МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Приложение

№4 Сентябрь 2011

Свидетельство о регистрации: ПИ №ФС 77-33762
от 16 октября 2008 г.

ТЕЗИСЫ ДОКЛАДОВ
X Сибирской научной школы-семинара с международным участием
«Компьютерная безопасность и криптография» — SIBECRYPT'11
(Томск, ТГУ, 5–10 сентября 2011 г.)

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

СОДЕРЖАНИЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Секция 7

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.7

О САМОЛОКАЛИЗАЦИИ МОБИЛЬНОГО АГЕНТА С ИСПОЛЬЗОВАНИЕМ ТОПОЛОГИЧЕСКИХ СВОЙСТВ СРЕДЫ

И. С. Грунский, С. В. Сапунов

В качестве топологической модели операционной среды рассматриваются конечные неориентированные графы. Вершины этих графов заранее помечены, и мобильный агент (МА) не меняет эти метки. Рассматривается задача определения МА своего положения в среде. Эта задача относится к проблематике взаимодействия управляющей и управляемой систем, являющейся классической для теоретической кибернетики [1, 2]. В настоящее время эта проблема актуальна в связи с задачами навигации автономных мобильных роботов [3].

Конечным графом с помеченными вершинами (помеченным графом) назовем четверку $G = (V, E, M, \mu)$, где V, E, M — конечные множества вершин, ребер и меток соответственно; $\mu : G \to M$ — сюръективная функция разметки. Помеченный неорграф назовем сильно детерминированным (СД-графом), если в замкнутой окрестности любой его вершины все вершины помечены различно. Языком L_g вершины g назовем множество всех слов, порожденных этой вершиной, т.е. последовательностей меток вершин, лежащих на всевозможных путях с началом в вершине g. Будем говорить, что вершины $g, h \in V$ ε-неотличимы, если $L_g = L_h$. Лингвистическим идентификатором (ЛИ) вершины $g \in V$ назовем конечное множество слов $W_g \subsetneq M^+$, таких, что для любой вершины $h \in V$ равенство $W_g \cap L_g = W_g \cap L_h$ выполняется тогда и только тогда, когда $g = h$. Через S_g обозначим подграф графа G, порожденный всеми вершинами, достижимыми из вершины $g \in V$. Будем говорить, что вершины $g, h \in V$ σ-неотличимы, если $S_g \cong S_h$. Пусть G_g и H_h являются инициально-связными помеченными графами с выделенными вершинами g и h соответственно. Обозначим через $G_g \sqcap H_h$ наибольший связный подграф $G'_g \subsetneq G_g$, содержащий выделенную вершину g и изоморфно вложимый в H_h с отображением вершины g в вершину h. Топологическим идентификатором (ТИ) вершины $g \in V$ назовем помеченный граф D_g, такой, что для любой вершины $h \in V$ изоморфизм $D_g \sqcap S_g \cong D_g \sqcap S_h$ существует тогда и только тогда, когда $g = h$. Показано, что $\sigma \subsetneq \varepsilon$, причем обратное включение не выполняется. Предложены полиномиальные методы построения ЛИ и ТИ вершин помеченных графов. Показано, что гомоморфный образ растущего помеченного дерева, соответствующего ЛИ вершины $g \in V$, является ТИ этой вершины. Показано, что обратное утверждение в общем случае неверно.

Экспериментом с графом G относительно априорной информации I, цели C и средств S назовем процесс, состоящий из трех этапов: 1) построение некоторого теста P на основе I и C; 2) получение мобильным агентом экспериментальных данных W на основе P и S; 3) вывод заключений о свойствах графа на основе W и I. Априорная информация — это класс графов, которому принадлежит G. В качестве S выступают возможности МА перемещаться по ребрам графа от вершины к вершине, оставлять маркер в текущей вершине, а также обнаруживать и подбирать маркер в случае его нахождения в текущей вершине. Эксперимент назовем диагностическим (ДЭ), если априори полностью известен граф G, МА установлен в произвольную начальную вершину этого графа, и целью эксперимента является определение этой вершины, т.е. различение этой вершины от всех других вершин.

В работах [4, 5] авторами были предложены методы построения и реализации ДЭ с помеченными графами, основывающиеся на проверке ε-эквивалентности вершин при помощи их ЛИ. В них в качестве теста P берётся множество слов, являющееся объединением ЛИ всех вершин графа.

В данной работе в качестве теста P используется помеченный граф, называемый далее диагностическим тестовым графом (ДТГ) и определяемый по следующим правилам: 1) отождествим все одинаково помеченные инициальные вершины ТИ D_g всех $g \in V$; 2) детерминизируем остовные деревья всех графов D_g, то есть многократно и исчерпывающе применим следующую операцию: если в множество преемников некоторой вершины попадают вершины с одинаковыми метками, то такие вершины отождествляются с заменой возникающих кратных дуг одной дугой.

Первый этап диагностического эксперимента состоит в построении ДТГ P. На втором этапе получение экспериментальных данных заключается в том, что МА, стартуя из неизвестной ему вершины h графа G, проверяет наличие/отсутствие в G путей, совпадающих по разметке с путями обхода в ширину графа P из его инициальной вершины. В зависимости от исхода каждой из этих проверок сокращается множество гипотетически возможных начальных вершин. По окончании работы алгоритма остается ровно одна такая вершина.

Показано, что для СД-графов временная сложность данного алгоритма проведения диагностического эксперимента полиномиальна от числа вершин исследуемого графа.

ЛИТЕРАТУРА

1. *Кудрявцев В. Б., Алешин С. В., Подколзин А. С.* Введение в теорию автоматов. М.: Наука, 1985.
2. *Капитонова Ю. В., Летичевский А. А.* Математическая теория проектирования вычислительных систем. М.: Наука, 1988.
3. *Dudek G. and Jenkin M.* Computational Principles of Mobile Robotics. Cambridge: Cambridge University Press, 2000.
4. *Сапунов С. В.* Определение положения робота в топологической среде // Искусственный интеллект. 2008. Т. 4. С. 558–565.
5. *Грунский И. С., Сапунов С. В.* Идентификация вершин помеченных графов // Труды ИПММ НАН Украины. 2010. Т. 21. С. 86–97.

УДК 512.2

О КОНГРУЭНЦИЯХ ЦЕПЕЙ

Е. О. Карманова

Под ориентированным графом (далее орграфом) понимается пара $G = (V, \alpha)$, где V — конечное непустое множество вершин; α — отношение на V, задающее множество дуг. Основные понятия приводятся в соответствии с [1].

Существуют различные методы преобразования графовых систем для приложений к проблемам оптимизации в различных ситуациях. В качестве допустимых реконструкций данного графа обычно рассматриваются следующие [2]:

1) отождествление некоторых вершин графа;
2) ориентация ребер данного неориентированного графа;
3) переориентация некоторых дуг;
4) добавление новых дуг (ребер);
5) удаление некоторых дуг (ребер).

Будем рассматривать реконструкцию типа 1.