathbf{r})$ в качестве базового множества используется некоторый частотный класс $\mathcal{K}_l(\mathbf{m})$, $\mathbf{m} = (m_i, i \in M)$, слов в алфавите A_0. Для нахождения набора $\mathbf{m}$ параметров этого класса понадобится следующее свойство точки Q, на которой достигается энтропия в (2). Его доказательство имеется в [2, 3].

Утверждение 3. Точка $Q = (q_i,\, i \in M)$ минимума функции $\mathcal{H}(P, Q)$ удовлетворяет условиям

$$\sum_{T\in\mathcal{T}:\, i\in T} \frac{p_T q_i}{\sum\limits_{j\in T} q_j} = q_i, \quad i \in M. \tag{12}$$

Докажем теперь основной результат данного раздела.

Лемма 3. Существует частотный класс $\mathcal{K}_l(\mathbf{m})$, при использовании которого в качестве базового множества градиентная процедура доопределения класса $\mathcal{K}_l(\mathbf{r})$ обеспечивает оценку

$$\log N_l(\mathbf{r}) \leqslant h_l(\mathbf{r}) + C_3 \log l. \tag{13}$$

Доказательство. Пусть $Q = (q_i,\, i \in M)$ — точка, в которой достигается квазиэнтропия $h_n(\mathbf{r})$, т. е. выполнено

$$-\sum_{T\in\mathcal{T}} r_T \log \sum_{i\in T} q_i = h_l(\mathbf{r}). \tag{14}$$

Введём величины s_{Ti} $(T \in \mathcal{T}, i \in M)$, положив

$$s_{Ti} = \begin{cases} \dfrac{r_T q_i}{l \sum\limits_{j\in T} q_j}, & i \in T, \\ 0, & i \notin T. \end{cases} \tag{15}$$

Величины s_{Ti} удовлетворяют условиям

$$\sum_i l s_{Ti} = r_T \sum_{i\in T} \frac{q_i}{\sum\limits_{j\in T} q_j} = r_T, \tag{16}$$

$$\sum_{T,i} l s_{Ti} = \sum_T \sum_i l s_{Ti} = \sum_T r_T = l$$

(если область изменения параметра T либо i при суммировании не указана, считается, что T пробегает множество $\mathcal{T}$, i — множество M. То же относится к параметрам величин, участвующих в произведении). Кроме того, поскольку на наборе Q, на котором достигается квазиэнтропия $h_l(\mathbf{r})$, достигается и энтропия $\mathcal{H}(\mathbf{r}/l)$, получаем с учётом равенства (12) при $p_T = r_T/l$

$$\sum_T l s_{Ti} = l \sum_{T:\, i\in T} s_{Ti} = l \sum_{T:\, i\in T} \frac{r_T q_i}{l \sum\limits_{j\in T} q_j} = l q_i. \tag{17}$$

Возьмём набор z_{Ti} $(T \in \mathcal{T},\, i \in M)$ целых чисел, такой, что при $i \in T$ величины $|z_{Ti} - l s_{Ti}|$ ограничены некоторой общей константой и выполняются равенства

$$\sum_i z_{Ti} = r_T, \quad T \in \mathcal{T}, \tag{18}$$

а при $i \notin T$ величины $|z_{Ti}|$ равны 0. Это легко сделать в силу (16), определения (15) величин s_{Ti} и того, что мощность множеств T не превосходит константы $|A_0|$.

Введём величины

$$m_i = \sum_T z_{Ti}, \quad i \in M, \tag{19}$$

и положим $\mathbf{m} = (m_i,\, i \in M)$. Тогда

$$\sum_i m_i = \sum_{i,T} z_{Ti} = \sum_T \sum_i z_{Ti} = \sum_T r_T = l. \tag{20}$$

Кроме того, из (17), условий на числа s_{Ti} и ограниченности мощности множеств T константой $|\mathcal{T}|$ следует, что все величины $|m_i - lq_i|$ не превосходят некоторой общей константы.

Принимая во внимание (20), образуем частотный класс $\mathcal{K}_l(\mathbf{m})$ и используем его в качестве базисного множества в градиентной процедуре построения доопределений для слов класса $\mathcal{K}_l(\mathbf{r})$. Построим таблицу, строки которой соответствуют словам $v \in \mathcal{K}_l(\mathbf{r})$, столбцы — словам $w \in \mathcal{K}_l(\mathbf{m})$. На пересечении строки v и столбца w поместим 1 либо 0 в зависимости от того, доопределяет слово w слово v или нет. Числа b и d соответственно строк и столбцов этой таблицы задаются выражениями

$$b = \frac{l!}{\prod\limits_T r_T!}, \qquad d = \frac{l!}{\prod\limits_i m_i!}.$$

При оценке снизу числа единиц в произвольной строке v таблицы будем учитывать только такие доопределения слова v, в которых для всех T и i символ a_T заменяется символом a_i в z_{Ti} позициях. Из (18) следует, что такие доопределения слова v существуют, а из (19) — что все они принадлежат классу $\mathcal{K}_l(\mathbf{m})$. Для каждого $v \in \mathcal{K}_l(\mathbf{r})$ число доопределений указанного вида равно

$$a = \prod_T \frac{r_T!}{\prod\limits_i z_{Ti}!} = \frac{\prod\limits_T r_T!}{\prod\limits_{T,i} z_{Ti}!}.$$

Воспользовавшись утверждением 2 при указанных значениях b, d и a, а также тем, что $\dfrac{ba}{d} < b < l! < l^l$, оценим размер k градиентного покрытия таблицы:

$$k \leqslant \frac{l! \prod\limits_{T,i} z_{Ti}!}{\prod\limits_T r_T! \prod\limits_i m_i!} l \ln l.$$

Комбинаторная энтропия $\log N_l(\mathbf{r})$ не превосходит $\log k$. Отсюда, применяя формулу Стирлинга к факториалам в оценке для k и учитывая равенства $\sum\limits_{T,i} z_{Ti} = \sum\limits_T r_T = \sum\limits_i m_i = l$, приходим к оценке

$$\log N_l(\mathbf{r}) \leqslant l \log l + \sum_{T,i} z_{Ti} \log z_{Ti} - \sum_T r_T \log r_T - \sum_i m_i \log m_i + C_4 \log l. \tag{21}$$

Заменим в этом выражении величины z_{Ti} на ls_{Ti}, а m_i — на lq_i. Поскольку каждая из этих величин не превосходит l и заменяется величиной, отличающейся от неё не более

чем на константу, соответствующий ей член в (21) изменится не более чем на $C_5 \log l$. Число этих членов в (21) ограничено константой, а потому оценка (21) превращается в

$$\log N_l(\mathbf{r}) \leqslant l \log l + \sum_{T,i} l s_{Ti} \log(l s_{Ti}) - \sum_T r_T \log r_T - \sum_i l q_i \log(l q_i) + C_3 \log l =$$
$$= -l\Big(\sum_{T,i} s_{Ti} \log s_{Ti} - \sum_T \frac{r_T}{l} \log \frac{r_T}{l} - \sum_i m_i \log q_i\Big) + C_3 \log l.$$

Принимая во внимание (16) и (17), получаем

$$\log N_l(\mathbf{r}) \leqslant -l\Big(\sum_{T,i} s_{Ti} \log s_{Ti} - \sum_{T,i} s_{Ti} \log \frac{r_T}{l} - \sum_{T,i} s_{Ti} \log q_i\Big) + C_3 \log l =$$
$$= l \sum_{T,i} s_{Ti} \log \frac{l s_{Ti}}{r_T q_i} + C_3 \log l.$$

Замена s_{Ti} в аргументе логарифма значением из (15) приводит к оценке

$$\log N_l(\mathbf{r}) \leqslant l \sum_{T,i} s_{Ti} \log \frac{1}{\sum\limits_{j \in T} q_j} + C_3 \log l = -\sum_T r_T \log \sum_{j \in T} q_j + C_3 \log l,$$

которая в силу (14) совпадает с (13). ■

4. Представительное множество системы частотных классов

Обозначим через $\mathfrak{K}_{\lambda,\mu}$ множество всех частотных классов $\mathcal{K}_l(\mathbf{r})$ (в рассматриваемом недоопределённом алфавите A), для которых длина l слов не превышает λ, а квазиэнтропия $h_l(\mathbf{r})$ не больше μ, где λ и μ — заданные натуральные параметры. Поскольку квазиэнтропия слов длины l не превосходит $l \log m$ (п. 1° леммы 2), можно считать

$$\mu \leqslant \lambda \log m, \tag{22}$$

а потому $\mu = \mathrm{O}(\lambda)$.

Используемая в работе процедура кодирования недоопределённых источников требует нахождения доопределений для всех классов системы $\mathfrak{K}_{\lambda,\mu}$. При рассмотрении систем $\mathfrak{K}_{\lambda,\mu}$ в произвольных недоопределённых алфавитах возникают трудности, связанные с возможностью эффективной проверки условия $h_l(\mathbf{r}) \leqslant \mu$.

Для частично определённых алфавитов подобных трудностей не возникает, ибо для них квазиэнтропия выразима в явном виде (п. 7° леммы 2). В последующем ограничимся частично определёнными алфавитами, но развитый подход может быть распространён в некотором модифицированном виде и на другие алфавиты с явно выразимой энтропией (примеры таких алфавитов имеются в [5]). Дальше в данном пункте считаем, что $\mathfrak{K}_{\lambda,\mu}$ — система в алфавите $A = A_0 \cup \{*\} = \{a_0, a_1, \ldots, a_{m-1}, *\}$. Она образована частотными классами $\mathcal{K}_l(\mathbf{r})$, $\mathbf{r} = (r_0, r_1, \ldots, r_{m-1}, r_*)$, удовлетворяющими условиям $l \leqslant \lambda$, $h_l(\mathbf{r}) \leqslant \mu$.

Лемма 4. В случае частично определённых алфавитов условие $h(v) \leqslant \mu$ проверяемо со сложностью, ограниченной полиномом от длины $|v|$ слова v.

Доказательство. Поскольку параметр μ целочислен, условие $h(v) \leqslant \mu$ можно заменить на $\lceil h(v) \rceil \leqslant \mu$ ($\lceil x \rceil$ означает целое число, ближайшие к x сверху). В силу (8) оно приобретает вид $\lceil \log \alpha \rceil \leqslant \mu$, где

$$\alpha = \frac{(|v| - r_*(v))^{|v| - r_*(v)}}{\prod\limits_{i=0}^{m-1} r_i(v)^{r_i(v)}}.$$

Нетрудно понять, что $\lceil \log \alpha \rceil$ совпадает с длиной двоичной записи числа $\lceil \alpha \rceil - 1$. Поэтому для проверки соотношения $h(v) \leqslant \mu$ достаточно найти по слову v двоичные записи параметров $r_i(v)$ и $r_*(v)$, вычислить по ним число $\lceil \alpha \rceil - 1$ в двоичной записи и сравнить длину этой записи с μ.

Для нахождения величины z^z, $z \in \{r_0(v), \ldots, r_{m-1}(v), |v| - r_*(v)\}$, входящей в выражение для α, достаточно выполнить не более $2 \log z \leqslant 2 \log l$ умножений чисел, длина двоичных записей которых не превышает $l \log l$. Это требует не более $\mathrm{O}(l^2 \log^3 l)$ (булевых) операций. Поскольку число значений z ограничено константой m', на вычисление всех z^z также затрачивается не более $\mathrm{O}(l^2 \log^3 l)$ операций. При известных значениях z^z число α может быть найдено применением $m - 1$ операций умножения и одной операции деления нацело (с избытком). На это расходуется $\mathrm{O}(l^2 \log^2 l)$ операций. Общее число операций для вычисления α не превосходит $\mathrm{O}(l^2 \log^3 l)$. Учёт других операций, используемых для проверки соотношения $h(v) \leqslant \mu$, не изменяет эту оценку. ■

Задача построения доопределений для всех классов системы $\mathfrak{K}_{\lambda,\mu}$ может быть сведена к аналогичной задаче для некоторой её подсистемы. Поставим задачу выделения в определённом смысле лучшей такой подсистемы. Отметим, что для доказательства основного результата работы (теоремы 2) достаточно более грубых рассмотрений, когда доопределения строятся для всех классов системы $\mathfrak{K}_{\lambda,\mu}$. Методы максимально возможного сокращения числа рассматриваемых классов могут быть полезны в приложениях.

Пусть π — перестановка множества $\{0, \ldots, m-1\}$. Для слова v (в алфавите $A = A_0 \cup \{*\}$) посредством πv будем обозначать слово, полученное из v заменой символов $a_i \in A_0$ на $a_{\pi(i)}$ и сохранением символов $*$. Для множества слов V положим $\pi V = \{\pi v,\ v \in V\}$. Если V — некоторое множество слов с длиной не меньше l, то через $V|_l$ будем обозначать множество начал длины l всех слов из V.

Пусть $\mathcal{K}_{l_1}(\mathbf{r}_1)$ и $\mathcal{K}_{l_2}(\mathbf{r}_2)$ — частотные классы слов (в частично определённом алфавите A). Будем говорить, что класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ *представительнее* класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$, если $l_1 \geqslant l_2$ и найдётся перестановка π множества $\{0, \ldots, m-1\}$, такая, что каково бы ни было доопределение $\mathcal{D}_{l_1}(\mathbf{r}_1)$ класса $\mathcal{K}_{l_1}(\mathbf{r}_1)$, множество $(\pi \mathcal{D}_{l_1}(\mathbf{r}_1))|_{l_2}$ образует доопределение класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Заметим, что если в определении представительности вместо начал слов брать другие подслова, расположенные в l_2 различных фиксированных разрядах, это не изменит отношения представительности, поскольку частотные классы замкнуты относительно перестановок символов в словах.

Подсистему $\mathfrak{M}$ некоторой системы $\mathfrak{K}$ частотных классов назовём *представительным множеством системы* $\mathfrak{K}$, если для любого класса $\mathcal{K}_l(\mathbf{r}) \in \mathfrak{K}$ в $\mathfrak{M}$ имеется более представительный класс. Таким образом, доопределение любого класса системы $\mathfrak{K}$ может быть образовано из доопределения подходящего класса системы $\mathfrak{M}$ переименованием символов алфавита и отбрасыванием некоторого количества заключительных символов слов. Представительное множество $\mathfrak{M}$ называется *минимальным*, если не существует представительного множества системы $\mathfrak{K}$, содержащего меньшее число частотных классов. Целью данного пункта является явное описание некоторого минимального представительного множества для системы $\mathfrak{K}_{\lambda,\mu}$

Наряду с наборами $\mathbf{r} = (r_0, \ldots, r_{m-1}, r_*)$ будем рассматривать соответствующие укороченные наборы $\acute{\mathbf{r}} = (r_0, \ldots, r_{m-1})$. Будем говорить, что укороченный набор $\acute{\mathbf{r}}_1 = (r_{1,0}, \ldots, r_{1,m-1})$ *мажорирует* $\acute{\mathbf{r}}_2 = (r_{2,0}, \ldots, r_{2,m-1})$, и записывать $\acute{\mathbf{r}}_1 \geqslant \acute{\mathbf{r}}_2$, если $r_{1,0} \geqslant r_{2,0}$, …, $r_{1,m-1} \geqslant r_{2,m-1}$. Величину $W(\acute{\mathbf{r}}) = r_0 + \ldots + r_{m-1}$ назовём *весом* укоро-

ченного набора $\acute{\mathbf{r}}$. С набором $\acute{\mathbf{r}}$ свяжем его квазиэнтропию

$$h(\acute{\mathbf{r}}) = W(\acute{\mathbf{r}}) \log W(\acute{\mathbf{r}}) - \sum_{i=0}^{m-1} r_i \log r_i.$$

В силу (11) квазиэнтропия $h_l(\mathbf{r})$ класса $\mathcal{K}_l(\mathbf{r})$ при любом $l \geqslant W(\acute{\mathbf{r}})$ совпадает с квазиэнтропией $h(\acute{\mathbf{r}})$ укороченного набора.

Результатом применения перестановки π к укороченному набору $\acute{\mathbf{r}}$ считается набор $\pi\acute{\mathbf{r}} = (r_{\pi(0)}, \ldots, r_{\pi(m-1)})$. Набор $\acute{\mathbf{r}}$, для которого $r_0 \geqslant \ldots \geqslant r_{m-1}$, будем называть *упорядоченным*. Перестановка π, переводящая заданный укороченный набор $\acute{\mathbf{r}}$ в упорядоченный набор $\pi\acute{\mathbf{r}}$, не единственна, ибо разным i могут соответствовать одинаковые r_i. Для её конкретизации дополнительно потребуем, чтобы при $r_i = r_j$ и $i < j$ было выполнено $\pi(i) < \pi(j)$. Эту перестановку обозначим $\pi_{\acute{\mathbf{r}}}$ и назовём *упорядочивающей* (для $\acute{\mathbf{r}}$). Для упорядоченных наборов $\acute{\mathbf{r}}_1$ и $\acute{\mathbf{r}}_2$ будем говорить, что $\acute{\mathbf{r}}_2$ *непосредственно следует* за $\acute{\mathbf{r}}_1$ ($\acute{\mathbf{r}}_1$ *непосредственно предшествует* $\acute{\mathbf{r}}_2$), если $\acute{\mathbf{r}}_2 \geqslant \acute{\mathbf{r}}_1$ и $W(\acute{\mathbf{r}}_2) = W(\acute{\mathbf{r}}_1) + 1$. Так, например, всеми непосредственно следующими за набором (3,1,1,0,0) являются наборы (4,1,1,0,0), (3,2,1,0,0) и (3,1,1,1,0).

Эффективный метод проверки наличия отношения представительности для заданных частотных классов даётся следующим утверждением.

Утверждение 4. Класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ представительнее класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$ тогда и только тогда, когда $l_1 \geqslant l_2$ и набор $\pi_{\acute{\mathbf{r}}_1}\acute{\mathbf{r}}_1$, полученный упорядочением набора $\acute{\mathbf{r}}_1$, мажорирует набор $\pi_{\acute{\mathbf{r}}_2}\acute{\mathbf{r}}_2$, полученный упорядочением $\acute{\mathbf{r}}_2$.

Доказательство. Будем считать $l_1 \geqslant l_2$.

1. Пусть имеет место мажорирование $\pi_{\acute{\mathbf{r}}_1}\acute{\mathbf{r}}_1 \geqslant \pi_{\acute{\mathbf{r}}_2}\acute{\mathbf{r}}_2$. Применив к обеим частям перестановку $\pi_{\acute{\mathbf{r}}_2}^{-1}$ и положив $\pi = \pi_{\acute{\mathbf{r}}_2}^{-1}\pi_{\acute{\mathbf{r}}_1}$, получаем соотношение $\pi\acute{\mathbf{r}}_1 \geqslant \acute{\mathbf{r}}_2$. Обозначим через $\mathbf{r}_2^+$ результат дописывания $l_1 - l_2$ нулей к набору $\mathbf{r}_2$. Из предшествующего соотношения и равенства $\acute{\mathbf{r}}_2^+ = \acute{\mathbf{r}}_2$ следует $\pi\acute{\mathbf{r}}_1 \geqslant \acute{\mathbf{r}}_2^+$.

Рассмотрим произвольное доопределение $\mathcal{D}_{l_1}(\mathbf{r}_1)$ класса $\mathcal{K}_{l_1}(\mathbf{r}_1)$. Ясно, что $\pi\mathcal{D}_{l_1}(\mathbf{r}_1)$ является некоторым доопределением класса $\mathcal{K}_{l_1}(\pi\mathbf{r}_1)$. Отсюда и из $\pi\acute{\mathbf{r}}_1 \geqslant \acute{\mathbf{r}}_2^+$ нетрудно заключить, что множество $\pi\mathcal{D}_{l_1}(\mathbf{r}_1)$ доопределяет класс $\mathcal{K}_{l_1}(\mathbf{r}_2^+)$, а потому $\big(\pi\mathcal{D}_{l_1}(\mathbf{r}_1)\big)\big|_{l_2}$ образует доопределение класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Это означает, что класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ представительнее $\mathcal{K}_{l_2}(\mathbf{r}_2)$.

2. Обратно, пусть $\mathcal{K}_{l_1}(\mathbf{r}_1)$ представительнее $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Перестановка π, присутствующая в определении соотношения этих классов по представительности, удовлетворяет условию $\pi\acute{\mathbf{r}}_1 \geqslant \acute{\mathbf{r}}_2$. Действительно, если это не так, то при некотором i имеет место $r_{1,\pi^{-1}(i)} < r_{2,i}$. Тогда, используя для слов класса $\mathcal{K}_{l_1}(\mathbf{r}_1)$ в качестве доопределений символов $*$ символы, отличные от $a_{\pi^{-1}(i)}$, можно получить доопределение $\mathcal{D}_{l_1}(\mathbf{r}_1)$, все слова которого содержат менее $r_{2,i}$ символов $a_{\pi^{-1}(i)}$, а потому число символов a_i в любом слове множества $(\pi\mathcal{D}_{l_1}(\mathbf{r}_1))|_{l_2}$ меньше $r_{2,i}$. Это противоречит тому, что данное множество доопределяет класс $\mathcal{K}_{l_2}(\mathbf{r}_2)$, слова которого используют $r_{2,i}$ символов a_i.

Покажем теперь, что если для некоторых числовых наборов $\mathbf{s}_1 = (s_{1,0}, \ldots, s_{1,m-1})$ и $\mathbf{s}_2 = (s_{2,0}, \ldots, s_{2,m-1})$ выполнено условие мажорирования $\mathbf{s}_1 \geqslant \mathbf{s}_2$, то аналогичному условию мажорирования удовлетворяют и соответствующие им упорядоченные наборы. Для доказательства можно ограничиться случаем, когда набор $\mathbf{s}_1$ с самого начала является упорядоченным. Возьмём максимальный по величине разряд набора $\mathbf{s}_2$ (если таких разрядов несколько, то первый из них); пусть это будет $s_{2,i}$. Поменяем в $\mathbf{s}_2$ местами разряды $s_{2,1}$ и $s_{2,i}$. Так как $s_{2,i} \leqslant s_{1,i} \leqslant s_{1,1}$ и $s_{2,1} \leqslant s_{2,i} \leqslant s_{1,i}$, то полученный в результате набор $\mathbf{s}_2'$ будет удовлетворять условию мажорирования $\mathbf{s}_1 \geqslant \mathbf{s}_2'$. Аналогич-

ные соображения показывают, что если среди разрядов набора $\mathbf{s}'_2$, отличных от первого, найти максимальный по величине и поменять его местами со вторым разрядом, получим набор $\mathbf{s}''_2$, для которого $\mathbf{s}_1 \geqslant \mathbf{s}''_2$. Эти рассуждения могут быть продолжены вплоть до перевода набора $\mathbf{s}_2$ в упорядоченный.

Используя в качестве $\mathbf{s}_1$ и $\mathbf{s}_2$ наборы $\pi\acute{\mathbf{r}}_1$ и $\acute{\mathbf{r}}_2$, удовлетворяющие условию $\pi\acute{\mathbf{r}}_1 \geqslant \acute{\mathbf{r}}_2$, и учитывая, что наборам $\pi\acute{\mathbf{r}}_1$ и $\acute{\mathbf{r}}_1$ соответствуют одинаковые упорядоченные наборы, приходим к $\pi_{\acute{\mathbf{r}}_1}\acute{\mathbf{r}}_1 \geqslant \pi_{\acute{\mathbf{r}}_2}\acute{\mathbf{r}}_2$. ■

Набор $\acute{\mathbf{r}}$ назовём (λ,μ)-*допустимым*, если он упорядочен и удовлетворяет условиям $W(\acute{\mathbf{r}}) \leqslant \lambda$, $h(\acute{\mathbf{r}}) \leqslant \mu$. Упорядоченный набор $\acute{\mathbf{r}}$, мажорируемый некоторым (λ,μ)-допустимым набором $\acute{\mathbf{r}}_1$, также (λ,μ)-допустим. Действительно, произвольное слово v класса $\mathcal{K}_{W(\acute{\mathbf{r}})}(\acute{\mathbf{r}})$ может быть продолжено до некоторого слова v_1 класа $\mathcal{K}_{W(\acute{\mathbf{r}}_1)}(\acute{\mathbf{r}}_1)$. В силу п. 5° леммы 2 выполнено $h(v) \leqslant h(v_1)$, а потому из соотношений $h(v) = h_{W(\acute{\mathbf{r}})}(\acute{\mathbf{r}}) = h(\acute{\mathbf{r}})$, $h(v_1) = h_{W(\acute{\mathbf{r}}_1)}(\acute{\mathbf{r}}_1) = h(\acute{\mathbf{r}}_1)$ и из (λ,μ)-допустимости набора $\acute{\mathbf{r}}_1$ следует $h(\acute{\mathbf{r}}) \leqslant h(\acute{\mathbf{r}}_1) \leqslant \mu$. Неравенство $W(\acute{\mathbf{r}}) \leqslant W(\acute{\mathbf{r}_1}) \leqslant \lambda$ очевидно.

Отношение мажорирования $\acute{\mathbf{r}}_1 \geqslant \acute{\mathbf{r}}_2$ является частичным порядком. Обозначим через $R_{\lambda,\mu}$ множество всех (λ,μ)-допустимых наборов, максимальных по этому порядку. В нем отсутствуют мажорирования одних наборов другими и всякий (λ,μ)-допустимый набор мажорируется некоторым набором из этого множества.

Опишем прямой способ построения множества $R_{\lambda,\mu}$. Сначала индуктивно построим последовательность множеств $R'_{\lambda,\mu}(i)$, $i = 0,\ldots,\lambda$. Для этого положим $R'_{\lambda,\mu}(0) = \{(0,0,\ldots,0)\}$, а множество $R'_{\lambda,\mu}(i+1)$ образуем, взяв все наборы, непосредственно следующие за наборами из $R'_{\lambda,\mu}(i)$, и устранив те из них, квазиэнтропия которых превышает μ. Обозначим через $R_{\lambda,\mu}(i)$ $(i = 0,\ldots,\lambda)$ результат удаления из $R'_{\lambda,\mu}(i)$ наборов, мажорируемых какими-либо наборами множества $R'_{\lambda,\mu}(i+1)$ (считаем $R'_{\lambda,\mu}(\lambda+1) = \varnothing$).

Утверждение 5. Множество $R_{\lambda,\mu}(i)$ $(i = 0,1,\ldots,\lambda)$ образовано всеми наборами множества $R_{\lambda,\mu}$, имеющими вес i, а потому $R_{\lambda,\mu} = \bigcup\limits_{i=0}^{\lambda} R_{\lambda,\mu}(i)$. Сложность построения множества $R_{\lambda,\mu}$ полиномиальна по λ.

Доказательство. Сначала индукцией по i убедимся, что множество $R'_{\lambda,\mu}(i)$ состоит из всех (λ,μ)-допустимых наборов веса i. Для $R'_{\lambda,\mu}(0)$ это очевидно. Считая факт справедливым для $R'_{\lambda,\mu}(i)$, $i < \lambda$, рассмотрим множество $R'_{\lambda,\mu}(i+1)$. Оно непусто, поскольку включает набор (1,...,1,0,...,0) веса $i+1$, имеющий нулевую квазиэнтропию. Наборы этого множества (λ,μ)-допустимы, ибо, непосредственно следуя за наборами из $R'_{\lambda,\mu}(i)$, они имеют вес $i+1 \leqslant \lambda$, а их квазиэнтропия не превышает μ по построению. С другой стороны, если некоторый набор $\acute{\mathbf{r}}$ веса $i+1$ (λ,μ)-допустим, то любой непосредственно предшествующий ему набор также (λ,μ)-допустим, а его вес равен i. По предположению индукции он содержится в $R'_{\lambda,\mu}(i)$, а потому непосредственно следующий за ним набор $\acute{\mathbf{r}}$ включается в $R'_{\lambda,\mu}(i+1)$ по построению. Индукция завершена.

Покажем теперь, что $R_{\lambda,\mu}(i)$ — множество всех максимальных по мажорированию (λ,μ)-допустимых наборов веса i. Произвольный (λ,μ)-допустимый набор $\acute{\mathbf{r}} = (r_0,\ldots,r_{m-1})$ веса i содержится в $R'_{\lambda,\mu}(i)$, и если $\acute{\mathbf{r}}$ не мажорируется, то, в частности, он не мажорируется и наборами из $R'_{\lambda,\mu}(i+1)$, а потому будет включён в $R_{\lambda,\mu}(i)$. Предположим теперь, что $\acute{\mathbf{r}}$ мажорируется некоторым (λ,μ)-допустимым набором $\acute{\mathbf{r}}' = (r'_0,\ldots,r'_{m-1})$, и пусть эти наборы впервые различаются в разряде j, т. е. $r_0 = r'_0$, $\ldots$, $r_{j-1} = r'_{j-1}$ и $r_j < r'_j$. Образуем набор $\acute{\mathbf{r}}'' = (r_0,\ldots,r_{j-1},r_j+1,r_{j+1},\ldots,r_{m-1})$. Он упорядочен и мажорируется (λ,μ)-допустимым набором $\acute{\mathbf{r}}'$, а потому (λ,μ)-допу-

стим. Этот набор имеет вес $i+1$ и, следовательно, содержится в $R'_{\lambda,\mu}(i+1)$. Набор $\acute{\mathbf{r}}''$ мажорирует $\acute{\mathbf{r}}$, и при построении множества $R_{\lambda,\mu}(i)$ набор $\acute{\mathbf{r}}$ будет исключен из $R'_{\lambda,\mu}(i)$.

Тот факт, что сложность построения множества $R_{\lambda,\mu}$ указанным способом полиномиальна по λ, легко извлекается из леммы 4 и того, что число укороченных наборов $\acute{\mathbf{r}}$ веса $W(\acute{\mathbf{r}}) \leqslant \lambda$ ограничено полиномом от λ. ■

С каждым набором $\acute{\mathbf{r}} \in R_{\lambda,\mu}$ свяжем частотный класс $\mathcal{K}_\lambda(\mathbf{r})$, где набор $\mathbf{r}$ получен из $\acute{\mathbf{r}}$ дописыванием компоненты $r_* = \lambda - W(\acute{\mathbf{r}})$. Совокупность этих частотных классов обозначим через $\mathfrak{M}_{\lambda,\mu}$.

Утверждение 6. Система $\mathfrak{M}_{\lambda,\mu}$ образует минимальное представительное множество системы $\mathfrak{K}_{\lambda,\mu}$. Её явное задание может быть найдено с полиномиальной по λ сложностью.

Доказательство. Убедимся сначала, что $\mathfrak{M}_{\lambda,\mu}$ является представительным множеством системы $\mathfrak{K}_{\lambda,\mu}$. Рассмотрим произвольный частотный класс $\mathcal{K}_l(\mathbf{r}) \in \mathfrak{K}_{\lambda,\mu}$. Пусть $\acute{\mathbf{r}}$ — укороченный набор для $\mathbf{r}$, $\pi_{\acute{\mathbf{r}}}$ — упорядочивающая его перестановка. Легко видеть, что набор $\pi_{\acute{\mathbf{r}}}\acute{\mathbf{r}}$, полученный упорядочением $\acute{\mathbf{r}}$, (λ,μ)-допустим, а потому в $R_{\lambda,\mu}$ имеется мажорирующий его набор $\acute{\mathbf{r}}'$. Возьмём соответствующий ему класс $\mathcal{K}_\lambda(\mathbf{r}')$ системы $\mathfrak{M}_{\lambda,\mu}$. Нетрудно понять, что для любого доопределения $\mathcal{D}_\lambda(\mathbf{r}')$ этого класса множество $\bigl(\pi_{\acute{\mathbf{r}}}^{-1}\mathcal{D}_\lambda(\mathbf{r}')\bigr)\big|_l$ доопределяет класс $\mathcal{K}_l(\mathbf{r})$. Это означает, что класс $\mathcal{K}_\lambda(\mathbf{r}')$ представительнее $\mathcal{K}_l(\mathbf{r})$. а потому $\mathfrak{M}_{\lambda,\mu}$ — представительное множество системы $\mathfrak{K}_{\lambda,\mu}$.

Покажем теперь, что представительное множество $\mathfrak{M}_{\lambda,\mu}$ минимально. Предположим, что это не так и существует представительное множество $\mathfrak{M}'$ меньшей мощности. Тогда в $\mathfrak{M}'$ найдётся класс $\mathcal{K}_\lambda(\mathbf{r}')$, который представительнее по крайней мере двух различных классов $\mathcal{K}_\lambda(\mathbf{r}_1)$ и $\mathcal{K}_\lambda(\mathbf{r}_2)$ системы $\mathfrak{M}_{\lambda,\mu}$. Наборы $\acute{\mathbf{r}}_1$ и $\acute{\mathbf{r}}_2$ упорядочены по определению и, согласно утверждению 4, мажорируются результатом упорядочивания набора $\acute{\mathbf{r}}'$. Будучи максимальными по отношению мажорирования, они совпадают с ним и, следовательно, одинаковы. Это противоречит тому, что классы $\mathcal{K}_\lambda(\mathbf{r}_1)$ и $\mathcal{K}_\lambda(\mathbf{r}_2)$ выбраны различными.

Система $\mathfrak{M}_{\lambda,\mu}$ явно задаётся множеством пар $(\mathbf{r},\lambda)$, где $\mathbf{r}$ — результат приписывания к набору $\acute{\mathbf{r}} \in R_{\lambda,\mu}$ компоненты $\lambda - W(\acute{\mathbf{r}})$. Согласно утверждению 5, сложность задания множества $R_{\lambda,\mu}$ полиномиальна по λ, а потому и сложность задания системы $\mathfrak{M}_{\lambda,\mu}$ полиномиальна по λ. ■

5. Справочная часть кода

Кодирование использует параметры λ и μ, которые будут назначены позже. Для каждого $v \in A^n$ кодовое слово $K(v)$ образовано подсловами K_0 и $K_1(v)$, $K(v) = K_0\,K_1(v)$, где K_0, одинаковое для всех v, называется *справочной частью* кодового слова, $K_1(v)$ — его *основной частью*. Справочная часть K_0 содержит сведения о параметре m задачи, параметрах λ и μ алгоритма кодирования, а также о доопределениях слов из частотных классов $\mathcal{K}_\lambda(\mathbf{r})$, входящих в минимальное представительное множество $\mathfrak{M}_{\lambda,\mu}$.

Будем использовать следующее представление натуральных чисел s в виде двоичных слов $\widehat{s}$. Если $\sigma_1\ldots\sigma_k$, $k = \lceil\log(s-1)\rceil$, — минимальная двоичная запись числа s, то $\widehat{s} = \sigma_1\sigma_1\ldots\sigma_k\sigma_k01$. Такое представление чисел удобно применять для задания совокупностей чисел и двоичных слов. Так, например, если s — число, а u_1 и u_2 — слова, то слово $\widehat{s}u_1$ однозначно задаёт пару (s,u_1), а слово $\widehat{|u_1|}u_1u_2$, где $\widehat{|u_1|}$ — представление длины $|u_1|$ слова u_1, однозначно задаёт пару слов (u_1,u_2). Очевидно, что

$$|\widehat{s}| \leqslant 2\log s + 4. \tag{23}$$

Для каждого класса $\mathcal{K}_\lambda(\mathbf{r})$ построим доопределение $\mathcal{D}_\lambda(\mathbf{r})$ с использованием градиентной процедуры из леммы 3. Обозначим через $\mathcal{D}_{\lambda,\mu}$ объединение доопределений $\mathcal{D}_\lambda(\mathbf{r})$ для всех классов $\mathcal{K}_\lambda(\mathbf{r})$ системы $\mathfrak{M}_{\lambda,\mu}$. Множество $\mathcal{D}_{\lambda,\mu}$ обладает тем свойством, что для любого слова v с $|v| \leqslant \lambda$ и $h(v) \leqslant \mu$ в нём найдётся слово, начало которого доопределяет слово v', полученное из v упорядочивающей перестановкой. Множество с таким свойством будем называть (λ,μ)-представительным. Множество $\mathcal{D}_{\lambda,\mu}$ упорядочим лексикографически.

Слова $w \in \mathcal{D}_{\lambda,\mu}$ в алфавите $A_0 = \{a_0,\dots,a_{m-1}\}$ имеют длину λ. Сопоставим каждому w двоичное слово $\tilde{w}$ длины $m\lambda$, заменив в w символы a_i двоичными словами $0\dots010\dots0$ длины m, содержащими 1 в разряде i, $0 \leqslant i \leqslant m-1$. Слова $\tilde{w}$ также будут расположены в лексикографическом порядке в соответствии с упорядочением слов w. Образуем слово $\tilde{w}_\Sigma$ путём приписывания в этом порядке слов $\tilde{w}$ друг к другу. В качестве справочной части кодовых слов $K(v)$, $v \in A^n$ будем использовать двоичное слово

$$K_0 = \widehat{m}\widehat{\lambda}\widehat{\mu}\widehat{|\tilde{w}_\Sigma|}\tilde{w}_\Sigma. \tag{24}$$

Подслово $\widehat{|\tilde{w}_\Sigma|}$ позволяет при декодировании кодового слова $K(v) = K_0\,K_1(v)$ отделить в нём справочную часть от основной.

Лемма 5.

1) Длина справочной части кода удовлетворяет оценке

$$|K_0| \leqslant \lambda^{C_6} 2^\mu. \tag{25}$$

2) Сложность построения справочной части ограничена величиной $(C_7)^\lambda$.

Здесь C_6 и C_7 — подходящие константы.

Доказательство.

1) По лемме 3 с учётом неравенства $h_\lambda(\mathbf{r}) \leqslant \mu$ получаем оценку мощности множества $\mathcal{D}_\lambda(\mathbf{r})$, доопределяющего класс $\mathcal{K}_\lambda(\mathbf{r})$:

$$\bigl|\mathcal{D}_\lambda(\mathbf{r})\bigr| \leqslant \lambda^{C_3} 2^\mu.$$

Для мощности объединения $\mathcal{D}_{\lambda,\mu}$ этих множеств справедливы оценки

$$|\mathcal{D}_{\lambda,\mu}| \leqslant \lambda^{C_3} 2^\mu |\mathfrak{M}_{\lambda,\mu}| \leqslant \lambda^{C_3} 2^\mu \lambda^{m+1}, \tag{26}$$

и потому длина слова $\tilde{w}_\Sigma$ удовлетворяет оценке

$$|\tilde{w}_\Sigma| \leqslant m\lambda^{C_3+m+1} 2^\mu.$$

Отсюда, учитывая (22), (23) и (24), приходим к оценке (25).

