Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Algebra 274 (2004) 772–803
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

The stack of Potts curves and its fibre at a prime of wild ramification

Matthieu Romagny [*]

Institut Fourier, BP 74, 38402 Saint Martin d'Hères cedex, France

Received 7 March 2003

Communicated by Laurent Moret-Bailly

Abstract

In this note we study the modular properties of a family of cyclic coverings of $\mathbb{P}^1$ of degree N, in all odd characteristics. We compute the moduli space of the corresponding algebraic stack over $\mathbb{Z}[1/2]$, as well as the Picard groups over algebraically closed fields. We put special emphasis on the study of the fibre of the stack at a prime of wild ramification; in particular we show that the moduli space has good reduction at such a prime.

Keywords: Covers of algebraic curves; Hurwitz moduli space; Algebraic stack; Wild ramification; Reduction mod p

We are interested here in algebraic curves called *N-state Potts curves*, previously studied here and there in the literature but not from a modular and arithmetic viewpoint. They provide an interesting example (quite unique in fact) of a stack of Galois covers where the study can be pursued quite far even at the primes of wild ramification. We discover interesting phenomena, as well as explanations and commentaries concerning the deformation theory of wild covers of curves (see [3]).

In the modular theory of covers of curves, much is known in the tame case where the characteristic $p \geqslant 0$ of the base field does not divide the indices of ramification: these covers form a smooth algebraic stack, and it is known how to compactify it with stable covers. By contrast, for example for a Galois cover of group G whose order is divisible by p, the (uni)versal deformation ring is very nasty (in general not even reduced), meaning that the

[*] Current address: Mathematisches Institut der Universitaet Bonn, Beringstrasse 1, 53115 Bonn, Germany.
E-mail addresses: romagny@math.uni-bonn.de, matthieu.romagny@ujf-grenoble.fr.

0021-8693/$ – see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2003.11.020

corresponding classifying stack is far from being smooth. Moreover, there exist smooth G-covers in characteristic 0 that do not have good (i.e., smooth) reduction to characteristic p, and vice versa there exist smooth G-covers in characteristic p that do not lift to characteristic 0. Giving a bridge between these characteristics usually means studying objects over a valuation ring of mixed characteristics $(0, p)$, and how they specialize or generalize. In the example of Potts curves everything can even be done over $\mathbb{Z}[1/2]$, and we will be able to describe quite precisely the behaviour at a prime of wild ramification.

Let us now describe in more detail the results of the article. Given an odd integer $N \geqslant 3$, an N-state Potts curve (or N-Potts curve) is by definition a smooth hyperelliptic curve of genus $N - 1$, which is a cyclic covering of $\mathbb{P}^1$ of degree N. We will simplify the treatment of hyperellipticity by avoiding the prime $p = 2$, and we will rather focus on wild ramification at primes dividing N. Hence in all the article the schemes and stacks considered are over $\mathbb{Z}[1/2]$. Thus the fibered category with objects N-Potts curves is an algebraic stack $\mathcal{P}_N$ over $\mathbb{Z}[1/2]$. Among the main results of the article is the following computation (Theorems 3.2.1 and 4.1):

- If N is not prime, the coarse moduli space of $\mathcal{P}_N$ is the scheme $\mathbb{A}^1_* \otimes \mathbb{Z}[\frac{\zeta_N+\zeta_N^{-1}}{2}, \frac{1}{2N}]$.
- If $N = p$ is prime, the coarse moduli space of $\mathcal{P}_p$ is the scheme $\mathbb{A}^1_* \otimes \mathbb{Z}[\frac{\zeta_p+\zeta_p^{-1}}{2}, \frac{1}{2}]$.

In this statement, $\mathbb{A}^1_* = \mathbb{A}^1 - \{0\}$ is the punctured line and the arithmetic rings that appear are subextensions of degree 2 of the ring of cyclotomic integers (see 1.4). Note that when N is a composite integer, there does not exist Potts curves in characteristics $p \mid N$. We see that, although the stacks (and moduli spaces) are connected for arithmetic reasons, at (geometric) primes of tame ramification they split as a sum of $\varphi(N)/2$ connected irreducible components, where φ is the Euler function. On the contrary, when $N = p$ is prime, we show that the moduli space "has good reduction" at p, that is to say its formation commutes with the base change $\mathbb{Z}[1/2] \to \mathbb{F}_p$:

- The coarse moduli space of $\mathcal{P}_p \otimes \mathbb{F}_p$ is $\mathbb{A}^1_* \otimes \frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}$, the fibre of the moduli space of $\mathcal{P}_p$ at p.

The result (Theorem 5.1.2) is even more precise and shows that the map from $\mathcal{P}_p \otimes \mathbb{F}_p$ to its moduli space is étale, and so this stack is connected but non-reduced with multiplicity $\varphi(p)/2$; its reduced part is smooth. Hence we can interpret the non-reducedness as coming from the collision of $\varphi(p)/2$ smooth components in characteristic 0 when we reduce to characteristic p.

We also compute the Picard groups of the geometric fibres of $\mathcal{P}_N \otimes k$ (k an algebraically closed field of characteristic $p \neq 2$). The first fact to be noted is that these groups are finite at primes of tame ramification, but not anymore at primes of wild ramification. The second interesting point is that the nilpotents contribute a lot to the Picard group of $\mathcal{P}_p \otimes \overline{\mathbb{F}}_p$, which would certainly not be the case for its moduli space P because it is an affine scheme, hence $\mathrm{Pic}(P_{\mathrm{red}}) = \mathrm{Pic}(P)$. The reason for this is of course the presence of automorphisms. Here is the result (Theorems 3.3.3 and 5.2.1):

- If $(N, p) = 1$ then the Picard group of any connected component of $\mathcal{P}_N \otimes k$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2N\mathbb{Z})$.
- If $N = p$ then the Picard group of $\mathcal{P}_p \otimes k$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times (1 + zA)$, where $A = \frac{k[z]}{z^{(p-1)/2}}\left[X, \frac{1}{X}\right]$ is the affine ring of the moduli space, and $1 + zA \subset A^\times$ is a multiplicative subgroup.

Finally we mention that in the tame case, it is likely that a little more work would give the expected results concerning the stack of *stable* N-Potts curves, namely, that its moduli space is $\mathbb{P}^1 \otimes \mathbb{Z}\left[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2N}\right]$. We will say no more than a word about this in 3.4. Concerning the stack of stable p-Potts curves over $\mathbb{Z}[1/2]$, similar questions arise but here the problems are of course more complicated. It is clear that the work done in the present article makes it tempting to ask what would stable p-Potts curves look like; if there is a 1-dimensional stack of stable N-Potts curves even over characteristics $p \mid N$; what are the stable reductions of N-Potts curves in characteristic p, when p divides a non-prime $N \ldots$ All this is left aside for the time being.

Here is a short overview of the organization of the article. In the text, the order of apparition of the results is actually rather different from the one above. The first section contains preliminaries on finite subgroups of the projective linear group PGL_2. The second section contains the computation of the automorphism groups of Potts curves. Here we make the essential observation that the good understanding of the stack $\mathcal{P}_N$ over $\mathbb{Z}[1/2N]$ is via the classical Hurwitz description of branched covers by the shape of the ramification. This leads us to start from a different definition for Potts curves, and of course we eventually show that the two coincide. In the third section, we treat the case of a composite N: we compute the moduli space of $\mathcal{P}_N$ and the Picard group of its fibres. In the fourth section we extend the construction of the moduli space to the case of the stack $\mathcal{P}_p$ with p prime. At last the fifth section is devoted to the study of the fibre of $\mathcal{P}_p$ at p.

Conventions

We will consider that every positive integer is prime to 0, so as not to make repeated particular cases when speaking of primality of an integer with the characteristic of a field. The Euler function is denoted by φ as usual. The cardinality of a finite set S is $|S|$. Finally, in a module M over a commutative ring A, we will denote by $m \propto m'$ the equality up to multiplication by an invertible element of A.

1. Preliminaries on Dickson's theorem

There is no pretense to originality in the contents of this section, but the results stated here could not be found in the literature. Because of their simplicity, proofs are sometimes elliptical, if not omitted. The reader may without prejudice skip this section and go straight to Section 2, referring to the results below when necessary.

In Section 2, in the course of the computation of the automorphism group of Potts curves over an algebraically closed field k of characteristic $p \neq 2$ (see 2.1.9 and 2.2.3), we will have to handle certain finite subgroups of $\mathrm{PGL}_2(k)$. Recall from [17, Chapter 3, Theorem 6.17] that Dickson's theorem for PGL_2 takes the following shape:

Theorem 1.1 (Dickson). *Let k be an algebraically closed field of characteristic $p \neq 2$. Any finite subgroup $G \subset \mathrm{PGL}_2(k)$ is isomorphic to a subgroup among the following list*:

- *If p is prime to $|G|$,*
  (1) *cyclic group, dihedral group, symmetric $\mathfrak{S}_4$, alternating $\mathfrak{A}_4$ or $\mathfrak{A}_5$.*
- *If p divides $|G|$,*
  (2) *$G = Q \rtimes C$ a semi-direct product of a normal, elementary abelian, p-Sylow Q by a cyclic group of order prime to p,*
  (3) *$\mathfrak{A}_5$ if $p = 3$,*
  (4) *$\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ for $q = p^s$, $s \geqslant 1$ integer.*

In this section we classify *conjugation* classes instead of merely *isomorphism* classes. We define an equivalence relation in $k^\times$ by $x' \sim x \Leftrightarrow x' \in \{x, x^{-1}\}$. The corresponding class is denoted $[x]$; the mapping $[x] \mapsto x + x^{-1}$ is a set-theoretic injection $k^\times/\sim \hookrightarrow k$. Finally let $\mu_n^* \subset k^\times$ be the set of primitive nth roots of unity (e.g., $\mu_p^* = \{1\}$).

Proposition 1.2. *Let $A \in \mathrm{PGL}_2(k)$ be an automorphism of finite order $n > 1$. Then,*

(i) *Either n is prime to p, or equal to p.*
(ii) *As an automorphism of $\mathbb{P}_k^1$, A is conjugated to $x \mapsto \zeta x$, for some $\zeta \in \mu_n^*$, when $(n, p) = 1$, and to $x \mapsto x + 1$, when $n = p$.*
(iii) *The set $\mu_n^*/\sim$ classifies conjugation classes of elements of order n, and more precisely,*

$$\mathrm{ord}(A) = n \quad \Leftrightarrow \quad \textit{there exists } [\zeta] \in \mu_n^*/\sim \textit{ such that}$$
$$\big(\zeta + \zeta^{-1} + 2\big)\det(A) - \mathrm{tr}(A)^2 = 0.$$

Proof. We work with a representative in $\mathrm{GL}_2(k)$, whose eigenvalues are given by the characteristic polynomial as $\lambda^\pm = (\mathrm{tr}(A) \pm \delta)/2$ with $\delta^2 = \mathrm{tr}(A)^2 - 4\det(A)$. In $\mathrm{PGL}_2(k)$, only the class (for the relation $\sim$) of the ratio $\zeta := \lambda^+/\lambda^-$ is well-determined.

We have $[\zeta] = 1$ if and only if, up to homothety, A is conjugated to a unipotent matrix, i.e. $n = p$ and, as a homography, A is conjugated to $x \mapsto x + 1$. We have $[\zeta] \neq 1$ if and only if A is conjugated to the diagonal matrix $\mathrm{diag}(\lambda^+, \lambda^-)$, and then A has order n if and only if $(n, p) = 1$ and $[\zeta] \in \mu_n^*/\sim$. As a homography, A is conjugated to $x \mapsto \zeta x$.

For the claim in (iii), one needs just checking that

$$\zeta + \zeta^{-1} = \frac{\mathrm{tr}(A) + \delta}{\mathrm{tr}(A) - \delta} + \frac{\mathrm{tr}(A) - \delta}{\mathrm{tr}(A) + \delta} = \frac{\mathrm{tr}(A)^2}{\det(A)} - 2. \qquad \square$$

Examples 1.3. As particular cases of 1.2(iii), an element $A \in \mathrm{PGL}_2(k)$ has order 2 (respectively order 3, 4, 6 or p) if and only if $\mathrm{tr}(A)^2 = i \det(A)$ for $i = 0$ (respectively $i = 1, 2, 3$ or 4).

Remark 1.4. Let ζ be a primitive nth root of unity (say as a complex number) and Φ_n the nth cyclotomic polynomial (of degree $\varphi(n)$). For future use, we observe that $(\zeta + \zeta^{-1})/2$

is integral over $\mathbb{Z}[1/2]$. Indeed its minimal polynomial over $\mathbb{Q}$ is $2^{-\varphi(n)/2}\psi_n(2t)$ where $\psi_n \in \mathbb{Z}[t]$ is the monic polynomial such that $\Phi_n(t) = t^{\varphi(n)/2}\psi_n(t + t^{-1})$. According to (iii) of the proposition we define an automorphism of the projective line over the spectrum of $\mathbb{Z}[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2n}]$, of exact order n on all the fibres, by the following matrix:

$$M_\zeta = \begin{pmatrix} \zeta + \zeta^{-1} & \zeta + \zeta^{-1} - 2 \\ 1 & 2 \end{pmatrix}.$$

Corollary 1.5. *Let $q = p^s$ for some $s \geqslant 1$. Then the order of an element $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ divides $q - 1$, $q + 1$, or p.*

Proof. Take A an element of order n prime to p. By Proposition 1.2, there exists $\zeta \in \mu_n^*$ algebraic over $\mathbb{F}_q$, of degree at most 2, such that A is conjugated to $x \mapsto \zeta x$. If $\zeta \in \mathbb{F}_q$, we have $\zeta^{q-1} = 1$. Else, the minimal polynomial of ζ over $\mathbb{F}_q$ is

$$P = X^2 + \left(2 - \frac{\mathrm{tr}(A)^2}{\det(A)}\right)X + 1.$$

But P can also be written $P = X^2 - (\zeta + \zeta^q)X + \zeta^{q+1}$ with the Frobenius $\mathrm{Fr}(x) = x^q$, generating $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q) = \mathbb{Z}/2\mathbb{Z}$. Hence $\zeta^{q+1} = 1$ and we are done. □

Corollary 1.6. *There are $q^2 - 1$ elements of order p in $\mathrm{PGL}_2(\mathbb{F}_q)$, and they all belong to $\mathrm{PSL}_2(\mathbb{F}_q)$. Moreover the set of fixed points of all order p elements of $\mathrm{PGL}_2(\mathbb{F}_q)$, acting on $\mathbb{P}^1(k)$, is $\mathbb{P}^1(\mathbb{F}_q)$.*

Proof. Simple calculations. □

In the sequel we use the concise notation $\langle\alpha(x)\rangle$ for the subgroup generated by a homography $\alpha \in \mathrm{PGL}_2(k)$.

