Gröbner Basis Computation in Group Rings and Applications for Groups

joint work with Martin Kreuzer

Gerhard Rosenberger

gerhard.rosenberger@math.uni-hamburg.de

University of Hamburg

Ischia, April 2014

Topics

1. Non-Commutative Polynomials
2. The Buchberger Procedure
3. Application to Group Rings
4. Hilbert-Dehn Functions
5. Growth in Hecke Groups

Non-Commutative Polynomials

Idea: Use the potential of Gröbner basis theory for computations in group theory.

K field

$K\langle X\rangle$ free associative algebra over the alphabet $X = \{x_1, \ldots, x_n\}$
(This will be called the non-commutative polynomial ring.)

X^* monoid of all words $x_{i_1} \cdots x_{i_r}$

$I \subseteq K\langle X\rangle$ two-sided ideal generated by $f_1, \ldots, f_s \in K\langle X\rangle$

$R = K\langle X\rangle / I$ finitely presented K-algebra

Non-Commutative Polynomials

Main Example:

$G = \langle x_1, \ldots, x_n; \ell_1 = r_1, \ldots, \ell_s = r_s \rangle$
finitely presented group (or monoid)

$K\langle G \rangle = \bigoplus_{g \in G} Kg$ group ring

$K\langle G \rangle = K\langle X \rangle / I$

$I = \langle \ell_1 - r_1, \ldots, \ell_s - r_s \rangle$ two-sided ideal generated by binomials

Non-Commutative Polynomials

Definition

(a) A complete ordering σ on X^* is called a word ordering if
   (1) it is multiplicative, i.e. $w_1 <_\sigma w_2$ implies $w_3 w_1 w_4 <_\sigma w_3 w_2 w_4$,
   (2) it is a well-ordering. (Equivalently, $1 <_\sigma w$ for all $w \neq 1$.)

(b) For a word $w = x_{i_1} \cdots x_{i_\ell}$, the number $\deg(w) = \ell$ is called the degree or the length of the word.

Non-Commutative Polynomials

Example

The length lexicographic word ordering $\mathtt{llex}$ is defined by $w_1 <_{\mathtt{llex}} w_2$ iff

(1) $\deg(w_1) < \deg(w_2)$ or

(2) $\deg(w_1) = \deg(w_2)$ and the first letter where w_1 and w_2 differ has a larger index in w_1.

Notice that $x_1 >_{\mathtt{llex}} \cdots >_{\mathtt{llex}} x_n$.

Remark

The lexicographic ordering is not a word ordering, because

$$x_1 >_{\mathtt{lex}} x_2x_1 >_{\mathtt{lex}} x_2x_2x_1 >_{\mathtt{lex}} \cdots$$

yields a set of words without minimal element.

Non-Commutative Polynomials

Definition

Let $f \in K\langle X\rangle \setminus \{0\}$. Then we have a unique representation $f = c_1 w_1 + \cdots + c_s w_s$ with $c_i \in K \setminus \{0\}$ and $w_i \in X^*$ satisfying $w_1 >_\sigma w_2 >_\sigma \cdots >_\sigma w_s$.

(a) The word $\mathrm{Lw}_\sigma(f) = w_1$ is called the leading word of f.

(b) The element $\mathrm{Lc}_\sigma(f) = c_1$ is called the leading coefficient of f.

(c) The set $\mathrm{Supp}(f) = \{w_1, \ldots, w_s\}$ is called the support of f. For $f = 0$ we set $\mathrm{Supp}(f) = \emptyset$.

Example

For the non-commutative polynomial $f = x_2x_1x_2 + x_1x_2 + 1$ we have $\mathrm{Lw}_{\mathtt{llex}}(f) = x_2x_1x_2$ and $\mathrm{Supp}(f) = \{x_2x_1x_2,\ x_1x_2,\ 1\}$.

Non-Commutative Polynomials

σ word ordering
$f_1, \ldots, f_s \in K\langle X \rangle \setminus \{0\}$ non-commutative polynomials
$I = \langle f_1, \ldots, f_s \rangle$ two-sided ideal generated by $\{f_1, \ldots, f_s\}$

Definition

(a) The ideal $\mathrm{Lw}_\sigma(I) = \langle \mathrm{Lw}_\sigma(f) \mid f \in I \setminus \{0\} \rangle$ is called the leading word ideal of I.

(b) A set of non-commutative polynomials $G = \{g_1, \ldots, g_s\}$ in $I \setminus \{0\}$ is called a σ-Gröbner basis of I if

$$\mathrm{Lw}_\sigma(I) = \langle \mathrm{Lw}_\sigma(g_1), \ldots, \mathrm{Lw}_\sigma(g_s) \rangle.$$

Example

For the ideal $I = \langle f_1, f_2, f_3, f_4 \rangle$ generated by $f_1 = x^2 - yx$, $f_2 = xy - zy$, $f_3 = xz - zy$, and $f_4 = yz - zy$ in $\mathbb{Q}\langle x, y, z \rangle$, we have the `llex`-Gröbner basis $G = \{f_1, f_2, f_3, f_4, zy^2 - z^2y, y^2x - zyx\}$.

Non-Commutative Polynomials

Example

The principal ideal $I = \langle x^2 - yx \rangle$ in $\mathbb{Q}\langle x, y \rangle$ has an infinite reduced `llex`-Gröbner basis G. We have

$$\begin{aligned} \mathrm{Lw}_{\mathtt{llex}}(I) &= \langle xy^i x \mid i \geq 0 \rangle \\ G &= \{xy^i x - xy^{i+1} \mid i \geq 0\}. \end{aligned}$$

Remark

Non-commutative Gröbner bases have characterizations similar to commutative Gröbner bases:

(a) *special generation of the ideal I*

(b) *convergence of the associated rewriting system*

(c) *Buchberger criterion*

The Buchberger Procedure

Idea: Construct an efficient enumerating procedure to compute non-commutative Gröbner bases!

If the given ideal has a finite Gröbner basis, the procedure shall stop after finitely many steps and return the answer.

If the given ideal has an infinite Gröbner basis, the procedure shall enumerate Gröbner basis elements for a specified amount of time.

The Division Algorithm

Given monic polynomials $f, g_1, \ldots, g_s \in K\langle X\rangle$ and a word ordering σ on X^*, consider the following steps.

(1) Starting initially with $j = 1$, $p = 0$ and $h = f$, find the smallest $i_j \in \{1, \ldots, s\}$ such that $\mathrm{Lw}_\sigma(h) = w\,\mathrm{Lw}_\sigma(g_{i_j})w'$ with $w, w' \in X^*$.

(2) If such an i_j exists, set $\ell_j = w$, $r_j = w'$, increase j by one, an replace f by $f - \ell_j g_{i_j} r_j$.

(3) If no such i_j exists, replace p by $p + \mathrm{Lw}_\sigma(v)$ and v by $v - \mathrm{Lw}_\sigma(v)$.

(4) Repeat (1) – (3) until $h = 0$. Then return the pairs (ℓ_j, r_j) and p.

This is an algorithm which computes a representation $f = \sum_j \ell_j g_{i_j} r_j + p$ such that no word in the support of the normal remainder $\mathrm{NR}_{\sigma,G}(f) = p$ is divisible by some $\mathrm{Lw}_\sigma(g_i)$ and such that $\ell_j\,\mathrm{Lw}_\sigma(g_{i_j})r_j \leq_\sigma \mathrm{Lw}_\sigma(f)$ for all j.

The Buchberger Procedure

σ (fixed) word ordering (usually `llex`) on X^*

$g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$ monic polynomials (i.e. $\mathrm{Lc}_\sigma(g_i) = 1$)

$I = \langle G\rangle$ two-sided ideal generated by $G = \{g_1, \ldots, g_s\}$

Definition

A quadruple $(\ell, r, \ell', r') \in X^{*4}$ is called an obstruction for (g_i, g_j) if $\ell\ \mathrm{Lw}_\sigma(g_i)\, r = \ell'\ \mathrm{Lw}_\sigma(g_j)\, r'$.

The Buchberger Procedure

Definition

Given an obstruction (ℓ, r, ℓ', r') for (g_i, g_j), the polynomial

$$S(g_i, g_j) \;=\; \frac{1}{\mathrm{Lc}_\sigma(g_i)}\,\ell\, g_i\, r - \frac{1}{\mathrm{Lc}_\sigma(g_j)}\,\ell'\, g_j\, r'$$

is called the corresponding S-polynomial.

Definition

A polynomial $f \in K\langle X\rangle$ has a (weak) Gröbner representation with respect to G if there exist $c_i \in K$ and $\ell_i, r_i \in X$ and $j_i \in \{1, \ldots, s\}$ such that

$$f \;=\; \sum_{i=1}^{m} c_i\, \ell_i\, g_{j_i}\, r_i \quad \text{and} \quad \ell_i\, \mathrm{Lw}_\sigma(g_{j_i})\, r_i \leq_\sigma \mathrm{Lw}_\sigma(f)$$

for $i = 1, \ldots, m$.

The Buchberger Procedure

Theorem (Buchberger Criterion)

The set G is a σ-Gröbner basis of I if and only if every S-polynomial of two elements of G has a Gröbner representation with respect to G.

It can be shown that it is indeed sufficient to consider the following finite set of non-trivial obstructions:

(a) right obstructions: $\mathrm{Lw}_\sigma(g_i) \cdot r = \ell' \cdot \mathrm{Lw}_\sigma(g_j)$

(b) left obstructions: $\ell \cdot \mathrm{Lw}_\sigma(g_i) = \mathrm{Lw}_\sigma(g_j) \cdot r'$

(c) center obstructions: $\ell \cdot \mathrm{Lw}_\sigma(g_i) \cdot r = \mathrm{Lw}_\sigma(g_j)$

Therefore one can check in finitely many steps whether G is a σ-Gröbner basis.

The Buchberger Procedure

Theorem (Buchberger Procedure)

Let $I = \langle g_1, \ldots, g_s \rangle$ be a two-sided ideal in $K\langle X \rangle$ generated by a set $G = \{g_1, \ldots, g_s\}$ of monic polynomials. Perform the following steps:

(1) *Let B be the set of all normal remainders $\mathrm{NR}_{\sigma,G}(S(g_i, g_j))$ of S-polynomials $S(g_i, g_j)$ corresponding to non-trivial obstructions.*

(2) *If $B = \emptyset$, return G and stop. Otherwise, choose $f \in B$ using a fair strategy, remove it from B and append f to G.*

(3) *Compute the non-trivial obstructions for the pairs (g_i, f) and append the non-zero normal remainders of the corresponding $S(g_i, f)$ to the set B.*

(4) *Interreduce G and update the set B correspondingly.*

This procedure enumerates a σ-Gröbner basis of I. If I has finite σ-Gröbner bases, the procedure stops and outputs one of them.

