PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 122, Number 3, November 1994

AN EXPLICIT FAMILY OF CURVES WITH TRIVIAL AUTOMORPHISM GROUPS

PETER TURBEK

(Communicated by Eric Friedlander)

Dedicated to the memory of Sheela Phansalkar (1966–1990)

ABSTRACT. It is well known that a generic compact Riemann surface of genus greater than two admits only the identity automorphism; however, examples of such Riemann surfaces with their defining algebraic equations have not appeared in the literature. In this paper we give the defining equations of a doubly infinite, two-parameter family of projective curves (Riemann surfaces if defined over the complex numbers), whose members admit only the identity automorphism.

It is well known that a generic curve of genus greater than two admits only the identity automorphism. Although this result was probably known by the turn of the century, the first published proof was given by Bailey in 1961 [1]. To obtain the strongest results, Bailey's method is necessarily nonconstructive; it does not yield an example of a defining algebraic equation for a curve with no nontrivial automorphisms. Similarly a proof by Greenberg [4], using techniques of Teichmüller theory, does not yield an explicit example of a Riemann surface with a trivial automorphism group. Much of the subsequent work on automorphisms of Riemann surfaces, including the author's, has relied on the representation of a given Riemann surface as the upper half plane under the action of a Fuchsian group. This again has the disadvantage of rarely yielding a defining algebraic equation for the given Riemann surface. Indeed, in the preface to his book, *The complex analytic theory of Teichmüller spaces,* Subhashis Nag exclaimed, "Almost every compact Riemann surface of genus $g \geq 3$ allows only the identity automorphism. (I don't know, though, of even a single explicit such algebraic curve whose automorphism group is demonstrably trivial!)."

The author believes that examples pertinent to famous theorems should be readily at hand. Therefore, in this paper we give the defining equations of a doubly infinite, two-parameter family of curves which admit only the identity automorphism (see equation (1) below). The curves in this family have genus $(n-1)(m-1)/2$ for relatively prime integers m and n which satisfy $n > m+1 > 3$.

Let C be a curve defined by (1) and let C' be a nonsingular projective model for C. The proof that C' admits only the trivial automorphism depends on the

Received by the editors February 5, 1993.
1991 *Mathematics Subject Classification.* Primary 14E09, 14H55, 30F99.

following salient property. If we exclude one exceptional case, C' contains a point Q with a gap sequence distinct from the gap sequence at any other point. Thus any automorphism of C' must fix Q. It is easily shown that only the identity automorphism fixes Q, thus C' has no nontrivial automorphisms.

I. Definition of C and preliminary properties

Let k be an algebraically closed field and let k^* denote the nonzero elements of k. We assume the characteristic of k is either 0 or $p > 2$. We denote two-dimensional affine space over k with coordinates (x, y) by $\mathbb{A}^2$. Let m and n be fixed positive integers such that $(m, n) = 1$ and $n > m + 1 > 3$. If the characteristic of k is $p > 2$, we also assume that p does not divide $(m-1)mn$. Let $C = C_{m,n,A,B}$ denote the locus in $\mathbb{A}^2$ of the equation

$$f(x, y) = x^n + y^m + Axy + Bx = 0 \tag{1}$$

for suitably chosen elements A and B in k^*. Let $C' = C'_{m,n,A,B}$ be a nonsingular projective model for $C_{m,n,A,B}$. We will prove that each member of the family $\{C'_{m,n,A,B}\}$ admits only the trivial automorphism group.

The only restriction required is that the choice of A and B makes the affine curve $C = C_{m,n,A,B}$ nonsingular. We note that (1) will be nonsingular in $\mathbb{A}^2$ if and only if (1) and its partial derivatives

$$f_x = nx^{n-1} + Ay + B, \quad f_y = my^{m-1} + Ax \tag{2}$$

have no simultaneous zero in $\mathbb{A}^2$. To see this always can be accomplished, we first choose an arbitrary value for A. If $f(x, y) = f_x(x, y) = f_y(x, y) = 0$, then

$$0 = xf_x - f = (n-1)x^n - y^m \quad \text{and} \quad x = \frac{-my^{m-1}}{A}, \tag{3}$$

so

$$(n-1)\left(\frac{-my^{m-1}}{A}\right)^n - y^m = 0. \tag{4}$$

Let $\{y_i\}_{i=1}^r$ be the distinct roots of (4). Choose B such that for each i,

$$f_x\left(\frac{-my_i^{m-1}}{A}, y_i\right) \neq 0. \tag{5}$$

Then C is nonsingular in $\mathbb{A}^2$. We shall henceforth assume that A and B are thus chosen. In the appendix we will determine explicit examples of A and B.

