Lifting Artin-Schreier covers with maximal wild monodromy

P. Chrétien

May 1, 2014

Abstract
Let $k$ be an algebraically closed field of characteristic $p > 0$. We consider the problem of lifting $p$-cyclic covers of $\mathbb{P}^1_k$ as $p$-cyclic covers of the projective line over some DVR under the condition that the wild monodromy is maximal. We answer positively the question for covers birational to $w^p - w = tR(t)$ for some additive polynomial $R(t)$.

1 Introduction
Let $(R, v)$ be a complete discrete valuation ring of mixed characteristic $(0, p)$ with fraction field $K$ containing a primitive $p$-th root of unity $\zeta_p$ and algebraically closed residue field $k$. The stable reduction theorem states that given a smooth, projective, geometrically connected curve $C/K$ of genus $g(C) \geq 2$, there exists a unique minimal Galois extension $M/K$ called the monodromy extension of $C/K$ such that $C_M := C \times M$ has stable reduction over $M$. The group $G = \text{Gal}(M/K)$ is the monodromy group of $C/K$.

Let us consider the case where $\phi : C \to \mathbb{P}^1_K$ is a $p$-cyclic cover. Let $\mathcal{C}$ be the stable model of $C_M/M$ and $\text{Aut}_k(\mathcal{C}_k)^\#$ be the subgroup of $\text{Aut}_k(\mathcal{C}_k)$ of elements acting trivially on the reduction in $\mathcal{C}_k$ of the ramification locus of $\phi \times \text{Id}_M : C_M \to \mathbb{P}^1_M$ (see [Liu02] 10.1.3 for the definition of the reduction map of $C_M$). One derives from the stable reduction theorem the following injection

$$\text{Gal}(M/K) \hookrightarrow \text{Aut}_k(\mathcal{C}_k)^\#.$$  (1)

When the $p$-Sylow subgroups of these groups are isomorphic, one says that the wild monodromy is maximal. We are interested in realization of smooth covers as above such that the $p$-adic valuation of $|\text{Aut}_k(\mathcal{C}_k)^\#|$ is large compared to the genus of $\mathcal{C}_k$ and having maximal wild monodromy. Moreover,
we will study the ramification filtration and the Swan conductor of their monodromy extension.

Recall that a big action is a pair \((X, G)\) where \(X/k\) is a smooth, projective, geometrically connected curve of genus \(g(X) \geq 2\) and \(G\) is a finite \(p\)-group of \(k\)-automorphisms of \(X/k\) such that \(|G| > \frac{2p}{p-1}g(X)\). According to \cite{LM05} Theorem 1.1 II f), if \((X, G)\) is a big action, then one has that \(|G| \leq \frac{4p}{(p-1)^2}g(X)^2\) with equality if and only if \(X/k\) is birationally given by \(w^p - w = tR(t)\) where \(R(t) \in k[t]\) is an additive polynomial. In this case, \(G\) is an extra-special \(p\)-group and equals the \(p\)-Sylow subgroup \(G_{\infty,1}(X)\) of the subgroup of \(\text{Aut}_k(X)\) leaving \(t = \infty\) fixed.

This motivates the following question, with the above notations, given a big action \((C, G)\) such that \(|G| = \frac{4p}{(p-1)^2}g(X)^2\), is it possible to find a field \(K\) and a \(p\)-cyclic cover \(C/K\) of \(\mathbb{P}^1_K\) such that \(C_k \simeq X\), that \(G \simeq \text{Aut}(C_k)_{\#}\) is a \(p\)-Sylow subgroup of \(\text{Aut}(C_k)_{\#}\) and the curve \(C/K\) has maximal wild monodromy?

Let \(n \in \mathbb{N}\), \(q = p^n\), \(\lambda = \zeta_p - 1\) and \(K = \mathbb{Q}_p^{ur}(\lambda^{1/(1+q)})\). For any additive polynomial \(R(t) \in k[t]\) of degree \(q\), let \(X/k\) be curve defined by \(w^p - w = tR(t)\). In section \[3\] we prove the following

**Theorem 1.1.** There exists a \(p\)-cyclic cover \(C/K\) of \(\mathbb{P}^1_K\) such that \(C_k \simeq X\), one has \(G_{\infty,1}(X) \simeq \text{Aut}(C_k)_{\#}\) and the curve \(C/K\) has maximal wild monodromy \(M/K\). The extension \(M/K\) is the decomposition field of an explicitly given polynomial and the group \(\text{Gal}(M/K) \simeq \text{Aut}_k(C_k)_{\#}\) is an extra-special \(p\)-group of order \(pq^2\).

The group \(G_{\infty,1}(C_k) = \text{Aut}_k(C_k)_{\#}\) is endowed with the ramification filtration \((G_{\infty,i}(C_k))_{i \geq 0}\) which is easily seen to be:

\[G_{\infty,0}(C_k) = G_{\infty,1}(C_k) \supseteq \mathbb{Z}(G_{\infty,0}(C_k)) = G_{\infty,2}(C_k) = \cdots = G_{\infty,1+q}(C_k) \supseteq \{1\}.\]

Moreover, \(G := \text{Gal}(M/K)\) being the Galois group of a finite extension of \(K\), it is endowed with the ramification filtration \((G_i)_{i \geq 0}\). Since \(G \simeq G_{\infty,1}(C_k)\) it is natural to ask for the behaviour of \((G_i)_{i \geq 0}\) under \((\Pi)\), that is to compare \((G_i)_{i \geq 0}\) and \((G_{\infty,i}(C_k))_{i \geq 0}\). In the general case, the arithmetic is quite tedious due to the expression of the lifting of \(X/k\). Actually we could not obtain a numerical example for the easiest case when \(p = 3\). Nonetheless, when \(p = 2\), one computes the conductor exponent \(f(\text{Jac}(C)/K)\) of \(\text{Jac}(C)/K\) and its Swan conductor \(\text{sw}(\text{Jac}(C)/K)\):

**Theorem 1.2.** Under the hypotheses of Theorem \[\square\], if \(p = 2\) the lower ramification filtration of \(G\) is:

\[G = G_0 = G_1 \supseteq \mathbb{Z}(G) = G_2 = \cdots = G_{1+q} \supseteq \{1\}.\]
Then, \( f(\text{Jac}(C)/K) = 2q + 1 \) and \( \text{sw}(\text{Jac}(C)/\mathbb{Q}^\text{ur}_2) = 1 \).

Remarks:

1. In Theorem 1.1, one actually obtains a family of liftings \( C/K \) of \( X/k \) with the announced properties. It is worth noting that there are finitely many additive polynomials \( R_0(t) \in k[t] \) such that \( w^p - w = tR(t) \) is \( k \)-isomorphic to \( w^p - w = tR_0(t) \) (see [LM05] 8.2), so we have to solve the problem in a somehow generic way. In [CM11], we obtain the analogous of Theorem 1.1 and Theorem 1.2 for \( p \geq 2 \) in the easier case \( R(t) = t^q \).

2. For \( p = 3 \), the easiest non-trivial case is such that \( [M : K] = 243 \), that is why we could not even do computations using Magma to guess the behaviour of the ramification filtration of the monodromy extension for \( p > 2 \). Nonetheless, one shows that if \( p \geq 3 \), the lower ramification filtration of \( G \) is

\[
G = G_0 \supseteq G_1 \supseteq G_2 = \cdots = G_u = Z(G) \supseteq \{1\},
\]

where \( u \in 1 + q\mathbb{N} \).

3. The value \( \text{sw}(\text{Jac}(C)/\mathbb{Q}^\text{ur}_2) = 1 \) is the smallest one among abelian varieties over \( \mathbb{Q}^\text{ur}_2 \) with non tame monodromy extension. That is, in some sense, a counter part of [BK05] and [LRS93] where an upper bound for the conductor exponent is given and it is shown that this bound is actually achieved.

2 Background

**Notations.** Let \( (R, v) \) be a complete discrete valuation ring (DVR) of mixed characteristic \((0, p)\) with fraction field \( K \) and algebraically closed residue field \( k \). We denote by \( \pi_K \) a uniformizer of \( R \) and assume that \( K \) contains a primitive \( p\)-th root of unity \( \zeta_p \). Let \( \lambda := \zeta_p - 1 \). If \( L/K \) is an algebraic extension, we will denote by \( \pi_L \) (resp. \( v_L \), resp. \( L^\circ \)) a uniformizer for \( L \) (resp. the prolongation of \( v \) to \( L \) such that \( v_L(\pi_L) = 1 \), resp. the ring of integers of \( L \)). If there is no possible confusion we note \( v \) for the prolongation of \( v \) to an algebraic closure \( K^\text{alg} \) of \( K \).

