JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jaap TOP et Carlo VERSCHOOR

Counting points on the Fricke–Macbeath curve over finite fields

Tome 30, n$^{\text{o}}$ 1 (2018), p. 117-129.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_1_117_0>

Journal de Théorie des Nombres de Bordeaux **30** (2018), 117–129

Counting points on the Fricke–Macbeath curve over finite fields

par Jaap TOP et Carlo VERSCHOOR

Résumé. La courbe de Fricke-Macbeath est une courbe projective lisse de genre 7 avec groupe d'automorphismes $\mathrm{PSL}_2(\mathbb{F}_8)$. Nous rappelons deux modèles de cette courbe (introduits respectivement par Maxim Hendriks et Bradley Brock) définis sur $\mathbb{Q}$, et nous établissons un isomorphisme explicite, défini sur $\mathbb{Q}(\sqrt{-7})$, entre ces deux modèles. De plus, nous décomposons à isogénie sur $\mathbb{Q}$ près la jacobienne de l'un des modèles. Comme une conséquence nous obtenons une formule simple pour le nombre de points sur $\mathbb{F}_q$ de (la réduction de) ce modèle, en termes de la courbe elliptique d'équation $y^2 = x^3 + x^2 - 114x - 127$. Enfin, des tordus de cette courbe par des éléments de $\mathrm{PSL}_2(\mathbb{F}_8)$ sur des corps finis sont décrits. La courbe donne un certain nombre de nouveaux records maintenus par `manYPoints` de courbes de genre 7 avec beaucoup de points rationnels sur des corps finis.

Abstract. The Fricke-Macbeath curve is a smooth projective algebraic curve of genus 7 with automorphism group $\mathrm{PSL}_2(\mathbb{F}_8)$. We recall two models of it (introduced, respectively, by Maxim Hendriks and by Bradley Brock) defined over $\mathbb{Q}$, and we establish an explicit isomorphism defined over $\mathbb{Q}(\sqrt{-7})$ between these models. Moreover, we decompose up to isogeny over $\mathbb{Q}$ the jacobian of one of these models. As a consequence we obtain a simple formula for the number of points over $\mathbb{F}_q$ on (the reduction of) this model, in terms of the elliptic curve with equation $y^2 = x^3 + x^2 - 114x - 127$. Moreover, twists by elements of $\mathrm{PSL}_2(\mathbb{F}_8)$ of the curve over finite fields are described. The curve leads to a number of new records as maintained on `manYPoints` of curves of genus 7 with many rational points over finite fields.

Manuscrit reçu le 24 mars 2016, révisé le 1$^{\text{er}}$ septembre 2016, accepté le 17 octobre 2016.

2010 *Mathematics Subject Classification.* 11N56, 14G42.

Mots-clefs. Hurwitz curve, automorphism group, jacobian, point counting.

It is our pleasure to thank the referee of this paper; a number of questions and suggestions they made did hopefully lead to improvements of some of the originally maybe too brief exposition. Moreover we are grateful to Brad Brock and to Everett Howe for generously sharing some of their ideas and results with us.

1. Introduction

It is well-known that an algebraic curve of genus $g > 1$ over $\mathbb{C}$ has at most $84(g-1)$ automorphisms. A curve attaining this bound is called a Hurwitz curve. The corresponding Riemann surface can in this case be described as $\Gamma\ \mathcal{H}$ in which Γ is a normal subgroup of finite index in the triangle group $G_{2,3,7}$, acting in the classical way on the complex upper half plane $\mathcal{H}$. See, e.g., §3.19 of Shimura's paper [15] and §5.3 of the exposition by Elkies [3] for details. The plane curve with equation $x^3y+y^3z+z^3z=0$, named after Felix Klein who studied it in 1879 in his paper [10], is the unique example up to isomorphisms for genus $g=3$. The next example occurs for $g=7$ and was introduced as a Riemann surface by Robert Fricke in 1899 [4]. Explicit equations realizing Fricke's example as an algebraic curve were presented in 1965 by A.M. Macbeath [11]; see also W.L. Edge's paper [2] which appeared two years later. Again, up to isomorphisms over $\mathbb{C}$ there is a unique curve of genus 7 admitting 504 automorphisms; here and elsewhere it is called the Fricke-Macbeath curve. Whereas Edge derives the equations first presented by Macbeath by starting from the property that they need to define a curve in $\mathbb{P}^6$ having a given subgroup of order 504 in $\mathrm{PGL}_7(\mathbb{C})$ as automorphism group, there is an alternative, very natural way to find the curve, as is explained in a letter dated 24-vii-1990 of J-P. Serre to S.S. Abhyankar [14]. Namely, Serre observes that $G = \mathrm{PSL}_2(\mathbb{F}_8)$ is a transitive subgroup of the alternating group A_9 (which in fact follows from the action of G on the 9 points in $\mathbb{P}^1(\mathbb{F}_8)$). The stabilizer $S \subset G$ of any of these 9 points then makes $X \to X/G$ the normal closure of $X/S \to X/G$, where we denote the desired curve as X. Both X/S and X/G are rational curves, and the ramification of the resulting degree 9 map $\mathbb{P}^1 \to \mathbb{P}^1$ is known and occurs only over three points. This information suffices to determine the degree 9 map explicitly, and hence to find the curve X.

