On Computing the Dual of a Plane Algebraic Curve

Emil Volcheck
National Security Agency
volcheck@acm.org—http://acm.org/~volcheck

11 April 1997

Abstract

Computing the dual curve of a plane algebraic curve can be accomplished using a classical elimination method. We present a new method that relies on interpolating the dual curve. For a curve of degree n, this method costs $O(n^{12})$ arithmetic operations. We refine this method by computing the class of the curve before interpolating. For a curve of known class m, this method requires $O(m^6)$ arithmetic operations.

1 Introduction

The notion of duality in plane projective geometry can be naively stated: any theorem (properly phrased) remains true if you replace every reference to "point" with "line" and vice versa. For example, the statement "any two points are incident to a unique line" corresponds to the dual statement "any two lines are incident to a unique point." Given a projective plane curve $\mathcal{C} : F(x_0 : x_1 : x_2) = 0$, we describe the *dual curve* $\hat{\mathcal{C}} : \hat{F}(u_0 : u_1 : u_2) = 0$ in the following way. Each place of $\mathcal{C}$ has a unique tangent of the form $L : a_0x_0 + a_1x_1 + a_2x_2 = 0$. The dual curve $\hat{\mathcal{C}}$ is the curve consisting of all points $P = (a_0 : a_1 : a_2)$ that correspond to such a tangent L.

The geometry of a curve and its dual are fundamentally related. This relationship has been an important topic in the study of algebraic curves, leading to, for example, the Plücker formulas. In 1991, Carlos Moreno posed the question

> Given a projective plane curve $\mathcal{C} : F = 0$, find an *efficient* algorithm to compute the homogeneous polynomial $\hat{F}$ which defines the dual curve $\hat{\mathcal{C}} : \hat{F} = 0$.

as an open problem in [Mor91, p. 227] (my emphasis). Moreno sought a better algorithm than the classic elimination method, which can effectively compute only small degree examples [Mor96].

We address Moreno's question in this paper by presenting a new algorithm that is more efficient than classical methods in certain cases. First, we present an elimination technique to compute the dual of a curve following a classic construction and then discuss its complexity. Second, we present a method that expresses the dual curve polynomial $\hat{F}$ in undetermined coefficients and solves for $\hat{F}$ by interpolation. Using a simple bound on the degree of the dual, we show this method costs $O(n^{12})$ arithmetic operations. By analyzing the singularities of $\mathcal{C}$, we can determine the degree m of its dual $\hat{\mathcal{C}}$ without computing the dual explicitly. Once we know m, we can bound the cost of interpolating the dual by $O(m^6)$ arithmetic operations.

We refer the reader to Walker's text for any background on curves and their duals not developed here [Wal78]. We work in the setting of an absolutely irreducible curve defined over a ground field k of characteristic zero, extending the ground field as necessary so that we implicitly work over the algebraic closure of k. We follow Walker's notation and abbreviate $\partial F/\partial x_i$ as F_i, a point $(a_0 : a_1 : a_2)$ as (a_i) or (a), and a line $a_0x_0 + a_1x_1 + a_2x_2 = 0$ as $\sum a_i x_i = 0$. We denote the dual of the coordinate system (x_i) with the coordinate system (u_i).

2 Classical Method

The tangent line at a smooth point $P = (a_i)$ of the curve $\mathcal{C} : F(x_i) = 0$ has the equation

$$\sum F_i(P)\, x_i = 0.$$

The dual curve $\hat{\mathcal{C}} : \hat{F}(u_i) = 0$ contains the point $(F_i(P))$, and it can be shown that $\hat{\mathcal{C}}$ is the closure of the image of $\mathcal{C}$ under the rational map

$$u_i = F_i(x).$$

The product variety $\mathcal{C} \times \hat{\mathcal{C}}$ can be expressed as the ideal I, where

$$I = \langle F(x),\, u_0 - F_0(x),\, u_1 - F_1(x),\, u_2 - F_2(x) \rangle$$

consists of bihomogeneous polynomials in (x_i) and (u_i). Finding the dual curve polynomial is equivalent to eliminating (x_i) from this ideal. See Berzolari's survey article [Ber06, p. 324] for an early reference to this approach, which uses resultants.

