acm

# SIGACT NEWS

PUBLISHED BY THE ACM SPECIAL INTEREST GROUP
ON AUTOMATA AND COMPUTABILITY THEORY

WINTER - SPRING 1983
VOLUME 15, NUMBER 1

A SPECIAL ISSUE ON CRYPTOGRAPHY



*Cartoons by Clay Geerdes*

# SIGACT NEWS

Published by the ACM Special Interest Group on

Automata and Computability Theory


---



---

Papers appearing in SIGACT NEWS are unrefereed working papers. Submissions of any material of interest to SIGACT members is encouraged. Persons wishing to do book reviews and organizations submitting books for review should correspond with Dr. Cherniavsky. Other material should be submitted to Professor Blattner. Submissions should be camera-ready, unless circumstances prevent it.

# *Letter from The Editor*

This issue contains a selection of theoretical papers from Crypto 81. In order to publish these articles we needed to obtain the permission of the authors. Some of the authors sent us revised copies of their original papers. The last issue of SIGACT News contained "Cryptographic Technology: Fifteen Year Forecast," by Whitfield Diffie. Diffie's article was also from Crypto 81. Those of you interested in the area of cryptography may wish to send for the entire Workshop Proceedings. Many interesting papers could not be included because of our space limitations. Stephen Wiesner's article on conjugate coding is included in this issue because of it's general interest to theoreticians. The Crypto 81 Workshop on Communications Security, supported in part by the National Science Foundation, was held at the University of California, Santa Barbara, August 24-26, 1981. Allen Gersho was the Chairman and Head of the Program Committee. If you are interested in the full Crypto 81 Workshop Proceedings send a check for $25 to the UCSB Foundation, The Department of Electrical and Computer Engineering, Santa Barbara, CA 93106.

No other than your Editor took the POPL photos. About half of the photos didn't work out. Never arrive at a conference expecting to buy black and white film and flash bulbs after you get there. I hope those of you going to theoretical conferences will take pictures that we can put into SIGACT News. I can only attend about two theoretical conferences a year.

There were too few entries for *Transitions* in this issue. People don't move around in the middle of the year. I hope you send in your address changes for the Spring-Summer issue.

We have a number of issues of the News planned that focus on special topics as does this issue. If you know of any small theoretical workshops or conferences whose proceedings will not appear in journals or books, please ask the program committee to consider publishing them in SIGACT News.

Finally, we had to omit many of our listings of technical reports because of the size of this issue. The reports that we didn't include this time will surely make it in the News next time.

Meera Blattner

# 15th Annual ACM Symposium on Theory of Computing

April 25-27, 1983
57 Park Plaza Hotel
Boston, Massachusetts

**Conference Information**

## HOTEL RESERVATION FORM

Mail before April 4,1983 to:

1983 ACM STOC
The 57 Park Plaza Hotel/Howard Johnson
57 Building
200 Stuart Street
Boston, MA 02116

Reservation Desk Phone: (617) 482-7352 (or 3)

Please reserve a room for me at the 15th Annual ACM-SIGACT Symposium on Theory of Computing, Sunday April 24 through Wednesday April 27, 1983.

____Single $75.00 per day
____Double $85.00 per day

(Rates subject to 5.7% sales tax.)

Arrival date_____ time_____

Departure date_____ time_____

Send me confirmation at:

Name_____
(Please print full name)

Address_____

City_____State_____Zip_____

Country (if other than USA)_____

For arrivals after 6PM, the hotel requests that arrival be guaranteed by providing a major credit card number, company name, or personal check for one night's deposit.

## PREREGISTRATION FORM

Use this form or a facsimile to preregister. **Advance registration closes April 10.** Preregistration by mail after April 10 is subject to a late fee. Registration after April 21 or at the conference site is subject to a larger* late fee.
Please mail form with check (drawn on US bank) or money order (in US funds) payable to 1983 ACM STOC to:

STOC REGISTRATION
c/o Professor Albert R. Meyer
M.I.T. Laboratory for Computer Science
545 Technology Square, NE43-801
Cambridge, MA 02139

Rates for registration:

| | | |
|---|---|---|
| Member of ACM, SIGACT, or IEEE Computer Society | $110.00 | _____ |
| Non-Member | 135.00 | _____ |
| Author or Committee Member | 100.00 | _____ |
| Student** | 30.00 | _____ |
| Extra banquet tickets @$27.00 | | _____ |
| Non-student late fee (after April 10 until April 21)* | 30.00 | _____ |
| Student late fee(after April 10) | 10.00 | _____ |
| Total enclosed | | $_____ |

***NOTE:** Registration fee at the conference site is $170 for all non-student registrants.

I would like assistance with day care

yes____ no____

Name_____
(Print last name first)

Affiliation_____

Address_____

City_____State_____Zip_____

Country (if other than USA)_____

**Student registration includes technical sessions, conference proceedings, reception, and coffee breaks; does not include luncheons or banquet.

Requests for special dietary considerations should accompany this registration form. Requests for refunds will be honored until April 21.

# Program - 15th STOC

**Sunday April 24**

- Registration 5:00 pm - 10:00 pm (6th Floor)
- Reception 7:30 pm - 10:30 pm (Ballroom 1, Mezzanine)

**Session I: Monday Morning, 9:20AM - 12:30PM** Convention Hall A, 6th floor
Chair: W. L. Ruzzo, Univ. of Washington

**9:20** **An O(nlogn) Sorting Network**
M. Ajtai, J. Komlos, E. Szemeredi
Budapest Academy of Sciences, UC San Diego, Univ. of South Carolina

**9:40** **A Logarithmic Time Sort for Linear Size Networks**
J.H. Reif, L.G. Valiant - Harvard Univ.

**10:00** **Parallel Algorithms for Algebraic Problems**
J. von zur Gathen - Univ. of Toronto

**10:20** **COFFEE BREAK** Convention Hall B, 6th floor

**10:50** **Topological Matching**
Q. F. Stout - SUNY Binghamton

**11:10** **Reliable Computation with Cellular Automata**
P. Gacs - Univ. of Rochester

**11:30** **Superconcentrators, Generalizers and Generalized Connectors with Limited Depth**
D. Dolev, C. Dwork, N. Pippenger, A. Wigderson
Hebrew Univ., Cornell Univ., IBM San Jose, Princeton Univ.

**11:50** **Unbounded Fan-in Circuits and Associative Functions**
A. K. Chandra, S. Fortune, R. Lipton
IBM Yorktown Hts., IBM Yorktown Hts., Princeton Univ.

