

УДК 519.17

ОБ УПОРЯДОЧЕННОМ МНОЖЕСТВЕ СВЯЗНЫХ ЧАСТЕЙ МНОГОУГОЛЬНОГО ГРАФА

В. Н. Салий

Охарактеризованы многоугольные графы, для которых упорядоченное вложением множество абстрактных связных частей является решёткой.

Ключевые слова: *многоугольный граф, линейный граф, двоичный вектор, двойственность, упорядоченное множество, решётка.*

Под графом понимается пара $G = (V, \alpha)$, где V — конечное непустое множество и $\alpha \subseteq V \times V$ — отношение на нём. Элементы множества V называются вершинами графа, а пары, входящие в отношение смежности α , дугами.

Если $V' \subseteq V$ и $\alpha' \subseteq \alpha$, то граф $G' = (V', \alpha')$ называется частью графа G . В случае, когда $\alpha' = \alpha \cap (V' \times V')$, говорят, что G' является подграфом графа G .

Пусть $G = (V, \alpha)$ и $H = (U, \beta)$ — некоторые графы. Вложение графа G в граф H — это такое инъективное отображение $\varphi : V \rightarrow U$, что $(\forall v, v' \in V)((v, v') \in \alpha \implies (\varphi(v), \varphi(v')) \in \beta)$. Если $(\forall v, v' \in V)((v, v') \in \alpha \iff (\varphi(v), \varphi(v')) \in \beta)$, то говорят, что φ — сильное вложение G в H . Биективное сильное вложение (фактически наложение) $\varphi : V \rightarrow U$ по определению является изоморфизмом графа G на граф H . Если граф G вкладывается в граф H , то G изоморфен некоторой части графа H , а при сильном вложении — некоторому его подграфу.

Вершины v, v' графа G называются связанными, если $(\exists v_1, v_2, \dots, v_k \in V)((v, v_1) \in \alpha \cup \alpha^{-1} \& (v_1, v_2) \in \alpha \cup \alpha^{-1} \& \dots \& (v_k, v') \in \alpha \cup \alpha^{-1})$. Граф, в котором любые две вершины связаны, по определению является связным.

Маршрутом с началом v и концом v' называется последовательность примыкающих дуг $(v, v_1), (v_1, v_2), \dots, (v_k, v')$. Маршрут можно представить в виде перечисления проходимых вдоль него вершин: $vv_1v_2 \dots v_kv'$. Цепь — это маршрут, в котором все вершины разные. Цепь, состоящую из n дуг, обозначим через P_n и будем использовать её стандартную запись $P_n = v_0v_1 \dots v_n$. Если «склеить» концы цепи, получим n -звенный (n -вершинный) контур, который будем записывать в виде $C_n = v_1v_2 \dots v_{n-1}v_1$, считая v_1 выбранной начальной вершиной.

Под линейным графом длины n понимается всякий граф L , полученный переориентацией некоторых дуг цепи P_n . Многоугольным графом порядка n называется всякий граф M , полученный переориентацией некоторых дуг контура C_n .

Все связные части линейного графа являются его подграфами. В многоугольном графе M порядка n все связные собственные части с не более чем $n - 1$ вершинами являются линейными подграфами в M ; если же из M удалить какую-нибудь дугу, то получится линейный граф, являющийся частью, но не подграфом графа M .

Для многоугольного графа M через $\text{ASubc } M$ обозначим класс всех связных графов, допускающих вложение в M . Если $\mathcal{L} \in \text{ASubc } M$, то это означает, что все графы из $\mathcal{L}$ изоморфны некоторой линейной части графа M или самому графу M . Класс $\text{ASubc } M$ упорядочивается отношением вложимости: если $\mathcal{L}'$ и $\mathcal{L}''$ определяются соответственно линейными частями L' и L'' графа M , то $\mathcal{L}' \leq \mathcal{L}''$ по определению означает, что L' вкладывается в L'' .

В [1] автором охарактеризованы линейные графы L , для которых упорядоченное множество $\text{ASubc } L$ всех связных абстрактных подграфов является решёткой. Настоящее сообщение существенно опирается на идеи и методы, представленные в [1].

