Platinum Jubilee Series

Statistical Science and
Interdisciplinary Research — Vol. 3

Algorithms, Architectures and Information Systems Security

Editors

Bhargab B. Bhattacharya
Susmita Sur-Kolay
Subhas C. Nandy
Aditya Bagchi

Series Editor: ***Sankar K. Pal***

World Scientific

Platinum Jubilee Series

Statistical Science and
Interdisciplinary Research — Vol. 3

Algorithms, Architectures and Information Systems Security

Editors

Bhargab B. Bhattacharya

Susmita Sur-Kolay

Subhas C. Nandy

Aditya Bagchi

Indian Statistical Institute, India

Series Editor: ***Sankar K. Pal***

World Scientific

NEW JERSEY · LONDON · SINGAPORE · BEIJING · SHANGHAI · HONG KONG · TAIPEI · CHENNAI

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ALGORITHMS, ARCHITECTURES AND INFORMATION SYSTEMS SECURITY

Statistical Science and Interdisciplinary Research — Vol. 3

ISBN-13 978-981-283-623-6

ISBN-10 981-283-623-3

Printed in Singapore by B & JO Enterprise

Algorithms, Architectures and Information Systems Security

Statistical Science and Interdisciplinary Research

Series Editor: Sankar K. Pal *(Indian Statistical Institute)*

Description:
In conjunction with the Platinum Jubilee celebrations of the Indian Statistical Institute, a series of books will be produced to cover various topics, such as Statistics and Mathematics, Computer Science, Machine Intelligence, Econometrics, other Physical Sciences, and Social and Natural Sciences. This series of edited volumes in the mentioned disciplines culminate mostly out of significant events — conferences, workshops and lectures — held at the ten branches and centers of ISI to commemorate the long history of the institute.

Vol. 1 Mathematical Programming and Game Theory for Decision Making
edited by S. K. Neogy, R. B. Bapat, A. K. Das & T. Parthasarathy
(Indian Statistical Institute, India)

Vol. 2 Advances in Intelligent Information Processing:
Tools and Applications
edited by B. Chandra & C. A. Murthy
(Indian Statistical Institute, India)

Vol. 3 Algorithms, Architectures and Information Systems Security
edited by Bhargab B. Bhattacharya, Susmita Sur-Kolay,
Subhas C. Nandy & Aditya Bagchi
(Indian Statistical Institute, India)

Foreword

The Indian Statistical Institute (ISI) was established on 17th December, 1931 by Prof. Prasanta Chandra Mahalanobis, a great visionary, to promote research in the theory and applications of statistics as a new scientific discipline in India. In 1959, Pandit Jawaharlal Nehru, the then Prime Minister of India introduced the ISI Act in the Parliament and designated it as an Institution of National Importance because of its remarkable achievements in statistical work as well as its contribution to economic planning for social welfare.

Today, the Indian Statistical Institute occupies a prestigious position in the academic firmament. It has been a haven for bright and talented academics working in a number of disciplines. Its research faculty has done India proud in the arenas of Statistics, Mathematics, Economics, Computer Science, among others. Over the last seventy five years, it has grown into a massive banyan tree, as epitomized in the emblem of the institute. The Institute now serves the nation as a unified and monolithic organization from different places, namely Kolkata, the Head Quarters, Delhi and Bangalore, two centers, a network of six SQC-OR Units located at Mumbai, Pune, Baroda, Hyderabad, Chennai and Coimbatore, and a branch (field station) at Giridih.

The platinum jubilee celebrations of ISI had been launched by Honorable Prime Minister Prof. Manmohan Singh on December 24, 2006, and the Govt. of India has declared 29th June as the "Statistics Day" to commemorate the birthday of Prof. Mahalanobis nationwide.

Prof. Mahalanobis was a great believer in interdisciplinary research, because he thought that this will promote the development of not only Statistics, but also the other natural and social sciences. To promote interdisciplinary research, major strides were made in the areas of computer science, statistical quality control, economics, biological and social sciences, physical and earth sciences.

