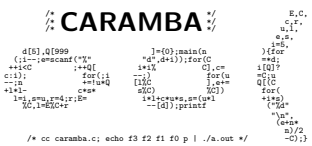
Computing Theta functions in quasi-linear time in genus two and above

Hugo Labrande and E. Thomé



ANTS-XII, Kaiserslautern, 2016/08/31

Outline

Jacobi's theta function

Definition (Jacobi's theta function)

For $z, \tau \in \mathbb{C}$, $\operatorname{Im}\tau > 0$, and with $q = e^{i\pi\tau}$, $w = e^{i\pi z}$, we define:

$$\theta(z,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2} w^{2n}.$$

We also define *theta constants*:

$$\underbrace{\theta_0(0,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2}}_{\theta(z+0,\tau)\text{at } z=0} \quad \underbrace{\theta_1(0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2}}_{\theta\left(z+\frac{1}{2},\tau\right)\text{at } z=0} \quad \underbrace{\theta_2(0,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2+n}}_{\theta\left(z+\frac{\tau}{2},\tau\right)\text{at } z=0}.$$

Goal: Compute $\theta(z,\tau)$ to precision P in quasi-linear time $\widetilde{O}(P)$ (e.g. $O(\mathcal{M}(P)\log P)$).

Applications

- Modular functions:

$$j(\tau) = 54\frac{(\theta_0(0,\tau)^8 + \theta_1(0,\tau)^8 + \theta_2(0,\tau)^8)^3}{\theta_0(0,\tau)^8\theta_1(0,\tau)^8\theta_2(0,\tau)^8},$$

$$\eta(\tau) = \frac{\theta_0(0,\tau)\theta_1(0,\tau)\theta_2(0,\tau)}{2}.$$

- Analytic-algebraic link $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \simeq E(\mathbb{C})$
  - Coefficients of E from theta-constants;
  - Isomorphism $z \mapsto (\wp(z,\tau), \wp'(z,\tau))$ expressed with $\theta(z,\tau)$.
- Others: solutions to heat equation, ...

Naive algorithm

The series for θ converges reasonably fast, but not fast enough.

$$S_B(z,\tau) = 1 + \sum_{1 \le n \le B} q^{n^2}(w^{2n} + w^{-2n})$$

Convergence of partial sums $S_B(z,\tau)$

For $\tau \in \mathcal{F}$ (i.e. $|\tau| \ge 1$, $|\operatorname{Re}(\tau)| \le 1/2$) and z reduced:

$$|\theta_0(z,\tau) - S_B(z,\tau)| \le 3|q|^{(B-2)^2}$$

Similar thing for $\theta_1(z,\tau), \theta_2(z,\tau)$ and the theta-constants.

- If $B = O\left(\sqrt{P/\operatorname{Im}(\tau)}\right)$, S_B is accurate to P bits.
- $e^{i\pi\tau}$: $O(\mathcal{M}(P)\log P)$; each term $O(\mathcal{M}(P))$ (recurrence relations).

Total complexity: $O\left(\mathcal{M}(P)\sqrt{P/\operatorname{Im}(\tau)}\right)$ (better as $\operatorname{Im}(\tau)$ grows)

Better complexities

There is a well-known link between theta-constants and the arithmetic-geometric mean.

Dupont used that link to compute theta-constants in quasi-linear time.

We recently extended this to $\theta(z, \tau)$.

Arithmetic-geometric mean

AGM of positive integers

$$a_0, b_0 \in \mathbb{R}^+, \qquad a_{n+1} = (a_n + b_n)/2, \quad b_{n+1} = \sqrt{a_n b_n}.$$

Then $\mathrm{AGM}(a, b) = \lim_{n\to\infty} a_n$.

Quadratic convergence:

- $O(\log P)$ iterations for precision P;
- bit complexity $O(\mathcal{M}(P) \log P)$.

