Manuscripta Math. 141 (2013), no. 1-2, 315-331, http://dx.doi.org/10.1007/s00229-012-0573-y

On some notions of good reduction for endomorphisms of the projective line

Jung Kyu Canci[*1], Giulio Peruginelli[†2], and Dajano Tossici[‡3]

[1]Departement Math. Universität Basel, Rheinsprung 21, CH-4051 Basel, Switzerland.
[2]Institut für Analysis und Comput. Number Theory, Technische Universität, Steyrergasse 30, A-8010 Graz, Austria.
[3]Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy.

October 6, 2015

Abstract

Let Φ be an endomorphism of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$, the projective line over the algebraic closure of $\mathbb{Q}$, of degree ≥ 2 defined over a number field K. Let v be a non-archimedean valuation of K. We say that Φ has critically good reduction at v if any pair of distinct ramification points of Φ do not collide under reduction modulo v and the same holds for any pair of branch points. We say that Φ has simple good reduction at v if the map Φ_v, the reduction of Φ modulo v, has the same degree of Φ. We prove that if Φ has critically good reduction at v and the reduction map Φ_v is separable, then Φ has simple good reduction at v.

1 Introduction

Throughout this paper K will be a number field and $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. More generally, for any arbitrary field Ω, the symbol $\overline{\Omega}$ will denote an algebraic closure of Ω.

In a recent paper, Szpiro and Tucker ([14]) use a particular notion of good reduction to prove a finiteness result for equivalence classes of endomorphisms of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$, which we will indicate simply with $\mathbb{P}^1$ in the sequel. This result implies the Shafarevich-Faltings finiteness theorem for isomorphism classes of elliptic curves.

[*] jkcanci@yahoo.it

[†] peruginelli@math.tugraz.at (Corresponding author; this author was partially supported by the Austrian Science Foundation (FWF) P23245-N18)

[‡] dajano.tossici@gmail.com

MSC Classification codes: 14H25, 37P05 and 37P35.

We recall the definition of good reduction used by Szpiro and Tucker. Before doing that, we fix some notation. Let O_K be the ring of integers of K. For a fixed finite place v of K, let O_v be the valuation ring and let $k(v)$ be the residue field. We will not distinguish between the place v and the associated valuation. Let S be a fixed finite set of places of K containing all the archimedean ones. We denote by O_S the set of S-integers, namely

$$O_S \doteqdot \{x \in K \mid |x|_v \leq 1 \text{ for all } v \notin S\}.$$

Let Φ be an endomorphism of $\mathbb{P}^1$ defined over K. We denote by $\mathcal{R}_\Phi$ the set of ramification points defined over $\overline{\mathbb{Q}}$ of the map Φ. Given a valuation v of $\overline{\mathbb{Q}}$ and a subset $E \subset \mathbb{P}^1(\overline{\mathbb{Q}})$, we denote by $(E)_v$ the subset of $\mathbb{P}^1(\overline{k(v)})$ whose elements are the reduction modulo v of the elements of E.

We give now the definition of good reduction used by Szpiro and Tucker in [14]:

Definition 1.1. Suppose that v has been extended to $\overline{\mathbb{Q}}$. Let Φ be an endomorphism of $\mathbb{P}^1$ of degree ≥ 2 defined over K. We say that Φ has *critically good reduction* (in the sequel C.G.R.) at v if

1) $\#\mathcal{R}_\Phi = \#(\mathcal{R}_\Phi)_v$,

2)$\#\Phi(\mathcal{R}_\Phi) = \#(\Phi(\mathcal{R}_\Phi))_v$.

As the authors of [14] note, this definition does not depend on the extension of v to $\overline{\mathbb{Q}}$.

We denote by $\mathrm{PGL}(2, O_S)$ the quotient group of $\mathrm{GL}(2, O_S)$ by scalar matrices. It is the automorphism groups of $\mathbb{P}^1_{O_S}$. In [14] the following equivalence relation on the set of endomorphisms of $\mathbb{P}^1$ is used: two endomorphisms Ψ and Φ of the projective line over K are S-equivalent if there exist automorphisms γ, σ of $\mathbb{P}^1_{O_S}$ such that

$$\Psi = \gamma_K \circ \Phi \circ \sigma_K,$$

where γ_K and σ_K are the restrictions of γ and σ over $\mathbb{P}^1_K$, which has a natural open immersion in $\mathbb{P}^1_{O_S}$.

With the above notations and definitions, the main result in [14] is the following. Let K be a number field, n a positive integer and S a finite set of places of K, containing the archimedean ones. Then there are finitely many equivalence classes of rational maps $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ defined over K of degree n that ramify at three or more points and have C.G.R. at all valuation v outside S.

In the context of endomorphisms of $\mathbb{P}^1$, there is another notion of good reduction. We give the definition of normalized form for endomorphisms of $\mathbb{P}^1$ with respect to a finite place v of K.

Definition 1.2. Let $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map defined over K, of the form

$$\Phi([X : Y]) = [F(X, Y) : G(X, Y)]$$

where $F, G \in K[X, Y]$ are coprime homogeneous polynomials of the same degree. Given a finite place v of K, we say that Φ is in *v-reduced form* if the coefficients of F and G are in O_v and at least one of them is a v-unit.

If we multiply $\Phi = [F : G]$ by a non-zero element of K and we factor out any common factor in O_v among the coefficients of the two polynomials, we can always assume that a rational map is in v-reduced form. We may now give the following definition.

Definition 1.3. Let $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map defined over K and let v be a finite place of K. Suppose that $\Phi([X : Y]) = [F(X,Y) : G(X,Y)]$ is in v-reduced form. The *reduced map* $\Phi_v : \mathbb{P}^1_{k(v)} \to \mathbb{P}^1_{k(v)}$ is defined by $[F_v(X,Y) : G_v(X,Y)]$, where F_v and G_v are the polynomials obtained from F and G by reducing their coefficients modulo v.

The second notion of good reduction that we are going to consider is the following:

Definition 1.4. A rational map $\Phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ defined over K has *simple good reduction* (in the sequel S.G.R.) at a place v if $\deg \Phi = \deg \Phi_v$.

In both definitions of good reduction we assume that a model or choice of coordinates for $\mathbb{P}^1$ in the domain of Φ is fixed. This assumption represents the main difference between our definition of good reduction and other similar definitions of good reduction (e.g. see [1], [5], [17]).

