Charles Phelps Taft Research Center
at the University of Cincinnati
Graduate Summer Fellowship Award

Each section (I-III) should be placed at the start of a new page. All required materials must be included in a single document, uploaded to the electronic submissions system, no later than 5PM on the published day of the deadline. Departmental review is required for this program, as well as a letter of support. Applicants should submit their application with enough time to receive review prior to the close of the deadline. Taft does not accept an obligation to review applications that have not received intradepartmental review by the close of the deadline.

I. General Information

a. Name: Sergio Molina
b. M#: xxxxxxxxxx
c. Department: Mathematics
d. Project title: Semi-Regular Systems of Equations
e. Project Location: Department of Mathematics
f. Probable Results of a Grant (such as publications, working papers, and presentations): Publication, presentations.
g. Have you already or will you in the future apply for other grants for this travel, including departmental support? Yes, I intend to apply to the Department of Mathematical sciences for additional support.

II. Taft Grant History

None.

PROJECT NARRATIVE

Introduction

One of the mathematical problems with a major importance is that of finding solutions to systems of polynomial equations of the form

$$p_1(x_1, \ldots, x_n) = \beta_1, \ldots, p_m(x_1, \ldots, x_n) = \beta_m.$$

The security of many of the new cryptosystems relies on the difficulty of solving a system of polynomial equations. Thus, the understanding of the complexity of solving polynomial equations (the difficulty in terms of number of computations needed for an algorithm to solve such a system of polynomial equations), is a critical problem which has not only theoretical significance but also serious practical implications in a world in which secure electronic communication is ubiquitous.

Background

A number of cryptographic systems have been proposed that involve quadratic functions over a finite field, in particular over the field $\mathbb{F}_2$, the field of two elements. Their security relies in part on the difficulty of finding solutions to systems of quadratic equations. The main types of algorithms used to solve such systems of equations are the Gröbner basis algorithm family including the $\mathbf{F}_4$ and $\mathbf{F}_5$ variants introduced by Faugère. In order to assess the complexity of these algorithms, the concept of "semi-regular" systems of polynomial equations over $\mathbb{F}_2$ was introduced in [1, 2]. Roughly speaking, a semi-regular system of polynomials $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)$, is a system in which no relations but the trivial ones, such as, $f_i f_j = f_j f_i$ or $f_i^2 = 0$, occurs. In other words, is a system in which the polynomials are independent of each other.

Semi-regular systems are important because experimental evidence suggests that most systems are semi-regular and we know the complexity of solving semi-regular systems of polynomial equations [2]. A proof that most sequences are semi-regular would prove current heuristic assumptions on complexity.

Specific Aims

Despite the experimental evidence that semi-regular systems are common, almost nothing was known about the existence of semi-regular sequences of m polynomials and n variables

$$f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n),$$

except in extremely trivial situations. As part of my dissertation research, I have been working in this problem under the supervision of Dr. Timothy Hodges, who is one of the authors of [5, 6, 7, 8]. In our research we have obtained some results about the existence of semi-regular systems. In [1, 2] the authors conjecture that the proportion of semi-regular systems tends to one as the number of variables tends to infinity. In [7] we prove this conjecture in the following precise sense. If $h(n)$ denotes the number of sets consisting of homogeneous polynomials of degree greater than or equal to one and $s(n)$ denotes the number of such subsets that are semi-regular then the ratio $s(n)/h(n)$ tends to one as the number of variables tends to infinity. This result is in a sense a statement that semi-regular systems are common. A different formulation of the conjecture that most systems are semi-regular is given in [2]. The authors conjecture that for any $(n, m, d_1, \ldots, d_m)$ the proportion $\pi(n, m, d_1, \ldots, d_m)$ of semi-regular systems of m equations of degrees $d_1, \ldots, d_m$ in n variables tends to 1 as n tends to ∞. In [7] we show that this conjecture is false.

As result of our research one paper [7] has been submitted to the Journal of Algebra which is an important journal in mathematics, and another paper [8] is under preparation. Also, I have presented our work in an important workshop [9], and a poster [10] will be presented at the UC Graduate Poster Forum.

Although, our results give a better understanding of semi-regular systems, it is still needed to prove the observed fact that "most" quadratic systems of length n in n variables are semi-regular. This is one of the most important open problems in multivariate cryptosystems. Even the question of the existence of quadratic semi-regular systems of length n in n variables for all n remains open. Our main goal is to give important results in this direction.

We expect to give an answer about the existence of quadratic semi-regular systems of length n in n variables for all n. To this purpose, we plan to make use of "generic" polynomials. Generic polynomials are polynomials whose coefficients are independent of each other. It is expected that this polynomials can determine the existence of the semi-regular systems. I will need to do lots of computations for small number of variables to check the semi-regularity of systems of generic polynomials. This computations will be handled in the computer programs MAGMA and MATHEMATICA. With the data collected, we will develop a theoretical model that describes the existence of quadratic semi-regular systems of length n in n variables for all n. Having a better understanding of this problem, we expect to deepen in the conjecture presented about whether "most" quadratic systems are semi-regular.

The results of this work will be part of my dissertation in support for the candidature for the degree of Doctor of Philosophy in Mathematical Sciences. Also, I expect that part of this work can be submitted to a specialized journal of algebra and/or cryptography.

