

ЛИТЕРАТУРА

1. Салий В. Н. Система абстрактных связанных подграфов линейного графа // Прикладная дискретная математика. 2012. № 2(16). С. 90–94.

УДК 519.7

ПРОСТОЕ ДОКАЗАТЕЛЬСТВО СИЛЬНОЙ РЕГУЛЯРНОСТИ
ГРАФА КЭЛИ БЕНТ-ФУНКЦИИ¹

Н. Н. Токарева

Получено простое доказательство известного результата об описании класса бент-функций в терминах сильно регулярных графов.

Ключевые слова: бент-функции, сильно регулярные графы.

Бент-функции возникают в ряде криптографических приложений и широко исследуются. В частности, очень важной является задача описания бент-функций в алгебраических и комбинаторных терминах [1].

Пусть f — булева функция от n переменных. Через $\text{supp}(f)$ обозначим её *носитель*, т. е. множество всех двоичных векторов длины n , на которых функция f принимает значение 1. Рассмотрим *граф Кэли* $G_f = G(\mathbb{Z}_2^n, \text{supp}(f))$ булевой функции f . Вершинами графа являются все векторы длины n . Две вершины x, y соединяются ребром, если вектор $x \oplus y$ принадлежит множеству $\text{supp}(f)$. Граф G называется *сильно регулярным* с параметрами (v, k, λ, μ) , если он содержит v вершин, степень каждой вершины равна k и для любых двух вершин x, y число общих смежных им вершин равно λ или μ в зависимости от того, соединены вершины x, y ребром или нет. Булева функция f от чётного числа переменных n называется *бент-функцией*, если ее производная по любому ненулевому направлению y уравновешена, т. е. выполняется $\sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x)+f(x+y)} = 0$.

В 2001 г. А. Бернаскони, Б. Коденотти и Дж. Ван-дер-Кам [2, 3] получили следующий результат, позволивший охарактеризовать множество бент-функций в терминах сильно регулярных графов.

Теорема 1. Булева функция f является бент-функцией тогда и только тогда, когда граф G_f является сильно регулярным, причем $\lambda = \mu$.

Доказательство было получено с помощью спектральной техники при исследовании графов, ассоциированных с булевыми функциями. Бент-функции при этом составили частный случай булевых функций с тремя различными спектральными коэффициентами. Недостатком такого доказательства служит его объёмность и малая наглядность: остаётся трудным объяснить по существу, почему же графы Кэли бент-функций (и только они) обладают таким примечательным свойством, как сильная регулярность. В связи с этим результат было трудно включить, например, в учебный курс.

В данной работе получено простое доказательство теоремы 1, непосредственно опирающееся на свойства бент-функций. Явно определены параметры сильно регулярных графов, соответствующих бент-функциям. Теорема 1 вытекает из следующих утверждений, доказательства которых теперь могут войти в любой учебный курс.

Утверждение 1. Граф Кэли G_f бент-функции f от n переменных сильно регулярный с параметрами $(2^n, 2^{n-1} \pm 2^{(n/2)-1}, \lambda = \mu = 2^{n-2} \pm 2^{(n/2)-1})$.

¹Работа поддержана грантами РФФИ № 11-01-00997, 12-01-31097.

Знаки « $\pm$ » считаются согласованными, т. е. одинаковыми в обоих случаях.

Утверждение 2. Пусть G — сильно регулярный граф на 2^n вершинах, $n \geq 2$, такой, что $\lambda = \mu > 0$. Тогда он имеет параметры из утверждения 1.

ЛИТЕРАТУРА

1. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. Saarbrücken: LAP Lambert Academic Publishing, 2011.
2. Bernasconi A. and Codenotti B. Spectral analysis of Boolean functions as a graph eigenvalue problem // IEEE Trans. Computers. 1999. V. 48. No. 3. P. 345–351.
3. Bernasconi A., Codenotti B., and VanderKam J. M. A characterization of bent functions in terms of strongly regular graphs // IEEE Trans. Computers. 2001. V. 50. No. 9. P. 984–985.

УДК 519.248, 519.176

АСИМПТОТИКИ ВЕРОЯТНОСТЕЙ СВЯЗНОСТИ ПАР ВЕРШИН ГРАФА¹

Г. Ш. Цициашвили, М. А. Осипова, А. С. Лосев

Для графов с низконадёжными ребрами построена асимптотика вероятности связности любой пары его вершин. Параметрами полученного соотношения являются характеристики кратчайших путей графа, для вычисления которых разработаны модификации классических алгоритмов. Проведенный вычислительный эксперимент продемонстрировал преимущества предложенных алгоритмов.

Ключевые слова: кратчайший путь, вероятность связности, вычислительная сложность.

Для случайных графов с низконадёжными рёбрами построен удобный в реализации алгоритм вычисления вероятности связности любой пары его вершин на основе доказанного асимптотического соотношения. Для параметров полученного соотношения (характеристик кратчайших путей) разработаны модификации классических алгоритмов. Особенностью предлагаемых алгоритмов является тот факт, что в них не требуется перечислять кратчайшие пути между узлами, нужно лишь определить их количество. Ещё одним существенным фактором упрощения вычислений является рассмотрение графов с ограниченным диаметром, которые в последние годы вызывают большой теоретический и практический интерес. Проведенный вычислительный эксперимент подтвердил быстроедействие построенной процедуры определения вероятности связности по сравнению с методом Монте-Карло.

Рассмотрим неориентированный связный простой граф G с множеством узлов U и множеством рёбер V . Предположим, что каждое ребро v графа G с вероятностью $p(v)$ работоспособно, причём все рёбра функционируют независимо. Обозначим $D(i, j)$ минимальное число ребер в путях, соединяющих узлы i, j графа G , $C(i, j)$ — число путей с $D(i, j)$ рёбрами. Для вероятности связности $P_{ij}(G)$ узлов i, j графа G доказаны следующие утверждения.

Теорема 1. Если $p(v) = h$, $v \in V$, то

$$P_{ij}(G) \sim C(i, j)h^{D(i, j)}, \quad h \rightarrow 0. \quad (1)$$

¹Работа поддержана грантом РФФИ № 12-01-00114-а.