ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 8–14
ISSN: 1930-1235; (**2018**)

THE *abc* CONJECTURE IMPLIES THE WEAK DIVERSITY CONJECTURE

HILAF HASSON

University of Maryland,
College Park, MD 20742, USA

ANDREW OBUS

University of Virginia,
Charlottesville, VA 22904, USA

Abstract. We show that the *abc* Conjecture implies the Weak Diversity Conjecture of Bilu and Luca. In addition, we unconditionally reduce the Weak Diversity Conjecture to the case of cyclic covers of prime order.

MSC 2010: Primary: 11G30, 14G25; Secondary: 14H25, 14H30
Keywords: Hilbert irreducibility theorem, rational points

1. Introduction

This note concerns the Weak and Strong Diversity Conjectures. The Strong Diversity conjecture, due to Andrzej Schinzel, first appeared in [DZ], in the discussion following Theorem 2 of that paper. (The name "Strong Diversity" first appeared in [BL], as Conjecture 1.5.) Recall that a geometrically irreducible branched cover of curves over a number field is one where both the source and the target are irreducible after base change to $\overline{\mathbb{Q}}$.

Conjecture 1.1. *("Strong Diversity") Let $X \to \mathbb{A}^1_{\mathbb{Q}}$ be a geometrically irreducible branched cover of curves over $\mathbb{Q}$, such that not all of its branch points are $\mathbb{Q}$-rational, or such that the cover is not abelian. Let $k(N)$ be the compositum of the fields of rationality of the points in the fibers over $x = 1, ..., N$. Then there exists a positive constant c, independent of N, such that the degree of $k(N)$ over $\mathbb{Q}$ is at least e^{cN}.*

E-mail addresses: hilaf@math.umd.edu, andrewobus@gmail.com.
Date: Received: June 15, 2018. Accepted: July 15, 2018.
The second author was supported by NSF grant DMS-1602054.

We note that the hypotheses in the above conjecture are necessary, and we refer the reader to [DZ] for further discussion. The Strong Diversity Conjecture is closely related to the "Weak Diversity Conjecture" (Conjecture 1.4 in [BL]), which is itself an extension of a conjecture of Cutter, Granville, and Tucker ([CGT, Conjecture 1]).

Conjecture 1.2. *("Weak Diversity") Let K be a number field, and let $X \to \mathbb{A}^1_K$ be a non-trivial geometrically irreducible branched cover of curves over K. Then there exists a positive constant c such that the number of different fields appearing as residue fields of the points in the fibers over $x = 1, ..., N$ is at least cN for all N.*

We remark that the Weak Diversity Conjecture was only stated in [BL] for $K = \mathbb{Q}$, but we, in fact, prove the more general form of Conjecture 1.2 under the assumption of the *abc* Conjecture. Note also that for $K = \mathbb{Q}$, the consequence of Conjecture 1.1 implies the consequence of Conjecture 1.2. The hypotheses of Conjecture 1.2, however, are weaker. In [BL], Bilu and Luca prove Weak Diversity (for $K = \mathbb{Q}$) in the case not covered by Strong Diversity, namely for covers where the branch points are $\mathbb{Q}$-rational, and the cover is abelian. They therefore conclude that Strong Diversity implies Weak Diversity for $K = \mathbb{Q}$.

Remark 1.3. The Weak and Strong Diversity Conjectures were stated in [BL] in terms of residue fields of a *given* point in each fiber. In light of the quantitative version of Hilbert's Irreducibility Theorem ([S, Theorem, p. 134]), all fibers except negligibly many have only one point. So the formulations of [BL] are equivalent to our formulations above. For Weak Diversity, it would also be equivalent to look at the *compositum* of the residue fields of all points in each fiber. We use this formulation in Propositions 3.2 and 3.3.

While this was not mentioned in earlier discussions of this conjecture, we remark that the Weak Diversity Conjecture is also closely related to the following conjectural form of a uniform Faltings' Theorem (although we are not aware of any clear connection between the *abc* conjecture and this uniform Faltings' theorem beyond the fact that the *abc* conjecture implies the basic Faltings' theorem [E]). This form first appeared in [P], where Pacelli proves this conjecture under the assumption of Lang's conjecture about rational points on varieties of general type; see also [CHM].

