Comments/errata for “Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology”

Kiran S. Kedlaya
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139, USA

October 13, 2003

Bas Edixhoven points out that the precision estimates for the algorithm as described do not properly account for the fact that the matrix of Frobenius in the given basis of $H^1(\overline{A}, K)_-$ does not have integral entries. One way to remedy this is to simply carry more precision: the denominators in the matrix M have valuation $O(\log(g))$, so carrying $O(n\log(g))$ extra precision suffices to correctly compute the characteristic polynomial of M' to the desired precision.

However, when one does this (as observed numerically by Frederik Vercauteren), one finds that the denominators actually remain bounded. The reason is because there is a basis on which M does have integral entries, given by generators of the crystalline H^1 of the complete curve; it is more convenient in practice to compute using such a basis. Concretely, if t is a uniformizer at infinity in the minus eigenspace of the hyperelliptic involution (e.g., x^g/y), then the submodule of the $\mathbb{Z}_q$-span of the $x^i\,dx/y$ for $i = 1, \ldots, 2g-1$ whose t-adic expansions can be integrated over $\mathbb{Z}_q$ is stable under Frobenius, so any basis of this submodule gives an integral matrix.

Other errata (also found by Edixhoven):

- page 326, line -4: the left side should be $d(x\,dy_1 \wedge \cdots \wedge dy_i)$.
- page 328, line 10: the closure of the affine curve is not smooth; C should be taken to be the normalization of that closure.
- page 329, line 10: $2g-1$ should be $2g-2$.
- page 330, line 17: “generated by y” should be “generated by p and y”.
- page 331, line 8: $2m+1$ should be $d(m+1)-2$.

- page 331, line 14: the $2g$ on the left should be the number of Weierstrass points which are rational over $\mathbb{F}_{q^i}$. The same is true of the $2g$ on the right in line 20 (so they still cancel each other).
- page 332, line 2: the equation $a_i = a_{2g-i}$ should read $q^{g-i} a_i = a_{2g-i}$.
- page 334, line 2 and 4: N should be N_1.

Finally, Vercauteren points out that a similar calculation in the genus 1 case appears in: G.C. Kato and S. Lubkin, Zeta matrices of elliptic curves, *J. Number Theory* **15** (1982), 318–330.