Optimizing the Buchberger Procedure

Remark (Trivial Obstructions)

(a) *If* (ℓ, r, ℓ', r') *is an obstruction of* (g_i, g_j) *i.e. if* $\ell \cdot \mathrm{Lw}_\sigma(g_i) \cdot r = \ell' \cdot \mathrm{Lw}_\sigma(g_j) \cdot r'$, *then all multiples*

$$(w\,\ell,\ r\,w',\ w\,\ell',\ r'\,w') \qquad \text{with } w, w' \in X^*$$

are also obstructions. If the S-polynomial of (ℓ, r, ℓ', r') *has a Gröbner representation, the S-polynomials of all such obstructions have Gröbner representations.*

(b) *(Product Criterion) If* $\mathrm{Lw}_\sigma(g_i)$ *and* $\mathrm{Lw}_\sigma(g_i)$ *have no overlap, then the S-polynomial of every obstruction of* (g_i, g_j) *has a Gröbner representation.*

The Buchberger Procedure

Proposition (Non-Commutative Criterion M)

Let $(\ell_i, r_i, \ell'_i, r'_i)$ be an obstruction of (g_i, g_s) and $(\ell_j, r_j, \ell'_j, r'_j)$ an obstruction of (g_j, g_s). If there exist words $w, w' \in X^*$ such that $\ell'_i = w\,\ell'_j$ and $r'_i = r'_j\,w$ then we can remove $(\ell_i, r_i, \ell'_i, r'_i)$ from B in the execution of the Buchberger Procedure provided $ww' \neq 1$.

Proposition (Non-Commutative Criterion F)

In the setting of the preceding proposition, assume that $w = w' = 1$, i.e. that $\ell'_i = \ell'_j$ and $r'_i = r'_j$. Then the obstruction $(\ell_i, r_i, \ell'_i, r'_i)$ can be removed from B in the execution of the Buchberger Procedure if $i > j$ or if $i = j$ and $\ell_i >_\sigma \ell_j$.

The Buchberger Procedure

Proposition (Non-Commutative Criterion B)

A non-trivial obstruction $(\ell_i, r_i, \ell_j, r_j)$ of (g_i, g_j) can be removed from the set B during the execution of the Buchberger Procedure if the following conditions hold.

(1) *There exist words $\ell_s, r_s \in X^*$ such that $(\ell_i, r_i, \ell_s, r_s)$ is an obstruction of (g_i, g_s) where g_s is the newly constructed Gröbner basis element.*

(2) *Each of the obstructions $(\ell_i, r_i, \ell_s, r_s)$ and $(\ell_j, r_j, \ell_s, r_s)$ is without overlap or a multiple of a non-trivial obstruction.*

Application to Group Rings

$G = \langle x_1, \ldots, x_n; \ell_1 = r_1, \ldots, \ell_s = r_s \rangle$
finitely presented group (or monoid)

$I = \langle \ell_1 - r_1, \ldots, \ell_s - r_s \rangle$ two-sided ideal in $K\langle X \rangle$

$K\langle G \rangle = K\langle X \rangle / I$ group ring (or monoid ring)

Remark

(a) *Notice that in general we have to include indeterminates representing the inverses* $y_i = x_i^{-1}$ *and relations* $x_i y_i - 1$, $y_i x_1 - 1$ *here.*

(b) *If* x_i *represents a group element of finite order, i.e. if we have a relation* $x_i^k - 1 \in I$, *we do not need* y_i.

The Word Problem

Proposition (Ideal Membership)

Given a two-sided ideal $I = \langle g_1, \ldots, g_s \rangle$ in $K\langle X \rangle$ and a polynomial $f \in K\langle X \rangle$, there is a semi-decision procedure for determining whether $f \in I$.

(1) *Perform one iteration of the Buchberger Procedure.*

(2) *Check whether the normal remainder of f after division by the intermediate partial Gröbner basis G is zero. If it is, return* `TRUE`*. Otherwise, continue with (1).*

Remark

For a word $w \in X^*$, we have a semi-decision procedure for checking whether w represents the neutral element of G by checking $w - 1 \in I$.

Application to Group Rings

Remark

A more careful computation, keeping track of the division steps, also solves the Explicit Membership Problem (also called Word Search Problem): if w represents the neutral element in G, write it as a product of the relators.

Elimination

Let $\{y_1, \ldots, y_m\} \subset \{x_1, \ldots, x_n\}$, and let Y^* be the monoid of words in the letters $y_1, \ldots, y_m$. For a two-sided ideal I of $K\langle X\rangle$, the set $I \cap K\langle Y\rangle$ is a two-sided ideal in $K\langle Y\rangle$. It is called the elimination ideal of I obtained by eliminating the indeterminates in $X \setminus Y$.

Definition

A word ordering σ on X^* is called an elimination ordering for $X \setminus Y$ if $\mathrm{Lw}_\sigma(f) \in K\langle Y\rangle$ implies $f \in K\langle Y\rangle$. Equivalently, an elimination ordering σ is characterized by the property that $w_1 >_\sigma w_2$ if $w_1 \notin Y^*$ and $w_2 \in Y^*$.

Application to Group Rings

Example

The total lexicographic word ordering $\mathtt{tlex}$ is defined as follows. For $t_1, t_2 \in X^*$ we let $t_1 <_{\mathtt{tlex}} t_2$ if the associated commutative terms $\tilde{t}_1, \tilde{t}_2$ satisfy $\tilde{t}_1 <_{\mathtt{lex}} \tilde{t}_2$ or if $\tilde{t}_1 = \tilde{t}_2$ and $t_1 <_{\mathtt{lex}} t_2$. The ordering $\mathtt{tlex}$ is an elimination ordering for $\{x_1, \ldots, x_k\}$ for every $k \in \{1, \ldots, n-1\}$.

Theorem (Main Theorem on Elimination)

Let $I \subset K\langle X \rangle$ be a two-sided ideal, and let G be a Gröbner basis of I with respect to an elimination ordering σ for $X \setminus Y$.
Then $G \cap K\langle Y \rangle$ is a Gröbner basis of $I \cap K\langle Y \rangle$ with respect to the restriction of σ.
In particular, a Gröbner basis of $I \cap K\langle Y \rangle$ can be enumerated.

Kernels of Algebra Homomorphisms

Let $I \subset K\langle X\rangle$ be a two-sided ideal, let $\{y_1, \ldots, y_m\}$ be a set of further indeterminates and let $\varphi : K\langle Y\rangle \longrightarrow K\langle X\rangle/I$ be the K-algebra homomorphism given by $\varphi(y_i) = \bar{h}_i$ for $i = 1, \ldots, m$.

Definition

The two-sided ideal $\Delta = \langle y_1 - h_1, \ldots, y_m - h_m\rangle + I$ of $K\langle X, Y\rangle$ is called the diagonal ideal of φ.

Proposition

We have $\ker(\varphi) = \Delta \cap K\langle Y\rangle$. *In particular, we can enumerate a Gröbner basis of the kernel of* φ.

The Order of a Group Element

$K\langle G\rangle = K\langle X\rangle/I$ group ring of a finitely presented group.

Corollary

For word $w \in X^*$ representing a group element $\bar{w} \in G$, we have a semi-decision procedure to check whether $\bar{w}$ has finite order.

Proof: Compute the kernel of the K-algebra homomorphism $K[t] \longrightarrow K\langle X\rangle/I$ given by $t \mapsto \bar{w}$. The element $\bar{w}$ has infinite order iff this kernel is zero.

Remark

To prove that $\bar{w}$ has infinite order, we can try to add polynomials to the diagonal ideal and show that the larger ideal $\widetilde{\Delta}$ satisfies $\widetilde{\Delta} \cap K\langle Y\rangle = \{0\}$. In particular, we can add the binomials defining a normal subgroup.

The Tits Alternative

If a finitely presented group $G = \langle x_1, \ldots, x_n; \ell_1 = r_1, \ldots, \ell_s = r_s \rangle$ contains a free subgroup of rank 2, two randomly chosen elements of G should generate such a subgroup.

Remark

Let $w_1, w_2 \in X^*$ be words representing two elements of G. Define a K-algebra homomorphism

$$\varphi : \; K\langle y_1, y_2, z_1, z_2 \rangle \longrightarrow K\langle G \rangle \quad \text{by } \varphi(y_i) = \bar{w}_i, \; \varphi(z_i) = \bar{w}_i^{-1}$$

and compute its kernel. The elements $\bar{w}_1, \bar{w}_2$ generate a free subgroup of G iff $\ker(\varphi) = \langle y_i z_i - 1, \, z_i y_i - 1 \rangle$.

The Generalized Word Problem

Proposition (Subalgebra Membership)

Let $\varphi : K\langle Y\rangle \longrightarrow K\langle X\rangle/I$ be a K-algebra homomorphism. Given $f \in K\langle X\rangle$, we have the following semi-decision procedure to check whether $\overline{f} \in \mathrm{im}(\varphi)$.

(a) *Run one iteration of the Buchberger Procedure to compute a Gröbner basis of Δ.*

(b) *Check whether the partial Gröbner basis G reduces f to an element in $K\langle Y\rangle$. If this is the case, return* `TRUE` *and stop. Otherwise, continue with (a).*

If we have $h = \mathrm{NR}_G(f) \in K\langle Y\rangle$ then $f = h(\varphi(y_1), \ldots, \varphi(y_m))$ is an explicit representation of f as an element of $\mathrm{im}(\varphi)$.

Application to Group Rings

Application to groups and monoids:

Let $G = \langle x_1, \ldots, x_n; \ell_1 = r_1, \ldots, \ell_s = r_s \rangle$ be a finitely presented group and let $w_1, \ldots, w_m \in X^*$ be words whose residue classes generate a subgroup H.

Given a word $f \in X^*$, we have a semi-decision procedure for the Generalized Word Problem which asks whether $\bar{f} \in H$ holds.