2) Оценим сложность градиентной процедуры доопределения класса $\mathcal{K}_\lambda(\mathbf{r}) \in \mathfrak{M}_{\lambda,\mu}$. Необходимый для построения градиентной таблицы набор Q, на котором достигается квазиэнтропия $h_\lambda(\mathbf{r})$, вычисляется с полиномиальной сложностью по формуле $Q = \mathbf{r}/(\lambda - r_*)$ (лемма 2, п. 7°). Числа строк и столбцов градиентной таблицы не более чем экспоненциальны (относительно λ), поэтому по замечанию 3 процедура реализуется с экспоненциальной оценкой сложности. Поскольку множество $\mathfrak{M}_{\lambda,\mu}$ содержит полиномиальное число классов $\mathcal{K}_\lambda(\mathbf{r})$, сложность построения доопределений всех слов из классов множества $\mathfrak{M}_{\lambda,\mu}$ остаётся экспоненциальной. Нетрудно понять, что учёт других операций, используемых для построения справочной части кода, не изменяет характер общей оценки сложности. ■

6. Основная часть кода

Перед построением основной части кодового слова производится обработка справочной части $K_0 = \widehat{m}\widehat{\lambda}\widehat{\mu}\widehat{|\tilde{w}_\Sigma|}\tilde{w}_\Sigma$. По ней находятся параметры m, λ, μ и слово $\tilde{w}_\Sigma$. Затем слово $\tilde{w}_\Sigma$ разбивается на подслова $\tilde{w}$ длины $m\lambda$ и по ним восстанавливаются соответствующие слова w длины λ в алфавите A_0. Согласно (26), число слов w не превосходит $\lambda^{C_8}2^\mu$. Слова w нумеруются в лексикографическом порядке двоичными числами (т. е. числами в двоичной записи) $\tilde{\delta}(w)$ длины $d = \lceil\log(\lambda^{C_8}2^\mu)\rceil$. Кроме того, все перестановки π множества $\{0, 1, \ldots, m-1\}$ нумеруются двоичными числами $\tilde{\varepsilon}(\pi)$ длины $z = \lceil\log m!\rceil$ (напомим, что m — константа рассматриваемой задачи).

Опишем метод построения основной части $K_1(v)$ кода для слова $v \in A^n$. Разобьём слово v на куски v_i, $i = 1, 2, \ldots$, последовательно отрезая от него подслова v_i максимально возможной длины $|v_i|$, удовлетворяющие условиям $h(v_i) \leqslant \mu$ и $|v_i| \leqslant \lambda$. Если число этих кусков равно t, то $v = v_1 v_2 \ldots v_t$. Такое разбиение однозначно в силу монотонности квазиэнтропии (п. 5° леммы 2). Положим $b = \lceil\log\lambda\rceil$ и b-разрядную двоичную запись длины куска v_i обозначим через $\tilde{\lambda}_i$.

Каждому куску v_i сопоставим его код $K(v_i)$ следующим образом. Рассмотрим укороченный набор $\acute{\mathbf{r}}(v_i) = (r_0(v_i), \ldots, r_{m-1}(v_i))$ для слова v_i, построим по нему упорядочивающую перестановку $\pi_{\acute{\mathbf{r}}(v_i)}$ и образуем слово $\pi_{\acute{\mathbf{r}}(v_i)}v_i = v_i'$. Слова w, возникшие в результате обработки справочной части кода, образуют (λ, μ)-представительное множество, поэтому в нём имеются слова, начала которых доопределяют v_i'. Возьмём любое из них, обозначим его через $w^{(i)}$ и положим

$$K(v_i) = \tilde{\delta}(w^{(i)})\tilde{\lambda}_i\tilde{\varepsilon}(\pi^{-1}_{\acute{\mathbf{r}}(v_i)}). \tag{27}$$

В качестве основной части кода для слова $v \in A^n$ возьмём

$$K_1(v) = \widehat{\widehat{d}\,\widehat{b}\,\widehat{z}\,\widehat{t}}\,K(v_1)K(v_2)\ldots K(v_t). \tag{28}$$

Из этих выражений с учётом (23) следует, что длина основной части кода может быть оценена величиной

$$|K_1(v)| \leqslant 2\log d + 2\log b + 2\log z + 2\log t + t(d + b + z) + 16. \tag{29}$$

Лемма 6.

1) Длина основной части $K_1(v)$ кода для слова $v \in A^n$ удовлетворяет оценке

$$|K_1(v)| \leqslant h(v) + n\Big(\frac{C_9\log\lambda}{\mu - \log\lambda - 2} + \frac{\mu + C_9\log\lambda}{\lambda}\Big) + 2\log n + C_{10}\lambda, \tag{30}$$

   где $h(v)$ — квазиэнтропия слова v.
2) Сложность построения основной части кода для слова $v \in A^n$ при заданной проверочной части ограничена величиной $n\lambda^{C_{11}}2^\mu$.

Доказательство.

1) Будем говорить, что кусок v_i слова v имеет тип 1, если $|v_i| < \lambda$, и тип 2, если $|v_i| = \lambda$. Количества кусков типа 1 и 2 в слове v обозначим соответственно t_1 и t_2. Очевидно, что $t_2 \leqslant n/\lambda$.

Оценим t_1. Если кусок v_i имеет тип 1, то либо он является заключительным в слове v, либо квазиэнтропия $h(v_i a)$ слова, полученного приписыванием к v_i символа a,

расположенного в слове v после v_i, превышает μ. Во втором случае в силу п. 6° леммы 2 имеем

$$h(v_i) \geqslant h(v_i a) - \log|v_i| - \log e \geqslant \mu - \log\lambda - 2.$$

Используя это неравенство и тот факт, что число незаключительных кусков типа 1 не превышает $t_1 - 1$, выводим на основе п. 4° леммы 2

$$h(v) = h(v_1 \dots v_t) \geqslant \sum_{i=1}^{t} h(v_i) \geqslant (t_1 - 1)(\mu - \log\lambda - 2).$$

Отсюда $t_1 \leqslant \dfrac{h(v)}{\mu - \log\lambda - 2} + 1$, а потому $t = t_1 + t_2 \leqslant \dfrac{h(v)}{\mu - \log\lambda - 2} + \dfrac{n}{\lambda} + 1$.

Перепишем (29) в виде

$$|K_1(v)| \leqslant [(t_1-1)(d+b+z)] + [t_2(d+b+z)] + [(d+b+z) + 2(\log d + \log b + \log z) + 2\log n + 16]$$

и найдём оценку этого выражения как сумму оценок трёх его фрагментов, выделенных квадратными скобками. Имеем

$$\begin{aligned}(t_1 - 1)(d + b + z) &\leqslant \frac{h(v)}{\mu - \log\lambda - 2}((C_8 + 1)\log\lambda + \mu + m\log m + 3) = \\ &= h(v) + \frac{h(v)}{\mu - \log\lambda - 2}((C_8 + 2)\log\lambda + m\log m + 5).\end{aligned}$$

Оценив здесь второе вхождение $h(v)$ максимально возможным значением $n\log m$ квазиэнтропии (п. 1° леммы 2), получаем

$$\begin{aligned}(t_1 - 1)(d + b + z) &\leqslant h(v) + \frac{n\log m((C_8 + 2)\log\lambda + m\log m + 5)}{\mu - \log\lambda - 2} \leqslant \\ &\leqslant h(v) + \frac{C_9 n\log\lambda}{\mu - \log\lambda - 2}.\end{aligned} \tag{31}$$

Оценка второго фрагмента даёт

$$t_2(d + b + z) \leqslant \frac{n((C_8 + 1)\log\lambda + \mu + m\log m + 3)}{\lambda} \leqslant n\,\frac{\mu + C_9\log\lambda}{\lambda}. \tag{32}$$

Оценим заключительный фрагмент, учитывая неравенства $t \leqslant n$ и $\mu \leqslant \lambda\log m$:

$$\begin{aligned}&(d + b + z) + 2(\log d + \log b + \log z) + 2\log t + 16 \leqslant \\ &\leqslant (d + b + z) + 6\log(d + b + z) + 2\log t + 16 \leqslant \\ &\leqslant \mu + C_9\log\lambda + 6\log(\mu + C_9\log\lambda) + 2\log n + 16 \leqslant 2\log n + C_{10}\lambda.\end{aligned} \tag{33}$$

Просуммировав (31), (32) и (33), получаем (30).

2) Алгоритм построения основной части $K_1(v)$ кода при заданной справочной части K_0 включает три основных этапа.

На первом этапе производится обработка справочной части кода, как описано в начале раздела. С учётом оценки (25) нетрудно заключить, что сложность этого этапа не превышает $\lambda^{C_{12}} 2^{\mu}$.

Второй этап посвящён разбиению слова v на куски v_i. Сложность этого этапа ограничена величиной $n\lambda^{C_{13}}$, где n — длина слова v.

Третий этап включает построение кодов $K(v_i)$ всех кусков в соответствии с (27) и образование из них основной части кода для слова v. Наибольшая сложность при построении $K(v_i)$ приходится на поиск слова $w^{(i)}$, начало которого доопределяет слово v_i', полученное из v_i упорядочивающей перестановкой. Слово $w^{(i)}$ может быть найдено путём последовательного просмотра слов w, возникших в результате обработки справочной части, и проверки, доопределяют ли их начала слово v_i'. С учётом того, что число слов w не превосходит $\lambda^{C_8}2^\mu$, для этого достаточно выполнить не более $\lambda^{C_{14}}2^\mu$ операций. Можно считать, что эта оценка покрывает также полиномиальное по λ число других операций, требуемых для построения кода $K(v_i)$ в соответствии с (27). Поскольку число t кусков v_i не превышает длину n слова v, на построение кодов всех кусков затрачивается не более $n\lambda^{C_{14}}2^\mu$ операций. Будем считать, что константа C_{14} выбрана так, что эта оценка учитывает также операции, используемые для построения $K_1(v)$ из кодов $K(v_i)$ в соответствии с (28) и, таким образом, оценивает сложность третьего этапа.

Величина сложности из п. 2 формулировки леммы 6 оценивает сверху при подходящем выборе C_{11} сумму сложностей всех трёх этапов. ■

7. Оценка характеристик кодирования

Покажем, что предложенное кодирование K удовлетворяет исходным требованиям к кодированию частично определённых слов.

Лемма 7. Кодирование K разделимо и позволяет для всякого слова $v \in A^n$ восстановить по его коду $K(v)$ некоторое доопределение слова v.

Доказательство.

1. Убедимся, что код обладает достаточным для разделимости свойством префикса. Пусть $K(v)$ и $K(v')$ — кодовые слова и $K(v)$ является префиксом (началом) слова $K(v')$. Это соотношение переносится на их основные части $K_1(v)$ и $K_1(v')$, поскольку справочные части совпадают. Тогда из (28) следует, что $t' = t$ и слово $K(v_1)\dots K(v_t)$ является префиксом слова $K(v_1')\dots K(v_t')$. Так как эти слова имеют одинаковую длину $t(d+b+z)$, они обязаны совпасть, что влечёт совпадение кодовых слов $K(v)$ и $K(v')$.

2. Метод декодирования — восстановления по $K(v)$ некоторого доопределения слова v — включает два этапа.

На первом этапе сначала по начальной части $\widehat{m}\widehat{\lambda}\widehat{\mu}\widehat{|\tilde{w}_\Sigma|}$ кодового слова $K(v)$ находятся параметры m, λ и μ, а также длина слова $\tilde{w}_\Sigma$, позволяющая отделить справочную часть K_0 от основной части $K_1(v)$. Затем производится изложенная в начале п. 6 обработка справочной части кода, результатом которой является (λ,μ)-представительное множество доопределений $\mathcal{D}_{\lambda,\mu}$, упорядоченное лексикографически.

На втором этапе сначала по основной части $K_1(v)$ кода находятся параметры d, b, z, t. Затем представляющие их слова $\widehat{d}$, $\widehat{b}$, $\widehat{z}$, $\widehat{t}$ удаляются и остаток основной части разбивается на подслова длины $d+b+z$, задающие коды $K(v_i)$ кусков. Чтобы получить доопределение куска v_i, следует в соответствии с (27) разделить слово $K(v_i)$ на части длины d, b и z, найти в $\mathcal{D}_{\lambda,\mu}$ слово, номер которого при лексикографическом упорядочении задаётся первой частью кода, взять его начальное подслово, длина которого определяется второй частью, и осуществить в нём переименование символов в соответствии с третьей частью. Доопределение слова v образуется заменой кусков v_i полученными доопределениями кусков. ■

Приведём оценки характеристик кодирования при заданных параметрах λ и μ.

Лемма 8. Представленное кодирование частично определённых слов $v \in A^n$
1) обеспечивает длину кода

$$|K(v)| \leqslant h(v) + n\Big(\frac{C_9 \log\lambda}{\mu - \log\lambda - 2} + \frac{\mu + C_9\log\lambda}{\lambda}\Big) + \lambda^{C_6} 2^\mu + 2\log n;$$

2) выполнимо со сложностью, не превосходящей $(C_7)^\lambda + n\lambda^{C_{11}} 2^\mu$;
3) допускает декодирование, сложность которого не выше $(n + 2^\mu)\lambda^{C_{15}}$.

Доказательство. Утверждения 1 и 2 получены суммированием соответствующих результатов лемм 5 и 6. Член $C_{10}\lambda$, возникающий при суммировании длин, покрывается членом $\lambda^{C_6}2^\mu$ (при подходящем выборе константы C_6) и потому в результат не включён.

Декодирование следует плану, описанному в лемме 7. На реализацию первого этапа затрачивается не более $\lambda^{C_{12}}2^\mu$ операций (см. доказательство леммы 6). Возникающее (λ,μ)-представительное множество используется на втором этапе для декодирования кодов кусков $K(v_i)$. Выделение, обработка и декодирование кода $K(v_i)$ одного куска выполнимо с полиномиальной относительно λ сложностью. Число t кусков не превосходит n, поэтому декодирование всех кусков требует не более $n\lambda^{C_{15}}$ операций. Нетрудно видеть, что эта величина при подходящем выборе C_{15} покрывает также сложность других операций, используемых на втором этапе. Суммарная сложность обоих этапов составляет $\lambda^{C_{12}}2^\mu + n\lambda^{C_{15}}$. Назначив константу C_{15} превосходящей C_{12}, приходим к утверждению 3 леммы 8. ■

Введём функцию $\phi(n) \to \infty$, в терминах которой будет сформулирована оценка средней длины кода (см. замечание 1). Имеет смысл рассматривать лишь функции $\phi(n)$ с порядком роста меньше $\Big(\dfrac{\log n}{\log\log n}\Big)^{1/2}$, ибо иначе остаточный член $\mathrm{O}\Big(\phi(n)\Big(\dfrac{\log\log n}{\log n}\Big)^{1/2}\Big)$ не стремится к 0 и асимптотическая оптимальность кодирования не гарантируется. Будем считать, что функция $\phi(n)$ удовлетворяет условию

$$\phi(n) = \mathrm{o}\big(\log^{1/2}(n)\big). \tag{34}$$

Назначим параметры λ и μ, положив

$$\lambda = \left\lfloor \frac{\log n}{\phi^2(n)} \right\rfloor; \tag{35}$$

$$\mu = \left\lfloor \frac{(\log n \log\log n)^{1/2}}{\phi(n)} \right\rfloor. \tag{36}$$

Запись $\lfloor x \rfloor$ означает ближайшее целое к x снизу. Используя в лемме 8 эти значения параметров, получаем следующий факт.

Лемма 9. Если растущая функция $\phi(n)$ удовлетворяет условию (34), то метод кодирования частично определённых слов длины n, использущий значения параметров λ и μ из (35), (36),
1) обеспечивает оценку длины кода

$$|K(v)| \leqslant h(v) + \mathrm{O}\left(n\phi(n)\Big(\frac{\log\log n}{\log n}\Big)^{1/2}\right);$$

2) допускает кодирование и декодирование со сложностью $\mathrm{O}(n^2)$.

Доказательство.

1) Перепишем утверждение 1 леммы 8 в виде

$$|K(v)| - h(v) \leqslant A_1 + A_2 + A_3 + A_4, \tag{37}$$

где $A_1 = \dfrac{C_9 n \log\lambda}{\mu - \log\lambda - 2}$; $A_2 = \dfrac{n(\mu + C_9\log\lambda)}{\lambda}$; $A_3 = \lambda^{C_6} 2^{\mu}$; $A_4 = 2\log n$.

Из (35) с учётом (34) следует, что $\lambda \to \infty$ и, кроме того, $\log\lambda \leqslant \log\log n$. Сравнение равенств (35) и (36) показывает, что $\mu \geqslant (\lambda\log\lambda)^{1/2} - 1$, а потому $\log\lambda = \mathrm{o}(\mu)$ и имеют место асимптотические равенства $\mu - \log\lambda - 2 \sim \mu$ и $\mu + C_9\log\lambda \sim \mu$. Принимая их во внимание, получаем

$$\begin{aligned} A_1 &\sim \frac{C_9 n\log\lambda}{\mu} \lesssim \frac{C_9 n \log\log n\,\phi(n)}{(\log n\log\log n)^{1/2}} \lesssim C_9 n\,\phi(n)\Big(\frac{\log\log n}{\log n}\Big)^{1/2}, \\ A_2 &\sim \frac{n\mu}{\lambda} \sim \frac{n(\log n\log\log n)^{1/2}\phi(n)}{\log n} \sim n\,\phi(n)\Big(\frac{\log\log n}{\log n}\Big)^{1/2}. \end{aligned}$$

Из последнего соотношения следует, в частности, что $\log A_2 \sim \log n$. В то же время $\log A_3 = C_6\log\lambda + \mu \sim \mu = \mathrm{o}(\log n)$, а потому $\log A_3 = \mathrm{o}(\log A_2)$ и, тем более, $A_3 = \mathrm{o}(A_2)$. Очевидно также, что $A_4 = \mathrm{o}(A_2)$. Подстановка полученных соотношений в (37) даёт

$$|K(v)| - h(v) \lesssim (C_9 + 1) n\phi(n)\Big(\frac{\log\log n}{\log n}\Big)^{1/2},$$

а потому для некоторой константы C_{15} выполнено

$$|K(v)| \leqslant h(v) + C_{15} n\phi(n)\Big(\frac{\log\log n}{\log n}\Big)^{1/2}, \tag{38}$$

что влечет первое утверждение леммы.

2) Параметры λ и μ, заданные равенствами (35) и (36), удовлетворяют условиям $\lambda = \mathrm{o}(\log n)$ и $\mu = \mathrm{o}(\log n)$. Подстановки этих соотношений в оценки сложности кодирования и декодирования из п. 2 и 3 леммы 8 показывают, что каждая из этих оценок не превосходит $n^{1+\mathrm{o}(1)} \leqslant \mathrm{O}(n^2)$. Это даёт утверждение п. 2 леммы 9. ■

Следующее утверждение имеет место для недоопределённых источников $X = (A, P)$ в произвольном недоопределённом алфавите $A = \{a_T : T \in \mathcal{T}\}$.

Лемма 10. Если R — кодирование недоопределённого источника $X = (A, P)$ общего вида и для всякого слова $v \in A^n$ длина кодового слова удовлетворяет условию

$$K(v) \leqslant h(v) + G(n)$$

с некоторой функцией $G(n)$ (не зависящей от v), то для средней длины кода K справедлива оценка

$$\bar{l}_K^{(n)} \leqslant \mathcal{H}(P) + \frac{G(n)}{n}.$$

Доказательство. Обозначим через $p(P, \mathbf{r}, n)$ суммарную вероятность слов класса $\mathcal{K}_n(\mathbf{r})$, $\mathbf{r} = (r_T, T \in \mathcal{T})$. Вероятности $p(P, \mathbf{r}, n)$ имеют вид

$$p(P, \mathbf{r}, n) = \frac{n!}{\prod\limits_{T\in\mathcal{T}} r_T!} \prod_{T\in\mathcal{T}} p_T^{r_T}$$

и образуют полиномиальное (мультиномиальное) распределение [24]. При каждом наборе вероятностей P оно обладает свойствами

$$\sum_{\mathbf{r}} p(P,\mathbf{r},n)=1, \qquad \sum_{\mathbf{r}} p(P,\mathbf{r},n)\frac{r_T}{n}=p_T \quad (T\in\mathcal{T}), \tag{39}$$

где r_T и p_T — компоненты наборов $\mathbf{r}$ и P.

В выражении (3) для средней длины кода $\bar{l}_K^{(n)}$ сгруппируем слова $v\in A^n$, принадлежащие одному частотному классу, и, воспользовавшись условиями леммы и тем, что слова класса $\mathcal{K}_n(\mathbf{r})$ имеют одинаковую квазиэнтропию $h(v)=h_n(\mathbf{r})=\mathbf{n}\mathcal{H}\Big(\dfrac{\mathbf{r}}{\mathbf{n}}\Big)$, придём к оценке

$$\bar{l}_K^{(n)}\leqslant\sum_{\mathbf{r}} p(P,\mathbf{r},n)\mathcal{H}\Big(\frac{\mathbf{r}}{n}\Big)+\sum_{\mathbf{r}} p(P,\mathbf{r},n)\frac{G(n)}{n}=\Sigma_1+\Sigma_2.$$

Оценим Σ_1, применив к вогнутой функции $\mathcal{H}$ (п. 2° леммы 1) неравенство Йенсена и второе равенство из (39). В результате имеем

$$\Sigma_1\leqslant\mathcal{H}\left(\sum_{\mathbf{r}} p(P,\mathbf{r},n)\frac{\mathbf{r}}{n}\right)=\mathcal{H}(P).$$

Первое равенство из (39) в применении к Σ_2 даёт $\Sigma_2=\dfrac{G(n)}{n}$. Утверждение леммы получается заменой Σ_1 и Σ_2 в оценке для $\bar{l}_K^{(n)}$ величинами $\mathcal{H}(P)$ и $\dfrac{G(n)}{n}$. ■

Лемма 11. Для любого частично определённого источника $X=(A,P)$ и любой функции $\phi(n)\to\infty$ имеется способ кодирования K, обеспечивающий оценку средней длины кода

$$\bar{l}_K^{(n)}\leqslant\mathcal{H}(P)+\mathrm{O}\left(\phi(n)\Big(\frac{\log\log n}{\log n}\Big)^{1/2}\right)$$

и допускающий кодирование и декодирование со сложностью $\mathrm{O}(n^2)$.

Доказательство. Если $\phi(n)$ удовлетворяет условию (34), то нужное утверждение получается из леммы 9 путём применения леммы 10 к неравенству (38).

Если условмие (34) нарушено, следует рассмотреть произвольную функцию $\phi'(n)\to\infty$, удовлетворяющую условиям $\phi'(n)\leqslant\phi(n)$ и (34). Утверждение леммы, справедливое по доказанному для функции $\phi'(n)$, будет верно и для исходной функции $\phi(n)$, которая не меньше $\phi'(n)$. ■

Утверждение теоремы 2 вытекает из леммы 11 при $\phi(n)=(\log\log n)^{1/2}$.

ЛИТЕРАТУРА

1. *Галлагер Р.* Теория информации и надежная связь. М.: Сов. радио, 1974. 720 с.
2. *Шоломов Л. А.* Элементы теории недоопределённой информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.
3. *Шоломов Л. А.* Сжатие частично определенной информации // Нелинейная динамика и управление. Вып. 4. М.: Физматлит, 2004. С. 377–396.
4. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1979. 536 с.
5. *Шоломов Л. А.* Энтропия системы частично определенных последовательностей с вложенными областями определения // Нелинейная динамика и управление. Вып. 3. М.: Физматлит, 2003. С. 305–320.

6. *Колмогоров А. Н.* Три подхода к определению понятия «количество информации» // Проблемы передачи информации. 1965. Т. 1. № 1. С. 3–11.
7. *Чашкин А. В.* Дискретная математика. М.: Академия, 2012. 352 с.
8. *Шеннон К. Э.* Синтез двухполюсных переключательных схем // Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 59–101.
9. *Лупанов О. Б.* Об одном подходе к синтезу схем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. М.: Наука, 1965. С. 31–110.
10. *Нечипорук Э. И.* О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // Докл. АН СССР. 1965. Т. 163. № 1. С. 40–43.
11. *Шоломов Л. А.* О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 21. М.: Наука, 1969. С. 215–226.
12. *Андреев А. Е.* О реализации частичных булевых функций схемами из функциональных элементов // Дискретная математика. 1989. Вып. 4. С. 36–45.
13. *Чашкин А. В.* Методы вычисления частичных булевых функций // Дискретные модели в теории управляющих систем: VII Междунар. конф. М.: МАКС Пресс, 2006. С. 390–404.
14. *Шоломов Л. А.* О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. М.: Наука, 1967. С. 123–139.
15. *Andreev A. E., Clementi A. E. F., and Rolim J. D. P.* Worst-case hardness suffices for derandomization: A new method for hardness–randomness trade-offs // LNCS. 1997. V. 1256. 1997. P. 177–187.
16. *Miltersen P. B.* On the Shannon function for partially defined Boolean functions. `http://www.brics.dk/~bromille/Papers/index.html`. 1999.
17. *Мадатян Х. А.* О реализации не всюду определенных k-значных матриц заданной «густоты» вентильными схемами глубины два // Методы дискретного анализа в теории булевых функций и схем. Вып. 35. Новосибирск: ИМ СО АН, 1980. С. 71–82.
18. *Andreev A. E.* Complexity of Nondeterministic Functions. BRICS report. Ser. RS-94-2. Febr. 1994. 47 p.
19. *Чашкин А. В.* Вычисление недоопределенных функций // Дискретная математика и ее приложения. Сб. лекций молодежных научных школ. Вып. VI. М.: ИПМ РАН, 2011. С. 29–40.
20. *Krichevsky R. E.* Occam's razor, partially specified Boolean functions, string matching, and independent sets // Information and Computation. 1994. Iss. 108. P. 158–174.
21. *Кричевский Р. Е.* Сжатие и поиск информации. М.: Радио и связь, 1989. 168 с.
22. *Шоломов Л. А.* Кодирование частично определенных дискретных источников без памяти // Докл. АН. 2004. Т. 397. № 2. С. 178–180.
23. *Васильев Ю. Л., Глаголев В. В.* Метрические свойства дизъюнктивных нормальных форм // Дискретная математика и математические вопросы кибернетики. Т. 1. М.: Наука, 1974. С. 99–148.
24. *Крамер Г.* Математические методы статистики. М.: Мир, 1975. 648 с.

REFERENCES

1. *Gallager R. G.* Information Theory and Reliable Communication. N.Y., Wiley Publ., 1968. 608 p.
2. *Sholomov L. A.* Elementy teorii nedoopredelennoy informatsii [Elements of the underdetermined information theory]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2009, no. 2, pp. 18–42. (in Russian)

3. *Sholomov L. A.* Szhatie chastichno opredelennoy informatsii [Compression of partial defined information]. Nelineinaya dinamika i upravlenie, vol. 4, Moscow, Fizmatlit, 2004, pp. 377–396. (in Russian)
4. *Aho A., Hopcroft J., and Ulman J.* The Design and Analisis of Computer Algorithms. Addison-Wesley Publ. Co, 1976. 480 p.
5. *Sholomov L. A.* Entropiya sistemy chastichno opredelennih posledovatelnoctei s vlozhennimi oblastyami opredeleniya [Entropy of a system of partially defined sequences with nested domains]. Nelineinaya Dinamika i Upravlenie, vol. 3, Moscow, Fizmatlit Publ., 2003, pp. 305–320. (in Russian)
6. *Kolmogorov A. N.* Three approaches to the quantitative definition of information. Problems Inform. Transmissions, 1965, no. 1, pp. 1–7.
7. *Chashkin A. V.* Diskretnaya matematika [Discrete Mathematics]. Moscow, Academia, 2012. 352 p. (in Russian)
8. *Shannon C. E.* The synthesis of two-terminal switching circuits. Bell Syst. Techn. J., 1949, vol. 28, no. 1. pp. 59–98.
9. *Lupanov O. B.* Ob odnom podhode k sintezu upravlyayushchikh sistem — printsipe lokalnogo kodirovaniya [On a certain approach to the synthesis of control systems — the principle of local coding]. Problemy Kibernetiki, iss. 14, Moscow, Nauka Publ., 1965, pp. 31–110. (in Russian)
10. *Nechiporuk E. I.* Complexity of gating circuits which are realized by Boolean matrices with undetermined elements. Soviet Phis. Dokl., 1966, iss. 10, pp. 591–593.
11. *Sholomov L. A.* Realization of partial Boolean functions by circuits from functional elements. Systems Theory Res., 1971, iss. 21, pp. 211–223.
12. *Andreev A. E.* On the complexity of the realization of Boolean functions by circuits of functional elements. Discrete Math. Appl., 1991, vol. 1, iss. 3, pp. 251–261.
13. *Chashkin A. V.* Metody vychisleniya chastichnyh bulevyh funktsii [Methods for computing partial Boolean functions.] Diskretnye Modeli v Teorii Upravlyayushchih Sistem: VII Mezhdunarodnaya Konferentsiya. Moscow, MAKS Press, 2006, pp. 390–404. (in Russian)
14. *Sholomov L. A.* On functionals characterizing the complexity of systems of undetermined Boolean functions. Systems Theory Res., 1970, iss. 20, pp. 123–140.
15. *Andreev A. E., Clementi A. E. F., and Rolim J. D. P.* Worst-case hardness suffices for derandomization: A new method for hardness–randomness trade-offs. LNCS, 1997, vol. 1256, pp. 177–187.
16. *Miltersen P. B.* On the Shannon function for partially defined Boolean functions. `http://www.brics.dk/~bromille/Papers/index.html`. 1999.
17. *Madatyan H. A.* O realizatsii ne vsyudu opredelennyh k-znachnyh matrits zadannoy "gustoty" ventilnymi shemami glubiny dva [On the implementation of not everywhere defined k-valued matrices of a given "density" by valve circuits of depth two]. Metody Diskretnogo Analiza v Teorii Bulevyx Funktsiy i Skhem, iss. 35, Novosibirsk, Institute of Mathematics Publ. House, 1980, pp. 71–82. (in Russian)
18. *Andreev A. E.* Complexity of nondeterministic functions. BRICS report Series, RS-94-2, Febr. 1994. 47 p.
19. *Chashkin A. V.* Vychislenie nedoopredelennyh funktsii [Computing of underdetermined functions.] Diskretnaya Matematika i ee Prilozheniya. Sbornik Lektsiy Molodezhnyh Nauchnyh Shkol, VI, Moscow, Keldysh Inst. of Appl. Math. Publ. House, 2011, pp. 29–40. (in Russian)
20. *Krichevsky R. E.* Occam's razor, partially specified Boolean functions, string matching, and independent sets. Information and Computation, 1994, iss. 108, pp. 158–174.
21. *Krichevsky R.* Universal Compression and Retrieval. Kluwer Acad. Publ., 2010. 219 p.

22. *Sholomov L. A.* Encoding of partially defined discrete memoryless sources. Doclady Mathematics, 2004, vol, 70, no. 1, pp. 651–653.
23. *Vasil'ev Yu. L. and Glagolev V. V.* Metricheskie svoystva diz"yunktivnykh normal'nykh form [Metric properties of disjunctive normal forms]. Discrete Mathematics and Mathematical Problems of Cybernetics, vol. 1, Moscow, Nauka, 1974, pp. 99–148. (in Russian)
24. *Cramer H.* Mathematical Methods of Statistics. Prinston University Press, 1946. 575 p.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.175.3

ЧИСЛО ПОМЕЧЕННЫХ ТЕТРАЦИКЛИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНО-ПАРАЛЛЕЛЬНЫХ БЛОКОВ

В. А. Воблый

Всероссийский институт научной и технической информации РАН, г. Москва, Россия

Последовательно-параллельный граф — это граф, не содержащий в качестве минора полный граф с четырьмя вершинами. Такие графы используются при построении надёжных коммуникационных сетей. Получена явная формула для числа помеченных последовательно-параллельных тетрациклических графов с заданным числом вершин. Доказано, что при равномерном распределении вероятностей вероятность того, что помеченный тетрациклический блок является последовательно-параллельным графом, асимптотически равна 3/11.

Ключевые слова: *помеченный граф, тетрациклический граф, последовательно-параллельный граф, блок, перечисление, асимптотика.*

DOI 10.17223/20710410/47/5

THE NUMBER OF LABELED TETRACYCLIC SERIES-PARALLEL BLOCKS

V. A. Voblyi

All-Russian Institut for Scientific and Technical Information, Moscow, Russia

E-mail: vitvobl@yandex.ru

A series-parallel graph is a graph that does not contain a complete graph with four vertices as a minor. Such graphs are used in the construction of reliable communication networks. Let $TB(n)$ be the number of labeled series-parallel tetracyclic blocks with n vertices. The formula $TB(n) = \dfrac{n!}{80640}(n^5 + 30n^4 + 257n^3 + 768n^2 + 960n + 504)\binom{n-3}{3}$ is obtained. It is proved that with a uniform probability distribution, the probability that the labeled tetracyclic block is a series-parallel graph is asymptotically 3/11.

Keywords: *labeled graph, tetracyclic graph, series-parallel graph, block, enumeration, asymptotics.*

Введение

Рассматриваются неориентированные простые связные графы.

Точкой сочленения связного графа называется его вершина, после удаления которой вместе с инцидентными ей рёбрами граф становится несвязным. *Блок* — это связный граф без точек сочленения, а также максимальный связный нетривиальный под-

граф, не имеющий точек сочленения. Граф называется *последовательно-параллельным*, если он не содержит минора, являющегося полным графом K_4 [1]. *Цикломатическим числом* связного графа называется увеличенная на единицу разность между числом рёбер и вершин графа. *k-Циклический граф* — это граф с цикломатическим числом k.

Последовательно-параллельные графы используются при построении надёжных коммуникационных сетей [2]. Целый ряд задач алгоритмической теории графов, являющихся NP-полными для произвольных графов, может быть решён полиномиальными алгоритмами в классе последовательно-параллельных графов [3].

В [1] найдена асимптотика для чисел помеченных связных и 2-связных последовательно-параллельных графов с большим количеством вершин. В [4] перечислены помеченные последовательно-параллельные связные графы и блоки по числу вершин. В [5] найдены числа помеченных последовательно-параллельных трициклических блоков с заданным числом вершин. В данной работе получена явная формула для числа помеченных последовательно-параллельных тетрациклических блоков с заданным числом вершин.

1. Перечисление графов

Теорема 1. Число $TB(n)$ помеченных последовательно-параллельных тетрациклических блоков с n вершинами при $n \geqslant 6$ равно

$$TB(n) = \frac{n!}{80640}(n^5 + 30n^4 + 257n^3 + 768n^2 + 960n + 504)\binom{n-3}{3}. \qquad (1)$$

Доказательство. Гомеоморфный тип — это общий граф (возможно, содержащий петли или кратные рёбра) без вершин степени 2, из которого все графы из заданного класса гомеоморфных графов получаются вставкой вершин степени 2 [6, 7]. Из 17 гомеоморфных типов тетрациклических блоков из списка Хипа только 6 не являются последовательно-параллельными графами [8]. Диаграммы этих блоков представлены на рис. 1.

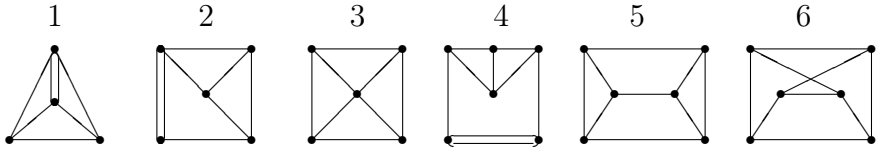


Рис. 1

Пусть H — гомеоморфный тип с a вершинами, b ребрами, b_0 петлями, b_i — число пучков рёбер кратности i, $A(H)$ — порядок вершинно-рёберной группы автоморфизмов графа H. Тогда число помеченных графов C_n с n вершинами и гомеоморфным типом H равно [7, лемма 2]

$$C_n = \frac{n!}{2^{b_0}A(H)}\mathrm{Coef}_{x^{n-a}}\frac{x^{b+b_0-\sum\limits_{i=1}^{b} b_i}\prod\limits_{i=1}^{b}(x + i(1-x))^{b_i}}{(1-x)^b}.$$

В нашем случае имеем
1) $a = 4$, $b = 7$, $A(H) = 8$, $b_0 = 0$, $b_1 = 5$, $b_2 = 1$,

$$C_{1,n} = \frac{n!}{8}\mathrm{Coef}_{x^{n-4}}\frac{x(x+2(1-x))}{(1-x)^7} = \frac{n!}{8}\mathrm{Coef}_{x^{n-4}}\Big(\frac{x^2}{(1-x)^7} + 2\frac{x}{(1-x)^6}\Big)\,.$$

С помощью известного разложения [9, с. 709]

$$(1-w)^{-m-1} = \sum_{n=0}^{\infty}\binom{m+n}{m}w^n$$

получим

$$C_{1,n} = \frac{n!}{8}\mathrm{Coef}_{x^{n-4}}\left(\sum_{k=0}^{\infty}\binom{k+6}{6}x^{k+2} + 4\sum_{k=0}^{\infty}\binom{k+5}{4}x^{k+1}\right) = \frac{n!}{8}\left(\binom{n}{6} + 2\binom{n}{5}\right).$$

Аналогично для остальных гомеоморфных типов графов:
2) $a = 5$, $b = 8$, $A(H) = 4$, $b_0 = 0$, $b_1 = 6$, $b_2 = 1$,

$$C_{2,n} = \frac{n!}{4}\mathrm{Coef}_{x^{n-5}}\frac{x(x+2(1-x))}{(1-x)^8} =$$
$$= \frac{n!}{4}\mathrm{Coef}_{x^{n-5}}\left(\sum_{k=0}^{\infty}\binom{k+7}{7}x^{k+2} + 2\sum_{k=0}^{\infty}\binom{k+6}{6}x^{k+1}\right) = \frac{n!}{4}\left(\binom{n}{7} + 2\binom{n}{6}\right);$$

3) $a = 5$, $b = 8$, $A(H) = 8$, $b_0 = 0$, $b_1 = 8$,

$$C_{3,n} = \frac{n!}{8}\mathrm{Coef}_{x^{n-5}}\frac{1}{(1-x)^8} = \frac{n!}{8}\mathrm{Coef}_{x^{n-5}}\left(\sum_{k=0}^{\infty}\binom{k+7}{7}x^{k}\right) = \frac{n!}{8}\binom{n+2}{7};$$

4) $a = 6$, $b = 9$, $A(H) = 8$, $b_0 = 0$, $b_1 = 7$, $b_2 = 1$,

$$C_{4,n} = \frac{n!}{8}\mathrm{Coef}_{x^{n-5}}\frac{x(x+2(1-x))}{(1-x)^8} =$$
$$= \frac{n!}{4}\mathrm{Coef}_{x^{n-6}}\left(\sum_{k=0}^{\infty}\binom{k+8}{8}x^{k+2} + 2\sum_{k=0}^{\infty}\binom{k+7}{7}x^{k+1}\right) = \frac{n!}{8}\left(\binom{n}{8} + 2\binom{n}{7}\right);$$

5) $a = 6$, $b = 9$, $A(H) = 12$, $b_0 = 0$, $b_1 = 9$,

$$C_{5,n} = \frac{n!}{12}\mathrm{Coef}_{x^{n-6}}\frac{1}{(1-x)^9} = \frac{n!}{12}\mathrm{Coef}_{x^{n-6}}\left(\sum_{k=0}^{\infty}\binom{k+8}{8}x^{k}\right) = \frac{n!}{12}\binom{n+2}{8};$$

6) $a = 6$, $b = 9$, $A(H) = 72$, $b_0 = 0$, $b_1 = 9$,

$$C_{6,n} = \frac{n!}{72}\mathrm{Coef}_{x^{n-6}}\frac{1}{(1-x)^9} = \frac{n!}{12}\mathrm{Coef}_{x^{n-6}}\left(\sum_{k=0}^{\infty}\binom{k+8}{8}x^{k}\right) = \frac{n!}{72}\binom{n+2}{8}.$$

Таким образом, число $\bar{C}_n$ не последовательно-параллельных блоков равно

$$\frac{n!}{8}\left(\binom{n}{6} + 2\binom{n}{5}\right) + \frac{n!}{4}\left(\binom{n}{7} + 2\binom{n}{6}\right) + \frac{n!}{8}\binom{n+2}{7} +$$
$$+\frac{n!}{8}\left(\binom{n}{8} + 2\binom{n}{7}\right) + \frac{n!}{12}\binom{n+2}{8} + \frac{n!}{72}\binom{n+2}{8}.$$

Пусть $u(n, n+3)$ — число помеченных блоков с n вершинами и $n+3$ рёбрами (тетрациклических блоков). Э. Райт получил формулу [10]

$$u(n,n+3)=\frac{n!}{720}\left(220\binom{n+3}{8}+275\binom{n+2}{+}120\binom{n+1}{6}-30\binom{n}{5}-\right.$$
$$\left.-117\binom{n-1}{4}-126\binom{n-2}{3}-72\binom{n-3}{2}\right).$$

Вычитая из числа всех тетрациклических блоков число тетрациклических не последовательно-параллельных блоков и приводя подобные члены, найдём $TB(n)$:

$$TB(n)=u(n,n+3)-\bar{C}_n=\frac{n!}{720}\left(220\binom{n+3}{8}+185\binom{n+2}{7}+120\binom{n+1}{6}-\right.$$
$$-210\binom{n}{5}-117\binom{n-1}{4}-126\binom{n-2}{3}-72\binom{n-3}{2}-450\binom{n}{6}-$$
$$\left.-360\binom{n}{7}-90\binom{n}{8}-70\binom{n+2}{8}\right).$$

Полученное выражение для $TB(n)$ ненамного длиннее формулы Райта для $u(n, n+3)$ и пригодно для вычисления. Представляя биномиальные коэффициенты в виде многочленов от n, после приведения подобных членов и выделения линейных множителей в полученном многочлене найдём компактную формулу (1). ■

2. Асимптотика и вероятность

Так как $\binom{n}{k}\sim\frac{n^k}{k!}$ при $n\to\infty$ и фиксированном k, из (1) получаем

Следствие 1. При $n\to\infty$ верно асимптотическое равенство

$$TB(n)\sim\frac{n^8}{483840}n!\,.$$

Зададим на множестве помеченных тетрациклических блоков с n вершинами равномерное распределение вероятностей.

