

член $\chi_g(x)$ неприводим. Кроме того, группа $C(g)$ 2-транзитивна тогда и только тогда, когда многочлен $\chi_g(x)$ примитивен.

Утверждение 1. Для произвольных вектора $\gamma \in V_n^\times$, преобразования $g \in GL_n$ с характеристическим многочленом $\chi_g(x)$ граф $\bar{\Gamma}_{(0,\gamma)}(g)$ связан для всех векторов $\gamma \in V_n^\times$ тогда и только тогда, когда характеристический многочлен $\chi_g(x)$ неприводим.

Утверждение 2. Для вектора $\gamma \in V_n^\times$ граф $\bar{\Gamma}_{(0,\gamma)}(g)$ связан тогда и только тогда, когда $m_{\gamma,g}(x) = \chi_g(x)$. Если группа $C(g)$ примитивна, то все её графы орбиталов изоморфны.

В алгебраической теории графов наибольший интерес представляют следующие классы графов: вершинно-транзитивные, рёберно-транзитивные, дистанционно-регулярные, дистанционно-транзитивные [1].

Утверждение 3. Пусть $n \geq 2$, $i \in \{1, \dots, d-1\}$, $\bar{\Gamma}_{(0,\gamma_i)}(g)$ — нетривиальный связный граф диаметра $b \geq 2$. Тогда: а) $\bar{\Gamma}_{(0,\gamma_i)}(g)$ — рёберно-транзитивный граф; б) если $\gamma_i^{(g)}$ является базисом V_n , то граф $\bar{\Gamma}_{(0,\gamma_i)}(g)$ является дистанционно-транзитивным и $\text{Aut} \bar{\Gamma}_{(0,\gamma_i)}(g) \approx S_2 \uparrow S_n$.

Графом Хемминга на V_n будем называть граф с множеством вершин V_n и множеством рёбер $\{(\alpha, \beta) \in V_n^2 : \chi_n(\alpha, \beta) = 1\}$. Очевидно, что если граф изоморфен графу Хемминга, то его метрика изоморфна метрике Хемминга. Отметим, если множество $\gamma_i^{(g)}$ является базисом V_n , то граф $\bar{\Gamma}_{(0,\gamma_i)}(g)$ изоморфен графу Хемминга и является дистанционно-регулярным.

Теорема 1. Пусть $n \geq 2$, преобразование $g \in GL_n$ и вектор $\gamma \in V_n$ такие, что

$$m_{\gamma,g}(x) = x^{r(q-1)} \oplus x^{r(q-2)} \oplus \dots \oplus x^r \oplus 1 = \frac{(x^r)^q - 1}{x^r - 1},$$

где $rq = m = |\gamma^{(g)}|$. Граф $\bar{\Gamma}_{(0,\gamma)}(g)$ дистанционно-регулярный тогда и только тогда, когда выполняется одно из условий: а) $r = 1$; б) $r \geq 2$ и $q = 3$.

ЛИТЕРАТУРА

1. *Godsil C. and Royle G. Algebraic Graph Theory.* Springer Verlag, 2001.

УДК 519.14

О БУЛЕВЫХ ФУНКЦИЯХ, ПОЧТИ УРАВНОВЕШЕННЫХ В ГРАНЯХ¹

В. Н. Потапов

Обозначим через E^n множество упорядоченных двоичных наборов (вершин) длины n . Введём операцию $[x, y] = (x_1y_1, \dots, x_ny_n)$ для наборов $x, y \in E^n$. Количество единиц в наборе $y \in E^n$ называется *весом набора* и обозначается через $\text{wt}(y)$. Множество вершин чётного веса будем обозначать через E_0^n (нечётного — через E_1^n). *Гранью размерности* $(n - \text{wt}(y))$ называется множество $E_y^n(z) = \{x \in E^n : [x, y] = [z, y]\}$.

