n	Среднее отклонение от минимума
10	5,13%
11	5,223%
12	4,904%
13	5,932%
14	6,339%
15	4,415%
16	4,497%
17	4,267%
18	3,552%
19	4,231%

Согласно приведенным выше результатам применение алгоритма комбинации позволило улучшить значение критерия в среднем на $4,849\%$ по сравнению с выбором минимума.

Список литературы

1. Афраймович Л. Г., Емелин М. Д. Комбинирование решений аксиальной задачи о назначениях // АиТ. — 2021. — № 8. — С. 159–168.

2. Spieksma F. C. R. Multi Index Assignment Problems. Complexity, Approximation, Applications // Nonlinear Assignment Problems: Algorithms and Applications. — Dordrecht: Kluwer Acad. Publishers, 2000. — P. 1–11.

DOI: 10.20948/dms-2022-46

СПОСОБЫ ПОСТРОЕНИЯ И РАЗЛИЧЕНИЯ 5-КОФИГУРАЦИЙ

М. М. Комягин, Ф. М. Малышев (Москва)

Понятие k-конфигурации важно в связи с использованием их матриц инциденций (k-матриц) в алгоритмах шифрования. Определение k-конфигурации использует сложение множеств, задаваемое правилом $A + B = (A \cup B) \setminus (A \cap B)$.

Определение. Совокупность $\mathcal{X} \subset 2^X$ из v подмножеств мощности k в множестве X, $|X| = v$, называем k-конфигурацией, если:

i) каждый элемент $x \in X$ принадлежит ровно k подмножествам из $\mathcal{X}$,

ii) каждый элемент $x \in X$ является суммой (как подмножество $\{x\}$) ровно k подмножеств из $\mathcal{X}$, причём каждое подмножество из $\mathcal{X}$ участвует в качестве слагаемого ровно в k таких суммах.

Когда важен размер v, говорим о (v, k)-конфигурациях. Называем k-конфигурацию неразложимой, если образованный ею гиперграф связен. В обзорной работе [1] приводится

Теорема. *При любых чётном v и нечётном k, $0 < k < v$, существует неразложимая (v, k)-конфигурация. Если при нечётных v и k существует (v, k)-конфигурация, то $v \geqslant k + (1 + \sqrt{4k-3})/2$. Для $k \leqslant 17$ и всех $v \geqslant k+(1+\sqrt{4k-3})/2$ существует (v, k)-конфигурация за исключением $k = 3$, $v = 7$, когда её не существует.*

При $v = 2w$, $w \geqslant 2$, $(v, 3)$-конфигурация состоит из подмножеств в группе вычетов по $\bmod v$ вида $\{2i, 2i+1, 2i+2\}$, $\{2i, 2i+1, 2i+3\}$, $i = 0, 1, \ldots, w-1$ [1]. Класс 5-конфигураций оказался существенно богаче. В известных примерах 5-конфигураций задействован весь спектр средств, привлекавшихся ранее для построения k-конфигураций, включая правильные многогранники, регулярные и симметрические графы, квадратичные вычеты по простому модулю, конечные группы, (v, k, λ)-конфигурации, включая конфигурации, которые отвечают совершенным разностным множествам, конечным проективным плоскостям и матрицам Адамара. Но для $v > 12$ известные к настоящему времени $(v, 5)$-конфигурации изоморфны 5-конфигурациям приводимых ниже трёх бесконечных серий.

Под 2-графом Γ будем понимать связный ориентированный граф на конечном множестве вершин V без петель и параллельных дуг с двумя входящими и двумя выходящими дугами для каждой вершины. Граф Γ в виде ориентированного цикла естественно считать 1-графом. Концы дуг, выходящих из вершины $v \in V$ 2-графа Γ, обозначаем v_0 и v_1, а для 1-графа — v_0.

Серия $\mathcal{A}$. Пусть Γ — 2-граф с множеством вершин V. Полагаем $X = V \times \{0, 1\}$, $X_x = \{(v, \varepsilon), (v_0, 0), (v_0, 1), (v_1, 0), (v_1, 1)\}$, $x = (v, \varepsilon) \in V \times \{0, 1\}$, $\mathcal{X} = \{X_x | \, x \in X\}$.

