CWI

UITNODIGING

SOIREE

9 FEBRUARI 2006

TER GELEGENHEID VAN HET 60-JARIG BESTAAN VAN HET
CENTRUM VOOR WISKUNDE EN INFORMATICA

UITREIKING
VAN WIJNGAARDEN AWARD 2006

1946 60 2006

Prof.dr.ir. A. (Adriaan) van Wijngaarden (1916-1987) wordt beschouwd als de grondlegger van de informatica in Nederland. Van 1961 tot 1980 was hij directeur van het toenmalige Mathematisch Centrum.

Prof.dr. N.A. Lynch is NEC Professor of Software Science and Engineering, Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

Prof.dr. P. Diaconis is Mary V. Sunseri Professor of Statistics and Mathematics, Stanford University.

Prof.dr. J.K. Lenstra is algemeen directeur van het Centrum voor Wiskunde en Informatica.

Prof.dr. F.W. Vaandrager is hoogleraar Informatica voor technische toepassingen aan de Radboud Universiteit Nijmegen.

Prof.dr. R.W. van der Hofstad is hoogleraar Kansrekening aan de Technische Universiteit Eindhoven.

Prof.dr. P.W. Adriaans is voorzitter van het Bestuur van het Centrum voor Wiskunde en Informatica.

Het Mondriaan Kwartet vierde in 2003 het 20-jarig bestaan en werkt aan het project 'Algoritmic Composer'.

Het Bestuur en de Directie van het Centrum voor Wiskunde en Informatica nodigen u van harte uit deel te nemen aan de viering van het 60-jarig bestaan van het instituut op donderdag 9 februari 2006.

Ter markering van dit jubileum wordt de Van Wijngaarden Award uitgereikt aan twee onderzoekers die een bijzondere betekenis hebben voor de wiskunde en informatica:

Nancy Lynch en Persi Diaconis

Locatie: Oude Lutherse Kerk, Singel 411 te Amsterdam
Ontvangst vanaf 18.45 uur; muzikaal intro door het Mondriaan Kwartet

19.30	Opening	Jan Karel Lenstra
19.40	Laudatio	Frits Vaandrager
19.45	Impossibility of consensus in distributed systems... and other tales	Nancy Lynch
20.25	Strijkkwartet no. 1 in C groot van Lambert Meertens	Mondriaan Kwartet
20.40	Laudatio	Remco van der Hofstad
20.45	The search for randomness	Persi Diaconis
21.25	Uitreiking Van Wijngaarden Awards	Pieter Adriaans
21.35	Receptie	

Graag ontvangen wij uw antwoordkaart vóór 30 januari 2006.
Aanmelding is ook mogelijk via www.cwi.nl/60jaarcwi

Centrum voor Wiskunde en Informatica
Kruislaan 413
1098 SJ Amsterdam
telefoon (020) 592 9333
www.cwi.nl

CWI Centrum voor Wiskunde en Informatica

Presentation Van Wijngaarden Award 2006

1946 60 2006

Soiree - Oude Lutherse Kerk - Amsterdam - 9 februari 2006

Centrum voor Wiskunde en Informatica 1946 – 2006

The 60th anniversary of the institute inspired the General Director and the Board of the Centrum voor Wiskunde en Informatica to introduce the Van Wijngaarden Award. This award is meant to honor researchers, who have made important contributions to mathematics and computer science. It consists of a bronze sculpture and will be presented every five years.

The Centrum voor Wiskunde en Informatica (CWI) is the Dutch national research institute for mathematics and computer science. It was founded on 11 February 1946 in Amsterdam with the mission to perform cutting-edge scientific research and to transfer the acquired knowledge to society. In 1983 the original name Mathematisch Centrum was changed into Centrum voor Wiskunde en Informatica.

During the 60 years of its existence CWI has lived up to its mission. Many striking research results have been realized. In the fifties the Mathematisch Centrum was involved in, among other things, research for the Deltaplan, and the first Dutch computers – the ARRA and the ARRA II - were developed at the institute. The computer language Python originated at the Mathematisch Centrum and in the development of other languages (Algol 60 and Algol 68) the institute was involved. CWI was also the home base for the internet domain .NL since its start in 1988. A vast quantity of scientific articles and books were published by CWI's scientists. Many international researchers visited or studied at CWI, and many CWI researchers found their way all over the world.

In the years to come CWI will focus on four major research themes: Earth and Life Sciences, Data Explosion, Societal Logistics, and Service-oriented Computing. These themes, directly linked to society, will fuel the enthusiasm of the CWI researchers to continue their never ending quest for fundamental scientific knowledge and solutions for practical problems.

