COMPLETE ADDITION LAWS ON ABELIAN VARIETIES OVER FINITE FIELDS

CHRISTOPHE ARENE, DAVID KOHEL, AND CHRISTOPHE RITZENTHALER

Keywords: completeness, addition law.

Abstract. The first results on completeness of addition laws, on a given abelian variety A over a field k, were obtained by Lange and Ruppert in 1985 [LR85]. Subsequent work [LR85, LR87, BL95] considered abelian varieties, particularly elliptic curves, over algebraically closed fields. One of their main results is the non existence of a single addition law describing the group law m of A embedded in a projective space. The study of the completeness of Edwards curves, initiated by Bernstein and Lange [BL07], naturally leads us to consider the arithmetic properties of addition laws. In this paper, we give a proof of the existence of a single addition law describing m on the k-rational points of A, provided k has an extension of degree greater than the dimension of A. We also describe the construction of such a law for elliptic curves and Jacobians of genus 2 curves over a finite field. The study of complete addition laws is motivated by their role in avoiding side channel attacks.

1. Introduction

Let A be an abelian variety of dimension g over a field k. We assume that A is embedded in some projective space $\mathbb{P}^n$ over k by a very ample line bundle L and we denote $\iota : A \hookrightarrow \mathbb{P}^n$ the corresponding morphism. We also assume the embedding is projectively normal, but not mention it in the sequel, so that the sections we use further come from polynomials.
The group law $m : (x, y) \mapsto x + y$ can be described locally by bihomogenous polynomials. More precisely, an *addition law* of bidegree (μ, ν) on $\iota(A) \subset \mathbb{P}^n$ is a nonempty open set $U \subset A \times A$ together with an $(n+1)$-tuple of polynomials

$$\mathfrak{p} = (p_0, \ldots, p_n) \in k[X_0, \ldots, X_n, Y_0, \ldots, Y_n]^{n+1},$$

not all zero, bihomogeneous of degree μ in $X_0, \ldots, X_n$ and of degree ν in $Y_0, \ldots, Y_n$ such that we have

$$\iota(x + y) = (p_0(\iota(x), \iota(y)) : \ldots : p_n(\iota(x), \iota(y)))$$

for all $(x, y) \in U$.

Definition 1.1. A set S of addition laws is called *complete* if for any point $(x, y) \in (A \times A)(k)$ there is a law in S defined on an open set U containing (x, y). A set S of addition laws is said *geometrically complete* if the previous

The authors acknowledge the financial support by grant ANR-09-BLAN-0020-01 from the French ANR, the AXA Research Fund for the PhD grant of the first author and of the grant MTM2006-11391 from the Spanish MEC for the third author.

property is true over $\bar{k}$. An addition law $\mathfrak{p}$ is called complete if $S = \{\mathfrak{p}\}$ is complete.

Remark 1.2. We call attention to the change of notation towards the original paper [LR85] where original *complete* means here *geometrically complete*.

In [LR85], the authors give the interpretation of the possible addition laws in terms of the section of a certain line bundle.

Proposition 1.3 ([LR85, Lem.2.1])**.** *Let $p_1, p_2 : A \times A \to A$ be the projection maps on the first and second factor. There is an addition law (resp. a geometrically complete set of addition laws) of bidegree (μ, ν) on A with respect to the embedding in $\mathbb{P}^n$ determined by L if and only if*

$$H^0(A \times A, M) \neq 0$$

where $M = m^*L^{-1} \otimes p_1^*L^\mu \otimes p_2^*L^\nu$ (resp. the line bundle M is base point-free).

To a nonzero section $w \in H^0(A \times A, M)$ one associates an addition law defined on the open set $A \times A \setminus (w)_0$.

Note that asking the embedding to be symmetric is natural to have a good behaviour of the inversion as we see below. Another interest is to guarantee the existence of sections of bidegree (2,2) on M (see 2.2).

