An analog of the Edwards model for Jacobians of genus 2 curves

arxiv:2211.01450 — joint with E. Victor Flynn

Kamal Khuri-Makdisi
American University of Beirut

SAGA, CIRM, Luminy
February 2023

1. Projective embeddings of an abelian variety

- Let A be a principally polarized abelian variety, with $\dim A = g$. Important example: $A = \operatorname{Jac} C$, $g = \operatorname{genus}(C)$.
- The principal polarization is given up to translation by $\mathcal{L} = \mathcal{O}_A(\Theta)$. We have $\dim H^0(A, \mathcal{L}^k) = k^g$ for $k \geq 1$.
- For $k \geq 3$, the bundle $\mathcal{L}^k$ gives a projective embedding of A, for example elliptic curve $\hookrightarrow \mathbf{P}^2$, or abelian surface $\hookrightarrow \mathbf{P}^8$.
- If $k = 4$ [or above], the equations are generated by quadrics. For abelian surfaces: 72 quadrics in $\mathbf{P}^{15}$. Nice symmetric equations but unwieldy. (Elliptic curves: 2 quadrics in $\mathbf{P}^3$.)
- The bundle $\mathcal{L}^2$ gives a morphism that is not an embedding. For $\operatorname{Jac} C$ in genus 2, embeds $A/[-1] \hookrightarrow \mathbf{P}^3$ as Kummer quartic. (Elliptic curves: $E \to \mathbf{P}^1$, basically x-coord. map.)
- Edwards model of elliptic curves: $E \hookrightarrow \mathbf{P}^1 \times \mathbf{P}^1$ basically via $P \mapsto (x(P), x(P + P_1))$ with fixed $P_1 \in E[4]$. Can get $E^{aff} \hookrightarrow \mathbf{A}^1 \times \mathbf{A}^1$ with all rational points in the affine part.
- Analog for abelian surfaces? (See [Lubicz & Robert 2016].) So $A = \operatorname{Jac} C \hookrightarrow \mathbf{P}^3 \times \mathbf{P}^3$.

2. The embedding into $\mathbf{P}^3 \times \mathbf{P}^3$

Setup: $A = \operatorname{Jac} C$, C a genus 2 curve/$\mathbf{K}$ ($y^2 =$ sextic, char $\mathbf{K} \neq 2$). Make further rationality assumptions, most notably a rational $D_1 \in A[4](\mathbf{K})$ and a rational Richelot isogeny $A \to A/\langle 2D_1, 2D_2 \rangle$ with $D_2 \in A[4]$, $2D_2 \in A[2](\mathbf{K})$, and $e_4(D_1, D_2) = -1$. Can parametrize all these over $\mathbf{K}[a, b, c]$, after inverting a discriminant.

Kummer map: $D \mapsto \ell(D) = [\ell_1(D) : \ell_2(D) : \ell_3(D) : \ell_4(D)] \in \mathbf{P}^3$.

The embedding: Send $D \in A$ to the following point in $\mathbf{P}^3 \times \mathbf{P}^3$:
$D \mapsto (\ell(D), \ell(D + D_1)) = ([u_1 : u_2 : u_3 : u_4], [y_1 : y_2 : y_3 : y_4])$.

Basic questions: (i) What are the generators of the bihomogeneous ideal $I \subset \mathbf{K}[\{u_i\}, \{y_j\}]$ defining the embedding? (ii) What are the equations of the group operation on A?

A remark about I: The bidegree (2,2) part of I defines A scheme-theoretically. Reason: combine our embedding with Segre to get $A \hookrightarrow \mathbf{P}^{15}$, $D \to [u_i y_j]_{i,j}$, which is like the embedding by $\mathcal{L}^4$. This new embedding is given by quadrics in the $u_i y_j$ variables, so linear combinations of $u_i y_j u_k y_l$, so bidegree (2,2). Note $\dim I_{2,2} = 36$ plus 36 "trivial" quadrics $u_i y_j \cdot u_k y_l = u_i y_l \cdot u_k y_j$.