Corollary 1.7. *The cyclic and dihedral subgroups of $\mathrm{PGL}_2(k)$ are conjugated to*:

(i) $\begin{cases} \mathsf{C}_n = \langle\zeta x\rangle & \text{for } (n, p) = 1 \text{ (any } \zeta \in \mu_n^*), \\ \mathsf{C}_p = \langle x + 1\rangle & \text{for } n = p. \end{cases}$

(ii) $\begin{cases} \mathsf{D}_n = \langle\zeta x, \frac{1}{x}\rangle & \text{for } (n, p) = 1 \text{ (any } \zeta \in \mu_n^*), \\ \mathsf{D}_p = \langle x + 1, -x\rangle & \text{for } n = p. \end{cases}$

Corollary 1.8. *The subgroups of $\mathrm{PGL}_2(k)$ isomorphic to $\mathfrak{S}_4$ ($p \neq 2, 3$) are conjugated to*

$$\mathsf{S}_4 = \left\langle ix, \frac{x+1}{x-1}\right\rangle \simeq \big\langle(1234), (12)\big\rangle.$$

Proof. Let $\nu : \mathfrak{S}_4 \xrightarrow{\sim} G$ be an isomorphism with values in a subgroup of $\mathrm{PGL}_2(k)$; $a = \nu(1234)$ and $b = \nu(12)$ generate G. Up to conjugation, $a(x) = ix$. A priori the involution b can be written $b(x) = (rx + s)/(tx - r)$; using the fact that $ab = \nu(134)$ has order 3, we get $r^2 = st$ (see 1.3). Conjugation by $\phi(x) = rx/t$ leaves a invariant while b maps to the desired $x \mapsto (x + 1)/(x - 1)$. To complete the proposition, one checks that these two elements generate a subgroup isomorphic to $\mathfrak{S}_4$. □

Corollary 1.9. *The subgroups isomorphic to* $\mathrm{PGL}_2(\mathbb{F}_q)$ *are all conjugated to the "standard"* $\mathrm{PGL}_2(\mathbb{F}_q)$ *corresponding to the field inclusion* $\mathbb{F}_q \hookrightarrow k$*; the same result holds for* $\mathrm{PSL}_2(\mathbb{F}_q)$*.*

Proof. The standard $\mathrm{PGL}_2(\mathbb{F}_q)$ is generated by the following three elements:

$$e(x) = x + 1, \qquad f(x) = ux, \qquad g(x) = 1/x$$

where u is any generator of the multiplicative group $\mathbb{F}_q^*$. Setting $m = (q - 1)/(p - 1)$ then $v = u^m$ is a generator of $\mathbb{F}_p^*$; in particular v is an integer modulo p. Then we have a relation $e^v f^m = f^m e$, it is just the homography $x \mapsto vx + v$. Also it is immediate that $n := \mathrm{ord}(eg)$ is prime to p.

Now let G be a subgroup of $\mathrm{PGL}_2(k)$, and $\nu : \mathrm{PGL}_2(\mathbb{F}_q) \to G$ be an isomorphism. Denote $\mathfrak{e} = \nu(e)$, $\mathfrak{f} = \nu(f)$, $\mathfrak{g} = \nu(g)$ so that $G = \langle \mathfrak{e}, \mathfrak{f}, \mathfrak{g} \rangle$. As $\mathfrak{f}$, $\mathfrak{g}$ generate a dihedral group, by the above result 1.7, with a first conjugation we can suppose that $\mathfrak{f} = f$ and $\mathfrak{g} = g$. The above relations in $\mathrm{PGL}_2(\mathbb{F}_q)$ yield:

(†) $\mathfrak{e}^p = 1$,
(††) $\mathfrak{e}^v \mathfrak{f}^m = \mathfrak{f}^m \mathfrak{e}$,
(†††) $(\mathfrak{e}\mathfrak{g})^n = 1$.

Let us write $\mathfrak{e}(x) = (ax + b)/(cx + d)$, then (†) reads $(a + d)^2 = 4(ad - bc)$ by 1.2. By induction,

$$\mathfrak{e}^k(x) = \frac{\left(\frac{k+1}{2}a - \frac{k-1}{2}d\right)x + kb}{kcx - \frac{k-1}{2}a + \frac{k+1}{2}d}.$$

We then write (††) explicitly and obtain $a = d$, and $c = 0$. At this point, $\mathfrak{e}(x) = x + b/a$. Then by (†††) and 1.2 there exists $\lambda \in \mu_n^* \subset \mathbb{F}_{q^2}^*$ such that

$$(1 + \lambda)^2 a^2 = -\lambda b^2.$$

As n divides $q - 1$ or $q + 1$ by 1.5, we have $\lambda + \lambda^{-1} \in \mathbb{F}_q$ and so $\beta := (b/a)^2 = -(\lambda + \lambda^{-1} + 2) \in \mathbb{F}_q$. Finally we apply a conjugation by $\phi : x \mapsto bx/a$, then $G = \langle x + b/a, ux, 1/x \rangle$ is mapped to $\langle x + 1, ux, 1/\beta x \rangle = \mathrm{PGL}_2(\mathbb{F}_q)$ as announced. The case of $\mathrm{PSL}_2(\mathbb{F}_q)$ is similar. □

2. Potts curves and their automorphisms

In this section we describe Potts curves defined over an algebraically closed field, before looking at families (hence moduli) in the rest of the article. Let us make precise definitions before we start: in all what follows, by a curve over a scheme S we will mean a proper, flat morphism $f:C\to S$ whose fibres are projective, geometrically connected and one-dimensional; also, except in 3.4, they will be assumed to be smooth. We recall that:

Definition 2.1. Let $N\geqslant 3$ be an odd integer. An N-Potts curve is a smooth hyperelliptic curve of genus $N-1$, which is a cyclic covering of $\mathbb{P}^1$ of degree N.

In Section 2.1 where N is prime to p, we have three main goals: showing the equivalence between two different definitions of Potts curves (2.1.5), giving a modular invariant (2.1.7), and computing automorphism groups (2.1.9 and 2.1.10). In Section 2.2 where p divides N, we also define an invariant and compute the automorphism groups (it turns out to be simpler).

2.1. Tame case

In this case, the curves we are dealing with can be described like in the classical Hurwitz setting, i.e., as maps to $\mathbb{P}^1$ with prescribed ramification. This is our starting point; it leads us to change Definition 2.1. Recall that if a finite group G acts faithfully on a smooth curve C over a field of characteristic p, such that $|G|$ and p are coprime, then the stabilizer of a fixed point is cyclic and its natural representation in the cotangent space of the point is faithful. This gives rise to the *Hurwitz ramification datum*, i.e., the list of all the corresponding characters at the fixed points.

Let $N\geqslant 3$ be an odd integer. Set $G=\mathbb{Z}/N\mathbb{Z}$, and assume that a generator for G, denoted g, has been chosen once for all. In the character group $\widehat{G}\simeq G$, we define an equivalence relation by $\chi'\sim\chi$ if and only if $\chi'\in\{\chi,\chi^{-1}\}$. Denote by $[\chi]$ the corresponding class.

Definition 2.1.1. Let k be an algebraically closed field of characteristic p prime to $2N$.

(i) An N-Potts curve of type $[\chi]$ over k is a curve C together with a faithful action $\rho:G\hookrightarrow \mathrm{Aut}_k(C)$ such that C/G has genus 0, with four ramification points all with stabilizer equal to G, and Hurwitz ramification datum $\{\chi,\chi,\chi^{-1},\chi^{-1}\}$. An N-Potts curve is an N-Potts curve of type $[\chi]$ for some $[\chi]$.

(ii) An isomorphism between two Potts curves C, C' is a G-equivariant isomorphism of algebraic curves $\varphi:C\xrightarrow{\sim}C'$.

Remarks 2.1.2.

(i) The action ρ being determined by $\sigma=\rho(g)$, a Potts curve will be denoted (C,σ). If (C,σ) and (C',σ') are isomorphic N-Potts curves then $[\chi]=[\chi']$.

(ii) Of course, from now up to 2.1.5 it is this definition that applies rather than Definition 2.1.

(iii) If σ acts via χ on the cotangent space m_a/m_a^2, then χ is determined by the root of unity $\zeta := \chi(\sigma)$. Hence, the quantity $\zeta + \zeta^{-1}$ is attached to C, and equivalent to $[\chi]$.

Hyperellipticity

Let (C, σ) be an N-Potts curve. By the Riemann–Hurwitz formula, we get the genus $g(C) = N - 1$. Notice that a birational equation can easily be drawn from the definition: by Kummer theory, the function field $k(C)$ is generated, as an extension of the rational function field $k(x)$, by a single $t \in k(C)$ such that $t^N \in k(x)$, i.e.,

$$t^N = \frac{(x-a)(x-b)}{(x-c)(x-d)} \tag{1}$$

according to the ramification. Substituting $t/(x-c)(x-d)$ to t we get

$$t^N = (x-a)(x-b)(x-c)^{N-1}(x-d)^{N-1}$$

where σ acts by $t \mapsto \zeta t$ for some ζ. Now in $\mathrm{Aut}_k(\mathbb{P}^1)$ there is one and only one subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generated by involutions that interchange the four points a, b, c, d (see [14, §1, Lemma 2]), namely

$$\tau_0 : \begin{cases} a \leftrightarrow b, \\ c \leftrightarrow d, \end{cases} \qquad \mu_0 : \begin{cases} a \leftrightarrow c, \\ b \leftrightarrow d, \end{cases} \qquad \tau_0\mu_0 = \mu_0\tau_0 : \begin{cases} a \leftrightarrow d, \\ b \leftrightarrow c. \end{cases}$$

In order to make the link between 2.1.1 and Definition 2.1 we must build a hyperelliptic involution from τ_0 and for that we need to recall the following classical construction:

2.1.3. It is known how to describe a tame cyclic covering of curves (or even, families of curves) in terms of invertible sheaves on the base. A perfect exposition is recalled in [2], so we just give a sketch here. For $n \geqslant 2$, let S be a scheme with $n \in \mathcal{O}_S^\times$, and $\zeta \in \mathcal{O}_S$ a primitive nth root of unity. Let $X \to S$ be a smooth curve, and σ an S-automorphism of order n. By smoothness the quotient morphism $f : X \to Y = X/\sigma$ is finite flat. By the assumption of invertibility of n, there is a decomposition $f_*\mathcal{O}_X = \bigoplus_{j=0}^{n-1} \mathcal{L}_j$ with $\mathcal{L}_j$ equal to the ζ^j-eigenspace for the action of σ. The $\mathcal{L}_j$ are invertible sheaves, and the multiplication in $f_*\mathcal{O}_X$ gives injective maps $\mathcal{L}_i \otimes \mathcal{L}_j \to \mathcal{L}_{i+j}$ ($i + j$ is read modulo n). In particular, as $\sigma^n = \mathrm{id}$, we get $\mathcal{L}_1^n \simeq \mathcal{O}_Y(-D)$ where D is the effective Cartier branch divisor of f.

Conversely, given $\mathcal{L} = \mathcal{L}_1$ and a global section s whose divisor of zeroes is D (so s is determined up to a global invertible section), we can reconstruct the $\mathcal{L}_j$ and endow $\mathcal{A} = \bigoplus_{j=0}^{n-1} \mathcal{L}_j$ with a product mapping $(\ell, \ell') \in \mathcal{L}_j \times \mathcal{L}_{n-j}$ to $s\ell\ell' \in \mathcal{O}_Y$, and we recover $X = \mathrm{Spec}(\mathcal{A})$.

As a conclusion, we can consider the datum of an S-curve X with an automorphism of order n as being equivalent, up to isomorphism, to that of a triple $(Y, \mathcal{L}, s)$ where $\mathcal{L} \in \mathrm{Pic}(Y)$ and s is a global section of $\mathcal{L}^{-n}$. Furthermore there is an obvious functoriality in $(Y, \mathcal{L}, s)$: for a map $(Y', \mathcal{L}', s') \to (Y, \mathcal{L}, s)$ given by an affine S-morphism $\alpha : Y' \to Y$

and a map $\beta : \mathcal{L} \to \alpha_* \mathcal{L}'$ respecting the sections, there is an induced morphism $h : X' \to X$ with $\sigma h = h\sigma'$.

Back to our situation, the action of σ on the Potts curve C is described by $\mathcal{L} = \mathcal{O}(-2)$ and $s = (X-a)(X-b)(X-c)^{N-1}(X-d)^{N-1}$. Clearly τ_0 gives an automorphism of the triple $(\mathbb{P}^1, \mathcal{L}, s)$, hence lifts to an automorphism $\tau : C \to C$.

Moreover, τ satisfies $\tau\sigma\tau^{-1} = \sigma$. Also we have that $\tau^2 = \sigma^j$ for some $j \in \mathbb{Z}/N\mathbb{Z}$, because it induces the identity on $\mathbb{P}^1$. But 2 being invertible modulo N, we may write $j = 2k$, and then, changing τ into $\tau\sigma^{-k}$ if necessary, we can assume that $\tau^2 = 1$.

As for μ_0, things are slightly different because it exchanges a, c and b, d. Let s' be the section $(X-c)(X-d)(X-a)^{N-1}(X-b)^{N-1}$ of $\mathcal{L} = \mathcal{O}(-2)$, then μ_0 gives a map between $(\mathbb{P}^1, \mathcal{L}, s)$ and $(\mathbb{P}^1, \mathcal{L}, s')$. The last triple gives rise to the same curve C of course, but with the automorphism σ^{-1}. So μ_0 lifts to $\mu : C \to C$ such that $\sigma^{-1}\mu = \mu\sigma$. As above, we may change μ so as to have $\mu^2 = 1$; then μ and σ generate a group isomorphic to the dihedral group $\mathbb{D}_N$.