In the above notation, Φ has S.G.R. at v if F_v and G_v have no common factors over $k(v)$. Alternatively, from a schematic point of view, the above definition means the following: if we consider Φ as a scheme morphism $\Phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$, then Φ has S.G.R. at v if there exists a morphism $\Phi_{O_v} : \mathbb{P}^1_{O_v} \to \mathbb{P}^1_{O_v}$ which extends Φ, i.e. the following diagram

$$\begin{tikzcd}
\mathbb{P}^1_K \arrow[r, "\Phi"] \arrow[d] & \mathbb{P}^1_K \arrow[d] \\
\mathbb{P}^1_{O_v} \arrow[r, "\Phi_{O_v}"] & \mathbb{P}^1_{O_v}
\end{tikzcd}$$

is cartesian, where the vertical maps are the natural open immersions. We stress that in this schematic definition the choice of a model of $\mathbb{P}^1_K$ corresponds to the choice of the open immersion of $\mathbb{P}^1_K$ in $\mathbb{P}^1_{O_v}$.

The definition of simple good reduction is, perhaps, more natural than the definition of critically good reduction. However, a rational map on $\mathbb{P}^1(K)$ associated to a polynomial in $K[z]$ has simple good reduction outside S if and only if the coefficients of the polynomial are S-integers and its leading coefficient is an S-unit. Therefore for sufficiently large n the main theorem of [14] would be false if we considered the simple good reduction instead of the critically one.

In this paper we are concerned with the relations between these two notions of good reduction for an endomorphism of $\mathbb{P}^1$. As the authors of [SzT] already remarked, the two notions are not equivalent. They also gave examples where none of the two conditions implies the other.

Nevertheless, they proved the following proposition, that for the ease of readers we quote here in a slightly simpler form:

Proposition 1.5. *Let K be a number field with ring of integers O_K, v a finite place of K and $\Phi(x) = f(x)/g(x)$ a rational function of degree d with coefficients in O_K, considered as a rational function from $\mathbb{P}^1$ in itself. Suppose that R_Φ has $2d-2$ elements and the leading coefficients of f, g and $f'(x)g(x) - f(x)g'(x)$ are all v-adic units. Then, if Φ has C.G.R. at v, it also has S.G.R. at v.*

We have obtained a significant improvement of this result.

Theorem 1.6. *Let $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism of degree ≥ 2 defined over K. Let v be a finite place of K. Suppose that the reduced map Φ_v is separable. Then the following are equivalent:*

a) Φ has C.G.R. at v;

b) Φ has S.G.R. at v and $\#\Phi(\mathcal{R}_\Phi) = \#(\Phi(\mathcal{R}_\Phi))_v$.

We recall that Φ_v is separable if it induces a separable extension of function fields $(k(v))(x) \supset (k(v))(\Phi_v(x))$. This is equivalent to say that the element x is separable over the field $(k(v))(\Phi_v(x))$. Let $\Phi_v(x) = f_v(x)/g_v(x)$, where f_v and g_v are two polynomials with no common factors and with coefficients in $k(v)$. Then, by definition, x is separable over $(k(v))(\Phi_v(x))$ if and only if the minimal polynomial $f_v(X) - \Phi_v(x)g_v(X)$ has no multiple roots in the algebraic closure of $k((v))(\Phi_v(x))$. This is equivalent to $f_v(X) - \Phi_v(x)g_v(X) \notin (k(v))(\Phi_v(x))[X^p]$, where p is the characteristic of $k(v)$. Since $\Phi_v(x)$ is transcendental over $k(v)$, the last condition is fulfilled if and only if $f_v(x)/g_v(x) \notin (k(v))(x^p)$. Since $k(v)$ is a finite field it is a perfect field; that allows us to conclude by saying that the map Φ_v is separable if and only if it is not a p-th power of a rational function. For more details about separability see for example [9, Chapter I.4].

The proposition of Szpiro and Tucker follows from the above theorem since the fact that the leading term of $f'(x)g(x) - f(x)g'(x)$ is a unit implies in particular that Φ_v is separable.

If we remove the condition of separability Theorem 1.6 can be false; for instance, let us consider $\Phi(x) = px^n$ over $\mathbb{Q}$, with p a prime number and n an integer. This endomorphism has not S.G.R. at p, but it has C.G.R. at p. In this case the reduced map is constant. One can find also a similar example where the reduced map is not constant. Take for example the map induced by the polynomial $\Phi(x) = -3x^4 + 4x^3$. On the other hand, the map given by $\Phi(x) = (x-2)^2(x-4)^2$ defined over $\mathbb{Q}$, has $\mathcal{R}_\Phi = \{2, 3, 4, \infty\}$ and $\Phi(\mathcal{R}_\Phi) = \{0, 1, \infty\}$. Hence condition b) of Theorem 1.6 holds at the prime 2, since Φ has S.G.R. at 2, but Φ has not C.G.R at 2. There are also examples where the map has both C.G.R. and S.G.R. at a prime p but the separability condition does not hold, like the family of maps $\Phi(x) = x^p$.

Nevertheless, the condition on separability seems to be a good condition. In fact if p, the integral prime under v, is bigger than the degree of a map Φ, then Φ_v is separable if and only if it is not constant. Therefore, a direct consequence of Theorem 1.6 is the following corollary:

Corollary 1.7. *Let $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism of degree ≥ 2 defined over K. Let v be a finite place of K. Let p be the prime of $\mathbb{Z}$ under the place v and suppose that $p > \deg(\Phi)$ and Φ has C.G.R. at v. Then Φ has S.G.R. at v if and only if Φ_v is not constant.*

Theorem 1.6 establishes some sufficient conditions for endomorphisms of $\mathbb{P}^1$ to have simple good reduction. A general result in this direction is [5, Thm 3.3], where Fulton proves and extends some results stated by Grothendieck in [6]. Analogue result to Fulton's theorem for covers of curves, using different methods, are proved by Beckmann in [1, Prop. 5.3]. For a similar theorem on plane curves see also [16]. Zannier also gave another result which is more related to ours. He proved a theorem concerning the good reduction for some particular covers $\mathbb{P}^1 \to \mathbb{P}^1$. The notion of good reduction used by Zannier is the following one: using the above notation, a rational map Φ of $\mathbb{P}^1$ defined over a field L has *good reduction* at a prime v if there exist $a, b \in L$ such that the composite map $\Phi(ax+b)$ has S.G.R. at v and $(\Phi(ax+b))_v$ is separable. We say that Φ has *potential good reduction* if it has good reduction over a finite extension of L. We recall that the *monodromy group* of a non-constant map between two curves $\Phi : C \to D$ defined over a field K is the Galois group of the Galois closure of the induced field extension $K(D) \subset K(C)$. Now we are ready to state Zannier's result:

Theorem 1 in [17] *Let L be a field of characteristic zero, with a discrete valuation v having residue field L_0 of characteristic $p > 0$. Let $\Phi \doteqdot f/g \in L(t)$ be a Belyi cover (i.e. unramified outside $\{0, 1, \infty\}$) with $f(t) = \prod_{i=1}^{h}(t - \xi_i)^{\mu_i}, g(t) = \prod_{j=1}^{k}(t - \eta_j)^{\nu_j}$ polynomials of positive degree n, the ξ_i, η_j are pairwise distinct and the degree of $f - g$ is equal to $n - k - h + 1$. If Φ does not have potential good reduction at v, then p divides the order of the monodromy group and also some nonzero integer of the form $\sum_{i \in A} \mu_i - \sum_{j \in B} v_j$ where $A \subset \{1, \ldots, h\}, B \subset \{1, \ldots, k\}$.*

The part of this theorem concerning the divisibility of the order of monodromy group can be seen as an application to curves of genus 0 of Beckmann's result in [1]. However, the method used by Zannier is completely different from the Beckmann's and Fulton's ones. Moreover, Zannier's result gives some new sufficient conditions to have good reduction for Belyi covers.

