

Wim van Dam

CURRICULUM VITAE

Department of Computer Science
Harold Frank Hall, room 2151
University of California, Santa Barbara
Santa Barbara, CA 93106-5110
United States of America

Work: +1-805-893 5211

Fax: +1-805-893 8553

vandam@cs.ucsb.edu

<http://www.cs.ucsb.edu/~vandam/>

APPOINTMENTS

July 2005–present Assistant Professor, Department of Physics, UC Santa Barbara
July 2004–present Assistant Professor, Department of Computer Science, UC Santa Barbara
Fall 2001 Lecturer, Computer Science Division, UC Berkeley

EDUCATION

Ph.D. Computer Science, University of Amsterdam, 2002
Thesis title: “On Quantum Computation Theory”, supervisor: Prof. P. Vitányi
Ph.D. Physics, University of Oxford, 2000
Thesis title: “Nonlocality & Communication Complexity”, supervisor: Prof. A. Ekert
M.Sc. Mathematics & Computer Science, University of Nijmegen, The Netherlands, 1996
Thesis title: “Quantum Cellular Automata”, supervisors: Prof. K. Koster and Prof. P. Vitányi

RESEARCH INTERESTS

I am interested in the interplay between theoretical computer science and physics. My current research focuses on the theory of quantum computation and quantum information, with an emphasis on the design of new quantum algorithms and on the computational consequences of nonlocality and other quantum mechanical phenomena.

PROFESSIONAL AND EDUCATIONAL BACKGROUND

2003–2004 Postdoctoral researcher at the quantum computation group of Ed Farhi at MIT’s Center for Theoretical Physics.
2001–2003 HP/MSRI-postdoctoral fellow at the Mathematical Sciences Research Institute in Berkeley and at the Information Theory Research group of Hewlett-Packard, Palo Alto, headed by Gadiel Seroussi. Also lecturer at the Computer Science Division of UC Berkeley and member of the quantum computation group of Umesh Vazirani.
2000–2001 Postdoctoral researcher at the quantum computation group of Umesh Vazirani, Computer Science Division, UC Berkeley.
1996–2000 Graduate research in quantum computation and communication at the National Research Institute for Mathematics and Computer Science in Amsterdam (under Paul Vitányi), and at the Centre for Quantum Computation, University of Oxford (under Artur Ekert).
1989–1996 Undergraduate and Master’s studies in computer science and mathematics at the University of Nijmegen in The Netherlands. Specialization in complexity theory, information theory, logic, and discrete mathematics. Also a preliminary year in physics.

