Bull. Aust. Math. Soc. **94** (2016), 169–170
doi:10.1017/S0004972716000058

ALGORITHMS FOR GALOIS GROUP COMPUTATIONS OVER MULTIVARIATE FUNCTION FIELDS

GARETH ANDREW WHITE

(Received 18 September 2015; first published online 12 May 2016)

2010 *Mathematics subject classification*: primary 12F10; secondary 11R32, 11Y40.
Keywords and phrases: Galois group computations, multivariate polynomials.

In this thesis, two separate algorithms are described to determine the Galois group of a polynomial f defined over a function field of the form $\mathbb{Q}(w_1, \ldots, w_a)$. Both of these algorithms use Stauduhar's method for polynomials over $\mathbb{Q}$ (introduced by Stauduhar in 1973 for polynomials of degree up to seven [2], and refined by Fieker and Klüners in 2014 to be compatible for polynomials of any degree [1]). In the thesis, various techniques are used to make the algorithms compatible for function fields as the base field. In particular, both algorithms construct the resolvent of f. This is shown to have integer coefficients and, through the use of valuation theory and Newton polygons, we obtain upper bounds on the degrees of the parameters $w_1, w_2, \ldots, w_a$. The algorithms deviate in the determination of upper bounds on the integer coefficients, as well as the construction and application of the resolvent itself.

The first algorithm uses a special form of Hensel lifting to express the roots as a multivariate power series. For each lift we square the ideal in whose modulus the roots are computed in order the minimise the number of lifts required. We also obtain a bound on the size of the integer coefficients of the resolvent by considering the roots of f as a contour integral of a complex power series. This allows us to construct a quotient ring in which we can compute the roots to sufficient precision to determine the resolvent exactly. The resolvent is then factorised over $\mathbb{Z}[w_1, \ldots, w_a]$.

The second algorithm constructs the resolvents of a set of specialisations of f. Since these specialisations are single-variable polynomials, fast techniques are known for computing their resolvents. Rational roots are also found for each specialised resolvent. The resolvents and roots are then interpolated to give the resolvent of the original multivariate polynomial, as well as a potential rational root, removing the need for factorisation.

Thesis submitted to the University of Sydney in September 2014; degree awarded on 18 March 2015; primary supervisor Steve Donnelly, associate supervisor Claus Fieker.

Computational complexity and timing of implementations in MAGMA for various polynomials of degree up to eight are determined for each algorithm. It is shown that the specialisation algorithm is superior in most cases.

References

[1] C. Fieker and J. Klüners, 'Computation of Galois groups of rational polynomials', *LMS J. Comput. Math.* **17**(1) (2014), 141–158.
[2] R. P. Stauduhar, 'The determination of Galois groups', *Math. Comp.* **27** (1973), 981–996.

GARETH ANDREW WHITE,
School of Mathematics and Statistics,
University of Sydney, New South Wales 2006,
Australia
e-mail: garethw@maths.usyd.edu.au

https://doi.org/10.1017/S0004972716000058 Published online by Cambridge University Press