There is a substantial difference between our result and the Beckmann's and Zannier's ones. Our Theorem 1.6 deals with the "good reduction" for a fixed model of a cover $\mathbb{P}^1 \to \mathbb{P}^1$. The results obtained by Zannier and Beckmann give some sufficient conditions for the existence of a model, of a given cover, with good reduction. For example, the polynomial $\Phi(z) = a^2z^2$ for all $a \in \mathbb{Z}$ does not have S.G.R. at all prime dividing the integer a, but it has good reduction according to Beckmann's and Zannier's definitions.

Zannier considers only covers $\mathbb{P}^1 \to \mathbb{P}^1$ unramified outside $\{0, \infty, 1\}$, because these covers are strictly related to the problem of the existence of distinct monic polynomials F, G having roots of prescribed multiplicities and such that $\deg(F - G)$ is as small as possible, according to Mason's *abc* theorem. Zannier treated this existence problem in [15] in characteristic 0 and in [17] in positive characteristic.

We conclude with an arithmetical and dynamical application of our result. Let E

be an elliptic curve defined over a number field K. Let us consider a fixed model for E given by an equation $y^2 = F(x) = x^3 + px + q$. Let S be the minimal finite set of places of K containing all the archimedean ones, all the finite places above 2 and such that the model of E is defined over O_S with good reduction at all finite places not in S. As proved in [14], the corresponding Lattés map $\Phi(x) = \frac{(F'(x))^2 - 8xF(x)}{4F(x)}$ has both C.G.R. and S.G.R. at v, for all places $v \notin S$. If $P \in E$ then $\Phi(x)$ is the x-coordinate of $2P$, where x is the x-coordinate of P. The set of K–rational pre-periodic points of Φ is the set of x–coordinates of the K–rational torsion points of E (see [13, p.33]). Therefore informations about pre-periodic points for Φ provide informations about torsion points of E. This is one of the motivations to study the arithmetic of dynamical systems, and in particular the set of pre-periodic points of rational maps having S.G.R. outside a prescribed set of places. The application that we present involves a theorem proved by Canci in [3] which is an extension to pre-periodic points of a result about periodic points due to Morton and Silverman (see [10]) in terms of simple good reduction.

It is natural to study pre-periodic points of arithmetical dynamical systems, given by maps having C.G.R. outside a prescribed set. Unfortunately, the notion of C.G.R. may not be preserved under iteration. Consider for example $\Phi(x) = (x-1)^2$, where Φ has C.G.R. everywhere but Φ^2 (i.e. $\Phi \circ \Phi$) does not have C.G.R at 2. On the contrary, the condition of S.G.R. is preserved under iteration. So it is a good notion for dynamical studies.

Before stating the dynamical result obtained by using our Theorem 1.6, Theorem 1 in [3] and Corollary B in [10], we give some notations.

Let K, S, v and Φ_v be as above. We denote by $\#\mathrm{PrePer}(\Phi, \mathbb{P}^1(K))$ the cardinality of the set of K–rational pre-periodic points of the map Φ.

Corollary 1.8. *Let t, d and D be fixed integers with $d \geq 2$. Then there exists a constant $C = C(t,d,D)$ such that given a number field K of degree D, a finite set of places S of K of cardinality less than t, a rational map $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree d defined over K, such that Φ has C.G.R. at every place v outside S and Φ_v is not constant for each v not in S, then the following inequalities holds:*

$$\#\mathrm{PrePer}(\Phi, \mathbb{P}^1(K)) \leq C(t,d,D).$$

A bound $C(t,d,D)$ as in the above corollary is effectively computable and it could be calculated with a simple formula involving the effective bounds proved in [3, Theorem 1] and in [10, Corollary B]. The idea behind our proof could provide an effective formula. But the estimate is not so interesting; the most important part in the above corollary is the existence of such a bound.

Corollary 1.8 represents a very particular case of the Uniform Boundedness Conjecture for pre-periodic points stated by Morton and Silverman in [10].

Computationally speaking it is worth noticing that, given a place v of K, it is easier to check that Φ_v is not constant than checking that Φ has S.G.R. at v. In the first case we have to compute $\binom{d+1}{2}$ determinants of 2×2 matrices, while in the second case we have to compute the determinant of a $(2d+2) \times (2d+2)$ matrix. In the first case we have to do an $O(d^2)$ number of calculations and in the second case the number is an $O(d^3)$. Note that the LU decomposition of a matrix reduce the number of operations from $O(d!)$, necessary by using the Leibniz rule, to $O(d^3)$ calculations (e.g. see [11]).

Here is a short overview of the contents of the paper. In section §2 we prove Theorem 1.6. The key result is Lemma 2.6 in which we give a characterization of rational maps having C.G.R. and such that the reduced map is separable. The proof is obtained interpretating the condition of C.G.R. in terms of the coefficients of an opportune representative in the class of equivalence of the rational map. In section §3 we give an example in which Theorem 1.6 cannot be applied and we explicitly treat the cases of Galois covers (see Proposition 3.2, which, in fact, is more general) and rational maps of degree two (see Proposition 3.3). The last section is dedicated to the proof of Corollary 1.8.

Acknowledgments

We worked on this problem during our stay in the Hausdorff Research Institute for Mathematics in Bonn for the trimester program on Algebra and Number Theory. We wish to thank the director Matthias Kreck and all the staff of the Institute for the given support while using the facilities of the Institute.
The notion of Critically Good Reduction in Szpiro and Tucker's article has been pointed out to us by Pietro Corvaja: we wish to thank him for that. We thank Thomas Tucker for reading the article and pointing us out some inaccuracies.
We thank Umberto Zannier for giving us precious references related to our work.
Finally we also thank the referee for the useful suggestions that improved the paper.

