Sequence with low correlation

Daniel Katz
California State University, USA

Abstract. Finite field arithmetic is an important source of pseudorandomness in the design of digital sequences for communications systems. For example, a maximum length linear feedback shift register sequence (m-sequence) is obtained by applying an additive character of a finite field to the nonzero elements of that field listed in an order based on the field's multiplicative structure (i.e., as powers of a primitive element). There are also sequences based on multiplicative characters of finite fields (e.g., the Legendre symbol) applied to the elements of that field listed in an order based on the field's additive structure. In both cases, the pseudorandomness of the sequence depends on the interaction between the additive and multiplicative structures of the field. One measure of pseudorandomness of sequences and sequence families is correlation. Correlation has both periodic and aperiodic versions (depending on whether the sequences are shifted cyclically or non-cyclically), and for each version one considers both autocorrelation (which measures resemblance between a sequence and shifted versions of itself) and crosscorrelation (which measures the resemblance between a sequence and shifted versions of another sequence). All these forms of correlation provide important indicators of performance for communications systems employing pseudorandom sequences. Typically periodic correlation is more mathematically tractable than aperiodic correlation, and autocorrelation more tractable than crosscorrelation. In this talk, we shall discuss advances in digital sequence design for low correlation, focusing especially on recent developments concerning aperiodic autocorrelation and crosscorrelation.