Известия вузов. Математика
2016, №2, с. 18–23

http://kpfu.ru/science/nauchnye-izdaniya/ivrm/
e-mail: izvuz.matem@kpfu.ru

А.В. ГАВРИКОВ

Т-НЕПРИВОДИМЫЕ РАСШИРЕНИЯ ДЛЯ МНОГОУГОЛЬНЫХ ОРГРАФОВ

Аннотация. Ориентированные графы представляют собой математические модели дискретных систем. Конструкции оптимальных расширений, которыми являются Т-неприводимые расширения, широко применяются в диагностике дискретных систем и криптографии. Многоугольный орграф — это орграф, полученный из контура переориентацией некоторого количества его дуг. В работе предложен полиномиальный алгоритм построения одного из Т-неприводимых расширений для многоугольного орграфа. Приведено доказательство корректности алгоритма.

Ключевые слова: многоугольный орграф, отказоустойчивость дискретных систем, Т-неприводимое расширение.

УДК: 519.173

Введение

Под *ориентированным графом* (*орграфом*) понимается пара $\overrightarrow{G} = (V, \alpha)$, где V — конечное непустое множество (вершины орграфа), а α — отношение на множестве V (дуги орграфа). Дуга в орграфе называется *инцидентной* вершине v, если v — конец или начало этой дуги. *Вложение* орграфа $\overrightarrow{G} = (V, \alpha)$ в орграф $\overrightarrow{H} = (W, \beta)$ — взаимно однозначное отображение $\phi : V \to W$ такое, что $((u, v) \in \alpha \to (\phi(u), \phi(v)) \in \beta) \quad \forall u, v \in V$. Тогда говорят, что орграф $\overrightarrow{G}$ вкладывается в орграф $\overrightarrow{H}$. *Часть* орграфа $\overrightarrow{G} = (V, \alpha)$ — это орграф $\overrightarrow{H} = (W, \beta)$ такой, что $W \subseteq V$ и $\beta \subseteq (W \times W) \cap \alpha$. Часть орграфа $\overrightarrow{G} = (V, \alpha)$ является *подграфом* орграфа $\overrightarrow{H} = (W, \beta)$, если $\beta = (W \times W) \cap \alpha$. Подграф $\overrightarrow{H}$ *максимален*, если он получается из исходного орграфа $\overrightarrow{G}$ удалением одной вершины v и всех инцидентных ей дуг. *Расширение* орграфа $\overrightarrow{G} = (V, \alpha)$ — это орграф $\overrightarrow{H} = (W, \beta)$ такой, что $|W| = |V| + 1$ и орграф $\overrightarrow{G}$ вкладывается в каждый максимальный подграф орграфа $\overrightarrow{H}$. *Объединение* орграфов $\overrightarrow{G} = (V, \alpha)$ и $\overrightarrow{H} = (W, \beta)$ таких, что $V \cap W = \varnothing$, — это орграф $\overrightarrow{G} \cup \overrightarrow{H} = (V \cup W, \alpha \cup \beta)$. *Соединение* орграфов $\overrightarrow{G} = (V, \alpha)$ и $\overrightarrow{H} = (W, \beta)$ таких, что $V \cap W = \varnothing$, — это орграф $\overrightarrow{G} + \overrightarrow{H} = (V \cup W, \alpha \cup \beta \cup V \times W \cup W \times V)$. *Изоморфизм* орграфа $\overrightarrow{G} = (V, \alpha)$ на орграф $\overrightarrow{H} = (W, \beta)$ — это взаимно однозначное соответствие $\phi : V \to W$, сохраняющее отношение смежности, т. е. $((u, v) \in \alpha \leftrightarrow (\phi(u), \phi(v)) \in \beta) \quad \forall u, v \in V$. *Изоморфность* орграфов $\overrightarrow{G}$ и $\overrightarrow{H}$ обозначается через $\overrightarrow{G} \cong \overrightarrow{H}$. Орграфы $\overrightarrow{G}$ и $\overrightarrow{H}$ в этом случае называются *изоморфными* [1].

