Gmail

Sam Schiavone <sam.schiavone@gmail.com>

Re: degree-7 Belyi maps on genus-3 curves (and degree 5 on genus 2)

9 messages

Noam D. Elkies <elkies@math.harvard.edu> Tue, Jul 17, 2018 at 1:11 PM
To: jvoight@gmail.com
Cc: sam.schiavone@gmail.com, michaelmusty@gmail.com

John Voight <jvoight@gmail.com> writes:

```
> I had some partial success this morning: for
>
> > sigma;
> [
>     (1, 2, 3, 4, 5, 6, 7),
>     (1, 3, 6, 4, 5, 2, 7),
>     (1, 2, 7, 3, 5, 6, 4)
> ]
>
> I compute the curve equation
>
> x^3*z - x^2*y^2 - 11*x^2*z^2 + 13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4 +
>     40*y^3*z - 156*y^2*z^2 + 144*y*z^3 - 297*z^4
>
> It's too nice not to be correct!  But I still need to compute the
> Belyi map, etc.
```

I believe it; the quartic seems to have good reduction away from {2,3,5,7}
as it should.

> So maybe this apparently huge genus 3 passport just has lots of
> curves over QQ!

Possibly. Though if I'm right about the Weil pairing then there should
be at least one pair over Q(sqrt(-7)).

Meanwhile, http://beta.lmfdb.org/Belyi/5T4/%5B5%2C5%2C5%5D/5/5/5/g2/a
isn't quite X_0(50) -- I should have realized this because its two
bielliptic quotients are the two elliptic curves of conductor 50
with 5-torsion, while X_0(50) is bielliptic but one of the quotients
is the sqrt(5) twist that has 3-torsion instead. But it's still
quite nice and it might yet have a modular interpretation of some
other kind. A much simpler model is Y^2 = 16 X^4 + 56 X^4 + 17 X^2 + 8,
which makes the Belyi function 1/f where

f = ((4*X^2+3)*Y + 16*X^5 + 40*X^3 + 5*X + 8) / 16 .

NDE

John Voight <jvoight@gmail.com> Tue, Jul 17, 2018 at 3:53 PM
To: "Noam D. Elkies" <elkies@math.harvard.edu>
Cc: Samuel Schiavone <sam.schiavone@gmail.com>, Michael Musty <michaelmusty@gmail.com>

> A much simpler model is Y^2 = 16 X^4 + 56 X^4 + 17 X^2 + 8,
> which makes the Belyi function 1/f where
>
> f = ((4*X^2+3)*Y + 16*X^5 + 40*X^3 + 5*X + 8) / 16 .

Should that be 16 X^6?

JV

Elkies, Noam <elkies@math.harvard.edu> Tue, Jul 17, 2018 at 4:13 PM
To: John Voight <jvoight@gmail.com>
Cc: Samuel Schiavone <sam.schiavone@gmail.com>, Michael Musty <michaelmusty@gmail.com>

John Voight <jvoight@gmail.com> writes:

>> A much simpler model is Y^2 = 16 X^4 + 56 X^4 + 17 X^2 + 8,
>> which makes the Belyi function 1/f where

>> f = ((4*X^2+3)*Y + 16*X^5 + 40*X^3 + 5*X + 8) / 16 .

> Should that be 16 X^6?

Sorry, it is indeed Y^2 = 16 X^6 + 56 X^4 + 17 X^2 + 8 .

(At first I thought you meant the term 16*X^5 in f; that one is right.)

Because the two bielliptic quotients are 3-isogenous,
the curve should have extra automorphisms, and indeed
the involution X --> (2X+3) / (4X-2) of the X-line lifts to
the genus-2 curve. (This involution of P^1, together with
X --> -X, generates a group S_3. As I told JV earlier this PM,
I suspect that we're dealing with a fiber product of the
quintic Belyi map P^1 --> P^1 with cycles 5, 32, 2111
with the S_3 Belyi map P^1 --> P^1.

