Taylor & Francis
Taylor & Francis Group

Experimental Mathematics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uexm20

Counterexamples to a Conjecture of Ahmadi and Shparlinski

Taylor Dupuy, Kiran Kedlaya, David Roe & Christelle Vincent

To cite this article: Taylor Dupuy, Kiran Kedlaya, David Roe & Christelle Vincent (2021): Counterexamples to a Conjecture of Ahmadi and Shparlinski, Experimental Mathematics, DOI: 10.1080/10586458.2021.1980463

To link to this article: https://doi.org/10.1080/10586458.2021.1980463

Published online: 26 Oct 2021.

EXPERIMENTAL MATHEMATICS
https://doi.org/10.1080/10586458.2021.1980463

Taylor & Francis
Taylor & Francis Group

Counterexamples to a Conjecture of Ahmadi and Shparlinski

Taylor Dupuy[a], Kiran Kedlaya[b], David Roe[c], and Christelle Vincent[a]

[a]Department of Mathematics and Statistics, University of Vermont, Burlington, VT, USA; [b]Department of Mathematics, University of California San Diego, CA, USA; [c]Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, USA

ABSTRACT
Ahmadi-Shparlinski conjectured that every ordinary, geometrically simple Jacobian over a finite field has maximal angle rank. Using the L-Functions and Modular Forms Database, we provide two counterexamples to this conjecture in dimension 4.

KEYWORDS
Angle rank; abelian varieties; finite fields; arithmetic geometry

1. Introduction

The following is a conjecture of Ahmadi–Shparlinski (in slightly reformulated language; see Lemma 2.1):

Conjecture 1.1 ([1, Section 5]). Every ordinary, geometrically simple Jacobian over a finite field has maximal angle rank.

In this paper we report that this conjecture is false. Our work used the L-Functions and Modular Forms Database (LMFDB), specifically its database of abelian varieties over finite fields which can be found here:

https://www.lmfdb.org/Variety/Abelian/Fq/.

Documentation, further conjectures, and interesting statistics are reported in [5].

Apart from the counterexamples of Section 7, this article briefly recalls the notion of angle rank in Section 2, presents how geometric simplicity is computed in the LMFDB (Section 3) and how Jacobians are tested for in the LMFDB (Section 4). Following this, we describe our search (Section 5), and because angle ranks are computed numerically in the LMFDB, we provide a proof of the computation of the angle rank for both examples in Section 6. Readers can verify these counterexamples themselves using the code provided at

https://github.com/LMFDB/abvar-fq/,

which uses Sage [12], PARI [9], and Magma [3]. We remark that in addition to providing counterexamples to the conjecture, we give two new methods for algebraically certifying angle ranks (as remarked above, as of February 2021, in the LMFDB the angle ranks are computed numerically using an LLL algorithm).

Remark 1.2. We began searching for counterexamples to Conjecture 1.1 since it is incompatible with the Shankar-Tsimerman conjecture [11, Conj. 2.5] which states that every simple abelian fourfold over $\overline{\mathbf{F}}_p$ is isogenous to a Jacobian; since angle rank, ordinarity, and geometric simplicity are preserved under base change and isogenies, this would imply that every simple abelian fourfold has maximal angle rank.

2. Frobenius angle rank

This section very briefly presents the definition of the angle rank of an abelian variety defined over a finite field; for more context and a longer discussion the reader is directed to [5, §2.6, 3.8] and [6].

For A an abelian variety of dimension g with L-polynomial $L(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$, the *angle rank* of A is the quantity

$$\delta(A) = \dim_{\mathbf{Q}}(\mathrm{Span}_{\mathbf{Q}}(\{\arg(\alpha_i) : 1 \le i \le 2g\} \cup \{\pi\})) - 1 \in \{0, \dots, g\},$$

where arg denotes the principal branch of the logarithm. When $\delta(A) = g$, we say that A has *maximal angle rank.*

Lemma 2.1. *With notation as above, assume that the α_i have been numbered so that $\alpha_i\alpha_{g+i} = q$ for $i = 1, \dots, g$. Then the following conditions are equivalent.*

CONTACT Christelle Vincent ✉ christelle.vincent@uvm.edu 🖃 Department of Mathematics and Statistics, University of Vermont, Burlington, VT 05405-0160, USA.