Generalizing the AGM to $\mathbb{C}$

Generalization to $\mathbb{C}$: several possible square roots.

- Many distinct AGM sequences starting from a pair (a_0, b_0).
- Good choice of signs:

$$|\sqrt{a_n} - \sqrt{b_n}| \leq |\sqrt{a_n} + \sqrt{b_n}|$$

- **Optimal** AGM sequence = good choice of signs at each step.
- If at most many bad choices: quadratic convergence.

Define $\mathrm{AGM}(a, b) = \lim_{n\to\infty} a_n$ where (a_n, b_n) is optimal:
well-defined homogeneous complex function.
Then computing P digits of $\mathrm{AGM}(a, b)$ costs $O(\mathcal{M}(P) \log P)$.

AGM and theta-constants

Proposition

$$\begin{aligned}\theta_0(0,2\tau)^2 &= \frac{\theta_0(0,\tau)^2+\theta_1(0,\tau)^2}{2}\\ \theta_1(0,2\tau)^2 &= \theta_0(0,\tau)\theta_1(0,\tau)\end{aligned}$$

i.e. $(\theta_0(0,2^n\tau)^2,\theta_1(0,2^n\tau)^2)_{n\geq 0}$ *is an AGM sequence.*

Actually for $\tau\in\mathcal{F}$ it is an optimal AGM sequence, so

$$\mathrm{AGM}(\theta_0(0,\tau)^2,\theta_1(0,\tau)^2)=1$$

We rephrase that using the homogeneity:

$$\mathrm{AGM}\left(1,\frac{\theta_1(0,\tau)^2}{\theta_0(0,\tau)^2}\right)=\frac{1}{\theta_0(0,\tau)^2}$$

Extracting τ

$$\theta_2(0,\tau)^2 = -i\tau\theta_1\left(0, \frac{-1}{\tau}\right)^2, \quad \theta_0(0,\tau)^2 = -i\tau\theta_0\left(0, \frac{-1}{\tau}\right)^2$$

Which means that

$$\mathrm{AGM}\left(1, \frac{\theta_2(0,\tau)^2}{\theta_0(0,\tau)^2}\right) = \frac{i}{\tau\theta_0(0,\tau)^2}$$

Jacobi's formula: $\theta_0(0,\tau)^4 = \theta_1(0,\tau)^4 + \theta_2(0,\tau)^4$, so

$$z \mapsto \frac{\mathrm{AGM}(1,z)}{\mathrm{AGM}\left(1, \sqrt{1-z^2}\right)} - i\tau$$

has $\frac{\theta_1(0,\tau)^2}{\theta_0(0,\tau)^2}$ as a zero.

Roadmap for genus 1 theta constants

- Expect τ known to precision (at least) P.
- Compute an approximation to $\frac{\theta_1(0,\tau)^2}{\theta_0(0,\tau)^2}$.
- Deduce approximations of other theta-constants: $\frac{\theta_2(0,\tau)^2}{\theta_0(0,\tau)^2}$.
- Use AGM to compute something which should be zero (we are using the action of $\mathrm{SL}_2(\mathbb{Z})$ here).
- Use the error made to improve on our initial approximation (Newton).

Bottom line: we reach complexity $O(M(P)\log P)$.

Uniformity of the $O()$ constant needs some extra care.

In genus 2

In genus 2: Borchardt mean of four numbers:

$$\mathcal{B}_2(x,y,z,t) = \left(\frac{x+y+z+t}{4}, \frac{\sqrt{x}\sqrt{y}+\sqrt{z}\sqrt{t}}{2}, \frac{\sqrt{x}\sqrt{z}+\sqrt{y}\sqrt{t}}{2}, \frac{\sqrt{x}\sqrt{t}+\sqrt{y}\sqrt{z}}{2}\right)$$

Good generalization of the AGM:

- *converges quadratically*;
- link with τ-duplication formula for genus 2 theta-constants

See Régis Dupont's PhD:

- $O(\mathcal{M}(P)\log P)$ algorithm for genus 2 theta-constants;
- Application: class polynomials in genus 2.

