



Apr 14th, 9:00 AM - Apr 1st, 10:00 AM

Testing Binary Polynomials for Irreducibility

Steven Hayman

Illinois Wesleyan University

Andrew Shallue, Faculty Advisor

Illinois Wesleyan University

Follow this and additional works at: <http://digitalcommons.iwu.edu/jwprc>

Hayman, Steven and Shallue, Faculty Advisor, Andrew, "Testing Binary Polynomials for Irreducibility" (2012). *John Wesley Powell Student Research Conference*. 9.

<http://digitalcommons.iwu.edu/jwprc/2012/posters/9>

This Event is brought to you for free and open access by The Ames Library, the Andrew W. Mellon Center for Curricular and Faculty Development, the Office of the Provost and the Office of the President. It has been accepted for inclusion in Digital Commons @ IWU by the faculty at Illinois Wesleyan University. For more information, please contact digitalcommons@iwu.edu.

©Copyright is owned by the author of this document.

Poster Presentation P17

TESTING BINARY POLYNOMIALS FOR IRREDUCIBILITY

Steven Hayman and Andrew Shallue*
Mathematics Department, Illinois Wesleyan University

A binary trinomial is a polynomial with three terms whose coefficients are either zero or one. A polynomial is irreducible if it does not have any nontrivial factors. Irreducible binary trinomials have a number of cryptographic and hardware applications. We have tested close to 5 billion binary polynomials for irreducibility. This computation was the result of combining various techniques from the literature.