3. The defining equations: generators of I

$D \mapsto (\ell(D), \ell(D + D_1)) = ([u_1 : u_2 : u_3 : u_4], [y_1 : y_2 : y_3 : y_4])$.

Theorem: I is generated by certain explicit elements of the following bidegrees:

- One element of bidegree (4,0) (Kummer quartic in the $\{u_i\}$)
- One element of bidegree (0,4) (same, in the $\{y_j\}$)
- Four elements of bidegree (2,1) and their "mirror images" of bidegree (1,2)
- five more elements of bidegree (2,2).

Ingredients: (i) general theory (theta functions) to find dim $I_{k,l}$ and control the bidegrees that generate I; (ii) careful study of $I_{2,1}$ and $I_{1,2}$, which connects to $I_{4,0}$ and $I_{0,4}$; (iii) finding further elements in $I_{2,2}$ from the above and other considerations, plus symbolic computation over $\mathbf{K}[a, b, c]$; (iv) certifying that we have generated the full spaces in bidegrees (2,2) and below (compute minors of certain matrices over $\mathbf{K}[a, b, c]$, and show they are divisible only by factors of the discriminant, hence are nonzero).

4. The group law: nicer (!) than the defining equations

Addition law for theta functions $\Longrightarrow$ $\ell_i(D'+D'')\ell_j(D'-D'') =$ linear combination of $\ell_{j_1}(D')\ell_{j_2}(D'')\ell_{j_3}(D')\ell_{j_4}(D'')$.

Consequence: $u_i(D+E)y_j(D-E) = \ell_i(D+E)\ell_j(D-E+D_1) =$ linear combination of $u_{i_1}(D)y_{i_2}(D)u_{i_3}(E)y_{i_4}(E)$. Similar formulas for $y_i(D+E)u_j(D-E)$.

Producing the u-coordinates of $D+E$: [similarly for y-coordinates] the projective u-coordinates are any column (or linear combination of columns) of the 4×4 matrix

$$\begin{pmatrix} u_1(D+E)y_1(D-E) & u_1(D+E)y_2(D-E) & \cdots \\ u_2(D+E)y_1(D-E) & u_2(D+E)y_2(D-E) & \cdots \\ u_3(D+E)y_1(D-E) & u_3(D+E)y_2(D-E) & \cdots \\ u_4(D+E)y_1(D-E) & u_4(D+E)y_2(D-E) & \cdots \end{pmatrix}$$

N.B. The fact that the above matrix has rank 1 is the source of some of our elements of $I_{2,2}$, for general D and specific Es. Also note that the $y_i(D-E)$ cannot all be zero, so at least one column will work. (Something similar happens for Edwards elliptic curves.)

5. Affine points and universal group law

A hyperplane without rational points: when certain expressions are not squares in $\mathbf{K}$, we can find $c_1, \dots, c_4 \in \mathbf{K}$ such that $\{D \in A(\overline{\mathbf{K}}) \mid \sum_i c_i \ell_i(D) = 0\}$ is the union of two conjugate curves defined only over a quadratic extension of $\mathbf{K}$, and which intersect in two conjugate points that are similarly not defined over $\mathbf{K}$. ($\lambda = \sum c_i \ell_i$ vanishes on a reducible curve without rational points in, roughly, the linear system $|2\Theta|$.) In that case, when we restrict the us and the ys to the affine part where $\lambda \neq 0$, we capture all the poinrs of $A(\mathbf{K})$.

Universal affine group law: Using the same $c_1, \dots, c_4$, take linear combinations of the columns of the previous 4×4 matrix $(u_i(D+E)y_j(D-E))_{ij}$; the common factor is $\sum_j c_j y_j(D-E) = \sum_j c_j \ell_j(D-E+D_1) = \lambda(D-E+D_1) \neq 0$, because $D-E$ is $\mathbf{K}$-rational. So the linear combination produces a universal formula for the projective point $[u_i(D+E)]_i$. The same argument gives a universal formula for $[y_i(D+E)]_i$. (See also [Arène & Cosset 2012] and [Arène-Cosset-Ritzenthaler 2012].)