Следствие 2. Пусть P_n — вероятность того, что помеченный тетрациклический блок с n вершинами является последовательно-параллельным графом. При $n\to\infty$ верна асимптотика $P_n\sim\frac{3}{11}$.

Доказательство. Очевидно, для $u(n, n+3)$ при $n\to\infty$ имеем асимптотику $u(n,n+3)\sim\frac{11n^8}{36\cdot 8!}n!$. Поэтому $P_n=\frac{TB(n)}{u(n,n+3)}\sim\frac{3}{11}$ при $n\to\infty$. ■

В таблице представлены числа $TB(n)$, вычисленные с помощью теоремы 1 и пакета программ Maple.

n	6	7	8	9	10	11
$TB(n)$	1215	55461	1722840	46312560	1171648800	29004544800

ЛИТЕРАТУРА

1. *Bodirsky M., Gimenez O., Kang M., and Noy M.* Enumeration and limit laws of series-parallel graphs // European J. Combinatorics. 2007. V. 28. P. 2091–2105.
2. *Radhavan S.* Low-connectivity network design on series-parallel graphs // Networks. 2004. V. 43. No. 3. P. 163–176.
3. *Takamizawa K., Nishezeki T., and Saito N.* Linear-time computability of combinatorial problems on series-parallel graphs // J. ACM. 1982. V. 29. No. 3. P. 623–641.
4. *Воблый В. А.* Второе соотношение Риддела и следствия из него // Дискретн. анализ и исследование операций. 2019. Т. 26. № 1. С. 20–32.
5. *Воблый В. А., Мелешко А. М.* О числе помеченных последовательно-параллельных трициклических блоков // Материалы XV Междунар. конф. «Алгебра, теория чисел и дискретная геометрия. Современные проблемы и приложения». Тула: Изд-во ТПГУ, 2018. С. 168–170.
6. *Ford G. W. and Uhlenbeck G. E.* Combinatorial problems in theory graphs. IV // Proc. Nat. Acad. Sci. USA. 1957. V. 43. P. 163–167.
7. *Степанов В. Е.* О некоторых особенностях строения случайного графа вблизи критической точки // Теория вероятн. и ее применения. 1987. Т. 32. Вып. 4. С. 633–657.
8. *Heap B. R.* Enumeration homeomorphically irreducible star graphs // J. Math. Phys. 1966. V. 7. No. 7. P. 1582–1587.
9. *Прудников А. П. и др.* Интегралы и ряды. Т. 1. М.: Наука, ГРФМЛ, 1981. 800 с.
10. *Wright E. M.* The number of connected sparsely edges graphs. II // J. Graph Theory. 1978. V. 2. P. 299–305.

REFERENCES

1. *Bodirsky M., Gimenez O., Kang M., and Noy M.* Enumeration and limit laws of series-parallel graphs. European J. Combinatorics, 2007, vol. 28, pp. 2091–2105.
2. *Radhavan S.* Low-connectivity network design on series-parallel graphs. Networks, 2004, vol. 43, no. 3, pp. 163–176.
3. *Takamizawa K., Nishezeki T., and Saito N.* Linear-time computability of combinatorial problems on series-parallel graphs. J. ACM, 1982, vol. 29, no. 3, pp. 623–641.
4. *Voblyy V. A.* Vtoroye sootnosheniye Riddella i sledstviya iz nego [The second Riddell relation and its consequences]. Diskretn. analiz i issled. oper., 2019, vol. 26, no. 1, pp. 20–32. (in Russian)
5. *Voblyy V. A. and Meleshko K. A.* O chisle pomechennykh parallel'nykh tritsiklicheskikh blokov [On the number of labeled series-parallel tricyclic blocks.] Proc. Intern. Conf. "Algebra, Teoriya Chisel i Diskretnaya Geometriya. Sovremennyye Problemy i Prilozheniya", Tula, TPSU Publ., 2018, pp. 168–170. (in Russian)
6. *Ford G. W. and Uhlenbeck G. E.* Combinatorial problems in theory graphs. IV. Proc. Nat. Acad. Sci. USA, 1957, vol. 43, pp. 163–167.
7. *Stepanov V. E.* O nekotorykh osobennostyakh stroeniya sluchaynogo grapha vblizi kriticheskoy tohki [On some features of the structure of a random graph near a critical point]. Teoriya Veroyatn. Primen., 1987, vol. 32, no. 4, pp. 633–657. (in Russian)
8. *Heap B. R.* Enumeration homeomorphically irreducible star graphs. J. Math. Phys., 1966, vol. 7, no. 7, pp. 1582–1587.
9. *Prudnikov A. P. et al.* Integraly i ryady [Integrals and Series]. Vol. 1, Moscow, Nauka Publ., 1981. 800 p. (in Russian)
10. *Wright E. M.* The number of connected sparsely edges graphs. II. J. Graph Theory, 1978, vol. 2, pp. 299–305.

УДК УДК 519.17+519.24

ДЕКОМПОЗИЦИЯ СЕТИ ПО СЕЧЕНИЯМ ПРИ РАСЧЁТЕ ЕЁ НАДЁЖНОСТИ[1]

Д. А. Мигов

Институт вычислительной математики и математической геофизики СО РАН, г. Новосибирск, Россия

Рассматривается задача расчёта такого показателя надёжности сети, как вероятность связности соответствующего случайного графа. Предполагается, что рёбра сети подвержены отказам, которые происходят независимо друг от друга с заданными вероятностями. Узлы сети полагаются абсолютно надёжными. Приводится общая методика получения формул, выражающих надёжность сети с сечением (вершинным разрезом) через надёжности её подсетей, получаемых при декомпозиции по сечению, а также через надёжности всевозможных вариантов стягивания таких подсетей по разрезающим вершинам. На её основе выводятся такие формулы для сечений из двух, трёх и четырёх вершин. Для двусвязных структур описаны математический аппарат и алгоритм, позволяющие при расчёте их надёжности эффективно учитывать все двухвершинные сечения. Приводятся результаты численных экспериментов, демонстрирующие применимость предлагаемых методов.

Ключевые слова: *надёжность сети, случайный граф, вероятность связности, метод факторизации, декомпозиция сети, сечение, разрез.*

DOI 10.17223/20710410/47/6

VERTEX DECOMPOSITION TO CALCULATE THE NETWORK PROBABILISTIC CONNECTIVITY

D. A. Migov

Institute of Computational Mathematics and Mathematical Geophysics of SB RAS, Novosibirsk, Russia

E-mail: mdinka@rav.sscc.ru

We consider the problem of calculating such an indicator of network reliability as the random graph probabilistic connectivity. It is assumed that the edges of the network are subject to failures that occur independently of each other with given probabilities. Network nodes are assumed to be absolutely reliable. The possibility of using network decomposition via vertex cuts for the network reliability calculation is investigated. By cut we mean a set of network elements, the removal of which makes the network disconnected. The history of the development of such methods is given, and the place of our results is indicated among them. The results related to the case of two nodes cuts are presented in detail, including the results of the author and R. K. Wood (1985). Next, we consider the cuts of arbitrary power. The results in this area were obtained by the author (2004–2008) and J. M. Burgos (2016). Also, certain results using cuts were obtained by the author for the cumulative bounds

[1]Работа поддержана грантом РФФИ № 18-07-00460 и ПФИ ИВМиМГ СО РАН № 0315-2016-0006.

updating of the random graph probabilistic connectivity (2012) and for the diameter constrained reliability calculation (2011–2012). Author results include the general method, which gives the formulas expressing the reliability of a network with a vertex cut through the reliabilities of its subnets obtained by cut decomposition, as well as through reliabilities of the subnets, contracted by all possible variants over cut vertices. On its basis, we derive such formulas for cuts of two, three, and four vertices. Some of the results of the author were previously published; some results are published for the first time, including the correct formula for four vertices cut and the valid proof of the solvability of a system of linear equations, which guarantees the existence of the above mentioned formulas. The results of numerical experiments showing the applicability of the proposed methods are given. For example, using the 3 cut formula the reliability calculation of the 3×16 grid shows an acceleration of about 120 times compared with the factoring method. For biconnected structures, a mathematical apparatus and an algorithm are given that make it possible to effectively take into account all two-vertex sections when calculating their reliability. Without such an approach we should use above mentioned cut formulas recursively, for graphs obtained by cut decomposition and for these graphs contracted by all possible variants over cut vertices. This inevitably leads to recalculation of reliability for certain graphs. Using the proposed algorithm allows to avoid such recalculation and additionally speeds up the reliability calculation for suitable network structures.

Keywords: *network reliability, random graph, probabilistic connectivity, factoring method, network decomposition, vertex cut, edge cut.*

Введение

При проектировании и оптимизации сетей различного назначения одной из важнейших задач является обеспечение их надёжного функционирования. В большинстве случаев при анализе надёжности сетей используют такой математический объект, как случайный граф [1]. Элементы случайного графа присутствуют с заданными вероятностями, что описывает надёжность соответствующих элементов моделируемой сети. В качестве показателей надёжности сети могут быть рассмотрены различные характеристики случайного графа.

Наиболее распространённым показателем стала вероятность связности подмножества вершин случайного графа с ненадёжными рёбрами [2], описывающая надёжность сети с точки зрения возможности установления соединения между каждой парой узлов сети из выделенного подмножества узлов сети — полюсов (k-terminal network reliability). При совпадении этого подмножества с множеством всех узлов сети получаем вероятность связности (all-terminal network reliability). Отдельно выделяют случай двух полюсов (2-terminal network reliability). Данные характеристики случайного графа долгое время были объектом всестороннего изучения, что сделало их «классическими» показателями сетевой надёжности.

Для каждого из указанных показателей задача его расчёта является NP-трудной [3], соответственно точный расчёт требует экспоненциальной трудоёмкости. Это, однако, не помешало развитию точных методов, наиболее известными из которых стали метод факторизации (ветвления, Мура — Шеннона) и его модификации [4] и логико-вероятностные методы на основе так называемой бинарной диаграммы решения (Binary Decision Diagram (BDD)) [5]. Отдельным направлением стала разработка универсальных методов преобразований графа (Reliability Preserved Graph Transformation (RPGT)), основанных, как правило, на редукции, которые позволяют переходить

к рассмотрению графа меньшей размерности. Методы включают в себя такие преобразования, как последовательно-параллельное [6], «многоугольник-на-цепь» [7] и «треугольник-звезда» [8].

С 90-х годов прошлого века вводятся в рассмотрение и активно изучаются различные другие показатели, что связано, в первую очередь, с резко возросшей потребностью в использовании объектов сетевой структуры нового типа. Для адекватного описания надёжности новых типов сетей уже не могут быть использованы классические показатели сетевой надёжности. Отметим беспроводные сенсорные сети [9], иерархические сети [10], сети с ограничением на количество транзитных узлов при передаче информации [11]. Трудоёмкость расчёта надёжности таких сетей, как правило, значительно превосходит трудоёмкость расчёта классических показателей сетевой надёжности. Классические показатели при этом не теряют своей актуальности и также продолжают активно исследоваться. Развиваются как приближённые алгоритмы [12], так и методы точного расчёта, в том числе BDD-методы [5]. Приведём краткий обзор важных результатов в данной области, полученных за последние 20 лет, исчерпывающие обзоры более ранних результатов можно найти в [2].

Приближённые алгоритмы основываются, как правило, на методах статистического моделирования [12] либо на структурном анализе графа в условиях различных предположений на входные данные. Важные результаты в этом направлении получены в работах Г. Ш. Цициашвили, М. А. Осиповой, А. С. Лосева [13]. Работы этого коллектива посвящены изучению асимптотических формул для вероятности связности графов с высоконадёжными либо с низконадёжными рёбрами, в том числе для планарных графов.

В области разработки точных методов за это время также получены важные результаты [14 – 18], что обусловлено в основном бурным развитием вычислительной техники. Отметим, в первую очередь, принципиально новый подход с разложением по остовному дереву [17]. С помощью него можно осуществлять точный расчёт вероятности связности графа, что в некоторых случаях оказалось предпочтительнее метода ветвления. Этот подход может быть использован и для оценки надёжности. А. С. Родионовым и О. К. Родионовой предложена модификация метода факторизации, позволяющая осуществлять ветвление по цепям произвольной длины [15]. В работах указанных авторов и Д. А. Мигова [16] получен также ряд формул для быстрого расчёта надёжности графов малой размерности, что значительно ускоряет расчёт надёжности сетей произвольной размерности с использованием факторизации. В [18] аналитически выведено несколько формул для выражения вероятности связности подмножества вершин графа через вероятности связности графов, построенных специальным образом на всевозможных разбиениях множества вершин с использованием функции Мёбиуса.

Одним из наиболее значимых результатов стал метод кумулятивного уточнения верхней и нижней границ надёжности сети [19]. При этом подходе необязательно осуществлять исчерпывающий расчёт, достаточно определить, пересекает ли верхняя или нижняя граница требуемый уровень, что позволяет принять решение о надёжности/ненадёжности сети по отношению к установленному порогу. За основу в качестве метода расчёта может быть взят как метод факторизации, так и логико-вероятностные методы и метод разложения по остовному дереву. Подход был далее развит в [20], в том числе и на другие показатели надёжности. Отдельным направлением стала разработка параллельных методов расчёта надёжности, как приближённых [21], так и точных [22].

Более полный обзор методов анализа сетевой надёжности можно найти, например, в [23].

Таким образом, к настоящему времени разработан обширный математический и алгоритмический аппарат для анализа показателей сетевой надёжности. Данный аппарат предоставляет различные инструменты: методы редукции и декомпозиции, кумулятивное уточнение границ, параллельные методы, имитационное моделирование, генетические алгоритмы и другие методы, обеспечивающие в совокупности возможность анализа надёжности сетей практически интересной размерности на современных вычислительных системах за приемлемое время. При этом для сетей из сотен элементов зачастую возможно осуществить точный расчёт их надёжности.

В данной работе рассматриваются классические показатели надёжности сетей с ненадёжными рёбрами и абсолютно надёжными узлами. Для таких сетей исследуется возможность применения декомпозиции по сечениям для расчёта надёжности. Под сечением понимается вершинный разрез, т. е. множество узлов, удаление которых делает сеть несвязной. В п. 1 приводится история развития подобных методов и обозначено место работ автора среди них. В п. 2 даны необходимые определения, в п. 3 изложены результаты автора, касающиеся случая с сечением произвольной мощности. В основном эти результаты ранее были опубликованы, за исключением доказательства разрешимости системы линейных уравнений, что даёт возможность корректного применения предлагаемых декомпозиционных методов. В п. 4 содержатся новые результаты, позволяющие эффективно использовать сразу все двухвершинные сечения произвольной двусвязной сети для расчёта её надёжности, что на порядки ускоряет расчёт для подходящих структур сетей.

1. Обзор методов расчёта надёжности сетей с применением декомпозиции по сечениям

Простейший пример использования сечений в расчёте надёжности сетей — использование точек сочленения, т. е. одновершинных сечений. Это позволяет разложить граф на двусвязные компоненты. При этом вероятность связности графа G равна произведению вероятностей связности его двусвязных компонент B_i:

$$R(G) = \prod_{i \in I} R(B_i).$$

Здесь $R(G)$ — вероятность связности G; I — множество индексов всех двусвязных компонент графа.

С учётом экспоненциальной трудоёмкости подобная декомпозиция может существенно ускорить расчёт надёжности. Авторство данного подхода установить достаточно затруднительно, так как в большинстве работ эта формула приводится как очевидный факт [24].

Новым этапом развития методов декомпозиции по сечениям стала работа Вуда [25]. Он первым рассмотрел возможность использования двухвершинных сечений (далее — 2-сечений), сделав это для наиболее универсального из трёх классических показателей надёжности — k-полюсной вероятности связности сети (k-terminal network reliability). Особенностью подхода стало его описание в рамках сохраняющего надёжность преобразования графа (RPGT). Это, на наш взгляд, несколько усложнило изложение и затруднило восприятие этого важного результата, сформулированного в виде следующей теоремы (приводится дословный перевод оригинала).

Теорема 1 [25]. Пусть G — граф без точек сочленения с сечением $\{u, v\}$, таким, что $G_K = \overline{G}_{\overline{K}} \cup \widehat{G}_{\widehat{K}}$, где $\overline{V} \cap \widehat{V} = \{u, v\}$, $\overline{E} \cap \widehat{E} = \varnothing$. Тогда $\overline{G}_{\overline{K}}$ может быть заменён цепью $\chi(u, v)$, состоящей из одного, двух или трех рёбер для получения графа $G'_{K'} = (\overline{G} \cup \chi)_{K'}$, такого, что $R(G_K) = \Omega R(G'_{K'})$ для вычисляемой константы Ω.

Здесь G_K — граф $G = (V, E)$ с множеством полюсов K; $\overline{G}_{\overline{K}}$ — граф $\overline{G} = (\overline{V}, \overline{E})$ с множеством полюсов $\overline{K}$; $\widehat{G}_{\widehat{K}}$ — граф $\widehat{G} = (\widehat{V}, \widehat{E})$ с множеством полюсов $\widehat{K}$; K' — множество полюсов графа G'.

Всего приводится шесть различных комбинаций $\overline{K}, \widehat{K}$ и соответствующих им χ и Ω, а также значений вероятностей присутствия некоторых рёбер в новом графе для описания всех возможных конфигураций полюсов и разрезающих вершин. При этом никакого экспериментального исследования не проводилось, а за поиском 2-сечений автор отсылает к работе [26], предлагающей алгоритм линейной трудоёмкости разложения графа на трёхсвязные компоненты. Кроме того, Вуд рассматривает возможность рекурсивного использования теоремы 1, применяя далее декомпозицию к получаемым графам.

Следующим этапом в развитии декомпозиционных методов стала серия результатов, полученных автором [27 – 29]. Первый из них — формула вероятности связности графа с 2-сечением (рис. 1), впервые опубликованная в 2004 г. на русском языке [27], а также на английском в 2006 г. [30] и 2012 г. [20]:

$$R(G) = R(G_1)\big(R(G'_2) - R(G_2)\big) + R(G_2)\big(R(G'_1) - R(G_1)\big) + R(G_1)R(G_2). \qquad (1)$$

Здесь через G'_i обозначен граф, полученный из G_i слиянием вершин x и y, $i = 1, 2$ (рис. 2).

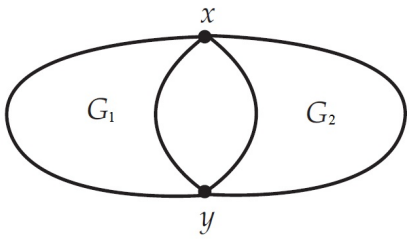


Рис. 1. Граф с двухвершинным сечением

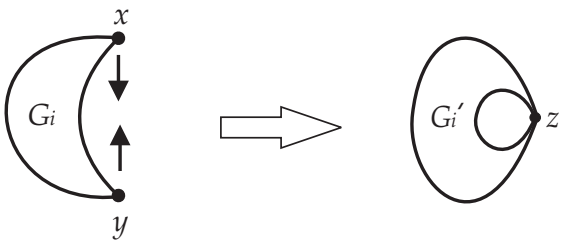


Рис. 2. Слияние вершин сечения в подграфах

В то время (2003–2006) автор не был знаком с результатами Вуда. Вследствие этого был предложен альтернативный подход к применению сечений, целью которого было получение удобных для расчёта формул, а не следование канонам RPGT. По сути, формула (1) является частным случаем теоремы Вуда при восстановлении соответствующих значений Ω и надёжности рёбер в новой цепи χ, что, однако, совершенно

не очевидно на первый взгляд. Вместе с тем, мы одновременно привели и экспериментальные данные, показывающие, что использование формулы (1) ускоряет расчёт на порядки для подходящих структур. Описан также случай, когда сечение разделяет граф более чем на две компоненты [28, 30, 31]. Если использовать формулу (1) или теорему Вуда рекурсивно для такого графа, необходимо пересчитывать надёжность для определённых компонент, что устранено в указанных работах. По этой же причине далее были исследованы определённые двусвязные структуры, содержащие группу 2-сечений, так называемые циклические и продольные графы [28, 29, 31]. Подробнее аспект учёта группы сечений освещается в п. 4.

Естественным развитием наших результатов стало рассмотрение сечений произвольной мощности для расчёта вероятности связности случайного графа в 2006–2008 гг. Общий подход [32, 31] предлагает методику вывода формул, аналогичных формуле (1) для графов с сечением из произвольного числа узлов. Так, получены формулы для графа с 3-сечением и с 4-сечением, которые приведены в п. 3.5 и 3.6 соответственно. Экспериментально исследована целесообразность применения этих формул, в частности и как альтернатива факторизации для скорейшего получения 2-сечений [31]. Кроме использования сечений для расчёта вероятности связности случайного графа, изучена возможность их применения для кумулятивного уточнения границ этой характеристики связности [20] и для расчёта надёжности сетей с ограничением на диаметр [33].

Ещё одним автором, изучавшим возможность декомпозиции по сечениям для расчёта надёжности сетей, стал Бургос (Juan Manuel Burgos) в 2016 г. К сожалению, значительная часть перечисленных результатов автора данной работы была опубликована только на русском языке, за исключением [30, 33, 20], в которых, в частности, и приведена формула (1). Видимо, не будучи знаком с нашими работами, Бургос получает результаты, касающиеся сечений произвольной мощности [34, 35]. Как итог, приводятся и формула (1), и формула для 3-сечения (15), впервые опубликованные приблизительно за 10 лет до работ Бургоса в [27] и [32] соответственно. На независимость наших результатов и результатов Бургоса указывает и существенное отличие в аппарате вспомогательных терминов и объектов, используемых для описания взаимозависимости надёжности сети с надёжностями её подсетей. При этом Бургос не упоминает и классических результатов Вуда [25], который первый изучил возможность использования 2-сечений для расчёта сетевой надёжности. Как и Вуд, Бургос не рассматривает вычислительный аспект, а также возможность и целесообразность использования предлагаемых результатов.

Подводя итог обзора, отметим, что в настоящее время имеется ряд теоретических и прикладных результатов, делающих возможным использование сечений в расчёте сетевой надёжности. Результаты, полученные разными авторами, так или иначе пересекаются друг с другом. Ниже мы приводим наш подход по использованию сечений произвольной мощности с некоторыми новыми аспектами и новый алгоритм для использования всех 2-сечений графа.

2. Обозначения и определения

Пусть $G = (V, E)$ — произвольный неориентированный граф, где V — множество вершин; E — множество рёбер графа G. Пусть для каждого ребра e задано вещественное число p_e, $0 \leqslant p_e \leqslant 1$, которое будем интерпретировать как вероятность присутствия ребра e в графе. При этом предполагается, что вершины абсолютно надёжны, то есть присутствуют с вероятностью 1.

Зададим дискретное вероятностное пространство $W = (\Omega, P)$. Здесь Ω — пространство элементарных событий (элементарных исходов), образованное всевозможными частными реализациями графа G, определяемыми присутствием или отсутствием каждого ребра. Для данного элементарного события присутствующие ребра будем называть *исправными*, а отсутствующие — *отказавшими*. Пространство Ω можно представить как объединение всевозможных двоичных векторов длины $|E|$, поэтому Ω состоит из $2^{|E|}$ элементов.

Вероятность элементарного события $Q \in \Omega$ определим как произведение вероятностей присутствия исправных ребер, умноженное на произведение вероятностей отсутствия отказавших рёбер:

$$P(Q) = \prod_{e \in Q_a} p_e \prod_{e \in Q_b} (1 - p_e).$$

Здесь Q_a — множество исправных ребер; Q_b — множество отказавших ребер.

Произвольное событие (объединение некоторых элементарных событий) будем называть *успешным*, если реализации графов, соответствующие всем элементарным событиям, образующим это событие, суть связные графы, то есть все вершины в них могут быть связаны исправными рёбрами.

Вероятность $R(G)$ связности графа G есть вероятность того, что все вершины G связаны исправными рёбрами, то есть вероятность события, состоящего из всех успешных событий, и только из них.

Указанные общие определения вероятностного пространства и меры надёжности заимствованы в основном из [17]. Введём некоторые обозначения и определения для описания графа с точки зрения содержащегося в нём сечения. Предположим, что граф G содержит сечение из h вершин $H = \{v_1, \ldots, v_h\}$, которое разделяет граф на два подграфа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$, т. е. $V_1 \cup V_2 = V$, $V_1 \cap V_2 = H$, $E_1 \cup E_2 = E$, $E_1 \cap E_2 = \varnothing$. Если сечение разделяет граф на более чем два подграфа, то G_1 и G_2 могут быть по-разному сформированы из данных подграфов.

Через $\mathbf{H}$ обозначим множество разбиений множества H. Отдельно выделим два разбиения: $\mathbf{0} = \{\{v_1\}, \ldots, \{v_h\}\}, \mathbf{1} = \{\{v_1, \ldots, v_h\}\}$, а также множество $\mathbf{K} = \mathbf{H} \backslash \{\mathbf{0}, \mathbf{1}\}$. Элементы разбиения будем называть *блоками разбиения*. В некоторых случаях для удобства будем использовать следующее обозначение для разбиения:

$$i_{1_1}, \ldots, i_{1_k} | \ldots | i_{l_1}, \ldots, i_{l_t} = \{\{i_{1_1}, \ldots, i_{1_k}\}, \ldots, \{i_{l_1}, \ldots, i_{l_t}\}\}.$$

Для каждого разбиения $\Phi \in \mathbf{H}$ определим *граф разбиения* T_Φ следующим образом: T_Φ — граф с множеством вершин H, в котором две вершины смежны, если и только если они входят в один и тот же блок Φ. Введём обозначение для объединения двух графов разбиений: $T_{\Phi\Upsilon} = T_\Phi \cup T_\Upsilon$.

Множество всех связных графов будем обозначать G_{Con}; Gr^Φ $(\Phi \in \mathbf{H})$ — граф $Gr \in \in \{G_1, G_2, T_\Upsilon, T_{\Upsilon\Psi}\}$, стянутый по каждому элементу из Φ, то есть если v_i и v_j входят в один блок Φ, то в графе в Gr^Φ вершины v_i и v_j стянуты в одну; Gr^Φ будем называть графом Gr, *стянутым по разбиению* Φ.

Пусть S^1_Φ $(\Phi \in \mathbf{H})$ — событие, соответствующее распаду G_1 на $|\Phi|$ компонент, причём вершины из одного блока Φ входят в одну и ту же компоненту. Такое событие будем называть Φ-*отделением в графе* G_1. Аналогично определяется S^2_Φ — Φ-*отделение в графе* G_2. Вероятности отделений будем обозначать как

$$x_\Phi = P(S^1_\Phi), \quad y_\Phi = P(S^2_\Phi).$$

Так как $|\mathbf{1}| = 1$, то $S^1_{\mathbf{1}}$ — событие, соответствующее распаду G_1 на одну компоненту, т. е. событие, образованное всеми связными реализациями G_1. Следовательно, $x_{\mathbf{1}} = R(G_1)$, $y_{\mathbf{1}} = R(G_2)$.

3. Расчёт вероятности связности случайного графа с использованием сечения

3.1. Вероятности отделений

Для установления значений всевозможных отделений в графах G_1 и G_2 через вероятности связности графов G_1, G_2, стянутых по всевозможным разбиениям, докажем следующую теорему.

Теорема 2. Имеют место равенства

$$\sum_{\substack{\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} x_\Phi = R(G_1^\Upsilon), \quad \Upsilon \in \mathbf{H}; \tag{2}$$

$$\sum_{\substack{\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} y_\Phi = R(G_2^\Upsilon), \quad \Upsilon \in \mathbf{H}. \tag{3}$$

Доказательство. Докажем первое равенство, второе доказывается аналогично.

Выберем произвольное $\Upsilon \in \mathbf{H}$. Пусть B_Υ такое событие, что $P(B_\Upsilon) = R(G_1^\Upsilon)$, то есть B_i состоит из реализаций, связных при стягивании G_1 по разбиению Υ. Тогда равенство (2) равносильно равенству

$$\bigcup_{\substack{\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} S^1_\Phi = B_\Upsilon. \tag{4}$$

Докажем включение

$$\bigcup_{\substack{\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} S^1_\Phi \subseteq B_\Upsilon.$$

Граф $T_{\Upsilon\Phi}$ связный, следовательно, T_Φ содержит рёбра, соединяющие все компоненты связности графа T_Υ. Так как при стягивании по разбиению Υ в графе T_Υ стягивания будут происходить только внутри компонент его связности, граф T_Φ, стянутый по Υ, связный.

По определению S^1_Φ образовано реализациями, состоящими из $|\Phi|$ компонент связности, каждая из которых содержит все вершины одного и только одного блока Φ. Граф T_Φ также состоит из $|\Phi|$ компонент, каждая из которых содержит все вершины одного блока из Φ, и только их. Так как T_Φ, стянутый по Υ, связен, каждая реализация из S^1_Φ, стянутая по Φ, связная. Следовательно, $S^1_\Phi \subseteq B_\Upsilon$.

Докажем обратное включение

$$\bigcup_{\substack{\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} S^1_\Phi \supseteq B_\Upsilon.$$

Рассмотрим произвольную реализацию $A \in B_\Upsilon$. Построим Φ следующим образом: все вершины из H, оказавшиеся в одной и той же компоненте связности A, и только они входят в один и тот же блок Υ. Таким образом, T_Φ соединяет вершины из H, находящиеся в разных компонентах A (так как A^Υ связен). Следовательно, $T_{\Upsilon\Phi}$ связный. По построению Φ очевидно, что $A \in S^1_\Phi$. Отсюда $B_\Upsilon \subseteq \bigcup\limits_{\substack{\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} S^1_\Phi$. ■

Нетрудно заметить, что выражения (2) и (3) для вероятностей всевозможных отделений в графе G_i через вероятности связности этого графа, стянутого всевозможными способами, являются системами линейных уравнений.

При подстановке в (2) значения $\Upsilon = \mathbf{0}$ получаем упомянутое в п. 2 равенство $x_{\mathbf{1}} = R(G_1^{\mathbf{0}}) = R(G_1)$. При подстановке значения $\Upsilon = \mathbf{1}$ получаем

$$\sum_{\Phi \in \mathbf{H}} x_\Phi = R(G_1^{\mathbf{1}}); \tag{5}$$

$$\sum_{\Phi \in \mathbf{H}} y_\Phi = R(G_2^{\mathbf{1}}). \tag{6}$$

Остальные равенства образуют систему линейных уравнений относительно отделений из $\mathbf{K}$.

Следствие 1. Имеет место

$$\sum_{\substack{\Phi \in \mathbf{K} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} x_\Phi = R(G_1^\Upsilon) - R(G_1), \quad \Upsilon \in \mathbf{K}; \tag{7}$$

$$\sum_{\substack{\Phi \in \mathbf{K} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} y_\Phi = R(G_2^\Upsilon) - R(G_2), \quad \Upsilon \in \mathbf{K}. \tag{8}$$

Доказательство. Возьмём произвольное $\Upsilon \in \mathbf{K}$. Граф $T_{\Upsilon\mathbf{0}}$ связен только для $\Upsilon = \mathbf{1}$, следовательно, $T_{\Upsilon\mathbf{0}} \notin G_{\mathrm{Con}}$ для $\Upsilon \in \mathbf{K}$. Выпишем уравнение (2) для Υ:

$$R(G_1^\Upsilon) = \sum_{\substack{\Phi \in \mathbf{H} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} x_\Phi = \sum_{\substack{\Phi \in \mathbf{K} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} x_\Phi + \sum_{\substack{\Phi \in \{\mathbf{0},\mathbf{1}\} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} x_\Phi = \sum_{\substack{\Phi \in \mathbf{K} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} x_\Phi + x_{\mathbf{1}} = \sum_{\substack{\Phi \in \mathbf{K} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} x_\Phi + R(G_1).$$

Перенесём $R(G_1)$ вправо и получим искомое выражение (7). Равенство (8) доказывается аналогично. ■

Возможность получения значений x_Φ, y_Φ из систем уравнений (2) и (3) следует из следующей теоремы.

Теорема 3. Системы (2) и (3) разрешимы относительно x_Φ и y_Φ соответственно и имеют единственное решение.

Доказательство. Докажем утверждение для системы (2), для системы (3) оно доказывается аналогично. Для каждого $\Phi \in \mathbf{H}$ существует $\Upsilon \in \mathbf{H}$, такой, что $T_{\Upsilon\Phi} \in G_{\mathrm{Con}}$, следовательно, количество уравнений и переменных в системе совпадает. Система линейных уравнений с квадратной матрицей разрешима, если строки матрицы линейно независимы. Предположим обратное, тогда верно равенство

$$R(G_1) = R(G_1^{\mathbf{0}}) = \sum_{\Phi \in \mathbf{I}} a_\Phi R(G_1^\Phi) \tag{9}$$

для некоторых a_Φ и для подходящего множества индексов $\mathbf{I} \subseteq \mathbf{H}$. Докажем, что это выражение приводит к противоречию, индукцией по h, т. е. по количеству элементов в сечении.

Б а з а и н д у к ц и и, $h = 2$. Формула (9) принимает следующий вид:

$$R(G_1) = aR(G^{\mathbf{1}}) = aR(G^{12}). \tag{10}$$

Положим значения вероятностей присутствия рёбер в G_1, смежных с v_1, равными 0, а для остальных рёбер — равными 1. Тогда G_1 несвязен, т. е. $R(G_1) = 0$, а G^{12} связен,

т. е. $R(G^{12}) > 0$, и в (10) $a = 0$, но в таком случае $R(G_1) = 0$ для любого случайного графа, что неверно.

Ш а г и н д у к ц и и. Пусть утверждение доказано для $h-1$, докажем его для h. Как и в базе индукции, положим значения вероятностей присутствия рёбер в G_1, смежных с v_1, равными 0. Тогда несвязными будут все графы G_1^{Φ}, такие, что $v_1 \in \Phi$, в том числе и G_1. Следовательно, $R(G_1) = 0$ и $R(G_1^{\Phi}) = 0$, если $v_1 \in \Phi$. Для остальных значений Φ имеет место равенство

$$R(G_1^{\Phi}) = R\left((G_1 \backslash v_1)^{\overline{\Phi}}\right),$$

где разбиение $\overline{\Phi}$ получается из Φ удалением вершины v_1 из содержащего её блока, так как безразлично, куда именно стягивать изолированную вершину v_1. Такие разбиения являются по сути всеми разбиениями на множестве $\{v_2, \ldots, v_h\}$, обозначим множество этих разбиений через J. Формула (9) принимает вид

$$0 = \sum_{\Phi \in \mathbf{J}} a_{\Phi} R\left((G_1 \backslash v_1)^{\Phi}\right).$$

Полученное выражение является модификацией (9), в которой левая часть перенесена под знак суммы в правой части, однако уже для разбиения на множестве из $h-1$ вершин. Но, по предположению индукции, это невозможно. ■

Так как системы (7) и (8) получаются из систем (2) и (3) соответственно исключением двух уравнений и двух переменных, верно

Следствие 2. Системы (7) и (8) разрешимы относительно x_{Φ} и y_{Φ} соответственно и имеют единственное решение.

3.2. О б щ и й в и д ф о р м у л ы д л я в е р о я т н о с т и с в я з н о с т и г р а ф а с с е ч е н и е м

Следующая теорема устанавливает взаимосвязь между вероятностью связности графа с сечением и вероятностями связности его подграфов, стянутых по всевозможным разбиениям.