Поступила 10.07.2014

Тривиальное расширение (ТР) орграфа $\overrightarrow{G} = (V, \alpha)$ — соединение $\overrightarrow{G} + w$ исходного орграфа $\overrightarrow{G}$ с вершиной $w \notin V$. В силу того, что тривиальное расширение орграфа $\overrightarrow{G}$ единственное с точностью до изоморфизма, возможно ввести функцию ТР($\overrightarrow{G}$). *Т-неприводимое расширение* (ТНР) орграфа $\overrightarrow{G}$ — расширение исходного орграфа $\overrightarrow{G}$, полученное удалением максимального множества дуг из ТР($\overrightarrow{G}$) [2]. ТНР для некоторых классов неориентированных (с симметричным и антирефлексивным отношением смежности) графов рассматривались С.Г. Курносовой в [2], [3]. В работе [3] показаны конструкции ТНР для полных бинарных деревьев.

Т-неприводимые расширения являются одним из видов оптимальных расширений для орграфов. Конструкции оптимальных расширений применяются в диагностике дискретных систем и криптографии [4], а также в задачах отказоустойчивости [5], [6]. В общем случае задача определения того, является ли орграф $\overrightarrow{H}$ расширением для орграфа $\overrightarrow{G}$, является $\mathbb{NP}$-полной, а задача поиска ТНР по заданному орграфу $\overrightarrow{G} = (V, \alpha)$ не принадлежит классу $\mathbb{NP}$ [7].

Следующий критерий, на который опирается доказательство процедуры построения ТНР, вытекает непосредственно из определения.

Теорема 1 (критерий ТНР для орграфов)**.** *Орграф $\overrightarrow{H} = (W, \beta)$ является ТНР для орграфа $\overrightarrow{G} = (V, \alpha)$ тогда и только тогда, когда одновременно выполняются следующие условия.*

1) $|W| = |V| + 1$.

2) *В орграфе $\overrightarrow{H} = (W, \beta)$ существует вершина w такая, что $\overrightarrow{H} - w \cong \overrightarrow{G}$.*

3) *Орграф $\overrightarrow{G} = (V, \alpha)$ вкладывает в каждый максимальный подграф $(\overrightarrow{H} - u)$ орграфа $\overrightarrow{H} = (W, \beta)$, где $u \neq w$.*

4) (*Свойство неприводимости*). *При удалении любой дуги, инцидентной вершине w, т. е. $(u, w) \in \beta$ или $(w, u) \in \beta$, из орграфа $\overrightarrow{H} = (W, \beta)$ полученный орграф не будет расширением для $\overrightarrow{G} = (V, \alpha)$.*

1. Общие сведения о многоугольных орграфах

Путь в орграфе — последовательность дуг вида (v_0, v_1), $(v_1, v_2), \ldots, (v_{n-2}, v_{n-1})$, где $(v_i, v_{i+1}) \in \alpha$, $0 \leq i \leq n-2$, и никакая дуга не встречается более одного раза. Путь в орграфе является *простым*, если каждая его вершина принадлежит не более чем двум его дугам. *Длина пути* — это количество входящих в него дуг. Путь является *циклическим*, если $v_0 = v_{n-1}$. *Контур* в орграфе — это простой циклический путь. Контур, состоящий из n вершин, обозначим через $\overrightarrow{C_n} = v_0 v_1 \ldots v_{n-1} v_0$, считая v_0 выбранной начальной вершиной. Многоугольным орграфом порядка n называется всякий орграф $\overrightarrow{M}$, полученный переориентацией некоторых дуг контура $\overrightarrow{C_n}$ [8].

Степень исхода вершины v — количество дуг в орграфе $\overrightarrow{G} = (V, \alpha)$, имеющих своим началом вершину v. Степень исхода вершины v обозначают через $d^+(v)$, $d^+(v) = |\alpha(v)|$. *Степень захода вершины v* — это количество дуг в орграфе $\overrightarrow{G} = (V, \alpha)$, имеющих своим концом вершину v. Степень захода вершины v обозначают через $d^-(v)$, $d^-(v) = |\alpha^{-1}(v)|$. Вершина v называется *источником*, если ее степень захода равна нулю, $d^-(v) = 0$. Вершина v называется *стоком*, если ее степень исхода равна нулю, $d^+(v) = 0$. Сумма степеней исхода и захода каждой вершины многоугольного орграфа $\overrightarrow{M}$=(Z, γ) равна двум, $(d^+(v)+d^-(v)=2)$ $\forall v \in Z$. Назовем две вершины u и v орграфа $\overrightarrow{G} = (V, \alpha)$ *смежными*, если в орграфе

существует дуга $(u, v) \in \alpha$ или дуга $(v, u) \in \alpha$. Все арифметические операции над индексами вершин в многоугольных орграфах в дальнейшем будем производить по модулю числа n. Для любой вершины v_i, $0 \le i \le n-1$, многоугольного орграфа $\overrightarrow{M}$ смежными вершинами являются вершины v_{i-1} и v_{i+1}.