**12:10** **Borel Sets and Circuit Complexity**
M. Sipser - MIT

**12:30** **LUNCH** Ballrooms 1 and 2, located on the Mezzanine

**Session II: Monday Afternoon, 2:00PM - 5:30PM** Convention Hall A, 6th floor
Chair: M. L. Fredman, UC San Diego

**2:00** **A Polynomial Linear Search Algorithm for the n-Dimensional Knapsack Problem**
F. Meyer auf der Heide - Johann Wolfgang Goethe Univ.

**2:20** **Lower Bounds for Algebraic Computation Trees**
M. Ben-Or - MIT and Hebrew Univ.

**2:40** **Bounds for Width-Two Branching Programs**
A. Borodin, D. Dolev, F. Fich, W. Paul
Univ. of Toronto, Hebrew Univ., IBM San Jose, IBM San Jose

**3:00** **Multi-Party Protocols**
A. K. Chandra, M. L. Furst, R. J. Lipton
IBM Yorktown Hts., Carnegie-Mellon Univ., Princeton Univ.

**3:20** **New Bounds for Parallel Prefix Circuits**
F. Fich - UC Berkeley and IBM San Jose

**3:40** **COFFEE BREAK** Convention Hall B, 6th floor

**4:10** **Exponential Lower Bounds for Restricted Monotone Formulae**
L. G. Valiant - Harvard Univ.

**4:30** **The Complexity of Approximate Counting**
L. Stockmeyer - IBM San Jose

**4:50** **Two Nonlinear Lower Bounds**
P. Duris, Z. Galil, W. Paul, R. Reischuk
Slovak Academy of Science, Columbia Univ. and Tel-Aviv Univ., IBM San Jose, Univ. of the Saarlandes

**5:10** **On Notions of Information Transfer in VLSI Circuits**
A. V. Aho, J. D. Ullman, M. Yannakakis
Bell Labs Murray Hill, Stanford Univ., Bell Labs Murray Hill

**5:30** **End of Session**

**9:00** **BUSINESS MEETING** Convention Hall A, 6th floor

# Program - 15th STOC

**Session III: Tuesday Morning, 9:00AM - 12:30PM** Convention Hall A, 6th floor
Chair: D.S. Johnson, Bell Labs, Murray Hill

**9:00** **Solvability by Radicals is in Polynomial Time**
S. Landau, G. L. Miller - MIT

**9:20** **On the Diameter of Permutation Groups**
J. R. Driscoll, M. L. Furst - Carnegie-Mellon Univ.

**9:40** **Normal Forms for Trivalent Graphs**
M. Furer, W. Schnyder, E. Specker
Univ. Zurich, ETH Zurich, ETH Zurich

**10:00** **Canonical Labeling of Graphs**
L. Babai, E. M. Luks - Eotvos Univ., Bucknell Univ.

**10:20** **COFFEE BREAK** Convention Hall B, 6th floor

**10:50** **How to Generate Random Integers with Known Factorization**
E. Bach - UC Berkeley

**11:10** **Factoring Multivariate Polynomials over a Finite Field**
A. K. Lenstra - Mathematisch Centrum

**11:30** **Improved Algorithms for Integer Programming and Related Lattice Problems**
R. Kannan - MIT

**11:50** **Retraction: A New Approach to Motion-Planning**
C. O'Dunlaing, M. Sharir, C. K. Yap
NY Univ., Tel-Aviv Univ., NY Univ.

**12:10** **Primitives for the Manipulation of Planar Subdivisions and the Computation of Voronoi Diagrams**
L. J. Guibas, J. Stolfi - Xerox PARC, Stanford Univ.

**12:30** **LUNCH** Ballrooms 1 and 2, located on the Mezzanine

**Session IV: Tuesday Afternoon, 2:00PM - 5:50PM** Convention Hall A, 6th floor
Chair: D. Harel, Weizmann Institute

**2:00** **Self-Adjusting Binary Trees**
D. D. Sleator, R. E. Tarjan - Bell Labs Murray Hill

**2:20** **A Linear-Time Algorithm for a Special Case of Disjoint Set Union**
H. N. Gabow, R. E. Tarjan
Univ. of Colorado, Bell Labs Murray Hill

**2:40** **Data Structures for On-Line Updating of Minimum Spanning Trees**
G. N. Frederickson - Purdue Univ.

**3:00** **New Results on Range Queries**
F. F. Yao - Xerox PARC

**3:20** **Unary Inclusion Dependencies Have Polynomial Time Inference Problems**
P. C. Kanellakis, S. S. Cosmadakis, M. Y. Vardi
Brown Univ., MIT, Stanford Univ.

**3:40** **COFFEE BREAK** Convention Hall B, 6th floor

**4:10** **On the Extremely Fair Treatment of Probabilistic Algorithms**
A. Pnueli - Weizmann Institute and Harvard Univ.

**4:30** **A Probabilistic PDL**
D. Kozen - IBM Yorktown Hts.

**4:50** **A Decidable Propositional Probabilistic Dynamic Logic**
Y. A. Feldman - Weizmann Institute

**5:10** **A Logic to Reason about Likelihood**
J. Y. Halpern, M. O. Rabin
IBM San Jose, Harvard Univ. and Hebrew Univ.

**5:30** **A Characterization of Hoare's Logic for Programs with Pascal-Like Procedures**
E.-R. Olderog - Univ. Kiel

**5:50** **End of session**

**6:30** Buses depart from hotel for the BANQUET at the New England Aquarium

Program - 15th STOC

**Session V: Wednesday Morning, 9:00AM - 12:30PM** Convention Hall A, 6th floor
Chair: J. Seiferas, Univ. of Rochester

**9:00** **A Complexity Theoretic Approach to Randomness**
M. Sipser - MIT

**9:20** **Speedups of Deterministic Machines by Synchronous Parallel Machines**
P. W. Dymond, M. Tompa
UC San Diego and Univ. of Waterloo, Univ. of Washington

**9:40** **Alternation and the Power of Nondeterminism**
R. Kannan - MIT

**10:00** **Languages which Capture Complexity Classes**
N. Immerman - Tufts Univ.

**10:20** **COFFEE BREAK** Convention Hall B, 6th floor

**10:50** **The Random Access Hierarchy**
D. Myers - Univ. of Hawaii

**11:10** **Iterated Pushdown Automata and Complexity Classes**
J. Engelfriet - Twente Univ. of Technology

**11:30** **Unique Decomposability of Shuffled Strings: A Formal Treatment of Asynchronous Time-Multiplexed Communication**
K. Iwama - Kyoto Sangyo Univ.