1. **Stable reduction of curves.** The first result is due to Deligne and Mumford (see for example [Lin02] for a presentation following Artin and Winters).
Theorem 2.1 (Stable reduction theorem). Let $C/K$ be a smooth, projective, geometrically connected curve over $K$ of genus $g(C) \geq 2$. There exists a unique finite Galois extension $M/K$ minimal for the inclusion relation such that $C_M/M$ has stable reduction. The stable model $\mathcal{C}$ of $C_M/M$ over $M^\circ$ is unique up to isomorphism. One has a canonical injective morphism:

$$\text{Gal}(M/K) \hookrightarrow \text{Aut}_k(C_k).$$ (2)

Remarks:

1. Let’s explain the action of $\text{Gal}(K^\text{alg}/K)$ on $C_k/k$. The group $\text{Gal}(K^\text{alg}/K)$ acts on $C_M := C \times M$ on the right. By unicity of the stable model, this action extends to $\mathcal{C}$:

$\begin{array}{ccc}
C & \xrightarrow{\sigma} & C \\
\downarrow & & \downarrow \\
M^\circ & \xrightarrow{\sigma} & M^\circ
\end{array}$

Since $k = k^\text{alg}$ one gets $\sigma \times k = \text{Id}_k$, whence the announced action. The last assertion of the theorem characterizes the elements of $\text{Gal}(K^\text{alg}/M)$ as the elements of $\text{Gal}(K^\text{alg}/K)$ that trivially act on $C_k/k$.

2. If $p > 2g(C) + 1$, then $C/K$ has stable reduction over a tamely ramified extension of $K$. We will study examples of covers with $p \leq 2g(C) + 1$.

3. Our results will cover the elliptic case. Let $E/K$ be an elliptic curve with additive reduction. If its modular invariant is integral, then there exists a smallest extension $M$ of $K$ over which $E/K$ has good reduction. Else $E/K$ obtains split multiplicative reduction over a unique quadratic extension of $K$ (see [Kra90]).

Definition 2.1. The extension $M/K$ is the monodromy extension of $C/K$. We call $\text{Gal}(M/K)$ the monodromy group of $C/K$. It has a unique $p$-Sylow subgroup $\text{Gal}(M/K)_1$ called the wild monodromy group. The extension $M/M^{\text{Gal}(M/K)_1}$ is the wild monodromy extension.

From now on we consider smooth, projective, geometrically integral curves $C/K$ of genus $g(C) \geq 2$ birationally given by $Y^p = f(X) := \prod_{i=0}^t (X - x_i)^{n_i}$ with $(p, \sum_{i=0}^t n_i) = 1$, $(p, n_i) = 1$ and $\forall 0 \leq i \leq t, x_i \in \mathbb{R^\times}$. Moreover, we assume that $\forall i \neq j, v(x_i - x_j) = 0$, that is to say, the branch locus
$B = \{x_0, \ldots, x_t, \infty\}$ of the cover has equidistant geometry. We denote by $\text{Ram}$ the ramification locus of the cover.

Remark : We only ask $p$-cyclic covers to satisfy Raynaud’s theorem 1’ [Ray90] condition, that is the branch locus is $K$-rational with equidistant geometry. This has consequences on the image of (2).

Proposition 2.1. Let $T = \text{Proj}(M^o[X_0, X_1])$ with $X = X_0/X_1$. The normalization $\mathcal{Y}$ of $T$ in $K(C_M)$ admits a blowing-up $\mathcal{Y}$ which is a semi-stable model of $C_M/M$. The dual graph of $\mathcal{Y}_k/k$ is a tree and the points in $\text{Ram}$ specialize in a unique irreducible component $D_0 \simeq \mathbb{P}^1_k$ of $\mathcal{Y}_k/k$. There exists a contraction morphism $h : \mathcal{Y} \rightarrow \mathcal{C}$, where $\mathcal{C}$ is the stable model of $C_M/M$ and

$$\text{Gal}(M/K) \hookrightarrow \text{Aut}_k(\mathcal{C}_k)^\#,$$

where $\text{Aut}_k(\mathcal{C}_k)^\#$ is the subgroup of $\text{Aut}_k(\mathcal{C}_k)$ of elements inducing the identity on $h(D_0)$.

Proof. see [CM11]. □

Remark : The component $D_0$ is the so called original component.

Definition 2.2. If (3) is surjective, we say that $C$ has maximal monodromy. If $v_p(|\text{Gal}(M/K)|) = v_p(|\text{Aut}_k(\mathcal{C}_k)^\#|)$, we say that $C$ has maximal wild monodromy.

Definition 2.3. The valuation on $K(X)$ corresponding to the discrete valuation ring $R[X]_{(\pi_K)}$ is called the Gauss valuation $v_X$ with respect to $X$. We then have

$$v_X \left( \sum_{i=0}^{m} a_i X^i \right) = \min \{v(a_i), 0 \leq i \leq m\}.$$

Note that a change of variables $T = \frac{X - y}{\rho}$ for $y, \rho \in R$ induces a Gauss valuation $v_T$. These valuations are exactly those that come from the local rings at generic points of components in the semi-stable models of $\mathbb{P}^1_K$.

2. Extra-special $p$-groups. The Galois groups and automorphism groups that we will have to consider are $p$-groups with peculiar group theoretic properties (see for example [Hup67] Kapitel III §13 or [Suz86] for an account on extra-special $p$-groups). We will denote by $Z(G)$ (resp. $D(G)$, $\Phi(G)$) the center (resp. the derived subgroup, the Frattini subgroup) of $G$. If $G$ is a $p$-group, one has $\Phi(G) = D(G)G^p$. 

5
Definition 2.4. An extra-special $p$-group is a non abelian $p$-group $G$ such that $D(G) = Z(G) = \Phi(G)$ has order $p$.

Proposition 2.2. Let $G$ be an extra-special $p$-group.

1. Then $|G| = p^{2n+1}$ for some $n \in \mathbb{N}$.

2. One has the exact sequence
   
   $0 \rightarrow Z(G) \rightarrow G \rightarrow (\mathbb{Z}/p\mathbb{Z})^{2n} \rightarrow 0$.

3. The group $G$ has an abelian subgroup $J$ such that $Z(G) \subseteq J$ and $|J/Z(G)| = p^n$.

3. Galois extensions of complete DVRs. Let $L/K$ be a finite Galois extension with group $G$. Then $G$ is endowed with a lower ramification filtration $(G_i)_{i \geq -1}$ where $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i + 1\}$. The integers $i$ such that $G_i \neq G_{i+1}$ are called lower breaks. For $\sigma \in G - \{1\}$, let $i_G(\sigma) := v_L(\sigma(\pi_L) - \pi_L)$. The group $G$ is also endowed with a higher ramification filtration $(G_i')_{i \geq -1}$ which can be computed from the $G_i$’s by means of the Herbrand’s function $\varphi_{L/K}$. The real numbers $t$ such that $\forall \epsilon > 0$, $G^{t+\epsilon} \neq G^t$ are called higher breaks.

Lemma 2.1. Let $M/K$ be a Galois extension such that $\text{Gal}(M/K)$ is an extra-special $p$-group of order $p^{2n+1}$. Assume that $\text{Gal}(M^{Z(G)}/K)_2 = \{1\}$, then the break $t$ of $M/M^{Z(G)}$ is such that $t \in 1 + p^n\mathbb{Z}$.

Proof. According to Proposition 2.2, there exists an abelian subgroup $J$ with $Z(G) \subseteq J \subseteq G$ and $|J/Z(G)| = p^n$. Thus, one has the following diagram

Let $t$ be the lower break of $M/L$, then $t$ is a lower break of $M/F$ and $\varphi_{M/F}(t) = \varphi_{L/F}(\varphi_{M/L}(t))$ is a higher break of $M/F$. Since $\varphi_{M/L}(t) = t$, one
has \(\varphi_{M/F}(t) = \varphi_{L/F}(t)\). Since \(\text{Gal}(L/K)_2 = \{1\}\), one has \(\text{Gal}(L/F)_2 = \{1\}\) and \(\varphi_{L/F}(t) = 1 + \frac{t}{p^n}\). The Hasse-Arf Theorem applied to the abelian extension \(M/F\) implies that \(1 + \frac{t}{p^n} \in \mathbb{N} - \{0\}\), thus \(t \in 1 + p^n\mathbb{N}\).

4. Torsion points on abelian varieties. Let \(A/K\) be an abelian variety over \(K\) with potential good reduction and \(\ell \neq p\) be a prime number. We denote by \(A[\ell]\) the \(\ell\)-torsion group of \(A(K_{\text{alg}})\) and by \(T_\ell(A) = \lim\ A[\ell^n]\) (resp. \(V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell\)) the Tate module (resp. \(\ell\)-adic Tate module) of \(A\).

The following result may be found in [Gur03] (paragraph 3). We recall it for the convenience of the reader.