2 Proof of main results

From now on, K will be a number field, v a non-archimedean valuation of K and O_v the associated valuation ring. For any polynomial $h(x) \in O_v[x]$, $h_v(x)$ will denote the polynomial obtained by reducing the coefficients of $h(x)$ modulo v. In the same way for any $\alpha \in K$ we will denote its reduction modulo v by α_v.

Given an endomorphism Φ of $\mathbb{P}^1$ with $\Phi([X : Y]) = [F(X,Y) : G(X,Y)]$, where $F, G \in O_v[X,Y]$ are homogeneous coprime polynomials of the same degree d, with an abuse of notation we still denote by Φ the rational function $\Phi(x) = f(x)/g(x)$, where $f(X/Y) = F(X,Y)/Y^d$ and $g(X/Y) = G(X,Y)/Y^d$. We can reverse this argument, so to any rational function $\Phi \in K(x)$ we associate a unique endomorphism Φ of $\mathbb{P}^1$. From now on, we suppose that $\Phi(x) = f(x)/g(x)$ is a rational function defined over K written in v-reduced form.

A rational function

$$\Phi(x) = \frac{f(x)}{g(x)} = \frac{a_d x^d + \cdots + a_0}{b_d x^d + \cdots + b_0}$$

is in v-reduced form if $a_i, b_j \in O_v$ for $0 \leq i \leq d$ and $0 \leq j \leq d$, $a_d \neq$ or $b_d \neq 0$ and

$$\min\{v(a_d), v(a_{d-1}), \ldots, v(a_0), v(b_d), \ldots, v(b_0)\} = 0.$$

In particular we have

$$\Phi_v(x) = \frac{f_v(x)}{g_v(x)} = \frac{(a_d)_v x^d + \cdots + (a_0)_v}{(b_d)_v x^d + \cdots + (b_0)_v}.$$

Note that in general f_v and g_v may not be coprime.

We define the following polynomial in $O_v[x]$:

$$\Phi^{(1)}(x) \doteqdot f'(x)g(x) - f(x)g'(x). \tag{1}$$

Its degree is less or equal to $2d-2$. It is quite easy to check that

$$\mathcal{R}_\Phi \setminus \{\infty\} = \{x \in \overline{\mathbb{Q}} \mid \Phi^{(1)}(x) = 0\}$$

and ∞ is a ramification point if and only if the polynomial has degree $< 2d-2$.

It may happen that the set of primes of critically bad reduction increases if we compose with homotheties which are not v-invertible, like for example: $f(x) = x^2 + x$ and $A(x) = x/3$. The map f has C.G.R. at 3 but the map $f^A = A \circ f \circ A^{-1}$ has not. The following lemma shows that the two notions of good reduction at a place v are preserved under equivalence with v-invertible elements of $\mathrm{PGL}(2, O_v)$.

Lemma 2.1. *Suppose that Φ has S.G.R. (resp. C.G.R.) at a place v. Suppose that α, β are invertible rational maps associated to elements $A, B \in \mathrm{PGL}(2, O_v)$, respectively. Then $\alpha \circ \Phi \circ \beta$ has S.G.R. (resp. C.G.R.) at v.*

Proof. To prove that Φ has S.G.R. we use the fact that the composition of maps having S.G.R. has S.G.R. (see [13, Thm 2.18]). To prove that Φ has C.G.R. we use [13, Prop. 2.9]: given $P_1, P_2 \in \mathbb{P}^1$ such that $P_1 \not\equiv P_2 \pmod{v}$ then if $A \in \mathrm{PGL}(2, O_v)$ we have that $A(P_1) \not\equiv A(P_2) \pmod{v}$. □

The condition of the previous lemma is not necessary, consider for example: $f(x) = x^2 + 3x$ and $A(x) = x/3$, then f as well $f^A = A \circ f \circ A^{-1}$ have C.G.R. at 3, even if $A \notin \mathrm{PGL}(2, \mathbb{Z}_{(3)})$.

We shall use the following equivalence relation:

Definition 2.2. Two rational maps Φ and Ψ defined over K are v–equivalent if there exist two rational maps α and β associated to two invertible elements $A, B \in \mathrm{PGL}(2, O_v)$, respectively, such that $\Phi = \alpha \circ \Psi \circ \beta$.

In general, the reduction modulo v of rational maps does not commute with the composition of rational functions. For example consider

$$\Phi(x) = \frac{x^2 + x}{x + p} \quad \text{and} \quad \Psi(x) = px$$

for a given prime integer p. We have

$$(\Phi \circ \Psi)_p = \frac{x}{x+1} \quad \text{and} \quad \Phi_p \circ \Psi_p = 1.$$

However, if the maps Φ and Ψ have both S.G.R. at v then

$$(\Phi \circ \Psi)_v = \Phi_v \circ \Psi_v.$$

(see Theorem 2.18 in [13]). In order to have the commutativity of reduction modulo v and composition, it is not always necessary that both maps have S.G.R.. For example, the following result holds:

Lemma 2.3. *Let Φ be an endomorphism of $\mathbb{P}^1$ defined over K. Let α and β two v-invertible rational maps (i.e. they are associated to two elements in $PGL(2, O_v)$, respectively). Then*

$$(\alpha \circ \Phi \circ \beta)_v = \alpha_v \circ \Phi_v \circ \beta_v.$$

Proof. Let

$$\alpha(x) = \frac{ax+b}{cx+d} \quad , \quad \Phi(x) = \frac{f(x)}{g(x)}$$

be in v-reduced form. Now observe that the function

$$(\alpha \circ \Phi)(x) = \frac{af(x) + bg(x)}{cf(x) + dg(x)} \tag{2}$$

is in v-reduced form too. This follows by considering a representation of α^{-1} in v-reduced form: let

$$\alpha^{-1}(x) = \frac{lx+r}{sx+t},$$

where $l, r, s, t \in O_v$ and the following identity holds

$$\begin{pmatrix} l & r \\ s & t \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

then

$$\begin{pmatrix} l & r \\ s & t \end{pmatrix} \begin{pmatrix} af(x) + bg(x) \\ cf(x) + dg(x) \end{pmatrix} = \begin{pmatrix} f(x) \\ g(x) \end{pmatrix}.$$

If (2) were not in the reduced form, then also $\Phi = f/g$ would not. Therefore we have

$$(\alpha \circ \Phi)_v(x) = \frac{a_v f_v(x) + b_v g_v(x)}{c_v f_v(x) + d_v g_v(x)} = (\alpha_v \circ \Phi_v)(x).$$

A similar argument can be given to prove that for any rational function Ψ defined over K, then $(\Psi \circ \beta)_v = \Psi_v \circ \beta_v$. Now we consider $\Psi = \alpha \circ \Phi$ and we obtain

$$\alpha_v \circ \Phi_v \circ \beta_v = (\alpha \circ \Phi)_v \circ \beta_v = (\alpha \circ \Phi \circ \beta)_v.$$

□

Note that by Lemma 2.3 it follows immediately that Φ_v is separable if and only if $(\alpha \circ \Phi \circ \beta)_v$ is separable.

