Abstract

Pseudorandom sequences are widely used in cryptography, coding theory and combinatorial design. In this talk, we will focus on binary sequences with length n and nonlinear complexity not less than n/2. By characterizing the general structure of these sequences, we propose a direct construction for these sequences, and establish a formula to calculate the exact number of such sequences.