On the de-Rham Cohomology of Hyperelliptic Curves

Bernhard Köck and Joseph Tait

Abstract. For any hyperelliptic curve X, we give an explicit basis of the first de-Rham cohomology of X in terms of Čech cohomology. We use this to produce a family of curves in characteristic $p > 2$ for which the Hodge-de-Rham short exact sequence does not split equivariantly; this generalises a result of Hortsch. Further, we use our basis to show that the hyperelliptic involution acts on the first de-Rham cohomology by multiplication by -1, i.e., acts as the identity when $p = 2$.

MSC-class: 14F40, 14G17, 14H37.

Keywords: hyperelliptic curve; de-Rham cohomology; Čech cohmology; Hodge-de-Rham short exact sequence; hyperelliptic involution.

Introduction

Recall that the de-Rham cohomology $H^*_{\mathrm{dR}}(X/k)$ of a smooth projective curve X over an algebraically closed field k is defined as the hypercohomology of the de-Rham complex

$$\mathcal{O}_X \xrightarrow{d} \Omega_X$$

where d denotes the usual differential map $f \mapsto df$. In particular, we have a long exact sequence relating $H^*_{\mathrm{dR}}(X/k)$ to ordinary cohomology of the structure sheaf $\mathcal{O}_X$ and of the sheaf Ω_X of differentials on X. The very general and famous fact that the Hodge-de-Rham spectral sequence degenerates at E_1 (e.g., see [Wed08]) means for our curve X that the following main part of that long sequence is a short exact sequence, see Propositon 2.1:

$$0 \to H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X/k) \to H^1(X, \mathcal{O}_X) \to 0.$$

We call this sequence the Hodge-de-Rham short exact sequence. In particular, the vector space $H^1_{\mathrm{dR}}(X/k)$ is the direct sum of the vector spaces $H^0(X, \Omega_X)$ and $H^1(X, \mathcal{O}_X)$ over k.

We now assume furthermore that a finite group G acts on our curve X. If $p := \mathrm{char}(k)$ does not divide the order of G, Maschke's Theorem implies that the Hodge-de-Rham short exact sequence also splits as a sequence of modules over the group ring $k[G]$.

However, the latter fact fails to be true in general when $p > 0$ does divide $\mathrm{ord}(G)$. A counterexample has been constructed in the recent paper [Hor12] by Hortsch. The main goal of this paper is to generalise that counterexample. More precisely, we will prove the following theorem, see Theorem 3.3 and Example 3.4.

Theorem. *Let $p \geq 3$ and let $q(z) \in k[z]$ be a monic polynomial of odd degree without repeated roots. Let X denote the hyperelliptic curve over k defined by the equation $y^2 = q(x^p - x)$ and let G denote the subgroup of $\mathrm{Aut}(X)$ generated by the automorphism τ given by $(x, y) \mapsto (x + 1, y)$. Then the Hodge-de-Rham short exact sequence does not split as a sequence of $k[G]$-modules.*

We remark that the hyperelliptic curves considered in this theorem are exactly those hyperelliptic curves $y^2 = f(x)$ which allow an automorphism that maps x to $x + 1$ and for which $f(x)$ is of odd degree, see Example 3.4 and Proposition 3.6.

When $q(z) = z$, the theorem above becomes the main theorem of [Hor12]. Beyond [Hor12], our theorem shows (see Remark 3.5) that, for every algebraically closed field k of characteristic $p \geq 3$, there exist infinitely many $g \geq 2$ and hyperelliptic curves X over k of genus g for which the Hodge-de-Rham short exact sequence does not split equivariantly. It also shows that, for every $g \geq 2$, there exists a prime $p \geq 3$ and hyperelliptic curves in characteristic p of genus g for which the Hodge-de-Rham short exact sequence does not split equivariantly.

In Example 3.8 and Remark 3.9 we show, using the modular curve $X_0(22)$ for $p = 3$, that, without assuming the degree of $q(x)$ to be odd, this theorem may be false.

To prove our main theorem, we follow the same broad strategy as in [Hor12]: we give an explicit basis of $H^1_{\mathrm{dR}}(X/k)$ in terms of Čech cohomology (in fact for an arbitrary hyperelliptic curve X), see Theorem 2.2, and study the action of τ on that basis. The actual computations towards the end however do not generalise those in [Hor12], see Remark 2.5 and Remark 3.7.

We provide a basis of $H^1_{\mathrm{dR}}(X/k)$ for any hyperelliptic curve X also when $p = 2$ and use this to show that the hyperelliptic involution acts trivially on $H^1_{\mathrm{dR}}(X/k)$ when $p = 2$. In fact, the hyperelliptic involution acts on $H^1_{\mathrm{dR}}(X/k)$

by multiplication by -1 for all p, see Theorem 3.1.

If $p = 2$, Elkin and Pries construct a subtler basis of $H^1_{\mathrm{dR}}(X/k)$ in [EP13] which is suitable to study the action of Frobenius and Verschiebung and, finally, to determine the Ekedahl-Oort type.

Acknowledgements. The authors would like to thank the referees for carefully reading the paper and for their elaborate and helpful comments.

1 Preliminaries

In this section, we introduce assumptions and notations used throughout this paper and collect and prove some auxiliary results.

We assume that k is an algebraically closed field of characteristic $p \geq 0$ and that X is a hyperelliptic curve over k of genus $g \geq 2$. We recall that a curve (always assumed to be smooth, projective and irreducible in this paper) is hyperelliptic if there exists a finite, separable morphism of degree two from the curve to $\mathbb{P}^1_k$. We fix such a map

$$\pi\colon X \to \mathbb{P}^1_k,$$

which is unique up to automorphisms of X and of $\mathbb{P}^1_k$ (see [Liu02, Remark 7.4.30]). Let $K(X)/K(\mathbb{P}^1_k) = k(x)$ denote the extension of function fields corresponding to π. According to [Liu02, Proposition 7.4.24 and Remark 7.4.25], we may and will furthermore assume the following concrete description of $K(X)$.

If $p \neq 2$, then $K(X) = k(x, y)$ where y satisfies

$$y^2 = f(x) \tag{1}$$

for some monic polynomial $f(x) \in k[x]$ which has no repeated roots; moreover, $f(x)$ is of degree $2g+1$ if $\infty \in \mathbb{P}^1_k$ is a branch point of π and of degree $2g+2$ otherwise. The branch points of π are then the roots of $f(x)$, together with $\infty \in \mathbb{P}^1_k$ if $\deg(f(x)) = 2g+1$.

If $p = 2$, then $K(X) = k(x, y)$ where y satisfies

$$y^2 - h(x)y = f(x) \tag{2}$$

for some polynomials $h(x), f(x) \in k[x]$ such that $h'(x)^2 f(x) + f'(x)^2$ and $h(x)$ have no common roots in k; moreover, we have $d := \deg(h(x)) \leq g+1$, with equality if and only if ∞ is not a branch point of π. The branch points of π are the roots of $h(x)$, together with $\infty \in \mathbb{P}^1_k$ if $d < g+1$.

The following estimate for the order of y above ∞ is true for both $p \neq 2$ and $p = 2$.

Lemma 1.1. *Let $P \in \pi^{-1}(\infty)$. Then we have:*

$$\mathrm{ord}_P(y) \geq \begin{cases} -(g+1) & \text{if } \pi \text{ is unramified at } P \\ -2(g+1) & \text{if } \pi \text{ is ramified at } P. \end{cases}$$

Proof. This is [KT15, Inequality (5.2)]. □

Lemma 1.2. *If $p \neq 2$, let $\omega := \frac{dx}{y}$ and, if $p = 2$, let $\omega := \frac{dx}{h(x)}$. Then the differentials $\omega, x\omega, \ldots, x^{g-1}\omega$ form a basis of the k-vector space $H^0(X, \Omega_X)$ of global holomorphic differentials on X.*

Proof. This is [Liu02, Proposition 7.4.26]. □

Remark 1.3. A different basis of $H^0(X, \Omega_X)$ is given in [Ma78, Lemma 5]. The action of the Cartier operator on $H^0(X, \Omega_X)$ is studied in [Sub75] and [Yui78].