Conjecture 1.4. *("Uniform Faltings' Theorem") Let $g \geq 2$ and d be natural numbers. Then there exists a constant $B_{d,g}$ such that for every number field L of degree d over $\mathbb{Q}$, and for every curve X of genus g over L, we have that $\#X(L) \leq B_{d,g}$.*

As we will soon see (Proposition 3.2), the Weak Diversity Conjecture can be reduced to the case of G-Galois covers $f : X \to \mathbb{A}^1_K$. In the Galois case, Conjecture 1.4 implies Weak Diversity for $g(X) \geq 2$, which will be shown in §5. In this way, Weak Diversity can be viewed as a weaker form of Conjecture 1.4 that, unlike Conjecture 1.4, also applies to genera 0 and 1. Note that Conjecture 1.4 is not even known for twists of a given curve; see related results in this direction in [S1] and [S2].

Strong Diversity is known in either of two cases: (a) when one of the branch points is of degree either 2 or 3 above $\mathbb{Q}$ ([DZ, Theorem 2(b)]), or (b) if the branch points are all $\mathbb{Q}$-rational and the normal closure of $X \to \mathbb{A}^1_{\mathbb{Q}}$ satisfies some condition (for example if its Galois group is either alternating, symmetric or non-abelian

simple group of non-square order; see [DZ]). Weak Diversity (but not Strong Diversity) was also proven ([CZ, Corollary 1]) in the case that X has at least 3 geometric points above ∞. See also Proposition 3.4, and preliminary discussion thereof, in this paper. We also remark that in [D], Dèbes proves a version of the strong diversity conjecture where one looks at fibers over $n+1, \ldots, n+N$ for some n depending on N.

In this paper we reduce Weak Diversity to the case of a cyclic Galois cover. As a consequence, we show that the *abc* Conjecture (for an appropriate number field) implies Weak Diversity (Theorem 4.2 — although this can be proven without our reduction, see Remark 4.4). We also show that *abc* implies Strong Diversity for the case that not all branch points are $\mathbb{Q}$-rational (Theorem 2.2).

We mention that Mochizuki claims to have proven the Vojta conjecture for all curves over number fields ([M, Discussion after Theorem A]), which implies the *abc* Conjecture over number fields. If Mochizuki's proof is verified, then Weak Diversity will hold unconditionally.

ACKNOWLEDGEMENTS

The authors thank Larry Washington for fruitful conversations, and Andrew Granville, Ram Murty and Taylor Dupuy for very thorough and helpful answers to their mathematical inquiries. They also thank Pierre Dèbes for useful comments.

2. PROOF OF THE NON-RATIONAL BRANCH POINT CASE OF STRONG DIVERSITY GIVEN *abc*

As was mentioned above, Dvornicich and Zannier proved Strong Diversity for $f : X \to \mathbb{A}^1_{\mathbb{Q}}$ whenever f has a branch point of index 2 or 3. Combining the *abc* Conjecture with a result of Granville allows us to weaken this assumption to f having a branch point not defined over the base field.

Lemma 2.1. *Assume the abc Conjecture. Then*

$$n = O(\#\{p \geq n \mid v_p(g(m)) = 1 \text{ for some } m \leq n\})$$

whenever $g \in \mathbb{Z}[x]$ is an irreducible polynomial of degree at least 2. If $\deg g \in \{2, 3\}$, then the abc Conjecture is not required.

Proof. By [DZ, Eq. (1) on p. 427], the lemma is true unconditionally if $v_p(g(m)) = 1$ is replaced by $p \mid g(m)$. So it suffices to show that

$$\#\{p \geq n \mid v_p(g(m)) > 1 \text{ for some } m \leq n\} = o(n).$$

If $\deg g \in \{2, 3\}$, this follows as on [DZ, p. 427], without the *abc* Conjecture. In any case, if $\deg g \geq 3$, this follows from [G, Theorem 8] applied to the homogenization of g, taking $N = n$ and $M = 1$. □

Theorem 2.2. *Suppose that the branch locus Δ of $f : X \to \mathbb{A}^1_{\mathbb{Q}}$ contains a point of degree ≥ 2 over $\mathbb{Q}$, and that the abc Conjecture is true. Then Strong Diversity holds for f.*

Proof. Let X' be a plane curve such that $X \dashrightarrow X' \xrightarrow{f'} \mathbb{A}^1_{\mathbb{Q}}$ is a factorization of f as a rational map with $X \dashrightarrow X'$ birational. To prove Strong Diversity for f, it suffices to prove it for f'.

