On the Classification of Cyclic Hadamard Sequences

– Solomon W. Golomb

Abstract

Binary sequences with two-level periodic correlation correspond directly to cyclic \((v, k, \lambda)\)-designs. When \(v = 4t - 1, k = 2t - 1,\) and \(\lambda = t - 1,\) for some positive integer \(t,\) the sequence (or design) is called a cyclic Hadamard sequence (or design). For all known examples, \(v\) is either a prime number, a product of twin primes, or one less than a power of 2. Except when \(v = 2^k - 1,\) all known examples are based on quadratic residues (using the Legendre symbol when \(v\) is prime, and the Jacobi symbol when \(v = p(p + 2)\) where both \(p\) and \(p + 2\) are prime); or sextic residues (when \(v\) is a prime of the form \(4a^2 + 27\)). However, when \(v = 2^k - 1,\) many constructions are now known, including \(m\)-sequences (corresponding to Singer difference sets), quadratic and sextic residue sequences (when \(2^k - 1\) is prime), GMW sequences and their generalizations (when \(k\) is composite), certain term-by-term sums of three and of five \(m\)-sequences, several constructions based on ovals and hyper-ovals in finite geometries, and the result of performing the Welch-Gong transformation on some of the foregoing. These constructions account for all known examples, which include all possible examples of cyclic Hadamard sequences with \(v = 2^k - 1\) for \(k \leq 10\) (for which exhaustive searches have been performed). It is thus plausible that all possible examples are now known, but this has not been proven.

The \(m\)-sequences also have the “span-\(k\)” property. They are a small subset (only \(\phi(2^k - 1)/k\) such sequences of period \(2^k - 1\)) of the \(2^{2^{k-1} - k}\) “modified de Bruijn sequences”, sequences of period \(2^k - 1\) obtainable from \(k\)-stage shift registers with (in general) nonlinear feedback in which every vector of length \(k\) except “all 0’s” occurs once in each period. It is conjectured that a cyclic Hadamard sequence of period \(2^k - 1\) which also has the span-\(k\) property must be an \(m\)-sequence, but to date neither a proof nor a counterexample has been found.