Let $K(C) = k(x, y)$ denote the function field of C. Note that f is the irreducible polynomial for y over $k(x)$. To see this, we apply Eisenstein's criterion to $y^m+Axy+x^n+Bx$. Observe that x divides both Ax and x^n+Bx, while x^2 does not divide $x^n + Bx$. Thus f is irreducible over $k[x]$, and so over $k(x)$.

If $h \in K(C)$ and $P \in C'$, we let $\mathrm{ord}_P(h)$ denote the order of h at P. We denote the divisor of h by (h) and the pole divisor of h by $(h)_\infty$; its support consists of the points where the order of h is negative. If $P \in C'$ and $\mathrm{ord}_P(h) = 1$, we say h is a local parameter at P. We let $\Omega(0)$ denote the holomorphic differentials of C. If D is a divisor, we let $L(D)$ denote those elements $h \in K(C)$ such that $(h) + D \geq 0$. We let $l(D)$ denote the dimension, over k, of $L(D)$. The automorphism group of C' is denoted by $\operatorname{Aut}(C')$. If $\sigma \in \operatorname{Aut}(C')$, then σ induces an automorphism of $k(x, y)$, denoted by σ^*, which satisfies $\sigma^*(h) = h \circ \sigma$ for all $h \in k(x, y)$.

Let $\mathbb{P}^2 = \mathbb{P}^2(k)$ denote two-dimensional projective space with coordinates denoted by (X, Y, Z). We consider the homogenization of (1) above, namely,

$$(6) \qquad F(X, Y, Z) = X^n + Y^m Z^{n-m} + AXYZ^{n-2} + BXZ^{n-1} = 0.$$

We denote the locus of (6) in $\mathbb{P}^2$ by $\bar{C}$. Note that C and $\bar{C}$ have the same nonsingular model C'. Let x and y denote X/Z and Y/Z respectively. The only point at infinity (i.e., point with $Z = 0$) on $\bar{C}$ is the singular point $(0, 1, 0)$. The following argument shows there is only one point on C', which lies over $(0, 1, 0)$. Let Q be any point on C' which lies over $(0, 1, 0)$. Both x and y must have a pole at Q. From (1) we obtain $n(\operatorname{ord}_Q(x)) = m(\operatorname{ord}_Q(y))$. Since $(m, n) = 1$, we have n divides $\operatorname{ord}_Q(y)$ and m divides $\operatorname{ord}_Q(x)$. But the degree of $(x)_\infty$ and $(y)_\infty$ are m and n respectively. Thus x and y have orders $-m$ and $-n$ respectively at Q. This implies that Q is the unique point on C' lying over $(0, 1, 0)$. Recall that we defined C to be the affine locus of (1). Thus we may view C' as $\{Q\}$ union C.

Lemma I.1. *Let $\omega = dx/f_y$. Then $\omega \in \Omega(0)$ and the genus of C is $(m-1)(n-1)/2$.*

Proof. Let $P = (a, b) \in C$. Recall that $(x - a)$ is a local parameter if and only if $f_y(a, b) \neq 0$. Thus, if $(x - a)$ is a local parameter, then $\omega = dx/f_y = d(x-a)/f_y$ has order 0 since $f_y(a, b) \neq 0$. If on the other hand $x - a$ is not a local parameter, then $y - b$ is a local parameter, so the same argument can be used on $\omega = -d(y-b)/f_x$. Thus at each point of the affine plane ω has order 0. Since the degree of a differential is $2g - 2$, where g is the genus of C, we obtain $\operatorname{ord}_Q(\omega) = (2g-2)Q$.