Lemma 1.4. *Let $p = 2$ and let $P \in \pi^{-1}(\infty)$. Then we have:*

$$\mathrm{ord}_P(dx) = \begin{cases} -2 & \text{if } \pi \text{ is unramified at } P \\ 2(g-1-d) & \text{if } \pi \text{ is ramified at } P. \end{cases} \tag{3}$$

Proof. By the Riemann-Hurwitz formula [Sti93, Theorem 3.4.6] we have

$$\mathrm{ord}_P(dx) = e_P \cdot \mathrm{ord}_\infty(dx) + \delta_P$$

where e_P denotes the ramification index of π at P and δ_P denotes the order of the ramification divisor of π at P. It is easy to see that $\mathrm{ord}_\infty(dx) = -2$. Therefore $\mathrm{ord}_P(dx) = -2$ if π is unramified at P. On the other hand, if π is ramified at P, we have $\delta_P = 2(g+1-d)$ by [KT15, Equation (5.3)] and hence

$$\mathrm{ord}_P(dx) = 2 \cdot (-2) + 2(g+1-d) = 2(g-1-d),$$

as claimed. □

We define $U_a = X\backslash\pi^{-1}(a)$ for any $a \in \mathbb{P}^1_k$ and let $\mathcal{U}$ be the affine cover of X formed by U_0 and U_∞. Given any sheaf $\mathcal{F}$ on X we have the Čech differential $\check{d}\colon \mathcal{F}(U_0)\times\mathcal{F}(U_\infty) \to \mathcal{F}(U_0\cap U_\infty)$, defined by $(f_0, f_\infty) \mapsto f_0|_{U_0\cap U_\infty} - f_\infty|_{U_0\cap U_\infty}$. In general we will suppress the notation denoting the restriction map. The first cohomology group $\frac{\mathcal{O}_X(U_0\cap U_\infty)}{\mathrm{Im}(\check{d})}$ of the cochain complex

$$0 \to \mathcal{O}_X(U_0) \times \mathcal{O}_X(U_\infty) \xrightarrow{\check{d}} \mathcal{O}_X(U_0 \cap U_\infty) \to 0.$$

is the first Čech cohomology group $\check{H}^1(\mathcal{U}, \mathcal{O}_X)$. By Leray's theorem [Liu02, Theorem 5.2.12] and Serre's affineness criterion [Liu02, Theorem 5.2.23] we therefore have

$$H^1(X, \mathcal{O}_X) \cong \frac{\mathcal{O}_X(U_0 \cap U_\infty)}{\{f_0 - f_\infty \mid f_0 \in \mathcal{O}_X(U_0),\ f_\infty \in \mathcal{O}_X(U_\infty)\}}. \tag{4}$$

When describing elements of $H^1(X, \mathcal{O}_X)$ using this isomorphisms we will denote the residue class of $f \in \mathcal{O}_X(U_0 \cap U_\infty)$ by $[f]$.

Proposition 1.5. *The elements $\frac{y}{x}, \ldots, \frac{y}{x^g} \in K(X)$ are regular on $U_0 \cap U_\infty$, and their residue classes $\left[\frac{y}{x}\right], \ldots, \left[\frac{y}{x^g}\right]$ form a basis of $H^1(X, \mathcal{O}_X)$.*

Proof. By [Liu02, Proposition 7.4.24(b)], we may identify $\mathcal{O}_X(U_\infty)$ with the k-algebra $k[x, y]$ defined by the relation given in (1) or (2). Then $\mathcal{O}_X(U_0\cap U_\infty)$ is $k[x^{\pm 1}, y]$. As the relations in (1) and (2) are quadratic in y, the elements $\ldots, \frac{1}{x^2}, \frac{1}{x}, 1, x, x^2, \ldots$ and $\ldots, \frac{y}{x^2}, \frac{y}{x}, y, xy, x^2y, \ldots$ form a k-basis of $k[x^{\pm 1}, y]$. The elements $1, x, x^2, \ldots$ and $y, xy, x^2y, \ldots$ obviously form a basis of the image of $\mathcal{O}_X(U_\infty)$ in $\mathcal{O}_X(U_0 \cap U_\infty)$. By [Liu02, Proposition 7.4.24(b)], the image of $\mathcal{O}_X(U_0)$ in $\mathcal{O}_X(U_0\cap U_\infty)$ consists of elements of the form $g\left(\frac{1}{x}, \frac{y}{x^{g+1}}\right)$ where $g \in k[s, t]$. Hence, the elements $\ldots, \frac{1}{x^2}, \frac{1}{x}, 1$ and $\ldots \frac{y}{x^{g+3}}, \frac{y}{x^{g+2}}, \frac{y}{x^{g+1}}$ form a basis of that image. We conclude that the residue classes $\left[\frac{y}{x}\right], \ldots, \left[\frac{y}{x^g}\right]$ form a basis of $H^1(X, \mathcal{O}_X)$, as was to be shown. $\square$

Remark 1.6. Let $\omega_j := \frac{x^{j-1}}{y}dx$ when $p \neq 2$ and let $\omega_j = \frac{x^{j-1}}{h(x)}dx$ when $p = 2$. Then, by Lemma 1.2, the elements ω_j, $j = 1, \ldots, g$, form a k-basis of $H^0(X, \Omega_X)$. Let $\langle\ ,\ \rangle : H^0(X, \Omega_X) \times H^1(X, \mathcal{O}_X) \to k$ denote the Serre duality pairing. Then $\langle\omega_j, \left[\frac{y}{x^i}\right]\rangle$ vanishes if $j \neq i$ and is non-zero if $j = i$, see the proof of [Tai14, Theorem 4.2.1]. In other words, up to multiplication by scalars, the basis $\left[\frac{y}{x^i}\right]$, $i = 1, \ldots, g$, of $H^1(X, \mathcal{O}_X)$, given in Proposition 1.5, is dual to the basis ω_j, $j = 1, \ldots, g$, with respect to Serre duality.

Remark 1.7. Different bases of $H^1(X, \mathcal{O}_X)$ are described in [Sul75, Lemma 6] and [Ma78, Lemma 6]. The action of Frobenius on $H^1(X, \mathcal{O}_X)$ is studied in [Bo01].

2 Bases of $H^1_{\mathbf{dR}}(X/k)$

The object of this section is to give an explicit k-basis for the first de-Rham cohomology group $H^1_{\mathrm{dR}}(X/k)$ using Čech cohomology. If $p \neq 2$, we will moreover refine our result when another open subset is added to our standard open cover of X.

The algebraic de-Rham cohomology of X is defined to be the hypercohomology of the de-Rham complex

$$0 \to \mathcal{O}_X \xrightarrow{d} \Omega_X \to 0 \tag{5}$$

where d denotes the usual differential map $f \mapsto df$. We use the cover $\mathcal{U}$ and the Čech differentials defined in the previous section to obtain the Čech bicomplex of (5):

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{O}_X(U_0) \times \mathcal{O}_X(U_\infty) \arrow[r] \arrow[d] & \Omega_X(U_0) \times \Omega_X(U_\infty) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{O}_X(U_0 \cap U_\infty) \arrow[r] \arrow[d] & \Omega_X(U_0 \cap U_\infty) \arrow[r] \arrow[d] & 0 \\
& 0 & 0 &
\end{tikzcd} \tag{6}$$

By a generalisation of Leray's theorem [Gro61, Corollaire 12.4.7] and Serre's affineness criterion [Liu02, Theorem 5.2.23], the first de-Rham cohomology of X is isomorphic to the first cohomology of the total complex of (6). Thus, $H^1_{\mathrm{dR}}(X/k)$ is isomorphic to the quotient of the space

$$\begin{aligned}\big\{(\omega_0, \omega_\infty, f_{0\infty}) \in \Omega_X(U_0) \times \Omega_X(U_\infty) \times \mathcal{O}_X(U_0 \cap U_\infty) \mid \\ df_{0\infty} = \omega_0|_{U_0\cap U_\infty} - \omega_\infty|_{U_0\cap U_\infty}\big\}\end{aligned} \tag{7}$$

by the subspace

$$\{(df_0, df_\infty, f_0|_{U_0\cap U_\infty} - f_\infty|_{U_0\cap U_\infty}) | f_0 \in \mathcal{O}_X(U_0), f_\infty \in \mathcal{O}_X(U_\infty)\}\,. \tag{8}$$

Via this representation of $H^1_{\mathrm{dR}}(X/k)$ and the isomorphism (4) we obtain the canonical maps

$$i\colon H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X/k), \qquad \omega \mapsto [(\omega|_{U_0}, \omega|_{U_\infty}, 0)] \tag{9}$$

and

$$p\colon H^1_{\mathrm{dR}}(X/k) \to H^1(X,\mathcal{O}_X), \qquad [(\omega_0,\omega_\infty,f_{0\infty})] \mapsto [f_{0\infty}]. \tag{10}$$

The following proposition is equivalent to the more familiar and fancier sounding statement that the Hodge-de-Rham spectral sequence for X degenerates at E_1 (see [Wed08]). This is in fact true for every smooth, proper curve X over k, see example (2) in section (1.5) of [Wed08].