The Institute's motto of 'unity in diversity' has been the guiding principle of all its activities since its inception. It highlights the unifying role of statistics in relation to various scientific activities.

In tune with this hallowed tradition, a comprehensive academic program, involving Nobel Laureates, Fellows of the Royal Society, and other dignitaries, has been implemented throughout the Platinum Jubilee year, highlighting the emerging areas of ongoing frontline research in its various scientific divisions, centres, and outlying units. It includes international and national-level seminars, symposia, conferences and workshops, as well as several special lectures. As an outcome of these events, the Institute is bringing out a series of comprehensive volumes in different subjects under the title Statistical Science and Interdisciplinary Research, published by the World Scientific Publishing, Singapore.

The present volume titled "Algorithms, Architectures, and Information Systems Security" is the third one in the series. It has sixteen chapters, written by eminent scientists from different parts of the world, dealing with three major topics of computer science. The first part of the book deals with computational geometric problems and related algorithms, which have several applications in areas like pattern recognition and computer vision, the second part addresses the issues of optimization in VLSI design and test architectures, and in wireless cellular networks, while the last part concerns with different problems, issues and methods of information systems security. I believe, the state-of-the art studies presented in this book will be very useful to the readers.

Thanks to the contributors for their excellent research articles and to volume editors Dr. B. B. Bhattacharya, Dr. S. Sur-Kolay, Dr. S. C. Nandy and Dr. A. Bagchi for their sincere effort in bringing out the volume nicely in time. Initial design of the cover by Mr. Indranil Dutta is acknowledged. Thanks are also due to World Scientific for their initiative in publishing the series and being a part of the Platinum Jubilee endeavor of the Institute. Sincere efforts by Prof. Dilip Saha and Dr. Barun Mukhopadhyay for editorial assistance are appreciated.

April 2008
Kolkata

Sankar K. Pal
Series Editor and Director

Preface

It is our great pleasure to compile the Platinum Jubilee Commemorative Monograph Series of the Indian Statistical Institute: Volume 3, titled Algorithms, Architectures, and Information Systems Security. This volume contains mostly a collection of invited papers from leading researchers. It also includes the extended versions of a few papers, which were presented at the Second International Conference on Information Systems Security (December 18–20, 2006), and in Track I of the International Conference on Computing: Theory and Applications (March 5–7, 2007), both held in Kolkata as part of the Platinum Jubilee celebration of the Institute (1931–2006).

There are sixteen chapters in this volume. The first five chapters (Chapters 1–5) address several challenging geometric problems and related algorithms. The next five chapters (Chapters 6–10) focus on various optimization issues in VLSI design and test architectures, and in wireless cellular networks. The last six chapters (Chapters 11–16) comprise scholarly articles on Information Systems Security.

Chapter 1 by Li and Klette presents two important rubberband algorithms for computing Euclidean shortest paths in a simple polygon, which have major applications in 2D pattern recognition, picture analysis, and in robotics. The second chapter by Cheng, Dey, and Levine contains the theoretical analysis of a Delaunay refinement algorithm for meshing various types of 3D domains such as polyhedra, smooth and piecewise smooth surfaces, volumes enclosed by them, and also non-manifold spaces. In Chapter 3, Pach and Tóth characterize the families of convex sets in a plane that are not representable by a point set of the same order type. Further, they establish the size of the largest subfamily representable by points and discuss related Ramsey-type geometric problems. The fourth chapter by Asano, Katoh, Mehlhorn, and Tokuyama describes efficient algorithms for some generalizations of least-squares method. These are useful in approximating a data set by a polyline with one joint that minimizes the total sum of squared vertical errors. A few other related geometric optimization problems have also been studied. Chapter 5 by Wei and Klette addresses the depth recovery problem from gradient

vector fields. This has tremendous significance in 3D surface reconstruction and has several applications in computer vision. The authors present three schemes: a two-scan method, a Fourier-transform based method, and a wavelet-transform based method.

