Abstract of talk

Row reduction for groups of twisted Lie type

by Arjeh Cohen

14 January 2015, Eindhoven

I will report on joint work with Don Taylor. It extends the results by the two of us and Scott Murray, published in 2004, on an algorithm working with a finite group G of untwisted Lie type and an irreducible G-module M over a field of the same characteristic as G. When given a linear transformation A on M, it decides whether A is in the image of G and if it is, find a pre-image in polynomial time in $\log(q)$ and the coefficients of the highest weight λ of the representation, subject to the existence of a discrete log oracle.

Let G be a finite group of Lie type (with a possible exception for ${}^2\mathrm{A}_{2n}$), of rank ℓ, non-Ree, over $\mathrm{GF}(q)$, presented by a reduced Curtis–Steinberg–Tits presentation. Suppose that $\rho : G \to \mathrm{GL}(d, \mathrm{GF}(q^e))$ is an absolutely irreducible representation of G. The extension states that there is an algorithm that, when given $A \in \mathrm{GL}(d, \mathrm{GF}(q^e))$, decides whether A is in $\rho(G)$ and if it is, finds an element $g \in G$ (as a normalized word in the generators) such that $\rho(g) = A$. The algorithm runs in time $\mathrm{O}((\log(q)de)^3\ell^2)$, subject to the existence of a discrete log oracle.