List of important publications in computer science

This is a list of **important publications** in computer science, organized by field.

Some reasons why a particular publication might be regarded as important:

- **Topic creator** – A publication that created a new topic
- **Breakthrough** – A publication that changed scientific knowledge significantly
- **Introduction** – A publication that is a good introduction or survey of a topic
- **Influence** – A publication which has significantly influenced the world
- **Latest and greatest** – The current most advanced result in a topic

Computability

Computability: An introduction to recursive function theory

- Nigel J. Cutland
- Cambridge University Press, 1980, ISBN 0-521-29465-7

Description: A very popular textbook.

Decidability of second order theories and automata on infinite trees

- Michael O. Rabin
- Trans. Amer. Math. Soc. 141 (1969) pp. 1–35

Description: The paper presented the tree automaton, an extension of the automata. The tree automaton had numerous applications to proofs of correctness of programs.

Finite automata and their decision problems

- Michael O. Rabin and Dana S. Scott
- IBM J. Research and Development, 3:114–125, 1959.
- Online version [1]

Description: Mathematical treatment of automata, proof of core properties, and definition of non-deterministic finite automaton.

Introduction to Automata Theory, Languages, and Computation

- John E. Hopcroft
- Jeffrey D. Ullman
- Rajeev Motwani
- Addison-Wesley, 2001, ISBN 0-201-02988-X

Description: A popular textbook.

On certain formal properties of grammars

- Noam Chomsky
- Information and Control 2 (1959), 137–167.

Description: This article introduced what is now known as the Chomsky hierarchy, a containment hierarchy of classes of formal grammars that generate formal languages.

On computable numbers, with an application to the Entscheidungsproblem

- Alan Turing
- Proceedings of the London Mathematical Society, Series 2, 42 (submitted May 28, 1936, read November 12, 1936), pp 230–265. Errata appeared in Series 2, 43 (1937), pp 544–546.
- Online version [2]
- PDF version of above page (verified to display properly with xpdf and acroread) [3]

Description: This article set the limits of computer science. It defined the Turing Machine, a model for all computations. On the other hand it proved the undecidability of the halting problem and Entscheidungsproblem and by doing so found the limits of possible computation.

Computational complexity theory

A machine-independent theory of the complexity of recursive functions

- Manuel Blum
- Journal of the ACM, **14**(2):322 336, 1967.

Description: The Blum axioms.

Algebraic methods for interactive proof systems

- Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan
- Journal of the ACM, 39(4):859–868, 1992.

Description: This paper showed that PH is contained in IP.

The complexity of theorem proving procedures'

- S. A. Cook
- *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing* (1971), pp. 151–158.

Description: This paper introduced the concept of NP-Completeness and proved that Boolean satisfiability problem(SAT) is NP-Complete. Note that similar ideas were developed independently slightly later by Leonid Levin at "Levin, Universal Search Problems. Problemy Peredachi Informatsii 9(3):265-266, 1973".

Computers and Intractability: A Guide to the Theory of NP-Completeness

- Michael R. Garey, David S. Johnson
- Freeman, New York, 1979
- ISBN 0-7167-1045-5

Description: The main importance of this book is due to its extensive list of more than 300 NP-Complete problems. This list became a common reference and definition. Though the book was published only few years after the concept was defined such an extensive list was found.

Degree of difficulty of computing a function and a partial ordering of recursive sets

- Michael O. Rabin
- Tech. Rep. No. 1, O.N,R., Jerusalem, 1960

Description: This technical report was the first publication talking about what later was renamed computational complexity

How to Construct Random Functions

- Oded Goldreich, Shafi Goldwasser, Silvio Micali
- *Journal of the ACM*, 33(4), 1984, 792–807.
- Online copy (PDF) [4]

Description: This paper showed that the existence of one way functions leads to computational randomness.

IP = PSPACE

- Adi Shamir
- Journal of the ACM, 39(4):869–877, 1992.

Description: IP is a complexity class whose characterization (based on interactive proof systems) is quite different from the usual time/space bounded computational classes. In this paper, Shamir extended the technique of the previous paper by Lund, et al., to show that PSPACE is contained in IP, and hence IP = PSPACE, so that each problem in one complexity class is solvable in the other.

Reducibility among combinatorial problems

- R. M. Karp
- In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, New York, NY, 1972.

Description: This paper showed that 21 different problems are NP-Complete and showed the importance of the concept.

The Knowledge Complexity of Interactive Proof Systems

- Shafi Goldwasser, Silvio Micali, Charles Rackoff
- SIAM Journal of Computing, 18(1):186–208, February 1989.

Description: This paper introduced the concept of zero knowledge.

Letter from Gödel to von Neumann

- Kurt Gödel
- A Letter from Gödel to John von Neumann, March 20, 1956
- Online version [5]

Description: Gödel discusses the idea of efficient universal theorem prover

On the computational complexity of algorithms

- Juris Hartmanis
- Richard Stearns
- Trans. Amer. Math. Soc. 117 (1965), 285–306.

Description: This paper gave computational complexity its name and seed.

Paths, trees, and flowers

- Jack Edmonds
- Canadian Journal of Mathematics, Vol 17, No -, 449-467, 1965

Description: There is a polynomial time algorithm to find a maximum matching in a graph that is not bipartite and another step toward the idea of computational complexity. For more information see[6]

Theory and Applications of Trapdoor functions

- Andrew Chi-Chih Yao
- Proc. 23rd Symposium on Foundations of Computer Science (1982), pp. 80–91

Description: This paper creates a theoretical framework for Trapdoor functions and described some of their applications, like in cryptography. Note that the concept of trapdoor functions was brought at "New directions in cryptography" six years earlier (See section V "Problem Interrelationships and Trap Doors.").

Computational Complexity

- C.H. Papadimitriou
- Addison-Wesley, 1994. ISBN 0-201-53082-1

Description: This book provides a very good introduction to Computational Complexity

Interactive Proofs and the Hardness of Approximating Cliques

- Uriel Feige, Shafi Goldwasser, Laszlo Lovász, Shmuel Safra, and Mario Szegedy
- Journal of the ACM, 43:268–292, 1996.

Probabilistic Checking of Proofs: A New Characterization of NP

- Sanjeev Arora and Shmuel Safra
- Journal of the ACM, 45:70–122, 1998.

Proof Verification and the Hardness of Approximation Problems

- Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy
- Journal of the ACM, 45:501–555, 1998.

Description: These three papers established the surprising fact that certain problems in NP remain hard even when only an approximative solution is required.

Computational Linguistics

Realization of Natural-Language Interfaces Using Lazy Functional Programming

- Richard A. Frost
- ACM Computing Surveys Volume 38 Issue 4 Article 11, December 2006
- Online copy [7]

Description: This survey documents relatively less researched importance of lazy functional programming languages (i.e. Haskell) to construct Natural Language Processors and to accommodated many linguistic theories.

Algorithms

See also List of algorithms.

A machine program for theorem proving

- M. Davis, G. Logemann, D. Loveland
- Communications of the ACM, 5:394–397, 1962. reprinted at Siekmann, Jörg and Graham Wrightson (eds), Automation of Reasoning, vol. 1, Springer Verlag, 1983, pp. 267–270.

Description: The DPLL algorithm. The basic algorithm for SAT and other NP-Complete problems.

A Machine-Oriented Logic Based on the Resolution Principle

- J. Alan Robinson
- *Communications of the ACM*, 5:23–41, 1965.

Description: First description of resolution and unification used in automated theorem proving; used in Prolog and logic programming.

The traveling-salesman problem and minimum spanning trees

- M. Held, Richard Karp
- *Operations Res. 18 (1970),1138-1162*

Description: The use of an algorithm for minimum spanning tree as an approximation algorithm for the NP-CompleteTravelling salesman problem. Approximation algorithms became a common method for coping with NP-Complete problems.

A polynomial algorithm in linear programming

- L. G. Khachiyan
- *Soviet Mathematics Doklady, 20:191—194, 1979.*

Description: For long, there was no provably polynomial time algorithm for the linear programming problem. Khachiyan was the first to provide an algorithm that was polynomial (and not just was fast enough most of the time as previous algorithms). Later, Karmarkar presented a faster algorithm at: Narendra Karmarkar(1984). "A New Polynomial Time Algorithm for Linear Programming", Combinatorica, Vol 4, nr. 4, p. 373–395.

Probabilistic algorithm for testing primality

- Michael O. Rabin
- Journal of Number Theory 12 (1980), no. 1, pp. 128–138.

Description: The paper presented the Miller-Rabin primality test and outlined the program of randomized algorithms.

Optimization by simulated annealing

- Kirkpatrick, S., Gelatt, C., & Vecchi, M.
- Science, Number 4598, 13, pages 671–680, May 1983.
- Online copy [8]

Description: This article described simulated annealing which is now a very common heuristic for NP-Complete problems.

The Art of Computer Programming

- Donald Knuth

Description: This monograph has three popular algorithms books and a number of fascicles. The algorithms are written in both English and MIX assembly language (or MMIX assembly language in more recent fascicles). This makes algorithms both understandable and precise. However, the use of a low-level programming language frustrates some programmers more familiar with modern structured programming languages.

Algorithms + Data Structures = Programs

- Niklaus Wirth
- Prentice Hall, 1976, ISBN 0-13-022418-9

Description: An early, influential book on algorithms and data structures, with implementations in Pascal.

The Design and Analysis of Computer Algorithms

- Alfred V. Aho
- John E. Hopcroft
- Jeffrey D. Ullman
- Addison-Wesley, 1974, ISBN 0-201-00029-6

Description: One of the standard texts on algorithms for the period of approximately 1975–1985.