PUBLICATIONS**Journal and Conference Articles***

- [1] “Quantum Algorithms for Algebraic Problems”, Andrew M. Childs and Wim van Dam, to appear in *Reviews of Modern Physics*.
- [2] “Classical and Quantum Algorithms for Exponential Congruences”, Wim van Dam and Igor E. Shparlinski, Proceedings of the 3rd Workshop on Quantum Computation, Communication, and Cryptography (TQC 2008), to appear in *Lecture Notes in Computer Science*; arXiv:quant-ph/0804.1109
- [3] “Optimal phase estimation in quantum networks”, Wim van Dam, G. Mauro D’Ariano, Artur Ekert, Chiara Macchiavello, and Michele Mosca, *Journal of Physics A: Mathematical and Theoretical*, Volume 40, pages 7971–7984 (2007); arXiv:quant-ph/0706.4412 (2007)
- [4] “Optimal quantum circuits for general phase estimation”, Wim van Dam, G. Mauro D’Ariano, Artur Ekert, Chiara Macchiavello, and Michele Mosca, *Physical Review Letters*, Volume 98, Number 9, Article 090501 (2007); arXiv:quant-ph/0609160 (2006)
- [5] “Quantum algorithm for a generalized hidden shift problem”, Andrew M. Childs and Wim van Dam, *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms*, pages 1225–1234 (2007); arXiv:quant-ph/0507190
- [6] “From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups”, Dave Bacon, Andrew M. Childs, and Wim van Dam, *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 469–478 (2005); arXiv:quant-ph/0504083
- [7] “Optimal measurements for the dihedral hidden subgroup problem”, Dave Bacon, Andrew M. Childs, and Wim van Dam, *Chicago Journal of Theoretical Computer Science*, Article 2 (2006); arXiv:quant-ph/0501044
- [8] “The Statistical Strength of Nonlocality Proofs”, Wim van Dam, Richard Gill, and Peter Grünwald, *IEEE Transactions on Information Theory*, Volume 51, Issue 8, pages 2812–2835 (2005); arXiv:quant-ph/0307125
- [9] “Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation”, Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev, *SIAM Journal on Computing*, Volume 37, Issue 1, pages 166–194 (2007); preliminary version in *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 42–51 (2004); updated version to appear in *SIAM Review*; arXiv:quant-ph/0405098
- [10] “Comment on ‘Quantum identification schemes with entanglements’ ”, Wim van Dam, *Physical Review A*, Volume 68, Number 2, Article 026301 (2003); arXiv:quant-ph/0307126
- [11] “Experimental implementation of an adiabatic quantum optimization algorithm”, Matthias Steffen, Wim van Dam, Tad Hogg, Greg Breyta, and Isaac Chuang, *Physical Review Letters*, Volume 90, Number 6, Article 067903 (2003); arXiv:quant-ph/0302057
- [12] “Quantum Algorithms for some Hidden Shift Problems”, Wim van Dam, Sean Hallgren, and Lawrence Ip, *SIAM Journal on Computing*, Volume 36, Issue 3, pages 763–778 (2006); preliminary version in *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms*, pages 489–498 (2003); arXiv:quant-ph/0211140

*The quant-ph no. refers to the e-print archive on quantum physics at <http://arxiv.org/>

- [13] “Universal entanglement transformations without communication”, Wim van Dam and Patrick Hayden, *Physical Review A*, Rapid Communications, Volume 67, Number 6, Article 060302(R) (2003); arXiv:quant-ph/0201041 (under the title “Embezzling Entangled Quantum States”)
- [14] “How Powerful is Adiabatic Quantum Computation?”, Wim van Dam, Mike Mosca, and Umesh Vazirani, *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, pages 279–287 (2001); arXiv:quant-ph/0206003
- [15] “Quantum Algorithms for Weighing Matrices and Quadratic Residues”, Wim van Dam, *Algorithmica*, Volume 34, No. 4, pages 413–428 (2002); arXiv:quant-ph/0008059
- [16] “Quantum Kolmogorov Complexity”, André Berthiaume, Wim van Dam, and Sophie Laplante, *Journal of Computer and System Sciences*, Volume 63, No. 2, pages 201–221, September 2001; preliminary version in *Proceedings of the 15th Annual IEEE Conference on Computational Complexity*, pages 240–249 (2000); arXiv:quant-ph/0005018
- [17] “Self-Testing of Universal and Fault-Tolerant Sets of Quantum Gates”, Wim van Dam, Frédéric Magniez, Michele Mosca, and Miklos Santha, *SIAM Journal on Computing*, Volume 37, Issue 2, pages 611–629 (2007); preliminary version in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 688–696 (2000); arXiv:quant-ph/9904108
- [18] “Quantum Bounded Query Complexity”, Harry Buhrman and Wim van Dam, *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pages 149–156 (1999); arXiv:quant-ph/9903035
- [19] “Quantum Communication Using a Nonlocal Zeno Effect”, Lucien Hardy and Wim van Dam, *Physical Review A*, Volume 59(4), pages 2635–2640 (1999); arXiv:quant-ph/9805037 (under the title “Quantum Whispers”)
- [20] “Quantum Oracle Interrogation: Getting all information for almost half the price”, Wim van Dam, *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science*, pages 362–367 (1998); arXiv:quant-ph/9805006
- [21] “Multiparty Quantum Communication Complexity”, Harry Buhrman, Wim van Dam, Peter Høyer, and Alain Tapp, *Physical Review A*, Volume 60(4), pages 2737–2741 (1999); arXiv:quant-ph/9710054
- [22] “Quantum Entanglement and the Communication Complexity of the Inner Product Function”, Richard Cleve, Wim van Dam, Michael Nielsen, and Alain Tapp, *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications*, (editor: C.P. Williams), Lecture Notes in Computer Science, Volume 1509, pages 61–74, Springer-Verlag (1999); arXiv:quant-ph/9708019
- [23] “Quantum Entanglement and Communication Complexity”, Harry Buhrman, Richard Cleve, and Wim van Dam, *SIAM Journal on Computing*, Volume 30, Number 6, pages 1829–1841 (2001); arXiv:quant-ph/9705033
- [24] “A Universal Quantum Cellular Automaton”, Wim van Dam, *Proceedings of PhysComp96*, New England Complex Systems Institute, (editors: T. Toffoli, M. Biafore, and J. Leão), pages 323–331; InterJournal manuscript no. 91 (1996)