2. Алгоритм построения THP для многоугольных орграфов

Рассмотрим полиномиальный алгоритм построения THP для многоугольных орграфов, имеющий асимптотическую сложность $O(n^3)$.

Алгоритм. Дан многоугольный орграф $\overrightarrow{M} = (Z, \gamma)$. Построим его THP.

1. Добавим к $\overrightarrow{M}$ вершину w.
2. Для каждой вершины $v \in Z$

∘ если $v \in Z$ является источником, то добавим дугу (v, w);

∘ если $v \in Z$ является стоком, то добавим дугу (w, v);

∘ если $v \in Z$ такая, что $d^+(v) = 1$ и $d^-(v) = 1$, то добавим дуги (v, w) и (w, v).

Орграф, построенный после вышеописанных пунктов, обозначим через $\overrightarrow{H}_0 = (W, \beta_0)$. Положим $k = 0$.

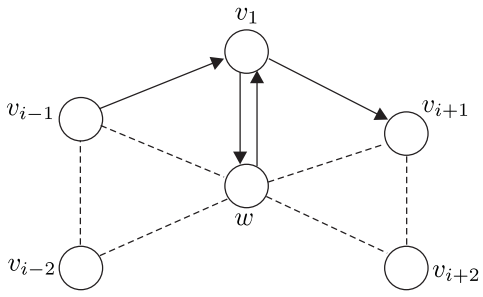

Рис.

3. Рассматриваем вершины v_i, имеющие степень исхода и степень захода, равные единице, $d^+(v_i) = 1$ и $d^-(v_i) = 1$, в многоугольном орграфе $\overrightarrow{M}$ в порядке возрастания их индексов. Тогда $\exists v_{i-1} \in Z : (v_{i-1}, v_i) \in \gamma$ и $\exists v_{i+1} \in Z : (v_i, v_{i+1}) \in \gamma$ (рис.). По построению в п. 2 алгоритма вершина v_i соединена с вершиной w дугами (v_i, w) и (w, v_i). Возможны следующие случаи.

Случай A: многоугольный орграф $\overrightarrow{M}$ вкладывается в орграф $\overrightarrow{H_k} - v_{i-1} - (w, v_i)$. Строим орграф $\overrightarrow{H}_{k+1} = (W, \beta_{k+1})$ такой, что $\overrightarrow{H}_{k+1} = \overrightarrow{H}_k - (w, v_i)$, $\beta_{k+1} = \beta_k - (w, v_i)$. Далее алгоритм продолжает работу с орграфом $\overrightarrow{H}_{k+1}$, переходим к следующей вершине в п. 3.

Случай B: многоугольный орграф $\overrightarrow{M}$ вкладывается в орграф $\overrightarrow{H_k} - v_{i+1} - (v_i, w)$. Строим орграф $\overrightarrow{H}_{k+1} = (W, \beta_{k+1})$ такой, что $\overrightarrow{H}_{k+1} = \overrightarrow{H}_k - (v, w)$, $\beta_{k+1} = \beta_k - (v_i, w)$. Далее алгоритм продолжает работу с орграфом $\overrightarrow{H}_{k+1}$, переходим к следующей вершине в п. 3.

Случай C: многоугольный орграф $\overrightarrow{M}$ не вкладывается ни в орграф $\overrightarrow{H_k} - v_{i-1} - (w, v_i)$, ни в орграф $\overrightarrow{H_k} - v_{i+1} - (v_i, w)$. Не производим никаких действий, переходим к следующей вершине в п. 3.

Уточнение: если в многоугольном орграфе $\overrightarrow{M}$ каждая вершина v_i является либо источником, либо стоком, то данный пункт алгоритма пропускается, так как применяется только к вершинам, имеющим степень исхода и степень захода, равные единице.

Каким способом вычислительно быстро за полиномиальное время проверить вложение многоугольного орграфа $\overrightarrow{M}$ в орграф $\overrightarrow{H_k} - v_{i-1} - (w, v_i)$ или в орграф $\overrightarrow{H_k} - v_{i+1} - (v_i, w)$, описано ниже.

После того, как все вершины рассмотрены, алгоритм завершает свою работу. Построенный орграф $\overrightarrow{H_k}$ из орграфа $\overrightarrow{H_0}$, где k — количество дуг, удаленных в п. 3 алгоритма, является THP для многоугольного орграфа $\overrightarrow{M}$.