One way to perform this elimination is to compute a Gröbner basis for I with a product term order where the variables (x_i) are greater than the variables (u_i) (for background see [CLO92], for instance). There is exactly one polynomial in $I \cap k[u_i]$, which is the dual curve polynomial $\hat{F}(u_i)$.

Let n be the degree of $F(x_i) = 0$. The ideal I has four polynomials of degrees at most n in 6 variables. I know no polynomial time bound for computing a Gröbner basis of such an ideal. Even small examples can require significant computing time by this method. Consider the Klein quartic curve:

$$xy^3 + yz^3 + zx^3 = 0.$$

The `Eliminate` function of `Mathematica` on a DECStation 5240 found the dual in just under 2000 seconds. This elimination can also be performed by taking resultants, which requires only polynomial arithmetic operations but is also very expensive.

3 The Degree of the Dual

The degree of a curve can be defined as the number of points (properly counted) in which an arbitrary line meets the curve. We define the *class* of a curve $\mathcal{C} : F = 0$ to be the number of tangents of the curve (properly counted) that all meet at an arbitrary point. By duality, the class of $\mathcal{C}$ is the degree of $\hat{\mathcal{C}}$.

Walker gives a formula for the class m of a curve of degree n:

$$m = n(n-1) - \sum_P \delta(P), \tag{1}$$

where the sum is over all places P of $\mathcal{C}$ and where $\delta(P)$ is defined as

$$\min_{(a_i)} \operatorname{ord}_P(\sum a_i F_i).$$

Hence the class m is at most $n(n-1)$. Clearly $\delta(P) > 0$ only if P is singular, so the class of a non-singular curve is exactly $n(n-1)$.

We can evaluate $\sum_P \delta(P)$ by finding the order of each partial F_i at all singular places. We can do this by calculating Puiseux expansions for all singular places and then substituting expansions into the partials to determine their order at the places. Puiseux expansions can be calculated in polynomial time: Walsh proves a bound that is $O(n^{34+\epsilon} \cdot \log^{2+\epsilon}(h))$ bit operations where h is the height of the polynomial [Wal94]. In practice, Puiseux expansions can be computed much more quickly than this bound suggests.

When the singularities of a curve are rather simple, only nodes and cusps, then resolution of singularities is trivial, and we know the class of the curve from the Plücker formulas [Wal78, p. 120]. For a curve with δ nodes and κ cusps, the class m is given by

$$m = n(n-1) - 2\delta - 3\kappa.$$

For the remainder of the paper, we assume that we know the class of $\mathcal{C}$. We show how to take advantage of the situation when the class is significantly smaller than the square of the degree.

4 Solving for the Dual

Given the degree m of the dual, we can express it as a polynomial in undetermined coefficients

$$\hat{F}(u_i) = \sum_{i+j+k=m} a_{ij}\, u_0^i\, u_1^j\, u_2^k. \tag{2}$$

By solving for the coefficients a_{ij}, we can determine the dual curve polynomial. Even if we do not know the class in advance, we can take m to be $n(n-1)$, the upper bound on the class from equation (1).

We describe two methods for setting conditions on the a_{ij}. The pull-back of $\hat{F}$ along the dual map must vanish in the function ring of $\mathcal{C}$, that is, F must divide $\hat{F}(F_i)$. We use this fact to solve for the a_{ij} in the following way. First we substitute the $F_i(x)$ for the u_i in equation (2). Next we pick a main variable, divide $F(F_i)$ by $F(x)$ with respect to the main variable, and take the remainder. The coefficients of this remainder are linear in the a_{ij}, and we can solve a linear system to make the remainder vanish identically.