Proposition 2.1. *The following sequence is exact:*

$$0 \to H^0(X,\Omega_X) \xrightarrow{i} H^1_{\mathrm{dR}}(X/k) \xrightarrow{p} H^1(X,\mathcal{O}_X) \to 0. \tag{11}$$

We will call the sequence (11) the *Hodge-de-Rham short exact sequence.*

An elementary proof of Proposition 2.1 (that works for every smooth projective curve) can be found in [Tai14, Proposition 4.1.2]; the main ingredient there is just the fact that the residue of differentials of the form df vanishes at every point of X and that hence the obvious composition $H^1(X,\mathcal{O}_X) \to H^1(X,\Omega_X) \xrightarrow{\sim} k$ is the zero map. For a hyperelliptic curve X, the surjectivity of p will also be verified in the proof of Theorem 2.2 below.

In order to state a basis of $H^1_{\mathrm{dR}}(X/k)$, we now define certain polynomials. To this end, we introduce the notations $f^{\leq m}(x) := a_0 + \ldots + a_m x^m$ and $f^{>m}(x) := a_{m+1}x^{m+1} + \ldots + a_n x^n$ for any polynomial $f(x) := a_0 + \ldots + a_n x^n \in k[x]$ and any $m \geq 0$. Let $1 \leq i \leq g$.

When $p \neq 2$ we define

$$s_i(x) := xf'(x) - 2if(x) \in k[x]$$

and put $\psi_i(x) := s_i^{\leq i}(x)$ and $\phi_i(x) := s_i^{>i}(x)$ so that $s_i(x) = \psi_i(x) + \phi_i(x)$.

When $p = 2$ we define

$$s_i(x,y) := xf'(x) + (xh'(x) + ih(x))y \in k[x] \oplus k[x]y \subseteq k(x,y)$$

(where $k[x] \oplus k[x]y$ denotes the $k[x]$-module generated by 1 and y) and put $\psi_i(x,y) := s_i^{\leq i}(x,y)$ and $\phi_i(x,y) := s_i^{>i}(x,y)$ where now the operations $\leq i$ and $> i$ are applied to both the coefficients $xf'(x)$ and $xh'(x) + ih(x)$. Again we have $s_i(x,y) = \psi_i(x,y) + \phi_i(x,y)$.

We now give a basis of $H^1_{\mathrm{dR}}(X/k)$ in terms of the polynomials just introduced and using the presentation of $H^1_{\mathrm{dR}}(X/k)$ developed above.

Theorem 2.2. *If $p \neq 2$, the residue classes*

$$\gamma_i := \left[\left(\frac{\psi_i(x)}{2x^{i+1}y}dx, \frac{-\phi_i(x)}{2x^{i+1}y}dx, \frac{y}{x^i}\right)\right], \quad i = 1, \ldots, g, \tag{12}$$

along with the residue classes

$$\lambda_i := \left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right], \quad i = 0, \ldots, g-1, \tag{13}$$

form a k-basis of $H^1_{\mathrm{dR}}(X/k)$.

On the other hand, if $p = 2$, the residue classes

$$\gamma_i := \left[\left(\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx, \frac{\phi_i(x,y)}{x^{i+1}h(x)}dx, \frac{y}{x^i}\right)\right], \quad i = 1, \ldots, g, \tag{14}$$

together with the residue classes

$$\lambda_i := \left[\left(\frac{x^i}{h(x)}dx, \frac{x^i}{h(x)}dx, 0\right)\right], \quad i = 0, \ldots, g-1, \tag{15}$$

form a k-basis of $H^1_{\mathrm{dR}}(X/k)$.

Remark 2.3.
(a) If $p \neq 2$ and $f(x) = x^p - x$, an easy calculation shows that the basis elements given above are the same as those given in Theorem 3.1 of [Hor12].
(b) If $p = 2$, another basis of $H^1_{\mathrm{dR}}(X/k)$ is given in [EP13, Section 4].

Proof. The elements in (13) and (15) are the images under the map i of the differentials $\frac{x^i}{y}dx$, $i = 0, \ldots, g-1$, and $\frac{x^i}{h(x)}dx$, $i = 0, \ldots, g-1$, respectively, which form a basis of $H^0(X, \Omega_X)$ by Lemma 1.2. Furthermore, provided the elements in (12) and (14) are well-defined elements of $H^1_{\mathrm{dR}}(X/k)$, these elements are mapped to the elements $[\frac{y}{x^i}]$, $i = 1, \ldots, g$, under p, which form a basis of $H^1(X, \mathcal{O}_X)$ by Proposition 1.5. By Proposition 2.1, it therefore suffices to check that the elements in (12) and (14) are well-defined elements of $H^1_{\mathrm{dR}}(X/k)$.

We first check the equality in (7). When $p \neq 2$, this is verified as follows:

$$\begin{aligned}
\left(\frac{\psi_i(x)}{2x^{i+1}y} - \frac{-\phi_i(x)}{2x^{i+1}y}\right) dx &= \frac{s_i(x)}{2x^{i+1}y}dx \\
&= \frac{xf'(x) - 2if(x)}{2x^{i+1}y}dx = \frac{x^i}{2y}\left(\frac{f'(x)}{x^{2i}} - \frac{2if(x)}{x^{2i+1}}\right) dx \\
&= \frac{x^i}{2y}d\left(\frac{f(x)}{x^{2i}}\right) = \frac{x^i}{2y}d\left(\left(\frac{y}{x^i}\right)^2\right) = d\left(\frac{y}{x^i}\right).
\end{aligned}$$

When $p = 2$, we obtain

$$h'(x)ydx + h(x)dy = f'(x)dx$$

by differentiating equation (2) and then verify the equality in (7) as follows (note that we replace all minus signs with plus signs):

$$\begin{aligned}\left(\frac{\psi_i(x,y)}{x^{i+1}h(x)} + \frac{\phi_i(x,y)}{x^{i+1}h(x)}\right)dx &= \frac{s_i(x,y)}{x^{i+1}h(x)}dx \\ &= \left(\frac{f'(x)}{x^i h(x)} + \frac{h'(x)y}{x^i h(x)} + \frac{iy}{x^{i+1}}\right)dx \\ &= \frac{dy}{x^i} + \frac{iy}{x^{i+1}}dx = d\left(\frac{y}{x^i}\right).\end{aligned}$$

It remains to prove that the first two entries of the triples in (12) and (14) are regular differentials on U_0 and U_∞, respectively.

We first consider the case $p \neq 2$. As $\frac{dx}{y}$ is a regular differential on $X = U_0 \cup U_\infty$ by Lemma 1.2, it suffices to observe that each of the functions $\frac{\psi_i(x)}{x^{i+1}}$, $i = 1, \ldots, g$, is regular on U_0 (in fact has a zero at ∞) and that each of the functions $\frac{\phi_i(x)}{x^{i+1}}$, $i = 1, \ldots, g$, is regular on U_∞.