The equations described by Macbeath (and explained in detail by Edge) define a curve $M \subset \mathbb{P}^6$, given (with ζ a primitive 7th root of unity) by the ideal with generators

$$\begin{array}{l}
M: \\
x_0^2+x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2, \\
x_0^2+\zeta x_1^2+\zeta^2x_2^2+\zeta^3x_3^2+\zeta^4x_4^2+\zeta^5x_5^2+\zeta^6x_6^2, \\
x_0^2+\zeta^6x_1^2+\zeta^5x_2^2+\zeta^4x_3^2+\zeta^3x_4^2+\zeta^2x_5^2+\zeta x_6^2, \\
(\zeta^5-\zeta^2)\,x_1x_4+(\zeta^6-\zeta)\,x_3x_5+(-\zeta^4+\zeta^3)\,x_0x_6, \\
(-\zeta^4+\zeta^3)\,x_0x_1+(\zeta^5-\zeta^2)\,x_2x_5+(\zeta^6-\zeta)\,x_4x_6, \\
(-\zeta^4+\zeta^3)\,x_1x_2+(\zeta^6-\zeta)\,x_0x_5+(\zeta^5-\zeta^2)\,x_3x_6, \\
(-\zeta^4+\zeta^3)\,x_2x_3+(\zeta^5-\zeta^2)\,x_0x_4+(\zeta^6-\zeta)\,x_1x_6, \\
(\zeta^6-\zeta)\,x_0x_2+(-\zeta^4+\zeta^3)\,x_3x_4+(\zeta^5-\zeta^2)\,x_1x_5, \\
(\zeta^6-\zeta)\,x_1x_3+(-\zeta^4+\zeta^3)\,x_4x_5+(\zeta^5-\zeta^2)\,x_2x_6, \\
(\zeta^5-\zeta^2)\,x_0x_3+(\zeta^6-\zeta)\,x_2x_4+(-\zeta^4+\zeta^3)\,x_5x_6.
\end{array}$$

A consequence of a very general criterion of Girondo, Torres-Teigell, and Wolfart [6] is that it is possible to define the Fricke-Macbeath curve as an algebraic curve over $\mathbb{Q}$. As part of his PhD research, Maxim Hendriks in Eindhoven did exactly this. He presented in his thesis [7, p. 192–194] a curve $H \subset \mathbb{P}^6$ given as an intersection of 10 quadrics. Generators of the ideal defining H are

$$\begin{array}{l}
H: \\
-x_1x_2 + x_1x_0 + x_2x_6 + x_3x_4 - x_3x_5 - x_3x_0 - x_4x_6 - x_5x_6, \\
x_1x_3 + x_1x_6 - x_2^2 + 2x_2x_5 + x_2x_0 - x_3^2 + x_4x_5 - x_4x_0 - x_5^2, \\
x_1^2 - x_1x_3 + x_2^2 - x_2x_4 - x_2x_5 - x_2x_0 - x_3^2 + x_3x_6 + 2x_5x_0 - x_0^2, \\
x_1x_4 - 2x_1x_5 + 2x_1x_0 - x_2x_6 - x_3x_4 - x_3x_5 + x_5x_6 + x_6x_0, \\
x_1^2 - 2x_1x_3 - x_2^2 - x_2x_4 - x_2x_5 + 2x_2x_0 + x_3^2 + x_3x_6 + x_4x_5 + x_5^2 - x_5x_0 - x_6^2, \\
x_1x_2 - x_1x_5 - 2x_1x_0 + 2x_2x_3 - x_3x_0 - x_5x_6 + 2x_6x_0, \\
-2x_1x_2 - x_1x_4 - x_1x_5 + 2x_1x_0 + 2x_2x_3 - 2x_3x_0 + 2x_5x_6 - x_6x_0, \\
2x_1^2 + x_1x_3 - x_1x_6 + 3x_2x_0 + x_4x_5 - x_4x_0 - x_5^2 + x_6^2 - x_0^2, \\
2x_1^2 - x_1x_3 + x_1x_6 + x_2^2 + x_2x_0 + x_3^2 - 2x_3x_6 + x_4x_5 - x_4x_0 + x_5^2 - 2x_5x_0 + x_6^2 + x_0^2, \\
x_1^2 + x_1x_3 - x_1x_6 + 2x_2x_5 - 3x_2x_0 + 2x_3x_6 + x_4^2 + x_4x_5 - x_4x_0 + x_6^2 + 3x_0^2.
\end{array}$$

Moreover Hendriks presents an explicit isomorphism between M and H (see also Theorem 2.1 below).

In §2.3 of a recent paper by Rubén Hidalgo [8], another model over $\mathbb{Q}$ of the Fricke-Macbeath curve is mentioned. It is attributed to Bradley Brock, and given by the affine equation in two variables

$$1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0.$$

One readily calculates that this curve in $\mathbb{A}^2$ has as singularities 14 nodes, and its closure in $\mathbb{P}^2$ has no singular points at infinity. So indeed the equation defines a curve of genus 7. Using a basis of the regular 1-forms on the normalization, one obtains an embedding of the curve in $\mathbb{P}^6$. The resulting curve $B \subset \mathbb{P}^6$ can be given as follows (here and in other calculations Magma [1] was used).

$$\begin{array}{l}
B: \\
x_0x_2 + 12x_3^2 - x_4x_6, \\
-x_1^2 + x_0x_3 - 2x_5x_6, \\
x_0x_4 + 16x_3x_5 + 8x_6^2, \\
-x_1x_3 + x_0x_5 + \frac{1}{2}x_2x_6, \\
-x_2x_3 + 2x_5^2 + x_0x_6, \\
x_1x_2 + 12x_3x_5 + 4x_6^2, \\
-2x_2x_3 + x_1x_4 - 8x_5^2, \\
-x_3^2 + x_1x_5 + \frac{1}{4}x_4x_6, \\
-\frac{1}{2}x_3x_4 - \frac{1}{2}x_2x_5 + x_1x_6, \\
x_2^2 + 2x_4x_5 + 8x_3x_6.
\end{array}$$

We learned from Brock that in fact he found the above model already in 2004. He discussed it with various colleagues including Macbeath and Elkies; however, he never published it.

