The p-rank of ramified covers of curves

Irene I. Bouw

1 Introduction

This paper is concerned with computing the p-rank of (ramified) covers of curves in characteristic p. Mainly we are interested in abelian covers of prime to p order of the generic r-pointed curve of genus g. This question can be reformulated in terms of quotients of tame fundamental groups.

Let X be a nonsingular connected projective curve over an algebraically closed field k of characteristic $p > 0$ and let $g = g(X)$. Put $U = X - S$. Not much is known on the tame fundamental group $\pi_1^t(U)$. Its structure is known only for $2g + r \leq 2$. By a result of Grothendieck [6, XII.2.12], $\pi_1^t(U)$ is a quotient of $\hat{\Gamma}_{g,r}$, the fundamental group of a curve over $\mathbb{C}$ with same g and r. The prime to p parts of both groups are equal, but $\pi_1^t(U) \simeq \hat{\Gamma}_{g,r}$ only in "trivial" cases. For $g \geq 1$ this is seen by considering the p-cyclic quotients of $\pi_1^t(U)$; they correspond to the étale p-cyclic covers of X. The maximal elementary abelian p-quotient of $\pi_1^t(U)$ is $(\mathbb{Z}/p)^{\sigma(X)}$, where $0 \leq \sigma(X) \leq g(X)$ is the p-rank of X. The maximal elementary abelian p-quotient of $\hat{\Gamma}_{g,r}$ is $(\mathbb{Z}/p)^{2g}$. This implies that there are less étale p-cyclic covers in characteristic p than in characteristic zero. In fact, the p-part of $\pi_1^t(U)$ is a free pro-p group on $\sigma(X)$ generators. This result is related to the Deuring–Shafarevich formula. This is a formula for the p-rank $\sigma(Y)$ in terms of $\sigma(X)$ and the ramification indices for a (possibly ramified) cover $Y \to X$ whose Galois group is a p-group, [2]. We will see that the situation for prime to p covers is more complicated.

The p-part and the prime to p part of $\pi_1^t(U)$ are known; the next case to consider is quotients G which are an extension of a prime to p group H by a p-group P. We may suppose that P is elementary abelian, since $\pi^p(X)$ is a free pro-p group. Suppose we are given a quotient $\pi_1^t(U) \twoheadrightarrow G$. To this quotient corresponds a G-cover $Z \to X$; it factors through $Y := Z/P$. The cover $Y \to X$ is prime to p; these covers we know exactly. The cover $Z \to Y$ is étale. We can reformulate the question of G-quotients of $\pi_1^t(U)$ as follows. For convenience, we consider only quotients which lie over a fixed H-quotient, i.e. we fix the H-cover $Y \to X$. Then G-quotients of $\pi_1^t(U)$ correspond to $\mathbb{F}_p[H]$-submodules P of $H^1(Y, \mathcal{O}_Y)^F$, where F is the Frobenius morphism. This means that in order to solve our problem, we have to compute the structure of $H^1(Y, \mathcal{O}_Y)^F$ as $\mathbb{F}_p[H]$-module. The dimensions of the isotypical spaces are called the generalized Hasse–Witt invariants. For a more precise definition, see Section 2. The generalized Hasse–Witt invariants can be viewed as generalizations of the p-rank by taking into account the H-Galois action. It is easy to see that if we consider a family of covers of curves with fixed (g, r), then the p-rank will depend on the bottom curve. Here we are interested in computing the p-rank in case the bottom curve is the generic r-pointed curve of genus g, i.e. corresponds to the generic point of the moduli space $M_{g,r} \otimes \mathbb{F}_p$.

The question of the p-rank of a prime to p cover has been considered previously in the étale case, [11], [14], [17]. In these papers it is shown that for many étale covers of the generic curve are ordinary, most importantly this holds for abelian covers. But in [17] it is shown that this is not true for all groups: there exist étale nonordinary covers of the generic curve X_g for every $g \geq 2$. In this paper we consider what happens for ramified covers. It is easy to see that it is not to be expected that all (abelian) covers of the generic r-pointed curve of genus g are ordinary. It turns out that there is an obvious bound $B(\mathbf{a}, g)$ on the p-rank coming from the structure of $H^1(Y, \mathcal{O}_Y)$ as $k[H]$-module, here $\mathbf{a}$ denotes the monodromy. The $k[H]$-module structure of $H^1(Y, \mathcal{O}_Y)$ is known by a results of Chevalley–Weil, see Section 3. The question we study is the following.

Question 1.1 Suppose (X, S) is the generic r-pointed curve of genus g. Let H be a group of order prime to p. Fix the monodromy $\mathbf{a}$. Is it true that all H-covers with monodromy $\mathbf{a}$ have p-rank equal to $B(\mathbf{a}, g)$?

It turns out that the answer to this question is no, in general, for nonabelian covers (Lemma 3.5). But for abelian covers it is yes, in many cases. We show that we can restrict to the cyclic case. In Section 6 we prove that the cyclic covers of $\mathbb{P}^1$ are ordinary, for p large and the branch points sufficiently general. We prove this by computing the coefficients of the Hasse–Witt matrix of Y. In Section 8 we show that the statement for genus greater than zero can be reduced to the case of genus zero. This is shown by degenerating covers in a suitable way.

The outline of the paper is as follows. In Section 2 we define the generalized Hasse–Witt invariants and study basic properties. We relate the generalized Hasse–Witt invariants to quotients of tame fundamental groups. In Section 3 we describe the $k[H]$-module structure of $H^1(Y, \mathcal{O}_Y)$ and use this to define a bound on $\sigma(Y)$. In Section 3 we also compute the generalized Hasse–Witt invariants for some nonabelian covers. We give an example, due to Raynaud, of a cover of $\mathbb{P}^1$ branched at three points whose p-rank is unequal to the bound. In Section 4 we concentrate on the case of cyclic covers. In Section 5 we compute the coefficients of the Hasse–Witt matrix of a cyclic cover of $\mathbb{P}^1$. In Section 6 we use this to compute the p-rank of a cyclic cover of $\mathbb{P}^1$ in case p is large and the branch points are general. In Section 7 we explain hoew we can get information on the p-rank of a cover by degenerating it to a cover of semistable curves. We use this to reprove the main theorem in case $p \equiv \pm 1 \pmod{\ell}$ or $r \leq 4$. In these cases we can drop the assumption p large. In Section 8 we use the same method to show that the computation of the generalized Hasse–Witt invariants of covers of the generic curve of g can be reduced to the computation of the generalized Hasse–Witt invariants of covers of $\mathbb{P}^1$.

This paper is a rewritten version of part of my PhD thesis. I would like to thank Kate Stevenson and Marco Garuti for their comments on an earlier version of this paper.

2 Generalized Hasse–Witt invariants

In this section we will define generalized Hasse–Witt invariants and study basic properties. Most importantly, we will give the relation between quotients of $\pi_1^t(U)$ which are an extension of a prime to p group H by a p-group P, and the generalized Hasse–Witt invariants of H-covers of X, unbranched outside S.

The generalized Hasse–Witt invariants were first introduced by Katsurada in [9] in the case of an étale ℓ-cyclic cover with $\ell|(p-1)$. In that paper they were used to show that $\pi_1(X)$ is not determined by the genus, the characteristic and the p-rank of X. Namely, it was shown that $\pi_1(X)$ also depends on the generalized Hasse–Witt invariants. The reason being that the number of (étale) covers of X whose Galois group is an extension of $\mathbb{Z}/\ell$ by $\mathbb{Z}/p$ can be expressed in terms of the generalized Hasse–Witt invariants. Later this was generalized by Nakajima [11], Rück [18] and Pacheco [13]. Of these authors Pacheco gave the most general definition, namely in the case of possibly ramified Galois covers whose Galois group is of order prime to the characteristic. Also in this case the generalized Hasse–Witt invariants of a G-Galois cover $Y \to X$ can be used to give a formula for the number of tame Galois covers of X factoring through Y, whose Galois group is an extension of G by an elementary abelian p-group. In the étale case this was proved by Pacheco.

Let $\pi : Y \to X$ be a Galois cover of nonsingular projective irreducible curves defined over an algebraically closed field k of characteristic $p > 0$. We allow the cover to be ramified. Let H be the Galois group of π, suppose that its order is prime to the characteristic. The group H acts naturally on $H^1(Y, \mathcal{O}_Y)$. As was explained in the introduction, we are interested in the dimension over $\mathbb{F}_p$ of the isotypical spaces of $H^1(Y, \mathcal{O}_Y)^F$, where F is the Frobenius morphism. For each irreducible k-character χ of G, we denote by $L(\chi)$ the χ-isotypical part of $H^1(Y, \mathcal{O}_Y)$, i.e. the largest subspace which, as a $k[G]$-module, is a sum of irreducible representation with character χ.

The Frobenius morphism F sends $L(\chi)$ to $L(\chi^p)$, here χ^p is the Frobenius twist of χ. For each irreducible character χ, we denote by $f(\chi)$ the minimal positive integer such that $F^{f(\chi)}$ sends $L(\chi)$ to itself. Recall that the p-rank $\sigma(X)$ of X is equal to the k-dimension of the largest subspace of $H^1(X, \mathcal{O}_X)$ on which F is a bijection. We mimic this to define the generalized Hasse–Witt invariants.

Definition 2.1 Let $\pi\colon Y \to X$ be a G-Galois cover of curves over k and suppose that $p \nmid |G|$. For each irreducible character χ of G, we define the *generalized Hasse–Witt invariant* $\gamma_\pi(\chi)(= \gamma(\chi))$ of the cover $\pi\colon Y \to X$ as the dimension of the largest subspace of $L(\chi^{-1})$ on which $F^{f(\chi^{-1})}$ is a bijection.

We consider the inverse character in the above definition to make our definition consistent with the literature. Let q be a sufficiently large power of p. We identify k-characters with $\mathbb{F}_q$-characters. The space $J(Y)[p] \otimes_{\mathbb{F}_p} \mathbb{F}_q$ is dual to $H^1(Y, \mathcal{O}_Y)^F \otimes_{\mathbb{F}_p} \mathbb{F}_q$ as $\mathbb{F}_p[G]$-module, [20, p. 38]. In [13] the generalized Hasse–Witt invariants are defined as the dimensions of the χ-isotypical part of $J(Y)[p] \otimes_{\mathbb{F}_p} \mathbb{F}_q$. One easily checks that this definition coincides with our definition. The following lemma gives some elementary properties of the generalized Hasse–Witt invariants (cf. [13]).

Lemma 2.2 *Let $\pi\colon Y \to X$ be a G-Galois cover of curves and suppose that $p \nmid |G|$. Let χ be an irreducible character of G and let n_χ be its dimension. Then*

(i) $\gamma(\chi) = \gamma(\chi^p)$,

(ii) more generally, let $g \in G$ then $\gamma(\chi) = \gamma(\chi^g)$,

(iii) $\sigma(Y) = \sum_\chi \gamma(\chi)$, where the sum is taken over the irreducible k-characters of H,

(iv) if χ is the trivial character, then $\gamma(\chi) = \sigma(X)$,

(v) $\gamma(\chi)$ is a multiple of n_χ,

(vi) let G_χ be the kernel of the representation corresponding to χ and write $\bar{\pi} = \pi/G_\chi$. Then χ may be considered as a character of G/G_χ and $\gamma_\pi(\chi) = \gamma_{\bar{\pi}}(\chi)$.

(vii) let $H < G$ be a subgroup and suppose $\chi = \mathrm{Ind}_H^G \chi'$. Let π' be the H-subcover of π. Then $[G : H]\gamma_{\pi'}(\chi') = \gamma_\pi(\chi)$.