The element $\bar{f}$ is contained in H iff $\bar{f}$ is contained in the image of the K-algebra homomorphism

$$\varphi : K\langle y_1, \ldots, y_m, z_1, \ldots, z_m \rangle \longrightarrow K\langle G \rangle$$

defined by $\varphi(y_i) = \bar{w}_i$ and $\varphi(z_i) = \bar{w}_i^{-1}$.

If we have $\bar{f} \in H$ then the second part of the preceding proposition yields $\bar{f} = h(\bar{w}_i, \bar{w}_i^{-1})$. This representation solves the Generalized Word Search Problem.

Hilbert-Dehn Functions

Let $I \subseteq K\langle X \rangle$ be a two-sided ideal and $R = K\langle X \rangle / I$.

Definition

For $i \geq 0$, let $\mathcal{F}_i$ be the K-vector subspace of $K\langle X \rangle$ generated by the words of length $\leq i$. Then $\mathcal{F} = (\mathcal{F}_i)_{i \in \mathbb{N}}$ is an increasing filtration of $K\langle X \rangle$. It is called the degree filtration.

The vector space $\mathcal{F}_i \,/\, (\mathcal{F}_i \cap I)$ measures the (lowest degree representatives of) elements of degree $\leq i$ contained in R.

Hilbert-Dehn Functions

Definition

(a) The function $\mathrm{HF}_R^{\mathrm{tot}} : \mathbb{N} \longrightarrow \mathbb{N}$ given by

$$\mathrm{HF}_R^{\mathrm{tot}}(i) = \dim_K(\mathcal{F}_i / (\mathcal{F}_i \cap I))$$

is called the total Hilbert function of R.

(b) Its first difference function $\mathrm{HF}_R(i) = \mathrm{HF}_R^{\mathrm{tot}}(i) - \mathrm{HF}_R^{\mathrm{tot}}(i-1)$ is called the Hilbert function of R.

(c) If G is a finitely presented group, the function $\mathrm{HD}_G(i) = \mathrm{HF}_{K\langle G\rangle}(i)$ is called the Hilbert-Dehn function of G.

The value $\mathrm{HD}_G(i)$ measures the number of normal words of degree i, i.e. of words which cannot be reduced with respect to a degree compatible word ordering.

In general, the Hilbert function of R in degree i cannot be calculated, but only an upper bound.

Hilbert-Dehn Functions

σ degree-compatible word ordering (e.g. $\sigma = \mathtt{llex}$)

Proposition (Macaulay's Basis Theorem)

The residue classes of the elements of the set of normal words $\mathcal{O}_\sigma(I) = X \setminus \mathrm{Lw}_\sigma(I)$ form a K-vector space basis of R.

Corollary

We have $\mathrm{HF}_R(i) = \mathrm{HF}_{K\langle X\rangle/\mathrm{Lw}_\sigma(I)}(i)$ for all $i \geq 0$.

Definition

The power series $\mathrm{HS}_R(t) = \sum_{i\geq 0} \mathrm{HF}_R(i)\, t^i$ is called the Hilbert series of R.

Goals: Determine whether R is a finite-dimensional K-vector space; if not, find out whether HF_R has polynomial or exponential growth; compute HS_R.

Checking Finite-Dimensionality of R

Let σ be a degree compatible term ordering, and let G be a σ-Gröbner basis of I.

Definition

Let S be a finite set of terms and $\ell = \max\{\mathrm{len}(w) \mid w \in S\}$. The Ufnarovski graph Γ_S has

(1) a vertex for each normal word $w \in S$ which has length $\ell - 1$, and

(2) a directed edge (v, w) iff there are x_i, x_j such that $vx_i = x_j w$ and this is a normal word.

Theorem (Ufnarovski's Finiteness Criterion)

Assume that G is finite. Then we have $\dim_K(R) < \infty$ if and only if $\Gamma_{\mathrm{Lw}_\sigma(G)}$ contains no cycle.

Computing the Growth Rate of R

We use again the Ufnarovski graph $\Gamma_{\mathrm{Lw}_\sigma(G)}$ of R and the following proposition.

Proposition

(a) *The normal words of length i are in 1–1 correspondence with the paths of length i in the Ufnarovski graph.*

(b) *The Hilbert function of R has exponential growth if and only if its Ufnarovski graph contains two intersecting cycles.*

Moreover, in the case of polynomial growth, the maximal number of disjoint cycles visited by a path in the Ufnarovski graph is the degree of the polynomial growth.

Thus, if we can compute a σ-Gröbner basis of I, we can determine the growth rate of R.

Hilbert-Dehn Functions

Example

Let $I = \langle x^2 - y^2 \rangle$ and $\sigma = \texttt{llex}$. Then the σ-Gröbner basis of I is $G = \{x^2 - y^2, xy^2 - y^2x\}$. This yields

$$\mathrm{Lw}_\sigma(I) = \langle x^2, xy^2 \rangle \quad \text{and} \quad \mathcal{O}_\sigma(I) = \{1, x, y, xy, yx, y^2, xyx, \dots\}$$

The Ufnarovski graph of $\mathrm{Lw}_\sigma(I)$ is $y^2 \circlearrowleft \rightarrow xy \leftrightarrows yx$. Since there are two non-intersectiong cycles, the algebra $R = K\langle x, y \rangle / \langle x^2 - y^2 \rangle$ has polynomial growth of degree 2.

Example

For the monomial algebra $R = K\langle x, y \rangle / \langle x^3, xy^2 \rangle$, the Ufnarovski graph is $x \leftrightarrows y \circlearrowleft \leftarrow x^2$. Since there are two intersecting cycles, the algebra has exponential growth.

Hilbert-Dehn Functions

Definition

The Gelfand-Kirillov dimension of R is

$$\mathrm{GKdim}(R) = \overline{\lim_{i\to\infty}} \frac{\ln(\mathrm{HF}_R^{\mathrm{tot}}(i))}{\ln(i)}.$$

The Gelfand-Kirillov dimension is finite iff HF_R has polynomial growth. It is a number in $\{0, 1\} \cup [2, \infty]$.

Computing the Hilbert Series

Let M be a minimal set of generators of $\mathrm{Lw}_\sigma(I)$. The Hilbert series can be computed from M as follows:

(a) Define the notion of n-chains in M.

(b) Construct the graph of chains $C(M)$.

(c) Perform certain transformations on $C(M)$, in particular certain identifications of vertices.

(d) If the graph becomes finite after several transformations, there is a formula for the Hilbert series of $K\langle X\rangle/\mathrm{Lw}_\sigma(I)$.

(e) This Hilbert series agrees with $\mathrm{HS}_R(t)$.

ApCoCoA

All computations mentioned in this talk can be executed using the packages implemented by X. Xiu in ApCoCoA 1.9, see

`http://www.apcocoa.org`

Hilbert-Dehn Functions in Hecke Groups

While studying Dirichlet series satisfying certain functional equations, E. Hecke introduced an infinite family of groups $\mathcal{H}(\lambda_q)$, where $q \geq 3$. Geometrically, they are discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$ consisting of linear fractional transformations preserving the upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$. For every $q \geq 3$, the group $\mathcal{H}(\lambda_q)$ is generated by the transformations $S: \ z \mapsto -1/z$ and $T: \ z \mapsto z + \lambda_q$ where $\lambda_q = 2\cos(\pi/q)$. Algebraically, the Hecke group $\mathcal{H}(\lambda_q)$ is given by the group presentation

$$\mathcal{H}(\lambda_q) \ = \ \langle s, t; \ s^2 = (st)^q = 1 \rangle.$$

and can also be viewed as the free product $\mathcal{H}(\lambda_q) = C_2 * C_q$ of two cyclic groups of orders 2 and q, respectively. Hecke groups are a natural generalization of the modular group which is nothing but $\mathcal{H}(\lambda_3)$.

Growth in Hecke Groups

We study the growth of the length of the elements in this group. Therefore it will be convenient to let $u = t^{-1}$ and to use the monoid presentation

$$H'_q \;=\; \langle s, t, u;\; s^2 = (st)^q = tu = ut = 1 \rangle.$$

Furthermore, the set $\{a, b\}$ consisting of the elements $a = s$ and $b = st$ is also a system of generators of the group $\mathcal{H}(\lambda_q)$, and it has the advantage that both generators have a finite order. Consequently, letting $c = b^{-1}$, we shall also consider the monoid presentation

$$H_q \;=\; \langle a, b, c;\; a^2 = b^q = bc = cb = 1 \rangle.$$

Our first goal is to study the Hilbert-Dehn function of $\mathcal{H}(\lambda_q)$ with respect to these two presentations. The Hilbert-Dehn function of a finitely presented monoid counts the number of elements whose shortest representation (in terms of the given generators) has a given length.

More generally, let K be a field and let $P = K\langle x_1, \ldots, x_n \rangle$ be the non-commutative polynomial ring (i.e. the free associative algebra) in the indeterminates $x_1, \ldots, x_n$. Then we can define the Hilbert-Dehn function of any residue class ring of P as follows.

Definition

Let I be a two-sided ideal in P, and for every $i \in \mathbb{Z}$ let $\mathcal{F}_i$ be the K-vector subspace of P generated by all words of length $\leq i$ in the letters $x_1, \ldots, x_n$. Then the **Hilbert-Dehn function** of the ring $R = P/I$ is defined by

$$\mathrm{HD}_R(i) \;=\; \dim_K(\mathcal{F}_i/(I \cap \mathcal{F}_i)) \;-\; \dim_K(\mathcal{F}_{i-1}/(I \cap \mathcal{F}_{i-1})).$$

Growth in Hecke Groups

Given a monoid presentation $M = \langle x_1, \ldots, x_n;\ w_1 = \cdots = w_s = 1 \rangle$, we choose a field K and consider the **monoid ring**

$$K\langle M \rangle \ = \ P/\langle w_1 - 1, \ldots, w_s - 1 \rangle.$$

Then the Hilbert-Dehn function of M, denoted by $\mathrm{HD}_M(i) = \mathrm{HD}_{K\langle M \rangle}(i)$, measures the number of elements of M whose shortest representation as a word in the residue classes $\bar{x}_1, \ldots, \bar{x}_n$ has length i. It is also called the **growth function** of M. If we want to compute this function via computer algebra, we can use the following result which is a non-commutative version of Macaulay's Basis Theorem.

