



PERSPECTIVES IN COMPUTING

W. RHEINBOLDT, D. SIEWIOREK, EDITORS

Discrete Algorithms and Complexity

**Proceedings of the Japan-US Joint Seminar
June 4–6, 1986, Kyoto, Japan**

Edited by
David S. Johnson, Takao Nishizeki,
Akihiro Nozaki, Herbert S. Wilf

Discrete Algorithms and Complexity

**Proceedings of the Japan-US Joint Seminar
June 4 – 6, 1986, Kyoto, Japan**

Edited by

David S. Johnson

*AT&T Bell Laboratories
Murray Hill, New Jersey*

Takao Nishizeki

*Tohoku University
Sendai, Japan*

Akihiro Nozaki

*International Christian University
Tokyo, Japan*

Herbert S. Wilf

*University of Pennsylvania
Philadelphia, Pennsylvania*



ACADEMIC PRESS, INC.
Harcourt Brace Jovanovich, Publishers

Boston Orlando San Diego
New York Austin London Sydney
Tokyo Toronto

Copyright © 1987 by Academic Press, Inc.

All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

Academic Press, Inc.

Orlando, Florida 32887

United Kingdom Edition published by

ACADEMIC PRESS INC. (LONDON) LTD.

24-28 Oval Road, London NW1 7DX

Library of Congress Cataloging-in-Publication Data

Discrete algorithms and complexity; proceedings
of the Japan-US Joint Seminar, June 4-6, 1986,
Kyoto, Japan.

(Perspectives in computing ; vol. 15)

1. Electronic digital computers—Programming—
Congresses. 2. Algorithms—Congresses. 3. Computational
complexity—Congresses. I. Johnson, David S., Date

II. Japan-US Joint Seminar on Discrete
Algorithms and Complexity Theory (1986 : Kyoto, Japan)

III. Series.

QA76.6.D577 1987 511 86-33469

ISBN 0-12-386870-X (alk. paper)

87 88 89 90 9 8 7 6 5 4 3 2 1

Printed in the United States of America

Discrete Algorithms and Complexity

PERSPECTIVES IN COMPUTING, Vol. 15

**(Formerly “Notes and Reports in Computer Science and
Applied Mathematics”)**

W. Rheinboldt and D. Siewiorek, editors

Contributors

- Akeo Adachi (311), *IBM Science Institute, 5-19 Sanban-cho, Chiyoda-ku, Tokyo 102, Japan*
- Leonard Adleman (237), *Department of Computer Science, University of Southern California, Los Angeles, CA 90089-0782, USA*
- Michael Albertson (35), *Department of Mathematics, Smith College, Northampton, MA 01063, USA*
- Takao Asano (51), *Department of Mechanical Engineering, Sophia University, Tokyo 102, Japan*
- Tetsuo Asano (51, 65), *Osaka Electro-Communication University, Neyagawa, Osaka 572, Japan*
- F.R.K. Chung (351), *Bell Communications Research, Morristown, New Jersey 07960, USA*
- Toru Fujiwara (263), *Department of Information and Computer Sciences, Faculty of Engineering Science, Osaka University, Toyonaka 560, Japan*
- Shafi Goldwasser (287), *MIT, Laboratory for Computer Science, Cambridge, MA 02139, USA*
- R.L. Graham (351), *Bell Laboratories, Murray Hill, New Jersey 07974, USA*
- E. Hare (437), *Department of Mathematical Sciences, Clemson University, Clemson, SC 29631, USA*
- Stephen T. Hedetniemi (437), *Department of Computer Science, Clemson University, Clemson, SC 29631, USA*
- John Hopcroft (201), *Department of Computer Science, Cornell University, Ithaca, NY 14853, USA*
- Juraj Hromkovič (389), *Department of Theoretical Cybernetics, Comenius University, 842-15 Bratislava, Czechoslovakia*
- Joan Hutchinson (81), *Department of Mathematics, Smith College, Northampton, MA 01063, USA*