Proposition 1.4. *If A is embedded in a $\mathbb{P}^n$ by a very ample symmetric line bundle L, then the inversion is induced by a linear automorphism of $\mathbb{P}^n$.*

Proof. If L is a very ample symmetric line bundle, $H^0(A, L)$ can be generated by even or odd sections s_i [BL04]. Let ι th embedding associated to L. Hence

$$\iota(-z) = (s_0(-z) : \cdots : s_n(-z)) = (\pm s_0(z) : \cdots : \pm s_n(z)).$$

□

2. Geometrically complete set of addition laws

Theorem 2.1. *Let A an abelian variety and a symmetric embedding $\iota : A \hookrightarrow \mathbb{P}^n$. If S is a geometrically complete set of addition laws on A then $\#S > g$.*

Proof. Up to a projective change of coordinates, assume the image of $\mathcal{O}$ is $(0 : \cdots : 0 : 1)$.
Let $(U_j, \mathfrak{p}_j)_{1 \leq j \leq s}$ be a complete system of addition on A and a the injection $a : A \to A \times A$, $x \mapsto (x, -x)$. Consider the morphisms

$$A \xrightarrow{a} A \times A \overset{\mathfrak{p}_j}{\dashrightarrow} A$$

Note that for all x such that $a(x) \in U_j$, $\mathfrak{p}_j \circ a(x) = \iota(O)$ and, in particular, $\mathfrak{p}_n^{(j)} \circ a \neq 0$. Considering g hypersurfaces defined by the equations $\mathfrak{p}_n^{(j)} \circ a(\iota(x)) = 0$, $j = 1, \ldots, g$, the intersection between A and g hypersurfaces in $\mathbb{P}^n$ being non empty, the addition laws $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$ are not defined at the points in this intersection. We hence get that $\#S = s > g$. □

We would like to have an upper bound on S as well. This is an easy consequence of the following results of [LR85].

Proposition 2.2 ([LR85, Prop.2.2,Prop.2.3])**.** *Let L be an ample line bundle on A. If $(\mu,\nu)=(2,2)$ then*

(1) if L is not symmetric then $H^0(A\times A,M)=\{0\}$.
(2) if L is symmetric, then $M=s^*L$ where $s:A\times A\to A$ is the difference map $(x,y)\mapsto x-y$. In particular M is base point-free and $h^0(M)=h^0(L)$.

If $(\mu,\nu)\neq(2,2)$ then $h^0(M)=h^0(L)^2(\mu\nu-\mu-\nu)^g$.

Proof. For $(\mu,\nu)=(2,2)$, only the equality $h^0(M)=h^0(L)$ has to be clarified. It is proven in [LR85, Prop.2.2] that $M|_{K(M)_0}$ is trivial. As L is ample his index in zero and, according to [Kem, Theorem 1(ii) p95], $H^0(A\times A,M)\cong H^0(A,L)$.
For the case $(\mu,\nu)\neq(2,2)$, one proves it like for the case $(\mu,\nu)=(2,3)$ of [LR85, Prop.2.3]. □

Corollary 2.3. *Let A be a principally polarized abelian variety. There exists an embedding of A for which a geometrically complete set of addition laws of order less or equal to 3^g exists.*

Proof. The line bundle L associated to the principal polarization is ample symmetric and has degree 1, so L^3 provides an embedding $A\hookrightarrow\mathbb{P}^{3^g}$. □

Remark 2.4. For $g=1$, our bounds show that there exists a geometrically complete set of addition laws of order 2 or 3. An explicit set of order 3 is given in [LR85, Sec.3] and in [LR87] in all characteristic and an explicit set of order 2 is given in [BL95].

3. Complete set of addition laws

Let L be a very ample symmetric line bundle defined by an effective rational divisor D on A. Let v be a section of $H^0(A,L)$ such that $(v)_0=D$ and let $w=s^*(v)$. As we have seen in Section 1, w is a section of $H^0(A\times A,M)$ with $M=m^*L^{-1}\otimes p_1^*L^2\otimes p_2^*L^2$ and an addition law (of bidegree $(2,2)$) is defined on the complementary of $(w)_0=s^*D$. Hence it is sufficient that D has no rational points for the group law to be complete. Note that it is also necessary since a rational point x on D gives the rational point $(x,0)$ on s^*D.

