THE UNIVERSITY OF HONG KONG

Institute of Mathematical Research
Department of Mathematics

PROBABILITY AND INFORMATION THEORY SEMINAR

Novel Polynomial Basis and Its Application to Reed-Solomon Erasure Codes

Professor Yunghsiang S. Han
Department of Electrical Engineering
National Taiwan University of Science and Technology

Abstract:

A fundamental issue in algebra is to reduce the computational complexities of arithmetic operations over polynomials. Many fast polynomial-related algorithms, such as encoding/decoding of Reed-Solomon codes, are based on fast Fourier transforms (FFT). However, it is algorithmically harder as the traditional fast Fourier transform (FFT) cannot be applied directly over characteristic-2 finite fields. To the best of our knowledge, no existing algorithm for characteristic-2 finite field FFT/polynomial multiplication has provably achieved $O(h \log_2(h))$ operations. In this talk, we present a new basis of polynomial over finite fields of characteristic-2 and then apply it to the encoding/decoding of Reed-Solomon erasure codes. The proposed polynomial basis allows that h-point polynomial evaluation can be computed in $O(h \log_2(h))$ finite field operations with small leading constant. As compared with the canonical polynomial basis, the proposed basis improves the arithmetic complexity of addition, multiplication, and the determination of polynomial degree from $O(h \log_2(h) \log_2\log_2(h))$ to $O(h \log_2(h))$. Based on this basis, we then develop the encoding and erasure decoding algorithms for the $(n = 2^r, k)$ Reed-Solomon codes. Thanks to the efficiency of transform based on the polynomial basis, the encoding can be completed in $O(n \log_2(k))$ finite field operations, and the erasure decoding in $O(n \log_2(n))$ finite field operations. To the best of our knowledge, this is the first approach supporting Reed-Solomon erasure codes over characteristic-2 finite fields while achieving a complexity of $O(n \log_2(n))$, in both additive and multiplicative complexities. As the complexity of leading factor is small, the algorithms are advantageous in practical applications.

This work was presented at the 55th Annual Symposium on Foundations of Computer Science (FOCS 2014).

Biography: Yunghsiang S. Han received B.Sc. and M.Sc. degrees in electrical engineering from the National Tsing Hua University, Taiwan, in 1984and 1986, respectively, and a Ph.D. degree from the School of Computer and Information Science, Syracuse University, NY, in 1993. He was with Hua Fan College of Humanities and Technology, National Chi Nan University, and National Taipei University, Taiwan. From August 2010, he is with the Department of Electrical Engineering at National Taiwan University of Science and Technology as a chair professor.

Dr. Han's research interests are in error-control coding, wireless net-works, and security. Dr. Han has conducting state-of-the-art research in the area of decoding error-correcting codes for more than twenty years. He first developed a sequential-type algorithm based on Algorithm A* from artificial intelligence. At the time, this algorithm drew a lot of attention since it was the most efficient maximum-likelihood decoding algorithm for binary linear block codes. Dr. Han has also successfully applied coding theory in the area of wireless sensor networks. He has published several highly cited works on wireless sensor networks such as random key pre-distribution schemes. He also serves as the editors of several international journals.

Dr. Han was the winner of the Syracuse University Doctoral Prize in 1994 and a Fellow of IEEE. One of his papers won the prestigious 2013 ACM CCS Test-of-Time Award in cybersecurity to recognize its significant impact on the security area over ten years.

Date:	February 11, 2015 (Wednesday)
Time:	4:30 – 5:30pm
Place:	Room ~~309~~ **320A**, Run Run Shaw Bldg., HKU

All are welcome