The Centrum voor Wiskunde en Informatica is associated with the Netherlands Organisation for Scientific Research (NWO) and it collaborates closely with universities, graduate schools, industry and large knowledge institutions. It is one of the founding members of the European Research Consortium for Informatics and Mathematics (ERCIM) and it manages the Benelux Office of the World Wide Web Consortium (W3C).

CWI has 212 FTE staff, including 161 researchers (29 full professors, 37 postdocs, 60 PhD students, 41 % international, 12% female); the annual budget is 15.8 M €. CWI is proud of its 4 Veni, 4 Vidi, 1 Vici winners and its Spinoza Prize Winner.

About

Prof.dr. A. van Wijngaarden (1916-1987) was one of the founding fathers of Computing Science in the Netherlands. From 1961-1980 he was director of the Mathematisch Centrum.

Prof.dr. N.A. Lynch is Professor in the Department of Electrical Engineering and Computer Science at MIT and heads the Theory of Distributed Systems research group in MIT's Computer Science and Artificial Intelligence Laboratory. Prior to joining MIT in 1981, she served at Tufts University, the University of Southern California, Florida International University, and Georgia Tech. She received her B.Sc. degree in mathematics from Brooklyn College, and her PhD in mathematics from MIT.

Prof.dr. P. Diaconis is Professor of Mathematics and Statistics at Stanford University. He works in graphical methods for high-dimensional data, Bayesian statistics, combinatorics, and group theory. He is, perhaps, best known for his work on shuffling cards. An early MacArthur Fellowship winner and a member of the U.S. National Academy, Diaconis went to New York's City College and Harvard University for his studies.

Prof.dr. J.K. Lenstra is General Director of Centrum voor Wiskunde en Informatica.

Prof.dr. F.W. Vaandrager is Professor in Informatics for Technical Applications at Radboud Universiteit Nijmegen.

Prof.dr. R.W. van der Hofstad is Professor in Probability and Statistics at Technische Universiteit Eindhoven.

Prof.dr. P.W. Adriaans is President of the Board of Stichting Centrum voor Wiskunde en Informatica

Prof. L.G.L.T. Meertens (Kestrel Institute, Utrecht University) composed in 1968 the string quartet No. 1 in C major by means of an ALGOL 60 program on the Electrologica X8 computer of the Mathematisch Centrum.

The Mondriaan Kwartet – Jan Erik van Regteren Altena, violin – Edwin Blankenstijn, violin – Annette Bergman, viola – Eduard van Regteren Altena, violoncello – is famous for its 20th century repertoire. The quartet has developed the online 'Algoritmic Composer'.

The Van Wijngaarden Award is a bronze sculpture, made by Hanneke van den Bergh.

Programme

19.00	INTRO	MONDRIAAN KWARTET
19.30	OPENING	JAN KAREL LENSTRA
19.40	LAUDATIO	FRITS VAANDRAGER
19.45	IMPOSSIBILITY OF CONSENSUS IN DISTRIBUTED SYSTEMS … AND OTHER TALES	NANCY LYNCH
20.25	STRING QUARTET No 1 IN C MAJOR LAMBERT MEERTENS	MONDRIAAN KWARTET
20.40	LAUDATIO	REMCO VAN DER HOFSTAD
20.45	THE SEARCH FOR RANDOMNESS	PERSI DIACONIS
21.25	PRESENTATION VAN WIJNGAARDEN AWARD	PIETER ADRIAANS
21.35	RECEPTION	

1946 60 2006

Abstracts

Abstract 'Impossibility of consensus in distributed systems ... and other tales'
This talk will summarize some of the contributions which my students, collaborators, and I have made to distributed computing theory over the past 25 years, with some history and perspective. The talk will highlight my best-known result – with Fischer and Paterson – showing the impossibility of reaching consensus in a distributed system in the presence of failures.

Abstract 'The search for randomness'
I will examine some of our most primitive images of random phenomena: flipping a coin, shuffling cards, and a pattern made by rain drops.
A careful look, using physics and mathematics, shows that while things *can* be made random, most often they are not.

