Kleiner maken van binaire vormen.

BSc-project. Begeleider: Marco Streng

De polynomen

$$\begin{aligned}
f = {} & 5448307749088046623505106215685160108463182591886755296687695394045634398355500573574958173285 6X^6 \\
& +9908095743733160730083264469242269621252586272417526943824326484128418827929307911380378788317 96X^5Z \\
& +9550240276628933798303625862171745458160135646268522819972302252550987899377800556235883602877325X^4Z^2 \\
& +5716554696986897344268267287947986615478944722726154348889934788409786512865150696091661091636489 4X^3Z^3 \\
& +1536803365492684422711866366515329696605222044753455761980854694898563428035488260183652290163009 91X^2Z^4 \\
& +3043203551226164272430459370687632551278629326350244032144195623317079083664488543425401290004800 50XZ^5 \\
& +1763017720401502347211017175135719421294439431290016688230258633330919470022725855330597190598219 057Z^6
\end{aligned}$$

en

$$g = X^6 + 6X^5Z + 11X^4Z^2 + 6X^3Z^3 + 5X^2Z^4 + 4Z^6 \in \mathbf{Q}[X, Z]$$

zijn equivalent, in de zin dat ze uit elkaar te verkrijgen zijn door middel van een $\mathbf{Z}$-lineaire verandering van variabelen.
Het zou handig zijn om, gegeven een polynoom zoals f, een 'kleiner' equivalent polynoom, zoals g te kunnen uitrekenen. In de praktijk kan dit met een algoritme van Stoll en Cremona [1], en dat werkt als volgt.

We kunnen lineaire verandering van variabelen zien als een werking van de groep $\mathrm{SL}_2(\mathbf{Z}) = \{M \in \mathbf{Z}^{2\times 2} : \det(M) = 1\}$ op de verzameling V_n van homogene polynomen over $\mathbf{Z}$ van graad $n > 5$. Dezelfde groep werkt op het *bovenhalfvlak* $\mathcal{H} = \{\tau \in \mathbf{C} : \mathrm{Im}(\tau) > 0\}$ door

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Binnen $\mathcal{H}$ is er het *fundamentele domein*

$$\mathcal{F} = \left\{ \tau \in \mathcal{H} : \begin{array}{l} |\tau| \geq 1, \\ |\mathrm{Re}(\tau)| \leq \frac{1}{2}, \\ \text{als } |\tau| = 1 \text{ of } |\mathrm{Re}(\tau)| = \frac{1}{2}, \text{ dan } \mathrm{Re}(\tau) \geq 0 \end{array} \right\}$$

dat van elke baan precies 1 element bevat. Bovendien bestaat er een snel algoritme dat voor elke $\tau \in \mathcal{H}$ een element $A \in \mathrm{SL}_2(\mathbf{Z})$ vindt met $A \cdot \tau \in \mathcal{F}$.

Stoll en Cremona geven een afbeelding van $\mathrm{SL}_2(\mathbf{Z})$-verzamelingen

$$z : V_n \to \mathcal{H},$$

en hun algoritme is als volgt. Gegeven $F \in V_n$, bereken een $A \in \mathrm{SL}_2(\mathbf{Z})$ met $A \cdot z(F) \in \mathcal{F}$. Dan is $G = A \cdot F$ in de praktijk één van de 'kleinste' elementen van de baan van F.

In dit project bestudeer je eerst [1], en kan je daarna verschillende kanten uit, zoals:

1. Open vraag: waarom werkt dit? Met andere woorden, kan je een verband geven tussen de 'grootte' van F en het de locatie van $z(F)$ binnen $\mathcal{H}$?

2. Stoll en Cremona geven in [1] al aan dat een variant van hun methode ook werkt voor bepaalde andere getallenringen. Werk dit in detail uit voor $\mathbf{Z}[\sqrt{-1}]$ of algemene(re) maximale imaginair kwadratische ordes.

3. Vervolg op 2: programmeer dit in het open source softwarepakket SageMath en maak het onderdeel van de standaardfunctionaliteit van SageMath

4. Open vraag: zijn er gevallen waarbij het beter is om met breuken in plaats van gehele getallen te werken? En wat moeten we dan gebruiken in plaats van $\mathcal{H}$ om dit nog te laten werken?

Referentie:

[1] Michael Stoll and John Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. 565 (2003), 79–99, `https://homepages.warwick.ac.uk/staff/J.E.Cremona/papers/redp1.pdf`