

Exceptional Covers and Bijections on Rational Points

Robert M. Guralnick¹, Thomas J. Tucker² and Michael E. Zieve³

¹Department of Mathematics, University of Southern California, Los Angeles, CA 90089–2532, USA, ²Department of Mathematics, Hylan Building, University of Rochester, Rochester, NY 14627, USA and ³Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540, USA

Correspondence to be sent to: Michael E. Zieve, Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540, USA. e-mail: zieve@idaccr.org

We show that if $f: X \rightarrow Y$ is a finite, separable morphism of smooth curves defined over a finite field \mathbb{F}_q , where q is larger than an explicit constant depending only on the degree of f and the genus of X , then f maps $X(\mathbb{F}_q)$ surjectively onto $Y(\mathbb{F}_q)$ if and only if f maps $X(\mathbb{F}_q)$ injectively into $Y(\mathbb{F}_q)$. Surprisingly, the bounds on q for these two implications have different orders of magnitude. The main tools used in our proof are the Chebotarev density theorem for covers of curves over finite fields, the Castelnuovo genus inequality, and ideas from Galois theory.

1 Introduction

Let X and Y be normal, geometrically irreducible varieties over \mathbb{F}_q , and let $f: X \rightarrow Y$ be a finite, generically étale \mathbb{F}_q -morphism. Then f is called an *exceptional cover* if the diagonal is the only geometrically irreducible component of the fiber product $X \times_Y X$ which is defined over \mathbb{F}_q .

The prototypical examples of exceptional covers are isogenies of abelian varieties, which are exceptional whenever zero is the only \mathbb{F}_q -rational point in the kernel. Other families of examples will be discussed in Section 5.

Received January 6, 2006; Revised January 10, 2007; Accepted January 11, 2007
Communicated by Bjorn Poonen

See http://www.oxfordjournals.org/our_journals/imrn/ for proper citation instructions.

© The Author 2007. Published by Oxford University Press. All rights reserved. For permissions, please e-mail: journals.permissions@oxfordjournals.org.

The primary interest of exceptional covers is that they induce bijections on rational points:

Theorem 1.1. If f is exceptional, then f maps $X(\mathbb{F}_q)$ bijectively onto $Y(\mathbb{F}_q)$. \square

This result is due to Lenstra (unpublished). Special cases and weaker versions were previously proved by Davenport and Lewis [1], MacCluer [2], Williams [3], Cohen [4], and Fried [5]–[7]. (See [8] for variants of this result over infinite constant fields.)

Note that, if f is exceptional over \mathbb{F}_q , then f is also exceptional over \mathbb{F}_{q^m} for infinitely many m . Thus, f induces a bijection $X(\mathbb{F}_{q^m}) \rightarrow Y(\mathbb{F}_{q^m})$ for infinitely many m . This unusual property is the most important feature of exceptional covers.

In the present article we show that this property characterizes exceptional covers. More precisely, we show (in Prop. 5.6) that f is exceptional if $X(\mathbb{F}_{q^m}) \rightarrow Y(\mathbb{F}_{q^m})$ is either injective or surjective for a single sufficiently large m . We can make this completely explicit in case $\dim X = 1$, where it suffices to test a single m larger than an explicit constant depending only on q , the genus of X , and the degree of f :

Theorem 1.2. Let X be a curve of genus g_X , and let n be the degree of f .

- (1) Suppose f maps $X(\mathbb{F}_q)$ injectively into $Y(\mathbb{F}_q)$, and $\sqrt{q} > 2n^2 + 4ng_X$. Then f is exceptional, and therefore bijective on rational points.
- (2) Suppose f maps $X(\mathbb{F}_q)$ surjectively onto $Y(\mathbb{F}_q)$, and $\sqrt{q} > n!(3g_X + 3n)$. Then f is exceptional, and therefore bijective on rational points. \square