Proposition 2.1.4. *C is hyperelliptic, and τ is the hyperelliptic involution.*

Proof. Using the fact that N and 2 are coprime, it is immediate that a point in C is fixed by τ if and only if its image in C/σ is fixed by τ_0. But the supports of the ramification loci for the quotients by τ and σ (i.e., their fixed points) are disjoint, because their images in C/σ are already. Hence we get $2N$ fixed points for τ, namely all the preimages of the fixed points of τ_0. They form two σ-orbits. Applying the Riemann–Hurwitz formula to the quotient $C \to C/\tau$ of degree 2:

$$2(N-1) - 2 = 2(2g_{C/\tau} - 2) + 2N$$

we have $g_{C/\tau} = 0$, as desired. □

Proposition 2.1.5. *Definitions* 2.1 *and* 2.1.1 *are equivalent.*

Proof. It only remains to prove the implication "2.1 ⇒ 2.1.1". But once again, using oddness of N, a point in C is fixed by σ if and only if its image in C/τ is fixed by σ_0 (the morphism induced from σ), and then the stabilizers are equal. An automorphism of $\mathbb{P}^1$ of order N has two fixed points with full stabilizer, and ramification characters inverses to each other. As the ramification loci for σ and τ are disjoint, the two points lifted in C give four fixed points with stabilizer $G = \mathbb{Z}/N\mathbb{Z}$ as in 2.1.1, and with the expected Hurwitz ramification datum. □

Remark 2.1.6. By the way, in [14], the definition chosen for Potts curves is a mix between ours: there, an N-Potts curve is a hyperelliptic curve of genus $N-1$, with an order N automorphism having exactly 4 fixed points.

Automorphisms

We will now compute the automorphisms of Potts curves (the results will be complete after Proposition 2.2.3). It should be said that similar computations of automorphism groups can be found in the literature, for example for general hyperelliptic curves in characteristic 0 (in [6]) or for curves that occur as cyclic coverings of $\mathbb{P}^1$ of degree prime to the characteristic (in [10]).

Using the quotient by τ we can get another affine equation for a Potts curve C. As a matter of fact, σ induces on $C/\tau \simeq \mathbb{P}^1$ an automorphism conjugated to $x \mapsto \zeta x$. The branch locus of τ is composed of two orbits of σ, i.e., $\{\zeta^j\alpha\} \cup \{\zeta^j\beta\}$ for $0 \leqslant j \leqslant N-1$, for certain α, β with α, β and 0 all distinct. The corresponding equation is

$$y^2 = \left(x^N - \alpha^N\right)\left(x^N - \beta^N\right) = x^{2N} + Ax^N + B. \tag{2}$$

We can recover (1) with the choice of a rational parameter for the conic $y^2 = u^2 + Au + B$ (e.g., with the coordinates $z = (y + \sqrt{B})/x^N$ and $t = x/((2\sqrt{B}\,)^{1/N})$, the equation is $t^N = (z-\lambda)/(z^2-1)$ with $\lambda = -A/(2\sqrt{B})$). The automorphisms σ, τ, μ have the following expressions on model (2):

$$\sigma(x,y) = (\zeta x, y); \qquad \tau(x,y) = (x,-y); \qquad \mu(x,y) = \left(\frac{B^{1/N}}{x}, \frac{\sqrt{B}y}{x^N}\right).$$

Let us define a modular invariant $j = B/(A^2 - 4B) \neq 0$ for a curve with Eq. (2). As is expected,

Proposition 2.1.7. *Two Potts curves (C,σ) and (C',σ') of invariants j and j' are isomorphic if and only if $j = j'$ and $[\chi] = [\chi']$.*

Proof. Let $\varphi : C \to C'$ be an isomorphism with $\sigma'\varphi = \varphi\sigma$. It induces a map $\tilde{\varphi} : C/\tau \to C'/\tau'$ on the quotients. Moreover, Proposition 1.2 says that for an automorphism of $\mathbb{P}^1$ of order prime to p, there is a unique coordinate x on $\mathbb{P}^1$ (up to $\sim$) such that the automorphism is a homothety. So if we consider equations of type (2) for C and C', then G-equivariance reads either $\tilde{\varphi}(\zeta x) = \zeta\tilde{\varphi}(x)$, or $\tilde{\varphi}(\zeta x) = \zeta^{-1}\tilde{\varphi}(x)$. In the first case we find $\tilde{\varphi}(x) = \lambda x$ for some λ, whence $A' = \lambda^N A$, $B' = \lambda^{2N} B$ and $j = j'$. In the second case we find $\tilde{\varphi}(x) = \lambda/x$ for some λ, whence $A' = \lambda^N A/B$, $B' = \lambda^{2N}/B$ and $j = j'$.

Conversely, assume that $j = j'$ and $[\chi] = [\chi']$ with C and C' given by Eq. (2). Then $\chi' =$ either χ or χ^{-1}. If $\chi' = \chi$ choose λ such that $A' = \lambda^N A$ and $B' = \lambda^{2N} B$; then $\varphi : (x,y) \mapsto (\lambda x, \lambda^N y)$ is a G-isomorphism from C to C'. If $\chi' = \chi^{-1}$ choose λ such that $A' = \lambda^N A/B$ and $B' = \lambda^{2N}/B$; then $\varphi : (x,y) \mapsto (\lambda/x, \sqrt{B}(\lambda/x)^N y)$ answers the question. □

Remark 2.1.8. Via j, there is a 1–1 correspondence between isomorphism classes of N-Potts curves and the sum of $\varphi(N)/2$ copies of $\mathbb{A}^1 - \{0\}$. Indeed, for fixed $[\chi]$ and $j \neq 0$, a curve with invariant j is given by the equation $y^2 = x^{2N} + (1+4j)x^N + j(1+4j)$ if $j \neq -1/4$, or by $y^2 = x^{2N} - 1$ if $j = -1/4$.

We are now in position to compute the automorphism groups of Potts curves, using the results of Section 1. On the way, we provide a correction to [14, Section 2, Proposition 5] where the case of $j = -1/4$ was forgotten.

Theorem 2.1.9. *Let $N \geqslant 3$ be an odd integer, and k an algebraically closed field of characteristic p prime to $2N$. Let (C, σ) be an N-Potts curve. Then the automorphism group of the curve C (alone) is the following*:

(i) *If $p \neq 3, 5$, $N = 3$, $j = -1/54$, then $\operatorname{Aut}_k(C) = \widetilde{\mathfrak{S}_4}$, the representation group of $\mathfrak{S}_4$ where the elements corresponding to transpositions have order* 2, *see* [17, Chapter 3, §2, (2.21)].

(ii) *If $p > 0$, $2N - 1 = q$ is a power of p, $j = -1/4$ (including the case $N = 3$, $p = 5$, $j = -1/54$), let $R \subset \mathbb{F}_{q^2}^\times$ be the subgroup of square roots of elements of $\mathbb{F}_q^\times$, then*

$$\operatorname{Aut}_k(C) = \mathrm{PGL}_2(\mathbb{F}_q) \times_{\mathbb{F}_q^\times} R$$

(the product is fibered with respect to the determinant and the square map $R \to \mathbb{F}_q^\times$).

(iii) *In all other cases, if $j \neq -1/4$ then $\operatorname{Aut}_k(C) = (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{D}_N$, and if $j = -1/4$ then $\operatorname{Aut}_k(C) = (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{D}_{2N}$.*

Proof. From now on we will denote by $O_\Gamma(x)$ the orbit of a point x under the action of a group Γ, and Γ_x its stabilizer. We know that τ has order 2 and is normal in $\operatorname{Aut}(C)$ (because of the uniqueness of the hyperelliptic involution), hence it is central. Denote $G = \operatorname{Aut}(C)/\langle\tau\rangle$ so that there is a central extension

$$1 \to \langle\tau\rangle \to \operatorname{Aut}(C) \to G \to 1. \tag{3}$$

When $f \in \operatorname{Aut}(C)$, f_0 denotes its image in G. Denote by $\Sigma = O_{\sigma_0}(\alpha) \cup O_{\sigma_0}(\beta)$ the set of the $2N$ branch points of τ, then by 2.1.3, G can be identified with the subgroup of $\operatorname{Aut}(\mathbb{P}^1)$ of the homographies stabilizing Σ. What we shall do is to determine G thanks to Dickson's list, and then find the class of the corresponding extension.

Notice that $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{D}_N \simeq \langle\tau, \sigma, \mu\rangle \subset \operatorname{Aut}(C)$ so that G contains a subgroup isomorphic to $\mathbb{D}_N$. Also G acts transitively on Σ, because $\mathbb{D}_N$ already does, and consequently

$$\forall s \in \Sigma, \quad 2N = \left|O_G(s)\right| = |G| / |G_s|.$$

Now, in four steps we read through the list in Dickson's theorem to find all possible G's. Before, we observe that we can allow conjugations of G in $\mathrm{PGL}_2(k)$ since it is just a change of variable on x in Eq. (2), so it does not change C up to isomorphism. That is why from Step 2 on, we shall identify G with the representatives given in Corollaries 1.7, 1.8, 1.9.

Step 1. *The groups that can not appear.*

First of all, neither the cyclic groups nor $\mathfrak{A}_4$ possess dihedral subgroups $\mathbb{D}_N$, so they are ruled out. Now, let us see that the occurrence of $G \simeq \mathfrak{A}_5$ is also impossible. The only dihedral subgroups in G are $\mathbb{D}_3$ and $\mathbb{D}_5$, whence $N = 3$ or 5. Assume $N = 3$; then we must have $G_s \simeq \mathbb{D}_5$ for some $s \in \Sigma$, because it is a subgroup of $\mathfrak{A}_5$ with 10 elements. Denote $H := \langle\sigma_0, \mu_0\rangle \simeq \mathbb{D}_3$; then one can show that $G_s \cap H \simeq \mathbb{Z}/2\mathbb{Z}$, and then there must be in H

a non trivial automorphism with a fixed point in Σ. This is a contradiction. When $N = 5$, just interchange the roles of $\mathbb{D}_3$ and $\mathbb{D}_5$ (the former stands for G_s, the latter for H), and the argument carries on. Also, note that this is true for any p (cases (1) and (3) of Dickson's Theorem 1.1).

Finally, a group of type $Q \rtimes C$ (case (2)) can not contain $\mathbb{D}_N$ with $(N, p) = 1$.

Step 2. *The case of* $G = \mathrm{PSL}_2(\mathbb{F}_q)$ *or* $\mathrm{PGL}_2(\mathbb{F}_q)$, $q = p^s$.

We proceed in three substeps.

(a) We show that Σ coincides with the set of fixed points of order p elements of G. Let Q be a p-Sylow of the stabilizer G_α, it is also a p-Sylow of G. If $g \in G$ has order p, then it belongs to some p-Sylow Q'. All Sylow subgroups are conjugated in G, so $Q' = tQt^{-1}$ and g fixes $t(\alpha) \in \Sigma$. Conversely, if $s \in \Sigma$, then G_s contains a p-Sylow of G, hence an element of order p. By Corollary 1.6, $\Sigma = \mathbb{P}^1(\mathbb{F}_q)$; in particular, $2N = |\Sigma| = q + 1$. In the sequel $\phi \in \mathbb{F}_{q^2}$ is a $2N$th root of unity such that $\zeta = \phi^2$; observe that $\phi + \phi^{-1}$ and $\zeta + \zeta^{-1}$ both belong to $\mathbb{F}_q$.

(b) We work out the curve and the group structure of $\mathrm{Aut}(C)$. By (a) we get the birational equation $y^2 = x^q - x$ with genus $(q - 1)/2 = N - 1$. Clearly $\mathrm{PGL}_2(\mathbb{F}_q) \subseteq G$ since it stabilizes $\mathbb{P}^1(\mathbb{F}_q)$. A priori G could be bigger, however the only subgroups of $\mathrm{PGL}_2(k)$ containing $\mathrm{PGL}_2(\mathbb{F}_q)$ are isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{q'})$ or $\mathrm{PGL}_2(\mathbb{F}_{q'})$, but then $q' = 2N - 1 = q$ and hence $G = \mathrm{PGL}_2(\mathbb{F}_q)$. In particular the group $\mathrm{PSL}_2(\mathbb{F}_q)$ is ruled out. Moreover, for an element $\gamma = \left(\begin{smallmatrix} a b \\ c d \end{smallmatrix}\right)$ and δ such that $\delta^2 = \det(\gamma)$, there is an automorphism

$$f_{\gamma,\delta}(x, y) = \left(\frac{ax + b}{cx + d}, \frac{\delta y}{(cx + d)^{(q+1)/2}}\right).$$

This is the fiber product structure stated in the theorem. We can now check that this is indeed a Potts curve by giving an element of order N in $\mathrm{PGL}_2(\mathbb{F}_q)$. For this just consider the matrix M_ζ of 1.4.

(c) At last we compute the invariant. In order to do this the quickest way is to notice that $\Sigma = \mathbb{P}^1(\mathbb{F}_q)$ is mapped to the $2N$th roots of unity via the following transformation

$$\gamma(x) = \frac{-x + 1 + \zeta^{-1}}{x - 1 - \zeta}.$$

Indeed, $u = \infty$ maps to -1 and for $u \in \mathbb{F}_q$ one has

$$\gamma(u)^{2N} = \gamma(u)^{q+1} = \left(\frac{-u^q + 1 + \zeta^{-q}}{u^q - 1 - \zeta^q}\right)\left(\frac{-u + 1 + \zeta^{-1}}{u - 1 - \zeta}\right) = 1$$

using that $u^q = u$ and $\zeta^q = \zeta^{-1}$. With the new variable $v = \gamma(x)$ we get an equation

$$w^2 = v^{q+1} - 1$$

and the invariant is $j = -1/4$.

Step 3. *The case of $G = \mathsf{S}_4 = \langle ix, (x+1)/(x-1)\rangle$ (for $N = 3$, see Corollary* 1.8).

This case can happen only if $p \neq 3$, cf. Theorem 1.1. Fix $\sqrt{i}$ a 8th root of unity and i its square. With the notations of Proposition 1.8, $x \mapsto ix$ is $\nu(1234)$ and $x \mapsto \frac{x+1}{x-1}$ is $\nu(12)$. Applying a permutation on $\{1, 2, 3, 4\}$ if necessary, we identify σ_0 and μ_0 with $\nu(123)$ and $\nu(12)$, respectively. For $s \in \Sigma$, its stabilizer G_s has cardinal 4, hence it is cyclic because two commuting involutions of $\mathbb{P}^1$ never have a common fixed point. We can choose s so that G_s is generated by $a_0(x) = ix$.