Proposition

In the setting above, let I be a two-sided ideal in P, and let $R = P/I$. For every $i \geq 0$, the value $\mathrm{HD}_R(i)$ of the Hilbert-Dehn function of R can be computed as follows.

(1) *Choose a length compatible word ordering σ and determine a σ-Gröbner basis G of I.*

(2) *Let $\mathcal{O}_\sigma(I)_i$ be the set of words of length i which are not subwords of a leading word of one of the elements of G.*

(3) *Return $\mathrm{HD}_R(i) = \#\mathcal{O}_\sigma(I)_i$.*

The problem with this approach is that, in general, the Gröbner basis G need not be finite. Hence this proposition my lead to an infinite computation. However, for the presentations of $\mathcal{H}(\lambda_q)$ considered in this presentation, there exist finite Gröbner bases and the proposition leads to an effective result.
Before dealing with the general situation, let us have a look at a couple of simple cases.

Example (The Modular Group)

Let $H_3 = \langle a, b, c;\ a^2 = b^3 = bc = cb = 1 \rangle$ be the modular group, and let `llex` be the length-lexicographic word ordering (i.e. we first compare the length of two words and then we break ties using the usual lexicographic ordering). Then the group ring of H_3 over a field K satisfies

$$K\langle H_3 \rangle = K\langle a, b, c \rangle / \langle a^2 - 1,\ b^3 - 1,\ bc - 1,\ cb - 1 \rangle$$

and has the `llex`-Gröbner basis

$$G_{H_3} = \{a^2 - 1,\ bc - 1,\ cb - 1,\ b^2 - c,\ c^2 - b\}.$$

The first 10 values of $\mathrm{HD}_{H_3}(i)$ are

$$\mathrm{HD}_{H_3}:\ 1,\ 3,\ 4,\ 6,\ 8,\ 12,\ 16,\ 24,\ 32,\ 48.$$

This Hilbert-Dehn function satisfies the recursive equation $\mathrm{HD}_{H_3}(i) = 2 \cdot \mathrm{HD}_{H_3}(i-2)$ for $i \geq 3$ with initial values $\mathrm{HD}_{H_3}(0) = 1$, $\mathrm{HD}_{H_3}(1) = 3$, and $\mathrm{HD}_{H_3}(2) = 4$.

Growth in Hecke Groups

The next case yields a pleasant surprise.

Example

Let us consider the Hecke group for $q = 4$ and its presentation $H_4 = \langle a, b, c;\ a^2 = b^4 = bc = cb = 1 \rangle$. Then the `llex`-Gröbner basis of the ideal $\langle a^2 - 1,\ b^4 - 1,\ bc - 1,\ cb - 1 \rangle$ is given by

$$G_{H_4} \ = \ \{a^2 - 1,\ bc - 1,\ cb - 1,\ b^2 - c^2,\ c^3 - b\}$$

and the first 10 values of the Hilbert-Dehn function are

$$\mathrm{HD}_{H_4} :\ 1,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144.$$

Of course, we recognize the well-known Fibonacci numbers $F(i)$ given by $F(1) = F(2) = 1$ and $F(i) = F(i-1) + F(i-2)$ for $i \geq 3$. The recursive equation $\mathrm{HD}_{H_4}(i) = \mathrm{HD}_{H_4}(i-1) + \mathrm{HD}_{H_4}(i-2)$ for $i \geq 3$ and the initial values $\mathrm{HD}_{H_4}(0) = 1$, $\mathrm{HD}_{H_4}(1) = 3$, and $\mathrm{HD}_{H_4}(2) = 5$ show that we have $\mathrm{HD}_{H_4}(i) = F(i+3)$ for $i \geq 1$.

The next proposition provides the `llex`-Gröbner basis for the two monoid presentations of $\mathcal{H}(\lambda_q)$ introduced above. As before, we let `llex` denote the length-lexicographic term ordering.

Proposition

Let $q \geq 3$, let $\mathcal{H}(\lambda_q)$ be the q-th Hecke group, and let K be a field.

(1) *With respect to the presentation*

$$H'_q = \langle s, t, u;\ s^2 = (st)^q = tu = ut = 1 \rangle$$

an `llex`*-Gröbner basis of the two-sided ideal $\langle s^2 - 1, (st)^q - 1, tu - 1, ut - 1 \rangle$ in the non-commutative polynomial ring $K\langle s, t, u \rangle$ is given by*

$$G_{H'_q} = \begin{cases} \{s^2 - 1, tu - 1, ut - 1, f_1, f_2\} & \text{if } q = 2m \text{ is even,} \\ \{s^2 - 1, tu - 1, ut - 1, g_1, g_2, g_3, g_4\} & \text{if } q = 2m + 1 \text{ is odd,} \end{cases}$$

where $f_1 = (st)^m - (us)^m$, $f_2 = (su)^m - (ts)^m$,
$g_1 = (st)^m s - (us)^m u$,
$g_2 = (su)^m s - (ts)^m t$, $g_3 = (st)^m t(st)^m - (us)^m u(us)^m$, and finally
$g_4 = (su)^m u(su)^m - (ts)^m t(ts)^m$.

Proposition

(2) *With respect to the presentation*

$$H_q = \langle a, b, c;\ a^2 = b^q = bc = cb = 1 \rangle$$

an `llex`*-Gröbner basis of the two-sided ideal* $\langle a^2 - 1,\ b^q - 1,\ bc - 1,\ cb - 1 \rangle$ *in the non-commutative polynomial ring* $K\langle a, b, c \rangle$ *is given by*

$$G_{H_q} = \{a^2 - 1,\ bc - 1,\ cb - 1,\ f_1, f_2\}$$

where $f_1 = b^m - c^m$, $f_2 = c^{m+1} - b^{m-1}$ *if* $q = 2m$ *is even, and where* $f_1 = b^{m+1} - c^m$, $f_2 = c^{m+1} - b^m$ *if* $q = 2m + 1$ *is odd.*

Growth in Hecke Groups

Knowing a Gröbner basis for the defining ideal I enables us to describe the set of irreducible words $\mathcal{O}_\sigma(I)_i$ for each degree i. Thus we can find and prove recursive equations satisfied by the Hilbert-Dehn functions of the group rings $K\langle G\rangle = P/I$. Our next two propositions achieve this task for the two presentations of the Hecke groups $\mathcal{H}(\lambda_q)$ introduced above.

Proposition

Let $q \geq 3$, and let $H'_q = \langle s, t, u;\ s^2 = (st)^q = tu = ut = 1 \rangle$ be the presentation of the q-th Hecke group $H'_q = \mathcal{H}(\lambda_q)$ introduced above. Then the Hilbert-Dehn function of H'_q satisfies
$\mathrm{HD}_{H'_q}(0) = 1$, $\mathrm{HD}_{H'_q}(i) = 3 \cdot 2^{i-1}$ *for* $1 \leq i \leq q-1$,
$\mathrm{HD}_{H'_q}(q) = 3 \cdot 2^{q-1} - 2$, *and* $\mathrm{HD}_{H'_q}(q+1) = 3 \cdot 2^q - 8$, *as well as the recursive equation*

$$\mathrm{HD}_{H'_q}(i) = 2 \cdot \mathrm{HD}_{H'_q}(i-1) - \mathrm{HD}_{H'_q}(i-q)$$

for every $i \geq q+2$.

Growth in Hecke Groups

The next proposition deals with the computation of the Hilbert-Dehn function for the second presentation of $\mathcal{H}(\lambda_q)$ given above.

Proposition

Let $q \geq 3$, and let $H_q = \langle a, b, c;\ a^2 = b^q = bc = cb = 1 \rangle$ be the presentation of the q-th Hecke group $H_q = \mathcal{H}(\lambda_q)$ introduced above.

(1) *If $q = 2m$ is an even number, then the Hilbert-Dehn function of H_q satisfies $\mathrm{HD}_{H_q}(0) = 1$, $\mathrm{HD}_{H_q}(i) = 3 \cdot 2^{i-1}$ for $1 \leq i \leq m-1$, $\mathrm{HD}_{H_q}(m) = 3 \cdot 2^{m-1} - 1$, and $\mathrm{HD}_{H_q}(m+1) = 3 \cdot 2^m - 4$, as well as the recursive equation*

$$\mathrm{HD}_{H_q}(i) \ = \ 2 \cdot \mathrm{HD}_{H_q}(i-1) - \mathrm{HD}_{H_q}(i-m-1)$$

for $i \geq m+2$.

Proposition

(2) *If $q = 2m+1$ is an odd number, then the Hilbert-Dehn function of H_q satisfies $\mathrm{HD}_{H_q}(0) = 1$, $\mathrm{HD}_{H_q}(i) = 3 \cdot 2^{i-1}$ for $1 \leq i \leq m$, $\mathrm{HD}_{H_q}(m+1) = 3 \cdot 2^m - 2$, $\mathrm{HD}_{H_q}(m+2) = 3 \cdot 2^{m+1} - 6$, and $\mathrm{HD}_{H_q}(m+3) = 3 \cdot 2^{m+2} - 16$, as well as the recursive equation*

$$\mathrm{HD}_{H_q}(i) \; = \; \cdot \mathrm{HD}_{H_q}(i-1) + 2 \cdot \mathrm{HD}_{H_q}(i-2) - 2 \cdot \mathrm{HD}_{H_q}(i-m-2)$$

for $i \geq m+4$.

Hilbert-Dehn Series of Hecke Groups

A more convenient way of administering the information contained in the Hilbert-Dehn function of a finitely presented group consists in coding it into its generating function, the Hilbert-Dehn series. This series is defined as follows.

Definition

Let $M = \langle x_1, \ldots, x_n;\ w_1 = \cdots = w_s = 1 \rangle$ be a finitely presented monoid, and let z denote a new indeterminate. Then the power series

$$\mathrm{HDS}_M(z) \ = \ \sum_{i=0}^{\infty} \mathrm{HD}_M(i)\, z^i \ \in \ \mathbb{Z}[[z]]$$

is called the **Hilbert-Dehn series** or the **(spherical) growth series** of M (or, more precisely, of the given presentation of M).

Growth in Hecke Groups

It is well-known that $\mathrm{HDS}(z)$ is a rational power series if $\mathrm{HD}_M(i)$ satisfies a linear recurrence relation for $i \gg 0$. Thus the Hilbert-Dehn series of the presentations of Hecke groups introduced there are rational power series.