Note that the bound in (1) is quite different from the bound in (2): the bound in (1) is a degree-2 polynomial in n , while the bound in (2) depends on $n!$. The reason we get such a better bound under the injectivity assumption is that injectivity is equivalent to the nonexistence of non-diagonal rational points on components of $X \times_Y X$, and these components have genus less than $n^2 + 2g_X n$. There seems to be no curve playing an analogous role for surjectivity, so we are forced to work on the Galois closure of $\mathbb{F}_q(X)/\mathbb{F}_q(Y)$, which may have genus on the order of $n!(g_X + 1)$. We do not know whether this phenomenon is indicative of the true situation, or merely an artifact of our proof. It is possible that there would be counterexamples to (2) if we replaced $n!$ by any polynomial in $\mathbb{Z}[n]$. However, we do not know any examples of non-exceptional maps f which are surjective on \mathbb{F}_q -points with $\sqrt{q} > 2n^2 + 4ng_X$.

Our proof of (1) uses the Weil lower bound on the number of rational points on a curve and Castelnuovo's bound on the arithmetic genus of curves in $X \times X$ to show that there are nondiagonal rational points in $X \times_Y X$ when $\sqrt{q} > 2n^2 + 4ng_X$. Our proof of (2) analyzes the decomposition and inertia groups of places of the Galois

closure of $\mathbb{F}_q(X)/\mathbb{F}_q(Y)$, using an analog of Chebotarev's density theorem to translate injectivity, surjectivity, and exceptionality into group-theoretic properties which are shown to be equivalent via purely group-theoretic arguments. This proof shows that, if $\sqrt{q} > n!(3g_X + 3n)$, then surjectivity and injectivity of f are equivalent to one another and to exceptionality. By contrast, our proof of (1) does not directly yield surjectivity of f (although surjectivity follows by combining (1) with Theorem 1.1).

Results along the lines of Theorem 1.2 were previously proved in the case $g_X = 0$, where of course injectivity and surjectivity are equivalent. Most previous work restricts further to the case where $g_X = 0$ and some point of $Y(\mathbb{F}_q)$ is totally ramified under f . In this case a noneffective version of our result was proved by Davenport and Lewis [1]. The best known effective version says that, if f is bijective on rational points and $q \geq n^4$, then f is exceptional [9, pp. 51–52] (see [10] for corrections to [9]). When $g_X = 0$ our result draws this conclusion under the assumption $q \geq 4n^4$; but it is easy to modify our argument to make use of the ramification assumption and recover the $q \geq n^4$ bound. The effective version of the Davenport-Lewis argument extends at once to the general case $g_X = 0$ (no longer assuming a totally ramified rational point), giving the bound $q \geq 16n^4$ [11]. Our result improves this to $q \geq 4n^4$.

We prove (1) in the next section, using an argument which is similar in spirit to that of Davenport and Lewis, although with several new ingredients to address difficulties new to the case $g_X > 0$. In Section 4 we prove (2) and Theorem 1.1, using a Galois-theoretic setup we learned from Lenstra. Our proof of (2) uses an analog of Chebotarev's density theorem, which we prove in Section 3. We conclude in Section 5 with some examples and conjectures.

Let us say a few words about the terminology in this article. Given a variety W over a field k and an extension k' of k , we let $W(k')$ denote the set of k' -morphisms from $\text{Spec } k'$ into W . In particular, $W(k)$ is the set of closed points of W with residue field k . Also \bar{k} denotes an algebraic closure of k . Throughout this article, all curves are assumed to be projective and geometrically integral. Not all curves are assumed to be smooth; some of the curves we work with in Section 2 may be singular.

2 Geometry

In this section we use a geometric approach. Our main result concerns maps and curves defined over the field \mathbb{F}_q . The first few propositions are valid over an arbitrary ground field k and are stated as such. Throughout this section, $f: X \rightarrow Y$ is a finite separable morphism between smooth curves, and f is defined over either k or \mathbb{F}_q depending on

context. We denote the geometric genus of a curve C as g_C and the arithmetic genus as $p_a(C)$. Finally, by 'component' we always mean geometric component.

Our first result shows that Castelnuovo's upper bound on the geometric genus of a curve on a split surface is also an upper bound on the arithmetic genus.