Several, but not all computational results mentioned in this paper were obtained using Sage or Magma. The actual code is not presented here; in a number of cases it can be found in Appendix A of the master's thesis [17]. The interested reader should be aware that this code was written for particular versions of Sage (and Magma). Specific details and requests for parts of the code may be addressed to the authors.

2. Results

This section states the main results of this paper; proofs are presented in Section 3 below.

First, we present explicit isomorphisms between the curves M, H, and B.

Theorem 2.1 (Hendriks, [7])**.** *With notations as in the previous section and $\alpha := \zeta + \zeta^{-1}$, an isomorphism $M \to H$ is given by $m \mapsto Am$, with* $7A =$

$$\begin{pmatrix} 0 & 0 & \alpha^2-\alpha-2 & -\alpha^2-\alpha-1 & 0 & 2\alpha^2-1 & 0 \\ \alpha^2-2\alpha & 0 & 0 & 0 & 3\alpha+1 & 0 & -\alpha^2-2\alpha+1 \\ 0 & 0 & -\alpha^2-\alpha-1 & -2\alpha^2+1 & 0 & \alpha^2-\alpha-2 & 0 \\ 0 & 7\alpha & 0 & 0 & 0 & 0 & 0 \\ -\alpha^2-2\alpha+1 & 0 & 0 & 0 & -\alpha^2+2\alpha & 0 & -3\alpha-1 \\ 0 & 0 & -3\alpha-1 & -\alpha^2+2\alpha & 0 & \alpha^2+2\alpha-1 & 0 \\ -3\alpha-1 & 0 & 0 & 0 & \alpha^2+2\alpha-1 & 0 & \alpha^2-2\alpha \end{pmatrix}.$$

Remark. In fact, the matrix A given above does not appear in the thesis of Hendriks. He presents a different one called U on page 193 of [7].

Theorem 2.2. *With notations as in the previous section, an isomorphism $B \to H$ is given by $b \mapsto A'b$, with*

$$A' = \frac{1}{2}\begin{pmatrix} 2 & -8 & 4 & -24 & 1 & 24 & 0 \\ 2\sqrt{-7} & -4\sqrt{-7} & -2\sqrt{-7} & 0 & -\sqrt{-7} & 0 & -8\sqrt{-7} \\ 6 & 4 & -2 & -16 & 3 & 16 & 0 \\ 2\sqrt{-7} & -4\sqrt{-7} & -2\sqrt{-7} & -8\sqrt{-7} & -\sqrt{-7} & -8\sqrt{-7} & 16\sqrt{-7} \\ 0 & -4\sqrt{-7} & -2\sqrt{-7} & -8\sqrt{-7} & 0 & -8\sqrt{-7} & -8\sqrt{-7} \\ -2 & 8 & -4 & -32 & -1 & 32 & 0 \\ 2\sqrt{-7} & 0 & 0 & -8\sqrt{-7} & -\sqrt{-7} & -8\sqrt{-7} & -8\sqrt{-7} \end{pmatrix}.$$

Note that Theorems 2.1 and 2.2 imply that the three curves M, H, and B are isomorphic over $\mathbb{Q}(\zeta)$. Although both H and B are defined over $\mathbb{Q}$, they are not isomorphic over $\mathbb{Q}$. This follows, e.g., from the fact that both have good reduction modulo 3, and $\#H(\mathbb{F}_3) = 3 \neq 5 = \#B(\mathbb{F}_3)$.

From now on we focus on the model H presented by Hendriks. Our aim is to describe the jacobian $\mathrm{Jac}(H)$ up to isogenies defined over $\mathbb{Q}$, in terms of jacobians of certain quotients of H. To this end, let $X \subset \mathbb{P}^2$ be the plane quartic of genus 3 defined by

$$\begin{aligned} X : \ & 5x^4 + 12x^3y + 6x^2y^2 - 4xy^3 + 4y^4 - 28x^3z + 16x^2yz - 24xy^2z \\ & + 16y^3z + 24x^2z^2 - 10y^2z^2 - 12xz^3 + 8yz^3 + 3z^4. \end{aligned}$$

Furthermore let E be the elliptic curve with equation

$$y^2 = x^3 + x^2 - 114x - 127.$$

The curve X turns out to be birational to the quotient of H by the involution defined by $\mathrm{Diag}(1, -1, 1, -1, -1, 1, -1)$. It is the image of H under $(x_0 : x_1 : x_2 : x_3 : x_4 : x_5 : x_6) \mapsto (x_0 : x_2 : x_5)$. The elliptic curve E is obtained as a quotient of H by a group of order 7. Such a quotient was also described by Klaus Wohlfahrt in the corrigendum to his paper [18]. His elliptic curve is in fact the quadratic twist by $\sqrt{-7}$ of E. The reader may verify that a very simple way to find the same elliptic curve as Wohlfahrt did, is by starting from the affine plane model of the Fricke-Macbeath curve given by Brock. Taking the quotient by $(x, y) \mapsto (\zeta x, \zeta^{-1} y)$ yields Wohlfahrt's elliptic curve.

