How to calculate rational coverings for subgroups of $\mathrm{PSL}_2\left(\mathbb{Z}\right)$ efficiently

Hartmut Monien

University Bonn

Embedded Graphs, St. Petersburg 2014



Sporadic finite simple groups

X compact connected Riemann surface ϕ nonconstant meromorphic function on X $Mon(X, \phi)$ monodromy group of the cover $X \xrightarrow{\phi} P^1$.

Theorem (K. Magaard, 1993)

Let G denote a sporadic finite simple group. There exists a Riemann surface X of genus zero and a nonconstant meromorphic function ϕ such that G is a composition factor of $Mon(X, \phi)$ iff $G \simeq M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2$ or Co_3 .

Remark: The Higman-Sims group was missed in the original paper.



Riemann surface X





Theorem (Atkin and Swinnerton-Dyer)

There is a one-to-one correspondence between the subgroups of index μ in the modular group and equivalence classes of legitimate pairs of permutations (s_2 , s_3) under the equivalence relation \sim_1 . If Γ is a subgroup and (s_2 , s_3) a representative of the corresponding equivalence class, then

- 1. e_2 and e_3 are the number of letters fixed by s_2 and s_3 respectively.
- 2. $s = s_2 s_3$ has h cycles of lengths $\mu_1, \mu_2, \dots, \mu_h$ and μ_1 is the is the length of the cycle containing 1.

・ロト ・ 日 ・ ・ ヨ ・ ・ ヨ ・

- 3. The group g is isomorphic to the factor group $SL_2(\mathbb{Z})/\Gamma^N$,
- 4. Γ is maximal iff g is primitive.

Farey symbols

A Farey symbol is a concise and compact notation for the geometric information of a special polygon in the hyperbolic upper half plane including the side pairing by the action of the group Γ . Essential geometrical as well as arithmetic information can be obtained easily i.e. the minimal set of generators of Γ .

- Original work by R. Kulkarni
- Sage: first experimental implementation by Chris Kurth and Ling Long
- Sage: partial implementation by David Loeffler
- Sage: efficient implementation by HM
- Magma (only for congruence subgroups) Helena Verrill.
- Gap (only for congruence subgroups) by Ann Dooms, Eric Jespers, Alexander Konovalov,

Recently added: LLT algorithm for membership test of the arithmetic subgroup (solves the word problem in Γ) and reduction universitated to elementary cusps.

Calculation of Farey symbols: pairing matrices

Kulkarni showed that only three types of pairings can occur: even labeled by \circ , odd labeled \bullet and free labeled by a unique integer.

For each even interval $[x_i, x_{i+1}]$, take the matrix

$$\left(\begin{array}{cc} a_{i+1}b_{i+1}+a_ib_i & -a_i^2-a_{i+1}^2 \\ b_i^2+b_{i+1}^2 & -a_{i+1}b_{i+1}-a_ib_i \end{array}\right)$$

For each odd interval $[x_j, x_{j+1}]$, take the matrix

$$\left(\begin{array}{cc} a_{j+1}b_{j+1}+a_{j}b_{j+1}+a_{j}b_{j}&-a_{j}^{2}-a_{j}a_{j+1}-a_{j+1}^{2}\\ b_{j}^{2}+b_{j}b_{j+1}+b_{i+1}^{2}&-a_{j+1}b_{j+1}-a_{j+1}b_{j}-a_{j}b_{j}\end{array}\right)$$

For each free interval $[x_k, x_{k+1}]$ and $[x_s, x_{s+1}]$ take the matrix

$$\begin{pmatrix} a_{s+1}b_{k+1} + a_{s}b_{k} & -a_{s}a_{k} - a_{s+1}a_{k+1} \\ b_{s}b_{k} - b_{s+1}b_{k+1} & -a_{k+1}b_{s+1} - a_{k}b_{s} \end{pmatrix}$$
 universe universe to the set of the

Computation of the Farey symbols: algorithm

- 1. Start with a list $\{-\infty,0,\infty\}$
- 2. Examine either a single or a pair of intervals and calculate corresponding pairing matrices
- 3. If any of the pairing matrices is in Γ assign a new unique label
- 4. Insert extra point $(a_i + a_{i+1})/(b_i + b_{i+1})$ into the list between $x_i = a_i/b_i$ and $x_{i+1} = a_{i+1}/b_{i+1}$ creating new unlabeled intervals.
- 5. Repeat steps 2.-4. until no intervals are left.