Now a_0 can not have a single fixed point lying in Σ, because else it would act freely on $\Sigma - \{s\}$, and hence its order would divide $2N - 1 = 5$. So the two fixed points $\{0, \infty\}$ are in Σ. The G-orbit of $\{0, \infty\}$ is $\{0, \infty, \pm 1, \pm i\} = \Sigma$. We can now give an equation

$$y^2 = x\bigl(x^4 - 1\bigr)$$

with the automorphisms

$$a(x, y) = \bigl(ix, \sqrt{i}y\bigr), \qquad \sigma(x, y) = \left(-i\frac{x-1}{x+1}, \frac{2\sqrt{2i}y}{(x+1)^3}\right),$$
$$\mu(x, y) = \left(\frac{x+1}{x-1}, \frac{2\sqrt{2}y}{(x-1)^3}\right), \qquad \lambda(x, y) = \left(-\frac{x-1}{x+1}, \frac{2\sqrt{2}y}{(x+1)^3}\right).$$

After after a conjugation changing σ_0 into $x \mapsto jx$ ($j \in \mu_3^*$) we obtain the "Potts" equation $y^2 = (x^3 - (2 + \sqrt{3})^3)(x^3 + 1)$. It allows to compute the invariant $j = -1/54$ but is less workable for the determination of the class of the extension (3). It can happen that $G \supsetneq \mathsf{S}_4$ only if G is $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$, and we know that this implies $q = 2N - 1 = 5$. When $p = q = 5$, we have $-1/54 = -1/4$, and according to what was done before, $G = \mathrm{PGL}_2(\mathbb{F}_5)$.

Now let us check, referring to the definition in [17, Chapter 2, §9, Definition 9.10], that $\mathrm{Aut}(C)$ is a representation group of $\mathfrak{S}_4$. This is the last step to prove (i) in the theorem; as it is quite technical and not needed in the sequel we remain sketchy. We adopt the notations of [17]. Denote $H = \mathrm{Aut}(C)$ and $Z = \langle\tau\rangle$. Assume L is a proper subgroup of H such that $H = ZL$, then $[H : L] = 2$, $L \cap Z = 1$, hence $H = Z \times L$ does not contain any element of order 8, contradicting the existence of a. Furthermore, denote by $M(G)$ the Schur multiplier, then $|Z| = |H' \cap Z| = 2 = |M(G)|$ by checking that $\tau = [\mu, \lambda]$ is a commutator. Third, obviously, $|H| = |G|.|M(G)|$. Then the result follows by [17, Chapter 3, §2, (2.21)].

Step 4. *The dihedral case $G = \mathsf{D}_M = \langle \varepsilon x, 1/x\rangle$, $\varepsilon \in \mu_M^*$, for $N \mid M$, see Corollary* 1.7.

It is the last possibility. For $w \in \mathbb{P}^1$ its D_M-orbit is

$$\bigl\{w, \varepsilon w, \dots, \varepsilon^{M-1}w, 1/w, \dots, \bigl(\varepsilon^{M-1}\bigr)/w\bigr\}.$$

This has cardinal 2 if $w = 0$ or ∞, $2M$ if w is in general position, and M if w is one of $\pm\sqrt{\varepsilon^j}$. We conclude that, in general, $M = N$; $M = 2N$ occurs when the points of the orbit are vertices of a regular $2N$-gon, yielding the equation $y^2 = x^{2N} - 1$. The invariant is then $j = -1/4$, and σ_0 has a "root" $\sqrt{\sigma_0}(x) = \zeta_{2N}x$. □

Corollary 2.1.10. *For all N, p, the group of automorphisms of (C, σ) is*:

$$\begin{aligned} j \neq -1/4: &\quad \mathrm{Aut}_k(C,\sigma) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z}), \\ j = -1/4: &\quad \mathrm{Aut}_k(C,\sigma) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2N\mathbb{Z}). \end{aligned}$$

Proof. The only non-obvious case is (ii) of the theorem. We keep the notations of Step 2 in the proof of the theorem. It suffices to check that the centralizer Z of σ_0 in $\mathrm{PGL}_2(\mathbb{F}_q)$ is cyclic of order $2N$. It is cyclic because, after a conjugation changing σ_0 into $x \mapsto \zeta x$, Z maps to a finite subgroup of $\mathbb{G}_m$. It has order $\leqslant 2N = q + 1$ by Corollary 1.5, observing that σ_0 is a power of a generator of Z. Finally it has order exactly $2N$ because there is in $\mathrm{PGL}_2(\mathbb{F}_q)$ an explicit square root for σ_0. Indeed, if σ_0 is given as above by the matrix M_ζ of 1.4, whose Cayley–Hamilton polynomial is $X^2 - (\zeta + \zeta^{-1})X + (\zeta + \zeta^{-1})$, one finds that $M_\zeta + (\phi + \phi^{-1})\,\mathrm{id}$ has a square equal to M_ζ in $\mathrm{PGL}_2(\mathbb{F}_q)$. □

2.2. Wild case

Now we study N-Potts curves when $p \mid N$. The ground field k is still assumed to be algebraically closed, of characteristic $p > 0$. Here it is Definition 2.1 that applies: the ramification data of Definition 2.1.1 do not make sense any more. As usual σ stands for the given automorphism of order N and τ is the hyperelliptic involution. Observe that if we have an isomorphism $\varphi : C \to C'$ between two Potts curves with $\varphi\sigma = \sigma'\varphi$, then it follows from unicity of the hyperelliptic involution that we also have $\varphi\tau = \tau'\varphi$.

As a matter of fact it is not so clear that such curves exist. Let (C, σ, τ) be an N-Potts curve with arbitrary N multiple of p. Then σ induces an automorphism of order N on the quotient $C/\tau \simeq \mathbb{P}^1$. By Proposition 1.2, the only possible case is

$$N = p,$$

and the induced automorphism σ_0 is $x \mapsto x + 1$ up to conjugation. As in Proposition 2.1.4, it is easy to count $2p$ fixed points for the hyperelliptic involution τ, they form two orbits of σ (just lift the 2 fixed points of the involution induced on C/σ). The corresponding affine model is

$$y^2 = \left(x^p - x\right)^2 + A\left(x^p - x\right) + B \quad (A, B \in k). \tag{4}$$

Hence, there exist N-Potts curves with $p \mid N$ exactly when $N = p$. In that case we define a modular invariant by

$$j = \frac{1}{A^2 - 4B}.$$

Proposition 2.2.1. *Two p-Potts curves (C,σ,τ) and (C',σ',τ') of invariants j and j' are isomorphic if and only if $j=j'$.*

Proof. Let $\varphi : C \to C'$ be an isomorphism with $\sigma'\varphi = \varphi\sigma$. It induces a map $\tilde{\varphi} : C/\tau \to C'/\tau'$ on the quotients. Moreover, again by 1.2 we can assume that both σ and σ' are $x \mapsto x+1$. So if we consider equations of type (4) for C and C', then G-equivariance reads $\tilde{\varphi}(x+1) = \tilde{\varphi}(x)+1$. It follows that $\tilde{\varphi}(x) = x+t$ and from this we deduce that $A' = A + 2(t^p - t)$ and $B' = B + (t^p - t)A + (t^p - t)^2$, and then $j' = j$.

Conversely if $j' = j$ then the choice of a root $t \in k$ of $t^p - t = (A' - A)/2$ satisfies also $B' = B + (t^p - t)A + (t^p - t)^2$. This ensures that $\varphi(x,y) = (x+t, y)$ defines an equivariant isomorphism between C and C' with Eqs. (4). □

Remark 2.2.2. Here, contrary to the tame case (compare with 2.1.7) there is no numerical invariant such as $[\chi]$ but only a continuous one. The computation of the moduli space in both cases will enlighten this in the next sections.

At last we compute the automorphism group of p-Potts curves. Let (C,σ,τ) be given by Eq. (4). Let r, s be the roots of $T^2 + AT + B$, and α (respectively β) a root of $T^p - T - r$ (respectively $T^p - T - s$), so that (4) reads

$$y^2 = \bigl(x^p - x - r\bigr)\bigl(x^p - x - s\bigr) = \prod_{i=0}^{p-1}(x - \alpha + i)\prod_{i=0}^{p-1}(x - \beta + i).$$

We have the following automorphisms:

$$\sigma(x,y) = (x+1, y); \qquad \tau(x,y) = (x, -y); \qquad \mu(x,y) = (\alpha + \beta - x, y).$$

Proposition 2.2.3. *Let (C,σ,τ) be a p-Potts curve, then* $\mathrm{Aut}_k(C) \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{D}_p$ *and* $\mathrm{Aut}_k(C,\sigma,\tau) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Proof. It is still true (cf. Theorem 2.1.9) that

(i) τ is of order 2, normal and central,

(ii) $G = \mathrm{Aut}(C)/\langle\tau\rangle$ is the subgroup of $\mathrm{Aut}(\mathbb{P}^1)$ of homographies stabilizing $\Sigma = O_{\sigma_0}(\alpha) \cup O_{\sigma_0}(\beta)$,

(iii) $\mathbb{D}_p \subset G$ and $2p = [G : G_x]$, $\forall x \in \Sigma$.

Let Q be a p-Sylow of G containing σ_0; by Dickson's theorem Q is elementary abelian. Assume that Q has order more than p, then there exists $\theta \in Q$ commuting with σ_0, hence $\theta(x) = x + u$, with $u \notin \mathbb{F}_p$. Moreover θ stabilizes Σ, and exchanges the orbits $O_{\sigma_0}(\alpha)$ and $O_{\sigma_0}(\beta)$ since $u \notin \mathbb{F}_p$. Therefore

$$(\exists i, j \in \mathbb{F}_p) \qquad \begin{cases} \alpha + u = \beta + i, \\ \beta + u = \alpha + j \end{cases}$$

which implies $u = (i + j)/2 \in \mathbb{F}_p$, a contradiction. Consequently $Q = \langle\sigma_0\rangle$; we can now read through the list in Dickson's theorem.

If $G = \mathrm{PSL}_2(\mathbb{F}_p)$ or $\mathrm{PGL}_2(\mathbb{F}_p)$, then G_α has order $(p^2 - 1)/d$ with $d = 2$ or 4. This is prime to p, hence G_α est cyclic, but this contradicts Corollary 1.5.

The only remaining possibility is $G = Q \rtimes C = \langle\sigma_0\rangle \rtimes \langle\varphi\rangle$, because $\mathfrak{A}_5$ is ruled out by the same arguments as in the case $(N, p) = 1$. The order of φ, denoted $2m$, is prime to p; changing the point α in the orbit if necessary, we can assume that its stabilizer is $G_\alpha = \langle\varphi^2\rangle$. As Q is normal, $\varphi^{-1}\sigma_0\varphi = \sigma_0^{\ell}$ for some $\ell \in \mathbb{F}_p^*$, from which we deduce that $\varphi(x) = \ell^{-1}x + b$ for some $b \in k$. As φ^2 fixes α, we derive $(\ell^2 - 1)\alpha = \ell(\ell + 1)b$. If $\ell + 1 \neq 0$ it implies $\varphi(\alpha) = \ell^{-1}\alpha + b = \alpha$; so $\ell = -1$, $\varphi^2 = 1$ and $m = 1$. □

We see that the remarkable symmetry previously obtained when $j = -1/4$ does not occur here in characteristic p. In particular, this implies that the p-Potts curve in characteristic 0 with invariant $j = -1/4$ can not have good reduction in characteristic p, i.e., that any model of C over a discrete valuation ring of residue characteristic p will have a singular special fibre.

This can be seen also directly as follows. Let R be a discrete valuation ring, K its fraction field, k its residue field, $\zeta \in R$ a pth root of unity. Assume that $\mathrm{char}(K) = 0$ and $\mathrm{char}(k) = p > 0$. Let C be the K-curve with invariant $j = -1/4$, with equation $y^2 = x^{2p} - 1$. Let $f : C \to \mathbb{P}^1$ be the hyperelliptic map and $\mathrm{Br} = \mathrm{Br}_1 \cup \mathrm{Br}_2 \subset \mathbb{P}^1$ its branch locus, i.e., $\mathrm{Br}_1 = \{1, \zeta, \ldots, \zeta^{p-1}\}$ and $\mathrm{Br}_2 = -\mathrm{Br}_1$. Consider the minimal model E of $(\mathbb{P}^1, \mathrm{Br})$ as a marked curve, possibly after a finite extension of R. The special fibre E_k is a chain of three projective lines, with the two tails marked by Br_1 and Br_2 respectively. Let $\mathcal{C}$ be the normalization of E in the function field of C. On the special fibre $\mathcal{C}$ has, over each tail of E_k, a component which is a hyperelliptic curve of genus $(p - 1)/2$. As $(p - 1)/2 + (p - 1)/2 = p - 1 = g(C)$, the curve $\mathcal{C}$ is semistable and the stable model of C is obtained by blowing-downs in $\mathcal{C}$. Thus C has bad reduction.

3. The stack $\mathcal{P}_N$ when N is composite

Let $N \geqslant 3$ be a non-prime integer fixed in the whole section. Let k be an algebraically closed field of characteristic $p \neq 2$. We established in the previous section that whenever p is prime to N, there is a bijection between isomorphism classes of N-Potts curves and a sum of $\varphi(N)/2$ copies of the affine punctured line $\mathbb{A}^1_* := \mathbb{A}^1 - \{0\}$ over k (see 2.1.8). Furthermore when p divides N we saw in 2.2 that there are no Potts curves at all. We now show (Theorem 3.2.1) that the coarse moduli space of the stack $\mathcal{P}_N$ is $\mathbb{A}^1_* \otimes \mathbb{Z}\big[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2N}\big]$ (which indeed splits as a disjoint sum over any field containing the Nth roots of unity). Here a couple of remarks are in order:

(i) To be more precise, in all what follows, whenever we write $\mathbb{Z}[1/2, \zeta]$ we mean the ring of cyclotomic integers, and whenever we write $\mathbb{Z}\big[1/2, \frac{\zeta+\zeta^{-1}}{2}\big]$, we mean its ring of invariants under $\zeta \mapsto \zeta^{-1}$. In other words, the former ring is $\mathbb{Z}[1/2][X]/(\Phi_N)$ and the latter is $\mathbb{Z}[1/2][X]/(\psi_N)$ where Φ_N and ψ_N are the cyclotomic polynomials of 1.4.