(a) *The abelian variety A has maximal angle rank.*

(b) *Every vector $(e_0, \dots, e_g) \in \mathbf{Z}^{g+1}$ such that $\alpha_1^{e_1} \cdots \alpha_g^{e_g} = q^{e_0}$ is identically zero. In this case, Ahmadi–Shparlinski* [1, §5.1] *say that* the Frobenius angles of A are linearly independent modulo 1.

(c) *Every vector $(e_0, \dots, e_{2g}) \in \mathbf{Z}^{2g+1}$ with the property that $\alpha_1^{e_1} \cdots \alpha_{2g}^{e_{2g}} = q^{e_0}$ has the property that $e_i = e_{g+i}$ for $i = 1, \dots, g$. In this case, Zarhin* [14, §2] *says that A is* neat *(or more precisely, some finite base extension of A has this property).*

Proof. We first check that (b) and (c) are equivalent. If (c) holds, then for every vector $(e_0, \dots, e_g) \in \mathbf{Z}^{g+1}$ such that $\alpha_1^{e_1} \cdots \alpha_g^{e_g} = q^{e_0}$, we have $e_1 = \cdots = e_g = 0$ and hence also $e_0 = 0$. Conversely, if (b) holds, then for every vector $(e_0, \dots, e_{2g}) \in \mathbf{Z}^{2g+1}$ with the property that $\alpha_1^{e_1} \cdots \alpha_{2g}^{e_{2g}} = q^{e_0}$, we have

$$\alpha_1^{e_1 - e_{g+1}} \cdots \alpha_g^{e_g - e_{2g}} = q^{e_0 - e_{g+1} - \cdots - e_{2g}}$$

and so $e_i = e_{g+i}$ for $i = 1, \dots, g$.

We next check that (a) implies (b). Note that since $\arg(\alpha_i) + \arg(\alpha_{g+i}) \in 2\pi\mathbf{Z}$, (a) is equivalent to the condition that $\arg(\alpha_1), \dots, \arg(\alpha_g), \pi$ are linearly independent over $\mathbf{Q}$. If this holds, then for every vector $(e_0, \dots, e_g) \in \mathbf{Z}^{g+1}$ such that $\alpha_1^{e_1} \cdots \alpha_g^{e_g} = q^{e_0}$, we have

$$e_1 \arg(\alpha_1) + \cdots + e_g \arg(\alpha_g) \in 2\pi\mathbf{Z}$$

and so $e_1 = \cdots = e_g = 0$ (and also $e_0 = 0$ as above).

We finally check that (b) implies (a). If (a) fails, then we must have a nonzero vector $(e_0, \dots, e_g)$ such that $e_1 \arg(\alpha_1) + \cdots + e_g \arg(\alpha_g) = e_0\pi$. In particular, $\alpha_1^{e_1} \cdots \alpha_g^{e_g}$ is real and hence equal to its complex conjugate $q^{e_1 + \cdots + e_g} \alpha_1^{-e_1} \cdots \alpha_g^{-e_g}$; we thus have $\alpha_1^{2e_1} \cdots \alpha_g^{2e_g} = q^{-e_1 - \cdots - e_g}$. □

The angle rank detects multiplicative relations among the roots of L; these are closely related to exceptional Hodge classes on powers of A. For example, by a theorem of Zarhin [13, Theorem 3.4.3], $\delta(A) = g$ if and only if there are no exceptional Hodge classes on any power of A. At the other extreme, $\delta(A) = 0$ if and only if A is supersingular.

3. Geometric simplicity

To check that an ordinary isogeny class defined over $\mathbf{F}_q$ is geometrically simple, we compute the tensor square of the L-polynomial, note that it has no nontrivial cyclotomic factors, and apply [4, Lemma 7.2.7 (b)] to deduce that all of the geometric endomorphisms are defined over $\mathbf{F}_q$; in particular, each simple isogeny factor is geometrically simple. In the counterexamples presented in this article, simplicity over $\mathbf{F}_q$ follows from the irreducibility of the L-polynomial and ordinarity from the Newton polygon. For a discussion of the geometric endomorphism algebra in more generality, see [5, §3.5].