More on this later.

Outline

Strategy for theta function

Just like previously:

- Find a quadratically convergent sequence involving theta-functions;
- Find a function f that gives predictable when evaluated on some values of theta-functions;
- Use two-dimensional Newton method on $f : \mathbb{C}^2 \to \mathbb{C}^2$.

Our idea: use τ-duplication formulas for $\theta_0(z, \tau), \theta_1(z, \tau)$ to create something that looks like the AGM.

τ-duplication formulas

$$\theta_0(z,2\tau)^2 = \frac{\theta_0(z,\tau)\theta_0(0,\tau) + \theta_1(z,\tau)\theta_1(0,\tau)}{2}$$
$$\theta_1(z,2\tau)^2 = \frac{\theta_0(z,\tau)\theta_1(0,\tau) + \theta_1(z,\tau)\theta_0(0,\tau)}{2}$$

Define $M(x,y,z,t) = \left(\frac{\sqrt{x}\sqrt{z}+\sqrt{y}\sqrt{t}}{2}, \frac{\sqrt{x}\sqrt{t}+\sqrt{y}\sqrt{z}}{2}, \frac{z+t}{2}, \sqrt{z}\sqrt{t}\right)$.

We can define a good choice of roots, and for some values of z,τ:

- $M(\theta_0^2(z,\tau),\theta_1^2(z,\tau),\theta_0^2(0,\tau),\theta_1^2(0,\tau)) = (\theta_0^2(z,2\tau),\theta_1^2(z,2\tau),\theta_0^2(z,2\tau),\theta_1^2(0,2\tau))$
- $\lim_{n\to\infty} M^n(\theta_0(z,\tau)^2,\theta_1(z,\tau)^2,\theta_0(0,\tau)^2,\theta_1(0,\tau)^2) = (1,1,1,1)$

But this iteration does not always converge quadratically:

$$M^n(2,2,1,1) = (2^{1/2^n}, 2^{1/2^n}, 1, 1)$$

Homogenization

Try to homogenize, just like with the AGM:

$$\begin{aligned}(x'_n, y'_n, z'_n, t'_n) &= M^n(\lambda x, \lambda y, \mu z, \mu t) \\ &= \left(\lambda^{1/2^n}\mu^{1-1/2^n}x_n, \lambda^{1/2^n}\mu^{1-1/2^n}y_n, \mu z_n, \mu t_n\right)\end{aligned}$$

So

$$\mu = \frac{\lim_{n\to\infty} z'_n}{\lim_{n\to\infty} z_n}, \quad \lambda = \frac{\lim_{n\to\infty}\left(\frac{x'_n}{z'_n}\right)^{2^n} z'_n}{\lim_{n\to\infty}\left(\frac{x_n}{z_n}\right)^{2^n} z_n}$$

We do get something quadratically convergent

$\left(\frac{x_n}{z_n}\right)^{2^n}$ converges quadratically; hence we can compute λ, μ in $O(\mathcal{M}(P)\log P)$.

The function we were looking for

$$\begin{aligned} \mathfrak{F} : \mathbb{C}^4 &\to \mathbb{C}^2 \\ (x, y, z, t) &\to \lim_{n\to\infty} \left(\left(\frac{x_n}{z_n} \right)^{2^n} \times z_n, z_n \right) \end{aligned}$$

where $(x_n, y_n, z_n, t_n) = M^n(x, y, z, t)$. We have

$$\mathfrak{F}\Big(\lambda\theta_0(z,\tau)^2, \lambda\theta_1(z,\tau)^2, \mu\theta_0(0,\tau)^2, \mu\theta_1(0,\tau)^2\Big) = (\lambda, \mu)$$

$$\mathfrak{F}\left(1, \frac{\theta_1(z,\tau)^2}{\theta_0(z,\tau)^2}, 1, \frac{\theta_1(0,\tau)^2}{\theta_0(0,\tau)^2}\right) = \left(\frac{1}{\theta_0(z,\tau)^2}, \frac{1}{\theta_0(0,\tau)^2}\right)$$