**Lemma 2.2.** Let \(k = k_{\text{alg}}\) be a field with \(\text{char} k = p \geq 0\) and \(C/k\) be a projective, smooth, integral curve. Let \(\ell \neq p\) be a prime number and \(H\) be a finite subgroup of \(\text{Aut}_k(C)\) such that \((|H|, \ell) = 1\). Then

\[
2g(C/H) = \dim_{\mathbb{F}} \text{Jac}(C)[\ell]^H.
\]

If \(\ell \geq 3\), then \(L = K(A[\ell])\) is the minimal extension over which \(A/K\) has good reduction. It is a Galois extension with group \(G\) (see [ST68]). We denote by \(r_G\) (resp. \(1_G\)) the character of the regular (resp. unit) representation of \(G\). We denote by \(I\) the inertia group of \(K_{\text{alg}}/K\). For further explanations about conductor exponents see [Ser67], [Ogg67] and [ST68].

**Definition 2.5.** 1. Let

\[
a_G(\sigma) := -i_G(\sigma), \quad \sigma \neq 1,
\]

\[
a_G(1) := \sum_{\sigma \neq 1} i_G(\sigma),
\]

and \(\text{sw}_G := a_G - r_G + 1_G\). Then, \(a_G\) is the character of a \(\mathbb{Q}_\ell[G]\)-module and there exists a projective \(\mathbb{Z}_\ell[G]\)-module \(\text{Sw}_G\) such that \(\text{Sw}_G \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell\) has character \(\text{sw}_G\).

2. We still denote by \(T_\ell(A)\) (resp. \(A[\ell]\)) the \(\mathbb{Z}_\ell[G]\)-module (resp. \(\mathbb{F}_\ell[G]\)-module) afforded by \(G \to \text{Aut}(T_\ell(A))\) (resp. \(G \to \text{Aut}(A[\ell])\)). Let

\[
\text{sw}(A/K) := \dim_{\mathbb{F}} \text{Hom}_G(\text{Sw}_G, A[\ell]),
\]

\[
\epsilon(A/K) := \text{codim}_{\mathbb{Q}} V_\ell(A)^I.
\]

The integer \(f(A/K) := \epsilon(A/K) + \text{sw}(A/K)\) is the so called conductor exponent of \(A/K\) and \(\text{sw}(A/K)\) is the Swan conductor of \(A/K\).
Proposition 2.3. Let $\ell \neq p$, $\ell \geq 3$ be a prime number.

1. The integers $\text{sw}(A/K)$ and $\epsilon(A/K)$ are independent of $\ell$.

2. One has

\[
\text{sw}(A/K) = \sum_{i \geq 1} \frac{|G_i|}{|G_0|} \dim_{\mathbb{F}_\ell} A[\ell]/A[\ell^{G_i}].
\]

Moreover, for $\ell$ large enough, $\epsilon(A/K) = \dim_{\mathbb{F}_\ell} A[\ell]/A[\ell^{G_0}]$.

Remark: It follows from the definition that $\text{sw}(A/K) = 0$ if and only if $G_1 = \{1\}$. The Swan conductor is a measure of the wild ramification.

5. Automorphisms of Artin-Schreier covers. See [LM05] for further results on this topic. Let $R(t) \in k[t]$ be a monic additive polynomial and $A_R/k$ be the smooth, projective, geometrically irreducible curve birationally given by $w^p - w = tR(t)$. There is a so called Artin-Schreier morphism $\pi : A_R \to \mathbb{P}_k^1$. The automorphism $t_a$ of $\mathbb{P}_k^1$ given by $t \mapsto t + a$ with $a \in k$ has a prolongation $\tilde{t}_a$ to $A_R$ if there is a commutative diagram

\[
\begin{array}{ccc}
A_R & \longrightarrow & A_R \\
\uparrow{\pi} & & \uparrow{\pi} \\
\mathbb{P}_k^1 & \longrightarrow & \mathbb{P}_k^1
\end{array}
\]

Proposition 2.4. Let $n \geq 1$, $q := p^n$ and $R(t) := \sum_{k=0}^{n-1} \bar{u}_k t^{p^k} + t^q \in k[t]$. The automorphism of $\mathbb{P}_k^1$ given by $t \mapsto t + a$ with $a \in k$ has a prolongation to $A_R/k$ if and only if one has

\[
a^2 + (2\bar{u}_0a)^q + \sum_{k=1}^{n-1} (\bar{u}_k^q a^{p^k} + (\bar{u}_k a)^{q/p^k}) + a = 0.
\]

3 Main theorem

We start by fixing notations that will be used throughout this section.

Notations. We denote by $\mathfrak{m}$ the maximal ideal of $(K^{alg})^\circ$. Let $n \in \mathbb{N}^\times$, $q := p^n$, $a_n := (-1)^q(-p)^{p^2+\cdots+q}$ and $\forall 0 \leq i \leq n-1, d_i := p^{a_{i+1}+\cdots+q}$. We denote by $\mathbb{Q}_p^{ur}$ the maximal unramified extension of $\mathbb{Q}_p$ and we put
$K := \mathbb{Q}_p^{ur}(\lambda^{1/(1+q)})$. Let $\rho := (\rho_0, \ldots, \rho_{n-1})$ where $\forall \; 0 \leq k \leq n - 1$, $\rho_k \in K$, $\rho_k = u_k \lambda^{(q-p^k)/(1+q)}$ and $v(u_k) = 0$ or $u_k = 0$. For $c \in R$, let

$$f_{c,\rho}(X) := 1 + \sum_{k=0}^{n-1} \rho_k X^{1+p^k} + cX^q + X^{1+q},$$

and $s_{1,\rho}(X) := 2\rho_0 X + \sum_{k=1}^{n-1} \rho_k X^{p^k} + X^q$.

One defines the modified monodromy polynomial $L_{c,\rho}(X)$ by

$$s_{1,\rho}(X)^q - a_n f_{c,\rho}(X)^{q-1}(c + X) - (-1)^q \sum_{k=1}^{n-1} (\rho_k X)^{q/p^k} (-p)^d_k f_{c,\rho}(X)^{q(p^k-1)/p^k}.$$

Let $C_{c,\rho}/K$ and $A_u/k$ be the smooth projective integral curves birationally given respectively by $Y^p = f_{c,\rho}(X)$ and $w^p - w = \sum_{k=0}^{n-1} \bar{u}_k t^{1+p^k} + t^{1+q}$.

**Theorem 3.1.** The curve $C_{c,\rho}/K$ has potential good reduction isomorphic to $A_u/k$.

1. If $v(c) \geq v(\lambda^{p/(1+q)})$, then the monodromy extension of $C_{c,\rho}/K$ is trivial.

2. If $v(c) < v(\lambda^{p/(1+q)})$, let $y$ be a root of $L_{c,\rho}(X)$ in $K^{alg}$. Then $C_{c,\rho}$ has good reduction over $K(y, f_{c,\rho}(y)^{1/p})$. If $L_{c,\rho}(X)$ is irreducible over $K$, then $C_{c,\rho}/K$ has maximal wild monodromy. The monodromy extension of $C_{c,\rho}/K$ is $M = K(y, f_{c,\rho}(y)^{1/p})$ and $G = \text{Gal}(M/K)$ is an extraspecial $p$-group of order $pq^2$.

3. Assume that $c = 1$. The polynomial $L_{1,\rho}(X)$ is irreducible over $K$. The lower ramification filtration of $G$ is

$$G = G_0 = G_1 \supset G_2 = \cdots = G_u = \mathbb{Z}(G) \supset \{1\},$$

with $u \in 1 + q\mathbb{N}$. Moreover, if $p = 2$, then $u = 1 + q$, one has $f(Jac(C_{1,\rho})/K) = 2q + 1$ and $\text{sw}(Jac(C_{1,\rho})/\mathbb{Q}_2^{ur}) = 1$.

**Proof.** 1. Assume that $v(c) \geq v(\lambda^{p/(1+q)})$. Set $\lambda^{p/(1+q)} T = X$ and $\lambda W + 1 = Y$. Then, the equation defining $C_{c,\rho}/K$ becomes

$$(\lambda W + 1)^p = 1 + \sum_{k=0}^{n-1} \rho_k \lambda^{p(1+p^k)/(1+q)} T^{1+p^k} + c\lambda^{pq/(1+q)} T^q + \lambda^p T^{1+q}.$$
After simplification by $\lambda^p$ and reduction modulo $\pi_K$ this equation gives:

$$w^p - w = \sum_{k=0}^{n-1} \bar{u}_k t^{1+p^k} + a t^q + t^{1+q}, \ a \in k. \quad (4)$$

By Hurwitz formula the genus of the curve defined by (4) is seen to be that of $C_{c,\rho}/K$. Applying [Liu02] 10.3.44, there is a component in the stable reduction birationally given by (4). The stable reduction being a tree, the curve $C_{c,\rho}/K$ has good reduction over $K$.

