Computing $L$-polynomials of Non-Hyperelliptic Genus 4 and 5 curves

Steven Galbraith$^1$ and Raminder S. Ruprai$^2$

Information Security Group, Royal Holloway University of London, Egham, Surrey, UK
$^1$ steven.galbraith@rhul.ac.uk $^2$ r.s.ruprai@rhul.ac.uk

June 12, 2008

Abstract

Given a non-singular, projective, non-hyperelliptic curve $C$ over $\mathbb{F}_q$ where $q$ is prime we present an algorithm that computes all the coefficients of the $L$-polynomial of $C$, in an expected time of $\tilde{O}(q^2)$ in both the genus 4 and genus 5 case. We represent $C$ as a plane model and if this model is of low degree the expected running time to recover all the coefficients of the $L$-polynomial can be reduced to $\tilde{O}(q^4/3)$. This is an improvement on the previous best running time of $\tilde{O}(q^{3/2})$ for genus 4 and $\tilde{O}(q^2)$ for genus 5 given by Elkies in [2].

Let $L(t) = \sum_{i=0}^{2g} a_i t^i$ be the $L$-polynomial of the curve of genus $g$. From the Theorem of Weil given in [5] we know that $a_0 = 1$, $a_{2g} = q^g$ and we have bounds on the other coefficients. A proof of Weil’s Theorem can be found in [3]. Let $J_C(\mathbb{F}_q^k)$ denote the group of $\mathbb{F}_p^k$-rational points on the Jacobian Variety of $C$.

The algorithm consists of 2 stages. The first stage is based upon Diem’s Index Calculus algorithm as described in [1]. We use an adapted version of the main algorithm in [1] to compute the $\#J_C(\mathbb{F}_q)$. This stage is the most time intensive and in both cases takes $\tilde{O}(q^2)$ but for a plane model of low degree can take as little as $\tilde{O}(q^{4/3})$.

By simply counting the number of $\mathbb{F}_q$-rational points on $C$, which takes time $\tilde{O}(q)$, we have the unknown coefficients $a_1$ and $a_{2g-1}$ by Weil’s Theorem. By Lemma 1 in [4] we have that $\#J_C(\mathbb{F}_q) = L(1)$ and $\#J_C(\mathbb{F}_q^2) = L(1) \cdot L(-1)$. We can write $L(-1)$ as a function of $L(1)$ and the coefficients $a_1, \ldots, a_g$. Using ‘Baby-Step Giant-Step’ techniques developed by Sutherland in [4] we can compute possible values of $L(-1)$ and therefore possible values of $\#J_C(\mathbb{F}_q^2)$ that can be checked. As we have computed the values of $L(1)$ and $a_1$ we can find the correct value of $L(-1)$ and the remaining unknown coefficients in time $\tilde{O}(q^{3/4})$ for genus 4 and $\tilde{O}(q^{5/4})$ for genus 5.
References