4. Searching for Jacobians

The current version of the LMFDB contains substantial data about whether isogeny classes contain Jacobians up to dimension 3 (see [5, §3.7]). However, for this paper we need data in dimension 4, for which the LMFDB currently contains only negative results (e.g., a given isogeny class may fail to contain a Jacobian because it contains no principally polarizable variety, or because it corresponds to an impossible sequence of point counts on a curve). We thus cannot use the LMFDB alone to certify that a given isogeny class contains a Jacobian.

We instead take the approach of constructing curves, computing their zeta functions, and matching their numerators to the Weil polynomials contained in the LMFDB. To construct the curves, we note that in genus 4, every nonhyperelliptic curve is isomorphic (via its canonical embedding) to the intersection of a quadric and a cubic in $\mathbf{P}^3$. (See [7, Example IV.5.2.2] for the corresponding statement over an algebraically closed field.) In practice, over $\mathbf{F}_2$, this allows us to make an exhaustive search over both hyperelliptic and nonhyperelliptic curves, using Magma to compute zeta functions. (In the nonhyperelliptic case, we limit the options for the quadric as in [10, Proposition 2.3].) Over $\mathbf{F}_3$ and $\mathbf{F}_5$, we enumerate only over hyperelliptic curves, using Sage to compute zeta functions. This was enough to find the two counterexamples presented here.

5. Results of the search

The Ahmadi-Shparlinski conjecture is a theorem in dimension 2, even without the ordinary condition [1, Theorem 2]. It is also a theorem in dimension 3, but this time it requires the ordinary condition [14, Theorem 1.1]. (That result implies that if an abelian threefold over a finite field is ordinary and absolutely simple, then it is *neat*; the latter condition is equivalent to having maximal angle rank by Lemma 2.1.) We verified the consistency of these results with the LMFDB database.

In dimension 4 over $\mathbf{F}_2$, there are 52 isogeny classes of ordinary, geometrically simple abelian varieties with angle rank at most 3 (in fact they are all equal to 3). Searching through curves, we found 620 distinct zeta functions, none of which occur among the previous list of 52 isogeny classes. Therefore there are no such 4-dimensional Jacobians over $\mathbf{F}_2$, and the conjecture holds in this case.

By contrast, the conjecture fails in dimension 4 over $\mathbf{F}_3$ and $\mathbf{F}_5$, as shown by the examples presented in Section 7. While we chose specific examples for definiteness, these are not particularly exceptional: over $\mathbf{F}_3$ there are 210 isogeny classes of ordinary, geometrically simple abelian varieties of dimension 4, and by comparing to a random sample of half a million hyperelliptic curves we found that at least 66 isogeny classes contain a Jacobian. (Over $\mathbf{F}_5$, there are 1304 isogeny classes of ordinary, geometrically simple abelian varieties of dimension 4; we did not attempt to determine how many of these contain Jacobians.)

6. Algebraic certification of angle ranks

We now describe the procedure we used to compute a rigorous upper bound on $\delta(A)$. See [5, §3.8] for an alternate approach that also gives a rigorous lower bound, which we do not need here; instead we use an estimate on the size of relations based on linear forms in logarithms (see Lemma 6.3).

Let $L(T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$ be the L-polynomial of an abelian variety A over $\mathbf{F}_q$. Fix a precision $\rho = \sigma^2$ (we default to $\rho = 625$).