**11:50** **On Sparse Sets in NP-P: EXPTIME vs NEXPTIME**
J. Hartmanis, N. Immerman, V. Sewelson
Cornell Univ., Tufts Univ., Cornell Univ.

**12:10** **Some Structural Properties of Polynomial Reducibilities and Sets in NP**
P. Young - Purdue Univ.

**12:30** **LUNCH** Convention Hall B and C, 6th floor

**Session VI: Wednesday Afternoon, 2:00PM - 5:30PM** Convention Hall A, 6th floor
Chair: R. L. Rivest, MIT

**2:00** **On Breaking the Iterated Merkle-Hellman Public Key Cryptosystem**
L. M. Adleman - Univ. of Southern California and MIT

**2:20** **How Discreet is the Discrete Log?**
D. L. Long, A. Wigderson - Princeton Univ.

**2:40** **On the Cryptographic Security of Single RSA Bits**
M. Ben-Or, B. Chor, A. Shamir
MIT, MIT, Weizmann Institute

**3:00** **Strong Signature Schemes and Authentication**
S. Goldwasser, S. Micali, A. Yao
UC Berkeley, Univ. of Toronto, Stanford Univ.

**3:20** **How to Exchange (Secret) Keys**
M. Blum - UC Berkeley

**3:40** **COFFEE BREAK** Convention Hall B, 6th floor

**4:10** **An Efficient Reduction Technique for Degree- Constrained Subgraph and Bidirected Network Flow Problems**
H. N. Gabow - Univ. of Colorado

**4:30** **Transitive Orientation in $O(n^2)$ Time**
J. Spinrad - Georgia Institute of Technology

**4:50** **Probabilistic Analysis of Bandwidth Minimization Algorithms**
J. Turner - Bell Labs Naperville

**5:10** **An Approximation Algorithm for Manhattan Routing**
B. S. Baker, S. N. Bhatt, F. T. Leighton
Bell Labs Murray Hill, MIT, MIT

FINAL PROGRAM

# CAAP 83

## 8TH COLLOQUIUM ON TREES IN ALGEBRA AND PROGRAMMING

Università degli Studi de L'Aquila, Italy
March 9-11, 1983


Sponsored by:

Università de L'Aquila
Università di Roma
Consiglio Nazionale delle Ricerche
Comune de L'Aquila
Provincia de L'Aquila
Cassa di Risparmio de L'Aquila
Scuola Superiore "G. Reiss Romoli"

European Association for Theoretical Computer Science

**Mailing Address** Marco Protasi
Secretary CAAP 83
Istituto di Matematica
Via Roma, 33
67100 - L'Aquila, Italy

## PROGRAM

### Wednesday, March 9

8.00 Registration.

9.15 Opening address.

9.30 G. Rozenberg (U. of Leiden)
*Some recent developments in the theory of graph grammars* (Invited lecture).

10.30 G. Slutzki (U. of Kansas)
*Alternating tree automata.*

11.00 Coffee break.

11.15 J. Beauquier (U. of Picardie)
*Prefix and perfect languages.*

11.45 M. F. Claerebout, E. Lilin (U. of Lille I)
*Continuité des transducteurs d'etats finis d'arbres.*

12.15 E. Best (GMD, Bonn), M. W. Shields (U. of Edinburgh)
*Some equivalence results for free-choice nets and simple nets and on the syntactic generation of live and safe free-choice nets.*

13.00 Lunch.

15.00 Z. Galil (New York U.)
*Algorithms for finding maximal matching in graphs* (Invited lecture).

16.00 A. Lingas (MIT and Linköping IT)
*An application of maximum bipartite C-matching to subtree isomorphism.*

16.30 Coffee break.

16.45 F. Makedon, C. H. Papadimitriou, I. H. Sudborough (T. U. of Athens)
*Topological bandwidth.*

17.15 B. Monien, E. Speckenmeyer (U. of Paderborn)
*Some further approximation algorithms for the vertex cover problem.*

17.45 A. Marchetti-Spaccamela, M. Talamo (U. of Rome)
*Probabilistic analysis of graph colouring algorithms.*

21.00 Concert.

### Thursday, March 10

9.00 M. Coppo, M. Dezani (U. of Turin), G. Longo (U. of Pisa)
*Applicative information systems* (Invited lecture).

10.00 M. Venturini (IAC, Rome)
*Cofinality in reduction graphs.*

10.30 Coffee break.

10.45 M. Coppo, E. Giovannetti (U. of Turin)
*Completeness results for a polymorphic type system.*

11.15 J. P. Jouannaud (CRI, Nancy)
*Confluent and coherent sets of reductions with equations.*

11.45 F. Fages, G. Huet (INRIA, Paris)
*Complete sets of unifiers and matchers in equational theories.*

12.30 Lunch.

14.30 M. Wirsing (U. of Munich)
Title to be announced (Invited lecture).

15.30 D. T. Sannella, R. M. Burstall (U. of Edinburgh)
*Structured theories in LCF.*

16.00 Coffee break.

16.15 J. Gonczarowski (The Hebrew U. of Jerusalem)
*Decidable properties of monadic recursive schemas with a depth parameter.*

16.45 B. Mahr, J. A. Makowsky (Technion, Haifa)
*Characterizing specification languages which admit initial semantics.*

17.15 B. Courcelle, F. Lavandier (U. of Bordeaux I)
*A class of program schemes based on tree rewriting systems.*

17.45 S. Istrail, C. Masalagiu (U. "Al. I. Cuza", Iasi)
*Nivat processing systems: decision problems related to protection and synchronization.*

20.00 Social dinner.

Friday, March 11

9.00 R. Fagin (IBM, San Josè)
*Acyclic data base schemes: an introduc*
(Invited lecture).

10.00 J. Paredaens, D. Van Gucht (U. of Antw
*An application of the theory of graphs hypergraphs to the decomposition of relational database schemes.*

10.30 Coffee break

10.45 P. Flajolet, N. Saheb (INRIA, Paris)
*The complexity of generating an exponentially distributed variate.*

11.15 M. A. Bonuccelli, E. Lodi, F. Luccio, P. Maestrini, L. Pagli (U. of Pisa)
*VLSI mesh of trees for data base processing.*

11.45 W. Rytter (U. of Warsaw)
*Remarks on the pyramidal structure.*

12.30 Lunch.

14.00 Excursion.

CAAP 83

In 1983 the annual International Colloquium on Trees in Algebra and Programming will be held in L'Aquila, Italy. Topics include formal aspects and properties of trees and, more generally, of combinatorial and algebraic structures in all fields of Computer Science: theory of algorithms and computational complexity, formal languages and automata, theory of sequential and parallel programs, theory of data structures and data bases, algebraic specification of software, etc.
Traditionally the Colloquium has been held in Lille, France, with the exception of 1981 when it was held in Genova, Italy.
In 1983 it will be held in L'Aquila, again in Italy. L'Aquila is a historical town of remarkable cultural interest in the center of Italy, about 100 km from Rome.

