ИЗВЕСТИЯ РАН. ТЕОРИЯ И СИСТЕМЫ УПРАВЛЕНИЯ, 2021, № 1, с. 73–78

КОМПЬЮТЕРНЫЕ МЕТОДЫ

УДК 519.175.3, 519.179.1, 519.72

АЛГОРИТМ ПЕРЕДАЧИ МНОГОМЕРНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ЭКСТРЕМАЛЬНЫХ ОДНОРОДНЫХ ГИПЕРГРАФОВ[1]

© 2021 г. Е. К. Егорова[a,b], А. В. Мокряков[a,b,*], А. А. Суворова[a], В. И. Цурков[c]

[a] *МАИ (национальный исследовательский ун-т), Москва, Россия*

[b] *РГУ им. А.Н. Косыгина, Москва, Россия*

[c] *ФИЦ ИУ РАН, Москва, Россия*

**e-mail: MokryakovAlVik@gmail.com*

Поступила в редакцию 09.06.2020 г.
После доработки 14.06.2020 г.
Принята к публикации 27.07.2020 г.

В последнее время беспилотные летательные аппараты все чаще применяются для разведки в боевых условиях. Связь с беспилотными летательными аппаратами должна проводиться в конфиденциальном режиме для защиты от перехвата управления, при этом быть быстрой и стойкой к атакам извне. Предлагается новый алгоритм передачи конфиденциальных данных, основанный на свойствах экстремальных однородных гиперграфов.

DOI: 10.31857/S0002338821010054

Введение. В работе рассматриваются вопросы передачи конфиденциальных данных с помощью одного из обобщений минимакса при транспортных ограничениях [1]. Сам минимакс имеет ряд обобщений [2, 3]. Здесь мы воспользуемся одним из них – гиперграфом [4]. Частным случаем гиперграфа является граф. Возможность использования графов для передачи конфиденциальных данных предполагал Клод Шеннон [5]. В современных исследованиях некоторые методы передачи защищенных данных применяют графы в качестве вспомогательных структур, например для работы с ключами или при анализе данных перед обработкой [6]. Также существуют методы, где граф является основным актором преобразования данных. В [7] основой для изменения данных выступает изоморфизм графов. Авторы [8] описывают два симметричных алгоритма для создания многомерных преобразований на базе трех семейств двудольных графов с множествами разбиений, изоморфных $\mathbb{K}^n$, где $\mathbb{K}$ – конечное коммутативное кольцо.

Но в целом, работ, применяющих графы непосредственно, не очень много, так как трудно использовать граф в виде ключевого элемента. Это связано с тем, что небольшой граф можно получить простым перебором, а большой занимает существенный объем данных при передаче. Однако эти проблемы можно минимизировать, если применить экстремальные однородные гиперграфы. Это дает два преимущества.

1. Экстремальный однородный гиперграф можно однозначно задать посредством вектора степеней его вершин. Вектор занимает существенно меньший объем памяти, чем список гиперребер или матрица смежности.

2. С помощью гиперграфа можно увеличить стойкость метода, так как количество экстремальных гиперграфов с ростом числа вершин растет быстрее экспоненциального.

Далее опишем метод конфиденциальной передачи данных посредством экстремальных однородных гиперграфов.

1. Экстремальные однородные гиперграфы. Сначала необходимо дать некоторые определения.

[1] Работа выполнена при финансовой поддержке Минобрнауки России (уникальный идентификатор проекта RFMEFI60719X0312).

О п р е д е л е н и е 1. *Гиперграф* $H = H(V, E) = H(V_n, E)$ – совокупность множества из m вершин V_n и множества непустых подмножеств множества вершин E [9], e_i – элементы множества E, где $i = \overline{1,|E|}$ называются *гиперребрами* [4].

О п р е д е л е н и е 2. Гиперграф $H^k = H^k(V_n, E)$ называют k-*однородным* гиперграфом (uniform hypergraph (UH)), если $|e_i| = k$, $\forall e_i \in E$.

Ненаправленные графы без петель – частный случай k-однородных гиперграфов при $k = 2$. Если рассмотреть 3-однородные гиперграфы, то они известны под названием 2-комплексов [10]. Этот термин пришел из топологии [11].

