LINEAR SYSTEMS ATTACHED TO CYCLIC INERTIA

MARCO A. GARUTI

Abstract. We construct inductively an equivariant compactification of the algebraic group $\mathbb{W}_n$ of Witt vectors of finite length over a field of characteristic $p > 0$. We obtain smooth projective rational varieties $\overline{\mathbb{W}}_n$, defined over $\mathbf{F}_p$; the boundary is a divisor whose reduced subscheme has normal crossings.

The Artin-Schreier-Witt isogeny $F - 1 : \mathbb{W}_n \to \mathbb{W}_n$ extends to a finite cyclic cover $\Psi_n : \overline{\mathbb{W}}_n \to \overline{\mathbb{W}}_n$ of degree p^n ramified at the boundary. This is used to give an extrinsic description of the local behavior of a separable cover of curves in char. p at a wildly ramified point whose inertia group is cyclic.

In an appendix, we give an elementary computation of the conductor of such a covering, which can otherwise be determined using class field theory.

Let $f : C \to D$ be a finite separable cover of (germs of) curves over a perfect field k of characteristic $p > 0$. Suppose that f is Galois of group G and let $y_0 \in C$ be a ramification point at which the residue field extension $k(y_0)/k(x_0)$ is separable, where $x_0 = f(y_0)$. Recall ([5], chap. IV), that the higher ramification groups G_i (in lower numbering) are defined as

$$G_i = \{g \in G |\, v_{y_0}(g(t) - t) \geq i + 1\}$$

where t is a local parameter at y_0; they do not depend on the choice of t. The inertia group G_0 is an extension of a p-group by a cyclic group of order prime to p and, for $i > 0$, the G_i are p-groups; they are trivial for large values of i. The degree (at y_0) of the different $\mathfrak{D}_{C/D} = Ann\,(\Omega^1_{C/D})$ of the extension C/D can be expressed as

$$\deg \mathfrak{D}_{C/D,y_0} = \sum_{i=0}^{\infty} (|G_i| - 1)$$

Using Herbrand's φ and ψ functions, one can introduce (*loc.cit.*, §3) higher ramification groups in upper numbering $G^{\varphi(r)} = G_r$, indexed over $\mathbf{R}_{\geq 0}$. Hence, if e is the largest integer such that G_e is nontrivial, the real number

$$m = \varphi(e)$$

is the largest for which G^m is nontrivial. When G is abelian, the classical Hasse-Arf theorem (*loc.cit.*) guarantees that this number is in fact an integer. We shall write $m(f)$ and $e(f)$ to emphasize that these integers are related to the cover $f : C \to D$. The conductor (at y_0) of the extension C/D is defined as

$$\mathrm{cond}\,(C/D, y_0) = m(f) + 1.$$

Geometrically, the conductor can be characterized as follows ([3], chap. VI, 2.12 and [4], 3.6): $m + 1 = \deg_{y_0} \mathfrak{m}$, where $\mathfrak{m}$ is the smallest modulus such that the cover

Research at MSRI is supported in part by NSF grant DMS-9701755.

C/D is isomorphic to a pull-back from an isogeny of the generalized jacobian $J_{\mathfrak{m}}$ of D.

We shall be concerned with the situation where G_0 is cyclic of order p^n. By Artin-Schreier-Witt theory, there are étale neighborhoods V of y_0 and U of x_0 and a map $\underline{u}$, from $U' = U - \{x_0\}$ to the group $\mathbb{W}_n$ of Witt vectors of length n, such that $V' = V - \{y_0\}$ is the fibred product

$$\begin{array}{ccc} V' & \longrightarrow & \mathbb{W}_n \\ {\scriptstyle f|_{V'}}\Big\downarrow & & \Big\downarrow{\scriptstyle F-1} \\ U' & \xrightarrow{\underline{u}} & \mathbb{W}_n \end{array}$$

The maps $\underline{u}$ and $\underline{u} + F\underline{w} - \underline{w}$, define isomorphic covers for any Witt-vector valued function $\underline{w}$.

We will make the following assumptions: f itself is cyclic of degree p^n, totally ramified at y_0; furthermore, $U = D$ and $V = C$ and $\underline{u}$ is defined over k. Working locally for the étale topology, this is no great loss of generality.

We are going to show that, for every positive integer n, there is a smooth projective rational variety $\overline{\mathbb{W}}_n$ over the prime field $\mathbf{F}_p$, equipped with a tautological line bundle $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ such that:

1. $\overline{\mathbb{W}}_n$ contains $\mathbb{W}_n$ as an affine open dense subvariety; the boundary $B_n = \overline{\mathbb{W}}_n \backslash \mathbb{W}_n$ is a divisor such that $\mathcal{L}(B_n) = \mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ and $(B_n)_{\text{red}}$ has normal crossings.
2. The isogeny $F - 1$ extends to a separable cyclic cover $\Psi_n : \overline{\mathbb{W}}_n \to \overline{\mathbb{W}}_n$ branched along B_n.

Our main result is then:

Theorem 1. *Let $f : C_n \to D$ be a separable cyclic cover of degree p^n of curves over a perfect field k, totally branched above $x_0 \in D(k)$. Let $\underline{u} = (u_0, \dots, u_{n-1})$ be a Witt vector of rational functions on D, with poles of order ν_i, prime to p, at x_0, such that $k(C_n)/k(D)$ is defined by $F(\underline{Y}) - \underline{Y} = \underline{u}$.*

Then $\underline{u}$ extends to a morphism $\underline{u} : D \to \overline{\mathbb{W}}_n \times k$ such that C_n is isomorphic to the normalization of the fibred product $D \times_{\overline{\mathbb{W}}_n} \overline{\mathbb{W}}_n$ and

$$\operatorname{cond}(C_n/D, y_0) - 1 = \deg \underline{u}^* \mathcal{O}_{\overline{\mathbb{W}}_n}(1) = \max_{0 \le i \le n-1} \{p^{n-i-1}\nu_i\}.$$

This work was completed while visiting the M.S.R.I. (october-december 1999) during the program on *Galois Groups and Fundamental Groups.* I would like to thank the participants for many stimulating conversations and in particular Ahmed Abbes and Mohamed Saïdi for pointing out to me the references [1] and [2] respectively.

We begin with the following

Definition 1. *For every positive integer n, define inductively a variety $\overline{\mathbb{W}}_n$ over the prime field $\mathbf{F}_p$, equipped with a tautological line bundle $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$, by letting*

$$\begin{aligned}\left(\overline{\mathbb{W}}_1, \mathcal{O}_{\overline{\mathbb{W}}_1}(1)\right) &= (\mathbf{P}^1, \mathcal{O}_{\mathbf{P}^1}(1))\\ \left(\overline{\mathbb{W}}_{n+1}, \mathcal{O}_{\overline{\mathbb{W}}_{n+1}}(1)\right) &= \left(\mathbf{P}\left(\mathcal{O}_{\overline{\mathbb{W}}_n} \oplus \mathcal{O}_{\overline{\mathbb{W}}_n}(p)\right), \mathcal{O}_{\mathbf{P}}(1)\right)\end{aligned}$$

(as usual, $\mathbf{P}(\mathcal{E})$ denotes the projective bundle associated to a locally free module $\mathcal{E}$ and $\mathcal{O}_{\mathbf{P}}(1)$ its tautological line bundle cf.[E.G.A. II]*, 4.1.1; for any $m \in \mathbf{Z}$, put $\mathcal{O}(m) = \mathcal{O}(1)^{\otimes m}$).*

By definition, there is a natural projection

$$\mathbf{r} : \overline{\mathbb{W}}_{n+1} \longrightarrow \overline{\mathbb{W}}_n \tag{1}$$

which is a fibration by projective lines; it follows immediately that $\overline{\mathbb{W}}_n$ is a smooth projective rational variety of dimension n. Note that $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ is not ample (for $n \geq 2$); it is only ample relative to $\mathbf{r}$.