References

[1] M. Bardet, *Étude des systèmes algébriques surdéterminés. Applications aux codes correctuers et la cryptograhie*. PhD thesis, Université Paris V!, Décembre 2004.

[2] M. Bardet, J-C. Faugre, B. Salvy, *Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$*, in: INRIA Research Report 5049, 2003.

[3] J.-C. Faugere, *A new efficient algorithm for computing GröbnerBases (F4)*, Pure App Alg, Volume 139, 1999, 61-88.

[4] J.-C. Faugere, *A new efficient algorithm for computing GröbnerBases without reduction to zero (F5)*, ISSAC 202, Pages 75-83.

[5] J. Ding, T. J. Hodges, V. Kruglov, D. Schmidt, S. Tohaneanu, *Growth of the ideal generated by a multivariate quadratic function over GF(3)*, J. of Algebra and Its Applications, 12 (2013), 1250219-1 to 23.

[6] T. J. Hodges, C. Petit and J. Schlather, *First Fall Degree and Weil Descent*, Finite Fields and Their Applications 30 (2014), 155-177.

[7] T. J. Hodges, S. D. Molina and J. Schlather, *On the Existance of Semi-Regular Sequences*, submitted. Available under http://arxiv.org/abs/1412.7865

[8] T. J. Hodges, S. D. Molina, *Homological Characterization of Semi-Regular Sequences over $\mathbb{F}_2$*, in preparation.

[9] S. Molina, *On the Existence of Semi-Regular Sequences*, DIMACS Workshop on The Mathematics of Post-Quantum Cryptography, DIMACS Center for Discrete Mathematics and Computer Science, Rutgers University, New Jersey, January 15, 2015.

[10] S. Molina, *On the Existence of Semi-Regular Sequences*, Poster to be presented at the 2015 Expo & Poster Forum, University of Cincinnati, Cincinnati, March 6, 2015.

Sergio Molina

310 Bryant Avenue Apt. 23
Cincinnati, OH 45220
molinasd@mail.uc.edu

University of Cincinnati
Department of Mathematical Sciences
2600 Clifton Avenue
Cincinnati, OH 45220

Education

2010–present	PhD in Mathematics (in progress), University of Cincinnati, Cincinnati, USA.
2006–2009	MSc in Mathematics, National University of Colombia, Medellín, Colombia.
1999–2005	BSc in Mathematics, National University of Colombia, Medellín, Colombia.

Professional Experience

2010–present	**Graduate Assistant, University of Cincinnati, Cincinnati, USA.** Taught the courses Foundations of Quantitative Reasoning, College Algebra, Applied Calculus I, Applied Calculus II, Calculus II.
2006–2010	**Graduate Assistant, National University of Colombia, Medellín, Colombia.** Taught the courses Calculus I, Calculus II, Multivariable Calculus.
2010	**Adjunct Instructor, University of Medellín, Medellín, Colombia.** Taught the courses Trigonometry, Multivariable Calculus.
2009	**Adjunct Instructor, University of Antioquia, Medellín, Colombia.** Taught the course Trigonometry.
2008–2009	**Adjunct Instructor, ITM University Institution, Medellín, Colombia.** Taught the courses Linear Algebra, Multivariable Calculus.
2005–2006	**Adjunct Instructor, University of Antioquia, Medellín, Colombia.** Worked as a "mentor" in mathematics for elementary school faculty in order to improve the use of ICTs in public schools in Colombia.
2003–2005	**Undergraduate Teaching Assistant, National University, Medellín, Colombia.** Conducted problem sessions for Multivariable Calculus.

Languages

Spanish	Native Language
English	Fluent

Academic Honors and Awards

2014	Maita Levine Summer Research Fellowship, University of Cincinnati, Cincinnati, USA.
2011	Maita Levine Award for Outstanding Beginning Doctoral Student, University of Cincinnati, Cincinnati, USA.
2011	Scholarship-Loan, COLFUTURO/Foundation for the Future of Colombia, Bogotá, Colombia.
2010-2011	Mazda Foundation Scholarship for Arts and Science, Bogotá, Colombia.
2005	Graduate Cum Laude, National University of Colombia, Medellín, Colombia.

Research Interests

Abstract Algebra	Commutative Algebra, Cryptography.

Publications

2015	T. Hodges, S. Molina, *Homological Characterization of Semi-Regular Sequences over F2*, in progress.
2014	T. Hodges, S. Molina, J. Schlather, *On the Existence of Semi-Regular Sequences*, submitted. Available under `http://arxiv.org/abs/1412.7865`
2013	C. Cadvid, S. Molina, J.D. Velez, *Limits of quotients of bivariative real analytic functions*, Journal of Symbolic Computation 50 (2013) 197-207.

Presentations

2015	*On the Existence of Semi-Regular Sequences*, Poster to be presented at the 2015 Expo & Poster Forum, University of Cincinnati, Cincinnati, USA.
2015	*On the Existence of Semi-Regular Sequences*, DIMACS Workshop on The Mathematics of Post-Quantum Cryptography, DIMACS Center for Discrete Mathematics and Computer Science, Rutgers University, New Jersey, USA.
2009	*Puiseaux Series, Galois Theory and Limits of quotients of bivariative real analytic functions*, XVII Colombian Congress of Mathematics, Cali, Colombia.