Solving Equations with Size Constraints for the Solutions

[Invited Talk]

Henry Cohn
Microsoft Research New England
One Memorial Drive
Cambridge, MA 02142
cohn@microsoft.com

ABSTRACT

In this talk, I'll survey some key applications within coding theory and cryptography for solving polynomial equations with size constraints on the solutions. Specifically, we seek solutions that are small integers or low-degree polynomials. In the single-variable case this is relatively well understood, thanks to important work in the late 1990's by Guruswami and Sudan and by Coppersmith, but higher dimensions hold many mysteries. I'll highlight connections with hot topics such as fully homomorphic encryption, as well as some problems for which progress should be possible.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*

Keywords

coding theory; polynomial systems

ISSAC'13, June 26–29, 2013, Boston, Massachusetts, USA.
ACM 978-1-4503-2059-7/13/06 .