In Chapter 6, Börner, Leininger, and Gössel present a new design of a single-output convolutional compactor for guaranteed 6-bit error detection. In Electronic Design Automation, such detectors are of importance for compressing test and diagnostic data of large VLSI circuits. Bhattacharya, Seth, and Zhang address the problem of low-energy pattern generation for random testing VLSI chips in Chapter 7. The method suits well in scan-based systems, and reduces test application time significantly. Chapter 8 by Taghavi and Sarrafzadeh has a review of existing methodologies for estimation and reduction of routing congestion at the floorplanning and placement phases of VLSI design cycle, followed by a novel contribution on a more general and accurate approach. The ninth chapter by Sinha and Audhya deals with the channel assignment problem in a hexagonal cellular network with two-band buffering that supports multimedia services. New lower bounds on minimum bandwidth requirement are derived and algorithms for channel assignment are presented. Chapter 10 by Das, Das, and Nandy contains an extensive survey on range assignment problems in various types of wireless networks, and their computational geometric solutions.

Focusing on the emerging problems of privacy in the electronic society, Ardagna, Cremonini, Damiani, De Capitani di Vimercati, and Samarati have highlighted in Chapter 11, the issues related to the protection of personal data released in an open public network. This chapter considers the combination of different security policies and their enforcement against a laid down privacy policy or a possible privacy law. It also considers the protection of location information in location-based services. In Chapter 12, Chen and Atluri discuss a situational role-based access control and risk-based access control mechanism in a networked environment where personal data often kept with third parties, need stringent security measures to be relaxed only in case of an emergency. In Chapter 13, Jajodia and Noel propose a framework for Topological Vulnerability Analysis (TVA) of a network connecting individual components of a distributed system. It simulates the possible ways for incremental network penetration and builds complete maps of multi-step-attacks discovering all possible attack paths. TVA also computes network hardening options to protect critical resources against minimal network changes. Chapter 14 by Dash, Reddy, and Pujari presents a new malicious code detection technique using variable length n-grams based on the concept of episodes. The authors have pointed out that proper feature extraction and selection technique can help in efficiently detecting virus programs. The next

chapter (Chapter 15) addresses an important area of research called digital image forensics, which stems from the need for creation, alteration and manipulation of digital images. Sencar and Memon provide an excellent survey of the recent developments covering image source identification, discrimination of synthetic images, and image forgery detection. The last chapter (Chapter 16) by Butler, Enck, Traynor, Plasterr, and McDaniel deals with privacy preserving web-based email. In spite of the privacy policies stipulated by the service providers of web-based applications, personal information of the users collected by them may have indefinite life and can later be used without restriction. The authors have proposed a method to create virtual channels over online services, through which messages and cryptographic keys are delivered for preserving privacy.

We take this opportunity to express our heartfelt gratitude to all the eminent contributors of this monograph on Algorithms, Architectures, and Information Systems Security. We are also grateful to Prof. Sankar K. Pal, Director of the Indian Statistical Institute, for his support and encouragement in preparing the volume. We earnestly hope that this collection of technical articles would be of archival value to the peer community. Finally, the help of Mr. Indranil Dutta to prepare the camera-ready version is gratefully acknowledged.

Bhargab B. Bhattacharya
Susmita Sur-Kolay
Subhas C. Nandy
Aditya Bagchi

Contents

Chapter 1

Euclidean Shortest Paths in a Simple Polygon

Fajie Li and Reinhard Klette

Computer Science Department, The University of Auckland, Auckland, New Zealand

Let p and q be two points in a simple polygon Π. This chapter provides two rubberband algorithms for computing a shortest path between p and q that is contained in Π. The two algorithms use previously known results on triangular or trapezoidal decompositions of simple polygons, and have either $O(n)$ or $O(n \log n)$ time complexity (where the super-linear time complexity is only due to preprocessing, i.e. for the trapezoidal decomposition of the simple polygon Π).