How to Solve It By Computer

- How to Solve It
- RG Dromey
- Prentice Hall (1982), ISBN 0-13-434001-9

Description: Explains the *Why*s of algorithms and data-structures. Explains the *Creative Process*, the *Line of Reasoning*, the *Design Factors* behind innovative solutions.

Algorithms

- Robert Sedgewick
- Addison-Wesley, 1983, ISBN 0-201-06672-6

Description: A very popular text on algorithms in the late 1980s. It was more accessible and readable (but more elementary) than Aho, Hopcroft, and Ullman. There are more recent editions.

Introduction to Algorithms

- Thomas H. Cormen
- Charles E. Leiserson
- Ronald L. Rivest
- Clifford Stein
- MIT Press and McGraw-Hill. 2nd Edition, 2001. 1st Edition (with first three authors) published in 1991.

Description: As its name indicates this textbook is a very good introduction to algorithms. This book became so popular that it is almost the de facto standard for basic algorithms teaching.

Algorithmic information theory

A formal theory of inductive inference

- Ray Solomonoff
- Information and Control, vol. 7, pp. 1–22, March 1964; pp. 224–254, June 1964.
- Online copy, Part I [9]
- Online copy, Part II [10]

Description: This was the beginning of Algorithmic information theory and Kolmogorov complexity. Note that though Kolmogorov complexity is named after Andrey Kolmogorov, he said that the seeds of that idea are due to Ray Solomonoff. Andrey Kolmogorov contributed a lot to this area but in later articles.

Algorithmic information theory

- Gregory Chaitin
- IBM Journal of Research and Development 21 (1977), pp. 350–359, 496.
- Online version [11]

Description: A good introduction to Algorithmic information theory by one of the important people in the area.

Information theory

A mathematical theory of communication

- C.E. Shannon
- *Bell System Technical Journal*, 27:379–423,623–656, 1948
- Online copy (HTML) [12]

Description: This paper created communication theory and information theory.

Error detecting and error correcting codes

- Richard Hamming
- *Bell Systems Technical Journal*, vol. 29, pp. 147–160, 1950
- Online copy [13]

Description: In this paper, Hamming introduced the idea of error-correcting code. He created the Hamming code and the Hamming distance and developed methods for code optimality proofs.

A Method for the Construction of Minimum Redundancy Codes

- David A. Huffman
- Proceedings of the Institute of Radio Engineers, September 1952, Volume 40, Number 9, pp. 1098–1101.
- Online copy [14]

Description: The Huffman coding.

A Universal Algorithm for Sequential Data Compression

- Jacob Ziv
- Abraham Lempel
- IEEE Transactions on Information Theory, Vol. 23, No. 3, pp. 337–343.
- Online copy [15]

Description: The LZ77 compression algorithm.

Elements of Information Theory

- Thomas M. Cover
- Joy A. Thomas
- Wiley, 1991.

Description: A good and popular introduction to information theory.

Operating systems

An experimental timesharing system.

- Fernando J. Corbató,M. Merwin-Daggett, and R.C. Daley
- Proceedings of the AFIPS FJCC, pages 335–344, 1962.
- Online copy (HTML) [16]

Description: This paper discuss time-sharing as a method of sharing computer resource. This idea changed the interaction with computer systems.

The Working Set Model for Program Behavior

- Peter J. Denning
- Communications of the ACM, Vol. 11, No. 5, May 1968, pp 323–333
- Online version(PDF) [17]

Description: The beginning of cache. For more information see SIGOPS Hall of Fame [18].

Virtual Memory, Processes, and Sharing in MULTICS

- Robert C. Daley, Jack B. Dennis
- Communications of the ACM, Vol. 11, No. 5, May 1968, pp. 306–312.
- Online version(PDF) [19]

Description: The classic paper on the most ambitious operating system in the early history of computing. Difficult reading, but it describes theimplications of trying to build a system that takes information sharing to its logical extreme. Most operating systems since Multics have incorporated a subset of its facilities.

A note on the confinement problem

- Butler W. Lampson
- Communications of the ACM, 16(10):613-615, October 1973.
- Online version(PDF) [20]

Description: This paper addresses issues in constraining the flow of information from untrusted programs. It discusses covert channels, but more importantly it addresses the difficulty in obtaining full confinement without making the program itself effectively unusable. The ideas are important when trying to understand containment of malicious code, as well as aspects of trusted computing.

The UNIX Time-Sharing System

- Dennis M. Ritchie and Ken Thompson
- Communications of the ACM 7, 7, July 1974.
- Online copy (few formats) [21]

Description: The Unix operating system and its principles were described in this paper. The main importance is not of the paper but of the operating system, which had tremendous effect on operating system and computer technology.

Weighted voting for replicated data

- David K. Gifford
- Proceedings of the 7th ACM Symposium on Operating Systems Principles, pages 150-159, December 1979. Pacific Grove, California
- Online copy (few formats) [22]

Description: This paper describes the consistency mechanism known as quorum consensus. It is a good example of algorithms that provide a continuous set of options between two alternatives (in this case, between the read-one write-all, and the write-one read-all consistency methods). There have been many variations and improvements by researchers in the years that followed, and it is one of the consistency algorithms that should be understood by all. The options available by choosing different size quorums provide a useful structure for discussing of the core requirements for consistency in distributed systems.

Experiences with Processes and Monitors in Mesa

- Butler W. Lampson, David D. Redell
- Communications of the ACM, Vol. 23, No. 2, February, 1980, pp. 105–117.
- Online copy (PDF) [23]

Description: This is the classic paper on synchronization techniques, including both alternate approaches and pitfalls.

Scheduling Techniques for Concurrent Systems

- J. K. Ousterhout
- Proceedings of Third International Conference on Distributed Computing Systems, 1982, 22—30.

Description: Algorithms for coscheduling of related processes were given

A Fast File System for UNIX

- Marshall Kirk Mckusick, William N. Joy, Samuel J. Leffler, Robert S. Fabry
- IACM Transactions on Computer Systems, Vol. 2, No. 3, August 1984, pp. 181–197.
- Online copy (PDF) [24]

Description: The file system of UNIX. One of the first papers discussing how to manage disk storage for high-performance file systems. Most file-system research since this paper has been influenced by it, and most high-performance file systems of the last 20 years incorporate techniques from this paper.

The Design and Implementation of a Log-Structured File System

- Mendel Rosenblum,J. K. Ousterhout
- ACM Transactions on Computer Systems, Vol. 10, No. 1 (February 1992), pp. 26–52.
- Online version [25]

Description: Log-structured file system.

Microkernel operating system architecture and Mach

- David L. Black, David B. Golub, Daniel P. Julin, Richard F. Rashid, Richard P. Draves, Randall W. Dean, Alessandro Forin, Joseph Barrera, Hideyuki Tokuda, Gerald Malan, David Bohman
- Proceedings of the USENIX Workshop on Microkernels and Other Kernel Architectures, pages 11–30, April 1992.

Description: This is a good paper discussing one particular microkernel architecture, and the benefits over more monolithic kernel approaches to system design. Mach underlies Mac OS X, and its architecture had a significant impact on the design of the Windows NT kernel and modern microkernels like L4.

An Implementation of a Log-Structured File System for UNIX

- Margo Seltzer, Keith Bostic, Marshall Kirk McKusick, Carl Staelin
- Proceedings of the Winter 1993 USENIX Conference, San Diego, CA, January 1993, 307-326
- Online version [26]

Description: The paper was the first production-quality implementation of that idea which spawned much additional discussion of the viability and short-comings of log-structured filesystems. While "The Design and Implementation of a Log-Structured File System" was certainly the first, this one was important in bringing the research idea to a usable system.

Soft Updates: A Solution to the Metadata Update problem in File Systems

- G. Ganger, M. McKusick, C. Soules, Y. Patt
- ACM Transactions on Computer Systems 18, 2. pp 127–153, May 2000
- Online version [27]

Description: A new way of maintaining filesystem consistency.

Databases

A relational model for large shared data banks

- E. F. Codd
- *Communications of the ACM*, 13(6):377–387, June 1970

Description: This paper introduced the relational model for databases. This model became the number one model.

Binary B-Trees for Virtual Memory

- Rudolf Bayer
- ACM-SIGFIDET Workshop 1971, San Diego, California, Session 5B, p. 219-235.

Description: This paper introduced the B-Trees data structure. This model became the number one model.

Relational Completeness of Data Base Sublanguages

- E. F. Codd
- In: R. Rustin (ed.): Database Systems: 65-98, Prentice Hall and IBM Research Report RJ 987, San Jose, California : (1972)
- Online version (PDF) [28]

Description: Completeness of Data Base Sublanguages

The Entity Relationship Model – Towards a Unified View of Data

- Peter Chen
- *ACM Transactions on Database Systems*, Vol. 1, No. 1, March 1976, pp. 9–36 [29]

Description: This paper introduced the Entity-relationship diagram(ERD) method of database design.

SEQUEL: A structured English query language

- Donald D. Chamberlin, Raymond F. Boyce
- International Conference on Management of Data, Proceedings of the 1974 ACM SIGFIDET (now SIGMOD) workshop on Data description, access and control, Ann Arbor, Michigan, pp. 249–264

Description: This paper introduced the SQL language.

The notions of consistency and predicate locks in a database system

- K.P. Eswaran, J. Gray, R.A. Lorie, I.L. Traiger
- Communications of the ACM 19, 1976, 624—633

Description: This paper defined the concepts of transaction, consistency and schedule.It also argued that a transaction needs to lock a logical rather than a physical subset of the database.

Mining association rules between sets of items in large databases

- Rakesh Agrawal, Tomasz Imielinski, Arun Swami
- *Proc. of the ACM SIGMOD Conference on Management of Data*, pages 207–216, Washington, D.C., May 1993
- Online copy (HTML) [30]

Description: Association rules, a very common method for data mining.