Серия $\mathcal{B}$. Пусть Γ — 2-граф с множеством вершин V, у которого дуги помечены либо 0 либо 1 так, что как входящие, так и выходящие дуги каждой вершины $v \in V$ помечены различно. Через v_ε обозначаем конец дуги, выходящей из вершины $v \in V$, помеченной как $\varepsilon \in \{0, 1\}$. Требуется $(v_0)_1 = (v_1)_0$ для всех $v \in V$. Полагаем $X =$

$V\times\{0,1\}\times\{0,1\}$, $X_x=\{(v,\varepsilon,\nu),(v_0,0,\nu),(v_0,1,\nu),(v_1,\varepsilon,0),(v_1,\varepsilon,1)\}$, $x=(v,\varepsilon,\nu)\in V\times\{0,1\}\times\{0,1\}$, $\mathcal{X}=\{X_x|\,x\in X\}$.

Серия $\mathcal{C}$. Пусть Γ — 1-граф с множеством вершин V. Полагаем $X=V\times\{0,1,2\}$, $X_x=\{(v,0),(v,1),(v,2),(v_0,\nu),\ \nu\in\{0,1,2\}\diagdown\{\varepsilon\}\}$, $x=(v,\varepsilon)\in V\times\{0,1,2\}$, $\mathcal{X}=\{X_x|\,x\in X\}$.

Имеем $\{x\}=\sum_{y\in X_x}X_y$, $x\in X$, для серий $\mathcal{A}$, $\mathcal{B}$ и $\{x\}=\sum_{y\in X:\,x\in X_y}X_y$ для серии $\mathcal{C}$.

Теорема. *Любые две 5-конфигурации, принадлежащие различным сериям $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, не изоморфны друг другу.*

Для доказательства этой теоремы достаточно рассматривать для каждого $y\in X$ спецификации частот встречаемости различных элементов из объединения $Y_y=\cup_{x\in X:\,y\in X_x}X_x$. Для 5-конфигураций серии $\mathcal{C}$ это $2^64^25^1$. Для $z\in X$ величину $\iota(z,y)=|\{x\in X|\,y\in X_x$ и $z\in X_x\}|$ назовём кратностью точки z по отношению к y, $\iota(y,y)=5$. Если $y=(v,\varepsilon)$ в конфигурации серии $\mathcal{A}$, то $\iota((v,\bar\varepsilon),y)=4$. Здесь $\{\varepsilon,\bar\varepsilon\}=\{0,1\}$. Для $u\in V\diagdown\{v\}$ имеем $\iota((u,o),y)=\iota((u,1),y)$, поэтому $|\{x\in X|\,\iota(x,y)=4\}|$ — нечётно. Осталось проверить, что 5-конфигураций серии $\mathcal{B}$ кратность 4 невозможна. Действительно, если $y=(v,\varepsilon,\nu)$ и $u_0=w_1=v$, u, $w\in V$, то $y\in X_{(u_0,0,\nu)}\cap X_{(u_0,1,\nu)}\cap X_{(u_1,\varepsilon,0)}\cap X_{(u_1,\varepsilon,1)}$ и в этих 4-х 5-подмножествах каждое $x\in X\diagdown\{y\}$ встречается не более 2-х раз, поэтому с учётом 5-го 5-подмножества $X_y\ni y$ заведомо $\iota(x,y)\leqslant 3$ для всех $x\in X\diagdown\{y\}$.