On the other hand, $\overline{\mathbb{W}}_{n+1}$ is the projective closure of the vector bundle $\mathbf{V}(\mathcal{O}_{\overline{\mathbb{W}}_n}(p))$ over $\overline{\mathbb{W}}_n$ (cf. [E.G.A. II], 8.4) and there are two canonical sections of $\mathbf{r}$. The zero section, whose divisor we will denote Z_{n+1}, arises from the exact sequence

$$0 \longrightarrow \mathcal{O}_{\overline{\mathbb{W}}_n} \longrightarrow \mathcal{O}_{\overline{\mathbb{W}}_n} \oplus \mathcal{O}_{\overline{\mathbb{W}}_n}(p) \longrightarrow \mathcal{O}_{\overline{\mathbb{W}}_n}(p) \longrightarrow 0$$

which gives a global section of $\mathcal{O}_{\overline{\mathbb{W}}_n} \oplus \mathcal{O}_{\overline{\mathbb{W}}_n}(p) = \mathbf{r}_*\mathcal{O}_{\overline{\mathbb{W}}_{n+1}}(1)$, whence a global section of $\mathcal{O}_{\overline{\mathbb{W}}_{n+1}}(1)$ (the latter restricts to $\mathcal{O}_{\mathbf{P}^1}(1)$ on the fibres of $\mathbf{r}$, so its higher direct images vanish and $H^i(\overline{\mathbb{W}}_n, \mathbf{r}_*\mathcal{O}_{\overline{\mathbb{W}}_{n+1}}(1)) = H^i(\overline{\mathbb{W}}_{n+1}, \mathcal{O}_{\overline{\mathbb{W}}_{n+1}}(1))$ for all i).

The infinity section is obtained by the same construction composed with the isomorphism

$$\mathbf{P}\left(\mathcal{O}_{\overline{\mathbb{W}}_n} \oplus \mathcal{O}_{\overline{\mathbb{W}}_n}(p)\right) \simeq \mathbf{P}\left(\mathcal{O}_{\overline{\mathbb{W}}_n}(-p) \oplus \mathcal{O}_{\overline{\mathbb{W}}_n}\right).$$

We denote Σ_{n+1} the corresponding divisor in $H^0(\overline{\mathbb{W}}_{n+1}, \mathcal{O}_{\overline{\mathbb{W}}_{n+1}}(1) \otimes \mathbf{r}^*\mathcal{O}_{\overline{\mathbb{W}}_n}(-p))$.

As suggested by the notation, $\overline{\mathbb{W}}_n$ is a compactification of the Witt group scheme $\mathbb{W}_n$; more precisely:

Proposition 1. *There is a natural system of open immersions $j_n : \mathbb{W}_n \subset \overline{\mathbb{W}}_n$, compatible w.r.t. the projections $\mathbf{r}$ and such that $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ trivializes over $j_n(\mathbb{W}_n)$.*

The closed subscheme $B_n = \overline{\mathbb{W}}_n \setminus j_n(\mathbb{W}_n)$ is a divisor linearly equivalent to $\Sigma_n + p\,\mathbf{r}^*B_{n-1}$ (and hence to Z_n) and $(B_n)_{\mathrm{red}}$ has normal crossings.

Proof: Indeed, we have a canonical embedding $j_1 : \mathbb{G}_{\mathrm{a}} \cong \mathbf{A}^1 \subset \mathbf{P}^1$; by induction, assume $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ trivializes over the affine open subset $j_n(\mathbb{W}_n) = U_n$: then, by definition (cf.[E.G.A. II], 3.1), $\mathbf{r}^{-1}(U_n) = \mathbf{P}^1_{U_n}$. Clearly, $\mathcal{O}_{\overline{\mathbb{W}}_{n+1}}(1)$ trivializes over the complement U_{n+1} of the infinity section, and, identifying $\mathbf{r}^{-1}(0) \cap U_{n+1}$ with $\mathbf{A}^1$, we can choose an isomorphism $j_{n+1} : \mathbb{W}_{n+1} \cong U_{n+1}$ fitting in the diagram

$$\begin{tikzcd} \mathbf{A}^1 \arrow[r] & U_{n+1} \arrow[r, "\mathbf{r}|_{U_{n+1}}"] & U_n \\ \mathbb{G}_a \arrow[u, "j_1"] \arrow[r, "V^n"] & \mathbb{W}_{n+1} \arrow[u] \arrow[r, "\mathbf{r}"] & \mathbb{W}_n \arrow[u, "j_n"'] \end{tikzcd}$$

where the bottom one is the exact sequence of group schemes defining $\mathbb{W}_{n+1}$.
The second statement follows easily, as $j_{n+1}(\mathbb{W}_{n+1})$ has been defined as the intersection of $\mathbf{r}^{-1}(U_n)$, which is the complement of the vertical divisor $\mathbf{r}^*(pB_n)$, with the complement of the horizontal infinity divisor Σ_{n+1}.

Corollary 1. *For all $1 \leq i \leq n$, let $B_{n,i} = (\mathbf{r}^{n-i})^*(\Sigma_i)$ be the pull back of the infinity divisor on $\overline{\mathbb{W}}_i$ via the iteration of the projection (1). The boundary divisor is then*

$$B_n = \sum_{i=1}^{n} p^{n-i} B_{n,i}$$

From now on, we identify $\mathbb{W}_n$ with its image in $\overline{\mathbb{W}}_n$. Choose a system of variables $Y_0, Y_1, \ldots, Y_n, \ldots$ such that $\mathbb{W}_n = \operatorname{Spec} \mathbf{F}_p[Y_0, \ldots, Y_{n-1}]$ and the projection $\mathbf{r}$ corresponds to the inclusion $\mathbf{F}_p[Y_0, \ldots, Y_{n-1}] \subset \mathbf{F}_p[Y_0, \ldots, Y_n]$. On the ring of polynomials

$$\mathsf{H} = \mathbf{F}_p[T, Y_0, \ldots, Y_n, \ldots]$$

we define a grading by $\deg T = 1$ and $\deg Y_i = p^i$ (recall [AC IX] that with this choice for the degrees, the polynomials defining the sum, product etc. of Witt vectors are isobaric). As usual, we denote by H_d the d-th graded piece, consisting of homogeneous elements of degree d.