Since X' is a plane curve, we are in the situation of [DZ]. If Δ has a point of degree 2 or 3 over $\mathbb{Q}$, then this is [DZ, Theorem 2(b)]. The only input to the proof in [DZ] that requires Δ to have a point of degree 2 or 3 is the result of Lemma 2.1 for some irreducible factor g of a polynomial cutting out Δ (see [DZ, (11), p. 437]). By our assumptions on Δ, there is such a factor of degree ≥ 2. Since we assume the *abc* Conjecture, the proposition follows from Lemma 2.1. □

3. Unconditional reduction of Weak Diversity to cyclic case

In this section, we reduce Weak Diversity to the case of cyclic covers of prime order. We do not assume the *abc* Conjecture.

Lemma 3.1. *If a cover $f : X \to \mathbb{A}^1_{K_0}$ is defined over a number field K_0, then Weak Diversity for f is equivalent to Weak Diversity for any base change f_K over a number field extension K/K_0.*

Proof. The residue field of a point in $f_K^{-1}(n)$ is the compositum of the residue field of the corresponding point of $f^{-1}(n)$ with K. If two number fields have distinct composita with K, they must be distinct. On the other hand, given a number field L, there are only finitely many distinct number fields whose compositum with K is L. The lemma follows. □

Proposition 3.2. *Suppose that $f : X \to \mathbb{A}^1_K$ is a cover defined over a number field K and L/K is a finite extension for which the Galois closure $f' : X' \to \mathbb{A}^1_L$ of the base-change f_L of f to L is geometrically irreducible and defined over L as a Galois cover. Then to prove Weak Diversity for f, it suffices to prove it for f'.*

Proof. By Lemma 3.1, we may assume that $L = K$ and $f_L = f$. Let L_n (resp. L'_n) be the field generated by the residue fields of the points of $f^{-1}(n)$ (resp. $(f')^{-1}(n)$). We note that L'_n is Galois over K and is contained in the Galois closure of L_n over K. So L'_n is the Galois closure of L_n over K. So if $L'_i \neq L'_j$, then $L_i \neq L_j$. Thus Weak Diversity for f' implies Weak Diversity for f. □

Proposition 3.3. *Suppose $f : X \to \mathbb{A}^1_K$ is a quotient cover of $g : Y \to \mathbb{A}^1_K$. Then Weak Diversity is true for g if it is true for f.*

Proof. Let L_n (resp. L'_n) be the field generated by the residue fields of the points of $f^{-1}(n)$ (resp. $g^{-1}(n)$). Then $L_n \subseteq L'_n$ and the degree of L'_n over the base field is bounded in terms of g, which means that there exists $d \in \mathbb{N}$ such that each L'_i can correspond to at most d non-isomorphic L_js. So if the number of distinct L'_n for $n \leq N$ is at least cN, then the number of distinct L_n for $n \leq N$ is at least cN/d. □

Proposition 3.4 below was stated in [BL] as a consequence of [CZ, Corollary 1], but we supply some more details on the proof here. Recall that if L is a number field and S is a finite set of places containing the archimedean places, then $\mathcal{O}_{L,S} \subset L$ is the subring of L consisting of elements whose valuations at all places outside of S are nonnegative.

Proposition 3.4. *Let $f : X \to \mathbb{A}^1_{K_0}$ be a branched cover defined over a number field K_0. If the smooth projective completion of f has at least three $\overline{\mathbb{Q}}$-points over ∞, then Weak Diversity holds for f.*

Proof. Embed $X \subset \mathbb{A}^m_{K_0}$ as an affine curve. If K/K_0 is a finite extension and S is a finite set of places of $\mathcal{O}_K$ including the archimedean places, [CZ, Corollary 1] implies that the number of $\mathcal{O}_{K,S}$-integral points of X is bounded in terms of the degree of K and the cardinality of S. Now, since the ring extension $K_0[X]/K_0[t]$ corresponding to f is generated by roots of finitely many monic polynomials over K_0, there is a finite set of places S_0 of K_0 such that the same is true for $\mathcal{O}_{K_0,S_0}[X]/\mathcal{O}_{K_0,S_0}[t]$. Taking S to be the set of places of K lying above S_0, we see that every K-point of X lying above an $\mathcal{O}_{K_0,S_0}$-point of $\mathbb{A}^1_{\mathcal{O}_{K_0,S_0}}$ is in fact an $\mathcal{O}_{K,S}$-point. Thus, the number of such points is bounded solely in terms of the degree of K.

