

Reparametrizing Algebraic Curves

Mark van Hoeij & Andrew Novocin
Department of Mathematics
Florida State University
Tallahassee, FL 32306-4510, USA
{hoeij,anovocin}@math.fsu.edu

April 8, 2008

- An irreducible polynomial $f \in \mathbb{C}[x, y]$ defines an algebraic curve, C , in $\mathbb{P}^2(\mathbb{C})$, see [...].
- A parametrization of a curve is a birational map from \mathbb{P}^1 to C . This is equivalent to an isomorphism from the functionfield $L_{\mathbb{C}}$ of C to the function field $\mathbb{C}(t)$ of \mathbb{P}^1 .
- If this isomorphism is defined over \mathbb{Q} then we have an isomorphism from $L_{\mathbb{Q}}$ to $\mathbb{Q}(t)$. Here $L_{\mathbb{Q}} = \mathbb{Q}(x)[y]/\langle f \rangle$.

Given a parametrization of a curve we would like to find a ‘small’ parametrization of the same curve. Where small simply refers to the number of bits required to display the parametrization. In order to be practical we must accomplish our task quickly, since the result is an aesthetic result. Presented here is a largely heuristic algorithm which is quite practical and could be easily included in any computer algebra system.

1 Introduction

Assume that we are given a parametrization of some curve, f . Then all parametrizations of f can be written as a composition of the given parametrization and an automorphism of \mathbb{P}^1 , which corresponds to an automorphism of $\mathbb{C}(t)$, i.e. some $\mu \in \mathbb{C}(t)$ for which $\mathbb{C}(t) = \mathbb{C}(\mu)$. Such μ are called Möbius transformations, which can be written in the form $\frac{at+b}{ct+d}$ with $ad - bc \neq 0$. Möbius transformations are uniquely determined by their actions on three points. We only consider parametrizations defined over \mathbb{Q} , and hence only $a, b, c, d \in \mathbb{Q}$.

The approach of this chapter will be to utilize the fact that any parametrization with small bit size must send the points $\infty, 0, 1$ on \mathbb{P}^1 , to points on the curve with small bit size. This is because, for a rational parametrization given by two

rational functions, $[X(t), Y(t)]$, the bit sizes of $X(\infty), X(0), X(1)$ are less than the bit size of $X(t)$ (since $X(\infty)$ is either $\infty, 0$ or the ratio of the leading coefficients of the numerator and denominator of $X(t)$, and similar arguments for $0, 1$). Other points p (except $p = -1$ which is equally as nice as $p = 1$) are less nice than $\infty, 0, 1$ because for such p the bit size of $X(p)$ need not be less than the bitsize of $X(t)$.

To make our goal more explicit let us observe that if $[X(t), Y(t)]$ is a small parametrization then it must be that $X(\infty), X(0), X(1)$ are small. Whereas if $\tilde{X}(\infty), \tilde{X}(0), \tilde{X}(1)$ is small for some parametrization $[\tilde{X}(t), \tilde{Y}(t)]$ then if there is a small parametrization $[X(t), Y(t)]$ we can compute the Möbius transformation $\mu : X(\infty), X(0), X(1) \leftrightarrow \tilde{X}(\infty), \tilde{X}(0), \tilde{X}(1)$ and it must have small coefficients (since it is uniquely determined by these six points all of which are small). Thus $X(t), \tilde{X}(t)$ only differ by a small Möbius transformation whenever $X(t)$ is small. So our goal is as follows: when given a parametrization find a Möbius transformation which will convert it into a parametrization which sends $\infty, 0, 1$ to small points, and this will be within a small Möbius transformation of optimal. It should be noted that the converse is not true as I can create a parametrization with large bit size which still maps $\infty, 0, 1$ to points on the curve with small bit size. But in this case no parametrization exists which is much smaller than the one which we will find.