NDE

John Voight <jvoight@gmail.com> Tue, Jul 17, 2018 at 4:35 PM
To: Noam Elkies <elkies@math.harvard.edu>
Cc: Samuel Schiavone <sam.schiavone@gmail.com>, Michael Musty <michaelmusty@gmail.com>

Just in case you were still wondering about this...

```
> f := 16*X^6 + 56*X^4 + 17*X^2 + 8;
> C := HyperellipticCurve(f);
> ReducedMinimalWeierstrassModel(C);
Hyperelliptic Curve defined by y^2 + (x^2 + x)*y = x^6 - 3*x^5 + 7*x^4 - 10*x^3
    + 7*x^2 - 3*x + 1 over Rational Field
Mapping from: CrvHyp: C to Hyperelliptic Curve defined by y^2 + (x^2 + x)*y =
    x^6 - 3*x^5 + 7*x^4 - 10*x^3 + 7*x^2 - 3*x + 1 over Rational Field
```

with equations :
1/2*$.1 + 1/4*$.3
-1/8*$.1^3 + 1/32*$.1*$.3^2 + 1/32*$.2
1/2*$.1 - 1/4*$.3
and inverse
-1/4*$.1 - 1/4*$.3
-1/4*$.1^2*$.3 - 1/4*$.1*$.3^2 - 1/2*$.2
-1/2*$.1 + 1/2*$.3
> GeometricAutomorphismGroup(C);
Permutation group acting on a set of cardinality 6
Order = 12 = 2^2 * 3
(1, 2, 3, 4, 5, 6)
(1, 6)(2, 5)(3, 4)

So yes, large automorphism group.

JV
[Quoted text hidden]

Elkies, Noam <elkies@math.harvard.edu> Tue, Jul 17, 2018 at 4:40 PM
To: John Voight <jvoight@gmail.com>
Cc: Samuel Schiavone <sam.schiavone@gmail.com>, Michael Musty <michaelmusty@gmail.com>

John Voight <jvoight@gmail.com> writes:

> Just in case you were still wondering about this...
>
>> f := 16*X^6 + 56*X^4 + 17*X^2 + 8;
>> C := HyperellipticCurve(f);
>> [. . .]
>> GeometricAutomorphismGroup(C);
> Permutation group acting on a set of cardinality 6
> Order = 12 = 2^2 * 3
> (1, 2, 3, 4, 5, 6)
> (1, 6)(2, 5)(3, 4)
>
> So yes, large automorphism group.

Thanks. But that only confirms what I just wrote.
What I don't know yet is the automorphism group of
your quartic with a degree-7 Belyi map. (Nor have I
verified the fiber-product picture of the genus-2 curve with
a quintic Belyi map, but that should be straightforward to check.)

NDE

Elkies, Noam <elkies@math.harvard.edu> Tue, Jul 17, 2018 at 5:45 PM
To: John Voight <jvoight@gmail.com>
Cc: Samuel Schiavone <sam.schiavone@gmail.com>, Michael Musty <michaelmusty@gmail.com>

Meanwhile, Magma won't run "GeometricAutomorphismGroup" on
a quartic plane curve C, but "AutomorphismGroup" does work;
combining your code with your suggestion of trying it over finite field

suggests that the geometric Aut(C) is Z/3Z. For example

```
> P<x,y,z> := ProjectiveSpace(FiniteField(11^2),2);
> #(AutomorphismGroup(Curve(P, x^3*z - x^2*y^2 - 11*x^2*z^2 + 13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4
+ 40*y^3*z - 156*y^2*z^2 + 144*y*z^3 - 297*z^4)));
```

returns 3, and likewise for each prime value of 11 up to 73
except that there are 6 automorphisms mod 19 (which I was not
able to find extra automorphisms mod 11 by going to the field of
11^4 or 11^6 elements). For some of those primes there are
already three automorphisms over the prime field. On further thought
those seem to be the primes congruent to 1 mod 3, so presumably
the field of definition of the nontrivial automorphisms is Q(sqrt(-3)).