2. The proof is divided into eight steps. Let $y$ be a root of $L_{c,\rho}(X)$.

**Step I**: One has $v(y) = v(a_n c)/q^2$.

By expanding $L_{c,\rho}(X)$, one shows that its Newton polygon has a single slope $v(a_n c)/q^2$. The polynomial $L_{c,\rho}(X)$ has degree $q^2$ and its leading (resp. constant) coefficient has valuation 0 (resp. $v(a_n c)$). One examines monomials from $a_n f_{c,\rho}^{q-1}(X)(c + X)$. Since $v(c) < v(\lambda^{p/(1+q)})$, one checks that

$$\forall 1 \leq i \leq q^2 - 1, \ \frac{v(a_n)}{q^2 - i} \geq \frac{v(a_n c)}{q^2}.$$ 

Then one examines monomials from $(\rho_i X)^{q/p^i} p^l f_{c,\rho}(X)^{(p^i-1)/p^i}$. They have degree at least $q/p^i$, thus one checks that

$$\forall 1 \leq i \leq n - 1, \ \frac{q/p^i v(\rho_i) + d_i v(p)}{q^2 - q/p^i} \geq \frac{v(a_n c)}{q^2}.$$ 

The monomial $X^{q^2}$ in $s_{1,\rho}(X)^q$ corresponds to the point $(0,0)$ in the Newton polygon of $L_{c,\rho}(X)$, the other monomials of $s_{1,\rho}(X)^q$ produce a slope greater than $v(\rho_i)/(q - p^i)$ and one checks that

$$\forall 0 \leq i \leq n - 1, \ \frac{v(\rho_i)}{q - p^i} \geq \frac{v(a_n c)}{q^2}.$$ 

Note that **Step I** implies that $v(f_{c,\rho}(y)) = 0$, we will use this remark throughout this proof.

**Step II**: Define $S$ and $T$ by $\lambda^{p/(1+q)} T = (X - y) = S$. Then $f_{c,\rho}(S + y)$ is congruent modulo $\lambda^p m[T]$ to

$$f_{c,\rho}(y) + s_{1,\rho}(y) S + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + \sum_{k=1}^{n-1} \rho_k y S^{p^k} + (c + y) S^q + S^{1+q}.$$
Using the following formula for $A \in K^{\text{alg}}$ with $v(A) > 0$ and $B \in (K^{\text{alg}})^o[T]$

$$k \geq 1, \ (A + B)^p \equiv (A^{p^{k-1}} + B^{p^{k-1}})^p \mod p^2 \mathfrak{m}[T],$$

one computes $\lambda \mathfrak{m}[T]$

$$f_{c,\rho}(y + S) = 1 + \sum_{k=0}^{n-1} \rho_k(y + S)^{1+p^k} + (y + S)^{1+q} + c(y + S)^{q}$$

$$\equiv 1 + \rho_0(y + S)^2 + \sum_{k=1}^{n-1} \rho_k(y + S)(y^{p^k-1} + S^{p^k-1})^p + (y + S + c)(y^{q/p} + S^{q/p})^p.$$

Using Step I, one checks that for all $1 \leq k \leq n - 1$

$$\rho_k(y^{p^k-1} + S^{p^k-1})^p \equiv \rho_k(y^{p^k} + S^{p^k}) \mod \lambda \mathfrak{m}[T],$$

and $(y^{q/p} + S^{q/p})^p \equiv y^q + S^q \mod \lambda \mathfrak{m}[T]$. It follows that

$$f_{c,\rho}(y + S) \equiv 1 + \rho_0(y + S)^2 + \sum_{k=1}^{n-1} \rho_k(y + S)(y^{p^k} + S^{p^k}) + (y + c + S)(y^q + S^q).$$

One easily concludes from this last expression.

**Step III**: Let $R_1 := K[y]^{o}$. For all $0 \leq i \leq n$, one defines $A_i(S) \in R_1[S]$ and $B_i \in R_1$ by induction :

$$B_n := -s_{1,\rho}(y), \ \forall \ 1 \leq i \leq n - 1, \ B_i := \frac{f_{q,c}(y)B_{i+1}}{(-p f_{c,\rho}(y))^{p^i}} - y \rho_{n-i},$$

$$\text{and} \ B_0 := \frac{f_{c,\rho}(y)B_{i}}{(-p f_{c,\rho}(y))^{p^i}},$$

$$A_0(S) := 0 \text{ and } \forall \ 0 \leq i \leq n - 1 \ SA_{i+1}(S) := SA_i(S) - \frac{B_{i+1}S_{q/p^{i+1}}}{p f_{q,c}(y)(p^{i-1}/p).}$$

Then for all $0 \leq i \leq n - 1$, $v(B_{i+1}) = (1 + \cdots + p^i)v(p)/p^i + v(c)/p^{i+1}$ and modulo $\lambda^{\frac{pq^2}{p^i}} \mathfrak{m}$ one has

$$B_n^{q} \equiv \frac{a_n}{(-1)^g} f_{c,\rho}(y)^{q-1} B_0 + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} f_{c,\rho}(y)^{q(p^k-1)/p^k}.$$  \ (5)

We prove the claim about $v(B_{i+1})$ by induction on $i$. Using Step I, one checks that $\forall \ 0 \leq k \leq n - 1, \ v(\rho_k y^{p^k}) > v(y^q)$, so $v(B_n) = v(y^q)$. Assume that
we have shown the claim for $i$, then one checks that $v((B_{i+1}/p)^p) < v(y_{n-i})$ and one deduces $v(B_i)$ from the definition of $B_i$. According to the expression of $v(B_i)$, one has $\forall \ 0 \leq i \leq n, A_i(S) \in R_i[S]$.

Then we prove the second part of Step III. From the definition of the $B_i$‘s one obtains that for all $1 \leq i \leq n-1$

$$B_{n-i+1}^{q/p^{i-1}} = (-p)^{q/p^{i-1}} \left(\rho_{n-i}^{q/p^{i-1} / p^i} (y_{n-i} + B_{n-i}(y))q/p^i\right).$$  \hfill (6)

Using Step I and $v(B_{n-1})$ one checks that for all $1 \leq i \leq n-1$ and $1 \leq k \leq q/p^i - 1$

$$p^i \left(q/p^i \right)(y_{n-i})^k B_{n-i}^{q/p^i - k} \equiv 0 \mod \lambda^p q^2/(1+q) m,$$

so $p^i(y_{n-i} + B_{n-1})^{q/p^i} \equiv p^i((y_{n-i})^{q/p^i} + B_{n-1})^q/p^i \mod \lambda^p q^2/(1+q) m$. Thus, applying equation (6) with $i = 1$, one gets

$$B_n^q = (-p)^q \rho_1 \left(\rho_1^{q/p^1} B_{n-1}^{q/p^1} \right) \equiv (-p)^q \rho_1 \left(\rho_1^{q/p^1} (y_{n-1} + B_{n-1})^{q/p^1} \right) \mod \lambda^p q^2/(1+q) m.$$

One checks using Step I and $v(B_{n-i})$ that for all $1 \leq i \leq n-1$ and $1 \leq k \leq q/p^i - 1$

$$p^i + \cdots + q/p^i - 1 \left(q/p^i \right)(y_{n-i})^k B_{n-i}^{q/p^i - k} \equiv 0 \mod \lambda^p q^2/(1+q) m,$$

then by induction on $i$, using equation (6), one shows that modulo $\lambda^p q^2/(1+q) m$

$$B_n^q \equiv (-p)^{p+\cdots+q} f_{c,\rho}(y)^{q-1} B_0 + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^d_k f_{c,\rho}(y)^{q(p^k-1)/p^k}. \hfill (7)$$

Step IV: One has modulo $\lambda^p m[T]$

$$f_{c,\rho}(S + y) \equiv f_{c,\rho}(y) + s_{1,\rho}(y) S + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + \sum_{k=1}^{n-1} y \rho_k S^{p^k} + B_0 S^q + S^{1+q}.$$

Since $L_{c,\rho}(y) = 0$, one has

$$s_{1,\rho}(y)^q = a_n f_{c,\rho}(y)^{q-1}(c + y) + (-1)^q \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^d_k f_{c,\rho}(y)^{q(p^k-1)/p^k}. \hfill (7)$$

Using $B_n := -s_{1,\rho}(y)$, equations (5) and (7) one gets

$$a_n f_{c,\rho}(y)^{q-1}(c + y - B_0) \equiv 0 \mod \lambda^p q^2/(q+1) m.$$
which is equivalent to $S_t(y + c - B_0) \equiv 0 \mod \lambda^p m[T]$. Then, Step IV follows from Step II.