Now we prove a lemma which contains a statement whose proof is completely trivial. However, this lemma, despite its simplicity, will be useful several times.

Lemma 2.4. *Let $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism defined over K. Let $w, z, x, y \in \mathbb{P}^1(K)$ such that $w \not\equiv z \mod v$, $\Phi(x) = z$ and $\Phi(y) = w$. Then there exists Ψ in the same v–equivalence class of Φ with $\Psi = \alpha \circ \Phi \circ \beta$ where α and β are two automorphisms associated to two elements in $\mathrm{PGL}(2, O_v)$, respectively, with $\alpha(w) = 0$, $\alpha(z) = \infty$, $\beta^{-1}(x) = \infty$; in particular we have $\Psi(\infty) = \infty$. Furthermore, if $x \not\equiv y \mod v$, the automorphism β can be taken with the additional property $\beta^{-1}(y) = 0$, which means $\Psi(0) = 0$.*

Proof. The proof easily follows from the fact that the action of $\mathrm{PGL}(2, O_v)$ is transitive on the pairs of elements of $\mathbb{P}^1(K)$ which does not have the same reduction modulo v. □

It is clear by definition of C.G.R. that, given an arbitrary finite extension L of K, a rational map Φ defined over K has C.G.R. at v if and only if Φ, as a rational map defined over L, has C.G.R. at one of the extensions $\tilde{v}$ of v in L. In this way, without loss of generality, up to enlarging K, we can suppose that all ramification points of Φ are K–rational. The same holds also for S.G.R. in the sense that it is completely trivial that a rational map has S.G.R. over K if and only if it has S.G.R. over a finite extension L of K. Therefore we can suppose K enlarged so that if a rational map Φ has C.G.R. at a place v, then we may assume that $\{0, \infty\} \subset \mathcal{R}_\Phi$, $\Phi(0) = 0$ and $\Phi(\infty) = \infty$.

Now we state a simple lemma that contains some characterizations of having S.G.R. at v.

Lemma 2.5. *For a morphism $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree ≥ 1 the following are equivalent:*

a) Φ has S.G.R. at a finite place v;

b) Φ_v is not constant and for any $x_1, x_2 \in \mathbb{P}^1$ if $x_1 \equiv x_2 \mod v$ then $\Phi(x_1) \equiv \Phi(x_2) \mod v$;

c) Φ_v is not constant and there exist $w, z \in \mathbb{P}^1$ with $w \not\equiv z \mod v$ such that for any $x_1, x_2 \in \mathbb{P}^1$ with $\Phi(x_1) = w$ and $\Phi(x_2) = z$ then $x_1 \not\equiv x_2 \mod v$.

Proof. a) $\Rightarrow$ b). If we consider the following commutative diagram

$$\begin{tikzcd}
\mathbb{P}^1_{k(v)} \arrow[r, "\Phi_v"] \arrow[d] & \mathbb{P}^1_{k(v)} \arrow[d] \\
\mathbb{P}^1_{O_v} \arrow[r, "\Phi_{O_v}"] & \mathbb{P}^1_{O_v}
\end{tikzcd}$$

where the vertical map are the natural closed immersions, then it is easy to prove the above assertion.

b) $\Rightarrow$ *c)*. This is immediate.

c) $\Rightarrow$ *a)*. Let $\Phi(x) = f(x)/g(x)$ be a rational function defined over K, with $f, g \in O_v[x]$ coprime, written in v-reduced form. By Lemma 2.1 and Lemma 2.4, up to enlarging K and taking a suitable element in the equivalence class of Φ, we can assume that $w = 0$, $z = \infty$, and $\Phi(\infty) = \infty$. So $\deg f > \deg g$. In this situation the preimage of w is the set of roots of $f(x)$ and the preimage of z is the union of the set of roots of $g(x)$ and $\{\infty\}$ (we enlarge the base field K so that all these elements are contained in it). We observe that, by assumption c), any preimage of 0 does not coincide modulo v with any preimage of ∞. Since $\Phi(\infty) = \infty$, any preimage of 0 does not coincide modulo v with ∞. This means that the roots of the polynomial $f(x)$ have non-negative valuation. This and the fact that Φ_v is not constant imply that $f(x)$ has v-invertible leading coefficient. Under this assumption Φ has S.G.R. at v if and only if f and g have no common roots modulo v. In this situation this last condition is equivalent to the statement in c). □

The previous characterizations of S.G.R., especially part c), will be used just to shorten some of the following proofs. On the contrary next lemma, which gives another characterization of having C.G.R. when the reduced map is separable, will play an important role in the proof of Theorem 1.6.

Lemma 2.6. *A morphism $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree ≥ 2 has C.G.R. at a finite place v and Φ_v is separable if and only if*

1) *Φ_v is not constant;*

2) *if $x_1 \in \mathcal{R}_\Phi$, $x_2 \in \Phi^{-1}(\Phi(\mathcal{R}_\Phi))$ then $x_1 \equiv x_2 \mod v$ if and only if $x_1 = x_2$;*

3) *the ramification index of any ramification point is not divisible by the characteristic of the residue field $k(v)$.*

Proof. We begin by proving that if Φ has C.G.R at v then Φ_v is separable if and only if 1), 2) and 3) hold. Let x_1 and x_2 be as in 2). By Lemma 2.4, without loss of generality, we may assume $x_1 = \infty, \Phi(\infty) = \infty$, $0 \in \Phi(\mathcal{R}_\Phi)$ and $x_2 \in \Phi^{-1}(0) \bigcup \Phi^{-1}(\infty)$. In particular $\deg(f) > \deg(g)$. Since C.G.R. is stable under a finite extension of the field of the coefficients of Φ and the properties 1), 2) and 3) do not depend on the field of definition, we may assume that all the polynomials we are dealing with have linear factors over K. So the following is the factorization of $\Phi^{(1)}(x)$ (see (1)) over K:

$$\Phi^{(1)}(x) = \theta \prod_k (x - \alpha_k)^{e_k} \tag{3}$$

where $\theta \in O_v$ is the leading coefficient of $\Phi^{(1)}(x)$ and $\{\alpha_k\}_k = \mathcal{R}_\Phi \setminus \{\infty\}$. Since Φ has C.G.R. at v, the α_k's are in O_v. Since $\deg(f) > \deg(g)$, by direct computation we get that

$$\theta = \mathrm{lc}(f)\mathrm{lc}(g)(\deg f - \deg g) \tag{4}$$

where, for a polynomial h, $\mathrm{lc}(h)$ denotes the leading coefficient of h.