Abstract Laudatio Nancy A. Lynch
Frits Vaandrager

Professor Lynch is one of the pioneers and leaders of the area of distributed computing theory. She has been instrumental in the development of much of the theory underlying this area, including mathematical models and proof techniques, algorithms, and impossible results. She has also applied this theory to obtain fundamental results about practical systems areas, including database transaction processing, communication, real-time and hybrid systems.
She is probably best known for her discoveries of fundamental impossibility results for distributed computing. Her result (with Fischer and Paterson) on the impossibility of reaching consensus in fault-prone asynchronous systems is widely cited in the practical distributed systems community, since it represents an important limitation on what guarantees such systems can provide. It has also served as the starting point for an extensive collection of theoretical papers by members in the distributed computing community aiming toward understanding the computation power of fault-prone distributed systems.
Other notable research contributions include the 'DLS' algorithms for stabilizing fault-tolerant consensus (with Dwork and Stockmeyer), and the I/O automata mathematical modeling frameworks (with Tuttle, Vaandrager, Segala, and Kaynar).
Professor Lynch is a member of the national Academy of Engineering and an ACM fellow.

Abstract Laudatio Persi Diaconis

Remco van der Hofstad

Persi Diaconis is one of the most colourful mathematicians of the present day. He left home at age 14, without saying goodbye and dropping out of college, to join the legendary magician Dai Vernon. He was a professional magician for ten years. While investigating a possible casino scam, and on a friend's recommendation, Diaconis bought the standard probability text by Feller, only to realize that he could not read it.

A few years later, at age 24, Diaconis decided to take evening math classes, performing as a magician during the day for a living. Within two years, he graduated, and he set his mind on a PhD at Harvard, which, given his unusual background, was not so easy to get into. Luckily he knew Martin Gardner, who had early on published two of his card tricks on the puzzles page in the Scientific American, and who helped him into Harvard. Three years and a PhD later, he was all set for a career in mathematics!

The mathematical work of Persi Diaconis is best known for the combination of deep mathematics applied to practical problems. This is best described with his work on Markov chains and the so-called cut-off phenomenon, which describes a rather sudden convergence to the equilibrium distribution. A key example of such a Markov chain is a card shuffle.
Together with David Bayer, Persi Diaconis showed that in order to shuffle a deck of cards sufficiently, seven shuffles would suffice. When shuffling less, the cards are not sufficiently mixed, and experienced card players can make money with this knowledge. More shuffles are unnecessary, since the improvement is minor. The proof is deep, and is based upon the determination of the idempotents of a natural commutative subalgebra in the symmetric group.

Diaconis also made other important contributions in, for example, Bayesian statistics, the statistics of (contingency) tables and on random matrices and permutations.

Centrum voor Wiskunde en Informatica
Amsterdam, 9 februari 2006

EMBARGO
tot donderdag 9 februari 2006, 21.25 uur

Laudatio
on the occasion of Nancy Lynch receiving the Van Wijngaarden Award 2006

Frits Vaandrager

It is a great honor and also a great pleasure for me to speak about the person and work of Nancy Lynch at the occasion of the 60th anniversary of CWI and the presentation of the Van Wijngaarden Awards.

The mission of CWI --- and Van Wijngaarden --- has always been to do cutting-edge research in Mathematics and Computer Science aimed at methods that may help to solve practical problems in society.
From the beginning, this mission has been criticized by some people: they argue that deep, frontier results in Mathematics and Computer Science cannot be applied (at least not within decades) and are of little or no use for solving the urgent problems of society. To silence these critics it is good to point now and then to researchers who did frontier research and applied their results in practice, living examples so to say in support of CWI's mission. Without doubt, Nancy Lynch is such an example.

I first heard about Nancy Lynch about 20 years ago, when I was PhD researcher at CWI. At the lunch table our colleague Paul Vitanyi was telling enthousiastically about his sabbatical, which he spent at MIT in the Theory of Distributed Systems group of Nancy Lynch. According to Paul, there could be no doubt about Nancy being the smartest woman on earth. He had stories about her enormous productivity and measured her annual research production in terms of meters of publications. So when after my PhD --- which I defended here in the Oude Lutherse Kerk in 1990 --- I had the opportunity to become postdoc in Nancy's group, I was, of course, delighted. Since my experience with women is definitely much smaller than Paul's, I find it hard to assert for this scholarly audience that Nancy really is the smartest women on earth. But of course she is extremely smart. Nevertheless, even more than intelligence I believe an incredible amount of energy in combination with resolve are the key factors behind Nancy's impressive career as a scientist.

Just to illustrate her working energy: I vividly remember a skiing weekend with the Lynch family in their lovely house in the White Mountains in New Hampshire. Rumors have it that Nancy used to drive to the mountains with a research paper on the steering wheel of her car, but that she gave up on this dangerous habit after some (near) accidents. For a full day, we skied downhill, and then going back up again, Nancy and I, sitting next to each other in the ski-lift, discussed our latest paper. Nancy brought a draft with her and was making notes. After alternating intense physical with mental labor for a day, I was exhausted. Nancy not. She was just having fun!