We now turn to the case $p = 2$. As above, we know from Lemma 1.2 that $\frac{dx}{h(x)}$ is regular on $X = U_0 \cup U_\infty$. Furthermore, for every $i \in \{1, \ldots, g\}$, the function $\frac{\phi_i(x,y)}{x^{i+1}}$ is regular on U_∞ since y is regular on U_∞ and since, by definition of $\phi_i(x,y)$, the $k[x]$-coefficients of 1 and y in $\phi_i(x,y)$ are divisible by x^{i+1}. Hence $\frac{\phi_i(x,y)}{x^{i+1}h(x)}dx$ is regular on U_∞, as was to be shown. It remains to show that $\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx$ is regular on U_0. As $\frac{\psi_i(x,y)}{x^{i+1}}$ and $\frac{dx}{h(x)}$ are regular on $U_0 \cap U_\infty$, this amounts to showing that $\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx$ is regular above ∞.

We first consider the case when ∞ is not a branch point of π. By Lemma 1.4, the differential dx has a pole of order 2 at each of the two points P_∞, $P'_\infty \in X$ above ∞. Furthermore, the $k[x]$-coefficient of 1 in $\psi_i(x,y)$ has a pole at P_∞ and P'_∞ of order at most i and the $k[x]$-coefficient of y has a pole at P_∞ and P'_∞ of order at most $i-1$ since the coefficient of x^i in $xh'(x) + ih(x)$ is zero (remember $\mathrm{char}(k) = 2$). Moreover, y has a pole at P_∞ and P'_∞ of order at most $g+1$ by Lemma 1.1. Finally, $\frac{1}{h(x)}$ has a zero at P_∞

and P'_∞ of order $d = \deg(h(x)) = g + 1$. Putting all this together we obtain

$$\begin{aligned}
&\mathrm{ord}_P\left(\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx\right)\\
&\quad = \mathrm{ord}_P\left(\psi_i(x,y)\right) + \mathrm{ord}_P\left(\frac{1}{x^{i+1}}\right) + \mathrm{ord}_P\left(\frac{1}{h(x)}\right) + \mathrm{ord}_P(dx)\\
&\quad \geq \min\{-i, -(i-1)-(g+1)\} + (i+1) + (g+1) - 2 = 0
\end{aligned}$$

for $P \in \{P_\infty, P'_\infty\}$, which shows that $\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx$ is regular at P_∞ and P'_∞.

We finally assume that ∞ is a branch point of π and prove that $\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx$ is regular at the unique point $P_\infty \in X$ above ∞. By Lemma 1.4, the order of the differential dx at P_∞ is $2(g-1-d)$ where $d = \deg(h(x))$. For similar reasons as above, the $k[x]$-coefficients of 1 and y in $\psi_i(x,y)$ have a pole at P_∞ of order at most $2i$ and $2(i-1)$, respectively, and $\frac{1}{h(x)}$ has a zero at P_∞ of order $2d$. Finally, y has a pole at P_∞ of order at most $2(g+1)$ by Lemma 1.1. Putting all this together we obtain

$$\begin{aligned}
&\mathrm{ord}_{P_\infty}\left(\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx\right)\\
&\quad = \mathrm{ord}_{P_\infty}\left(\psi_i(x,y)\right) + \mathrm{ord}_{P_\infty}\left(\frac{1}{x^{i+1}}\right) + \mathrm{ord}_{P_\infty}\left(\frac{1}{h(x)}\right) + \mathrm{ord}_{P_\infty}(dx)\\
&\quad \geq \min\{-2i, -2(i-1)-2(g+1)\} + 2(i+1) + 2d + 2(g-1-d) = 0,
\end{aligned}$$

which shows that $\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx$ is regular at P_∞. □

In the proofs in the next section, we will need a refined description of the basis elements given in (12) when another open subset is added to our standard cover $\mathcal{U} = \{U_0, U_\infty\}$. To this end, we now fix $a \in \mathbb{P}^1_k \backslash \{0, \infty\}$ and define the covers $\mathcal{U}' := \{U_a, U_\infty\}$ and $\mathcal{U}'' := \{U_0, U_a, U_\infty\}$ of X. Similarly to (7) and (8), the first de-Rham cohmology group $H^1_{\mathrm{dR}}(X/k)$ is then isomorphic to the k-vector space

$$\begin{aligned}
(16)\quad &\{(\omega_0, \omega_a, \omega_\infty, f_{0a}, f_{0\infty}, f_{a\infty}) \in\\
&\Omega_X(U_0)\times\Omega_X(U_a)\times\Omega_X(U_\infty)\times\mathcal{O}_X(U_0\cap U_a)\times\mathcal{O}_X(U_0\cap U_\infty)\times\mathcal{O}_X(U_a\cap U_\infty) \mid\\
&f_{0a} - f_{0\infty} + f_{a\infty} = 0,\ df_{0a} = \omega_0 - \omega_a,\ df_{0\infty} = \omega_0 - \omega_\infty,\ df_{a\infty} = \omega_a - \omega_\infty\}
\end{aligned}$$

quotiented by the subspace

$$(17)\quad \{(df_0, df_a, df_\infty, f_0 - f_a, f_0 - f_\infty, f_a - f_\infty) \mid \\ f_0 \in \mathcal{O}_X(U_0), f_a \in \mathcal{O}_X(U_a), f_\infty \in \mathcal{O}_X(U_\infty)\}\,.$$

We use the notations $\check{H}^1_{\mathrm{dR}}(\mathcal{U})$ and $\check{H}^1_{\mathrm{dR}}(\mathcal{U}'')$ for the representations of $H^1_{\mathrm{dR}}(X/k)$ introduced in (7), (8) and (16), (17), respectively. The canonical isomorphism $\rho\colon \check{H}^1_{\mathrm{dR}}(\mathcal{U}'') \to \check{H}^1_{\mathrm{dR}}(\mathcal{U})$, is then induced by the projection

$$(18)\qquad \rho\colon (\omega_0, \omega_a, \omega_\infty, f_{0a}, f_{0\infty}, f_{a\infty}) \mapsto (\omega_0, \omega_\infty, f_{0\infty}).$$

When $p \neq 2$, the next proposition explicitly describes the pre-image of the basis elements $\gamma_i = \left[\left(\frac{\psi_i(x)}{2x^{i+1}y}dx, \frac{-\phi_i(x)}{2x^{i+1}y}dx, \frac{y}{x^i}\right)\right]$, $i = 1, \ldots, g$, of $H^1_{\mathrm{dR}}(X/k)$ under ρ. To this end, we define the polynomials

$$g(x) := (x-a)^g, \quad r_i(x) := g^{\leq i-1}(x) \quad \text{and} \quad t_i(x) := g^{>i-1}(x)$$

in $k[x]$ for $1 \leq i \leq g$ so that $r_i(x) + t_i(x) = (x-a)^g$.

Proposition 2.4. *Let $p \neq 2$. For $i \in \{1, \ldots, g\}$, let*

$$\omega_{0i} := \frac{\psi_i(x)}{2x^{i+1}y}dx, \quad \omega_{\infty i} := \frac{-\phi_i(x)}{2x^{i+1}y}dx,$$

$$\omega_{ai} := \frac{(\psi_i(x)t_i(x) - \phi_i(x)r_i(x))(x-a) - 2if(x)(-1)^{g-i}\binom{g}{i}a^{g-i+1}x^i}{2x^{i+1}(x-a)^{g+1}y}dx$$

and

$$f_{0ai} := \frac{r_i(x)y}{x^i(x-a)^g}, \quad f_{0\infty i} := \frac{y}{x^i}, \quad f_{a\infty i} := \frac{t_i(x)y}{x^i(x-a)^g}.$$

Then we have:

$$(19)\qquad \rho^{-1}(\gamma_i) = [(\omega_{0i}, \omega_{ai}, \omega_{\infty i}, f_{0ai}, f_{0\infty i}, f_{a\infty i})].$$

Remark 2.5. This description of $\rho^{-1}(\gamma_i)$ does not generalise the description given in Lemma 3.3 of [Hor12] in case of the hyperelliptic curve $y^2 = x^p - x$. In fact, the proof of that lemma seems to contain various mistakes.