Proposition 2.1. Let C_1 and C_2 be smooth curves and let C' be a curve for which there is a generically injective map $\phi : C' \rightarrow C_1 \times_k C_2$. For $i = 1, 2$, let g_i be the genus of C_i , let π_i denote projection from $C_1 \times_k C_2$ onto its i -th factor, and let d_i be the degree of the map $\pi_i \circ \phi : C' \rightarrow C_i$. Then

$$p_a(\phi(C')) \leq (d_1 - 1)(d_2 - 1) + d_1 g_1 + d_2 g_2. \quad (2.1)$$

□

Proof. We use several results from [12, §V.1], which is the source of all references in this proof. For divisors D_1 and D_2 , denote the intersection pairing by $D_1.D_2$. By Thm. 1.1, this pairing is symmetric, additive, and depends only on the linear equivalence class of each D_i . Let F_i be a fiber of π_i . Since F_1 is linearly equivalent to any other (disjoint) fiber of π_1 , we have $F_1.F_1 = 0$. The adjunction formula (Prop. 1.5) implies $2g_2 - 2 = F_1.K$, where K is the canonical divisor on $C_1 \times_k C_2$. Next, ex. 1.5 says that $K.K = 8(g_1 - 1)(g_2 - 1)$, so $K.K = 2(F_1.K)(F_2.K)$. By ex. 1.9, K is numerically equivalent to $(2g_1 - 2)F_1 + (2g_2 - 2)F_2$.

Let $D = \phi(C')$. By ex. 1.9, $D.D \leq 2d_1 d_2$, so ex. 1.3 implies $2p_a(D) - 2 \leq 2d_1 d_2 + D.K$. Since $K \equiv (2g_1 - 2)F_1 + (2g_2 - 2)F_2$, we have $D.K = (2g_1 - 2)d_1 + (2g_2 - 2)d_2$. Thus

$$2p_a(D) - 2 \leq 2d_1 d_2 + (2g_1 - 2)d_1 + (2g_2 - 2)d_2,$$

and the desired result follows. ■

Write $Z = X \times_Y X$, and note that Z embeds naturally into $X \times_k X$ as the locus of points (P, Q) for which $f(P) = f(Q)$.

Proposition 2.2. Let $(P, Q) \in Z(\bar{k})$ be a point which lies in more than one component of Z . Then f is ramified at both P and Q . □

Proof. If f is unramified at P then f is étale at P , so f is smooth on an open subset U of X containing P . Since the projection $\pi_1 : Z \rightarrow X$ is obtained from f by base extension, it follows that $U \times_Y X$ is smooth over X (by [12, Prop. III.10.1]) and thus over k . This contradicts the fact that (P, Q) lies in multiple components. ■

Corollary 2.3. Let $f: X \rightarrow Y$ be a finite separable morphism of smooth curves and suppose that f is injective on $X(k)$. Then any component of $X \times_Y X$ other than the diagonal contains at most $(2g_X + 2 \deg f - 2)$ k -rational points. \square

Proof. Let D be a nondiagonal component of $Z = X \times_Y X$. Since f is injective on $X(k)$, every point in $Z(k)$ has the form (P, P) ; hence $D(k)$ lies in the support of the intersection of D with the diagonal. It follows that all points in $D(k)$ have the form (P, P) where f ramifies at P . By the Riemann-Hurwitz theorem, the number of such P is at most

$$2g_X - 2 - \deg f(2g_Y - 2) \leq 2g_X + 2 \deg f - 2.$$

This completes the proof. \blacksquare

Our next result generalizes the Weil bound for the number of \mathbb{F}_q -rational points on a smooth curve to the case of an arbitrary curve.

