Igusa class invariants and the AGM

David Kohel

with

Christophe Ritzenthaler

et al.

Canonical Lifting and the AGM

The AGM algorithm applies to any ordinary hyperelliptic curve C/k of genus 2, where $k = \mathbb{F}_{2^r}$, which we may represent in Weierstrass form:

$$C/k : y^2 + v(x)y = u(x)v(x)$$

where v is squarefree of degree 3 and u is of degree at most 3.

The Jacobian J of C, has four 2-torsion points over some extension field, generated by the three points $(\alpha_i, 0)$ where $v(\alpha_i) = 0$.

Let K be the unramified extension of degree r over $\mathbb{Q}_2$. The AGM algorithm constructs a canonical lift — a principally polarized abelian surface $\mathcal{J}/K$ which lifts the polarised Jacobian J/k, together with its ring of endomorphisms: $\mathrm{End}_K(J) \simeq \mathrm{End}_k(\mathcal{J})$. We do so by recursively solving for a sequence of 2-adic numbers which converge to 'invariants' associated to $\mathcal{J} = \mathrm{Jac}(\mathcal{C})$.

AGM: Initializing the Curve

Lift C over K: Lift v and u arbitrarily to V and U in $K[x]$ and set

$$C/K : Y^2 = (2y + V(x))^2 = V(x)(V(x) + 4U(x)).$$

Extend K, if necessary, so that $V(x)$ has three distinct roots α_1, α_2, and α_3. Then we can write in K,

$$C/K : Y^2 = \prod_{i=1}^{3}(x - \alpha_i)\prod_{i=1}^{3}(x - (\alpha_i + 4\beta_i)).$$

Initialise of 2-adic invariants of the curve:

$$\begin{array}{lll} e_1 = \alpha_1, & e_3 = \alpha_2, & e_5 = \alpha_3, \\ e_2 = \alpha_1 + 4\beta_1, & e_4 = \alpha_2 + 4\beta_2, & e_6 = \alpha_3 + 4\beta_3 \end{array}$$

AGM: Initialising the Lift

The Thomae formulas give us 4 initial invariants

$$
\begin{aligned}
A &= \sqrt{(e_1-e_3)(e_3-e_5)(e_5-e_1)(e_2-e_4)(e_4-e_6)(e_6-e_2)} \\
B &= \sqrt{(e_1-e_3)(e_3-e_6)(e_6-e_1)(e_2-e_4)(e_4-e_5)(e_5-e_2)} \\
C &= \sqrt{(e_1-e_4)(e_4-e_5)(e_5-e_1)(e_2-e_3)(e_3-e_6)(e_6-e_2)} \\
D &= \sqrt{(e_1-e_4)(e_4-e_6)(e_6-e_1)(e_2-e_3)(e_3-e_5)(e_5-e_2)}
\end{aligned}
$$

where the square root of an element of the form $1 + 8\mathcal{O}_K$ is taken as the unique element of $\mathbb{Z}_q$ of the form $1 + 4\mathcal{O}_K$.

These numbers are 2-adic analogues of special values of the theta functions for the period lattice of a CM Jacobian.

AGM: Recursion

The AGM recursion starts from the initial values:

$$(A_0, B_0, C_0, D_0) := (1, B/A, C/A, D/A),$$

then we use duplication formulas on these elements of K:

$$(A_n, B_n, C_n, D_n) \mapsto (A_{n+1}, B_{n+1}, C_{n+1}, D_{n+1})$$

These formulas are:

$$A_{n+1} = \frac{A_n + B_n + C_n + D_n}{4} \quad C_{n+1} = \frac{\sqrt{A_n C_n} + \sqrt{B_n D_n}}{2}$$
$$B_{n+1} = \frac{\sqrt{A_n B_n} + \sqrt{C_n D_n}}{2} \quad D_{n+1} = \frac{\sqrt{A_n D_n} + \sqrt{B_n C_n}}{2}$$

The sequence of 4-tuples (A_n, B_n, C_n, D_n) converges to a Galois cycle of invariants of curves.