1. Compute the inverse roots $\{\alpha_i\}$ of $L(T)$ that have positive imaginary part, in a complex field C of precision ρ. Set $t_i = \arg(\alpha_i)/\pi$, where arg is the principal branch of the logarithm. Throw away duplicates, obtaining (after possibly reordering) $0 < t_1 < \cdots < t_m < 1$.
2. Use LLL to find independent integer relations $R_1, \ldots, R_s$ among $\{t_1, \ldots, t_m, 1\}$. A relation is considered spurious if all coefficients are larger than 2^σ, with $\sigma = \sqrt{\rho}$ as above, and we interrupt the computation if some value is larger than 2^σ but others are not (this did not happen for any isogeny class in the database). The *numerical angle rank* is $m - s$.
3. Find a number field K in which $L(T)$ splits completely. Choose an embedding $\iota\colon K \hookrightarrow C$, where as before C is a complex field of precision ρ, and let $\beta_1, \ldots, \beta_m$ be the roots of $P(T)$ in K with $0 < \arg(\iota(\beta_1)) < \cdots < \arg(\iota(\beta_m)) < \pi$. (In other words, the root β_i has argument approximated by πt_i above.)
4. The roots $\beta_1, \ldots, \beta_m$ together with the relations $R_1, \ldots, R_s$ provide a certificate that the angle rank of A is at most $m - s$. One can check using exact arithmetic in K that a relation $R_i = (c_1, \ldots, c_{m+1})$ holds by confirming that
$$(-q)^{c_{m+1}} \prod_{i=1}^{m} \beta_i^{c_i} = 1.$$

Remark 6.1. The upper bound $m - s$ can only fail to be sharp if at some point we discarded a relation as spurious when it was real. Such a relation would have all coefficients larger than 2^σ.

Remark 6.2. Let $P(T) = \prod_{i=1}^{2g}(\alpha_i - T)$ be a Weil polynomial, with roots ordered so that $\alpha_i\alpha_{i+g} = q$ (where the indices are taken modulo $2g$). This remark explains an alternative method, using resultants and "taking cyclotomic parts," to verify the existence of a relation of the form
$$\alpha_{i_1}^{e_1}\alpha_{i_2}^{e_2}\cdots\alpha_{i_j}^{e_j} = \zeta q^{j/2}, \tag{1}$$
where $e_1, \ldots, e_j$ are specified positive integers and ζ is an unspecified root of unity. Such a relation is guaranteed to be nontrivial (i.e., not a consequence of the known relations $\alpha_i\alpha_{i+g} = q$) provided that $i_1, \ldots, i_j$ are pairwise distinct mod g; when this occurs, the existence of the relation implies that the angle rank is not maximal. Note however that as presented, this method cannot always certify a sharp upper bound on the angle rank.

Before presenting this method, we present three preliminary facts which we will need and take for granted:

1. If $F(T)$ and $G(T)$ are any two polynomials, the polynomial
$$H(T) = \operatorname{Res}_S(F(S), G(T/S)S^{\deg G})$$
is a polynomial whose roots are products of the roots of F and G.

Proof. It is well known that if $F(S) = a\prod_i(S - \alpha_i)$ and $G(S) = b\prod_j(S - \beta_j)$ then
$$\operatorname{Res}_S(F(S), G(S)) = a^{\deg(G)} b^{\deg(F)} \prod_{i,j}(\alpha_i - \beta_j).$$

Without loss of generality, we can suppose F and G are monic. In the above we have $S^{\deg(G)}G(T/S) = (-1)^{\deg(G)}\prod_j \beta_j \prod_j (S - T/\beta_j)$. This means
$$\operatorname{Res}_S(F(S), G(T/S)S^{\deg G}) = (-1)^{\deg(G)\deg(F)}\left(\prod_j \beta_j\right)^{\deg(G)} \prod_{i,j}(\alpha_i - T/\beta_j) = \prod_{i,j}(T - \alpha_i\beta_j),$$
as claimed. □

2. If A is an abelian variety over $\mathbf{F}_q$ of dimension g with characteristic polynomial $P(T) = P_{A_{\mathbf{F}_q}}(T) = \prod_{i=1}^{2g}(T - \alpha_i)$, then for any positive integer n, $P_{A_{\mathbf{F}_{q^n}}}(T) = \prod_{i=1}^{2g}(T - \alpha_i^n)$. One can show that there is a formula for this polynomial in terms of resultants given by $P_{A_{\mathbf{F}_{q^n}}}(T) = \mathrm{Res}_S(P(S), S^n - T)$.
3. If $F(T)$ is a polynomial with integer coefficients, then it factors as $F(T) = C(T)G(T)$ where $C(T)$ is a cyclotomic polynomial and $G(T)$ has no cyclotomic factors. The computation of the cyclotomic part $C(T)$ can be done efficiently using an algorithm described in [2]; this is implemented in Sage by the function `cyclotomic_part()` called on $F(T)$, which returns $C(T)$.