- Toshihide Ibaraki (185), *Department of Applied Mathematics and Physics, Faculty of Engineering, Kyoto University, Kyoto 606, Japan*
- Yoshihide Igarashi (161), *Department of Computer Science, Gunma University, Kiryu 376, Japan*
- Hiroshi Imai (417), *Department of Computer Science and Communication Engineering, Kyushu University, Fukuoka 812, Japan*
- Katsushi Inoue (389), *Department of Electronics, Faculty of Engineering, Yamaguchi University, Ube 755, Japan*
- Masao Iri (417), *Department of Mathematical Engineering and Instrumentation Physics, Faculty of Engineering, University of Tokyo, Tokyo 113, Japan*
- Kazuo Iwama (223), *Kyoto Sangyo University, Kyoto 603, Japan*
- Shigeki Iwata (405), *Information Science Laboratory, Tokai University, Hiratsuka 259-12, Japan*
- Yoji Kajitani (5), *Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo 152, Japan*
- Anna R. Karlin (459), *Computer Science Department, Stanford University, Stanford, CA 94305, USA*
- Richard M. Karp (1), *Computer Science Division, University of California, Berkeley, CA 94720, USA*
- Takumi Kasai (311, 405), *Department of Computer Science, University of Electro-Communications, Chofu, Tokyo 182, Japan*
- Tadao Kasami (263), *Department of Information and Computer Sciences, Faculty of Engineering Science, Osaka University, Toyonaka 560, Japan*
- Kojiro Kobayashi (325), *Department of Information Sciences, Tokyo Institute of Technology, O-okayama, Meguro-ku, Tokyo 152, Japan*
- Renu Laskar (437), *Department of Mathematical Sciences, Clemson University, Clemson, SC 29631, USA*
- Hajime Machida (107), *Department of Computer Science, University of Electro-Communications, Chofu, Tokyo 182, Japan*
- Mark S. Manasse (459), *DEC Systems Research Center, Palo Alto, CA, USA*
- Kevin S. McCurley (237), *Department of Mathematics, University of Southern California, Los Angeles, CA 90089-1113, USA*
- Silvio Micali (287), *MIT, Laboratory for Computer Science, Cambridge, MA 02139, USA*
- Gary L. Miller (81), *Department of Computer Science, University of Southern California, Los Angeles, CA 90089, USA*
- Takao Nishizeki (99), *Department of Electrical Communications, Faculty of Engineering, Tohoku University, Sendai 980, Japan*
- Takao Ozawa (5), *Department of Electrical Engineering, Kyoto University, Kyoto 606 Japan*
- Ken Peters (437), *Department of Mathematical Sciences, Clemson University, Clemson, SC 29631, USA*

- Carl Pomerance (119), *Department of Mathematics, The University of Georgia, Athens, Georgia 30602, USA*
- Ronald L. Rivest (287), *MIT, Laboratory for Computer Science, Cambridge, MA 02139, USA*
- Larry Rudolph (459), *Computer Science Department, Hebrew University, Jerusalem, Israel*
- Kakuhiro Sado (161), *Department of Computer Science, Gunma University, Kiryu 376, Japan*
- Nobuji Saito (99), *Department of Electrical Communications, Faculty of Engineering, Tohoku University, Sendai 980, Japan*
- M.E. Saks (351), *Bell Communications Research, Morristown, New Jersey 07960, USA*
- Daniel D. Sleator (459), *Computer Science Department, Carnegie-Mellon University, Pittsburgh, PA 15213, USA*
- Hitoshi Suzuki (99), *Department of Electrical Communications, Faculty of Engineering, Tohoku University, Sendai 980, Japan*
- Naofumi Takagi (145), *Department of Information Science, Faculty of Engineering, Kyoto University, Kyoto, 606, Japan*
- Itsuo Takanami (389), *Department of Electronics, Faculty of Engineering, Yamaguchi University, Ube 755, Japan*
- Ken-ichi Taniguchi (263), *Department of Information and Computer Sciences, Faculty of Engineering Science, Osaka University, Toyonaka 560, Japan*
- Godfried T. Toussaint (65), *School of Computer Science, McGill University, Montreal, Canada*
- Shuichi Ueno (5), *Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo 152, Japan*
- Herbert S. Wilf (341), *Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104, USA*
- T.V. Wimer (437), *Department of Mathematics, Clarion University of Pennsylvania, Clarion, PA 16214, USA*
- Shuzo Yajima (145), *Department of Information Science, Faculty of Engineering, Kyoto University, Kyoto, 606, Japan*
- Hiroto Yasuura (145), *Department of Information Science, Faculty of Engineering, Kyoto University, Kyoto, 606, Japan*
- Nancy A. Yoshimura (341), *Department of Computer and Information Science, University of Pennsylvania, Philadelphia, PA 19104, USA*