Lemma 1. *The tautological line bundle $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ is generated by global sections; there is a canonical isomorphism $H^0(\overline{\mathbb{W}}_n, \mathcal{O}_{\overline{\mathbb{W}}_n}(1)) = \mathsf{H}_{p^{n-1}}$ under which $Z_n = (Y_{n-1})_0$ and $B_n = (T^{p^{n-1}})_0$.*

Proof: The assertions being clear for $n = 1$, the proof is by induction. We need a classical explicit description of the projective bundle $\overline{\mathbb{W}}_{n+1}$.
By inductive assumption, the complete linear series $|pZ_n|$ defines a morphism

$$\phi_{|pZ_n|} : \overline{\mathbb{W}}_n \longrightarrow \mathbf{P}^m = \mathbf{P}H^0(\overline{\mathbb{W}}_n, \mathcal{O}_{\overline{\mathbb{W}}_n}(p)).$$

The vector space decomposition $\mathsf{H}_{p^n} = H^0(\overline{\mathbb{W}}_n, \mathcal{O}_{\overline{\mathbb{W}}_n}(p)) \oplus \langle Y_n \rangle$ induces a rational map

$$\pi : \mathbf{P}^{m+1} = \mathbf{P}\mathsf{H}_{p^n} \dashrightarrow \mathbf{P}^m$$

defined outside $[0 : \cdots : 0 : 1]$. The indeterminacy is solved on the blow-up of this point, $\tilde{\mathbf{P}}^{m+1} = \mathbf{P}(\mathcal{O}_{\mathbf{P}^m} \oplus \mathcal{O}_{\mathbf{P}^m}(1))$, and $\overline{\mathbb{W}}_{n+1}$ is canonically isomorphic to the fibred product:

$$\begin{tikzcd} \overline{\mathbb{W}}_{n+1} \arrow[r] \arrow[d, "\mathbf{r}"'] & \tilde{\mathbf{P}}^{m+1} \arrow[d, "\tilde{\pi}"] \\ \overline{\mathbb{W}}_n \arrow[r, "\phi_{|pZ_n|}"] & \mathbf{P}^m \end{tikzcd}$$

To complete the proof of the lemma it suffices to remark that the composite morphism $\overline{\mathbb{W}}_{n+1} \to \tilde{\mathbf{P}}^{m+1} \to \mathbf{P}^{m+1}$ is given by the complete linear system $|Z_{n+1}|$; its image is the projective cone over $\phi_{|pZ_n|}(\overline{\mathbb{W}}_n)$.

Proposition 2. *The action of $\mathbb{W}_n$ on itself extends to an action of $\mathbb{W}_n$ on $\overline{\mathbb{W}}_n$ and the line bundle $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ is stable under this action.*

In particular, $\mathbf{Z}/p^n\mathbf{Z} = \mathbb{W}_n(\mathbf{F}_p)$ acts on $\overline{\mathbb{W}}_n$ and the the Artin-Schreier-Witt isogeny $(F-1) : \mathbb{W}_n \to \mathbb{W}_n$ extends to a cyclic cover

$$\Psi_n : \overline{\mathbb{W}}_n \longrightarrow \overline{\mathbb{W}}_n$$

of degree p^n, defined over $\mathbf{F}_p$, commuting with the projection $\mathbf{r}$. It is branched along the boundary divisor B_n and the inertia subgroup of the infinity section Σ_n has order p.

The induced map Ψ_n^* on the group of k-cycles modulo rational equivalence is multiplication by p^{n-k}.

Proof: Clearly, $\mathbb{G}_a$ acts on $\mathbf{P}^1$ and the isogeny $\wp : \mathbb{G}_a \to \mathbb{G}_a$ extends to a cyclic cover of degree p of $\mathbf{P}^1$ branched at ∞; we proceed by induction.
The group $\mathbb{W}_{n+1}$ acts on itself by translations; recall (e.g. [AC IX]) that the sum of two Witt vectors $\underline{X}, \underline{Y}$ is expressed by polynomials $S_i(\underline{X};\underline{Y}) \in \mathbf{Z}[X_0, \dots, X_i, Y_0, \dots, Y_i]$ characterized by the relations

$$\Phi_n(S_0, \dots, S_n) = \Phi_n(X_0, \dots, X_n) + \Phi_n(Y_0, \dots, X_n)$$

If the variables X_i and Y_i are given the weight p^i, then S_i is isobaric of weight p^i. Moreover:

$$S_i(\underline{X};\underline{Y}) = X_i + Y_i + c_i(\underline{X};\underline{Y}), \qquad c_i \in \mathbf{Z}[X_0, \dots, X_{i-1}; Y_0, \dots, Y_{i-1}] \tag{2}$$

Therefore, given an $\mathbf{F}_p$-algebra A, for any $\underline{a} \in \mathbb{W}_{n+1}(A)$, the polynomial

$$T^{p^n} S_n(\frac{Y_0}{T}, \dots, \frac{Y_n}{T^{p^n}}; \underline{a}) = Y_n + a_n T^{p^n} + T^{p^n} c_n(\frac{Y_0}{T}, \dots, \frac{Y_{n-1}}{T^{p^{n-1}}}; \underline{a})$$

is a homogeneous element in $\mathsf{H}_{p^n} \otimes A$.
As $\mathcal{O}_{\overline{\mathbb{W}}_n}(1)$ is stable under the action, $\mathbb{W}_n(A)$ acts A-linearly on $H^0(\overline{\mathbb{W}}_{n,A}, \mathcal{O}_{\overline{\mathbb{W}}_n}(p))$: we extend it to an action of $\mathbb{W}_{n+1}(A)$ on $\mathsf{H}_{p^n} \otimes A$ by

$$\underline{a} \cdot Y_n = Y_n + a_n T^{p^n} + T^{p^n} c_n(\frac{Y_0}{T}, \dots, \frac{Y_{n-1}}{T^{p^{n-1}}}; \underline{a}) \tag{3}$$

The point $[0 : \cdots : 0 : 1] \in \mathbf{P}_A^{m+1} = \mathbf{P}\mathsf{H}_{p^n} \otimes A$ is fixed and one easily checks that the action extends on the blow-up $\tilde{\mathbf{P}}^{m+1} \subset \mathbf{P}^{m+1} \times \mathbf{P}^m$; in particular, the inertia subgroup of the exceptional divisor for the action of $\mathbf{Z}/p^{n+1}\mathbf{Z} = \mathbb{W}_{n+1}(\mathbf{F}_p)$ has order p. As $\overline{\mathbb{W}}_{n+1} = \tilde{\mathbf{P}}^{m+1} \times_{\mathbf{P}^m} \overline{\mathbb{W}}_n$, we have the obtained the desired action; moreover, the $\mathbf{Z}/p^{n+1}\mathbf{Z}$-inertia of the infinity section Σ_{n+1} is of order p.

Let $\pi : P \to \overline{\mathbb{W}}_{n+1}$ be the cyclic cover of degree p^n given by the fibred product

$$\begin{array}{ccc} P & \xrightarrow{\pi} & \overline{\mathbb{W}}_{n+1} \\ {\scriptstyle q}\big\downarrow & & \big\downarrow{\scriptstyle \mathbf{r}} \\ \overline{\mathbb{W}}_n & \xrightarrow{\Psi_n} & \overline{\mathbb{W}}_n \end{array}$$

As Ψ_n^* is multiplication by p, we have $P = \mathbf{P}\left(\mathcal{O}_{\overline{\mathbb{W}}_n} \oplus \mathcal{O}_{\overline{\mathbb{W}}_n}(p^2)\right)$. We have a sheaf of graded $\mathcal{O}_{\overline{\mathbb{W}}_n}$-algebras

$$\mathcal{S} = \bigoplus_{d\geq 0} \mathcal{O}_{\overline{\mathbb{W}}_n}(pd)$$

and, with the notations as in [E.G.A. II] §2, $\overline{\mathbb{W}}_{n+1} = \mathrm{Proj}\ \mathcal{S}[Y_n]$ and $P = \mathrm{Proj}\ \mathcal{S}^{(p)}[X_n]$. Define a morphism of graded $\mathcal{O}_{\overline{\mathbb{W}}_n}$-algebras:

$$\varphi^{\#} : \mathcal{S}^{(p)}[X_n] \longrightarrow (\mathcal{S}[Y_n])^{(p)}$$

which is the identity on $\mathcal{S}^{(p)}$ and sends X_n to

$$T^{p^{n+1}} S_n\Big(\frac{Y_0^p}{T^p}, \dots, \frac{Y_n^p}{T^{p^{n+1}}}; -\Big(\frac{Y_0}{T}, \dots, \frac{Y_n}{T^{p^n}}\Big)\Big) = Y_n^p - Y_n T^{p^n(p-1)} + T^{p^{n+1}} c_n\Big(\frac{Y_0^p}{T^p}, \dots; -\frac{Y_0}{T}, \dots\Big).$$