Proof. We can write $L(\chi)$ as $L(\chi)^{\mathrm{s}} \oplus L(\chi)^{\mathrm{n}}$, where $F^{f(\chi)}$ is a bijection on $L(\chi)^{\mathrm{s}}$ and is nilpotent on $L(\chi)^{\mathrm{n}}$, [20, no. 9]. The Frobenius morphism is a bijection from $L(\chi)^{\mathrm{s}}$ to $L(\chi^p)^{\mathrm{s}}$. This proves the first statement. The second statement follows similarly, since $g \in G$ induces an isomorphism from $L(\chi)$ to $L(\chi^g)$. The third statement follows immediately from the first, since $H^1(Y, \mathcal{O}_Y)^{\mathrm{s}} = \oplus_{\chi \in X} L(\chi)^{\mathrm{s}}$. Let χ be the trivial character, then $L(\chi) = H^1(Y, \mathcal{O}_Y)^G \simeq H^1(X, \mathcal{O}_X)$. This proves the fourth statement. The fifth statement follows from the fact the $H^1(Y, \mathcal{O}_Y)^{\mathrm{s}}$ is a G-module. The sixth statement is obvious. To prove the last statement, note that as an H-module

$$L_H(\chi) = \oplus_{g \in G/H} L_G((\chi')^g).$$

This implies $\gamma(\chi^{-1}) = \sum_{g \in G/H} \gamma((\chi')^{-g})$. The statement now follows from (ii). □

We will now relate the generalized Hasse–Witt invariants to the quotients of $\pi_1^t(U)$. The p-rank of a curve X is related to the number of étale p-cyclic covers of X. If σ denotes the p-rank of X, then the number of étale p-cyclic covers of X is equal to the number of p-cyclic quotients of $(\mathbb{Z}/p)^\sigma$. In fact, something more general holds. The p-part of the fundamental group $\pi^p(X)$ is a free pro-p group on σ generators. Hence a p-group P occurs as Galois group of an étale cover over X iff P can be generated by σ elements. A similar statement holds for the generalized Hasse–Witt invariants.

Lemma 2.3 *Let $\pi : Y \to X$ be an H-Galois cover, with H prime to p. There is a 1-1 correspondence between Galois covers $Z \to X$ which dominate π with Galois group an extension of H by an elementary abelian p-group and H-submodules of* $\mathrm{Hom}(\pi_1(Y), \mathbb{Z}/p)$.

Proof. Suppose given a Galois cover $Z \to X$ which dominates π, whose Galois group G is an extension of H by an elementary abelian p-group $P \simeq (\mathbb{Z}/p)^n$. Let $V = \mathrm{Hom}(\mathrm{Gal}(Z, Y), \mathbb{Z}/p)$. We may regard V as a subspace of $\mathrm{Hom}(\pi_1(Y), \mathbb{Z}/p)$ via the exact sequence

$$0 \to \pi_1(Z) \to \pi_1(Y) \to \mathrm{Gal}(Z, Y) = P \to 0.$$

Note that V as an $\mathbb{F}_p[H]$-module is dual to P.

Conversely, suppose given $V \subset \mathrm{Hom}(\pi_1(Y), \mathbb{Z}/p)$ with $\dim_{\mathbb{F}_p} V = n$. Then V corresponds to an étale $(\mathbb{Z}/p)^n$-Galois cover $Z \to Y$. The cover $Z \to X$ is Galois iff V is H-equivariant. The space V with the action of H can be identified with $\mathrm{Hom}(\mathrm{Gal}(Z, Y), \mathbb{Z}/p)$. $\square$

Let $X(H)$ be the set of irreducible k-characters of H. Write $\chi \sim \chi'$ if $\chi' = \chi^{p^j}$ for some j. Let $\bar{X}(H) = X(H)/\sim$. Recall that the set $\bar{X}(H)$ corresponds to the set of $\mathbb{F}_p$-irreducible characters of H.

For an $\mathbb{F}_p[H]$-module P, write $\sum_{[\chi] \in \bar{X}(H)} m_P(\chi)(\chi + \chi^p + \cdots + \chi^{p^{f-1}})$ for its character and let $n_P = \dim_{\mathbb{F}_p} P$. Let $P^* = \mathrm{Hom}(P, \mathbb{Z}/p)$ be the dual $\mathbb{F}_p[H]$-module. The proof of the above lemma shows that $P^* \subset H^1(Y, \mathcal{O}_Y)^F$ corresponds to a tame $P \rtimes H$ cover dominating π. The character of $H^1(Y, \mathcal{O}_Y)^F$ is

$$\sum_{[\chi] \in \bar{X}(H)} (\gamma(\chi^{-1})/n(\chi))(\chi + \chi^p + \cdots + \chi^{p^{f-1}}).$$

Therefore $P^* \subset H^1(Y, \mathcal{O}_Y)^F$ iff $m_P(\chi) \le \gamma(\chi)/n(\chi)$ for all χ.

Let $\phi \in \mathrm{Aut}(H)$. For an irreducible k-character χ, denote by χ^ϕ the character obtained by twisting by ϕ. Let P be as above and put $G = P \rtimes H$. Then there exists a tame G-cover dominating π iff there exists a $\phi \in \mathrm{Aut}(H)$ such that

$$m_P(\chi) \le \gamma(\chi^\phi)/n(\chi).$$

We need to twist by ϕ because for two different $\mathbb{F}_p[H]$-modules P and P', the groups $P \rtimes H$ and $P' \rtimes H$ might be isomorphic. This proves the following proposition.

Proposition 2.4 *Let $\pi : Y \to X$ be a tame H-Galois cover of nonsingular curves. Let P be an $\mathbb{F}_p[H]$-module and put $G = P \rtimes H$. Then there exists a tame G-Galois cover of X dominating π if and only if there exists an automorphism ϕ of H such that*

$$m(\chi) \le \frac{\gamma(\chi^\phi)}{n(\chi)} \text{ for each } [\chi] \in \bar{X}(H),$$

where $n(\chi)$ is the dimension of the representation with character χ.

Results similar to the proposition above can be found in [11] and [13]. The result of [11] is a special case of the result in [13] which is a special case of the present case. Our proof follows the proof of [11].

We can phrase this proposition differently. Let $G_{\max}$ be the group which is an extension of H by the elementary abelian p-group $P = (\mathbb{Z}/p)^{\sigma(Y)}$, where H acts on P via $\sum_{\chi \in X(H)} (\gamma(\chi)/n(\chi))\chi$. Then $G_{\max}$ is the largest extension of H by an elementary abelian p-group for which there is a Galois cover dominating π. A group G as in the proposition exists if and only if G is a quotient of $G_{\max}$.

Proposition 2.5 *Let G be a group which is an extension of a prime to p group H by a p-group P. Let $\Phi(P) = P^p[P,P]$ be the Frattini subgroup of P and $\overline{P} = P/\Phi(P)$. Write $\overline{G} = \overline{P} \rtimes H$. Suppose given a tame $\overline{G}$-cover $f: Z \to X$. Then there exists a tame G-cover $g: W \to X$ dominating f.*

Proof. The proposition is proved in [14] for étale covers, but the proof carries over immediately to the case of tamely ramified covers. The results follows from the fact that, for $Y = Z/\bar{P}$, the p-part of the fundamental group $\pi_1^p(Y)$ is a free pro-p group. □

3 A bound on the p-rank

From Lemma 2.2 it follows that

$$\gamma(\chi^{-1}) \leq \min_j \dim L(\chi^{p^j}).$$

For the p-rank of Y, this implies

$$\sigma(Y) - \sigma(X) \leq \sum_{\chi \neq 1} \min_j \dim L(\chi^{p^j}). \tag{1}$$

Therefore knowledge of the dimensions of the $L(\chi^j)$ gives nontrivial information on the generalized Hasse–Witt invariants and the p-rank of the cover. These dimensions are known by a classical result of Chevalley–Weil [1] (Proposition 3.1 below). The results was originally stated for $k = \mathbb{C}$, but can be extended to the our case, since $p \nmid |G|$ (see [8], [12]).

For each $y \in Y$ write G_y for the decomposition group of y, let e_y be the order of G_y. Choose a local parameter u_y at y. Define a character

$$\theta_y : G_y \to k^\star,\ \theta_y(g) = \frac{g \cdot u_y}{u_y} \pmod{(u_y)}. \tag{2}$$

Note that if $y_1,\ y_2 \in Y$ both map to $x \in X$ then the characters θ_{y_1} and θ_{y_2} are conjugate.

Proposition 3.1 (Chevalley–Weil) *There exists a unique $k[G]$-module R such that*

$$|G| \cdot R \simeq \bigoplus_{y \in Y} (\bigoplus_{d=0}^{e_y - 1} d \cdot \mathrm{Ind}_{G_y}^G \theta_y^d) \tag{3}$$

as $k[G]$-modules. The $k[G]$-module structure of $H^1(Y, \mathcal{O}_Y)$ is given by

$$H^1(Y, \mathcal{O}_Y) \simeq k \oplus k[G]^{g(X)-1} \oplus R.$$

Definition 3.2 Let $x_1, \ldots, x_r$ be the branch points of the G-Galois cover $\pi: Y \to X$. For each branch point $x_i \in X$ choose $y_i \in \pi^{-1}(x_i)$. Let θ_{y_i} be the character defined in (2). Then the set of characters $(G; \theta_{y_1}, \ldots, \theta_{y_r})$ we will call the *type* of $\pi: Y \to X$.

Note that the Galois module structure of $H^1(Y, \mathcal{O}_Y)$ can be described in terms of the type. Let $\theta = (G; \theta_{y_1}, \ldots, \theta_{y_r})$ be a type corresponding to some group G of order prime to p. Let $R = R_\theta$ be the module defined in (3). For an irreducible character χ of G, let V_χ be the G-module over k with character χ and write n_χ for the dimension of V_χ. By $f(\chi)$ we denote the smallest positive integer f such that the p^fth twist of χ is equal to χ. Write $R = \oplus_\chi m_\chi V_\chi$. Then for $\chi \neq 1$ the multiplicity of V_χ in $k \oplus k[G]^{g-1} \oplus R$ is $m_\chi + (g-1)n_\chi$. For each nonnegative integer g define

$$B(\theta, g) := \sum_{1 \neq \chi \in \bar{X}} f(\chi) \min_j [(m_{\chi^{p^j}} + (g-1)n_\chi) \cdot n_\chi].$$

Let $Y \to X$ be a G-Galois cover with type θ and $g(X) = g$. Then, using the notation explained above, the multiplicity of a nontrivial irreducible character χ of G in $H^1(Y, \mathcal{O}_Y)$ is $m_\chi + (g-1)n_\chi$ by the result of Proposition 3.1. The result of (1) becomes with the new notation

$$\sigma(Y) - \sigma(X) \le B(\theta, g). \tag{4}$$

One can ask the following question.

Question 3.3 Suppose (X, S) is the generic r-pointed curve of genus g. Let H be a group of order prime to p. Fix the monodromy $\mathbf{a}$. Is it true that all H-covers with monodromy $\mathbf{a}$ have p-rank equal to $B(\theta, g)$?

Example 3.4 (i) Let E be an elliptic curve with an automorphism ϕ of order three, defined over an algebraically closed field k of characteristic not three. Then $g(E/<\phi>) = 0$. This implies that ϕ acts nontrivially on the 1-dimensional space $H^1(E, \mathcal{O}_E)$. Let χ be the character of this representation. Then $\dim L(\chi) = 1$ and $\dim L(\chi^2) = 0$. We find

$$\sum_{\chi \in \bar{X}} f(\chi) \min_j \dim L(\chi^{-p^j}) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ 0 & \text{if } p \equiv 2 \pmod 3). \end{cases}$$

Of course, it is well known that $\sigma(E) = 1$ if $p \equiv 1 \pmod 3$ and $\sigma(E) = 0$ if $p \equiv 2 \pmod 3$. So in this case, $\sigma(E)$ is equal to the bound.
(ii) Let E_λ be the 2-cyclic cover of $\mathbb{P}^1$ branched at $0, 1, \infty, \lambda$ and suppose that $p \neq 2$. The $\sigma(E_\lambda)$ is one for almost all λ and zero for finitely many λ. This illustrates that the p-rank varies in a family of covers. This explains the condition (X, S) generic in Question 3.3.

