Using algebraic values of modular forms to obtain models of modular curves

Kamal Khuri-Makdisi
Center for Advanced Mathematical Sciences
American University of Beirut
kmakdisi@aub.edu.lb

Preprint on arXiv:

AGCT-13, C.I.R.M., Luminy, March 2011
Models of curves: an example

Given: $X \subset \mathbb{P}^3/\mathbb{F}_{13}$, a genus 1 intersection of 2 quadric surfaces, passing through $\{P_i\} = [1 : 0 : \pm 1 : 0], [1 : 4 : 0 : 3], [1 : -1 : 0 : 1], [1 : 10 : 0 : 9], [1 : 2 : \pm 3 : 4], [1 : 6 : \pm 3 : 10], [1 : 5 : \pm 3 : -1]$. Find the equations.

Answer: Using coordinates $[T_0 : T_1 : T_2 : T_3]$, we have $T_2^2 - T_1T_3 - T_0^2 = 0$. Found by linear algebra to solve for the coefficients $\{c_{jk}|j \leq k\}$ that make $\sum c_{jk}T_jT_k = 0$ on all the $P_i$. (Interpolation!)

Where this came from: $X = (\text{elliptic curve } y^2 = x^3 + 1)$, $X \hookrightarrow \mathbb{P}^3$ by the line bundle $\mathcal{L} = \mathcal{L}(4O)$. $H^0(X, \mathcal{L})$ has basis $\{T_0, T_1, T_2, T_3\} = \{1, x, y, x^2\}$.

Products: Represent $T_i$ by a vector of “values”: for example, $T_1 = (0, 0, 4, -1, 10, 2, 2, 6, 6, 5, 5)$. Each product $T_jT_k \in H^0(X, \mathcal{L}^2)$ is determined by its values at the 11 points (take componentwise product). Note $\mathcal{L}^2 = \mathcal{L}(8O)$ has degree 8, so 9 points would have been enough.
Models of curves: the general formalism

Setup: $X \subset \mathbf{P}^n/K$ a smooth projective curve of degree $d$ and genus $g$. Line bundle on $X$ is $\mathcal{L} = \mathcal{O}_X(1)$. Homogeneous ideal $I = I_X$ defining $X$.

Ambient polynomial ring: $\mathcal{R} = K[T_0, \cdots , T_n] = K \oplus V \oplus \text{Sym}^2 V \oplus \cdots$. Each $T_j$ maps to $s_j \in H^0(X, \mathcal{L})$. The projective coordinate ring of $X$ is $\mathcal{R}/I_X = K \oplus V_1 \oplus V_2 \oplus \cdots$, where $V_k = \text{Sym}^k V/I_k \hookrightarrow H^0(X, \mathcal{L}^k)$.

Further assumption: we know that $I$ is generated by $\{I_k | k \leq m\}$. E.g., if $d \geq 2g + 2$ and $V = V_1 = H^0(X, \mathcal{L})$, then $m = 2$ works: $X$ is projectively normal, and $I$ is generated by $I_2 = \ker(\text{Sym}^2 V \to V_2)$ (C-M-F-St D).

Efficiency: Say $d \geq 2g + 2$ and $d = O(g)$ above. Then $\dim V_1, V_2$ are $O(g)$ but $\dim I_2, \text{Sym}^2 V$ are $O(g^2)$. Get fast algorithms using $V_1 \times V_1 \to V_2$.

Interpolating to find $I$: Knowing $md + 1$ points $P_0, \ldots, P_{md}$ on $X \subset \mathbf{P}^n$ determines $I_{\leq m}$ and enables multiplication $V_k \times V_\ell \to V_{k+\ell}$ for $k + \ell \leq m$. 
The modular curve $X(N)$

Complex points: $X(C) = X(N)(C) = \widetilde{\Gamma \backslash \mathcal{H}}$, where $\Gamma = \Gamma(N)$.

Line bundle: When $N \geq 3$, there exists a line bundle $\mathcal{L}$ on $X$ such that $H^0(X, \mathcal{L}^k) = \mathcal{M}_k(\Gamma) =$ space of modular forms of weight $k$ on $\Gamma(N)$. Moreover, $\deg \mathcal{L}^2 = 2g - 2 + \#\text{cusps} \geq 2g + 2$. Use $\mathcal{L}$ or $\mathcal{L}^2$ to get projective model for $X$ via interpolation.

Evaluating a modular form at a point of $X$: Points on the open subset $Y(N)$ ("$\Gamma \backslash \mathcal{H}$") "are" a tuple $(E, P_1, P_2)$ with $E$ an elliptic curve, $P_1, P_2 \in E[N]$, Weil pairing $e_N(P_1, P_2) = \zeta_N = a$ fixed primitive $N$th root of 1. Can view modular forms algebraically as functions of $(E, \eta, P_1, P_2)$ where $\eta \in \Omega^1(E)$. $f \in \mathcal{M}_k$ means $f(E, c\eta, P_1, P_2) = c^{-k}f(E, \eta, P_1, P_2)$. Example: the choice of $\eta$ normalizes an equation $E : y^2 = x^3 + ax + b$ with $\eta = dx/2y$. Then $a, b$ are essentially weight 4,6 Eisenstein series on $\Gamma(1)$. 
Eisenstein series on $\Gamma(N)$

**Analytic definition:** For $i,j \in \mathbb{Z}/N\mathbb{Z}$, let $Q = [i]P_1 + [j]P_2 \in E[N]$. Then $G_{k,(i,j)} = G_{k,Q} \in \mathcal{M}_k(\Gamma)$ is defined as a function of $(E, \eta, P_1, P_2)$ by:

$$(E, \eta, Q) \cong (\mathbb{C}/\Lambda, dz, \alpha \in N^{-1}\Lambda/\Lambda) \mapsto G_{k,Q} = \sum_{\ell \in \Lambda - \{-\alpha\}} (\ell + \alpha)^{-k}.$$ 

As written, this converges only for $k > 2$, but can be fixed for $k = 1, 2$. Note above that $\Lambda$ is the lattice of periods of $\eta$ on $E$.