Пусть $S \subset E^n$; через χ^S будем обозначать характеристическую функцию множества S . Функция χ^S называется *корреляционно-иммунной порядка* $(n - m)$, если для любой грани $E_y^n(z)$ размерности m пересечения $E_y^n(z) \cap S$ имеют одинаковую мощность.

¹Работа выполнена при поддержке РФФИ (проекты 11-01-997, 10-01-00616) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0362).

Через $\text{cor}(S)$ будем обозначать максимальный порядок корреляционной иммунности, $\text{cor}(S) = \max\{n - m\}$. Корреляционно-иммунная функция χ^S называется *уравновешенной*, если $|S| = 2^{n-1}$. Тогда множество S пересекается с гранями размерности m ровно по половине вершин, т. е. $|E_y^n(z) \cap S| = |E_y^n(z)|/2$. В [1] установлено, что неуровновешенная непостоянная булева функция χ^S удовлетворяет неравенству $\text{cor}(S) \leq 2n/3 - 1$. Ясно, что непостоянная корреляционно-иммунная функция порядка $n - 1$ является счётчиком чётности или нечётности ($\chi^{E_0^n}$ или $\chi^{E_1^n} = \chi^{E_0^n} \oplus 1$). Корреляционно-иммунные функции порядка $n - \text{const}$ немногочисленны и описаны в [2]. Некоторые оценки числа корреляционно-иммунных функций меньших порядков имеются в [2–4].

Ниже рассматривается класс почти уравновешенных функций, содержащий значительное количество не эквивалентных булевых функций, максимально подобных корреляционно-иммунным функциям высокого порядка. Функцию χ^S будем называть *почти уравновешенной*, если для любой грани $E_y^n(z)$ любой размерности пересечение $E_y^n(z) \cap S$ отличается от половины мощности грани не более чем на 1, т. е. $-1 \leq |E_y^n(z) \cap S| - |E_y^n(z)|/2 \leq 1$.

В соответствии с определением класс почти уравновешенных функций является *наследственным*, т. е. все ретракты почти уравновешенных функций, полученные произвольной фиксацией произвольного набора переменных, являются почти уравновешенными. Одним из способов задания наследственного класса булевых функций является перечисление минимальных запретов. Булева функция g размерности k называется *минимальным запретом* для наследственного класса P , если $g \notin P$, но все её ретракты содержатся в P . Поскольку P — наследственный класс, функции из класса P не имеют ретрактов, совпадающих с запретом g .

Теорема 1. Множество почти уравновешенных булевых функций является наследственным классом с бесконечным набором минимальных запретов.

Будем обозначать через $P(n)$ множество функций от n аргументов из класса P . Пусть $f \in P(n)$, вершину $x \in E^n$ будем называть *свободной* относительно f , если найдётся функция $f' \in P(n)$, отличающаяся от f только на аргументе x .

Утверждение 1. Пусть P — наследственный класс и для некоторого m любая функция $f \in P(m)$ не имеет свободных вершин. Тогда $|P(n)| \leq 2^{\sum_{k=0}^{m-1} \binom{n}{k}}$.

Далее рассмотрим множество трёхзначных функций $f : E^n \rightarrow \{-1, 0, 1\}$, определённых на булевом кубе. Приведённые выше определения наследственного класса, минимального запрета и свободной вершины естественным образом распространяются на такие функции. Определим класс B трёхзначных уравновешенных функций следующим образом: $f \in B$, если для любой грани $\gamma = E_y^n(z)$ любой размерности сумма значений функции в ней не превышает по модулю единицы, т. е. $\sum_{x \in \gamma} f(x) \in \{-1, 0, 1\}$.

Через B_0 будем обозначать подкласс класса B , удовлетворяющий дополнительным условиям $f^{-1}(1) \subset E_0^n$ и $f^{-1}(-1) \subset E_1^n$. Ясно, что классы B и B_0 являются наследственными.

Утверждение 2. Булева функция f является почти уравновешенной тогда и только тогда, когда $f - \chi^{E_1^n} \in B_0$.