Action of $\mathrm{SL}_2(\mathbb{Z})$

For theta constants, we looked at $\tau' = \frac{-1}{\tau}$. Similarly:

$$\theta_2(z,\tau)^2 = (-i\tau)e^{2i\pi z^2/\tau}\theta_1\left(\frac{z}{\tau}, \frac{-1}{\tau}\right)^2$$

$$\theta_0(z,\tau)^2 = (-i\tau)e^{2i\pi z^2/\tau}\theta_0\left(\frac{z}{\tau}, \frac{-1}{\tau}\right)^2$$

$$\Rightarrow \quad \mathfrak{F}\left(1, \frac{\theta_2(z,\tau)^2}{\theta_0(z,\tau)^2}, 1, \frac{\theta_2(0,\tau)^2}{\theta_0(0,\tau)^2}\right) = \left(\frac{-i\tau e^{2i\pi z^2/\tau}}{\theta_0(z,\tau)^2}, \frac{-i\tau}{\theta_0(0,\tau)^2}\right)$$

Given $\frac{\theta_1(z,\tau)}{\theta_0(z,\tau)}, \frac{\theta_1(0,\tau)}{\theta_0(0,\tau)}$: apply $\mathfrak{F}$ then apply $\mathfrak{F}$ to $\frac{\theta_2(z,\tau)}{\theta_0(z,\tau)}, \frac{\theta_2(0,\tau)}{\theta_0(0,\tau)}$; we should get the pair $(-i\tau, e^{2i\pi z^2/\tau})$.

- Newton $\to O(\mathcal{M}(P)\log P)$.

Some work needed to guard against corner cases.

Implementation

Implementation in C (MPC); compare timings (in s) to

- our MPC implem of the naive algorithm computing simultaneously $\theta_0(z,\tau), \theta_0(0,\tau), \theta_1(z,\tau), \theta_1(0,\tau)$;
- Magma's Theta function.

Prec (decimal digits)	Magma	Naive	Fast
4000	0.17	0.03	0.09
16000	4.36	0.38	0.87
64000	116	4.60	6.78
256000	2426	41.6	45.5
325000		63.9	62.7
1024000		390	264
4096000		3921	1468

Outline

Generalization of Jacobi's theta

Definition

For $z \in \mathbb{C}^g$ and
$\tau \in \mathcal{H}_g = \{\tau \in \mathcal{M}_{g\times g}(\mathbb{C}),\ \text{symmetric},\ \mathrm{Im}(\tau) > 0\}$:

$$\theta(z,\tau) = \sum_{n\in\mathbb{Z}^g} e^{i\pi^t n\tau n} e^{2i\pi^t nz}$$

For $a, b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ $\qquad$ $\theta_{[a;b]}(z,\tau) = \sum_{n\in\mathbb{Z}^g} e^{i\pi^t (n+a)\tau(n+a)} e^{2i\pi^t (n+a)(z+b)}$

Background

Applications:

- In genus 2: isogeny computation (Robert & al.), fast arithmetic, class polynomial computations.
- In genus g: general Riemann surfaces (Mumford vol. 2).

Already done:

- Naive algorithm in genus g (Deconinck & al., 2004).
- Fast algorithm for theta constants in genus 2 (Dupont's PhD), applied to record computation of class polynomials (Enge & Thomé 2014).
- Hints of generalization to genus g.

Naive algorithm

As before, partial summation is a good start.