Теорема 4. Имеет место равенство

$$R(G) = \sum_{\substack{\Upsilon, \Phi \in \mathbf{H} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} x_{\Upsilon} y_{\Phi}. \tag{11}$$

Доказательство. Пусть S такое событие, что $P(S) = R(G)$, то есть S состоит из всех связных реализаций, и только из них. Тогда равенство (11) равносильно равенству

$$S = \bigcup_{\substack{\Upsilon, \Phi \in \mathbf{H} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} (S_{\Upsilon}^1 \cap S_{\Phi}^2).$$

Докажем включение

$$S \subseteq \bigcup_{\substack{\Upsilon, \Phi \in \mathbf{H} \\ T_{\Upsilon\Phi} \in G_{\mathrm{Con}}}} (S_{\Upsilon}^1 \cap S_{\Phi}^2).$$

Пусть $A \in S$ — связная реализация G; A_1 — граф A, индуцированный на множестве вершин V_1 графа G_1; A_2 — граф A, индуцированный на множестве вершин V_2 графа G_2. Построим разбиение Υ следующим образом: все вершины из H, оказавшиеся в одной и той же компоненте связности A_1, и только они, входят в один и тот же блок Υ.

Аналогично построим Φ: все вершины из H, оказавшиеся в одной и той же компоненте связности A_2, и только они, входят в один и тот же блок Φ.

Так как A связный, для любых двух блоков b_1, b_p из Υ или Φ существует последовательность блоков $b_1, b_2, \ldots, b_p$ из Υ и Φ, такая, что при $1 \leqslant l \leqslant p-1$ блоки b_l и b_{l+1} пересекаются по крайней мере по одному элементу, то есть все элементы из b_l соединимы со всеми элементами из b_{l+1} в $T_{\Upsilon\Phi}$. Следовательно, b_1 и b_p соединимы в $T_{\Upsilon\Phi}$, то есть $T_{\Upsilon\Phi} \in G_{\mathrm{Con}}$. По построению $A \in S^1_\Upsilon \cap S^2_\Phi$. Включение доказано.

Докажем обратное включение

$$S \supseteq \bigcup_{\substack{\Upsilon,\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} (S^1_\Upsilon \cap S^2_\Phi),$$

что равносильно связности произвольной реализации $A \in S^1_\Upsilon \cap S^2_\Phi$ при условии $T_{\Upsilon\Phi} \in$ $\in G_{\mathrm{Con}}$. Как и ранее, пусть A_1 — граф A, индуцированный на множестве вершин V_1, A_2 — граф A, индуцированный на множестве вершин V_2.

Граф $T_{\Upsilon\Phi}$ связный, то есть все вершины из H связаны в $T_{\Upsilon\Phi}$, следовательно, все компоненты связности A_1 и A_2 будут связаны друг с другом через вершины H в A, то есть A связен. Обратное включение доказано. ■

С помощью (5) и (6) можно переписать равенство (11).

Следствие 3. Имеет место равенство

$$R(G) = \sum_{\substack{\Upsilon,\Phi\in\mathbf{K}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} x_\Upsilon y_\Phi + R(G_1)R(G_2^{\mathbf{1}}) + R(G_1^{\mathbf{1}})R(G_2) - R(G_1)R(G_2). \tag{12}$$

Доказательство. Учитывая, что $T_{\Upsilon\mathbf{0}} \notin G_{\mathrm{Con}}$ для $\Upsilon \in \mathbf{K}$, равенство (11) влечёт

$$R(G) = \sum_{\substack{\Upsilon,\Phi\in\mathbf{H}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} x_\Upsilon y_\Phi = \sum_{\substack{\Upsilon,\Phi\in\mathbf{K}\\ T_{\Upsilon\Phi}\in G_{\mathrm{Con}}}} x_\Upsilon y_\Phi + x_{\mathbf{1}} \sum_{\Phi\in\mathbf{H}} y_\Phi + y_{\mathbf{1}} \sum_{\Upsilon\in\mathbf{H}} x_\Upsilon - x_{\mathbf{1}} y_{\mathbf{1}}.$$

Используя (5) и (6), получаем искомый результат. ■

Может показаться, что в формуле (12) нет необходимости, потому что на первый взгляд она более громоздкая, чем (11). На самом деле формула (12) содержит значительно меньше слагаемых, так как свёрнуты все слагаемые вида $x_{\mathbf{1}} \sum\limits_{\Phi\in\mathbf{H}} y_\Phi$ и $y_{\mathbf{1}} \sum\limits_{\Upsilon\in\mathbf{H}} x_\Upsilon$.

3.3. Вывод формул для вероятности связности графа с h-сечением

Теоремы 2–4 в совокупности позволяют использовать декомпозицию графа по сечению для расчёта его надёжности. Например, пусть нас интересует сечение из h вершин, разделяющее граф на два подграфа. Тогда мы должны решить систему линейных уравнений (2) в символьном виде для одного из подграфов, выразив вероятность каждого отделения подграфа через надёжности этого подграфа, стянутого по вершинам сечения. Теорема 3 гарантирует существование такого решения. Приписывая соответствующие индексы в эти выражения, получаем выражения для вероятностей отделения второго подграфа.

Теорема 4 даёт выражение для надёжности исходного графа через вероятности отделений обоих подграфов. Подставив в него полученные значения вероятностей отделений и приведя подобные, получим формулу для надёжности графа с h-сечением.

Использование следствий 1–3 вместо теорем 2–4 упрощает вывод подобных формул, так как формула (12) для надёжности графа через вероятности отделений содержит меньше слагаемых, чем формула (11). Таким образом, решив системы уравнений (7) и (8) для нахождения значений x_Υ и y_Φ соответственно и подставив их в (12), получим формулу для надёжности графа с h-сечением.

Эта формула выражает надёжность графа с h-сечением через надёжности двух его подграфов, стянутых по всевозможным разбиениям множества вершин сечения. Количество таких разбиений есть число Белла B_h для каждого из подграфов, соответственно для расчёта надёжности исходного графа потребуется рассчитать надёжность для $2B_h$ графов меньшей размерности. Однако числа Белла B_h быстро растут с ростом h: так, $B_2 = 2$, $B_3 = 5$, $B_4 = 15$, $B_5 = 52$. Таким образом, для расчёта надёжности графа с 2-сечением придётся предварительно вычислить надёжности для $2B_2 = 4$ графов меньшей размерности, для графа с 3-сечением — $2B_3 = 10$ графов, для графа с 4-сечением — $2B_4 = 30$ графов, для графа с 5-сечением — $2B_5 = 104$ графов. Будет ли такой расчёт более быстрым — вопрос неочевидный. Далее мы выводим такие формулы для случаев с 2-, 3-, 4-сечениями и исследуем эффективность их применения.

Заметим также, что при рассмотрении сечений из h вершин нигде не использована h-связность графа, поэтому все полученные результаты справедливы и для случая, если граф не является h-связным или даже вообще связным. Например, пусть подграф G_1 несвязен и не может распасться ровно на $|\Upsilon|$ компонент ($\Upsilon \in \mathbf{H}$) так, чтобы вершины из одного блока Υ входили бы в одну и ту же компоненту связности. Тогда вероятность этого события равна 0, то есть $x_\Upsilon = 0$.

3.4. Двухвершинное сечение

Пусть граф G содержит двухвершинное сечение $H = \{1, 2\}$. Граф G_i, стянутый по разбиению 12, обозначим как G'_i. В этом случае имеем

$$\mathbf{H} = \{12, 1|2\}, \quad \mathbf{1} = 12, \quad \mathbf{0} = 1|2, \quad \mathbf{K} = \varnothing.$$

Формула (12) даёт

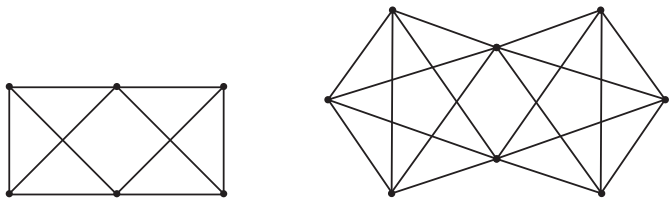
$$\begin{aligned} R(G) = \sum_{\substack{\Upsilon,\Phi\in\varnothing \\ T_{\Upsilon\Phi\in G_{\mathrm{Con}}}}} x_\Upsilon y_\Phi + R(G_1)R(G_2^{\mathbf{1}}) + R(G_1^{\mathbf{1}})R(G_2) - R(G_1)R(G_2) = \\ = R(G_1)R(G'_2) + R(G'_1)R(G_2) - R(G_1)R(G_2) = \\ = R(G_1)\big(R(G'_2) - R(G_2)\big) + R(G_2)\big(R(G'_1) - R(G_1)\big) + R(G_1)R(G_2), \end{aligned} \tag{13}$$

что есть в точности формула (1).

В качестве базового алгоритма, к которому будем применять предлагаемые методики ускорения с использованием сечений, возьмём метод факторизации с последовательно-параллельным преобразованием на каждом шаге. Рекурсию будем продолжать до получения пятивершинных графов, для графов такой и меньшей размерности будем рассчитывать вероятность связности по формулам из [16]. Этот алгоритм будем называть *Factoring*. Алгоритм *Factoring*, усиленный применением формулы (13), назовём *2CutsFactoring*.

Первый вопрос, который возникает при использовании формулы (13), — начиная с какой размерности графа целесообразно её применять. Предполагается, что перед процедурой нахождения сечения граф прошёл через последовательно-параллельное преобразование, поэтому он не содержит вершин степени 1 и 2. Самый «маленький» такой граф с двухвершинным сечением изображён на рис. 3, *а*, $N = 6$, $M = 12$. Этот

граф получен объединением двух полных графов размера 4 с двумя совпадающими вершинами без ребра между ними. Будем обозначать такие графы K'_L, на рис. 3 представлены графы K'_4 и K'_5. Алгоритм *Factoring* этот граф обсчитал за три итерации рекурсии, а с использованием декомпозиции по формуле (13) — за пять. Были обсчитаны и другие малые графы ($M \leqslant 20$). Использование (13) даёт выигрыш по количеству итераций при $M \geqslant 15$ для некоторых графов. Однако существует граф при $M = 19$, $N = 14$ с 2-сечением, для которого количество итераций в обоих методах одинаковое. Если $M \geqslant 20$, то алгоритм *Factoring* всегда выполняет большее количество итераций. Время расчёта этих графов сравнить не удалось, так как во всех случаях оно меньше миллисекунды (даже на очень слабых ПЭВМ). Поэтому сделан следующий вывод [31]: исследовать граф на наличие двухвершинного сечения целесообразно при условии $M \geqslant 20$.



а *б*

Рис. 3. Графы K'_4 (*а*) и K'_5 (*б*)

Отметим, что приведённые ниже тестовые примеры представляют эффект от однократного применения формул с использованием сечений, так как получаемые при декомпозиции графы не содержат сечений такой же или меньшей размерности. В общем случае имеет смысл рекурсивно применять эти формулы, при этом, например, получаемые при декомпозиции по (13) графы должны быть сначала разложены на двусвязные компоненты.

Для максимального ускорения из всех двухвершинных сечений имеет смысл выбрать то, которое разбивает граф на максимально близкие друг другу по количеству рёбер подграфы. В приведённых ниже экспериментах оптимальное двухвершинное сечение находилось простым перебором всех пар вершин графа, что реализуется со сложностью $O(MN^2)$. Отметим, что возможно и более быстрое нахождение 2-сечений, этот вопрос рассматривается в п. 4.1.

В таблице приведены результаты экспериментов на графах K'_L. Расчёты для этого и всех остальных экспериментов проводились на ПЭВМ с процессором AMD Athlon 3500+, 2,2 GHz, RAM 3Gb.

L	*Factoring*		*2CutsFactoring*	
	Время	Количество итераций	Время	Количество итераций
8	2 с	305487	<0,01 с	477
9	2 мин 27 с	13394427	0,01 с	3357
10	7 ч	$1{,}7 \cdot 10^{11}$	0,17 с	26877
11	—	—	1,5 с	241917
12	—	—	15,5 с	2419197

В менее плотных графах с 2-сечениями эффект ускорения меньше, но всё ещё очень значителен. Например, для ста случайно сгенерированных графов с 40 вершинами и 72 рёбрами с 2-сечением, разделяющим его на две равные части, среднее время рас-

чёта составило 0,12 с, тогда как алгоритму *Factoring* потребовалось 2 мин 23 с. Среднее число итераций составило 12762 и 912891 соответственно.

Если в графе заведомо нет 2-сечений, время работы алгоритма *2CutsFactoring* с предварительной проверкой их наличия практически не отличается от времени работы алгоритма *Factoring*. Например, для полного 13-вершинного графа время расчёта составило 1 мин 27 с, что на одну секунду больше алгоритма *Factoring*. При этом поиск сечения на каждом шаге факторизации только замедляет процесс расчёта. Имеет смысл вести направленную факторизацию с целью скорейшего получения 2-сечения, что в некоторых случаях делает расчёт более быстрым, чем просто *Factoring*, но всё равно этот метод проигрывает декомпозиции по 3-сечению [31].

3.5. Трёхвершинное сечение

Пусть граф G содержит сечение из трёх вершин $\{1, 2, 3\}$ (рис. 4). Опишем этот случай более подробно, так как он не так тривиален, как случай с 2-сечением, и не такой громоздкий, как с 4-сечением.

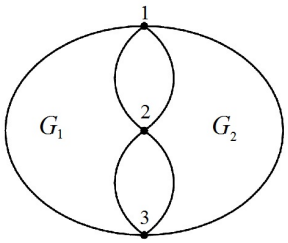


Рис. 4. Граф с трёхвершинным сечением

Тогда $\mathbf{K} = \{12|3, 13|2, 1|23\}$, $\mathbf{0} = 1|2|3$, $\mathbf{1} = 123$. Графы G_i^{Φ} представлены на рис. 5; графы, образующие всевозможные отделения S^i_{Φ}, — на рис. 6 ($i \in \{1, 2\}$, $\Phi \in \mathbf{H}$).

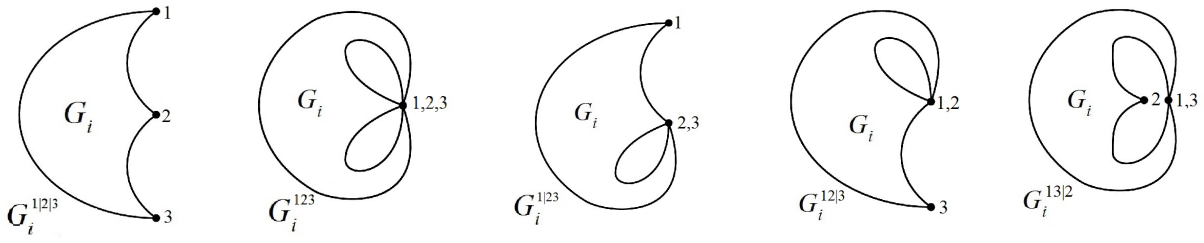


Рис. 5. Графы, стянутые по разбиениям

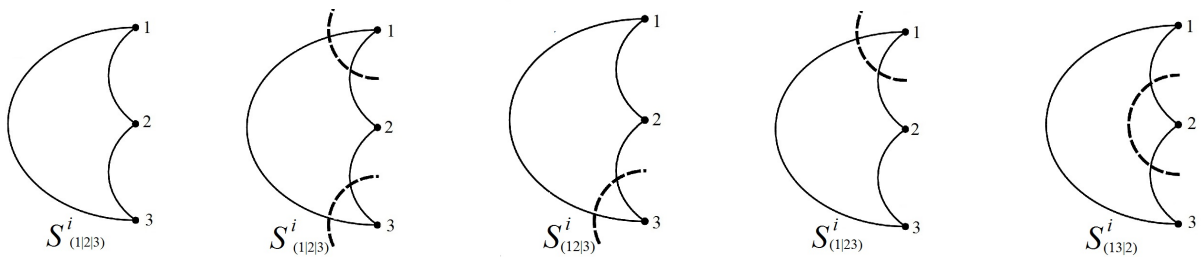


Рис. 6. Графы, образующие отделения

Для каждого разбиения выпишем такие разбиения, для которых объединение графов разбиений будет связным:

$$\begin{gathered}\{\Phi : T_{\mathbf{1}\Phi} \in G_{\mathrm{Con}}\} = \mathbf{H},\\ \{\Phi : T_{\mathbf{0}\Phi} \in G_{\mathrm{Con}}\} = \mathbf{1},\\ \{\Phi \in \mathbf{K} : T_{12|3\Phi} \in G_{\mathrm{Con}}\} = \{13|2, 1|23\},\\ \{\Phi \in \mathbf{K} : T_{13|2\Phi} \in G_{\mathrm{Con}}\} = \{1|23, 12|3\},\\ \{\Phi \in \mathbf{K} : T_{1|23\Phi} \in G_{\mathrm{Con}}\} = \{12|3, 13|2\}.\end{gathered}$$

Тогда системы (7) и (8) имеют вид ($i = 1, 2$)

$$\begin{cases} P(S^i_{12|3}) + P(S^i_{13|2}) = R(G_i^{1|23}) - R(G_i),\\ P(S^i_{12|3}) + P(S^i_{1|23}) = R(G_i^{13|2}) - R(G_i),\\ P(S^i_{13|2}) + P(S^i_{1|23}) = R(G_i^{12|3}) - R(G_i). \end{cases}$$

Решив данную систему, получим следующие значения ($i = 1, 2$):

$$\begin{aligned} P(S^i_{12|3}) &= \frac{1}{2}(R(G_i^{13|2}) + R(G_i^{1|23}) - R(G_i^{12|3}) - R(G_i)),\\ P(S^i_{13|2}) &= \frac{1}{2}(R(G_i^{12|3}) + R(G_i^{1|23}) - R(G_i^{13|2}) - R(G_i)),\\ P(S^i_{1|23}) &= \frac{1}{2}(R(G_i^{12|3}) + R(G_i^{13|2}) - R(G_i^{1|23}) - R(G_i)). \end{aligned}$$

Выпишем равенство (12):

$$\begin{gathered} R(G) = x_{1|23}(y_{12|3} + y_{13|2}) + x_{13|2}(y_{1|23} + y_{12|3}) + x_{12|3}(y_{1|23} + y_{13|2}) +\\ + R(G_1)R(G_2^{\mathbf{1}}) + R(G_1^{\mathbf{1}})R(G_2) - R(G_1)R(G_2). \end{gathered} \tag{14}$$

Подставив в (14) значения $x_\Phi = S^1_\Phi$ и $y_\Phi = S^2_\Phi$ и приведя подобные, получим

$$\begin{aligned} R(G) = \frac{1}{2}\Big[& R(G_1^{1|23})\big(R(G_2^{12|3}) + R(G_2^{13|2}) - R(G_2^{1|23})\big) +\\ & + R(G_1^{12|3})\big(R(G_2^{1|23}) + R(G_2^{13|2}) - R(G_2^{12|3})\big) +\\ & + R(G_1^{13|2})\big(R(G_2^{12|3}) + R(G_2^{1|23}) - R(G_2^{13|2})\big) -\\ & - R(G_1)\big(R(G_2^{12|3}) + R(G_2^{13|2}) + R(G_2^{1|23})\big) -\\ & - R(G_2)\big(R(G_1^{12|3}) + R(G_1^{13|2}) + R(G_1^{1|23})\big) + R(G_1)R(G_2)\Big] +\\ & + R(G_1)R(G_2^{123}) + R(G_1^{123})R(G_2). \end{aligned} \tag{15}$$

Как и в случае с 2-сечением, проведены численные эксперименты на графах небольшой размерности, которые показали, что применять формулу (15) целесообразно для графов с количеством рёбер больше 26. При этом подграфы G_1 и G_2 должны содержать не менее пяти ребер. Алгоритм *Factoring*, усиленный предварительным применением формулы (15), назовём *3CutsFactoring*.

Приведённые ниже тестовые примеры представляют эффект от однократного применения формулы, но в общем случае стоит применять данную формулу рекурсивно. То есть подграфы, возникающие при рассмотрении 3-сечения, далее проверяем на наличие подходящего 2-сечения, если его нет — на наличие подходящего трёхвершинного.

В области анализа сетевой надёжности популярными тестовыми графами являются решётки [17]. Для сравнения алгоритма с использованием сечений *3CutsFactoring* с базовым алгоритмом *Factoring* проведён эксперимент на решетках ширины 3. Так, для решётки 3×16 время расчёта алгоритмом *Factoring* составило 30 с при 3188645 итерациях, алгоритмом *3CutsFactoring* — 0,25 с при 7127 итерациях.

На решётке размера 3×18 преимущество в использовании формулы (15) уже существенно больше: 0,52 с при 213383 итерациях против 3 м 41 с при 28697813 итерациях алгоритмом *Factoring*.

3.6. Четырёхвершинное сечение

Рассмотрим случай, когда граф G содержит сечение из четырёх вершин $H = \{1, 2, 3, 4\}$. Будем использовать следующие обозначения для вероятностей отделений для двух подграфов G_1 и G_2 $(i = 1, 2)$:

$$\begin{array}{lll} S_0^i = P(S^i_{1|2|3|4}), & S_1^i = P(S^i_{12|34}), & S_2^i = P(S^i_{13|24}), \\ S_3^i = P(S^i_{14|23}), & S_4^i = P(S^i_{1|234}), & S_5^i = P(S^i_{2|134}), \\ S_6^i = P(S^i_{3|124}), & S_7^i = P(S^i_{4|123}), & S_8^i = P(S^i_{1|2|34}), \\ S_9^i = P(S^i_{12|3|4}), & S_{10}^i = P(S^i_{1|23|4}), & S_{11}^i = P(S^i_{14|2|3}), \\ S_{12}^i = P(S^i_{1|24|3}), & S_{13}^i = P(S^i_{13|2|4}), & S_{14}^i = P(S^i_{1234}). \end{array}$$

Системы (7) и (8) и их решения приводить не будем из-за их громоздкости, их можно найти, например, в [31]. Приведём формулу (12) в терминах отделений:

$$\begin{aligned} R(G) = {} & S_4^1(S_5^2 + S_6^2 + S_7^2 + S_9^2 + S_{13}^2 + S_{11}^2 + S_1^2 + S_2^2 + S_3^2) + \\ & + S_5^1(S_4^2 + S_6^2 + S_7^2 + S_9^2 + S_{10}^2 + S_{12}^2 + S_1^2 + S_2^2 + S_3^2) + \\ & + S_6^1(S_4^2 + S_5^2 + S_7^2 + S_{13}^2 + S_{10}^2 + S_8^2 + S_1^2 + S_2^2 + S_3^2) + \\ & + S_7^1(S_4^2 + S_5^2 + S_6^2 + S_{11}^2 + S_{12}^2 + S_8^2 + S_1^2 + S_2^2 + S_3^2) + \\ & + S_1^1(S_4^2 + S_5^2 + S_6^2 + S_7^2 + S_2^2 + S_3^2 + S_{13}^2 + S_{11}^2 + S_{10}^2 + S_{12}^2) + \\ & + S_2^1(S_4^2 + S_5^2 + S_6^2 + S_7^2 + S_1^2 + S_3^2 + S_9^2 + S_{11}^2 + S_{10}^2 + S_8^2) + \\ & + S_3^1(S_4^2 + S_5^2 + S_6^2 + S_7^2 + S_1^2 + S_2^2 + S_9^2 + S_{13}^2 + S_{12}^2 + S_8^2) + \\ & + S_9^1(S_4^2 + S_5^2 + S_2^2 + S_3^2) + S_{13}^1(S_4^2 + S_6^2 + S_1^2 + S_3^2) + \\ & + S_{11}^1(S_4^2 + S_7^2 + S_1^2 + S_2^2) + S_{10}^1(S_5^2 + S_6^2 + S_1^2 + S_2^2) + \\ & + S_{12}^1(S_5^2 + S_7^2 + S_1^2 + S_3^2) + S_8^1(S_6^2 + S_7^2 + S_2^2 + S_3^2) + \\ & + R(G_1)R(G_2^{\mathbf{1}}) + R(G_1^{\mathbf{1}})R(G_2) - R(G_1)R(G_2). \end{aligned} \tag{16}$$

В таком виде формула для графа с 4-сечением приводится впервые. Аналогичная формула [31, (2.21)] написана в терминах отделений и содержит ошибку после второго знака равенства.

Численные эксперименты на графах небольшой размерности показали, что применять формулу (16) целесообразно для графов с количеством рёбер больше 35. При этом подграфы G_1 и G_2 должны содержать не менее 8 рёбер.

Как это сделано для формулы (15) в п. 3.5, выявим эффективность использования (16) на решётках. Для решётки 4×9 время расчёта алгоритмом *Factoring* составило 22 с при 2473799 итерациях, с использованием (16) — 0,37 с при 7351 итерациях. На решётке размера 4×11 преимущество в использовании формулы (16) уже существенно больше: 1,5 с при 57661 итерациях вместо 22,5 мин при 154117959 итерациях алгоритмом *Factoring*.

4. Особенности использования двухвершинных сечений в расчёте вероятности связности графа

4.1. Проблема учёта группы двухвершинных сечений

Как показано выше, использование формул (13), (15), (16) способно значительно ускорить расчёт надёжности для подходящих графов, в особенности для двусвязных графов с двухвершинным сечением. Если подграфы, получаемые при декомпозиции, а также всевозможные варианты их стягивания по разрезающим вершинам, в свою очередь, также содержат двухвершинные сечения, появляется возможность повторного использования формулы (1). Рассмотрим для примера двусвязный граф, представленный на рис. 7 и содержащий два двухвершинных сечения.

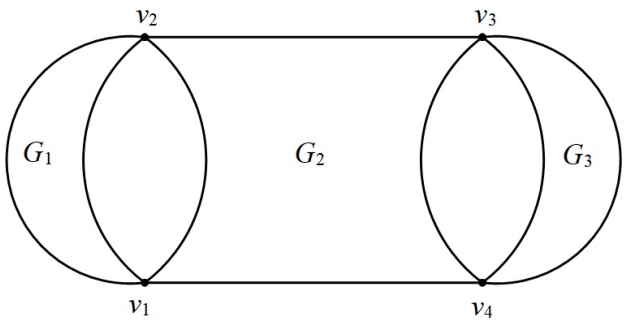


Рис. 7. Пример графа, содержащего два двухвершинных сечения

Если сначала делать декомпозицию G по v_1, v_2, придём к рассмотрению $G_{23} = G_2 \cup \cup G_3$, G_{23}^{12}. При декомпозиции G_{23} по v_3, v_4 получим G_2, G_2^{34}, G_3, G_3^{34}; при декомпозиции G_{23}^{12} по $v_3, v_4 - G_2^{12|34}$, G_2^{12}, G_3, G_3^{34}. Таким образом, придётся пересчитывать надёжность для G_3, G_3^{34} по два раза.

Тем не менее имеется возможность рекурсивного использования формулы (1), пусть и с пересчётом для отдельных графов, что всё равно ускоряет расчёт в силу экспоненциальной сложности точного расчёта надёжности. Данный подход предложен как окончательный в работах Вуда [25] и в более поздних наших работах [27 – 31]. Работы [28 – 31] содержат также представление обозначенной проблемы пересчёта надёжности для отдельных графов и методы учёта группы сечений специального вида. Например, для графов продольной структуры, как на рис. 7, автором ранее предложен алгоритм, в рамках которого можно учесть оба сечения и соответствующие компоненты. Кроме этого, рассмотрены циклические графы [28, 31] и случай, когда граф разделяется сечением более чем на две компоненты. Для последних двух случаев показано, как можно учесть все сечения и соответствующие компоненты в рамках одной формулы (для каждого случая своя формула).

В наших работах предлагается искать 2-сечения перебором. Целесообразно для этого не перебирать все пары, а удалять узлы по одному и делать разложение полученного подграфа на двусвязные компоненты. Как указывает Вуд [25], его подход использует разложение на трёхсвязные компоненты [26]. Однако собственно трёхсвязные компоненты для расчёта надёжности не требуются, так как для их получения добавляются виртуальные рёбра, соединяющие вершины 2-сечений, что делает трёхсвязные компоненты трёхсвязными графами. При использовании формулы (1) и, фактически, при использовании метода Вуда мы переходим к новым подграфам и графам, получаемым из них стягиванием разрезающих вершин. В отличие от случая с двусвязными

компонентами, когда двусвязная компонента далее неразлагаема по точкам сочленения, эти новые подграфы могут быть далее разложены по собственным 2-сечениям, не обязательно являющимися 2-сечениями исходного графа, и так далее рекурсивным способом. Например, если граф G на рис. 7 содержит только указанные на рисунке три 2-сечения, то каждый из подграфов G_i может, в свою очередь, также иметь 2-сечения, а может иметь структуру, аналогичную исходному графу G. Естественно, в этих случаях поиск 2-сечений в подграфах G_i также является целесообразным, как и далее по рекурсии.

Разложение на трёхсвязные компоненты естественным образом даёт информацию обо всех 2-сечениях исходного графа. Вуд не касается аспекта практической реализации своего метода, упоминая при этом, что для нахождения 2-сечений теоретически может быть использован классический результат Хопкрофта — Тарьяна [26] по разложению на трёхсвязные компоненты за линейное время $O(M + N)$. С момента выхода этой работы в 1972 г. в ней найдено немало неточностей [36]. Предложены альтернативные подходы к описанию разложения [37], в качестве аргументации их необходимости упоминается слишком большая сложность восприятия результатов их практической реализации. Своеобразной точкой в этом вопросе стала работа [36], в которой исправлены все ошибки и предложен корректный алгоритм на основе результатов Хопкрофта — Тарьяна. Полученный для описания разложения объект получил название SPQR-дерева и нашёл широкое применение в области представления планарных графов.

В данной работе для решения проблемы учёта всех 2-сечений предлагается использовать мультиграф разбиений и алгоритм его обхода, представленные ниже.

4.2. Мультиграф разбиений и алгоритм расчёта вероятности связности графа с учётом всех двухвершинных сечений

Для представления структуры произвольного графа с точки зрения всех его двухвершинных сечений и двухвершинных сечений его трёхсвязных компонент (без добавленных виртуальных рёбер, соединяющих вершины 2-сечений), и так далее по рекурсии, предлагается ввести в рассмотрение такой объект, как мультиграф разбиений. Определим *мультиграф разбиений* G_{split} для графа $G = (V, E)$ на множестве его подграфов $\{G_i : 1 \leqslant i \leqslant L\}$ следующим образом:

1) Узлы G_{split} суть графы G_i.
2) Если G_i и G_j пересекаются по вершинам $v_1, \ldots, v_l$, то существует l рёбер между узлами G_i и G_j, каждое с соответствующей меткой v_m.

Здесь мы используем термин «метка ребра» вместо распространённого «вес ребра», так как в данном случае принципиальное значение имеет не количественное, а символьное значение, присвоенное каждому ребру. В качестве множества подграфов G_i графа G при построении его мультиграфа разбиений нецелесообразно использовать непосредственно трёхсвязные компоненты в силу того, что, как уже упоминалось, они содержат добавленные виртуальные рёбра, а графы, которым добавляются рёбра, могут также содержать 2-сечения, что позволяет рекурсивно вести разложение дальше. Вместо этого введём в рассмотрение трёхсвязные ядра графа G.

Пусть G — двусвязный граф, $\{u, v\}$ — сечение в нём, разделяющее его на G_1 и G_2. Эти подграфы также могут содержать 2-сечения и даже 1-сечения, т. е. точки сочленения, например в случае циклического графа [28, 31]. Этими сечения подграфы разделяются на новые подграфы и т. д. Если при такой рекурсивной процедуре получен подграф, не содержащий 1- и 2-сечений, будем называть его *трёхсвязным ядром* гра-

фа G. Пример структуры двусвязного графа с 2-сечениями и его мультиграфа разбиений приведён на рис. 8.

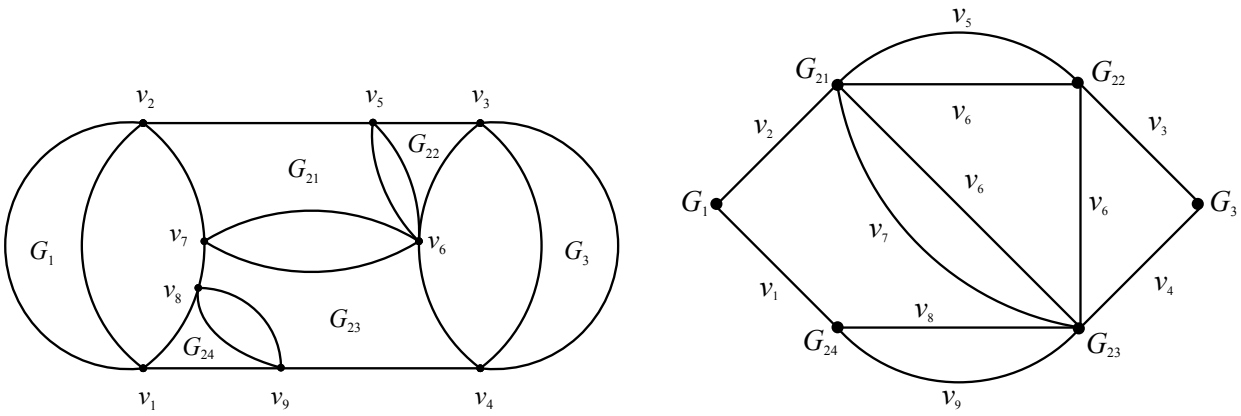


Рис. 8. Пример структуры двусвязного графа с сечениями и его мультиграф разбиений

Алгоритм построения мультиграфа разбиений двусвязного графа на его трёхсвязных ядрах следует непосредственно из определений этих объектов. Для расчёта надёжности графа мы предлагаем алгоритм обхода его мультиграфа разбиений, позволяющий для каждого трёхсвязного ядра вычислять надёжность только один раз, как и для графов, получаемых из них стягиваниями всевозможным образам разрезающих вершин.

В рекурсивной процедуре RelCut(H) (алгоритм 1) каждый узел мультиграфа разбиений G_i содержит список стянутых в нём вершин Merged(G_i), которые стягиваются в процессе рекурсии; с каждым узлом g исходного мультиграфа разбиений (т. е. с каждым трёхсвязным ядром исходного графа) в глобальной памяти связан список вида $R(g)$, $R(g^{12})$, …, т. е. список со значениями надёжности графов, получаемых из g стягиванием различными способами разрезающих вершин, которые содержатся в g. Использование этих переменных и меток мультиграфа разбиений позволяет осуществлять расчёт надёжности двусвязной сети без перерасчёта надёжности трёхсвязных ядер.

В алгоритме используется функция Rel(H), вычисляющая надёжность графа, задающегося мультиграфом разбиений H (не обязательно именно исходного графа). Для её реализации может быть использован любой из известных методов, например метод факторизации [4].

Если делать расчёт надёжности графа на рис. 8 рекурсивным применением формулы (13) с перебором сечений в лексикографическом порядке, то придётся посчитать надёжность $G_1, G_1' - 1$ раз, $G_3, G_3' - 2$ раза, $G_{21}, G_{21}^{67}, G_{21}^{56}, G_{21}^{567} - 1$ раз, $G_{22}, G_{22}^{56} - 2$ раза, $G_{23}, G_{23}^{89} - 3$ раза, $G_{23}^{67}, G_{23}^{67|89} - 2$ раза, $G_{24}, G_{24}^{89} - 5$ раз. С помощью алгоритма 1 можно это сделать без пересчёта.

К настоящему времени введено в рассмотрение значительное количество математических объектов для описания структуры графов, большинство из которых было предназначено для той или иной конкретной задачи [38, 39]. Автор отдаёт себе отчёт в том, что, возможно, описаны и объекты, близкие мультиграфу разбиений. Однако принято решение использовать именно данный объект, который, при подходящем определении подграфов G_i для разбиения, приводит к решению поставленной задачи. Отметим также, что для этой цели мы могли бы и немного по-другому определить мультиграф разбиений. Например, можно за основу разбиений взять не подграфы, а

Алгоритм 1. RelCut(H)

Если существует разрез в H, все рёбра которого, кроме одного, с одной меткой, **то**
  // пусть разрез разделяет H на G_1 и G_2, а рёбра имеют метки u, v
  Для всех $i \in \{1, 2\}$
    Если G_i — узел в H, **то**
      $r_i := \mathrm{Rel}\left(G_i^{\mathrm{Merged}(G_i)}\right)$, если эта величина ранее не была вычислена;
      $\mathrm{Merged}(G_i) := \mathrm{Merged}(G_i) + |uv|$;
      $r'_i := \mathrm{Rel}\left(G_i^{\mathrm{Merged}(G_i)}\right)$, если эта величина ранее не была вычислена;
    иначе
      Если G_i раскладывается на двусвязные компоненты $B_1, \ldots, B_l$ (без учёта рёбер-компонент), **то**
        $r_i := \prod \mathrm{RelCut}(B_i)$;
      иначе
        $r_i := \mathrm{RelCut}(G_i)$;
        обновить метки с учётом слияния u, v;
        $r'_i := \mathrm{RelCut}(G_i^{uv})$.
  $Result := r_1 r'_2 + r'_1 r_2 - r_1 r_2$;
иначе
  $Result := \mathrm{Rel}(H)$.

подмножества вершин. Или можно мультиграф разбиений представить гиперграфом, заменив рёбра с одинаковыми метками гиперрёбрами. Это приведёт к определённой разнице в процессах обхода данных объектов. В итоге, по совокупности факторов, как наиболее простой объект выбран мультиграф разбиений.

Для наших целей можно вместо мультиграфа разбиений использовать, например, SPQR-дерево [36]. Однако в данном случае потребуется также формировать и SPQR-дерево для каждого R-узла дерева и т. д. По сути, необходимо иметь некое «рекурсивное SPQR-дерево». Другой альтернативой могло бы стать использование древесной декомпозиции [39], что, однако, привело бы к аналогичной проблеме — дальнейшего разложения узлов этого дерева, так как трёхсвязные компоненты без виртуальных рёбер также могут содержать 2-сечения.

При этом в перспективе, для описания группы сечений произвольной мощности, мультиграф разбиений может быть использован без каких-либо изменений, в отличие от SPQR-дерева. Теоретически для его построения может быть использован известный алгоритм построения SPQR-дерева за $O(M+N)$ операций [36], однако разработка подобного алгоритма является отдельной сложной задачей, поэтому пока предлагается делать это рекурсивным перебором сечений. Кроме этого, представляется также возможным разработать алгоритм построения и одновременно обхода мультиграфа разбиений.

Заключение

Представленный математический аппарат позволяет эффективно использовать декомпозицию сети по сечениям для расчёта вероятности её связности. Так как известные алгоритмы точного расчета вероятности связности сети имеют экспоненциаль-

ную сложность, использование предлагаемого подхода позволяет значительно ускорить процесс расчёта, для некоторых структур — на порядки.

Часть результатов уже была представлена [20, 30 – 32], часть публикуется впервые. К последним относится корректное доказательство разрешимости системы линейных уравнений, решив которую, мы выразим вероятности отделений подграфа через надёжности всевозможных вариантов его стягивания по разрезающим вершинам. Среди новых результатов также корректная формула для надёжности сети с четырёхвершинным сечением и метод, позволяющий при расчёте надёжности двусвязной сети эффективно учитывать все её двухвершинные сечения и двухвершинные сечения её подсетей, на которые сеть делится двухвершинными сечениями. Подобным рекурсивным способом учитываются и другие двухвершинные сечения.