Преобразованием Мёбиуса функции $h : E^n \rightarrow \mathbb{R}$ называется функция

$$M[h] : E^n \rightarrow \mathbb{R}, \quad \text{где} \quad M[h](y) = (-1)^{\text{wt}(y)} \sum_{\substack{x \in E^n, \\ [x, y] = x}} h(x).$$

Из формулы включения-исключения и определения классов B и B_0 получаем

Утверждение 3.

- а) $M[M[h]] = h$ для любой функции $h : E^n \rightarrow \mathbb{R}$.
- б) $M[B] = B$.
- в) $M[f] \in B_0 \cup (-B_0)$, если и только если $f \in B$ и $\bar{0}$ — свободная вершина функции f .

Справедливость п. в следует из того, что вершина является свободной, только если во всех гранях, содержащих вершину, сумма значений функции имеет одинаковый знак.

В следующих утверждениях приведены несколько способов построения функций из классов B и B_0 .

Утверждение 4.

- а) Пусть $f \in B$ (или $f \in B_0$), тогда $f \cdot \chi^\gamma \in B$ (или $f \cdot \chi^\gamma \in B_0$) для любой грани γ .
- б) Пусть $f \in B_0(n)$, тогда $(-1)^{\chi^{E_1^n}} - f \in B_0(n)$.
- в) Пусть γ_1, γ_2 — грани в E^n и $\gamma_1 \cap \gamma_2 \neq \emptyset$. Определим функцию f равенством $f(x_1, \dots, x_n, x_{n+1}) = x_{n+1}\chi^{\gamma_1}(-1)^{\chi^{E_1^n}} + (x_{n+1} \oplus 1)\chi^{\gamma_2}(-1)^{\chi^{E_0^n}}$. Тогда $f \in B_0(n+1)$.

Утверждение 5.

- а) Пусть $f \in B(n)$, $g \in B(m)$ и $F(x, y) = f(x)g(y)$. Тогда $F \in B(n+m)$.
- б) Пусть $f \in B_0(n)$, $g \in B_0(m)$ и $F(x, y) = f(x)g(y)$. Тогда $F \in B_0(n+m)$.

Доказательства утверждений 4 и 5 легко получить непосредственной проверкой.

Булев n -мерный куб E^n естественным образом наделяется структурой векторного пространства над полем $\text{GF}(2)$. Будем называть *носителем* вектора $x \in E^n$ множество позиций, на которых в векторе x находятся единицы. Рассмотрим набор векторов $z^1, \dots, z^k$ с попарно не пересекающимися носителями. Пусть $V \subset E^n$ — подпространство, натянутое на векторы $z^1, \dots, z^k$, $V = \{\bigoplus \alpha_i z^i : \alpha \in E^k\}$. Пусть $f : E^k \rightarrow \{-1, 0, 1\}$. Определим функцию $G_V[f] : E^n \rightarrow \{-1, 0, 1\}$ равенствами $G_V[f](x) = f(\alpha)$, если $x = \bigoplus \alpha_i z^i$, и $G_V[f](x) = 0$, если $x \notin V$.

Теорема 2.

- а) Если $f \in B(k)$, то $G_V[f] \in B(n)$.
- б) Класс $B(n)$ содержит не менее $e^{c\sqrt{n}}$, $c > 0$, неэквивалентных функций.

ЛИТЕРАТУРА

1. *Fon-Der-Flaass D. G.* A bound of correlation immunity // Siberian Electronic Mathematical Reports. 2007. V. 4. P. 133–135.
2. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 91–148.
3. *Воробьев К. В., Фон-Дер-Флаасс Д. Г.* О совершенных 2-раскрасках гиперкуба // Сибирские электронные математические известия. 2010. Т. 7. С. 65–75.
4. *Потапов В. Н.* О совершенных раскрасках булева n -куба и корреляционно-иммунных функциях малой плотности // Сибирские электронные математические известия. 2010. Т. 7. С. 372–382.