**Algebraic values:** For example, if $Q = (x_Q, y_Q)$, then $x_Q \sim \wp(\alpha) \sim G_{2,Q}$ and $y_Q \sim \wp'(\alpha) \sim G_{3,Q}$. In weight 1, the $G_1$'s can be related to slopes $(y_P - y_Q)/(x_P - x_Q)$. A wider class of modular forms can be obtained from coefficients of Laurent expansions of rational functions $f \in K(E)$ with $\text{supp div } f \subset E[N]$. All can be evaluated purely algebraically (exact arithmetic, no infinite series) from the moduli interpretation.
Projective embedding of $X(N)$

**Theorem (KKM):** All the algebraic modular forms listed above belong to the ring of modular forms generated by weight 1 Eisenstein series, and this ring contains all forms in weights $\geq 2$. (Only $S_1(\Gamma(N))$ is missing). Hence the incomplete linear series $V = Ei_{s_1}(\Gamma(N)) \subset M_1(\Gamma) = H^0(X, \mathcal{L})$ gives a projective embedding of $X$. Over $\mathbb{C}$, the projective coordinate ring is $\mathcal{R}/I = \mathbb{C} \oplus Ei_{s_1} \oplus M_2 \oplus M_3 \oplus \cdots$. Moreover, $I$ is generated by $I_{\leq 3}$.

**Computing generators for $I$:** Interpolate through sufficiently many points of $X$. A nice way is to fix one elliptic curve $E_0$ and to consider all possible level $N$ structures on it. Thus $E_0 \in X(1)$ and we take the points of $\pi^{-1}(E_0)$ where $\pi : X(N) \to X(1)$. This gives enough points to find relations all the way up to $I_{\leq 11}$ if needed. The calculations take place over $\mathbb{Q}(E_0[N])$ but one should be able to lump Galois conjugates together and work over $\mathbb{Q}(\zeta_N)$ or maybe even over $\mathbb{Q}$. 
What are the generators of $I$?

The elements of $I_1$ are the linear relations between the Eisenstein series $\{G_{1,Q} : Q \in E[N]\}$. These were already known to Hecke. For example, $G_{1,-Q} = -G_{1,Q}$. There is also a second, subtler, symmetry of order 2, that is essentially a duality under the Fourier transform with respect to the Weil pairing. For example, if $N = 13$, then there are 169 possible $Q$, but the first symmetry reduces the dimension to 84, and the subtle symmetry brings this further down to 42. (General fact: the “easy” symmetries bring you down to the number of cusps, but the space $Eis_1$ has half that dimension.)

Several elements of $I_2$ and $I_3$ are known. For example, if $P, Q, R \in E[N] - \{O\}$ and $P + Q + R = O$, then $(G_{1,P} + G_{1,Q} + G_{1,R})^2 \sim G_{2,P} + G_{2,Q} + G_{2,R}$. Eliminate the $G_{2,P}$ to get elements of $I_2$. Observation (Borisov-Gunnells, also work in progress by KKM-Raji): many relations are parallel to the Manin relations between modular symbols. But these do not account for everything.
Example: results on the generators of $I$, when $N = 13$

To avoid coefficient explosion, I worked modulo $p = 10037$. I chose $E_0/F_p$ such that $E_0[13] \subset E[F_p]$. Hence all points of $\pi^{-1}(E_0)$ were defined over $F_p$, simplifying computations. I computed $I_{\leq 3}$ by interpolation, and studied the ideal $J$ defined by the known relations in weights 1 and 2.

Hilbert-Poincaré series: The Hilbert series for $\mathcal{R}/I$ is $1 + (\dim \mathcal{E} \cdot s_1)t + (\dim \mathcal{M}_2)t^2 + \cdots = 1 + 42t + 133t^2 + 224t^3 + 315t^4 + \cdots$. This matches up with the known dimension formulas ($g = 50$, $\deg \mathcal{L} = 91$). On the other hand, the Hilbert series for $J$ is $1 + 42t + 161t^2 + 224t^3 + 315t^4 + \cdots$. (There are 28 “mysterious” relations in weight 2.)

Remarks: In this example, $I$ is generated by $I_{\leq 2}$. With respect to grevlex order in 169 variables, $I$ has a Gröbner basis with 127 elements in weight 1, 770 in weight 2, and 60 in weight 3. The numbers for $J$ are 127 in weight 1, 742 in weight 2, and 174 in weight 3.
Can this be generalized to Shimura curves?

**Hopefully:** we can try to evaluate algebraic modular forms on an indefinite quaternion algebra $B$ and to interpolate. This would need:

1) Some “simple” modular forms on $B$ with a nice moduli interpretation. (Eisenstein series are out: there are no cusps). Perhaps restriction of simple Hilbert modular forms from a real quadratic field $F \subset B$?

2) Understanding the algebra generated by the “simple” forms. We can also consider Hecke algebra orbits of products of forms; this mixes up automorphic representations. At least, we need a bound on the regularity of the ideal sheaf attached to $I$, to bound the $I_{\leq m}$ that we need to compute.

**A last question for the elliptic case:** Can one do these computations for larger $N$ in reasonable time? It would be nice to do Gröbner bases taking into account the action of $SL(2, \mathbb{Z}/N\mathbb{Z})$. 