Экстремальные комбинаторные конфигурации и совершенные раскраски графов

В. Н. Потапов

семинар "Геометрическая теория функций", 20 февраля 2024 г.

Совершенная раскраска

Пусть $\{1, \ldots, k\}$ — множество из k цветов. Раскраской вершин графа $G = (V, E)$ называется функция $f : V \to \{1, \ldots, k\}$.
Для каждой вершины $x \in V(G)$ определим окрестность вершины (единичную сферу с центром в вершине) следующим образом: $U_1(x) = \{y \in V \mid \{x, y\} \in E\}$. Множество $U_1(x)$ состоит из вершин смежных с вершиной x.
Пусть $f(x) = i$, обозначим $s_{ij}(x) = |U_1(x) \cap f^{-1}(j)|$.

Определение

Раскраска называется совершенной, если величина $s_{ij}(x) = s_{ij}$ не зависит от выбора вершины x цвета i.

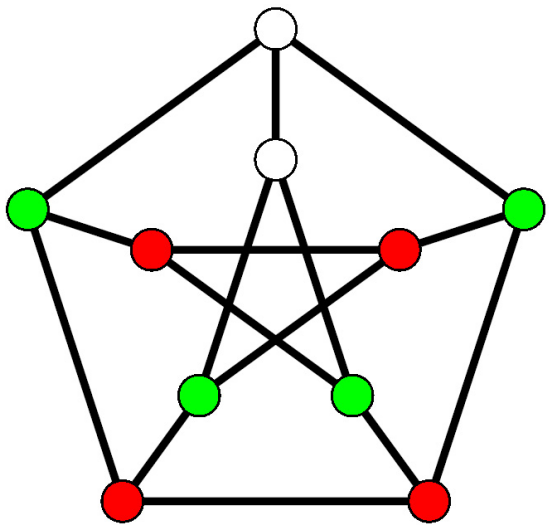
Совершенная раскраска

Определение

Матрицей параметров совершенной раскраски называется матрица

$$S_{k\times k} = (s_{ij})$$

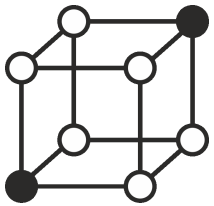
Совершенная раскраска графа Петерсена, порядок цветов: белый, зелёный, красный.



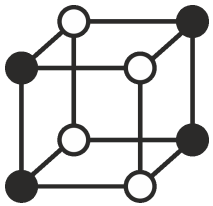
$$S = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

Совершенная раскраска

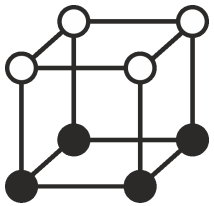
Совершенные раскраски булева куба в 2 цвета. Первому цвету соответствует черный цвет, второму — белый.



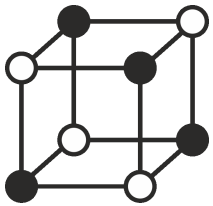
$$S = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$$



$$S = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$



$$S = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$



$$S = \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}$$

частные случаи совершенных раскрасок

- дистанционно регулярные графы
- накрытия графов
- трансверсали и 1-факторы гиперграфов
- комбинаторные дизайны
- латинские квадраты и ортогональные системы
- ассоциативные схемы
- разностные множества
- факторизации групп и замощения
- полностью регулярные коды, совершенные коды, МДР-коды
- бент-функции и корреляционно-иммунные функции

Границы

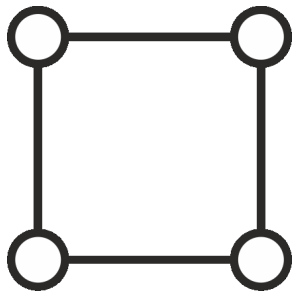
- Хэмминга
- Синглтона
- Дельсарта – Хоффмана
- Хемерса
- Бирбрауэра – Фридмана
- Фон-дер-Флаасса

матрица смежности графа

Матрица смежности графа $G = (V, E)$ определена равенством

$$M_{n\times n}(G) = (m_{ij}) = \begin{cases} 1, \text{ если } (v_i, v_j) \in E(G); \\ 0, \text{ иначе.} \end{cases}$$

Собственные функции и собственные числа графа — это собственные вектора и собственные числа его матрицы смежности.

Цикл на четырех вершинах  имеет следующую матрицу смежности

$$M = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

матричное уравнение

Пусть $f : V(G) \to \{1, \ldots, k\}$ — раскраска графа. Рассмотрим матрицу F размера $n \times k$, у которой столбец F_i является характеристической функцией цвета i.

Лемма

Пусть M — матрица смежности графа G. Функция f является совершенной раскраской графа G с матрицей параметров S тогда и только тогда, когда $MF = FS$.

Следствие

Функция f является совершенной 2-раскраской регулярного связного графа G тогда и только тогда, когда при некоторых α и c функция $\alpha f + c$ является собственной функцией графа G.