Therefore we get that

$$\Phi^{(1)} \not\equiv 0 \pmod v \Leftrightarrow \theta \not\equiv 0 \pmod v$$

since each α_k is a v-integer.

Let f_v and g_v be the reduction modulo v of the polynomials f and g, respectively. If we have

$$f_v(x) = h(x)f_1(x) \quad , \quad g_v(x) = h(x)g_1(x)$$

with suitable $h, f_1, g_1 \in k(v)[x]$ and f_1, g_1 coprime, then $h(x)$ is not zero because $\Phi = f/g$ is in v-reduced form. Furthermore, if $(\Phi^{(1)})_v(x)$ is the reduction modulo v of the polynomial $\Phi^{(1)}(x)$, we have that

$$(\Phi^{(1)})_v(x) = h(x)^2(f_1'g_1 - f_1g_1').$$

Hence $(\Phi^{(1)})_v$ is zero if and only if $f_1'g_1 - f_1g_1'$ is zero, which is equivalent to $\Phi_v = f_1/g_1$ being inseparable.

Therefore Φ_v is separable if and only if the leading coefficients of f and g are v-units and $\deg f - \deg g$ is not divisible by the characteristic of $k(v)$. The ramification index at ∞ is exactly equal to $\deg f - \deg g$, hence it is not divisible by the characteristic of $k(v)$.

If the leading coefficients of $f(x)$ and $g(x)$ are v-units then all the elements in $\Phi^{-1}(0) \cup \Phi^{-1}(\infty)$ different from ∞ are not equivalent to ∞ modulo v. In particular this holds for x_2. Hence we have proved that under the assumption that Φ has C.G.R. at v, the separability of Φ_v is equivalent to conditions 1), 2) and 3).

Now we prove that conditions 1), 2) imply that Φ has C.G.R. at v. By 2), in order to prove that Φ has C.G.R. at v, it is sufficient to verify the condition on the branch locus. We have to prove that for any pair of distinct points $y_1, y_2 \in \Phi(\mathcal{R}_\Phi)$, they are also distinct modulo v. Again from Lemma 2.4, and by condition 2), we can suppose that $y_1 = \infty$, $\Phi(\infty) = \infty$, $\Phi(0) = y_2$, and $0, \infty \in \mathcal{R}_\Phi$. We write Φ in the following v-normal form

$$\Phi(x) = \frac{a_d x^d + \cdots + a_0}{b_m x^m + \cdots + b_0} = \frac{a_d \prod_i (x - \eta_i)}{b_m \prod_j (x - \rho_j)} \tag{5}$$

where $d > m + 1$ and $a_i, b_j \in O_v$ for all indexes i, j. Since conditions 1) an 2) are stable by extension field and the critically good reduction does not depend on the field of definition, we can suppose that K contains all the roots η_i and ρ_j. Note that $y_2 = a_0/b_0$. Since any root ρ_j of the denominator $b_m x^m + \cdots + b_0$ is in the fiber of $\infty \in \mathcal{R}_\Phi$ and also 0 is a ramification point, then by 2) each ρ_j has to be a v-unit. Since Φ_v is not constant, then $b_0 = b_m \prod_j \rho_j$ is a v-unit, thus $v(y_2) \geq 0$. Therefore the reduction modulo v of y_2 is not ∞. This proves that Φ has C.G.R at v. □

Remark 2.7. We stress that in the second part of the proof we show that conditions 1) and 2) imply that Φ has C.G.R. at v. The condition 3) is only necessary for the separability of Φ_v.

Proof of Theorem 1.6. Firstly we prove that *a)* $\Rightarrow$ *b)*. Let $\Phi(x) = f(x)/g(x)$ be a rational function defined over K, written in v-reduced form, with $f, g \in O_v[x]$ coprime. By Lemma 2.4 we can assume that $\{0, \infty\} \subset \mathcal{R}_\Phi$ and $\Phi(0) = 0$, $\Phi(\infty) = \infty$. In particular we have that $\deg(f) > \deg(g)$. We use here the notation of the proof of Lemma 2.6, see in particular formula (3). Furthermore, we suppose K enlarged so that it contains all roots of the polynomials f, g and $\Phi^{(1)}$.

Let us suppose that Φ has not S.G.R. at v. This means that there exist $\beta_1 \in \Phi^{-1}(0)$ and $\beta_2 \in \Phi^{-1}(\infty)$ such that $\beta_1 \equiv \beta_2 \mod v$. Let us define $\beta_v \doteqdot (\beta_1)_v = (\beta_2)_v$. Note that it is not possible that β_v is ∞, by part 2) of Lemma 2.6. Since

$$(\Phi^{(1)})_v(x) = f_v'(x)g_v(x) - f_v(x)g_v'(x),$$

we have that β_v is a root of the polynomial $(\Phi^{(1)})_v$. Since Φ_v is separable, the polynomial $(\Phi^{(1)})_v$ is not zero. Thus any root of the polynomial $(\Phi^{(1)})_v$ is the reduction modulo v of a ramification point α_i of Φ. Since β_v is a root of $\Phi^{(1)}(x)$, it is equal to the reduction modulo v of one of the ramification points α_i. Clearly, $\alpha_i \neq \beta_1$ or $\alpha_i \neq \beta_2$. This contradicts 2) of Lemma 2.6.

We prove now that *b)* implies *a)*. Since K has characteristic 0, the Riemann-Hurwitz Formula in our situation becomes:

$$2 \deg \Phi - 2 = \sum_{P \in \mathbb{P}^1(\overline{\mathbb{Q}})} (e_P(\Phi) - 1). \tag{6}$$

Since the map Φ_v is separable, (6) holds for Φ_v. However, this map is defined over $k(v)$, a finite field with positive characteristic, so we could have wild ramification. Let R_{Φ_v} be the ramification divisor associated to the map Φ_v. By [7, Prop. 2.2] we have that

$$\deg \mathrm{R}_{\Phi_v} \geq \sum_{P \in \mathbb{P}^1(\overline{k(v)})} (e_P(\Phi_v) - 1).$$