Proposition 2.4. For any curve C over \mathbb{F}_q , we have

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2p_a(C)\sqrt{q}. \quad \square$$

Proof. Let \tilde{C} be the normalization of C . Then \tilde{C} is regular (by [13, Thm. 11.2]) and therefore smooth (by [13, Thms. 25.2 and 25.3]). The normalization map $\tilde{C} \rightarrow C$ is an isomorphism away from at most $p_a(C) - g_C$ points of \tilde{C} , so

$$|\#\tilde{C}(\mathbb{F}_q) - \#C(\mathbb{F}_q)| \leq p_a(C) - g_C.$$

Since \tilde{C} is smooth, we also have [14]

$$|\#\tilde{C}(\mathbb{F}_q) - q - 1| \leq 2g_C\sqrt{q}.$$

Our result follows. \blacksquare

Theorem 2.5. Let $f: X \rightarrow Y$ be a finite separable morphism of degree $n \geq 2$ between smooth curves over \mathbb{F}_q . Suppose that f induces an injection from $X(\mathbb{F}_q)$ into $Y(\mathbb{F}_q)$ and that

$$\sqrt{q} > 2(n-2)^2 + 4(n-1)g_X + 1. \quad (2.2)$$

Then f is exceptional. \square

Proof. We argue by contradiction. Suppose that f is not exceptional. Then there exists a non-diagonal geometric component C of $X \times_Y X$ that is defined over \mathbb{F}_q . Since the projection maps from $X \times_Y X$ onto X are generically n -to-1, one sees that the projection maps restricted to C are generically at most $(n - 1)$ -to-1 (since the diagonal is also a component of $X \times_Y X$). Proposition 2.1 implies that $p_a(C) \leq (n - 2)^2 + 2g_X(n - 1)$. Now Proposition 2.4 gives

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a(C)\sqrt{q} \geq q + 1 - 2((n - 2)^2 + 2g_X(n - 1))\sqrt{q}.$$

On the other hand, by Corollary 2.3 we have $\#C(\mathbb{F}_q) \leq 2g_X + 2n - 2$. Finally, it is easily checked that (2.2) implies

$$q + 1 - 2((n - 2)^2 + 2g_X(n - 1))\sqrt{q} - (2g_X + 2n - 2) > 0,$$

so we have our contradiction. ■

Remark 2.6. The proof of Theorem 2.5 can be modified to work under the weaker hypothesis that f is injective over non-branch points of Y . Injectivity is used only in Corollary 2.3; since this weaker hypothesis still implies that if (P, Q) is a k -rational point on $X \times_Y X$ then $f(P) = f(Q)$ is a branch point of f , we can replace the bound $(2g_X + 2 \deg f - 2)$ from Cor. 2.3 with the bound $(2g_X + 2 \deg f - 2)(\deg f - 1)$. This enlarges the bound (2.2) slightly (adding 2 to the right hand side is sufficient), but otherwise the reasoning is identical.

3 Chebotarev

In this section we prove analogs of Chebotarev's density theorem for normal varieties over a finite field, which we apply in the next two sections.

Let R be a commutative ring, and let A be a group of automorphisms of R . We denote the fixed ring R^A as B , and we say that R is a Galois extension of B . For a single element $a \in A$ we write R^a instead of $R^{(a)}$. Fix a prime \mathcal{Q} in R lying over a prime \mathcal{P} in B , and let $D = D(\mathcal{Q}/\mathcal{P})$ and $I = I(\mathcal{Q}/\mathcal{P})$ denote the decomposition and inertia groups at \mathcal{Q} . If \mathcal{J} is a prime ideal in the commutative ring Z , we write $m_{\mathcal{J}}$ for the field of fractions of Z/\mathcal{J} .

The following result is standard and easy (e.g. see [15, Thm. 2, p. 331]).

Lemma 3.1. Suppose that $m_{\mathcal{P}}$ is perfect. Then

- (1) A is transitive on the set of primes of R lying over \mathcal{P} ;

- (2) $m_{\mathcal{Q}}/m_{\mathcal{P}}$ is a finite Galois extension of degree $[D : I]$; and
 (3) $D/I \cong \text{Gal}(m_{\mathcal{Q}}/m_{\mathcal{P}})$. □

The next result is also known (e.g. see [16]), but we include a proof for the sake of completeness. Let H be a subgroup of A , let $U = R^H$, and let \mathcal{S} be the set of left cosets of H in A . We may view A as a group of permutations of the set \mathcal{S} .