В отличие от произвольных гиперграфов k-однородные гиперграфы можно представить в виде k-индексной матрицы смежности $X^k(H^k) = (x_{i_1 \ldots i_k})$, где индексы $i_j = \overline{1,n}$ при $j = \overline{1,k}$.

Среди всех k-однородных гиперграфов нас интересует определенное подмножество – экстремальные однородные гиперграфы. Пусть $\mathbb{Z}_+$ – множество неотрицательных целых чисел и n – количество координат вектора $\mathbf{A}$. Введем следующие обозначения: $\mathbb{Z}_+^n = \{\mathbf{A} = (a_1, \ldots, a_n) : a_i \in \mathbb{Z}_+ \ \forall i\}$ – множество неотрицательных n-координатных векторов и $\overline{\mathbb{Z}}_+^n = \{\mathbf{A} \in \mathbb{Z}_+^n : a_i \geq a_{i+1}, \forall i, i = \overline{1, n-1}\}$ – множество неотрицательных n-координатных векторов с упорядоченными по невозрастанию координатами.

О п р е д е л е н и е 3. *Реализацией* вектора $\mathbf{A} \in \mathbb{Z}_+^n$ в k-однородный гиперграф $H = H(\mathbf{A}) = H(V, E)$ называется такой гиперграф, что вектор степеней его вершин есть вектор $\mathbf{A}$.

Пусть вектор $\mathbf{A}$ из $\mathbb{Z}_+^n$ есть реализуемый в k-однородный гиперграф вектор и $\Gamma^k = \{H(\mathbf{A})\}$ – множество всех реализаций (с множеством вершин V_n).

О п р е д е л е н и е 4. Вектор $\mathbf{A}$ из $\mathbb{Z}_+^n$, где $n \geq 2$, называется k-*совершенным*, если $|\Gamma^k| = 1$. При этом единственная реализация $H(\mathbf{A})$ обозначается k-*совершенным однородным гиперграфом*.

Для определения экстремальности вектора (и гиперграфа) удобно перейти к вектору, координаты которого упорядочены по невозрастанию.

О п р е д е л е н и е 5. Вектор $\mathbf{A}$ из $\overline{\mathbb{Z}}_+^n$, где $n \geq 2$, называется k-*экстремальным*, если $\mathbf{A}$ – k-совершенный вектор. Единственная реализация $H(\mathbf{A})$ будет *экстремальным* k-*однородным гиперграфом*.

Основное преимущество использования экстремальных гиперграфов состоит в том, что между множеством k-экстремальных векторов и множеством экстремальных k-однородных гиперграфов установлено взаимно-однозначное соответствие. Кроме того, существуют быстрые редукционные алгоритмы восстановления k-экстремальных векторов в k-однородный гиперграф при $k = 2$ [12] и $k = 3$ [13].

Для создания экстремальных гиперграфов понадобится еще одно понятие – база [14] экстремального k-однородного гиперграфа.

Пусть $n, k \in \mathbb{Z}$, $k \geq 2$. Для множества индексов $I_n = \{i \in \mathbb{Z} : i = \overline{n}\}$ (номеров) введем обозначение k-индексных упорядоченных подмножеств множества I_n: $I_n^k = \{(i_1, \ldots i_k) : i_j = \overline{n}, \ i_j < i_{j+1} \ \forall j\}$. Определим на I_n^k частичный порядок: положим $(i_j : j = \overline{k}) \geq (m_j : j = \overline{k})$, если $i_j \geq m_j \ \forall j$, и $(i_j : j = \overline{k}) > (m_j : j = \overline{k})$ при $(i_j : j = \overline{k}) \geq (m_j : j = \overline{k})$ и $(i_j : j = \overline{k}) \neq (m_j : j = \overline{k})$.

Построим конструкцию, позволяющую алгебраическим способом описать экстремальный k-комплекс. Для $H^k = H^k(V_n, E)$ и $X^k(H^k) = (x_{i_1 \ldots i_k})$ зададим $I_n^k(H^k) = \{(i_1, \ldots, i_k) \in I_n^k : x_{i_1 \ldots i_k} = 1\} =$ $= \{(i_1, \ldots, i_k) \in I_n^k : \{v_{i_j} : j = \overline{k}\} \in E\}$.

