MILITARY UNIVERSITY OF TECHNOLOGY
FACULTY OF CYBERNETICS

Abstract

Effective irreducibility testing of binary polynomials with particular forms

The thesis deals with the problem of effective irreducibility testing of binary polynomials with particular forms. The key idea was to construct and implement the new irreducibility testing algorithm, which fulfils the requirements of modern Central Processing Units (CPUs) and Graphical Processing Units (GPUs). Subsequently, the vast computational experiment was conducted in order to provide the list of all irreducible trinomials and sedimentary polynomials with degree less than 513000. Having data collected, it was possible to reject the well-known hypothesis about the inner degree of sedimentary polynomials and find new infinite classes of irreducible trinomials.

Furthermore, a new search method of the nonlinear feedback shift registers (NLFSRs) with a particular form was presentented. The algorithm complies with the prerequisites of modern parallel and distributed environments. By using the novel search algorithm, I was able to provide the full list of NLFSRs with a particular form with degrees less than 31.