Principles of Transaction-Oriented Database Recovery

- Theo Härder, Andreas Reuter
- *ACM Computing Surveys 15(4)*, May 1983

Description: Introduced the ACID paradigm for transactions.

Information Retrieval

A Vector Space Model for Automatic Indexing

- Gerard Salton, A. Wong, C. S. Yang
- Commun. ACM 18(11): 613-620 (1975)

Description: Presented the vector-space model.

Extended Boolean Information Retrieval

- Gerard Salton, Edward A. Fox, Harry Wu
- Commun. ACM 26(11): 1022-1036 (1983)

Description: Presented the inverted-index

Cryptography

The index of coincidence and its applications in cryptology

- William F. Friedman
- The index of coincidence and its applications in cryptology, Department of Ciphers. Publ 22. Geneva, Illinois, USA: Riverbank Laboratories, 1922.

Description: Presented the index of coincidence method for codebreaking.

Treatise on the Enigma

- Alan Turing
- Online version [31]

Description: The breaking of the Enigma.

Communication Theory of Secrecy Systems

- C.E. Shannon
- *Communication Theory of Secrecy Systems*, Bell System Technical Journal, vol.28-4, page 656–715, 1949.
- Online copy (PDF) [32]

Description: Information theory based analysis of cryptography. The original form of this paper was a confidential Bell Labs report from 1945, not the one published.

The Codebreakers, The Story of Secret Writing

- David Kahn
- New York: The Macmillan Company, 1967, (ISBN 0-684-83130-9).

Description: Almost nothing had been published in cryptography in several decades and very few non-government researchers were thinking about it. The Codebreakers, a popular and not academic book, made many more people aware and contains a lot of technical information, although it requires careful reading to extract it. Its 1967 appearance was followed by the appearance of many papers over the next few years.

Cryptographic Coding for Data-Bank Privacy

- Horst Feistel
- IBM Research Report 2827, March 18, 1970.

Description: Feistel ciphers are a form of cipher of which DES is the most important. It would be hard to overestimate the importance of either Feistel or DES. Feistel pushed a transition from stream ciphers to block ciphers. Although most ciphers operate on streams, most of the important ciphers today are block ciphers at their core.

Data Encryption Standard

- NBS Federal Standard FIPS PUB 46, 15 Jan 1977.

Description: DES is not only one of the most widely deployed ciphers in the world but has had a profound impact on the development of cryptography. Roughly a generation of cryptographers devoted much of their time to attacking and improving DES.

New directions in cryptography

- W.Diffie, M.E.Hellman
- IEEE Transactions on Information Theory, IT-22, 6, 1976, pp. 644–654
- Online copy (HTML) [33]

Description: This paper suggested public key cryptography and presented Diffie-Hellman key exchange. For more information about this work see: W.Diffie, M.E.Hellman, "Privacy and Authentication: An Introduction to Cryptography" [34], in Proc. IEEE, Vol 67(3) Mar 1979, pp 397–427.

On the Signature Reblocking Problem in Public Key

- Loren M. Kohnfelder
- Commun. ACM, vol. 21, no. 2, p. 179, 1978.

Description: In this paper (along with Loren M. Kohnfelder,"Using Certificates for Key Distribution in a Public-Key Cryptosystem", MIT Technical report 19 May 1978), Kohnfelder introduced certificates (signed messages containing public keys) which are the heart of all modern key management systems.

Secure Communications Over Insecure Channels

- Ralph C. Merkle
- Commun. ACM, vol. 21, no. 4, pages. 294-299, April 1978.

Description: This paper introduced a branch public key cryptography, known as public key distribution systems. Merkle work predated "New directions in cryptography" though it was published after it. The Diffie-Hellman key exchange is an implementation of such a Merkle system. Hellman himself has argued [35] that the more correct name would be Diffie-Hellman-Merkle key exchange.

A Method for Obtaining Digital Signatures and Public Key Cryptosystems

- R. Rivest, A. Shamir, L. Adleman
- Communications of the ACM, Vol. 21 (2), 1978, pages 120–126
- Online copy (HTML) [36]

Description: The RSA encryption method. The first public key encryption method.

Using encryption for authentication in large networks of computers

- R M Needham, M D Schroeder
- Communications of the ACM, Vol 21, No 12 (1978)
- Online version(PDF) [37]

Description: This paper introduced the basic ideas of cryptographic protocols and showed how both secret-key and public-key encryption could be used to achieve authentication.

How to Share a Secret

- Shamir, A.
- Communications of the ACM, vol. 22, no. 11, pp. 612–613 (November 1979)
- Online copy (HTML) [38]

Description: A safe method for sharing a secret.

Data Security

- Dorothy E. Denning ,Peter J. Denning
- Computing Surveys, Vol. 11, No. 3, September 1979, if pp. 227–249.

Description: A paper that surveys the problems in creating secure systems. The description of database inference is particularly chilling; after reading this you'll understand why it is very difficult to publish aggregated information such as census data without accidentally exposing the private information of individuals.

Security policies and security models

- J. Goguen, J. Meseguer
- IEEE symposium on security and privacy, 1982, pp11–20
- Online version(PDF) [39]

Description: Noninterference is the study of when interaction by one user with a system can affect what a second user sees. It can be applied to trying to stop an attacker disrupting the second user's view of the system, or to analysing whether a high-security first user can pass information to a low-level second user via a covert channel. This paper was the first to give a useful characterisation of this property.

On the security of public key protocols

- D Dolev, A Yao
- IEEE transactions on Information Theory Vol 2 number 3, 1983

Description: Introduced the model of the adversary against which almost all cryptographic protocols are judged.

Probabilistic Encryption

- Shafi Goldwasser, Silvio Micali
- Special issue of Journal of Computer and Systems Sciences, Vol. 28, No. 2, pages 270-299, April 1984.
- Online version (PDF) [40]

Description: The paper provides a rigorous basis to encryption (e.g., partial information) and shows that it possible to equate the slightest cryptanalysis to solve a pure math problem. Second, it introduces the notion of computational indistinguishability that has and will underpin our understanding of the world, since ultimately we all are bounded computational entities.

Fast, rigorous factorization and discrete logarithm algorithms

- Carl Pomerance
- D. S. Johnson, T. Nishizeki, A. Nozaki, H. S. Wilf, eds., Academic Press, Orlando, Florida, 1987, pp. 119–143.

Description: First published sub exponential algorithm to the Discrete logarithm problem. The Discrete logarithm problem is the base of many cryptographic systems. Pomerance algorithm is second chronologically to the work of Rich Schroeppel's work. Schroeppel rarely published and preferred to circulate his work to interested researchers. Schroeppel's work is referenced at Knuth, vol. 2, 2nd edition, pages 383-384.

How to Prove all NP-Statements in Zero-Knowledge, and a Methodology of Cryptographic Protocol Design

- Goldreich, O, Micali, S., Wigderson, A.
- CRYPTO, LNCS vol 263, pp. 171–185, 1987
- Online copy(HTML) [41]

Description: This paper explains how to construct a zero-knowledge proof system for any language in NP.

How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority

- Goldreich, O, Micali, S., Wigderson, A.
- ACM Symposium on Theory of Computing, pgs. 218-229, 1987
- Online copy(HTML) [42]

Description: Seminal paper in secure function evaluation

The Digital distributed system security architecture

- M. Gasser, A. Goldstein, C. Kaufman, B. Lampson
- Proceedings of the 1989 National Computer Security Conference, pages 305-319, 1989.
- Online copy [43]

Description: This paper discusses issues related to privileges and authentication of software and hardware components in distributed systems. It is interesting in that it formalizes the understanding of the rights used by programs and software running on bahalf of users and other entities. The concepts from this paper provide an early glimpse at the issues of atestation addressed much later by trusted computing architectures.

Kerberos: An Authentication Service for Open Network Systems

- Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller
- B. Clifford Neuman and Theodore Ts'o IEEE Communications, 32(9) pp33–38, September 1994.
- See also Proc. USENIX Winter Conference, February 1988, pp. 191–202
- Online version (HTML) [44]

Description: The Kerberos authentication protocol, which allows individuals communicating over an insecure network to prove their identity to one another in a secure and practical manner.

Differential Cryptanalysis of DES-like Cryptosystems

- Eli Biham, Adi Shamir
- Journal of Cryptology, Vol. 4 No. 1 1991
- Online version [45]

Description: The method of Differential cryptanalysis.

A new method for known plaintext attack of FEAL cipher

- Matsui, M., Yamagishi, A
- EUROCRYPT Advances in Cryptology - 1992
- Online version [46]

Description: The method of Linear cryptanalysis.

Breaking and Fixing the Needham-Schroeder Public-Key protocol using FDR

- Gavin Lowe
- Software - concepts and tools 1996
- Online version [47]

Description: Used a standard model checker to analyse one of the original cryptographic protocols that had long been believed correct. By exposing what is now the most famous protocol attack using this method, this paper inspired an explosion of interest in the verification and analysis of such protocols that continues to this day.

Differential Collisions in SHA-0

- Florent Chabaud, Antoine Joux
- Advances in Cryptology — CRYPTO '98

Description: A method for finding collisions in SHA-0 hash function.

EFF DES cracker

- Paul Kocher
- 1998

Description: "the EFF DES cracker" (nicknamed "Deep Crack") is a machine built by the Electronic Frontier Foundation (EFF) to perform a brute force search of DES's keyspace—that is, to decrypt an encrypted message by trying every possible key. The aim in doing this was to prove that DES's key is not long enough to be secure.

Artificial intelligence

Computing machinery and intelligence

- Alan Turing
- Mind, 59:433–460, 1950.
- Online copy [48]

Description: This paper discusses whether machine can think and suggested the Turing test as a method for checking it.

