Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®
Journal of Complexity 20 (2004) 134–136
Journal of COMPLEXITY
http://www.elsevier.com/locate/jco

A short biography of Harald Niederreiter

It is a great challenge for us to introduce Professor Harald Niederreiter's personal life and academic achievements. Fully understanding that giving a complete description of Harald's achievements and life would have been difficult, if not impossible, we have instead chosen to provide just some glimpses.

Harald was born on 7 June 1944 in Vienna. He spent his childhood in Salzburg, the birthplace of Mozart, before moving back to Vienna in 1963 to study at the Department of Mathematics of the University of Vienna, where he received his Ph.D. in 1969 under the supervision of Professor E. Hlawka.

Upon graduation from the University of Vienna, Harald worked as an assistant professor in the same university for about 8 months. He subsequently moved to the United States, where he joined Southern Illinois University as an assistant professor in September 1969. Harald spent a total of 9 years in the United States, inclusive of a 2-year stint at the Institute for Advanced Study in Princeton. These 9 years in the US were "formative years" that molded his career and outlook. In 1978, the challenge of heading the Department of Mathematics of the University of the West Indies made him move on to sunny Jamaica. In 1981, by then an established researcher, Harald returned to his native Austria, where he was with the Austrian Academy of Sciences until 2000. Between October 1989 and December 2000, he served consecutively as the director of the Institute of Information Processing and the Institute of Discrete Mathematics at the Academy. In 2001, Harald joined the National University of Singapore as a professor of mathematics and computer science and is leading a research group there.

Numerous awards and honors have been bestowed on Harald. He is an elected full member of the Austrian Academy of Sciences, a member of the Presidium of the German Academy of Sciences Leopoldina, and a recipient of the Cardinal Innitzer Prize for Natural Science in 1998. He delivered a 45-minute invited lecture at the International Congress of Mathematicians 1998 in Berlin, and was a plenary speaker

0885-064X/$ - see front matter
doi:10.1016/j.jco.2003.12.001

at the International Congress of Industrial and Applied Mathematics 2003 in Sydney.

Harald has a broad range of research interests. He started his academic career as an algebraist, working on Abelian groups and finite fields initially. He soon became interested in numerical analysis and pseudorandom numbers in 1970 and began to work in these areas. His first book, *Uniform Distribution of Sequences*, was published when he was 30.

The quasi-Monte Carlo method—the deterministic version of the Monte Carlo method—has proved to be a very powerful tool in numerical integration, financial mathematics, and other areas. In the mid 1970s, seeing the potential and promise in the quasi-Monte Carlo method, Harald started investigations in this area and pioneering work was done in 1978. One of his papers on this subject has been cited at least 240 times. Furthermore, his book *Random Number Generation and Quasi-Monte Carlo Methods*, published in 1995, has become very popular in this area and has received the Outstanding Simulation Publication Award from the United States.

The theory of finite fields goes back to the 17th and 18th centuries, with contributions from many eminent mathematicians. There has been a surge of interest in this subject in the last 50 years because of its diverse applications in computer science and engineering. Harald's book *Finite Fields*, co-authored with Professor Rudolf Lidl and published in 1983, is regarded as the bible on this subject for many people in mathematics, computer science, and electrical engineering.

Harald started to get involved in cryptography when the subject was coming of age, evolving from the intuitive into the scientific. With his background in pseudorandom number generation, his research was initially on stream ciphers, but later included public key cryptography and other topics. In 1986, one of his cryptosystems, now generally referred to as Niederreiter's scheme, was invented. Today, with advances in hardware technology, industrial research and development of his scheme is currently underway, with the objective of incorporating it as the encryption algorithm for digital signature applications.

Harald has never ceased to look for new and promising research topics. Ten years ago, he encountered a fascinating area—algebraic curves over finite fields with many points. His achievements in this area include the discovery of many record curves suitable for applications and the application of the powerful tools in this area to coding theory, digital nets, and cryptography. In particular, the low-discrepancy sequences constructed via this approach have been found to be significantly better than all previously known ones. The paper on this result received a featured review in *Mathematical Reviews*.

To date, Harald has published more than 300 scientific papers and 9 books and has edited dozens of proceedings. He has served, and continues to serve, on the editorial boards of about a dozen international journals. According to the Institute for Scientific Information, Harald is also one of the most highly cited authors in science.

Apart from mathematics, family and friends constitute another important part of Harald's life. He spends his leisure time with them pursuing his favorite pastimes, the choice of which shows a clear Austrian influence. He is an aficionado of classical

music and attends concerts and operas regularly with his wife, Gerlinde. His favorite outdoor activities are hiking and excursion, particularly in the Alps. He also enjoys good food of diverse cultural origins. To those who know him, Harald is a trustworthy person with a good sense of humor.

It is clear that Harald has been a great blessing to the mathematical community as well as to his loved ones. There is no doubt that his list of achievements, scientific or otherwise, will continue to grow.

Cunsheng Ding
Chaoping Xing