AGM: Reconstruction of the Curve

The Rosenhain normal form of a genus 2 curve $\mathcal{C}$ is a model

$$\mathcal{C} : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3),$$

where the λ_i are given by the following expressions:

$$\lambda_1 = -\frac{\theta_1^2\theta_3^2}{\theta_6^2\theta_4^2}, \quad \lambda_2 = -\frac{\theta_2^2\theta_3^2}{\theta_6^2\theta_5^2}, \quad \lambda_3 = -\frac{\theta_2^2\theta_1^2}{\theta_4^2\theta_5^2}$$

The θ_i^2 are determined from A_n, B_n, C_n, D_n as:

$$\begin{aligned}
\theta_1^2 &= B_n, & \theta_2^2 &= D_n,\\
\theta_3^2 &= \frac{\sqrt{A_{n-1}B_{n-1}} - \sqrt{C_{n-1}D_{n-1}}}{2}, & \theta_4^2 &= \frac{A_{n-1} - B_{n-1} + C_{n-1} - D_{n-1}}{4},\\
\theta_5^2 &= \frac{\sqrt{A_{n-1}C_{n-1}} - \sqrt{B_{n-1}D_{n-1}}}{2}, & \theta_6^2 &= \frac{A_{n-1} - B_{n-1} - C_{n-1} + D_{n-1}}{2}.
\end{aligned}$$

This allows is to write down a p-adic approximation to the canonical lift of C/k (or a Galois conjugate) after determining the invariants A_n, B_n, C_n, D_n to sufficient precision.

AGM: Reconstruction of Invariants

Given the λ_i we can then compute the Igusa invariants I_2, I_4, I_6, I_{10} of the associated curve (or sextic), then define the "absolute invariants"

$$i_1 = I_2^5/I_{10}, \quad i_2 = I_2^3 I_4/I_{10}, \quad i_3 = I_2^2 I_6/I_{10}.$$

From these absolute invariants, determined to sufficient precision, we use LLL on the space of p-adic relations among the powers $\{1, i_k, i_k^2 \ldots, i_k^{2h}\}$ of degree $2h$ to solve for

$$H_1(i_1) = H_2(i_2) = H_3(i_3) = 0.$$

Such relations appear as short vectors in the space of all relations over $\mathbb{Z}_p$ to some precision p^N.

In addition, we reconstruct additional relations

$$L_1(i_1, i_2, i_3) = L_2(i_1, i_2, i_3) = 0,$$

in order to record the dependencies among the diffferent invariants.

Class invariants on $\mathcal{M}_2$

Remark. The CM invariants i_1, i_2, and i_3 define special points on the three-dimensional moduli space $\mathcal{M}_2/\mathbb{Q}$. It is a rational variety (birational to $\mathbb{P}^3$) whose function field is generated by the *functions* i_1, i_2, i_3.

The special CM invariants for K are cut out, over $\mathbb{Q}$, by a zero dimensional subscheme of degree $2h$, defined by the ideal

$$(H_1, H_2, H_3, L_1, L_2)$$

of relations. The relations H_1, H_2, and H_3 determine a subscheme of degree $(2h)^3$. Over a splitting field, the additional relations L_1 and L_2 removes a combinatorial matching problem among $(2h)^3$ choices for independent roots of the H_j.

We note that the polynomials H_1, H_2, and H_3 are not in general monic. The possible prime divisors of the leading coefficient are characterised by Goren and Lauter.

Curve Selection

The starting point for the AGM lifting is a random draw — we first have to blindly search through curves to find one that is a suitable starting point. From a particular curve C/k, we can determine the minimal polynomial of Frobenius π:

$$\chi = x^4 - s_1 x^3 + s_2 x^2 - q s_1 + q^2,$$

where $q = |k|$. Moreover, we know that $\bar{\pi} = q/\pi$ exists in the endomorphism ring $\mathrm{End}(J)$.

The ring $\mathbb{Z}[\pi]$ is contained in the maximal order $\mathcal{O}_K$ of $K = Q(\pi)$; the ring $\mathbb{Z}[\pi, \bar{\pi}]$ is larger by some power of 2. We would like to identify a curve with $\mathrm{End}(J) = \mathcal{O}_K$, so we need to characterise the indices

$$\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathrm{End}(J) \subseteq \mathcal{O}_K.$$

And secondly, we would like to restrict to K of reasonably small class number h and, furthermore to $L = K(\pi + \bar{\pi})$ of class number 1. In the class of the maximal order $\mathcal{O}_K$ such that $\mathcal{O}_L$ has class number 1, we know that the degree of the CM subscheme we seek is exactly $2h$.