Before we consider the complexity of this method, let us recall that a polynomial of degree d has $1/2 \cdot (d+2)(d+1)$ terms. Note that m is of $O(n^2)$ by equation (1), and $\hat{F}$ in (2) has therefore $O(n^4)$ terms.

The intermediate polynomial $\hat{F}(F_i)$ has degree $O(n^3)$ in the (x_i). The remainder will have degree $O(n)$ in the main variable and degree $O(n^3)$ in the other variables, for a total of $O(n^4)$ terms. Forcing these terms to vanish requires solving a system of $O(n^4)$ equations in the $O(n^4)$ unknowns a_{ij}, which costs $O(n^{12})$ arithmetic operations for Gaussian elimination.

We now consider a second method that locates points on the dual curve and then interpolates the dual curve through them. We select sufficiently many places P on $\mathcal{C}$ and map them to points $\hat{P}$ on the dual curve $\hat{\mathcal{C}}$, i.e., find the tangent of each place P. Then we interpolate the dual curve through these points $\hat{P}$ by the method of undetermined coefficients described above. That is, if the tangent at P is $\sum b_i x_i = 0$, then set $\hat{F}(b_i) = 0$ as a linear condition on the a_{ij}.

Let us count how many points we need to determine the dual curve uniquely.

Lemma 1 *A curve of degree d is uniquely determined by any $d^2 + 1$ distinct points through which it passes.*

Proof: By Bézout's theorem, a second curve of degree d would meet the first in exactly d^2 points.

Although a polynomial of degree d has only $1/2 \cdot (d+2)(d+1)$ terms, the linear conditions imposed on a polynomial by a set of points may have dependencies. We may require more points than terms, but $d^2 + 1$ points always impose enough independent conditions to determine the curve.

The dual curve $\hat{\mathcal{C}}$ has degree m, so $O(m^2)$ points on $\mathcal{C}$ with distinct tangents suffice to determine $\hat{\mathcal{C}}$. If some points that we choose on $\mathcal{C}$ turn out to have the same tangent, then they map to different places of a singular point of $\hat{\mathcal{C}}$. Since there can be no more than $O(m^2)$ singular points on $\hat{\mathcal{C}}$, we can indeed bound the number of points we choose by $O(m^2)$. To solve for $\hat{F}$, we must solve a system of $O(m^2)$ equations in $O(m^2)$ unknowns, for which Gaussian elimination costs $O(m^6)$. Since m is of $O(n^2)$, this computation can also be bounded with $O(n^{12})$ arithmetic operations, as with the previous method.

We summarize this result as the following theorem:

Theorem 1 *Given a plane algebraic curve, whose class is known to be m, we can compute its dual curve in $O(m^6)$ arithmetic operations.*

5 Examples

Computing the dual of the Klein quartic using the `Eliminate` function of `Mathematica` on a DECStation 5240 found the dual in about 1980 seconds. In `Maple`, interpolating through the images of 97 (affine) points formed by the intersection with the curve of vertical lines $x = i$ for i from -16 to 16 was much slower. I stopped the computation at over 7500 seconds, and it would have run much longer. Setting up the equations required just under 790 seconds with the rest of the time spent in linear algebra.

Consider an example where the degree of the dual is much smaller than the $n(n-1)$ bound. The following curve has degree 12 and class 4:

$$\begin{aligned} F(x:y:z) &= 27\,x^{10}y^2 + 42\,x^5y^6z - 282\,x^7y^3z^2 \\ &\quad -4\,x^9z^3 + 651\,x^4y^4z^4 + 42\,x^6yz^5 \\ &\quad +42\,xy^5z^6 - 4\,x^3y^9 - 282\,x^3y^2z^7 \\ &\quad -282\,x^2z^3y^7 + 27\,x^2z^{10} + 27\,y^{10}z^2 - 4\,y^3z^9 \end{aligned}$$

Using `Maple`, I dehomogenized by setting $z = 1$ and mapped the points over the lines $x = 2$, $x = 3$, and $x = 4$ (small integer values that avoid roots of the discriminant) to the dual curve. I set up a degree four polynomial in 15 undetermined coefficients and solved a system of 33 equations in 15 variables with `linalg[nullspace]` to find the dual

$$\hat{F}(x:y:z) = xy^3 + yz^3 + zx^3,$$

which is the Klein quartic curve again.