(ii) It will become clear while reading that everything in this section applies equally well to the tame stack $\mathcal{P}_p \otimes \mathbb{Z}[1/2p]$ when $N = p$ is prime.

As an immediate consequence we have a result of good reduction (3.2.2). In 3.3, we compute the modular Picard group of the fibres of the stack $\mathcal{P}_N$. At last we determine topologically the stable curves that are involved as stable limits in the process of compactification of the moduli space of $\mathcal{P}_N$, in 3.4.

3.1. Preliminaries

Definition 3.1.1. Let S be a scheme over $\mathbb{Z}[1/2]$. An N-Potts curve over S is a triple (C, σ, τ) composed of a smooth projective S-curve, and two automorphisms, $\sigma : C \to C$ of order N and $\tau : C \to C$ of order 2, such that the geometric fibers are Potts curves in the sense of Definition 2.1.

It follows from standard arguments that the stack $\mathcal{P}_N$ of N-Potts curves is a separated Deligne–Mumford stack over $\mathbb{Z}[1/2]$. Also, as N is non-prime, for any N-Potts curve over S, the base S factors through $\mathrm{Spec}(\mathbb{Z}[1/2N])$ (as we saw in 2.2). Then it seems that we might as well use:

Definition 3.1.2. Let S be a scheme over $\mathbb{Z}[1/2N]$. An N-Potts curve is a proper smooth morphism of schemes $f : C \to S$, together with an S-automorphism $\sigma : C \to C$ of order N, such that the geometric fibers (C_s, σ_s) are Potts curves in the sense of Definition 2.1.1.

This gives a much better understanding of the stack, so we will work with this definition. However, it raises the ambiguity of the existence of τ, which we now wipe out. Let $f : C \to S$ be a Potts curve over S in the sense of Definition 3.1.2 (remark: the type $[\chi]$ is locally constant over S).

Lemma 3.1.3. *There exists an involution $\tau : C \to C$ such that $f : C \to S$ becomes a family of hyperelliptic curves* (*in the sense of* [9, Definition 5.4 and Theorem 5.5]).

Proof. Let $G = \langle\sigma\rangle$. As C is projective over S, the quotient $D = C/G$ exists; by smoothness the quotient map $\pi : C \to D$ is finite flat of degree N. As $N \in \mathcal{O}_S^\times$ its formation commutes with base change (see [8, A7.1.3.4]), as is also the case for the branch locus $B = \pi_*(C^G)$. In particular D is a $\mathbb{P}^1$-bundle over S and B is étale and finite of degree 4 over S. We may localize (in the étale topology) as much as desired, because by unicity the hyperelliptic involution will exist globally.

Hence we may assume that $S = \mathrm{Spec}(R)$ is affine, that $D = \mathbb{P}^1_R$, and B is a sum of four disjoint sections $\alpha, \beta, \gamma, \delta$. Write the sections as $\alpha = (a_1 : a_2), \ldots, \delta = (d_1 : d_2)$. We define a linear transformation of D by the matrix

$$\tau_0 = \begin{bmatrix} a_1b_1c_2d_2 - c_1d_1a_2b_2 & a_1c_1d_1b_2 + b_1c_1d_1a_2 - a_1b_1c_1d_2 - a_1b_1d_1c_2 \\ (a_1b_2 + a_2b_1)c_2d_2 - (c_1d_2 + c_2d_1)a_2b_2 & -(a_1b_1c_2d_2 - c_1d_1a_2b_2) \end{bmatrix}$$

(we mimic the expression in the case where the base is a field). Its determinant $\det(\tau_0) = -(a_1c_2 - a_2c_1)(a_1d_2 - a_2d_1)(b_1c_2 - b_2c_1)(b_1d_2 - b_2d_1)$ is indeed invertible, as is clear fibrewise, and τ_0 is involutive because of the vanishing of the trace (cf. 1.3). We must now lift it to C. By 2.1.3 the cyclic covering $\pi : C \to D = \mathbb{P}^1_R$ is described by $\mathcal{L} \simeq \mathcal{O}(-2)$ and a global section s of $\mathcal{L}^N$, with $\mathcal{L}^N \simeq \mathcal{O}(-\mathcal{D})$ where $\mathcal{D} = \alpha + \beta + (N-1)\gamma + (N-1)\delta$. By construction τ_0 respects the data $(\mathcal{L}, s)$, hence it lifts to an automorphism τ of C with $\tau\sigma = \sigma\tau$. As in the case of a single Potts curve, we can assume $\tau^2 = \mathrm{id}$. This completes the proof. □

3.2. The moduli space

We now compute the moduli space of $\mathcal{P}_N$. The proof below will in fact give a concrete expression of $\mathcal{P}_N$ as a quotient stack of an open subset in the affine 3-space of homogeneous polynomials of the form $H(X,Z) = UX^{2N} + AX^NZ^N + BZ^{2N}$ by the action of the group $(\mathbb{G}_m)^2$. The first $\mathbb{G}_m$ factor acts simply (and freely) by multiplication, and the second factor acts by $\lambda.H(X,Z) := H(\lambda X, Z)$ (this is just the isomorphism relation between Potts curves, see Proposition 2.1.7). This description is at least totally correct over an algebraically closed field. Being rather interested in the arithmetic and reduction of the moduli space, we will not insist on this aspect. Hence we will show:

Theorem 3.2.1. *The moduli space of $\mathcal{P}_N$ is $\mathbb{A}^1_* \otimes \mathbb{Z}[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2N}]$.*

To avoid heavy notations we will write P for $\mathbb{A}^1_* \otimes \mathbb{Z}[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2N}]$. We split the proof into two steps:

Step 1. *We build the morphism to the moduli space.*

Here again we will work étale locally on S, and take care that the construction of the morphism is canonical enough so that it descends. Notations are as above. By 3.1.3 there is an involution $\tau \in \mathrm{Aut}_S(C)$. Then $E = C/\tau$ is a $\mathbb{P}^1$-bundle over S, we denote by $r : C \to E$ the natural projection and by $q : E \to S$ the structure morphism. As σ commutes with τ it induces an automorphism of order N on E. The divisor of fixed points $T = E^\sigma$ is an étale cover of degree 2 of S, étale locally it is a sum of two disjoint sections $\Delta + \Delta'$. Choosing one of the two (say Δ) defines an invertible sheaf $\mathcal{O}(\Delta)$ of degree 1. We may call it $\mathcal{O}(1)$ and then $E \simeq \mathbb{P}(V)$ with $V = q_*\mathcal{O}(1)$. By disjointness, if L and M are the restrictions of $\mathcal{O}(1)$ to Δ and Δ' respectively (viewed as sheaves on S), then V splits as $L \oplus M$. By construction the action of σ is now diagonal, given by multiplication by two invertible global sections $s, t \in \Gamma(S, \mathcal{O}_S)^\times$. We can normalize by changing V into $V \otimes L^{-1}$, so that $L = \mathcal{O}_S$ and $s = 1$. Then as σ has order N, t is a primitive Nth root of unity.

Now let us consider the double cover $r : C \to E$. It is described by the decomposition $r_*\mathcal{O}_C = \mathcal{O}_E \oplus \mathcal{L}$ and by a "Weierstrass" section $\theta \in \Gamma(E, \mathcal{L}^{-2})$, well determined up to an element of $\Gamma(E, \mathcal{O}_E^\times)$ (see 2.1.3). Since $\mathcal{L}^{-1}$ has degree N on the fibres, we have $\mathcal{L}^{-1} \simeq \mathcal{O}(N) \otimes q^*K$ for some $K \in \mathrm{Pic}(S)$. Also as $\theta_{|\Delta}$ is everywhere nonzero (the fixed loci for the actions of G and τ are disjoint fibrewise), by restriction to $\varDelta$ we get $K^2 \simeq \mathcal{O}_S$, hence $\mathcal{L}^{-2} \simeq \mathcal{O}_E(2N)$. Consequently we can identify θ with a σ-invariant section of

$$\varGamma\big(E, \mathcal{O}_E(2N)\big) = \varGamma\big(S, \mathrm{Sym}^{2N}(V)\big) = \bigoplus_{j=0}^{2N} \varGamma\big(S, M^j\big).$$

The most convenient writing is to use global coordinates X, Z on $\mathbb{P}(V)$, with say X corresponding to M. Then $\theta \in \varGamma(S, \mathcal{O}_S \oplus M^N \oplus M^{2N})$, so $\theta \propto H = UX^{2N} + AX^N Z^N + BZ^{2N}$ for some sections U, A, B of $\mathcal{O}_S$, M^N and M^{2N} respectively (recall that $\propto$ means equality up to an invertible element). Looking locally on the fibers, one sees that U is invertible. Finally note that the smoothness of the fibres of C/S requires that the section θ has no multiple zero (on all fibres). This means that neither B nor $A^2 - 4UB$ vanish, hence there is a well-defined section $j = UB/(A^2 - 4UB) \in \varGamma(S, \mathcal{O}_S)^\times$. The assignments $F(\zeta) = t$ and $F(X) = j$ give a map $F : \mathbb{Z}[\zeta, \frac{1}{2N}][X, X^{-1}] \to \varGamma(S, \mathcal{O}_S)^\times$.

Now we proceed to check the independence of this map with respect to the choices made. In fact the only place where there is a different possibility is the choice of $\varDelta$ rather than $\varDelta'$. Choosing $\varDelta'$ is equivalent to exchanging the coordinates X, Z on $\mathbb{P}(V)$, so clearly j is unchanged. However t is changed into t^{-1}; so in any case if we set $F(\zeta + \zeta^{-1}) = t + t^{-1}$ then the map

$$\mathbb{Z}\left[\frac{\zeta + \zeta^{-1}}{2}, \frac{1}{2N}\right]\big[X, X^{-1}\big] \to \varGamma(S, \mathcal{O}_S)^\times$$

is independent of the choice. Eventually we have a map $S \to \mathbb{A}^1_* \otimes \mathbb{Z}\big[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2N}\big] = P$. It is clear that the construction is functorial, providing a morphism $\varPhi : \mathcal{P}_N \to P$.

Step 2. *We check the properties of the moduli space.*

Recall that we must check two things: first, that for any geometric point $\mathrm{Spec}(k) \to \mathrm{Spec}(\mathbb{Z}[1/2])$, the morphism $\varPhi$ induces a bijection between isomorphism classes in $\mathcal{P}_N(k)$ and $P(k)$. If the characteristic of k divides N then it is clear because both are empty, and else this is exactly 2.1.8 (observe that $P \otimes k$ splits as $\varphi(N)/2$ copies of $\mathbb{A}^1_*(k)$). The second thing is to see that every map from $\mathcal{P}_N$ to an algebraic space factors through P. This can be done as in [12], using a family whose classifying morphism $S \to P$ is finite surjective (such a family is sometimes called *tautological*). For this we consider the one-parameter family C_0 with equation $y^2 = x^{2N} + \lambda x^N + 1$, over the base $S_0 = \mathrm{Spec}\big(\mathbb{Z}\big[\zeta, \frac{1}{2N}\big]\big[\lambda, \frac{1}{\lambda^2-4}\big]\big)$. (This is of course only an affine smooth curve; to make the definition rigorous we actually glue C_0 with another copy of itself, compatibly with the maps to S_0, along the open set $x \neq 0$, via the isomorphism $x' = 1/x$, $y' = y/x^N$). The data of ζ and of the invariant $j_0 = 1/(\lambda^2 - 4)$ determine a morphism $S_0 \to P$ which we denote by $\varPhi_0$. Now let $\varPsi : \mathcal{P}_N \to Q$ be a morphism of stacks to an algebraic space, and let $\varPsi_0 : S_0 \to Q$ be the morphism corresponding to $\Psi(C_0)$; let $\Gamma \subset P \times Q$ be the scheme-theoretic image of $h = (\Phi_0, \Psi_0)$.

$$\begin{tikzcd}
& S_0 \arrow[ddl, "\Phi_0"'] \arrow[d, "h"] \arrow[ddr, "\Psi_0"] & \\
& \Gamma \arrow[dl, "p_1"] \arrow[dr, "p_2"'] & \\
P \arrow[rr, dotted] & & Q
\end{tikzcd}$$

We observe that, Φ_0 being finite and p_1 separated, h is finite. In particular, h is closed, hence $\Gamma = h(S_0)$ as sets. Second notice that Γ is integral because S_0 is. Third p_1 is closed and bijective: it is closed and surjective because Φ_0 is, and injective because for $s, s' \in S_0$, $\Phi_0(s) = \Phi_0(s') \Rightarrow C_{0,s} \simeq C_{0,s'} \Rightarrow \Psi_0(s) = \Psi_0(s')$ (Q being a space). Thus p_1 is dominant, bijective and separable (since Φ_0 is), hence it is a birational map. At last, as P is normal, Zariski's Main Theorem states that p_1 is an isomorphism. Then the composition $p_2 \circ p_1^{-1} : P \to Q$ gives a morphism which factors Ψ.

Of course it must be said that P is not a fine moduli space. This is due to the presence of automorphisms; actually, in view of 2.1.10 we could get rid of the group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ by a process to be explained in 5.1.1, but the extra automorphism when $j = -1/4$ still causes ramification of j above $-1/4$:

$$j + \frac{1}{4} = \frac{A^2}{4(A^2 - 4B)}.$$

A consequence of the explicit construction of the classifying morphism is that obviously reduction modulo $\mathfrak{p}$ can be done at any prime $\mathfrak{p} > 2$. The result is straightforward:

Theorem 3.2.2. *Assume that $N \geqslant 3$ is a composite integer and that $\mathfrak{p} > 2$ is a prime. Then the moduli space of $\mathcal{P}_N$ has good reduction at $\mathfrak{p}$, i.e., the moduli space of $\mathcal{P}_N \otimes \mathbb{F}_\mathfrak{p}$ is the* (*possibly empty*) *fibre at $\mathbb{F}_\mathfrak{p}$ of the moduli space of $\mathcal{P}_N$.*

3.3. The Picard group

Let k be an algebraically closed field of characteristic p prime to $2N$. We are now going to compute the Picard group of the geometric fibre $\mathcal{P}_N \otimes k$. This will, in some sense, reveal that the *geometry* of the stack carries the dependence on N (whereas the subring of cyclotomic integers involved in the moduli space is of an *arithmetic* nature). Actually, as $\mathcal{P}_N \otimes k$ splits as a sum of isomorphic stacks $(\mathcal{P}_N \otimes k)_{[\chi]} = \mathcal{P}_{N,[\chi]}$ according to the classes of characters $[\chi]$, we will compute the Picard group of one of them.