Proposition

Let $q \geq 3$, and let $H'_q = \langle s, t, u;\ s^2 = (st)^q = tu = ut = 1 \rangle$ be the presentation of the q-th Hecke group $H'_q = \mathcal{H}(\lambda_q)$. Then the Hilbert-Dehn series of H'_q is given by

$$\mathrm{HDS}_{H'_q}(z) = \frac{1 + 2z + 2z^2 + \cdots + 2z^{q-1} + z^q}{1 - z - z^2 - \cdots - z^{q-1}}.$$

Growth in Hecke Groups

In a similar way, we can determine the Hilbert-Dehn series of the second Hecke group presentation.

Proposition

Let $q \geq 3$, and let $H_q = \langle a, b, c;\ a^2 = b^q = bc = cb = 1 \rangle$ be the presentation of the q-th Hecke group $H_q = \mathcal{H}(\lambda_q)$.

(1) *If $q = 2m$ is an even number, then the Hilbert-Dehn series of H_q is given by*

$$\mathrm{HDS}_{H_q}(z) = \frac{1 + 2z + 2z^2 + \cdots + 2z^m}{1 - z - z^2 - \cdots - z^m}.$$

(2) *If $q = 2m + 1$ is an odd integer, then the Hilbert-Dehn series of H_q is given by*

$$\mathrm{HDS}_{H_q}(z) = \frac{1 + 3z + 4z^2 + 4z^3 + \cdots + 4z^m + 2z^{m+1}}{1 - 2z^2 - 2z^3 - \cdots - 2z^{m+1}}.$$

Growth in Hecke Groups

From the recursive formulas for the Hilbert-Dehn functions of Hecke groups it is already clear that these groups have exponential growth. A more precise information about this growth is provided by the following notion.

Definition

Let $M = \langle x_1, \ldots, x_n;\ w_1 = \cdots = w_s = 1 \rangle$ be a finitely presented monoid. The limit $\omega(M) = \limsup_{n\to\infty} \sqrt[n]{\mathrm{HD}_M(n)}$ is called the **(exponential) growth rate** or the **entropy** of M with respect to the given presentation.

It is well-known that $\omega(M) = 1/R$ where R is the radius of convergence of the generating series of $\mathrm{HD}_M(n)$. In other words, the number R is the smallest absolute value of a zero of the denominator of $\mathrm{HDS}_M(z)$. The above results allow us to determine the growth rates of the Hecke group presentations under consideration.

Remark

We have the approximate values

q	3	4	5	6	7	8	9	10
$\omega(H_q')$	τ	1.8393	1.9276	1.9659	1.9836	1.9920	1.9960	1.9980
$\omega(H_q)$	$\sqrt{2}$	τ	1.7693	1.8393	1.8993	1.9276	1.9535	1.9659

where $\tau = (1+\sqrt{5})/2$ *is the golden ratio. By writing the denominator in the form* $2-(z^q-1)/(z-1)$*, one sees that the growth rate of* $\mathcal{H}(\lambda_q)$ *approaches 2 as* $q \to \infty$*.*

Subgroup Growth and Zeta Functions of Finitely Generated Groups

In the following we let G be a finitely generated group. For every $n \geq 1$, there exist only finitely many subgroups of index n in G. Since the index behaves multiplicatively when taking Cartesian products of groups, it makes sense to consider the following Dirichlet series.

Definition

For every $n \geq 1$, let $a_n(G)$ be the number of subgroups of G of index n. Moreover, let $b_n(G)$ be the number of normal subgroups of G of index n.

(1) The formal Dirichlet series

$$\zeta_G(s) = \sum_{n=1}^{\infty} a_n(G)\, n^{-s}$$

is called the **subgroup zeta function** of the group G.

(2) The formal Dirichlet series

$$\zeta_G^N(s) = \sum_{n=1}^{\infty} b_n(G)\, n^{-s}$$

is called the **normal subgroup zeta function** of G.

Growth in Hecke Groups

In order to be able to view these series as complex analytic functions on a right half plane in $\mathbb{C}$, we need to assume that the numbers $a_n(G)$ and $b_n(G)$ grow at most polynomially in n.
By

A. Lubotzky, A. Mann and D. Segal.
Finitely generated groups of polynomial subgroup growth.
Israel J. Math. **82** (1993), 363-371.

it is known that this holds if G is residually finite and has a subgroup of finite index which is soluble and of finite rank. In this case, we denote the **abscissa of convergence** of $\zeta_G(s)$ by σ_G and that of $\zeta_G^N(s)$ by σ_G^N. For a suitable version of an Euler product decomposition, we need local versions of the above Dirichlet series. They are defined as follows.

Definition

Given a finitely generated group G, a prime number p, and $n \geq 0$, we let $a_{p^n}(G)$ be the number of subgroups of G of index p^n and $b_{p^n}(G)$ the number of normal subgroups of G of index p^n.

(1) The formal p-Dirichlet series

$$\zeta_G^p(s) = \sum_{n=0}^{\infty} a_{p^n}(G)\, p^{-ns}$$

is called the **subgroup Euler factor** of G at the prime p.

(2) The formal p-Dirichlet series

$$\zeta_G^{N,p}(s) = \sum_{n=0}^{\infty} b_{p^n}(G)\, p^{-ns}$$

is called the **normal subgroup Euler factor** of G at the prime p.

Growth in Hecke Groups

If the zeta function of a finitely generated group converges in some half plane, it is an important question whether there exists an Euler product expansion. The first important case in which this was shown is the case of finitely generated nilpotent groups in which the hypotheses for the existence of σ_G and σ_G^N hold.

Theorem

Let G be a finitely generated, nilpotent group, and let $\mathcal{P}$ be the set of prime numbers.

(1) *For all $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > \sigma_G$, we have $\zeta_G(s) = \prod_{p \in \mathcal{P}} \zeta_G^p(s)$.*

(2) *For all $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > \sigma_G^N$, we have $\zeta_G^N(s) = \prod_{p \in \mathcal{P}} \zeta_G^{N,p}(s)$.*

Growth in Hecke Groups

For the case of torsion-free nilpotent groups, this was shown in

F. Grunewald, D. Segal and G.C. Smith.
Subgroups of finite index in nipotent groups.
Invent. Math. **93** (1988), 185-223.

A straightforward, purely group-theoretic proof in the general case is given in

M. Dörfer and G. Rosenberger.
Zeta functions of finitely generated nilpotent groups.
in: A.C. Kim (ed.) et al., Groups - Korea '94, Proc. Int. Conf. Pusan (Korea) 1994, de Gruyter, Berlin 1995, pp. 35-46.

To get a better feeling for these subgroup zeta functions and Euler product decompositions, we consider some important examples.

Example

Let $r \geq 1$, and let $G = \mathbb{Z}^r$ be the free abelian group of rank r. In this case, the zeta function of G satisfies

$$\zeta_{\mathbb{Z}^r}(s) \;=\; \zeta^N_{\mathbb{Z}^r}(s) \;=\; \zeta(s)\cdot\zeta(s-1)\cdots\zeta(s-r+1)$$

where $\zeta(s) = \sum_{n\geq 1} n^{-s}$ is the Riemann zeta function. Clearly, we have $\sigma_{\mathbb{Z}^r} = r$ here.

In the case $r = 2$, i.e. for the group $G = \mathbb{Z}^2$, one can go into considerably more detail. The subgroup zeta function of G satisfies $\zeta_G(s) = \zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \sigma_1(n) n^{-s}$ where $\sigma_1(n)$ is the sum of the divisors of n. Letting $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ be the Gamma function and $R(s) = (2\pi)^{-s}\Gamma(s)\zeta_G(s)$, we have the functional equation $R(2-s) = -R(s)$ for all $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > \sigma_G = 2$. (Here $R(s)$ has a meromorphic continuation to all of $\mathbb{C}$.) Finally, the function $f(\tau) = -1/24 + \sum_{n=1}^{\infty} \sigma_1(n)\, e^{2\pi i n\tau}$ defines a modular integral of weight 2 with rational period function $q(\tau) = -1/(4\pi i\tau)$.

This case suggests that we may look for further finitely generated groups whose subgroup zeta function satisfies a functional equation and gives rise to an automorphic integral.

Example

Let H_3 be the discrete Heisenberg group, i.e. the group consisting of all upper triangular matrices $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ such that $a, b, c \in \mathbb{Z}$.

Then the subgroup zeta function of H_3 is given by

$$\zeta_{H_3}(s) = \frac{\zeta(s)\,\zeta(s-1)\,\zeta(2s-2)\,\zeta(2s-3)}{\zeta(3s-3)}$$

and satisfies $\sigma_{H_3} = 2$. Furthermore, the normal subgroup zeta function of H_3 is given by $\zeta^N_{H_3}(s) = \zeta(s)\zeta(s-1)\zeta(3s-2)$ and satisfies $\sigma^N_{H_3} = 2$.

Notice that the group H_3 could also have been introduced by its presentation

$$H_3 = \langle x, y, z \mid [x, y] = z,\ [x, z] = [y, z] = 1 \rangle$$

and that it is a subgroup of index 12 in the generalized triangle group $\langle a, b \mid a^2 = b^6 = (ababab^{-1})^2 = 1 \rangle$.

Our third example contains a direct product of groups.

Example

Let $G = \mathbb{Z} \times C_p$, where p is a prime number and C_p the cyclic group of order p. Then the subgroup zeta function of G is given by

$$\zeta_G(s) = \zeta_G^N(s) = (1 + p^{-s+1}) \cdot \zeta(s)$$

and satisfies $\sigma_G = 1$.

In general, for an arbitrary finitely generated group G, it is not clear how to calculate the subgroup zeta function of G. In general, there is no Euler product decomposition and subgroup zeta functions do not have functional equations. However, there are additional possibilities if we concentrate on certain classes of groups (such as free products of cyclic groups) or if we consider only subgroups having further properties (such as normal subgroups or free subgroups). Thus we start our investigation of the case of Hecke groups in the next section.

Subgroup Growth of Hecke Groups

In 1949, M. Hall discovered a fundamental enumeration relation between subgroups of finite index in free groups and permutation representations of the free group, see

M. Hall Jr.
Subgroups of finite index in free groups.
Canad. J. Math. **1** (1949), 187-190.

Later this method was generalized to the case of free products by I.M.S. Dey, cf.