ЛИТЕРАТУРА

1. *Жуковский М. Е., Райгородский А. М.* Случайные графы: модели и предельные характеристики // Успехи математических наук. 2015. Т. 70. № 1(421). С. 35–88.
2. *Colbourn Ch. J.* The Combinatorics of Network Reliability. N.Y.: Oxford Univ. Press, 1987. 160 p.
3. *Valiant L.* The complexity of enumeration and reliability problems // SIAM J. Comput. 1979. V. 8. No. 3. P. 410–421.
4. *Page L. B. and Perry J. E.* A practical implementation of the factoring theorem for network reliability // IEEE Trans. Reliability. 1988. V. 37. No. 3. P. 259–267.
5. *Рябинин И. А.* Логико-вероятностное исчисление как аппарат исследования надежности и безопасности структурно-сложных систем // Автомат. и телемех. 2003. Т. 7. С. 178–186.
6. *Satyanarayana A. and Wood R. K.* A linear-time algorithm for computing K-terminal reliability in series-parallel networks // SIAM J. Comput. 1985. V. 18. P. 818–883.
7. *Shooman A. M. and Kershenbaum A.* Methods for communication-network reliability analysis: probabilistic graph reduction // IEEE Proc. Reliability and Maintainability Symp. 1992, Las Vegas, USA. N.Y.: IEEE Press, 1992. P. 441–448.
8. *Wood R. K.* A factoring algorithm using polygon-to-chain reductions for computing K-terminal network reliability // Networks. 1985. V. 15. No. 2. P. 173–190.
9. *Мочалов В. А.* Метод синтеза отказоустойчивой струкутры сенсорной сети при наличии ограничений по размещению узлов сети в разнородном пространстве // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6. № 10. С. 71–75.
10. *Rodionov A. S. and Rodionova O. K.* Random hypernets in reliability analysis of multilayer networks // Lecture Notes in Electrical Engineering. 2015. V. 343. P. 307–315.
11. *Мелентьев В. А.* Функция структурной отказоустойчивости и d-ограниченная компонента связности графа вычислительной системы // Прикладная дискретная математика. 2008. Т. 2. № 2. С. 102–106.
12. *Levendovszky J., Jereb L., Elek Zs., and Vesztergombi Gy.* Adaptive statistical algorithms in network reliability analysis // Performance Evaluation. 2002. V. 48. No. 1–4. P. 225–236.
13. *Цицашвили Г. Ш., Осипова М А., Лосев А. С.* Вывод асимптотических констант для вероятности несвязности планарного взвешенного графа // Прикладная дискретная математика. 2014. № 2(24). С. 97–100.
14. *Лотоцкий А. Д.* Исследование точных методов вычисления структурной надёжности компьютерных сетей // Инновации на основе информационных и коммуникационных технологий. 2014. Т. 1. С. 233–235.
15. *Родионов А. С., Родионова О. К.* Некоторые методы ускорения расчета надёжности информационных сетей // Тр. 30-й Междунар. конф. «Информационные технологии в на-

уке, образовании, телекоммуникации и бизнесе» (IT+SF'2003), Гурзуф, Украина, 2003. Запорожье: Изд-во Запорож. ун-та, 2003. С. 215–217.

16. *Мигов Д. А.* Формулы для быстрого расчета вероятности связности подмножества вершин в графах небольшой размерности // Проблемы информатики. 2010. Т. 6. С. 10–17.
17. *Chen Y., Li J., and Chen J.* A new algorithm for network probabilistic connectivity // Proc. IEEE Military Communications Conf. V. 2. N.Y.: IEEE Press, 1999. P. 920–923.
18. *Tittmann P.* Partitions and network reliability // Discr. Appl. Math. 1999. V. 95. No. 1–3. P. 445–453.
19. *Won J.-M. and Karray F.* Cumulative update of all-terminal reliability for faster feasibility decision // IEEE Trans. Reliability. 2010. V. 59. No. 3. P. 551–562.
20. *Rodionov A., Migov D., and Rodionov O.* Improvements in the efficiency of cumulative updating of all terminal network reliability // IEEE Trans. Reliability. 2012. V. 61. No. 2. P. 460–465.
21. *Martinez S. P., Calvino B. O., and Rocco S. C. M.* All-terminal reliability evaluation through a Monte Carlo simulation based on an MPI implementation // European Safety and Reliability Conference: Advances in Safety, Reliability and Risk Management (PSAM 2011/ESREL 2012). Helsinki, 2012. P. 1–6.
22. *Родионов А. С., Сакерин А. В., Мигов Д. А.* Некоторые вопросы параллельной реализации алгоритма полного перебора (на примере задач надёжности сетей) // Вестник СибГУТИ. 2014. Т. 4. С. 79–84.
23. *Hebert P.-R.* Sixty years of network reliability // Mathematics in Computer Science. 2018. V. 12. P. 275–293.
24. *Попков В. К.* Математические модели связности. Ч. 1–3. Новосибирск: Изд-во ИВМиМГ СО РАН, 2000–2002.
25. *Wood R. K.* Triconnected decomposition for computing K-terminal network reliability // Networks. 1989. V. 19. P. 203–220.
26. *Hopcroft J. and Tarjan R.* Dividing a graph into triconnected components // SIAM J. Comput. 1973. V. 2. P. 135–158.
27. *Мигов Д. А.* Использование разрезов случайного графа для вычисления вероятности его связности // Труды конф. молодых ученых ИВМиМГ СО РАН, 2004. Новосибирск: ИВМиМГ СО РАН, 2004. С. 133–130.
28. *Мигов Д. А.* Расчет вероятности связности сети с применением вершинных разрезов специального вида // Тез. докл. V Всерос. конф. молодых ученых по мат. моделированию и инф. технологиям, 2004. Новосибирск: ИВТ СО РАН, 2004. С. 24–25.
29. *Мигов Д. А.* Расчет вероятности связности сети с применением продольных разрезов // Труды конф. молодых ученых ИВМиМГ СО РАН, 2006. Новосибирск: ИВМиМГ СО РАН, 2006. С. 144–151.
30. *Migov D. A., Rodionova O. K., Rodionov A. S., and Choo H.* Network probabilistic connectivity: using node cuts // LNCS. 2006. V. 4097. P. 702–709.
31. *Мигов Д. А.* Расчёт вероятности связности случайного графа с применением сечений: дис. ... канд. физ.-мат. наук. Новосибирск: Институт вычислительной математики и математической геофизики, 2008. 96 с.
32. *Мигов Д. А.* Методы расчета надежности сетей, основанные на использовании сечений // Вычислительные технологии. 2008. Т. 13. С. 425–431.
33. *Мигов Д. А.* Расчёт надёжности сети с ограничением на диаметр с применением точек сочленения // Автоматика и телемеханика. 2011. Т. 7. С. 69–74.
34. *Burgos J. M. and Amoza F. R.* Factorization of network reliability with perfect nodes I: Introduction and statements // Discr. Appl. Math. 2016. V. 198. P. 82–90.

35. *Burgos J. M.* Factorization of network reliability with perfect nodes II: Connectivity matrix // Discr. Appl. Math. 2016. V. 198. P. 91–100.
36. *Gutwenger C. and Mutzel P. A.* A linear time implementation of SPQR-trees // LNCS. 2001. V. 1984. P. 77–90.
37. *Tsin Y. H.* Decomposing a multigraph into split components // Proc. CATS'12, Melbourne, Australia. 2012. V. 128. P. 3–12.
38. *Карпов Д. В.* Дерево разрезов и минимальный k-связный граф // Записки научных семинаров ПОМИ. 2014. Т. 427. С. 22–40.
39. *Halin R.* S-functions for graphs // J. Geometry. 1976. V. 8. No. 2. P. 171–186.

REFERENCES

1. *Zhukovskiy M. E. and Raygorodskiy A. M.* Sluchaynyye grafy: modeli i predelnyye kharakteristiki [Random graphs: models and asymptotic characteristics]. Uspekhi Matematicheskikh Nauk, 2015, vol. 70, no. 1(421), pp. 35–88. (in Russian)
2. *Colbourn Ch. J.* The combinatorics of network reliability. N.Y., Oxford Univ. Press, 1987. 160 p.
3. *Valiant L.* The complexity of enumeration and reliability problems. SIAM J. Comput., 1979, vol. 8, no. 3, pp. 410–421.
4. *Page L. B. and Perry J. E.* A practical implementation of the factoring theorem for network reliability. IEEE Trans. Reliability, 1988, vol. 37, no. 3, pp. 259–267.
5. *Ryabinin I. A.* Logical-probabilistic calculus: A tool for studying the reliability and safety of structurally complex systems. Automation and Remote Control, 2003, vol. 64, no. 7, pp. 178–186.
6. *Satyanarayana A. and Wood R. K.* A linear-time algorithm for computing K-terminal reliability in series-parallel networks. SIAM. J. Comput., 1985, vol. 18, pp. 818–883.
7. *Shooman A. M. and Kershenbaum A.* Methods for communication-network reliability analysis: probabilistic graph reduction. IEEE Proc. Reliability and Maintainability Symp., 1992, Las Vegas, USA. N.Y.: IEEE Press, 1992, pp. 441–448.
8. *Wood R. K.* A factoring algorithm using polygon-to-chain reductions for computing K-terminal network reliability. Networks, 1985, vol. 15, no. 2, pp. 173–190.
9. *Mochalov V. A.* Metod sinteza otkazoustoychivoy strukutry sensornoy seti pri nalichii ogranicheniy po razmeshcheniyu uzlov seti v raznorodnom prostranstve [The method of synthesis of fault-tolerant structure of the sensor network in restrictions on the placement of network nodes in a heterogeneous space]. T-Comm: Telekommunikatsii i Transport, 2012, vol. 6, no. 10, pp. 71–75. (in Russian)
10. *Rodionov A. S. and Rodionova O. K.* Random hypernets in reliability analysis of multilayer networks. Lecture Notes in Electrical Engineering, 2015, vol. 343, pp. 307–315.
11. *Melentyev V. A.* Funktsiya strukturnoy otkazoustoychivosti i d-ogranichennaya komponenta svyaznosti grafa vychislitelnoy sistemy [Function of structural fault tolerance and d-limited connected component of graph of a computational system]. Prikladnaya Diskretnaya Matematika, 2008, vol. 2, no. 2, pp. 102–106. (in Russian)
12. *Levendovszky J., Jereb L., Elek Zs., and Vesztergombi Gy.* Adaptive statistical algorithms in network reliability analysis. Performance Evaluation, 2002, vol. 48, no. 1–4, pp. 225–236.
13. *Tsitsiashvili G. Sh., Osipova M A., and Losev A. S.* Vyvod asimptoticheskikh konstant dlya veroyatnosti nesvyaznosti planarnogo vzveshennogo grafa [Derivation of asymptotic constants for the probabilistic connectivity of a planar weighted graph]. Prikladnaya Diskretnaya Matematika, 2014, no. 2(24), pp. 97–100. (in Russian)

14. *Lototsky A. D.* Issledovaniye tochnykh metodov vychisleniya strukturnoy nadyozhnosti kompyuternykh setey [Study of accurate methods for calculating the structural reliability of computer networks]. Innovatsii na Osnove Informatsionnykh i Kommunikatsionnykh Tekhnologiy, 2014, vol. 1, pp. 233–235. (in Russian)
15. *Rodionov A. S. and Rodionova O. K.* Nekotoryye metody uskoreniya rascheta nadyozhnosti informatsionnykh setey [Some methods for speeding up the calculation of the reliability of information networks]. Proc. IT+SF 2003, Gurzuf, Ukraine, 2003. Zaporozhye: Zaporozhye State University Publ., 2003, pp. 215–217. (in Russian)
16. *Migov D. S.* Formuly dlya bystrogo rascheta veroyatnosti svyaznosti podmnozhestva vershin v grafakh nebolshoy razmernosti [Formulas for quickly calculating the probabilistic connectivity of a subset of vertices in graphs of small dimension]. Problemy Informatiki, 2010, vol. 6, pp. 10–17. (in Russian)
17. *Chen Y., Li J., and Chen J.* A new algorithm for network probabilistic connectivity. Proc. IEEE Military Communications Conf., N.Y., IEEE Press, 1999, vol. 2, pp. 920–923.
18. *Tittmann P.* Partitions and network reliability. Discr. Appl. Math., 1999, vol. 95, no. 1–3, pp. 445–453.
19. *Won J.-M. and Karray F.* Cumulative update of all-terminal reliability for faster feasibility decision. IEEE Trans. Reliability, 2010, vol. 59, no. 3. pp. 551–562.
20. *Rodionov A., Migov D., and Rodionov O.* Improvements in the efficiency of cumulative updating of all terminal network reliability. IEEE Trans. Reliability, 2012, vol. 61, no. 2, pp. 460–465.
21. *Martinez S. P., Calvino B. O., and Rocco S. C. M.* All-terminal reliability evaluation through a Monte Carlo simulation based on an MPI implementation. European Safety and Reliability Conference: Advances in Safety, Reliability and Risk Management (PSAM 2011/ESREL 2012), Helsinki, 2012, pp. 1–6.
22. *Rodionov A., Sakerin A., and Migov D.* Nekotoryye voprosy parallelnoy realizatsii algoritma polnogo perebora (na primere zadach nadyozhnosti setey) [Some issues of parallel implementation of the exhaustive search algorithm (by the example of network reliability problems)]. Vestnik SibGUTI, 2014, vol. 4, pp. 79–84. (in Russian)
23. *Hebert P.-R.* Sixty years of network reliability. Mathematics in Computer Science, 2018, vol. 12, pp. 275–293.
24. *Popkov V. K.* Matematicheskiye modeli svyaznosti [Mathematical Models of Connectivity]. Vol. 1–3. Novosibirsk, ICMMG Publ., 2000–2002. (in Russian)
25. *Wood R. K.* Triconnected decomposition for computing K-terminal network reliability. Networks, 1989, vol. 19, pp. 203–220.
26. *Hopcroft J. and Tarjan R.* Dividing a graph into triconnected components. SIAM J. Comput., 1973, vol. 2, pp. 135–158.
27. *Migov D. A.* Ispolzovaniye razrezov sluchaynogo grafa dlya vychisleniya veroyatnosti yego svyaznosti [Using vertex cuts of a random graph to calculate the probability of its connectivity]. Proc. Young Scientists Conf. ICMMG of SB RAS, 2004, Novosibirsk, ICMMG Publ., pp. 133–130. (in Russian)
28. *Migov D. A.* Raschet veroyatnosti svyaznosti seti s primeneniyem vershinnykh razrezov spetsialnogo vida [Calculation of the probability of network connectivity using vertex cuts of a special kind]. Proc. All-Russian Young Scientists Conf. Math. Modeling and Inf. Technology, 2004, Novosibirsk, ICT of SB RAS, pp. 24–25. (in Russian)
29. *Migov D. A.* Raschet veroyatnosti svyaznosti seti s primeneniyem prodolnykh razrezov [Calculation of the probability of network connectivity using longitudinal cuts]. Proc. Young Scientists Conf. ICMMG SB RAS, 2006, Novosibirsk, ICMMG Publ., pp. 144–151. (in Russian)

30. *Migov D. A., Rodionova O. K., Rodionov A. S., and Choo H.* Network probabilistic connectivity: using node cuts. LNCS, 2006 vol. 4097, pp. 702–709.
31. *Migov D. A.* Raschyot veroyatnosti svyaznosti sluchaynogo grafa s primeneniyem secheny [Calculation of the Connectivity Probability of a Random Graph Using Cuts]. PhD Thesis, Novosibirsk, ICMMG, 2008. 96 p. (in Russian)
32. *Migov D. A.* Metody rascheta nadezhnosti setey, osnovannyye na ispolzovanii secheny [Methods for calculating the reliability of networks based on the use of sections]. Vychislitelnyye Tekhnologii, 2008, vol. 13, pp. 425–431. (in Russian)
33. *Migov D. A.* Computing diameter constrained reliability of a network with junction points. Automation and Remote Control, 2011, vol. 72, no.7, pp. 1415–1419.
34. *Burgos J. M. and Amoza F. R.* Factorization of network reliability with perfect nodes I: Introduction and statements. Discr. Appl. Math., 2016, vol. 198, pp. 82–90.
35. *Burgos J. M.* Factorization of network reliability with perfect nodes II: Connectivity matrix. Discr. Appl. Math., 2016, vol. 198, pp. 91–100.
36. *Gutwenger C. and Mutzel P. A.* A linear time implementation of SPQR-trees. LNCS, 2001, vol. 1984, pp. 77–90.
37. *Tsin Y. H.* Decomposing a multigraph into split components. Proc. CATS'12, Melbourne, Australia, 2012, vol. 128, pp. 3–12.
38. *Karpov D. V.* Derevo razrezov i minimalny k-svyazny graf [Section tree and minimally k-connected graph]. Zapiski Nauchnykh Seminarov POMI, 2014, vol. 427, pp. 22–40. (in Russian)
39. *Halin R.* S-functions for graphs. J. Geometry, 1976, vol. 8, no. 2, pp. 171–186.

УДК 519.87

ПОИСК КРАТЧАЙШИХ ПУТЕЙ В ОПТИМАЛЬНЫХ ДВУМЕРНЫХ ЦИРКУЛЯНТАХ[1]

Э. А. Монахова

Институт вычислительной математики и математической геофизики СО РАН, г. Новосибирск, Россия

Для семейства оптимальных двумерных циркулянтных сетей с аналитическим описанием получены две новые улучшенные версии алгоритма поиска кратчайших путей с константной оценкой сложности. Дано простое, основанное на геометрической модели циркулянтных графов, доказательство формул, используемых для алгоритма поиска кратчайших путей. Представлены алгоритмы парных обменов и даны их оценки для сетей на кристалле с топологией в виде рассмотренных графов. Новые версии алгоритма улучшают также предложенный ранее автором алгоритм поиска кратчайших путей для оптимальных обобщённых графов Петерсена с аналитическим описанием.

Ключевые слова: *двумерные циркулянтные графы, диаметр, кратчайшие пути, оптимальные обобщённые графы Петерсена, сети на кристалле.*

DOI 10.17223/20710410/47/7

A COMPUTATION OF THE SHORTEST PATHS IN OPTIMAL TWO-DIMENSIONAL CIRCULANT NETWORKS

E. A. Monakhova

Institute of Computational Mathematics and Mathematical Geophysics SB RAS, Novosibirsk, Russia

E-mail: emilia@rav.sscc.ru

A family of tight optimal two-dimensional circulant networks designed by analytical formulas has a description of the form $C(N; d, d+1)$, where N is the order of a graph and the generator d is the nearest integer to $(\sqrt{2N-1}-1)/2$. For this family, two new improved versions of a shortest-path routing algorithm with a complexity O(1) are presented. Simple proofs for formulas used for routing algorithms based on the plane tessellation are received. In the routing algorithm, for a graph $C(N; d, d+1)$ the following formulas for the computing shortest routing vector (x, y) from 0 to a node $k \leqslant \lfloor N/2 \rfloor$ are used: if $k \bmod (d+1) = 0$ or $\lfloor k/(d+1) \rfloor < d+1-2k \bmod (d+1)$, then $x = -k \bmod (d+1)$, $y = \lfloor k/(d+1) \rfloor - x$, else $x = -k \bmod (d+1) + d + 1$, $y = \lfloor k/(d+1) \rfloor - x + 1$. The routing algorithms and their estimates are considered for using in topologies of networks-on-chip. For implementation in networks-on-chip the proposed routing algorithm requires $\lceil \log_2 N \rceil + \lceil \log_2 \lceil \sqrt{N/2} \rceil \rceil$ bits. New versions of the routing algorithm improve also the routing algorithm proposed early by the author for optimal generalized Petersen graphs with an analytical description of the form $P(N, a, a+1)$, where $2N$ is the order of a graph and $a = \lceil \sqrt{(N-1)/2} \rceil - 1$.

[1]Исследование выполнено в рамках проекта № 0315-2016-0006.

Keywords: *two-dimensional circulant networks, diameter, shortest paths, optimal generalized Petersen graphs, networks-on-chip.*

Введение

Наряду с широким интересом к циркулянтным сетям в различных областях информатики и вычислительной техники [1 – 3] актуальным становится их применение в качестве топологии для сетей на кристалле (networks-on-chip) [4 – 6]. Это обусловлено их лучшими структурными характеристиками [1, 4] и высокими показателями масштабируемости при большом количестве узлов по сравнению со стандартными топологиями сетей на кристалле (mesh, torus). В связи с необходимостью сокращения аппаратурных затрат ресурсов для сетей на кристалле важной задачей становится разработка эффективных алгоритмов маршрутизации в сетях с циркулянтной топологией. В данной работе рассматриваются эффективные алгоритмы парной маршрутизации, разработанные для двумерных циркулянтных сетей.

Пусть $s_1, s_2, \ldots, s_k, N$ — целые числа, такие, что $1 \leqslant s_1 < s_2 < \ldots < s_k < N$. Неориентированный граф C с множеством вершин $V = \{0, 1, \ldots, N-1\}$ и множеством рёбер $E = \{(i,j) : i - j \equiv \pm s_m \pmod N, m = 1, \ldots, k\}$ называется циркулянтной сетью, а множество $S = \{s_1, s_2, \ldots, s_k\}$ — множеством образующих графа. Параметрическое описание вида $(N; S)$ определяет циркулянт порядка N и размерности k. Свойство симметрии циркулянтов позволяет в дальнейшем ограничиться рассмотрением циркулянтных графов с образующими, не превосходящими $\lfloor N/2 \rfloor$.

Диаметром графа C называется $D(N;S) = \max\limits_{i,j \in V} D(i,j)$, где $D(i,j)$ — длина кратчайшего пути между вершинами i и j, принадлежащими C. Точная нижняя граница диаметра двумерных циркулянтов для любого порядка $N > 4$ равна [7]

$$D(N) = \lceil (-1 + \sqrt{2N-1})/2 \rceil.$$

Средним расстоянием (средним диаметром в некоторых источниках) графа $C(N;S)$ называется $\overline{d}(N;S) = (1/N(N-1)) \sum\limits_{i,j} D(i,j)$. Диаметр и среднее расстояние оценивают максимальную и среднюю структурные задержки в сети. Как показали исследования, наилучшими структурами вычислительных систем по различным критериям функционирования при равном количестве узлов и линий связи являются структуры с минимальными диаметром и средним расстоянием.

1. Оптимальные двумерные циркулянты

Двумерные циркулянты интенсивно изучаются в литературе в связи с различными практическими приложениями. Для $k = 2$ в 1981 г. доказано [7], что для каждого числа вершин N циркулянтные графы могут иметь одновременно минимальный диаметр $D(N)$ и минимально возможное среднее расстояние, т. е. являются оптимальными.

Теорема 1 [7]. Для любого целого $N > 4$ оптимальный двумерный циркулянт порядка N есть

$$C(N; d, d+1), \text{ где } d = [(\sqrt{2N-1} - 1)/2], \tag{1}$$

$[x]$ — ближайшее целое к x.

В 1991 г. Р. Байвиде с соавт. [8] получили то же самое семейство циркулянтов (1), записанное в другом виде.

Теорема 2 [8]. Для любого целого $N > 2$ оптимальный двумерный циркулянт порядка N есть

$$C(N; b-1, b), \text{ где } b = \lceil \sqrt{N/2} \rceil. \tag{2}$$

Два оптимальных семейства (1) и (2) идентичны как по числовым значениям образующих и порядков, так и по диапазонам существования с данными образующими. Докажем это.

Лемма 1. Для любого порядка $N > 4$ циркулянтные графы $C(N; d, d+1)$ и $C(N; b-1, b)$, описываемые соответственно (1) и (2), совпадают при $b-1 = d$ и являются оптимальными при изменении N в диапазоне $2d^2 < N \leqslant 2(d+1)^2$ и соответственно $2(b-1)^2 < N \leqslant 2b^2$.

Доказательство. Пусть $N > 4$ — любое заданное число. Для семейства (1) из определения ближайшего целого следует $d - 1/2 \leqslant (\sqrt{2N-1} - 1)/2 < d + 1/2$. Отсюда после простых преобразований получаем $2d^2 + 1/2 \leqslant N < 2(d+1)^2 + 1/2$. Так как N — целое число, имеем

$$2d^2 < N \leqslant 2(d+1)^2.$$

Аналогично для семейства (2) из определения b следует $b - 1 < \sqrt{N/2} \leqslant b$ и

$$2(b-1)^2 < N \leqslant 2b^2.$$

Поскольку полученные диапазоны изменения N имеют место при любом заданном N, отсюда следует $b - 1 = d$, что и требовалось доказать. ■

Вопросы исследования найденного семейства оптимальных двумерных циркулянтов как сетей связи компьютерных систем широко изучаются последние 20 лет. В работе [9] изучены сетевые свойства двумерных циркулянтов, в частности оптимальных графов вида $C(N_d; d, d+1)$, и исследовали возможность вложимости в них решёток. Здесь и далее $N_d = 2d^2 + 2d + 1$ — максимально возможный порядок двумерного циркулянта диаметра $d \geqslant 0$ (подробнее см. [1]). В [10 – 12] рассматриваются оптимальные сети (2), названные Midimew-сетями, в качестве технической реализации сетей связи суперкомпьютерных систем высокой производительности. В [11] показано для Midimew-сетей увеличение сетевой производительности при реальных нагрузках, а также уменьшение длины среднего пути сообщения по сравнению с торами. В [10, 11] для этой топологии представлено практическое решение проблемы предотвращения дедлоков (блокировок пути при передаче пакетов). В [12] использовано несколько примеров таких графов как базис при проектировании сетей связи параллельных систем. В [13, 14] применены двумерные циркулянтные сети, в частности семейство вида $C(N_d; d, d+1)$, в теории кодирования при построении совершенных групповых кодов. Реализация графов, описываемых (1) или (2), предложена в качестве топологии при проектировании суперкомпьютеров с массовым параллелизмом и сетей на кристалле [4, 5, 12, 15].

При использовании циркулянтных графов в качестве коммуникационных сетей суперкомпьютерных систем актуальным вопросом является эффективное решение проблемы организации алгоритмов маршрутизации в них. При парной маршрутизации (routing) сообщение должно быть передано из узла-источника в узел-приёмник. Далее рассматривается модель дуплексной ненаправленной передачи информации методом коммутации сообщений. Для организации парных обменов требуется определение кратчайших путей в графе. В [16] установлено, что проблема поиска кратчайших путей по параметрическому описанию циркулянтных сетей общего вида относится к классу NP-трудных задач. Аналитическое решение задачи поиска кратчайших путей по параметрическому описанию для оптимальных циркулянтных графов, описываемых (1) и (2), предложено в [8, 11, 17]. В настоящей работе это решение улучшено и скорректировано для [8, 11] и использовано для разработки алгоритмов парной маршрутизации.

2. Поиск кратчайших путей в двумерных циркулянтах

Рассмотрим эффективное решение задачи поиска кратчайших путей по параметрическому описанию для оптимальных циркулянтных графов $C(N; d, d+1)$, где d определяется по (1).

Пусть $A^{0k} = (x^{0k}, y^{0k}) = (x, y)$ обозначает вектор кратчайшего пути из вершины 0 в вершину k, $0 \leqslant k < N$, в циркулянтном графе $C(N; s_1, s_2)$. Здесь $|x^{0k}|$ задает число образующих s_1, $|y^{0k}|$ — образующих s_2, входящих в кратчайший путь из 0 в k, а $\operatorname{sgn}(x^{0k})$ и $\operatorname{sgn}(y^{0k})$ определяют направления движения в кратчайшем пути по $(+)$ или против $(-)$ соответствующей образующей. Покажем, что для указанных графов связь между номерами вершин i и j и вектором кратчайших путей A^{ij} из i в j может быть получена аналитически.

Для этого надо рассмотреть геометрическую модель графа $C(N; d, d+1)$ (подробнее см. в [1]). Граф $C(N; d, d+1)$ конструируется на плоскости $\mathbb{Z}^2$ в виде ромбоподобной конфигурации из единичных квадратов целочисленной решётки, где каждая точка решётки (x, y) помечена числом $k = xd + y(d+1) \bmod N$. Здесь k, $0 \leqslant k < N$, — номер вершины графа. Все отметки вершин $0 \leqslant k < N$ повторяются на плоскости бесконечное число раз, образуя плотную упаковку ромбоподобных конфигураций из единичных квадратов. На рис. 1 показано, как из ромба с числом вершин $N = N_d$ (обозначен сплошной линией) получаются все оптимальные конфигурации с числом вершин N, $2d^2 - 1 \leqslant N \leqslant 2(d+1)^2 + 1$, путём наращивания (рис. 1, *а*) и сокращения (рис. 1, *б*) клеток (вершин) на последнем ярусе. Все вершины графа $C(N; d, d+1)$ диаметра

$$D = \begin{cases} d, & \text{если } 2d^2 - 1 \leqslant N \leqslant N_d, \\ d+1, & \text{если } N_d < N \leqslant 2(d+1)^2 + 1, \end{cases}$$

расположены внутри ромба $R_D = \{(x, y) : |x| + |y| \leqslant D\}$, причём ярусы от 0 до $D-1$ заполнены полностью и среди номеров вершин, расположенных на этих ярусах, нет одинаковых. В силу указанных свойств для вершин k, $0 \leqslant k < N$, графа $C(N; d, d+1)$ диаметра D имеем следующее: для определения вектора кратчайших путей из 0 в k достаточно вычислить пути в ромбе R_D.

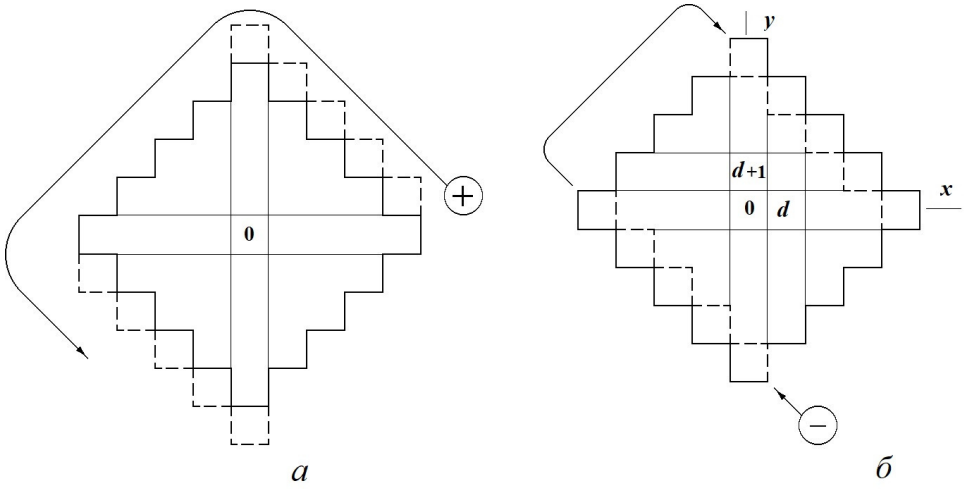


Рис. 1. Геометрическая модель графов $C(N; d, d+1)$

В качестве примера геометрического представления графов семейства $C(N; d, d+1)$ на рис. 2 представлен граф $C(50; 4, 5)$ диаметра $D = 5$ в системе координат (x, y).

Для простоты изображения не показаны рёбра между вершинами $i = xs_1 + ys_2$ и $j = x's_1 + y's_2$, для которых не выполняется $|x - x'| = 1$, $y = y'$ либо $x = x'$, $|y - y'| = 1$. Граф $C(50; 4, 5)$ имеет максимально возможный порядок среди графов семейства (1) с образующими $s_1 = 4$, $s_2 = 5$. Теоремы 3 и 4 решают задачу вычисления вектора кратчайших путей из нулевой вершины во все вершины графов семейства (1). При этом в доказательстве теоремы 3 используется деление номера вершины графа на образующую s_1, что соответствует выделенным горизонтальным областям графа на рис. 2, *а*, а в теореме 4 — на образующую s_2, что соответствует выделенным вертикальным областям графа на рис. 2, *б*.

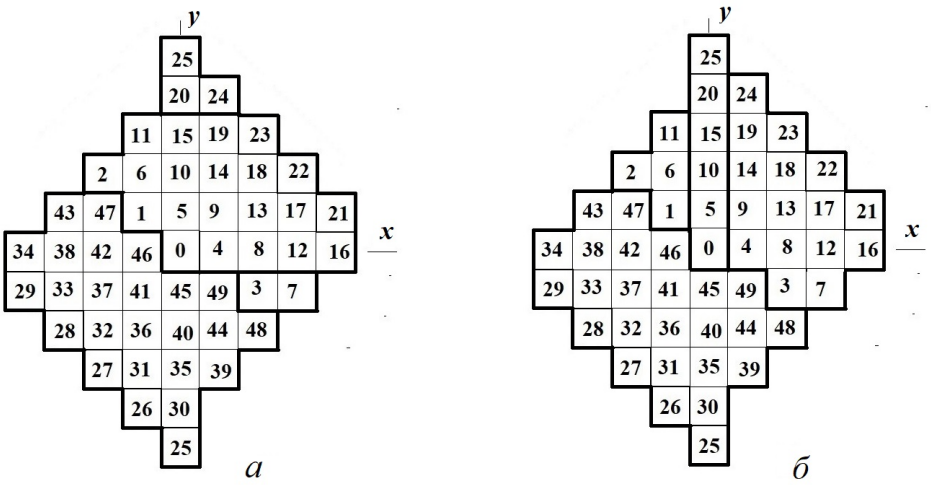


Рис. 2. Граф $C(50; 4, 5)$

Теорема 3. Пусть k, $0 \leqslant k < N$, — номер вершины в графе $C(N; d, d+1)$. Тогда координаты вектора $A^{0k} = (x^{0k}, y^{0k})$ вычисляются следующим образом:

— при $k \leqslant \lfloor N/2 \rfloor$

$$(x^{0k}, y^{0k}) = \begin{cases} (\alpha, \beta), & \text{если } \beta - d \leqslant \alpha \leqslant d, \\ (\alpha + d + 1, \beta - d), & \text{если } \alpha < \beta - d, \\ (\alpha - (d+1), \beta + d) & \text{иначе,} \end{cases} \tag{3}$$

где $\beta = k \bmod d$; $\alpha = \lfloor k/d \rfloor - \beta$;

— при $k > \lfloor N/2 \rfloor$

$$(x^{0k}, y^{0k}) = (-x^{0N-k}, -y^{0N-k}).$$

Доказательство. Согласно свойству циркулянтов, $(x^{0k}, y^{0k}) = (-x^{0N-k}, -y^{0N-k})$ для любой вершины $k \in \{0, \ldots, N-1\}$. Таким образом, определение вектора кратчайших путей A^{0k} для всех k, $\lfloor N/2 \rfloor < k < N$, сводится к определению вектора кратчайших путей вершины с номером $(N-k)$, лежащей в верхней части ромба (не левее линий $y = -x$ для $x \leqslant 0$ и $y = -x + 1$ для $x > 0$) и замене знаков полученных координат на противоположные.

Пусть теперь $0 \leqslant k \leqslant \lfloor N/2 \rfloor$. Требуется найти $x^{0k} = x$, $y^{0k} = y$ — такие координаты вершины с номером k, что

$$k = xd + y(d+1). \tag{4}$$

При доказательстве используем тот факт, что для любых натуральных k и d число k единственным образом представимо через целую часть и остаток от деления на d:

$$k = \lfloor k/d \rfloor d + k \bmod d, \qquad \lfloor k/d \rfloor \geqslant 0, \qquad 0 \leqslant k \bmod d < d. \tag{5}$$

1. Рассмотрим область ромба R_D, представляющего граф $C(N; d, d+1)$, ограниченную следующими условиями:

$$\begin{cases} 0 \leqslant y < d, \\ -y \leqslant x \leqslant d + 1 - y, \\ y - d \leqslant x \leqslant d. \end{cases}$$

В этой области ромба

$$\begin{cases} x + y \geqslant 0, \\ 0 \leqslant y < d. \end{cases}$$

Если представить номер k вершины из этой области, записанный в виде (4) как $k = (x+y)d + y$, то в силу единственности выражения (5) для k получим

$$\lfloor k/d \rfloor = x + y, \quad k \bmod d = y.$$

Отсюда следует

$$x = \lfloor k/d \rfloor - k \bmod d, \quad y = k \bmod d.$$

Подставляя найденные выражения для x и y в уравнения прямых, ограничивающих рассматриваемую область, получим, что найденные формулы для x и y имеют место при выполнении условия

$$k \bmod d - d \leqslant \lfloor k/d \rfloor - k \bmod d \leqslant d.$$

2. Рассмотрим теперь область ромба, ограниченную условиями

$$\begin{cases} y < 0, \\ -y + 1 \leqslant x \leqslant d + y. \end{cases}$$

В этой области ромба

$$\begin{cases} x + y - 1 \geqslant 0, \\ 0 < d + y < d. \end{cases}$$

Если представить номер k вершины из этой области, записанный в виде (4) как $k = (x+y-1)d + (d+y)$, то в силу единственности выражения (5) для k получим

$$\lfloor k/d \rfloor = x + y - 1, \quad k \bmod d = d + y.$$

Отсюда следует

$$x = \lfloor k/d \rfloor - k \bmod d + (d+1), \quad y = k \bmod d - d.$$

Аналогично случаю 1 получаем, что найденные формулы для x и y имеют место при выполнении условия

$$\lfloor k/d \rfloor - k \bmod d < k \bmod d - d.$$

3. Для вершин с номерами $k = d^2 + d$, $d^2 + 2d$, $d^2 + 2d + 1$ координаты равны соответственно $(0, d)$, $(1, d)$, $(0, d+1)$. Вычисленные по формулам (3) координаты (x^{0k}, y^{0k}) совпадают с данными. Эти формулы имеют место при выполнении условия

$$\lfloor k/d \rfloor - k \bmod d > d.$$

Теорема доказана. ■

Заметим, что в графах $C(N; d, d+1)$ при $2d^2 < N < N_d$ для вычисления вектора кратчайших путей из 0 в любую вершину достаточно использовать только первые два вида формул из (3). Теорема 3 даёт аналитическое решение задачи определения вектора кратчайших путей по номеру вершины графа $C(N; d, d+1)$ относительно нулевой вершины. Таким образом, вычисление кратчайших путей в структурах рассматриваемого описания оказывается проще, чем аналогичная процедура для двумерных циркулянтов с описанием, отличным от этого [18]. Решение, полученное в теореме 3, по сравнению с найденным в [17] отличается заменой переменной $i^*(N) \geqslant \lfloor N/2 \rfloor$ на $\lfloor N/2 \rfloor$, где $i^*(N)$ — номер той вершины графа $C(N; d, d+1)$, начиная с которого все его вершины располагаются в нижней части ромба R_D левее линий $x = -y$ для $x \leqslant 0$ и $x - 1 = -y$ для $x > 0$. Тем самым при поиске кратчайших путей не требуется вычисления переменной $i^*(N)$.

