9. *Canfield E. R., Gao Z., Greenhill C., et al.* Asymptotic enumeration of correlation-immune Boolean functions // Cryptography and Communications. 2010. No. 1. P. 111–126.
10. *Панков К. Н.* Уточнённые асимптотические оценки для числа (n, m, k)-устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.

УДК 519.7 DOI 10.17223/2226308X/11/16

СВЯЗЬ ОДНОРОДНЫХ БЕНТ-ФУНКЦИЙ И ГРАФОВ ПЕРЕСЕЧЕНИЙ[1]

А. С. Шапоренко

Исследуется связь однородных бент-функций и графов пересечений $\Gamma_{(n,k)}$. Граф $\Gamma_{(n,k)}$ — граф, вершины которого соответствуют $\binom{n}{k}$ неупорядоченным подмножествам размера k множества $\{1, \ldots, n\}$, две вершины соединены ребром в том и только в том случае, если соответствующие им подмножества имеют в точности один общий элемент. Выделены те n и k, для которых справедливо, что в $\Gamma_{(n,k)}$ есть клики размера $k+1$. Выдвинуто предположение о том, что для таких n и k клики размера $k+1$ являются максимальными. Получено, что при $n = (k+1)k/2$ количество клик размера $k+1$ в графе $\Gamma_{(n,k)}$ равно $n!/(k+1)!$. Установлено, что однородные булевы функции, полученные путём взятия дополнения к кликам максимального размера в графах $\Gamma_{(10,4)}$ и $\Gamma_{(28,7)}$, не являются бент-функциями.

Ключевые слова: *графы пересечений, однородные бент-функции.*

Бент-функцией называется булева функция от n переменных (n чётно), такая, что расстояние Хэмминга от данной функции до множества всех аффинных функций является максимально возможным. Бент-функция называется однородной, если все одночлены её АНФ имеют одинаковые степени.

В [1] определён граф пересечений $\Gamma_{(n,k)}$, вершины которого соответствуют $\binom{n}{k}$ неупорядоченным подмножествам размера k множества $\{1, \ldots, n\}$. Две вершины соединены ребром в том и только в том случае, если соответствующие подмножества имеют в точности один общий элемент. Будем называть дополнением к клике графа $\Gamma_{(n,k)}$ множество всех вершин этого графа, кроме тех, которые являются вершинами рассматриваемой клики.

В графе $\Gamma_{(6,3)}$ 20 вершин вида $\{a, b, c\}$, где $a, b, c \in \{1, \ldots, 6\}$ и различны. В этом графе были выделены клики размера 4 $(k+1)$ и, как указано в [1], такой размер клики является максимальным. Всего в графе $\Gamma_{(6,3)}$ 30 таких клик.

В $\Gamma_{(6,3)}$ дополнением к клике C с вершинами $\{1, 3, 6\}$, $\{1, 4, 5\}$, $\{2, 3, 5\}$ и $\{2, 4, 6\}$ будет множество, состоящее из 16 вершин. Если мы будем сопоставлять вершинам $\{\ell, m, n\}$ одночлены $x_\ell x_m x_n$, то 16 вершин дополнения к клике C будут соответствовать 16 одночленам АНФ однородной бент-функции от шести переменных степени 3 [2]. Поскольку таких клик 30 (равно как и однородных бент-функций от шести переменных степени 3 [2]), справедливо, что такие функции находятся во взаимно однозначном соответствии с дополнениями клик (максимальных) C_i графа $\Gamma_{(6,3)}$, $i = 1, \ldots, 30$. Встаёт вопрос о возможности классификации однородных бент-функций от большего числа переменных с помощью выделения некоторого подмножества вершин графа $\Gamma_{(n,k)}$.

[1]Работа поддержана Министерством образования и науки (задание № 1.12875.2018/12.1).

Теорема 1. В графе $\Gamma_{(n,k)}$, $n, k \in \mathbb{N}$, не всегда есть клика размера $k+1$.

Теорема 2. Пусть $n \geqslant (k+1)k/2$, $k \in \mathbb{N}$. Тогда в графе $\Gamma_{(n,k)}$ найдётся клика размера $k+1$.

Теорема 3. Если в графе $\Gamma_{(n,k)}$, $n, k \in \mathbb{N}$, есть клика размера $k+1$, она не всегда является максимальной.

Компьютерные вычисления показали, что для $n = 10$ и $k = 4$ максимальный размер клики в графе $\Gamma_{(10,4)}$ равен 5. В этом случае (как и в случае $n = 6$ и $k = 3$) n выражается через k формулой $n = (k+1)k/2$. В связи с этим появляется предположение о том, что при $n = (k+1)k/2$, $k \in \mathbb{N}$, в графе $\Gamma_{(n,k)}$ клика размера $k+1$ является максимальной.

Теорема 4. Пусть $n = (k+1)k/2$, $k \in \mathbb{N}$. Тогда в графе $\Gamma_{(n,k)}$ количество клик размера $k+1$ равно $n!/(k+1)!$.

Было установлено, что однородные булевы функции, полученные путём взятия дополнения к кликам максимального размера в графах $\Gamma_{(10,4)}$ и $\Gamma_{(28,7)}$, не являются бент-функциями.

ЛИТЕРАТУРА

1. *Charnes C., Rotteler M., and Beth T.* Homogeneous bent functions, invariants, and designs // Designs, Codes and Cryptography. 2002. No. 26. P. 139–154.
2. *Qu C., Seberry J., and Pieprzyk J.* Homogeneous bent functions // Discrete Appl. Math. 2000. V. 102. No. 1–2. P. 133–139.