разрез графа

Пусть A и B подмножества вершин в простом графе G. Определим величину $e(A,B) = |\{(a,b) \in E(G) : a \in A, b \in B\}|$ — число рёбер, соединяющих вершины из множества A с вершинами из множества B, причём если $a, b \in A \cap B$, то ребро $\{a,b\}$ считается дважды. Заметим, что $e(A,B) = (\mathbf{1}_A, M\mathbf{1}_B)$, где M — матрица смежности графа G.

Определение

Разрезом графа G называется пара множеств вершин $A \subset V(G)$ и $B = V(G) \setminus A$ или множество рёбер между ними, величиной разреза называется число $e(A,B)$.

expander mixing lemma

Теорема [expander mixing lemma N. Alon, F. R. K. Chung 1988, K. Devriendt, P. Van Mieghem 2019]

Пусть G — r-регулярный связный граф и λ — максимальное по модулю, за исключением r, собственное число его матрицы смежности M. Тогда для любых подмножеств вершин A и B справедливо неравенство

$$|e(A,B) - \frac{r|A||B|}{|V(G)|}| \leq |\lambda| \sqrt{|A||B|(1-|A|/|V(G)|)(1-|B|/|V(G)|)}.$$

Причём, если в неравенстве достигается равенство, то $\mathbf{1}_A$ — совершенная раскраска с собственным числом λ и $B = A$ или $B = V(G) \setminus A$.

Теорема [N. Alon, V. Milman 1986, Tanner 1984, Golubev 2020]

Пусть G — r-регулярный связный граф и $\lambda_k < \lambda_{k-1} < \cdots < \lambda_1 < \lambda_0 = r$ — собственные числа его матрицы смежности M. Пусть $A \subset V(G)$, $B = V(G) \setminus A$. Тогда справедливы неравенства

$$\frac{(r-\lambda_1)|A||B|}{|V(G)|} \leq e(A,B) \leq \frac{(r-\lambda_k)|A||B|}{|V(G)|}.$$

Причём, если для некоторого множества A в одном из неравенств достигается равенство, то его характеристическая функция есть совершенная раскраска.

Теорема [Haemers 1979]

Пусть G — r-регулярный связный граф и $\lambda_k < \lambda_{k-1} < \cdots < \lambda_1 < \lambda_0 = r$ — собственные числа его матрицы смежности M. Пусть $C \subset V(G)$, $C \neq V(G)$ и $e(C, C)$ — удвоенное число пар смежных вершин в множестве C. Тогда справедливы неравенства

$$\lambda_k |C| + \frac{(r - \lambda_k)|C|^2}{|V(G)|} \leq e(C, C) \leq \lambda_1 |C| + \frac{(r - \lambda_1)|C|^2}{|V(G)|}.$$

Причём, если для некоторого множества C в одном из неравенств достигается равенство, то его характеристическая функция есть совершенная раскраска.

Определение

Множеств вершин $C \subset V(G)$ в графе G называется независимым, если $e(C, C) = 0$.

Теорема [граница Дельсарта—Хоффмана , Hoffman 1970]

Пусть G — r-регулярный граф и λ_{min} — минимальное собственное число его матрицы смежности M. Тогда мощность любого независимого множества в графе G не превосходит $\frac{\lambda_{min}|V(G)|}{\lambda_{min}-r}$. Независимое множество имеет мощность $\frac{\lambda_{min}|V(G)|}{\lambda_{min}-r}$ тогда и только тогда, когда его характеристическая функция есть совершенная раскраска с матрицей параметров $S = \begin{pmatrix} 0 & r \\ -\lambda_{min} & r+\lambda_{min} \end{pmatrix}$.

Граф Хэмминга

$Q_q = \{0, 1, \ldots, q-1\}$
$(x_1, \ldots, x_n) \in Q_q^n$

Определение

Весом набора $x = (x_1, \ldots, x_n)$ называется $\mathrm{wt}(x)$ — число ненулевых координат в x. Расстоянием Хэмминга $d_H(x, y)$ называется число различных координат в x и y, $d_H(x, y) = \mathrm{wt}(x - y)$.

Определение

Вершинами графа Хэмминга $H(n, q)$ является множество Q_q^n, вершины на расстоянии 1 соединены ребром.

Граф Хэмминга

$\xi = e^{2\pi i/q}$, $\xi^q = 1$
$\phi_z(x) = \xi^{(x,z)}$
$(x, z) = x_1 z_1 + x_2 z_2 + \cdots + x_n z_n \bmod q$
$\mathcal{F}(H(n, q))$ — пространство функций на графе Хэмминга.
$\mathcal{F}(H(n, q)) = \{f : Q_q^n \to \mathbb{C}\}$

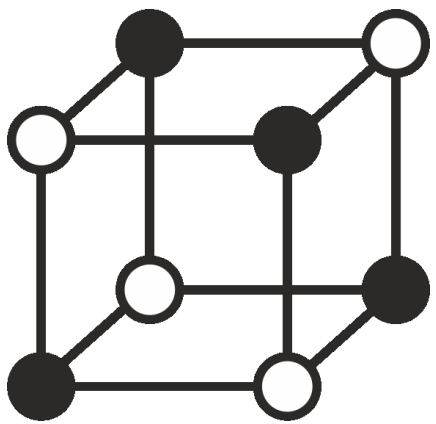
Лемма

1. $\{\phi_z(x) : z \in Q_q^n\}$ — ортогональный базис в $\mathcal{F}(H(n, q))$.
2. $\phi_z(x)$ — собственная функция графа $H(n, q)$ с собственным числом $\lambda_z = (q-1)n - q\mathrm{wt}(z)$.