A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence

- John McCarthy
- Marvin Minsky
- N. Rochester
- C.E. Shannon
- Online copy [49]

Description: This summer research proposal inaugurated and defined the field. It contains the first use of the term artificial intelligence and this succinct description of the philosophical foundation of the field: "every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it." (See philosophy of AI) The proposal invited researchers to the Dartmouth conference, which is widely considered the "birth of AI". (See history of AI.)

Fuzzy sets

- Lotfi Zadeh
- Information and Control, Vol. 8, pp. 338–353. (1965).
- Online copy [50]

Description: The seminal paper published in 1965 provides details on the mathematics of fuzzy set theory.

Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference

- Judea Pearl
- ISBN 1-55860-479-0 Publisher: Morgan Kaufmann Pub, 1988

Description: This book introduced Bayesian methods to AI.

Artificial Intelligence: A Modern Approach

- Stuart J. Russell and Peter Norvig
- Prentice Hall, Englewood Cliffs, New Jersey, 1995, ISBN 0-13-080302-2
- Textbook's website [51]

Description: The standard textbook in Artificial Intelligence. The book web site [51] lists over 1000 colleges and universities in 93 countries using it.

Machine learning

An Inductive Inference Machine

- Ray Solomonoff
- *IRE Convention Record*, Section on Information Theory, Part 2, pp. 56–62, 1957
- (A longer version of this, a privately circulated report, 1956, is online [52]).

Description: The first paper written on machine learning. Emphasized the importance of training sequences, and the use of parts of previous solutions to problems in constructing trial solutions to new problems.

Language identification in the limit

- E. M. Gold
- *Information and Control*, 10:447–474, 1967
- Online version(HTML) [53]

Description: This paper created Algorithmic learning theory.

On the uniform convergence of relative frequencies of events to their probabilities

- V. Vapnik, A. Chervonenkis
- *Theory of Probability and its Applications*, 16(2):264—280, 1971

Description: Computational learning theory, VC theory, statistical uniform convergence and the VC dimension.

A theory of the learnable

- Leslie Valiant
- *Communications of the ACM*, 27(11):1134–1142 (1984)

Description: The Probably approximately correct learning (PAC learning) framework.

Learning representations by back-propagating errors

- David E. Rumelhart, Geoffrey E. Hinton and Ronald J. Williams
- Nature, 323, 533—536, 1986

Description: Development of Backpropagation algorithm for artificial neural networks. Note that the algorithm was first described by Paul Werbos in 1974.

Induction of Decision Trees

- J.R. Quinlan
- Machine Learning, 1. 81—106, 1986.
- Online version(PDF) [54]

Description: Decision Trees are a common learning algorithm and a decision representation tool. Development of decision trees was done by many researchers in many areas, even before this paper. Though this paper is one of the most influential in the field.

Learning Quickly When Irrelevant Attributes Abound: A New Linear-threshold Algorithm

- Nick Littlestone
- Machine Learning 2: 285-318, 1988
- Online version(PDF) [55]

Description: One of the papers that started the field of on-line learning. In this learning setting, a learner receives a sequence of examples, making predictions after each one, and receiving feedback after each prediction. Research in this area is remarkable because (1) the algorithms and proofs tend to be very simple and beautiful, and (2) the model makes no statistical assumptions about the data. In other words, the data need not be random (as in nearly all other learning models), but can be chosen arbitrarily by "nature" or even an adversary. Specifically, this paper introduced the winnow algorithm.

Learning to predict by the method of temporal differences

- Richard S. Sutton
- Machine Learning 3(1): 9-44
- Online copy [56]

Description: The temporal differences method for reinforcement learning.

Learnability and the Vapnik-Chervonenkis dimension

- A. Blumer
- A. Ehrenfeucht
- D. Haussler
- M. K. Warmuth
- Journal of the ACM, 36(4):929–965, 1989.

Description: The complete characterization of PAC learnability using the VC dimension.

Cryptographic limitations on learning boolean formulae and finite automata

- M. Kearns
- L. G. Valiant
- In Proceedings of the 21st Annual ACM Symposium on Theory of Computing, pages 433–444, New York. ACM.
- Online version(HTML) [57]

Description: Proving negative results for PAC learning.

The strength of weak learnability

- Robert E. Schapire
- Machine Learning, 5(2):197–227, 1990.
- Online version(HTML) [58]

Description: Proving that weak and strong learnability are equivalent in the noise free PAC framework. The proof was done by introducing the boosting method.

Learning in the presence of malicious errors

- Michael Kearns
- Ming Li
- Journal on Computing, 22(4):807–837, August 1993.
- Online version(HTML) [59]

Description: Proving possibility and impossibility result in the malicious errors framework.

A training algorithm for optimum margin classifiers

- Bernhard E. Boser
- Isabelle M. Guyon
- Vladimir N. Vapnik
- Proceedings of the Fifth Annual Workshop on Computational Learning Theory 5 144-152, Pittsburgh (1992).
- Online version(HTML) [60]

Description: This paper presented support vector machines, a practical and popular machine learning algorithm. Support vector machines utilize the kernel trick, a generally used method.

Knowledge-based analysis of microarray gene expression data by using support vector machines

- MP Brown
- WN Grundy
- D Lin
- Nello Cristianini
- CW Sugnet
- TS Furey
- M Ares Jr,
- David Haussler
- PNAS, 2000 Jan 4;97(1):262-7 (http://www.pnas.org/cgi/content/abstract/97/1/262)

Description: The first application of supervised learning to gene expression data, in particular Support Vector Machines. The method is now standard, and the paper one of the most cited in the area.

Computer vision

The Phase Correlation Image Alignment Method

- C.D. Kuglin and D.C. Hines
- IEEE 1975 Conference on Cybernetics and Society, 1975, New York, pp. 163–165, September

Description: A correlation method based upon the inverse Fourier transform

Determining Optical Flow

- B.K.P. Horn and B.G. Schunck
- Artificial Intelligence, Volume 17, 185–203, 1981

Description: A method for estimating the image motion of world points between 2 frames of a video sequence.

An Iterative Image Registration Technique with an Application to Stereo Vision

- Lucas, B.D. and Kanade, T.
- Proceedings of the 7th International Joint Conference on Artificial Intelligence, 674–679,Vancouver, Canada,1981
- Online version [61]

Description: This paper provides efficient technique for image registration

The Laplacian Pyramid as a compact image code

- Peter J. Burt and Edward H. Adelson
- IEEE Transactions on Communications, volume = "COM-31,4", pp. 532–540, 1983.
- Online version [62]

Description: A technique for image encoding using local operators of many scales.

Snakes: Active contour models

- Michael Kass, Andrew Witkin, and Demetri Terzopoulos
- International Journal of Computer Vision, 1(4):321–331, 1988. (Marr Prize Special Issue)
- Online version [63]

Description: An interactive variational technique for image segmentation and visual tracking.

Condensation – conditional density propagation for visual tracking

- M. Isard and A. Blake
- International Journal of Computer Vision, 29(1):5–28, 1998.
- Online version [64]

Description: A technique for visual tracking

Object recognition from local scale-invariant features

- David Lowe
- International Conference on Computer Vision, pp. 1150–1157, 1999
- [65]

Description: A technique (Scale-invariant feature transform) for robust feature description

Compilers

On the translation of languages from left to right

- Donald Knuth
- *Information and Control* 8 (1965), 607-639.

Description: Bottom up parsing for deterministic context-free languages from which later the LALR approach of Yacc developed.

Semantics of Context-Free Languages.

- Donald Knuth
- *Math. Systems Theory* 2:2 (1968), 127-145.

Description: About grammar attribution, the base for yacc's s-attributed and zyacc's LR-attributed approach.

A program data flow analysis procedure

- F.E. Allen, J. Cocke
- Commun. ACM, 19, 137—147.

Description: From the abstract: "The global data relationships in a program can be exposed and codified by the static analysis methods described in this paper. A procedure is given which determines all the definitions which can possibly reach each node of the control flow graph of the program and all the definitions that are live on each edge of the graph."

A Unified Approach to Global Program Optimization

- Gary Kildall
- Proceedings of ACM SIGACT-SIGPLAN 1973 Symposium on Principles of Programming Languages.

Description: Formalized the concept of data-flow analysis as fixpoint computation over lattices, and showed that most static analyses used for program optimization can be uniformly expressed within this framework.

YACC: Yet another compiler-compiler

- Stephen C. Johnson
- *Unix Programmer's Manual* Vol 2b, 1979
- Online copy (HTML) [66]

Description: Yacc is a tool that made compiler writing much easier.

gprof: A Call Graph Execution Profiler

- Susan L. Graham, Peter B. Kessler, Marshall Kirk McKusick
- Proceedings of the ACM SIGPLAN 1982 Symposium on Compiler Construction, SIGPLAN Notices 17, 6, Boston, MA. June 1982.
- Online copy [67]

Description: The gprof profiler

Compilers: Principles, Techniques and Tools

- Alfred V. Aho
- Ravi Sethi
- Jeffrey D. Ullman
- Monica Lam
- Addison-Wesley, 1986. ISBN 0-201-10088-6

Description: This book became a classic in compiler writing. It is also known as the Dragon book, after the (red) dragon that appears on its cover.

Formal verification

On computable numbers, with an application to the Entscheidungsproblem

- Alan Turing
- Proceedings of the London Mathematical Society, Series 2, 42 (submitted May 28 1936, read November 12 1936), pp 230–265. Errata appeared in Series 2, 43 (1937), pp 544–546.
- Online version (MS IExplorer only) [2]
- PDF version of above page (verified to display properly with xpdf and acroread) [3]

Description: In his paper on the Entscheidungsproblem, Alan Turing introduces the idea of a Turing Machine which he uses to prove the undecidability of the Halting Problem and (consequently) the undecidability of first-order logic (because if FOL were decidable then the Halting Problem would be decidable). This is the first of a series of so-called "negative" results formally proving that the set of all possible programs does not include a program V that is able to decide the formal correctness of (i.e. formally verify) any given program P - any attempt to write a "program verifier" V (always returning a yes/no result in a finite time) is therefore futile because the problem is provably impossible. However, it is still possible to write a program V' (returning a yes/no/maybe result) that is able to formally verify some programs but not all programs, even if it is not possible to define in advance exactly for which programs V' will be able to return "yes/no" rather than "maybe".