I.M.S. Dey.
Schreier systems in free products.
Proc. Glasgow Math. Ass. **7** (1965), 61-79.

Since we are interested in $\mathcal{H}(\lambda_q) = C_2 * C_q$, we describe this method explicitly.

Growth in Hecke Groups

Let G be a finitely generated group, let $n \geq 1$, and let $h_n(G)$ be the number of homomorphisms of G into the symmetric group S_n. As previously, we let $a_n(G)$ be the number of subgroups of G of index n. Then we have the recursive equation

$$a_n(G) = \frac{h_n(G)}{(n-1)!} - \frac{h_{n-1}(G)\,a_1(G)}{(n-1)!} - \frac{h_{n-2}(G)\,a_2(G)}{(n-2)!} - \cdots - \frac{h_1(G)\,a_{n-1}(G)}{1!}$$

for every $n \geq 1$, see

M. Hall Jr.
Subgroups of finite index in free groups.
Canad. J. Math. **1** (1949), 187-190.

Next we introduce a new indeterminate z and consider the generating series $f(z) = \sum_{n\geq 1} \frac{h_n(G)}{n!} z^n$. Then the above equalities can be combined to a formal power series identity

$$\sum_{n=1}^{\infty} a_n(G)\, z^n = \frac{z\, f'(z)}{f(z)}.$$

Growth in Hecke Groups

For an arbitrary finitely generated group G, the numbers $h_n(G)$ are about as hard to come by as the desired numbers $a_n(G)$. However, if G is a free product $G = A_1 * \cdots * A_r$ of finitely generated groups, then we have $h_n(G) = h_n(A_1) \cdots h_n(A_r)$ by

I.M.S. Dey.
Schreier systems in free products.
Proc. Glasgow Math. Ass. **7** (1965), 61-79.

For instance, if G is a free product of cyclic groups, this offers a good way to calculate the numbers $a_n(G)$. Let us see a case in point.

Example

It is easy to determine the subgroup counting function for the group $G = C_2 * C_2$ as follows. The recursive equation $h_{n+1}(C_2) = h_n(C_2) + n\, h_{n-1}(C_2)$ together with the initial values $h_0(C_2) = h_1(C_2) = h_2(C_2) = 1$ is used to derive the recursive equation

$$a_n(G) \;=\; a_{n-1}(G) + a_{n-2}(G) - a_{n-3}(G)$$

for $n > 3$ with initial values $a_1(G) = 1$ and $a_2(G) = a_3(G) = 3$. This recursion is solved by $a_{2k}(G) = a_{2k+1}(G) = 2k + 1$ for $k \geq 0$. Hence the subgroup zeta function of $G = C_2 * C_2$ is

$$\zeta_G(s) \;=\; 2^{-s}\,\zeta(s) \;+\; \zeta(s-1).$$

The abscissa of convergence is $\sigma_G = 2$.

Growth in Hecke Groups

Hall's method can be used to determine the subgroup zeta function of some Hecke groups. Based on the results of Chowla et al. about the number of elements in S_n whose order divides a given integer, we present a more complete answer using recursive formulas.

Proposition

Let $q \geq 3$, and let $\mathcal{H}(\lambda_q)$ be the q-th Hecke group.

(1) *The numbers $a_n(\mathcal{H}(\lambda_q))$ satisfy the recursive equations*

$$a_n(G) = \frac{A_n(2)A_n(q)}{(n-1)!} - \frac{A_{n-1}(2)A_{n-1}(q)a_1(G)}{(n-1)!} - \cdots - \frac{A_1(2)A_1(q)a_{n-1}(G)}{1!}$$

where $A_n(d)$ denotes the number of elements of S_n whose order divides d.

(2) *The numbers $A_n(d)$ satisfy the recursive equations*

$$A_n(d) = A_{n-1}(d) + \sum_{1<k\leq n;\ k|d} (n-1)(n-2)\cdots(n-k+1)\, A_{n-k}(d).$$

A particularly simple formula results from the second part of this proposition if d is a prime number p. In this case, we have $A_n(p) = \sum_{i+jp=n} \frac{n!}{i!\, j!\, p^j}$. In particular, for the group $\mathcal{H}(\lambda_p)$ we obtain

$$h_n(\mathcal{H}(\lambda_p)) \;=\; \left(\sum_{i+2j=n} \frac{1}{i!\, j!\, 2^{j-1}} \right) \left(\sum_{i+pj=n} \frac{n!}{i!\, j!\, p^j} \right).$$

Let us compute the subgroup growth of the Hecke groups $\mathcal{H}(\lambda_q)$ in some important cases.

Example

Let us consider the modular group $G = \mathcal{H}(\lambda_3)$. Here we get the recursive equations

$$a_n(G) = \frac{A_n(2)A_n(3)}{(n-1)!} - \sum_{k=1}^{n-1} \frac{1}{n!} A_{n-k}(2)\, A_{n-k}(3)\, a_k(G)$$

where $A_n(2)$ and $A_n(3)$ are given by the explicit formulas above and $a_1(G) = 1$. Thus it is possible to calculate the first values of $a_n(G)$. We find

n	1	2	3	4	5	6	7	8	9
$a_n(\mathcal{H}(\lambda_3))$	1	1	4	8	5	22	42	40	120

.

Example

In

C. Godsil, W. Imrich and R. Razen.
On the number of subgroups of given index in the modular group.
Monatsh. Math. **87** (1979), 273-280.

the authors combined the recurrence relations for the numbers $a_n(G)$ and $A_n(G)$. They showed that for $n \geq 10$ we have the recurrence relation

$$\begin{aligned} a_n(G) &= 4a_{n-3}(G) + 2a_{n-4}(G) + (n-3)a_{n-6}(G) + 2a_{n-7}(G) - (n-6)a_{n-9}(G) \\ &\quad + \sum_{i=1}^{n-7} a_{n-6-i}(G)a_i(G) - \sum_{i=1}^{n-10} a_{n-9-i}(G)a_i(G). \end{aligned}$$

If $q = p \geq 3$ is a prime number, it is possible to determine the first $2p$ values of $a_n(\mathcal{H}(\lambda_p))$ explicitly, as the next example shows.

Example

Let $p \geq 3$ be a prime number, and let $G = \mathcal{H}(\lambda_p)$. Then we have $a_1(G) = a_2(G) = 1$, $a_3(G) = \cdots = a_{p-1}(G) = 0$, $a_p(G) = A_p(2)$, and

$$a_{p+k}(G) \;=\; \binom{p-1}{k-1} \frac{p+k}{p} A_{p-k}(2)$$

for $k = 1, \ldots, p-1$, where $A_n(2) = \sum_{i+2j=n} \frac{n!}{i!\, j!\, 2^j}$. In particular, we have $a_{2p-1}(G) = 2p-1$. For $a_{2p}(G)$, an explicit (but more complicated) formula can be given as well.

Normal Subgroup Growth of Hecke Groups

To count normal subgroups of a given index n in a finitely generated group G, we may try to use a variant of the method introduced in the preceding section. The number $b_n(G)$ of these subgroups can be calculated from the number $c_n(G)$ of group homomorphisms $\varphi : G \longrightarrow S_n$ for which the centralizer of $\varphi(G)$ operates transitively on $\{1, \ldots, n\}$. Using combinatorial arguments, it is possible to derive the equalites

$$c_n(G) \;=\; n! \cdot \sum_{m|n} \frac{b_n(G)}{\binom{n}{m}!\; m^{n/m}}$$

for every $n \geq 1$. Unfortunately, it appears difficult to compute the numbers $c_n(G)$ in concrete cases such as the Hecke groups.

Growth in Hecke Groups

For the modular group, M. Newman determined the first values of $b_n(\mathcal{H}(\lambda_3))$ as follows.

Example

Let $\mathcal{H}(\lambda_3) = C_2 * C_3 = \langle a, b \mid a^2 = b^3 = 1 \rangle$ be the modular group. For a subgroup G of $\mathcal{H}(\lambda_3)$, we call $\ell(G) = \min\{i \geq 1 \mid (ab)^i \in G\}$ the **level** of G and note that a normal subgroup G of finite index in $\mathcal{H}(\lambda_3)$ has genus one if and only if $\ell(G) = 6$.

Except for the three groups $\mathcal{H}(\lambda_3)$, $\mathcal{H}(\lambda_3)^2$, and $\mathcal{H}(\lambda_3)^3$, every normal subgroup of the modular group has an index which is a multiple of 6. The first numbers $b_n(\mathcal{H}(\lambda_3))$ are given by the following table:

n	1	2	3	6	12	18	24	30	36	42	48	54	60	66
$b_n(\mathcal{H}(\lambda_3))$	1	1	1	2	1	1	2	0	0	2	2	1	1	0

Example

The normal subgroups of $\mathcal{H}(\lambda_3)$ of genus one have been completely described, see

M. Newman.
A complete description of the normal subgroups of genus one of the modular group.
Amer. J. Math. **86** (1964), 17-24.

and for every genus $g(G) \geq 2$ there are only finitely many normal subgroups of $\mathcal{H}(\lambda_3)$. Many further restrictions for normal subgroups of $\mathcal{H}(\lambda_3)$ are given in

L. Greenberg and M. Newman.
Normal subgroups of the modular group.
J. Res. Natl. Bur. Stand. **74B** (1970), 121-123.

Growth in Hecke Groups

Also for the Hecke group $\mathcal{H}(\lambda_4)$ and other Hecke groups $\mathcal{H}(\lambda_q)$ with indices $q \geq 5$, a number of individual facts are known about their normal subgroups, but a complete description for the normal subgroup counting function seems to be unknown.
In the remainder of this section we therefore restrict our attention to a special class of normal subgroups, namely normal subgroups of genus one. Recall that the genus of a free normal subgroup G of index n in $\mathcal{H}(\lambda_q)$ is given by $g = 1 - \frac{t}{2} + \frac{n(q-2)}{4q}$ where t is the number of conjugacy classes of maximal cyclic parabolic subgroups in G. For general normal subgroups of $\mathcal{H}(\lambda_q)$, the genus can be computed via the Riemann-Hurwitz formula. We note that the genus of a subgroup G of $\mathcal{H}(\lambda_q)$ is exactly the genus of the quotient space $\mathbb{H}/G$, where $\mathbb{H}$ denotes the upper half plane.