This defines a $\overline{\mathbb{W}}_n$-morphism $\varphi : G(\varphi^{\#}) \to P$ from an open subset of Proj $(\mathcal{S}[Y_n])^{(p)} = \overline{\mathbb{W}}_{n+1}$ (*loc.cit*, prop. 3.1.8). The only homogeneous prime ideal containing $\mathcal{S}^{(p)}$ and Y_n is the irrelevant ideal, hence $G(\varphi^{\#}) = \overline{\mathbb{W}}_{n+1}$. As φ is equivariant under the action of $\mathbf{Z}/p\mathbf{Z}$ given by equation (3) (via the n-th iteration of the Verschiebung), the composite morphism

$$\Psi_{n+1} : \overline{\mathbb{W}}_{n+1} \xrightarrow{\varphi} P \xrightarrow{\pi} \overline{\mathbb{W}}_{n+1}$$

extends the Artin-Schreier-Witt isogeny and is equivariant under the $\mathbf{Z}/p^{n+1}\mathbf{Z}$-action defined above (it suffices to check it over the dense open subset $\mathbb{W}_{n+1}$) and satisfies

$$\Psi_n \circ \mathbf{r} = \mathbf{r} \circ \Psi_{n+1}.$$

To prove the last statement, recall that, via $\mathbf{r}^*$, the cohomology group $A^*(\overline{\mathbb{W}}_{n+1})$ is a free $A^*(\overline{\mathbb{W}}_n)$-module generated by the classes 1 and $\xi = [Z_{n+1}]$. As Ψ commutes with $\mathbf{r}$, it suffices to prove that $\Psi_{n+1}^*\xi = p\,\xi$. Write:

$$\Psi_{n+1}^*\xi = a\xi + \beta \qquad a \in \mathbf{Z},\ \beta \in \mathbf{r}^*A^1(\overline{\mathbb{W}}_n). \tag{4}$$

Intersecting with a fibre of $\mathbf{r}$, we deduce $a = p$. On the other hand, let $\eta = \mathbf{r}^*[Z_n]$; since $c_t(\mathcal{O}_{\overline{\mathbb{W}}_n} \oplus \mathcal{O}_{\overline{\mathbb{W}}_n}(p)) = c_t(\mathcal{O}_{\overline{\mathbb{W}}_n}(p)) = 1 + p\,[Z_n]t$, we have

$$\xi^2 = p\,\xi\eta.$$

As $\Psi_{n+1}^*\eta = p\,\eta$, taking self intersection on both sides of (4) we get:

$$p^2\xi^2 + p^2\beta\eta = p(p\xi + \beta)p\eta = \Psi_{n+1}^*(p\xi\eta) = \Psi_{n+1}^*(\xi^2) = p^2\xi^2 + 2p\xi\beta + \beta^2$$

whence $(2p\beta)\,\xi + (\beta^2 - p^2\beta\eta) = 0$. Since $1, \xi$ form a $A^*(\overline{\mathbb{W}}_n)$-basis, this implies $\beta = 0$.

Corollary 2. *With the notation as in Corollary 1, the inertia subgroup at the i-th component $B_{n,i}$ of the boundary divisor B_n on $\overline{\mathbb{W}}_n$ is cyclic of order p^{n-i}.*

Let now $f_n : C_n \to D$ be a cyclic cover as in Theorem 1 and $\underline{u} : D - \{x_0\} \to \mathbb{W}_n$ the corresponding Witt representative; clearly, $\underline{u}$ extends to

$$\underline{u} : D \longrightarrow \overline{\mathbb{W}}_n.$$

Lemma 2. *With the notation as above,* $\deg \underline{u}^* \mathcal{O}_{\overline{\mathbb{W}}_n}(1) = \max_{0 \le i \le n-1} \{p^{n-i-1} \nu_i\}$.

Proof: It suffices to consider the composite map (cf. lemma 1)

$$D \xrightarrow{\underline{u}} \overline{\mathbb{W}}_n \xrightarrow{\phi_{|Z_n|}} \mathbf{PH}_{p^{n-1}}.$$

In a neighborhood of x_0, it is defined by $[s^M : s^M u_0^{p^{n-1}} : \ldots, s^M u_{n-1}]$, where s is a local parameter at x_0 and

$$\begin{aligned} M &= \max \{ i_0 \nu_0 + \cdots + i_{n-1} \nu_{n-1} | \, 0 \le i_h \le p^{n-1-h} \text{ and } \textstyle\sum_{h=0}^{n-1} p^h i_h = p^{n-1} \} \\ &= \max_{0 \le i \le n-1} \{ p^{n-i-1} \nu_i \}. \end{aligned}$$

Proposition 3. *Let $f_n : C_n \to D$ be as in Theorem 1 and let $M(f_n) = \deg \underline{u}^* \mathcal{O}_{\overline{\mathbb{W}}_n}(1)$. If $m(f_n) + 1$ is the degree of the conductor, then*

$$m(f_n) \le M(f_n).$$

Proof: We show that $\mathfrak{u} = (1 + M(f_n)).\infty$ is a modulus, in the sense of [3], chap. III, for the rational map $\underline{u} : D - \{\infty\} \to \mathbb{W}_n$, with the smallest possible degree. By the universal property of the generalized jacobians, $\underline{u}$ factors through $J_{\mathfrak{u}}$ and, by the minimality of the conductor, $\mathfrak{m} \le \mathfrak{u}$.

We have to show that $(\underline{u}, \alpha)_\infty = \underline{0} \in \mathbb{W}_n(k)$ for any rational function α on D such that $\alpha \equiv 1 \bmod \mathfrak{u}$, where $(\underline{u}, -)_\infty$ denotes the local symbol associated to $\underline{u}$: it is the "Residuenvektor" defined in [6], §2, whose j-th phantom component is

$$\Phi_j \left((\underline{u}, \alpha)_\infty \right) = \operatorname{Res} \left(\Phi_j(u_0, \ldots, u_j) \frac{d\alpha}{\alpha} \right)$$

Let s be a local parameter on D at ∞; if A is any complete discrete valuation ring of characteristic zero with residue field k, we can lift $\alpha \in k[[s]]$ and $u_0, \ldots, u_{n-1} \in k((s))$ to formal power series $\tilde{\alpha} \in A[[s]]$ and $\tilde{u}_0, \ldots, \tilde{u}_{n-1} \in A((s))$, with the $\tilde{u}_i$ having a pole at $s = 0$ of the same order as u_i: by definition, $(\underline{u}, \alpha)$ is the reduction modulo pA of $(\underline{\tilde{u}}, \tilde{\alpha})$.

