ANNALES

DE

L'INSTITUT FOURIER

Everett W. HOWE & Kristin E. LAUTER

Corrigendum to: Improved upper bounds for the number of points on curves over finite fields

Tome 57, n° 3 (2007), p. 1019-1021.

<http://aif.cedram.org/item?id=AIF_2007__57_3_1019_0>

Ann. Inst. Fourier, Grenoble
57, 3 (2007) 1019-1021

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

Tome 53 (2003), n° 6, p. 1677-1737

by Everett W. HOWE & Kristin E. LAUTER

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. We have new arguments that can replace the invalid ones. Sketches of these new arguments can be found in the second appendix to [2]; 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.

Keywords: Curve, rational point, zeta function, Weil bound, Serre bound, Oesterlé bound.
Math. classification: 11G20, 14G05, 14G10, 14G15.

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 $2 \operatorname{ord}_P g \geqslant 3 \operatorname{ord}_P f$.

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 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 $2 \operatorname{ord}_P g \geqslant 3 \operatorname{ord}_P f$ 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 $2 \operatorname{ord}_P g \geqslant 0 = 3 \operatorname{ord}_P f$. 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 $2 \operatorname{ord}_P(g + c_P^3 - c_P f) \geqslant 3 \operatorname{ord}_P f$ 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
>
> $$\begin{cases} 1 & \text{if } 3 \operatorname{ord}_P f - 2 \operatorname{ord}_P g_P \leqslant 0; \\ 2 + 3 \operatorname{ord}_P f - 2 \operatorname{ord}_P g_P & \text{if } 3 \operatorname{ord}_P f - 2 \operatorname{ord}_P g_P > 0. \end{cases}$$
>
> 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.

BIBLIOGRAPHY

[1] G. VAN DER GEER & M. VAN DER VLUGT, "Tables of curves with many points", *Math. Comp.* **69** (2000), p. 797-810, Updates at `http://www.science.uva.nl/~geer/`.

[2] E. W. HOWE & K. E. LAUTER, "Improved upper bounds for the number of points on curves over finite fields", `http://arxiv.org/pdf/math.NT/0207101`.

[3] E. W. HOWE & K. E. LAUTER, "Improved upper bounds for the number of points on curves over finite fields", *Ann. Inst. Fourier (Grenoble)* **53** (2003), p. 1677-1737.

Everett W. HOWE
Center for Communications Research,
4320 Westerra Court,
San Diego, CA 92121-1967, USA.
however@alumni.caltech.edu

Kristin E. LAUTER
Microsoft Research
One Microsoft Way,
Redmond, WA 98052, USA.
klauter@microsoft.com