

минимальному расстоянию между бент-функциями $2^{n/2}$. Особенностью метода является то, что он зависит от конкретного вида бент-функции, в отличие от конструкции Мак-Фарланда.

ЛИТЕРАТУРА

1. *Paterson K. G.* Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. P. 46–71.
2. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
3. *Колмеев Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.

УДК 519.175.1

О НОВОМ ПОЛНОМ ИНВАРИАНТЕ АЦИКЛИЧЕСКИХ ГРАФОВ

А. В. Пролубников

В задаче проверки изоморфизма графов (задача ИГ) даны два обыкновенных графа с одинаковым числом вершин и ребер. Необходимо ответить на вопрос, существует ли такое биективное отображение (изоморфизм) множества вершин одного графа на множество вершин второго, которое сохраняло бы смежность соответствующих вершин?

Поскольку любой алгоритм решения задачи ИГ представляет собой проверку равенства некоторых инвариантных относительно изоморфизма количественных характеристик графов, неясный статус задачи ИГ в иерархии теории сложности непосредственно связан с вопросом сложности вычисления полного инварианта графа. На данный момент не доказано, что задача ИГ является NP -полной, равно как и не найдено полиномиальных алгоритмов решения общего случая задачи.

Единственным известным полным инвариантом графа является его канонический код — максимальное число, двоичная запись которого может быть получена путем некоторой конкатенации строк верхне-(нижне-)треугольной подматрицы матрицы смежности графа [1].

Полные инварианты известны лишь для немногих относительно простых классов графов, поскольку наличие полиномиально вычислимого полного инварианта для графов из некоторого класса эквивалентно полиномиальной разрешимости задачи ИГ для графов из этого класса. Так, в работе [2] представлен полный инвариант для деревьев и в целом класса ациклических графов, в работе [3] — для планарных графов. Однако в этих работах, как и в большинстве работ, нацеленных на нахождение полного инварианта для ограниченного класса графов, полный инвариант ищется как результат канонизации графа — процесс, который может быть описан следующим образом. Пусть $\mathbf{G}$ — некоторый класс графов. Пусть $f : \mathbf{G} \rightarrow \{0, 1\}^*$ — функция, отображающая граф в пространство битовых строк (канонических кодов), такая, что для всех $G, H \in \mathbf{G}$ имеем $G \simeq H \Leftrightarrow f(G) = f(H)$, то есть f — полный инвариант для графов из $\mathbf{G}$. Если f дает для G граф $f(G)$ такой, что $G \simeq f(G)$, то $f(G)$ — канонический код графа, по которому восстанавливается сам граф.

В этой работе предлагается алгебраический полный инвариант ациклических графов, который не получается в результате канонизации графа, а представляет собой множество из $1 + n(n + 1)/2$ числовых значений, каждое из которых есть произведе-

ние собственных значений из спектра графа и спектров его подграфов. Этот подход позволяет рассмотреть вопрос поиска полного инварианта для классов графов, используя алгебраические свойства матриц, представляющих графы, и допускает обобщения на более широкие классы графов. Вариант такого обобщения также рассматривается в работе.

ЛИТЕРАТУРА

1. *Balasubramanian K., Parthasarathy K. R.* In search of a complete invariant for graphs // *Lect. Notes Mathem.* 1981. V. 885. P. 42–59.
2. *Lindell S.* A Logspace Algorithm for Tree Canonization // *Proc. of the 24th Annual ACM Symposium on the Theory of Computing.* New York: ACM, 1992. P. 400–404.
3. *Datta S., Limaye N., Nimbhorkar P., Thierauf T., Wagner F.* Planar Graph Isomorphism is in Log-Space // *24th Annual IEEE Conference on Computational Complexity.* Paris, France, July 15 – July 18, 2009. ISBN: 978-0-7695-3717-7.

УДК 519.17

О КАРКАСЕ АВТОМАТА

В. Н. Салий

В [1] было введено понятие каркаса автомата. Это упорядоченное множество, которое образуют слои автомата вместе с отношением обратной достижимости. Оно сыграло весьма существенную роль в описании автоматов, у которых каждая конгруэнция является ядром подходящего эндоморфизма. В работе устанавливаются некоторые свойства каркаса, связанные с основными алгебраическими конструкциями для автоматов, такими, как подавтомат, гомоморфизм, конгруэнция.

Автомат — это тройка $\mathbf{A} = (S, X, \delta)$, где S и X — конечные непустые множества, соответственно множество состояний и множество входных сигналов, а $\delta : S \times X \rightarrow S$ — отображение, называемое функцией переходов.

Подмножество $S' \subseteq S$ называется устойчивым в автомате $\mathbf{A}$, если $\delta(s, x) \in S'$ для любых $s \in S'$ и $x \in X$. Если S' устойчиво в $\mathbf{A}$, то, ограничивая функцию переходов δ на $S' \times X$, получают автомат $\mathbf{A}' = (S', X, \delta)$ — подавтомат автомата $\mathbf{A}$, соответствующий S' . Совокупность $\text{Sub}\mathbf{A}$ всех подавтоматов автомата $\mathbf{A}$, упорядоченная отношением $\mathbf{A}_1 \leq \mathbf{A}_2 \iff S_1 \subseteq S_2$, где $\mathbf{A}_i = (S_i, X, \delta)$, $i = 1, 2$, является дистрибутивной решеткой.

Пусть $\mathbf{A} = (S, X, \delta)$ и $\mathbf{B} = (T, X, \delta)$ — сравнимые автоматы, т. е. автоматы с одним и тем же множеством входных сигналов. Отображение $\varphi : S \rightarrow T$ по определению является гомоморфизмом автомата $\mathbf{A}$ в автомат $\mathbf{B}$, если $\varphi(\delta(s, x)) = \delta(\varphi(s), x)$ для любых $s \in S$, $x \in X$. Взаимно однозначные гомоморфизмы автоматов называются вложениями, а их биективные гомоморфизмы — изоморфизмами. Эндоморфизмы автомата — это его гомоморфизмы в себя, автоморфизмы — изоморфизмы на себя.

Отношение эквивалентности $\theta \subseteq S \times S$ называется конгруэнцией автомата $\mathbf{A} = (S, X, \delta)$, если оно согласовано с функцией переходов в том смысле, что $(\forall s, t \in S)(\forall x \in X)((s, t) \in \theta \implies (\delta(s, x), \delta(t, x)) \in \theta)$. Каждая конгруэнция θ автомата $\mathbf{A}$ определяет его фактор-автомат $\mathbf{A}/\theta = (S/\theta, X, \delta)$, где $\delta(\theta(s), x) := \theta(\delta(s, x))$ для любых $s \in S$, $x \in X$.

Пусть X^* — множество всех конечных слов над алфавитом X . Продолжим функцию переходов δ на множество $S \times X^*$, полагая $\delta(s, e) = s$, где $e \in X^*$ — пустое слово, и $\delta(s, px) = \delta(\delta(s, p), x)$ для любых $s \in S$, $x \in X$, $p \in X^*$. Говорят, что состояние t