Assigning Meaning to Programs

- Robert Floyd
- Mathematical Aspects of Computer Science, pages 19–32, 1967
- scanned copy [68]

Description: Robert Floyd's landmark paper Assigning Meanings to Programs introduces the method of inductive assertions and describes how a program annotated with first-order assertions may be shown to satisfy a pre- and post-condition specification - the paper also introduces the concepts of loop invariant and verification condition.

An Axiomatic Basis for Computer Programming

- C.A.R. Hoare
- Communications of the ACM, 12:576–580, 1969
- online version (PDF) [69]

Description: Tony Hoare's paper An Axiomatic Basis for Computer Programming describes a set of inference (i.e. formal proof) rules for fragments of an Algol-like programming language described in terms of (what are now called) Hoare-triples.

Guarded Commands, Nondeterminacy and Formal Derivation of Programs

- Edsger W. Dijkstra
- Communications of the ACM, 18:453–457, 1975
- online version (PDF), requires ACM membership [70]
- online version (HTML), not necessarily exactly what was published [71]

Description: Edsger Dijkstra's paper Guarded Commands, Nondeterminacy and Formal Derivation of Programs (expanded by his 1976 postgraduate-level textbook A Discipline of Programming) proposes that, instead of formally verifying a program after it has been written (i.e. post facto), programs and their formal proofs should be developed hand-in-hand (using predicate transformers to progressively refine weakest pre-conditions), a method known as program (or formal) refinement (or derivation), or sometimes "correctness-by-construction".

Proving Assertions about Parallel Programs

- Edward A. Ashcroft
- J. Comput. Syst. Sci. 10(1): 110-135 (1975)

Description: The paper that introduced invariance proofs of concurrent programs.

An Axiomatic Proof Technique for Parallel Programs I

- Susan S. Owicki, David Gries
- Acta Inf. 6: 319-340 (1976)

Description: In this paper, along with the same authors paper "Verifying Properties of Parallel Programs: An Axiomatic Approach. Commun. ACM 19(5): 279-285 (1976)", the axiomatic approach to parallel programs verification was presented.

A Discipline of Programming

- Edsger W. Dijkstra
- 1976

Description: Edsger Dijkstra's classic postgraduate-level textbook A Discipline of Programming extends his earlier paper Guarded Commands, Nondeterminacy and Formal Derivation of Programs and firmly establishes the principle of formally deriving programs (and their proofs) from their specification.

Denotational Semantics

- Joe Stoy
- 1977

Description: Joe Stoy's Denotational Semantics is the first (postgraduate level) book-length exposition of the mathematical (or functional) approach to the formal semantics of programming languages (in contrast to the operational and algebraic approaches).

The Temporal Logic of Programs

- Amir Pnueli
- In Proc. 18th IEEE Symposium on Foundation of Computer Science, pages 46—57, 1977.

Description: The use of temporal logic was suggested as a method for formal verification.

Time, clocks, and the ordering of events in a distributed system

- Leslie Lamport
- CACM, 21(7):558—565, July 1978
- online version(PDF) [72]

Description: The ordering of events is critical to consistency and correctness of many algorithms used in distributed computer systems. This paper discusses how such ordering can be managed consistently and introduces a set of rules for managing virtual time in such systems. These rules are the basis for many subsequent algorithms for ordering events in distributed system.
The paper received the PODC Influential Paper Award in 2000[73] .

Communicating Sequential Processes (1978)

- C.A.R. Hoare
- 1978

Description: Tony Hoare's (original) Communicating Sequential Processes (CSP) paper introduces the idea of concurrent processes (i.e. programs) that do not share variables but instead cooperate solely by exchanging synchronous messages.

A Calculus of Communicating Systems

- Robin Milner
- 1980

Description: Robin Milner's A Calculus of Communicating Systems (CCS) paper describes a process algebra permitting systems of concurrent processes to be reasoned about formally, something which has not been possible for earlier models of concurrency (semaphores, critical sections, original CSP).

Software Development: A Rigorous Approach

- Cliff Jones
- 1980

Description: Cliff Jones' textbook Software Development: A Rigorous Approach is the first full-length exposition of the Vienna Development Method (VDM), which had evolved (principally) at IBM's Vienna research lab over the previous decade and which combines the idea of program refinement as per Dijkstra with that of data refinement (or reification) whereby algebraically-defined abstract data types are formally transformed into progressively more "concrete" representations.

The Science of Programming

- David Gries
- 1981

Description: David Gries' textbook The Science of Programming describes Dijkstra's weakest precondition method of formal program derivation, except in a very much more accessible manner than Dijkstra's earlier *A Discipline of Programming*.

Communicating Sequential Processes (1985)

- C.A.R. Hoare
- 1985

Description: Tony Hoare's Communicating Sequential Processes (CSP) textbook (currently the third most cited computer science reference of all time) presents an updated CSP model in which cooperating processes do not even have program variables and which, like CCS, permits systems of processes to be reasoned about formally.

Linear logic (1987)

- J.-Y, Girard
- In Theoretical Computer Science, 50:1-102, 1987.
- Online version [74]

Description: Girard's linear logic was a breakthrough in designing typing systems for sequential and concurrent computation, especially for resource conscious typing systems.

A Calculus of Mobile Processes (1989)

- R. Milner, J. Parrow, D. Walker
- 1989
- Online version: Part 1 [75] and Part 2 [76]

Description: This paper introduces the Pi-Calculus, a generalisation of CCS which allows process mobility. The calculus is extremely simple and has become the dominant paradigm in the theoretical study of programming languages, typing systems and program logics.

The Z Notation: A Reference Manual

- Mike Spivey
- 1989
- Online version [77]

Description: Mike Spivey's classic textbook The Z Notation: A Reference Manual summarises the formal specification language Z which, although originated by Jean-Raymond Abrial, had evolved (principally) at Oxford University over the previous decade.

Communication and Concurrency

- Robin Milner
- Prentice-Hall International, 1989

Description: Robin Milner's textbook Communication and Concurrency is a more accessible, although still technically advanced, exposition of his earlier CCS work.

Software engineering

Software engineering: Report of a conference sponsored by the NATO Science Committee

- Peter Naur, Brian Randell (eds.)
- Garmisch, Germany, 7–11 October 1968, Brussels, Scientific Affairs Division, NATO (1969) 231pp.
- Online copy (PDF) [78]

Description: Conference of leading figures in software field circa 1968
The paper defined the field of Software engineering

Go To Statement Considered Harmful

- Dijkstra, E. W.
- *Communications of the ACM*, 11(3):147–148, March 1968
- Online copy (PDF) [79]

Description: Don't use goto – the beginning of structured programming.

On the criteria to be used in decomposing systems into modules

- David Parnas
- Communications of the ACM, Volume 15, Issue 12:1053–1058, December 1972.
- Online copy (HTML) [80]

Description: The importance of modularization and information hiding. Note that information hiding was first presented in a different paper of the same author - "Information Distributions Aspects of Design Methodology", Proceedings of IFIP Congress '71, 1971, Booklet TA-3, pp. 26–30

Hierarchical Program Structures

- Ole-Johan Dahl, C. A. R. Hoare
- in Dahl, Dijkstra and Hoare, Structured Programming, Academic Press, London and New York, pp. 175–220, 1972.

Description: The beginning of Object-oriented programming. This paper argued that programs should be decomposed to independent components with small and simple interfaces. They also argued that objects should have both data and related methods.

A technique for software module specification with examples

- David Parnas
- Comm. ACM 15, 5 [(May, 1972), 330-336.
- Online copy (PDF) [81]

Description: software specification.

Structured Design

- Wayne Stevens, Glenford Myers, and Larry Constantine
- *IBM Systems Journal, 13* (2), 115-139, 1974.
- On-line copy (PDF) [82]

Description: Seminal paper on Structured Design, data flow diagram, coupling, and cohesion.

The Emperor's Old Clothes

- C.A.R. Hoare
- Communications of the ACM, Vol. 24, No. 2, February 1981, pp. 75–83.
- Archived copy (PDF) [83]

Description: A lovely story of how large software projects can go right, and then wrong, and then right again, told with humility and humor. Illustrates the "second-system effect" and the importance of simplicity.

The Mythical Man-Month: Essays on Software Engineering

- Brooks, Jr., F. P.
- Addison Wesley Professional. 2nd edition, 1995.

Description: Throwing more people at the task will not speed its completion...

No Silver Bullet: Essence and Accidents of Software Engineering

- Brooks, Jr., F. P.
- *Computer*, 20(4):10–19, April 1987
- Online copy (HTML) [84]

Description: We will keep having problems with software...

The Cathedral and the Bazaar

- Raymond, E.S.
- *First Monday*, 3, 3 (March 1998)
- Online copy (HTML) [85]

Description: Open source methodology.

Design Patterns: Elements of Reusable Object Oriented Software

- E. Gamma, R. Helm, R. Johnson, J. Vlissides
- Addison-Wesley, Reading, Massachusetts, 1995.

Description: This book was the first to define and list design patterns in computer science.

Statecharts: A Visual Formalism For Complex Systems

- David Harel
- D. Harel. Statecharts: A visual formalism for complex systems. Science of Computer Programming, 8:231—274, 1987
- Online version [86]

Description: Statecharts are a visual modeling method. They are an extension of state machine that might be exponentially more efficient. Therefore, statcharts enable formal modeling of applications that were too complex before. Statecharts are part of the UML diagrams.