With these facts granted, note first that, for purposes of verifying the nontrivial relation as in (1), we are free to make the test after performing a base change as in the second point above; we may thus assume without loss of generality that q is a perfect square, so that $\overline{P}(T) = P(q^{1/2}T)$ is a root-unitary polynomial with rational coefficients. Set $\widetilde{\alpha}_i = q^{-1/2}\alpha_i$, so that the roots of $\overline{P}(T)$ are $\widetilde{\alpha}_1, \dots, \widetilde{\alpha}_{2g}$. For our counter-examples in Section 7, we will not renormalize as in this remark.

Using the first and second points, we compute the polynomial

$$Q(T) = \prod_{i_1, i_2, \dots, i_j} (T - \widetilde{\alpha}_{i_1}^{e_1}\widetilde{\alpha}_{i_2}^{e_2} \cdots \widetilde{\alpha}_{i_j}^{e_j}),$$

where the product is taken over all tuples $(i_1, i_2, \dots, i_j)$ in which $1 \le i_k \le 2g$. When j is even, whenever there is a way to divide the set of e_i into equal pairs, then the relations $\alpha_i\alpha_{i+g} = q$ will yield a cyclotomic factor of $Q(T)$ that does not correspond to a nontrivial relation. However, we can compute the degree of this expected factor and compare with the degree of the cyclotomic part determined as in (3). A nontrivial factor with the given e_is will arise exactly when these two degrees don't match.

In practice, we predict j and $e_1, \dots, e_j$ in the relation (1) using LLL, and then verify the existence of a relation as we have just described.

The following gives an upper bound on the size of any e_i in a relation $(e_1, \dots, e_n)$. This can be used to derive a lower bound on the angle rank.

Lemma 6.3. *Let $\alpha_1, \dots, \alpha_n$ be roots of characteristic polynomials of Frobenius of an abelian variety over $\mathbf{F}_q$. If there exist integers $e_1, \dots, e_n$, not all zero, such that $\alpha_1^{e_1} \cdots \alpha_n^{e_n} = 1$, then these integers may be chosen to satisfy*

$$\max_i |e_i| \le (n-1)!(e \log_2 q^{1/2})^{n-1}.$$

Proof. In [8] they give a general bound for relations among root unitary polynomials. We apply [8, Theorem 1, part (a), equation (5)] to our situation by letting

$$\begin{aligned} d(\alpha_i) &= \log q^{1/2} \\ E &= \max\{e, d(\beta_j)\log 2/\log q^{1/2}\} = e \\ V_j &= \max\{d(\beta_j), (e/\log 2)\log q^{1/2}\}/\log(E/\log E) = (e/\log 2)\log q^{1/2}. \end{aligned}$$ □

7. Counterexamples

In the examples that follow we re-index the roots as in the previous section. That is,

$$0 < \arg(\beta_1) < \cdots < \arg(\beta_g) < \pi$$

and $\beta_i\beta_{i+g} = q$.

7.1. A Counterexample when g = 4 and q = 3

Let C be the hyperelliptic curve over $\mathbf{F}_3$ given by

$$y^2 = x^9 + x^8 + x^7 + 2x^5 + x.$$

Then

$$L(C/\mathbf{F}_3, T) = 1 - T + 2T^2 - 4T^3 - 2T^4 - 12T^5 + 18T^6 - 27T^7 + 81T^8,$$

so the Jacobian A of C belongs to isogeny class 4.3.ab_c_ae_ac, which is ordinary and geometrically simple. We compute the minimal splitting field of this polynomial, which has degree 48 over $\mathbf{Q}$. Using the method of Section 6, we show that these roots satisfy the nontrivial relation

$$\beta_1\beta_3\beta_4 = -3\beta_2.$$

The angle rank of A is thus at most 3, and is equal to 3 unless there is a relation with exponents all larger than 2^{25}. However, Lemma 6.3 implies that if the angle rank is less than 3, then there is a relation among $\beta_1, \beta_2, \beta_3$ with exponents of absolute value at most 9.