Since Φ has S.G.R. at v, by Riemann-Hurwitz Formula we have

$$2 \deg \Phi - 2 = 2 \deg \Phi_v - 2 = \deg \mathrm{R}_{\Phi_v}. \tag{7}$$

For any ramification point P of Φ, the point $P_v \in \mathbb{P}^1(\overline{k(v)})$ (i.e. the reduction mod v of the point P) is a ramification point for Φ_v and the ramification index $e_{P_v}(\Phi_v)$ is equal or grater than the ramification index $e_P(\Phi)$. Furthermore, by the condition of the branch locus $\underline{\Phi(\mathcal{R}_\Phi) \text{ of } \Phi}$, if $Q_1, Q_2 \in \Phi(\mathcal{R}_\Phi)$ are distinct points, then also the points $(Q_1)_v, (Q_2)_v \in \mathbb{P}^1(\overline{k(v)})$ are distinct and by Lemma 2.5 the sets $(\Phi^{-1}(Q_1))_v$ and $(\Phi^{-1}(Q_2))_v$ are disjoint. Thus the following inequalities hold

$$\deg \mathrm{R}_{\Phi_v} \geq \sum_{P \in \mathbb{P}^1(\overline{k(v)})} (e_P(\Phi_v) - 1) \geq \sum_{P \in \mathbb{P}^1(\overline{\mathbb{Q}})} (e_P(\Phi) - 1).$$

If there exist two distinct ramification points $P_1, P_2 \in \mathcal{R}_\Phi$ such that $(P_1)_v = (P_2)_v$, then by the S.G.R. condition we have $(\Phi(P_1))_v = (\Phi(P_2))_v$ and by the condition on the branch locus the identity $\Phi(P_1) = \Phi(P_2)$ holds. In this situation the second inequality becomes strict:

$$\deg \mathrm{R}_{\Phi_v} \geq \sum_{P\in\mathbb{P}^1(\overline{k(v)})} (e_P(\Phi_v) - 1) > \sum_{P\in\mathbb{P}^1(\overline{\mathbb{Q}})} (e_P(\Phi) - 1)$$

which gives a contradiction with identities (6) and (7). □

3 Some examples

In this section we consider some cases in which the residue map is not separable, so that the main theorem cannot be applied directly. The following is an example in which the residue map is not separable and the implication *b*) ⇒ *a*) in Theorem 1.6 does not hold. The example also shows that the condition C.G.R. is not stable under composition of maps.

Example 3.1. The set of ramification points of the rational map $\Phi(x) = (x-1)^2$ is $\mathcal{R}_\Phi = \{\infty, 1\}$ and the branch locus is $\Phi(\mathcal{R}_\Phi) = \{\infty, 0\}$. The set of ramification points of $\Phi^2 = \Phi\circ\Phi$ is $\mathcal{R}_{\Phi^2} = \{\infty, 0, 1, 2\}$ and the branch locus is $\Phi^2(\mathcal{R}_{\Phi^2}) = \{\infty, 0, 1\}$. Therefore Φ has C.G.R. at all finite places v and Φ^2 does not have C.G.R. at 2. Given any finite place v, we have that Φ^2 has S.G.R. at v and any two distinct points of the branch locus of Φ^2 remain distinct after reduction modulo v. Therefore Theorem 1.6 does not apply to Φ^2 because it is inseparable modulo 2.

Proposition 3.2. *Let $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism defined over K of degree ≥ 2 such that $\Phi^{-1}(\Phi(R_\Phi)) = R_\Phi$ (e.g. a Galois cover). Then the following are equivalent:*

a) Φ has S.G.R and C.G.R. at v;

b) Φ_v is not constant and $\#\mathcal{R}_\Phi = \#(\mathcal{R}_\Phi)_v$.

Proof. We have just to prove that *b*) implies *a*). We remark that since $\Phi^{-1}(\Phi(R_\Phi)) = R_\Phi$ then condition *b*) is equivalent to conditions 1) and 2) of Lemma 2.6. Then by Lemma 2.6 end Remark 2.7 we obtain that Φ has C.G.R at v.

Now it is clear that Φ has S.G.R. at v using the hypothesis and Lemma 2.5. □

If the degree of the map is equal to 2, we have the following simple situation:

Proposition 3.3. *Let K be a number field, v a finite place of K and Φ a rational map of degree 2. Then:*

1. *If v does not lie above 2, then*

   $$\Phi \text{ has S.G.R. at } v \;\Leftrightarrow \Phi \text{ has C.G.R. at } v \text{ and } \Phi_v \text{ is not constant.}$$

2. *If v lies above 2, then the following are equivalent:*

i) Φ *has S.G.R. at* v *and* Φ_2 *factors through the relative Frobenius of* $\mathbb{P}^1_{O_v/2O_v}$*;*

ii) Φ *has C.G.R. at* v *and* Φ_v *is not constant.*

Remark 3.4. In the statement above, by Φ_2 we denote the restriction of Φ to the scheme ${\mathbb{P}^1}_{O_v/2O_v}$. We refer to [8, sec. 3.2.4] for the notion of the relative Frobenius.

Proof. The *if* part of the first case and $(ii) \Rightarrow (i)$ of the second case, except the sentence on the inseparability of Φ_2, follow from Proposition 3.2. If Φ has C.G.R by Lemma 2.4, we can assume that Φ is of the form ax^2. Then, if v is above 2, Φ_2 is purely inseparable.

Now let us suppose that Φ has S.G.R. at v. By Lemma 2.4 we can suppose that $\infty \in \mathcal{R}_\Phi$ and $\Phi(\infty) = \infty$. Therefore Φ has the form $ax^2 + bx + c$ with $a, b, c \in K$. By Proposition 3.2 we have only to check the condition on the ramification locus in order to prove that Φ has C.G.R at v. Since Φ has S.G.R. at v, then a is a v–unity and b, c are v–integers. The set of ramification points of Φ is:

$$\mathcal{R}_\Phi = \left\{ \infty, -\frac{b}{2a} \right\}.$$

Now, if v is not above 2, then $2a$ is a v-unity so that Φ has C.G.R. at v. If v is above 2 and Φ_2 is purely inseparable, then $2 \mid b$ are in O_v. Hence, also in this case Φ has C.G.R. at v. □

4 An application to arithmetical dynamics

As already remarked in the introduction, the notion of C.G.R. does not have a good behaviour with dynamical problems associated to a rational map.

The next example shows that the behaviour of the critical good reduction under iteration of a rational map can be truly bad. Indeed, we give an example of a rational map Φ defined over $\mathbb{Q}$ such that it does not exist a finite set S of valuations of $\overline{\mathbb{Q}}$ with the property that all iterates of Φ have C.G.R. at all finite valuations outside S.