Technology of Automata-based programming

- Anatoly Shalyto
- Shalyto A. Logic Control and "Reactive" Systems: Algorithmization and Programming, Automation and Remote Control, 2001, Vol. 62, No. 1, pp. 1–29. [87]
- Shalyto A. Technology of Automata-Based Programming. CodeProject. 2004. [88]
- Gurov V., Mazin M., Narvsky A., Shalyto A. Tools for Support of Automata-Based Programming, Programming and Computer Software, 2007, Vol. 33, No. 6, pp. 343–355. [89]
- Kuzmin E.V., Sokolov V.A. Modeling, Specification and Verification of Automaton Programs, Programming and Computer Software, 2008, Vol. 34, No. 1, pp. 27-43. [90]

Description: Technology of Automata-based programming is a programming techology based on a principle of using finite state machine as a description of behavior and isomorphical transformation from state machine to code.

Parallel computing

The Structure of "THE"-Multiprogramming System

- Edsger W. Dijkstra
- Communication of the ACM, Vol. 11, No. 5 May 1968, pp. 345–346
- Online copy (HTML) [91]

Description: The introduction of basic primitives like mutex as the basis of multiprocessing programming.

How to Make a Multiprocessor Computer That Correctly Executes Multiprocess Programs

- Leslie Lamport
- IEEE Transactions on Computers, volume C-28, number 9, pp. 690–691, September 1979.

Description: Requirements that guarantee the correct execution of multi process programs were defined.

LogP: Towards a realistic model of parallel computation

- David Culler, Richard Karp, David Patterson, Abhijit Sahay, Klaus Erik Schauser, Eunice Santos, Ramesh Subramonian, Thorsten von Eicken
- In Proceedings 4th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, May 1993.
- Online version [92], doi:10.1145/173284.155333 [93]

Description: The LogP framework for parallel computing was suggested. The LogP provided a way to bridge the gap between theoretical analysis of algorithm and building real world systems.

Computer networks

A Protocol for Packet Network Interconnection

- Vint Cerf, Bob Kahn
- IEEE Transactions on Communication Technology, 1974
- Online copy (PDF) [94]

Description: Packet Network Interconnection.

Ethernet: Distributed packet switching for local computer networks

- R.M. Metcalfe, D.R. Boggs
- *Communications of the ACM* 19, 7 (July 1976), 395–404
- Online copy (HTML) [95]

Description: The Ethernet protocol.

End-To-End Arguments in System Design

- J.H. Saltzer, D.P. Reed, D.D. Clark
- Proceedings of the 2nd International Conference on Distributed Systems, 509-512, April 1981.
- Online copy (PDF) [96]

Description: Many of critical design problems in networking and systems focus on the right "layer" in which to provide particular functionality. The basic debate is whether the core system or network should provide the functionality, or whether it should be left to the end-system or application to implement using more basic primitives provided in the core network or base system. This paper highlights these issues and argues for one side. The argument has occurred over and over again in various aspects of system design and it is important to understand the basic philosophy of both sides of the debate.

Internet Protocol

- RFC 791, Information Sciences Institute, Marina Del Rey, California, September 1981
- Online copy (HTML) [97]

Description: The Internet Protocol (IP).This paper describes the he Internet Protocol (IP), a fundamental protocol that drive the Internet. Required (but quite technical) reading for anyone who wants to understand networking.

Transmission Control Protocol

- RFC 793, Information Sciences Institute, Marina del Rey, California, September 1981.
- Online copy (HTML) [98]
- [99]

Description: The Transmission Control Protocol (TCP).

Implementing Remote Procedure Calls

- Andrew D. Birrell, Bruce Jay Nelson
- ACM Transactions on Computer Systems, Vol. 2, No. 1, February 1984, pp. 39–59.
- Online copy [99]

Description: This is the seminal paper on Remote Procedure Call, which provides a higher-level mechanism for communicating between the components of a distributed system.

A Dynamic Network Architecture

- Sean W. O'Malley, Larry L. Peterson
- *ACM Transactions on Computer Systems*, 10(2), May 1992
- Online copy [100]

Description: Network software in distributed systems.

Distributed computing

The Byzantine Generals Problem

- Leslie Lamport, Robert Shostak, Marshall Pease
- Advances in Ultra-Dependable Distributed Systems, N. Suri, C. J. Walter, and M. M. Hugue (Eds.), IEEE Computer Society Press
- Online version [101]

Description: Impossibility result for distributed computing, see Byzantine failure.

Impossibility of Distributed Consensus with One Faulty process

- Michael J. Fischer, Nancy Lynch, Michael S. Paterson
- Online version [102]

Description: Impossibility to achieve consensus in asynchronous systems if one process is faulty.

Nancy A. Lynch and Mark R. Tuttle. An introduction to input/output automata. CWI-Quarterly, 2(3):219-246, September 1989. Also available as MIT Technical Memo MIT/LCS/TM-373. (ps, pdf)

An introduction to input/output automata

- Nancy Lynch, Mark R. Tuttle
- CWI-Quarterly, 2(3):219-246, September 1989. Also available as MIT Technical Memo MIT/LCS/TM-373.
- Online version [103]

Description: input/output automata

The Topological Structure of Asynchronous Computability

- Maurice Herlihy, Nir Shavit
- Journal of the ACM, Vol. 46 (1999), 858-923
- Online version (PDF) [104]

Description: The paper improved the understanding of asynchronous wait-free deterministic computation in the basic shared memory model. The authors transform a dynamic model into a static one by associating computational tasks with simplicial complexes and translating the question of existence of a wait-free protocol into (distinct but related) topological questions about the complexes. The paper won the Gödel Prize at 2004 [105] with "Wait-Free k-Set Agreement Is Impossible: The Topology of Public Knowledge".

Wait-Free k-Set Agreement Is Impossible: The Topology of Public Knowledge

- Michael Saks, Fotios Zaharoglou
- Siam J. on Computing, Vol. 29 (2000), 1449-1483.

Description: The paper improved the understanding of asynchronous wait-free deterministic computation in the basic shared memory model. These papers transforming a dynamic model into a static one by associating computational tasks with simplicial complexes and translating the question of existence of a wait-free protocol into (distinct but related) topological questions about the complexes. The paper won the Gödel Prize at 2004 [105] with "The Topological Structure of Asynchronous Computability".

Internet

As We May Think

- Vannevar Bush
- The Atlantic Monthly, July 1945
- *As we may think* from the *Atlantic Monthly* archives [106]

Description: The paper argued that as humans turned from war, scientific efforts should shift from increasing physical abilities to making all previous collected human knowledge more accessible. *As We May Think* predicted many kinds of technology invented after its publication, including hypertext, personal computers, the Internet, the World Wide Web, speech recognition, and online encyclopedias such as Wikipedia.

Grapevine: An Exercise in Distributed Computing

- Andrew D. Birrell, Roy Levin, Roger M. Needham, Michael D. Schroeder
- Communications of the ACM\fR, Vol. 25, No. 4, April 1982, pp. 260–274.
- Online version(PDF) [107]

Description: The Grapevine system. The paper describes one of the first attempts to build a large-scale distributed system (the Xerox mail system). Exposes many interesting problems related to distributed systems and describes how they were solved in this particular system.

The Design Philosophy of the DARPA Internet Protocols

- David D. Clark
- Proceedings of ACM SIGCOMM '88, August, 1988.
- Online version(PDF) [108]

Description: The DARPA Internet Protocols (TCP/IP).

The Anatomy of a Large-Scale Hypertextual Web Search Engine

- Sergey Brin and Lawrence Page
- Computer Networks and ISDN Systems, volume 30,number = 1-7,pages = 107–117, 1998.
- Online version [109]

Description: The Anatomy of a Search Engine, known today as Google.

Programming languages

The FORTRAN Automatic Coding System

- John Backus et al.
- Proceedings of the WJCC (Western Joint Computer Conference), Los Angeles, California, February, 1957.
- Online version(PDF) [110]

Description: This paper describes the design and implementation of the first FORTRAN compiler by the IBM team. Fortran is a general-purpose, procedural, imperative programming language that is especially suited to numeric computation and scientific computing.

Recursive functions of symbolic expressions and their computation by machine, part I

- John McCarthy.
- Communications of the ACM, 3(4):184-195, April 1960.
- Several online versions [111]

Description: This paper introduced LISP, the first functional programming language, which was used heavily in many areas of computer science, especially in AI. LISP also has powerful features for manipulating LISP programs within the language.

ALGOL 60

- Revised Report on the Algorithmic Language Algol 60 [112] by Peter Naur, et al. – The very influential ALGOL definition; with the first formally defined syntax.
- B. Randell and L.J. Russell, *ALGOL 60 Implementation: The Translation and Use of ALGOL 60 Programs on a Computer*. Academic Press, 1964. The design of the **Whetstone Compiler**. One of the early published descriptions of implementing a compiler. See the related papers: Whetstone Algol Revisited, [113] and The Whetstone KDF9 Algol Translator [114] by B. Randell
- Edsger W. Dijkstra, *Algol 60 translation: an Algol 60 translator for the x1 and making a translator for Algol 60*, report MR 35/61. Mathematisch Centrum, Amsterdam, 1961. [115]

Description: Algol 60 introduced block structure.

The next 700 programming languages

- Peter Landin
- Communications of the ACM 9(3):157–65, March 1966 [116]

Description: This seminal paper proposed an ideal language ISWIM, which without being ever implemented influenced the whole later development.

Simula 67

Description: Simula 67 introduced object orientation to the field of programming languages.

