ERRATUM: SPRINGER LNM 2054

RATIONAL POINTS AND ARITHMETIC OF FUNDAMENTAL GROUPS EVIDENCE FOR THE SECTION CONJECTURE

JAKOB STIX

1. Space filling curves in their Jacobian §15.2

Unfortunately, the computations on page 199 in the paragraph *Reduction to small cases* suffer from a sign mistake marked in red below. The conclusion towards Theorem 223 still holds true but requires some extra care. Because also the computations of examples for genus 2 and 3 on page 201 contain a bug, Theorem 223 in the new version is now sharper: there are only two isomorphism classes of curves, both of genus 2 over $\mathbb{F}_2$, that are space filling in their jacobian.

1.1. **Estimates for the class number.** We recall the notation of [Sti13, §15.2], so $X/\mathbb{F}_q$ is a smooth, projective curve of genus $g \geq 2$ and $\alpha_1, \ldots, \alpha_{2g}$ are the inverses of the eigenvalues of Frobenius sorted such that $\alpha_{i+g} = q/\alpha_i$ for all $i = 1, \ldots, g$. Due to the Albenese embedding $X \hookrightarrow \operatorname{Pic}^0_X$ we have the inequality

$$N := \#X(\mathbb{F}_q) \leq \# \operatorname{Pic}^0_X(\mathbb{F}_q) =: h$$

We determine all cases when we have in fact equality. Let

$$D_n = \#\{D \geq 0 \ ; \ \text{divisor of } \deg(D) = n\}$$

be the number of effective $\mathbb{F}_q$-rational divisors of degree n on X. Then [LMD90] Theorem 1 reads

$$\sum_{n=0}^{g-2} D_n + \sum_{n=0}^{g-1} q^{g-1-n} D_n = h \cdot \sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2}. \tag{1.1}$$

We observe that $D_0 = 1$ and $D_n \geq N$ for $n \geq 1$, and combine [LMD90] §4 (5)

$$\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2} \leq \frac{(g+1)(q+1) - N}{(q-1)^2} \tag{1.2}$$

with (1.1) to obtain the estimate

$$h \geq (q-1)^2 \cdot \frac{1 + q^{g-1} + N(g - 2 + \frac{q^{g-1}-1}{q-1})}{(g+1)(q+1) - N} = (*). \tag{1.3}$$

We set $n(q-1) = N$ and analyse $(*) > N$ to be equivalent to

$$1 + q^{g-1} + n\left((g-2)(q-1) + q^{g-1} - 1\right) > n\left((g+1) \cdot \frac{q+1}{q-1} - n\right)$$

$$\iff \quad n^2 + n\left(q^{g-1} + (g-2)(q-1) - 1 - (g+1) \cdot \frac{q+1}{q-1}\right) + 1 + q^{g-1} > 0$$

$$\iff \quad n^2 + n\left(q^{g-1} + (g-2)\big(q - 1 - \frac{q+1}{q-1}\big) - 1 - 3\frac{q+1}{q-1}\right) + 1 + q^{g-1} > 0$$

$$\iff \quad n^2 + n\left(q^{g-1} + q(g-2)\big(1 - \frac{2}{q-1}\big) - 4 - \frac{6}{q-1}\right) + 1 + q^{g-1} > 0. \tag{1.4}$$

Date: December 4, 2017.

The coefficient of the linear term in n is monotone increasing as a function in g and q separately in the range $g \geq 3$ and $q \geq 3$. The value of this coefficient for $g = q = 3$ is 2, hence the entire inequality holds true except possibly if $g = 2$ or $q = 2$.

1.2. **The case of genus 2.** If $g = 2$, then (1.4) reads

$$n^2 + n\left(q - 4 - \frac{6}{q-1}\right) + 1 + q = (n-2)^2 + n\frac{(q+2)(q-3)}{q-1} + q - 3 > 0$$

which is true for all $n \geq 0$ if $q \geq 4$, and in case of $q = 3$ unless $n = 2$. Therefore, if $h = N$ we necessarily have $q = 2$, or we have $q = 3$ with $n = 2$ and consequently $N = 4$. We argue first that the latter case does not occur.

Let $\sigma_i(\alpha)$ denote the i-th elementary symmetric polynomial in the α_i. Thus, for $g = 2$, the L-polynomial of X is given by

$$L(t) = \prod_{i=1}^{4}(1 - \alpha_i t) = 1 - \sigma_1(\alpha)t + \sigma_2(\alpha)t^2 - q\sigma_1(\alpha)t^3 + q^2t^4.$$

By Poncaré duality we have $\sigma_{g+r}(\alpha) = q^r\sigma_{g-r}(\alpha)$, and the Lefschetz trace formula yields

$$S_m(\alpha) = \sum_i \alpha_i^m = 1 + q^m - \#X(\mathbb{F}_{q^m}).$$

Using $\sigma_1(\alpha) = S_1$ and $2\sigma_2 = S_1^2 - S_2$ we obtain the following exact formula for the class number:

$$\begin{aligned} h = L(1) &= 1 + q^2 - (1+q)(1+q-N) + \frac{1}{2}\Big((1+q-N)^2 - (1+q^2) + N_2\Big) \\ &= -q + \frac{1}{2}\big(N^2 + N_2\big). \end{aligned}$$

Now in case $h = N$ the condition $N_2 \geq N$ reads as follows:

$$2q = N^2 - 2N + N_2 \geq N^2 - N.$$

This is impossible if $q = 3$ and $N = 4$, and this concludes the proof that q must be 2 in all cases.