Proof. We fix $i \in \{1, \dots, g\}$. We obviously only need to show that the sextuple on the right-hand side of (19) is a well-defined element of the space (16).

From the proof of Theorem 2.2 we already know that $d(f_{0\infty i}) = \omega_{0i} - \omega_{\infty i}$ and that $f_{0\infty i}, \omega_{0i}$ and $\omega_{\infty i}$ are regular on the appropriate open sets.

Since $r_i(x) + t_i(x) = (x-a)^g$, we have

$$f_{0ai} - f_{0\infty i} + f_{a\infty i} = \frac{r_i(x)y}{x^i(x-a)^g} - \frac{y}{x^i} + \frac{t_i(x)y}{x^i(x-a)^g} = 0,$$

as desired.

The function f_{0ai} is obviously regular above $\mathbb{P}^1_k \backslash \{0, a, \infty\}$. We furthermore observe that $\mathrm{ord}_\infty \left(\frac{r_i(x)}{x^i(x-a)^g} \right) \geq -(i-1) + i + g = g+1$ and that, by Lemma 1.1, the order of y above ∞ is at least $-2(g+1)$ or at least $-(g+1)$ depending on whether ∞ is a branch point of π or not. Thus, f_{0ai} is regular above ∞ and hence on $U_0 \cap U_a$.

As above, the function $f_{a\infty i}$ is regular above $\mathbb{P}^1_k \backslash \{0, a, \infty\}$. Furthermore, the functions $\frac{t_i(x)}{x^i}$, y and $\frac{1}{(x-a)^g}$ are obviously regular above 0. Therefore, $f_{a\infty i}$ is regular above 0 as well and hence on $U_a \cap U_\infty$.

We next show that $df_{0ai} = \omega_{0i} - \omega_{ai}$. Using the product rule and the chain rule we obtain

$$\begin{aligned}
df_{0ai} &= d\left(\frac{r_i(x)y}{x^i(x-a)^g} \right) \\
&= \frac{r_i(x)}{x^i(x-a)^g} dy + d\left(\frac{r_i(x)}{x^i(x-a)^g} \right) y \\
&= \frac{f'(x)r_i(x)}{2x^i(x-a)^g y} dx + \left(\frac{r_i'(x)}{x^i(x-a)^g} - \frac{ir_i(x)}{x^{i+1}(x-a)^g} - \frac{gr_i(x)}{x^i(x-a)^{g+1}} \right) y dx \\
&= \frac{xf'(x)r_i(x)(x-a) + 2f(x)\left(xr_i'(x)(x-a) - ir_i(x)(x-a) - gxr_i(x)\right)}{2x^{i+1}(x-a)^{g+1}y} dx.
\end{aligned}$$

We now recall that

$$xf'(x) - 2if(x) = \psi_i(x) + \phi_i(x).$$

We furthermore recall that $r_i(x) = g^{\leq i-1}(x)$ where $g(x) = (x-a)^g$. Therefore

$$\begin{aligned} &r_i'(x) \cdot (x-a) - g \cdot r_i(x) \\ &\quad = [g'(x)]^{\leq i-2} \cdot (x-a) - g \cdot g^{\leq i-1}(x) \\ &\quad = \left([g'(x) \cdot (x-a)]^{\leq i-1} + a \cdot b_{i-1} \cdot x^{i-1}\right) - g \cdot g^{\leq i-1}(x) \\ &\quad = a \cdot b_{i-1} \cdot x^{i-1} \end{aligned}$$

where $b_{i-1} = (-1)^{g-i} i \binom{g}{i} a^{g-i}$ denotes the coefficient of x^{i-1} in $g'(x)$.

Thus we obtain

$$\begin{aligned} df_{0ai} &= \frac{(\psi_i(x) + \phi_i(x)) r_i(x)(x-a) + 2f(x)(ab_{i-1}x^i)}{2x^{i+1}(x-a)^{g+1}y} dx \\ &= \frac{\psi_i(x)\left((x-a)^{g+1} - t_i(x)(x-a)\right) + \phi_i(x) r_i(x)(x-a) + 2f(x)(ab_{i-1})x^i}{2x^{i+1}(x-a)^{g+1}y} dx \\ &= \frac{\psi_i(x)}{2x^{i+1}y} dx - \frac{(\psi_i(x) t_i(x) - \phi_i(x) r_i(x))(x-a) - 2f(x)(ab_{i-1})x^i}{2x^{i+1}(x-a)^{g+1}y} dx \\ &= \omega_{0i} - \omega_{ai}, \end{aligned}$$

as claimed.

From the above we moreover obtain that

$$df_{a\infty i} = df_{0\infty i} - df_{0ai} = (\omega_{0i} - \omega_{\infty i}) - (\omega_{0i} - \omega_{ai}) = \omega_{ai} - \omega_{\infty i}.$$

Finally, ω_{ai} is regular on U_a because $\omega_{ai} = \omega_{0i} - df_{0ai}$ and ω_{ai} is hence regular on $U_0 \cap U_a$ and because $\omega_{ai} = \omega_{\infty i} + df_{a\infty i}$ and ω_{ai} is hence regular on $U_a \cap U_\infty$. □

3 Actions on $H^1_{\mathrm{dR}}(X/k)$

In this section we study the action of certain automorphisms on $H^1_{\mathrm{dR}}(X/k)$. We first prove that the hyperelliptic involution acts by multiplication by -1 on $H^1_{\mathrm{dR}}(X/k)$ when $p \neq 2$ and as the identity when $p = 2$. We then give a family of hyperelliptic curves for which the Hodge-de-Rham short exact sequence (11) does not split equivariantly.

Theorem 3.1. *The hyperelliptic involution acts on $H^1_{\mathrm{dR}}(X/k)$ by multiplication by -1.*

Proof. Recall that the hyperelliptic involution is the unique non-trivial automorphism σ of X such that $\pi \circ \sigma = \pi$.

If $p \neq 2$, the involution σ acts on $K(X)$ by $(x,y) \mapsto (x,-y)$. Hence, σ maps each entry of the triples in (12) and (13) to its negative. Thus, the $p \neq 2$ part of Theorem 2.2 implies Theorem 3.1.

If $p = 2$, the involution σ acts on $K(X)$ by $(x,y) \mapsto (x, y + h(x))$. In particular, it fixes the basis elements (15) of $H^1_{\mathrm{dR}}(X/k)$. According to the $p = 2$ part of Theorem 2.2, it remains to show that σ also fixes the residue classes $[(\omega_{0i}, \omega_{\infty i}, f_{0\infty i})]$, $i = 1, \ldots, g$, in (14). For $i \in \{1, \ldots, g\}$, this follows from the description of $H^1_{\mathrm{dR}}(X/k)$ given in (7) and (8) and from the equation

$$\begin{aligned} &\sigma((\omega_{0i}, \omega_{\infty i}, f_{0\infty i})) - (\omega_{0i}, \omega_{\infty i}, f_{0\infty i}) \\ &\qquad\qquad = \left(d\left(\frac{h^{\leq i}(x)}{x^i}\right), d\left(\frac{h^{>i}(x)}{x^i}\right), \frac{h^{\leq i}(x)}{x^i} - \frac{h^{>i}(x)}{x^i} \right) \end{aligned}$$

which in turn is verified in the following three lines (where we replace all minus signs with plus signs):

$$\sigma\left(\frac{\psi_i(x,y)}{x^{i+1}h(x)}dx\right) + \frac{\psi_i(x,y)}{x^{i+1}h(x)}dx = \frac{[xh'(x) + ih(x)]^{\leq i} h(x)}{x^{i+1}h(x)}dx = d\left(\frac{h^{\leq i}(x)}{x^i}\right)$$

$$\sigma\left(\frac{\phi_i(x,y)}{x^{i+1}h(x)}dx\right) + \frac{\phi_i(x,y)}{x^{i+1}h(x)}dx = \frac{[xh'(x) + ih(x)]^{>i} h(x)}{x^{i+1}h(x)}dx = d\left(\frac{h^{>i}(x)}{x^i}\right)$$

$$\sigma\left(\frac{y}{x^i}\right) + \frac{y}{x^i} = \frac{h(x)}{x^i}.$$

□

Remark 3.2. If $p \neq 2$, Theorem 3.1 can also be proved as follows. By Lemma 1.2, the involution σ acts by multiplication by -1 on $H^0(X, \Omega_X)$. By Serre duality, it then acts by multiplication by -1 also on $H^1(X, \mathcal{O}_X)$. Finally, by Maschke's Theorem (for the cyclic group of order 2) applied to the Hodge-de-Rham short exact sequence (11), it acts by multiplication by -1 also on $H^1_{\mathrm{dR}}(X/k)$.