Recall that u_i has a pole of order ν_i and that $M = \max \{ p^{n-i-1} \nu_i : 0 \le i \le n-1 \}$. It is then clear that M is the smallest integer ρ for which

$$\begin{aligned} \Phi_j \left((\underline{\tilde{u}}, \tilde{\alpha}) \right) &= \operatorname{Res} \left(\Phi_j(\tilde{u}_0, \ldots, \tilde{u}_j) \tfrac{d\tilde{\alpha}}{\tilde{\alpha}} \right) \\ &= \operatorname{Res} \left(\left(\tilde{u}_0^{p^j} + \cdots + p^j \tilde{u}_j \right) \tfrac{d\tilde{\alpha}}{\tilde{\alpha}} \right) \end{aligned}$$

vanishes for any $0 \le j \le n-1$ and for any $\tilde{\alpha}$ such that $1 - \tilde{\alpha}$ has a zero of order $\rho + 1$ at $s = 0$.

To complete the proof of the Theorem, we need to show that the bound provided by Proposition 3 is attained. When k is finite, this was done by H.L. Schmid, [2], §3:

if $\chi : G^{ab}_{k(D)} \to \mathbf{Z}/p^n\mathbf{Z}$ is the character corresponding to the cover f_n, then the residue vector is related to the reciprocity map by the formula

$$\chi(\mathrm{rec}(\alpha)) = \mathrm{Tr}\left((\underline{u}, \alpha)_\infty\right) \qquad \forall \alpha \in k(D)^\times,$$

where $\mathrm{Tr} : \mathbb{W}_n(k) \to \mathbb{W}_n(\mathbf{F}_p)$ is the trace map. The computation of the conductor follows at once from its classical description in terms of norms of units (e.g. [5], chap. XV, §2).

For an arbitrary field k, this classical approach no longer holds, but it is still possible to prove the desired equality using higher class field theory: see [1], §2.

In the appendix we give an elementary proof of this formula; the reader who is willing to venture through it will certainly appreciate the difference between the clean and conceptual approach via class field theory and the following tedious but elementary computations.

Appendix: Elementary computation of the conductor of a cyclic extension.

Our goal is to show that the inequality in Proposition 3 is indeed an equality. Again, our proof is by induction on n, the case $n = 1$ being classical (e.g. [4], 4.4). We shall therefore assume that the Theorem is true for cyclic extensions of degree p^l, for $l \leq n$ and prove that it is true for $l = n+1$ by showing that, with the notations of Proposition 3, $m(f_{n+1}) = M(f_{n+1})$.

To this end, we need to compute the conductor of C_{n+1}/D or, which amounts to the same, that of C_{n+1}/C_n. The latter is a cyclic extension of degree p and hence it is described by an Artin-Schreier equation $y^p - y = z$, for a suitable rational function z on C_n which is not, however, in standard form i.e. z has a pole of order divisible by p, and we cannot read off the conductor immediately.

Some work is needed in order to bring the Artin-Schreier equation describing the cover C_{n+1}/C_n in standard form. The key to all our computations is the following, elementary

Lemma 3. *(Adjustment lemma). Let $f : Y \to X$ be a finite separable cover of curves of degree p^n, totally ramified at y_0. Let t (resp. s) be local parameters at y_0 (resp. $x_0 = f(y_0)$). Then, in a neighborhood of y_0*

$$s = t^{p^n}\left(\alpha_1^p + t^{\mu(f)}\alpha_0\right)$$

for some $\alpha_0, \alpha_1 \in \mathcal{O}^\times_{Y,y_0}$, with

$$\mu(f) = \deg \mathfrak{D}_{Y/X,y_0} - p^n + 1$$

Proof: Let $s = \alpha t^{p^n}$ for some unit $\alpha \in \mathcal{O}^\times_{Y,y_0}$ and expand $\alpha = \sum_{r\geq 0} a_r t^r$ with $a_r \in k$ and $a_0 \in k^\times$. If μ is the smallest positive integer prime to p such that $a_\mu \neq 0$, then

$$\deg \mathfrak{D}_{Y/X,y_0} = v_{y_0}\left(\frac{ds}{dt}\right) = p^n + v_{y_0}\left(\frac{d\alpha}{dt}\right) = p^n + \mu - 1$$

We can therefore collect: $\alpha = \sum_{0\le r<\frac{\mu}{p}} a_{pr}t^{pr} + t^{\mu}\sum_{r\ge\mu} a_r t^r = \alpha_1^p + t^{\mu}\alpha_0$.

Corollary 3. *With the notations above, let g be a rational function on X. Then $f^*(g) = g_1^p + g_0$ for suitable rational functions g_i on Y with $v_{y_0}(g_0) = p^n v_{x_0}(g) + \mu(f)$.*

Proof: Expanding g as a power series in s, it is sufficient to prove it when $g(s) = as^r$ is a monomial of degree prime to p:

$$as^r = at^{p^n r}\left(\alpha_1^p + t^{\mu}\alpha_0\right)^r = at^{p^n r}\left(\alpha_1^{pr} + t^{\mu}\alpha_0'\right) = (a^{\frac{1}{p}}t^{p^{n-1}}\alpha_1^r)^p + at^{p^n r+\mu}\alpha_0'$$

When the cover is Galois, it is easy to relate the number $\mu(f)$ to the conductor of the extension and how it varies in towers:

Proposition 4. *With the notation as in Lemma 3, suppose moreover that f is Galois of group G and conductor $m(f)+1$.*

1. *If $e(f)$ is the largest integer such that $G_e \neq 1$, then*
$$\mu(f) = p^n m(f) - e(f)$$
2. *Let $g : Z \to Y \to X$ be a second separable Galois cover, totally ramified above x_0 whose group $\tilde{G}$ is an extension of G by $H = \mathbf{Z}/p\mathbf{Z}$. Let $e(g)$ be the largest integer such that $\tilde{G}_e \neq 1$ and suppose that $\tilde{G}_{e(g)} \cap H \neq 1$. If $m(g)+1$ denotes the conductor of g, then*
$$e(g) = p^n m(g) - \mu(f)$$

Proof: (1). Denote, as usual, by $g_i = |G_i|$; as f is totally ramified, $G_0 = G$. By[5], chap. IV, proposition 12, $m = \frac{1}{g_0}\sum_{i=0}^{e} g_i - 1$, hence

$$\begin{aligned}
\mu(f) &= \deg \mathfrak{D}_{Y/X,y_0} - p^n + 1\\
&= \textstyle\sum_{i=0}^{e}(g_i - 1) - p^n + 1\\
&= \textstyle\sum_{i=0}^{e} g_i - e - p^n\\
&= p^n\left(\frac{1}{p^n}\textstyle\sum_{i=0}^{e} g_i - 1\right) - e.
\end{aligned}$$

(2). Denote by φ the Herbrand function of the cover g and by $\tilde{g}_i = |\tilde{G}_i|$. The hypotheses imply that $\tilde{g}_i = pg_i$ for $0 \le i \le e(f)$, hence

$$\begin{aligned}
m(g) = \varphi(e(g)) &= \tfrac{1}{p^{n+1}}\left(\tilde{g}_1 + \cdots + \tilde{g}_{e(f)} + p\,[e(g) - e(f)]\right)\\
&= \tfrac{1}{p}\varphi(e(f)) + \tfrac{1}{p^n}[(e(g) - e(f)]\\
&= m(f) + \tfrac{1}{p^n}[e(g) - e(f)].
\end{aligned}$$