Lemma 3.2. The number of primes $\mathcal{J} \subset U$ lying over \mathcal{P} such that $m_{\mathcal{J}} = m_{\mathcal{P}}$ is equal to the number of common orbits of D and I on \mathcal{S} . In particular, if $I = 1$ then the number of primes $\mathcal{J} \subset U$ lying over \mathcal{P} such that $m_{\mathcal{J}} = m_{\mathcal{P}}$ is equal to the number of fixed points of D on \mathcal{S} . □

Proof. For $a \in A$, let $\mathcal{Q}' = a^{-1}\mathcal{Q}$ and $\mathcal{J} = \mathcal{Q}' \cap U$. Since $H \cap a^{-1}Da$ and $H \cap a^{-1}Ia$ are the decomposition and inertia groups for \mathcal{Q}' over \mathcal{J} , we have

$$[m_{\mathcal{J}} : m_{\mathcal{P}}] = \frac{[m_{\mathcal{Q}'} : m_{\mathcal{P}}]}{[m_{\mathcal{Q}'} : m_{\mathcal{J}}]} = \frac{[a^{-1}Da : a^{-1}Ia]}{[H \cap a^{-1}Da : H \cap a^{-1}Ia]}.$$

Using the fact that $|H \cap a^{-1}Ma| = |M||H|/|MaH|$ for any subgroup M of G , we thus obtain

$$[m_{\mathcal{J}} : m_{\mathcal{P}}] = [D : I] \cdot \frac{|DaH|}{|D||H|} \cdot \frac{|I||H|}{|IaH|} = \frac{|DaH|}{|IaH|},$$

which is equal to 1 if and only if DaH is a common orbit of D and I .

For $b \in A$, we have $(b^{-1}\mathcal{Q}) \cap U = \mathcal{J}$ if and only if $DaH = DbH$. Thus, we achieve the desired result by summing over all orbits DbH of D on \mathcal{S} . ■

Let W be a normal variety over the finite field k , and let V be a normal variety over a finite extension ℓ of k . Let $\rho : V \rightarrow W$ be a finite, generically étale map of k -schemes. Write K and L for the fields of rational functions on W and V , so that ρ induces an inclusion $K \hookrightarrow L$. Assume that L/K is Galois, and put $A = \text{Gal}(L/K)$ and $G = \text{Gal}(L/K.\ell)$ (here $K.\ell$ denotes the compositum of K and ℓ in L). Then $A/G \cong \text{Gal}(\ell/k)$ is cyclic. Pick $a \in A$ with $\langle aG \rangle = A/G$. Let t be an extension of k such that $[t : k] = \#\langle a \rangle$. Note that t contains ℓ . Pick an automorphism \tilde{a} of the compositum $L.t$ such that $\tilde{a}|_L = a$ and $t^{\tilde{a}} = k$; such an automorphism exists because $\ell^a = k$. Then $(L.t)^{\tilde{a}} \supseteq R_i^a \supseteq B_i$, and k is algebraically closed in $(L.t)^{\tilde{a}}$.

Galoisness of L/K implies that $V^A = W$, in the sense that W admits an affine cover $M_i = \text{Spec } B_i$ such that $\rho^{-1}(M_i) = \text{Spec } R_i$ and $R_i^A = B_i$. Then each R_i is normal, so each B_i is as well ([15, V.1.9]). Furthermore, R_i is the integral closure of B_i in L since R_i is normal and integral over B_i . The ring $T_i = R_i.t$ is mapped to itself by \tilde{a} . Let V_t be the variety

obtained from V by base-extension from ℓ to t , and let $V_t^{\bar{a}}$ be the quotient variety of V_t obtained by piecing together the fixed rings $T_i^{\bar{a}}$.