Contents

1.1 Introduction

Algorithms for computing Euclidean shortest paths (ESPs) between two points p and q of a simple polygon Π, where the path is restricted to be fully contained in Π, have applications in two-dimensional (2D) pattern recognition, picture analysis, robotics, and so forth. They have been intensively studied.[1–4]

There is Chazelle's[5] linear-time algorithm for triangulating a simple polygon, or an easier to describe, but $O(n \log n)$ algorithm for partitioning a simple polygon into trapezoids.[6] The design of algorithms for calculating ESPs within a simple polygon may use one of both partitioning algorithms as a preprocess. This chapter shows how rubberband algorithms[7] may be used to calculate approximate or exact ESPs within simple polygons, using either decompositions into triangles or into trapezoids.

For a start we prove a basic property of exact ESPs for such cases; see also Ref. 8:

Proposition 1.1 *Each vertex* ($\neq p, q$) *of the shortest path is a vertex of* Π.

To see this, let $\rho = \langle p, p_1, p_2, \ldots, p_k, q \rangle$ be the shortest path from p to q completely contained in simple polygon Π. Assume that at least one $p_i \in \rho$ is not a vertex of Π. Also assume that each p_i is not *redundant*, which means that $p_{i-1}p_ip_{i+1}$ must be a triangle (i.e., three points p_{i-1}, p_i and p_{i+1} are not collinear), where $i = 1, 2, \ldots, k$ and $p_0 = p$, $p_{k+1} = q$.

Case 1: Non of the two edges $p_{i-1}p_i$ and p_ip_{i+1} is on a tangent of Π (see Figure 1.1, left); then there exists a sufficiently small neighborhood of p_i, denoted by $U(p_i)$, such that for each point $p' \in U(p_i) \cap \triangle p_{i-1}p_ip_{i+1} \subset \Pi^\bullet$ (the topological closure of a simple polygon Π), both edges $p_{i-1}p_i$ and p_ip_{i+1} are completely contained in Π. By elementary geometry, we have that $d_e(p_{i-1}, p') + d_e(p', p_{i+1}) < d_e(p_{i-1}, p_i) + d_e(p_i, p_{i+1})$, where d_e denotes Euclidean distance. Therefore we may obtain a shorter path from p to q by replacing p_i by p'. This is a contraction to the assumption that p_i is a vertex of the shortest path ρ.

Case 2: Both $p_{i-1}p_i$ and p_ip_{i+1} are on tangents of Π (see Figure 1.1, middle); then we can also derive a contradiction. In fact, let p'_{i-1} and p'_{i+1} be the closest vertices of Π such that $p'_{i-1}p_i$ and $p_ip'_{i+1}$ are on tangents of Π. Analogous to the first case, there exists a point p' such that the polygonal path $p'_{i-1}p'p'_{i+1}$ is completely contained in $\Pi^\bullet$ and the length of $p'_{i-1}p'p'_{i+1}$ is shorter than $p'_{i-1}p_ip'_{i+1}$. This is a contradiction as well.

Case 3: Either $p_{i-1}p_i$ or p_ip_{i+1} is a tangent of Π (see Figure 1.1, right); then we may arrive at the same result as in Case 2.

This chapter is organized as follows. At first we introduce into rubberband algorithms. Then we recall briefly decompositions of simple polygons and specify (as a preliminary result) two approximate rubberband algorithms; we provide examples of using them. These two algorithms are finally transformed into two exact rubberband algorithms; we analyze their correctness and time complexity.