Corollary 4. *Let $f_n : C_n \to D$ be a separable cyclic cover of degree p^n, totally ramified above ∞. For any $0 \le i \le n$, let $f_i : C_i \to D$ be the quotient cover of degree p^i and by $g_i : C_n \to C_i$ the subcover of degree p^{n-i}. Put $m_i = m(f_i)$ (resp. $e_i = e(f_i)$, resp. $\mu_i = \mu(f_i)$). Then:*

$$e_n = \sum_{i=1}^{n} p^{i-1}(m_i - m_{i-1}); \qquad \mu_n = \sum_{i=1}^{n}(p^i - p^{i-1})m_i; \qquad \mu(g_i) = \mu_n - p^{n-i}\mu_i.$$

Proof: From Proposition 4.2, we deduce the inductive relations

$$e_n - e_{n-1} = p^{n-1}(m_n - m_{n-1}); \qquad \mu_n - \mu_{n-1} = (p^n - p^{n-1})m_n$$

from which the first two formulas in the claim follow at once. As for the third, it is a consequence of the transitivity of the different of a composite extension:

$$\mu(g_i) = \deg \mathfrak{D}_{C_n/C_i} - p^{n-i} + 1 = \deg \mathfrak{D}_{C_n/D} - p^n + 1 - p^{n-i}\left(\deg \mathfrak{D}_{C_i/D} - p^i + 1\right).$$

We are now ready to resume the discussion interrupted before Lemma 3. We are given a separable cyclic cover $f_{n+1} : C_{n+1} \to D$ of degree p^{n+1}, as in the theorem, and we want to compute its conductor, to show that the inequality provided by Proposition 3 is indeed an equality.

Equivalently, we can compute the conductor of the degree p subextension C_{n+1}/C_n. With the notations as in Proposition 4, let $\tilde{G} = \mathbf{Z}/p^{n+1}\mathbf{Z}$ be the group of C_{n+1}/D and $H = \mathbf{Z}/p\mathbf{Z}$ that of C_{n+1}/C_n: by [5], IV, prop. 2, $H_i = H \cap \tilde{G}_i$ and it is clear that $H = H_{e_{n+1}} = \tilde{G}_{e_{n+1}}$ is the last nontrivial subgroup for both extensions.

We begin by making the Artin-Schreier equation defining the cover C_{n+1}/C_n more explicit. Away from ∞, the cover C_{n+1}/D is described by the Witt vector equation

$$F(\underline{Y}) - \underline{Y} = (u_0, \ldots, u_n) \tag{5}$$

where the left hand side should be understood as a difference of two vectors, while the equation defining C_n/D is the image of (5) under the restriction homomorphism $\mathbf{r} : \mathbb{W}_{n+1} \to \mathbb{W}_n$. Therefore, the n-th component of (5) is

$$Y_n^p - Y_n + c_n\left(F(\underline{Y}), -\underline{Y}\right) = u_n$$

where the polynomial $c_n(\underline{X}, \underline{Y})$ is the one defined by equation (2). If $\underline{y} = (y_0, \ldots, y_{n-1})$ denotes any solution of the Artin-Schreier-Witt equation defining C_n/D, the cover C_{n+1}/C_n is described by the Artin-Schreier equation

$$Y_n^p - Y_n = u_n - c_n\left(\underline{y}^p, -\underline{y}\right). \tag{6}$$

As remarked, this equation is not in standard form: the datum on the right hand side has, in general, poles of order divisible by p. We can get rid of them by adding terms of the type $\wp(h) = h^p - h$ for suitable rational functions h on C_n; the result will be a rational function with a pole at ∞ of order e_{n+1}. By Proposition 4.2, $e_{n+1} = p^n m_{n+1} - \mu_n$.

To complete the proof of the theorem, we should then prove the following:

Claim 1. *The right hand side of equation (6) is congruent* $\bmod\ \wp\left(k(C_n)\right)$ *to a function with a pole at ∞ of order $p^n M - \mu_n$, where $M = \max\{p^{n-i}\nu_i : 0 \le i \le n\}$.*

It is easy to handle the term u_n in (6) with the adjustment lemma: u_n is a rational function on D with a pole of order ν_n at ∞, hence we can find rational functions u_n', u_n'' on C_n such that:

$$u_n = {u_n'}^p + u_n'' \qquad \text{with } v_n(u_n'') = -p^n\nu_n + \mu_n \tag{7}$$

We can then rewrite $u_n = u_n'' + u_n' + \wp(u_n')$. When $M = \nu_n$, the function u_n'' has the predicted valuation and in any event the contribution of u_n' is negligible, as $v_n(u_n') = -p^{n-1}\nu_n \geq -p^{n-1}M$, hence

$$(8)\qquad \begin{aligned} -p^n M + \mu_n + p^{n-1}\nu_n &\leq -(p^n - p^{n-1})M + \textstyle\sum_{i=1}^n (p^i - p^{i-1})m_i \\ &< -m_n(p^{n+1} - 2p^n + 1) < 0 \end{aligned}$$

as $m_i < m_n$ for $i < n$ and $M \geq pm_n$ (by our inductive hypothesis, $m_{j+1} = \max\{p^{j-i}\nu_i : i \leq j\}$ for $j \leq n-1$).

We must then analyze the contribution of the second term on the right hand side of (6); according to the claim, it should be dominant when $\nu_n < M$. Indeed, we will prove the following:

Claim 2. *The function $c_n(\underline{y}^p, -\underline{y})$ is congruent $\bmod\, \wp\,(k(C_n))$ to a function with a pole at ∞ of order $p^{n+1}m_n - \mu_n$.*

By the induction hypothesis, $M = \max\{\nu_n, pm_n\}$, and these two numbers cannot be equal; hence, the latter claim implies the former.

The following lemma gathers the information we shall need about the polynomials c_i.

Lemma 4. *Fix integers n and $i \leq n-1$. Then*

$$c_n(\underline{X}, \underline{Y}) = -X_i^{p^{n-i}-1}\left(Y_i + c_i(\underline{X}, \underline{Y})\right) + R_{i,n}$$

where $R_{i,n}$ is an isobaric polynomial of weight p^n in which the variable X_i appears with degree strictly smaller than $p^{n-i} - 1$.

Proof: It is well known that $c_0 = 0$ and $c_1 = -\sum_{r=1}^{p-1} \frac{1}{p}\binom{p}{r} X_0^r Y_0^{p-r}$. We proceed by induction. Using the recursive relation $\Phi_n(X_0, \ldots, X_n) = \Phi_{n-1}(X_0^p, \ldots, X_{n-1}^p) + p^n X_n$, we see that

$$c_n = S_n - X_n - Y_n = \frac{1}{p^n}\left[\sum_{h=0}^{n-1} p^h \left(X_h^{p^{n-h}} + Y_h^{p^{n-h}} - S_h^{p^{n-h}}\right)\right].$$

Fix $0 \leq h \leq n-1$; applying the binomial formula twice:

$$(9)\qquad \begin{aligned} &X_h^{p^{n-h}} + Y_h^{p^{n-h}} - (X_h + Y_h + c_h)^{p^{n-h}} = \\ &-c_h^{p^{n-h}} - \textstyle\sum_{s=1}^{p^{n-h}-1} \binom{p^{n-h}}{s} X_h^s Y_h^{p^{n-h}-s} - \sum_{r=1}^{p^{n-h}-1} \sum_{s=0}^{r} \binom{p^{n-h}}{r}\binom{r}{s} X_h^s Y_h^{r-s} c_h^{p^{n-h}-r}. \end{aligned}$$

The variable X_i appears in the expression above only if $h \geq i$; suppose $h > i$, then by the induction hypothesis we can write

$$c_h = -X_i^{p^{h-i}-1}(Y_i + c_i) + R_{i,h}$$

hence the highest power of X_i in (9) appears in the term $c_h^{p^{n-h}}$ and its contribution in c_n is of degree at most $(p^{h-i} - 1)p^{n-h}$.