Theorem 2.3. $\mathrm{Jac}(H)$ *is isogenous over* $\mathbb{Q}$ *to* $\mathrm{Jac}(X) \times \mathrm{Jac}(X) \times E$.

The next goal will be to analyse $\mathrm{Jac}(X)$. It turns out that $\mathrm{Aut}(X)$ contains a group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with involutions defined over $\mathbb{Q}(\alpha)$. Moreover, these involutions are permuted by $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Let σ be a generator of this (cyclic) Galois group of order 3. The quotient of X by one of the involutions turns out to be a genus one curve C over $\mathbb{Q}(\alpha)$, with jacobian E' isogenous, again over $\mathbb{Q}(\alpha)$, to E. The action of σ yields the jacobians of the three quotients of X by the involutions. The restriction of scalars $\mathrm{Res}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(E')$, which is over $\mathbb{Q}(\alpha)$ isomorphic to $E' \times \sigma(E') \times \sigma^2(E')$, is the abelian threefold over $\mathbb{Q}$ we look for.

Theorem 2.4. $\mathrm{Jac}(X)$ *is over* $\mathbb{Q}$ *isogenous to* $\mathrm{Res}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(E')$*, and the elliptic curves* E *and* E' *are isogenous over* $\mathbb{Q}(\alpha)$*.*

A straightforward consequence of Theorem 2.4 is a formula for $\#X(\mathbb{F}_q)$, for $q = p^n$ and p a prime $\neq 2, 7$:

Corollary 2.5. *The curve* X *has good reduction modulo every prime number* $p \neq 2, 7$*. If* $q = p^n$ *is a positive power of such a prime* p*, then*

$$\#X(\mathbb{F}_q) = \begin{cases} q + 1 & \text{if } q \not\equiv \pm 1 \bmod 7; \\ 3\#E(\mathbb{F}_q) - 2q - 2 & \text{if } q \equiv \pm 1 \bmod 7. \end{cases}$$

Combining Theorem 2.3 and Corollary 2.5 leads to the main result of this paper:

Theorem 2.6. *The curve* H *has good reduction modulo every prime number* $p \neq 2, 7$*. If* $q = p^n$ *is a positive power of such a prime* p*, then*

$$\#H(\mathbb{F}_q) = \begin{cases} \#E(\mathbb{F}_q) & \text{if } q \not\equiv \pm 1 \bmod 7; \\ 7\#E(\mathbb{F}_q) - 6q - 6 & \text{if } q \equiv \pm 1 \bmod 7. \end{cases}$$

Somewhat similar results to the ones presented in Corollary 2.5 and Theorem 2.6, but for curves of smaller genus, are presented in Chapter 4 of the PhD thesis [16]. In the next section the results described above are proven. In Section 4 we apply Theorem 2.6 to some particular prime powers q, resulting in various new records in the tables [5] maintained on `manYPoints` of curves with many points over finite fields. In the same section we describe twists of $H/\mathbb{F}_q$ and we show examples where these lead to new records as well.

Most results of this paper were obtained during the master's project of the second author [17], supervised by the first author.

3. Proofs

The statements in Theorem 2.1 and in Theorem 2.2 can be easily verified, so we omit this here. Instead, some comments are presented explaining how the isomorphisms were found. By construction, the curves M, H, and B are canonically embedded curves in $\mathbb{P}^6$. Hence an isomorphism between two of these curves is necessarily given by an element of $\mathrm{PGL}_7(\overline{\mathbb{Q}})$. Conjugation by this element then yields an isomorphism from the automorphism group of one curve to that of the other. By first determining such a conjugation, i.e., an $A \in \mathrm{PGL}_7(\overline{\mathbb{Q}})$ satisfying $A\alpha_1 = \alpha_2 A$ with α_1 running over the generators of some subgroup of the automorphisms of one curve, and the α_2 analogous generators of an isomorphic subgroup coming from the other curve, the isomorphisms were determined.

To make this explicit, consider the generators T, W of $\mathrm{Aut}(M) \subset \mathrm{PGL}_7(\mathbb{Q})$, defined as

$$T = \begin{pmatrix} -1 & 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 & -1 \\ 0 & 1 & -1 & 1 & 0 & 1 & 0 \\ -1 & -1 & -1 & 0 & -1 & 0 & 0 \\ -1 & 1 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 & -1 & -1 & -1 \end{pmatrix},$$

$$W = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then $T^3 = W^7 = (TW)^2 = id$. Corresponding generators R, S of $\mathrm{Aut}(H)$ satisfying $R^3 = S^7 = (SR)^2 = id$ one finds using p. 192-193 of the thesis of

Hendriks [7]. With $\alpha = \zeta + \zeta^{-1}$ as before, they are $R :=$

$$\left(\begin{matrix} 2\alpha^2+3\alpha-7 & 3\alpha^2+4\alpha+1 & 4\alpha^2+2\alpha-6 & -\alpha^2+\alpha+2 \\ 4\alpha^2+8\alpha-4 & 4\alpha^2+\alpha-11 & -9\alpha^2-3\alpha+14 & 2\alpha^2+\alpha-3 \\ 2\alpha^2+4\alpha-2 & 6\alpha^2+3\alpha-9 & \alpha^2+\alpha-6 & -2\alpha^2-\alpha+3 \\ 14\alpha^2+7\alpha-21 & 7\alpha+7 & -7\alpha^2+7\alpha+14 & 0 \\ 6\alpha^2+9\alpha-7 & 5\alpha^2-\alpha-4 & -11\alpha^2-7\alpha+16 & -\alpha^2-2\alpha+1 \\ 6\alpha^2-10 & 3\alpha^2-5 & 4\alpha^2+8\alpha-4 & -\alpha^2-3 \\ 4\alpha^2+11\alpha-3 & 5\alpha^2-13 & -8\alpha^2-4\alpha+12 & -\alpha^2+\alpha+2 \end{matrix}\right. \quad \cdots$$