1.3. **The case of $q = 2$ and large genus.** For $q = 2$, the estimate (1.4) reduces to

$$n^2 + n(2^{g-1} - 2g - 6) + 1 + 2^{g-1} > 0.$$

This holds for all $n \geq 0$ if $g \geq 5$, and in case of $g = 4$ unless $n = 3$. Therefore, if $h = N$ we have $g = 2$ or $g = 3$, or we have $g = 4$ and necessarily $N = n = 3$.

We argue now that the latter case may not occur. Indeed, now the inequality (1.3) yields

$$3 = N = h \geq (*)_{q=2,g=4,N=3} = 3$$

and is in fact an equality. However, the inequality was derived from (1.1) by estimating in particular $D_2 \geq N = 3$, although considering all divisors of degree 2 with support in the rational points yields the better bound

$$D_2 \geq \binom{N+1}{2} = 6.$$

This is a contradiction.

1.4. **The case of genus 3.** We abbreviate $N_m := \#X(\mathbb{F}_{q^m})$ and keep the notation S_m and $\sigma_i(\alpha)$ from the $g = 2$ case; however now for $g = 3$. Manipulating symmetric polynomials we find

$$\begin{aligned}
\sigma_1(\underline{\alpha}) &= S_1 = 1 + q - N,\\
\sigma_2(\underline{\alpha}) &= q - (1+q)N + (N^2 + N_2)/2,\\
\sigma_3(\underline{\alpha}) &= \frac{1}{3}\Big(1 + q^3 - N_3 + (1+q-N)(-1+q-q^2-(1+q)N + (N+3N_2)/2)\Big).
\end{aligned}$$

Using again Poincaré duality in the form $\sigma_{g+r}(\alpha) = q^r\sigma_{g-r}(\alpha)$, that allows to compute the L-polynomial and in particular its value $h = L(1)$ as (we set $q = 2$)

$$h = \frac{1}{3}N_3 + \frac{1}{2}NN_2 + \frac{1}{6}N^3 - 2N.$$

Now $N_3 = 3n_3 + N$ and $N_2 = 2n_2 + N$ for some $n_i = \#\{\mathfrak{q} \in X \ ; \ \deg(\mathfrak{p}) = i\} \in \mathbb{N}_0$, so the formula for the class number becomes

$$h = n_3 + Nn_2 + \frac{1}{6}N(N-2)(N+5).$$

It is easy to see that $h > N$ unless $N = 1$ or $N = 2$. In both cases together we can determine in total five pairs of values for (n_2, n_3). In each case we can determine the L-polynomial and SAGE tells us that two of its roots are real but not of absolute value $\sqrt{2}$. This concludes the argument to exclude curves of genus 3.

We also performed a search among curves of genus 3 by a SAGE program [S$^+$09]. The search divides naturally into the case of hyperelliptic curves and non-hyperelliptic curves. The latter embed as a smooth quartic in $\mathbb{P}^2$ by means of the canonical embedding. My SAGE program found no curves with $N = h$ in both cases, thus indeed confirming the above proof.

1.5. **Theorem and examples.** Unfortunately, the table of genus 2 curves with $N = h$ in [Sti13] page 201 contains a further mistake. The curve of type III has $N = 2$ and $N_2 = 6$ and consequently $h = 3$. The correct SAGE computation gives us a complete list of isomorphism classes of examples. By analysing Artin–Schreier double covers $y^2 + y = f(x)$ for rational functions $f \in \mathbb{F}_2(x)$, the list of examples can be confirmed by hand. We conclude that Theorem 223 of loc. cit. improves to:

Theorem. *There are smooth projective curves $X/\mathbb{F}_q$ of genus $g \geq 2$ such that*

$$\#X(\mathbb{F}_q) = \#\operatorname{Pic}^0_X(\mathbb{F}_q)$$

if and only if $q = 2$ and $g = 2$. More precisely, there are exactly two isomorphism classes of such curves:

type	$N = h$	N_2	$L(T)$	*equation*
I	1	5	$1 - 2T + 2T^2 - 4T^3 + 4T^4$	$Y^2 + Y = X^5 + X^3 + 1$
II	2	4	$1 - T - 2T^3 + 4T^4$	$Y^2 + Y = X^3 + 1 + \frac{1}{X}$

References

[LMD90] Lachaud, G., Martin-Deschamps, M., Nombre de points des jacobiennes sur un corps fini, *Acta Arithmetica* **56** (1990), no. 4, 329–340.

[S$^+$09] *SageMath, the Sage Mathematics Software System (Version 7.5.1)*, The Sage Developers, 2017, `http://www.sagemath.org`.

[Sti13] Stix, J., *Rational Points and Arithmetic of Fundamental Groups, Evidence for the Section Conjecture*, Springer Lecture Notes in Mathematics **2054**, Springer Verlag, 2013, xx + 249pp.

Jakob Stix, Institut für Mathematik, Goethe–Universität Frankfurt, Robert-Mayer-Strasse 6–8, 60325 Frankfurt am Main, Germany

E-mail address: `stix@math.uni-frankfurt.de`