Remarks:

- ► The only requirement is that the membership in Γ can be tested.
- ► In the general case this is an O (n²) algorithm. It can be improved to O (n) for congruence subgroups.

э

Comparison of implementations

Subgroup	# gens	magma	GAP	SAGE
Г(8)	33	15.6 sec	0.2 sec	0.01 sec
Г(16)	257	866.6 sec	14.9 sec	0.62 sec
Г(32)	2049	failed	1118.6 sec	55.73 sec

Here we are still using the general $O(n^2)$ algorithm for congruence subgroups. This can be improved to an O(n) algorithm without too much trouble. The SAGE implementation also works for non-congruence subgroups.



Arithmetic subgroups defined by permutations of cosets

Homomorphism $\theta : \operatorname{SL}_2(\mathbb{Z}) \to g$ defined by

$$\begin{array}{rcl} \theta\left(\gamma_{2}\right) &=& s_{2} \\ \theta\left(\gamma_{3}\right) &=& s_{3} \end{array}$$

We may consider 0 as representing Γ and $1 \dots n-1$ its left cosets in $SL_2(\mathbb{Z})$. The action of γ_2 and γ_3 permutes the cosets.

Remark

Depending on Γ the group g may or may not correspond to a geometric group. The most famous example by Klein is the congruence group $\Gamma(5)$ with corresponding group $g = A_5$ representing the symmetries of the icosahedron.



Example: M_{24}

From Atlas: representation of \mathcal{M}_{24} as permutation group $\subset \mathrm{S}_{24}$ with two generators of order 2 and 3 respectively.

$$S_2 = (1,4)(2,7)(3,17)(5,13)(6,9)(8,15)(10,19)(11,18)$$

(12,21)(14,16)(20,24)(22,23)
$$S_3 = (1,9,4)(3,14,5)(6,8,17)(7,12,16)(10,20,22)(11,19,13)$$

```
sage: g = ArithmeticSubgroup_Permutation(S2=s2, S3=s3); g
Arithmetic subgroup of index 24
sage: g.perm_group().order()
244823040
sage: gap.StructureDescription(g.perm_group())
M24
sage: g.is_congruence()
False
sage: g.genus()
0
universitätion
```

◆□▶ ◆圖▶ ◆臣▶ ◆臣▶ ─ 臣・

Fundamental domain



0.8 1 universitätbonn ペロ → 《母 → 《き → 《き → ミ の Q.ペ





Farey symbol for the Matthieu group M_{24} .



Finitely generated by seven generators:

$$\left\langle \begin{array}{cc} \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right), \left(\begin{array}{cc} -2 & 1 \\ -7 & 3 \end{array}\right), \left(\begin{array}{cc} -22 & 13 \\ -39 & 23 \end{array}\right), \left(\begin{array}{cc} -30 & 19 \\ -49 & 31 \end{array}\right), \end{array} \right\rangle, \end{array} \right\rangle$$