$$\cdots \quad \left.\begin{matrix} -4\alpha^2-3\alpha+1 & -7\alpha^2-5\alpha+10 & 3\alpha^2-3\alpha-6 \\ -5\alpha^2-5\alpha+2 & -2\alpha^2-\alpha+3 & \alpha^2+6\alpha+5 \\ -\alpha^2+3\alpha-2 & -2\alpha^2-7\alpha+1 & -\alpha^2-4\alpha+5 \\ 7\alpha^2-7 & 0 & -7\alpha^2-7\alpha+14 \\ -3\alpha^2-4\alpha-1 & \alpha^2+2\alpha-1 & 5\alpha-3 \\ -4\alpha^2+2 & -3\alpha^2-4\alpha-1 & 3\alpha^2-5 \\ -6\alpha^2-5\alpha+13 & \alpha^2-\alpha-2 & -\alpha^2+3\alpha-2 \end{matrix}\right)$$

and $S :=$

$$\left(\begin{matrix} -\alpha^2+4 & -\alpha-5 & 2\alpha^2+2\alpha-5 & 0 \\ 3\alpha+1 & -\alpha^2-2\alpha+1 & -2\alpha^2-3\alpha & \alpha-2 \\ 2\alpha+3 & \alpha^2-4 & 2\alpha^2+\alpha-3 & 0 \\ -7\alpha^2+14 & 0 & -7\alpha & 0 \\ -\alpha^2+2\alpha & -3\alpha-1 & -2\alpha^2-\alpha+3 & \alpha^2-4 \\ 2\alpha^2+3\alpha & 5\alpha^2+2\alpha-10 & -\alpha^2+\alpha+2 & 0 \\ \alpha^2+2\alpha-1 & \alpha^2-2\alpha & -3\alpha^2-3\alpha+4 & -\alpha^2-\alpha-1 \end{matrix}\right. \quad \cdots$$

$$\cdots \quad \left.\begin{matrix} -\alpha+2 & -2\alpha^2-\alpha+3 & -\alpha+2 \\ -3\alpha^2-\alpha+7 & \alpha^2+\alpha+1 & 3\alpha^2+3\alpha-4 \\ \alpha^2+3 & -\alpha^2-2\alpha+1 & \alpha^2-4 \\ 0 & -7 & 0 \\ -\alpha^2+\alpha+2 & -\alpha+2 & 2\alpha^2+3\alpha \\ -2\alpha^2-5\alpha+4 & -\alpha^2-\alpha-1 & -2\alpha^2+2\alpha+4 \\ -3\alpha^2+5 & -\alpha^2+4 & 2\alpha^2+\alpha-3 \end{matrix}\right)$$

Solving for the matrix A in the linear equations $RA = AT, SA = AW$ then results in the desired isomorphism.

In the case of the curves B and H, the only obvious automorphisms of B form a dihedral group of order 14. On the plane model, this group is generated by $(x, y) \mapsto (y, x)$ and $(x, y) \mapsto (\zeta x, \zeta^{-1} y)$. On B this yields the matrices

$$D := \mathrm{Diag}(\zeta^5, \zeta^3, \zeta^4, \zeta, \zeta^2, \zeta^6, 1)$$

and

$$F := \begin{pmatrix} 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

as can be found by considering the action of the two given automorphisms on a basis of the regular differentials of the curve. A corresponding dihedral group in $\mathrm{Aut}(H)$ is the one with generators

$$\tau := (S^{-1}RS^{-1})^2RS = \mathrm{Diag}(-1,1,-1,1,1,-1,1)$$

and $L := (S^{-2}R)^2S^{-1}$, given by $14L :=$

$$\left(\begin{matrix} -4\alpha^2-\alpha+4 & 3\alpha^2-12 & 4\alpha^2+2\alpha-6 & -\alpha^2+\alpha+2 \\ -2\alpha^2-6\alpha+6 & -3\alpha-1 & 7\alpha^2+7\alpha-7 & -\alpha-5 \\ 2\alpha^2+4\alpha-2 & -2\alpha^2-5\alpha-3 & 5\alpha^2-\alpha-11 & -2\alpha^2-\alpha+3 \\ -7\alpha & -7\alpha-7 & 7\alpha^2+7\alpha-7 & 7 \\ -7\alpha & -3\alpha^2-7\alpha+5 & \alpha^2+3\alpha-3 & -\alpha^2-3 \\ 4\alpha^2+8\alpha-4 & 5\alpha^2-4\alpha-12 & -4\alpha^2-2\alpha+6 & -\alpha^2+4 \\ 2\alpha^2-\alpha-6 & 3\alpha^2-4\alpha-4 & 6\alpha^2+4\alpha-4 & \alpha^2+\alpha-6 \end{matrix}\right. \quad \cdots$$

$$\cdots \quad \left.\begin{matrix} -4\alpha^2 5\alpha+4 & \alpha^2+5\alpha & -5\alpha^2-3\alpha+12 \\ -7\alpha^2-3\alpha+13 & -2\alpha^2+\alpha-1 & 7\alpha^2+4\alpha-8 \\ 3\alpha^2+3\alpha+3 & -4\alpha^2+\alpha+7 & -5\alpha^2+6 \\ -7\alpha^2+7 & -7 & 7\alpha^2+7\alpha-14 \\ -3\alpha^2+5 & 3\alpha^2+2\alpha-9 & 4\alpha^2+7\alpha-2 \\ -6\alpha^2-2\alpha+14 & -\alpha^2+2\alpha & -\alpha^2+6\alpha+6 \\ -4\alpha^2+3\alpha+10 & -\alpha^2-3\alpha-4 & 3\alpha^2+3\alpha-4 \end{matrix}\right).$$

Solving the system $\tau A' = A'F$, $LA' = A'D$ for the matrix A' yields the map given in Theorem 2.2.