Computer architecture

Colossus computer

- T. H. Flowers
- *Annals of the History of Computing*, Vol. 5 (No. 3), 1983, pp. 239–252.
- The Design of Colossus [117]

Description: The *Colossus* machines were early computing devices used by British codebreakers to read encrypted German messages during World War II. Colossus was an early binary electronic digital computer. The design of Colossus was later described in the referenced paper.

First Draft of a Report on the EDVAC

- John von Neumann
- June 30,1945, the ENIAC project.
- First Draft of a report on the EDVAC [118] (PDF)

Description: It contains the first published description of the logical design of a computer using the stored-program concept, which has come to be known as the von Neumann architecture.

Architecture of the IBM System/360

- Gene Amdahl, Fred Brooks, G. A. Blaauw
- IBM Journal of Research and Development, 1964.
- *Architecture of the IBM System/360* [119]

Description: The IBM System/360 (S/360) is a mainframe computer system family announced by IBM on April 7, 1964. It was the first family of computers making a clear distinction between architecture and implementation.

The case for the reduced instruction set computer

- DA Patterson,DR Ditzel
- Computer ArchitectureNews, vol. 8, no. 6, October 1980, pp 25–33.
- Online version(PDF) [120]

Description: The *reduced instruction set computer*(*RISC*) CPU design philosophy. The RISC is a CPU design philosophy that favors a reduced instruction set as well as a simpler set of instructions.

Comments on "the Case for the Reduced Instruction Set Computer"

- DW Clark, WD Strecker
- Computer Architecture News, 1980.
- Online version(PDF) [121]

Description:

The CRAY-1 Computer System

- DW Clark, WD Strecker
- Communications of the ACM, January 1978, volume 21, number 1, pages 63–72.
- Online version(PDF) [122]

Description: The Cray-1 was a supercomputer designed by a team including Seymour Cray for Cray Research. The first Cray-1 system was installed at Los Alamos National Laboratory in 1976, and it went on to become one of the best known and most successful supercomputers in history.

Validity of the Single Processor Approach to Achieving Large Scale Computing Capabilities

- Gene Amdahl
- AFIPS 1967 Spring Joint Computer Conference, Atlantic City, N.J.
- Online version(PDF) [123]

Description: The Amdahl's Law.

A Case for Redundant Arrays of Inexpensive Disks (RAID)

- David A. Patterson, Garth Gibson, Randy H. Katz
- In International Conference on Management of Data, pages 109—116, 1988.
- Online version(PDF) [124]

Description: This paper discusses the concept of RAID disks, outlines the different levels of RAID, and the benefits of each level. It is a good paper for discussing issues of reliability and fault tolerance of computer systems, and the cost of providing such fault-tolerance.

Computer graphics

The Rendering Equation

- J. Kajiya
- SIGGRAPH: ACM Special Interest Group on Computer Graphics and Interactive Techniques pages 143—150 [125]

Elastically deformable models

- D. Terzopoulos, J. Platt, A. Barr, K. Fleischer
- Computer Graphics, 21(4), 1987, 205-214, Proc. ACM SIGGRAPH'87 Conference, Anaheim, CA, July, 1987.
- Online version(PDF) [126]

Description: The Academy of Motion Picture Arts and Sciences cited this paper as a "milestone in computer graphics".

History of computation

The Computer from Pascal to von Neumann

- Herman H. Goldstine
- Princeton University Press, 1972, ISBN 0-691-08104-2

Description: Perhaps the first book on the history of computation.

A History of Computing in the Twentieth Century

edited by:

- Nicholas Metropolis
- J. Howlett
- Gian-Carlo Rota
- Academic Press, 1980, ISBN 0-12-491650-3

Description: Several chapters by pioneers of computing.

Computer science humor

The Complexity of Songs

- Donald Knuth
- Knuth, D. *The Complexity of Songs*, *SIGACT News*, Summer 1977, 17-24.
- Knuth, D. *The Complexity of Songs*, Communications of the ACM, 1984, 27 (4) pp. 345—348.
- *The Complexity of Songs* [127], Knuth, Donald E. (1984). (pdf)

Description: The article capitalizes on the tendency of popular songs to evolve from long and content-rich ballads to highly repetitive "content-free" texts.

On Folk Theorems

- David Harel, "On Folk Theorems", Comm. Assoc. Comput. Mach. 23 (1980), 379-389
- Online version(PDF) [128]

Description: A paper that is both serious and funny about "the things we all know".

How to prove it

- Dana Angluin
- Sigact News, Winter-Spring 1983, Volume 15 #1
- Online version [129]

Description: Angluin presents some common proof techniques that should become less common.

See also

- DBLP (Digital Bibliography & Library Project in computer science)
- List of publications in science
- List of open problems in computer science
- Notable publications in software engineering
- The Collection of Computer Science Bibliographies

Awards for publications (and not for general contribution):

- Dijkstra Prize, a prize for outstanding papers on the principles of distributed computing
- Gödel Prize, a prize for outstanding papers in theoretical computer science
- Paris Kanellakis Award, a prize given to honor specific theoretical accomplishments that have had a significant and demonstrable effect on the practice of computing.

Notes

[1] http://domino.research.ibm.com/tchjr/journalindex.nsf/0/cdf6b2949432156385256bfa00683d63?OpenDocument
[2] http://www.abelard.org/turpap2/tp2-ie.asp
[3] http://web.comlab.ox.ac.uk/oucl/research/areas/ieg/e-library/sources/tp2-ie.pdf
[4] http://theory.lcs.mit.edu/~cis/pubs/shafi/1986-jacm.pdf
[5] http://weblog.fortnow.com/2006/04/kurt-gdel-1906-1978.html
[6] http://nvl.nist.gov/pub/nistpubs/sp958-lide/140-144.pdf
[7] http://cs.uwindsor.ca/~richard/PUBLICATIONS/NLI_LFP_SURVEY_DRAFT.pdf
[8] http://citeseer.ist.psu.edu/kirkpatrick83optimization.html
[9] http://world.std.com/~rjs/1964pt1.pdf
[10] http://world.std.com/~rjs/1964pt2.pdf
[11] http://www.cs.auckland.ac.nz/CDMTCS/chaitin/ibm.pdf
[12] http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html
[13] http://www.engelschall.com/~sb/hamming/?page=1
[14] http://compression.ru/download/articles/huff/huffman_1952_minimum-redundancy-codes.pdf
[15] http://citeseer.nj.nec.com/ziv77universal.html
[16] http://larch-www.lcs.mit.edu:8001/~corbato/sjcc62/
[17] http://cs.gmu.edu/cne/pjd/PUBS/WSModel_1968.pdf
[18] http://cs.gmu.edu/cne/pjd/pjdsigopshof05.html
[19] http://www.cs.virginia.edu/~zaher/classes/CS656/p306-daley.pdf
[20] http://www.cs.cornell.edu/andru/cs711/2003fa/reading/lampson73note.pdf
[21] http://citeseer.ist.psu.edu/ritchie74unix.html
[22] http://citeseer.ist.psu.edu/gifford79weighted.html
[23] http://www.cs.berkeley.edu/~brewer/cs262/Mesa.pdf
[24] http://www.cs.berkeley.edu/~brewer/cs262/FFS.pdf
[25] http://www.cs.berkeley.edu/~brewer/cs262/LFS.pdf
[26] http://citeseer.ist.psu.edu/seltzer93implementation.html
[27] http://www.hpl.hp.com/personal/Craig_Soules/papers/TOCS.softupdates.pdf
[28] http://www.informatik.uni-bonn.de/III/lehre/vorlesungen/Informationssysteme/WS06/materialien/Codd72a.pdf
[29] http://portal.acm.org/citation.cfm?id=320440
[30] http://citeseer.nj.nec.com/agrawal93mining.html
[31] http://www.turingarchive.org/browse.php/C/30
[32] http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf
[33] http://www-ee.stanford.edu/%7Ehellman/publications/24.pdf
[34] http://www-ee.stanford.edu/~hellman/publications/32.pdf
[35] http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci1077600,00.html
[36] http://citeseer.nj.nec.com/rivest78method.html
[37] http://inst.eecs.berkeley.edu/~cs268/sp02/cached_papers/needham.pdf
[38] http://szabo.best.vwh.net/secret.html
[39] http://www.cs.ucsb.edu/~kemm/courses/cs177/noninter.pdf
[40] http://theory.lcs.mit.edu/~cis/pubs/shafi/1984-jcss.pdf
[41] http://www.wisdom.weizmann.ac.il/~oded/gmw1.html
[42] http://www.wisdom.weizmann.ac.il/~oded/gmw2.html
[43] http://citeseer.ist.psu.edu/gasser89digital.html
[44] http://gost.isi.edu/publications/kerberos-neuman-tso.html
[45] http://citeseer.ist.psu.edu/biham91differential.html
[46] http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E92/81.PDF
[47] http://citeseer.ist.psu.edu/lowe96breaking.htmll
[48] http://www.abelard.org/turpap/turpap.htm
[49] http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html
[50] http://www-bisc.cs.berkeley.edu/Zadeh-1965.pdf
[51] http://aima.cs.berkeley.edu/
[52] http://world.std.com/~rjs/indinf56.pdf
[53] http://www.isrl.uiuc.edu/~amag/langev/paper/gold67limit.html
[54] http://www.cs.toronto.edu/~roweis/csc2515-2006/readings/quinlan.pdf
[55] http://www.springerlink.com/content/x1022977778l1777/fulltext.pdf