For $h=i$, the variable X_i does not appear in c_i hence the term containing the highest power of X_i in (9) is

$$-\binom{p^{n-i}}{1}X_i^{p^{n-i}-1}Y_i-\binom{p^{n-i}}{p^{n-i}-1}\binom{p^{n-i}-1}{p^{n-i}-1}X_i^{p^{n-i}-1}c_i=-p^{n-i}X_i^{p^{n-i}-1}\left(Y_i+c_i\right).$$

Our task is now to compute the valuation at ∞ of a rational function on C_n, congruent to $c_n(\underline{y}^p,-\underline{y})$ mod $\wp(k(C_n))$ and having a pole of order prime to p, where $\underline{y}=(y_0,\ldots,y_{n-1})$ is a vector of solutions for the Artin-Schreier-Witt equation defining C_n/D.

Lest the reader should get lost or depressed (or both) by the following computations, let us state immediately that we are going to show that, for any $i\le n-1$, only the monomials

$$y_i^{p(p^{n-i}-1)+1}$$

are relevant. More precisely, if $j\le n-1$ is the (necessarily unique) integer for which

$$m_n=p^{n-j-1}\nu_j=\max\left\{p^{n-i-1}\nu_i\,:\;0\le i\le n-1\right\}$$

then $y_j^{p(p^{n-j}-1)+1}$ is congruent mod $\wp\left(k(C_n)\right)$ to a function with a pole at ∞ of order $p^{2n-j}\nu_j-\mu_n$ and that $c_n(\underline{y}^p,-\underline{y})-y_j^{p(p^{n-j}-1)+1}$ is congruent to a function with a pole of order strictly smaller.

The approach is in two steps: first, we obtain an estimate of the valuation of $c_n(\underline{y}^p,-\underline{y})$ and then we apply the adjustment lemma to the functions y_i to get rid of the terms in $\wp(k(C_n))$. In both steps, the problem to sort out the relevant monomials is reduced to a linear optimization.

The proof is only a tedious exercise in linear programming, and the reader would loose very little, should he indulge in the temptation to skip the rest of this section.

When the variables X_i and Y_i are given the weight p^i, the polynomial $c_n(\underline{X},\underline{Y})$ is isobaric of weight p^n; evaluating at $\underline{X}=\underline{y}^p$ and $\underline{Y}=-\underline{y}$, our task is to compute the valuation of a sum of monomials $\prod_{i=0}^{n-1}y_i^{pa_i+b_i}$.

Put $v_n(y_i)=w_i$; regarding a_i and b_i ad variables, the question can be rephrased as an optimization problem for a linear function under a linear constraint:

$$\text{Minimize}:\sum_{i=0}^{n-1}w_i(pa_i+b_i)\qquad\text{under}:\sum_{i=0}^{n-1}p^i(a_i+b_i)=p^n\tag{10}$$

with $a_i\in[0,p^{n-i}-1]$ and $b_i\in[0,p^{n-i}]$. The range of the a_i's is restricted by Lemma 4; we do not apply it to the b_i's because of the irregular behavior in characteristic 2 of the polynomials $I_i(\underline{Y})$ expressing the opposite of a Witt vector.

Actually, it is more convenient to rephrase the problem slightly: putting $\alpha_i=pa_i+b_i$ and taking α_i,b_i as variables, it becomes:

$$\text{Minimize}:\ \sum_{i=0}^{n-1}w_i\alpha_i\qquad\text{under}:\sum_{i=0}^{n-1}p^i\alpha_i+\sum_{i=0}^{n-1}(p^{i+1}-p^i)b_i=p^{n+1}\tag{11}$$

with $\alpha_i \in [0, p^{n-i+1} - p + 1]$ and $b_i \in [0, p^{n-i}]$.

Extremal values of a linear function on a convex polytope are attained at the vertices; as $b_i = p^{n-i}$ forces $a_i = 0$, hence $\alpha_i = p^{n-i}$, best admissible solutions are for $\alpha_i = p^{n-i+1} - p + 1$, $b_i = 1$ and and $\alpha_l = b_l = 0$ for $l \neq i$. We have thus:

$$v_n(c_n(\underline{y}^p, -\underline{y})) \geq \min \left\{ (p^{n-i+1} - p + 1)w_i \mid \quad 0 \leq i \leq n-1 \right\}$$

and this in turn implies our first estimate:

Lemma 5. 1. *$v_n(c_n(\underline{y}^p, -\underline{y})) \geq -(p^{n+1} - p + 1)m_n$.*

2. *$v_{n+1}(y_n) \geq -p^n m_{n+1}$, with an equality if and only if $\nu_n = m_{n+1}$.*

Proof: Induction on n: the case $n = 0$ being clear, assume (1) and (2) hold for c_i and y_i for all $i \leq n-1$. Then, since $m_n \geq p^{n-i-1} m_{i+1}$, we have

$$\begin{aligned} v_n(y_i^{p(p^{n-i}-1)+1}) &= p^{n-i-1} v_{i+1}(y_i^{p(p^{n-i}-1)+1}) \\ &\geq -p^{n-i-1}(p^{n+1} - p^{i+1} + p^i) m_{i+1} \\ &\geq -(p^{n+1} - p^{i+1} + p^i) m_n \end{aligned}$$

Finally, as y_n is a solution of the equation $y_n^p - y_n = u_n - c_n$ and clearly $v_n(u_n) = -p^n \nu_n \geq -p^n m_{n+1}$, with equality holding if and only if $\nu_i = m_{i+1}$, (2) follows at once.

To compute the valuation of $c_n(\underline{y}^p, -\underline{y}) \bmod \wp(k(C_n))$, we have to apply the adjustment lemma twice, first on C_i and then on C_n.

Fix $i \leq n-1$ and denote by v_i the discrete valuation of $\mathcal{O}_{C_i,\infty}$. By definition, y_i is the solution (on C_{i+1}) of the Artin-Schreier equation $y_i^p - y_i = u_i - c_i(\underline{y}^p, -\underline{y})$; applying the adjustment lemma to u_i and the induction hypothesis to c_i, we can find rational functions g_i and $\tilde{u}_i$ on C_i such that

$$u_i - c_i(\underline{y}^p, -\underline{y}) = \tilde{u}_i + g_i^p - g_i$$

with $v_i(\tilde{u}_i) = p^i m_{i+1} - \mu_i$ and, by the lemma above, $v_i(g_i^p) \geq -p^n m_{n+1}$, equality holding iff $\nu_i = m_{i+1}$.

On C_{i+1} we have thus $y_i = \tilde{y}_i + g_i$ with

$$v_{i+1}(\tilde{y}_i) = -p^i m_{i+1} + \mu_i; \qquad v_{i+1}(y_i) = v_{i+1}(g_i) \geq p^i m_{i+1}$$

with an equality iff $\nu_i = m_{i+1}$.