Since any field L arising as the residue field of a point of $f^{-1}(n)$ for $n \in \mathbb{N}$ has degree at most $\deg(f)$ over K_0, there is an absolute bound, depending only on f, on the number of such points with residue field L. This immediately implies Weak Diversity for f. □

Proposition 3.5. *To prove Weak Diversity for a cover defined over a number field with a given branch locus Δ, it suffices to prove it for cyclic covers of prime order with branch locus contained in Δ.*

Proof. By Lemma 3.1 and Proposition 3.2, we may assume the cover is Galois for some group G. If the cover has at least three $\overline{\mathbb{Q}}$-points defined over ∞, then the proposition follows from Proposition 3.4, so assume there are at most two such points. Then the stabilizer of one of these points is a cyclic group of index at most 2 in G. So either G is cyclic or G has $\mathbb{Z}/2$ as a quotient. In either case, G has a cyclic group of prime order as a quotient, and the quotient cover has branch locus contained in Δ, so we are done by Proposition 3.3. □

Remark 3.6. The most difficult case for the Weak Diversity Conjecture seems to be that of a *quadratic* cover. In this case, it is tantamount to showing that for a separable polynomial $f \in K[x]$, the number of distinct square classes in the set $\{f(1), \ldots, f(N)\}$ is at least cN for some constant $c > 0$ and all N.

4. Proof of Weak Diversity given *abc*

Lemma 4.1. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let $f(x) \in \mathcal{O}_K[x]$ be a non-constant polynomial. Then there is a constant c, depending on f, such that for any ideal $I \subseteq \mathcal{O}_K$, the set $\{n \in \mathbb{N} \mid (f(n)) = I\}$ has cardinality bounded by c.*

Proof. It suffices to bound the number of n such that $N_{K/\mathbb{Q}}(f(n))$ equals any particular constant. But $N_{K/\mathbb{Q}}(f(n))$ is a polynomial in n over $\mathbb{Q}$, whose absolute value is easily seen to go to ∞ as $n \to \infty$. Thus it is non-constant, and the lemma follows. □

Theorem 4.2. *Let $f : X \to \mathbb{A}^1_K$ be a geometrically irreducible branched cover over some number field K, and let L be a number field such that each branch point of f is L-rational. Then the abc Conjecture[1] for L implies Weak Diversity holds for f.*

Proof. By Lemma 3.1 we may, without loss of generality, assume that $L = K$. By Proposition 3.5, we may assume that f is a $\mathbb{Z}/p$-cover, for some prime p. After a base change, and using Lemma 3.1 again, we may assume that f is given by an

[1] See, e.g., [V, p. 84]

equation $y^p = g(x)$, where $g(x) \in \mathcal{O}_K[x]$ is a polynomial with roots exactly at the branch points and all roots of $g(x)$ have order at most $p-1$.

Let $h(x) \in \mathcal{O}_K[x]$ be a separable polynomial with the same leading coefficient and roots as $g(x)$. By the number field version[2] of [G, Theorem 1], there exists a positive constant c and an ideal $I \subseteq \mathcal{O}_K$ such that for large enough N, the ideal $(h(n))I^{-1} \subseteq \mathcal{O}_K$ is squarefree for at least cN elements $n \in \{1, \dots, N\}$. By Lemma 4.1, after replacing c by a smaller positive constant, we can find cN elements $n \in \{1, \dots, N\}$ such that $(h(n))I^{-1}$ is squarefree and the ideals $(h(n))$ are pairwise distinct. After replacing c by yet a smaller constant, we may assume that the prime factorizations of the ideals $(h(n))$ are pairwise distinct even when prime factors of I and of (p) are ignored.

Now, $h(n) \mid g(n) \mid h(n)^{p-1}$, so the primes ramified in $K(g(n)^{1/p})/K$, other than those dividing I or (p), are exactly those primes dividing $(h(n))$. Thus the fields $K(g(n)^{1/p})$ are pairwise distinct, which proves Weak Diversity for f. □

Remark 4.3. Combining Theorem 4.2 with Theorem 2.2, we see that assuming the *abc* Conjecture over $\mathbb{Q}$ suffices to prove Weak Diversity for covers defined over $\mathbb{Q}$, even if the branch locus does not consist of $\mathbb{Q}$-points.