We first briefly recall the definitions. The *étale site* of $\mathcal{P}_N$ has as open sets the étale morphisms $u : U \to \mathcal{P}_N$ from an algebraic space, denoted (U, u) or U. A map between two open sets U, V is a couple (f, α) with a morphism of algebraic spaces $f : U \to V$ and a 2-isomorphism $\alpha : v \circ f \xrightarrow{\sim} u$. Equivalently, it is a 2-commutative triangle with vertices $U, V, \mathcal{P}_N$. Briefly said, the coverings of (U, u) are the étale, surjective families $\coprod U_i \to U$, and the topology generated by all these is the *étale site* $(\mathcal{P}_N)_{\text{ét}}$. Finally an *invertible sheaf* L on $(\mathcal{P}_N)_{\text{ét}}$ is given by a collection of invertible sheaves $L|_U$ on U for every open set $U \to \mathcal{P}_N$, and isomorphisms $\ell_{f,\alpha} : f^*L|_V \xrightarrow{\sim} L|_U$ for all maps as above between open sets, such that any composition

$$U \xrightarrow{(f,\alpha)} V \xrightarrow{(g,\beta)} W$$

gives rise to an equality $\ell_{g\circ f,\alpha\circ f^*\beta} = \ell_{f,\alpha} \circ f^*\ell_{g,\beta}$. The Picard group is the set of isomorphism classes of invertible sheaves, endowed with the obvious tensor product.

Lemma 3.3.1. *There is a morphism of groups $\beta : \mathrm{Pic}(\mathcal{P}_{N,[\chi]}) \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$.*

Proof. We define it as Mumford does in [13]. Let L be an invertible sheaf on $\mathcal{P}_{N,[\chi]}$ and $U \to \mathcal{P}_{N,[\chi]}$ an open set, corresponding to an N-Potts curve (C, σ, τ) over U (we use Definition 2.1). In terms of the topology on $\mathcal{P}_{N,[\chi]}$, σ gives an automorphism of the open set U, so that there is an isomorphism $\ell_{\mathrm{id},\sigma} : L|_U \xrightarrow{\sim} L|_U$. It is given by an invertible global section of $\mathcal{O}_U$, and actually by the compatibility of L w.r.t composition this section is an Nth root of unity. Finally we get a morphism $U \to \mu_N$ to the scheme μ_N of Nth roots of unity.

It is clear that for a connected U the image in μ_N is constant; it is even independent of the chosen open set U, because the stack $\mathcal{P}_{N,[\chi]}$ is irreducible, so two nonempty open sets (U, u) and (V, v) have images that intersect in $\mathcal{P}_{N,[\chi]}$. In particular, if we choose U to be an atlas, one k-point $x \in U$ will give the curve C_x with the extra automorphism σ_0 whose square is σ (for the value $-1/4$ of the invariant). As above, we then get a point in μ_{2N}, and obviously its square is the point in μ_N computed before.

Now recall that a primitive Nth (respectively $2N$th) root of unity ζ (respectively $\phi = -\zeta$) is determined up to inversion by $[\chi]$. This yields an isomorphism $\mu_{2N} \simeq \mathbb{Z}/2N\mathbb{Z}$ mapping ϕ to 1, hence for given L there is a well-defined element $\beta_2(L) \in \mathbb{Z}/2N\mathbb{Z}$ computed with any nonempty open set U. The same works with the hyperelliptic involution τ; in order to keep additive notation we define $\varepsilon = \beta_1(L) \in \mathbb{Z}/2\mathbb{Z}$ to be such that $\ell_{\mathrm{id},\tau}$ is the multiplication by $(-1)^\varepsilon$. This completes the definition of $\beta = (\beta_1, \beta_2)$. □

As noticed in the proof, β is determined up to inversion of the generator in $\mathbb{Z}/2N\mathbb{Z}$. The following should now be quite close to intuition:

Lemma 3.3.2. *β is surjective.*

Proof. Let $U \to \mathcal{P}_{N,[\chi]}$ be an atlas, and $(f : C \to U, \tau, \sigma)$ be the corresponding curve. It is tempting, as in [13], to evaluate β on the Hodge bundle $L = \bigwedge^{N-1} f_*\Omega_C$ where Ω_C is the sheaf of differential 1-forms. Clearly we can compute β on the fibre of L over a single point of U, and of course we choose a point $x \in U$ whose fibre is the curve C_x with an extra automorphism σ_0 (for $j = -1/4$). Up to isomorphism C_x has equation $y^2 = x^{2N} - 1$. The basis of $\Gamma(C, \Omega_C)$ given by the forms $\omega_i = x^{i-1}dx/y$ for $1 \leqslant i \leqslant N-1$, has the virtue of diagonalizing the action of the group $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ generated by τ and σ_0. Indeed

$$\tau(\omega_i) = -\omega_i, \qquad \sigma_0(\omega_i) = \phi^i \omega_i.$$

Unfortunately we see that σ_0 maps $\omega_1 \wedge \cdots \wedge \omega_{N-1}$ to $(-1)^{(N-1)/2}$ times itself (as does τ) so we can not conclude. Thus taking maximal exterior power was too crude, but instead we can use the fact that $f_*\Omega_C$ is a G-sheaf, so

$$f_*\Omega_C = \bigoplus_{i=1}^{N-1} L_i$$

where $L_i = \ker(\sigma^* - \phi^i \mathrm{id})$ is an invertible sheaf. We obtain $\beta(L_1) = (1,1)$ and $\beta(L_2) = (1,2)$, that generate the image. □

The end result is very similar to the one in the elliptic case (see [13]):

Theorem 3.3.3. *β is injective, i.e.,* $\mathrm{Pic}((\mathcal{P}_N \otimes k)_{[\chi]}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2N\mathbb{Z})$.

Proof. Given an invertible sheaf L such that $\beta(L) = 0$, we show that $L|_U$ is trivial for any $u : U \to \mathcal{P}_N$. Let $f : C \to U$ be the corresponding curve, and let us simplify the notations to $\mathcal{P} := \mathcal{P}_{N,[\chi]}$ and $L := L|_U$. As in [13] we will show that L "descends" to the moduli space P, but we will write down carefully the argument (only allusive in [13]) since it involves nonflat descent. Consider the diagram

$$\begin{tikzcd} U \times_{\mathcal{P}} U \arrow[r, "a"] & U \times_P U \arrow[r, hook, "b"] & U \times_S U \arrow[r, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & U. \end{tikzcd}$$

Let $q_i := p_i \circ b \circ a$, then by definition of an invertible sheaf we have an isomorphism $\ell : q_1^*L \xrightarrow{\sim} q_2^*L$ between sheaves on $U \times_{\mathcal{P}} U$. But the latter space is just $I := \mathrm{Isom}(p_1^*C, p_2^*C)$, finite and unramified over $U \times_S U$. By definition of the coarse moduli space, $U \times_P U$ is the image of I in $U \times_S U$. So actually I is a "torsor" over $U \times_P U$, with structure group $G = \mathrm{Aut}((p_1 \circ b)^*C)$. We must be careful that G is not flat, so the meaning of a torsor here is just that $I \times I \simeq G \times I$. We have as usual an invariant pushforward a_*^G (pushing forward and then taking invariant sections) and it satisfies $a_*^G a^* F \simeq F$ for any locally free sheaf F of finite rank on $U \times_P U$. Here flatness of G is indeed unnecessary, if F is locally free: using that both I and G are affine over $U \times_P U$, we may locally reduce to the following situation of commutative algebra. We have $U \times_P U = \mathrm{Spec}(A)$, $I = \mathrm{Spec}(B)$, $G = \mathrm{Spec}(A[G])$ with a coaction $B \to A[G] \otimes B$ such that $A = B^G$; finally F is given by a free module M. It remains to check that $(M \otimes_A B)^G = M$ which is clear since M is free.

The initial assumption that $\beta(L) = 0$ says exactly that $\ell : q_1^*L \xrightarrow{\sim} q_2^*L$ is a G-equivariant isomorphism, so applying a_*^G we obtain an isomorphism $\psi : (p_1 \circ b)^*L \xrightarrow{\sim} (p_2 \circ b)^*L$. Fortunately, the stack $\mathcal{P}$ as well as its moduli space P are smooth, therefore the map $\mathcal{P} \to P$ is flat. Thus the map $U \to P$ is flat, and ψ is a descent datum for L. Finally L descends to P, so it is trivial since $\mathrm{Pic}(P) = \mathrm{Pic}(\mathbb{A}^1_* \otimes k) = 0$. □

3.4. Compactification by stable curves

It is known by the general theory of tame Hurwitz spaces that there exists a compactification $\overline{\mathcal{P}}_N$ for $\mathcal{P}_N$, classifying stable curves with action of $G = \mathbb{Z}/N\mathbb{Z}$. Let k an algebraically closed field of characteristic p prime to $2N$ like in the previous subsection; here we will just briefly find out the "cusps" of the geometric fibre $\overline{\mathcal{P}}_{N,[\chi]} = (\overline{\mathcal{P}}_N \otimes k)_{[\chi]}$, i.e., the points of the boundary.

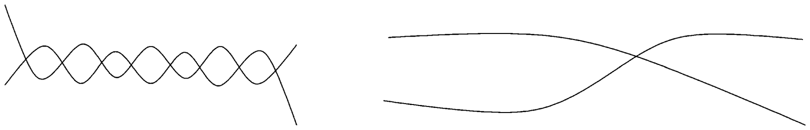
We refer to [5] for a precise definition of $\overline{\mathcal{P}}_N$; we will only need to know that there is a so-called "discriminant" morphism

$$\delta : \overline{\mathcal{P}}_{N,[\chi]} \to \overline{\mathcal{M}}_{0,(2,2)}$$

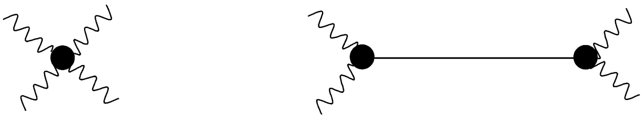
with values in the stack of curves of genus 0 with four marked points gathered by pairs. This morphism maps a Potts curve C to the quotient C/G marked by the branch points.

Recall the data $G = \mathbb{Z}/N\mathbb{Z}$, $g = N - 1$ and $\xi = \{\chi, \chi, \chi^{-1}, \chi^{-1}\}$ of Definition 2.1.1. In order to determine combinatorially the stable curves lying on the boundary $\partial\overline{\mathcal{P}}_{N,[\chi]}$ we use the combinatorial description of stable curves via their dual graph Γ, as in [5,7]. For a stable curve C, the graph Γ_C has the irreducible components of C as vertices, and the double points as edges.

Proposition 3.4.1. *The coarse moduli space of $\overline{\mathcal{P}}_{N,[\chi]}$ is $\overline{P} = \mathbb{P}^1 \otimes k$, and the two cusps are topologically the following two curves. The first has* 2 *branches isomorphic to* $\mathbb{P}^1$ *intersecting N times, and the second has* 2 *branches of genus* $(N-1)/2$ *intersecting in only one point.*



Proof. First, $\overline{P}$ is a normal proper curve of genus zero, hence it is $\mathbb{P}^1$. In dual graphs, we shall indicate marked points by wavy edges. Hence let (C, G) be a stable Potts curve. We have $\Gamma_\Sigma = \Gamma_C/G$, where $\Sigma = C/G$ has genus 0. We recall that $g' = \sum_i g_{\Sigma_i} + h^1(\Gamma_\Sigma)$, so that the irreducible components Σ_i of Σ are all rational, and that Γ_Σ is a (connected) tree. Taking into account the four marked points and the stability conditions, Γ_Σ must be one of the two graphs:



But, G being cyclic, a double point in C maps to a double point in Σ. Hence the first graph can not occur. So let C_i, $i = 1, 2$, be irreducible components of C above each of the components Σ_i of Σ, and intersecting at a point x. The stabilizer of x is $H = G_x$, and $h = [G : H]$ is its index. Take $a \in C_1$ a (smooth) ramification point; the stabilizer of C_1 is $G_1 = G$ because by assumption $G = G_a \subset G_1$. Similarly $G_2 = G$, thus C has only two irreducible components.

Now let us write the Riemann–Hurwitz formula for the quotient maps $\pi|_{C_i} : C_i \to C_i/G_i \simeq \Sigma_i \simeq \mathbb{P}^1$. There is only one orbit of double points, therefore their number is $[G : G_x] = h$:

$$2g_i - 2 = N(-2) + \underbrace{2(N-1)}_{(r)} + \underbrace{h(N-h)}_{(d)} = h(N-h) - 2, \quad \forall i = 1, 2,$$

where (r) is the contribution of the ramification points, and (d) the contribution of the double points. In particular $g_1 = g_2$, and we also know that $g(C) = N - 1 = g_1 + g_2 + h^1(\Gamma_C) = g_1 + g_2 + h - 1$. So, $h(N-h) = 2g_1 = N - h$, whence $h = N$ or 1.

Letting the family $y^2 = x^{2N} + 2x^N + t$ degenerate when $t \to 1$, we get $y^2 = (x^N + 1)^2$. In this way we see that the first cusp described above is the Potts curve of invariant $j = \infty$. Moreover, it is obvious that there is only one (isomorphism class of) Potts curve with this combinatorial aspect. A similar description with equations for the other cusp would be more tricky. However, since we know that the other cusp can not have the same combinatorics, we necessarily get the second picture for $j = 0$. □

4. Moduli space of $\mathcal{P}_p$

Theorem 4.1. *The moduli space of $\mathcal{P}_p$ is $\mathbb{A}^1_* \otimes \mathbb{Z}\left[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2}\right]$.*

The rest of this section is devoted to the proof of the theorem. We keep the former scheme of proof in two steps, but the complication coming from wild ramification implies that we won't be able to "normalize" the construction as well as before. Because of this we will need two additional lemmas. In the first, which we now state, it is only for later convenience that a primitive root of unity is denoted by t instead of ζ.

