Constructing covering arrays from m-sequences

Daniel Panario
Carleton University, Canada
daniel@math.carleton.ca

Let q be a prime power and $\mathbb{F}_q$ the finite field of q elements. A q-ary m-sequence is a periodic sequence of elements from $\mathbb{F}_q$, which is generated by a linear recurrence relation of order n, and has maximal period $q^n - 1$. These sequences play a crucial role in a wide variety of communications and cryptographic applications.

A covering array $CA(N; t; k; v)$ is a $N \times k$ array with entries from an alphabet of size v, with the property that any $N \times t$ sub-array has at least one row equal to every possible t-tuple. Covering arrays are used in applications such as software and hardware testing. It is crucial for such applications to find covering arrays $CA(N; t; k; v)$ with the smallest N possible, for given t, k, v.

There are various algebraic and combinatorial constructions, as well as computer generation methods for covering arrays. Although constructions using m-sequences exist in the literature, these are a few and, until recently, only focused on similar combinatorial objects ("orthogonal arrays" that are covering arrays with more restrictions). Moura, Raaphorst and Stevens (2013) give a construction for covering arrays of strength 3 using m-sequences, which are the best known for many cases. For any prime power q, they give a covering array of strength $t = 3$ with $k = q^2 + q + 1$ columns over $v = q$ symbols that has size $N = 2q^3 - 1$ (number of rows).

In this talk we present an extension of this construction to strengths greater than or equal to 4. The construction is based on Linear Feedback Shift Register (LFSR) sequences constructed using primitive polynomials over finite fields. We have also developed a backtracking algorithm that yields new covering arrays of strength 4. For certain parameters, these are either the best, or close to being the best known when compared to the best known covering array tables kept by Colbourn. Furthermore, our findings show interesting connections with finite geometry.

Joint work with Lucia Moura (University of Ottawa, Canada), Brett Stevens (Carleton University, Canada) and Georgios Tzanakis (Carleton University, Canada).