**Step V:** One has

$$f_{c,\rho}(S + y) \equiv (f_{c,\rho}(y)^{1/p} + S A_n(S))^p + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + S^{1+q} \mod \lambda^p m[T].$$

Let $R := \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + S^{1+q} + s_{1,\rho}(y)S$. Since $B_n = -s_{1,\rho}(y)$ one has

$$(f_{c,\rho}(y)^{1/p} + S A_n(S))^p + \sum_{k=0}^{n-1} \rho_k S^{1+p^k} + S^{1+q}$$

$$= (f_{c,\rho}(y)^{1/p} + S A_n(S))^p + B_n S + R$$

$$= \left( f_{c,\rho}(y)^{1/p} + S A_n(S) - \frac{B_n S}{p f_{q,c}(y)^{(p-1)/p}} \right)^p + B_n S + R$$

$$= (f_{c,\rho}(y)^{1/p} + S A_n(S))^p + \left( \frac{-B_n S}{p f_{q,c}(y)^{(p-1)/p}} \right)^p + B_n S + R + \Sigma, \quad (8)$$

where

$$\Sigma = \sum_{k=1}^{p-1} \binom{p}{k} (f_{c,\rho}(y)^{1/p} + S A_n(S))^{p-k} \left( \frac{-B_n S}{p f_{q,c}(y)^{(p-1)/p}} \right)^k. \quad (9)$$

Using the expression of $v(B_n)$ computed in Step III, one checks that the terms with $k \geq 2$ in (9) are zero modulo $\lambda^p m[T]$. It implies the following relations

$$\Sigma + B_n S \equiv B_n S \left[ 1 - \frac{(f_{c,\rho}(y)^{1/p} + S A_n(S))^{p-1}}{f_{c,\rho}(y)^{(p-1)/p}} \right]$$

$$\equiv \frac{B_n S}{f_{c,\rho}(y)^{(p-1)/p}} \left[ f_{c,\rho}(y)^{(p-1)/p} - (f_{c,\rho}(y)^{1/p} + S A_n(S))^{p-1} \right]$$

$$\equiv \frac{B_n S}{f_{c,\rho}(y)^{(p-1)/p}} \left[ - \sum_{k=1}^{p-1} \binom{p-1}{k} f_{c,\rho}(y)^{(p-1-k)/p} (S A_n(S))^k \right]$$

$$\equiv 0 \mod \lambda^p m[T], \text{ since for } k \geq 1, \ B_n S^{k+1} \equiv 0 \mod \lambda^p m[T].$$

According to the definition of $B_{n-1}$ (see Step III) one obtains

$$(f_{c,\rho}(y)^{1/p} + S A_{n-1}(S))^p + R + B_n S^p + y \rho_{1,S^p} \mod \lambda^p m[T]. \quad (10)$$
Using the same process, one shows by induction on $i$ that $\mathbf{S}$ is congruent to

$$(f_{c,\rho}(y)^{1/p} + SA_{i+1}(S))^p + B_{i+1}S^{q-1} + \sum_{k=1}^{n-i-1} y\rho_k S^{p^k} + R \mod \lambda^p m[T]. \quad (11)$$

Thus, one applies equation (11) with $i = 0$

$$\mathbf{S} \equiv (f_{c,\rho}(y)^{1/p} + SA_1(S))^p + B_1 S^{q/p} + \sum_{k=1}^{n-1} y\rho_k S^{p^k} + R \mod \lambda^p m[T].$$

One defines $\Sigma'$ by $(f_{c,\rho}(y)^{1/p} + SA_1(S))^p = f_{c,\rho}(y) + (SA_1(S))^p + \Sigma'$. From $pf_{c,\rho}(y)^{(p-1)/p}SA_1(S) = -B_1 S^{q/p}$ (see the definition of $SA_1(S)$) one gets

$$\Sigma' + B_1 S^{q/p} = \sum_{k=2}^{p-1} \binom{p}{k} f_{c,\rho}(y)^{(p-k)/p}(SA_1(S))^k,$$

so using the expression of $v(B_1)$ computed in Step III, one checks that $\Sigma' + B_1 S^{q/p} \equiv 0 \mod \lambda^p m[T]$. From the definition of $SA_1(S)$ and $B_0$ one has $(SA_1(S))^p = B_0 S^q$, thus

$$\mathbf{S} \equiv f_{c,\rho}(y) + B_0 S^q + \sum_{k=1}^{n-1} y\rho_k S^{p^k} + R \mod \lambda^p m[T].$$

Then, Step V follows from Step IV and this last relation.

**Step VI**: The curve $C_{c,\rho}/K$ has good reduction over $K(y, f_{c,\rho}(y)^{1/p})$.

According to Step V, the change of variables in $K(y, f_{c,\rho}(y)^{1/p})$

$$X = \lambda^{p/(1+q)} Y + y = S + y \quad \text{and} \quad Y = \lambda W + f_{c,\rho}(y)^{1/p} + SA_n(S),$$

induces in reduction $w^p - w = \sum_{k=0}^{n-1} u_k t^{1+p^k} + t^{1+q}$ with genus $g(C_{c,\rho})$. So [Lin02] 10.3.44 implies that this change of variables gives the stable model. Note that the $\rho_k$’s were chosen to obtain this equation for the special fiber of the stable model.

**Step VII**: For any distinct roots $y_i, y_j$ of $L_{c,\rho}(X)$, $v(y_i - y_j) = v(\lambda^{p/(1+q)})$.

The changes of variables $\lambda^{p/(1+q)} T = X - y_i$ and $\lambda^{p/(1+q)} T = X - y_j$ induce equivalent Gauss valuations of $K(C_{c,\rho})$, else applying [Lin02] 10.3.44 would contradict the uniqueness of the stable model. Thus $v(y_i - y_j) \geq v(\lambda^{p/(1+q)})$.

One checks that $v(f'_{c,\rho}(y)) > 0$, $\forall 0 \leq k \leq n - 1$ $v(\rho_k^{q/^k}) > v(a_n)$, $v(s_{1,\rho}(y)) > 0$, $v(s_{1,\rho}(y)) = v(\lambda^{q^2})$ and $v(qs_{1,\rho}(y)^{q-1}s'_{1,\rho}(y)) > v(a_n)$, so

$$v(L'_{c,\rho}(y)) = v(a_n) = (q^2 - 1)v(\lambda^{p/(1+q)})$$.
Taking into account that \( L'_{c,\rho}(y_i) = \prod_{j \neq i} (y_i - y_j) \) and \( \deg L_{c,\rho}(X) = q^2 \), one obtains \( v(y_i - y_j) = v(\lambda^{p/(1+q)}) \).

**Step VIII:** If \( L_{c,\rho}(X) \) is irreducible over \( K \), then \( K(y, f_{c,\rho}(y)^{1/p}) \) is the monodromy extension \( M \) of \( C_{c,\rho}/K \) and \( G := \text{Gal}(M/K) \) is an extra-special \( p \)-group of order \( pq^2 \).

Let \( (y_i)_{i=1,\ldots,q^2} \) be the roots of \( L_{c,\rho}(X) \), \( L := K(y_1, \ldots, y_{q^2}) \) and \( M/K \) be the monodromy extension of \( C_{c,\rho}/K \). Any \( \tau \in \text{Gal}(L/K) - \{1\} \) is such that \( \tau(y_i) = y_j \) for some \( i \neq j \). Thus, the change of variables

\[
X = \lambda^{p/(1+q)} T + y_i \quad \text{and} \quad Y = \lambda W + f_{c,\rho}(y)^{1/p} + S A_n(S),
\]

induces the stable model and \( \tau \) acts on it by:

\[
\tau(T) = \frac{X - y_i}{\lambda^{p/(1+q)}}, \quad \text{hence} \quad T - \tau(T) = \frac{y_j - y_i}{\lambda^{p/(1+q)}}.
\]

According to **Step VII**, \( \tau \) acts non-trivially on the stable reduction. It follows that \( L \subseteq M \). Indeed if \( \text{Gal}(K^{\text{alg}}/M) \not\subset L^{\text{alg}}/L \) it would exist \( \sigma \in \text{Gal}(K^{\text{alg}}/M) \) inducing \( \bar{\sigma} \neq \text{Id} \in \text{Gal}(L/K) \), which would contradict the characterization of \( \text{Gal}(K^{\text{alg}}/M) \) (see remark after Theorem 2.1).

According to [LM05], the \( p \)-Sylow subgroup \( \text{Aut}_k(C_k)^\# \) of \( \text{Aut}_k(C_k)^\# \) is an extra-special \( p \)-group of order \( pq^2 \). Moreover, one has:

\[
0 \to Z(\text{Aut}_k(C_k)^\#) \to \text{Aut}_k(C_k)^\# \to (\mathbb{Z}/p\mathbb{Z})^{2n} \to 0,
\]

where \( (\mathbb{Z}/p\mathbb{Z})^{2n} \) is identified with the group of translations \( t \mapsto t + a \) extending to elements of \( \text{Aut}_k(C_k)^\# \). Therefore we have morphisms:

\[
\text{Gal}(M/K) \xrightarrow{i} \text{Aut}_k(C_k)^\# \xrightarrow{\varphi} \text{Aut}_k(C_k)^\# / Z(\text{Aut}_k(C_k)^\#).
\]

The composition is seen to be surjective since the image contains the \( q^2 \) translations \( t \mapsto t + (y_i - y_j)/\lambda^{p/(1+q)} \). Consequently, \( i(\text{Gal}(M/K)) \) is a subgroup of \( \text{Aut}_k(C_k)^\# \) of index at most \( p \). So it contains \( \Phi(\text{Aut}_k(C_k)^\#) = Z(\text{Aut}_k(C_k)^\#) = \text{Ker} \varphi \). It implies that \( i \) is an isomorphism and \( [M : K] = pq^2 \).