Growth in Hecke Groups

In free products of finite cyclic groups $C_{r_1} * \cdots * C_{r_s}$, there are either no or infinitely many genus one normal subgroups of finite index, and in

G. Kern-Isberner and G. Rosenberger.
Normalteiler vom Geschlecht eins in freien Produkten endlicher zyklischer Gruppen.
Results in Math. **11** (1987), 272-288.

the authors give necessary and sufficient conditions for their existence in terms of the numbers r_i. For the Hecke groups $\mathcal{H}(\lambda_q) = C_2 * C_q$, these conditions amount to $\gcd(q, 12) \geq 3$. Only in the four cases $C_2 * C_2 * C_2$, $\mathcal{H}(\lambda_3) = C_2 * C_3$, $\mathcal{H}(\lambda_4) = C_2 * C_4$, and $C_3 * C_3$, all normal subgroups of genus one and finite index are free. In all other cases where genus one normal subgroups of finite index exist, at least some of them are not free.

Growth in Hecke Groups

The counting function for normal subgroups of genus one has sometimes interesting number-theoretic properties. Therefore we introduce the following notion.

Definition

Let $G = C_{r_1} * \cdots * C_{r_s}$ be a finite free product of finite cyclic groups. For every $n \geq 1$, let $b_n^{(1)}(G)$ be the number of normal subgroups of genus one and index n in G. Then the formal Dirichlet series

$$\zeta_G^{N,1}(s) = \sum_{n=1}^{\infty} b_n^{(1)}(G)\, n^{-s}$$

is called the **normal genus one subgroup zeta function** of G.

Now we consider some cases in point, starting with the modular group.

Example

Let $\mathcal{H}(\lambda_3) = C_2 * C_3$ be the modular group. Its normal subgroups of genus one were classified in

M. Newman.
A complete description of the normal subgroups of genus one of the modular group.
Amer. J. Math. **86** (1964), 17-24.

All of them are free groups. Since the index of these subgroups is always divisible by 6, we let $a_1(n) = b_{6n}^{(1)}(\mathcal{H}(\lambda_3))$ be the number of normal subgroups of genus one and index $6n$ for every $n \geq 1$. Then it turns out that

$$a_1(n) \;=\; \tfrac{1}{6} \cdot \#\{(x,y) \in \mathbb{Z}^2 \mid x^2 + xy + y^2 = n\}$$

is a multiplicative number-theoretic function.

Example

In particular, if $n = p^k$ is a prime power, then

$$a_1(p^k) = \begin{cases} 1 & \text{if } p = 3, \\ (1 + (-1)^k)/2 & \text{if } p = 2 \text{ or } p \neq 3,\ \left(\frac{p}{3}\right) = -1, \\ k + 1 & \text{if } p \neq 3,\ \left(\frac{p}{3}\right) = 1. \end{cases}$$

Here $\left(\frac{p}{3}\right)$ denotes the Legendre symbol.
Let us define the character $\chi_{-3} : \mathbb{N} \longrightarrow \mathbb{Z}$ by $\chi_{-3}(n) = 1$ if $n \equiv 1 \pmod 3$, by $\chi_{-3}(n) = -1$ if $n \equiv -1 \pmod 3$, and by $\chi_{-3}(n) = 0$ if n is a multiple of 3. Then the function $a_1(n)$ satisfies $a_1(n) = \sum_{d \geq 1;\ d|n} \chi_{-3}(d)$. This description can be used to derive a recursive equation for $a_1(n)$.

Example

Recall that the Möbius function is given by $\mu(n) = (-1)^k$ if n is the product of k distinct primes and $\mu(n) = 0$ otherwise. By the Möbius inversion formula, we get

$$\chi_{-3}(n) \;=\; \sum_{d \geq 1;\; d|n} \mu\left(\frac{n}{d}\right)\, a_1(n).$$

For the function $a_1(n)$, this leads to the recursive equation

$$a_1(n) \;=\; \chi_{-3}(n) \;-\; \sum_{1 \leq d < n;\; d|n} \mu\left(\frac{n}{d}\right)\, a_1(d).$$

Example

Based on the explicit description of $a_1(n)$, we can also study the normal genus one zeta function of $\mathcal{H}(\lambda_3)$. We have

$$\zeta^{N,1}_{\mathcal{H}(\lambda_3)}(s) = \sum_{n=1}^{\infty} b_n^{(1)}(\mathcal{H}(\lambda_3)) \cdot n^{-s} = \sum_{k=1}^{\infty} b_{6k}^{(1)}(\mathcal{H}(\lambda_3)) \cdot (6k)^{-s}$$
$$= \sum_{k=1}^{\infty} a_1(k) \cdot (6k)^{-s} = 6^{-s} \cdot \varphi_3(s)$$

where we let $\varphi_3(s)$ be the formal Dirichlet series $\varphi_3(s) = \sum_{k=1}^{\infty} a_1(k) \cdot k^{-s}$. The abscissa of convergence is $\sigma_{\varphi_3} = 1$. By introducing the Dirichlet series $L_{-3}(s) = \sum_{n=1}^{\infty} \chi_{-3}(n)\, n^{-s}$ of the character χ_{-3}, we obtain a factorization $\varphi_3(s) = \zeta(s) \cdot L_{-3}(s)$ where $\zeta(s)$ is the Riemann zeta function. Notice that this is exactly the zeta function of the number field $\mathbb{Q}(\sqrt{-3})$.

Example

Moreover, the Dirichlet series $\varphi_3(s)$ satisfies a functional equation. Let $R(s) = (2\pi/\sqrt{3})^{-s}\,\Gamma(s)\,\varphi_3(s)$. Then we have $R(s) = R(1-s)$. Hence, if we let $a_1(0) = 1/6$, then the function

$$f(\tau) \;=\; \sum_{n=0}^{\infty} a_1(n)\exp(2\pi i\, n\,\tau/\sqrt{3})$$

defines an automorphic $(\sqrt{3},1,1)$-form, i.e. an entire automorphic form for the Hecke group $\mathcal{H}(\lambda_6) = G(\sqrt{3})$ of weight one and multiplier one. The $\mathbb{C}$-vector space of all automorphic $(\sqrt{3},1,1)$-forms is 1-dimensional. Thus the function $f(\tau)$ is a basis for this vector space.

Growth in Hecke Groups

Following the same procedure for the group $\mathcal{H}(\lambda_6)$ does not yield new insights.

Example

The group $\mathcal{H}(\lambda_6) = C_2 * C_6$ contains also non-free normal subgroups of genus one, but the total number of free normal subgroups of genus one is, for every index n, the same number as for the modular group.

Similarly, the group $C_3 * C_3$ does not produce new numbers of normal subgroups of genus one and finite index.

Example

The group $G = C_3 * C_3$ is a subgroup of the modular group of index 2. Hence the number $b_n^{(1)}(G)$ of normal subgroups of genus one and index n is zero if n is not a multiple of 3, and we have $b_{3k}^{(1)}(G) = a_1(k)$ for every $k \geq 1$ with the numbers $a_1(k)$ studied in Example before.

Growth in Hecke Groups

The next group has a rather simple normal genus one subgroup zeta function.

Example

Let G be the free product $G = C_2 * C_2 * C_2$. Here all normal subgroups of genus one are free and have an even index in G. Denoting the number of normal subgroups of genus one and index $2n$ by $c_1(n) = b_{2n}^{(1)}(G)$, we find that $c_1(n)$ is the sum of positive divisors of n, i.e. $c_1(n) = \sigma_1(n)$, see

G. Kern-Isberner and G. Rosenberger.
Normalteiler vom Geschlecht eins in freien Produkten endlicher zyklischer Gruppen.
Results in Math. **11** (1987), 272-288.

Notice that $c_1(n)$ is a multiplicative function. For the normal genus one subgroup zeta function we obtain

$$\zeta_G^{N,1}(s) = \sum_{n=1}^{\infty} b_n^{(1)}(G)\, n^{-s} = 2^{-s} \cdot \sum_{k=1}^{\infty} c_1(k)\, k^{-s} = 2^{-s}\, \zeta(s)\, \zeta(s-1).$$

Growth in Hecke Groups

Our final example leads again to an interesting normal genus one zeta function.

Example

Consider the Hecke group $\mathcal{H}(\lambda_4) = C_2 * C_4$. Every normal subgroup H of finite index and genus one is free and its index in $\mathcal{H}(\lambda_4)$ is divisible by 4. Moreover, the group H has level $\ell(H) = \min\{i > 0 \mid (ab)^i \in H\} = 4$. In fact, a free normal subgroup H of $\mathcal{H}(\lambda_4)$ has genus one if and only if $\ell(H) = 4$, see

G. Kern-Isberner and G. Rosenberger.
Normalteiler vom Geschlecht eins in freien Produkten endlicher zyklischer Gruppen.
Results in Math. **11** (1987), 272-288.

Let $b_1(n)$ be the number of such subgroups of index $4n$. Then we get

$$b_1(n) \;=\; \tfrac{1}{4} \cdot \#\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\},$$

a multiplicative number-theoretic function again.

Example

Using the character $\chi_{-4} : \mathbb{N} \longrightarrow \mathbb{Z}$ defined by $\chi_{-4}(n) = 1$ if $n \equiv 1 \pmod 4$, by $\chi_{-4}(n) = -1$ if $n \equiv -1 \pmod 4$, and by $\chi_{-4}(n) = 0$ for even n, we have the formula $b_1(n) = \sum_{d \geq 1;\ d|n} \chi_{-4}(d)$. Now we use the Möbius reverse formula again and get

$$\chi_{-4}(n) \ = \ \sum_{d \geq 1;\ d|n} \mu(\frac{n}{d})\ b_1(n).$$

This yields the recurrence relation

$$b_1(n) \ = \ \chi_{-4}(n) \ - \ \sum_{0 < d < n;\ d|n} \mu(\frac{n}{d})\, b_1(d).$$

Example

Next we study the normal genus one zeta function of $\mathcal{H}(\lambda_4)$. We introduce the Dirichlet series $L_{-4}(s) = \sum_{n=1}^{\infty} \chi_{-4}(n) n^{-s}$ and get

$$\begin{aligned}
\zeta^{N,1}_{\mathcal{H}(\lambda_4)}(s) &= \sum_{n=1}^{\infty} b_n^{(1)}(\mathcal{H}(\lambda_4))\, n^{-s} \\
&= 4^{-s} \sum_{k=1}^{\infty} b_1(k)\, k^{-s} \\
&= 4^{-s}\, \varphi_4(s) \\
&= 4^{-s}\, \zeta(s)\, L_{-4}(s)
\end{aligned}$$

where $\varphi_4(s) = \sum_{k=1}^{\infty} b_1(k)\, k^{-s}$. The abscissa of convergence is $\sigma_{\varphi_4} = 1$, and $\varphi_4(s)$ is exactly the zeta function of the field of Gaußian numbers $\mathbb{Q}(i)$.