Before we state the main result of this paper, we recall that any automorphism τ of X induces a map $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ since $\mathbb{P}^1_k$ is the quotient of X by the hyperelliptic involution and since the hyperelliptic involution σ belongs to the centre of $\mathrm{Aut}(X)$ (see [Liu02, Corollary 7.4.31]). The following commutative diagram visualises this situation:

$$\begin{tikzcd} X \arrow[r, "\tau"] \arrow[d, "\pi"] & X \arrow[d, "\pi"] \\ \mathbb{P}^1_k \arrow[r, "\bar{\tau}"] & \mathbb{P}^1_k \end{tikzcd}$$

Theorem 3.3. *Let $p \geq 3$. We assume that the degree of the polynomial $f(x)$ defining the hyperelliptic curve X is odd. We furthermore assume that there exists $\tau \in \mathrm{Aut}(X)$ such that the induced map $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ is given by $x \mapsto x + a$ for some $a \neq 0$. Let G denote the subgroup of $\mathrm{Aut}(X)$ generated by τ. Then the Hodge-de-Rham short exact sequence (11) does not split as a sequence of $k[G]$-modules.*

The following example explicitly describes hyperelliptic curves that allow an automorphism τ as assumed in the previous theorem.

Example 3.4. Let $p \geq 3$, let $a \in k^\times$ and let $q(z) \in k[z]$ be any monic polynomial without repeated roots. Then $f(x) := q(x^p - a^{p-1}x) \in k[x]$ obviously has no repeated roots either and thus $y^2 = f(x)$ defines a hyperelliptic curve X. Moreover, $(x, y) \mapsto (x + a, y)$ defines an automorphism τ of X and the induced automorphism $\bar{\tau}$ is given by $x \mapsto x + a$.

Remark 3.5.
(a) When applied to $a = 1$ and to the hyperelliptic curve X given by $q(z) = z$ in Example 3.4, Theorem 3.3 becomes the main theorem of [Hor12].
(b) Theorem 3.3 and Example 3.4 imply that, for every algebraically closed field k of characteristic $p \geq 3$, there exist infinitely many $g \geq 2$ and hyperelliptic curves over k of genus g for which the Hodge-de-Rham spectral sequence does not split equivariantly.
(c) Suppose $g \geq 2$ is given. If p is a prime divisor of $2g+1$ then, according to Theorem 3.3 and Example 3.4, every monic polynomial $q(z) \in k[z]$ of degree $(2g + 1)/p$ without repeated roots defines a hyperelliptic curve X of genus g for which the Hodge-de-Rham sequence does not split equivariantly.

The following proposition shows that any hyperelliptic curve satisfying the assumptions of Theorem 3.3 is in fact of the form as given in Example 3.4.

Proposition 3.6. *Let $p \geq 3$ and let $\tau \in \mathrm{Aut}(X)$. If the induced isomorphism $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ is given by $x \mapsto x+a$ for some $a \neq 0$, then the action of τ^* on y is given by $\tau^*(y) = y$ or $\tau^*(y) = -y$ and $f(x)$ is of the form $f(x) = q(x^p - a^{p-1}x)$ for some polynomial $q \in k[z]$ without repeated roots.*

Proof. We first show that $\tau^*(y) = \pm y$. There exist $g_1(x)$ and $g_2(x) \neq 0$ in $k(x)$ such that

$$\tau^*(y) = g_1(x) + g_2(x)y \in k(x, y).$$

Hence

$$f(x+a) = \tau^*(y^2) = (\tau^*(y))^2 = g_1(x)^2 + 2g_1(x)g_2(x)y + g_2(x)^2 f(x). \tag{20}$$

This implies that $g_1(x) = 0$ because otherwise

$$y = \frac{f(x+a) - g_1(x)^2 - g_2(x)^2 f(x)}{2g_2(x)g_1(x)}$$

would belong to $k(x)$. By comparing the degrees in (20) we see that $g_2(x)$ is a constant, and then by comparing coefficients in the same equation we see that $g_2(x)^2 = 1$. Hence $\tau^*(y) = \pm y$, as claimed.

We now show that $f(x)$ is of the form $q(x^p - a^{p-1}x)$. The extension $k(x) = k(z, x)$ of the rational function field $k(z)$ obtained by adjoining an element x satisfying the equation $x^p - a^{p-1}x - z = 0$ is a Galois extension with cyclic Galois group generated by the automorphism $x \mapsto x + a$. We derived above that $f(x) = f(x+a)$. Hence $f(x)$ belongs to $k(z)$. Furthermore, x and hence $f(x)$ is integral over $k[z]$. Therefore, $f(x) \in k(z)$ belongs to $k[z]$, i.e., $f(x) = q(x^p - a^{p-1}x)$ for some $q \in k[z]$ without repeated roots, as was to be shown. □

Proof (of Theorem 3.3). We suppose that the sequence (11) does split and that

$$s\colon H^1(X, \mathcal{O}_X) \to H^1_{\mathrm{dR}}(X/k)$$

is a $k[G]$-linear splitting map. Then we have

$$s(\tau^*(\alpha)) = \tau^*(s(\alpha)) \in H^1_{\mathrm{dR}}(X/k) \tag{21}$$

and

$$p(s(\alpha)) = \alpha \tag{22}$$

for all $\alpha \in H^1(X, \mathcal{O}_X)$. We will show that these equalities give rise to a contradiction when α is the residue class $\left[\frac{y}{x^g}\right]$ in $H^1(X, \mathcal{O}_X)$ (see Proposition 1.5).

We first show that $\left[\frac{y}{x^g}\right] \in H^1(X, \mathcal{O}_X)$ is fixed by τ^*. To this end, we recall that $\mathcal{U} = \{U_0, U_\infty\}$, $\mathcal{U}' = \{U_a, U_\infty\}$ and $\mathcal{U}'' = \{U_0, U_a, U_\infty\}$ and consider the following obviously commutative diagram of isomorphisms where ρ and ρ' are defined as in (18) and the equalities denote the identification (4):

$$\begin{tikzcd}
H^1(X, \mathcal{O}_X) \arrow[r, equal] \arrow[d, "\tau^*"] & \check{H}^1(\mathcal{U}, \mathcal{O}_X) & \check{H}^1(\mathcal{U}'', \mathcal{O}_X) \arrow[l, "\rho"'] \arrow[d, "\rho'"] \\
H^1(X, \mathcal{O}_X) \arrow[r, equal] & \check{H}^1(\mathcal{U}, \mathcal{O}_X) & \check{H}^1(\mathcal{U}', \mathcal{O}_X). \arrow[l, "\tau^*"']
\end{tikzcd}$$

By (the proof of) Proposition 2.4, the triple $\left(\frac{r_g(x)y}{x^g(x-a)^g}, \frac{y}{x^g}, \frac{t_g(x)y}{x^g(x-a)^g}\right)$ defines a well-defined element of $\check{H}^1(\mathcal{U}'', \mathcal{O}_X)$. Hence we have

$$\begin{aligned}
\rho^{-1}\left(\left[\frac{y}{x^g}\right]\right) &= \left[\left(\frac{r_g(x)y}{x^g(x-a)^g}, \frac{y}{x^g}, \frac{t_g(x)y}{x^g(x-a)^g}\right)\right] \\
&= \left[\left(\frac{((x-a)^g - x^g)y}{x^g(x-a)^g}, \frac{y}{x^g}, \frac{y}{(x-a)^g}\right)\right] \text{ in } \check{H}^1(\mathcal{U}'', \mathcal{O}_X).
\end{aligned}$$

We therefore obtain

$$\begin{aligned}
\tau^*\left(\left[\frac{y}{x^g}\right]\right) &= \tau^*\left(\rho'\left(\rho^{-1}\left(\left[\frac{y}{x^g}\right]\right)\right)\right) \\
&= \tau^*\left(\rho'\left(\left[\left(\frac{((x-a)^g - x^g)y}{x^g(x-a)^g}, \frac{y}{x^g}, \frac{y}{(x-a)^g}\right)\right]\right)\right) \\
&= \tau^*\left(\left[\frac{y}{(x-a)^g}\right]\right) = \left[\frac{y}{x^g}\right],
\end{aligned}$$

as claimed.