О п р е д е л е н и е 6. Пусть $H^k(V_n, E)$ – непустой экстремальный k-однородный гиперграф ($E \neq \varnothing$), а $X^k(H^k) = (x_{i_1 \ldots i_k})$ – его матрица смежности. Подмножество индексов $\overline{I}_n^k(H^k) =$ $= \{(i_1, \ldots, i_k)\}$ из $\hat{I}_n^k$ называется *базой* для комплекса H^k, если выполняются следующие условия:

– для разных элементов $(i_1, \ldots, i_k)$ и $(m_1, \ldots, m_k)$ из $\overline{I}_n^k(H^k)$ отношение порядка в $\hat{I}_n^k(H^k)$ не определено;

– для $\forall(i_1,\ldots,i_k) \in \hat{I}_n^k(H^k)\backslash\bar{I}_n^k(H^k)$ существует такой $(m_1,\ldots,m_k) \in \bar{I}_n^k(H^k)$, что существует отношение частичного порядка: $(i_1,\ldots,i_k) < (m_1,\ldots,m_k)$.

Пример 1. Возьмем 4-экстремальный вектор $\mathbf{A} = (4,4,4,1,1,1,1)$. Построим его единственную реализацию $H^4 = H^4(V_7, E) = H^4(\mathbf{A})$, где множество гиперребер $E = \{\{v_1,v_2,v_3,v_4\},\{v_1,v_2,v_3,v_5\},$ $\{v_1,v_2,v_3,v_6\},\{v_1,v_2,v_3,v_7\}\}$. Следовательно, $\bar{I}_7^4(H^4) = \{(1,2,3,7)\}$.

Определение 7. Подмножество индексов $(m_1,\ldots,m_k)$ из $\hat{I}_n^k(H^k)$ (т. е. $x_{m_1\ldots m_k} = 1$) называется *максимальным*, если $x_{i_1\ldots i_k} = 0$, $\forall(i_1,\ldots,i_k) > (m_1,\ldots,m_k)$.

Теорема 1. База состоит из всех максимальных подмножеств индексов.

Теорема 2. Любой экстремальный k-однородный гиперграф $H^k = H^k(V_n, E)$ имеет единственную базу.

Теорема 3. Пусть $\tilde{I}_n^k = \{(i_1,\ldots,i_k) \in I_n^k\}$ и между элементами $\tilde{I}_n^k$ отсутствует отношение частичного порядка. Тогда $\tilde{I}_n^k$ – база некоторого экстремального k-однородного гиперграфа.

Из теорем 2 и 3 вытекает следующая теорема.

Теорема 4: k-однородный гиперграф H^k является экстремальным тогда и только тогда, когда H^k имеет базу.

Доказательство последних теорем не вызывает затруднений. Приведенные здесь алгоритмы будут расширением и уточнением работы [15], доложенной на конференции “Авиация и космонавтика-2019”.

2. Конфиденциальная передача данных с помощью экстремальных однородных гиперграфов. Для передачи данных нам потребуется ввести несколько переменных:

– $EUH_n^k = EUH_n^k(\mathbf{A}) = EUH_n^k(V_n, E)$ – экстремальный k-однородный гиперграф с множеством вершин V_n, и множеством гиперребер E;

– n – количество вершин гиперграфа EUH;

– N – общее количество данных для передачи (в байтах);

– k – размерность гиперграфа EUH;

– b – размер малого блока (в байтах);

– B – размер большого блока (в байтах).

Опишем непосредственно алгоритм действий.

Алгоритм 1. **Преобразование данных перед их передачей.** На вход подается N байт данных.

Шаг 1. Выбираем размер малого блока b, размерность гиперграфа k и количество вершин в нем n. Подсчитываем размер большого блока: $B = bn$.

Шаг 2. Разбиваем на $p = \lceil N/B \rceil$ больших блоков входной поток данных. Дописываем в последний блок с номером $t = pB - N$ следующие значения по одному в каждый малый блок: t, $t+1$, $t+2$, $t+3$, …, $2t-1$ (если заполнить одинаковыми значениями, то последний блок может быть менее устойчив к линейному перебору).

Шаг 3. Выбирается k-экстремальный вектор $\mathbf{A}$ требуемой размерности и соответствующий ему экстремальный k-однородный гиперграф $EUH_n^k(\mathbf{A})$ (алгоритм 2 далее).

