CORRIGENDUM TO: IMPROVED UPPER BOUNDS FOR THE NUMBER OF POINTS ON CURVES OVER FINITE FIELDS

EVERETT W. HOWE AND KRISTIN E. LAUTER

Abstract. We correct an error in Section 7 of our paper "Improved upper bounds for the number of points on curves over finite fields." The error involves a standard form for triple covers of elliptic curves in characteristic 3, and it invalidates the arguments we used to show that two particular polynomials do not occur as Weil polynomials of curves over a finite field. We sketch two new arguments that prove that these Weil polynomials do not occur.

1. Introduction

In Section 7.2 of our paper [3] there is a mistake in an argument about a standard form for triple covers of elliptic curves in characteristic 3. In this corrigendum we identify the error and make a corrected statement about the standard form for such triple covers. The goal of [3, §7] was to show that two particular polynomials do not occur as Weil polynomials of curves over a finite field. The error we made invalidates our arguments that these polynomials do not occur. In Sections 3 and 4 we sketch new arguments that show that these polynomials are not the Weil polynomials of curves. In a forthcoming paper we will give the full details of the new techniques, and use them to further improve some of the upper bounds in the van der Geer-van der Vlugt tables of curves with many points [1].

2. The error, and a corrected statement.

We use the notation and conventions of [3] without further explanation.

Recall that the goal of [3, §7.1] was to find a standard form for triple covers of elliptic curves over finite fields of characteristic 3. In that section, we showed that every such triple cover of an elliptic curve E can be written in the form $z^3 - fz = g$, where f and g are functions on E satisfying certain conditions. Specifically, let us say a pair (f, g) is *well-conditioned* at a point P of E if one of the following conditions holds: either

(1) the order $\operatorname{ord}_P g$ of g at P is not a multiple of 3, or
(2) we have $2 \operatorname{ord}_P g \geq 3 \operatorname{ord}_P f$.

We showed in [3, §7.1] that every triple cover of E has a model $z^3 - fz = g$ such that f has no poles outside ∞ and no multiple zeros anywhere, and such that (f, g) is well-conditioned at every finite pole of g. The model could be made to satisfy

Date: 10 September 2006.
2000 *Mathematics Subject Classification.* Primary 11G20; Secondary 14G05, 14G10, 14G15.
Key words and phrases. Curve, rational point, zeta function, Weil bound, Serre bound, Oesterlé bound.

the further requirement that (f, g) be well-conditioned at ∞, unless f is constant and g has a triple pole at ∞.

The error in [3] occurs in §7.2, starting at the second full paragraph on page 1717. The problem lies in the statement that for all P we have either $2 \operatorname{ord}_P g \geq 3 \operatorname{ord}_P f$ or $\operatorname{ord}_P g \not\equiv 0 \bmod 3$, except when $P = \infty$ and $\operatorname{ord}_P g = -3$. In particular, the erroneous statement claims that the model can be chosen so that (f, g) is well-conditioned at all finite P, not just at the poles of g. The erroneous statement is in fact true for those finite points P for which $\operatorname{ord}_P f = 0$, because for these points either P is a pole of g or we have $2 \operatorname{ord}_P g \geq 0 = 3 \operatorname{ord}_P f$. However, the statement can fail to hold for points P for which $\operatorname{ord}_P f = 1$.

What *is* true is that for every $P \neq \infty$ for which $\operatorname{ord}_P f > 0$, there is a constant $c_P \in \overline{k}$ such $(f, g + c_P^3 - c_P f)$ is well-conditioned at P. Note that over $\overline{k}$ the triple cover $z^3 - fz = g + c_P^3 - c_P f$ is isomorphic to the triple cover $z^3 - fz = g$. To take account of this change, the final paragraph of [3, §7.2] should be replaced with the following:

> If $\operatorname{ord}_P f$ is odd, let c_P be an element of $\overline{k}$ such that either $2 \operatorname{ord}_P(g + c_P^3 - c_P f) \geq 3 \operatorname{ord}_P f$ or $\operatorname{ord}_P(g + c_P^3 - c_P f) \not\equiv 0 \bmod 3$. Let $g_P = g + c_P^3 - c_P f$. Then the contribution to the different at P is
>
> $$\begin{cases} 1 & \text{if } 3 \operatorname{ord}_P f - 2 \operatorname{ord}_P g_P \leq 0; \\ 2 + 3 \operatorname{ord}_P f - 2 \operatorname{ord}_P g_P & \text{if } 3 \operatorname{ord}_P f - 2 \operatorname{ord}_P g_P > 0. \end{cases}$$
>
> In particular, when $\operatorname{ord}_P f$ is odd the contribution at P to the different is odd.