**Location**

The Colloquium will be held at Hotel "Le Cannelle" (Piazzale Le Cannelle, 67100 - L'Aquila, phone (862) 27510/27847/27848, Telex 600120 EDIRTI) within the town walls in a private park. The Hotel is provided of a covered heated swimming pool and a tennis ground. On the morning of the first day the Opening Session will take place in the Aula Magna of the University.

**Accompanying persons**

Participants are kindly requested to communicate the number of accompanying persons in the registration form. All expenses concerning accompanying persons, except participation in the Concert and transportation from Rome to L'Aquila by the special coach, are on charge of the participant himself.

**Registration**

To register, please, return the enclosed registration form as soon as possible.
The registration fee is 90.000 Lire and includes the Colloquium Proceedings, the lunches on March 9,10 and 11, the social dinner on March 10, the transportation by special coach from Rome to L'Aquila.
The registration fee has to be paid on bank account 51708/2 - Giorgio Ausiello - Marco Protasi - CAAP 83 of the Cassa di Risparmio della Provincia de L'Aquila, before Febraury 20, 1983. Otherwise the fee may be paid cash in Italian currency, directly at the Conference Registration desk.
The Registration will take place on March 8 from 6 p.m. to 10 p.m. and on March 9 from 8 a.m. to 9 a.m. at Hotel Le Cannelle.

Travel

L'Aquila can be easily reached from Rome by coach (about two hours). It is not advisable to reach L'Aquila by train because the line Roma - L'Aquila is not served by fast trains. The coaches (companies ARPA and OGNIVIA) leave Rome from Piazza della Repubblica, close to the main train Station and to the city Air Terminal. In the afternoon of March 8 at 5 p.m. a coach rented for the participants to the Colloquium will leave from Piazza della Repubblica.
Further travel information will be provided upon request.

**Accomodation**

All the participants will be lodged at Hotel "Le Cannelle" where the Colloquium will be held. The room rate (included breakfast) is 33.000 for accomodation in single room and 23.500 per person for accomodation in double room. All rooms are with bathroom. The participants who do not wish this accomodation are requested to write it in the registration form. In this case, or in the case that the registration form is not received by February 20, the Colloquium Organization will not be responsible for the accomodation.

Lunch

The lunches of March 9,10 and 11 will be served at Hotel "Le Cannelle".

Social Program

In the evening of March 9 a concert will be performed for the participants. A social dinner will be arranged on March 10. A coach trip in the region near L'Aquila will take place on March 11 afternoon.
The above social activities are free for all registrants except the coach trip for which a contribution will be required.

