CORR 99-13

Enumeration and Criteria for Cyclically Shift-Distinct GMW Sequences

Zongduo Dai, Solomon W. Golomb and Guang Gong

Abstract GMW sequences (also called *cascaded GMW sequences*) have two-level autocorrelations. This property makes them widely used in various communication and cryptographic systems. The generation of q-ary GMW sequences of period $q^n - 1$ involves three types of parameters. To determine whether GMW sequence are cyclically shift distinct for differing parameters has remained an open question until now. In this paper, we completely solve this problem for varying all three types of parameters. We find a criterion for cyclically shift distinct q-ary GMW sequences of period $q^n - 1$, and obtain the number of such sequences. For the special case of $q = 2$, this solution facilitates counting the number of cyclic Hadamard difference sets which correspond to binary GMW sequences of period $2^n - 1$.

Index Terms (Cascaded) GMW sequences, GMW functions, trace functions, finite field chains, cyclic Hadamard difference sets.