Другой вид формул, которые можно использовать при расчёте векторов кратчайших путей в циркулянтных графах $C(N; d, d+1)$, определяет

Теорема 4. Пусть k, $0 \leqslant k < N$, — номер вершины в графе $C(N; d, d+1)$. Тогда координаты вектора $A^{0k} = (x^{0k}, y^{0k})$ вычисляются следующим образом:

— при $k \leqslant \lfloor N/2 \rfloor$

$$(x^{0k}, y^{0k}) = \begin{cases} (-\beta, \alpha), & \text{если } \beta = 0 \text{ или } \alpha + \beta < d + 1, \\ (d + 1 - \beta, \alpha - d) & \text{иначе,} \end{cases} \tag{6}$$

где $\beta = k \bmod (d+1)$; $\alpha = \lfloor k/(d+1) \rfloor + \beta$;

— при $k > \lfloor N/2 \rfloor$

$$(x^{0k}, y^{0k}) = (-x^{0N-k}, -y^{0N-k}).$$

Доказательство. По аналогии с доказательством теоремы 3 определение вектора A^{0k} для всех k, таких, что $\lfloor N/2 \rfloor < k < N$, сводится к определению вектора кратчайших путей вершины с номером $(N - k)$ и замене знаков полученных координат на противоположные.

Пусть $0 \leqslant k \leqslant N/2$. Требуется найти $x^{0k} = x$, $y^{0k} = y$ — такие координаты вершины с номером k, что

$$k = xd + y(d+1). \tag{7}$$

Для любых натуральных k и $d+1$ число k единственным образом представимо через целую часть и остаток от деления на $d+1$:

$$k = \lfloor k/(d+1) \rfloor (d+1) + k \bmod (d+1), \quad \lfloor k/(d+1) \rfloor \geqslant 0, \quad 0 \leqslant k \bmod (d+1) < d+1. \tag{8}$$

1. Для вершин с номерами $k = i(d+1)$ координаты равны

$$x = 0, \quad y = \lfloor k/(d+1) \rfloor.$$

2. Рассмотрим область ромба R_D, представляющего граф $C(N; d, d+1)$, ограниченную следующими условиями:

$$\begin{cases} x < 0, \\ -x \leqslant y \leqslant x + d. \end{cases}$$

В этой области

$$\begin{cases} x + y \geqslant 0, \\ 0 < -x < d. \end{cases}$$

Таким образом, если представить номер k вершины из этой области, записанный в виде (7) как $k = (x+y)(d+1) + (-x)$, то в силу единственности для k выражения (8) получим

$$\lfloor k/(d+1) \rfloor = x + y, \quad k \bmod (d+1) = -x.$$

Отсюда следует

$$x = -k \bmod (d+1), \quad y = \lfloor k/(d+1) \rfloor + k \bmod (d+1).$$

Подставляя найденные выражения для x и y в уравнения прямых, ограничивающих рассматриваемую область ромба, получим, что найденные формулы для x и y имеют место при выполнении условия

$$\lfloor k/(d+1) \rfloor < d + 1 - 2k \bmod (d+1).$$

Таким образом, вид формул для случая 2 имеет место и для случая 1 при выполнении условия $k \bmod (d+1) = 0$.

3. Рассмотрим теперь область ромба, ограниченную условиями

$$\begin{cases} 0 < x < d + 1, \\ x - d \leqslant y, \\ 1 - x \leqslant y \leqslant d + 1 - x. \end{cases}$$

В этой области

$$\begin{cases} x + y - 1 \geqslant 0, \\ 0 < d + 1 - x < d + 1. \end{cases}$$

Из представления номера k в виде $k = (x + y - 1)(d+1) + (d + 1 - x)$ получим

$$\lfloor k/(d+1) \rfloor = x + y - 1, \quad k \bmod (d+1) = d + 1 - x.$$

Отсюда следует

$$x = -k \bmod (d+1) + d + 1, \quad y = \lfloor k/(d+1) \rfloor + k \bmod (d+1) - d.$$

Аналогично случаю 2 получаем, что найденные формулы для x и y имеют место при выполнении условия $d + 1 - 2k \bmod (d+1) \leqslant \lfloor k/(d+1) \rfloor$.

Теорема доказана. ■

Результаты теоремы 4 позволяют скорректировать алгоритмы поиска кратчайших путей, представленные в [8, 11]. В обоих вариантах алгоритмов неправильно определены (возможно, это опечатки в текстах работ) значения координат y_0 и x_0 вектора

кратчайшего пути из нулевой вершины в вершину с номером m графа $C(N; b-1, b)$: $y_0 = -m \bmod b$, $x_0 = -\lfloor m/b \rfloor - y_0$ [8, с. 1121] и $y_0 = m \bmod b$, $x_0 = \lfloor m/b \rfloor - y_0$ [11, с. 46]. В наших обозначениях $x_0 = x^{0k}$, $y_0 = y^{0k}$, где k — номер вершины в графе $C(N; d, d+1)$.

Поменяем местами образующие графа $C(N; d, d+1)$, как показано на рис. 3. Тогда, применяя метод, используемый в доказательстве теоремы 4, получим значения

$$y_0 = -m \bmod b, \quad x_0 = \lfloor m/b \rfloor - y_0, \quad \text{где } b = d+1. \tag{9}$$

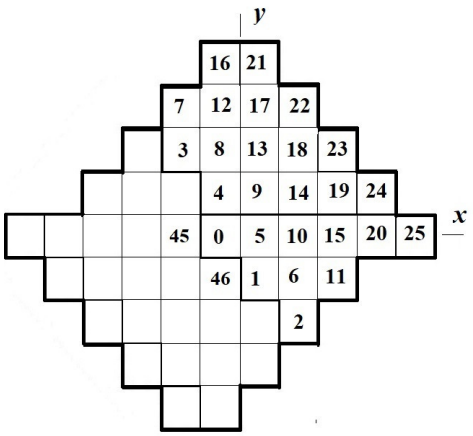


Рис. 3. Возможное представление графа $C(50; 4, 5)$

В качестве примера рассмотрим вычисление координат вектора кратчайшего пути из нулевой вершины в различные вершины графа $C(50; 4, 5)$ (рис. 3). Результат представлен в таблице. В первой колонке даны номера вершин, во второй и третьей колонках — значения координат, вычисленные по формулам из [8] и [11] соответственно, в четвёртой — правильные значения, найденные по формулам (9).

Номер вершины	Из [8]	Из [11]	Правильные значения
1	$x_0 = 1$, $y_0 = -1$	$x_0 = -1$, $y_0 = 1$	$x_0 = 1$, $y_0 = -1$
2	$x_0 = 2$, $y_0 = -2$	$x_0 = -2$, $y_0 = 2$	$x_0 = 2$, $y_0 = -2$
6	$x_0 = 0$, $y_0 = -1$	$x_0 = 0$, $y_0 = 1$	$x_0 = 2$, $y_0 = -1$
11	$x_0 = -1$, $y_0 = -1$	$x_0 = 1$, $y_0 = 1$	$x_0 = 3$, $y_0 = -1$
12	$x_0 = 0$, $y_0 = -2$	$x_0 = 0$, $y_0 = 2$	$x_0 = 0$, $y_0 = 3$

3. Алгоритм парных обменов в двумерных циркулянтах

Рассмотрим путевую процедуру, реализующую парные взаимодействия (парный обмен), в сети на кристалле с топологией в виде оптимальных двумерных циркулянтов, описываемых (1). Пусть требуется передать пакет из узла-источника s в узел-приёмник j. При условии, что вектор кратчайших путей A^{ij} (узла-приёмника j относительно узла i, исполняющего путевую процедуру) известен в каждом транзитном узле i, модификация вектора кратчайших путей для определения выходного направления, принадлежащего кратчайшему пути до узла приемника, сводится к выполнению операции

$$(x_p^{ij})' = x_p^{ij} - \operatorname{sgn}(x_p^{ij}) \cdot 1 \quad \text{для любого} \quad x_p^{ij} \neq 0,\ x_p^{ij} \in \{x^{ij}, y^{ij}\}. \tag{10}$$

При отсутствии отказов узлов и линий связи в узле-источнике по номеру узла-приёмника вычисляется вектор кратчайших путей между ними и записывается в заголовок пакета. В каждом транзитном узле по пути к приёмнику выбирается любое из направлений, принадлежащих кратчайшему пути, и вектор кратчайших путей модифицируется операцией (10) с целью уменьшения по абсолютной величине ненулевых координат вектора. Модифицированный вектор записывается в заголовок пакета, который передаётся дальше. Концом путевой процедуры служит равенство нулю всех координат вектора кратчайших путей.

В описанном ниже алгоритме 1 парных обменов: A^{ij} — вектор кратчайших путей узла-приёмника с номером j относительно узла i, исполняющего путевую процедуру; V — множество номеров выходных направлений, принадлежащих кратчайшему пути до узла-приёмника; запись $\mathrm{inp}_0 > 0$ означает, что на входной порт с номером 0 (т. е. из узла-источника) поступил пакет с признаком «парный обмен»; запись $\mathrm{inp}_h > 0$ означает, что на входной порт с номером h, $h = 1, \ldots, 4$, из соседнего узла поступил пакет с признаком «парный обмен»; запись «поставить пакет в выходной порт out_p» означает, что пакет ставится в выходной порт с номером p. В зависимости от выбранного способа вычисления вектора кратчайших путей A^{0k} по формулам (3) или (6) получаются две версии алгоритма: версия 1 и версия 2 соответственно.

Алгоритм 1. Алгоритм парных обменов

Вход: параметры N, d для версии 1 или N, $d+1$ для версии 2; j — номер узла-приёмника, i — номер узла, исполняющего путевую процедуру (в узле-источнике $i = s$).
Выход: модифицированный вектор кратчайших путей A^{ij}.

1: **Если** $\mathrm{inp}_0 > 0$, **то**
   $k := |s - j|$ и перейти в п. 5.
2: **Если** $\mathrm{inp}_h > 0$, **то**
3: **Если** $A^{ij} = 0$, **то**
      перейти в п. 9,
4: **иначе** перейти в п. 8.
5: **Если** $j \leqslant s$, **то**
   $\mathrm{sgn} := 1$ и перейти в п. 7,
6: **иначе** $\mathrm{sgn} := -1$.
7: **Если** $k > \lfloor N/2 \rfloor$, **то**
   $\mathrm{sgn} := -\mathrm{sgn}$ и $k := N - k$.
   Вычислить A^{0k} по формулам (3) или (6), $A^{ij} := \mathrm{sgn} \cdot A^{0k}$.
8: Выбрать любой номер $p \in V$, модифицировать A^{ij} операцией (10), записать A^{ij} в заголовок пакета, поставить пакет в выходной порт out_p.
9: Конец алгоритма.

Приведём оценки алгоритма 1. В сети на кристалле с числом узлов N требуется $\lceil \log_2 N \rceil + \lceil \log_2 \lceil \sqrt{N/2} \rceil \rceil$ битов для хранения в памяти значений двух параметров: N и образующей d для версии 1 или образующей $d + 1$ для версии 2. Пункты 1 и 5–8 алгоритма 1 выполняются в узле-источнике. В общей сложности для версии 1 независимо от числа узлов в сети требуется одна операция взятия по модулю, две операции деления, две операции умножения, 19 операций типа сложения и около 40 слов оперативной памяти. Для версии 2 алгоритма 1 требуется на пять операций типа сложения меньше. В транзитных узлах выполняются пункты 2–4 и 8, что требует одну операцию умножения, три операции типа вычитания и 10 слов оперативной памяти.

Приведённый алгоритм 1 поиска кратчайших путей в оптимальных двумерных циркулянтах не использует таблиц маршрутизации и задания матриц смежности, адаптируем к отказам узлов и линий связи и распределению нагрузки узлов, имеет константную оценку сложности, не зависящую от размера графа, в отличие от следующих алгоритмов: 1) Дейкстры с квадратичной сложностью $\mathrm{O}(N^2)$ для любого связного графа порядка N; 2) Б. Робича [18] с оценкой $\Theta(\sqrt{N})$ времени вычисления кратчайших путей для циркулянтов вида $C(N; s_1, s_2)$ и $l = \mathcal{O}(d)$ шагов маршрутизации, где l — расстояние между вершинами и d — диаметр сети; 3) Д. Гомеса с соавт. [19] с оценкой $\mathrm{O}(\log N)$ арифметических операций; 4) Б. Чена с соавт. [20] с константной оценкой сложности времени вычисления кратчайшего пути для циркулянтов вида $C(N; s_1, s_2)$, но требующего предварительного вычисления параметров для расчёта с временной сложностью $\mathrm{O}(2\log N)$; 5) К. Мартинеса с соавт. [14] в циркулянтах вида $C(N_d; d, d+1)$ с оценкой $\mathrm{O}(d)$.

4. Улучшение алгоритма поиска кратчайших путей для обобщённых графов Петерсена

Теоремы 3 и 4 можно использовать для улучшения алгоритма поиска кратчайших путей, разработанного в [21] для оптимальных обобщённых графов Петерсена. Обобщённые графы Петерсена как регулярные графы степени три позволяют увеличить надёжность сети по сравнению с используемыми в современных инфраструктурах кольцевыми сетями и деревьями и существенно лучше хордальных колец степени три по ряду показателей, включая диаметр и средний диаметр, в то же время они сохраняют низкую стоимость сети. Таким образом, обобщённые графы Петерсена степени три могут рассматриваться как перспективная топология для реализации в сетях на кристалле. Дадим необходимые определения.

Обобщённые графы Петерсена $P(N, a, b)$ порядка $n = 2N$ представляют собой графы, состоящие из внешнего (вершины V_0, связанные образующей $2a$) и внутреннего (вершины V_1, связанные образующей $2b$) колец с равным числом вершин N, связанных рёбрами. Рёбра, связывающие вершины $2i$ и $2i+1$, $i = 0, \ldots, N-1$, будем считать соответствующими образующей $c = 1$. Графы $P(N, a, b)$ с минимально возможным диаметром при заданном порядке называются оптимальными.

В работе [21] найдено отображение семейства оптимальных двумерных циркулянтов, описываемых (1), в класс обобщённых графов Петерсена, сохраняющее оптимальность графа, и получено параметрическое описание оптимальных обобщённых графов Петерсена для любого порядка графа $n = 2N$.

Теорема 5 [21]. Для каждого $N > 9$ существует оптимальный обобщённый граф Петерсена $P(N, a, a+1)$, где $a = \lceil\sqrt{(N-1)/2}\rceil - 1$.

Это позволило на основе алгоритма поиска кратчайших путей [17] для оптимальных циркулянтов, описываемых (1), найти аналитическое решение задачи поиска кратчайших путей для класса оптимальных обобщённых графов Петерсена.

Полученные в данной работе результаты дают возможность улучшить алгоритм из [21] для обобщённых графов Петерсена по требуемой памяти и быстродействию, так как основную долю вычислений в нём составляет определение вектора кратчайшего пути из 0 в любую вершину циркулянтного графа $C(N; d, d+1)$. При использовании формул (3) для расчёта кратчайших путей в оптимальных двумерных циркулянтах требуется меньшее число операций и памяти за счёт отсутствия необходимости вычисления параметра $i^*(N)$ [21, с. 52] (где параметр k^* соответствует $i^*(N)$). При ис-

пользовании формул (6) для расчёта кратчайших путей в оптимальных двумерных циркулянтах требуется меньшее число проверок условий, чем у формул (3).

Таким образом, в данной работе для семейств оптимальных двумерных циркулянтных сетей и оптимальных обобщённых графов Петерсена, задаваемых аналитически двумя параметрами и достигающих минимумов диаметра сети, предложены эффективные динамические алгоритмы парной маршрутизации, обладающие оптимальными свойствами с точки зрения построения сетей на кристалле.

ЛИТЕРАТУРА

1. *Монахова Э. А.* Структурные и коммуникативные свойства циркулянтных сетей // Прикладная дискретная математика. 2011. № 3. С. 92–115.
2. *Monakhova E. A.* A survey on undirected circulant graphs // Discrete Math., Algorithms Appl. 2012. No. 4. `https://www.researchgate.net/publication/267143246_A_survey_on_undirected_circulant_graphs`.
3. *Perez-Roses H.* Algebraic and computer-based methods in the undirected degree/diameter problem — A brief survey // Electr. J. Graph Theory Appl. 2014. No. 2(2). P. 166–190.
4. *Romanov A., Amerikanov A., and Lezhnev E.* Analysis of approaches for synthesis of networks-on-chip by using circulant topologies // J. Physics: Conf. Ser. 2018. V. 1050. P. 1–12.
5. *Romanov A. Yu.* Development of routing algorithms in networks-on-chip based on ring circulant topologies // Heliyon. 2019. V. 5. Iss. 4. `https://www.sciencedirect.com/science/article/pii/S2405844018355208`
6. *Щеголева М. А., Романов А. Ю.* Разработка алгоритма маршрутизации в сетях на кристалле с топологией мультипликативный циркулянт // МЭС-2018. Россия, Москва, октябрь 2018. С. 119–124.
7. *Монахова Э. А.* Об аналитическом описании оптимальных двумерных диофантовых структур однородных вычислительных систем // Вычислительные системы. 1981. № 90. С. 81–91.
8. *Beivide R., Herrada E., Balcazar J. L., and Arruabarrena A.* Optimal distance networks of low degree for parallel computers // IEEE Trans. Computers. 1991. V. 40. No. 10. P. 1109–1124.
9. *Liestman A. L., Opatrny J., and Zaragoza M.* Network properties of double and triple fixed-step graphs // Int. J. Found. Comp. Sci. 1998. V. 9. P. 57–76.
10. *Puente V., Gregorio J.-A., Prellezo J. M., et al.* Adaptive bubble router: a design to balance latency and throughput in networks for parallel computers // Proc. ICCP'99. Toulouse, France, August/September 1999. P. 58–67.
11. *Puente V., Izu C., Gregorio J.-A., et al.* Improving parallel system performance by changing the arrangement of the network links // Proc. ISC'00. Santa Fe, New Mexico, USA, May 8–11, 2000. P. 44–53.
12. *Yang Y., Funashashi A., Jouraku A., et al.* Recursive diagonal torus: An interconnection network for massively parallel computers // IEEE Trans. Parallel and Distributed Systems. 2001. V. 12. No. 7. P. 701–715.
13. *Мартинес К., Стаффорд Э., Байвиде Р., Габидулин Э. М.* Представление гексагональных созвездий с помощью графов Эйзенштейна — Якоби // Проблемы передачи информации. 2008. Т. 44. № 1. С. 3–13.
14. *Martinez C., Beivide R., Stafford E., et al.* Modeling toroidal networks with the Gaussian integers // IEEE Trans. Comput. 2008. V. 57. No. 8. P. 1046–1056.
15. *Beivide R., Martinez C., Izu C., et al.* Chordal topologies for interconnection networks // LNCS. 2003. V. 2858. P. 385–392.
16. *Cai J.-Y. et al.* On routing in circulant graphs // LNCS. 1999. V. 1627. P. 360–369.

17. *Монахова Э. А.* Алгоритмы межмашинных взаимодействий и реконфигурации графов связей в вычислительных системах с программируемой структурой // Вычислительные системы. 1982. № 94. С. 81–102.
18. *Robič B.* Optimal routing in 2-jump circulant networks. Technical Report 397, University of Cambridge, U.K., Computer Laboratory, 1996.
19. *Gomez D., Gutierrez J., Ibeas A., and Beivide R.* Optimal routing in double loop networks // Theor. Computer Sci. 2007. V. 381. Iss. 1–3. P. 68–85.
20. *Chen B.-X., Meng J.-X., and Xiao W.-J.* A constant time optimal routing algorithm for undirected double-loop networks // Proc. MSN 2005, Wuhan, China, December 2005. P. 309–316.
21. *Монахова Э. А.* Оптимальные обобщенные графы Петерсена // Дискретный анализ и исследование операций. 2009. Т. 16. № 4. С. 47–60.

REFERENCES

1. *Monakhova E. A.* Strukturnye i kommunikativnye svoystva tsirkulyantnykh setey [Structural and communicative properties of circulant networks]. Prikladnaya Diskretnaya Matematika, 2011, no. 3, pp. 92–115. (in Russian)
2. *Monakhova E. A.* A survey on undirected circulant graphs. Discrete Math., Algorithms Appl., 2012, no. 4. `https://www.researchgate.net/publication/267143246_A_survey_on_undirected_circulant_graphs`.
3. *Perez-Roses H.* Algebraic and computer-based methods in the undirected degree/diameter problem — A brief survey. Electr. J. Graph Theory Appl., 2014, no. 2(2), pp. 166–190.
4. *Romanov A., Amerikanov A., and Lezhnev E.* Analysis of approaches for synthesis of networks-on-chip by using circulant topologies. J. Physics: Conf. Ser., 2018, vol. 1050, pp. 1–12.
5. *Romanov A. Yu.* Development of routing algorithms in networks-on-chip based on ring circulant topologies. Heliyon, 2019, vol. 5, iss. 4. `https://www.sciencedirect.com/science/article/pii/S2405844018355208`
6. *Shchegoleva M. A. and Romanov A. Yu.* Razrabotka algoritma marshrutizatsii v setyakh na kristalle s topologiey mul'tiplikativnyy tsirkulyant [Development of routing algorithm in networks-on-chip with a multiplicative circulant topology]. Proc. MES-2018, Russia, Moscow, October 2018, pp. 119–124. (in Russian)
7. *Monakhova E. A.* Ob analiticheskom opisanii optimal'nykh dvumernykh diofantovykh struktur odnorodnykh vychislitel'nykh sistem [On analytical representation of optimal two-dimensional Diophantine structures of homogeneous computer systems]. Vychislitel'nye Sistemy, 1981, no. 90, pp. 81–91. (in Russian)
8. *Beivide R., Herrada E., Balcazar J. L., and Arruabarrena A.* Optimal distance networks of low degree for parallel computers. IEEE Trans. Computers, 1991, vol. 40, no. 10, pp. 1109–1124.
9. *Liestman A. L., Opatrny J., and Zaragoza M.* Network properties of double and triple fixed-step graphs. Int. J. Found. Comp. Sci., 1998, vol. 9, pp. 57–76.
10. *Puente V., Gregorio J.-A., Prellezo J. M., et al.* Adaptive bubble router: a design to balance latency and throughput in networks for parallel computers. Proc. ICCP'99, Toulouse, France, August/September 1999, pp. 58–67.
11. *Puente V., Izu C., Gregorio J.-A., et al.* Improving parallel system performance by changing the arrangement of the network links. Proc. ISC'00, Santa Fe, New Mexico, USA, May 8–11, 2000, pp. 44–53.
12. *Yang Y., Funashashi A., Jouraku A., et al.* Recursive diagonal torus: An interconnection network for massively parallel computers. IEEE Trans. Parallel and Distributed Systems, 2001, vol. 12, no. 7, pp. 701–715.

13. *Martines K., Stafford E., Bayvide R., and Gabidulin E. M.* Predstavlenie geksagonal'nykh sozvezdiy s pomoshch'yu grafov Eyzenshteyna — Yakobi [Modeling hexagonal constellations with Eisenstein — Jacobi graphs]. Problemy Peredachi Informatsii, 2008, vol. 44, no 1, pp. 3–13. (in Russian)
14. *Martinez C., Beivide R., Stafford E., et al.* Modeling toroidal networks with the Gaussian integers. IEEE Trans. Comput., 2008, vol. 57, no. 8, pp. 1046–1056.
15. *Beivide R., Martinez C., Izu C., et al.* Chordal topologies for interconnection networks. LNCS, 2003, vol. 2858, pp. 385–392.
16. *Cai J.-Y. et al.* On routing in circulant graphs. LNCS, 1999, vol. 1627, pp. 360–369.
17. *Monakhova E. A.* Algoritmy mezhmashinnykh vzaimodeystviy i rekonfiguratsii grafov svyazey v vychislitel'nykh sistemakh s programmiruemoy strukturoy [Algorithms of interprocessor exchanges and reconfiguration of interconnection networks in computer systems with programmable structure]. Vychislitel'nye Sistemy, 1982, no. 94, pp. 81–102. (in Russian)
18. *Robič B.* Optimal routing in 2-jump circulant networks. Technical Report 397, University of Cambridge, U.K., Computer Laboratory, 1996.
19. *Gomez D., Gutierrez J., Ibeas A., and Beivide R.* Optimal routing in double loop networks. Theor. Computer Sci., 2007, vol. 381, iss. 1–3, pp. 68–85.
20. *Chen B.-X., Meng J.-X., and Xiao W.-J.* A constant time optimal routing algorithm for undirected double-loop networks. Proc. MSN 2005, Wuhan, China, December 2005, pp. 309–316.
21. *Monakhova E. A.* Optimal'nye obobshchennye grafy Petersena [Optimal generalized Petersen graphs]. Diskretnyy Analiz i Issledovanie Operatsiy, 2009, vol. 16, no. 4, pp. 47–60. (in Russian)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52

О ГЕНЕРИЧЕСКОЙ NP-ПОЛНОТЕ ПРОБЛЕМЫ ВЫПОЛНИМОСТИ БУЛЕВЫХ СХЕМ[1]

А. Н. Рыбалов

Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

Генерический подход к алгоритмическим проблемам предложен Каповичем, Мясниковым, Шуппом и Шпильрайном в 2003 г. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. В 2017 г. А. Н. Рыбалов ввёл понятие полиномиальной генерической сводимости алгоритмических проблем, которое сохраняет свойство разрешимости проблемы для почти всех входов и обладает свойством транзитивности, и доказал, что классическая проблема выполнимости булевых формул является полной относительно этой сводимости в генерическом аналоге класса NP. При этом булевы формулы представлялись в виде двоичных размеченных деревьев. В данной работе доказывается генерическая NP-полнота проблемы выполнимости для булевых схем.

Ключевые слова: *булева схема, генерическая сложность, проблема выполнимости, NP-полнота.*

DOI 10.17223/20710410/47/8

ON GENERIC NP-COMPLETENESS OF THE PROBLEM OF BOOLEAN CIRCUITS SATISFIABILITY

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

E-mail: alexander.rybalov@gmail.com

Generic-case approach to algorithmic problems was suggested by Miasnikov, Kapovich, Schupp and Shpilrain in 2003. This approach studies behavior of an algorithm on typical (almost all) inputs and ignores the rest of inputs. In 2017 A. Rybalov introduced a concept of polynomial generic reducibility of algorithmic problem that preserves the decidability property problems for almost all inputs and has the property of transitivity, and proved that the classical problem of the satisfiability of Boolean formulas is complete with respect to this reducibility in the generic analogue of class NP. Then the Boolean formulas were represented by binary labeled trees. In this paper, we prove the generic NP-completeness of the satisfiability problem for the so-called Boolean circuits. Boolean circuit is a way to represent Boolean functions, which show how the

[1]Работа поддержана грантом РНФ № 18-71-10028.

value of a Boolean function is obtained from values of variables using logical connectives. Boolean circuits are convenient models for the development of microprocessors, and are also the most important object of studying in computational complexity theory. Boolean circuit contains a finite number of variables $x_1, \ldots, x_n$. Every variable x_i can be either input, or defined through other variables by assigning one of the following types: $x_i = x_j \vee x_k$ or $x_j \wedge x_k$, where $j, k < i$; $x_i = \neg x_j$ or x_j, where $j < i$. The last variable x_n of the circuit is called output. By the size of a Boolean circuit we mean the number of variables in it. The number of Boolean circuits of size n is $\prod_{m=1}^{n} (1 + 2(m-1)^2 + 2(m-1))$.

Keywords: *Boolean circuit, generic complexity, Boolean satisfiability problem, NP-completeness.*

Введение

Генерический подход к алгоритмическим проблемам предложен в [1]. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют так называемое генерическое множество. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения практики алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов. Классическим примером такого алгоритма является симплекс-метод — он за полиномиальное время решает задачу линейного программирования для большинства входных данных, но имеет экспоненциальную сложность в худшем случае. Более того, может так оказаться, что проблема трудноразрешима или вообще неразрешима в классическом смысле, но легкоразрешима на генерическом множестве.

Важнейшим понятием классической теории сложности вычислений является понятие полиномиальной сводимости алгоритмических проблем. С его помощью можно сравнивать проблемы по вычислительной сложности и развивать богатую теорию NP-полноты [2]. Л. Левин ввёл понятие полиномиальной сводимости и NP-полноты в среднем [3]. Ю. Гуревич привёл примеры алгоритмических проблем, которые являются NP-полными в среднем [4]. При анализе вычислительной сложности проблемы в среднем изучается математическое ожидание времени работы алгоритма для всех входов данного размера. А. Н. Рыбалов ввёл понятие полиномиальной генерической сводимости алгоритмических проблем, которое сохраняет свойство разрешимости проблемы для почти всех входов и обладает свойством транзитивности, и доказал, что классическая проблема выполнимости булевых формул является полной относительно этой сводимости в генерическом аналоге класса NP [5]. При этом булевы формулы представлялись в виде двоичных размеченных деревьев. Отметим, что А. Мясников и А. Ушаков в [6] дали другое определение генерической полиномиальной сводимости и в рамках этого определения доказали генерическую NP-полноту рандомизированной ограниченной версии проблемы остановки для машин Тьюринга.

В данной работе доказывается генерическая NP-полнота проблемы выполнимости для так называемых булевых схем. Булева схема — это способ представления булевых функций, в котором указывается, как значение булевой функции получается из значений переменных с помощью логических связок. Булевы схемы являются удобными моделями для разработки микропроцессоров, а также важнейшим объектом изучения в теории сложности вычислений [7].

1. Генерические алгоритмы

Пусть I — некоторое множество. Функция $\mathrm{size} : I \to \mathbb{N}$ называется *функцией размера*, если для любого $n \in \mathbb{N}$ множество $I_n = \{x \in I : \mathrm{size}(x) = n\}$ конечно. Например, если $I = \Sigma^*$ — множество слов над конечным алфавитом Σ, то функцией размера будет функция, определённая для любого слова w как его длина $|w|$. Для множества натуральных чисел $\mathbb{N}$ функция размера сопоставляет любому натуральному числу длину его двоичной записи. Как обычно делается в теории вычислимости, будем под алгоритмическими проблемами понимать проблемы распознавания подмножеств из некоторого множества входов с определённой на нем функцией длины. Для подмножества $S \subseteq I$ определим последовательность

$$\rho_n(S) = \frac{|S_n|}{|I_n|},\ n = 1, 2, 3, \ldots,$$

где $S_n = S \cap I_n$ — множество входов из S размера n. Заметим, что $\rho_n(S)$ — это вероятность попасть в S при случайной и равновероятной генерации входов из I_n. *Асимптотической плотностью* S назовём предел

$$\rho(S) = \overline{\lim_{n\to\infty}} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$, и *пренебрежимым*, если $\rho(S) = 0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо.

Следуя [1], назовём множество S *строго пренебрежимым*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к нулю, т. е. существуют константы σ, $0 < \sigma < 1$, и $C > 0$, такие, что для любого n

$$\rho_n(S) < C\sigma^n.$$

Теперь S называется *строго генерическим*, если его дополнение $I \setminus S$ строго пренебрежимо.

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{?\}$ ($? \notin J$) называется (*строго*) *генерическим*, если

1) $\mathcal{A}$ останавливается на всех входах из I;
2) множество $\{x \in I : \mathcal{A}(x) \neq ?\}$ является (строго) генерическим.

Аналогично определяется понятие вероятностного генерического алгоритма. Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если $(\mathcal{A}(x) = y \in J) \Rightarrow (f(x) = y)$ для всех $x \in I$. Ситуация $\mathcal{A}(x) = ?$ означает, что $\mathcal{A}$ не может вычислить функцию f на аргументе x. Но условие 2 гарантирует, что $\mathcal{A}$ корректно вычисляет f на почти всех входах (входах из генерического множества). Множество $S \subseteq I$ называется (*строго*) *генерически разрешимым за полиномиальное время*, если существует (строго) генерический полиномиальный алгоритм, вычисляющий его характеристическую функцию.

2. Генерическая полиномиальная сводимость

Напомним определения генерической полиномиальной сводимости и генерической NP-полноты из [5].

Пусть I, J — некоторые множества входов с определёнными на них функциями размера. Множество $A \subseteq I$ *генерически полиномиально сводится* к множеству $B \subseteq J$ (обозначается $A \leqslant_{\mathrm{GenP}} B$), если существуют вероятностный полиномиальный алгоритм $\mathcal{R} : I \times \mathbb{N} \to P(J) \cup \{?, \perp\}$ ($P(J)$ — это множество всех подмножеств J), полином $p(n)$, полином $q(n)$ степени больше 2 и константа $C > 0$, такие, что

1. Для всех $x \in I$ либо $(\forall n\,(\mathcal{R}(x,n) = ?))$, либо для всех $n \geqslant q(k)$, где $k = \mathrm{size}(x)$, выполнены следующие свойства:
   а) $\forall y \in \mathcal{R}(x,n)\ (y \neq \perp \ \Rightarrow\ \mathrm{size}(y) = n)$;
   б) все элементы в $\mathcal{R}(x,n) \setminus \{\perp\}$ выдаются алгоритмом $\mathcal{R}$ равновероятно;
   в) вероятность получить ответ $\perp$ в $\mathcal{R}(x,n)$ не больше 2^{-Ck};
   г) $\dfrac{|\mathcal{R}(x,n)|}{|J_n|} > \dfrac{1}{(p(n))^k}$;
   д) $x \in A \Rightarrow \mathcal{R}(x,n) \subseteq B$;
   е) $x \notin A \Rightarrow \mathcal{R}(x,n) \subseteq J \setminus B$.
2. Множество $\{x \in I : \forall n\ (\mathcal{R}(x,n) = ?)\}$ строго пренебрежимо.

В [5] доказано, что определённая таким образом сводимость сохраняет свойство «быть строго генерически разрешимым за полиномиальное время» для алгоритмических проблем, а также обладает свойством транзитивности.

Определим генерический аналог класса NP. Множество $S \subseteq I$ принадлежит классу $\mathrm{sg\,NP}$, если существует полиномиальное строго генерическое множество $G \subseteq I$, такое, что $S \cap G \in \mathrm{NP}$. Множество $S \in \mathrm{sg\,NP}$ называется *генерически NP-полным*, если для любого $A \in \mathrm{sg\,NP}$ имеет место $A \leqslant_{\mathrm{GenP}} S$.

3. Булевы схемы

Булева схема содержит конечное число переменных $x_1, \ldots, x_n$. Переменная x_i может быть либо *входной*, либо определяться через другие переменные с помощью присваивания одного из следующих типов:

1) $x_i = x_j \vee x_k$, где $j, k < i$;
2) $x_i = x_j \wedge x_k$, где $j, k < i$;
3) $x_i = \neg x_j$, где $j < i$;
4) $x_i = x_j$, где $j < i$.

Заметим, что первая переменная любой булевой схемы обязана быть входной. Последняя переменная x_n схемы называется *выходной*. Естественным образом любая булева схема C задаёт булеву функцию от входных переменных схемы следующим образом. Входным переменным схемы можно присвоить любые булевы значения. Затем значения всех остальных переменных схемы вычисляются в порядке возрастания их индексов через значения входных и предыдущих переменных схемы согласно соответствующим присваиваниям. Значение выходной переменной и будет значением соответствующей функции. С другой стороны, для любой булевой схемы можно легко построить булеву схему (и не одну), задающую эту функцию. Под *размером булевой схемы* будем понимать число переменных в ней. Обозначим через $\mathcal{BC}$ множество всех булевых схем.

Лемма 1. Число булевых схем размера n равно

$$|\mathcal{BC}_n| = \prod_{m=1}^{n} \big(1 + 2(m-1)^2 + 2(m-1)\big).$$

Доказательство. Для переменной x_m имеются следующие варианты:

1) переменная x_m является входной — один вариант;
2) $x_m = x_j \vee x_k$, где $j, k < m$, — $(m-1)^2$ вариантов;
3) $x_m = x_j \wedge x_k$, где $j, k < m$, — $(m-1)^2$ вариантов;
4) $x_m = \neg x_j$, где $j < m$, — $(m-1)$ вариантов;
5) $x_m = x_j$, где $j < m$, — $(m-1)$ вариант.

Итого получается $\big(1+2(m-1)^2+2(m-1)\big)$ вариантов выбора для переменной x_m; для всех n переменных булевой схемы получаем $\prod\limits_{m=1}^{n}\big(1+2(m-1)^2+2(m-1)\big)$ вариантов выбора. ■

Выясним порядок роста функции $|\mathcal{BC}_n|$. Оценим каждый множитель в произведении $|\mathcal{BC}_n|$ снизу:

$$2m(m-1)=2(m-1)^2+2(m-1)<1+2(m-1)^2+2(m-1).$$

Отсюда $2^n n!(n-1)!<|\mathcal{BC}_n|$. Оценим каждый множитель в произведении $|\mathcal{BC}_n|$ сверху:

$$1+2(m-1)^2+2(m-1)=2m(m-1)+1<2m(m-1)+2m=2m^2.$$

Отсюда $|\mathcal{BC}_n|<2^n(n!)^2$. Итого получаем

$$\frac{2^n(n!)^2}{n}<|\mathcal{BC}_n|<2^n(n!)^2.$$

Для любой булевой схемы $C(x_1,\ldots,x_n)$ определим множество $Eq(C)$ всевозможных булевых схем от переменных $x_1,\ldots,x_n,x_{n+1},\ldots,x_{n+m}$, в которых переменные $x_1,\ldots,x_n$ определяются так же, как в схеме C, переменные $x_{n+1},\ldots,x_{n+m-1}$ определяются произвольным образом, а выходная переменная x_{n+m} определяется так: $x_{n+m}=x_n$. Очевидно, что любая схема из $Eq(C)$ вычисляет ту же булеву функцию, что и схема C.

Лемма 2. Для любой булевой схемы C имеет место

$$\frac{|Eq(C)\cap\mathcal{BC}_n|}{|\mathcal{BC}_n|}>\frac{1}{5n^{2k}}$$

для любого $n>k$, где k — размер схемы C.

Доказательство. Пусть булева схема C имеет размер k и $n>k$. В любой булевой схеме из множества $Eq(C)\cap\mathcal{BC}_n$ присваивания для первых k переменных и для последней переменной фиксированы. Переменные $x_{n+1},\ldots,x_{n+m-1}$ определяются произвольным образом. Поэтому, аналогично тому, как это делалось в доказательстве леммы 1, можно подсчитать

$$|Eq(C)\cap\mathcal{BC}_n|=\prod_{m=k+1}^{n-1}\big(1+2(m-1)^2+2(m-1)\big).$$

Отсюда

$$\frac{|Eq(C)\cap\mathcal{BC}_n|}{|\mathcal{BC}_n|}=\frac{\prod\limits_{m=k+1}^{n-1}\big(1+2(m-1)^2+2(m-1)\big)}{\prod\limits_{m=1}^{n}\big(1+2(m-1)^2+2(m-1)\big)}=\frac{1}{\prod\limits_{m=1}^{k}\big(1+2(m-1)^2+2(m-1)\big)}.$$

Так как $\dfrac{1}{\big(1+2(m-1)^2+2(m-1)\big)}>\dfrac{1}{5n^2}$ для любого $m<n$, то имеем

$$\frac{|Eq(C)\cap\mathcal{BC}_n|}{|\mathcal{BC}_n|}>\frac{1}{5n^{2k}}.$$

Лемма доказана. ■

4. Основной результат

Под *проблемой выполнимости булевых схем* будем понимать следующую алгоритмическую проблему. Для любой булевой схемы нужно определить, существуют ли булевы значения её входных переменных, при которых значение выходной переменной равно 1. Известно [7], что существует полиномиальный алгоритм, который по любой булевой формуле строит булеву схему, которая вычисляет ту же функцию. Поэтому проблема выполнимости булевых схем является NP-полной в классическом смысле. Следующее утверждение показывает, что она является генерически NP-полной.