By Theorem 2.2, the elements λ_i, $i = 0, \ldots, g-1$, defined in (13) together with the elements γ_i, $i = 1, \ldots, g$, defined in (12) form a basis of $H^1_{\mathrm{dR}}(X/k)$. Since the canonical projection $p : H^1_{\mathrm{dR}}(X/k) \to H^1(X, \mathcal{O}_X)$ is $k[G]$-linear and maps γ_g to the residue class $\left[\frac{y}{x^g}\right]$, it follows that

$$\tau^*(\gamma_g) = \gamma_g + \sum_{i=0}^{g-1} c_i \lambda_i \tag{23}$$

for some $c_0, \ldots, c_{g-1} \in k$. On the other hand, we have

$$s\left(\left[\frac{y}{x^g}\right]\right) = \gamma_g + \sum_{i=0}^{g-1} d_i \lambda_i$$

for some $d_0, \dots, d_{g-1} \in k$. Now the action of τ^* on λ_i for $0 \le i \le g-1$ is easily seen to be given by

$$\begin{aligned} \tau^*(\lambda_i) &= \tau^*\left(\left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right]\right) \\ &= \left[\left(\frac{(x+a)^i}{y}dx, \frac{(x+a)^i}{y}dx, 0\right)\right] = \sum_{k=0}^{i}\binom{i}{k}a^{i-k}\lambda_k. \end{aligned} \tag{24}$$

Plugging the equations obtained so far into equation (21) we obtain

$$\begin{aligned} \gamma_g + \sum_{i=0}^{g-1} d_i\lambda_i &= s\left(\left[\frac{y}{x^g}\right]\right) = s\left(\tau^*\left(\left[\frac{y}{x^g}\right]\right)\right) \\ &= \tau^*\left(s\left(\left[\frac{y}{x^g}\right]\right)\right) = \tau^*\left(\gamma_g + \sum_{i=0}^{g-1} d_i\lambda_i\right) \\ &= \left(\gamma_g + \sum_{i=0}^{g-1} c_i\lambda_i\right) + \sum_{i=0}^{g-1} d_i\left(\sum_{k=0}^{i}\binom{i}{k}a^{i-k}\lambda_k\right). \end{aligned}$$

By comparing coefficients of the basis element λ_{g-1}, we see that $c_{g-1} = 0$. On the other hand, we will below derive the equation $c_{g-1} = a/4$ from the defining equation (23). Since we assumed that $a \neq 0$, this gives us the desired contradiction.

The left-hand side of equation (23) is $\tau^*(\gamma_g)$. To compute $\tau^*(\gamma_g)$ we consider the following commutative diagram of isomorphisms where ρ is the canonical projection (18), ρ' is given by $(\omega_0, \omega_a, \omega_\infty, f_{0a}, f_{0\infty}, f_{a\infty}) \mapsto (\omega_a, \omega_\infty, f_{a\infty})$ and the equalities denote the identification given by (7) and (8):

$$\begin{tikzcd} H^1_{\mathrm{dR}}(X/k) \arrow[r, equal] \arrow[d, "\tau^*"] & \check{H}^1_{\mathrm{dR}}(\mathcal{U}) & \check{H}^1_{\mathrm{dR}}(\mathcal{U}'') \arrow[l, "\rho"'] \arrow[d, "\rho'"] \\ H^1_{\mathrm{dR}}(X/k) \arrow[r, equal] & \check{H}^1_{\mathrm{dR}}(\mathcal{U}) & \check{H}^1_{\mathrm{dR}}(\mathcal{U}'). \arrow[l, "\tau^*"'] \end{tikzcd} \tag{25}$$

Then, by Proposition 2.4, we have:

$$\begin{aligned} \tau^*(\gamma_g) &= \tau^*(\rho'(\rho^{-1}(\gamma_g))) \\ &= \tau^*\left(\left[\omega_{ag}, \frac{-\phi_g(x)}{2x^{g+1}y}dx, \frac{y}{(x-a)^g}\right)\right] \\ &= \left[\left(\tau^*(\omega_{ag}), \frac{-\phi_g(x+a)}{2(x+a)^{g+1}y}dx, \frac{y}{x^g}\right)\right]. \end{aligned} \tag{26}$$

On the other hand, the right hand side of equation (23) is equal to

$$\left[\left(\frac{\psi_g(x)}{2x^{g+1}y}dx, \frac{-\phi_g(x)}{2x^{g+1}y}dx, \frac{y}{x^g}\right)\right] + \sum_{i=0}^{g-1} c_i \left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right]. \tag{27}$$

Note that the third entry in both (26) and (27) is $\frac{y}{x^g}$. Now, if the third entry of a triple $(df_0, df_\infty, f_0|_{U_0\cap U_\infty} - f_\infty|_{U_0\cap U_\infty})$ in the subspace (8) of the space (7) vanishes, then f_0 and f_∞ glue to a global and hence constant function and the whole triple vanishes. Hence, the triples in (26) and (27) are equal already before taking residue classes. By comparing the second entries of (26) and (27) we therefore obtain the equation

$$-\frac{\phi_g(x+a)}{2(x+a)^{g+1}y}dx = -\frac{\phi_g(x)}{2x^{g+1}y}dx + \sum_{i=0}^{g-1} c_i \frac{x^i}{y}dx \quad \text{in} \quad \Omega_{K(X)}.$$

Since dx is a basis of $\Omega_{K(X)}$ considered as a $K(X)$-vector space, the equation above is equivalent to the equation

$$\frac{\phi_g(x+a)}{2(x+a)^{g+1}} = \frac{\phi_g(x)}{2x^{g+1}} - \sum_{i=0}^{g-1} c_i x^i$$

(in the rational function field $k(x)$) which in turn is equivalent to the equation

$$\phi_g(x+a)x^{g+1} = \phi_g(x)(x+a)^{g+1} - 2(x+a)^{g+1}x^{g+1}\sum_{i=0}^{g-1} c_i x^i \quad \text{in} \quad k[x].$$

Now, the assumption that the degree of $f(x)$ is odd means that the degree of $f(x)$ is precisely $2g+1$. By definition, the terms of highest degree in $\phi_g(x)$ are the same as the terms of highest degree in

$$s_g(x) = xf'(x) - 2gf(x) = x^{2g+1} + 0\cdot x^{2g} + \dots .$$

We therefore have

$$\begin{aligned}&\left((x+a)^{2g+1} + 0\cdot (x+a)^{2g} + \dots\right) x^{g+1}\\ &\quad = (x^{2g+1} + 0\cdot x^{2g} + \dots)(x+a)^{g+1} - 2(x+a)^{g+1}x^{g+1}(c_{g-1}x^{g-1} + \dots).\end{aligned}$$

Hence, by comparing the coefficients of x^{3g+1}, we obtain

$$(2g+1)a = (g+1)a - 2c_{g-1}.$$

and hence

$$c_{g-1} = \frac{((g+1)-(2g+1))a}{2} = -\frac{g}{2}a.$$

Finally, we have $2g+1 = \deg(f(x)) \equiv 0 \bmod p$ by Proposition 3.6 and hence

$$c_{g-1} = \frac{a}{4},$$

as claimed above. This concludes the proof of Theorem 3.3. $\square$

Remark 3.7. While the method of calculating $\tau^*\left(\left[\frac{y}{x^g}\right]\right)$ and $\tau^*(\gamma_g)$ in the proof above is the same as in [Hor12], the actual computations do not generalise those in [Hor12], not only due to Remark 2.5 but also because of further mistakes in [Hor12]. Finally, the argument in the proof above for obtaining the desired contradiction is different from the one in [Hor12] the very end of which has unfortunately not been carried out anyway.