Strategy for Algorithm

1. For a given small finite field $k = \mathbb{F}_{2^r}$, choose a curve defined by $u(x)$, $v(x)$ in $k[x]$, hence with field of moduli equal to k, then determine theta constants over some extension.

2. Determine index of $\mathbb{Z}[\pi, \bar{\pi}]$ in the maximal order O_K, the class number of $\mathcal{O}_K$, and the structure of the ring extension $O_K/\mathbb{Z}[\pi, \bar{\pi}]$.

3. Let $f_1(\pi)/m_1, \ldots, f_t(\pi)/m_t$ generate O_K over $\mathbb{Z}[\pi, \bar{\pi}]$. For each m_i determine the action of π on $J[m_i]$ and reject the curve if the restriction of $f_i(\pi)$ to $J[m_i]$ is nonzero.

4. Lift the theta constants and reconstruct by LLL the defining relations for the CM igusa invariants.

Examples. Here we provide a few examples of canonical lifts of the Igusa invariants of hyperelliptic curves of the form

$$C : y^2 + v(x)y = v(x)u(x)/\mathbb{F}_{2^n}.$$

1. For the curve $C/\mathbb{F}_2$ with $v = x^3 + 1$ and $u = x^2$, the minimal polynomial of Frobenius in $\mathrm{End}(J)$ is equal to

$$x^4 + 2x^3 + 3x^2 + 4x + 4,$$

defining an imaginary quadratic extension of the field $\mathbb{Q}(\sqrt{2})$. The relations for the canonical lifts fo the Igusa invariants are:

$$\begin{aligned}
&i_1^2 - 531441 i_1 + 55788550416,\\
&i_2^2 - 426465 i_2 - 68874753600,\\
&i_3^2 - 216513 i_3 - 221011431552,\\
&140 i_1 - 243 i_2 + 135 i_3,\\
&69 i_1 - 119 i_2 + 66 i_3 - 104976.
\end{aligned}$$

2. For the curve $C/\mathbb{F}_2$ with $v = x^3 + x^2 + 1$ and $u = x^2 + 1$ the minimal polynomial of Frobenius in $\mathrm{End}(J)$ is equal to

$$x^4 + x^3 + x^2 + 2x + 4,$$

defining an imaginary quadratic extension of the field $\mathbb{Q}(\sqrt{13})$. The relations for the canonical lifts fo the Igusa invariants are:

$$\begin{aligned}
&4i_1^2 + 8218017i_1 + 146211169851, \\
&i_2^2 + 1008855i_2 - 342014432400, \\
&i_3^2 + 1368387i_3 - 240090131376, \\
&4480i_1 + 7499i_2 - 12255i_3, \\
&716i_1 + 1212i_2 - 1971i_3 - 1666737
\end{aligned}$$

3. For the curve $C/\mathbb{F}_2$ with $v = x^3 + x^2 + 1$ and $u = x^2$ the minimal polynomial of Frobenius in $\mathrm{End}(J)$ is equal to

$$x^4 + x^3 + 3x^2 + 2x + 4,$$

defining an imaginary quadratic extension of the field $\mathbb{Q}(\sqrt{5})$. The relations for the canonical lifts fo the Igusa invariants are:

$$\begin{aligned}
&4i_1^2 + 115322697i_1 - 10896201253125,\\
&i_2^2 + 9073863i_2 - 2152336050000,\\
&i_3^2 + 14410143i_3 - 1214874126000,\\
&896i_1 + 369i_2 - 2025i_3,\\
&300i_1 + 122i_2 - 677i_3 + 273375
\end{aligned}$$

4. Let $C : y^2 + v(x)y = u(x)v(x)$ be the hyperelliptic curve over $\mathbb{F}_{2^3} = \mathbb{F}_2[w]$ where $w^3 + w + 1 = 0$ where u and v are given by

$$u = (w^2 + w + 1)x^2 + w^2 x + w^2,$$
$$v = x^3 + (w^2 + w + 1)x^2 + x + w + 1.$$