Popular Articles and Book Reviews

- [25] Book review of David Mermin’s “Quantum Computer Science”, Wim van Dam, to appear in *American Scientist*

- [26] “Quantum computing: In the ‘death zone’?”, Wim van Dam, *Nature Physics*, Volume 3, Number 4, pages 220–221 (2007)
- [27] “Think Nonlocally” (book review of Amir D. Aczel’s “Entanglement: the greatest mystery in physics”), Wim van Dam, *American Scientist*, Volume 91, No. 3, pages 270–271 (2003)
- [28] “Physicists triumph at ‘Guess My Number’”, Andrew Steane and Wim van Dam, *Physics Today*, Volume 53(2), pages 35–39 (2000)

Theses

- [29] “On Quantum Computation Theory”, Wim van Dam, Ph.D. thesis, Department of Computer Science, University of Amsterdam, The Netherlands (2002)
- [30] “Nonlocality & Communication Complexity”, Wim van Dam, Ph.D. thesis, Department of Physics, University of Oxford, United Kingdom (1999)
- [31] “Quantum Cellular Automata”, Wim van Dam, Master thesis, Department of Mathematics and Computer Science, University of Nijmegen, The Netherlands (1996)

Articles in Submission or Unpublished

- [32] “Implausible Consequences of Superstrong Nonlocality”, submitted, Wim van Dam, arXiv:quant-ph/0501159
- [33] “Quantum Computing and Zeroes of Zeta Functions”, submitted, Wim van Dam, arXiv:quant-ph/040581
- [34] “Summary of Delsarte’s ‘Nombre de Solutions des Équations Polynomiales sur un Corps Fini’”, Wim van Dam, arXiv:math.HO/0401066
- [35] “Quantum Computing Discrete Logarithms with the Help of a Preprocessed State”, Wim van Dam, arXiv:quant-ph/0311134 (2003)
- [36] “Efficient Quantum Algorithms for Estimating Gauss Sums”, Wim van Dam and Gadiel Seroussi, submitted, arXiv:quant-ph/0207131 (2002)
- [37] “Rényi-entropic bounds on quantum communication”, Wim van Dam and Patrick Hayden, arXiv:quant-ph/0204093 (2002)
- [38] “Efficient quantum algorithms for Shifted Quadratic Character Problems”, Wim van Dam and Sean Hallgren, arXiv:quant-ph/0011067 (2000)
- [39] “Two Classical Queries versus One Quantum Query”, Wim van Dam, arXiv:quant-ph/9806090 (1998)

TEACHING EXPERIENCE

(Courses taught at UCSB unless stated otherwise)

- “Classical Mechanics”, undergraduate course (Winter 2007)
- “Information Theory”, graduate course (Spring 2006, Spring 2008)
- “Automata and Formal Languages”, undergraduate course (Winter 2006, Winter 2007, Fall 2007)
- “Things Computers Can’t Do”, Freshman Seminar (Winter 2006)
- “Quantum Information and Quantum Computation”, graduate course (Spring 2005, Spring 2007)
- “Foundations of Computer Science”, undergraduate course (Fall 2004, Fall 2005)
- “Computability and Complexity”, undergraduate course (Fall 2001, Spring 2001, UC Berkeley)