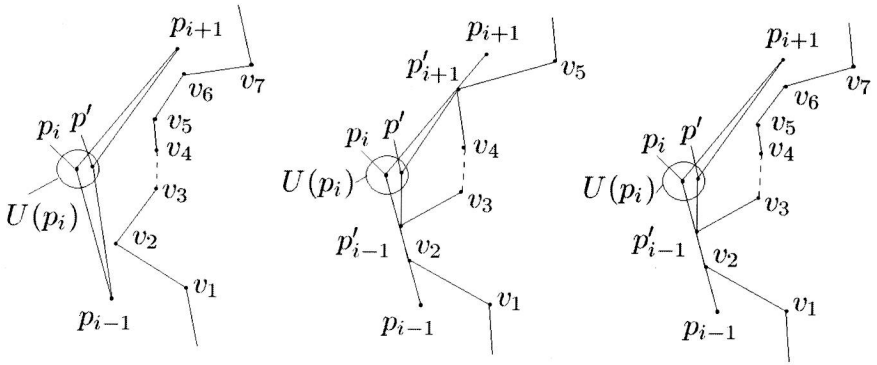

Fig. 1.1 Illustration that each vertex of a shortest path is a vertex of Π, where $v_1v_2v_3v_4v_5...$ is a polygonal part of the border of the simple polygon Π. Left, middle, right illustrate Cases 1, 2, 3 as discussed in the text, respectively.

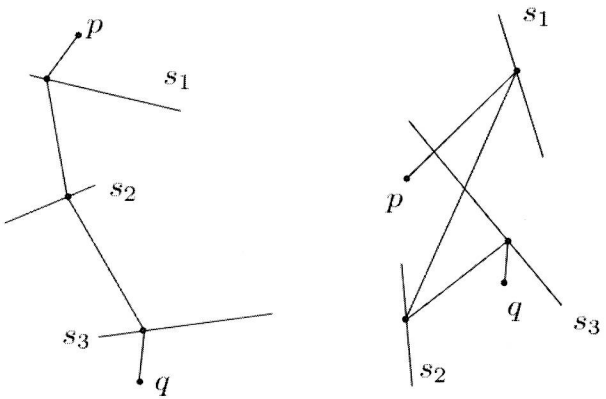

Fig. 1.2 Two step sets with possible initializations of Algorithm 1, both for $k = 3$.

1.2 Basics of Rubberband Algorithms

We explain basic ideas of a rubberband algorithm by using the following, very simple 2D example. In general, rubberband algorithms are for exact or approximate calculations of ESPs for 2D or 3D applications.[9]

Let Π be a plane. Assume that there are $k > 1$ line segments $s_i \subset \Pi$ (for $i = 1, 2, \ldots, k$) such that $s_i \cap s_j = \emptyset$, for $i \neq j$ and $i, j = 1, 2, \ldots, k$; see Figure 1.2. The following simple rubberband algorithm (see Figure 1.3) approximates a shortest path from p to q that intersects all the given segments s_i (at least once) in the given order.

The accuracy parameter in Step 1 can be chosen such that maximum possible numerical accuracy (on the given computer) is guaranteed. The initial path in Step 2 may, for example, be defined by centers of line segments. Vertices of the calculated path move by local optimization, until the total length of the path between two iterations only differs by ε at most. The series of lengths L calculated for each iteration forms a decreasing Cauchy sequence lower bounded by zero, and is thus guaranteed to converge to a minimum length. The path defined by this convergence is called *the limit path* of Algorithm 1. In relation to Proposition 1.1, we have the following for Algorithm 1:

Proposition 1.2 *Each vertex* ($\neq p, q$) *of the limit path of Algorithm 1 is a vertex of* Π.

