CORR 99-60

Discrepancy Transforms and their Applications

Guang Gong

Abstract In this paper, a new transform of ultimately periodic binary sequences, called a *discrepancy transform*, is developed. The discrepancy transform is computed in terms of the Berlekamp-Massey algorithm. It is shown that the discrepancy transform is a one-to-one correspondence between a set consisting of all ultimately periodic binary sequences and a set of sequences of all zeros but finite ones. A characteristic of linear span profiles of sequences is discovered by means of the discrepancy transform. A dynamic version of the Berlekamp-Massey algorithm is the presented. In terms of a restriction of the discrepancy transform computed by this version, a family of nonlinear permutations of $GF(2^n)$ is constructed. Applying a class of such permutations to filter function generators yields a new type of pseudo-random sequence generators, called *D-filter generators*. Sequences generated by a D-filter generator have period $2^n - 1$ with the balance property and achieve the maximal linear span $2^n - 2$ in most of cases for different LFSRs. The D-filter generator is dynamic and easier to randomly switch at different communication sections. The number of bit operations for output of one bit is bounded by $O(n^3)$; thus, it can be efficiently implemented in both hardware and software. D-filter generators have important applications in stream cipher cryptosystems and secure communication network. It is worth to point it out that the discrepancy transform provide a way for analysis of the Berlekamp *iterative* algorithm in permutational *functional* models. It can be applied to various decoding techniques in which decoding algorithms are related to the Berlekamp algorithm.

Key words The Berlekamp-Massey algorithm, pseudo-random sequences, permutation, Boolean function, cryptology, and coding.