The degree of the field $L.t$ over the field of fractions of $T_i^{\bar{a}}$ is equal to $\#\langle \bar{a} \rangle = \#\langle a \rangle = [t : k]$, so $T_i^{\bar{a}}.t$ has field of fractions $L.t$. Now, $T_i^{\bar{a}}.t$ and T_i are both normal, because R and $T_i^{\bar{a}}$ are normal ([17, 6.7.4]). Both T_i and $T_i^{\bar{a}}.t$ are integral over $T_i^{\bar{a}}$ as well, so we must have $T_i = T_i^{\bar{a}}.t$. Since T_i is a finite Galois extension of both $T_i^{\bar{a}}$ and $B_i.t$, it is also a finite Galois extension of $T_i^{\bar{a}} \cap B_i.t = B_i$.

We define the degree of a maximal ideal \mathcal{J} in any of the rings $B, R, T_i, T_i^{\bar{a}}$ to be $[m_{\mathcal{J}} : k]$. Let $J \in V_t^{\bar{a}}(k)$ and let \mathcal{J} be the corresponding degree one maximal ideal in some $T_i^{\bar{a}}$. Then $T_i/T_i\mathcal{J} \cong k \otimes_{\ell} t \cong t$, so $T_i\mathcal{J}$ is the unique prime in T_i lying over \mathcal{J} . Thus, the map $\phi_i : \mathcal{J} \mapsto T_i\mathcal{J} \cap R_i$ gives a well-defined map from degree one maximal ideals in $T_i^{\bar{a}}$ to maximal ideals in R_i .

Lemma 3.3. Let \mathcal{Q} be a maximal ideal in R_i that lies over a degree-one maximal ideal \mathcal{P} of B_i . If $\langle aI(\mathcal{Q}/\mathcal{P}) \rangle = D(\mathcal{Q}/\mathcal{P})/I(\mathcal{Q}/\mathcal{P})$, then there are exactly $[m_{\mathcal{Q}} : \ell]$ degree one maximal ideals $\mathcal{J} \in T_i^{\bar{a}}$ such that $\phi_i(\mathcal{J}) = \mathcal{Q}$. Otherwise, there are no degree one maximal ideals $\mathcal{J} \in T_i^{\bar{a}}$ such that $\phi_i(\mathcal{J}) = \mathcal{Q}$. \square

Proof. Suppose that $\langle aI(\mathcal{Q}/\mathcal{P}) \rangle = D(\mathcal{Q}/\mathcal{P})/I(\mathcal{Q}/\mathcal{P})$. Since $a\mathcal{Q} = \mathcal{Q}$, we must have $\bar{a}T_i\mathcal{Q} = T_i\mathcal{Q}$. Thus \bar{a} acts on $T_i/T_i\mathcal{Q} \cong m_{\mathcal{Q}} \otimes_{\ell} t$ by acting as a acts on $m_{\mathcal{Q}}$ and as \bar{a} acts on ℓ . The primes in T_i lying over \mathcal{Q} correspond to the primes in $m_{\mathcal{Q}} \otimes_{\ell} t$. Now, since a generates $\text{Gal}(m_{\mathcal{Q}}/k)$ and \bar{a} generates $\text{Gal}(t/k)$, there is a map $\psi : m_{\mathcal{Q}} \hookrightarrow t$ such that $\psi(ax) = \bar{a}\psi(x)$. Then the $[m_{\mathcal{Q}} : \ell]$ primes in $m_{\mathcal{Q}} \otimes_{\ell} t$ correspond to the kernels of the maps $p_j : m_{\mathcal{Q}} \otimes_{\ell} t \rightarrow t$ given by $p_j(u \otimes v) = (\psi(a^{[\ell:k]j}u)v)$ for $0 \leq j \leq [m_{\mathcal{Q}} : \ell] - 1$. Since the kernel of p_j is the set of all $\sum_n (u_n \otimes v_n)$ such that $\sum_n \psi(a^{[\ell:k]j}u_n)v_n = 0$, the kernel of p_j is preserved by the action of \bar{a} , so $\bar{a}\mathcal{Q}' = \mathcal{Q}'$ for all \mathcal{Q}' lying over \mathcal{Q} . Writing $\mathcal{J} = \mathcal{Q}' \cap T_i^{\bar{a}}$, we then have $\langle \bar{a} \rangle = D(\mathcal{Q}'/\mathcal{J})$ since T_i is unramified over $T_i^{\bar{a}}$. For each of these $[m_{\mathcal{Q}} : \ell]$ maximal ideals \mathcal{J} , we have $\phi_i(\mathcal{J}) = \mathcal{Q}$.