Lemma 4.2. *Let t, ψ be elements of a ring A, note $t^{[0]} = 0$ and $t^{[i]} = 1 + t + \cdots + t^{i-1}$ for $i \geqslant 1$. Let σ be the endomorphism of the graded polynomial A-algebra $A[X, Z]$ given by $\sigma(X) = tX + \psi Z$ and $\sigma(Z) = Z$. Then σ has exact order p after any base change $A \to A'$ if and only if $1 + t + \cdots + t^{p-1} = 0$ and $(t - 1, \psi) = A$. If this is so then the algebra of invariants $A[X, Z]^\sigma$ is generated by Z and the norm*

$$N(X, Z) = \prod_{i=0}^{p-1} \sigma^i(X) = \prod_{i=0}^{p-1} \left(X - t^{[i]}\psi Z\right).$$

Proof. It is clear that Z plays no role, so we can dehomogenize and make $Z = 1$. Clearly, $\sigma^p = \mathrm{id} \Leftrightarrow t^p = 1$ and $(1 + t + \cdots + t^{p-1})\psi = 0$. Now let A' run through all residue fields κ of A. Whenever $\bar{t} = 1$ in κ, the fact that σ has exact order p on the corresponding fibre implies $\overline{\psi} \neq 0$. This means that $(t - 1, \psi) = A$, hence $1 = u(t - 1) + v\psi$ for some u, v. From this we deduce that $1 + t + \cdots + t^{p-1} = 0$. Conversely this is easily seen to imply that σ has exact order p "universally".

As for the invariants we always have $A[N(X)] \subset A[X]^\sigma$. It is clear that we have equality when A is a field. In the general case, let M be the cokernel of the inclusion, it is a finite A-module. The crucial point is that, as the action is faithful fibrewise, the formation of $A[X]^\sigma$ commutes with base change (this is a special case of results concerning actions on smooth curves, see [4, Proposition 3.7]). So for every residue field we have $M \otimes \kappa = 0$. By Nakayama's lemma, it follows that $M = 0$. □

Remark 4.3. We recall that for a p-Potts curve (C, σ, τ) over an algebraically closed field, there are 2 fixed points in C for the action of σ, and each has conductor $m = 1$. This follows from the description made in 2.2.

Step 1. *We build the morphism to the moduli space.*

Here we keep the notations of the proof of 3.2.1. Let $(f : C \to S, \sigma, \tau)$ be a p-Potts curve over S in characteristic p. Let $C \xrightarrow{r} E \xrightarrow{q} S$ be the factorization of f through the quotient by τ. Then σ induces an automorphism of order p of E, still denoted σ. By the remarks above, the divisor of fixed points $T = E^\sigma$, finite of degree 2, is no longer étale but nevertheless fppf over S. In fact, locally for the fppf topology it is a sum of two disjoint sections $\Delta + \Delta'$, and above $S \otimes \mathbb{F}_p$ these sections have the same support but infinitesimally they might be distinct (see below).

From now on we work with the section Δ. Choosing $\mathcal{O}(1) := \mathcal{O}(\Delta)$, we set $V := q_*\mathcal{O}(1)$ so $E = \mathbb{P}(V)$. The section corresponding to Δ gives a surjective map $h : V \to M = \mathcal{O}(1)_{|\Delta}$, and unfortunately here we can not go further to split the bundle. But $\ker(h)$ is known to be $N_\Delta^\vee \otimes M$, with $N_\Delta^\vee$ the conormal sheaf of Δ in E: to see this, remember the fundamental exact sequence

$$0 \to \Omega^1_{\mathbb{P}(V)/S}(1) \to q^*V \to \mathcal{O}(1) \to 0$$

and restrict to Δ. Now $N_\Delta^\vee \simeq \mathcal{O}(-\Delta)_{|\Delta} \simeq \mathcal{O}(-1)_{|\Delta}$, so that $\ker(h) \simeq \mathcal{O}_S$. Hence we have an extension

$$0 \to \mathcal{O}_S \to V \to M \to 0.$$

Let us see now how σ acts on this. As an automorphism of E, it pulls back $\mathcal{O}(1)$ to an invertible sheaf of degree 1, i.e., there is an isomorphism $u_\sigma : \sigma^*\mathcal{O}(1) \simeq q^*K \otimes \mathcal{O}(1)$ for some $K \in \mathrm{Pic}(S)$. Moreover σ is the identity on Δ, so that restricting u_σ to Δ shows that K is trivial. Now σ is given by a surjective morphism of sheaves

$$q^*V \to \sigma^*\mathcal{O}(1) \overset{u_\sigma}{\simeq} \mathcal{O}(1).$$

Taking direct images by q, we obtain an automorphism $\varphi_\sigma : V \to V$. This map induces an automorphism of M and of $\ker(h) \simeq \mathcal{O}_S$, and is well determined up to an invertible global section of $\mathcal{O}_S$, but requiring $\varphi_\sigma|_{\mathcal{O}_S} = \mathrm{id}$ makes φ_σ canonical. Now the action on M is given by multiplication by a global section $t \in \Gamma(S, \mathcal{O}_S^\times)$, this means that if we choose locally a coordinate X for M as in the proof of 3.2.1, the action is

$$\begin{aligned} &\varphi_\sigma(X) = tX + \psi Z \quad \bigl(\text{for some } \psi \in \Gamma(M, \mathcal{O}_S)\bigr), \\ &\varphi_\sigma(Z) = Z. \end{aligned}$$

As σ has order p on the fibres, we have $1 + t + \cdots + t^{p-1} = 0$, and $t - 1$ and ψ generate $\mathcal{O}_S$, by Lemma 4.2. In particular, denoting by $\omega = t^{[1]} \dots t^{[p-1]}$ we have $p = \omega(t-1)^{p-1}$ (notations of Lemma 4.2).

The double cover r is described by the decomposition $r_*\mathcal{O}_C = \mathcal{O}_E \oplus \mathcal{L}$ and by a section $\theta \in \Gamma(E, \mathcal{L}^{-2})$, well determined up to an element of $\Gamma(E, \mathcal{O}_E^\times)$ (see the first step in the proof of 3.2.1). Also, $\mathcal{L}^{-2} \simeq \mathcal{O}_E(2p)$, so we can identify θ with a σ-invariant section of $\Gamma(E, \mathcal{O}_E(2p)) = \bigoplus_{j=0}^{2N} \Gamma(S, M^j)$. By Lemma 4.2 we get

$$\theta \propto H = UN(X,Z)^2 + AN(X,Z)Z^p + BZ^{2p}$$

for some sections U, A, B of $\mathcal{O}_S, M^p, M^{2p}$. As in the proof of 3.2.1 we see that U is invertible. Now we must express that the fibres of C/S are smooth, i.e., that θ has no multiple zero. To this aim we compute its discriminant, it turns out that

$$\mathrm{Res}\bigl(H, H'\bigr) = -U^p \omega^{2p} \delta^{p-1} \bigl(A^2 - 4BU\bigr)^p$$

where $\delta := H(-\psi, t-1) = U\psi^{2p} - A\psi^p(t-1)^p + B(t-1)^{2p}$ and we recall that $\omega = t^{[1]} \dots t^{[p-1]}$. In this expression both U and ω are invertible. So the smoothness condition is that $\mathrm{Res}(H, H')$, or equivalently $\delta(A^2 - 4UB)$, is invertible (remark: this contains the condition that $t-1$ and ψ generate $\mathcal{O}_S$). We are led to define

$$j = \frac{U(U\psi^{2p} - A\psi^p(t-1)^p + B(t-1)^{2p})}{A^2 - 4UB}.$$

It lies in $\Gamma(S, \mathcal{O}_S^\times)$ because numerator and denominator are invertible sections of M^{2p}. Also it is independent of the leading coefficient of H. If our invariant were merely the discriminant of H then, being intrinsic, it would be obviously invariant under changes of variables. Here this is not the case, so we will proceed to check this in the form of a lemma.

Lemma 4.4. *The definition of j is independent of the choice of coordinate X, Z and of the choice of section Δ.*

Proof. From now on we always normalize the expressions by setting $U = 1$. First, in the choice of the coordinate system the only loose variable is X so we can assume that

$Z' = Z$ and $X' = \alpha X + \beta Z$. Then $\sigma(X') = tX' + \psi'$ where $\psi' = \alpha\psi - (t-1)\beta$. The norm $N'(X', Z')$ with $t' = t$ and ψ' is

$$N'(X', Z') = \prod_{i=0}^{p-1} \bigl(X' - t^{[i]}\psi' Z'\bigr) = \prod_{i=0}^{p-1} \bigl(\alpha X + \beta Z - t^{[i]}\psi' Z\bigr).$$

Being φ_σ-invariant, this is a polynomial in N and Z^p, hence there exists ξ such that $N'(X', Z') = \alpha^p N(X, Z) + \xi Z^p$. The polynomial $H' = N'(X', Z')^2 + A'N'(X', Z')Z'^p + B'Z'^{2p}$ associated to θ can be expressed in terms of $N(X, Z)$ and Z^p (here H' is not the derivative of H!). As the change of variables $(N, Z^p) \leftrightarrow (N', Z'^p)$ has determinant α^p, the discriminant of H' viewed as a polynomial of degree 2 in (N, Z^p) is $\alpha^{2p}(A'^2 - 4B')$. Of course since $H \propto H'$ we have $H' = \alpha^{2p} H$. Computing discriminants gives $\alpha^{2p}(A'^2 - 4B') = \alpha^{4p}(A^2 - 4B)$. Then substituting $(X, Z) = (-\psi, t-1)$, first in $N' = \alpha^p N + \xi Z^p$, second in $H' = \alpha^{2p} H$, gives $\delta' = \alpha^{2p}\delta$. Finally $j' = \delta'/(A'^2 - 4B') = \delta/(A^2 - 4B) = j$.

Now, assume that we choose the section Δ' instead of Δ. It is not as obvious as in 3.2.1 that formally this has the effect of changing t to t^{-1}, and not even that the invariant will not change; so we sketch the details. The equation of Δ' is given by the new coordinate $Z' = \varphi_\sigma(X) - X = (t-1)X + \psi Z$. As we saw just above, we can choose X' as we like; to simplify matters we recall that there exist sections u, v such that $u(t-1) + v\psi = 1$ and we choose $X' = vX - uZ$ so as to have a unimodular change of variables

$$\left\{ \begin{array}{l} X' = vX - uZ \\ Z' = (t-1)X + \psi Z \end{array} \right\} \quad \Leftrightarrow \quad \left\{ \begin{array}{l} X = \psi X' + uZ' \\ Z = -(t-1)X' + vZ' \end{array} \right\}.$$

Then we have $\varphi_\sigma(X') = X' + vZ'$ and $\varphi_\sigma(Z') = tZ'$. The condition that φ_σ acts trivially on Z' leads to consider $\varphi'_\sigma = t^{-1}\varphi_\sigma$, and we obtain

$$\varphi'_\sigma\bigl(X'\bigr) = t^{-1}\bigl(X' + vZ'\bigr), \qquad \varphi'_\sigma\bigl(Z'\bigr) = Z'.$$

With $t' = t^{-1}$ and $\psi' = t^{-1}v$, the norm is $N'(X', Z') = \prod_{i=0}^{p-1}(X' - (t^{-1})^{[i]}t^{-1}vZ')$. Using that $-(t^{-1})^{[i]}t^{-1} = t^{[p-i]}$ we compute

$$N'(X', Z') = \prod_{i=0}^{p-1} \bigl(vX - uZ - t^{[i]}Z\bigr)$$

which is φ_σ-invariant, so there exists ξ such that $N'(X', Z') = v^p N(X, Z) + \xi Z^p$. Substituting $(X, Z) = (-\psi, t-1)$ yields immediately $-1 = -v^p\psi^p + (t-1)^p\xi$, so the change of variables between the invariants of degree p is unimodular:

$$\begin{cases} Z'^p = \psi^p Z^p + (t-1)^p N(X, Z), \\ N'(X', Z') = \xi Z^p + v^p N(X, Z). \end{cases}$$

Thus for $H' = N'(X', Z')^2 + A'N'(X', Z')Z'^p + B'Z'^{2p}$, its discriminant as a polynomial of degree 2 in (N, Z^p) is still $A'^2 - 4B'$. Now, when expressed in terms of (N, Z^p) the polynomial H' has leading coefficient $\delta' = H'(-t^{-1}v, t^{-1} - 1)$, so $H' = \delta' H$. Computing discriminants gives $A'^2 - 4B' = \delta'^2(A^2 - 4B)$, and substituting $(X, Z) = (-\psi, t-1)$ gives $1 = \delta'\delta$, so here again $j' = j$. □

Therefore the only change is that having chosen Δ' instead of Δ, we recover t^{-1} instead of t as a pth root of unity. So we have a well-defined map

$$\mathbb{Z}\left[\frac{\zeta + \zeta^{-1}}{2}, \frac{1}{2}\right]\left[X, X^{-1}\right] \to \Gamma(S, \mathcal{O}_S)^\times$$

if we set $F(\zeta + \zeta^{-1}) = t + t^{-1}$ and $F(X) = j$. Eventually we have a map $S \to \mathbb{A}^1_* \otimes \mathbb{Z}\left[\frac{\zeta+\zeta^{-1}}{2}, \frac{1}{2}\right] = P$. In fact we completed the construction after base change to $T = E^\sigma$, but the construction being canonical, by fppf descent we obtain a morphism defined on S. It is clear that the construction is functorial in S, providing a morphism $\Phi : \mathcal{P}_p \to P$.

Step 2. *We check the properties of a moduli space.*

Here, provided we give a family of Potts curves with a finite, surjective associated morphism to the moduli space, the arguments of the proof of 3.2.1 carry on. We consider the norm for $\psi = 1$, $N(x) = \prod_{i=0}^{p-1}(x - \zeta^{[i]})$ and the curve with equation $y^2 = N(x)^2 + \lambda N(x) + 1$, with invariant $j_0(\lambda) = (1 - \lambda(\zeta - 1)^p + (\zeta - 1)^{2p})/(\lambda^2 - 4)$, over the base

$$S_0 = \operatorname{Spec}\left(\mathbb{Z}\left[\zeta, \frac{1}{2}\right]\left[\lambda, j_0(\lambda), \frac{1}{j_0(\lambda)}\right]\right).$$

As in the proof of 3.2.1, to be rigorous we can easily give another smooth affine part for this curve, but we omit this detail. Then the proof of 3.2.1 works similarly, ending the proof of Theorem 4.1.

