Polarizations of abelian varieties over finite fields via canonical liftings – Additional Examples

Jonas Bergström, Valentijn Karemaker, and Stefano Marseglia

October 26, 2021

In the following examples we present the output of our computation of principal polarizations for all squarefree isogeny classes of abelian varieties of dimension two and three over the finite fields $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$, and of dimension four over $\mathbb{F}_2$ and $\mathbb{F}_3$.

Example 1. We consider abelian varieties of dimension 2 defined over $\mathbb{F}_p$ for $p = 2, 3, 5$ and 7. There are 6 (resp. 8, 10, 12) isogeny classes over $\mathbb{F}_2$ (resp. $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$) corresponding to non-squarefree characteristic polynomials, to which our result do not apply. In Table 1 we summarize the results for the squarefree characteristic polynomials.

squarefree dimension 2			$p=2$	$p=3$	$p=5$	$p=7$
total			29	55	119	195
ordinary			14	36	94	168
almost ordinary			8	14	20	24
p-rank 0	no RRC		0	0	0	0
	yes RRC	5.5.2(R_w) yes	6	2	5	3
		5.5.2(R_w) no	1	3	0	0

Table 1: Squarefree isogeny classes of dimension 2. Here "yes RRC" (resp. "no RRC") means that there is a (resp. is no) CM-type satisfying the residual reflex condition, cf. Definition 2.14; "5.5.2(R_w) yes" (resp. "5.5.2(R_w) no") means that we can (resp. cannot) apply Theorem 5.5.2 for the order R_w. By Remark 5.8, "5.5.2(R_w) yes" implies we can compute the principal polarizations for the whole isogeny class.

We see that there are only 1 isogeny class over $\mathbb{F}_2$ and 3 isogeny classes over $\mathbb{F}_3$ for which we cannot compute principal polarizations using Theorem 5.5.2. These isogeny classes correspond to the following characteristic polynomials:

$$\begin{aligned} x^4+4 &= (x^2-2x+2)(x^2+2x+2), \\ x^4-3x^2+9 &= (x^2-3x+3)(x^2+3x+3), \\ x^4-3x^3+6x^2-9x+9 &= (x^2-3x+3)(x^2+3), \\ x^4+3x^3+6x^2+9x+9 &= (x^2+3)(x^2+3x+3). \end{aligned}$$

In the isogeny class over $\mathbb{F}_2$ there are 5 endomorphism rings, each giving a single isomorphism class of abelian varieties, and for 4 of them we can compute the principal polarizations using Theorem 5.9. Similarly, in each case over $\mathbb{F}_3$, there are 6 endomorphism rings, each giving a single isomorphism class of abelian varieties, and for 4 of them we can compute principal polarizations.

Example 2. We consider abelian varieties of dimension 3 defined over $\mathbb{F}_p$ for $p = 2, 3, 5$ and 7. There are 30 (resp. 56, 90, 132) isogeny classes over $\mathbb{F}_2$ (resp. $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$) corresponding to non-squarefree characteristic polynomials, to which our results do not apply. In Table 2 we summarize the results for the squarefree characteristic polynomials. From Table 2 we

squarefree dimension 3			$p=2$	$p=3$	$p=5$	$p=7$
total			185	621	2863	7847
ordinary			82	390	2280	6700
almost ordinary			58	170	474	996
p-rank 1	no RRC		0	0	0	0
	yes RRC	5.5.2(R_w) yes	20	26	76	118
		5.5.2(R_w) no	4	16	12	8
p-rank 0	no RRC		0	3	2	1
	yes RRC	5.5.2(R_w) yes	20	15	17	23
		5.5.2(R_w) no	1	1	2	1

Table 2: Squarefree isogeny classes of dimension 3. The notation is the same as in Table 1.

see that there are 5 isogeny classes over $\mathbb{F}_2$, 17 over $\mathbb{F}_3$, 14 over $\mathbb{F}_5$, and 9 over $\mathbb{F}_7$ for which we cannot compute the principal polarizations using Theorem 5.5.2. Nevertheless, using Theorem 5.9we can compute the total number of isomorphism classes of principally polarized abelian varieties with any endomorphism ring in all of these 45 isogeny classes except for 13. For these 13 isogeny classes, of which 3 are over $\mathbb{F}_2$ and 10 over $\mathbb{F}_3$, we can still obtain information for most endomorphism rings, as we summarize in Table 3.