# Denotational Semantics of Programming Languages

A Short Course: July 11-15, 1983,

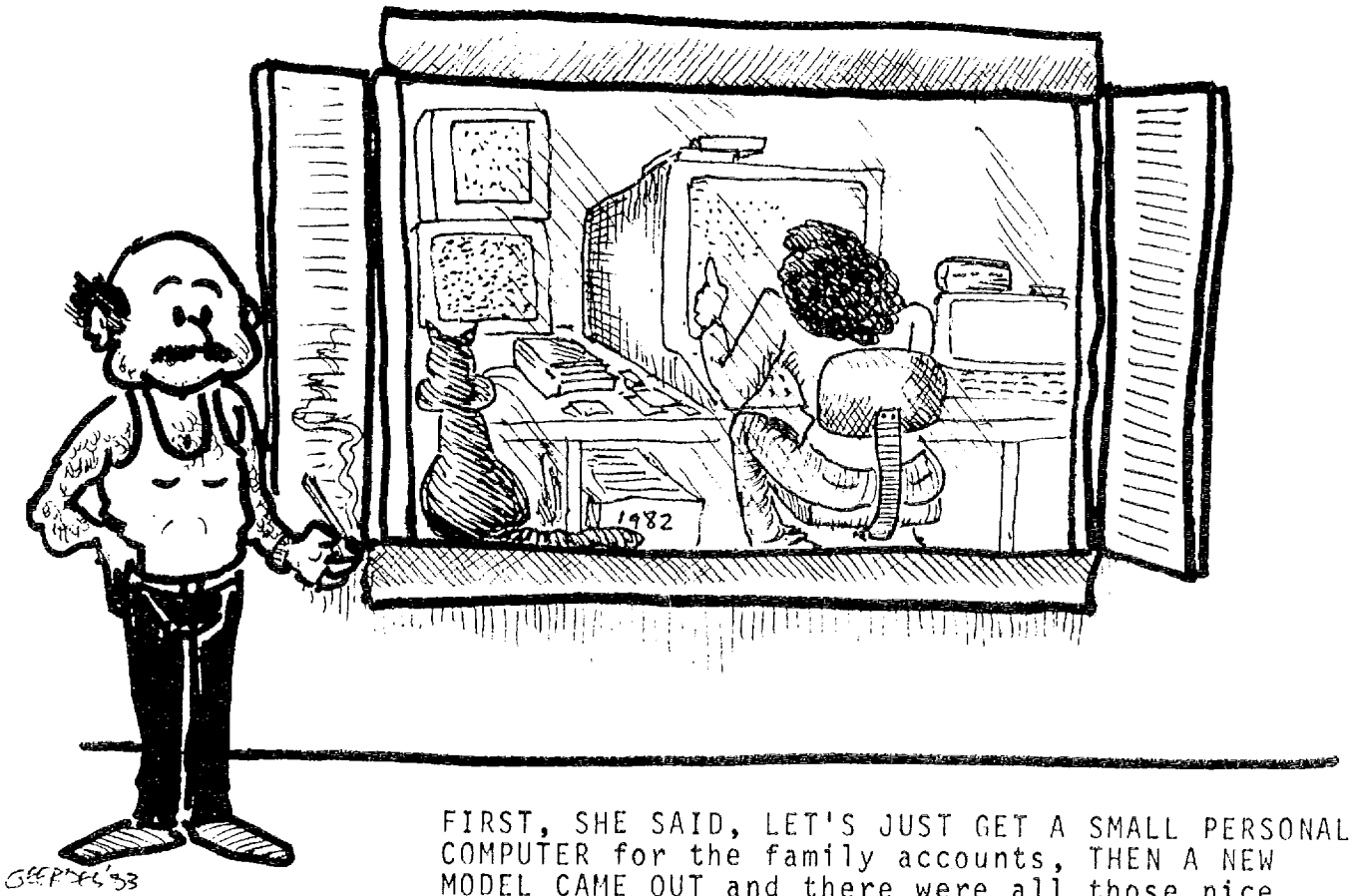
Massachusetts Institute of Technology

Instructors: Albert R. Meyer and Joseph E. Stoy

Introduction to the basic concepts and techniques of denotational semantics. A principal objective is to enable participants to make use of denotational definitions now being published for many major high-level programming languages. Examples of denotational definitions of significant features of these languages will be given, as well as a complete definition of a smaller pedagogical language. Other formal approaches to programming language specification such as axiomatic and operational semantics will be considered and related to the denotational approach -- particularly for parallel tasking and concurrency features.

For further information, please contact:

Director of the Summer Session
Massachusetts Institute of Technology, E19-356
Cambridge, MA 02139, USA




FIRST, SHE SAID, LET'S JUST GET A SMALL PERSONAL COMPUTER for the family accounts, THEN A NEW MODEL CAME OUT and there were all those nice accessories, and.....

INVITATION TO

INTERNATIONAL CONFERENCE ON

# FOUNDATIONS OF COMPUTATION THEORY

## FCT

AUGUST 21 - 27, 1983
BORGHOLM, SWEDEN

Organized by
LINKÖPING UNIVERSITY


The International Conference on Foundations of Computation Theory is to follow thematically the series of the international FCT-conferences founded in 1977 in Poznan-Kornik, Poland. The program of the conference, including invited lectures and selected contributions, is to fall into eight categories:

* ***Constructive Mathematics in Models of Computation and Programming***
* ***Abstract Calculi and Denotational Semantics***
* ***Theory of Machines, Computations, and Languages***
* ***Nondeterminism, Concurrency, and Distributed Computing***
* ***Abstract Algebras, Logics, and Combinatorics in Computation Theory***
* ***General Computability and Decidability***
* ***Computational and Arithmetic Complexity***
* ***Analysis of Algorithms and Feasible Computing***

**Program Committee**

K.R.Apt (Paris), G.Ausiello (Rome), A.J.Blikle (Warsaw), E.Börger (Dortmund), W.Brauer (Hamburg), M.Broy (Munich), L.Budach (Berlin), R.Burstall (Edinburgh), P.van Emde Boas (Amsterdam), F.Gecseg (Szeged), J.Gruska (Bratislava), M.A.Harrison (Berkeley), J.Hartmanis (Ithaca), K.Indermark (Aachen), M.Karpinski (Bonn), D.Kozen (Yorktown Heights), J.van Leeuwen (Utrecht), L.Lovasz (Budapest), A.Mazurkiewicz (Warsaw), G.L.Miller (Cambridge Mass.), P.Mosses (Aarhus), B.Nordström (Gothenburg), M.Paterson (Warwick), A.Salomaa (Turku), C.P.Schnorr (Frankfurt), J.W.Thatcher (Yorktown Heights)

**Program Committee Chairman**

Prof. Marek Karpinski
Computer Science Department
University of Bonn
Wegelerstr. 6
D-5300 Bonn 1
W. Germany

**Invited Speakers** (preliminary list)

Stephen A. Cook (Toronto)
David Harel (Rehovot)
Per Martin-Löf (Stockholm)
Hendrik W. Lenstra, Jr. (Amsterdam)
Gordon D. Plotkin (Cambridge, Mass.)
Dana S. Scott (Pittsburgh)

The submitted papers are presently being evaluated by the International Program Committee. The final program of the conference will be announced by April 30, 1983. The proceedings will be available at the conference.

The "Foundations of Computation Theory 1983" Conference is being organized under the auspices of the European Association for Theoretical Computer Science and is sponsored by the University of Linköping, Sweden.

### Organizing Committee

E. Sandewall (Chairman)
A. Lingas
J. Maluszynski

### Conference Office

"Foundations of Computation Theory 1983"
Department of Mathematics
Linköping University
S - 581 83 Linköping, Sweden
Tel. (international prefix 46-13) 111700 ext. 1483

Organizing Secretary: Lillemor Wallgren
Program Secretary: Mariele Knepper

### Location

Following the tradition of the FCT-Conferences it was decided to move the "Foundations of Computation Theory 1983" Conference outside the city to provide better possibilities for informal discussions and recreation after the sessions. The conference will be held in the Öland Conference Center at Borgholm (tel. 46-485-11020). Öland is an island on the Baltic sea famous for its unique nature and interesting history. It is one of the most popular recreation areas of Sweden. It is connected with the mainland by the longest bridge of Europe. Borgholm is one of the tourist centers of the island. The conference hotel is situated on the seashore in a walking distance from the summer residence of the King of Sweden.

### Prices

The registration fee is SKr 750 if paid before June 15 and SKr 900 if paid later. Each participant receives a free copy of the proceedings to be published as a volume of LNCS, Springer-Verlag.

The participation fee given below includes accommodation with full pension in the Borgholm Conference Center from Sunday, August 21,1983 (arrival day) until Friday, August 26, 1983. The first meal is dinner on Sunday, August 21, to be served at 7 p.m., or in case of later arrival, just after arrival. The last meal is the lunch on Friday. There are four price categories, depending on the requested accommodation:

A. Single room with bath/shower: SKr 2150 ;
B. Single room in a two-room apartment
(2 persons in the apartment): SKr 1775 ;
C. Double shared room with bath/shower: SKr 1650 ;
D. Double shared room in a two-room apartment
(4 persons in the apartment): SKr 1325 ;

Children of age 3 through 14 can be accommodated with parents for SKr 50 per child per day including additional bed and breakfast. For prolongation of the stay advance reservation is necessary.

### Social Events and Recreation

Informal meeting on Monday afternoon before dinner.
A guided sightseeing tour on Wednesday afternoon.
The Conference Dinner on Thursday.

There is a possibility to organize an evening fishing tour. The hotel has its own indoor swimming pool and sauna to be used by participants free of charge.

### Travel Information

There are direct flights and train connections from Copenhagen to Kalmar. On request local transportation from Kalmar to Borgholm (approx. distance 30 km) can be organized by the hotel (round trip price SKr 80). There is also a regular public bus service. More information can be obtained from the SJ Travel Office at Kalmar tel. 46-480-28034.