sage: %time rational function(M24, prec=2048) CPU times: user 14.93 s. svs: 0.11 s. total: 15.03 s Wall time: 18.97 s 1/4835703278458516698824704*(125542034707733615276715788464153328322047108889280 69025792*z^6 - 2923003274661805836407369665432566039311865085952*z^5*(5453580025 $*I*sart(23) = 1008220915141) = 340282366920938463463374607431768211456*z^4*(1106)$ 6315563550740782939*I*sqrt(23) - 33034672403480189462271) - 31691265005705735037 4175801344*z^3*(58099022166525442370783933574519*I*sqrt(23) + 219827970420533069 154563705261589) - 18446744073709551616*z^2*(-2031242230389565954280974536472772 436372565*I*sart(23) + 12321437310693103556231828320317986982962929) - 858993459 2*z*(-5722210833402808994471531853067973640001837297566583*I*sgrt(23) - 27394995 793116899078882292964132693387978256382046229) - 2344434299187586169827160789879 6160551716622709105255597291637*I*sqrt(23) + 76464419838352984876971234073475487 083936228540212806990514321)^3*(125542034707733615276715788464153328322047108889 28069025792*z^6 - 2923003274661805836407369665432566039311865085952*z^5*(3708434 417*I*sqrt(23) + 7102103203) - 340282366920938463463374607431768211456*z^4*(6914 2628662047092811*I*sqrt(23) + 45378825986714492625) - 31691265005705735037417580 1344*z^3*(-143770342692460138023115007985*I*sqrt(23) + 2828297979071142382909054 202205) - 18446744073709551616*z^2*(-16350947797952385520991827801517039037301*I *sart(23) - 63897554482322689881941970579901541384303) - 8589934592*z*(340987396 07582218849375988570857219733459174195041*I*sqrt(23) - 7225179773904700771938175 3859937441307758975012877) + 541974834799571040704022047453594447016348259781497 0286939*I*sqrt(23) - 44788520723700534400189300207915317122784153354193609824537 5)/(1073741824*z - 218143201*I*sart(23) - 1933641587)^23 sage:



Analytic number theory



Starting point: "Fourier Coefficients of the Modular Invariant $J(\tau)$ " Hans Rademacher 1938, MR1507331 in which he obtained a converging series for the Fourier coefficients of J(z). The main idea of these papers is to split the integral for the Fourier coefficients into integrals over Farey arcs:

$$c_n = \frac{1}{2\pi i} \int_C \frac{f(z)}{q^{n+1}} dq = \sum_{0 \le h < k \le N} \int_{\xi(h,k)} \frac{f(z)}{q^{n+1}} dq$$

where $\xi(h, k)$ are the so called Farey arcs of order N of the circle C with $|z| = \exp(-2\pi/N^2)$ and the sums runs over h and k with (h, k) = 1.



Details

A change of variables
$$q = \exp\left(-2\pi N^{-2} + 2\pi i h/k + 2\pi i \phi\right)$$
 yields:

$$c_n = \sum_{0 \le h < k \le N} e^{-2\pi i h/k} \int_{\alpha(h,k)}^{\beta(h,k)} f\left(e^{(2\pi i h/k - 2\pi N^{-2} - i \phi)}\right) e^{2\pi n \left(N^{-2} - i \phi\right)} d\phi$$

where $\alpha(h, k)$ and $\beta(h, k)$ can be determined uniquely from the neighbors in the Farey sequence.

$$\frac{h_1}{k_1} < \frac{h}{k} < \frac{h_2}{k_2}$$

Using the modular invariance one obtains

$$c_n = \sum_{0 \le h < k \le N} e^{-2\pi i h/k} \int_{\alpha(h,k)}^{\beta(h,k)} f\left(e^{\frac{2\pi i h'}{k} - \frac{2\pi N}{k^2 w}}\right) e^{2\pi n w} d\phi$$

where $w = N^{-2} - i\phi$. Now split f(z) into a principal and regular part:

$$f(z) = q^{-1} + \sum_{n} c_n q^n$$
 universitätbonn

Details

A change of variables
$$q = \exp\left(-2\pi N^{-2} + 2\pi i h/k + 2\pi i \phi\right)$$
 yields:

$$c_n = \sum_{0 \le h < k \le N} e^{-2\pi i h/k} \int_{\alpha(h,k)}^{\beta(h,k)} f\left(e^{(2\pi i h/k - 2\pi N^{-2} - i \phi)}\right) e^{2\pi n \left(N^{-2} - i \phi\right)} d\phi$$

where $\alpha(h, k)$ and $\beta(h, k)$ can be determined uniquely from the neighbors in the Farey sequence.