We will now prove Theorem 2.3. Let π denote the projection $(x_0 : \ldots : x_6) \mapsto (x_0 : x_2 : x_5)$, with $\pi(H) = X$. Let $\omega_1, \omega_2, \omega_3$ be a basis for the space of regular differentials $H^0(X, \Omega^1)$. A calculation (compare [17, p. 27–28]) shows that $\pi^*\omega_1, \pi^*\omega_2, \pi^*\omega_3, \tau^*\pi^*\omega_1, \tau^*\pi^*\omega_2, \tau^*\pi^*\omega_3$ are linearly independent in $H^0(H, \Omega^1)$. Hence

$$(\pi, \pi\tau) \;:\; H \to X \times X$$

induces a homomorphism $\mathrm{Jac}(X) \times \mathrm{Jac}(X) \to \mathrm{Jac}(H)$ with finite kernel (see [12, Section 3.3] for more information). Consequenctly, the cokernel is an abelian variety of dimension 1 defined over $\mathbb{Q}$, i.e., it is an elliptic curve over $\mathbb{Q}$. We briefly sketch two methods to find an equation for this elliptic curve (in the first case, up to isogeny over $\mathbb{Q}$).

For the first method, observe that the curve B (and hence also H) has good reduction except at the primes 2 and 7. A convenient way to verify this, is by using the plane model of B: one needs to verify that the 14 nodes that appear as singularities of B in characteristic zero, reduce to nodes in positive characteristic $\neq 2$, $\neq 7$ and that no new singularities appear. A consequence of this is, that the desired elliptic curve has good reduction away from 2 and 7. So its conductor divides $2^8 \cdot 7^2$. Moreover, by construction the number of rational points on this elliptic curve over $\mathbb{F}_p$ for a prime $p \neq 2, 7$ equals

$$\#H(\mathbb{F}_p) - 2\#X(\mathbb{F}_p) + 2p + 2.$$

This information suffices to determine the correct isogeny class among the finitely many possible ones.

Alternatively, and more geometrically, take $\rho := (SR^{-1}S)^3$ which is an automorphism defined over the ground field, of order 3. A calculation (for details, compare [17, p. 13–15]) reveals that $H/\langle\rho\rangle$ is a curve of genus 1, given by $y^2 = -7t^4 - 28t^3 - 56t^2 - 28$. The jacobian of this curve is our curve E. Since ρ^* fixes no differentials in the subspace of $H^0(X, \Omega^1)$ spanned by $\pi^*\omega_1, \pi^*\omega_2, \pi^*\omega_3, \tau^*\pi^*\omega_1, \tau^*\pi^*\omega_2, \tau^*\pi^*\omega_3$, it follows that $\mathrm{Jac}(H) \sim \mathrm{Jac}(X) \times \mathrm{Jac}(X) \times E$.

Next we prove Theorem 2.4. For this, one observes that X admits over $\mathbb{Q}(\alpha)$ the involution given by

$$A := \frac{1}{7}\begin{pmatrix} -4\alpha^2 - 4\alpha + 3 & -2\alpha^2 + 2\alpha + 4 & 4\alpha^2 + 2\alpha - 6 \\ -4\alpha^2 - 2\alpha + 6 & 2\alpha^2 + 2\alpha - 5 & 2\alpha^2 + 4\alpha - 2 \\ 2\alpha^2 - 2\alpha - 4 & 6\alpha + 2 & 2\alpha^2 + 2\alpha - 5 \end{pmatrix}.$$

Moreover, A and its conjugates $\sigma(A)$ and $\sigma^2(A)$ generate a group of automorphisms of X isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The quotient of X by any nontrivial element of this group turns out to be an elliptic curve over $\mathbb{Q}(\alpha)$, and the three elliptic curves obtained in this way are obviously conjugate. There are no nontrivial regular differentials on X fixed by all three involutions. This suffices to conclude that $\mathrm{Jac}(X)$ is isogenous over $\mathbb{Q}$ to the restriction of scalars of any of the three elliptic curves. The elliptic curve E has its three points of order 2 defined over $\mathbb{Q}(\alpha)$. The 2-isogenies resulting from this, turn out to have as image curves exactly the three elliptic curves we found as quotients of X. This proves Theorem 2.4.