Proof Let $\rho = \langle p, p_1, p_2, \ldots, p_k, q \rangle$ be the limit path from p to q of Algorithm 1. Let $i = 1, 2, \ldots,$ or k and $p_0 = p$, $p_{k+1} = q$. Assume that each $p_i \in \rho$ is not redundant. Then p_i must be an endpoint of s_i. (Otherwise, $p_i = p_{i-1}p_{i+1} \cap s_i$. This contradicts the assumption that p_i is not redundant.) It follows that p_i must be a vertex of Π. □

1. Let $\varepsilon = 10^{-10}$ (the chosen accuracy).
2. Compute the length L_1 of the initial path $\rho = \langle p, p_1, p_2, \ldots, p_k, q \rangle$.
3. Let $q_1 = p$ and $i = 1$.
4. While $i < k - 1$ do:
4.1. Let $q_3 = p_{i+1}$.
4.2. Compute a point $q_2 \in s_i$ such that
$d_e(q_1, q_2) + d_e(q_3, q_2) = \min\{d_e(q_1, q) + d_e(q_3, q) : q \in s_i\}$.
4.3. Update ρ by replacing p_i by q_2.
4.4. Let $q_1 = p_i$ and $i = i + 1$.
5.1. Let $q_3 = q$.
5.2. Compute $q_2 \in s_k$ such that
$d_e(q_1, q_2) + d_e(q_3, q_2) = \min\{d_e(q_1, q) + d_e(q_3, q) : q \in s_k\}$.
5.3. Update ρ by replacing p_k by q_2.
6. Compute the length L_2 of the updated path $\rho = \langle p, p_1, p_2, \ldots, p_k, q \rangle$.
7. Let $\delta = L_1 - L_2$.
8. If $\delta > \varepsilon$, then let $L_1 = L_2$ and go to Step 3.
Otherwise, stop.

Fig. 1.3 Algorithm 1: a simple rubberband algorithm for a given set of line segments.

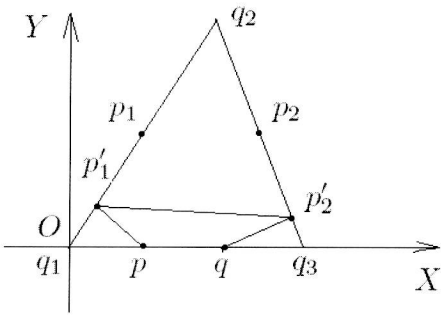

Fig. 1.4 Illustration of steps with joint endpoints.

The set $\{s_1, s_2, \ldots, s_k\}$ is a *step set* of a rubberband algorithm if its union contains all the vertices of the calculated path, and each s_i is a *step element* of the rubberband algorithm that contains at least one vertex of the calculated path, for $i = 1, 2, \ldots, k$.

In this chapter, step sets are sets of line segments, which may have joint endpoints, but cannot have further points in common. Furthermore, in this chapter, each step element contains exactly one vertex of the shortest path. For example, if the input for Algorithm 1 is as in Figure 1.4, with

$$s_1 = q_1q_2, s_2 = q_2q_3, q_1 = (0,0), q_2 = (2,4), q_3 = (3,0), p = (1,0), q = (2,0)$$

then we also have segments with joint endpoints. Assume a path initialization using p_1 and p_2, the centers of s_1 and s_2, respectively [i.e., $p_1 = (1,2)$, and $p_2 = (2.5,2)$]. We obtain that the length of the initialized polyline $\rho = \langle p, p_1, p_2, q \rangle$ is equal to 5.5616 (rounded to four digits). Algorithm 1 calculates an approximate shortest path $\rho = \langle p, p'_1, p'_2, q \rangle$ where $p'_1 = (0.3646, 0.7291)$, $p'_2 = (2.8636, 0.5455)$ and the length of it is equal to 4.4944 (see Table 1.1, which lists resulting δs for the number I of iterations). That means, Algorithm 1 is also able to deal with this input for the assumed initialization.

Table 1.1 Number I of iterations and resulting δs for the initialization illustrated by Figure 1.4 [i.e., with $p_1 = (1,2)$ and $p_2 = (2.5,2)$ as initial points on the path].

I	δ	I	δ	I	δ	I	δ
1	−0.8900	3	−0.0019	5	−8.4435e-008	7	−3.5740e-012
2	−0.1752	4	−1.2935e-005	6	−5.4930e-010		