Our strategy will require finding points on the curve which can be expressed with small bit size. If we cannot find three small points on the curve then we must decide what to do with the degrees of freedom granted by our Möbius transformation. We have devised a method for utilizing this freedom which is near optimal if we find only two points. If we can only find one point then we adapt a strategy which is consistent with our method for two points, but it is possibly not optimal. If we find no points then we have a method which will work whenever we find a factor of degree 3 in either $X(t)$ or $Y(t)$. This algorithm has polynomial complexity and works quite well in practice. It works so quickly, in fact, that there is no reason not to include this algorithm in any parametrization computation.

2 Finding small points on the curve

Since our metric of success is merely bit size the nicest points are ∞ and any single bit numbers. So when searching for nice points we do an exhaustive search for values of t which make $X(t)$ or $Y(t)$ equal to some $\frac{0,1,2,3}{0,1,2,3}$ (not $\frac{0}{0}$), this is a fast (polynomial) process and we also will know the degree of each of the points we find. Our goal is to find three nice places on the curve, one each for $\infty, 0, 1$. If we find three such points it is simple to find an appropriate Möbius transformation (the one which sends the value of t for a given nice point and maps it to $\infty, 0, 1$) and we are almost done. All that remains is to decide which points to assign to each of $\infty, 0, 1$. We choose the best point (highest degree) on the curve for ∞ the next best for 0 and the last for 1 . The reason for this assignment is that choosing the highest degree point for ∞ creates smaller

denominators. Also, when we do not find three nice points and we must develop our strategy for the remaining freedom, and by making our choices in the order $\infty, 0, 1$ our strategy is simple.

If we follow the guideline of having ∞ mapped to the best point we find (by composing our given parametrization by some Möbius transformation) that we can still compose this new parametrization by any transformation of the form $t \mapsto at + b$ without disrupting our first choice ($a \times \infty + b = \infty$). If we also have 0 map to the second smallest point on the curve then we can still compose with a transformation of the form $t \mapsto at$, without disrupting either 0 or ∞ . So if we find only one point we have two problems to solve, finding the best additive transformation ($t \mapsto t + b$), and finding the best multiplicative transformation ($t \mapsto at$). Our algorithm for solving the multiplicative transformation is new, fast, and near-optimal so we will give it a section of its own.

3 Multiplicative Transformations

In this section we want to find the best transformation of the form $x \mapsto ax$. Our approach will be to solve the subproblem of considering only a of the form p^k for some specific p . By solving this subproblem on a well-chosen list of relatively prime p_i we will create an optimal solution for $x \mapsto ax$. Let us formulate these problems formally:

Problem 1. *Given $f(x) \in \mathbb{Z}[x]$, find $a \in \mathbb{Q}^\times$ such that $g(x) \stackrel{\text{def}}{=} (1/q)f(ax) \in \mathbb{Z}[x]$ and the product of absolute values of non-zero coefficients of $g(x)$ is minimal. Note: $q = \text{content}(f(ax))$.*

We solve this problem by solving the following problem:

Problem 2. *Given $f(x) \in \mathbb{Z}[x]$, and a number $p \in \mathbb{N}$, find $k \in \mathbb{Z}$ such that $g(x) \stackrel{\text{def}}{=} (1/q)f(p^k x)$ and the product of absolute values of non-zero coefficients of $g(x)$ is minimal. Note that in this problem we can only control powers of p so that we really are minimizing the occurrences of p , counted with valuations, in the non-zero coefficients of $g(x)$.*

To measure occurrences of p we will use the map $\|\cdot\|_p: \mathbb{Z}[x] \rightarrow \mathbb{N} \cup \{0\}$ which sends $g(x) = a_n x^n + \dots + a_0 \mapsto \sum_{a_i \neq 0} \nu_p(a_i) - \alpha_g$ where $\alpha_g = \min\{\nu_p(a_i) \mid 0 \leq i \leq n\}$ and

$$\nu_p(a) = \begin{cases} \infty & a = 0 \\ n & p^n \mid a \text{ and } p^{n+1} \nmid a \end{cases}$$

The α_g above is there to take care of any common factors amongst the non-zero coefficients of g and otherwise we have just counted how many factors of p exist amongst the coefficients of g (with multiplicity). Now we shall seek to minimize this number.