The minimal polynomial of Frobenius on the Jacobian of C is

$$\chi = x^4 - 3x^3 + 3x^2 - 24x + 64,$$

defining an imaginary quadratic extension of the field $\mathbb{Q}(\sqrt{61})$. The ring $\mathbb{Z}[\pi] = \mathbb{Z}[x]/(\chi)$ has index 8 in $\mathcal{O}_K$, but $\mathbb{Z}[\pi, \bar{\pi}] = \mathcal{O}_K$. And the class number of $\mathcal{O}_K$ is 3 (for other curves over $\mathbb{F}_{2^3}$ the class number is 6 or 12).

The defining relations of canonical lifts of the Igusa invariants are given on the following page...

$$
\begin{aligned}
&2^6 3^{42} i_1^6 - 234491210550311611628857604795305712539 2i_1^5 \\
&-11263958439030423845617227684513015003940255658628315 6i_1^4 \\
&-2177415103395854060041246748534717663224784831560700934285483051075i_1^3 \\
&-15936419940544408709376306530703638369363662226923214713038080125439887 02i_1^2 \\
&-77232882710173372962531506548540432736193603391160944219774880180377797557219 1i_1 \\
&+3229972085033537914429040962774032984067557246793927712359509170553758171259197704 3, \\
&3^{18} i_2^6 + 30345890982308051019805350i_2^5 \\
&-28813619164983289391706207738871090837 5i_2^4 \\
&+7531108325158213677490969908994270293693678526563 75i_2^3 \\
&-649127309475920539312400482687597914255658885551562830000i_2^2 \\
&+512065244591992233358858681228726038539915018527646447680800000i_2 \\
&-24272920155156909628661627097113112044952744390034202392223340 8000000, \\
&3^{24} i_3^6 + 274374611813847636940118813 46i_3^5 \\
&-352040806049318452655962733807057489240331i_3^4 \\
&+11789221533340810664841739684807257004447396394229660 03i_3^3 \\
&+509928790982645514856427558535377505816658890920020722687216i_3^2 \\
&+228130282826174574878551565831919365949825510821776329730159434 24i_3 \\
&-194627707132727224036285973133204401034007902817343828521298858611945472, \\
&633895738920000i_1^3 + 8517595035131037i_1^2 i_2 - 2422318926838275i_1^2 i_3 \\
&+52888701255649776 0i_1^2 - 2671415018933342i_1 i_2^2 + 10103099744994882i_1 i_2 i_3 \\
&+4980682705166674 79i_1 i_2 - 31685827189272975i_1 i_3 + 184986870963530306 0i_1 \\
&+1100241578433867 4i_2^3 - 16195247750833904i_2^2 i_3 + 800164846490774071i_2^2 \\
&+228622640238253145i_2 i_3, \\
&525860400509222240i_1^3 + 348046133200631478i_1^2 i_2 + 197889720810578 10i_1^2 i_3 \\
&+2623630964591332972 8i_1^2 - 1611043809046282405i_1 i_2 i_3 - 3753782789770657910i_1 i_2 \\
&+1519575925397564523i_1 i_3^2 + 2446649956939951033i_1 i_3 - 1746640058954627936i_1 \\
&+1153484491100961901i_2 i_3^2 - 6729087358177501571i_2 i_3 - 3413986566072687702i_2 \\
&-1585090558318459827i_3^3 - 1037783410918613004 0i_3^2 - 12385238120639343570i_3, \\
&14283163413570062i_1 i_2^2 - 21965217242026530i_1 i_2 i_3 - 9110050391167390 6i_1 i_2 \\
&+8753819554156320i_1 i_3^2 + 7414107877502670i_1 i_3 - 8509767043223936 0i_1 \\
&+3160028075123540i_2^3 - 19415412647408141i_2^2 i_3 - 11227855503503951i_2^2 \\
&+28513098102060099i_2 i_3^2 - 10104997618986857 3i_2 i_3 - 10890112918608090i_3^3 \\
&+42818455041104040i_3^2
\end{aligned}
$$