5. The fibre of $\mathcal{P}_p$ at the prime p

At last we study the stack of p-Potts curves in characteristic p, that is to say $\mathcal{P}_p \otimes \mathbb{F}_p$. First we compute its moduli space, along the same lines as above; the main difficulty here is that this space is not normal anymore, so we need the help of deformation theory as well as the operation of "2-quotient" of an algebraic stack (see [1,15]). The result shows that the moduli space of the $\mathbb{Z}[1/2]$-stack $\mathcal{P}_p$ has good reduction at p. Then, we compute the Picard group of $\mathcal{P}_p \otimes \mathbb{F}_p$.

5.1. Moduli space in characteristic p

We still assume that $p > 3$. Before we state the theorem, let us consider the problem of constructing the moduli space of the stack $\mathcal{P}_p \otimes \mathbb{F}_p$ along the same lines as above (Section 4). In the first step of the proof of 4.1 nothing needs any change (except perhaps the fact that ψ can be chosen to be equal to 1; this makes the computations slightly simpler but is anecdotical). We obtain a classifying morphism Φ from $\mathcal{P}_p$ to $P = \mathbb{A}^1_* \otimes \mathbb{F}_p\big[\frac{\zeta+\zeta^{-1}}{2}\big]$. Here, throughout the construction, $(\zeta + \zeta^{-1})/2$ is still a root of the polynomial ψ_p of 1.4, which is none other than the polynomial ψ of [3, 4.2.5 and 4.2.6]. In characteristic p we simply have $\psi(X) = X^{(p-1)/2}$, so $P = \mathbb{A}^1_* \otimes \frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}$.

The difference comes with the 2nd step where we must check the properties of a moduli space. The problem is that P is not a normal scheme anymore, so we will have to use a different strategy. One ingredient will be the "2-quotient" of an algebraic stack whose objects all possess a fixed finite group inside their automorphism group. Here is a brief summary of its properties ([15, Chapter I, Proposition 3.0.2] or [1, Proposition 3.5.1]):

Proposition 5.1.1. *Let S be a scheme and $\mathcal{M}$ an algebraic stack over S. Let G be a finite group, assume that for every object $x \in \mathcal{M}(T)$ there is an injection $i_x : G_T \hookrightarrow \mathrm{Aut}_T(x)$, whose formation is compatible with cartesian diagrams* (*see* [15]). *Then there exists an algebraic stack $\mathcal{M} /\!\!/ G$ and a map $f : \mathcal{M} \to \mathcal{M} /\!\!/ G$, such that f maps the elements of G to the identity, and is universal with respect to this property. The geometric points of $\mathcal{M} /\!\!/ G$ are the same as those of $\mathcal{M}$, but for x such a point we have $\mathrm{Aut}_{\mathcal{M}/\!\!/G}(x) = \mathrm{Aut}_{\mathcal{M}}(x)/G$. The formation of $\mathcal{M} /\!\!/ G$ commutes with base change on S. Moreover, f is an étale gerbe. The stack $\mathcal{M} /\!\!/ G$ has a coarse moduli space if and only if $\mathcal{M}$ has one, and if this is the case the moduli spaces are the same. Finally, if $\mathcal{M}$ is separated or proper, then $\mathcal{M} /\!\!/ G$ has the same properties.*

A basic example of this is given by the classifying stack BG of a finite abelian group G over a scheme S. Its objects are G-torsors, and G lies in all automorphism groups. In this case $\mathcal{M} = BG$, and $\mathcal{M} /\!\!/ G = S$. Now let us come back to the stack $\mathcal{P}_p \otimes \mathbb{F}_p$. We are going to show:

Theorem 5.1.2. *If $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, then we have an isomorphism*

$$(\mathcal{P}_p \otimes \mathbb{F}_p) /\!\!/ G \xrightarrow{\sim} \mathbb{A}^1_* \otimes \frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}.$$

In particular, $\mathbb{A}^1_* \otimes \frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}$ is the coarse moduli space of $\mathcal{P}_p \otimes \mathbb{F}_p$.

From Proposition 2.2.3 we know that p-Potts curves (over any base S/k) have the constant group scheme $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ as their automorphism group (use non-ramification of $\mathrm{Aut}_S(C, \sigma, \tau)$). Hence by definition of the 2-quotient the morphism Φ factors through

$$\Psi : (\mathcal{P}_p \otimes \mathbb{F}_p) /\!\!/ G \to \mathbb{A}^1_* \otimes \frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}$$

with the stack $\mathcal{Q} := \mathcal{P}_p \otimes \mathbb{F}_p /\!\!/ G$ representable by an algebraic space [11, 8.1.1]. Thanks to deformation theory, known from [3], we shall show that Ψ is étale:

Proposition 5.1.3. *Let (C,σ,τ) be a p-Potts curve over k. Then the ring that prorepresents the functor of deformations of C to local, artinian $\mathbb{F}_p$-algebras is $\frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}[\![t]\!]$.*

Proof. This is an example of the computation of deformations of $\mathbb{Z}/p\mathbb{Z}$-actions on smooth curves by Bertin and Mézard [3]. In their work everything is done over an algebraically closed field, as is usual in arithmetic geometry in mixed characteristic, but one can check that this assumption is not necessary in their article. Indeed the results they use are Schlessinger's criteria that need no assumption on the base field, and Serre's *Corps Locaux* that uses perfect fields. So their results are valid over $\mathbb{F}_p$.

Now, as τ has order 2 which is assumed to be prime to p, the deformation ring of (C,σ,τ) is the deformation ring of $(D=C/\tau,\sigma)$ (we still denote σ the automorphism induced on C/τ). We first look at deformations of (D,σ) to algebras over the ring of Witt vectors $W(\mathbb{F}_p)$, like in [3]. In the article, Corollary 3.3.5 shows that the universal deformation ring of (D,σ) is

$$R_{\text{gl}}=\big(R_1\widehat{\otimes}\cdots\widehat{\otimes}R_r\big)[\![U_1,\dots,U_N]\!]$$

with $N=\dim_k H^1(D/\sigma,\pi_*^\sigma(\mathcal{T}_D))$. Here there is only $r=1$ orbit of fixed points, with conductor $m=1$ (see Remark 4.3). Also $R_1=W(\mathbb{F}_p)[\![X]\!]/\psi(X)$ by [3, Theorem 4.2.8]. Finally, the computation of N is done in the course of the proof of Theorem 4.2.8, namely $N=1$. Reducing modulo p, we have $R_1/pR_1=\frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}$. We obtain the universal ring for deformations to $\mathbb{F}_p$-algebras as $\frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}[\![u]\!]$. □

Proof of Theorem 5.1.2 (*end*). As the 2-quotient $\mathcal{P}_p\otimes\mathbb{F}_p\to\mathcal{Q}$ is étale, it follows from the proposition that the extensions of complete local rings corresponding to Ψ are trivial, meaning that both Φ and Ψ are étale. A first consequence is that $\mathcal{Q}$ is not only an algebraic space, but in fact a scheme. Also, considering the scheme $\mathcal{Q}'$ defined by the fibre square:

$$\begin{tikzcd}
\mathcal{Q}' \arrow[r, "u'"] \arrow[d] & \mathbb{A}^1_*\otimes\mathbb{F}_p \arrow[d] \\
\mathcal{Q} \arrow[r, "u"] & \mathbb{A}^1_*\otimes\frac{\mathbb{F}_p[z]}{z^{(p-1)/2}}
\end{tikzcd}$$

we have that u' is étale, hence $\mathcal{Q}'$ reduced. Moreover u' is bijective, so by Zariski's Main Theorem for schemes u' is an isomorphism. So $\mathcal{Q}_{\text{red}}=\mathcal{Q}'$ is affine, which implies that $\mathcal{Q}$ itself is. Now using [16, Exposé I, Théorème 6.1] we get that u is an isomorphism. □

5.2. *The Picard group of $\mathcal{P}_p\otimes\mathbb{F}_p$*

Let k be an algebraically closed field of characteristic $p\neq 2$ (actually the assumption of algebraic closure will not be necessary). Let P be the moduli space of $\mathcal{P}_p\otimes k$ and $A=\frac{k[z]}{z^{(p-1)/2}}\big[X,\frac{1}{X}\big]$ its ring of functions. The adaptation of the arguments of 3.3 gives the following result:

Theorem 5.2.1. *There is an isomorphism* $\mathrm{Pic}(\mathcal{P}_p \otimes k) \simeq \mathbb{Z}/2\mathbb{Z} \times (1 + zA)$ *where* $1 + zA$ *is a subgroup of the multiplicative group of invertible elements in* A.

Proof. Put $\mathcal{P} := \mathcal{P}_p \otimes k$. Let $U \to \mathcal{P}$ an open set of the étale site of $\mathcal{P}_p$, corresponding to a p-Potts curve (C, σ, τ) over U. We know that $\mathrm{Aut}_U(C, \sigma, \tau)$ is the constant group scheme $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then, as in 3.3.1, for any invertible sheaf L and any $g \in G$ we have an automorphism $\ell_{\mathrm{id},g} : L|_U \xrightarrow{\sim} L|_U$ given by a global section of $\mathcal{O}_U^{\times}$. This gives a map β from $\mathrm{Pic}(\mathcal{P})$ to the abelian group of homomorphisms of abelian sheaves over $\mathcal{P}$ from G to $\mathcal{O}_{\mathcal{P}}^{\times}$. Let $q : \mathcal{P} \to P$ be the map to the moduli space, then we have an exact sequence:

$$0 \to \mathrm{Pic}(P) \xrightarrow{q^*} \mathrm{Pic}(\mathcal{P}) \xrightarrow{\beta} \mathrm{Hom}_{\mathcal{O}_{\mathcal{P}}}\big(G, \mathcal{O}_{\mathcal{P}}^{\times}\big) \to 0.$$

Indeed, exactness in the middle is proved exactly by the proof of 3.3.3. The pullback q^* is injective because $\mathrm{Pic}(P) = 0$. The fact that β is surjective is also clear because, given a character $f : G \to \mathcal{O}_{\mathcal{P}}^{\times}$, we can twist the structure sheaf $\mathcal{O}_{\mathcal{P}}$ so as to define a sheaf L by $L|_U = \mathcal{O}_U$ for all U, and $\ell_{\mathrm{id},g} : \mathcal{O}_U \xrightarrow{\sim} \mathcal{O}_U$ equal to multiplication by $f(U)(g)$. This sheaf satisfies $\beta(L) = f$.

It remains to compute $\mathrm{Hom}(G, \mathcal{O}_{\mathcal{P}}^{\times})$, which is just the character group of G. Using adjunction and the property of the moduli space that $q_*\mathcal{O}_{\mathcal{P}} = \mathcal{O}_P$, we have

$$\mathrm{Hom}_{\mathcal{P}}\big(G, \mathcal{O}_{\mathcal{P}}^{\times}\big) = \mathrm{Hom}_P\big(G, \mathcal{O}_P^{\times}\big) = \mu_2(A) \times \mu_p(A) = \mathbb{Z}/2\mathbb{Z} \times (1 + zA)$$

and this is the result. □

Acknowledgments

It has been a long awaited moment the time to thank here my advisor José Bertin, who followed from the beginning the story of Potts curves, with a lot of energy and disponibility. Also I express warm thanks to Laurent Moret-Bailly and Ariane Mézard, who read former versions of this work. Their thorough reading and numerous comments were the source of many improvements. I am grateful to the referee who suggested a quick way to see that the exceptional Potts curve has bad reduction. Finally I acknowledge a grant from the EAGER network, hospitality of Stockholm University and the Institut Fourier in Grenoble where most of this work was done.

References

[1] D. Abramovich, A. Vistoli, Complete moduli for families over semistable curves, electronic preprint, arXiv: math.AG/9811059.

[2] A. Arsie, A. Vistoli, Stacks of cyclic covers of projective spaces, electronic preprint, arXiv: math.AG/0301008.

[3] J. Bertin, A. Mézard, Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques, Invent. Math. 141 (2000) 195–238.

[4] J. Bertin, A. Mézard, Induction and restriction in formal deformation of coverings, electronic preprint, arXiv: math.AG/0205228.

[5] J. Bertin, M. Romagny, Compactification des schémas de Hurwitz et applications, in preparation.

[6] R. Brandt, H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven, Manuscripta Math. 55 (1986) 83–92.

[7] P. Deligne, D. Mumford, The irreducibility of the space of curves of given genus, Publ. Math. Inst. Hautes Études Sci. 36 (1969) 75–109.

[8] N. Katz, B. Mazur, Arithmetic moduli of elliptic curves, in: Ann. of Math. Stud., vol. 108, Princeton University Press, 1985.

[9] S.L. Kleiman, K. Lønsted, Basics on families of hyperelliptic curves, Compositio Math. 38 (1979) 83–111.

[10] A. Kontogeorgis, The group of automorphisms of cyclic extensions of rational function fields, J. Algebra 216 (2) (1999) 665–706.

[11] G. Laumon, L. Moret-Bailly, Champs algébriques, in: Ergeb. Math. Grenzgeb. (3), vol. 39, Springer, 2000.

[12] D. Mumford, K. Suominen, Introduction to the theory of moduli, in: F. Oort (Ed.), Algebraic Geometry, Oslo, 1970, Wolters–Noordhoff, Groningen, 1972.

[13] D. Mumford, Picard groups of moduli problems, in: Proc. Conf. on Arith. Alg. Geom. at Purdue, 1963.

[14] S.-S. Roan, A characterization of "rapidity" curve in the Chiral Potts Model, Comm. Math. Phys. 145 (1992) 605–634.

[15] M. Romagny, Sur quelques aspects des champs de revêtements de courbes algébriques, Thesis, Institut Fourier, Université Grenoble 1, available at http://www-fourier.ujf-grenoble.fr/~romagny, 2002.

[16] A. Grothendieck et al., Revêtements étales et groupe fondamental (SGA1), in: Lecture Notes in Math., vol. 224, Springer-Verlag, 1971.

[17] M. Suzuki, Group Theory I, Springer-Verlag, 1980.