$$\frac{h_1}{k_1} < \frac{h}{k} < \frac{h_2}{k_2}$$

Using the modular invariance one obtains

$$c_n = \sum_{0 \le h < k \le N} e^{-2\pi i h/k} \int_{\alpha(h,k)}^{\beta(h,k)} f\left(e^{\frac{2\pi i h'}{k} - \frac{2\pi N}{k^2 w}}\right) e^{2\pi n w} d\phi$$

where $w = N^{-2} - i\phi$. Now split f(z) into a principal and regular part:

$$f(z) = q^{-1} + \sum_{n} c_n q^n$$
universitätbonn
universitätbonn

What Rademacher was able to proof was that the sum is completely dominated by the principal part and that the remainder does vanish. The final result is

$$c_n = \frac{2\pi}{\sqrt{n}} \sum_{k=1}^N \frac{A_k(n)}{k} \mathrm{I}_1\left(\frac{4\pi\sqrt{n}}{k}\right) + O\left(e^{2\pi N^2 n^{1/3} N^{-1/3} + \epsilon}\right)$$

with

. .

$$A_k(n) = \sum_{h \mod k} e^{-\frac{2\pi i}{k}(nh+h')}$$

where the sum runs over h and k for (h, k) = 1 and h'h = -1mod k. The estimation of the error term required on a nontrivial bound on an incomplete Kloosterman sum.

$$|A_k(n)| \leq k$$

 $|A_k(n)| \leq Ck^{2/3+\epsilon} \cdot (k,n)^{1/3}$



This work was extended by Zuckerman 1938 in a paper "On the coefficients of certain modular forms belonging to subgroups of the modular group" MR1501993. who considered arbitrary subgroups but had to constraint the weight of the modular form k to k > 0 since for arbitrary subgroups an estimate for the more complicated partial Kloosterman sums seems out of reach.

The basis input for the calculation of the modular form are the principal parts at all cusps. The main difference to the work by Rademacher is that for subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ the pullback to a cusp representative is required.



Expansion at all cusps

At each cusp x the j-function can be expanded in terms of

$$q = \exp\left(-\frac{2\pi i}{w^2(z-x)}\right)$$

where w is the width of the cusp at x. At every cusp (with exception $i\infty$) we have the expansion

$$j(z)=\sum_{n=0}^{\infty}a_nq^n$$

At the cusp $i\infty$ we have

$$j(z) = \frac{1}{q} + \sum_{n=0}^{\infty} a_n q^n$$

with $q = \exp(2\pi i z)$.



Expansion at all cusps: $\Gamma_0(23)$



Algorithm for reduction to elementary cusp

Once the Farey symbol is computed then the pullback to an elementary cusp can be computed relatively quickly.

Let Γ be a finite index subgroup of $\mathrm{PSL}_2\mathbb{Z}$. Given a rational number $h/k\in\mathbb{Q}$ define

$$\rho = \left(\begin{array}{cc} -h' & -(hh'+1)/k \\ k & -h \end{array}\right)$$

where h' solve $hh' = -1 \mod k$. Then $\rho \in SL_2(\mathbb{Z})$ and sends h/k to ∞ . There is exactly one γ amongst the coset representatives of Γ for which $T = \gamma^{-1}\rho \in \Gamma$. Then T maps h/k to a Farey fraction in the fundamental domain. To reduce to a particular cusp representative we can use the pairing matrices (generators).

The operation count is proportional to the index of Γ .



The first test we performed was the calculation of the hauptmodul for the $\Gamma_0(p)$ for $p \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$. In all these cases an N < 128 was sufficient to calculate the first 64 Fourier coefficients with an absolute error of less than 0.1 which is sufficient in this case. Once a sufficient number of coefficients (≈ 64 in these cases) is known the information from the dessin to obtain the remaining coefficients.



Practical procedure

Using a Kloosterman sum with the largest denominator 128:

$$j_{\Gamma_0(3)}(z) \approx \frac{1}{q} + (53.9957408792064 + 2.04005607269908 \times 10^{-14}i) q - (76.0539191990603 - 0.0222442568873815i) q^2 + \dots$$

using the fact that the coefficients are in $\ensuremath{\mathbb{Z}}$ we extrapolate to

$$j_{\Gamma_0(3)}(z) = \frac{1}{q} + 54q - 76q^2 \dots$$

Inverting the the reciprocal of the series and substituting q:

subst(ellj(q), q, serreverse(1/j3))

we obtain the rational function:

$$\frac{(27t+1)(243t+1)^3}{t}$$

A new method





Hejhal method: random use of transformations depending on height, radius of convergence of q-series do not overlap



- Hejhal method: random use of transformations depending on height, radius of convergence of q-series do not overlap
- Rademacher, Zuckermann: generalized Kloosterman sums with very slow convergence



- Hejhal method: random use of transformations depending on height, radius of convergence of q-series do not overlap
- Rademacher, Zuckermann: generalized Kloosterman sums with very slow convergence
- Puiseux series
- ▶ ...