In what follows we will mainly consider Question 3.3 for cyclic covers. Here the results are quite general. The case of abelian covers can be reduced to the case of cyclic covers. In the rest of this section we will consider the question for nonabelian covers. We will see that the answer to the question is no, in general: there exists a nonabelian cover $Y \to \mathbb{P}^1$ branched at three points with $\sigma(Y) < B(\theta, 0)$.

This situation is similar to the situation for étale covers. For $Y \to X$ étale, the statement of Proposition 3.1 becomes:

$$H^1(Y, \mathcal{O}_Y) \simeq k \oplus k[G]^{g(X)-1},$$

as $k[G]$-modules. Therefore the expression for the bound $B(\theta, g)$ in (4) becomes very easy:

$$B(\theta, g) = g(Y) - g(X).$$

Question 3.3 becomes in this case: are all étale Galois covers of prime to p order of the generic curve ordinary? Nakajima [11] has proved that this is true for all abelian covers. Raynaud [17] has shown that there exist nonabelian étale covers of the generic curve which are nonordinary. In fact, (some of) the covers given in that paper have nilpotent Galois group; the nonordinary cover discussed below has a solvable Galois group.

This example was suggested to me by M. Raynaud. Consider Galois covers $\pi\colon Y \to \mathbb{P}^1_{\mathbb{Q}}$ branched at three points $0, 1, \infty$, with Galois group S_4 and ramification of order $4, 4, 3$. We are going to show that for infinitely many primes p the curve Y has good supersingular reduction mod p. Note that for S_n covers of $\mathbb{P}^1$ in characteristic $p > n$ the bound is equal to the genus, since all irreducible characters of S_n are defined over the prime field.

Let C_1 (resp. C_2) be the conjugacy class in S_4 of a 4-cycle (resp. a 3-cycle). The triple (C_1, C_1, C_2) is rational and rigid and therefore $Y \to \mathbb{P}^1$ is defined over $\mathbb{Q}$. Note that $g(Y) = 3$. Define $H_1 = <(12)(34)>$, $H_2 = <(13)(24)>$, $H_3 = <(14)(23)>$ as subgroups of S_4 and let $E_i = Y/H_i$. The E_i are isomorphic elliptic curves defined over $\mathbb{Q}$. (They have j-invariant

$2^4 \cdot 13^3 \cdot 3^{-2}$.) This implies that $J(Y) \sim E_1 \times E_2 \times E_3 \simeq E_1^3$. To compute the p-rank of the reduction Y_p of Y to characteristic p it suffices to compute the p-rank of $E_{1,p}$. By the result of Elkies [3] the elliptic curve E_1 has infinitely many primes of supersingular reduction. Since $J(Y) \sim E_1^3$, the same holds for Y.

This proves the following lemma.

Lemma 3.5 *There exist a $p \neq 2, 3$ and a S_4-cover $Y \to \mathbb{P}^1$ unbranched outside $0, 1, \infty$ for which $\sigma(Y) < B(\mathbf{a}, 0)$.*

4 Cyclic covers

In the previous section it is shown that there exists a nonabelian cover of $\mathbb{P}^1 - \{0, 1, \infty\}$ for which the p-rank is less than the bound. Therefore the answer to Question 3.3 is no, in general. We may ask what happens for abelian covers. It turn out that for abelian cases the answer to the question is yes, in many cases. In this section we specialize the results of the previous two sections to abelian covers. Note that by part (vi) of Lemma 2.2 we may reduce the computation of the generalized Hasse–Witt invariants of an abelian cover to the generalized Hasse–Witt invariants of suitable cyclic subcovers. In case of a cyclic cover the result of Chevalley–Weil becomes easier to formulate.

Let $\pi : Y \to X$ be a H-Galois cover with $p \nmid |H|$ and H cyclic of order ℓ. Note that ℓ is not supposed to be prime. We fix a generator ϕ of H and a primitive ℓth root of unity $\zeta \in k$. The definition of type can be reformulated as follows in this case. This reformulation is less canonical, but will facilitate the formulas in what follows. Let $x_1, \ldots, x_r$ be the branch points of π. Write $n_i = |\pi^{-1}(x_i)|$. For each i, choose some $y_i \in \pi^{-1}(x_i)$ and a local parameter u_i at y_i. Let χ be the character of H which sends ϕ to ζ. We will write L_i and γ_i in stead of $L(\chi)$ and $\gamma(\chi)$.

Definition 4.1 We say that π is of *type* $(\ell; a_1, \ldots, a_r)$ if for all $i \in \{1, \ldots, r\}$ we have that $0 \leq a_i < \ell$ and $n_i | a_i$ and $(\phi^{n_i})^\star u_i = \zeta^{n_i b_i} u_i \pmod{(u_i^2)}$, where $b_i \cdot a_i / n_i \equiv 1 \pmod{\ell / n_i}$.

We will suppose the branch points to be ordered. In the statement '$Y \to X$ is a cover of type $\mathbf{a} = (\ell; a_1, \ldots, a_r)$ branched at $x_1, \ldots, x_r$' we will assume the a_i corresponds to the x_i as in the definition above.

We can interpret the type of an ℓ-cyclic cover $\pi : Y \to X$ in terms of the map $f : \pi_1^t(X - \{x_1, \ldots, x_r\}) \twoheadrightarrow \mathbb{Z}/\ell$ corresponding to the cover. Choose generating elements $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g, \delta_1, \ldots, \delta_r$ of $\pi_1^t(X - \{x_i\})$ such that $\prod [\alpha_i, \beta_i] \prod \delta_i = 1$ and such that for each continuous $\pi_1^t(X - \{x_i\}) \twoheadrightarrow G$, with G finite, the images of the δ_i generate a decomposition group above x_i (see [6, XIII.2.12]). The cover π is of type $(\ell; f(\delta_1), \ldots, f(\delta_r))$. If $(\ell; a_1, \ldots, a_r)$ is a type, then $\sum a_i \equiv 0 \pmod{n}$. Conversely, if $\sum a_i \equiv 0 \pmod{\ell}$ then there exists a (not necessarily connected) cover of type $(\ell; a_1, \ldots, a_r)$.

The type of a cyclic cover as defined above, contains the same information as the type defined in the previous section. The two definitions can be related as follows. Let $\pi : Y \to X$ be as above. Let y_i be some point mapping to a branch point x_i. Then ϕ^{n_i} generates the decomposition group of y_i. The character θ_{y_i}, which was defined in (2), sends ϕ^{n_i} to $\zeta^{n_i b_i}$. Conversely, given the character θ_{y_i} we find a_i as the integer $0 \leq a_i < \ell$ which is a multiple of n_i and satisfies $a_i b_i / n_i \equiv 1 \pmod{\ell / n_i}$.

The definition of type is independent of the choice of μ_i and u_i. Replacing ϕ or ζ changes $(\ell; a_1, \ldots, a_r)$ into $(\ell; n a_1, \ldots, n a_r)$ for some $n \in (\mathbb{Z}/\ell)^\star$. Hence we should consider the type as an element of

$$\{(a_1, \ldots, a_r) \quad | \quad 0 \leq a_i < \ell, \ \sum a_i \equiv 0 \pmod{\ell}\} / (\mathbb{Z}/\ell)^\star.$$

We will always choose a representative of such a class.

Example 4.2 Suppose $g(X)=0$ and choose $x_1,\dots,x_r\in X$. If $\sum a_i\equiv 0 \pmod{\ell}$ then, up to isomorphism, there is a unique cover $Y\to\mathbb{P}^1$ of type $(\ell;a_1,\dots,a_r)$ with Y nonsingular, branched at $x_1,\dots x_r\in\mathbb{P}^1_k$. If none of the x_i is ∞, this curve is the nonsingular curve associated to the equation

$$y^\ell=(x-x_1)^{a_1}(x-x_2)^{a_2}\cdots(x-x_r)^{a_r}.$$

The curve Y is connected iff $\gcd(\ell,a_1,\dots,a_r)=1$.

Lemma 4.3 *Let $\pi\colon Y\to X$ be of type $(\ell;a_1,\dots,a_r)$. Then*

$$\dim_k L_i=\begin{cases} g(X) & \textit{if } i=0,\\ (\sum_{j=1}^r\langle\frac{ia_j}{\ell}\rangle)-1+g(X) & \textit{otherwise.}\end{cases}$$

Here $\langle\cdot\rangle$ denotes the fractional part.

Proof. The lemma follows from Proposition 3.1; in a slightly different terminology, it is a special case of [8, Proposition 1]. But we can also prove it directly.

We can write $\pi_\star\mathcal{O}_Y=\oplus_{i=0}^{\ell-1}\mathcal{L}_i$, where locally $\mathcal{L}_i$ is the eigenspace of ϕ with eigenvalue ζ^i. This is Kummer theory. Choose $y_j\in\pi^{-1}(x_j)$ for each j. Let u_j be a local parameter at y_j such that $\phi^{n_j}(u_j)=\zeta^{n_jb_j}u_j$, with notation as in Definition 4.1. Then, by the definition of type, $\pi_\star((u_j\phi(u_j)\cdots\phi^{n_j-1}(u_j))^{\langle ia_j/\ell\rangle n_j})$ generates $\mathcal{L}_i$ locally around x_j. It follows that

$$\mathcal{L}_i^{\otimes\ell}\simeq\mathcal{O}_X(-\sum_{j=1}^r\langle\frac{ia_j}{\ell}\rangle\ell x_j).$$

In fact $\mathcal{L}_i=\mathcal{L}^i$. Hence

$$\deg\mathcal{L}_i=\frac{1}{\ell}\sum_{j=1}^r\langle\frac{ia_j}{\ell}\rangle\ell.$$

Note that $H^1(X,\mathcal{L}_i)\simeq L_i$. We find that

$$\dim_k L_i=\dim_k H^1(X,\mathcal{L}_i)=(\sum_{j=1}^r\langle\frac{ia_j}{\ell}\rangle)+g(X)-1,$$

by the Riemann–Roch Theorem. □

Notation 4.4 For a type $\mathbf{a}=(\ell;a_1,\dots,a_r)$ we will denote $\|i\|=\|i\|_{\mathbf{a}}=(\sum_{j=1}^r\langle ia_j/\ell\rangle)-1$ for $i\in(\mathbb{Z}/\ell)-\{0\}$. In case $\|i\|_{\mathbf{a}}\geq 0$, it is equal to the dimension of the ith eigenspace L_i of $H^1(Y,\mathcal{O}_Y)$, where $Y\to\mathbb{P}^1$ is a cover of type $\mathbf{a}$. If all a_j's are zero $\pmod{\ell/(i,\ell)}$ then $\|i\|_{\mathbf{a}}=-1$ and then $\|i\|$ does not have an interpretation as a dimension of an isotypical space of a cover of $\mathbb{P}^1$, but we will use the notation in this case nonetheless.

Lemma 4.5 *Fix a type $(\ell;a_1,\dots,a_r)$. Let s be the number of a_j unequal to $0 \bmod \ell/(i,\ell)$. Then*

$$\begin{array}{ll}\|i\|+\|-i\|=s-2 & \textit{if } \ell/(i,\ell)\neq 2,\\ \|i\|=\frac{s}{2}-1 & \textit{if } \ell/(i,\ell)=2.\end{array}$$

In particular, $\|i\|\leq s-2$.