Corollary 2.5 is an immediate consequence of Theorem 2.4. The statement concerning good reduction is easily verified. In the case $q \equiv \pm 1 \bmod 7$, all 7th roots of unity exist in $\mathbb{F}_{q^2}$ and hence $\mathbb{F}_q$ contains the residue class field at the primes dividing q of $\mathbb{Q}(\alpha)$. As a consequence, $\mathrm{Jac}(X)$ is isogenous over $\mathbb{F}_q$ to $E \times E \times E$, from which the formula for the number of points in this case is immediate. For $q \not\equiv \pm 1 \bmod 7$, the residue class field of $\mathbb{Q}(\alpha)$ at primes dividing q is not contained in $\mathbb{F}_q$ but in its cubic extension. Hence the qth power Frobenius permutes the reductions of the three curves $E', \sigma(E')$, and $\sigma^2(E')$. This implies that the trace of Frobenius on $\mathrm{Res}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(E')$ is zero, implying the remaining formula.

$$\begin{tikzcd}
T_\ell\sigma(E') \arrow[dddd, bend right, "\mathrm{Frob}_q"'] & & & \\
& \sigma(E') \arrow[dd, bend right] & & \\
& & E' \arrow[ul, bend right] & T_\ell E' \arrow[ulll, bend right, "\mathrm{Frob}_q"'] \\
& \sigma^2(E') \arrow[ur, bend right] & & \\
T_\ell\sigma^2(E') \arrow[urrr, bend right, "\mathrm{Frob}_q"'] & & &
\end{tikzcd}$$

This completes the proof of the results presented in Section 2.

4. Examples and twists

The website `manYPoints` [5] lists, for small genera g and small cardinalities q of a finite field, an upper bound `up` for the cardinality $\#C(\mathbb{F}_q)$ of any smooth, complete and absolutely irreducible curve C of genus g defined over $\mathbb{F}_q$. In many instances this is the Hasse–Weil–Serre bound $q + 1 + gm$, in which m is the largest integer $\leq \sqrt{4q}$. In case a curve reaching this bound is known to exist, this means the number $N_q(g)$, denoting the maximum over all such cardinalities $\#C(\mathbb{F}_q)$ for fixed g, q is determined. If no curve reaching the upper bound is known then the tables aim to list an example with at least $\mathtt{up}/\sqrt{2}$ rational points. For instance, using Corollary 2.5 one readily verifies that for $q = 71^2$, the genus 3 curve X reaches the Hasse–Weil–Serre bound, so $N_{71^2}(3) = 5468$. We now list the cases in which the curve H provides an example with at least $\mathtt{up}/\sqrt{2}$ points. Instances where an example with at least as many points is known, will be ignored. Somewhat surprisingly, even with $q \not\equiv \pm 1 \bmod 7$, in which case Theorem 2.6 shows that H has (only) as many rational points as the elliptic curve E, some new entries were found. While new lower bounds for several larger field sizes q were found, there is no reason to think that they are anywhere near the best possible lower bounds.

q	3^3	5^3	5^5	11^5	13^2	13^3	13^4	13^5
$\mathtt{up}$	95	277	3903	166666	352	2849	30928	379820
$\lceil \mathtt{up}/\sqrt{2} \rceil$	68	196	2760	117851	249	2015	21870	268574
$\#H(\mathbb{F}_q)$	84	252	3183	161625	324	2688	27540(*)	362880(*)

q	17^3	17^5	19^4	19^5	29	97
$\mathtt{up}$	5892	1436539	135376	2498129	100	231
$\lceil \mathtt{up}/\sqrt{2} \rceil$	4167	1015787	95726	1766444	71	164
$\#H(\mathbb{F}_q)$	5796	1417575	129675(*)	2477811	72	168

In a sense the "smallest" example here is $\#H(\mathbb{F}_{27}) = 84$. The previous record for $q = 27$ and $g = 7$ was obtained by Sémirat [13] in 2000, who found an example having 82 rational points. The three marked $(*)$ entries show examples which we will improve now, as follows.

A natural attempt to obtain more examples with many points from the curve H, is to consider twists of it over $\mathbb{F}_q$, i.e., curves over the same field which are isomorphic to H over some extension field. We refer to [12], in particular Sections 2-3 for some general theory concerning twists. The twists over $\mathbb{F}_q$ are in $1-1$ correspondence with $H^1(\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q), \mathrm{Aut}(H))$, and the latter set allows a natural bijection to the set of "Frobenius conjugacy classes" in $\mathrm{Aut}(H)$.

In our case, we consider $H^1(\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q), G)$, with $G \subset \mathrm{PGL}_7(\overline{\mathbb{F}_q})$ the simple group of order 504 acting as automorphisms on H. These automorphisms are defined over $\mathbb{F}_q(\zeta + \zeta^{-1})$ with ζ a primitive 7th root of unity. Hence the Galois action on G is trivial precisely when $q \equiv \pm 1 \bmod 7$. In this case, Frobenius conjugacy classes coincide with ordinary conjugacy classes, and there are 9 of these. For $q \not\equiv \pm 1 \bmod 7$ a calculation with Magma shows that there exist only 3 Frobenius conjugacy classes.

If an automorphism β defines some Frobenius conjugacy class, then the corresponding cocycle class is represented by the cocycle defined by $\mathrm{Frob}_q \mapsto \beta$. It defines a twist H^{tw}, and by construction rational points on this twist correspond to points $P \in H(\overline{\mathbb{F}_q})$ such that $\beta(\mathrm{Frob}_q(P)) = P$. This allows one to calculate effectively, for given q and β, the number of rational points $\#H^{\mathrm{tw}}(\mathbb{F}_q)$. Namely, as the proof of Proposition 9 in [12] explains, one has an *a priori* bound on the degree over $\mathbb{F}_q$ of the field of definition of any point P with $\beta(\mathrm{Frob}_q(P)) = P$.

Ignoring the trivial twist which results in the curve H itself, we can improve 3 of the records presented in the earlier table. They are given below.

(1) $q = 13^4 \equiv 1 \bmod 7$. The (cubic) twist corresponding to $\mathrm{Frob}_q \mapsto R$ has 28854 rational points. This exceeds $\#H(\mathbb{F}_{13^4}) = 27540$.