isogeny class	tot	ok	isogeny class	tot	ok
$(x^2-2x+2)(x^2-x+2)(x^2+2x+2)$	10	8	$(x^2-2x+2)(x^2+x+2)(x^2+2x+2)$	10	8
$(x^2-2x+2)(x^2+2)(x^2+2x+2)$	22	19	$(x^2-3x+3)(x^2+3)(x^2+2x+3)$	24	18
$(x^2-3x+3)(x^2-2x+3)(x^2+3x+3)$	12	2	$(x^2-3x+3)(x^2+3)(x^2+x+3)$	18	12
$(x^2-3x+3)(x^2-x+3)(x^2+3)$	12	8	$(x^2-3x+3)(x^2-2x+3)(x^2+3)$	12	9
$(x^2-2x+3)(x^2+3)(x^2+3x+3)$	24	18	$(x^2-3x+3)(x^2+2x+3)(x^2+3x+3)$	12	8
$(x^2-x+3)(x^2+3)(x^2+3x+3)$	18	12	$(x^2+3)(x^2+x+3)(x^2+3x+3)$	12	8
$(x^2-3x+3)(x^2+3)(x^2+3x+3)$	60	40			

Table 3: "tot" is the number of endomorphism rings in the given isogeny class and "ok" is the number of these for which we can determine the number of isomorphism classes of principally polarized abelian varieties.

Example 3. We consider abelian varieties of dimension 4 defined over $\mathbb{F}_p$ for $p = 2$ and 3. There are 214 (resp. 510) isogeny classes over $\mathbb{F}_2$ (resp. $\mathbb{F}_3$) corresponding to non-squarefree characteristic polynomials, to which our results do not apply.

In Table 4 we summarize the results for the squarefree characteristic polynomials.

Some of these isogeny classes have a characteristic polynomial h with splitting field M over $\mathbb{Q}$ of degree 384. We therefore had to outsource the computation of M and of the roots of h in M from Magma [1] to Pari [2]. A reduction of the defining polynomial of M returned by Pari in order to obtain a polynomial defining an isomorphic field but with smaller coefficients did not finish in reasonable time. Hence, we had to carefully optimize all arithmetic operations within M.

squarefree dimension 4			$p=2$	$p=3$
total			1431	10453
ordinary			656	6742
almost ordinary			392	2506
p-rank 2	no RRC		0	0
	yes RRC	5.5.2(R_w) yes	149	500
		5.5.2(R_w) no	49	312
p-rank 1	no RRC		6	36
	yes RRC	5.5.2(R_w) yes	80	184
		5.5.2(R_w) no	14	40
p-rank 0	no RRC		3	6
	yes RRC	5.5.2(R_w) yes	73	88
		5.5.2(R_w) no	9	39

Table 4: Squarefree isogeny classes of dimension 4. The notation is the same as in Table 1.

From Table 4 we see that there are 72 isogeny classes over $\mathbb{F}_2$ and 391 over $\mathbb{F}_3$ for which we cannot compute the principal polarizations using Theorem 5.5.2. Out of these, we can compute the total number of isomorphism classes of principally polarized abelian varieties with any endomorphism ring in 20 isogeny classes over $\mathbb{F}_2$ and 199 over $\mathbb{F}_3$, using Theorem 5.9. For the remaining 52 isogeny classes over $\mathbb{F}_2$ we can only get information about certain endomorphism rings. More precisely, for these 52 isogeny classes, we can compute the polarizations for 723 endomorphism rings, while for 223 we cannot. Similarly, we can get only partial information for 183 isogeny classes over $\mathbb{F}_3$: we can determine the number of isomorphism classes of principally polarized abelian varieties for 3481 endomorphism rings, while for 1155 we cannot. Unfortunately, there are 9 isogeny classes over $\mathbb{F}_3$ for which the current algorithm to compute the (unpolarized) isomorphism classes does not finish.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[2] The PARI Group, Univ. Bordeaux, *PARI/GP version 2.11.4*, 2020, available from `http://pari.math.u-bordeaux.fr/`.

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, SE-106 91 STOCKHOLM, SWEDEN
E-mail address: jonasb@math.su.se

MATHEMATISCH INSTITUUT, UNIVERSITEIT UTRECHT, POSTBUS 80010, 3508 TA UTRECHT, THE NETHERLANDS
E-mail address: v.z.karemaker@uu.nl

MATHEMATISCH INSTITUUT, UNIVERSITEIT UTRECHT, POSTBUS 80010, 3508 TA UTRECHT, THE NETHERLANDS
E-mail address: s.marseglia@uu.nl