We conclude with an example which demonstrates that the requirement in Theorem 3.3 of $f(x)$ to be of odd degree is a necessary condition.

Example 3.8. Let $p = 3$ and X be the hyperelliptic curve of genus 2 defined by the equation

$$y^2 = f(x) = x^6 + x^4 + x^2 + 2.$$

As in Theorem 3.3 let τ denote the automorphism of X given by $(x, y) \mapsto (x+1, y)$ and let $G := \langle \tau \rangle$.

By Theorem 2.2, a basis of $\check{H}^1_{\mathrm{dR}}(\mathcal{U})$ is given by

$$\lambda_0 = \left[\left(\frac{1}{y}dx, \frac{1}{y}dx, 0\right)\right], \quad \lambda_1 = \left[\left(\frac{x}{y}dx, \frac{x}{y}dx, 0\right)\right],$$

$$\gamma_1 = \left[\left(\frac{1}{x^2y}dx, \frac{x^4+2x^2}{y}dx, \frac{y}{x}\right)\right], \quad \gamma_2 = \left[\left(\frac{x^2+1}{2x^3y}dx, \frac{2x^3}{y}dx, \frac{y}{x^2}\right)\right].$$

By Proposition 1.5, the residue classes $\bar{\gamma}_1 := \left[\frac{y}{x}\right]$ and $\bar{\gamma}_2 := \left[\frac{y}{x^2}\right]$ form a basis of $H^1(X, \mathcal{O}_X)$. We define a map

$$s\colon H^1(X, \mathcal{O}_X) \to H^1_{\mathrm{dR}}(X/k)$$

of vector spaces over k by

$$\bar{\gamma}_1 \mapsto \gamma_1 \quad \text{and} \quad \bar{\gamma}_2 \mapsto \gamma_2 + \lambda_1.$$

Clearly $p \circ s$ is the identity map on $H^1(X, \mathcal{O}_X)$, and hence, if s is $k[G]$-linear, the sequence in Proposition 2.1 does split as a sequence of $k[G]$-modules.

We now show that s is $k[G]$-linear. By Proposition 2.4, the pre-images of γ_1 and γ_2 under ρ in $\check{H}^1_{\mathrm{dR}}(\mathcal{U}'')$ are the residue classes of

$$\nu_1 = \left(\frac{1}{x^2 y}dx, \frac{x^4+2x^3+2x^2}{2(x-1)^3 y}dx, \frac{x^4+2x^2}{y}dx, \frac{y}{x(x-1)^2}, \frac{y}{x}, \frac{(x+1)y}{(x-1)^2}\right)$$

and

$$\nu_2 = \left(\frac{x^2+1}{2x^3 y}dx, \frac{x^3+x^2+x+1}{2(x-1)^3 y}dx, \frac{2x^3}{y}dx, \frac{(x+1)y}{x^2(x-1)^2}, \frac{y}{x^2}, \frac{y}{(x-1)^2}\right),$$

respectively. Using a computation similar to (26), it is easy to verify that

$$\begin{aligned}
\tau^*(\gamma_1) &= \tau^*(\rho'(\nu_1)) \\
&= \left[\left(\frac{x^4+2x^2+2x+2}{2x^3 y}dx, \frac{x^4+x^3+2x^2+2x}{y}dx, \frac{(x+2)y}{x^2}\right)\right] \\
&= \gamma_1 + 2\gamma_2 + 2\lambda_1
\end{aligned}$$

and that

$$\begin{aligned}
\tau^*(\gamma_2) &= \tau^*(\rho'(\nu_2)) \\
&= \left[\left(\frac{x^3+x^2+1}{2x^3 y}dx, \frac{2x^3+2}{y}dx, \frac{y}{x^2}\right)\right] \\
&= \gamma_2 + 2\lambda_0.
\end{aligned}$$

Furthermore, we have seen in (24) that

$$\tau^*(\lambda_0) = \lambda_0 \quad \text{and} \quad \tau^*(\lambda_1) = \lambda_1 + \lambda_0.$$

We finally conclude that

$$s(\tau^*(\bar{\gamma}_1)) = s(\bar{\gamma}_1 + 2\bar{\gamma}_2) = \gamma_1 + 2\gamma_2 + 2\lambda_1 = \tau^*(\gamma_1) = \tau^*(s(\bar{\gamma}_1))$$

and

$$s(\tau^*(\bar{\gamma}_2)) = s(\bar{\gamma}_2) = \gamma_2 + \lambda_1 = \tau^*(\gamma_2 + \lambda_1) = \tau^*(s(\bar{\gamma}_2)).$$

Hence s is $k[G]$-linear, and the Hodge-de-Rham short exact sequence (11) splits.

Remark 3.9. The curve X defined in the previous example is isomorphic to the modular curve $X_0(22)$.

To see this, we first note that, by [KY10, Table 2], the modular curve $X_0(22)$ is the hyperelliptic curve of genus 2 defined by

$$y^2 = f(x) = x^6 + 2x^4 + x^3 + 2x^2 + 1.$$

Now, $x \mapsto x - 1$, $y \mapsto y$ defines an isomorphism between $X_0(22)$ and the curve defined by $y^2 = x^6 + 2x^4 + 2x^2 + 2$. We finally apply the isomorphism described in the following general procedure.

If $g(x) = a_s x^s + \ldots + a_0$ with $a_0 \neq 0 \neq a_s$, we define $g^*(x) := a_0^{-1} x^s g\left(\frac{1}{x}\right)$. It is stated after Lemma 2.6 in [KY10] that, if $y^2 = g(x)$ defines a hyperelliptic curve and s is even, then the curves defined by $y^2 = g(x)$ and $y^2 = g^*(x)$ are isomorphic.

References

[Bo01] I. I. Bouw, *The p-rank of ramified covers of curves*, Compositio Math. **126** (2001), no. 3, 295-322.

[EP13] A. Elkin and R. Pries, *Ekedahl-Oort strata of hyperelliptic curves in characteristic 2*, Algebra Number Theory **7** (2013), no. 3, 507-532.

[Gro61] A. Grothendieck, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11.

[Hor12] Ruthi Hortsch, *On the canonical representation of curves in positive characteristic*, New York J. Math. **18** (2012), 911–924.

[KT15] B. Köck and J. Tait, *Faithfulness of actions on Riemann-Roch spaces,* Canad. J. Math. **67** (2015), no. 4, 848-869.

[KY10] A. Kontogeorgis and Y. Yang, *Automorphisms of hyperelliptic modular curves $X_0(N)$ in positive characteristic*, LMS J. Comput. Math. **13** (2010), 144-163.

[Liu02] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[Ma78] D. J. Madden, *A*rithmetic in generalized Artin-Schreier extensions of $k(x)$, J. Number Theory **10** (1978), no. 3, 303-323.

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Universitext. Springer-Verlag, Berlin, 1993.

[Sub75] D. Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), no. 2, 169-193.

[Sul75] F. J. Sullivan, *p-torsion in the class group of curves with too many automorphisms*, Arch. Math. (Basel) **26** (1975), 253-261.

[Tai14] J. Tait, *Group actions on differentials of curves and cohomology bases of hyperelliptic curves*, PhD thesis, University of Southampton, 2014.

[Wed08] T. Wedhorn, *De Rham cohomology of varieties over fields of positive characteristic*, Higher-dimensional geometry over finite fields, 269-314, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 16, IOS, Amsterdam, 2008.

[Yui78] N. Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$*, J. Algebra **52** (1978), no. 2, 378-410.