Lercier, Reynald; Ritzenthaler, Christophe; Rovetta, Florent; Sijsling, Jeroen

Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. (English) Zbl 1333.14060

LMS J. Comput. Math. 17A, Spec. Iss., 128-147 (2014).

Let $\mathcal{M}_g$ denote the coarse moduli space of (projective, geometrically irreducible, nonsingular algebraic) curves of genus $g > 1$ defined over a field k of characteristic p. One is often interested to explicitly write down models for a curve corresponding to a point of $\mathcal{M}_g$; this can be done e.g. if a *universal family* is available which is not the case in general. In the paper under review, new concepts that substitute the notion of universal family are introduced whenever $p = 0$ or $p > 2g + 1$; specially the so-called *representative family* which, given a subvariety $\mathcal{S}$ of $\mathcal{M}_g$, is a family of curves $\mathcal{C} \to \mathcal{S}$ whose points are in a natural bijection with those of $\mathcal{S}$. It turns out that the existence of a representative family is quite related to the question of whether the field of moduli of a curve is a field of definition.

The authors illustrate their results by working out on families of quartic plane curves $C \subseteq \mathbb{P}^2$ and by taking $\mathcal{S} = \mathcal{S}_G$ to be a subvariety of such curves with a given automorphism group $G \subseteq \mathrm{PGL}_3$. It turns out that the classification of such groups is known if $p = 0$ or $p \geq 5$; cf. *I. V. Dolgachev*'s book [Classical algebraic geometry. A modern view. Cambridge: Cambridge University Press (2012; Zbl 1252.14001)]. Then one can compute representative family of $\mathcal{S}_G$ via Galois descent to extensions of function fields. They also give an algorithm to compute the twists of a plane quartic and work out an implementation with MAGMA of some results of the paper for prime fields of order p with $7 < p < 256$.

Reviewer: Fernando Torres (Campinas)

MSC:

14Q05	Computational aspects of algebraic curves
13A50	Actions of groups on commutative rings; invariant theory
14H10	Families, moduli of curves (algebraic)
14H37	Automorphisms of curves

Keywords:
moduli space of curves; plane quartic

Full Text: DOI arXiv

References:

[1] DOI: 10.1016/j.jalgebra.2012.07.054 · Zbl 1276.14088 · doi:10.1016/j.jalgebra.2012.07.054
[2] Lercier, Proceedings of the Tenth Algorithmic Number Theory Symposium pp 463– (2012)
[3] DOI: 10.1007/BF02566434 · Zbl 0885.14013 · doi:10.1007/BF02566434
[4] DOI: 10.1007/s00029-002-8107-1 · Zbl 1036.11028 · doi:10.1007/s00029-002-8107-1
[5] Silverman (2009)
[6] Shioda, Comment. Math. Univ. St. Pauli 42 pp 61– (1993)
[7] Serre (1968)
[8] Sekiguchi, Compos. Math. 54 pp 33– (1985)
[9] Satoh, Advances in cryptology: EUROCRYPT 2009 (2009)
[10] DOI: 10.1090/conm/574/11422 · Zbl 1317.11006 · doi:10.1090/conm/574/11422
[11] DOI: 10.1112/S1461157009000576 · Zbl 1278.11068 · doi:10.1112/S1461157009000576
[12] Howe, Algebra, Geometry, and Coding Theory (AGCT 2003) 11 (2005)
[13] DOI: 10.1007/BF01298341 · Zbl 0459.14005 · doi:10.1007/BF01298341
[14] DOI: 10.1016/j.jnt.2010.06.003 · Zbl 1245.11075 · doi:10.1016/j.jnt.2010.06.003
[15] Henn · Zbl 0783.01020

[16] DOI: 10.1017/CBO9781139084437 · Zbl 1252.14001 · doi:10.1017/CBO9781139084437

[17] DOI: 10.1007/BF01393371 · Zbl 0506.14016 · doi:10.1007/BF01393371

[18] DOI: 10.1016/0001-8708(87)90010-7 · Zbl 0668.14006 · doi:10.1016/0001-8708(87)90010-7

[19] DOI: 10.1007/978-3-642-36334-4_16 · Zbl 1305.94053 · doi:10.1007/978-3-642-36334-4_16

[20] DOI: 10.1016/S1071-5797(03)00039-X · Zbl 1091.11023 · doi:10.1016/S1071-5797(03)00039-X

[21] Gross, Contributions to automorphic forms, geometry, and number theory pp 279– (2004)

[22] DOI: 10.1007/s00209-007-0173-9 · Zbl 1132.14011 · doi:10.1007/s00209-007-0173-9

[23] Bergström, J. reine angew. Math. 622 pp 155– (2008)

[24] DOI: 10.1080/00927879708825947 · Zbl 0888.20013 · doi:10.1080/00927879708825947

[25] Girard, Algorithmic number theory. 7th International Symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006 4076 pp 346– (2006)

[26] DOI: 10.2307/2372670 · Zbl 0072.16001 · doi:10.2307/2372670

[27] DOI: 10.1007/s00013-012-0427-6 · Zbl 1267.14040 · doi:10.1007/s00013-012-0427-6

[28] DOI: 10.1007/978-3-0348-8399-3_3 · doi:10.1007/978-3-0348-8399-3_3

[29] DOI: 10.1007/978-3-540-24847-7_29 · doi:10.1007/978-3-540-24847-7_29

[30] Newstead, Introduction to moduli problems and orbit spaces (1978) · Zbl 0411.14003

[31] DOI: 10.1016/j.ffa.2010.06.001 · Zbl 1254.11064 · doi:10.1016/j.ffa.2010.06.001

[32] Magaard, Communications in arithmetic fundamental groups 1267 pp 112– (2002)

[33] DOI: 10.1080/00927878008822521 · Zbl 0454.14007 · doi:10.1080/00927878008822521

[34] Katz, Random matrices, Frobenius eigenvalues, and monodromy (1999) · Zbl 0958.11004