By **Step VI**, one has \( M \subseteq K(y, f_{q,c}(y)^{1/p}) \), hence \( M = K(y, f_{q,c}(y)^{1/p}) \).

We show that \( K(y_1)/K \) is Galois and that \( \text{Gal}(M/K(y_1)) = Z(G) \). Indeed, \( M/K(y_1) \) is \( p \)-cyclic and generated by \( \sigma \) defined by:

\[
\sigma(y_1) = y_1 \quad \text{and} \quad \sigma(f_{c,\rho}(y_1)^{1/p}) = \zeta_p f_{c,\rho}(y_1)^{1/p}.
\]

According to **Step VI**, \( \sigma \) acts on the stable model by:

\[
\sigma(S) = S, \quad \sigma(Y) = Y = \lambda \sigma(W) + \zeta_p f_{c,\rho}(y_1)^{1/p} + S A_n(S).
\]
Hence
\[ \sigma(W) = W - f_{c, \rho}(y_1)^{1/p}. \]

It follows that, in reduction, \( \sigma \) induces a morphism that generates \( \mathbb{Z}(\text{Aut}_k(C_k))^{\#} \).

It implies that \( K(y_1)/K \) is Galois, \( \text{Gal}(M/K(y_1)) = \mathbb{Z}(G) \) and \( \text{Gal}(K(y_1)/K) \simeq (\mathbb{Z}/p\mathbb{Z})^{2n} \).

3. Let \( L_\rho(X) := L_{1, \rho}(X) \), \( f_\rho(X) := f_{1, \rho}(X) \), \( s_\rho(y) := s_{1, \rho}(y) \), \( y \) be a root of \( L_\rho(X) \) and \( b_n := (-1)(-p)^{1+p+\ldots+p^{n-1}} \). Note that \( b_n^p = a_n \), \( L = K(y) \) and we do not assume \( p = 2 \) until Step E.

**Step A:** The polynomial \( L_\rho(X) \) is irreducible over \( K \).

Let \( \bar{s} := s_\rho(y)/y^q \), \( \sigma := \sum_{k=1}^{\#} \binom{\bar{q}}{k} \bar{s}^k y^{q(k-1)} \) and \( R_1 := \sum_{k=1}^{p-1} \binom{p}{k} y^{kq^2/p}(-b_n)^{p-k} \).

Since \( L_\rho(y) = 0 \) one has

\[ y^q + \sigma = s_\rho(y)^q = a_n f_\rho(y)(1 + y) + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} (-1)^q f_\rho(y)^{q(p^k-1)/p^k}. \]

It implies that \( (y^{q^2/p} - b_n)^p \) equals

\[ a_n \left[ f_\rho(y)(1 + y) + (-1)^p \right] + \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} (-1)^q f_\rho(y)^{q(p^k-1)/p^k} + R_1 - \sigma. \]

We are going to remove monomials with valuation greater than \( v(a_n y) \) in the above expression by taking \( p \)-th roots. Note that if \( \forall i \geq 1, \rho_i = 0 \), then one could skip most of Step A (see equation (14)). Assume that \( \rho_i \neq 0 \) for some \( i \geq 1 \), let \( j := \max\{1 \leq i \leq n-1, \rho_i \neq 0\} \) and \( l := \min\{1 \leq i \leq n-1, \rho_i \neq 0\} \). The following relations are straightforward computations using Step I:

\[ v(f_\rho(y)(1 + y) + (-1)^p) = v(y), \quad v(\bar{s}) = v(\rho_j y^p), \quad v(\sigma) = qv(\bar{s}), \quad (12) \]

\[ v\left( \sum_{k=1}^{n-1} (\rho_k y)^{q/p^k} (-p)^{d_k} (-1)^q f_\rho(y)^{q(p^k-1)/p^k} \right) = v((\rho_1 y)^{p^{n-1} p^d}). \]

Then one checks that

\[ v(R_1) > v(a_n y) > v((\rho_1 y)^{p^{n-1} p^d}) > v(\sigma). \quad (13) \]

It implies that \( v((y^{q^2/p} - b_n)^p) = qv(\bar{s}) \), so one considers \( (y^{q^2/p} - b_n + \bar{s}^{q/p})^p \).

By expanding this last expression, using (12), (13) and taking into account

\[ v\left( \sum_{k=1}^{q-1} (\binom{q}{k} \bar{s}^k y^{q(k-1)}) \right) > v(a_n y), \quad v\left( \sum_{k=1}^{p} \binom{p}{k} (y^{q^2/p} - b_n)^k \bar{s}^{(p-k)q/p} \right) > v(a_n y), \]

16
one obtains that \( pv(y^{n'/p} - b_n + \tilde{s}/p) = v((\rho y)^{p_{n-1}}p^k) \), leading us to consider
\[
(y^{n'/p} - b_n + \tilde{s}/p + (\rho y)^q/p^{l+1}(-p)^{d_i}/p) f_p(y)^q(p^{l-1}/p^{l+1})p.
\]
By expanding this expression and using (12) and (13) one easily checks that it has valuation \( v((\rho y)^{p_{n-1}}p^{l_i}) \) where \( l_i := \min\{l + 1 \leq i \leq n - 1, \rho_i \neq 0\} \).
By induction one shows that
\[
t := y^{n'/p} - b_n + \tilde{s}/p + \sum_{k=1}^{n-1}(\rho_k y)^q/p^{k+1}(-p)^{d_k}/p) f_p(y)^q(p^{k-1}/p^{k+1},
\]
satisfies \( pv(t) = v(a_n y) \). Then \( v_L(p^{\nu_1}t^{-q(p+1)}) = v_L(p)/q^2 = [L : \mathbb{Q}_p]/q^2 \), so \( q^2 \) divides \( [L : K] \). It implies that \( L_p(X) \) is irreducible over \( K \).

**Step B : Reduction step.**

The last non-trivial group \( G_{i_0} \) of the lower ramification filtration \( (G_i)_{i \geq 0} \) of \( G := \text{Gal}(M/K) \) is a subgroup of \( Z(G) \) (see [Ser79] IV §2 Corollary 2 of Proposition 9) and as \( Z(G) \simeq \mathbb{Z}/p\mathbb{Z} \), it follows that \( G_{i_0} = Z(G) \).

According to **Step VIII** the group \( H := \text{Gal}(M/L) \) is \( Z(G) \). Consequently, the filtration \( (G_i)_{i \geq 0} \) can be deduced from that of \( M/L \) and \( L/K \) (see [Ser79] IV §2 Proposition 2 and Corollary of Proposition 3).

**Step C :** Let \( \sigma \in \text{Gal}(L/K) - \{1\} \), then \( v(\sigma(t) - t) = q^2 v(\pi_K) \).
Let \( y' := \sigma(y) \), one deduces the following easy lemma from **Step VII**.

**Lemma 3.1.** For any \( n \geq 0 \), \( v(y^n - y'^n) \geq nv(y) \).

Recall the definition \( \tilde{s} := 2\rho_0 y + \sum_{k=1}^{n-1} \rho_k y^{p^k} \). First one shows that modulo \( (y - y')^{n'/p}m \) one has
\[
\sigma(\tilde{s})^{q/p} - \tilde{s}^{q/p} \equiv (2\rho_0)^{q/p} (y^{q/p} - y^{q/p}) + \sum_{k=1}^{n-1} \rho_k^{q/p} (y^{q/p} - y^{q/p}).
\]
Indeed, let \( (m_i)_{i=0,\ldots,n-1} \in \mathbb{N}^n \) such that \( m_0 + m_1 + \cdots + m_{n-1} = q/p \) and \( t := m_0 + m_1 p + \cdots + m_{n-1} p^{n-1} \), then using lemma 3.1 one checks that
\[
v(\rho_0^{m_0} \rho_1^{m_1} \cdots \rho_{n-1}^{m_{n-1}} (y^t - y'^t)) > \frac{q^2}{p} v(y - y').
\]
This inequality implies (15).