Proof. Immediate. □

Lemma 4.6 *Let* $\mathbf{a}$ *be a type and* X *any curve. Denote by* $\Delta_r \subset X^r$ *the generalized diagonal. Define* $U_{\mathbf{a}} \subset X^r - \Delta$ *as the set of* $(x_1, \ldots, x_r) \in X^r - \Delta$ *such that for all* ℓ*-cyclic covers* $Y \to X$*, unbranched outside the* x_i*, of type* $\mathbf{a}$*, we have* $\sigma(Y) - \sigma(X) = B(\mathbf{a}, g(X))$*. Then* $U_{\mathbf{a}}$ *is open.*

Proof. For each $(x_1, \ldots, x_r) \in X^r - \Delta$ we define $Y_{x_1,\ldots,x_r} \to X$ as the smallest cover which has all covers of X of type $\mathbf{a}$ branched at the x_i as subcovers. Choose generators $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g, \delta_1, \ldots, \delta_r$ of $\pi_1^t(X - \{x_1, \ldots, x_r\})$ such that for each finite quotient the images of the δ_i generate a decomposition group above x_i. The cover $Y_{x_1,\ldots,x_r} \to X$ corresponds to the maximal quotient

$$\pi_1^t(X - \{x_1, \ldots, x_r\}) \twoheadrightarrow (\mathbb{Z}/\ell)^n$$

which sends δ_i to $a_i, \ldots, a_i$. For suitable ℓ-cyclic subcovers of $Y_{x_1,\ldots,x_r} \to X$ we have

$$J(Y_{x_1,\ldots,x_r}) \sim J(X) \times \prod_{j=1}^{n} (J(Y_j)/J(X)).$$

Here, for a curve Z we denote by $J(Z)$ its Jacobian. This implies $\sigma(Y_{x_1,\ldots,x_r}) \leq \sigma(X) + nB(\mathbf{a}, g(X)) =: s$. We obtain a family $f\colon \mathcal{A} \to X^r - \Delta_r$, with $\mathcal{A}_{x_1,\ldots,x_r} = J(Y_{x_1,\ldots,x_r})$. Let $W_{\mathbf{a}} = X^r - (\Delta_r \cup U_{\mathbf{a}}) = \{(x_1, \ldots, x_r) | \sigma(Y_{x_1,\ldots,x_r}) \leq s - 1\}$. From [15, Cor. 1.5] it follows that $W_{\mathbf{a}}$ is closed. This proves the lemma. $\square$

5 Coefficients of the Hasse–Witt matrix

Let $\pi\colon Y \to \mathbb{P}^1$ be an ℓ-cyclic cover, defined over an algebraically closed field k of characteristic p with $(\ell, p) = 1$. In this section we will compute the coefficients of the Hasse–Witt matrix of Y and relate these coefficients to the generalized Hasse–Witt invariants. We fix the following notations. The branch points of π we will denote by $x_1, \ldots, x_r$, and $\mathbf{a} = (\ell; a_1, \ldots, a_r)$ will be the type of the cover π (defined in Section 4). We choose a coordinate on $\mathbb{P}^1$ such that none of the x_i is ∞. We will suppose that none of the a_i is congruent to zero $\bmod\, \ell$. We denote by L_i the ith eigenspace of $H^1(Y, \mathcal{O}_Y)$ with respect to a fixed primitive ℓth root of unity ζ and a fixed generator ϕ of $\mathrm{Gal}(Y, \mathbb{P}^1)$ as in Section 4, i.e. $L_i = \{\xi | \phi \cdot \xi = \zeta^i \xi\}$. The dimension of L_i we denote by $\|i\|$; it is equal to $(\sum_{j=1}^r \langle i a_j/\ell \rangle) - 1$. The integer f denotes the order of p in $(\mathbb{Z}/\ell)^\star$. Note $F^f\colon L_i \to L_i$. Put $m = (p^f - 1)/\ell$. The curve Y is the nonsingular projective curve defined by the equation

$$y^\ell = (x - x_1)^{a_1} (x - x_2)^{a_2} \cdots (x - x_r)^{a_r}.$$

We are going to calculate the coefficients of the matrix of F^f on L_i. We will compute them using Čech cohomology; we first describe a basis of $H^1(Y, \mathcal{O}_Y)$ (cf. [21, Section 5], note that the $\|i\|$ from that paper is $+1$ more than our $\|i\|$). A special case of this result is proved in [4], using a different method. Write $U_1 = \mathbb{P}^1 - \{0\}$ and $U_2 = \mathbb{P}^1 - \{\infty\}$. As open sets we take $V_s = \pi^{-1}(U_s) \subset Y$ for $s = 1, 2$. For $i = 1, \ldots, \ell - 1$ let

$$v_i = y^i (x - x_1)^{-[i\frac{a_1}{\ell}]} \cdots (x - x_r)^{-[i\frac{a_r}{\ell}]}.$$

Note

$$\begin{aligned}
\Gamma(V_1, \mathcal{O}_{V_1}) &= \bigoplus_{i=1}^{\ell-1} k[x]\, v_i, \\
\Gamma(V_2, \mathcal{O}_{V_2}) &= \bigoplus_{i=1}^{\ell-1} k[x^{-1}]\, x^{-\|i\|-1} v_i, \\
\Gamma(V_1 \cap V_2, \mathcal{O}) &= \bigoplus_{i=1}^{\ell-1} k[x, x^{-1}]\, v_i.
\end{aligned}$$

Define

$$\xi_{i,j} = x^{-j} v_i \quad \text{for } j = 1, \ldots, \|i\|$$

as an element of $H^1(Y, \mathcal{O}_Y) = \Gamma(V_1 \cap V_2)/(\Gamma(V_1) + \Gamma(V_2))$. Then the $\{\xi_{i,j} | 0 < i < \ell,\ 0 < j \leq \|i\|\}$ form a basis of $H^1(Y, \mathcal{O}_Y)$. More precisely, $L_i = <\xi_{i,j}>$. Let B_i be the matrix of $F^f : L_i \to L_i$ with respect to the basis $\xi_{i,j}$, for $1 \leq j \leq \|i\|$. We will compute the coefficients of B_i. To calculate the (j, j')-th coefficient of B_i we have to find the coefficient of $\xi_{i,j'}$ in $(\xi_{i,j})^{p^f}$. We have

$$(\xi_{i,j})^{p^f} = x^{-jp^f} y^{ip^f} (x - x_1)^{-p^f [i \frac{a_1}{\ell}]} \cdots (x - x_r)^{-p^f [i \frac{a_r}{\ell}]}.$$

Note $-p^f [ia/\ell] = -[p^f ia/\ell] + [p^f \langle ia/\ell \rangle] = -[ia/\ell] - iam + \ell m \langle ia/\ell \rangle$ and $y^\ell (x - x_1)^{-a_i} \ldots (x - x_r)^{-a_r} = 1$. Hence

$$(\xi_{i,j})^{p^f} = (x)^{-jp^f} (x - x_1)^{\ell m \langle \frac{ia_1}{\ell} \rangle} \cdots (x - x_r)^{\ell m \langle \frac{ia_r}{\ell} \rangle} v_i. \tag{5}$$

The coefficient of $\xi_{i,j'}$ in $(\xi_{i,j})^{p^f}$ is

$$(-1)^N \sum_{n_1 + \cdots + n_r = N} \binom{m\ell \langle \frac{ia_1}{\ell} \rangle}{n_1} \cdots \binom{m\ell \langle \frac{ia_r}{\ell} \rangle}{n_r} x_1^{n_1} \cdots x_r^{n_r}, \tag{6}$$

where $N = (\|i\| + 1 - j)\ell m + j' - j$. This proves the first part of the following lemma. The other part is proved analogously.

Lemma 5.1 *Let $(\xi_{i,j})_{i,j}$ be the basis of $H^1(Y, \mathcal{O}_Y)$ which was described above.*
(i) The $(i, j), (i, j')$-th coefficient of the matrix of F^f on $H^1(Y, \mathcal{O}_Y)$ is

$$(-1)^N \sum_{n_1 + \cdots + n_r = N} \binom{m\ell \langle \frac{ia_1}{n} \rangle}{n_1} \cdots \binom{m\ell \langle \frac{ia_r}{n} \rangle}{n_r} x_1^{n_1} \cdots x_r^{n_r}, \tag{7}$$

where $N = (\|i\| + 1 - j)\ell m + j' - j$.
(ii) If $i' \equiv pi \pmod{\ell}$, then the $(i, j), (i', j')$-th coefficient of the Hasse–Witt matrix of Y is equal to

$$(-1)^N \sum_{\substack{n_1 + \cdots + n_r = N \\ 0 \leq n_j \leq [p \langle \frac{ia_j}{n} \rangle]}} \binom{[p \langle \frac{ia_1}{n} \rangle]}{n_1} \cdots \binom{[p \langle \frac{ia_r}{n} \rangle]}{n_r} x_1^{n_1} \cdots x_r^{n_r}, \tag{8}$$

where $N = p(\|i\| + 1 - j) - (\|i'\| + 1 - j')$. If $i' \not\equiv pi \pmod{\ell}$, then the $(i, j), (i', j')$th coefficient of the Hasse–Witt matrix is zero.

6 Main Theorem

Theorem 6.1 *Suppose $p \geq \ell(r - 3)$. Then for each $\mathbf{a} = (\ell; a_1, \ldots, a_r)$ there exist $x_1, \ldots, x_r$ such that for the ℓ-cyclic cover $Y \to \mathbb{P}^1$ of type $\mathbf{a}$ branched at $x_1, \ldots, x_r$ we have*

$$\sigma(Y) = B(\mathbf{a}, 0).$$

To prove the theorem, we have to prove that there exist $x_1, \ldots, x_r \in \mathbb{P}^1_k$ such that for every $1 \leq j \leq \ell$ we have $\gamma_j = \min_i \|p^i j\|$. It is no restriction to suppose that $j = 1$ and $n := \|1\| \leq \|p^i\|$ for all i. Let B be the matrix of $F^f : L_1 \to L_1$ with respect to the basis $\xi_{1,j}$. Let A be the matrix of $F : \oplus_{i=0}^{f-1} L_{p^i} \to \oplus_{i=0}^{f-1} L_{p^i}$ and A_i the matrix of $F : L_{p^i} \to L_{p^{i+1}}$. To prove the theorem, we will prove that $\det(B)$ is not identically zero as polynomial in the x_i. We will prove this by showing that a certain monomial occurs in $\det(B)$ with a nonzero coefficient. The strategy of the proof is the following. We define an ordering on monomials in $x_1, \dots, x_r$. We give an expression for $\det(B)$ as a sum over an index set $\mathcal{J}$ of terms which are products of determinants of $n \times n$ submatrices of the A_i (Lemma 6.2). We find for each $J \in \mathcal{J}$ the largest monomial T_J with respect to the ordering (Lemma 6.4). We conclude the proof by showing that for $J \neq J'$ we have $T_J \neq T_{J'}$ (Lemma 6.5).

Recall that each L_{p^i} has a basis $\xi_{p^i,j}$ with $0 < j \leq \|p^i\|$ (see the previous section). Number the rows and columns of A as (i,j) with $0 \leq i \leq f-1$ and $1 \leq j \leq \|p^i\|$. Here (i,j) corresponds to the basis vector $\xi_{p^i,j}$ of L_{p^i}. Put $I = \{(i,j) | 0 \leq i \leq f-1,\ 1 \leq j \leq \|p^i\|\}$. Let $\mathcal{J}$ be the set of $J \subset I$ such that J contains for each i exactly n indices $(i, j_i(\alpha))$ and $j_i(1) < j_i(2) < \cdots < j_i(n)$. For $i = 0$ we put $j_i(n) = n$. To a $J \in \mathcal{J}$ we associate for each i a matrix $M_{J,i}$. This $M_{J,i}$ is the $n \times n$ submatrix of A_i consisting of the columns $(i, j_i(1)), \cdots, (i, j_i(n))$ and the rows $(i+1, j_{i+1}(1)), \cdots, (i+1, j_{i+1}(n))$. For $i = f-1$, the matrix $M_{J,i}$ has columns $(i, j_i(1)), \cdots, (i, j_i(n))$ and rows $(1, j_1(1)), \cdots, (1, j_1(n))$.