Now, suppose that $\langle aI(\mathcal{Q}/\mathcal{P}) \rangle \neq D(\mathcal{Q}/\mathcal{P})/I(\mathcal{Q}/\mathcal{P})$. Let \mathcal{Q}' be a maximal ideal in T_i such that $\mathcal{Q}' \cap R_i = \mathcal{Q}$ and let $\mathcal{J} = \mathcal{Q}' \cap T_i^{\bar{a}}$. If $a \notin D(\mathcal{Q}/\mathcal{P})$, then $\bar{a}\mathcal{Q}' \neq \bar{a}\mathcal{Q}'$, so there is more than one prime in T_i lying over \mathcal{J} , which means that \mathcal{J} cannot have degree one. If $a \in D(\mathcal{Q}/\mathcal{P})$ but does not generate $D(\mathcal{Q}/\mathcal{P})/I(\mathcal{Q}/\mathcal{P})$, then $\mathcal{Q} \cap R_i^a$ has degree greater than one, by (3) of Lemma 3.1, so \mathcal{J} does also, since \mathcal{J} lies over $\mathcal{Q} \cap R_i^a$. \blacksquare

If Q and P are closed points of V and W with $\rho(Q) = P$, we denote the decomposition and inertia groups of Q over P as $D(Q/P)$ and $I(Q/P)$, respectively. Clearly, these are the same as $D(\mathcal{Q}/\mathcal{P})$ and $I(\mathcal{Q}/\mathcal{P})$ where \mathcal{Q} is a prime in some R_i corresponding to Q and \mathcal{P} is a prime in B_i such that $\mathcal{Q} \cap B_i = \mathcal{P}$. Similarly, we define $m_{\mathcal{Q}}$ to be $m_{\mathcal{Q}}$.

Proposition 3.4. With notation as above,

$$\sum_{P \in W(k)} \sum_{\substack{\rho(Q)=P \\ \langle aI(Q/P) \rangle = D(Q/P)}} [m_Q : \ell] = \#V_t^{\tilde{a}}(k) \quad (3.1)$$

where $I(Q/P)$ is the inertia group of Q over P . □

Proof. The maps ϕ_i patch together to form a map ϕ from $J(k)$ to closed points in V ; indeed if we let ϕ be the map that takes a point $J \in W_t^{\tilde{a}}(k)$ to the closed point Q of W lying under the unique closed point of W_t that lies over J , then ϕ agrees with ϕ_i on each affine piece $\text{Spec } W_t^{\tilde{a}}$. The proposition thus follows from Lemma 3.3. ■

Corollary 3.5. Suppose that V and W are nonsingular and projective. Let $r = \dim V$ and let b_0, \dots, b_{2r} be the Betti numbers (see [12, p. 451 and 456]) of V . Then

$$\left| \left(\sum_{P \in W(k)} \sum_{\substack{\rho(Q)=P \\ \langle aI(Q/P) \rangle = D(Q/P)}} [m_Q : \ell] \right) - (\#k)^r \right| \leq \left| \sum_{i=0}^{2r-1} (-1)^i b_i (\#k)^{i/2} \right| \quad \square$$

Proof. Since $T_i^{\tilde{a}} \cdot t = T_i$ on each affine piece $\text{Spec } T_i$ of V_t , we see that $V_t^{\tilde{a}}$ with the base extended from k to t is isomorphic to V_t (i.e., $(V_t^{\tilde{a}})_t \cong V_t$). Thus, $V_t^{\tilde{a}}$ is also nonsingular ([17, 6.7.4]), and V , V_t , and $V_t^{\tilde{a}}$ all have the same Betti numbers. Thus, applying the Weil bound ([18], see also [12, Appendix 3] for an overview) to $V_t^{\tilde{a}}(k)$ in (3.1) gives the desired result. ■