For a recent review consult M. Klug, M. Musty, S. Schiavone and J. Voight (http://lanl.arxiv.org/pdf/1311.2081v3.pdf).



Analyticity

All these methods attempt to find a solution of two partial differential equations for the real and imaginary part of $u(x, y) = \Re(j_{\Gamma}(x + iy))$ and $v(x, y) = \Im(j_{\Gamma}(x + iy))$ in two dimensions:

$$\Delta u(x,y) = 0$$

 $\Delta v(x,y) = 0$

with boundary condition $j_{\Gamma}(z) \rightarrow \frac{1}{q} + \text{constant} + c_1q + c_2q^2 + \dots$ as $z \rightarrow i\infty$. The complicated part is how to incorporate the boundary conditions.



Symmetric group S_{10}

Boundary conditions!



Finite element

Very technical, but can be done ...



Elliptic points

Special points of the fundamental domain:



Elliptic points

Special points of the fundamental domain:



Using the solution of the Laplace equation

The values of the numerical approximation $\tilde{j}(z)$ at the elliptic points of order three give us a handle on the numerator of the Belyi function

$$\frac{\left(z^3 + x_2 z^2 + x_1 z + x_0\right)^3 (z + x_3)}{(z + x_4)^5 (z + x_5)^3}.$$

There are three elliptic points of order three in the fundamental domain and one on the boundary. Call the first three points z_0 , z_1 , z_2 and the fourth z_3 . Then we know that the approximate values calculated at these points give approximations for x_0 , x_1 , x_2 , x_3 :

$$\begin{array}{rcl} x_2 &\approx& \tilde{j}(z_0) + \tilde{j}(z_1) + \tilde{j}(z_2) \\ x_1 &\approx& \tilde{j}(z_0)\tilde{j}(z_1) + \tilde{j}(z_0)\tilde{j}(z_2) + \tilde{j}(z_1)\tilde{j}(z_2) \\ x_3 &\approx& \tilde{j}(z_0)\tilde{j}(z_1)\tilde{j}(z_2) \end{array}$$



Refinement

The results from numerical solution of the *linear* partial differential equation can be used as an input for the *nonlinear* polynomial equations.

- ► Using a finite element pde solver the relative accuracy of the hauptmodul evaluated at the elliptic points is 10⁻³. This is enough to be in the bassin of attraction for the standard Newton algorithm.
- The newton algorithm converges quickly (typically 30 iterations for 1024 bits of accuracy). The exact jacobian of the polynomial equations is used.
- The resulting numbers are identified as algebraic numbers using pari.
- The solution is verified by substituting the candidate solution.



The final result for the modular function is

$$\frac{\left(5\sqrt{5}+16z\right)\left(625\sqrt{5}+16000z+163840\sqrt{5}z^{2}+104857z^{3}\right)^{3}}{78125\sqrt{5}z^{2}\left(25\sqrt{5}+512z\right)^{3}}$$

For the q-expansion of the hauptmodul at the cusp ∞ we find

$$\frac{1}{q} - \frac{232}{25\sqrt{5}} + \frac{3796q}{625} - \frac{131072q^2}{15625\sqrt{5}} - \frac{50796598q^3}{1953125} + O\left(q^4\right)$$

with $q = \exp(\pi i z)$.



```
sage: %time rational_function(HsuExample10(), prec=2048)
CPU times: user 1.59 s, sys: 0.01 s, total: 1.60 s
Wall time: 1.95 s
1/15625*(390625*z^3 - 175000*sqrt(5)*z^2 + 85464000*z - 37022208*sqrt(5))^3*(125
*z - 152*sqrt(5))/((125*z - 232*sqrt(5))^5*(25*z + 56*sqrt(5))^3)
sage:
```