The contribution to the different at P thus depends on f and g in a more complicated manner than we had thought, and several of the cases we consider in §7.3 and §7.4 of [3] cannot be eliminated as easily as we argued in those sections.

3. A corrected argument for the case $q = 3$, $g = 6$, $N = 15$.

Suppose that C is a genus-6 curve over $\mathbb{F}_3$ with exactly 15 rational points. In [3, §4.7] we showed that the real Weil polynomial of the Jacobian J of C must be

$$h = (x + 2)^2 (x + 3)(x^3 + 4x^2 + x - 3).$$

Let F be the unique elliptic curve over $\mathbb{F}_3$ with real Weil polynomial $x + 2$, and let B be the abelian surface $F \times F$. Note that B is the only abelian surface over $\mathbb{F}_3$ with real Weil polynomial $(x + 2)^2$. We can show that there is an injection $B \hookrightarrow J$ such that the canonical polarization on J pulls back to a polarization μ on B whose degree is 9. By looking at the degree-9 polarizations of B, we see that there will be an injection $F \hookrightarrow B$ such that the pullback of μ to F is a polarization λ of degree 1 or 4. Now consider the composition

$$F \hookrightarrow B \hookrightarrow J.$$

The canonical polarization on J pulls back via this composition to the polarization λ of F, and it follows that there is a map from C to F of degree 1 or 2. Certainly there is no such map of degree 1. But there are no such maps of degree 2 either, because F has 6 rational points and C is supposed to have 15. Therefore there is no genus 6 curve over $\mathbb{F}_3$ with real Weil polynomial equal to h.

4. A corrected argument for the case $q = 27$, $g = 4$, $N = 65$.

The appendix to [4] shows that a genus-4 curve over $\mathbb{F}_{27}$ with 65 rational points must have real Weil polynomial $(x+7)(x+10)^3$. Suppose C is such a curve, and let J be its Jacobian. Let F be the unique elliptic curve over $\mathbb{F}_{27}$ with real Weil polynomial $x+10$. Note that F^3 is the unique abelian threefold over $\mathbb{F}_{27}$ with real Weil polynomial $(x+10)^3$. We see from [3, Lemma 7] that there is a degree-9 isogeny $E \times F^3 \to J$, and that the pullback to F^3 of the canonical principal polarization on J is a degree-9 polarization on F^3. Using the knowledge of the isomorphism classes of principal polarizations of F^3 that we obtain from Hoffmann's classification [2] of the rank-3 unimodular lattices over $\mathbb{Z}[\sqrt{-2}]$, together with an easy argument that shows that every degree-9 polarization of F^3 is the pullback of a principal polarization on F^3 via a 3-isogeny, we can write down representatives for all of the isomorphism classes of degree-9 polarizations on F^3. For each representative μ, we check that there is an embedding $F \hookrightarrow F^3$ such that the pullback of μ to F is a polarization of degree 1 or 4. It follows that there must be a map from C to F of degree 1 or 2. A degree-1 map would be impossible, so there must be a degree-2 map. But it is not hard to adapt the method explained in [3, §6.1] to enumerate the genus-4 double covers of F, and to verify that none of them has 65 points. Therefore there is no genus-4 curve over $\mathbb{F}_{27}$ having 65 points.

References

[1] Gerard van der Geer and Marcel van der Vlugt: Tables of curves with many points, *Math. Comp.* **69** (2000) 797–810.

[2] Detlev W. Hoffmann: On positive definite Hermitian forms, *Manuscripta Math.* **71** (1991) 399–429.

[3] E. W. Howe and K. E. Lauter: Improved upper bounds for the number of points on curves over finite fields, *Ann. Inst. Fourier (Grenoble)* **53** (2003) 1677–1737.

[4] David Savitt with an Appendix by Kristin Lauter: The maximum number of rational points on a curve of genus 4 over $\mathbb{F}_8$ is 25, *Canad. J. Math.* **55** (2003) 331-352. `arXiv:math.NT/0201226`.

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1967, USA.

E-mail address: `however@alumni.caltech.edu`

URL: `http://www.alumni.caltech.edu/~however/`

Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA.

E-mail address: `klauter@microsoft.com`