Proposition 3.4 also gives rise to a generalization of the effective Chebotarev density theorem for curves that Murty and Scherk proved in [19] (see also [9, Chapter 5]). Let \mathcal{V} denote the set of all unramified points in $V(\bar{\ell})$ that lie over points in $W(k)$; let \mathcal{V}_a denote the set of all points in \mathcal{V} that correspond to closed points Q of V such that $I(Q/\rho(Q))$ is trivial and $\langle a \rangle = D(Q/\rho(Q))$. Note that counting points in $V(\bar{\ell})$ is different from counting closed points; each closed point Q on V corresponds to $[m_Q : \ell]$ distinct points in $V(\bar{\ell})$.

Corollary 3.6. Suppose that V and W are nonsingular and projective. Let $r = \dim V$, let b_0, \dots, b_{2r} be the Betti numbers of V , let c_0, \dots, c_{2r} be the Betti numbers of W , and let U

be the ramification locus of ρ in W (thought of as a subscheme of W). Then

$$\begin{aligned} \left| \#\mathcal{V}_a - \frac{\#\mathcal{V}}{\#G} \right| &\leq (\#G)(\#U(k)) + \left| \sum_{i=0}^{2r-1} (-1)^i b_i(\#k)^{i/2} \right| \\ &\quad + \left| \sum_{i=0}^{2r-1} (-1)^i c_i(\#k)^{i/2} \right|. \end{aligned} \tag{3.2}$$

□

Proof. If $I(Q/P)$ is trivial then ρ does not ramify at Q , so Q does not lie over a point in the ramification locus of ρ . As noted above, each such Q corresponds to $[m_Q : \ell]$ points in \mathcal{V}_a . Letting \mathcal{U}_a denote the set of $J \in V_t^{\bar{a}}(k)$ lying over points in $U(k)$ and applying Proposition 3.4, we obtain $\#\mathcal{V}_a = \#V_t^{\bar{a}}(k) - \#\mathcal{U}_a$. Since the degree of $V_t^{\bar{a}}$ over W is $\#G$, we have $\#\mathcal{U}_a \leq (\#G)(\#U(k))$. Thus, the Weil bound for $V_t^{\bar{a}}(k)$ yields

$$\begin{aligned} (\#k)^r - \left| \sum_{i=0}^{2r-1} (-1)^i b_i(\#k)^{i/2} \right| - (\#G)(\#U(k)) \\ \leq \#\mathcal{V}_a \\ \leq (\#k)^r + \left| \sum_{i=0}^{2r-1} (-1)^i b_i(\#k)^{i/2} \right|. \end{aligned} \tag{3.3}$$

Similarly, we obtain

$$\begin{aligned} (\#G) \left((\#k)^r - \left| \sum_{i=0}^{2r-1} (-1)^i c_i(\#k)^{i/2} \right| - (\#U(k)) \right) \\ \leq \#\mathcal{V} \\ \leq (\#G) \left((\#k)^r + \left| \sum_{i=0}^{2r-1} (-1)^i c_i(\#k)^{i/2} \right| \right), \end{aligned} \tag{3.4}$$

by using the Weil bound for $W(k)$. Dividing (3.4) by $\#G$ and subtracting it from (3.3) yields (3.2). ■

Remark 3.7. When V and W are smooth curves, Corollary 3.6 is a slight improvement of [19, Theorem 1]. Note that in this case, the ramification locus corresponds to a finite set of points in $W(\bar{k})$. To make Corollary 3.6 completely explicit in the higher-dimensional case, one must use bounds on $U(k)$ (such as those that come from applying the Weil bounds to desingularizations of the components of U , for example).

Recall that g_C denotes the genus of a curve C .