Theorem 3.1. *Let A an abelian variety over a non algebraically closed field and an embedding $\iota_0:A\hookrightarrow\mathbb{P}^n$. If there exists $\alpha\in\bar{k}$ whose degree d over k is greater than n then there exists an embedding $\iota:A\hookrightarrow\mathbb{P}^{n(2d-1)}$ and a complete addition law on $\iota(A)$.*

Proof. Let $\alpha_0,\ldots,\alpha_{d-1}$ the Galois conjugates of α in $\bar{k}$.
For $i=0,\ldots,d-1$, let H_i be the hyperplane

$$H_i: X_0+\alpha_iX_1+\ldots+\alpha_i^nX_n=0.$$

Since $d>n$, $\{1,\alpha_i,\ldots,\alpha_i^n\}$ are linearly independent for every i over k and $H_i(k)$ is empty. Now $\sum H_i$ is a divisor over k, let $D_0=\iota_0^*(\sum H_i)$ and $D=D_0+(-1)^*D_0$. D is a symmetric rational divisor on A without rational points. Denoting L_0 the line bundle associated to ι_0, the line bundle $L=\mathcal{L}(D)$ is linearly equivalent to L_0^{2d}, so L is very ample and provides an embedding $A\hookrightarrow\mathbb{P}^{n(2d-1)}$ with a complete addition law. □

We want to minimize the dimension of the projective space in which embed the variety, considering a finite map $\varphi : A \to \mathbb{P}^n$. Indeed $\varphi^*\mathcal{O}_{\mathbb{P}^n}(1)$ is ample (and conversely). Moreover, such a map exists for $n = g$ (got from Noether's normalisation theorem). Hence this proves the following theorem:

Theorem 3.2. *Let A an abelian variety of dimension g over a non algebraically closed field. If there exists in $\bar{k}$ an element of degree d greater than g then there exists an embedding ι of A in $\mathbb{P}^{g(2d-1)}$ and an arithemetically complete addition law on $\iota(A)$.*

Over finite fields, every abelian variety of dimension g can be embedded in a projective space of dimension $g(2g+1)$ with a complete addition law.

4. Example in genus one and two

In the previous section, the complete addition law is proved to exist but for a large embedding of the abelian variety. When A over a finite field has dimension 1 or 2, we make explicit the construction of a desired divisor.

4.1. **Elliptic curves.** First, let us consider a particular case.

Theorem 4.1. *Let $E : y^2 = f(x)$ be an elliptic curve embedded in $\mathbb{P}^2$. If f is irreducible there exists a complete addition law on $E \subset \mathbb{P}^2$.*

Proof. Consider the zero divisor of the section y on E. It is a very ample symmetric rational divisor without rational points which provides a complete addition law on $E \subset \mathbb{P}^2$. □

Theorem 4.2. *If $E/\mathbb{F}_q$ is an elliptic curve with a point whose field of definition is $\mathbb{F}_{q^2}$, then there is an embedding on E in $\mathbb{P}^3$ on which one can define a complete addition law.*

Proof. Let $P \in E(\overline{k})$ as in the statement. Then, $D := D_0 + (-1)^* D_0$, where $D_0 = P + P^\sigma$, is the divisor we want to. □

Remark 4.3. Previously we used the fact that D symmetric divisor implies $\mathcal{L}(D)$ symmetric line bundle. But the converse is not true: if $D \sim D'$ with D not symmetric and D' symmetric divisors then $\mathcal{L}(D) \sim \mathcal{L}(D')$ are symmetric line bundles. In particular, this is the case if the points of the Galois orbit lie on a line. That's what we use in the theorem 4.4.

Theorem 4.4. *Let $E/\mathbb{F}_q, q \geq 5$, an elliptic curve defined by $y^2 = f(x)$. There exists an embedding on E in $\mathbb{P}^2$ on which we can define a complete addition law.*

Proof. Consider the group homomorphism $N : E(\mathbb{F}_{q^3}) \to E(\mathbb{F}_q)$, $P \mapsto P + P^\sigma + P^{\sigma^2}$, where σ denotes here the Frobenius. $ker(N)$ restricts on $E(\mathbb{F}_q)$ to the $\mathbb{F}_q$-rational 3-torsion points on E. Now $\#\ker(N) \geq \frac{\#E(\mathbb{F}_{q^3})}{\#E(\mathbb{F}_q)} \geq \frac{q^3+1-2\sqrt{q^3}}{q+1+2\sqrt{q}} > 9$. Hence there exists $P_0 \in E(\mathbb{F}_{q^3})$ non $\mathbb{F}_q$-rational whose Galois orbit provides the aligned points we searched for. □

Remark 4.5. If the trace of E is positive the points in the Galois orbit can be chosen on a horizontal line.