Let \( 1 \leq k \leq n - 1 \) and write \( f_p(y)^q(p^{k-1}/p^{k+1}) = 1 + \sum_{i \in I_k} \alpha_i y^{i} \), for some
set $I_k$. Then

$$y^{q/pk+1} f_{\rho}(y^{(p^h-1)q/pk+1} - y^{q/pk+1} f_{\rho}(y^{(p^h-1)q/pk+1}) = y^{q/pk+1} - y^{q/pk+1} + \sum_{i \in I_k} \alpha_i(ky_i - y').$$

Let $i \in I_k$. Consider the case when $v(\alpha_{i,k}) \geq v(\rho_i)$ for some $0 \leq h \leq n - 1$, then using Step VII, one checks that $\forall 1 \leq k \leq n - 1$, $v(\alpha_{i,k}) > qv(y' - y)/p^{k+1}$. If this case does not occur, then according to the expression of $f_{\rho}(y)$ one has $i \geq q/p^{k+1} + q$ and using lemma 3.1 one checks that $v(y^n - y') > qv(y' - y)/p^{k+1}$. In any case $v(\alpha_{i,k}(y^n - y')) > qv(y' - y)/p^{k+1}$ and one checks that

$$v(p^{d_k/p} \rho_k^{q/pk+1} \alpha_{i,k}(y^n - y')) > q^2v(y' - y)/p.$$  (16)

Taking into account (14), (15) and (16), one gets mod $(y' - y)^{q^2/p}m$

$$\sigma(t) - t = y^{q^2/p} - y^{q^2/p} + (2\rho_0)^q(y^{q/p} - y^{q/p}) + \sum_{k=1}^{n-1} \rho_k^{q/p}(y^{q/p} - y^{q/p}) + \sum_{k=1}^{n-1} (-p)^{d_k/p} \rho_k^{q/pk+1} (y^{q/pk+1} - y^{q/pk+1}).$$

Using lemma 3.1, it is now straight forward to check the following relations mod $(y' - y)^{q^2/p}m$.

$$y^{q^2/p} - y^{q^2/p} \equiv (y' - y)^{q^2/p},$$

$$\rho_k^{q/p}(y^{q/p} - y^{q/p}) \equiv \rho_k^{q/p}(y' - y)^{q/p},$$

$$(-p)^{d_k/p} \rho_k^{pk+1} (y^{q/pk+1} - y^{q/pk+1}) \equiv (-p)^{d_k/p} \rho_k^{q/pk+1} (y' - y)^{q/pk+1}.$$

Using Step VII, one sees that each of these three elements has valuation $q^2v(y' - y)/p$, thus one gets

$$(\sigma(t) - t)^p \equiv (y' - y)^{q^2} + (2\rho_0)^q(y' - y)^{q} + \sum_{k=1}^{n-1} \rho_k^{q/pk} (y' - y)^{q/pk}$$  (18)

$$+ \sum_{k=1}^{n-1} (-p)^{d_k/p} \rho_k^{q/pk} (y' - y)^{q/pk} \mod (y' - y)^{q^2}m.$$

Now recall Step VII, the definitions of the $\rho_k$’s and of $\lambda$, then for some $v \in R^+$ and $\Sigma \in R$

$$\rho_k = u_k \lambda^{p(q-p^k)/(1+q)}, \quad y' - y = v \lambda^{p/(1+q)} \quad \text{and} \quad -p = \lambda^{p-1} + p\lambda \Sigma.$$
Since \( q^2v(y' - y) = \frac{pq^2}{1 + q}v(\lambda) \), equation (18) becomes

\[
(\sigma(t) - t)^p \equiv \lambda^{\frac{q^2}{1 + q}} \left[ v^q + (2u_0v)^q + \sum_{k=1}^{n-1} (u_k^q v^{q^k} + (u_k v)^q)^k \right] \mod \lambda^{\frac{q^2}{1 + q}}.
\]

From the action of \( \sigma \) on the stable reduction (see Step VIII), one has that the automorphism of \( \mathbb{P}_k^1 \) given by \( t \mapsto t + \bar{v} \) has a prolongation to \( A_u/k \), so Proposition 2.4 implies that

\[
\bar{v}v^q + (2\bar{u}_0\bar{v})^q + \sum_{k=1}^{n-1} (\bar{u}_k^q \bar{v}^{q^k} + (\bar{u}_k \bar{v})^{q^k}) + \bar{v} = 0. \tag{19}
\]

Assume that \( \bar{v}v^q + (2\bar{u}_0\bar{v})^q + \sum_{k=1}^{n-1} (\bar{u}_k^q \bar{v}^{q^k} + (\bar{u}_k \bar{v})^{q^k}) = 0 \), then from (19) one has \( \bar{v} = 0 \), which contradicts \( v \in R^\times \). It implies that \( v(\sigma(t) - t) = q^2v(\lambda)/(1 + q) = q^2v(y - y')/p = q^2v(\pi_K) \).

**Step D** : The ramification filtration of \( L/K \) is:

\[
(G/H)_0 = (G/H)_1 \supseteq (G/H)_2 = \{1\}.
\]

Since \( K/\mathbb{Q}_p^ur \) is tamely ramified of degree \( (p-1)(q+1) \), one has \( K = \mathbb{Q}_p^ur(\pi_K) \) with \( \pi_K^{(p-1)(q+1)} = p \) for some uniformizer \( \pi_K \) of \( K \). In particular \( z := \pi_K^2/t \), is a uniformizer of \( L \). Let \( \sigma \in \text{Gal}(L/K) - \{1\} \), then

\[
\sigma(z) - z = \frac{t - \sigma(t)}{\sigma(t)t} \pi_K^2 = \frac{t - \sigma(t)}{\pi_K^2} \pi_K^2 \pi_K^2 = \frac{t}{\sigma(t)}.
\]

Using Step C one obtains \( v(\sigma(z) - z) = 2v(z) \), i.e. \( (G/H)_2 = \{1\} \).

**Step E** : From now on, we assume \( p = 2 \). Let \( s := (q + 1)(2q^2 - 1) \). There exist \( u, h \in L \) and \( r \in \pi_L^2m \) such that \( v_L(2y^{q/2}h) = s \) and

\[
f_\rho(y)u^2 = 1 + \rho_{n-1}y^{1+q/2} + 2y^{q/2}h + r.
\]

To prove the first statement we note that, from the definition of \( f_\rho(y) \), one has \( f_\rho(y) = 1 + T \) with \( v(T) = qv(y) \) and \( L_\rho(y) = 0 \), thus

\[
\left( \frac{s_{2q/2}(y)}{b_0} \right)^2 = f_\rho(y)q^{-1}(1 + y) + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2^k}}{2^{2+\cdots+2^{n-k}}} f_\rho(y)^{q(2^k-1)/2^k},
\]

and \( f_\rho(y)q^{-1}(1 + y) = 1 + y + \sum_{k=1}^{q-1} \left( \frac{q - 1}{k} \right) T^k(1 + y) \).
Then, we put \( \tilde{\Sigma} := \sum_{k=1}^{q-1} \binom{q-1}{k} T^k (1 + y) \) and

\[
h := \frac{s_p^{q/2}(y)}{b_n} + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2k+1}}{2^{1 + \cdots + 2^{n-k-1}}} f_\rho(y)^{q(2^{k-1})/2k+1} - 1.
\]

Then one computes

\[
h^2 = \left[ \frac{s_p^{q/2}(y)}{b_n} + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2k+1}}{2^{1 + \cdots + 2^{n-k-1}}} f_\rho(y)^{q(2^{k-1})/2k+1} \right]^2 + 1 - 2(h + 1)
\]

\[
= \left( \frac{s_p^{q/2}(y)}{b_n} \right)^2 + \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2k}}{2^{2 + \cdots + 2^{n-k}}} f_\rho(y)^{q(2^{k-1})/2k} + \tilde{\Sigma} + 1 - 2(h + 1)
\]

\[
= 2 + y + 2 \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2k}}{2^{2 + \cdots + 2^{n-k}}} f_\rho(y)^{q(2^{k-1})/2k} + \Sigma_1 + \tilde{\Sigma} - 2(h + 1).
\]

In **Step III**, we proved that \( v(B_n) = qv(y) = 2v(b_n)/q \) where \( B_n = -s_\rho(y) \), so \( v(\frac{s_p^{q/2}(y)}{b_n}) = 0 \) and one checks using **Step I** that

\[
v(2) > v(y), \quad \forall \ 1 \leq k \leq n - 1, \quad v \left( \frac{(\rho_k y)^{q/2k+1}}{2^{1 + \cdots + 2^{n-k-1}}} \right) \geq 0,
\]

thus \( v(h + 1) \geq 0 \) and \( v(2(h + 1)) \geq v(2) > v(y) \). One checks in the same way that \( v(\Sigma_1) > v(y) \). One has \( v(\tilde{\Sigma}) \geq v(T) > v(y) \), so \( v(h^2) = v(y) \) and \( v_L(2y^{q/2}h) = s \).