Foreword

The Japan-US Joint Seminar on Discrete Algorithms and Complexity Theory was held 4 – 6 June, 1986, in Kyoto, Japan. It was jointly organized by A. Nozaki and H.S. Wilf and generously sponsored by the Japan Society for Promotion of Sciences and the U.S. National Science Foundation. Thirty-three of the participants were invited to give talks. This volume contains most of the papers presented there.

Some papers describe the state of the art in specific fields, some explore new problems, and others present new results that will soon appear in more detailed form in scientific journals. We expect that the reader will come away from this volume with a better understanding of and insight into Discrete Algorithms and Complexity.

The editors wish to thank all delegates; their efforts made the seminar stimulating and fruitful. Especially we would like to express our gratitude to the executive committee of the Seminar: Takao Asano, Tetsuo Asano, Kazuo Iwama, Shigeki Iwata, Takumi Kasai and Hajime Machida. Finally, we would like to thank the staff of Academic Press Boston for their cooperation in producing this volume.

*David S. Johnson
Takao Nishizeki
Akihiro Nozaki
Herbert S. Wilf*

PERSPECTIVES IN COMPUTING

- Vol. 1 John R. Bourne, *Laboratory Minicomputing*
- Vol. 2 Carl Tropper, *Local Computer Network Technologies*
- Vol. 3 Kendall Preston, Jr., and Leonard Uhr, editors, *Multicomputers and Image Processing: Algorithms and Programs*
- Vol. 4 Stephen S. Lavenberg, editor, *Computer Performance Modeling Handbook*
- Vol. 5 R. Michael Hord, *Digital Image Processing of Remotely Sensed Data*
- Vol. 6 Sakti P. Ghosh, Y. Kambayashi, and W. Lipski, editors, *Data Base File Organization: Theory and Applications of the Consecutive Retrieval Property*
- Vol. 7 Ulrich W. Kulisch and Willard L. Miranker, editors, *A New Approach to Scientific Computation*
- Vol. 8 Jacob Beck, Barbara Hope, and Azriel Rosenfeld, editors, *Human and Machine Vision*
- Vol. 9 Edgar W. Kaucher and William L. Miranker, *Self-Validating Numerics for Function Space Problems: Computation with Guarantees for Differential and Integral Equations*
- Vol. 10 Mohamed S. Abdel-Hameed, Erhan Çinlar, and Joseph Quinn, editors, *Reliability Theory and Models: Stochastic Failure Models, Optimal Maintenance Policies, Life Testing, and Structures*
- Vol. 11 Mark G. Karpovsky, editor, *Spectral Techniques and Fault Detection*
- Vol. 12 Selim G. Akl, *Parallel Sorting Algorithms*
- Vol. 13 Azriel Rosenfeld, editor, *Human and Machine Vision II*
- Vol. 14 Y.C. Tay, *Locking Performance in Centralized Databases*
- Vol. 15 David S. Johnson, Takao Nishizeki, Akihiro Nozaki, Herbert S. Wilf, editors, *Discrete Algorithms and Complexity: Proceedings of the Japan-US Joint Seminar, June 4 – 6, 1986, Kyoto, Japan*

Volumes 1 – 12 were published as **Notes and Reports in Computer Science and Applied Mathematics**.

