

# Preface

The conference Mathematical Methods in Computer Science (MMICS) was held in the memory of Thomas Beth during December 17–19 in Karlsruhe. The conference was meant to reflect the many interests of Thomas Beth. Even though these interests might seem diverse the mathematical methods employed and especially algebra as a language were the common denominator of all his scientific achievements. The 12 contributed talks reaching from t-designs to integrated circuits were selected from 30 submissions from 14 countries.

The contributed talks were complemented by three invited talks. Teo Mora gave a talk on “Decoding Cyclic Codes: The Cooper Philosophy” embracing the areas of coding theory and symbolic computation. These areas were especially appreciated by Thomas Beth, because they combine algebra and algorithmics. Richard Jozsa lectured about “Embedding Classical into Quantum Computation” in the area of quantum information. Quantum information was a focus of research of Tomas Beth since 1993 when he co-organized one of the earliest workshops on quantum cryptography in Dagstuhl. Quantum information became his passion in 1994 when the connection between the Fourier transformation and breaking the RSA crypto system became apparent via Shor’s algorithm, which can factor integers in polynomial time on a quantum computer. The Fourier transform and cryptography were topics that played an important role in Thomas Beth’s research and this connection, once again, justified his broad view on computer science.

We were especially delighted by the very personal talk from Fred Piper, a former colleague of Thomas Beth from the time he spent at Royal Holloway College. His talk was about “Zeros and Ones” and his abstract summarizes the scope of the conference better than we can do:

Tom was a personal friend as well as being a colleague and collaborator. He was interdisciplinary in the truest sense of the word with expertise in computer science, mathematics and physics. In this short talk I will look at those areas where our personal interests overlapped. These began with finite projective planes, generalised on to block designs and then changed (from pure mathematics) to coding theory and cryptography. The talk will be historical with little technical detail but, using zeros and ones as the theme, will try to show that the path we followed was ‘natural’.

Thomas Beth would have enjoyed this conference. His legacy should support us in our research projects and remind us to never forget the pleasure of intellectual work.

October 2008

Jacques Calmet  
Willi Geiselmann  
Jörn Müller-Quade

## In Memoriam



Prof. Dr.-Ing. habil. Dr. rer. nat. Thomas Beth, professor and long-standing spokesman of the Institut für Algorithmen und Kognitive Systeme (IAKS), was born November 16, 1949 in Hannover. He studied mathematics, physics, and medicine at the Universität Göttingen and received his Dr. rer. nat. in Mathematics from the Universität Erlangen-Nürnberg in 1978 after four years of employment as a research associate.

After receiving the degree of Dr. Ing. habil. in the area of informatics in 1984 from the same university he was appointed Professor of Computer Science at the University of London and head of the Department of Computer Science and Statistics at the Royal Holloway College, University of London. There he created the research group for cryptography.

In 1985 he took a Chair of Informatics at the Universität Karlsruhe (TH) and, together with two colleagues, co-founded the Institut für Algorithmen und Kognitive Systeme, which he has represented as a spokesman ever since.

The scientific achievements of Prof. Beth were aimed at understanding algorithmic structures in larger systems or applications. This line of research, which started with his algebraic explanation of the general Fourier transform, was continued at his institute, becoming the groundwork in modern signal and image processing. Automated tools for the decomposition of signal transforms were one result of his research that yielded efficient algorithms for different applications. New methods for medical image processing were based on these methods and the algebraic models for signal transforms. Professor Beth recognized very early the importance of the wavelet transform for data compression and pattern

classification. This research was guided by the general idea to use mathematical techniques to develop solutions for a broad spectrum of tasks in signal processing and automatically realize these in very highly integrated circuits. This homogeneous development process avoids inefficiencies and design errors to a large extent.

Cryptology was another focus in the work of Prof. Beth, where he followed an analogous approach. As in his other work he kept an eye on the applicability of his methods, which is reflected by his work in the European Institute of System Security (E.I.S.S.) that he founded in 1988 and headed since then. In his research in cryptology he successfully applied methods from the mathematical areas of combinatorics and algebra. In 1982 he organized an international cryptology conference at Castle Feuerstein, from which the renowned series of EUROCRYPT conferences emerged.

With this background Thomas Beth was early on attracted by the newly emerging field of quantum computing. This area linking informatics, mathematics and physics appealed to him, not only as a researcher, but also due to the implications quantum computing has on cryptology. Encryption mechanisms which are classically considered to be secure become insecure with respect to techniques from quantum computing.

Thomas Beth became a pioneer of quantum computing on the national level as well as internationally. His activities led to the first priority program of the Deutsche Forschungsgemeinschaft and to the first European funding program in this area. In Germany he headed the first and largest research group on quantum computing in informatics.

In the Faculty for Informatics in Karlsruhe he was one of the initiators of the new scientific field of anthropomatics. This young area uses methods and models from informatics to describe the interaction of humans with their environment to supply solutions which are well adapted for individual requirements.

Teaching and research were inseparable for Prof. Beth. Passing on his knowledge was of great concern to him and he kept up a scientific dialogue at all levels: during lectures, at his institute, in the faculty and at national and international conferences. Many of his pupils are now in high positions in science and industry.

In spite of his severe illness he was actively involved in designing the future of informatics. Unfortunately, he could pursue this task for a quarter of a century only. He died on August 17, 2005.