

Errata for “An Extension of Kedlaya’s Algorithm to Hyperelliptic Curves in Characteristic 2 ”, and related papers.

J. Denef

Department of Mathematics, K.U.Leuven,
Celestijnenlaan 200B, B-3001 Leuven, Belgium

F. Vercauteren

Department of Electrical Engineering, K.U.Leuven,
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium

In this note we correct a gap in the proof of the complexity estimates appearing in our papers [1],[2]. The complexity estimates are correct, but the proof was incomplete at a certain point. The same gap appears in our paper [3], but there the estimate for the space complexity has to be multiplied with a power of $\log(g)$, where g is the genus of the curve.

First we fill in the gap in [2]. In this paper we gave an algorithm to compute the zeta function of an hyperelliptic curve of genus g over a field with $q = 2^n$ elements. We proved that the worst-case time complexity is $O(g^{5+\epsilon}n^{3+\epsilon})$, and that the worst-case space complexity is $O(g^4n^3)$. For the average-case time and space complexity we obtained $O(g^{4+\epsilon}n^{3+\epsilon})$ and $O(g^3n^3)$, respectively. These estimates are correct, but there is a gap in the proof, which we will now correct. The gap in [1] can be treated in the same way.

The gap has to do with the precision estimates. The matrix M of the small Frobenius (induced by squaring) on the given basis of the Monsky-Washnitzer cohomology H^1 does not have integral entries. We proved in [2] that the denominators have valuation $O(\log(g))$. Hence the denominators in the norm M_F of M have valuation at most $O(n \log(g))$. This can cause a loss of precision of $O(n \log(g))$ q -adic digits, as we noted in section 4.2 of [2]. What we overlooked is that in the calculation of the characteristic polynomial of M_F , using the Hessenberg algorithm, there can be an accumulation of loss of precision, so that we lose g times more digits. Thus we lose at most $O(ng \log(g))$ digits, instead of at most $O(n \log(g))$ digits. In our paper we worked with a precision of $O(ng)$ digits.

One way to remedy this is to simply carry more precision in our calculations, from the start on. It is easy to see that this does not change the time complexity, but it would increase the space complexity by multiplying it with a power of $\log(g)$.

However it is not necessary to increase our estimate for the space complexity. To prove this, we will use the following claim.

Let C be a smooth proper curve over the ring \mathbb{Z}_q of q -adic integers, and let D be an effective divisor on C whose support has normal crossings over \mathbb{Z}_q , such that $C \setminus D$ is affine. Assume that $\deg(D) \geq 2g$. Let L be the \mathbb{Z}_q -module of differentials ω on $C \setminus D$ over \mathbb{Z}_q with $\text{div}(\omega) + D \geq 0$, which satisfy the following condition: For each point P of D , each term with valuation < -1 in a local expansion of ω at P , is integrable over \mathbb{Z}_q (meaning that it is the differential of a power of the uniformizer multiplied by an element of \mathbb{Z}_q). Then the image of L in the Monsky-Washnitzer cohomology H^1 of $C \setminus D$ is invariant under the action of the small Frobenius, and generates H^1 as a vector space over \mathbb{Q}_q . Moreover this image of L equals the image in H^1 of the hypercohomology of the logarithmic de Rham complex on C over \mathbb{Z}_q , with respect to D .

The claim is a slight generalization of Proposition 5.3.1 of [4], and can be proved in the same way.

To obtain the desired complexity estimate, the algorithm has to calculate a new basis for H^1 that is a \mathbb{Z}_q -module basis for the image of L in H^1 . Moreover all calculations have to be done in the new basis. Then the matrix of the small Frobenius has integral entries, and the problem disappears.

When $\log(g)$ is bounded by a multiple of n , one can avoid calculating such a new basis. Indeed the valuation of the denominators in the matrix that expresses the new basis in terms of the old basis, is bounded by $O(\log(g))$, and the same holds for the matrix that expresses the old basis in terms of the new basis. This implies that the denominators of M_F have valuation at most $O(\log(g))$, and one can recover the desired complexity estimates. This bound on the entries of M_F was observed empirically in [2] (at the end of section 4.2). Edixhoven [4] proved this bound for hyperelliptic curves over finite fields of odd characteristic.

The same gap appears in our paper [3], but there we have a worse bound $O(g \log(g))$ on the valuation of the denominators in M . The construction of the new basis requires more space, namely $O(g^3(\log(g))^c n^2)$, for some integer c , because we have a worse bound on the invariant factors that appear while doing the required linear algebra over \mathbb{Z}_q . For this reason the space complexity of algorithm in [3] has to be multiplied with some power of $\log(g)$.

References

- [1] J. DENEFF and F. VERCAUTEREN, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic number theory (Sydney, 2002), 308–323, Lecture Notes in Comput. Sci., **2369**, Springer, Berlin, 2002.
- [2] J. DENEFF and F. VERCAUTEREN, *An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2*, J. Cryptology **19** (1), pp. 1-25 (2006).
- [3] J. DENEFF and F. VERCAUTEREN, *Computing Zeta functions of C_{ab} curves using Monsky-Washnitzer cohomology*, Finite Fields Appl. **12** (1), pp. 78-102 (2006).
- [4] B. EDIXHOVEN, *Point counting after Kedlaya*, EIDMA-Stieltjes Graduate Course, Leiden, September 2003.