I've now confirmed this (in 4 seconds), but my minimal knowledge of Magma
does not include how to extract the automorphisms reported by

```
_<u> := PolynomialRing(Rationals());
P<x,y,z> := ProjectiveSpace(NumberField(u^2+3),2);
G := AutomorphismGroup(Curve(P, x^3*z - x^2*y^2 - 11*x^2*z^2 +
13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4 + 40*y^3*z - 156*y^2*z^2 +
144*y*z^3 - 297*z^4));
#G;
```

NDE

John Voight <jvoight@gmail.com> Tue, Jul 17, 2018 at 9:36 PM
To: Noam Elkies <elkies@math.harvard.edu>
Cc: Samuel Schiavone <sam.schiavone@gmail.com>, Michael Musty <michaelmusty@gmail.com>

Hi Noam,

This is great. To make the $.1 go away, you just need to name the
generator of the number field; and to get the elements, you just need
to ask for generators:

```
> _<u> := PolynomialRing(Rationals());
> K<w> := NumberField(u^2+3);
> P<x,y,z> := ProjectiveSpace(K,2);
> G := AutomorphismGroup(Curve(P, x^3*z - x^2*y^2 - 11*x^2*z^2 +
> 13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4 + 40*y^3*z - 156*y^2*z^2 +
> 144*y*z^3 - 297*z^4));
> G.1;
Mapping from: Curve over K defined by
-x^2*y^2 - 11*y^4 + x^3*z + 13*x*y^2*z + 40*y^3*z - 11*x^2*z^2 - 40*x*y*z^2 -
    156*y^2*z^2 + 75*x*z^3 + 144*y*z^3 - 297*z^4 to Curve over K defined by
-x^2*y^2 - 11*y^4 + x^3*z + 13*x*y^2*z + 40*y^3*z - 11*x^2*z^2 - 40*x*y*z^2 -
    156*y^2*z^2 + 75*x*z^3 + 144*y*z^3 - 297*z^4
with equations :
1/4*(-w - 3)*x*y^3 + 1/4*(-11*w + 7)*y^4 + 1/4*(w + 3)*x^2*y*z - 9*x*y^2*z +
    1/2*(15*w + 25)*y^3*z + 1/4*(-w + 33)*x^2*z^2 + 1/4*(w - 69)*x*y*z^2 +
    1/2*(-123*w + 111)*y^2*z^2 + (27*w - 72)*x*z^3 + 1/2*(-33*w - 359)*y*z^3 +
    1/4*(-787*w + 799)*z^4
1/4*(w + 3)*x*y^3 + 1/4*(-w + 1)*y^4 + 1/4*(-w - 3)*x^2*y*z + (-w - 13)*y^3*z +
```

```
    1/4*(w + 3)*x^2*z^2 + 1/4*(-w + 33)*x*y*z^2 + 1/2*(21*w + 75)*y^2*z^2 -
    9*x*z^3 + (3*w - 67)*y*z^3 + 1/4*(-49*w + 169)*z^4
y^4 + 1/2*(-w - 5)*y^3*z + (-3*w + 6)*y^2*z^2 + 1/2*(15*w - 17)*y*z^3 + (-4*w +
    4)*z^4
and inverse
1/4*(w - 3)*x*y^3 + 1/4*(11*w + 7)*y^4 + 1/4*(-w + 3)*x^2*y*z - 9*x*y^2*z +
    1/2*(-15*w + 25)*y^3*z + 1/4*(w + 33)*x^2*z^2 + 1/4*(-w - 69)*x*y*z^2 +
    1/2*(123*w + 111)*y^2*z^2 + (-27*w - 72)*x*z^3 + 1/2*(33*w - 359)*y*z^3 +
    1/4*(787*w + 799)*z^4
1/4*(-w + 3)*x*y^3 + 1/4*(w + 1)*y^4 + 1/4*(w - 3)*x^2*y*z + (w - 13)*y^3*z +
    1/4*(-w + 3)*x^2*z^2 + 1/4*(w + 33)*x*y*z^2 + 1/2*(-21*w + 75)*y^2*z^2 -
    9*x*z^3 + (-3*w - 67)*y*z^3 + 1/4*(49*w + 169)*z^4
y^4 + 1/2*(w - 5)*y^3*z + (3*w + 6)*y^2*z^2 + 1/2*(-15*w - 17)*y*z^3 + (4*w +
    4)*z^4
> %P
_<u> := PolynomialRing(Rationals());
P<x,y,z> := ProjectiveSpace(NumberField(u^2+3),2);
G := AutomorphismGroup(Curve(P, x^3*z - x^2*y^2 - 11*x^2*z^2 +
13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4 + 40*y^3*z - 156*y^2*z^2 +
144*y*z^3 - 297*z^4));
G;
G.1;
G.2;
_<u> := PolynomialRing(Rationals());
K<w> := NumberField(u^2+3);
P<x,y,z> := ProjectiveSpace(K,2);
G := AutomorphismGroup(Curve(P, x^3*z - x^2*y^2 - 11*x^2*z^2 +
13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4 + 40*y^3*z - 156*y^2*z^2 +
144*y*z^3 - 297*z^4));
G.1;
```