To determine the genus of the curve we first observe that $\operatorname{ord}_Q(x) = -m$ and $\operatorname{ord}_Q(dx) = -m - 1$. From (2) we obtain $\operatorname{ord}_Q(f_y) = n(1 - m)$. Thus $\operatorname{ord}_Q(\omega) = n(m-1) - m - 1$. Upon equating this to $2g - 2$ we obtain $g = (n-1)(m-1)/2$.

Recall that t is said to be a gap at $P \in C'$ if there exists no function f such that $(f)_\infty = tP$. A simple consequence of the Riemann Roch theorem [2], [3] is that t is not a gap at P if $t \geq 2g$, and there are g positive integers which are gaps at P. Thus to each point $P \in C'$ we can associate its (increasing) gap sequence $(t_1, \dots, t_i \dots, t_g)$, where each t_i is a gap at P and $1 \leq t_g \leq 2g-1$.

Let W denote the divisor $(2g-2)Q$. Thus $W + Q = (2g-1)Q$. The Riemann Roch Theorem yields that $l(W+Q) = 2g - 1 + 1 - g = g$.

Lemma I.2. *Let $P \in C$. Then t is a gap at P if and only if there exists an $h \in L(W)$ such that $\operatorname{ord}_P(h) = t - 1$.*

Proof. Apply the Riemann Roch theorem to $L\big((t-1)P\big)$ and $L(tP)$. Observe that t is a gap at $P \iff l\big((t-1)P\big) = l(tP) \iff l(W - tP) < l\big(W - (t-1)P\big)$.

II. The gap sequence at Q

In this section we construct a basis for $L(W+Q)$ and use it to examine the gap sequence at Q. To do this we need a preliminary lemma on the greatest integer function.

Proposition II.1. *Let N and M denote positive integers, and let $(N, M) = 1$. Then*

$$\sum_{k=1}^{M-1}\left[\frac{kN}{M}\right] = \frac{(N-1)(M-1)}{2}. \tag{7}$$

Proof. See [6].

Proposition II.2. *Let M and N be arbitrary positive integers, such that $N > M$ and M does not divide N. Then $[N/M]$ equals the number of nonnegative integers less than N which are congruent to N* mod *M.*

Proof. Assume $N = Mq+r$, with $0 < r < M$. Then $[N/M] = q$. In addition, the q integers: $r, M+r, 2M+r, \dots, (q-1)M+r$, are the nonnegative integers which are both congruent to N and less than N. This proves the proposition.

Lemma II.3. *$L((m-1)nQ)$ is spanned by the set $T = \{x^i y^j : i \geq 0, j \geq 0, mi + nj \leq (m-1)n\}$.*

Proof. Let $U = \{0, 1, 2, \dots, (m-1)n\}$ and $S = \{c : c \in U$ and $c = mi + nj$ for some nonnegative integers i and $j\}$. Each $c \in U$ corresponds to the order of a pole of an element $x^i y^j \in T$. We determine the cardinality of S by determining the elements of U which are in S^C, the complement of S. Since $(m, n) = 1$, the integers $0, n, 2n, \dots, (m-1)n$ form a complete set of residues mod m. Thus a given element of U is congruent to kn for a unique k with $0 \leq k < m$. Let $a \in U$. A little thought shows that $a \notin S$ if and only if $a \equiv kn \pmod{m}$ and $a < kn$. From Proposition II.2 the number of nonnegative integers congruent to kn and less than kn is $[kn/m]$. Thus, from Proposition II.1, there are

$$\sum_{k=1}^{m-1}\left[\frac{kn}{m}\right] = \frac{(m-1)(n-1)}{2} = g \tag{8}$$

elements in $U \cap S^C$. Thus there are $(m-1)n + 1 - g$ elements is S and thus in T. Since $(m, n) = 1$, $\operatorname{ord}(x^i y^k) \neq \operatorname{ord}(x^{i'} y^{k'})$ for $0 \leq k < m-1$ and $0 \leq k' < m-1$ unless $i = i'$ and $k = k'$. Thus the elements of T are linearly independent over k. To show they span $L((m-1)nQ)$, we appeal to the Riemann Roch theorem:

$$l((m-1)nQ) = (m-1)n + 1 - g + l(W - (m-1)nQ) = (m-1)n + 1 - g. \tag{9}$$

Thus we see that T spans $L((m-1)nQ)$.