Example 4.1. Consider the rational function $\Phi(x) = x(x-1)$. Its set of ramification points is $\mathcal{R}_\Phi = \{\infty, 1/2\}$ and its branch locus is $\Phi(\mathcal{R}_\Phi) = \{\infty, -1/4\}$. Hence the map Φ does not have C.G.R. only at 2. Let Φ^n be the n–th iterated map of Φ. We denote by $\mathcal{B}_n$ the branch locus of Φ^n, that is

$$\mathcal{B}_n = \Phi^n(\mathcal{R}_{\Phi^n}) = \bigcup_{i=1}^{n} \Phi^i(\mathcal{R}_\Phi) = \{\infty\} \cup \{\Phi^i(1/2) \mid 1 \le i \le n\}.$$

Note that the element $1/2$ is not a preperiodic point for Φ. Indeed we have

$$\Phi^i(1/2) = \frac{a_i}{2^i} \quad \text{for any index } i \ge 1$$

where the $a_i's$ are suitable odd integers. Therefore the sequence $\{\mathcal{B}_n\}$ of sets of elements in $\{\infty\} \cup \mathbb{Q}$ is strictly increasing. Let S be a finite fixed set of finite places of $\overline{\mathbb{Q}}$. Let p

be the minimum of the prime integers that are below a valuation not in S. Thus any set of elements in $\{\infty\} \cup \mathbb{Q}$ of cardinality bigger than $p+1$ has two distinct points that are equal modulo at least at one valuation outside S. Hence it does not exist a finite set S of valuation of $\overline{\mathbb{Q}}$ such that all iterates of Φ have C.G.R. at all finite valuations outside S.

If Φ is a rational map having C.G.R at a valuation v and Φ_v is separable, then, by Theorem 1.6, Φ has S.G.R. at v. Therefore it has good behaviour in a dynamical sense. The proof of Corollary 1.8 is a simple application of Theorem 1.6, Corollary B of [10] and Theorem 1 of [3].

In [10, Corollary B] Morton and Silverman proved that if Φ is a rational map of degree ≥ 2 which has good reduction outside a finite set S of valuations of K containing all the archimedean ones and $P \in \mathbb{P}^1(K)$ is a periodic point with minimal period n, then we have the inequality

$$n \leq [12(t+1)\log(5(t+1))]^{4[K:\mathbb{Q}]}$$

where $t = |S|$.

In [3, Theorem 1], Canci extended the Morton and Silverman's result to any finite orbit (so he considered also pre-periodic points). With the same hypothesis as in [10, Corollary B], the Canci's result says that there exists a number $c(t)$, depending only on t, such that the length of every finite orbit in $\mathbb{P}^1(K)$, for rational maps having good reduction outside S, is bounded by $c(t)$. The number $c(t)$ can be chosen to be equal to

$$\left[e^{10^{12}}(t+1)^8(\log(5(t+1)))^8\right]^t.$$

Proof of Corollary 1.8. Let Φ be an endomorphism of $\mathbb{P}^1$ as in the hypothesis of the corollary. For any prime integer $p \leq \deg \Phi$ we consider all valuations v_p over K which extend the valuation associate to p. We enlarge S adding all these valuations v_p for all $p \leq \deg \Phi$. The cardinality of the new set S depends only on t, the degree d of the map and the degree D of K over $\mathbb{Q}$. With this enlarged set S, for any $v \notin S$, the reduced map Φ_v is separable if and only if it is not constant. Therefore the map Φ has S.G.R. at any valuation outside S. We denote by $b(t,d,D)$ the lowest integer bigger than the Morton and Silverman's bound, which depends on the cardinality of the enlarged set S. There exists a bound $B(t,d,D)$ which bounds the cardinality of the set of K–rational periodic points of Φ. Indeed, any K–rational point is a fixed point for the map $\Phi^{b(t,d,D)!}$. Hence we can take $B(t,d,D) = b(t,d,D)! + 1$. By the Canci's Theorem 1 in [3] there exists a number, which depends only on the cardinality of the enlarged set S, that bounds the length of every finite orbit in $\mathbb{P}^1(K)$ for Φ. Since the cardinality of the enlarged set S depends only on t, d, D, also this bound depends only on t, d, D. We denote by $c(t,d,D)$ this number. Since the preimage of each point has at most d points, any K–rational periodic point of Φ is contained in at most $d^{c(t,d,D)}$ finite orbits. Thus we can take $C(t,d,D) = B(t,d,D)d^{c(t,d,D)}c(t,d,D)$. □

Any number depending on t, d, D in our proof could be not optimal. Our aim was to show the existence of a bound $C(t,d,D)$ and not to find an optimal limit.

References

[1] S. Beckmann. *Ramified Primes in the Field of Moduli of Branched Coverings of Curves*, J. Algebra 125 (1989), no. 1, 236-255.

[2] E. Bombieri, W. Gubler *Heights in Diophantine Geometry*, New Mathematical Monographs, 4, Cambridge University Press, 2006.

[3] J.K. Canci. *Finite orbits for rational functions*, Indag. Math. (N.S.), 18(2), 2007, 203-214.

[4] B. Dwork, P. Robba. *On natural radii of p–adic convergence*, Trans. Amer. Math. Soc. 256 (1979), 199-213.

[5] W. Fulton. *Hurwitz schemes and irreducibility of moduli algebraic curves*, Ann. of Math. (2) 90 1969 542-575.

[6] A. Grothendieck. *Géométrie formelle et géomérie algébrique*, Séminaire Bourbaki, exposé 182, 1958-9.

[7] R. Hartshorne. *Algebraic Geometry*, Springer-Verlag, GTM 52, 1977.

[8] Q. Liu. *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics, 2002.

[9] P. Morandi. *Field and Galois Theory*, Springer-Verlag, GTM 167, 1996.

[10] P. Morton, J.H. Silverman *Rational periodic points of rational functions*, Internat. Math. Res. Notices 1994, no. 2, 97-110.

[11] A. Quarteroni, R. Sacco and F. Saleri. *Numerical Mathematics* Second Ed., Springer-Verlag, 2007.

[12] I. R. Shafarevich. Algebraic Number Fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 163-176. Inst. Mittag-Leffler, Djursholm, 1963.

[13] J. H. Silverman. *The Arithmetic of Dynamical Systems*, Springer-Verlag, GTM 241, 2007.

[14] L. Szpiro, T. Tucker. *A Shafarevich-Faltings Theorem for Rational Functions.* Pure Appl. Math. Q., 4 (2008), no. 3, part 2, 715-728.

[15] U. Zannier. *On Davenport's bound for the degree $f^3 - g^2$ and Riemann's Existence Theorem*, Acta Arith. 71 (1995), no. 2, 107-137.

[16] U. Zannier. *On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$*, Arch. Math. 68 (1997), no. 2, 129-138.

[17] U. Zannier. *Good reduction for certain covers $\mathbb{P}^1 \to \mathbb{P}^1$*, Israel J. Math. 124 (2001), 93-114.