It's frustrating that this isn't represented by a nice linear map, but
I suppose we could just interpolate that if we wanted to.

To really get this going, the next step is to compute the Belyi map so
we have the preimages of 0,1,oo to play with...

JV

[Quoted text hidden]

Noam D. Elkies <elkies@math.harvard.edu>
To: jvoight@gmail.com
Cc: sam.schiavone@gmail.com, michaelmusty@gmail.com

Wed, Jul 18, 2018 at 5:01 PM

I wrote:

```
>> I've now confirmed this (in 4 seconds), but my minimal knowledge of Magma
>> does not include how to extract the automorphisms reported by

>> _<u> := PolynomialRing(Rationals());
>> P<x,y,z> := ProjectiveSpace(NumberField(u^2+3),2);
>> G := AutomorphismGroup(Curve(P, x^3*z - x^2*y^2 - 11*x^2*z^2 +
>> 13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4 + 40*y^3*z - 156*y^2*z^2 +
>> 144*y*z^3 - 297*z^4));
```

>> #G;

John Voight <jvoight@gmail.com> replies:

> This is great. To make the $.1 go away, you just need to name the
> generator of the number field; and to get the elements, you just need
> to ask for generators:
>
> > _<u> := PolynomialRing(Rationals());
> > K<w> := NumberField(u^2+3); [...]

Thanks. I didn't even know how to get to the point where I'd see
the $.1 stuff.

> It's frustrating that this isn't represented by a nice linear map, but
> I suppose we could just interpolate that if we wanted to.

Yipes . . .

> To really get this going, the next step is to compute the Belyi map so
> we have the preimages of 0,1,oo to play with...

It turns out you've computed it already :-)

I mentioned already that I had computed coordinates of the curve's
24 Weierstrass points and found an imprimitive Galois orbit of 18
which was how I surmised the 3-cycle in the first place. I should
have paid more attention to the beginning of the factorization:
there's a double Weierstrass point, i.e. a point and where the
tangent line meets the curve with multiplicity 4. It is unique,
and thus must be fixed, together with the tangent line, by
any automorphism. So I changed coordinates to put that point and
its tangent line at a unit vector and a coordinate axis, and then used
the remaining freedom to find an even simpler model: starting from your

  Q(x,y,z) = x^3*z - x^2*y^2 - 11*x^2*z^2 + 13*x*y^2*z - 40*x*y*z^2 + 75*x*z^3 - 11*y^4 + 40*y^3*z - 156*y^2*z^2 + 144*y*z^3 - 297*z^4

(in gp syntax) I find that

  -Q(t + 10*u + 22/3, -t + u + 13/3, u - 5/3) / 12

is simply

(*) t^4 - 19*t^3 + 201*t^2 + (-45*u^3 - 3047/3)*t + 2916

which makes Aut(C) visible: just multiply u by cube roots of unity.