Шаг 4. Формируем ключевой элемент в виде целочисленного массива из следующих переменных: b, t, p, k, n, вектор $\mathbf{A}$. Преобразуем ключевой элемент по одному из известных алгоритмов, например ГОСТ или AES.

Шаг 5. Передаем преобразованный ключ контрагенту.

Шаг 6. Устанавливаем $i = 1$.

Шаг 7. Выбираем большой блок B_i и изменяем его (алгоритм 3 далее).

Шаг 8. Передаем преобразованный большой блок контрагенту.

Шаг 9. Если рассматриваемый большой блок не последний ($i < p$), то переходим к следующему большому блоку ($i = i + 1$) и к шагу 7, иначе завершаем алгоритм.

Здесь задействованы вспомогательные алгоритмы выбора экстремального вектора и изменения большого блока данных.

Для построения гиперграфа и соответствующего ему вектора воспользуемся тем, что множество баз однозначно соответствует множеству экстремальных k-однородных гиперграфов (см. теорему 4).

Алгоритм 2. **Выбор вектора и** $EUH_n^k(\mathbf{A})$. На вход подается n и k.

Шаг 1. Формируем множество I_n^k, соответствующее множеству всех возможных одноэлементных баз, в этом множестве есть C_n^k элементов.

Шаг 2. Устанавливаем результирующий n-координатный вектор $\mathbf{A} = 0$.

Шаг 3. Выбираем случайным образом от n до n^2 количество итераций выбора вектора: n_c.

Шаг 4. Выбираем случайным образом базу из множества I_n^k и уменьшаем n_c на единицу.

Шаг 5. Получаем вектор $\mathbf{A}_{n_c}$ из выбранной базы.

Шаг 6. Выполняем операцию объединения векторов $\mathbf{A}$ и $\mathbf{A}_{n_c}$ по правилу, описанному в работе [16].

Шаг 7. Если $n_c > 0$, то переходим к шагу 4.

Шаг 8. Результирующий вектор устанавливаем как вектор $\mathbf{A}$.

Шаг 9. По редукционному алгоритму восстанавливаем искомый гиперграф [10, 12, 18, 17].

Отдельно опишем алгоритм для непосредственного изменения большого блока.

Алгоритм 3. **Преобразование большого блока.** На вход передается b, n, k и выбранный $EUH_n^k(\mathbf{A})$.

Шаг 1. Разбиваем большой блок на n малых блоков (обозначим их s) с нумерацией от 1 до n. Устанавливаем взаимно-однозначное соответствие между вершинами выбранного гиперграфа и малыми блоками.

Шаг 2. Устанавливаем $j = 1$.

Шаг 3. Выделяем в гиперграфе подмножество вершин, имеющих общее гиперребро с j-той вершиной гиперграфа, и чей номер больше j: $M_j = \{v_{tj}\}$, где v_{tj} – вершина v_t инцидентная вершине j и $t > j$.

Шаг 4. Находим $Y = \bigoplus_i s_i$, где i такой, что $v_{ij} \in M_j$.

Шаг 5. Изменяем j блок: $s_j = s_j \oplus Y$.

Шаг 6. Изменяем другие блоки: $s_i = s_i \oplus Y$, где i такой, что $v_{ij} \in M_j$.

Шаг 7. Если $j < n - k$, то увеличиваем j на 1 и переходим к шагу 3.

Полученный блок в результате работы алгоритма 3 легко восстановить в первоначальный вариант, если знать структуру использованного гиперграфа.

3. Получение исходных данных. Для этого нужно по вектору построить однородный гиперграф, а затем выполнить процесс преобразования блока данных с помощью функции, обратной к функции из алгоритма 3.

Алгоритм 4. **Обратное преобразование блока данных.** Входными данными являются ключевой элемент, восстановленный по методу, использованному в шаге 4 алгоритма 1, и данные, измененные по алгоритму 1. Ключевой элемент состоит из переменных b, t, p, k, n и вектора $\mathbf{A}$. Данные могут поступать по одному большому блоку или потоком, что несущественно для алгоритма. Поэтому в рамках алгоритма предполагаем, что каждый раз разбирается очередной большой блок данных.

Шаг 1. Восстанавливаем k-однородный гиперграф по одному из известных редукционных алгоритмов [10, 12, 18, 17].

Шаг 2. Устанавливаем $j = n - k$.