Contents

<i>Contributors</i>	<i>vii</i>
<i>Foreword</i>	<i>xi</i>
An Upper Bound on the Expected Cost of an Optimal Assignment <i>R.M. Karp</i>	1
The Principal Partition of Vertex-Weighted Graphs and Its Applications <i>T. Ozawa*, Y. Kajitani, and S. Ueno</i>	5
Generalized Colorings <i>M.O. Albertson</i>	35
Voronoi Diagram for Points in a Simple Polygon <i>T. Asano* and T. Asano</i>	51
Computing the Geodesic Center of a Simple Polygon <i>T. Asano* and G. Toussaint</i>	65
On Deleting Vertices to Make a Graph of Positive Genus Planar <i>J.P. Hutchinson* and G.L. Miller</i>	81
Algorithms for Routing around a Rectangle (Extended Abstract) <i>H. Suzuki, T. Nishizeki*, and N. Saito</i>	99
A Remark on the Complexity of the Knapsack Problem <i>H. Machida</i>	107
Fast, Rigorous Factorization and Discrete Logarithm Algorithms <i>C. Pomerance</i>	119
Redundant Coding for Local Computability <i>H. Yasuura*, N. Takagi, and S. Yajima</i>	145
Some Properties of the Parallel Bubbling and Parallel Sorts on a Mesh-Connected Processor Array <i>K. Sado and Y. Igarashi*</i>	161
Game Solving Procedure H* Is Unsurpassed <i>T. Ibaraki</i>	185

Algorithmic Problems in Modeling and Electronic Prototyping <i>J. Hopcroft</i>	201
Complementary Approaches to CNF Boolean Equations <i>K. Iwama</i>	223
Open Problems in Number Theoretic Complexity (Preliminary Version) <i>L.M. Adleman* and K.S. McCurley</i>	237
Decision Problem of the Security for Cryptographic Protocols <i>T. Fujiwara*, K. Taniguchi, and T. Kasami</i>	263
A Digital Signature Scheme Secure Against Adaptive Chosen Message Attack (Extended Abstract) <i>S. Goldwasser, S. Micali, and R. Rivest*</i>	287
Are Problems Having a Polynomial Time Upper Bound Actually Thought to Be Feasible? <i>A. Adachi* and T. Kasai</i>	311
On Probability that a Randomly Selected Set Has Some Complexity Theoretical Property <i>K. Kobayashi</i>	325
Ranking Rooted Trees and a Graceful Application <i>H.S. Wilf* and N. Yoshimura</i>	341
Dynamic Search in Graphs <i>F.R.K. Chung, R.L. Graham*, and M.E. Saks</i>	351
A Leaf-Size Hierarchy of Two-Dimensional Alternating Turing Machines <i>K. Inoue, I. Takanami, and J. Hromkovič</i>	389
Simple Programs with a Fixed Number of Variables Seem Still Hard to Analyze <i>S. Iwata* and T. Kasai</i>	405
Theory of the Multiplicative Penalty Function Method for Linear Programming <i>M. Iri and H. Imai*</i>	417
Linear-Time Computability of Combinatorial Problems on Generalized Series-Parallel Graphs <i>E. Hare, S. Hedetniemi, R. Laskar*, K. Peters, and T. Wimer</i>	437
Competitive Snoopy Caching <i>A.R. Karlin, M.S. Manasse, L. Rudolph, and D.D. Sleator*</i>	459

An Upper Bound on the Expected Cost of an Optimal Assignment

Richard M. Karp[†]

Computer Science Division
University of California,
Berkeley, California 94720

Introduction

An instance of the $n \times n$ assignment problem (AP) is specified by a $n \times n$ matrix (c_{ij}) of real numbers. The problem is to find a permutation that minimizes

$$A^* = \sum_{i=1}^n c_{i, \sigma(i)}.$$

When n is fixed and the c_{ij} are drawn independently from the uniform distribution over $[0,1]$, A^* becomes a random variable. Computational experiments indicate that, when $n > 100$, $E[A^*]$ is close to 1.6. Lazarus [1979] shows that

$$E[A^*] \geq 1 + \frac{1}{e} + O\left[\frac{1}{n}\right] \approx 1.37,$$

and Walkup [1979] shows that

$E[A^*] < 3$ for all n . Our main result is

Theorem 1. For all n , $E[A^*] < 2$.

A Regularity Condition

Call the matrix (c_{ij}) regular if no two distinct subsets of its elements have the same sum. This implies in particular that the optimal assignment σ is unique. Under the stated assumptions about the probability distribution of the c_{ij} the matrix (c_{ij}) is regular with probability 1. Throughout the paper we restrict attention to regular instances of the AP .

