DANIEL PANARIO, Carleton University

Covering arrays from m-sequences and character sums over finite fields

A covering array of strength t on v symbols is an array with the property that, for every t-combination of column vectors, every one of the possible v^t t-tuples of symbols appears as a row at least once in the subarray defined by these column vectors. Arrays whose rows are cyclic shifts of an m-sequence over a finite field possess many combinatorial properties and have been used to construct various combinatorial objects; see [2].

In this talk we consider covering arrays consisting of discrete logarithms of carefully selected m-sequence elements. Inspired by [1], we connect the covering array definition for this type of arrays to the value of certain character sums over finite fields. Taking advantage of the balanced way in which the m-sequence elements are distributed, we are able to evaluate these sums. This provides new infinite families of covering arrays of arbitrary strength [3].

Joint work with L. Moura, B. Stevens and G. Tzanakis.

References:

[1] C.J. Colbourn, Covering arrays from cyclotomy, Designs, Codes and Cryptography 55 (2010), 201-219.

[2] L. Moura, G. L. Mullen, D. Panario. Finite field constructions of combinatorial arrays, Designs, Codes and Cryptography 78 (2016), 197-219.

[3] G. Tzanakis, L. Moura, D. Panario, B. Stevens. Covering arrays from m-sequences and character sums, Designs, Codes and Cryptography 85 (2017), 437-456.