▸ ALAN WOODS, *Quadratic equations over $GF(q)$ and proofs of unsatisfiability.*
School of Mathematics and Statistics, University of Western Australia, Nedlands W.A. 6009, Australia.
E-mail: woods@maths.uwa.edu.au.

The problem of determining whether a system of simultaneous quadratic equations in n variables has a solution in the q element field $GF(q)$, is known to be NP-complete, even for $q = 2$. If the system is satisfiable, there is a short proof of this fact, namely exhibit a solution. In general it seems to be much more difficult to prove that a given system does not have a solution. The obvious brute force search involves looking at all potential solutions, of which there are q^n.

Of course, the number N of solutions of a system can also be computed in this way. However by utilizing the fact that all the equations are *quadratics*, it is possible to do better in cases where the number of equations k is significantly smaller than n. Daniel Hawtin, Grant Keady and the speaker have recently implemented two practical algorithms for computing N which run in time q^k times a polynomial in n and q.

Probably more of theoretical interest, it turns out that for any quadratic system unsatisfiable in $GF(q)$, there is a "proof of unsatisfiability", whose size, and machine checking time, are only about the squareroot of the number of steps required for an exhaustive search of all q^n potential solutions. With Hawtin and Keady, it has been observed recently that these ideas also lead to "proofs" that a given graph is *not* 3-colourable.

I'll mainly concentrate on $q = 2$ and $q = 3$, so the talk should be accessible even without any knowledge of finite fields.