Characteristic polynomials of automorphisms of hyperelliptic curves

Robert M. Guralnick[1] Everett W. Howe[2]

[1]University of Southern California

[2]Center for Communications Research, La Jolla

Arithmetic, Geometry, Cryptography, and Coding Theory
CIRM, November 2007

The basic questions.

Let C be a genus-g curve over an algebraically closed field k. Assume $g > 1$.

Let α be an automorphism of C.

Then α^* is an automorphism of the Jacobian of C.

$$
\begin{aligned}
\text{Let } n &= \text{order of } \alpha. \\
\text{Let } f &= \text{characteristic polynomial of } \alpha^* \\
&= x^{2g} + \cdots + 1 \in \mathbb{Z}[x]
\end{aligned}
$$

Questions

What does the value of n tell us about f?
In particular, does n determine f?

Partial answers.

The order does tell us some things.

- Every root ζ of f satisfies $\zeta^n = 1$.
- n is the smallest integer for which this holds.
- At most $2 + (2g - 2)/n$ of the ζ are equal to 1.
  - Consider the degree-n map $C \longrightarrow D := C/\langle\alpha\rangle$.
  - We have $\operatorname{Jac} D \sim (\operatorname{Jac} C)^{\alpha=1}$.
  - Thus the genus of D is half the number of ζ equal to 1.
  - Apply Riemann-Hurwitz.

But the order does not tell us everything.

Suppose α is an involution of a genus-3 curve C.
Three polynomials $x^6 + \cdots + 1$ meet the conditions above.
All three occur, for some choice of C and α.

Hyperelliptic curves.

Suppose C is hyperelliptic, with hyperelliptic involution ι.

Then α induces an automorphism $\overline{\alpha}$ of $C/\langle\iota\rangle \cong \mathbb{P}^1$.

Let $\bar{n}$ be the order of $\overline{\alpha}$. Note that $\bar{n} = n$ or $\bar{n} = n/2$.

Question

Do the values of n and $\bar{n}$ determine f?

Another partial answer.

In general, n and $\bar{n}$ do not determine f.

Suppose C is genus-3 hyperelliptic curve.

Suppose $\alpha \neq \iota$ is an involution, so $n = \bar{n} = 2$.

Then f can be either $(x-1)^2(x+1)^4$ or $(x-1)^4(x+1)^2$.

Both possibilities occur.

A case where n and $\bar{n}$ *do* determine f.

Define ε by the conditions

$$\varepsilon \equiv -2g \bmod \bar{n} \qquad \text{and} \qquad 0 \leq \varepsilon < \bar{n}.$$

Theorem

Suppose g is even or $\bar{n}$ is odd. Then

$$f = \begin{cases} \dfrac{(x^{\bar{n}} + 1)^{(2g+\varepsilon)/\bar{n}}}{(x+1)^{\varepsilon}} & \text{if } n = 2\bar{n}; \\[2ex] \dfrac{(x^{\bar{n}} - 1)^{(2g+\varepsilon)/\bar{n}}}{(x-1)^{\varepsilon}} & \text{if } n = \bar{n} \text{ and } \bar{n} \text{ is odd}; \\[2ex] \dfrac{(x^{\bar{n}} - 1)^{(2g+2)/\bar{n}}}{(x^2-1)} & \text{if } n = \bar{n} \text{ and } \bar{n} \text{ is even.} \end{cases}$$

Restrictions on g and $\bar{n}$.

We defined ε so that

$$\varepsilon \equiv -2g \bmod \bar{n} \qquad \text{and} \qquad 0 \le \varepsilon < \bar{n}.$$

We can say more about ε, and hence about g and $\bar{n}$.

Theorem

- *We have* $\varepsilon \in \{0, 1, 2\}$.
- *Suppose* g *and* $\bar{n}$ *are even and* $n = \bar{n}$.
  Then $\bar{n} \equiv 2 \bmod 4$, *and if* $\bar{n} > 2$ *then* $\varepsilon = 2$.
- *Suppose* g *and* $\bar{n}$ *are even and* $n = 2\bar{n}$. *Then* $\varepsilon = 0$.

Idea of the proof of the first theorem.