The suggested connections on Sunday, Aug.21:
by plane:
dep. Copenhagen 20.10 arr. Kalmar 21.35
by train:
dep. Copenhagen 15.19 arr. Kalmar 21.05

### Registration

The number of places is limited. To help us plan better you are kindly asked to fill in and mail the attached reply card.

In order to register you are asked to send to the Conference Office the registration form with enclosed check made payable to the Linköping University.

It is strongly recommended that you register before June 15. We cannot guarantee accommodation in case of registration after July 15.

# CALL FOR PAPERS

## –12th International Conference–

# 1983 International Conference on Parallel Processing

**August 23-26, 1983**

**Co-sponsored By**
**The Ohio State University** and the **IEEE Computer Society**
in cooperation with
**Association for Computing Machinery**

Authors are invited to submit papers describing recent advances on all aspects of parallel/distributed processing. These may include parallel/distributed logic circuits, impact of VLSI to parallel processor architecture; various concurrent-, distributed-, parallel-, pipeline-, or multiple-processor architectures; processor-memory interconnections; computer networks; distributed data bases; reliability and diagnostics; modeling and simulation techniques; performance measurements; operating systems; languages; or various application studies.

### INSTRUCTIONS FOR AUTHORS

The conference will accept both regular and short papers. **The deadline for submitting papers is February 15, 1983.**

For **regular papers**, four copies each of a 100-word abstract and the full text are required.

For **short papers**, authors should submit four copies each of a 100-word abstract and a summary of 500 words.

**Please make sure that summaries are of sufficient detail to permit careful evaluation by referees**. Appropriate references and figures should be included in the summaries. Please include office and/or home telephone numbers.

The papers should be submitted before **February 15,** 1983 to:

Dr. Howard J. Siegel (317) 494-3444
Dr. Leah J. Siegel (317) 494-3653
School of Electrical Engineering
Purdue University
West Lafayette, IN 47907

Submitted papers will be acknowledged promptly and authors will be notified of acceptance by **April 15, 1983.**

### CONFERENCE PROCEEDINGS

The regular papers and the summaries of the short papers will be published in the conference proceedings. Special sheets for the preparation of accepted papers for the proceedings will be sent to each author.

### CONFERENCE AWARDS

The conference will give two awards: one for **Most Original Paper**, the other for the **Best Presentation**.

### CONFERENCE ENVIRONMENT

The conference will be held at the Shanty Creek Lodge in Bellaire, Michigan, in the northern part of Michigan's lower peninsula, about 250 miles northwest of Detroit and approximately 30 miles east of Traverse City. The picturesque and modern lodge, resort, and conference center is located atop a small mountain overlooking beautiful scenery and lakes. The lodge complex has over 200 rooms accommodating singles, doubles, small groups, and families.

Special children's activities are regularly scheduled, and there is nightly entertainment in the main lodge. Accommodation and meal charges are billed separately.

Informal, open bar gatherings will be held nightly for the conference participants

Lodge facilities include: tennis courts; an 18 hole golf course; a private beach club for swimming, with sailboats, canoes, rowboats, and motorboats available for rent (local transportation is provided); heated indoor and outdoor swimming pools at the lodge; fishing; nature trails; and many other nearby sports facilities.

Regular limousine service to Shanty Creek is provided for a small fee and is available from the Traverse City Airport, which is regularly serviced by Republic Airlines.

A conference brochure with preregistration form and the technical program will be prepared and mailed in June 1983.

### PRECONFERENCE TUTORIALS

At the request of many conference attendees, preconference tutorials on parallel/distributed processing will be offered.

CALL FOR PAPERS

# ACM 1983 ANNUAL CONFERENCE

OCTOBER 24-26, 1983 • SHERATON CENTRE • NEW YORK, NY

## COMPUTERS: EXTENDING THE HUMAN RESOURCE

The 1983 ACM Annual Conference will cover recent developments in computing theory, computing practices and personal computing.

The Program Committee is inviting tutorials, proposals for panel discussions and technical papers or surveys to be presented at the Conference.

Suggested topics include:

| | | |
|---|---|---|
| Business Applications | Office Automation | Data Communications |
| Personal Computing | Graphics | Education |
| Software Development | Hardware Innovations | Artificial Intelligence |
| Privacy & Security | Database Systems | Computers & Society |
| Electronic Funds Transfer | Simulation | History of Computing |

*WRITE!* Authors of papers should submit four copies of their work, typed and double-spaced, not exceeding twelve pages in length. Proposals for special sessions or tutorials should contain sufficient detail to explain the presentation.

The deadline for submission is March 7, 1983. Authors will be notified of acceptance or rejections by May 1, 1983.

The Conference Proceedings will consist of accepted papers and surveys, which will be available at the conference and later from the Association for Computing Machinery.

Selected authors will be sent special paper and instructions for preparing camera-ready copy (due August 15, 1983) and must sign the copyright release form which will be included in the instructions.

Send papers to:

Thomas A. D'Auria
ACM '83 Conference Chairman
City of New York
Computer Services Center
111 Eighth Avenue
New York, NY 10011
Telephone: (212) 620-5055

acm

For further information contact: Thomas A. D'Auria at the above address.

## 24th FOCS Symposium

# Call For Papers

## 1983 IEEE Symposium on Foundations of Computer Science

The 24th Annual IEEE Symposium on Foundations of Computer Science, sponsored by the Computer Society's Technical Committee on Mathematical Foundations of Computing, will be held in Tucson, Arizona on November 7-9, 1983. Papers presenting original research on theoretical aspects of computer science are being sought.

**Suggested Topics:** Typical, but not exclusive, topics include:

Algorithms and Data Structures
Computability and Complexity Theory
Cryptography
Theory of Data Bases
Theory of Formal Languages and Automata
Theory of Logical Design, Layout and VLSI
Models of Computation
Semantics of Programming Languages

**Submission of papers:** Authors should send ten copies of a detailed abstract (*not* a full paper) by May 9, 1983 to the Program Committee Chairman:

Professor Lawrence Snyder
Department of Computer Sciences
Mathematical Sciences Building
Purdue University
West Lafayette IN 47907

Authors will be notified of acceptance or rejection by July 13, 1983. A copy of each accepted paper, typed on special forms for inclusion in the symposium proceedings, will be due by September 9, 1983.