[†]Research supported by NSF Grant MCS-8105217

The Transportation Problem and its Dual

The proof of Theorem 1 is based on well-known properties of the following dual pair of linear programming problems ([1]).

<p>PRIMAL</p> $\min \sum_{i=1}^m \sum_{j=1}^n c_{ij} x_{ij}$ <p>subject to</p> $x_{ij} \geq 0$ $j = 1, 2, \dots, m$ $j = 1, 2, \dots, n$ $\sum_i x_{ij} = a_i \quad i = 1, 2, \dots, m$ $\sum_j x_{ij} = b_j \quad j = 1, 2, \dots, n$	<p>DUAL</p> $\max \sum_{i=1}^m a_i u_i + \sum_{j=1}^n b_j v_j$ <p>subject to</p> $c_{ij} - u_i - v_j \geq 0$ $i = 1, 2, \dots, m$ $j = 1, 2, \dots, n.$
---	--

Here the a_i and b_j are nonnegative real numbers satisfying

$$\sum_{i=1}^m a_i = \sum_{j=1}^n b_j.$$

The AP is the special case in which $m = n$ and all a_i and b_j are equal to 1. In this special case the primal and dual have A^* as their common optimal value. Also, every basic feasible solution to the primal has all x_{ij} equal to 0 or 1; for every such basic feasible solution there is a permutation σ of $\{1, 2, \dots, n\}$ such that $x_{ij} = 1$ and only if $j = \sigma(i)$.

In general, the basic solutions of the primal and dual can be characterized in graph-theoretic terms. Let G be the complete bipartite graph with vertex set $\{s_1, s_2, \dots, s_m\} \cup \{t_1, t_2, \dots, t_n\}$ and edge set

$$\{\{s_i, t_j\}, i = 1, 2, \dots, m, j = 1, 2, \dots, n\}.$$

Let T be the edge set of a spanning tree of G . There is a unique solution of the primal satisfying: if $\{s_i, t_j\} \notin T$ then $x_{ij} = 0$. There is a unique solution of the dual satisfying: $u_1 = 0$ and if $\{s_i, t_j\} \in T$ then $c_{ij} - u_i - v_j = 0$. The solutions obtained in this way from spanning trees of G are the basic solutions of the primal and dual. Call T *feasible* if the associated basic solution of the primal satisfies $x_{ij} \geq 0$ for all i and j ; call T *dual feasible* if the associated basic solution of the dual satisfies $c_{ij} - u_i - v_j \geq 0$ for all i and j . If T is both feasible and dual feasible we say that T is *optimal*; in this case the basic solutions associated with T are optimal

for the primal and dual respectively.

In the special case of the AP there are in general many optimal spanning trees of G . If the AP satisfies our regularity hypothesis there is a unique optimal tree which remains feasible when the a_i and b_j are perturbed by setting

$$a_i = 1 + n\epsilon \quad i = 1, \quad i = 2, \dots, n$$

and $b_j = 1 + \epsilon, \quad j = 1, 2, \dots, n$. Let us call this unique tree the canonical optimal tree.

Proof of Theorem 1: Each regular instance (c_{ij}) of the AP determines a 3-tuple $\langle T, u, v \rangle$. Here T is the canonical optimal tree and the n -vectors $u = (u_1, u_2, \dots, u_n)$ and $v = (v_1, v_2, \dots, v_n)$ are the associated optimal solution of the dual; call this 3-tuple the *optimality data* for (c_{ij}) .

