Solving Polynomial Systems over Finite Fields

As a theoretical shortcoming in our lectures is that we did not mention the Hilbert Nullstellensatz. This Satz (or theorem) provides a criterion for the infeasibility of a polynomial system. As a practical shortcoming, we have not yet addressed at all the problem of solving polynomial systems over a finite field.

The goal of our first computational project is to study the application of Hilbert Nullstellensatz, based on two papers [1] and [2].

1. Assignment One: Summarize two Papers

Read the papers [1] and [2] and summarize the essence of the content in one single page, using your own words to explain the assumptions, ideas, methods, and results in [1] and [2].

2. Assignment Two: Problem Setup

The aim of [1] and [2] is to solve combinatorial graph problems. The goal of this assignment is to formulate the problems in any standard computer algebra system, so that a Gröbner basis can be computed. Show that by solving a polynomial system one can solve a combinatorial graph problem.

3. Assignment Three: Solve the Problems

Experiment with the linear algebra methods over finite fields available in the computer algebra system of your choice to obtain a proof-of-concept calculation on one of the sample systems solved in [1] and [2].

While the example used in the previous assignment could very well be a toy problem, the point of this assignment is to solve a problem that could not be handled by the Gröbner basis engine of the computer algebra system.

4. The deadline is Monday 17 February 2014 at 2PM

On the deadline, bring your answers to the assignments:

1. a summary of the two papers,
2. computer algebra code to set up the problems,
3. computational results of your proof-of-concept calculations.

This project must be solved individually.

Feel free to come to my office for help.

References

[1] J.A. De Loera, J. Lee, P.N. Malkin, and S. Margulies. Hilbert's Nullstellensatz and an algorithm for proving combinatorial infeasibility. In D. Jeffrey, editor, *Proceedings of the 2008 International Symposium on Symbolic and Algebraic Computation (ISSAC 2008)*, pages 197–206. ACM, 2008.

[2] J.A. De Loera, J. Lee, S. Margulies, and S. Onn. Expressing combinatorial problems by systems of polynomial equations and Hilbert's Nullstellensatz. *Combinatorics, Probability and Computing*, 18(4):551–582, 2009.