4.2. **Genus 2 curves.** Let $C/\mathbb{F}_q, q \geq 5$, be a genus 2 curve. Assume C has a model over k of the form $y^2 = f(x)$ with f of degree 5. Let us denote by $\overline{\ }$ the canonical involution on C, *i.e.* if $P = (x, y)$, $\overline{P} = (x, -y)$ and $\Theta = W_1$. Θ is an ample symmetric rational divisor on $\operatorname{Jac} C$ which defines the canonical principal polarization on $\operatorname{Jac} C$. For any $z \in \operatorname{Jac}(C)(\bar{k})$, we denote $\Theta_z = \Theta + z$ the translation of Θ by z.

Lemma 4.6 ([Mum75, p.272],[Deb86])**.** *If $z \sim P - Q \in (\operatorname{Jac} C)(\bar{k})$ then*

$$\Theta \cdot \Theta_z = \{(P) - (P_\infty)\} \cup \left\{(\overline{Q}) - (P_\infty)\right\}.$$

Lemma 4.7. *There exists $x_0 \in \mathbb{F}_{q^2}$ such that $f(x_0)$ is not a square in $\mathbb{F}_{q^2}$.*

Proof. If it were not the case, there would be at least $2(q^2 - q) + \#C(\mathbb{F}_q)$ $\mathbb{F}_{q^2}-$rational points on C which contradicts the Hasse-Weil bounds. □

Theorem 4.8. *Let C be a genus two curve as above. There exists an embedding ι of $\operatorname{Jac} C$ in $\mathbb{P}^{15}$ such that there is a complete group law on $\iota(\operatorname{Jac} C)$.*

Proof. Let x_0 be as in Lemma 4.7, let $P = (x_0, y_0) \in C(\mathbb{F}_{q^4})$ where y_0 is a choice of square root of $f(x_0)$. The Galois orbit of P is $\{P, P^\sigma, \overline{P}, \overline{P}^\sigma\}$ where σ is the Frobenius.
Now we construct points $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ such that $\Theta_{\alpha_0} \cdot \Theta_{\alpha_1} \cdot \Theta_{\alpha_2} \cdot \Theta_{\alpha_3} = \emptyset$. We take $\alpha_0 = P + P^\sigma, \alpha_1 = P^\sigma + \overline{P}, \alpha_2 = \overline{P} + \overline{P}^\sigma, \alpha_3 = \overline{P}^\sigma + P$ in $\operatorname{Jac} C$. They verify the relations

$$\Theta_{\alpha_0} \cdot \Theta_{\alpha_1} = t^*_{\alpha_0}(\Theta \cdot \Theta_{\overline{P}-P}) = t^*_{\alpha_0}(\overline{P}),$$

$$\Theta_{\alpha_0} \cdot \Theta_{\alpha_3} = t^*_{\alpha_0}(\Theta \cdot \Theta_{\overline{P}^\sigma - P^\sigma}) = t^*_{\alpha_0}(\overline{P}^\sigma).$$

So the divisor $D = \sum \Theta_{\alpha_i}$ is ample, symmetric, rational by construction, and without rational points according to relations above. □

References

[BL95] W. Bosma and H.W.jun. Lenstra. Complete systems of two addition laws for elliptic curves. *J. Number Theory*, 53(2):229–240, 1995.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BL07] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. Kurosawa, Kaoru (ed.), Advances in cryptology – ASIACRYPT 2007. 13th international conference on the theory and application of cryptology and information security, Kuching, Malaysia, December 2-6, 2007. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 4833, 29-50 (2007)., 2007.

[Deb86] O. Debarre. Sur la démonstration de A. Weil du théorème de Torelli pour les courbes. *Compositio Math.*, 58(1):3–11, 1986.

[Kem] G. Kempf. Appendix to *"Varieties defined by quadratic equations"* by D. Mumford. In: Questions on algebraic varieties. CIME.

[LR85] H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, 79:603–610, 1985.

[LR87] H. Lange and W. Ruppert. Addition laws on elliptic curves in arbitrary characteristics. *J. Algebra*, 107(1):106–116, 1987.

[Mum75] David Mumford. *Curves and their Jacobians*. The University of Michigan Press, Ann Arbor, Mich., 1975.