Lemma 6.2 *We have*

$$\det(B) = \sum_{J \in \mathcal{J}} \Big(\prod_{i=0}^{f-1} |M_{J,i}|^{p^{f-1-i}} \Big).$$

Proof. The lemma follows from the fact that

$$B = A_{f-1} A_{f-2}^{(p)} \cdots A_0^{(p^{f-1})},$$

here A^p is the matrix obtained by raising all the coefficients of A to the pth power. □

Notation 6.3 Define an ordering on monomials $x_1^{n_1} \cdots x_r^{n_r}$ by $x_1^{n_1} \cdots x_r^{n_r} > x_1^{k_1} \cdots x_r^{k_r}$ if there exists an i such that $k_j = n_j$ for all $j < i$ and $n_i > k_i$.

Lemma 6.4 *The largest monomial in* $\det(M_{J,i})$ *is the largest monomial in the trace of* $M_{J,i}$*. Define* T_J *as the largest monomial in* $\prod_{i=0}^{f-1} |M_{J,i}|^{p^{f-1-i}}$*. Then* T_J *is not identically zero as polynomial in the* x_i*.*

Proof. Let $M = M_{J,i}$. Recall that the columns of M are $(i, j_i(\alpha))$ and the rows are $(i+1, j_{i+1}(\alpha))$ and $1 \leq j_i(1) < \cdots < j_i(n) \leq \|p^i\|$ and $1 \leq j_{i+1}(1) < \cdots < j_{i+1}(n) \leq \|p^{i+1}\|$. We simplify the notation in this proof by numbering the rows and columns of M by $1, \dots, n$ and dropping i from the notation. The coefficients of M are

$$b_{xy} = (-1)^{N_{xy}} \sum_{n_1 + \cdots + n_r = N_{xy}^i} \binom{[p\langle \frac{p^i a_1}{\ell} \rangle]}{n_1} \cdots \binom{[p\langle \frac{p^i a_r}{\ell} \rangle]}{n_r} x_1^{n_1} \cdots x_r^{n_r},$$

with $N_{xy} = p(\|p^i\| + 1 - x) - (\|p^{i+1}\| + 1 - y)$, as was explained in the previous section.

Define $c_{xy}^i = c_{xy}$ as the smallest number c in $\{1, \dots, r\}$ such that

$$[p\langle \frac{p^i a_1}{\ell} \rangle] + \cdots + [p\langle \frac{p^i a_c}{\ell} \rangle] > N_{xy}.$$

And let

$$C_{xy}^i = C_{xy} = N_{xy} - ([p\langle \frac{p^i a_1}{\ell} \rangle] + \cdots + [p\langle \frac{p^i a_{c-1}}{\ell} \rangle]), \text{ where } c = c_{xy}.$$

Note that c_{xy} is well defined, since $p > r-2$. Furthermore, $0 \leq C_{xy} < [p\langle \frac{p^i a_c}{\ell} \rangle]$.

The largest monomial in b_{xy} is

$$T_{xy} := (-1)^{N_{xy}} \binom{[p\langle \frac{p^i a_c}{\ell} \rangle]}{C_{xy}} x_1^{[p\langle \frac{p^i a_1}{\ell} \rangle]} \cdots x_{c-1}^{[p\langle \frac{p^i a_{c-1}}{\ell} \rangle]} x_c^C.$$

One checks that

$$\begin{aligned} T_{xy} &\geq T_{zy} \text{ if } x \leq z, & (9)\\ T_{xy} &\leq T_{xz} \text{ if } y \leq z. & (10)\end{aligned}$$

We will prove the first claim of the lemma by induction. For $n = 1$ there is nothing to prove. In case $n = 2$ the lemma follows from (9) and (10). For $n > 2$ we have

$$\det(M) = \sum_{\alpha=1}^{n} (-1)^{\alpha} m_{1\alpha} |M_{1\alpha}|, \tag{11}$$

where $M_{1\alpha}$ is the determinant of of the submatrix of M obtained by omitting the first column and the αth row. Therefore, by the induction hypothesis

$$T_{\alpha} := T_{1\alpha} T_{21} \cdots T_{\alpha,\alpha-1} T_{\alpha+1,\alpha+1} \cdots T_{nn} \text{ for } \alpha = 1, \dots, n$$

is the largest monomial in $m_{1\alpha}|M_{1\alpha}|$ (cf. (11)). One checks that

$$T_{\alpha} - T_{\alpha+1} = T_{21} \cdots T_{\alpha,\alpha-1} T_{\alpha+2,\alpha+2} \cdots T_{nn} (T_{1\alpha} T_{\alpha+1,\alpha+1} - T_{1\alpha+1} T_{\alpha+1,\alpha}).$$

Now $T_{xy} > 0$ for all x and y and $T_{1\alpha} T_{\alpha+1,\alpha+1} > T_{1,\alpha+1} T_{\alpha+1,\alpha}$ by the $n = 2$ case. This proves the first statement of the lemma.

It follows that

$$T_J = \prod_{i=0}^{f-1} (T^{i}_{j_i(1) j_{i+1}(1)} \cdots T^{i}_{j_i(n) j_{i+1}(n)})^{p^{f-1-i}}. \tag{12}$$

It is clear from the expression for the T^i_{xy} given above that T_J is not identically zero as polynomial in the x_i. □

To finish the proof of Main Theorem, we have to find a nonvanishing monomial in the expression for $\det(B)$ given in Lemma 6.2. This is done if we show that for $J_1 \neq J_2$ we have that the monomials T_{J_1} and T_{J_2} are nonidentical. In that case the largest of the T_J does not cancel in $\det(B)$. This is proved in the next lemma. This is the only place where we use the assumption $p \geq \ell(r-2)$. Up to now we only used $p \geq r - 2$.

Lemma 6.5 *Suppose $p \geq \ell(r-3)$. Let $J_1, J_2 \in \mathcal{J}$. If T_{J_1} and T_{J_2} are equal up to a (nonzero) constant, then $J_1 = J_2$.*

Proof. In this proof we use a somewhat different notation for the expression for T_J. Put

$$\Psi(i,j) := [p\langle \frac{p^i a_{j+1}}{\ell} \rangle] + \cdots + [p\langle \frac{p^i a_r}{\ell} \rangle].$$

Given i, m, J, let $d_{i,m}(J)$ be the unique integer $1 \leq j \leq r$ such that

$$\Psi(i,j) < p j_i(m) - j_{i+1}(m) \leq \Psi(i-1,j) = \Psi(i,j) + [p\langle \frac{p^i a_j}{\ell} \rangle],$$

and define $D_{i,m}(J)$ as

$$D_{i,m}(J) = -p j_i(m) + j_{i+1}(m) + \Psi(i-1,j), \quad \text{where } j = d_{i,m}(J).$$

In other words, we want to compare the monomials T_J for different J. For $j < d_{i,m}(J)$ the powers of the x_j in T_J are $[p\langle p^i a_j/\ell\rangle]$. For $j = d_{i,m}(J)$ the power of x_j is $D_{i,m}(J)$. For $j > d_{i,m}(J)$ the powers of the x_j in T_J are zero. Using this notation the expression for T_J given in (12) becomes

$$\begin{aligned} T_J &:= \prod_{i=0}^{f-1}(T^i_{j_i(1)j_{i+1}(1)}\cdots T^i_{j_i(n)j_{i+1}(n)})^{p^{f-1-i}} \quad \text{with} \\ T^i_{j_i(m)j_{i+1}(m)} &= (-1)^N \begin{pmatrix} [p\langle\frac{p^i a_{d_{i,m}(J)}}{\ell}\rangle] \\ D_{i,m}(J) \end{pmatrix} x_1^{[p\langle\frac{p^i a_1}{\ell}\rangle]}\cdots x_{d_{i,m}(J)}^{D_{i,m}(J)}, \end{aligned}$$

with $N = p(\|p^i\| + 1 - j_i(m)) - (\|p^{i+1}\| + 1 - j_{i+1}(m))$.

Claim Suppose $p \geq \ell(r-3)$. Then $d_{i,m+1}(J) < d_{i,m}(J)$.

Proof of the Claim. Suppose $p \geq \ell(r-3)$, then $\|p^{i+1}\| \leq r-2 \leq p/\ell + 1$. Since $pj_i(m+1) - j_{i+1}(m+1) > p(j_i(m)+1) - \|p^{i+1}\| > pj_i(m) > pj_i(m) - j_{i+1}(m)$ we have $d_{i,m+1}(J) \leq d_{i,m}(J)$. Suppose $d_{i,m}(J) = d_{i,m+1}(J) = j$, i.e.

$$\begin{aligned} \Psi(i,j) &< pj_i(m) - j_{i+1}(m) \leq \Psi(i,j) + [p\langle\frac{p^i a_j}{\ell}\rangle] \quad \text{and} \\ \Psi(i,j) &< pj_i(m+1) - j_{i+1}(m+1) \leq \Psi(i,j) + [p\langle\frac{p^i a_j}{\ell}\rangle]. \end{aligned}$$

Then

$$pj_i(m+1) - j_{i+1}(m+1) - pj_i(m) + j_{i+1}(m) < [p\langle\frac{p^i a_j}{\ell}\rangle]. \tag{13}$$

We assumed that

$$1 \leq j_x(m) \leq j_x(m+1) - 1 \qquad \text{for } x = i,\ i+1.$$

Hence

$$p(j_i(m+1) - j_i(m)) - j_{i+1}(m+1) + j_{i+1}(m) \geq p - j_{i+1}(m+1) + 1. \tag{14}$$

Equations (13) and (14) imply that $[p\langle p^i a_j/\ell\rangle] \geq p - j_{i+1}(m+1) + 1$. Hence

$$\begin{aligned} j_{i+1}(m+1) &\geq p + 1 - [p\langle\frac{p^i a_j}{\ell}\rangle] = p + 1 - p\langle\frac{p^i a_j}{\ell}\rangle + \langle\frac{p^{i+1} a_j}{\ell}\rangle \geq p + 1 - p\left(\frac{\ell-1}{\ell}\right) + \frac{1}{\ell} \\ &= p + 1 - p + \frac{p+1}{\ell} = 1 + \frac{p+1}{\ell} > 1 + \frac{p}{\ell} \geq \|p^{i+1}\|. \end{aligned}$$

This is impossible since $j_{i+1}(m+1) \leq \|p^{i+1}\|$. Hence $d_{i,m+1}(J) < d_{i,m}(J)$. This proves the claim.

Let J_1 and J_2 be as in the statement of the lemma. We will write $x_1^{n_1}\cdots x_r^{n_r} \sim_\alpha x_1^{k_1}\cdots x_r^{k_r}$ if $k_\beta = n_\beta$ for all $\beta \leq \alpha$. Write $J_1 = \{j_i(m)\}$ and $J_2 = \{k_i(m)\}$.

Claim The following two statements are equivalent:

- $J_1 \sim_\alpha J_2$,
- for each m and $\beta \leq \alpha$ the sets $\{i \mid d_{i,m}(J_1) = \beta\}$ and $\{i \mid d_{i,m}(J_2) = \beta\}$ are equal. Furthermore, for each i, m with $d_{i,m}(J_1) = \alpha$ we have that $pj_i(m) - j_{i+1}(m) = pk_i(m) - k_{i+1}(m)$.