Теорема. *Две 5-конфигурации серии $\mathcal{A}$ изоморфны тогда и только тогда, когда изоморфны соответствующие им 2-графы.*

Эта теорема будет доказана, если по 5-конфигурации серии $\mathcal{A}$ сможем однозначно восстановить соответствующий 2-граф. Для этого достаточно восстановить разбиение множества точек X на пары вида $\{(v,0),(v,1)\}$, $v\in V$. Снова для каждого $y\in X$ рассмотрим частоты $\iota(x,y)$, $x\in X$. Пусть $y=(v,\varepsilon)$. Тогда $\iota((v,\bar\varepsilon),y)=4$. Если кратность 4 окажется только у одной точки из Y_y, то точка $(v,\bar\varepsilon)$ будет определена. Поскольку $\sum_{x\in X}\iota(x,y)=5\times 5$, то кратность 4 может быть ещё у двух или четырёх точек из Y_y. В последнем случае имеем $|V|=3$, а на трёх вершинах возможен один 2-граф. Пусть $\iota(y_i,y)=4$, $i=1,2,3$, $\{y_1,y_2,y_3\}=\{(v,\bar\varepsilon),(w,0),(w,1)\}$, $w\in V\diagdown\{v\}$. Обозначим $\bar y=(v,\bar\varepsilon)$. Заметим, что $Y_{\bar y}=Y_y$ и $\iota(z,y)=\iota(z,\bar y)$ для всех $z\in X\diagdown\{y,\bar y\}$. При нарушении одного из равенств $Y_{y_i}=Y_{y_j}$, $\iota(z,y_i)=\iota(z,y_j)$, $z\in X\diagdown\{y_i,y_j\}$, $1\leqslant i<j\leqslant 3$, вершина (v,ε) определяется.

Пусть далее $Y_{y_1}=Y_{y_2}=Y_{y_3}=Y_y$, $y_0=y$, $\iota(y_i,y_j)=4$,

$\iota(z, y_i) = \iota(z, y_j)$, $z \in X \setminus \{y_i, y_j\}$ $0 \leqslant i < j \leqslant 3$. Такое возможно либо при отсутствии в графе Γ дуг (v, w) и (w, v), либо при наличии их обеих. При их наличии в Γ будут вершины u', u'' и дуги (u', v), (u', w), (v, u''), (w, u''). При отсутствии дуг (v, w), (w, v) должны быть вершины u'_0, u'_1, u''_0, u''_1 и дуги (u'_0, v), (u'_1, v), (u'_0, w), (u'_1, w), (v, u''_0), (v, u''_1), (w, u''_0), (w, u''_1), причём возможны равенства $u'_0 = u''_0$, $u'_1 = u''_1$. Если этих равенств нет, или имеет место только одно из них, как и при наличии дуг (v, w), (w, v), как бы не разбивали четвёрку точек $\{y, y_1, y_2, y_3\}$ на пары, будем получать изоморфные 2-графы и одну и ту же 5-конфигурацию. Если $u'_0 = u''_0$ и $u'_1 = u''_1$, то в 2-графе Γ будет только 4 вершины. Таких 2-графов только два, как и 5-конфигураций на 8 вершинах только две, получающиеся инвертированием элементов матриц инциденций разложимой и не разложимой $(8, 3)$-конфигурации. Теорема полностью доказана.

Теорема. *Имеется ровно* 22 *попарно не изоморфных* 2*-графа с множеством вершин мощности* 6.

Кроме 22 различных $(12, 5)$-конфигураций, отвечающих 2-графам на 6 вершинах, к настоящему времени построено несколько сотен не изоморфных друг дружке $(12, 5)$-конфигураций.

Поскольку $(6, 5)$- и $(8, 5)$-матрицы получаются соответственно инвертированием элементов подстановочных и $(8, 3)$-матриц, а $(7, 5)$-матриц не существует, значение $v = 9$ является минимальным, для которого задача построения $(v, 5)$-конфигураций не тривиальна.

Теорема. *Любая* $(9, 5)$*-конфигурация изоморфна конфигурации серии* $\mathcal{C}$*. Имеется* 34 *различных* $(10, 5)$*-конфигураций и* 540 *различных* $(11, 5)$*-конфигураций.*

Эта теорема была доказана с помощью компьютерных вычислений. Главная сложность состояла в исключении 5-конфигураций, изоморфных ране полученным.

Список литературы

1. Малышев Ф. М. k-конфигурации // Труды МИАН. — 2022. — 316. — С. 233–253.

DOI: 10.20948/dms-2022-47