Corollary II.4. *$L(W)$ and $L(W+Q)$ are spanned by*

$$T' = \{x^i y^j : mi+nj \leq (2g-2)\} \quad \textit{and} \quad T'' = \{x^i y^j : mi+nj \leq (2g-1)\} \tag{10}$$

respectively.

Proof. This follows directly from the facts that $L(W)$ and $L(Q+W)$ are subsets of $L((m-1)nQ)$ and the orders of elements of T are distinct.

For the purpose of later comparing Q with points of C we note the following corollaries.

Corollary II.5. *Let* $n = mq - r$ *with* $0 < r < m$. *Then* m *is not a gap at* Q. *However* $n + r - 1$ *is a gap at* Q *if* $r \neq 1$.

Proof. Follows directly from (10). Since $(x)_\infty = mQ$, m is not a gap at Q. To prove the second statement we note that $n + r - 1 < 2n$ and $n + r - 1$ is not a multiple of m. The only nongaps less than $2n$ which are not multiples of m are congruent to n mod m. Thus $n + r - 1$ is a gap if $r \neq 1$.

Corollary II.6. *If* P *is a point of* C *and there exist functions* h *and* g *such that* $h_\infty = mP$ *and* $g_\infty = nP$, *a basis for* $L((2g - 1)P)$ *is given by* $T_P = \{h^i g^j : mi + nj \leq 2g - 1\}$.

Proof. $\text{ord}_P(h^i g^j) = \text{ord}_Q(x^i y^j)$ for all nonnegative i and j. Thus there are g elements in T_P. Since elements in T_P have distinct orders at P, they form a linearly independent set over k. Thus T_P is a basis for $L((2g - 1)P)$.

III. The gap sequence at points of C

We first turn our attention to the gap sequences of points on $P \in C$ with $P \neq (0, 0)$.

Lemma III.1. *Let* $P = (a, b) \neq (0, 0)$. *Then* $\text{ord}_P(x - a) = 1$ *or 2.*

Proof. Consider the curve $G = mY^{m-1} + AXZ^{m-2}$ and let F be defined as in (6). By Bezout's theorem [3], $F = 0$ and $G = 0$ intersect at exactly $n(m - 1)$ points in $\mathbb{P}^2$ counting multiplicities. Since $G(0, 1, 0) \neq 0$, all points of intersection lie in $\mathbb{A}^2$. However, $G(a, b, 1) = 0$ if and only if $f_y(a, b) = 0$. Thus the points of intersection of F and G are the points (a, b) on C where $x - a$ is not a local parameter. These are the points where $h(y) = f(-my^{m-1}/A, y) = 0$. This is a polynomial in y of degree $n(m - 1)$. From elementary algebra, $h(y)$ will have multiple roots only at points where the formal derivative of h has a root in common with h. But the formal derivative of h is $(f_x)(-m(m - 1)y^{m-2}/A) + f_y$ evaluated at the point $(-my^{m-1}/A, y)$. Since $f_y = 0$ at this point, $f_x \neq 0$ there. By our assumptions on the characteristic of k, $m(m-1) \neq 0$. Thus $y = 0$ is the only multiple root of $h(y)$. Since $y = 0$ is a root of order $m - 1$, we see that $h(y)$ has $(n - 1)(m - 1) = 2g$ distinct, nonzero roots, say $b_1, \dots b_{2g}$. Let $a_i = -mb_i^{m-1}/A$ and let $P_i = (a_i, b_i)$ for $i = 1, 2, \dots, 2g$. Then $(0, 0)$ and the points (a_i, b_i) are the points where $x - a_i$ is not a local parameter. Thus at these places, $\text{ord}_{P_i}(dx) \geq 1$. But the degree of dx is $2g - 2$, $\text{ord}_Q(dx) = -m - 1$, and $\text{ord}_{(0,0)}(dx) = m - 1$. This forces $\text{ord}_{P_i}(dx) = 1$ for $i = 1, 2, \dots, 2g$. Thus if $x - a$ is not a local parameter and $a \neq 0$, then $x - a$ has order 2.