Impossibility Results
In his famous 36/37 paper *On computable numbers, with an application to the Entscheidungsproblem*, Alan Turing defined a computational model of what we now call Turing machines and proved that there are certain problems, such as whether a given computer program halts on a given input, that cannot be solved by any Turing machine. This surprising result has profound philosophical implications on the limits of man-made machines and on our own limits as mortals with finite mass. Moreover it is fair to say that Turing's result marked the birth of Theoretical Computer Science.

In the days of Turing, a computer was a huge device, filling a large room and crunching numbers in splendid isolation. Today, computers are connected: we have telephone networks, the internet, local area networks, wireless networks, sensor networks, etc. and we seek ways to build and reason about these distributed computing systems. What Alan Turing did for Computer Science in general, Nancy Lynch did for the area of Distributed Computing through the discovery of some fundamental impossibility results. The most famous of these results is reported in the 1987 paper with Fischer and Paterson *Impossibility of Distributed Consensus with One Faulty Process*. The result of this paper (commonly known as FLP) is that, surprisingly, it is impossible for a set of processors in an asynchronous distributed system to agree on a binary value, even if only a single processor is subject to an unannounced crash. Although the result was motivated by the problem of committing transactions in distributed database systems, the proof is sufficiently general that it directly implies the impossibility of a number of related problems, including consensus.

The FLP result has had a monumental impact in distributed computing, both theory and practice. Systems designers were motivated to clarify their claims concerning under what circumstances the systems work. Think, for instance, of a system for control of an airplane in which - to achieve fault-tolerance - three computers have to agree on control actions like switching off an engine. On the theory side, people have attempted to get around the impossibility result by changing the system assumptions or the problem statement. Interestingly, it turned out that this is easier for models of distributed computing than for the very generic computational model proposed by Turing. The proof technique used in FLP, valency arguments, has been used and adapted (by Nancy and others) to show many other impossibility and lower bound results in distributed computing. The original FLP paper is written masterfully, and although it contains an unusually deep result, it is accessible even to advanced undergraduate computer science students.

I/O Automata

Nancy Lynch has been instrumental in putting the distributed computing field on a formal foundation. Starting in 1979 with work (with Fischer) on modelling asynchronous shared memory systems, she introduced in 1987 (with Tuttle) I/O automata, a mathematical framework for modelling and analyzing distributed algorithms. The motivation for introducing I/O automata is formulated very clearly in the introduction of the '87 paper:

> "A major obstacle to progress in the field of distributed computation is that many of the important algorithms, especially communications algorithms, seem to be too complex for rigorous understanding. Although the designers of these algorithms are often able to convey the intuition underlying their algorithms, it is often difficult to make this intuition formal and precise.
> [FV: This is a polite way of saying that many published algorithms in the area were flawed!]
> When this intuition is formalized, the result is typically an analysis performed at a very low level of abstraction, involving messages and local process variables. Reasoning precisely about the interaction between these messages and process variables can be extremely difficult, and the resulting proofs of correctness are generally quite difficult to understand. An indication that the situation is not completely hopeless is the fact that designers are able to convey an informal understanding of the key ideas behind their algorithms. What is needed is a way of formalizing these high-level ideas, and incorporating them into a proof of the detailed algorithms correctness."

And indeed this is exactly what the I/O automata framework accomplishes. It is interesting to note that the first overview paper on I/O automata was published via CWI in the CWI-Quarterly in September 1989.
Since 1987, research on I/O automata has continued. Together with co-workers (including Segala, Kaynar and myself), Nancy Lynch defined a series of state-machine models which provide a much-needed mathematical basis for the field of distributed computing. The original framework has been extended to allow for the modelling of real-time and probabilistic systems, and systems that involve both discrete and continuous components, like a computer controlled car. The models come equipped with a collection of simple and practical proof methods, mostly involving composition, invariants and abstraction.

Applications

The I/O automata modelling framework has been been used extensively in the description and proof of complex distributed algorithms and systems. Nancy Lynch herself has been pioneering the application of the theory she developed to practical distributed systems problems. For example, she has used the I/O automaton model as the foundation for a theory for database transaction concurrency control and recovery. She has used I/O automata and compositional methods to model, verify and analyze algorithms used in distributed operating systems -- for example, the main algorithms used in the implementation of the Orca distributed shared memory system (a logical error was found). She has modelled and verified complex communication protocols, mobile wireless ad-hoc networks, security protocols, pieces of automated transit systems, a wide range of distributed system building blocks, a traffic collision and avoidance system for airplanes, etc.