**IMPORTANT**

Because a large number of submissions is anticipated, authors are advised to prepare their detailed abstract carefully. It is recommended that each submission begin with a succinct statement of the problem, a statement of the main result(s) and an explanation of their significance that is suitable for a general research audience. Technical development of the work, directed to the specialist, should follow as appropriate. In any case, the entire extended abstract, with comparison to extant work, should not exceed 2500 words (ten typed double-spaced pages). Submissions departing significantly from these guidelines risk rejection without consideration of their merits.

**Meeting Format:** The format of the meeting, including time allocations for presentations, will be determined by the Program Committee. Authors having a preference for a short (10-15 minute) or long (20-25 minute) presentation should express it at the time of submission. Such a preference will not influence acceptance, and time allocation will not be noted in the proceedings or affect the space allocation for the paper.

**Machtey Award for Best Student Paper:** This award, of up to $400 to help defray expenses for attending the Symposium, will be given for that paper which the Program Committee adjudges the most outstanding paper written solely by a student or students. To be considered for the award, an abstract must be accompanied by a letter identifying all authors as full-time students at the time of submission. (At its discretion, the Committee may decline to make the award or may split the award among two or more papers.)

## Symposium Committees

**Program**

Manuel Blum
Zvi Galil
Oscar Ibarra
Dexter Kozen
Gary Miller
J. Ian Munro
W. Larry Ruzzo
Larry Snyder
Richard Statman
Robert Tarjan

**Local Arrangements**

Peter J. Downey
Department of Computer Science
The University of Arizona
Tucson AZ 85721

# TWENTY-FIRST ANNUAL ALLERTON CONFERENCE ON COMMUNICATION, CONTROL, AND COMPUTING

## OCTOBER 5-7, 1983

The Twenty-First Annual Allerton Conference will be held at Allerton House, the conference center of the University of Illinois, on October 5-7, 1983. Allerton House is located twenty-six miles southwest of the Urbana-Champaign campus of the University in a wooded area on the Sangamon River. It is part of the fifteen-hundred-acre Robert Allerton Park, near Monticello, Illinois.

Papers are solicited which present new results in the areas of communication systems, information theory and coding, detection and estimation, stochastic processes, communication networks, control systems, optimization, dynamic games, large-scale systems modeling and stability, robustness of adaptive control and identification, bifurcation and asymptotic methods in deterministic and stochastic systems, geometric methods in nonlinear systems, digital signal and image processing, analysis and design of algorithms, computational complexity, parallel computation, VLSI algorithms, computer architecture, and fault-tolerant computing.

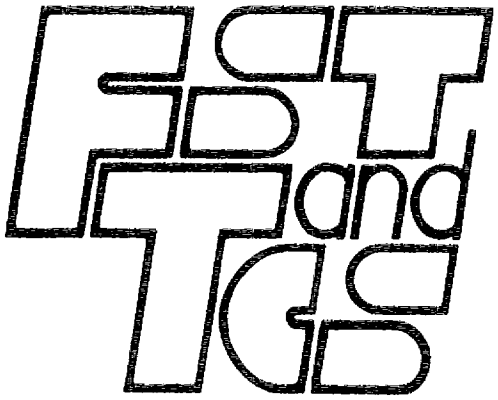
Two kinds of papers are solicited. The first are regular papers requiring approximately twenty minutes for presentation; these will be reproduced in full in the conference PROCEEDINGS. The second are short papers suitable for presentation in ten minutes; summaries of these papers will be published in the PROCEEDINGS. The purpose of the short paper category is to encourage authors to present preliminary results of their work.

INSTRUCTIONS FOR AUTHORS: For regular papers, a title and one-thousand-word summary are required. Summaries should include references and be of sufficient detail and length to permit careful reviewing. For short papers, a title and five-hundred-word summary are required. These must be received by July 31, 1983. Manuscripts that are submitted as regular papers and cannot be accommodated in that category will be considered in the short paper category unless the authors indicate otherwise.

Authors will be notified of acceptance by September 1, 1983. Special sheets for the preparation of accepted papers for the PROCEEDINGS will be sent to each author. The length of regular papers is limited to the equivalent of ten single-spaced 8 1/2-by-11 inch pages. Short papers are limited to the equivalent of two single-spaced 8 1/2-by-11 inch pages.

All manuscripts are to be mailed to Allerton Conference, c/o Prof. Tamer Başar Coordinated Science Laboratory, University of Illinois at Urbana Champaign, 1101 W. Springfield Avenue, Urbana, Illinois 61801. Please indicate clearly the name and address of the author who should receive all subsequent correspondence.

CONFERENCE CO-CHAIRMEN: T. BAŞAR, D. J. BROWN AND H. V. POOR




# CALL FOR PAPERS

## Third Conference on Foundations of Software Technology and Theoretical Computer Science

Bangalore, India, 12-14 December 1983

*Sponsored by*

National Centre for Software Development and Computing Techniques
Tata Institute of Fundamental Research



Papers are invited for the Third Conference on Foundations of Software Technology and Theoretical Computer Science, to be held in Bangalore, India, on 12-14 December 1983. The areas of interest include

> **Foundations of Software Technology**: program specifications, correctness of programs, programming methodology, programming languages, operating systems, computer networks, data bases, computer graphics.
>
> **Theoretical Computer Science**: automata theory, formal languages, theory of computation, program semantics, design of algorithms.

This is the third in a series of annual computer science conferences which are being organised to provide a forum for presenting research results, from India and abroad.

Papers will be refereed and a final selection will be made by the Programme Committee.

Authors should send *four* copies of each paper to

> Chairman, FST & TCS Programme Committee
> NCSDCT
> Tata Institute of Fundamental Research
> Colaba
> Bombay 400 005, India

to reach him by **31 May 1983**. Authors will be informed of acceptance by **20 July 1983** and final manuscripts of papers must be received by 1 **September 1983** to be included in the Proceedings.

# Snapshots

*POPL – 1983*

*POPL – 1983*

## NSF News

In this issue's column I want to discuss the Fiscal Year 1984 budget request submitted by the Reagan administration to Congress. As a whole, the National Science Foundation has done quite well. The administration request is 18% greater than Fiscal Year 1983 expenditures which is far higher than budget requests for other non-defense areas. The Mathematical and Physical Sciences Directorate (MPS) did even better. The FY 1984 budget request is 21.8% above the FY 1983 expenditures. Congressional hearings have already begun on the NSF budget. The above percentage increases should be viewed as tentative for Congress may choose to modify them. Below are two tables outlining the budget requests for both the Computer Science Section and the Division of Electrical, Computer, and Systems Engineering.