Lemma III.2. *Let* $P = (a, b) \neq (0, 0)$. *Then* m *is a gap at the point* P.

Proof. From Lemma I.2 it suffices to show there exists an $h \in L(W)$ with $\text{ord}_P(h) = m - 1$. Assume first that $(x - a)$ is a local parameter. Then $\text{ord}_P(x - a)^{m-1} = m - 1$. In addition, since $n > m + 1$, we see from (10) after a short calculation that $(x - a)^{m-1} \in L(W)$. Thus mP is a gap. If $x - a$ is not a local parameter, Lemma III.1 yields that $\text{ord}_P(x - a) = 2$. If $m - 1 = 2t + s$ with $s = 0$ or 1, then $\text{ord}_P(x - a)^t y^s = m - 1$, and from (10), after a short calculation, we see $(x - a)^t y^s \in L(W)$. Thus in either case m is a gap at P.

Lemma III.3. *If* $(0, 0) \neq P \in C$, *then* P *and* Q *have different gap sequences.*

Proof. From the above lemma and Corollary II.5, m is a gap at P, but m is not a gap at Q.

We now consider the gap sequence at $P = (0, 0)$.

Lemma III.4. *Let* $P = (0, 0)$ *and* $n = mq - r$ *with* $0 < r < m$. *Then* $n + r - 1$ *is not a gap at* P.

Proof. The function y/x^q has order $1 - mq$ at P. Since the function is defined at every other point, we see $mq - 1 = n + r - 1$ is not a gap at P.

Lemma III.5. *Let* $P = (0, 0)$. *If* $n = mq - r$ *for nonnegative integers* q *and* r, *with* $1 < r < m$, *then* Q *and* P *have different gap sequences.*

Proof. Lemma III.4 and Corollary II.5 yield that $n + r - 1$ is not a gap at P but is a gap at Q.

Corollary III.6. *If* $n = mq - 1$, *then the gap sequences for* Q *and* $P = (0, 0)$ *are identical. In addition, a basis for* $L((2g - 1)P)$ *is* $\{x^{-i}(y/x^q)^{-j} : mi + nj \leq (2g - 1)\}$.

Proof. $(1/x)_\infty = mP$. In addition, $(y/x^q)_\infty = nP$. Thus Corollaries II.4 and II.6 yield that Q and P have the same gap sequences and that the stated set is a basis.

IV. The automorphism group of C'

Proposition IV.1. *If* $n \not\equiv -1 \bmod m$, *any automorphism of* C' *must fix* Q. *If* $n \equiv -1 \bmod m$, *any automorphism of* C' *must either fix* Q *or map* Q *to* $(0, 0)$.

Proof. A point and its image under an automorphism must have the same gap sequence. Thus the proposition follows from Lemmas III.3, III.5, and III.6.

Theorem IV.2. *The curve* C' *has no nontrivial automorphisms.*

Proof. From the proposition, it suffices to prove the following two lemmas.

Lemma IV.3. *There is no nontrivial automorphism of* C' *which fixes* Q.

Proof. Let $n = mq + r$ with $0 < r < m$. Let $\sigma \in \operatorname{Aut}(C')$ such that $\sigma(Q) = Q$. Thus σ induces a map σ^* on the function field $K(C)$. Since σ fixes Q, σ must map x and y to functions with poles of order m and n respectively at Q. From (10) we obtain $\sigma^*(x) = a_1 x + a_0$ and $\sigma^*(y) = by + h(x)$, where h is a polynomial of degree at most q, $a_0 \in k$, and $a_1, b \in k^*$. From

$$\sigma^*(x^n + y^m + Axy + Bx) = 0, \tag{11}$$

we obtain

$$(a_0 + a_1 x)^n + (h(x) + by)^m + A(a_0 + a_1 x)(h(x) + by) + B(a_0 + a_1 x) = 0. \tag{12}$$

By the uniqueness of the irreducible polynomial (1) we see that $h(x)$ is identically 0. Thus, again by the uniqueness of the irreducible polynomial (1) we obtain $a_0 = 0$. Thus

$$(a_1 x)^n + (by)^m + A(a_1 x)(by) + B(a_1 x) = 0. \tag{13}$$

This forces $a_1 = ba_1$, so $b = 1$. Thus $a_1 = 1$. Thus σ is the identity.

