A new technique for solving polynomial systems of equations over finite fields via stochastic local search.

Date Tuesday, November 9

Time 4 pm

Location 303 Mudd

Abstract: Polynomial systems of equations over finite fields arise in cryptanalysis, and elsewhere. The DEMOCRACY algorithm is a new technique for finding one solution in the coefficient field, for low degree systems. First, start with a random temporary assignment of a field element to each variable. Then "erase" the value of one variable, call it x. Each equation is now a univariate polynomial, considering the unerased variables as being constants equal to their temporary assignment, and only x as unknown.

If x is never raised to a power > 3, then simple algebra is sufficient to produce a set of values for x that satisfy any particular equation in the system. The equations then "vote" for values of x, with a "ballot box" for each field element, and each equation voting for any field element that will satisfy it. It is easy to see that the box with the most votes corresponds to the coefficient field element that will satisfy the largest number of the given equations. Now x is changed to that value, and another variable is targeted.

This is a simplified version of the actual method. While extremely heuristic, this method has been eective on systems of up to 100 equations and can quickly solve systems that cause MAGMA to crash for lack of memory.