Оценим асимптотическую сложность алгоритма. Время выполнения п. 2 алгоритма равно $O(n)$, так как в нем анализируется степень исхода и степень захода каждой вершины $v_i \in Z$ многоугольного орграфа $\overrightarrow{M} = (Z, \gamma)$ порядка n. Для реализации п. 3 для каждой вершины $v_i \in Z$, не являющейся ни источником, ни стоком, необходимо произвести одну или две проверки многоугольных орграфов на изоморфизм. Изоморфизм многоугольных орграфов устанавливается через анализ их двоичных кодов. Асимптотическая сложность проверки изоморфизма для данного типа орграфов равна $O(n^2)$, так как необходимо из $2n = O(n)$ двоичных векторов многоугольного орграфа выбрать лексикографически минимальный. Так как такую проверку необходимо произвести для не более чем $O(n)$ вершин, то асимптотическая сложность выполнения п. 3 оценивается как $O(n^3)$.

В итоге асимптотическая сложность алгоритма составляет $O(n^3)$.

3. Верхние и нижние оценки количества добавленных дуг в THP для многоугольных орграфов

В THP $\overrightarrow{H}$ для многоугольного орграфа $\overrightarrow{M}$ порядка n может быть от n до $2n$ добавленных дуг, т. е. дуг, инцидентных вершине w. Предложенный алгоритм позволяет описать семейства многоугольных орграфов, на которых достигаются верхняя и нижняя оценки количества добавленных дуг, где под верхней оценкой подразумевается $2n$ добавленных дуг, а под нижней — n добавленных дуг.

Теорема 2 (о верхней оценке количества добавленных дуг в THP для многоугольных орграфов)**.** *Из многоугольных орграфов контуры и только они имеют THP, содержащее $2n$ добавленных дуг.*

Доказательство. Покажем, что контуры имеют $2n$ добавленных дуг в THP. Рассмотрим произвольный контур $\overrightarrow{C_n} = (V, \alpha)$ порядка n, тогда орграф $\overrightarrow{H} = (V \cup \{w\}, \beta)$ такой, что $\overrightarrow{H} \cong \mathrm{TP}(C_n)$, получается из контура $\overrightarrow{C_n}$ добавлением $2n$ дуг, инцидентных вершине w.

Докажем, что орграф $\overrightarrow{H} \cong \mathrm{TP}(\overrightarrow{C_n})$ является THP для контура $\overrightarrow{C_n} = (V, \alpha)$ порядка n. Для этого покажем выполнение всех пунктов теоремы 1.

Очевидно, что первые три пункта теоремы 1 выполняются для тривиальных расширений.

Докажем свойство неприводимости. Пусть некоторой дуги $(v_i, w) \in \beta$, $0 \le i \le n-1$, входящей в вершину w, нет в орграфе $\overrightarrow{H}$. Рассмотрим максимальный подграф $\overrightarrow{H} - v_{i+1} - (v_i, w)$ орграфа $\overrightarrow{H} - (v_i, w)$ такой, что $\overrightarrow{H} - (v_i, w) \cong \mathrm{TP}(\overrightarrow{C}_n) - (v_i, w)$. В подграфе $\overrightarrow{H} - v_{i+1} - (v_i, w)$ получаем $d^+(v_i) = 0$, в то время как степень исхода каждой вершины контура $\overrightarrow{C}_n$ равна единице, $d^+(v) = 1 \quad \forall v \in V$. Следовательно, контур $\overrightarrow{C}_n$ не вкладывается в один из максимальных подграфов орграфа $\overrightarrow{H} - (v_i, w)$. В силу произвольности выбора дуги $(v_i, w) \in \beta$, входящей в вершину w, получаем, что каждая дуга, входящая в вершину w, должна присутствовать в THP для контура $\overrightarrow{C}_n$.