Example

Introducing $R(s) = \pi^{-s}\,\Gamma(s)\,\varphi_4(s)$, we find that the functional equation $R(s) = R(1-s)$ holds. Now we let $b_1(0) = 1/4$ and get an automorphic $(2,1,1)$-form

$$f(\tau) \;=\; \sum_{n=0}^{\infty} b_1(n)\,\exp(2\pi i\, n\,\tau)$$

i.e. an entire automorphic form of weight one and multiplier one for the theta group $G(2)$ which is generated by the linear fractional transformations $z \mapsto -\frac{1}{z}$ and $z \mapsto z+2$, see

E. Hecke.
Lectures on Dirichlet Series, Modular Functions and Quadratic Forms.
Vandenhoeck & Ruprecht, Göttingen 1983.

Group theoretically, the theta group is a subgroup if index 3 in the modular group and isomorphic to $C_2 * C_\infty$. The $\mathbb{C}$-vector space of all automorphic $(2,1,1)$-forms for $G(2)$ is 1-dimensional. Consequently, $f(\tau)$ is a basis of this vector space.

Free Subgroup Growth of Hecke Groups

In the preceding section we saw that many normal subgroups of genus one in Hecke groups are free. This leads us to the idea to study the growth of the numbers of free subgroups of a given finite index in a finitely generated group G.

Definition

For every $n \geq 1$, let $f_n(G)$ be the number of free subgroups of index n in G. Then the formal power series

$$F_G(z) = \sum_{n=1}^{\infty} f_n(G)\, z^n$$

is called the **free subgroup counting series** of G.

Growth in Hecke Groups

The most obvious example is the case of a free group, since all of its subgroups are free.

Example

For the free group F_r of rank r, the number of group homomorphisms $F_r \longrightarrow S_n$ is clearly $(n!)^r$. As in

M. Hall Jr.
Subgroups of finite index in free groups.
Canad. J. Math. **1** (1949), 187-190.

it follows that the numbers $f_n(F_r)$ satisfy $f_1(F_r) = 1$ and

$$f_n(F_r) \;=\; n\,(n!)^{r-1} \;-\; \sum_{i=1}^{n-1}((n-i)!)^{r-1} \cdot f_i(F_r).$$

Growth in Hecke Groups

For arbitrary finitely generated groups, not much is known about their free subgroup counting series. One approach to compute the numbers $f_n(G)$ is to use the following variant of the method of Hall, which was first suggested in

W. Imrich.
On the number of subgroups of given index in $\mathrm{SL}(2,\mathbb{Z})$.
Archiv Math. **31** (1978), 224-231.

It is based on the observation that the number $f_n(G)$ is related to the number of homomorphisms from G to S_n with the property that the preimages of all stabilizers are free or trivial.

Assume that G is non-trivial, and let $k_n(G)$ be the number of these homomorphisms. Then we have the recursive equations

$$f_n(G) = \frac{k_n(G)}{(n-1)!} - \frac{k_{n-1}(G)\,f_1(G)}{(n-1)!} - \frac{k_{n-2}(G)\,f_2(G)}{(n-2)!} - \cdots - \frac{k_1(G)\,f_{n-1}(G)}{1!}$$

for all $n \geq 1$ where $f_1(G) = 1$ if G is free and $f_1(G) = 0$ otherwise. As for the analogous formulas for the numbers $a_n(G)$, these recursive equations are, in general, only of limited help, since it is not easy to determine the numbers $k_n(G)$.

Growth in Hecke Groups

The situation improves if we restrict our attention to finite free products of cyclic groups, a case including the Hecke groups. In this setting, the following explicit formulas for the numbers $k_n(G)$ were worked out in Thm. 1.4 from

W.W. Stothers.
Free subgroups of the free product of cyclic groups.
Math. Comp. **32** (1978), 1274-1280.

Proposition

Let $G = C_{r_1} * \cdots * C_{r_d} * (C_\infty)^{*u}$ *and* $t = \mathrm{lcm}(r_1, \ldots, r_d)$ *if* $d \geq 1$ *and* $t = 1$ *if* $d = 0$.

(1) *If* t *does not divide* n, *then we have* $k_n(G) = 0$.

(2) *For* $n = kt$, *we have* $k_n(G) = (n!)^u \cdot \prod_{i=1}^{d} \frac{n!}{(n/r_i)!\ r_i^{n/r_i}}$.

Growth in Hecke Groups

Explicit, but very complicated formulas for $f_n(G)$ were derived in

T. Camps, M. Dörfer and G. Rosenberger.
A recurrence relation for the number of free subgroups in free products of cyclic groups.
in: B. Fine (ed.) et al., *Aspects of Infinite Groups*, World Scientific, Singapore 2008, pp. 54-74.

from these values of $k_G(n)$. In the following we give the results only for some basic cases, including certain Hecke groups.

Example

For the group $G = C_2 * C_2$, we have $f_{2k}(G) = 1$ and $f_{2k-1}(G) = 0$ for all $k \geq 1$. In particular, the free subgroup counting series is the rational power series $F_{C_2 * C_2}(z) = z^2/(1 - z^2)$.

Example

For the free group $F_2 = C_\infty * C_\infty$, we get $f_1(F_2) = 1$ and for $n \geq 1$ the recursive equation

$$f_{n+1}(F_2) \;=\; (n+2)\, f_n(F_2) \;+\; \sum_{k=1}^{n-1} f_k(F_2)\, f_{n-k}(F_2).$$

Notice that we found linear recursive equations in Example above.

Example

Let $G(2) = C_2 * C_\infty$ be the theta group. Then we have $f_n(G(2)) = 0$ if n is odd, $f_2(G(2)) = 1$, and for $k \geq 1$ the recursive equation

$$f_{2(k+1)}(G(2)) \;=\; (2k+3)\, f_{2k}(G(2)) \;+\; \sum_{i=1}^{n-1} f_{2i}(G(2))\, f_{2(k-i)}(G(2)).$$

Example

Consider the modular group $\mathcal{H}(\lambda_3) = C_2 * C_3$. Then the numbers $f_n(\mathcal{H}(\lambda_3))$ are zero if n is not a multiple of 6. We have $f_6(\mathcal{H}(\lambda_3)) = 5$ and the recursive equation

$$f_{6(k+1)}(\mathcal{H}(\lambda_3)) \;=\; 6\,(k+1)\,f_{6k}(\mathcal{H}(\lambda_3)) \;+\; \sum_{i=1}^{k-1} f_{6i}(\mathcal{H}(\lambda_3))\,f_{6(k-i)}(\mathcal{H}(\lambda_3))$$

for $k \geq 1$.

This result was first given in

K. Wohlfahrt.

Über einen Satz von Dey und die Modulgruppe.

Arch. Math. **29** (1977), 455-457.

Example

This function grows very fast, as its initial values show:

n	6	12	18	24	30	36
$f_n(\mathcal{H}(\lambda_3))$	5	60	1105	27120	828250	30220800

Writing the free subgroup counting series in the Form $F(z) = \widehat{F}(u)$ with $u = z^6$, it is known that $\widehat{F}(u)$ satisfies a homogeneous linear differential equation of Riccati type with integral coefficients, see

T.W. Müller.
Parity patterns in Hecke groups and Fermat primes.
in: T.W. Müller (ed.), *Groups: Topological, Combinatorial, and Arithmetic Aspects*, London Math. Soc. Lect. Notes **311** (2004), Cambridge Univ. Press, Cambridge 2004, pp. 327-374.

from which the numbers $f_n(\mathcal{H}(\lambda_3))$ can also be computed recursively.

Example

Consider the modular group $\mathcal{H}(\lambda_4) = C_2 * C_4$. Then the numbers $f_n(\mathcal{H}(\lambda_4))$ are zero if n is not a multiple of 4. We have $f_4(\mathcal{H}(\lambda_4)) = 3$ and for $k \geq 1$ the recursive equation

$$f_{4(k+1)}(\mathcal{H}(\lambda_4)) \;=\; 4\,(k+1)\,f_{4k}(\mathcal{H}(\lambda_4)) \;+\; \sum_{i=1}^{k-1} f_{4i}(\mathcal{H}(\lambda_4))\,f_{4(k-i)}(\mathcal{H}(\lambda_4)).$$

Example

Consider the modular group $\mathcal{H}(\lambda_6) = C_2 * C_6$. Then the numbers $f_n(\mathcal{H}(\lambda_6))$ are zero if n is not a multiple of 6. Letting $f_n = f_n(\mathcal{H}(\lambda_6))$, we have $f_6 = 15$, $f_{12} = 1695$, and for $k \geq 2$ the recursive equation

$$\begin{aligned} f_{6(k+1)} &= (36k^2 + 54k + 23)\, f_{6k} \;+\; 405\, f_{6(k-1)} \\ &\quad + \sum_{i=1}^{k-2} \left[\left(\sum_{j=0}^{i-1} f_{6(j+1)} f_{6(i-j)} \right) f_{6(k-i-1)} \;+\; 9(2k-2i+1)\, f_{6i}\, f_{6(k-i)} \right] \end{aligned}$$

Again, if we write $F(z) = \widehat{F}(u)$ with $u = z^4$, then $\widehat{F}(u)$ satisfies a homogeneous linear differential equation of Riccati type with integral coefficients.

It is important to note that the given examples are commensurable with the modular group, and hence arithmetic Fuchsian groups. It would be interesting to find the free subgroup counting series in these cases and for other Hecke groups.

Thank you for your attention!

It is important to note that the given examples are commensurable with the modular group, and hence arithmetic Fuchsian groups. It would be interesting to find the free subgroup counting series in these cases and for other Hecke groups.

Thank you for your attention!