Proof of the Claim. The second statement trivially implies the first statement. Suppose that $J_1 \sim_\alpha J_2$ and suppose that the claim is proved for all $\beta < \alpha$. For $\alpha = 1$ this is an empty assumption. If $d_{i,m}(J_1) < \alpha$ then $d_{i,m}(J_2) < \alpha$ by assumption. Since $d_{i,m+1} < d_{i,m}$, there is an m_0 such that

$$\begin{aligned} &d_{i,\beta}(J_1) < \alpha \qquad \text{for all } \beta > m_0, \\ &d_{i,m_0}(J_1) \geq \alpha. \end{aligned}$$

If $d_{i,\beta} < \alpha$ for all $\beta \in \{1, \dots, n\}$, put $m_0 = 0$. Write

$$T_{J_x} = (\text{constant}) x_1^{n_1(J_x)} \cdots x_r^{n_r(J_x)} \qquad \text{for } x = 1,\ 2.$$

The assumption that $J_1 \sim_\alpha J_2$ implies that $n_\beta(J_1) = n_\beta(J_2)$ for $\beta \leq \alpha$.

Consider $\sum_{i=0}^{f-1} p^{f-1-i} \eta_{i,\alpha}$ with

$$\eta_{i,\alpha} = \begin{cases} 0 & \text{if } d_{i,m_0}(J_1) > \alpha \quad \text{and} \quad d_{i,m_0}(J_2) > \alpha, \\ D_{i,m_0}(J_1) - [p\langle \frac{p^i a_j}{\ell} \rangle] & \text{if } d_{i,m_0}(J_1) = \alpha \quad \text{and} \quad d_{i,m_0}(J_2) > \alpha, \\ [p\langle \frac{p^i a_j}{\ell} \rangle] - D_{i,m_0}(J_2) & \text{if } d_{i,m_0}(J_1) > \alpha \quad \text{and} \quad d_{i,m_0}(J_2) = \alpha, \\ D_{i,m_0}(J_1) - D_{i,m_0}(J_2) & \text{if } d_{i,m_0}(J_1) = d_{i,m_0}(J_2) = \alpha. \end{cases}$$

This sum is equal to $n_\alpha(J_1) - n_\alpha(J_2)$. Note that $-p < -[p\langle \frac{p^i a_\alpha}{\ell} \rangle] \leq \eta_{i,\alpha} \leq [p\langle \frac{p^i a_\alpha}{\ell} \rangle] < p$. Let i_0 be the smallest i such that $\eta_{i,j\alpha} \neq 0$, then

$$\begin{aligned} &\eta_{i_0,\alpha} < 0 \Longrightarrow n_\alpha(J_1) > n_\alpha(J_2) \quad \text{and} \\ &\eta_{i_0,\alpha} > 0 \Longrightarrow n_\alpha(J_1) < n_\alpha(J_2). \end{aligned}$$

This is seen by noting that if $\eta_{i_0,\alpha} \geq 1$ then $n_\alpha(J_1) - n_\alpha(J_2) \geq p^{f-1-i_0} - \sum_{i=i_0+1}^{f-1} p^{f-1-i}(p-1) = p^{f-1-i_0} - p^{f-1-i_0} + p^{f-2-i_0} \cdots + p - p + 1 = 1$. For the other inequality, interchange J_1 and J_2. Our assumptions imply that $n_\alpha(J_1) = n_\alpha(J_2)$. In particular, $\eta_{i,\alpha} = 0$ for all i. Looking at the explicit statement for $\eta_{i,\alpha}$ yields that one of the following holds

- $d_{i,m_0}(J_1) > \alpha \quad \text{and} \quad d_{i,m_0}(J_2) > \alpha$ or,
- $d_{i,m_0}(J_1) = d_{i,m_0}(J_2) = i \quad \text{and} \quad D_{i,m}(J_1) = D_{i,m}(J_2)$.

This last condition implies

$$pj_i(m) - j_{i+1}(m) = pk_i(m) - k_{i+1}(m).$$

This proves the claim.

For each J and each i, m there exists an $\alpha \leq r$ with $d_{i,m}(J) = \alpha$, since $d_{i,m} > r$ is equivalent to $0 = \Psi(i, r) > pj_i(m) - j_{i+1}(m) \geq p - \|p^{i+1}\| \geq p - r + 2 > 0$, which is impossible. Hence the claim implies that if $J_1 \sim_r J_2$ then for each i, m we have

$$pj_i(m) - j_{i+1}(m) = pk_i(m) - k_{i+1}(m).$$

Furthermore, we have $1 \leq j_0(1) < \cdots < j_0(n) \leq \|p^0\| = n$, hence $j_0(m) = m$. The same holds for the $k_0(m)$. This shows that $j_i(m) = k_i(m)$ for all i, m we conclude $J_1 = J_2$. This finishes the proof of the lemma. □

Proof of the theorem. Consider the set of all $J \in \mathcal{J}$ for which T_J is maximal. Lemma 6.5 implies that this set consists of one element, i.e. there is a unique $J' \in \mathcal{J}$ such that $T_{J'}$ is maximal among the T_J's. Therefore, in the expression for $\det(B)$ given in Lemma 6.2, the term $T_{J'}$ does not cancel. Furthermore, $\deg(T'_J) \neq 0$. This implies that $\det(B)$ is a polynomial in $x_1, \dots, x_r$ of positive degree. □

It is not clear to me if the condition p large in the Main Theorem is really necessary. I do not know of any counterexample for small p. In the case that $\|i\| = 1$ the proof can be simplified considerably, and we can improve on the condition on p.

Proposition 6.6 *Fix a type* $\mathbf{a} = (\ell; a_1, \ldots, a_r)$*. Suppose* $p \geq r - 2$*. Suppose furthermore that* $\|i\| = 1$ *and* $\|ip^j\| \geq 1$ *for all* j*. Then there exist* $x_1, \ldots, x_r$ *such that* $\gamma_i = 1$*.*

Proof. We will use the same notation as before. It is no restriction to suppose that $i = 1$. We have $\mathcal{J} = \{(i, j_i) | 0 \leq i < f \quad, 1 \leq j_i \leq \|p^i\|\}$. To prove the lemma, we have to show that the matrix of $F^f : L_1 \to L_1$ is invertible, for some choice of the branch points $x_1, \ldots, x_r$. By assumption L_1 is one dimensional. The matrix is given by

$$\sum_{J \in \mathcal{J}} \prod_{i=0}^{f-1} b_{i,J}^{p^{f-1-i}},$$

with

$$b_{i,J} = (-1)^N \sum_{n_1 + \cdots + n_r = N} \binom{[p\langle \frac{p^i a_1}{\ell} \rangle]}{n_1} \cdots \binom{[p\langle \frac{p^i a_r}{\ell} \rangle]}{n_r} x_1^{n_1} \cdots x_r^{n_r}.$$

Here $N = p(\|p^i\| + 1 - j_i) - (\|p^{i+1}\| + 1 - j_{i+1})$. As before, the $b_{i,J}$ are not identically zero as polynomial in the x_i. The proof that for $J_1 \neq J_2$ the largest of b_{i,J_1} does not cancel against the largest monomial of b_{i,J_2} is obvious in this case. We do not need the assumption $p \geq \ell(r-3)$, which was needed in the general case. $\square$

Corollary 6.7 *Let* $Y \to \mathbb{P}^1$ *be a cover of type* $\mathbf{a}$ *branched at three points. Then*

$$\sigma(Y) = B(\mathbf{a}, 0).$$

Proof. This follows immediately from the above proposition, since Lemma 4.5 implies that the dimension of the eigenspaces are at most one in this case. $\square$

This result can also be deduced from the results of [23] by using the formula for the zeta function of Y, where $Y \to \mathbb{P}^1$ is an ℓ-cyclic cover unbranched outside $0, 1, \infty$, [5, Section 1]. Actually one can calculate not only the p-rank of Y, but also the isogeny type of the p-divisible group of the Jacobian of Y.

7 Degeneration

A way to get information on the p-rank of a cover is to degenerate the cover, and deduce information on the original cover from the, hopefully easier, degenerate cover. In the case of Galois covers of degree prime to p, this method works very well, as one knows exactly which covers one gets by degenerating it, namely the so called admissible covers. In this section and the next, we use this idea to strengthen the results from the previous section, under certain extra hypotheses. Unfortunately, this method does not work in general. Under specialization, the p-ranks drops. It is possible to find examples were all degenerations of a given cover $Y_K \to X_K$ have p-rank strictly less than the p-rank that one want to show the original cover has, namely $B(\theta, g)$.

The following notations will be fixed throughout this section and the next. Suppose $k = \bar{k}$ and the characteristic of k is $p > 0$. Let $A := k[[t]]$ have maximal ideal m_A and field of fractions K. Put $S := \mathrm{Spec}(A)$. For a scheme $\mathcal{X}$ over S we denote by $\mathcal{X}_{\bar{K}} = X \otimes_A \overline{Q(A)}$ the generic fiber and $\mathcal{X}_s = X \otimes_A k$ the special fiber. A curve $\mathcal{X}/S$ is a flat scheme such that the geometric fibers are projective, connected, reduced and of dimension one. A semistable curve $\mathcal{X}/S$ is a curve over S such that the geometric fibers of $\mathcal{X}$ have at most ordinary double points as singularities. A morphism $\pi : \mathcal{Y} \to \mathcal{X}$ of curves over S is a cover if it is finite and generically étale. Let G be a subgroup of $\mathrm{Aut}(\mathcal{Y}/\mathcal{X})$. The cover π is called G-Galois if $\mathcal{Y}/G \xrightarrow{\sim} \mathcal{X}$ and the order of G is equal to the degree of π.

Definition 7.1 Let $\pi : Y \to X$ be a tame G-Galois cover of semistable curves over k. Then π is called *admissible* if for each singular point τ of Y the following condition is satisfied. Let ϕ be a generator of the decomposition group of τ. Let u_i for $i = 1, 2$ be a uniformizing parameter at τ of the branches of Y meeting at τ. We require $\phi^\star u_1 = \zeta u_1 \pmod{(u_1^2)}$ and $\phi^\star u_2 = \zeta^{-1} u_2 \pmod{(u_2^2)}$, for some root of unity $\zeta \in k$.

Let $\mathcal{X}$ be a semistable curve over S, whose generic fiber $\mathcal{X}_{\bar{K}}$ is smooth. Suppose we are give a G-Galois cover $\pi_K : Y_K \to \mathcal{X}_K$ of smooth curves and suppose $p \not| |G|$. Denote the branch locus of π_K by $x_1, \ldots, x_r$. Let $\mathcal{Y}$ be the normalization of $\mathcal{X}$ in the function field of Y_K. After replacing A be a finite extension of A, we may assume $\mathcal{Y}$ is reduced, by Abhyankar's Lemma. Suppose that $x_1, \ldots, x_r$ specialize to distinct points in the smooth locus of $\mathcal{X}_s$.

Proposition 7.2 *Let $\mathcal{Y} \to \mathcal{X}$ be as above. The cover $\mathcal{Y}_s \to \mathcal{X}_s$ is admissible and unbranched outside $\{x_1(s), \ldots, x_r(s)\} \cup \mathrm{Sing}(\mathcal{X}_s)$.*

Proof. [19, Théorème 3.2]. Note that what is called admissible here is called *kummérien* in that paper. □

In fact, a stronger result is true. In the situation as above, one can show that admissible covers of $\mathcal{X}_s$ can be lifted to covers of $\mathcal{X}$, unbranched outside $x_1, \ldots, x_r$, see [7] or [22]. There is an isomorphism between the prime to p part of the fundamental group of $\mathcal{X}_{\bar{K}}$ and the prime to p part of a suitably defined *admissible fundamental group* of $\mathcal{X}_s$, but we do not need this here.

If $\mathcal{X}/S$ is a curve with semistable fibers then $\sigma(\mathcal{X}_{\bar{K}}) \geq \sigma(\mathcal{X}_s)$, [16, p. 1281]. The analogous statement for generalized Hasse-Witt invariants is also true, as follows from the next proposition.