[56] http://citeseer.ist.psu.edu/sutton88learning.html
[57] http://citeseer.ist.psu.edu/kearns89cryptographic.html
[58] http://citeseer.nj.nec.com/schapire90strength.html
[59] http://citeseer.nj.nec.com/kearns93learning.html
[60] http://citeseer.ist.psu.edu/boser92training.html
[61] http://citeseer.ist.psu.edu/lucas81iterative.html
[62] http://citeseer.ist.psu.edu/burt83laplacian.html
[63] http://www.mrl.nyu.edu/~dt/papers/ijcv88/ijcv88.pdf
[64] http://citeseer.ist.psu.edu/isard98condensation.html
[65] http://citeseer.ist.psu.edu/lowe99object.html
[66] http://citeseer.nj.nec.com/johnson79yacc.html
[67] http://citeseer.ist.psu.edu/graham82gprof.html
[68] http://www.eecs.berkeley.edu/~necula/Papers/FloydMeaning.pdf
[69] http://www.spatial.maine.edu/~worboys/processes/hoare%20axiomatic.pdf
[70] http://portal.acm.org/citation.cfm?doid=360933.360975
[71] http://www.cs.utexas.edu/users/EWD/transcriptions/EWD04xx/EWD418.html
[72] http://research.microsoft.com/users/lamport/pubs/time-clocks.pdf
[73] Neiger, Gil (2003-01-23). http://www.podc.org/influential/2000.html|"PODC Influential Paper Award: 2000". http://www.podc.org/influential/2000.html. Retrieved on 2007-02-02.
[74] http://iml.univ-mrs.fr/~girard/linear.pdf
[75] https://www.lfcs.inf.ed.ac.uk/reports/89/ECS-LFCS-89-85/index.html
[76] https://www.lfcs.inf.ed.ac.uk/reports/89/ECS-LFCS-89-86/index.html
[77] http://spivey.oriel.ox.ac.uk/mike/zrm
[78] http://homepages.cs.ncl.ac.uk/brian.randell/NATO/nato1968.PDF
[79] http://www.kbs.uni-hannover.de/Lehre/SWTG/goto.pdf
[80] http://www.acm.org/classics/may96/
[81] http://people.cs.uchicago.edu/~robby/contract-reading-list/parnas.05.72.pdf
[82] http://www.research.ibm.com/journal/sj/382/stevens.pdf
[83] http://web.archive.org/web/20070211210228/http://www.braithwaite-lee.com/opinions/p75-hoare.pdf
[84] http://www.virtualschool.edu/mon/SoftwareEngineering/BrooksNoSilverBullet.html
[85] http://www.redhat.com/support/wpapers/community/cathedral/whitepaper_cathedral.html
[86] http://www.wisdom.weizmann.ac.il/~dharel/SCANNED.PAPERS/Statecharts.pdf
[87] http://is.ifmo.ru/articles_en/_logic_control_and_reactive_systems.pdf
[88] http://www.codeproject.com/KB/architecture/abp.aspx?print=true
[89] http://is.ifmo.ru/articles_en/_ProCom6_07GurovLO.pdf
[90] http://is.ifmo.ru/download/2008-03-12_verification-en.pdf
[91] http://www.acm.org/classics/mar96/
[92] http://citeseer.ist.psu.edu/culler93logp.html
[93] http://dx.doi.org/10.1145%2F173284.155333
[94] http://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf
[95] http://www.acm.org/classics/apr96/
[96] http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf
[97] http://tools.ietf.org/html/rfc791
[98] http://tools.ietf.org/html/rfc793
[99] http://citeseer.ist.psu.edu/birrell84implementing.html
[100] http://citeseer.ist.psu.edu/malley92dynamic.html
[101] http://citeseer.ist.psu.edu/lamport82byzantine.html
[102] http://theory.lcs.mit.edu/tds/papers/Lynch/jacm85.pdf
[103] http://www.markrtuttle.com/papers/lt89-cwi.pdf
[104] http://www.cs.brown.edu/~mph/HerlihyS99/p858-herlihy.pdf
[105] http://sigact.acm.org/prizes/godel/2004.html
[106] http://www.theatlantic.com/doc/194507/bush
[107] http://www.cs.ucsb.edu/~ravenben/papers/coreos/BLS+82.pdf
[108] http://www.cs.princeton.edu/~jrex/teaching/spring2005/reading/clark88.pdf
[109] http://infolab.stanford.edu/~backrub/google.html
[110] http://web.mit.edu/6.035/www/papers/BackusEtAl-FortranAutomaticCodingSystem-1957.pdf
[111] http://www-formal.stanford.edu/jmc/recursive.html
[112] http://www.masswerk.at/algol60/report.htm
[113] http://www.cs.ncl.ac.uk/research/pubs/articles/papers/427.pdf

[114] http://www.cs.ncl.ac.uk/publications/books/papers/124.pdf

[115] http://www.cs.utexas.edu/users/EWD/MCReps/MR35.PDF

[116] http://scholar.google.com/scholar?hl=uk&lr=&cluster=2856797924573721037&um=1&ie=UTF-8&sa=X&oi=science_links&resnum=1&ct=sl-allversions

[117] http://www.ivorcatt.com/47c.htm

[118] http://www.virtualtravelog.net/entries/2003-08-TheFirstDraft.pdf

[119] http://www.research.ibm.com/journal/rd/441/amdahl.pdf

[120] http://inst.eecs.berkeley.edu/%7En252/sp07/Papers/RISC-patterson.pdf

[121] http://inst.eecs.berkeley.edu/%7En252/sp07/Papers/RISC-clark.pdf

[122] http://inst.eecs.berkeley.edu/%7En252/sp07/Papers/Cray.pdf

[123] http://inst.eecs.berkeley.edu/%7En252/sp07/Papers/Amdahl.pdf

[124] http://inst.eecs.berkeley.edu/%7En252/sp07/Papers/RAID-patterson.pdf

[125] http://doi.acm.org/10.1145/15922.15902

[126] http://www.cs.ucla.edu/~dt/papers/siggraph87/siggraph87.pdf

[127] http://www.cs.utexas.edu/users/arvindn/misc/knuth_song_complexity.pdf

[128] http://www.wisdom.weizmann.ac.il/~harel/SCANNED.PAPERS/OnFolkTheorems.pdf

[129] http://web.archive.org/web/20070209050002/http://www.stanford.edu/~plegresl/proveit.html

Further reading

- Laplante, Phillip (ed). (1996) *Great Papers in Computer Science.* New York: IEEE Press. ISBN 031406365X.
- Randell, Brian (ed). (1982). *The Origins of Digital Computers: Selected Papers.* 3rd ed. Berlin: Springer-Verlag. ISBN 0387113193.
- Turning Points in Computing: 1962-1999, Special Issue, *IBM Systems Journal, 38* (2/3),1999.
- Yourdon, Edward (ed.) (1979) *Classics in Software Engineering.* New York: Yourdon Press. ISBN 0917072146

External links

- Lots of video lectures on Computer Science (http://freevideolectures.com/computerscience.html)
- Most cited articles in Computer Science (http://citeseer.ist.psu.edu/articles.html) (Cite.Seer Database)
- 50 most influential papers ACM SIGPLAN papers published in PLDI from 1979 through 1999 (http://www.cs.rutgers.edu/tmp/webarchives/ZmdgIBGXEwUXUpAXaXxQ/); organized into a special SIGPLAN proceedings.

Academic Search Engines

- Google Scholar (http://scholar.google.com/)
- CiteSeer (http://citeseer.ist.psu.edu/)
- Live Academic (http://academic.live.com/)

Article Sources and Contributors

List of important publications in computer science *Source*: http://en.wikipedia.org/windex.php?oldid=296360210 *Contributors*: APH, Abdull, Adrianwn, Alex.g, Altenmann, Amwebb, Ancheta Wis, AngelHaf, Angela, Anthius, Arcenciel, Art LaPella, Artem M. Pelenitsyn, Arvindn, Bachrach44, Bduke, Bkkbrad, BobKeim, Bobblewik, Bovineone, Brianga, Bubba73, Bunnyhop11, Calbaer, Caltas, CanisRufus, Chanheigeorge, Charles Matthews, CharlesGillingham, Chip Zero, Chris 73, Chris the speller, Compupdate, CryptoDerk, David.Monniaux, Dcljr, Dcoetzee, Demyn, Docu, Dpbsmith, Dysprosia, Edemaine, Facopad, Fawcett5, Four Dog Night, GabrielF, Gaius Cornelius, Galoubet, Giftlite, Gpvos, Greenrd, Gregbard, Guruduttmallapur, Ham Pastrami, Harshavsn, Hermel, Hike395, Hilverd, Humbugde, Ian Cheese, Intgr, JIP, Jamessungjin.kim, Janm67, Jesse Viviano, Jkliff, JonHarder, Jpbowen, JuanXonValdez, Just Another Dan, Jwfour, Kafziel, Kku, Kope, Kusunose, Libcub, LoneBorgersen, Lquilter, Lukas Mach, Lwoodyiii, Mahmoud zouari, MarkSweep, Martclau, Mateo SA, Matt Crypto, Merzul, Metageek, Mhkay, Minesweeper, Miym, Mkehrt, Mmernex, Mneser, Moxon, MrPrada, Neilc, Nethgirb, Nickg, Night Gyr, Nmnhuq, OCNative, Oneiros, Orderud, Ortylp, Oskar Sigvardsson, Palaeovia, Paul A, Phatom87, Phil Boswell, Phoebe, Plasticup, Plotnick, Quuxplusone, Rdsmith4, ResidueOfDesign, Retired username, ReyBrujo, Rich Farmbrough, Rjwilmsi, Rstevens27, Rtc, Ruud Koot, Rwwww, S.K., Sam Hocevar, Sanders muc, Schissel, Scog, Seabhcan, Senator Palpatine, Shalyto, Skittleys, Smimram, Softnhard.es, Spoon!, SpuriousQ, Stirrer, Superdosh, Tagishsimon, TestPilot, The Transhumanist, Thv, Tim32, Tizio, Tobias Bergemann, Tom-, TreasuryTag, Uzume, Vivohobson, Wellithy, Whiner01, Wiki alf, Wimvandorst, Xezbeth, 193 anonymous edits

License