COMPUTER RESEARCH SUBACTIVITY ..... **$34,675,000**

| *Program Element* | *Actual FY 1982* | *Request FY 1983* | *Current Plan FY 1983* | *Estimate FY 1984* | *Difference FY 1984/83* |
|---|---|---|---|---|---|
| Theoretical Computer Science ..... | $3,224,555 | $3,250,000 | $3,200,000 | $3,700,000 | $500,000 |
| Software Systems Science ..... | 3,149,751 | 3,400,000 | 3,100,000 | 3,700,000 | 600,000 |
| Software Engineering ..... | 3,132,891 | 3,200,000 | 3,000,000 | 3,500,000 | 500,000 |
| Intelligent Systems ..... | 3,347,627 | 3,200,000 | 3,000,000 | 3,500,000 | 500,000 |
| Computer Systems Design ..... | 3,077,885 | 3,400,000 | 3,100,000 | 3,600,000 | 500,000 |
| Coordinated Experimental Research ..... | 8,552,738 | 11,250,000 | 11,175,000 | 13,725,000 | 2,550,000 |
| Special Projects ..... | 1,259,645 | 1,600,000 | 1,245,000 | 1,450,000 | 205,000 |
| Computer Research Equipment ..... | —0— | —0— | 1,300,000 | 1,500,000 | 200,000 |
| Total ..... | $25,745,092 | $29,300,000 | $29,120,000 | $34,675,000 | $5,555,000 |

ELECTRICAL, COMPUTER, AND SYSTEMS ENGINEERING SUBACTIVITY ... $36,700,000

| *Program Element* | *Actual FY 1982* | *Request FY 1983* | *Current Plan FY 1983* | *Estimate FY 1984* | *Difference FY 1984/83* |
|---|---|---|---|---|---|
| Automation, Bioengineering, and Sensing Systems ..... | $4,758,147 | $5,140,000 | $4,939,000 | $6,350,000 | $1,411,000 |
| Electrical and Optical Communications ..... | 4,478,200 | 5,300,000 | 5,141,000 | 6,350,000 | 1,209,000 |
| Computer Engineering ..... | 2,607,298 | 2,590,000 | 2,500,000 | 3,700,000 | 1,200,000 |
| Quantum Electronics, Waves and Beams ..... | 4,095,336 | 4,670,000 | 4,534,000 | 5,400,000 | 866,000 |
| Solid State and Microstructures Engineering . | 4,793,000 | 5,730,000 | 5,556,000 | 7,200,000 | 1,644,000 |
| Systems Theory and Operations Research ... | 4,404,983 | 4,770,000 | 4,630,000 | 5,400,000 | 770,000 |
| Science and Technology to Aid the Handicapped ..... | 646,823 | —0— | 2,000,000 | 2,300,000 | 300,000 |
| Total ..... | $25,783,787 | $28,200,000 | $29,300,000 | $36,700,000 | $7,400,000 |

In addition to the above, the President has proposed that funds be allocated to new Presidential Young Investigator awards. The purpose of this program is to encourage young faculty (defined as scientists within 7 years of their Ph.D.) to remain within academic institutions in those scientific disciplines where there is a shortage of university faculty. The details of the program are now being formulated (National Science Board action is required). This is a program that could be of great significance to computer scientists (ours being both a young field and one in which there is a university faculty shortage). I will report further on the program when I have more information.

To add to my column of the last issue, there is one additional advising body of interest. This is the Computer Research Advisory subcommittee. It consists of academic and industrial scientists drawn from the disciplines supported within the Computer Science section and reports to the National Science Board. Its purpose is to review the Computer Science section programs, to review the section as a whole, and to provide advice concerning how the NSF can best serve the needs of the research community. The current chairman of the committee is Al Aho (until Summer 1983); after that the chairman is Ray Miller.

A final note to give you an update on the status of the Theoretical Computer Science program. As of this date (mid-February), the number of proposals is running about 8% above last years level. I expect the final total to be about 10-12% above last year's requests. I have used more than 300 reviewers (thank you all!) already and the response rate this year is higher than last year. The FY 1982 summary of awards is out and available. Write to me if you wish a copy.


John C. Cherniavsky
Program Director
Theoretical Computer Science

# HOW TO PROVE IT*

Dana Angluin

proof by example:
The author gives only the case n = 2 and suggests that it contains most of the ideas of the general proof.

proof by intimidation:
'Trivial.'

proof by vigorous handwaving:
Works well in a classroom or seminar setting.

proof by cumbersome notation:
Best done with access to at least four alphabets and special symbols.

proof by exhaustion:
An issue or two of a journal devoted to your proof is useful.

proof by omission:
'The reader may easily supply the details.'
'The other 253 cases are analogous.'
'...'

proof by obfuscation:
A long plotless sequence of true and/or meaningless syntactically related statements.

proof by wishful citation:
The author cites the negation, converse, or generalization of a theorem from the literature to support his claims.

proof by funding:
How could three different government agencies be wrong?

proof by eminent authority:
'I saw Karp in the elevator and he said it was probably NP-complete.'

proof by personal communication:
'Eight-dimensional colored cycle stripping is NP-complete [Karp, personal communication].'

---

*with apologies to G. Polya and contributions from the Yale Computer Science Department.

proof by reduction to the wrong problem:
'To see that infinite-dimensional colored cycle stripping is decidable, we reduce it to the halting problem.'

proof by reference to inaccessible literature:
The author cites a simple corollary of a theorem to be found in a privately circulated memoir of the Slovenian Philological Society, 1883.

proof by importance:
A large body of useful consequences all follow from the proposition in question.

proof by accumulated evidence:
Long and diligent search has not revealed a counterexample.

proof by cosmology:
The negation of the proposition is unimaginable or meaningless. Popular for proofs of the existence of God.

proof by mutual reference:
In reference A, Theorem 5 is said to follow from Theorem 3 in reference B, which is shown to follow from Corollary 6.2 in reference C, which is an easy consequence of Theorem 5 in reference A.

proof by metaproof:
A method is given to construct the desired proof. The correctness of the method is proved by any of these techniques.

proof by picture
A more convincing form of proof by example. Combines well with proof by omission.

proof by vehement assertion:
It is useful to have some kind of authority relation to the audience.

proof by ghost reference:
Nothing even remotely resembling the cited theorem appears in the reference given.

proof by forward reference:
Reference is usually to a forthcoming paper of the author, which is often not as forthcoming as at first.

proof by semantic shift:
Some standard but inconvenient definitions are changed for the statement of the result.

proof by appeal to intuition:
Cloud-shaped drawings frequently help here.