$|\phi_z|^2 = q^n$
$f(x) = \frac{1}{q^{n/2}} \sum_z a_f(z)\phi_z(x)$
$\sum_x |f(x)|^2 = \sum_z |a(z)|^2$ равенство Парсеваля

Определение

Пусть $f : Q_q^n \to \{-1, 1\}$. Обозначим через $l[f] = e(f^{-1}(-1), f^{-1}(1))$ число рёбер, в концах которых значения функции f отличаются. Для константы эта величина равна нулю, а для булева счётчика чётности — $n2^{n-1}$.



Лемма [Nisan, Szegedy 1994]

$I[f] = \frac{q}{4} \sum\limits_{z \in Q_q^n} \mathrm{wt}(z)|a_f(z)|^2.$

Доказательство. Пусть M — матрица смежности $H(n, q)$.
Нетрудно непосредственно проверить, что

$$2I[f] - (n(q-1)q^n - 2I[f]) = -(Mf, f), \qquad (1)$$

поскольку в правой сумме каждое ребро учитывается два раза.
$M\phi_z = \lambda_z \phi_z$, где $\lambda_z = (q-1)n - q\mathrm{wt}(z)$
Представим функцию f в виде линейной комбинации
$f = \frac{1}{q^{n/2}} \sum\limits_{z \in Q_q^n} a_z \phi_z$. Подставляя это выражение в (1) и
используя ортогональность характеров, а также равенство
Парсеваля $\sum\limits_{z \in Q_q^n} |a_f(z)|^2 = q^n$, получаем равенства

$$4I[f] = n(q-1)q^n - \sum_{z \in Q_q^n} \lambda_z |a_f(z)|^2 = \sum_{z \in Q_q^n} q\mathrm{wt}(z)|a_f(z)|^2.$$

Пусть $Im(f)$ — множество значений, которое принимает функция f.

Определение

Функция f называется корреляционно-иммунной порядка k, если для любого $b \in Im(f)$ она принимает значение b одинаковое число раз во всех гранях размерности $n - k$.

Лемма [Таранников 2002]

Для функции $f : Q_q^n \to \{-1, 1\}$ равенство $\mathrm{cor}(f) = k$ верно тогда и только тогда, когда $a_f(z) = 0$ для всех $z \in Q_q^n$ веса $0 < \mathrm{wt}(z) \leq k$ и $a_f(v) \neq 0$ для некоторого $v \in Q_q^n$ веса $\mathrm{wt}(v) = k + 1$.

Теорема

$I[f] \geq q^n(\mathrm{cor}(f)+1)(\rho(f)-\rho^2(f))$, где $\rho(f) = |f^{-1}(-1)|/q^n$.

Доказательство. Из леммы Таранникова следует, что $a_f(z) = 0$ при $0 < \mathrm{wt}(z) \leq \mathrm{cor}(f)$. Следовательно, имеем равенство

$$4I[f] \geq \sum_{z \in Q_q^n \setminus \bar{0}} q(\mathrm{cor}(f)+1)|a_f(z)|^2.$$

$\sum\limits_{z \in Q_2^n} |a_f(z)|^2 = q^n$ и $a_f(\bar{0}) = q^{n/2}(1-\rho(f)-\rho(f))$. Тогда

$$\sum_{z \in Q_2^n \setminus \bar{0}} |a_f(z)|^2 = q^n - q^n(1-2\rho(f))^2 = 4q^n\rho(f)(1-\rho(f)).$$

Если $I[f] = q^n(\mathrm{cor}(f)+1)(\rho(f)-\rho^2(f))$, то f — совершенная 2-раскраска.

Неравенство Бирбрауэра – Фридмана

Для фиксированной плотности $\rho(f)$ величина $I[f]$ достигает своего наибольшего значения, если все вершины, на которых функция f равна -1, несмежны. Поэтому

$$I[f] \leq q^n(q-1)\rho(f)n$$

$$(\mathrm{cor}(f)+1)(\rho(f)-\rho^2(f)) \leq (q-1)\rho(f)n$$

Теорема [неравенство Бирбрауэра—Фридмана 1992, 1998]

Пусть $f : Q_q^n \to \{0,1\}$, $f \neq \mathbf{0}$, тогда $\rho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Литература

Potapov V.N. On extremal properties of perfect 2-colorings arXiv:2204.03308 [math.CO]
Потапов В.Н. Совершенные структуры в кодировании и криптографии http://old.math.nsc.ru/∼potapov/