Пусть b — некоторый двоичный вектор. Двойственным для него называется вектор b^δ , получаемый из b так: компоненты вектора b надо записать в обратном порядке, а затем взаимно заменить в компонентах нули и единицы, т. е. осуществить преобразование $b \mapsto (b^{-1})'$. Например, для $b = 011100$ получим $b^\delta = 110001$. Понятно, что $b^{\delta\delta} = b$.

Под отрезками вектора понимаются блоки, состоящие из подряд идущих компонент этого вектора. Через $\text{ASubc } b$ обозначим совокупность всех попарно не двойственных отрезков двоичного вектора b . На множестве $\text{ASubc } b$ вводится порядок: $b' \leq b''$, если b' является отрезком в b'' или в b''^δ .

Двоичными векторами естественным образом кодируются линейные и многоугольные графы. Линейному графу L длины n соотносится двоичный n -мерный вектор $b = b(L)$ путём сопоставления каждой дуге графа символа 1, если при переориентации цепи $P = v_0 v_1 \dots v_n$ в граф L эта дуга оказалась направленной от v_0 к v_n , и символа 0 в противном случае. Например, для $L = v_0 \leftarrow v_1 \leftarrow v_2 \rightarrow v_3 \rightarrow v_4 \leftarrow v_5$ будет $b(L) = 001110$. С другой стороны, каждому n -мерному двоичному вектору b соответствует линейный граф $L = L(b)$ длины n , получающийся из цепи P_n переориентацией её дуг, согласованной в вышеуказанном смысле со значениями компонент вектора b . Так, для $b = 1011$ будет $L(b) = v_0 \rightarrow v_1 \leftarrow v_2 \rightarrow v_3 \rightarrow v_4$. Двоичным кодом для связного подграфа линейного графа L , очевидно, является отрезок вектора $b(L)$ или двойственного. Заметим, что двойственные векторы являются кодами изоморфных линейных графов. Будем считать, что $b(L)$ является лексикографически меньшим из них.

Пусть M — многоугольный граф, полученный из контура C_n переориентацией некоторых дуг. Выберем в C_n в качестве начальной вершину v_1 и построим n -мерный двоичный вектор b^1 , полагая $b_i^1 = 1$, если $(v_i, v_{i+1}) \in \alpha$ в M , и $b_i^1 = 0$, если $(v_{i+1}, v_i) \in \alpha$ в M (сложение в индексах — по модулю n). Аналогично построим вектор b^2 , считая начальной вершиной v_2 , и т. д. Выбрав из векторов $b^1, b^2, \dots, b^n$ лексикографически минимальный, сопоставим его графу M и обозначим через $b(M)$. Например, для четырёхугольного графа $M = v_1 \rightarrow v_2 \leftarrow v_3 \leftarrow v_4 \rightarrow v_1$ получим $b^1 = 1001$, $b^2 = 0011$, $b^3 = 0110$, $b^4 = 1100$, и значит, $b(M) = 0011$. С другой стороны, каждому n -мерному вектору b соответствует n -угольный граф $M = M(b)$, получающийся из контура C_n переориентацией некоторых его дуг, согласованной в вышеуказанном смысле со значениями компонент вектора b . Например, для $b = 01001$ будет $M(b) = v_1 \leftarrow v_2 \rightarrow v_3 \leftarrow v_4 \leftarrow v_5 \rightarrow v_1$.

Лемма 1. Если M — многоугольный граф и b — соответствующий ему двоичный вектор, то упорядоченные множества $\text{ASubc } M$ и $\text{ASubc } b$ изоморфны.

Из леммы 1 следует, что упорядоченное множество $\text{ASubc } M$ абстрактных связных частей многоугольного графа M тогда и только тогда будет решёткой, когда решёткой является упорядоченное множество $\text{ASubc } b$ попарно не двойственных отрезков двоичного вектора b , кодирующего граф M .

При записи двоичных векторов в них группируются одинаковые компоненты и используется экспоненциальное обозначение: $01100110010 = 0(1^2 0^2)^2 10$ и т. п.

Теорема 1. Пусть M — многоугольный граф с n вершинами. Упорядоченное множество $\text{ASubc } M$ его абстрактных связных частей тогда и только тогда является решёткой, когда вектор $b = b(M)$ имеет один из следующих видов: 1) 0^n ; 2) $0^{n-1}1$, $n \leq 4$; 3) $0^{n-2}1^2$; 4) $(0^k 1^k)^l$ при $k \geq 1$, $l \geq 1$, $2kl = n$.

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.