Now assume that the c_{ij} are drawn independently from the uniform distribution over $[0, 1]$. Define the following two random variables is

$$\text{therefore} \quad \frac{1}{2} + \frac{1}{2}$$

$\max(0, u_i + v_j)$. Hence,

over the sample space of instances (c_{ij}) :

$$X = \sum_{i=1}^n \sum_{j=1}^n c_{ij}$$

and $Y = \langle T, u, v \rangle$, the optimality data for (c_{ij}) . The proof of Theorem 1 will emerge from consideration of the identity

$$E[X] = E[E[X|Y]].$$

Clearly $E[X] = \frac{n^2}{2}$, since the

expected value of each c_{ij} is $\frac{1}{2}$. Let

us compute $E[X|Y]$, where $Y = \langle T, u, v \rangle$ is fixed. The matrices from our sample space having $\langle T, u, v \rangle$ as optimality data are precisely those satisfying

$$c_{ij} - u_i - v_j = 0, \quad \{s_i, t_j\} \in T$$

$$c_{ij} - u_i - v_j \geq 0 \quad \{s_i, t_j\} \in T$$

The *a priori* distribution of each c_{ij} is uniform over $[0, 1]$. The *a posteriori* distribution of c_{ij} given $\langle T, u, v \rangle$ is uniform over $[\max(0, u_i + v_j), 1]$, and its conditional expectation given $\langle T, u, v \rangle$

□

Dyer, Frieze and McDiarmid (1984) have recently used the proof

$$\begin{aligned}
& E\left[\sum_{i=1}^n \sum_{j=1}^n c_{ij} \mid < T, u, v >\right] \\
&= \sum_{\{s_i, t_j\} \in T} (u_i + v_j) \\
&+ \sum_{\{s_i, t_j\} \notin T} \left(\frac{1}{2} + \frac{1}{2} \max(0, u_i + v_j)\right).
\end{aligned}$$

Noting that $u_i + v_j = c_{ij} \geq 0$ when $\{s_i, t_j\} \in T$, that

$\max(0, u_i + v_j) \geq u_i + v_j$ and

that $\sum_{i=1}^n u_i + \sum_{j=1}^n v_j = A^*$, we obtain

$$\begin{aligned}
& E\left[\sum_{i=1}^n \sum_{j=1}^n c_{ij} \mid < T, u, v >\right] \geq \\
& \frac{1}{2} \sum_{\{s_i, t_j\} \in T} (u_i + v_j) + \sum_{\{s_i, t_j\} \notin T} \left(\frac{1}{2} + \frac{1}{2} (u_i + v_j)\right) \\
&= \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n (u_i + v_j) + \frac{n^2 - 2n + 1}{2} \\
&= \frac{n}{2} A^* + \frac{n^2 - 2n + 1}{2}.
\end{aligned}$$

Applying $E[X] = E[E[X \mid Y]]$ we obtain

$$\begin{aligned}
\frac{n^2}{2} &\geq \frac{n}{2} E[A^*] + \frac{n^2 - 2n + 1}{2}, \\
\text{giving } E[A^*] &\leq \frac{2n - 1}{n} < 2
\end{aligned}$$

technique introduced in this paper to obtain a broad generalization of Theorem 1.

Acknowledgement

Thanks to Colin McDiarmid for suggesting a major simplification in the proof.

References

- [1] G. B. Dantzig, *Linear Programming and Extensions*, Princeton University Press (1963).
- [2] M. E. Dyer, A. M. Frieze and C. J. H. McDiarmid, "On Linear Programs with Random Objective Functions," private communication (1984).
- [3] A. Lazarus, *The Assignment Problem with Uniform (0,1) Cost Matrix*, B. A. Thesis, Department of Mathematics, Princeton University (1979).
- [4] D. W. Walkup, "On the Expected Value of a Random Assignment Problem," *SIAM J. Computing* 8, 440-442 (1979).

The Principal Partition of Vertex-Weighted Graphs
and Its Applications

Takao Ozawa

Department of Electrical Engineering

Kyoto University

Kyoto 606, Japan

Yoji Kajitani and Shuichi Ueno

Department of Electrical and Electronic Engineering

Tokyo Institute of Technology

Tokyo 152, Japan

Abstract The principal partition of vertex-weighted graphs is utilized to solve certain assignment problems or flow problems which are formulated using such graphs. The well-known labeling algorithm or labyrinth algorithm for augmenting flows is used to find the principal partition and to solve the first three problems. The fourth problem which is originated from a routing problem in three-dimensional integrated circuits, requires, in addition to the flow augmentation step, a step of finding an optimal flow assignment for a part of the graph.

1. Introduction.

The principal partition introduced by Kishi and Kajitani is a partition of a graph into three parts satisfying certain minimality