Теорема 1. Проблема выполнимости булевых схем генерически NP-полна.

Доказательство. Пусть $A \in \operatorname{sg}\mathrm{NP}$. Тогда существует полиномиальное строго генерическое множество G, такое, что $A \cap G \in \mathrm{NP}$. Так как проблема выполнимости булевых схем NP-полна, существует классическая полиномиальная сводимость f множества $A \cap G$ к ней. Полиномиальный вероятностный алгоритм $\mathcal{R}$, генерически сводящий проблему A к проблеме выполнимости булевых схем, работает на входе (x, n) следующим образом:

1) проверяет, принадлежит ли x множеству G;
2) если $x \notin G$, выдаёт ?;
3) если $x \in G$, то строит булеву схему $C = f(x)$, такую, что C выполнима тогда и только тогда, когда $x \in A$;
4) случайно и равновероятно генерирует булеву схему из множества $Eq(C) \cap \mathcal{BC}_n$.

Проверим свойства полиномиальной сводимости. Свойство 2 следует из того, что множество G строго генерическое. Свойства 1а и 1б следуют из описания шага 4. Свойство 1в очевидно выполняется: алгоритм вообще не выдаёт ответ $\perp$. Свойства 1д и 1е также выполняются по построению схемы C. Наконец, свойство 1г следует из леммы 2. ■

Автор выражает благодарность рецензенту за полезные замечания и предложения по улучшению текста статьи.

ЛИТЕРАТУРА

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
2. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 419 с.
3. *Levin L.* Average case complete problems // SIAM J. Computing. 1987. V. 15. P. 285–286.
4. *Gurevich Y.* Average case completeness // J. Computer System Sciences. 1991. V. 42. P. 346–398.
5. *Рыбалов А.* О генерической NP-полноте проблемы выполнимости булевых формул // Прикладная дискретная математика. 2017. № 36. С. 106–112.
6. *Miasnikov A. and Ushakov A.* Generic case completeness // J. Computer System Sciences. 2016. V. 82. No. 8. P. 1268–1282.
7. *Сэвидж Д.* Сложность вычислений. М.: Факториал, 1998. 368 с.

REFERENCES

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
2. *Garey M. and Johnson D.* Computers and Intractability. N. Y., Freeman & Co, 1979. 340 p.
3. *Levin L.* Average case complete problems. SIAM J. Computing, 1987, vol. 15, pp. 285–286.

4. *Gurevich Y.* Average case completeness. J. Computer System Sciences, 1991, vol. 42, pp. 346–398.
5. *Rybalov A.* O genericheskoy NP-polnote problemy vypolnimosti bulevyh formul [On generic NP-completeness of the Boolean satisfiability problem]. Prikladnaya Diskretnaya Matematika, 2017, no. 36, pp. 106–112. (in Russian)
6. *Miasnikov A. and Ushakov A.* Generic case completeness. J. Computer System Sciences, 2016, vol. 82, no. 8, pp. 1268–1282.
7. *Savage J.* The Complexity of Computing. John Wiley and Sons Inc., 1977. 391 p.

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

UDC 519.7 DOI 10.17223/20710410/47/9

A METHOD FOR BI-DECOMPOSITION OF PARTIAL BOOLEAN FUNCTIONS

Yu. V. Pottosin

United Institute of Informatics Problems National Academy of Sciences of Belarus, Minsk, Belarus

E-mail: pott@newman.bas-net.by

A method for bi-decomposition of incompletely specified (partial) Boolean functions is suggested. The problem of bi-decomposition is reduced to the problem of two-block weighted covering a set of edges of a graph of rows orthogonality of a ternary or binary matrix that specify a given function, by complete bipartite subgraphs (bicliques). Each biclique is assigned in a certain way with a set of arguments of the given function, and the weight of a biclique is the cardinality of this set. According to each of bicliques, a Boolean function is constructed whose arguments are the variables from the set, which is assigned to the biclique. The obtained functions form a solution of the bi-decomposition problem.

Keywords: *partial Boolean function, bi-decomposition, cover problem, complete bipartite subgraph.*

Introduction

The problem of decomposition of a Boolean function consists in searching a representation of a given Boolean function in a form of superposition of two of more functions that are simpler in a certain sense than the given one. The decomposition problem is one of important and complicated problems in logical design. Its successful solution influences directly on the quality and cost of digital devices being designed. In a number of cases, a solution of this problem of decomposition gives a possibility to replace a complicated hardware implementation of a Boolean function in a large number of arguments by a simpler problem of implementation of several functions of less complexity.

There exist rather many various kinds of a Boolean function decomposition [1]. One of them is bi-decomposition. The bi-decomposition problem is set as follows. Given a Boolean function $y = f(\mathbf{x})$ where the components of vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ are Boolean variables forming a set X, find a superposition $f(\mathbf{x}) = \varphi(g_1(\mathbf{z}_1), g_2(\mathbf{z}_2))$ where the components of vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ are Boolean variables from sets $Z_1 \subset X$ and $Z_2 \subset X$, respectively, the type of the function φ of two variables is given, as well. It can be any of ten Boolean functions with two essential arguments represented by logic algebra operations. As usual, the sets Z_1 and Z_2 are given and $Z_1 \cap Z_2 = \varnothing$. Such a bi-decomposition is called disjoint in contrast to non-disjoint bi-decomposition where the condition $Z_1 \cap Z_2 = \varnothing$ is not obligatory, but restrictions can be put on the cardinalities of the sets Z_1 and Z_2.

There are known examples of applying methods for bi-decomposition in increasing performance of circuits [2, 3] and in the synthesis of circuits based on FPGA [4]. The problem of bi-decomposition using XOR operation with a given partition $\{Z_1, Z_2\}$ of X is considered in [5] where logical equations are suggested to be used for solving the problem. The probability of existence of any kind of decomposition for a completely specified Boolean function is very low, while the situation differs in the case of incompletely specified (partial) functions, especially when they are defined at a small part of Boolean space. Such a case of disjoint bi-decomposition at a given partition $\{Z_1, Z_2\}$ of X was investigated in detail in [6].

Below, the problem of bi-decomposition of a partial Boolean function is considered. In this case, a superposition $\varphi(g_1(\mathbf{z}_1), g_2(\mathbf{z}_2)) \geqslant f(\mathbf{x})$ for a given partial Boolean function $y = f(\mathbf{x})$ must be found where $\geqslant$ denotes the relation of realization, i.e. the values of the function φ coincide with the values of the function f anywhere they are defined. As well as in the problem set above, the components of the vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ are the variables from $Z_1 \subset X$ and $Z_2 \subset X$, respectively. The sets Z_1 and Z_2 are not given. They can intersect, but it is naturally that the sum of their cardinalities should be minimal. There exist various methods for disjoint and non-disjoint bi-decompositions [7 – 10]. Here we describe a method for bi-decomposition that uses the approach to solving the problem of parallel decomposition of partial Boolean functions suggested in [11].

1. The applied approach

The Boolean function is supposed to be given in a matrix form, i.e. by a pair of matrices $\mathbf{X}$ and $\mathbf{Y}$ where $\mathbf{X}$ is a Boolean or ternary matrix representing a part of Boolean space of arguments that is the definition domain of the given function f and $\mathbf{Y}$ is a one-column Boolean matrix that shows the values of the function f on elements or intervals of the Boolean space represented by $\mathbf{X}$. The rows of $\mathbf{X}$ and one-element rows of $\mathbf{Y}$ have a natural common numeration.

Let us consider graphs $G_X = (V, E_X)$ and $G_Y = (V, E_Y)$ where V is the set of common numbers of rows in matrices $\mathbf{X}$ and $\mathbf{Y}$. The edges from the set E_X correspond to the pairs of orthogonal rows in $\mathbf{X}$. Two rows of a ternary matrix are orthogonal if there is a column where 0 is in one of them and 1 in the other [12]. The edges from the set E_Y correspond to the pairs of elements in Y with different values. Evidently, G_Y is a complete bipartite graph where one part corresponds to the set of 0s in $\mathbf{Y}$, and the other to the set of 1s. The function is given correctly by matrices $\mathbf{X}$ and $\mathbf{Y}$ if $E_Y \subseteq E_X$, i.e. G_Y is a spanning subgraph of G_X. Any pair of matrices $(\mathbf{X}, \mathbf{Y})$ of the described form can be considered as a representation of a partial Boolean function if the graph G_Y is a spanning subgraph of the graph G_X.

Let every edge in G_X be assigned with the set of variables from the set $X = \{x_1, x_2, \ldots, x_n\}$, by which the corresponding pair of rows in $\mathbf{X}$ is orthogonal. Let a complete bipartite subgraph, or *biclique*, of G_X be assigned with a set of variables from X taken one by one from each edge belonging to that biclique.

The set of variables assigned to a biclique is formed as follows. Let $\{x_i, x_j, \ldots, x_k\}$ be the set of variables, by which two rows of $\mathbf{X}$ correspond to an edge of G_X. Form elementary disjunction $x_i \vee x_j \vee \ldots \vee x_k$ from those variables. For a biclique, construct conjunctive normal form (CNF) with terms which are those elementary disjunctions taken from all edges belonging to the biclique. After deleting possible absorbed disjunctions, transform the CNF into disjunctive normal form (DNF) by opening the brackets. The variables from the term of minimal rank in the obtained DNF constitute the set assigned to the biclique.

A biclique is called admissible if it contains at least one edge from E_Y and the number of variables assigned to it is less than the number n of arguments of the given function f.

If the type of the function φ is not given, then the problem of bi-decomposition can be considered as a particular case of the parallel decomposition problem for a system of partial Boolean functions considered in [11]. In our case, only one function is decomposed, and the number of sub-functions is limited to two. The following Proposition is a base of the method.

Proposition 2. For a partial Boolean function $f(\mathbf{x})$ given by matrices $\mathbf{X}$ and $\mathbf{Y}$, there exists a realizing it superposition $\varphi(g_1(\mathbf{z}_1), g_2(\mathbf{z}_2))$ if there is a two-block cover of the set E_Y by admissible bicliques of the graph G_X.

Let bicliques B_1 and B_2 constitute that cover. Every biclique B_i, $i = 1, 2$, can be given by a pair of vertex sets $\langle V_i', V_i'' \rangle$ such that each vertex from V_i' is connected with all the vertices of V_i'' by edges. Any function $g_i(\mathbf{z}_i)$ is given by matrices $\mathbf{X}_i$ and $\mathbf{Y}_i$. The matrix $\mathbf{X}_i$ is the minor of $\mathbf{X}$ formed by the columns corresponding to variables assigned to the biclique B_i. The matrix $\mathbf{Y}_i$ has only one column with 0s in rows corresponding to vertices in V_i', and with 1s in rows corresponding to vertices in V_i'' (or vice versa). An element of this column has value "$-$" if its corresponding vertex is absent in both V_i' and V_i''. The function φ is given by matrices $\mathbf{U}$ and $\mathbf{\Phi}$. The matrix $\mathbf{U}$ consists of the columns representing $\mathbf{Y}_1$ and $\mathbf{Y}_2$, and the matrix $\mathbf{\Phi}$ coincides with $\mathbf{Y}$. As it was said above, a pair of matrices $(\mathbf{U}, \mathbf{\Phi})$ can be considered as a representation of a partial Boolean function. It is easy to see that for any value of vector $\mathbf{x}$ taken arbitrarily from the definition domain of the given function f, the values of φ and f coincide. So, the pairs of matrices $(\mathbf{X}_1, \mathbf{Y}_1)$, $(\mathbf{X}_2, \mathbf{Y}_2)$ and $(\mathbf{U}, \mathbf{\Phi})$ represent the desired superposition. This representation can be redundant as there can be repeated or absorbed rows in the matrices and symbol "$-$" in one-column matrices $\mathbf{Y}_i$. This redundancy can be eliminated easily by removing rows from the matrices.

Thus, the process of solving the considered problem with minimizing the sum of the numbers of arguments in the functions g_1 and g_2 consists of the following stages.

1. Finding all the maximal admissible bicliques in graph G_X. The method described in [13] can be used for this purpose. Note that graph G_Y is a biclique of G_X, which should not be admissible because it is a one-block cover of E_Y leading to a trivial solution — one of the functions g_i is a constant. Any found biclique B_j is assigned with weight as an ordered pair (r_j, s_j) where r_j is the minimal rank of a term in the corresponding DNF, s_j is the number of such terms. This stage is a "bottle-neck" in the suggested method, as the upper bound of the number of all the maximal bicliques in a graph with m vertices is $2^{m-1} - 1$. It is reached in a complete graph. Graph G_X is the same one if $\mathbf{X}$ is a Boolean matrix.

2. Obtaining a two-block cover of E_Y by the found bicliques. The cover must have the best weight. The weight of a cover consisting of bicliques B_i and B_j is an ordered pair (R_k, S_k) where $R_k = r_i + r_j$ and $S_k = s_i + s_j$. A weight (R_k, S_k) is considered better than a weight (R_l, S_l) if $R_k < R_l$ or $S_k > S_l$ when $R_k = R_l$. At this stage, the demand of non-intersecting sets Z_1 and Z_2 in disjoint bi-decomposition is satisfied. The complexity of finding all the two-block covers is expressed by the second power polynomial relative to the number of sets, among which the cover is looked for. Therefore, the enumeration of all the two-block covers is not considered as a laborious task.

3. Constructing Boolean functions $g_1(\mathbf{z}_1)$ and $g_2(\mathbf{z}_2)$ that are represented by matrices $\mathbf{X}_1$, $\mathbf{Y}_1$ and $\mathbf{X}_2$, $\mathbf{Y}_2$, and obtaining function φ if its type is not given.

If the type of the function φ is given, the linear and non-linear functions should be considered separately, as it was done in [6], because the sets of admissible bicliques

and two-block covers have different peculiarities in those cases. Among Boolean functions depending essentially on two arguments, the linear functions are ones expressed by XOR and equivalence operations. The rest are non-linear functions.

2. Bi-decomposition with a non-linear function

To give the type of the function φ, every pair of rows in matrices $\mathbf{X}$ and $\mathbf{Y}$ of the same name should be assigned with the set of possible values of functions g_1 and g_2 that are required according to the value of the given function f. For instance, if $\varphi = g_1 \wedge g_2$ (that is, φ is expressed by conjunction), then that set is $\{(1,1)\}$ at $f = 1$ or $\{(0,0),(0,1),(1,0)\}$ at $f = 0$. The latter set can be given as $\{(0,-),(-,0)\}$, i.e. the value of one of the functions g_1 or g_2 can be indefinite. Note that according to the way of construction of the functions g_1 and g_2, the vertices of graph G_X, to which the rows of $\mathbf{X}$ and $\mathbf{Y}$ with assigned one-element set $\{(1,1)\}$ correspond, are in the same part in any of all the admissible bicliques. Denote the set of them by W. At that, the number of maximal admissible bicliques is limited to $2^{m-|W|-1}$ where m is the number of vertices of a graph, $|W|$ is the cardinality of W. That is almost $2^{|W|-1}$ times less than the number of all the maximal bicliques.

Such reasons are true for other non-linear functions as well, but, for example, the set W will consist of vertices with corresponding one-element set $\{(0,0)\}$ for disjunction and of vertices with $\{(1,0)\}$ for implication.

As an example, let us take a partial Boolean function given by matrices

$$\mathbf{X} = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & - & 0 & 1 & 0 \\ 0 & - & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & - & 1 & 0 \\ 0 & - & - & 0 & 1 & - \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & - & 1 & 1 & - \\ - & 0 & 1 & - & 1 & 1 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix} \end{array}, \quad \mathbf{Y} = \begin{array}{c} \begin{matrix} y \end{matrix} \\ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \end{array}.$$

The values of y are not defined at the part of Boolean space of variables x_1, x_2, x_3, x_4, x_5, x_6, which is not covered by the intervals represented by $\mathbf{X}$. The sets of variables assigned to the edges of graph G_X are shown in Table 1 where rows and columns correspond to the vertices of G_X. The empty squares show absence of edges between corresponding vertices.

Table 1

v_2	v_3	v_4	v_5	v_6	v_7	
x_1, x_4, x_5, x_6	x_2	x_1	x_1, x_2, x_4, x_6	x_4	x_6	v_1
	x_1, x_5, x_6	x_4, x_5	x_3, x_5	x_1, x_5	x_5	v_2
		x_1	x_1, x_3, x_6	x_2	x_2, x_6	v_3
			x_4	x_1, x_4		v_4
				x_1, x_2	x_2, x_3	v_5
						v_6

Let the function φ be expressed by Sheffer function (inverse conjunction). In this case $W = \{v_1, v_2, v_3\}$.

All the maximal admissible bicliques of the graph G_X in the form of a pair of subsets of vertices with corresponding CNF and DNF are:

1) $\langle\{v_1, v_2, v_3, v_4, v_5\}, \{v_6\}\rangle$, $x_2x_4(x_1 \vee x_5) = x_1x_2x_4 \vee x_2x_4x_5$;
2) $\langle\{v_1, v_2, v_3, v_5, v_6\}, \{v_4\}\rangle$, x_1x_4;

3) $\langle\{v_1, v_2, v_3, v_6\}, \{v_4, v_5\}\rangle$, $x_1(x_4 \vee x_5)(x_3 \vee x_5) = x_1x_3x_4 \vee x_1x_5$;
4) $\langle\{v_1, v_2, v_3\}, \{v_4, v_5, v_6\}\rangle$, $x_1x_2x_4(x_3 \vee x_5) = x_1x_2x_3x_4 \vee x_1x_2x_4x_5$;
5) $\langle\{v_1, v_2, v_3, v_5\}, \{v_6, v_7\}\rangle$, $x_2x_4x_5x_6$;
6) $\langle\{v_1, v_2, v_3, v_4, v_6, v_7\}, \{v_5\}\rangle$, $x_4(x_3 \vee x_5)(x_1 \vee x_3 \vee x_6)(x_1 \vee x_2) = x_1x_2x_4x_5 \vee x_1x_3x_4 \vee$ $\vee\, x_2x_3x_4 \vee x_2x_4x_5x_6$;
7) $\langle\{v_1, v_2, v_3, v_4\}, \{v_5, v_6, v_7\}\rangle$, $x_2x_4x_5x_6$;
8) $\langle\{v_1, v_2, v_3, v_5\}, \{v_4, v_6, v_7\}\rangle$, $x_1x_2x_4x_5x_6$;
9) $\langle\{v_1, v_2, v_3\}, \{v_4, v_5, v_7\}\rangle$, $x_1x_5x_6$.

The table of covering the edge set of G_Y by those bicliques after application of reduction rules [12] looks as Table 2 where the obtained bicliques are represented by their numbers. The two-block cover with the best weight consists of the bicliques 1 and 9.

Table 2

No	v_1v_4	v_1v_5	v_1v_6	v_1v_7	v_2v_4	v_2v_5	v_2v_6	v_2v_7	v_3v_4	v_3v_5	v_3v_6	v_3v_7	Weight
1			1				1				1		3, 2
2	1				1				1				2, 1
3	1	1			1	1			1	1			2, 1
4	1	1	1		1	1	1		1	1	1		4, 2
5			1	1			1	1			1	1	4, 1
6		1				1				1			3, 2
7		1	1	1		1	1	1		1	1	1	4, 1
8	1		1	1	1		1	1	1		1	1	5, 1
9	1	1		1	1	1		1	1	1		1	3, 1

The functions $g_1(x_1, x_2, x_4)$ (or $g_1(x_2, x_4, x_5)$) and $g_2(x_1, x_5, x_6)$ are constructed by these bicliques with corresponded DNFs and the given matrices $\mathbf{X}$, $\mathbf{Y}$. This is a non-disjoint decomposition with intersection of the set Z_1 and Z_2 by x_1. None of the obtained covers leads to disjoint decomposition. One of the variants of the solution is represented by the following matrices (the type of φ is given):

$$\mathbf{X}_1 = \begin{matrix} x_1 & x_2 & x_4 \end{matrix}\!\!\begin{bmatrix} 1 & 0 & 0 \\ 0 & - & 1 \\ 1 & 1 & - \\ 0 & - & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ - & 0 & - \end{bmatrix}\!\!\begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix}, \quad \mathbf{Y}_1 = \begin{matrix} g_1 \end{matrix}\!\!\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ - \end{bmatrix}; \quad \mathbf{X}_2 = \begin{matrix} x_1 & x_5 & x_6 \end{matrix}\!\!\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & - \\ 0 & 1 & 1 \\ 1 & 1 & - \\ - & 1 & 1 \end{bmatrix}\!\!\begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix}, \quad \mathbf{Y}_2 = \begin{matrix} g_2 \end{matrix}\!\!\begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ - \\ 0 \end{bmatrix}.$$

The result of bi-decomposition of the given partial Boolean function after minimizing DNF is represented by the following formulas (the variable x_3 turns out to be an inessential argument):

$$g_1 = \overline{x_1} \vee x_2 \vee \overline{x_4},\ g_2 = x_1\overline{x_6} \vee \overline{x_5},\ y = g_1|g_2 = \overline{g_1 \wedge g_2}.$$

3. Bi-decomposition with a linear function

According to the values of a given function f, for a linear function φ, certain pairs of rows in matrices $\mathbf{X}$ and $\mathbf{Y}$ of the same name are assigned with the set $\{(0,0),(1,1)\}$ of possible values of functions g_1 and g_2, the others are assigned with $\{(0,1),(1,0)\}$. Since the values of functions g_1 and g_2 must be defined at any row of matrix $\mathbf{X}$, it must be orthogonalized in order to obtain a complete graph of row orthogonality. Orthogonalization of a ternary

matrix consists in obtaining a matrix equivalent to it with mutually orthogonal rows. Since the values of functions g_1 and g_2 are required to be defined at any row of matrix $\mathbf{X}$, not every cover of E_X by two bicliques can be the base for constructing g_1 and g_2. It would be better not to refer to the cover problem, but look for pairs of bicliques agreed with the values of g_1 and g_2.

Denote by W the set of vertices of G_X corresponding to the rows of the orthogonalized matrix $\mathbf{X}$ with assigned set $\{(0,1),(1,0)\}$. Let us find all maximal bicliques $B_1, B_2, \ldots, B_p$ of the subgraph of G_X induced by the set W. Every biclique is represented as $B_i = \langle V_i^0, V_i^1\rangle$ where upper index 0 (1) shows the value of g_j $(j = 1, 2)$ at the sets of argument values corresponding to V_i^0 (to V_i^1). The number of those bicliques is $p = 2^{|W|-1} - 1$. For every of them we form the pair $\langle\langle V_i^0, V_i^1\rangle, \langle U_i^0, U_i^1\rangle\rangle$ where $U_i^0 = V_i^1$ and $U_i^1 = V_i^0$ at first. The further process of obtaining the pairs of bicliques that define the values of the functions g_1 and g_2 can be described by the Algorithm 1. The input data for it are p pairs in the form of $\langle\langle V_i^0, V_i^1\rangle, \langle U_i^0, U_i^1\rangle\rangle$ and the set $V \setminus W$.

Algorithm 1.

1: $A := V \setminus W$, choose $v \in A$, $A := A \setminus \{v\}$, $i := 0$.
2: $i := i + 1$. **If** $i > p$, go to 3, **otherwise** $C_i^0 := V_i^0$, $C_i^1 := V_i^1$, $D_i^0 := U_i^0$, $D_i^1 := U_i^1$, $C_i^0 := C_i^0 \cup \{v\}$, $D_i^0 := D_i^0 \cup \{v\}$, go to 2.
3: **If** $A = \varnothing$, go to 6, **otherwise** choose $v \in A$, $A := A \setminus \{v\}$, $i := 0$, $j := p$;
4: $i := i + 1$. **If** $i > p$, $p := j$, $i := 0$, go to 5, **otherwise** $V_i^0 := C_i^0 \cup \{v\}$; $U_i^0 := D_i^0 \cup \{v\}$; $V_i^1 := C_i^1$; $U_i^1 := D_i^1$, $j := j + 1$, $V_j^1 := C_i^1 \cup \{v\}$, $U_j^1 := D_i^1 \cup \{v\}$, $V_j^0 := C_i^0$, $U_j^0 := D_i^0$, go to 4;
5: $i := i + 1$. **If** $i > p$, go to 3, **otherwise** $C_i^0 := V_i^0$, $C_i^1 := V_i^1$, $D_i^0 := U_i^0$, $D_i^1 := U_i^1$, go to 5.
6: **End.**

The result of the algorithm executing is the set of transformed pairs in the form of $\langle V_i^0, V_i^1\rangle, \langle U_i^0, U_i^1\rangle$ where the union of parts of bicliques V_i^0, V_i^1 or U_i^0, U_i^1 has all the vertices of V. The number of those pairs is expressed by the following formula:

$$p = (2^{|W|-1} - 1)2^{|V\setminus W|-1}. \tag{1}$$

The algorithm does not describe how to form the corresponded CNFs. It is done in order not to complicate the algorithm description. The bicliques and corresponding CNFs can be formed simultaneously or separately.

Solution of the bi-decomposition problem for the function $\varphi = g_1 \oplus g_2$ (XOR operation) is shown on the example above. After orthogonalization of matrix X the pair of matrices $\mathbf{X}$ and $\mathbf{Y}$ are as follows:

$$\mathbf{X} = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & - & 0 & 1 & 0 \\ 0 & - & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & - & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & - & - & 0 & 1 & - \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & - & 1 & 1 & - \end{bmatrix} \end{array} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{matrix}, \quad \mathbf{Y} = \begin{array}{c} \begin{matrix} y \end{matrix} \\ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \end{array}.$$

Table 3 represents the sets of variables assigned to the edges of G_X likewise Table 1. In this case $W = \{v_4, v_5, v_6, v_7, v_8\}$. The maximal bicliques of the subgraph of G_X induced by W with corresponding CNFs and DNFs are given below:

$\langle\{v_4, v_5, v_6, v_7\}, \{v_8\}\rangle$, x_1x_4;
$\langle\{v_4, v_5, v_6, v_8\}, \{v_7\}\rangle$, x_1x_4;
$\langle\{v_4, v_5, v_6\}, \{v_7, v_8\}\rangle$, x_1;
$\langle\{v_4, v_5, v_7, v_8\}, \{v_6\}\rangle$, $x_1x_4(x_2 \vee x_3) = x_1x_2x_4 \vee x_1x_3x_4$;
$\langle\{v_4, v_5, v_7\}, \{v_6, v_8\}\rangle$, $x_4(x_2 \vee x_3)(x_1 \vee x_2) = x_1x_3x_4 \vee x_2x_4$;
$\langle\{v_4, v_5, v_8\}, \{v_6, v_7\}\rangle$, $x_1x_4(x_2 \vee x_3) = x_1x_2x_4 \vee x_1x_3x_4$;
$\langle\{v_4, v_5\}, \{v_6, v_7, v_8\}\rangle$, $x_1x_4(x_2 \vee x_3) = x_1x_2x_4 \vee x_1x_3x_4$;
$\langle\{v_4, v_6, v_7, v_8\}, \{v_5\}\rangle$, x_1x_4;
$\langle\{v_4, v_6, v_7\}, \{v_5, v_8\}\rangle$, x_1x_4;
$\langle\{v_4, v_6, v_8\}, \{v_5, v_7\}\rangle$, x_4;
$\langle\{v_4, v_6\}, \{v_5, v_7, v_8\}\rangle$, x_1x_4;
$\langle\{v_4, v_7, v_8\}, \{v_5, v_6\}\rangle$, $x_1x_4(x_2 \vee x_3) = x_1x_2x_4 \vee x_1x_3x_4$;
$\langle\{v_4, v_7\}, \{v_5, v_6, v_8\}\rangle$, $x_1x_4(x_2 \vee x_3) = x_1x_2x_4 \vee x_1x_3x_4$;
$\langle\{v_4, v_8\}, \{v_5, v_6, v_7\}\rangle$, $x_1x_4(x_2 \vee x_3) = x_1x_2x_4 \vee x_1x_3x_4$;
$\langle\{v_4\}, \{v_5, v_6, v_7, v_8\}\rangle$, $x_4(x_2 \vee x_3)(x_1 \vee x_2) = x_1x_3x_4 \vee x_2x_4$.

Table 3

v_2	v_3	v_4	v_5	v_6	v_7	v_8	
x_1, x_4, x_5, x_6	x_2	x_1, x_2, x_4, x_6	x_1	x_1, x_4, x_6	x_6	x_4	v_1
	x_1, x_5, x_6	x_3, x_5	x_4, x_5	x_5	x_1, x_4, x_6	x_1, x_5	v_2
		x_1, x_3, x_6	x_1	x_1, x_2, x_6	x_2, x_6	x_2	v_3
			x_4	x_2, x_3	x_1, x_2, x_3, x_4	x_1, x_2	v_4
				x_4	x_1	x_1, x_4	v_5
					x_1, x_4	x_1	v_6
						x_4	v_7

As input data for Algorithm 1, the following set of pairs of bicliques is given:

$\langle\{v_4, v_5, v_6, v_7\}, \{v_8\}\rangle$, $\langle\{v_8\}, \{v_4, v_5, v_6, v_7\}\rangle$;
$\langle\{v_4, v_5, v_6, v_8\}, \{v_7\}\rangle$, $\langle\{v_7\}, \{v_4, v_5, v_6, v_8\}\rangle$;
$\langle\{v_4, v_5, v_6\}, \{v_7, v_8\}\rangle$, $\langle\{v_7, v_8\}, \{v_4, v_5, v_6\}\rangle$;
$\langle\{v_4, v_5, v_7, v_8\}, \{v_6\}\rangle$, $\langle\{v_6\}, \{v_4, v_5, v_7, v_8\}\rangle$;
$\langle\{v_4, v_5, v_7\}, \{v_6, v_8\}\rangle$, $\langle\{v_6, v_8\}, \{v_4, v_5, v_7\}\rangle$;
$\langle\{v_4, v_5, v_8\}, \{v_6, v_7\}\rangle$, $\langle\{v_6, v_7\}, \{v_4, v_5, v_8\}\rangle$;
$\langle\{v_4, v_5\}, \{v_6, v_7, v_8\}\rangle$, $\langle\{v_6, v_7, v_8\}, \{v_4, v_5\}\rangle$;
$\langle\{v_4, v_6, v_7, v_8\}, \{v_5\}\rangle$, $\langle\{v_5\}, \{v_4, v_6, v_7, v_8\}\rangle$;
$\langle\{v_4, v_6, v_7\}, \{v_5, v_8\}\rangle$, $\langle\{v_5, v_8\}, \{v_4, v_6, v_7\}\rangle$;
$\langle\{v_4, v_6, v_8\}, \{v_5, v_7\}\rangle$, $\langle\{v_5, v_7\}, \{v_4, v_6, v_8\}\rangle$;
$\langle\{v_4, v_6\}, \{v_5, v_7, v_8\}\rangle$, $\langle\{v_5, v_7, v_8\}, \{v_4, v_6\}\rangle$;
$\langle\{v_4, v_7, v_8\}, \{v_5, v_6\}\rangle$, $\langle\{v_5, v_6\}, \{v_4, v_7, v_8\}\rangle$;
$\langle\{v_4, v_7\}, \{v_5, v_6, v_8\}\rangle$, $\langle\{v_5, v_6, v_8\}, \{v_4, v_7\}\rangle$;
$\langle\{v_4, v_8\}, \{v_5, v_6, v_7\}\rangle$, $\langle\{v_5, v_6, v_7\}, \{v_4, v_8\}\rangle$;
$\langle\{v_4\}, \{v_5, v_6, v_7, v_8\}\rangle$, $\langle\{v_5, v_6, v_7, v_8\}, \{v_4\}\rangle$.

At the initial stage of Algorithm 1 (step 2), the vertex v_1 from $V \setminus W$ is added to all the pairs of bicliques, and $\langle\{v_1, v_4, v_5, v_6, v_7\}, \{v_8\}\rangle, \langle\{v_1, v_8\}, \{v_4, v_5, v_6, v_7\}\rangle$ will be the first of them. Then it is transformed into the following pairs:

$\langle\{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}, \{v_8\}\rangle$, $\langle\{v_1, v_2, v_3, v_8\}, \{v_4, v_5, v_6, v_7\}\rangle$;

$\langle\{v_1, v_2, v_4, v_5, v_6, v_7\}, \{v_3, v_8\}\rangle$, $\langle\{v_1, v_2, v_8\}, \{v_3, v_4, v_5, v_6, v_7\}\rangle$;
$\langle\{v_1, v_3, v_4, v_5, v_6, v_7\}, \{v_2, v_8\}\rangle$, $\langle\{v_1, v_3, v_8\}, \{v_2, v_4, v_5, v_6, v_7\}\rangle$;
$\langle\{v_1, v_4, v_5, v_6, v_7\}, \{v_2, v_3, v_8\}\rangle$, $\langle\{v_1, v_8\}, \{v_2, v_3, v_4, v_5, v_6, v_7\}\rangle$.

Such transformations are fulfilled concurrently for all the pairs. Among all the pairs of bicliques that are obtained by the algorithm above (according to the formula (1) the number of them is $p = 60$), the pair with the best weight (6, 2) is

$\langle\{v_1, v_2, v_3, v_4, v_5, v_6\}, \{v_7, v_8\}\rangle$, $x_1x_2x_4x_6$;
$\langle\{v_1, v_2, v_3, v_7, v_8\}, \{v_4, v_5, v_6\}\rangle$, x_1x_5.

According to these bicliques and matrices $\mathbf{X}$ and $\mathbf{Y}$ the functions $g_1(x_1, x_2, x_4, x_6)$ and $g_2(x_1, x_5)$ are constructed that are given as follows:

$$\mathbf{X}_1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_4 & x_6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & - & 1 & 1 \\ 1 & 1 & - & 0 \\ 0 & 1 & 1 & 1 \\ 0 & - & 0 & - \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & - \end{bmatrix} \end{array} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{matrix}, \quad \mathbf{Y}_1 = \begin{array}{c} g_1 \\ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \end{array}; \quad \mathbf{X}_2 = \begin{array}{c} \begin{matrix} x_1 & x_5 \end{matrix} \\ \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \end{array} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{matrix}, \quad \mathbf{Y}_2 = \begin{array}{c} g_2 \\ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \end{array}.$$

Minimizing DNFs leads to the following expressions:

$$g_1 = \overline{x_1} \vee x_2 \vee \overline{x_4}\,\overline{x_6}, \quad g_2 = x_1 \vee \overline{x_5}, \quad y = g_1 \oplus g_2.$$

The result is in the form of non-disjoint bi-decomposition (the variable x_1 is an argument of both g_1 and g_2). The variant of disjoint bi-decomposition is not found out in this example.

Conclusion

The described method for bi-decomposition differs from many known ones primarily in that it does not demand to give a partition of the set of arguments of a given function. The method has strong restrictions in practical application because of exponential growth of the number of bicliques with the growth of the number of rows of the matrices of specification. Its advantage can be that it shows the direction of the search for a solution. This can be used in developing heuristic methods.

REFERENCES

1. *Perkowski M. A. and Grygiel S.* A Survey of Literature on Functional Decomposition, Version IV (Technical Report). Portland, USA, Portland State University, Department of Electrical Engineering, 1995. 188 p.
2. *Cortadella J.* Timing-driven logic bi-decomposition. IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, 2003, vol. 22, no. 6, pp. 675–685.
3. *Mishchenko A., Steinbach B., and Perkowski M.* An algorithm for bi-decomposition of logic functions. Proc. 38th Ann. Design Automation Conf., Las Vegas, NV, USA, ACM, June 2001, pp. 103–108.
4. *Chang S.-C., Marek-Sadowska M., and Hwang T.* Technology mapping for TLU FPGA's based on decomposition of binary decision diagrams. IEEE Trans. Computer-Aided Design, 1996, vol. 15, no. 10, pp. 1226–1235.

5. *Bibilo P. N.* Dekompozitsiya bulevykh funktsiy na osnove resheniya logicheskikh uravneniy [Decomposition of Boolean Functions Based on Solving Logical Equations]. Minsk, Belaruskaya Navuka, 2009. 211 p. (in Russian)
6. *Zakrevskij A. D.* On a special kind decomposition of weakly specified Boolean functions. Second Intern. Conf. CAD DD'97, Minsk, Republic of Belarus, November 12–14, 1997. Minsk, NAS of Belarus, Institute of Engineering Cybernetics, 1997, vol. 1, pp. 36–41.
7. *Cheng D. and Xu X.* Bi-decomposition of logical mappings via semi-tensor product of matrices. Automatica, 2013, vol. 49, no. 7, pp. 1979–1985.
8. *Choudhury M. and Mohanram K.* Bi-decomposition of large Boolean functions using blocking edge graphs. IEEE/ACM Intern. Conf. ICCAD, San Jose, CA, USA, IEEE Press, 2010, pp. 586–591.
9. *Fišer P. and Schmidt J.* Small but nasty logic synthesis examples. Proc. IWSBP'8, Freiberg, Germany, Freiberg University of Mining and Technology, Sept. 2008, pp. 183–190.
10. *Steinbach B. and Posthoff C.* Vectorial bi-decomposition for lattices of Boolean functions. Further Improvements in the Boolean Domain (ed. B. Steinbach). Cambridge Scholars Publishing, 2018, pp. 175–198.
11. *Pottosin Yu. V. and Shestakov E. A.* Dekompozitsiya sistemy chastichnykh bulevykh funktsiy s pomoshch'yu pokrytiya grafa polnymi dvudol'nymi podgrafami [Decomposition of a system of partial Boolean functions with the help of covering a graph by complete bipartite subgraphs]. Proc. 2nd Conf. "New Information Technologies in the Study of Discrete Structures", Yekaterinburg, UrS RAS, 1998, pp. 185–189. (in Russian)
12. *Zakrevskij A. D., Pottosin Yu. V., and Cheremisinova L. D.* Combinatorial Algorithms of Discrete Mathematics. Tallinn, TUT Press, 2008. 193 p.
13. *Pottosina S., Pottosin Yu., and Sedliak B.* Finding maximal complete bipartite subgraphs in a graph. J. Appl. Math., 2008, vol. 1, no. 1, pp. 75–81.