Proposition 7.3 *Let $\mathcal{X} \to S$ be a semistable curve with $\mathcal{X}_{\bar{K}}$ nonsingular. Let $\pi : \mathcal{Y} \to \mathcal{X}$ be a G-Galois cover of order prime to p. For each irreducible character χ of G we have*

$$\gamma_{\pi_{\bar{K}}}(\chi) \geq \gamma_{\pi_k}(\chi).$$

Proof. Let Y be a semistable curve over k on which acts a group G of prime to p order. Then G acts on $H^1(Y, \mathcal{O}_Y)^F$. Using the identification

$$H^1(Y, \mathcal{O}_Y)^F \simeq H^1_{\text{ét}}(Y, \mathbb{Z}/p) \simeq (\mathbb{Z}/p)^{\sigma(Y)}$$

[10, III.4.12], we can define an action of G on $(\mathbb{Z}/p)^{\sigma(Y)}$. Now let χ be a (k-)irreducible character of G. Then the generalized Hasse–Witt invariant $\gamma(\chi)$ is equal to the product of the dimension of χ and the multiplicity of $\chi^{-1} \oplus (\chi^p)^{-1} \cdots (\chi^{p^f-1})^{-1}$ in $(\mathbb{Z}/p)^{\sigma(Y)} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$.

Let $\pi : \mathcal{Y} \to \mathcal{X}$ be as in the statement of the proposition. There exists a canonical map

$$H^1(\mathcal{Y}_s, \mathbb{Z}/p) \hookrightarrow H^1(\mathcal{Y}_{\bar{K}}, \mathbb{Z}/p),$$

[16, p. 1281]. Since the map is G-equivariant,

$$\gamma_{\pi_k}(\chi) \leq \gamma_{\pi_{\bar{K}}}(\chi).$$

□

Suppose that $p \equiv 1 \pmod{\ell}$. Let $Y \to \mathbb{P}^1$ be an ℓ-cyclic cover. Decompose $H^1(Y, \mathcal{O}_Y) = \oplus_{i=1}^{\ell-1} L_i$ into isotypical spaces. Then $F : L_i \to L_i$. Hence in this case $B(\mathbf{a}, 0) = g(Y)$. Question 3.3 boils down to: for a fixed type $\mathbf{a}$, do there exist $x_1, \ldots, x_r$ such that the cover of $\mathbb{P}^1$ branched at the x_i of type $\mathbf{a}$ is ordinary? This is the case as is shown in the following proposition.

Proposition 7.4 *Let $\ell|(p-1)$. There exists $x_1,\dots,x_r \in \mathbb{P}^1$ such that all ℓ-cyclic covers $\pi\colon Y \to \mathbb{P}^1_k$, unbranched outside $x_1,\dots,x_r$, are ordinary.*

Proof. We use induction on r. For $r=2$ there is nothing to prove since each cover of $\mathbb{P}^1$ branched at 2 points has genus zero. For $r=3$ the result follows from Corollary 6.7.

Suppose the statement holds for all $s<r$. Let $A=k[[t]]$, $S=\operatorname{Spec} A$ and let K be the quotient field of A. Construct a semistable curve $\mathcal{X}\to S$, with semistable special fiber consisting of two curves X_1 and X_2 of genus 0 meeting in one point τ, and generic fiber a nonsingular curve of genus 0. Choose sections $x_1,\dots,x_r\colon S\to\mathcal{X}$, such that x_1,x_2 meet $X_1-\{\tau\}$ and $x_3,\dots,x_r$ meet $X_2-\{\tau\}$. By induction, we can choose the x_i such that for all $m|\ell$, the m-cyclic covers of X_2, unbranched outside $x_3,\dots,x_r,\tau$, are ordinary.

Let $\pi_K: Y_{\bar K}\to\mathcal{X}_{\bar K}$ be an ℓ-cyclic cover, unbranched outside $x_1,\dots,x_r$. This cover will be defined over some finite extension of K, so, after replacing A by a finite extension, we may assume that the cover is defined over K. We now proceed as in the beginning of this section. Let $\mathcal{Y}$ be the normalization of $\mathcal{X}$ in the function field of Y_K. Assume $\mathcal{Y}$ is reduced (replace A by a finite extension, if necessary). Proposition 7.2 implies that $\mathcal{Y}_s\to\mathcal{X}_s$ is an admissible ℓ-cyclic cover which is unbranched outside $x_1(s),\dots,x_r(s)$.

Let Z be an irreducible component of $\mathcal{Y}_s$. Let m be the order of the decomposition group of Z. Then $Z/{<}\phi^{\ell/m}{>}$ is isomorphic to X_i for i equal to 1 or 2 hence $Z\to X_i$ is an m-cyclic cover of X_i and Z is ordinary by assumption. Since all components of $\mathcal{Y}_s$ are ordinary, the curve $\mathcal{Y}_s$ itself is ordinary. It follows that

$$g(\mathcal{Y}_{\bar K})\ge\sigma(\mathcal{Y}_{\bar K})\ge\sigma(\mathcal{Y}_s)=p_a(\mathcal{Y}_s).$$

Because $\mathcal{Y}\to S$ is flat, $p_a(\mathcal{Y}_s)=g(\mathcal{Y}_{\bar K})$ and $\mathcal{Y}_{\bar K}$ is ordinary. □

Lemma 7.5 *Suppose that* **a** *is a type such that $\|-p^i\|=r-2$ for all i. Then there exist $x_1,\dots,x_r\in\mathbb{P}^1$ such that for all covers of type* **a***, unbranched outside the x_i, we have $\gamma_1=r-2$.*

Proof. This lemma follows easily by induction, using an argument similar to the argument used in the previous proposition. □

The situation of the lemma above is very special. Here is a case were it occurs.

Example 7.6 Let $\ell=(p^{r_1}-1)/(p-1)$ and let $\mathbf{a}:=(\ell;1,p,p^2,\dots p^{r-1})$. Let $\pi\colon Y\to\mathbb{P}^1$ be an ℓ-cyclic cover of type **a** branched at $x_1,\dots,x_r$. Then

$$\|p^j\|=\|1\|=\frac{1}{\ell}(1+\dots+p^{r_1-1})-1=0\qquad\text{for all } j.$$

Hence $\|-p^j\|=\|-1\|=r-2$ for all j by Lemma 4.5. From the lemma above it follows that $\gamma_1=r-2$, in case $x_1,\dots,x_r$ are sufficiently general.

Proposition 7.7 *Let $Y_x\to\mathbb{P}^1$ be the cover of type* **a** *branched at $0,1,\infty,x$. Then there exists an $x\in\mathbb{P}^1$ such that*

$$\sigma(Y_x)=B(\mathbf{a},0).$$

Proof. To prove the proposition, it suffices to show that for each $j=1,\dots,\ell-1$ we have $\gamma_{-j}=\min_i\|p^ij\|$. As before we may assume $j=1$ and $\|p^i\|\ge\|1\|$. From Lemma 4.5 we know that $\|p^i\|\le r-2=2$ for all i. Therefore, distinguish three cases:

(i) $\|1\|=0$,

(ii) $\|1\|=1$,

(iii) $\|p^i\|=2$ for all i.

We have to show for a suitable choice of x we have $\gamma_{-1} = 0$ in the first case, $\gamma_{-1} = 1$ in the second case and $\gamma_{-1} = 2$ in the third case.

In Case (i) the action of Frobenius on $\oplus_i L_{p^i}$ is nilpotent, so $\gamma_{-1} = 0$. Case (ii) follows from Corollary 6.6. Case (iii) follows from Lemma 7.5. $\square$

Proposition 7.8 *Suppose $p \equiv -1 \pmod{\ell}$. Let $\mathbf{a} = (\ell; a_1, \ldots, a_r)$ be a type. There exist $x_1, \ldots, x_r$ such that for the ℓ-cyclic cover $Y \to \mathbb{P}^1$ of type $\mathbf{a}$, branched at the x_i, we have $\sigma(Y) = B(\mathbf{a}, 0)$.*

Proof. Let $\pi\colon Y \to \mathbb{P}^1$ be a cover of type $\mathbf{a} = (\ell; a_1, \ldots, a_r)$ with $0 < a_i < \ell \neq 2$. Suppose that $p \equiv -1 \pmod{\ell}$. The coset of $<p>$ in $(\mathbb{Z}/\ell)^\star$ containing i consists of two elements: i and $-i$. We Want to show

$$\gamma_{-i} = \min \|i\|, \|-i\|.$$

We may suppose $i = 1$.

From Lemma 4.5 we know that $\|1\| + \|-1\| = r - 2$. Put $n = \|1\|$. We may suppose $0 \leq n \leq [(r-2)/2]$. If $n = 0$ the matrix of Frobenius on $L_1 \oplus L_{-1}$ is nilpotent and $\gamma_1 = 0$. Suppose that $n > 0$.

We will prove the proposition by induction. For $r = 3, 4$ the statement follows from Corollary 6.7 and Proposition 7.7. Suppose the statement holds for $r' < r$.

Case 1 Suppose $n < (r-2)/2$. For r odd this always holds. Choose $i \neq j$ with $a_i + a_j < \ell$. We can do this since if $a_{2s-1} + a_{2s} \geq \ell$ for each s, then $a_1 + \cdots + a_r \geq [r/2]\ell$. But $a_1 + \cdots + a_r = n\ell < (r-2)\ell/2 < [r/2]\ell$, so we get a contradiction. Put $\mathbf{a}_1 = (a_i, a_j, -a_i - a_j)$ and $\mathbf{a}_2 = (a_i + a_j, a_1, \ldots, \hat{a}_i, \ldots, \hat{a}_j, \ldots)$, i.e. in $\mathbf{a}_2$ we omit a_i and a_j. For a cover $f\colon X \to \mathbb{P}^1$ of type $\mathbf{a}_1$ we find

$$\|1\|_{\mathbf{a}_1} = \frac{a_i + a_j + (\ell - a_i - a_j)}{\ell} - 1 = 0 \quad \text{and} \quad \|-1\|_{\mathbf{a}_1} = 1.$$

For a cover $g\colon Z \to \mathbb{P}^1$ of type $\mathbf{a}_2$ we find

$$\|1\|_{\mathbf{a}_2} = \frac{a_1 + \cdots + a_r}{\ell} - 1 = n \quad \text{and} \quad \|-1\|_{\mathbf{a}_2} = r - 3 - n.$$

Note $k \leq r - n - 3$. By induction $\gamma_1(f) = 0$ and $\gamma_1(g) = n$. As in the proof of the previous proposition, Proposition 7.3 implies $\gamma_1(\pi) \geq \gamma_1(g) = n$. Hence $\gamma_1(\pi) = n$.

Case 2 Suppose $r = 2s$ with $s > 2$ and $n = s - 1$. Then $a_1 + \ldots + a_r = s\ell$.

Claim there exist distinct h, i, j, such that $\ell < a_h + a_i + a_j < 2\ell$. To prove the claim, put $x_i = a_i/\ell - 1/2$. Note $-1/2 < x_i < 1/2$ and $x_1 + \ldots + x_r = 0$. We will see that for any m there exist distinct $i_1, \ldots, i_m \in \{1, \ldots, r\}$ such that $-1/2 < \sum_{j=1}^m x_{i_j} < 1/2$. The claim follows from this by taking $m = 3$.

We use induction. For $m = 1$ it is trivial. Let $m > 1$. Choose $I = \{i_1, \ldots i_{m-1}\}$ such that $-1/2 < S_{m-1} := \sum_{i \in I} x_i < 1/2$. If $S_{m-1} \geq 0$ then $(\sum x_i) - S_{m-1} < 0$, so there is an $j \notin I$ with $x_j < 0$. We can add j to I to fulfill the condition for m. Analogously for $S_{m-1} < 0$. This proves the claim.