To prove the second statement of **Step E**, we first remark that \( \forall i \geq 1 \)

\[
f_\rho(y)^i = 1 + \sum_{k=1}^{i-1} \binom{i}{k} T^k = 1 + \Sigma_i, \quad \text{whence} \quad v(\Sigma_i) \geq v(T).
\]

Since, for all \( 0 \leq k \leq n - 1, \ v(p_k y^q) > qv(y) \) one has \( \pi_L^* m \) mod \( \pi_L^* m \)

\[
\frac{s_p^{q/2}(y)}{b_n} \cdot 2y^{q/2} \equiv \left[ (2\rho_0 y)^{q/2} + \sum_{k=1}^{n-1} (\rho_k y^{2k})^{q/2} + y^{q/2} \right] \frac{y^{q/2}}{2^{2 + \cdots + 2^n - 1}}.
\]

One also checks that \( \forall i \geq 1 \), \( v_L(2y^{q/2} \Sigma_i) > s \), then according to \( (20) \), \( \forall i \geq 1 \) and \( 1 \leq k \leq n - 1 \)

\[
v_L \left( \frac{(\rho_k y)^{q/2k+1}}{2^{1 + \cdots + 2^{n-k-1}}} 2^y y^{q/2} \right) \Sigma_i \right) > s \)

and one checks that \( v_L \left( \frac{(2\rho_0 y^{q/2} y^q}{2^{2 + \cdots + 2^n - 1}} \right) > s. \)

Thus, applying relations \( (21), (22) \) and the definition of \( h \), one has

\[
2hy^{q/2} \equiv \left[ \sum_{k=1}^{n-1} (\rho_k y^{2k})^{q/2} + y^{q/2} \right] \frac{y^{q/2}}{2^{2 + \cdots + 2^n - 1}}
\]

\[
+ \sum_{k=1}^{n-1} \frac{(\rho_k y)^{q/2k+1}}{2^{1 + \cdots + 2^{n-k-1}}} 2y^{q/2} - 2y^{q/2} \mod \pi_L^* m.
\]

20
Finally one puts

\[ u := 1 - y^{q/2} - \sum_{k=0}^{n-2} y^{2^k(1+q)} + \sum_{i=1}^{n-1} \sum_{k=n-i-1}^{n-2} \rho_i^{2^k} y^{2^k(1+2^i)} y^{2^k(1+2^i)} = 1 + \tilde{u}, \]

and one checks that \( v(\tilde{u}) = v(y^{q/2}) \). From the equality

\[ f_\rho(y)u^2 - 1 = \sum_{k=0}^{n-1} \rho_k y^{1+2^k} + y^q + y^{1+q} + (1 + T)2\tilde{u} + (1 + T)\tilde{u}^2, \]

taking into account that \( v_L(2T\tilde{u}) > s, v_L(T\tilde{u}^2) > s, \forall 0 \leq k \leq n - 2, v_L(\rho_k y^{1+2^k}) > s \) and expanding \( \tilde{u} \) and \( \tilde{u}^2 \) one gets modulo \( \pi_L^2 \mathfrak{m} \)

\[ f_\rho(y)u^2 - 1 \equiv \rho_{n-1} y^{1+q/2} - 2y^{q/2} + 2y^q - \sum_{k=1}^{n-2} 2y^{2^k(1+q)} + \sum_{k=1}^{n-1} y^{2^k(1+q)} \]

\[ + \sum_{i=1}^{n-1} \sum_{k=n-i-1}^{n-2} 2\rho_i^{2^k} y^{2^k(1+2^i)} + \sum_{i=1}^{n-1} \sum_{k=n-i}^{n-1} \rho_i^{2^k} y^{2^k(1+2^i)} \]

\[ = 2 \sum_{i=1}^{n-1} \sum_{k=n-i-1}^{n-2} \rho_i^{2^k} y^{2^k(1+2^i)} + \sum_{i=1}^{n-1} \sum_{k=n-i}^{n-1} \rho_i^{2^k} y^{2^k(1+2^i)}. \]

(24)

Arranging the terms of (24), taking into account that \( v_L(2y^q) > s \) and for all \( 2 \leq i \leq n - 1 \) and \( n - i \leq k \leq n - 2 \)

\[ v_L \left( \rho_i^{2^k} y^{2^k(1+2^i)} \frac{2}{2^{2^i+...+2^k}} \right) \]

\[ > s, \]

and comparing with (23), one obtains \( f_\rho(y)u^2 - 1 \equiv \rho_{n-1} y^{1+q/2} + 2hy^{q/2} \mod \pi_L^2 \mathfrak{m}. \)

**Step F:** *The ramification filtration of \( M/L \) is*

\[ H_0 = H_1 = \cdots = H_{1+q} \supseteq \{1\}. \]

One has to show that \( v_M(\mathcal{D}_{M/L}) = q + 2 \), we will use freely results from [Ser79] IV. If \( \rho_{n-1} = 0 \), then according to **Step E**, one has

\[ f_\rho(y)u^2 = 1 + 2y^{q/2}h + r, \]

and one concludes using [CM11] Lemma 2.1. Else, if \( \rho_{n-1} \neq 0 \), one has

\[ \max_{u \in L^x} v_L(f_\rho(y)u^2 - 1) \geq v_L(\rho_{n-1} y^{1+q/2}), \]

then [LRS93] Lemma 6.3 implies that \( v_M(\mathcal{D}_{M/L}) \leq q + 3 \). Using **Step B**, **Step D** and [Ser79] IV §2 Proposition 11, one has that the break in the ramification filtration of \( M/L \) is congruent to 1 mod 2, i.e. \( v_M(\mathcal{D}_{M/L}) \leq q + 2. \)
According to Step D and lemma 2.1 the break $t$ of $M/L$ is in $1 + qN$. If $t = 1$ then $G_2 = \{1\}$ and $G_1/G_2 = G/G_2 \simeq G$ would be abelian, so $t \geq 1 + q$, i.e. $v_M(D_{M/L}) \geq q + 2$.

Step G: Computations of conductors.
For $l \neq 2$ a prime number, the $G$-modules $\text{Jac}(C)[l]$ and $\text{Jac}(C_k)[l]$ being isomorphic one has that for $i \geq 0$:

$$\dim_{\mathbb{F}_l} \text{Jac}(C)[l]^{G_i} = \dim_{\mathbb{F}_l} \text{Jac}(C_k)[l]^{G_i}.$$ 

Moreover, for $0 \leq i \leq 1 + q$ one has $\text{Jac}(C_k)[l]^{G_i} \subseteq \text{Jac}(C_k)[l]^{G_{q+1}}$, then from $C_k/Z(G) \simeq \mathbb{P}^1_k$ and lemma 2.2 it follows that for $0 \leq i \leq 1 + q$, $\dim_{\mathbb{F}_l} \text{Jac}(C_k)[l]^{G_i} = 0$. Since $g(C) = q/2$ one gets $f(\text{Jac}(C)/K) = 2q + 1$ and $\text{sw}(\text{Jac}(C)/\mathbb{Q}^{ur}) = 1$.

Example: Magma codes are available on the author webpage. Let $K := \mathbb{Q}^{ur}_2(2^{1/5})$ and $f(X) := 1 + 2^{6/5}X^2 + 2^{4/5}X^3 + X^4 + X^5 \in K[X]$, one checks that the smooth, projective, integral curve birationally given by $Y^2 = f(X)$ has the announced properties, that is the wild monodromy $M/K$ has degree 32 and one can describe its ramification filtration. The first program checks that Step A and Step D hold for this example. The second program checks Step F and is due to Guardia, J., Montes, J. and Nart, E. (see [GMN11]) and computes $v_M(D_{M/\mathbb{Q}^{2^{1/5}}}) = 194$. Using [Ser79] III §4 Proposition 8, one finds that $v_M(D_{M/K}) = 66$, which was the announced result in Theorem 3.1.

Remarks:
1. The above example was the main motivation for Step F since it shows that one could expect the correct behaviour for the ramification filtration of $\text{Gal}(M/K)$ when $p = 2$.
2. The naive method to compute the ramification filtration of $M/K$ in the above example fails. Indeed, in this case Magma needs a huge precision when dealing with 2-adic expansions to get the correct discriminant.

Acknowledgements: I would like to thank M. Monge for pointing out lemma 2.1.

References
[BK05] A. Brumer and K. Kramer. The conductor of an abelian variety. Compositio mathematica, n 2(92), 2005.
[CM11] P. Chrétien and M. Matignon. *Maximal monodromy in unequal characteristic*. submitted, 2011.

[GMN11] J. Guardia, J. Montes, and E. Nart. *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*. Journal de théorie des nombres de Bordeaux, 2, 2011.

[Gur03] R. Guralnick. *Monodromy groups of coverings of curves*. In Galois groups and fundamental groups, volume 41. MSRI Publications, 2003.

[Hup67] B. Huppert. *Endliche Gruppen I*. Grundlehren der Mathematischen Wissenschaften, (134), 1967.

[Kra90] A. Kraus. *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*. Manuscripta Mathematica, (69), 1990.

[Liu02] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2002.

[LM05] C. Lehr and M. Matignon. *Automorphism groups for $p$-cyclic covers of the affine line*. Compositio Mathematica, n 5(141), 2005.

[LRS93] P. Lockhart, M.I. Rosen, and J. Silverman. *An upper bound for the conductor of an abelian variety*. Journal of algebraic geometry, n 2, 1993.

[Ogg67] A.P. Ogg. *Elliptic curves and wild ramification*. American Journal of Mathematics, 89(1), 1967.

[Ray90] M. Raynaud. *p-groupes et réduction semi-stable des courbes*. In Birkhäuser, editor, The Grothendieck Festschrift, Vol. III, 1990.

[Ser67] J.-P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, 1967.

[Ser79] J.-P. Serre. *Local Fields*. Graduate Texts in Mathematics (67), 1979.

[ST68] J.-P. Serre and J. Tate. *Good reduction of abelian varieties*. Annals of Mathematics, (88), 1968.

[Suz86] M. Suzuki. *Group Theory II*. Grundlehren der Mathematischen Wissenschaft (248), 1986.