Constructing covering arrays from m-sequences

Georgios Tzanakis, Carleton University

A *covering array* $CA(N; t, k, v)$ is an $N \times k$ array with entries from an alphabet A of size v, with the property that for any t-tuple of elements from A, any $N \times t$ sub-array has at least one row equal to that t-tuple. The minimum number of rows N such that a $CA(N; t, k, v)$ exists is the *covering array number* for the parameters t, k and v. Few constructions of covering arrays are known that attain the minimum number of rows. New constructions aim instead to improve upon current upper bounds for covering array numbers.

A q-ary m-sequence is a linear recurrence sequence of elements from $GF(q)$ with maximum period. Raaphorst, Moura and Stevens (2014) give a construction for covering arrays of strength 3 over $GF(q)$ using m-sequences. In this talk we present a method that extends this construction to strengths higher than 3. Our computer implementation of this method resulted in 38 new covering arrays that improve upon previously best known upper bounds for covering array numbers. Furthermore, our findings show connections of our construction with finite geometry. We also briefly describe another construction of covering arrays using m-sequences,which is based on character sums and is part of ongoing research.

This is joint work with Lucia Moura, Brett Stevens and Daniel Panario.

Keywords: covering arrays, linear feedback shift register sequences, primitive polynomials over finite fields, exhaustive search algorithms, character sums