(2) $q = 13^5 \equiv -1 \bmod 7$. The quadratic twist corresponding to the cocycle $\mathrm{Frob}_q \mapsto \tau = (S^{-1}RS^{-1})^2RS$ has 372496 rational points, while $\#H(\mathbb{F}_{13^5}) = 362880$.

(3) (Again) $q = 13^5 \equiv -1 \bmod 7$. The cubic twist corresponding to the cocycle $\mathrm{Frob}_q \mapsto R$ has 373698 rational points, improving what was found in (2) above.

(4) $q = 19^4 \equiv 2 \bmod 7$. Here, the quadratic twist corresponding to the cocycle $\mathrm{Frob}_q \mapsto \tau = (S^{-1}RS^{-1})^2RS$ has 130969 rational points, whereas $\#H(\mathbb{F}_{19^4}) = 129675$.

Using the `Sage` code from Appendix A.2.3 of [17] one can calculate explicit models for the desired twists. As an example, the quadratic twist corresponding to the cocycle $\mathrm{Frob}_q \mapsto$ the automorphism $(x, y) \mapsto (y, x)$ of the affine curve $1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0$ is given by:

$$\begin{aligned}&7d^4x^8 + 2d^4x^7 - 28d^3x^6y^2 + 35d^4x^6 + 42d^3x^5y^2 + 42d^2x^4y^4\\&- 105d^3x^4y^2 + 70d^2x^3y^4 - 28dx^2y^6 + 84d^4x^4 + 105d^2x^2y^4 + 14dxy^6\\&+ 7y^8 - 168d^3x^2y^2 - 35dy^6 + 112d^4x^2 + 84d^2y^4 - 112d^3y^2 + 64d^4 = 0.\end{aligned}$$

After our work was completed, many but not all of the new records described above have been improved by Everett Howe [9]. It is interesting to note that his results were partly inspired by the Fricke–Macbeath curve.

References

[1] W. Bosma, J. Cannon & C. Playoust, "The Magma algebra system. I. The user language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265.

[2] W. L. Edge, "A canonical curve of genus 7", *Proc. Lond. Math. Soc.* **17** (1967), p. 207-225.

[3] N. D. Elkies, "Shimura curve computations", in *Algorithmic number theory. 3rd international symposium*, Lect. Notes Comput. Sci., vol. 1423, Springer, 1998, p. 1-47.

[4] K. E. R. Fricke, "Ueber eine einfache Gruppe von 504 Operationen", *Math. Ann.* **52** (1899), p. 321-339.

[5] G. van der Geer, E. W. Howe, K. E. Lauter & C. Ritzenthaler, "Tables of Curves with Many Points", 2009, `http://manypoints.org`.

[6] E. Girondo, D. Torres-Teigell & J. Wolfart, "Fields of definition of uniform dessins on quasiplatonic surfaces", in *Riemann and Klein surfaces, automorphisms, symmetries and moduli spaces*, Contemporary Mathematics, vol. 629, American Mathematical Society, 2015, p. 155-170.

[7] M. Hendriks, "Platonic Maps of Low Genus", PhD Thesis, Eindhoven University of Technology, The Netherlands, 2013, `https://pure.tue.nl/ws/files/3493571/748466.pdf`.

[8] R. A. Hidalgo, "Edmonds maps on Fricke-Macbeath curve", *Ars Math. Contemp.* **8** (2015), no. 2, p. 275-289.

[9] E. W. Howe, "Curves of medium genus with many points", `https://arxiv.org/abs/1609.01838v2`, 2016.

[10] F. Klein, "Ueber die Transformation siebenter Ordnung der elliptischen Functionen", *Clebsch Ann.* **XIV** (1879), p. 428-471.

[11] A. M. Macbeath, "On a curve of genus 7", *Proc. Lond. Math. Soc.* **15** (1965), p. 527-542.

[12] S. Meagher & J. Top, "Twists of genus three curves over finite fields", *Finite Fields Appl.* **16** (2010), no. 5, p. 347-368.

[13] S. Sémirat, “2-extensions with many points”, http://arxiv.org/abs/math/0011067v1, 2000.

[14] J.-P. Serre, “Appendix to “Square-root parametrization of plane curves””, in *Algebraic geometry and its applications*, Springer, 1994, p. 85-88.

[15] G. Shimura, “Construction of class fields and zeta functions of algebraic curves”, *Ann. Math.* **85** (1967), p. 58-159.

[16] M. A. Soomro, “Algebraic Curves over Finite Fields”, PhD Thesis, University of Groningen, The Netherlands, 2013, https://www.rug.nl/research/portal/files/2371262/Afzal_Thesis.pdf.

[17] C. Verschoor, *Twists of the Klein Curve and of the Fricke Macbeath Curve*, Memoir, University of Groningen, The Netherlands, 2015, http://irs.ub.rug.nl/dbi/55e5a09cbf723.

[18] K. Wohlfahrt, “Macbeath’s Curve and the Modular Group”, *Glasg. Math. J.* **27** (1985), p. 239-247, corrigendum in *ibid.*, **28** (1986), p. 241.

Jaap Top
Johann Bernoulli Institute
University of Groningen
P.O.Box 407, 9700 AK Groningen, the Netherlands
E-mail: j.top@rug.nl
URL: http://www.math.rug.nl/~top

Carlo Verschoor
Johann Bernoulli Institute
University of Groningen
P.O.Box 407, 9700 AK Groningen, the Netherlands
E-mail: carlovmm@gmail.com