Computing the singular parts of all Puiseux expansions of F required less than 15 seconds, using Mark van Hoeij's `AlgCurves` package [vH95]. The linear algebra also required less than 15 seconds. In contrast, the `Eliminate` function of `Mathematica` ran for over an hour before I stopped it. Note that this curve is highly singular: a non-singular curve of degree 12 has genus 55, whereas this curve has genus only 3. Nevertheless, the Puiseux expansions were calculated quickly.

6 Conclusions and Further Work

Computing the class of a curve is relatively cheap. So before computing the dual of a degree n plane algebraic curve, first compute its degree, which is the class of the original curve. If the class m is close to $n(n-1)$, then use a classical elimination technique. On the other hand, if the class is significantly less than $n(n-1)$, use interpolation to take advantage of the smaller degree. Finding the break-even point between these two methods will require further work.

Without any analysis of singularities, we can bound the work of the interpolation method by $O(n^{12})$ arithmetic operations. I would like to know whether the complexity of performing the elimination using Gröbner bases has a similar or better bound. By analyzing singularities to obtain the class, we can bound the linear algebra by $O(m^6)$ arithmetic operations.

We have a high degree bound on the bit complexity of computing the class, and it would be worthwhile to find a better bound. This problem closely depends on the difficulty of resolving singularities and computing Puiseux expansions. Teitelbaum has shown that the singularities of a curve can be resolved in $O(n^{12})$ arithmetic operations using quadratic transformations and Gröbner basis computations [Tei90]. To derive this bound, note that since the Milnor number of a singular point is bounded by the degree of the conductor, the sum of the Milnor numbers of all singular points is of $O(n^2)$. Teitelbaum's estimate of $O(\mu^6)$ arithmetic operations to resolve a singularity of Milnor number μ gives us the $O(n^{12})$ bound.

Teitelbaum also shows that the Milnor number and conductor of a singularity can be computed in the same time bound. I believe that the class of a curve can also be computed in the same time bound. Improvements in the bounds of Teitelbaum or Walsh would imply a better bound on computing the class.

We have made some progress on Moreno's question by studying an interpolation method and considering its complexity. However, finding the duals of larger degree curves with few singularities is still difficult for both elimination and interpolation methods.

Acknowledgements

I thank the referees for their comments, and I thank the National Security Agency and the Research Institute for Symbolic Computation (RISC-Linz)

for their support.

References

[Ber06] Luigi Berzolari. *Theorie der höheren ebenen algebraischen Kurven*, volume Band 3.II.I of *Encyklopädie der mathematischen Wissenschaften*, pages pp. 313–455. Teubner-Verlag, 1906.

[CLO92] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

[Mor91] Carlos J. Moreno. *Algebraic Curves over Finite Fields*, volume 97 of *Cambridge Tracts in Mathematics*. Cambridge University Press, 1991.

[Mor96] Carlos Moreno, 1992, 1996. Personal communications.

[Tei90] Jeremy Teitelbaum. The computational complexity of the resolution of plane curve singularities. *Mathematics of Computation*, 54(190):797–837, 1990.

[vH95] Mark van Hoeij, 1995. The `AlgCurves` package, available at `http://www-math.sci.kun.nl/math/compalg/`.

[Wal78] Robert J. Walker. *Algebraic Curves*. Springer-Verlag, 1978.

[Wal94] Peter Garth Walsh. *The Computation of Puiseux Expansions and a Quantitative Version of Runge's Theorem on Diophantine Equations*. PhD thesis, University of Waterloo, 1994.