- Deconinck & al. analyze the remainder. The best strategy is to sum over an ellipsoid within $\mathbb{Z}^g$, whose directions depend on (the quadratic form defined by) $\operatorname{Im}\tau$.
- With $O(P^{g/2})$ summation terms, the remainder is less than $2^{-}P$.
- Using tricks to compute all terms with amortized cost $O(\mathcal{M}(P))$, we get $O(\mathcal{M}(P)P^{g/2})$.
  (for genus 2, see article, §3.2 p. 167 and appendix A).

Better complexities

We want to try to generalize the AGM-like approach.

- Step 1: Exhibit the link between duplication formulae and the relevant AGM analogue;
- Step 2: Find the set of τ for which the limit can be prediced;
- Step 3: Use the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$;
- Step 4: Use Newton iteration.

Step 1: τ-duplication formulas, function F

$$\theta_{[a;b]}(z,\tau)^2 = \frac{1}{2^g} \sum_{\beta \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} e^{-4i\pi^t a\beta} \theta_{[0;b+\beta]}\left(z, \frac{\tau}{2}\right) \theta_{[0;\beta]}\left(0, \frac{\tau}{2}\right).$$

In genus 2, we define the function: $F(a_{0,\ldots,3}, b_{0,\ldots,3}) =$

$$\left(\frac{\sqrt{a_0}\sqrt{b_0} + \sqrt{a_1}\sqrt{b_1} + \sqrt{a_2}\sqrt{b_2} + \sqrt{a_3}\sqrt{b_3}}{4}, \frac{\sqrt{a_0}\sqrt{b_1} + \sqrt{a_1}\sqrt{b_0} + \sqrt{a_2}\sqrt{b_3} + \sqrt{a_3}\sqrt{b_2}}{4}, \right.$$
$$\frac{\sqrt{a_0}\sqrt{b_2} + \sqrt{a_1}\sqrt{b_3} + \sqrt{a_2}\sqrt{b_0} + \sqrt{a_3}\sqrt{b_1}}{4}, \frac{\sqrt{a_0}\sqrt{b_3} + \sqrt{a_1}\sqrt{b_2} + \sqrt{a_2}\sqrt{b_1} + \sqrt{a_3}\sqrt{b_0}}{4},$$
$$\left. \frac{b_0 + b_1 + b_2 + b_3}{4}, \frac{2\sqrt{b_0}\sqrt{b_1} + 2\sqrt{b_2}\sqrt{b_3}}{4}, \frac{2\sqrt{b_0}\sqrt{b_2} + 2\sqrt{b_1}\sqrt{b_3}}{4}, \frac{2\sqrt{b_0}\sqrt{b_3} + 2\sqrt{b_1}\sqrt{b_2}}{4} \right).$$

Steps 1 and 2: AGM analogue, and the set $\mathcal{U}$

By construction the 2×2^g-uples

$$(\theta_{0,\dots,2^g-1}(\bullet, 2^n\tau)^2)_{n\geq 0}$$

(with $\bullet$ describing $\{z, 0\}$) are iterates of the function F, for some choice of square roots at each step.

Do we have $F^n(\theta_{0,\dots,2^g-1}(\bullet,\tau)^2) = \theta_{0,\dots,2^g-1}(\bullet, 2^n\tau)^2$?

Let $\mathcal{U} = \{$the nice matrices τ which yield optimal sequences$\}$.

- At least $\mathcal{U}$ contains the fundamental domain under Sp_{2g}.
- And certainly more, but the complete characterisation of $\mathcal{U}$ is difficult.

Note: whether or not $\tau \in \mathcal{U}$, ensuring we compute the "right" sequence is easy anyway, using low-precision approximations.

