BULL. AUSTRAL. MATH. SOC. 11G20, 11Y99, 14Q05
VOL. 74 (2006) [479–480]

Explicit endomorphisms and correspondences

BENJAMIN SMITH

ABSTRACT

In this work, we investigate methods for computing explicitly with homomorphisms (and particularly endomorphisms) of Jacobian varieties of algebraic curves. Jacobians of hyperelliptic curves have been a subject of considerable interest in recent years since their proposal as a source of groups for cryptography by Koblitz. While efficient algorithms and compact representations for computing with Jacobians are well-known, methods for explicitly computing with homomorphisms between them are relatively undeveloped. The intent of this thesis is to contribute to the understanding of constructing explicit homomorphisms of Jacobians, and to provide a variety of efficient and practical examples and applications of the theory.

We begin by discussing the theory of correspondences on curves. This geometric approach to homomorphisms of Jacobians is analogous to the study of a function by analysis of its graph. The advantage of correspondences is that they permit the expression of any homomorphism of Jacobians in a compact way, as a divisor on a product of curves. In particular, correspondences do not require the construction of the Jacobians themselves. While correspondences are a classical subject, we treat the theory in a constructive, algorithmic fashion.

We then give a series of explicit examples of correspondences inducing non-trivial homomorphisms. Extending work of Cassou–Noguès and Couveignes, we give families of hyperelliptic curves of genus three, five, six, seven, ten and fifteen, defined over number fields of low degree, whose Jacobians have isogenies to other hyperelliptic Jacobians. For each family, we construct a correspondence to making these isogenies explicitly computable.

We describe several families of hyperelliptic curves whose Jacobians have complex multiplication and/or real multiplication, including families described by Mestre and by Tautz, Top and Verberkmoes. Again, we construct correspondences to make the complex and real multiplication explicit. We then use the correspondences to derive efficiently

Received 23rd August, 2006
Thesis submitted to The University of Sydney, December 2005. Degree approved, July 2006. Supervisors: Dr David R. Kohel and Professor John Cannon.

computable maps on ideal class representatives for Jacobian points. These forms for the explicit endomorphisms may be used for efficient integer multiplication on hyperelliptic Jacobians, extending Gallant–Lambert–Vanstone fast multiplication techniques from elliptic curves to higher dimensional Jacobians.

Finally, we describe Richelot isogenies for curves of genus two. In contrast to classical treatments of these isogenies, we consider all the Richelot isogenies from a given Jacobian simultaneously. The inter-relationship of Richelot isogenies may be used to deduce information about the endomorphism ring structure of Jacobian surfaces. We conclude with a brief exploration of these techniques.

Department of Mathematics
Royal Holloway
University of London
Surrey TW20 OEX
United Kingdom