Conclusions

Nancy Lynch has made vital contributions to the theory of distributed computing, including mathematical models and proof techniques, algorithms and impossibility results. She has pioneered the use of formal, mathematical models to address practical problems in this area. Her vision in which mathematical modelling and analysis plays a key role in handling the complexity of distributed systems fits seamlessly with CWI's research mission. And finally (less important, but good to mention in a country in which woman rarely choose to pursue a career in Computer Science) she is a role model showing how women can be highly successful as in Computer Science.

Centrum voor Wiskunde en Informatica
Amsterdam, 9 februari 2006

EMBARGO
tot donderdag 9 februari 2006, 21.25 uur

LAUDATIO
on the occasion of Persi Diaconis receiving the Van Wijngaarden Award 2006

Remco van der Hofstad

Persi Diaconis is one of the most colourful mathematicians of the present times. He left home at age 14, without saying goodbye and dropping out of college, to join the legendary magician Dai Vernon. He was a professional magician for 10 years. In this profession, probabilities play an essential role. While investigating a casino scam, and on a friend's recommendation, Diaconis bought the standard probability text by Feller, only to realize that he could not read it. This would change thoroughly, though...

A few years later, at age 24, Diaconis decided to take evening math classes, performing as a magician during the day for a living. Within two years, he graduated, and he set his mind on a PhD at Harvard. Given his unusual background, Harvard was not so easy to get into. Luckily, he knew Martin Gardner, who had early on published two of his card tricks on the puzzles page in the Scientific American, and who helped him into Harvard. Three years and a PhD later, he was all set for an career in mathematics!

The mathematical work of Persi Diaconis is best known for the combination of deep mathematics applied to practical problems. This is best described with his work on Markov chains and the so-called cut-off phenomenon, which describes a rather sudden convergence to the equilibrium distribution. A key example of such a Markov chain is a card shuffle.

Together with David Bayer, Persi Diaconis showed that in order to shuffle a deck of cards sufficiently, seven shuffles would suffice. When shuffling less, the cards are not sufficiently mixed, and experienced card players can make money with this knowledge. More shuffles are unnecessary, since the improvement is minor. The proof is deep and abstract, and uses representation theory of groups and non-commutative Fourier analysis. However, I doubt that this proof will change the fact that cards are typically not shuffled seven times or more...

Another wide belief is that a coin flip is fair. Indeed, a coin flip is THE way to invoke chance in practice. Diaconis himself says about this: ``Mathematicians are always doing that. Everyone knows it is true, and then we prove it. So what, right?" Wrong! Diaconis first showed that coin flips do not depend on chance, but only on physics. For this, a team of Harvard technicians built a mechanical coin tosser, which can toss a coin with the same side up, time after time. Diaconis has trained himself so that he can toss heads ten times out of ten. I bet that all of you are silently hoping for a demonstration of this, or another, trick...

However, the above does not show that unrehearsed tosses are unfair. After studying the way a coin is flipped with the most advanced high speed cameras, Diaconis, together with Richard Montgomery, figured out that a coin is biased to land on the same side it starts out on. However, the bias is marginal, since it is suggested that it will land the same side up in 51 percent of the cases. Diaconis calls this a ``gem-like example of what we know that isn't so", but also concludes that ``if you flipped a coin vigorously, it was going to be fair."

The mathematics of Persi Diaconis is characterized by an ingenious use of several brands of mathematics, as well as physics. Of course, Diaconis is well-known for his use of discrete mathematical techniques in several of his key papers. In the Netherlands, one of the papers that has been very influential is an unpublished paper with Coppersmith from 1986 on `Reinforced Random Walks', a topic which is currently internationally flourishing. Reinforced random walks are such that the walker has a tendency to stick to places he has seen in the past. Probably all of you recognize this behavior in how we tend to explore new surroundings!

Reinforced Random Walks were picked up by Mike Keane at the CWI. Keane made important contributions, among others with Silke Rolles.

Diaconis also made other important contributions in, for example, Bayesian statistics (primarily with David Freedman), on the statistics of (contingency) tables and on random matrices and permutations.

The combination of deep mathematics and a practical mind, as well as his experience in magic, has also made Diaconis an authority in exposing research on extra sensory perception. He has exposed several psychics, including Uri Geller.

Persi will visit the Netherlands on several occasions this year. Of course, he is here to celebrate the 60th anniversary of the CWI. In March, he will visit Eurandom in Eindhoven for a workshop on Reinforced Random Walks. In July, he will be at the Lorentz Center in Leiden for a workshop in honour of Piet Groeneboom. Finally, somewhere this year, he will give an EIDMA course in Eindhoven.

Tonight, Persi Diaconis will pick up one of his favourite topics: The Search for Randomness, which has been THE main focus in his research.