2005

Gröbner Bases: A Natural Extension of Gaussian Reduction and the Euclidean Algorithm (Abstract)

Patrick Flinn

Follow this and additional works at: http://ecommons.udayton.edu/mth_kcs

Part of the Mathematics Commons

eCommons Citation
http://ecommons.udayton.edu/mth_kcs/6

This Article is brought to you for free and open access by the Math Events at eCommons. It has been accepted for inclusion in Kenneth C. Schraut Memorial Lectures by an authorized administrator of eCommons. For more information, please contact frice1@udayton.edu, mschlange1@udayton.edu.
Gröbner bases: A Natural Extension of Gaussian Reduction and the Euclidean Algorithm

Dr. Patrick Flinn
Senior Cryptologic Mathematician, National Security Agency

Abstract:
Gröbner bases can be used to answer fundamental questions concerning certain sets of polynomials. For example, when are two such sets equal? Given such a set and another polynomial, is this polynomial a member of that set? Surprisingly, given the simplicity of its concepts, Gröbner bases are of relatively recent invention, being an active field of research today and a popular topic for Ph.D. theses.

In this introduction to Gröbner bases, we motivate their salient features by considering the Euclidean algorithm and Gaussian row reduction of matrices from a slightly different point of view.

Patrick Flinn received a Bachelor's Degree in mathematics from the University of Dayton, where an excellent faculty, and in particular Professor K.C. Schraut, prepared him for and inspired him to pursue a Ph.D. The latter was obtained in functional analysis at the Ohio State University, under the direction of Professor William Davis. Pat met his future wife, Barbara Brown, a brilliant mathematician who would earn her Ph.D. in complex analysis at the University of Michigan, while both were on fellowship at Cambridge University, England. Interestingly, Barb's father and Pat are from Sidney, Ohio, but Barb and Pat had to "cross the pond" to meet. While Barb was at the University of Texas in Austin on her postdoc and Pat was on the faculty of Texas A&M University, Bob Karkoska, a classmate of Pat's at both Dayton and Ohio State, and his new bride, stopped in Austin to visit on their honeymoon. Bob suggested a solution to the problem of finding collocated jobs for research mathematicians in a difficult job market for mathematicians: The National Security Agency (NSA). Now, twenty years later, Barb and Pat are senior cryptologic mathematicians at NSA, Pat running a division of 150 mathematicians, computer scientists, and engineers on the front line of cryptomathematical research and applications.