Remark 4.4. A similar argument to prove Theorem 4.2 can also be made combining the paper [G] with arguments from [DZ] using the discriminant of the cover f as a substitute for the Kummer generator $g(x)$ without first reducing to the cyclic case. Since [DZ] is is written in the context of covers over $\mathbb{Q}$, we provide the above proof so as not to have to adapt their result.

5. The Uniform Faltings' Theorem and Weak Diversity

In this section, we prove the following proposition.

Proposition 5.1. *Let $f : X \to \mathbb{A}^1_K$ be a Galois branched cover over a number field K with $g(X) \geq 2$. Then Conjecture 1.4 implies Weak Diversity for f.*

Proof. Let G be the Galois group of f and let K be a field Let T be a right G-torsor over K. There exists a twist X^T of X, defined over K such that for K-rational points P of $\mathbb{A}^1_K$, the restriction $X \times_{\mathbb{A}^1_K} \{P\}$ is isomorphic to T as a right G-torsor iff X^T has a K-rational point above P. See, for example, Lemma 3.3.1 of [H], and surrounding discussion. Since all of these twists have the same genus and are defined over K, Conjecture 1.4 implies that there is a uniform bound on the number of rational points on any given twist. This implies that for any given G-extension L/K, there is a uniform bound on the number of K-rational points $\{P\}$ of $\mathbb{A}^1_K$ such that $f^{-1}(P)$ is a point with residue field L. Combining this with Hilbert's irreducibility theorem as in Remark 1.3, we obtain Weak Diversity for f. □

Remark 5.2. Proposition 5.1 is more or less the same as the second statement in [D, Theorem 1.3]. The first statement of that same theorem shows that a weaker statement than Weak Diversity holds unconditionally.

[2] See the remark on [G, p. 993]

References

[DZ] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **21** (1994), no. 3, 421–443. MR1310635

[BL] Yuri Bilu and Florian Luca, *Diversity in parametric families of number fields*, 2016. Preprint, arXiv:1607.00904.

[CGT] Pamela Cutter, Andrew Granville, and Thomas J. Tucker, *The number of fields generated by the square root of values of a given polynomial*, Canad. Math. Bull. **46** (2003), no. 1, 71–79. MR1955614

[BL] Yuri Bilu and Florian Luca, *Number fields in fibers: the geometrically abelian case with rational critical values*, 2016. Preprint, arXiv:1606.09164.

[S] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Third, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR1757192

[E] Noam D. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices **7** (1991), 99–109. MR1141316

[P] Patricia L. Pacelli, *Uniform boundedness for rational points*, Duke Math. J. **88** (1997), no. 1, 77–102. MR1448017

[CHM] Lucia Caporaso, Joe Harris, and Barry Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35. MR1325796

[S1] Joseph H. Silverman, *A uniform bound for rational points on twists of a given curve*, J. London Math. Soc. (2) **47** (1993), no. 3, 385–394. MR1214903

[S2] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661

[DZ] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions. II. (On a conjecture of Schinzel)*, Acta Arith. **72** (1995), no. 3, 201–210. MR1347486

[CZ] Pietro Corvaja and Umberto Zannier, *On the number of integral points on algebraic curves*, J. Reine Angew. Math. **565** (2003), 27–42. MR2024644

[D] Pierre Dèbes, *On a problem of Dvornicich and Zannier*, Acta Arith. **73** (1995), no. 4, 379–387. MR1366044

[M] Shinichi Mochizuki, *Inter-Universal Teichmuller theory IV: Log-volume computations and set-theoretic foundations*, 2012. Preprint.

[G] Andrew Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices **19** (1998), 991–1009. MR1654759

[V] Paul Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, vol. 1239, Springer-Verlag, Berlin, 1987. MR883451

[H] Hilaf Hasson, *Minimal fields of definition for Galois action*, J. Pure Appl. Algebra **220** (2016), no. 9, 3327–3331. MR3486304

[D] Pierre Dèbes, *On the Malle conjecture and the self-twisted cover*, Israel J. Math. **218** (2017), no. 1, 101–131. MR3625127