Шаг 3. Выделяем в гиперграфе подмножество вершин, инцидентных j-той вершине гиперграфа, объединяем множество вершин, связанных с первой вершиной $M_j = \{v_{tj}\}$, где v_{tj} – вершина v_t, инцидентная вершине j и $t > j$.

Шаг 4. Изменяем блоки: $s_i = s_j \oplus s_i$, где i такой, что $v_{ij} \in M_j$.

Шаг 5. Находим $Y = \bigoplus_i s_i$, где i такой, что $v_{ij} \in M_j$.

Таблица 1. Зависимость $|EUH_n^3|$ от количества вершин

n	$N = \|EUH_n^3\|$	$(\ln N)/n$
3	1	0.000
4	4	0.347
5	15	0.542
6	65	0.696
7	351	0.837
8	2430	0.974
9	21759	1.110
10	252585	1.244
11	3803647	1.377
12	74327144	1.510
13	1885102079	1.643
14	62062015499	1.775
15	2652584509439	1.907
16	147198472495019	2.039

Ш а г 6. Изменяем j блок: $s_j = s_j \oplus Y$.

Ш а г 7. Если $j > 1$, то уменьшаем j на 1 и переходим к шагу 3.

Если $t \neq 0$, то необходимо последние t байтов убрать из последнего большого блока.

4. Устойчивость алгоритма к атакам. Защита от атак на этот метод преобразования данных базируется на двух вещах. Во-первых, защита ключевого элемента проводится с помощью известного стойкого алгоритма, т.е. гиперграф злоумышленнику. Во-вторых, защита обуславливается мощностью множества экстремальных k-однородных гиперграфов. Рассмотрим экстремальные 2-однородные гиперграфы: $|EUH_n^2| = 2^{n-1}$. Легко видеть, что стойкость алгоритма, сравнимая с AES128, достигается только на 129 вершинах ($|EUH_2^{129}| = 2^{128}$). Это приводит к тому, что ключ становится больше, как и время работы редукционного алгоритма, что не позволяет в реальных приложениях базироваться на преобразовании с помощью EUH_n^2.

Обратимся к случаю $k = 3$. Рост количества таких гиперграфов на n вершинах быстрее экспоненциального. Этого легко видеть на основе следующего ряда (таблица), полученного экспериментальным способом. В третьем столбце мы видим функцию, демонстрирующую рост $|EUH_n^3|$ выше экспоненциального. При этом если данную функцию экстраполировать, то можем получить $|EUH_{28}^3| \approx 10^{44}$, что существенно больше $2^{128} \approx 3.4 \times 10^{38}$. Таким образом каждый вектор на 28 вершинах содержит больше информации, чем 128-битное число.

Можно задаться вопросом о длине записи вектора **A**, состоящего из 28 степеней вершин. Максимальная степень вершины при $k = 3$, $n = 28$ равна $C_{n-1}^{k-1} = C_{27}^2 = 351$. Так как $2^8 < 351 < 2^9$, то для записи одной степени вершины достаточно 9 бит, для всех 28 вершин необходимо $28 \cdot 9 = 252$ бита. Более точная оценка: $28 \log_2 351 = 237$ бит.

В работе [17] рассматривается общая формула мощности, которая полностью не определена, но имеет следующий общий вид:

$$|EUH_n^3| = \sum_{i=1}^{\lceil n(n-2)/8 \rceil} \sum_q a_q C_{n+l_q}^{3i}, \tag{4.1}$$

где q, l_q, a_q – целочисленные коэффициенты, нелинейно зависящие от n. Это позволяет при сравнительно небольшом количестве вершин получить надежный, устойчивый к линейному перебору ключ, т.е. подобрать его за разумное время не представляется возможным. Также отметим, что при использовании гиперграфов большего порядка стойкость возрастает аналогично

формуле (1), только верхняя граница первой суммы будет больше (предположительно сравнимо с n^k), также в числе сочетаний 3 заменяется на k.

Заключение. Сформулируем главный вопрос, возникающий при работе с данным алгоритмом: чем данный метод лучше, чем известные методы, например AES или ГОСТ?