7.2. A Counterexample when $g = 4$ and $q = 5$

Similarly, let C be the hyperelliptic curve over $\mathbf{F}_5$ given by

$$y^2 = x^9 + x^6 + 2x^5 + x.$$

Then

$$L(C/\mathbf{F}_5, T) = 1 - T + 2T^2 - 4T^3 + 16T^4 - 20T^5 + 50T^6 - 125T^7 + 625T^8,$$

so the Jacobian A of C belongs to isogeny class 4.5.ab_c_ae_q. Again, A is ordinary, geometrically simple, and has angle rank bounded above by 3. There is now a nontrivial relation of the form

$$\beta_1\beta_4 = \beta_2\beta_3.$$

In this case, Lemma 6.3 implies that if the angle rank is less than 3, then there is a relation among $\beta_1, \beta_2, \beta_3$ with exponents of absolute value at most 19.

Acknowledgments

We thank the referee for helpful suggestions, including pointing out the reference [8].

Declaration of Interest

No potential conflict of interest was reported by the author(s).

Funding

The authors began this project during the semester program "Computational aspects of the Langlands program" held at ICERM in fall 2015. Subsequent workshops in support of the project were sponsored by the American Institute of Mathematics and the Simons Foundation. In addition Dupuy was partially supported by the European Research Council under the European Unions Seventh Framework Programme (FP7/2007-2013) / ERC Grant agreement no. 291111/ MODAG while working on this project. Kedlaya was supported by NSF (grants DMS-1501214, DMS-1802161), IAS (visiting professorship 2018–2019), UCSD (Warschawski Professorship), and a Guggenheim Fellowship (fall 2015). Roe was supported by Simons Foundation grant 550033. Vincent was partially supported by NSF (grant DMS-1802323).

References

[1] Ahmadi, O., Shparlinski, Igor E. (2010). On the distribution of the number of points on algebraic curves in extensions of finite fields. *Math. Res. Lett.* 17(4): 689–699.

[2] Beukers, F., and Smyth, C. J. (2002). Cyclotomic points on curves. In: Bennett, M. A., Berndt, B .C., Boston, N., Diamond, H. G., Hildebrand, A. J., Philipp, W., eds. *Number Theory for the Millennium, I (Urbana, IL, 2000)*, Natick, MA: A K Peters; pp. 67–85.

[3] Bosma, W., Cannon, J., Playoust, C. (1993). The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24(3/4): 235–265, 1997. Computational algebra and number theory (London).

[4] Costa, E., Mascot, N., Sijsling, J., Voight, J. (2019). Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.* 88(317): 1303–1339.

[5] Dupuy, T., Kedlaya, K. S., Roe, D., and Vincent, C. (2020). Isogeny classes of abelian varieties over finite fields in the LMFDB.

[6] Dupuy, T., Kedlaya, K. S., Zureick-Brown, D. Angle ranks of abelian varieties.

[7] Hartshorne, R. (1977). *Algebraic Geometry*, Vol. 52. Springer.

[8] Loxton, J. H., van der Poorten, A. J. (1983). Multiplicative dependence in number fields. *Acta Arith.* 42(3): 291–302.

[9] The PARI Group. *PARI/GP version* `2.11.2`. Univ. Bordeaux, 2019. Available at: http://pari.math.u-bordeaux.fr/.

[10] Savitt, D. (2003). The maximum number of points on a curve of genus 4 over $\mathbb{F}_8$ is 25. *Canad. J. Math.* 55(2): 331–352. With an appendix by Kristin Lauter.

[11] Shankar, A. N., Tsimerman, J. (2018). Unlikely intersections in finite characteristic. *Forum Math. Sigma*. 6: e13, 17.

[12] Stein, W. A. et al. (2020). *Sage Mathematics Software (Version 9.1.beta0)*. The Sage Development Team. Available at: http://www.sagemath.org.

[13] Zarhin, Y. G. (1994). The Tate conjecture for nonsimple abelian varieties over finite fields. In: Frey, G., Ritter, J., eds. *Algebra and number theory (Essen, 1992)*. Berlin: de Gruyter; pp. 267–296.

[14] Zarhin, Y. G. (2015). Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension. *J. Pure Appl. Algebra*. 219(6): 2076–2098.