CHARLIE COLBOURN, Arizona State University, Tempe, Arizona, USA
Distributing Hash Families and Covering Arrays

A (k, v)-*hash function* is a function from a domain of size k to a range of size v. An $(N ; k, v)$-*hash family* is a set of N (k, v)-hash functions. A *perfect hash family* $\mathrm{PHF}(N ; k, v, t)$ (of *strength* t) is an $(N ; k, v)$-hash family with the property that for every t-subset of the domain, at least one of the N functions maps the subset onto t distinct elements of the range. Perfect hash families have arisen in numerous cryptographic applications and in the recursive construction of many allied types of combinatorial arrays. In particular they provide one of the best explicit construction techniques for covering arrays, which in turn arise in software testing, circuit testing, and the like.

Distributing hash families are introduced in order to unify three constructions for covering arrays using perfect hash families, Turán families, and intersecting codes. This unification underlies both an improvement in the sizes of the covering arrays produced, and a generalization to numerous additional parameter sets. For strengths three through six, the construction improves frequently on the sizes of the smallest covering arrays previously known.