Lemma IV.4. *There is no automorphism mapping Q to $P = (0, 0)$.*

Proof. From Proposition IV.1 we may assume $n = mq - 1$. Let $\sigma \in \mathrm{Aut}(C')$ with $\sigma(P) = Q$. P is the unique point of C with the same gap sequence as Q. From Lemma IV.3, it is clear that σ must have order two, and must interchange P and Q. Thus $\sigma^*(x)$ and $\sigma^*(y)$ must have poles of order m and n at P respectively. Corollary III.6 yields that $\sigma^*(x) = a_1/x + a_0$ and $\sigma^*(y) = h(1/x) + by/x^q$, where $a_0 \in k$, $a_1, b \in k^*$, and h is a polynomial of degree at most $q - 1$. Since σ^* has order 2, this yields

$$(14) \qquad x = \sigma^*(a_1/x + a_0) \Rightarrow x = \frac{a_1}{a_1/x + a_0} + a_0 \Rightarrow a_0 = 0.$$

Thus

$$(15) \qquad \sigma^*(x^n + y^m + Axy + Bx) = 0$$

yields

$$(16) \quad (a_1/x)^n + (h(1/x) + by/x^q)^m + A(a_1/x)(h(1/x) + by/x^q) + B(a_1/x) = 0.$$

By the uniqueness of the irreducible polynomial (1), we see $h(1/x)$ is identically 0. Thus,

$$(17) \qquad (a_1/x)^n + (by/x^q)^m + A(a_1/x)(by/x^q) + B(a_1/x) = 0.$$

Multiplying (17) by $x^{qm} = x^{n+1}$ we obtain

$$(18) \qquad a_1^n x + (by)^m + Aa_1 byx^{n-q} + Ba_1 x^n = 0.$$

This forces $n = q + 1$, which contradicts $n = mq - 1 > m + 1 > 3$.

This completes the proof of the theorem.

Appendix

We now restrict our field k to be the complex numbers. Recall that A and B are required to be chosen to insure that (1) is nonsingular in $\mathbb{A}^2$. From (4) and (5) we observe that for each choice of A at most $(m-1)(n-1)$ choices of B will be unsuitable. The following lemma states a sufficient (but by no means necessary) condition for A and B to make (1) nonsingular. We leave the proof, which uses elementary properties of integral ring extensions, as an exercise.

Lemma. *If A and B are nonzero integers such that either $nm - m - n$ does not divide B or A does not divide $Bm^2(n-1)$, then* (1) *is nonsingular in* $\mathbb{A}^2$.

As a simple consequence, we note that for arbitrary n and m, if $B = 1$, then A can be chosen to be any nonzero integer.

References

1. W. L. Bailey, *On the automorphism group of a generic curv e of genus greater than* 2, J. Math. Kyoto Univ. **1** (1961), 101–108.
2. H. M. Farkras and I. Kra, *Riemann surfaces*, 2nd ed., Graduate Texts in Math., vol. 71, Springer-Verlag, Berlin and New York, 1991.
3. W. Fulton, *Algebraic curves, an introduction to algebraic geometry*, Benjamin, New York, 1969.

4. L. Greenberg, *Maximal fuchsian groups*, Bull. Amer. Math. Soc. **69** (1963), 569–573.

5. S. Nag, *The complex anayltic theory of Teichmüller spaces*, Wiley, New York, 1988.

6. I. Niven and H. Zuckerman, *An introduction to the theory of numbers*, 2nd ed., Wiley, New York, 1966.

Department of Mathematics, Statistics, and Computer Science, Purdue University Calumet, Hammond, Indiana 46323

E-mail address: turbekps@pucal.bitnet