Главное преимущество рассматриваемого алгоритма состоит в том, что он исполняется быстрее. Например, для преобразования большого блока потребуется выполнить не более чем $(n-1)(n-k)$ операций побитового XOR. Таким образом, при условии использования параметров $b = 1$, $k = 3$ и $n = 32$ потребуется не более 900 операций. В AES128, к примеру, требуется выполнить более 1600 операций для блока длиной 32 байта. Кроме того, редукционный алгоритм восстановления k-однородного гиперграфа является полиномиальным и имеет сложность $O(n^{k-1})$, что также не сильно усложняет процесс получения изначальных данных, так как выполняется единственный раз при начале процесса преобразования или восстановления данных. Стоит отметить, что для рассмотренного алгоритма существует большое пространство для модификаций и улучшений и их изучение – дело дальнейших исследований.

СПИСОК ЛИТЕРАТУРЫ

1. *Mironov A.A.* Minimax under Transportation Constraints Dordrecht: Kluwer Acad. Publ., 1999. 309 p.
2. *Mironov A.A., Tsurkov V.I.* Network Models with Fixed Parameters at the Communication Nodes. 1 // J. Computer and Systems Sciences International. 1995. V. 33. № 3. P. 107–116.
3. *Mironov A.A., Tsurkov V.I.* Network Models with Fixed Parameters at the Communication Nodes. 2 // J. Computer and Systems Sciences International. 1994. V. 32. № 6. P. 1–11.
4. *Зыков А.А.* Гиперграфы // УМН. 1974. Т. XXIX. № 6 (180). С. 89–154.
5. *Moore E.F., Shannon C.E.* Reliable circuits using less reliable relays // J. Franklin Institute. 1956. V. 262. № 4. P. 281–297.
6. *Фомичев В.М., Авезова Я.Э., Коренева А.М., Кяжин С.Н.* Примитивность и локальная примитивность орграфов и неотрицательных матриц // Дискретный анализ и исследование операций. 2018. Т. 25. № 3 (137). С. 95–125.
7. *Ustimenko V., Romańczuk-Polubiec U., Wróblewska A., Polak M.K., Zhupa E.* On the Constructions of New Symmetric Ciphers Based on Nonbijective Multivariate Maps of Prescribed Degree // Security and Communication Networks. 2019. 2137561.
https://doi.org/10.1155/2019/2137561
8. *Пролубников А.В., Файзуллин Р.Т.* Шифрование видеоизображений с помощью шифра двойной перестановки // Изв. Челябинск. научн. центра УрО РАН. 2004. № 1. С. 17–21.
9. *Ванг Л., Егорова Е.К., Мокряков А.В.* Развитие теории гиперграфов // Изв. РАН. ТиСУ. 2018. 1. С. 111–116.
10. *Mironov A.A., Mokryakov A.V., Sokolov A.A.* About Realization of Integer Non-Negative Numbers Tuple into 2-Dimensional Complexes // Applied and Computational Mathematics. 2007. V. 6. № 1. P. 58–68.
11. *Александров П.С.* Комбинаторная топология. М.: Гостехтеориздат, 1947. 660 с.
12. *Миронов А.А.* Геометрия точек пространства R^n, реализуемых в граф // УМН. Т. XXXII. № 6 (198). 1977. С. 232–233.
13. *Мокряков А.В., Цурков В.И.* Восстановление 2-комплексов по целочисленному неотрицательному вектору // АиТ. 2011. № 12. С. 130–143.
14. *Мокряков А.В.* Представление гиперграфов в качестве алгебраической структуры // Изв. РАН. ТиСУ. 2011. № 5. С. 53–59.
15. *Егорова Е.К., Мокряков А.В., Суворова А.А.* Концепция шифрования данных с помощью экстремальных однородных гиперграфов // Тез. докл. 18-й Междунар. конф. “Авиация и космонавтика-2019”. М.: МАИ (НИУ), 2019. С. 98–99.
16. *Егорова Е.К., Есенков А.С., Мокряков А.В.* Операции над k-однородными гиперграфами и их векторы степеней вершин // Изв. РАН. ТиСУ. 2020. № 3. С. 75–80.
17. *Мокряков А.В., Селин П.С., Цурков В.И.* Минимакс и восстановление по вектору в графах. М.: Физматлит, 2017. 309 с.
18. *Костяной Д.С., Мокряков А.В., Цурков В.И.* Алгоритмы восстановления гиперграфов по заданному вектору степеней вершин // Изв. РАН. ТиСУ. 2014. № 4. С. 43–48.