First observe that when we replace x by px , we have moved the coefficient of x^m from a_m to $p^m a_m$. Likewise a replacement of x by $p^k x$ will shift the

coefficient of x^m from a_m to $p^{mk}a_m$. In particular, note that a shift of this form will never change a_0 .

Lemma 1. *Let k be a value for which $\|f(p^kx)\|$ is minimal, then $M \leq k \leq N$ where $-M = \lfloor \min\{\frac{\nu_p(a_n) - \nu_p(a_i)}{n-i} \mid \forall i < n\} \rfloor$ and $N = \lceil \max\{\frac{\nu_p(a_0) - \nu_p(a_i)}{-i} \mid \forall i > 0\} \rceil$.*

Proof. $M \leq \frac{\nu_p(a_i) - \nu_p(a_n)}{i-n}$ for all $i < n \Rightarrow M(i-n) \leq \nu_p(a_i) - \nu_p(a_n) \Rightarrow \nu_p(a_n) - Mn \leq \nu_p(a_i) - in$ for all $i < n$. Which is the same as saying $\nu_p(a_n p^{-Mn}) \leq \nu_p(a_i p^{-Mi})$ for all $i < n$. Now compare $\|f(xp^{-M})\|$ to $\|f(xp^{-M-j})\|$ for any $j > 0$. $\|f(xp^{-M})\| = \sum \nu_p(a_i) - Mi - Mn$ (since α_g will be the a_n term and $\|f(xp^{-M-j})\| = \sum \nu_p(a_i) - Mi - ji - (Mn - jn) = \sum \nu_p(a_i) - Mi - Mn + \sum j(n-i)$ which is just $\|f(xp^{-M})\|$ plus some positive number. Therefore the optimal value k is greater than or equal to $-M$. A similar argument shows that $k \leq N$. \square

Note that $-M, N$ are the two extreme slopes of the p -adic Newton Polygon of $f(x)$. Now we just try all values k such that $-M \leq k \leq N$. Each computation is done using only integer arithmetic and is very fast. Now we have guaranteed the optimal k so that $f(p^kx)$ has the fewest occurrences of p .

The next step in this multiplicative problem is deciding which p_i to run this process on. Here we use a process called balanced factoring (Abramov), by which we find a list $\{p_1, \dots, p_m\}$ where $\gcd(p_i, p_j) = 1$, for all $i \neq j$ using gcds, rather than integer factoring. This is quick and if for each p_i we find k_i such that $f(p_i^{k_i}x)$ has the fewest occurrences of p_i then our final answer to this problem will be sending $x \mapsto p_1^{k_1} \dots p_m^{k_m} x$ which must be optimal.

4 Additive Transformations

For the degree of freedom $x \mapsto x + b$ we decide to let $b = \frac{-a_n}{a_{n-1}}$ as this will eliminate the second largest coefficient. We are aware that this is not optimal but given the little control this transformation actually provides we decide to make some guarantee of progress, rather than anything else.

5 Other Strategies and conclusion

When we cannot find any small points on the curve we have a few techniques that will work, but only in a few situations. This method involves the freedom of a Möbius transformation to send and monic cubic factor to any other monic cubic factor, and ideas from the next chapter which will allow us to construct a small polynomial whose root represents the same field extension as a given polynomial. We will reserve this technique until then.

The techniques that we've presented so far have an advantage that when they work they produce an aesthetic improvement and they regardless of success these methods take almost no computational time. Everything we've presented has a

small complexity and can thus be implemented any time a parametrization is being performed.