Choose h, i, j as in the claim. Put $\mathbf{a}_1 = (a_h, a_i, a_j, -a_h - a_i - a_j)$, and $\mathbf{a}_2 = (a_h + a_i + a_j,$ rest of the $a_t)$. Then $\|1\|_{\mathbf{a}_1} = \|-1\|_{\mathbf{a}_1} = 1$ and $\|1\|_{\mathbf{a}_2} = \|-1\|_{\mathbf{a}_2} = s - 1$. As in the previous case the proposition follows by induction. $\square$

Remark 7.9 In this section, we showed several results of the form: under this condition there exists a position of the branch points such that all covers have maximal p-rank. Recall that by Lemma 4.6 the set U of all branch points with this property is open. So in fact, we could reformulate eg Proposition 7.4 as follows. Suppose $p \equiv 1 \pmod{\ell}$. Then there exists a dense open subset $U \subset (\mathbb{P}^1)^r - \Delta$ such that all ℓ-cyclic covers branched at $(x_1, \ldots, x_r) \in U$ are ordinary. Similar for the other results.

8 Cyclic covers of generic curves

Let X be an ordinary elliptic curve or the generic curve of genus ≥ 2. In this section we will show that we can reduce Question 3.3 on the p-rank of an ℓ-cyclic cover of X to the case of ℓ-cyclic covers of $\mathbb{P}^1$.

Proposition 8.1 *Let X be the generic curve of genus $g \geq 2$ or an ordinary elliptic curve. Let* $\mathbf{a}$ *be a type such that there exists a (not necessarily connected) cover of $\mathbb{P}^1$ of type* $\mathbf{a}$ *with p-rank $B(\mathbf{a}, 0)$. Then there exist $x_1, \dots x_r \in X$ such that each cover of X of type* $\mathbf{a}$*, unbranched outside the x_i, has p-rank $B(\mathbf{a}, g) + g(X)$.*

We need to consider nonconnected covers of $\mathbb{P}^1$ in the statement of the proposition because of the following. Suppose $\gcd(\ell, a_1, \dots, a_r) \neq 1$ and suppose $g(X) \geq 1$. Then there exist connected covers of X of type $\mathbf{a} := (\ell; a_1, \dots, a_r)$, but the covers of $\mathbb{P}^1$ of type $\mathbf{a}$ are nonconnected.

Proof. Let $g \geq 1$ be an integer. Let X be the generic curve of genus g if $g \geq 2$ or an ordinary elliptic curve if $g = 1$ and let k be some algebraically closed field of characteristic p over which X is defined. Put $S = \operatorname{Spec} k[[t]]$ and $K = Q(k[[t]])$. Construct a semistable curve $\mathcal{X} \to S$ as follows. The generic fiber $\mathcal{X}_{\bar{K}}$ is a trivial deformation of X and the special fiber X_s consist of two components X_1 and X_2 meeting in one point τ, where $X_1 \simeq X$ and X_2 is a nonsingular curve of genus zero. A curve like this can be constructed by blowing up the trivial deformation of X over S in one point of the special fiber. Choose distinct sections $x_1, \dots, x_r$ of $S \to \mathcal{X}$ such that the x_i meet the special fiber $\mathcal{X}_s$ in $X_2 - \{\tau\}$. Let $n_2 = \gcd(\ell_1, a_1, \dots, a_r)$ and write $\mathbf{a}' = (\ell_2; a'_1, \dots, a'_r)$, where $a'_i = a_i/n_2$ and $\ell_2 = \ell/n_2$. We assume that the ℓ_2-cyclic cover $Y'_2 \to X_2$ of type $\mathbf{a}'$ with branch locus $x_1(s), \dots, x_r(s)$ has p-rank $B(\mathbf{a}', 0)$. (This is equivalent to the assumption in the statement of the proposition.)

Recall that starting from the cover $Y'_2 \to X_2$ we can form a (nonconnected) $\mathbb{Z}/\ell$-cover by taking the induced cover, i.e. take $n_2 = \ell/\ell_2$ copies of Y'_2 and let $\mathbb{Z}/\ell$ permute the copies suitably. Call the resulting cover $Y_2 \to X_2$; it is of type $\mathbf{a}$. Consider all admissible covers $Y \to \mathcal{X}_s$ whose restriction to X_2 is isomorphic to $Y_2 \to X_2$. (These covers are what one could call "admissible covers of $\mathcal{X}_s$ of type $\mathbf{a}$ with branch locus $x_1(s), \dots, x_r(s)$".) We would like to show that all these covers have p-rank equal to $B(\mathbf{a}, g) + g$. The proposition follows from this, as in the proof of Proposition 7.4.

We will now compute the p-rank of the "admissible covers of $\mathcal{X}_s$ of type $\mathbf{a}$ with branch locus $x_1(s), \dots, x_r(s)$". Let $Y \to \mathcal{X}_s$ be such a cover. Write $Y_1 = Y|_{X_1}$ and let n_1 be the number of connected components of Y_1 and put $\ell_1 = \ell/n_1$. Note $\gcd(n_1, n_2) = 1$ since Y is supposed to be connected. Let Y'_1 be a connected component of Y_1. If $g(X_1) = 1$ then $Y'_1 \to X_1$ is an étale cover of an ordinary elliptic curve and Y'_1 is ordinary. If $g(X_1) \geq 2$ it follows from [11, Section 5.III] that Y'_1 is ordinary.

By assumption, the curve Y'_2 has p-rank

$$\sigma(Y'_2) = \sum_{i \in I'} f'_i \min_j \left(\sum_{n=1}^{r} \langle \frac{ip^j a'_n}{\ell_2} \rangle - 1 \right),$$

where I' is a set of representatives of the cosets of $<p>$ in $\mathbb{Z}/\ell_2 - \{0\}$ and f'_i is the number of elements of the coset containing i. Of course, since all components of Y_2 are isomorphic, the same statement holds for the other components of Y_2. Note that $H^1(Y_2, \mathcal{O}_{Y_2}) = \operatorname{Ind}_{\mathbb{Z}/\ell_2}^{\mathbb{Z}/\ell} H^1(Y'_2, \mathcal{O}_{Y'_2})$ as a $k[\mathbb{Z}/\ell]$-module. This yields

$$\sigma(Y_2) = n_2(\sigma(Y'_2)) = \sum_{i \in I} f_i \min_j \left(\sum_{n=1}^{r} \langle \frac{ip^j a_n}{\ell_2} \rangle - 1 \right) + n_2 - 1,$$

where I is a set of representatives of the cosets of $<p>$ in $\mathbb{Z}/\ell - \{0\}$ and f_i is the number of elements of the coset containing i.

The curve Y contains $1+\ell-n_1-n_2$ loops. Therefore, we find for the p-rank of Y that

$$\begin{aligned}\sigma(Y) &= n_1\cdot g(Y_1')+1+\ell-n_1-n_2+\sigma(Y_2)= \\ &= \ell g+\sum_{i\in I} f_i \min_j \left(\sum_{n=1}^{r}\langle\frac{ip^j a_n}{\ell}\rangle-1\right)=B(\mathbf{a},g)+g.\end{aligned}$$

Recall that $B(\mathbf{a},g)=\sum_{i\in I} f_i\min_j\big(\sum_{n=1}^r\langle ip^ja_n/\ell\rangle-1\big)+(\ell-1)g$. Note that for i divisible by ℓ_2, we have

$$\sum_{n=1}^{r}\langle\frac{ip^j a_n}{\ell}\rangle-1=-1,$$

since all a_n's are divisible by n_2. This finishes the proof of the proposition. □

In fact, the proof applies for every curve X such that all étale cyclic covers $Y\to X$ whose order m divides ℓ, have p-rank $\sigma(X)+(m-1)(g-1)$. In [11] it is proved that this holds for curves in a dense open subset of the moduli space $\mathcal{M}_g$.

Corollary 8.2 *Let X be the generic curve of genus $g\geq 2$ or an ordinary elliptic curve. Let ℓ be an integer prime to p, and suppose one of the following holds:*

- $p>\ell(r-3)$,
- $r\leq 4$,
- $p\equiv\pm1 \pmod{\ell}$.

Then there exists $x_1,\ldots,x_r\in X$ such that all ℓ-cyclic covers $Y\to X$, unbranched outside the x_i of type $\mathbf{a}$ satisfy

$$\sigma(Y)=B(\mathbf{a},g)+g.$$

Irene I. Bouw
Department of mathematics
209 South 33rd street
Philadelphia, PA 19104
bouw@math.upenn.edu

References

[1] C. Chevalley and A. Weil, Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers, *Abh. Math. Sem. Univ. Hamburg* 10, 1934, 358–361.

[2] R.M. Crew, Etale p-covers in characteristic p. *Comp. Math.* 52, 1984, 31–45.

[3] N.D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.* 89, 1987, 561–567.

[4] J. González, Hasse–Witt matrices for the Fermat curves of prime degree. *Tôhoku Math. J.* 49, 1997, 149–163.

[5] B.H. Gross and D.H. Rohrlich, Some results on the Mordell–Weil group of the Jacobian of the Fermat curve. *Invent. Math.* 44, 1978, 201–224.

[6] A. Grothendieck et al., *Revêtements étales et géometrie algébrique* (SGA 1). Lecture Notes in Math. 224, Springer-Verlag, Heidelberg, 1971.

[7] D. Harbater and K.F. Stevenson, Patching and thickening problems. *J. of Alg.* 212, 1999, 272–304.

[8] E. Kani, The Galois-module structure of the space of holomorphic differentials of a curve. *J. reine Angew. Math.* 367, 1986, 187–206.

[9] H. Katsurada, On generalized Hasse–Witt invariants and unramified Galois extensions of an algebraic function field. *J. Math. Soc. Japan* 31, 1979, 101–125.

[10] J.S. Milne, *Étale cohomology*. Princeton University Press, Princeton, 1980.

[11] S. Nakajima, On generalized Hasse–Witt invariants of an algebraic curve. In: *Galois groups and their representations, Nagoya 1981* (ed. Y. Ihara), Advanced Studies in pure Mathematics 2, North-Holland Publishing Company, Amsterdam, 1983, 69–88.

[12] S. Nakajima, Galois module structure of cohomology groups for tamely ramified coverings of algebraic varieties. *J. of Number Theory* 22, 1986, 115–123.

[13] A. Pacheco, Unramified coverings of algebraic curves. *J. of Number Theory* 53, 1995, 211–228.

[14] A. Pacheco, K.F. Stevenson, Galois modules and the algebraic fundamental group of projective curves in positive characteristic. To appear in *Pacific J. of Math.*

[15] F. Oort, Subvarieties of moduli spaces. *Invent. Math.* 24, 1974, 95–119.

[16] M. Raynaud, Mauvaise réduction des courbes et p-rang. *C. R. Acad. Sci. Paris* 319, Série I, 1994, 1279–1282.

[17] M. Raynaud, Revêtements des courbes en caractéristique p et ordinarité, preliminary version.

[18] H.-G. Rück, Class groups and L-series of function fields. *J. of Number Theory* 22, 1986, 177–189.

[19] M. Saïdi, Revêtements modérés et groupe fondamental de graphe de groupes. *Comp. Math.* 107, 1997, 321–340.

[20] J-P. Serre, Sur la topologie des variétés algébriques en caractéristiques p. *Symp. Int. Top. Alg.* Mexico, 1958, 24–53. (=Œvres no. 38.)

[21] J. Stienstra, M. van der Put, B. van der Marel, On p-adic monodromy. *Math. Z.* 208, 1991, 309–325.

[22] S. Wewers, Deformation of tame admissible covers of curves. To appear in *Aspects of Galois theory, Gainsville 1996* (ed. H. Völklein), Cambridge university press.

[23] N. Yui, On the Jacobian variety of the Fermat curve. *J. of Alg.* 65, 1980, 1–35.