Properties retained from genus 1

As before, we unveil multiplicative factors with the 2^n-th power:

$$\lambda = \lim_{n\to\infty} \left(\frac{a_{0,n}}{b_{0,n}}\right)^{2^n} \times b_{0,n}.$$

And optimal sequences define homogeneous functions.

$$\lim_{n\to\infty} F^\infty\left(1, \frac{\theta^2_{1,\ldots,2^g-1}(z,\tau)}{\theta^2_0(z,\tau)}, 1, \frac{\theta^2_{1,\ldots,2^g-1}(0,\tau)}{\theta^2_0(0,\tau)}\right) = \left(\frac{1}{\theta_0(z,\tau)^2}, \frac{1}{\theta_0(0,\tau)^2}\right)$$

The variables we work on are $2^{g+1}-2$ quotients of theta functions and theta constants (genus 2: six variables).

Step 3 (genus 2): action of $\mathrm{Sp}_4(\mathbb{Z})$

Use the action of three "somewhat well"-chosen matrices of Sp_4.
If the corresponding $M \cdot \tau$ are all within $\mathcal{U}$, we have:

Theorem

$$F^\infty\left(\frac{\theta^2_{9,0,1}}{\theta^2_8}(z,\tau), \frac{\theta^2_{9,0,1}}{\theta^2_8}(0,\tau)\right) = \frac{e^{-2i\pi z_1^2/\tau_{11}}}{-\tau_{11}\theta_8(z,\tau)^2} = \frac{\lambda_1}{\mu_1\theta_8(z,\tau)^2}$$

$$F^\infty\left(\frac{\theta^2_{0,6,2}}{\theta^2_4}(z,\tau), \frac{\theta^2_{0,6,2}}{\theta^2_4}(0,\tau)\right) = \frac{e^{-2i\pi z_2^2/\tau_{22}}}{-\tau_{22}\theta_4(z,\tau)^2} = \frac{\lambda_2}{\mu_2\theta_4(z,\tau)^2}$$

$$F^\infty\left(\frac{\theta^2_{8,4,12}}{\theta^2_0}(z,\tau), \frac{\theta^2_{8,4,12}}{\theta^2_0}(0,\tau)\right) = \frac{e^{-2i\pi\frac{z_1^2\tau_{22}+z_2^2\tau_{11}-2z_1z_2\tau_{12}}{\det(\tau)}}}{(\tau_{12}^2-\tau_{11}\tau_{22})\theta_8(z,\tau)^2} = \frac{\lambda_3}{\mu_3\theta_8(z,\tau)^2}$$

If not: no real difficulty, low-precision approximation to the rescue.

Step 4: Newton

Counting variables (genus 2):

- We have $2^{g+1} - 2 = 6$ variables.
- Action of Sp_4 yields 6 multiplicative factors.
- We would like to re-express z and τ, which are $g + \frac{g(g+1)}{2} = 5$ complex numbers.

Not good for Newton. We can:

- Constrain the variables to lie on the Kummer surface (tedious because variety equation is heavy).
- Use the multipliers directly as the "predictable output" It works, but can only conjecture that the Jacobian is always invertible.

Eventually: conjectural complexity $O(\mathcal{M}(P) \log P)$.

Summary for quasi-linear algorithm $g \geq 2$

- Reduction of the input to fundamental domain is an issue for $g > 2$. A coarser domain is probably a viable option though.
- For $g \geq 2$, determining $\mathcal{U}$ explicitly is an annoying challenge, but not an obstacle.
- Successful Newton on $2^{g+1} - 2$ variables to find a point on a $(g + \frac{g(g+1)}{2})$-dimensional variety is the key point.
  - In genus 2, we conjecture that the Jacobian we get with the matrices proposed is invertible.
  - In genus $g > 2$, we have no universal proposition of "good" symplectic matrices.

Results

Timings in s:

Prec (digits)	Magma	Naive	This work
1000	0.42	0.38	0.38
2000	2.58	1.86	1.86
4000	18.4	9.51	6.65
8000	129	53.8	13.2
16000	889	303	25
32000	6368	1535	50
64000	46566	8798	120

Much better much earlier ($\log P$ versus P instead of vs $\sqrt{P}$)