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

УДК 004.942

СОПУТСТВУЮЩАЯ КЛАСТЕРНАЯ СТРУКТУРА, ФОРМИРУЕМАЯ АЛГОРИТМОМ ХАММЕРСЛИ — ЛИСА — АЛЕКСАНДРОВИЦА ПРИ ГЕНЕРАЦИИ ПЕРКОЛЯЦИОННЫХ КЛАСТЕРОВ

Д. В. Алексеев, Г. А. Казунина

Кузбасский государственный технический университет им. Т. Ф. Горбачёва, г. Кемерово, Россия

Построен трёхмерный клеточный автомат, реализующий моделирование роста перколяционного кластера на простой кубической решётке по алгоритму Хаммерсли — Лиса — Александровица и впервые вводящий в рассмотрение сопутствующую кластерную структуру, формируемую из клеток, исключаемых из процесса роста. Сопутствующая кластерная структура промоделирована в широком интервале значений вероятности прорастания периметра $0{,}3117 < P < 0{,}6883$ на решётке размером $100 \times 100 \times 100$ и проанализирована с помощью функций распределения числа и массы кластеров сопутствующей структуры по размерам. В результате вычислительного эксперимента получены зависимости от вероятности прорастания периметра основных характеристик кластерной структуры, таких, как масса основного кластера, масса максимального кластера сопутствующей структуры, полная масса сопутствующей структуры, среднеквадратичные радиусы основного кластера и максимального кластера сопутствующей структуры, число кластеров сопутствующей структуры, отношение массы максимального кластера сопутствующей структуры к массе основного кластера. Установлено, что в интервале вероятности прорастания $0{,}3117 < P < 0{,}62$ в сопутствующей структуре формируется доминирующий кластер, среднеквадратичный радиус которого близок к среднеквадратичному радиусу основного кластера. При дальнейшем росте вероятности прорастания размеры доминирующего кластера резко уменьшаются, а при $P \leqslant 0{,}67$ наблюдается его распад.

Ключевые слова: *клеточный автомат, модели кинетического роста, алгоритм Хаммерсли — Лиса — Александровица.*

DOI 10.17223/ 20710410/47/10

CONCOMITANT CLUSTERS STRUCTURE CREATING BY HAMMERSLEY — LEATH — ALEXANDROWICHZ ALGORITHM FOR PERCOLATION CLUSTER GENERATING

D. V. Alekseev, G. A. Kazunina

Kuzbass State Technical University named after T. F. Gorbachev, Kemerovo, Russia

E-mail: dmitryalekseev@live.ru, gt-kga@yandex.ru

A three-dimensional cellular automaton implementing the simulation of growth of a percolation cluster on a simple cubic lattice according to the Hammersley — Leath —

Alexandrowichz algorithm was built for the first time introducing into consideration the concomitant cluster structure formed out of cells excluded from the growth process. The concomitant cluster structure is modelled in a wide interval of perimeter germination probability values $0{,}3117 < P < 0{,}6883$ on a $100 \times 100 \times 100$ lattice and analyzed by using the functions of distribution of number and mass of clusters of the accompanying structure by size. As a result of the computational experiment, there were obtained dependencies on the probability of perimeter germination for such basic characteristics of the cluster structure as the mass of the main cluster; the mass of the maximum cluster of concomitant structure; the total mass of the concomitant structure; mean-square radii of the main cluster and the maximum cluster of the concomitant structure; the number of clusters of concomitant structure; mass ratio of the maximum cluster of the concomitant structure to the mass of the main cluster. It has been established that in the interval of germination probability $0{,}3117 < P < 0{,}62$ in the concomitant structure, the dominant cluster is formed with the mean-square radius close to the mean-square radius of the main cluster. With a further increase in probability of germination, the size of the dominant cluster decreases sharply, and at $P \leqslant 0{,}67$ its decay is observed.

Keywords: *cellular automaton, kinetic growth models, Hammersley — Leath — Alexandrowichz algorithm.*

Введение

Моделирование разнообразных физических и физико-химических процессов клеточными автоматами, приводящее к фрактальным кластерным структурам, широко используется в настоящее время [1 – 8]. При этом значительное число работ посвящено исследованию перколяционных кластеров [1, 2, 9 – 11], для генерации которых используются алгоритмы типа Хаммерсли — Лиса — Александровица (далее — ХЛА) [1, 2, 5, 6, 9, 12, 13]. Такие алгоритмы формируют перколяционный кластер путём случайного проращивания периметра затравочной клетки (первый шаг) и периметра растущего кластера на дальнейших шагах. В ходе работы алгоритма на каждом шаге могут возникать клетки, которые не присоединяются к кластеру и исключаются из процесса роста на последующих шагах, то есть алгоритмы типа ХЛА генерируют не только основной кластер, но и сопутствующую кластерную структуру.

Если свойства основного ХЛА-кластера изучены подробно (см., например, [1, 2, 9]), то свойства сопутствующей кластерной структуры фактически не изучались. Только в [14] впервые рассмотрена сопутствующая кластерная структура на двумерных решётках (квадратной и треугольной). В то же время модели, включающие одновременно как основной ХЛА-кластер, так и сопутствующую кластерную структуру, могут оказаться полезными, например при моделировании химических реакций в твёрдой фазе, когда в неоднородной среде образуются два продукта реакции.

В настоящей работе изучены свойства сопутствующей кластерной структуры, образующейся при генерации трёхмерных перколяционных кластеров ХЛА-алгоритмом на простой кубической решётке (шесть ближайших соседей) в широком интервале $0{,}3117 < P < 0{,}6883$ вероятности прорастания периметра. Как известно [1], при формировании перколяционных кластеров на простой кубической решётке алгоритмом многократной маркировки для значений вероятности оккупации из указанного интервала перколяция происходит как по оккупированным, так и по свободным узлам.

1. Формализация и реализация алгоритма

Использованная в работе реализация ХЛА-алгоритма представляется в виде клеточного автомата, манипулирующего состояниями клеток, локализованных на узлах решётки. Алфавит клеточного автомата, описывающий возможные состояния клетки, задаётся вектором, формируемым парой булевых переменных:

$$A = \{(0;0), (0;1), (1;0), (1;1)\}.$$

Первая переменная указывает, занята клетка или свободна. Вторая — активна клетка (способна изменить состояние) или дезактивирована (остаётся в неизменном состоянии). То есть на каждом шаге алгоритма клетка может находиться в одном из четырёх состояний:

1) (0;0) — клетка свободна и активна;
2) (1;0) — клетка занята и активна;
3) (0;1) — клетка свободна и дезактивирована;
4) (1;1) — клетка занята и дезактивирована.

Каждая клетка идентифицируется именем $(I;J;K)$ — тройкой координат; на множестве имён

$$M = \{(I;J;K) : I, J, K = 0, 1, \ldots, N\}$$

задаётся шаблон соседства $T(I,J,K)$, определяемый типом решётки. Так, на простой кубической решётке шаблон соседства указывает для каждой клетки имена шести её ближайших соседей:

$$T(I,J,K) = \{(I{-}1;J;K);(I{+}1;J;K);(I;J{-}1;K);(I;J{+}1;K);(I;J;K{-}1);(I;J;K{+}1)\}.$$

Состояния клеток изменяются под действием локального оператора, выполняющего проращивание основного кластера по периметру, и реализуются следующей последовательностью шагов:

1) все клетки переводятся в состояние (0;0);
2) задаётся вероятность прорастания периметра P;
3) переводом в состояние (1;0) фиксируется затравочная клетка (как правило, в центре решётки);
4) в случайном порядке перебираются ближайшие соседи затравочной клетки и с вероятностью P переводятся в состояние (1;0) или, с вероятностью $1-P$, в состояние (0;1). При этом затравочная клетка переходит в состояние (1;1);
5) клетки, перешедшие в состояние (1;0), формируют периметр растущего кластера и способны изменять состояние своих ближайших соседей, находящихся в состоянии (0;0);
6) в случайном порядке перебираются ближайшие соседи клеток периметра и те из них, которые находятся в состоянии (0;0), переводятся или в состояние (1;0), или в состояние (0;1) по правилам шага 4, а все клетки периметра переводятся в состояние (1;1);
7) клетки, перешедшие в состояние (1;0), формируют обновленный периметр;
8) шаги 6, 7 повторяются до тех пор, пока:
    а) рост кластера не остановится (при переборе ближайших соседей периметра не образовалось ни одной клетки в состоянии (1;0));
    б) из клеток в состоянии (1;1) не сформировался кластер, соединяющий пару противоположных граней решётки;

9) из клеток в состоянии (0;1) формируются кластеры при помощи алгоритма маркировки [6, 15].

Таким образом, в результате работы клеточного автомата формируются два набора клеток:

1) основной кластер (клетки в состоянии (1;1));
2) сопутствующая кластерная структура (клетки в состоянии (0;1)).

При этом клетки в состоянии (1;0) отсутствуют, но остаются клетки в состоянии (0;0), незатронутые процессом роста.

Для непосредственного моделирования описанный вероятностный клеточный автомат реализован в MicrosoftVisualBasic 2017 в виде однодокументного Windows-приложения с программным подключением MicrosoftExcel в качестве клиента сохранения и обработки данных моделирования и является трёхмерной версией прототипа, использованного для моделирования сопутствующей кластерной структуры на двумерных решётках [15].

2. Результаты моделирования

Качественные различия характеристик кластерной структуры вблизи границ рассматриваемого интервала вероятности P прорастания периметра ($0{,}3117 < P < 0{,}6883$) видны уже из её визуального представления (рис. 1 и 2). Так, при 0,312 (рис. 1) чётко видна рыхлая структура основного кластера и наличие в сопутствующей кластерной структуре доминирующего (максимального) кластера, размеры которого многократно превышают размеры остальных кластеров. Напротив, при 0,688 (рис. 2) легко прослеживается плотная структура основного кластера и присутствие в сопутствующей структуре кластеров разнообразных размеров при отсутствии явно выделяющегося максимального кластера.

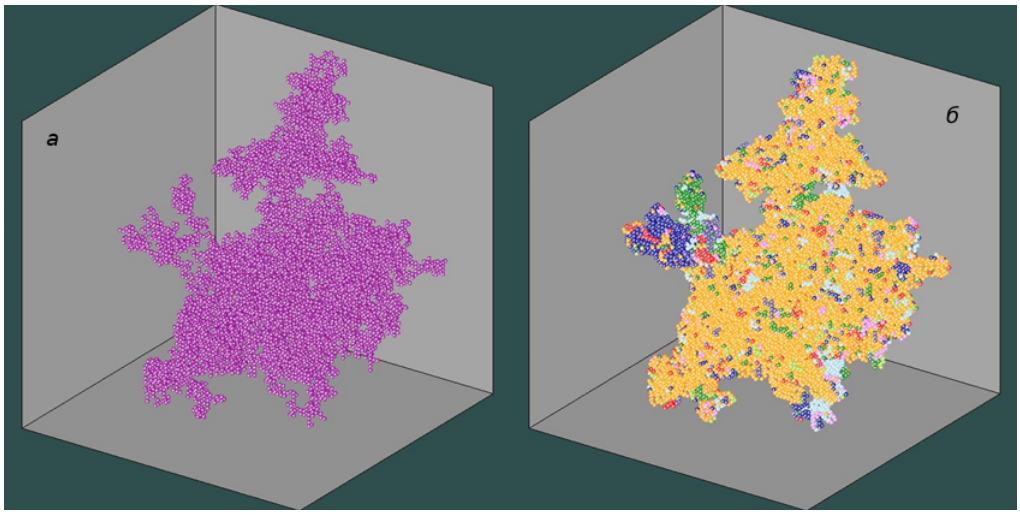


Рис. 1. Основной кластер ($а$) и сформировавшаяся в ходе его роста сопутствующая кластерная структура ($б$) для вероятности $P = 0{,}312$ на решётке $100 \times 100 \times 100$

Наиболее полную информацию о характеристиках сопутствующей кластерной структуры дают функции распределения числа и массы кластеров этой структуры по размерам (рис. 3).

Функции распределения строятся как зависимости числа N или общей массы (числа клеток) M кластеров, размер которых не превосходит заданного значения R. В нор-

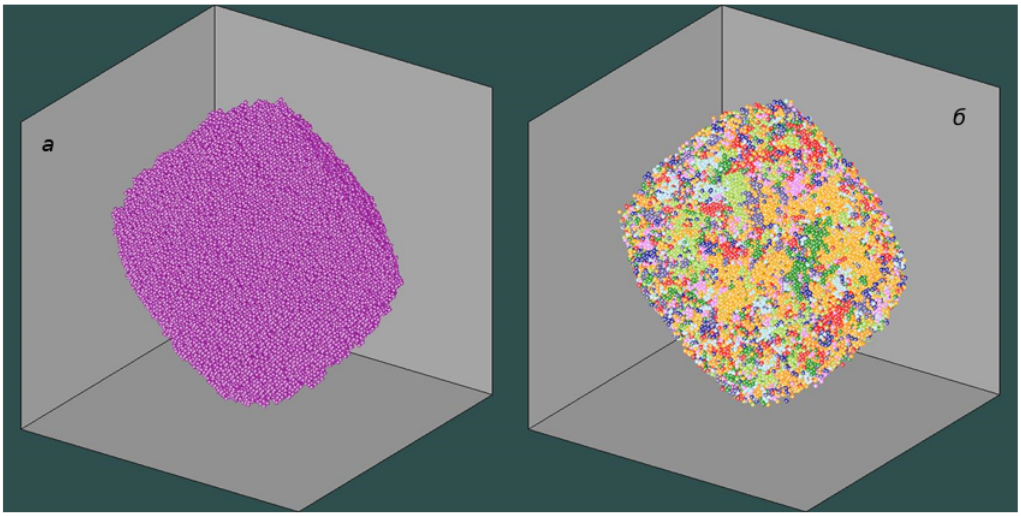


Рис. 2. Основной кластер (*а*) и сформировавшаяся в ходе его роста сопутствующая кластерная структура (*б*) для вероятности $P = 0{,}688$ на решётке $100 \times 100 \times 100$

мированных координатах размер нормируется на среднеквадратичный радиус максимального кластера $R_{\max}$, масса — на полную массу M_{total}, а число кластеров — на полное число кластеров N_{total}.

На функциях распределения, полученных при различных значениях вероятности прорастания периметра, чётко выделяются три группы кластеров:

1) кластеры, состоящие из одной клетки;
2) кластеры средних размеров (квазинепрерывный участок функций распределения);
3) один или несколько крупных кластеров.

Из функций распределения также извлекаются такие характеристики сопутствующей кластерной структуры, как масса (число клеток) максимального кластера и полная масса сопутствующей структуры, число кластеров сопутствующей структуры, число «одноклеточных» кластеров и т. п.

На рис. 4 и 5 приведены зависимости относительных вкладов кластеров трёх выделенных выше типов от вероятности прорастания периметра в полное число и полную массу сопутствующей структуры. Из рис. 4 видно, что доля одноклеточных кластеров $N_{\text{one}}/N_{\text{total}}$ лежит в интервале 60–80 %, проходя через максимум при $P \approx 0{,}45$, а доля кластеров средних размеров $N_{\text{mid}}/N_{\text{total}}$ лежит в интервале 20–40 %, проходя через минимум. Доля крупных кластеров пренебрежимо мала. Так, на решётке $100 \times 100 \times 100$ общее число кластеров при всех рассматриваемых значениях вероятности прорастания лежит в интервале от четырёх до семнадцати тысяч, тогда как число крупных кластеров не превосходит двух десятков.

Для распределения массы кластеров (рис. 5) картина противоположная. Для вероятности прорастания $0{,}3117 < P < 0{,}62$ подавляющая часть массы сопутствующей структуры, от 79 до 94 %, сосредоточена в максимальном кластере $M_{\max}$, масса кластеров средних размеров M_{mid} составляет 3–15 %, а масса одноклеточных кластеров M_{one} — от 3 до 7 %.

При дальнейшем увеличении вероятности прорастания вклад максимального кластера в общую массу сопутствующей структуры начинает резко падать, а вклад кластеров средних размеров — резко расти. Вблизи верхней границы интервала, начиная

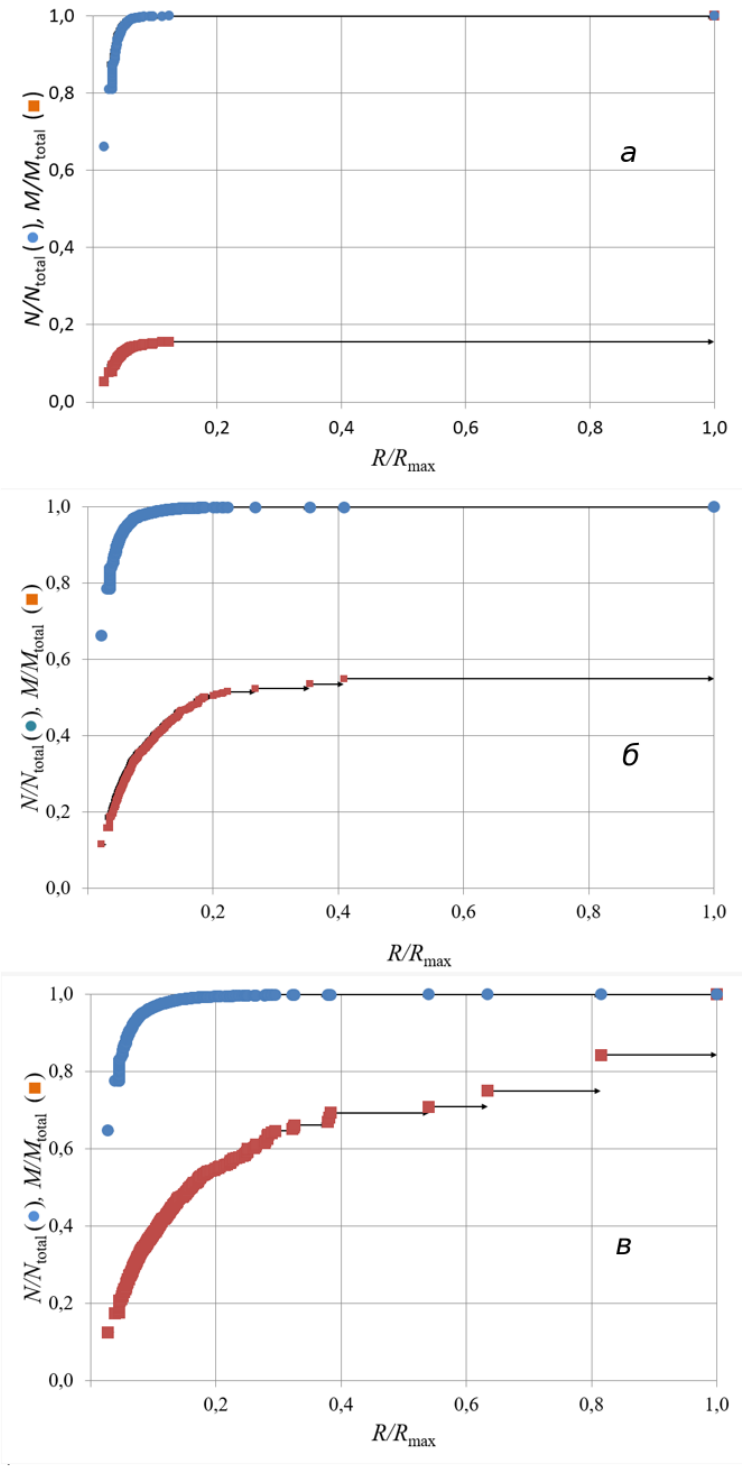


Рис. 3. Распределение числа и массы кластеров сопутствующей структуры по размеру для вероятностей $P = 0{,}32$ ($а$), $0{,}67$ ($б$) и $0{,}68$ ($в$)

с вероятности $P \approx 0{,}67$, когда максимальный кластер начинает распадаться, вклад крупных кластеров в общую массу становится меньше 50 %, а затем падает до 26 %. В то же время вклад в общую массу кластеров средних размеров резко растёт, превышая 60 % вблизи верхней границы интервала. Доля одноклеточных кластеров в общей массе на всём интервале изменения вероятности прорастания составляет от 3 до 13 %: сначала незначительно убывает с 6 до 3 %, а затем медленно возрастает до 13 %.

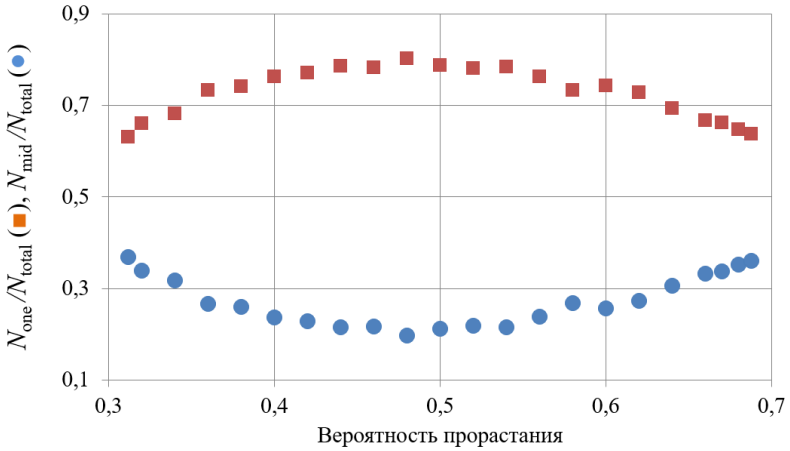


Рис. 4. Зависимость числа одноклеточных кластеров и кластеров средних размеров от вероятности P в нормированных координатах

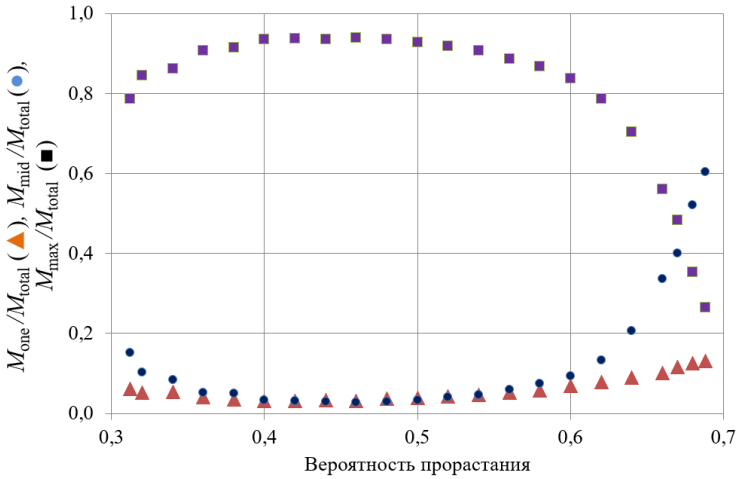


Рис. 5. Зависимость массы одноклеточных кластеров, кластеров средних размеров и максимального кластера сопутствующей структуры от вероятности P

На рис. 6–8 приведены зависимости от вероятности прорастания периметра дополнительных характеристик кластерной структуры:

1) масс основного кластера M_{hla}, максимального кластера $M_{\max}$ и всей сопутствующей структуры M_{total}, нормированных на число узлов решётки N_{latt} (рис. 6);
2) среднеквадратичных радиусов основного кластера R_{hla} и максимального кластера сопутствующей структуры $M_{\max}$, нормированных на половину длины ребра решетки L (рис. 7);
3) числа кластеров сопутствующей структуры N_{total}, нормированного на число узлов решётки, и отношения массы максимального кластера сопутствующей структуры к массе основного кластера (рис. 8).

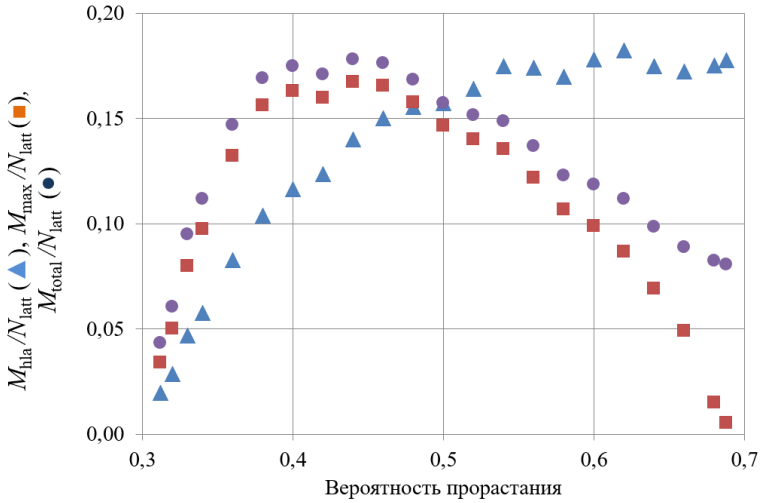


Рис. 6. Зависимости от вероятности P массы основного кластера, массы максимального кластера и полной массы сопутствующей структуры, нормированных на число узлов решётки

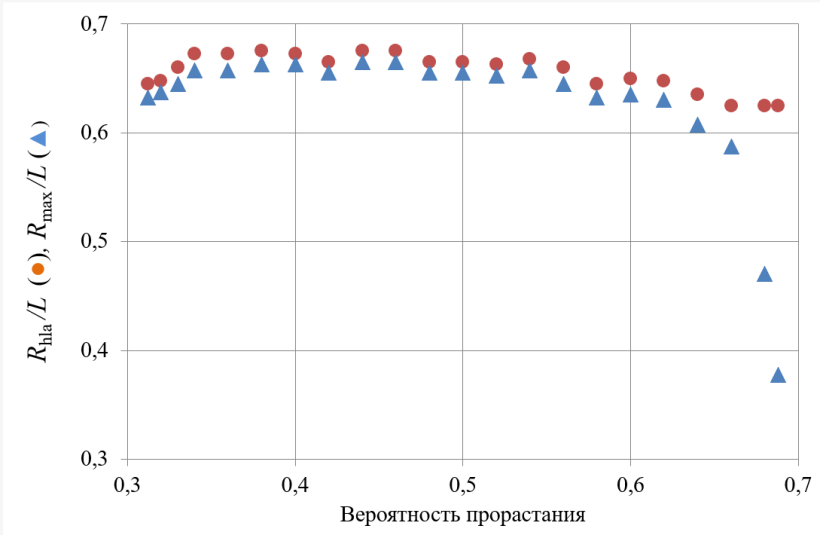


Рис. 7. Зависимость от вероятности P среднеквадратичных радиусов основного кластера и максимального кластера сопутствующей структуры

Из рис. 6 видно, что в интервале $0{,}312 < P < 0{,}55$ масса основного кластера монотонно возрастает, а далее остаётся практически неизменной (так проявляется конечность размеров решётки), тогда как полная масса и масса максимального кластера сопутствующей структуры сначала растут, проходя через максимум при $P \approx 0{,}45$, а далее убывают. При этом убывание массы максимального кластера идёт значительно резче, что является следствием его распада на более мелкие кластеры.

Следствием распада максимального кластера является и поведение его среднеквадратичного радиуса (рис. 7). Так, на интервале вероятности прорастания $0{,}3117 < P < 0{,}62$ среднеквадратичный радиус максимального кластера сопутствующей структуры составляет более 95 % от среднеквадратичного радиуса основного кластера и резко уменьшается при дальнейшем увеличении вероятности прорастания.

В то же время общее число кластеров сопутствующей структуры увеличивается примерно в 4 раза: сначала наблюдается резкий рост, затем небольшой спад и далее монотонный рост (рис. 8).

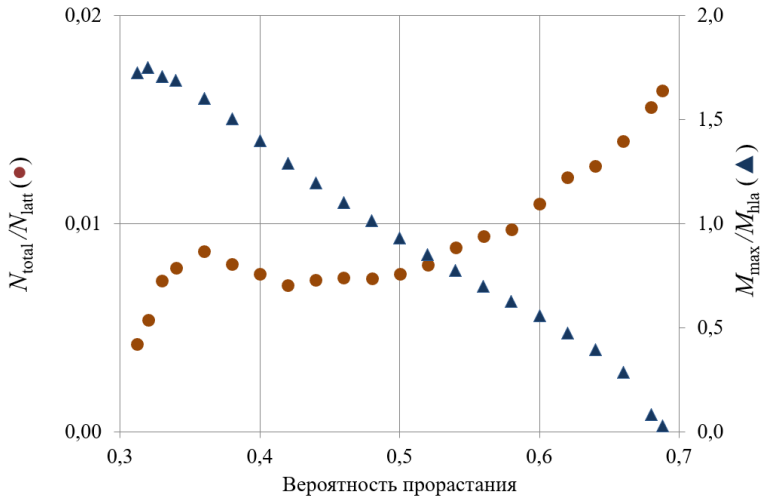


Рис. 8. Зависимости отношения масс (по правой оси) и полного числа кластеров сопутствующей структуры от вероятности прорастания периметра

Заключение

Построена и реализована трёхмерная клеточно-автоматная модель роста кластера по алгоритму Хаммерсли — Лиса — Александровица, включающая как основной перколяционный кластер, так и образующуюся в ходе его роста сопутствующую кластерную структуру. Она может оказаться полезной для построения моделей химических реакций в твёрдой фазе, когда в результате реакции образуются два продукта.

На основе анализа функций распределения числа и массы кластеров сопутствующей структуры по размерам получены зависимости от вероятности прорастания периметра следующих числовых характеристик кластерной структуры:

1) масс основного кластера и максимального кластера сопутствующей структуры, а также полной массы сопутствующей структуры;
2) среднеквадратичных радиусов основного кластера и максимального кластера сопутствующей структуры;
3) числа кластеров сопутствующей структуры и отношения массы максимального кластера сопутствующей структуры к массе основного кластера.

Установлено, что вблизи верхней границы рассмотренного интервала вероятности прорастания периметра при $P \geqslant 0{,}67$ наблюдается необратимый распад максимального кластера сопутствующей структуры на более мелкие кластеры, число которых лежит в пределах двух десятков.

ЛИТЕРАТУРА

1. *Федер Е.* Фракталы. М.: Мир, 1991. 258 с.
2. *Гулд Х., Тобочник Я.* Компьютерное моделирование в физике: в 2-х частях. Ч. 2. М.: Мир, 1990. 390 с.
3. *Бандман О. Л.* Дискретное моделирование физико-химических процессов // Прикладная дискретная математика. 2009. № 3 (5). С. 33–49.

4. *Бандман О. Л* Дискретная стохастическая модель просачивания жидкости через пористое вещество // Сибирский журнал вычислительной математики. 2018. № 1. С. 5–22.
5. *Алексеев Д. В., Казунина Г. А.* Моделирование кинетики накопления повреждений вероятностным клеточным автоматом // ФТТ. 2006. Т. 48. № 2. С. 255–261.
6. *Алексеев Д. В., Казунина Г. А., Чередниченко А. В.* Клеточно-автоматное моделирования процесса разрушения хрупких материалов // Прикладная дискретная математика. 2015. № 2 (28). С. 103–118.
7. *Лобанов А. И.* Моделирование клеточных автоматов // Компьютерные исследования и моделирование. 2010. Т. 2. № 3. С. 273–293.
8. *Матюшкин И. В., Заплетина М. А.* Обзор по тематике клеточных автоматов на базе современных отечественных публикаций // Компьютерные исследования и моделирование. 2019. Т. 11. № 1. С. 9–57.
9. *Тарасевич Ю. Ю.* Перколяция: теория, приложения, алгоритмы. М.: Книжный дом «ЛИБРОКОМ», 2018. 112 с.
10. *Москалев П. В.* Анализ структуры перколяционного кластера // ЖТФ. 2009. Т. 79. № 6. С. 2–7.
11. *Москалев П. В.* Структура модели перколяционных узлов на трехмерных квадратных решётках // Компьютерные исследования и моделирование. 2013. Т. 5. № 4. С. 607–622.
12. *Alexandrowicz Z.* Critically branched chains and percolation clusters // Phys. Lett. A. 1980. V. 80. No. 4. P. 284–286.
13. *Leath P.* Cluster size and boundary distribution near percolation threshold // Phys. Rev. B. 1976. V. 14. No. 11. P. 5046–5055.
14. *Алексеев Д. В., Казунина Г. А.* Сопутствующая кластерная структура, образующаяся при генерации перколяционного кластера по алгоритму Хаммерсли — Лиса — Александровица // Актуальные направления научных исследований XXI века: теория и практика. 2018. № 6 (42). С. 18–20.
15. *Алексеев Д.* Введение в компьютерное моделирование физических задач: использование Microsoft Visual Basic. М.: ЛЕНАНД, 2019. 272 с.

REFERENCES

1. *Feder J.* Fractals. N.Y., Springer, 1988, 258 p.
2. *Guld Kh. and Tobochnik Ya.* Kompyuternoe modelirovanie v fizike [Computer Modeling in Physics]. P. 2. Moscow, Mir Publ., 1990. 390 p. (in Russian)
3. *Bandman O. L.* Diskretnoe modelirovanie fiziko-khimicheskikh protsessov [Discrete models of physical-chemical processes]. Prikladnaya Diskretnaya Matematika, 2009, no. 3 (5), pp. 33–49. (in Russian)
4. *Bandman O. L.* A discrete stochastic model of water permeation through a porous substance: parallel implementation peculiarities. Numer. Analys. Appl., vol. 11, iss. 1, pp. 4–15.
5. *Alekseev D. V. and Kazunina G. A.* Modelirovanie kinetiki nakopleniya povrejdenii veroyatnostnim kletochnim avtomatom [Modeling the of damage accumulation of probabilistic cellular automata]. Fizika Tverdogo Tela, 2006, vol. 48, no. 2, pp. 255–261. (in Russian)
6. *Alekseev D. V., Kazunina G. A., and Cherednichenko A. V.* Kletochno-avtomatnoe modelirovanie prozessa razrushetiya hrupkih materialov[Cellular automaton simulation of the fracture process for brittle materials]. Prikladnaya Diskretnaya Matematika, 2015, no. 2 (28), pp. 103–118. (in Russian)
7. *Lobanov A. I.* Modelirovanie kletochnykh avtomatov [Model of cellular automata]. Computer Research and Modeling, 2010, vol. 2, iss. 3, pp. 273–293. (in Russian)

8. *Matyushkin I. V. and Zapletina M. A.* Obzor po tematike kletochnikh avtomatov na baze sovremennykh otechestvennykh publikatsciy [Review on the subject of cellular automata on the basis of modern Russian publications]. Computer Research and Modeling, 2019, vol. 11, no. 1, pp. 9–57. (in Russian)
9. *Tarasevich Yu. Yu.* Perkolyaciya: teoriya, prilojeniya, algoritmi [Percolation: theory, applications, algorithms]. Moscow, Librokom Publ., 2018. 112 p. (in Russian)
10. *Moskalev P. V.* Analiz struktury perkolayzhionnogo klastera [Analysis of the percolation cluster structure]. J. Tehnicheskoi Fiziki, 2009, vol. 79, no. 6, pp. 2–7. (in Russian)
11. *Moskalev P. V.* Struktura modeli perkolayzionnih uzlo na trehmernih kvadratnix rehsetkah [The structure of site percolation models on three-dimensional square lattices]. Computer Research and Modeling, 2013, vol. 5, no. 4, pp. 607–622. (in Russian)
12. *Alexandrowicz Z.* Critically branched chains and percolation clusters. Phys. Lett. A, 1980, vol. 80, no. 4, pp. 284–286.
13. *Leath P.* Cluster size and boundary distribution near percolation threshold. Phys. Rev. B, 1976, vol. 14, no. 11, pp. 5046–5055.
14. *Alekseev D. V. and Kazunina G. A.* Soputstvuyushchaya klasternaya struktura, obrazuyushchayasya pri generatsii perkolyatsionnogo klastera po algoritmu Khammersli — Lisa — Aleksandrovitsa [Concomitant clusters structure creating by percolation cluster generating Hammersley — Leath — Alexandrowichz algorithm]. Aktualnie Napravleniya Nauchnih Issledovanii XXI Veka: Teorya i Praktika, 2018, no 6 (42), pp. 18–20. (in Russian)
15. *Alekseev D. V.* Vvedenie v kompyuternoe modelirovanie fizicheskih zadach: ispolzovanie MicrosoftVisualBasic [An Introduction to Computer Simulation Physical Systems: Using MicrosoftVisualBasic]. Moscow, LENAND Publ., 2019. 272 p. (in Russian)

СВЕДЕНИЯ ОБ АВТОРАХ

АЛЕКСЕЕВ Дмитрий Валентинович — доктор технических наук, профессор, г. Кемерово. E-mail: **dmitryalekseev@live.ru**

АЛЕХИНА Марина Анатольевна — доктор физико-математических наук, профессор, заведующая кафедрой математики и физики Пензенского государственного технологического университета, г. Пенза. E-mail: **alekhina@penzgtu.ru, alekhina.marina19@yandex.ru**

БАРСУКОВА Оксана Юрьевна — кандидат физико-математических наук, доцент кафедры компьютерных технологий Пензенского государственного университета, г. Пенза. E-mail: **oksana.barsukova.71@gmail.com**

ВОБЛЫЙ Виталий Антониевич — доктор физико-математических наук, ведущий научный сотрудник Всероссийского института научной и технической информации РАН, г. Москва. E-mail: **vitvobl@yandex.ru**

ГОРОДИЛОВА Анастасия Александровна — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, старший преподаватель кафедры теоретической кибернетики ММФ Новосибирского государственного университета, г. Новосибирск. E-mail: **gorodilova@math.nsc.ru**

ДРОНОВ Сергей Вадимович — кандидат физико-математических наук, доцент, доцент Алтайского государственного университета, г. Барнаул.
E-mail: **dsv@math.asu.ru**

КАЗУНИНА Галина Алексеевна — доктор технических наук, доцент, профессор кафедры математики Кузбасского государственного технического университета им. Т. Ф. Горбачёва, г. Кемерово. E-mail: **gt-kga@yandex.ru**

МИГОВ Денис Александрович — кандидат физико-математических наук, старший научный сотрудник Института вычислительной математики и математической геофизики СО РАН, г. Новосибирск. E-mail: **mdinka@rav.sscc.ru**

МОНАХОВА Эмилия Анатольевна — кандидат технических наук, доцент, старший научный сотрудник Института вычислительной математики и математической геофизики СО РАН, г. Новосибирск. E-mail: **emilia@rav.sscc.ru**

ПОТТОСИН Юрий Васильевич — кандидат физико-математических наук, доцент, ведущий научный сотрудник Объединённого института проблем информатики НАН Беларуси, г. Минск. E-mail: **pott@newman.bas-net.by**

РЫБАЛОВ Александр Николаевич — кандидат физико-математических наук, старший научный сотрудник лаборатории комбинаторных и вычислительных методов алгебры и логики Института математики им. С. Л. Соболева СО РАН, г. Омск.
E-mail: **alexander.rybalov@gmail.com**

ШОЛОМОВ Лев Абрамович — доктор физико-математических наук, профессор, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук, г. Москва. E-mail: **levshol@mail.ru**