GRANTS

- “CAREER: Algebraic and Semiclassical Methods for Quantum Computing”, National Science Foundation, \$400,000 (2008–2013)
- “Quantum algorithms for data streams”, National Science Foundation, \$70,000 (2007–2008)
- “Quantum Algorithms for Algebraic Problems”, Army Research Office, \$600,000 (2005–2008); Co-PI with Cris Moore (PI, University of New Mexico) and Alexander Russell (co-PI, University of Connecticut)
- “Expected Topological Properties of Random Sets of Equations”, UCSB Academic Senate, \$5,400 (2006–2008)

ACADEMIC AND PROFESSIONAL SERVICE

- Coordinator (with David DiVincenzo and Debbie Leung) of the KITP program “Quantum Information Science”, Kavli Institute of Theoretical Physics, Santa Barbara, Fall 2009
- Program committee member of The Twelfth Workshop on Quantum Information Processing (QIP2009), January 12–16, 2009, Santa Fe (New Mexico)
- Editorial board member of *Virtual Journal of Quantum Information* of the American Institute of Physics and the American Physical Society, which is available at <http://www.vjquantuminfo.org/>.
- Member of the Association for Computing Machinery (ACM), ACM’s Special Interest Group on Algorithms and Computation Theory (SIGACT), the American Physical Society (APS), and the American Mathematical Society (AMS).

NON-SCIENTIFIC ACADEMIC SERVICE OUTSIDE DEPARTMENT

- Member of UCSB’s campus-wide Student-Faculty Committee on Student Conduct (2007–present)
- Member of University Committee on Scholarly Communications (2005–2008)
- Member of the College of Engineering Executive Committee (2005–2006)

AWARDS, HONORS AND FELLOWSHIPS

- Postdoctoral fellowship, Cambridge-MIT Institute, 2003/2004
- Postdoctoral fellowship, Hewlett-Packard/Mathematical Sciences Research Institute, 2002/2003
- Postdoctoral fellowship, Hewlett-Packard/Mathematical Sciences Research Institute, 2001/2002
- TALENT fellowship from The Netherlands Organization for Scientific Research for postdoctoral research at UC Berkeley in 2000/2001
- Graduate award of Wolfson College, University of Oxford, November 1998
- Graduate fellowship from the Institute for Logic, Language and Computation at the University of Amsterdam, 1996–2000
- Highest possible grade (10 out of 10) for M.Sc. thesis
- Cum laude first-year examination Computer Science
- Qualification for the finals of the Dutch Math Olympics, 1988 and 1989
- Eleventh place at the Dutch Physics Olympics, 1989

SERVED AS REFEREE

Journals: Algorithmica, Communications of the ACM, Electronic Transactions on Numerical Analysis, Information Processing Letters, International Journal of Foundations of Computer Science, Journal of Modern Optics, Journal of Optics B, Journal of Physics A: Mathematical and General, Journal of the ACM, Nature Physics, New Journal of Physics, Physics Letters A, Physical Review A, Physical Review Letters, Proceedings of the Royal Society of London, Quantum Information

& Computation, Quantum Information Processing, SIAM Journal on Computing, The Computer Journal, Theoretical Computer Science, Theory of Computing, and Theory of Computing Systems.

Conferences: IEEE Symposium on Foundations of Computer Science, ACM Symposium on Theory of Computing, ACM-SIAM Symposium on Discrete Algorithms International Colloquium on Automata, Languages and Programming, Conference on Foundations of Software Technology and Theoretical Computer Science, Theory of Cryptography Conference, and IEEE Conference on Computational Complexity.

Books: Kluwer Academic Publishers and Cambridge University Press.

In reaction to their pricing policies, I no longer referee for the journals: *Physics Letters A*, *Theoretical Computer Science*, *Information and Computation* (all published by Elsevier), and World Scientific's *International Journal of Foundations of Computer Science*.