Fundamental domain M_{24}





sage: %time rational function(M24, prec=2048) CPU times: user 14.93 s. svs: 0.11 s. total: 15.03 s Wall time: 18.97 s 1/4835703278458516698824704*(125542034707733615276715788464153328322047108889280 69025792*z^6 - 2923003274661805836407369665432566039311865085952*z^5*(5453580025 $*I*sart(23) = 1008220915141) = 340282366920938463463374607431768211456*z^4*(1106)$ 6315563550740782939*I*sqrt(23) - 33034672403480189462271) - 31691265005705735037 4175801344*z^3*(58099022166525442370783933574519*I*sqrt(23) + 219827970420533069 154563705261589) - 18446744073709551616*z^2*(-2031242230389565954280974536472772 436372565*I*sart(23) + 12321437310693103556231828320317986982962929) - 858993459 2*z*(-5722210833402808994471531853067973640001837297566583*I*sgrt(23) - 27394995 793116899078882292964132693387978256382046229) - 2344434299187586169827160789879 6160551716622709105255597291637*I*sqrt(23) + 76464419838352984876971234073475487 083936228540212806990514321)^3*(125542034707733615276715788464153328322047108889 28069025792*z^6 - 2923003274661805836407369665432566039311865085952*z^5*(3708434 417*I*sqrt(23) + 7102103203) - 340282366920938463463374607431768211456*z^4*(6914 2628662047092811*I*sqrt(23) + 45378825986714492625) - 31691265005705735037417580 1344*z^3*(-143770342692460138023115007985*I*sqrt(23) + 2828297979071142382909054 202205) - 18446744073709551616*z^2*(-16350947797952385520991827801517039037301*I *sart(23) - 63897554482322689881941970579901541384303) - 8589934592*z*(340987396 07582218849375988570857219733459174195041*I*sqrt(23) - 7225179773904700771938175 3859937441307758975012877) + 541974834799571040704022047453594447016348259781497 0286939*I*sqrt(23) - 44788520723700534400189300207915317122784153354193609824537 5)/(1073741824*z - 218143201*I*sart(23) - 1933641587)^23 sage:



$j = \frac{1}{q} - \frac{5251677912867089081 - 4957825574864843837i\sqrt{23}}{9223372036854775808}q + O\left(q^2\right)$

Remark

The value of the first coefficient calculated with the generalized Kloosterman sum (largest denominator 128)

 $a_1 \approx -0.536598303357083 + 2.45376485846676i$

with an error of less than 5%.



General triangle groups: M_{23}



comparison of methods:



General triangle groups: M_{23}



comparison of methods:

 p-adic methods (N. D. Elkies 2013, S. Siksek): several CPU days for initial search + extra calculations for proof



General triangle groups: M_{23}



comparison of methods:

- p-adic methods (N. D. Elkies 2013, S. Siksek): several CPU days for initial search + extra calculations for proof
- our method: approximately 10 minutes on this laptop



Conformal maps



A conformal map





A natural domain decomposition







Conformal map as q-expansion at $i\infty$:

$$q \rightarrow \frac{q}{432} - \frac{5q^2}{7776} + \frac{685q^3}{2239488} - \frac{197585q^4}{1088391168} + O\left(q^5\right)$$

The asymptotic behavior at the cusps

$$j_2(z) = rac{432}{q} + 96 - rac{208q}{9} + rac{8192q^2}{729} - rac{45056q^3}{6561} + O\left(q^4
ight)$$

is only modified by trivial factors.



```
[Shostakovitsh:MultiPrecision> tp 8
NX = 257, NY = 1537
512.069618 -256.141200
-64.154023 -256.141200
-64.154023 -256.141200
512.069618 -256.141200
512.069618 -256.141200
[Shostakovitsh:MultiPrecision>
```

All of this is easily parallelizable



Patched solution





• The remaining groups: J_1 , J_2 and Co_3 .





- The remaining groups: J_1 , J_2 and Co_3 .
- ► General Fuchsian groups (e.g. *M*₂₂).