Let $\zeta_1, \ldots, \zeta_{2g}$ be the roots of f. For each divisor d of n, define

$$M_d = (\text{number of } \zeta \text{ that satisfy } \zeta^d = 1)$$

To determine f, it is enough to determine the M_d for all d.

Key idea: M_d is twice the genus of the quotient of C by $\langle \alpha^d \rangle$.

Quotients of hyperelliptic curves.

Let $\beta = \alpha^d$, and let $D = C/\langle\beta\rangle$. Goal: Compute genus h of D.

If $\iota \in \langle\beta\rangle$ then D has genus 0.

Otherwise, let $\overline{\beta}$ be the induced automorphism on $C/\langle\iota\rangle = \mathbb{P}^1$.
Set $m = \text{order}\,\beta = \text{order}\,\overline{\beta}$.

$$\begin{array}{ccc}
C & \xrightarrow[\text{degree } m]{\langle\beta\rangle} & D \\
\text{degree } 2 \Big\downarrow & & \Big\downarrow \text{degree } 2 \\
\mathbb{P}^1 & \xrightarrow[\text{degree } m]{\langle\overline{\beta}\rangle} & \mathbb{P}^1.
\end{array}$$

We understand the bottom map: In appropriate coördinates, it's

$$x \mapsto x^m \qquad \text{or} \qquad x \mapsto x^p - x.$$

How are g and h related to one another?

$$\begin{array}{ccc} C & \xrightarrow{\langle\beta\rangle} & D \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \xrightarrow{\langle\overline{\beta}\rangle} & \mathbb{P}^1 \end{array}$$

Let $e = \begin{pmatrix} \text{\# points of } \mathbb{P}^1 \text{ ramified in both} \\ \text{the right and the bottom map} \end{pmatrix}$

Proposition

We have $e \in \{0, 1, 2\}$, *and if* $\operatorname{char} k \neq 2$ *then*

	m *odd*	m *even*
$e = 0$	$h = (\ g + 1)/m - 1$	$h = (\ g + 1)/m - 1$
$e = 1$	$2h = (2g + 1)/m - 1$	$2h = (2g + 2)/m - 1$
$e = 2$	$h = g/m$	$h = (\ g + 1)/m$

Notice: If m and e are both even then g must be odd.

So if g is even:

	m odd	m even
$e = 0$	$2h = (2g + 2)/m - 2$	(not possible)
$e = 1$	$2h = (2g + 1)/m - 1$	$2h = (2g + 2)/m - 1$
$e = 2$	$2h = 2g/m$	(not possible)

Corollary

If g is even or m is odd, then e is determined by g and m:

- *If m is even then $e = 1$.*
- *If m is odd then $0 \leq e < m$ and $e \equiv 2g + 2 \bmod m$.*

Likewise, h is determined by g and m.

Note: Corollary is true in all characteristics.

The structure of the complete argument.

To recapitulate:

1. α is an automorphism of genus-g curve C.
2. By assumption, either g is even or the order of $\overline{\alpha}$ is odd.
3. Characteristic polynomial f of α^* is determined by the values of M_d for the divisors d of n.
4. Here M_d is number of roots ζ of f with $\zeta^d = 1$.
5. M_d is twice the genus of quotient of C by α^d.
6. By (2), either g is even or the order of $\overline{\alpha}^d$ is odd.
7. In this case, we have a formula for the genus of the quotient.

Completing the argument.

All that is left:

Show that the values of M_d we calculate agree with the values predicted by the f's in the theorem.

This is an easy exercise.

Example: Genus-2 curves.

$(n, \bar{n})$	characteristic polynomial
$(1, 1)$	$(x-1)^4$
$(2, 1)$	$(x+1)^4$
$(2, 2)$	$(x-1)^2(x+1)^2$
$(3, 3)$	$(x^2+x+1)^2$
$(4, 2)$	$(x^2+1)^2$
$(5, 5)$	$x^4+x^3+x^2+x+1$
$(6, 3)$	$(x^2-x+1)^2$
$(6, 6)$	$(x^2-x+1)(x^2+x+1)$
$(8, 4)$	x^4+1
$(10, 5)$	$x^4-x^3+x^2-x+1$

Characteristic polynomials for automorphisms of genus-2 curves. Igusa: The list is complete in characteristic $\neq 2, 3$.

The end.

Fin