We now apply the adjustment lemma on C_n both to $\tilde{y}_i$ and g_i: we can write

$$\tilde{y}_i = \tilde{\gamma}_i^p + \tilde{\eta}_i \qquad g_i = \gamma_i'^p + \eta_i'$$

with $v_n(\tilde{\gamma}_i) = p^{-1} v_n(y_i) = -p^{n-2} m_{i+1} + p^{n-i-1} \mu_{i+1}$ and, applying Corollary 4,

$$\begin{aligned} v_n(\tilde{\eta}_i) &= v_n(\tilde{y}_i) + \mu(C_n/C_{i+1}) \\ &= -p^{n-i-1}(p^i m_{i+1} - \mu_i) + \mu_n - p^{n-i-1}\mu_{i+1} \\ &= -p^{n-1} m_{i+1} - p^{n-i-1}(p^{i+1} - p^i) m_{i+1} + \mu_n \\ &= -p^n m_{i+1} + \mu_n. \end{aligned}$$

As g_i comes from C_i, we have $v_n(\gamma_i') = p^{-1}v_n(g_i) \geq -p^{n-2}m_{i+1}$, with equality iff $\nu_i = m_{i+1}$ and

$$\begin{aligned} v_n(\eta_i') &= v_n(g_i) + \mu(C_n/C_i) \\ &= p^{n-i}v_i(g_i) + \mu_n - p^{n-i}\mu_i \\ &\geq -p^{n-1}m_{i+1} + \mu_n - p^{n-i}\mu_i \end{aligned}$$

Trivially, $v_n(\gamma_i') \lneq v_n(\tilde{\gamma}_i)$; the same rough estimates as in equation (8) yield $v_n(\tilde{\eta}_i) \lneq v_n(\eta_i')$. Putting $\gamma_i = \tilde{\gamma}_i + \gamma_i'$ and $\eta_i = \tilde{\eta}_i + \eta_i'$, we can write

$$y_i = \gamma_i^p + \eta_i \qquad \text{with:} \quad v_n(\eta_i) = -p^n m_{i+1} + \mu_n; \; v_n(\gamma_i) \geq -p^{n-2}m_{i+1}$$

again the last inequality being an equality iff $\nu_i = m_{i+1}$.

Substituting in $\prod_{i=0}^{n-1} y_i^{\alpha_i}$ we get:

$$\prod_{i=0}^{n-1}(\gamma_i^p + \eta_i)^{\alpha_i} = \prod_{i=0}^{n-1}\gamma_i^{p\alpha_i} + \sum_{i=0}^{n-1}\left(\alpha_i\gamma_i^{p\alpha_i - 1}\eta_i\prod_{h\neq i}\gamma_h^{p\alpha_h}\right) + \dots$$

The first term is a p-power and, by Lemma 5, its valuation is bounded from below by $-(p^{n+1} - p + 1)m_n$; the same estimates as those of formula (8) show that its p-th root has a pole of order strictly smaller than $p^{n+1}m_n - \mu_n$ and we can get rid of it $\mathrm{mod}\,\wp(k(C_n))$.

To prove the claim, we should therefore compute, for all $i, h \leq n-1$, the valuation of the monomials $\gamma_i^{p\alpha_i - 1}\eta_i\prod_{h\neq i}\gamma_h^{p\alpha_h}$.

Our optimization problem (11) becomes then:

$$\text{Minimize}: v_n(\eta_i) + w_i\alpha_i + \sum_{h\neq i} w_h\alpha_h \qquad \text{under}: \sum_{l=0}^{n-1} p^l\alpha_l + \sum_{l=0}^{n-1}(p^{l+1} - p^l)b_l = p^{n+1}$$

with $\alpha_l \in [0, p^{n-l+1} - p + 1]$ and $b_l \in [0, p^{n-l}]$.

Proof of Claim 2. All we have to do is check the extremal values of the function above, for all i. For $\alpha_i = p^{n-i+1} - p + 1$ and $b_i = 1$ we get

$$v_n(\gamma_i^{p^{n-i+2} - p^2}\eta_i) \geq -(p^{n-i+2} - p^2)p^{n-2}m_{i+1} - p^n m_{i+1} + \mu_n = -p^{2n-i}m_{i+1} + \mu_n$$

with an equality iff $\nu_i = m_{i+1}$. Hence, if $j \leq n-1$ is the (necessarily unique) integer for which

$$m_n = p^{n-j-1}\nu_j = \max\{p^{n-i-1}\nu_i : \; 0 \leq i \leq n-1\}$$

then $y_j^{p(p^{n-j}-1)+1}$ is congruent $\bmod \wp(k(C_n))$ to a function with a pole at ∞ of order $p^{2n-j}\nu_j - \mu_n$. If $i \neq j$ then $p^{n-i-1}\nu_i \lneq m_n$ and the contribution of y_i is strictly smaller.

Finally, consider $c_n(\underline{y}^p, -\underline{y}) - y_j^{p(p^{n-j}-1)+1}$: repeating the argument above, to show that it is congruent $\mathrm{mod}\,\wp(k(C_n))$ to a function with a pole of order strictly smaller than $p^{2n-j}\nu_j - \mu_n$, it suffices to show that the term containing the highest power of y_j, namely

$$y_j^{p(p^{n-j}-1)}c_j(\underline{y}^p, -\underline{y})$$

(cf. Lemma 4) satisfies this property. As above, after a double application of the adjustment lemma on C_n, we can write

$$c_j(\underline{y}^p, -\underline{y}) = \theta_j^p + \xi_j$$

with $v_n(\theta_j^p) = p^{n-j}v_j(c_j) \geq -p^{n-j}(p^{j+1} - p + 1)m_j$ (cf. Lemma 5) and

$$v_n(\xi_j) = -p^{n-j}(p^{j+1}m_j - \mu_j) + \mu_n - p^{n-j}\mu_j = -p^{n+1}m_j + \mu_n.$$

Therefore, $\mathrm{mod}\,\wp(k(C_n))$ we can get rid of $y_j^{p(p^{n-j}-1)}\theta_j^p$ and, by Lemma 5.2,

$$\begin{aligned} v_n(y_j^{p(p^{n-j}-1)}\xi_j) &= p(p^{n-j} - 1)p^{n-j-1}v_{j+1}(y_j) - p^{n+1}m_j + \mu_n \\ &= -(p^{n+1} - p^{j+1})p^{n-j-1}\nu_j - p^{n+1}m_j + \mu_n \\ &= -p^{2n-j}\nu_j + p^j(\nu_j - pm_j) + \mu_n \end{aligned}$$

and the assumption on j implies that $\nu_j - pm_j$ is strictly positive.

References

[AC IX] N. Bourbaki, *Algèbre Commutative, Chap IX*, Masson, Paris (1983).

[E.G.A. II] A. Grothendieck et J. Dieudonné, *Eléments de Géométrie Algébrique, Chap II*, Publications Mathématiques de l'I.H.E.S. **8** (1961).

[1] J.-L. Brylinski, *Théorie du corps de classes de Kato et revêtements abéliens de surfaces*, Annales de l'Institut Fourier **33** (1983), 23-38.

[2] H.L. Schmid, *Zur Arithmetik der zyklische p-Körper*, Journal für die reine und angewandte Mathematik **176** (1936), 161-167.

[3] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris (1961).

[4] J.-P. Serre, *Sur les corps locaux à corps résiduel algébriquement clos*, Bulletin de la SMF, **89** (1961), 105-154.

[5] J.-P. Serre, *Corps locaux*, Hermann, Paris (1968).

[6] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, Journal für die reine und angewandte Mathematik **176** (1936), 126-140.

Marco A. Garuti, Dipartimento di Matematica Pura ed Applicata, Università degli Studi di Padova, Via Belzoni 7, 35131, Padova - ITALY

E-mail address: mgaruti@galileo.math.unipd.it