When I first surmised there was a 3-cycle, I leaped to the guess
that it had 3 different eigenvalues and the quotient curve had genus 1,
and that the Belyi map would be a fiber product from a Belyi map on
that quotient curve. I was then puzzled because I couldn't find
in your tables an appropriate degree-7 Belyi map on an elliptic curve.
But in fact here the quotient curve is rational: just the t-line.

So, I asked beta.lmfdb.org/Belyi for degree 7, ABC triple [7,3,3],
and genus zero, and got the unique hit

http://beta.lmfdb.org/Belyi/7T6/[7,3,3]/7/31111/331/g0/a

Let's conjugate the map by z <--> 1/z, to bring the fully ramified
points from zero to infinity in both the x and the phi coordinates;
I suggest you do this in general -- put the first point and the highest-
multiplicity preimage at infinity, and the second at 0, which tends to
produce simpler models, which are polynomials when, as here, there is
a fully ramified point. Here this makes Phi := 1/phi equal

(729*X^7 + 3402*X^5 + 1512*X^4 + 4725*X^3 + 5040*X^2 + 1792*X + 4096) / 3888
= (X+1) * (9*X^2 - 3*X + 16)^3 / 3888
= 1 + ((3*X+1)^3 * (27*X^4 - 27*X^3 + 144*X^2 - 80*X + 208) / 3888)

where X is your 1/x. We can get two genus-3 curves with
[7,7,7] Belyi maps maps from this. One is Phi - 1 = Tau^3, so Tau is
3*X+1 times a cube root of (27*X^4 - 27*X^3 + 144*X^2 - 80*X + 208) / 3888 .
Then that cube root generates 3:1 cyclic cover of the X-line on which
Tau is a Belyi function of degree 7. But you've not found that one yet.
Yours is obtained from a cube root of (Phi-1) / Phi -- so for this purpose
I might as well have stuck with your phi, which makes this 1 - phi.
This leads us to a cube root (27*X^4 - 27*X^3 + 144*X^2 - 80*X + 208) / (X+1),
or equivalently of 486*Z^4 - 557*Z^3 + 387*Z^2 - 135*Z + 27 where
X = 1/Z - 1. In (*) above, u was a cube root of 1/45 times
(t^4 - 19*t^3 + 201*t^2 + - 3047/3 + 2916) / t, or equivalently of
2916*z^4 - 3047/3*z^3 + 201*z^2 - 19*z + 1 where t = 1/z. Take
z = (-5*Z+3)/18, multiply by 17496/625 (the numerator is 8*3^7),
and we've identified our curve with 486*Z^4 - 557*Z^3 + 387*Z^2 - 135*Z + 27
up to cubic twist. Whew.

--NDE

Noam Elkies <elkies@math.harvard.edu> Thu, Jul 19, 2018 at 1:29 AM
To: jvoight@gmail.com, elkies@math.harvard.edu
Cc: sam.schiavone@gmail.com, michaelmusty@gmail.com

Correction -- I wrote

> [.....] We can get two genus-3 curves with [7,7,7] Belyi maps maps
> from this. One is Phi - 1 = Tau^3, so Tau is 3*X+1 times
> a cube root of (27*X^4 - 27*X^3 + 144*X^2 - 80*X + 208) / 3888 .
> Then that cube root generates 3:1 cyclic cover of the X-line on which
> Tau is a Belyi function of degree 7. But you've not found that one yet.

But you won't find it because we can't let one of the e=7 preimages
ramify further. Likewise for the cyclic cubic covers of genus-1 curves:
the triple cover must ramify only at the simple preimages of \infty,0,1.
So we don't get quite as many genus-3 covers this way as I imagined.

On the other hand, there's another such source: the three Galois orbits in
http://beta.lmfdb.org/Belyi/?deg=7&abc_list=[7,7,2]&g=1 (7,7,22111).
Here the fiber product will be one of the double covers of the

elliptic curves that are ramified at the three simple preimages
and one of the sevenfold ones.

Good night,
--NDE