PRESENTED LECTURES (SINCE FALL 2004)

1. Quantum Reading Seminar, Hebrew University, Israel, May 29, 2008: "Quantum Computing and Zeroes of Zeta Functions"
2. Theory of Computing Seminar, Tel-Aviv University, Israel, May 20, 2008: "Classical and Quantum Algorithms for Exponential Congruences"
3. Institute for Quantum Information Seminar, California Institute of Technology, April 15, 2008: "Algebraic Quantum Circuits"
4. Meeting at D-Wave Systems, Vancouver, Canada, March 17, 2008: "Universal Quantum Adiabatic Computing"
5. Physics Graduate Seminar, UC Santa Barbara, February 22, 2008: "Applied Metaphysics: Nonlocality as a Resource"
6. Panel on Progress in Quantum Computing, Super Computing 07, Reno, NV, November 15, 2007: "Quantum Computing Science anno 2007"
7. Dagstuhl Seminar on Algebraic Methods in Computational Complexity, Dagstuhl, Germany, October 12, 2007: "Algebraic Quantum Circuits"
8. QAP Workshop on Non-locality and Quantum Physics, Bristol, UK, April 20, 2007: "Multiparty quantum communication and quantum algorithms on data streams"
9. 49th British Applied Mathematics Colloquium, Bristol, UK, April 19, 2007: "Complexity of Algebraic Quantum Circuits"
10. Faculty Research Seminar, Department of Computer Science, UC Santa Barbara, March 16, 2007: "Physics versus Computer Science"
11. Quantum Information Seminar, UC Santa Barbara, February 8, 2007: "Recent results in the search for new quantum algorithms"
12. Colloquium, Perimeter Institute for Theoretical Physics, Waterloo, Canada, December 13, 2006: "Quantum computing & Zeta Functions"
13. CSE Theory Seminar, University of Michigan, October 27, 2006: "Progress on quantum algorithms"

14. ARO/DTO/NSA Quantum Algorithm Review, San Diego, CA, July 26, 2006: “Quantum Algorithms for Algebraic Problems”
15. Physics Graduate Seminar, UC Santa Barbara, May 12, 2006: “Applied Metaphysics: Nonlocality as a Resource”
16. Quantum Information Seminar, University of Bristol, UK, March 29, 2006: “Quantum computing, zeroes of zeta functions, and approximate counting”
17. Quantum Computation Seminar, University of Cambridge, UK, March 31, 2006: “Quantum computing, zeroes of zeta functions, and approximate counting”
18. 9th Workshop on Quantum Information Processing, Paris, France, January 16, 2006: “From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups”
19. Condensed Matter/Quantum Information Seminar, UC Santa Barbara, January 6, 2006: “Quantum computing, zeroes of zeta functions and approximate counting”
20. Discrete Mathematics Seminar, UC Davis, December 9, 2005: “Quantum computing, zeroes of zeta functions and approximate counting”
21. Institute for Quantum Information Seminar, California Institute of Technology, November 8, 2005: “Quantum computing, zeroes of zeta functions & approximate counting”
22. 46th Annual IEEE Symposium on Foundations of Computer Science, Pittsburgh, PA, October 25, 2005: “From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups”
23. ERATO Conference on Quantum Information Science, Tokyo, Japan, August 26, 2005: “New Quantum Algorithms for the Hidden Subgroup Problem”
24. Quantum Information Lunch, UC Santa Barbara, May 16, 2005: “What to do with a few reliable qubits, or a lot of not-so reliable ones”
25. Bellairs Research Institute, Barbados, March 23, 2005: “Zeta Functions, Random Matrices and Quantum Computing”
26. ARO/ARDA/IPS/NASA/JPL/UCSD Workshop on Quantum Algorithms for Signal, Image and Data Processing, San Diego, California, December 7, 2004: “The Power of Quantum Computing”
27. Distinguished Lecture Series on Complexity, Entropy, and the Physics of Information, Santa Fe Institute, Santa Fe, New Mexico, November 10, 2004: “Quantum Computing, Zeroes of Zeta Functions & Approximate Counting”