Пусть некоторой дуги $(w, v_i) \in \beta$, $0 \leq i \leq n-1$, выходящей из вершины w, нет в орграфе $\overrightarrow{H}$. Рассмотрим максимальный подграф $\overrightarrow{H} - v_{i-1} - (w, v_i)$ орграфа $\overrightarrow{H} - (w, v_i)$ такой, что $\overrightarrow{H} - (w, v_i) \cong \text{ТР}(\overrightarrow{C}_n) - (w, v_i)$. В подграфе $\overrightarrow{H} - v_{i-1} - (w, v_i)$ получаем $d^-(v_i) = 0$, в то время как степень захода каждой вершины контура $\overrightarrow{C}_n$ равна единице, $d^-(v) = 1 \quad \forall v \in V$. Следовательно, контур $\overrightarrow{C}_n$ не вкладывается в один из максимальных подграфов орграфа $\overrightarrow{H} - (w, v_i)$. В силу произвольности выбора дуги $(w, v_i) \in \beta$, выходящей из вершины w, получаем, что каждая дуга, выходящая из вершины w, должна присутствовать в ТНР для контура $\overrightarrow{C}_n$.

Свойство неприводимости доказано.

Докажем теперь, что контуры порядка n являются единственными многоугольными орграфами, в ТНР которых существует $2n$ добавленных дуг. Действительно, если многоугольный орграф $\overrightarrow{M}$ порядка n не является контуром, то в нем существует хотя бы одна вершина v, являющая либо источником, либо стоком. Тогда по схеме алгоритма у него будет существовать такое ТНР, в котором меньше $2n$ дуг, так как в п. 2 между вершиной v и w будет добавлена только одна дуга.

Таким образом, доказано, что из многоугольных орграфов контуры и только они имеют ТНР, содержащие $2n$ добавленных дуг. □

Следующая теорема показывает общий вид многоугольных орграфов, в ТНР которых содержится n добавленных дуг, т. е. минимально возможное количество.

Теорема 3 (о нижней оценке количества добавленных дуг в ТНР для многоугольных орграфов)**.** *Многоугольные орграфы порядка n, где n четное, с двоичным кодом вида* $0101\ldots01$*, имеют ТНР, содержащие n добавленных дуг.*

Доказательство. Каждая вершина многоугольных орграфов с кодом вида $0101\ldots01$ является либо источником, либо стоком. Следовательно, по схеме алгоритма в п. 2 для таких орграфов будет добавлено ровно n дуг, и впоследствии ни одна из n добавленных дуг не будет удалена. □

Литература

[1] Богомолов А.М., Салий В.Н. *Алгебраические основы теории дискретных систем* (Наука, М., 1997).

[2] Курносова С.Г. Т-*неприводимые расширения для некоторых классов графов*, Теоретические проблемы информатики и ее приложений: Сб. науч. тр. Под ред. проф. А.А. Сытника (Изд-во Саратовск. ун-та, Саратов, 2004), с. 113–125.

[3] Курносова С.Г. Т-*неприводимые расширения полных бинарных деревьев*, Вестн. Томск. гос. ун-та. Прилож., № 14, 158–160 (2005).

[4] Салий В.Н. *Доказательства с нулевым разглашением в задачах о расширениях графов*, Вестн. Томск. гос. ун-та. Прилож., № 6, 63–65 (2003).

[5] Абросимов М.Б. *Некоторые вопросы о минимальных расширениях графов*, Изд-во Саратовск. ун-та. Сер. Матем. Механ. Информатика **6** (1/2), 86–91 (2006).

[6] Hayes J.P. *A graph model for fault-tolerant computing systems*, IEEE transaction on computer **C-26** (9), 875–884 (1976).

[7] Абросимов М.Б. *О сложности некоторых задач, связанных с расширениями графов*, Матем. заметки **88** (5), 643–650 (2010).

[8] Салий В.Н. *Упорядоченное множество связных частей многоугольного графа*, Изв. Саратовск. гос. ун-та **13** (2), 44–51 (2013).

А.В. Гавриков
аспирант, кафедра теоретических основ компьютерной безопасности и криптографии,
Саратовский государственный университет,
ул. Астраханская, д. 83, г. Саратов, 410012, Россия,
e-mail: alexandergavrikov1989@gmail.com

A.V. Gavrikov

T-irreducible extension of polygonal digraphs

Abstract. Directed graphs are mathematical models of discrete systems. T-irreducible extensions are widely used in cryptography and diagnosis of discrete systems. A polygonal origraph is a digraph obtained from a circuit by some orientation of its edges. We propose an algorithm to construct a T-irreducible extension of a polygonal graph.

Keywords: polygonal graph, fault-tolerance of discrete systems, T-irreducible extension.

A.V. Gavrikov
Postgraduate, Chair of Computer Security and Cryptography,
Saratov State University,
83 Astrahanskaya str., Saratov, 410012 Russia,
e-mail: alexandergavrikov1989@gmail.com