CLAREMONT CENTER
for MATHEMATICAL SCIENCES

C C M S C O L L O Q U I U M

Binary linear feedback shift register sequences

by

Solomon Golomb

University of Southern California

Abstract: A binary linear feedback shift register sequence (BLFSRS) of degree n, $A = \{a_k\}_0^\infty$, is described mathematically by a linear recurrence relation $a_k = \sum_{i=1}^{n} c_i a_{k-1}$ over GF(2), plus an initial state $(a_{-1}, a_{-2}, \ldots, a_{-n})$. The characteristic polynomial of the corresponding shift register is $f(x) = x^n + \sum_{j=1}^{n} c_j x^{n-j}$. The period of the sequence A depends on its initial state and properties of $f(x)$. If A has its maximum possible period of $2^n - 1$ it is called an m-sequence. Such sequences have a number of interesting (pseudo)-randomness properties, which are described. Interesting results and open problems are enumerated.

About the speaker: Solomon Golomb received his BA in 1951 from Hopkins and his MA and Ph.D. degrees from Harvard in 1953 and 1957, all in mathematics. After a Fulbright year (1955-1956) in Norway, he joined the staff at the Jet Propulsion Laboratory (1956) as a Senior Research Engineer, becoming Group Leader of the Information Processing Group (1958), and Deputy Chief of the Telecommunications Research Section (1960). In 1963 he joined the faculty of the University of Southern California, where he holds the rank of Distinguished and University Professor, with a joint appointment in Electrical Engineering and Mathematics. At USC, he was President of the Faculty Senate (1976-1977), Vice Provost for Research (1986-1989), and Director of Technology - Annenberg Center for Communication (1995-1998). The central theme of his research has been developing and applying concepts of discrete mathematics to signal design for secure, reliable, and synchronized communications. He has published over 200 technical papers, and is author or co-author of five books currently in print. He is a Fellow of the IEEE and of the AAAS. He has served on the Board of Governors of the Information Theory Society, and was its Shannon Lecturer in 1985. He was elected to the U.S. National Academy of Engineering (1976); to the U.S. National Academy of Sciences in 2003; and to the Russian Academy of Natural Sciences (1994) as a foreign member. His numerous awards include three honorary doctorate degrees; the Hamming Gold Medal of the IEEE; and the William Procter Prize of Sigma Xi.

Wednesday, February 8, 2012, at 4:15pm

Freeburg Forum (Kravis Center, LC 62), Claremont McKenna College

Refreshments at 3:45 p.m. in Freeburg Forum Courtyard & wine and cheese after the talk in CMC Math Commons Room (Adams 208)

The dinner will be hosted by Prof. Lenny Fukshansky.
Please contact Prof. Fukshansky if you are interested in attending the dinner.