THE COLENGTH OF A HECKE IMAGE

Prerequisites. Modules over a discrete valuation ring and the elementary divisor theorem [La, Ch. III, §7]. Chapter 19, Theorem 19.5.1; Chapter 40: edges, the lattices $H(L)$, and the condition LP of Section 40.3. Theorem 37.4.2 of Chapter 37, which states the result of this chapter in the form of [Adr, Thm. 12.18].

Chapter 40 asked, at one edge, for vectors whose pairings are nondegenerate up to p^D on all but a fraction κ of the dimension. What does that buy for the image of a product of Hecke operators, acting on forms over a whole class set and at several Frobenius orbits at once? The answer is a bound for the colength of the image that is linear in the depth and the denominator, plus a term in $\sum \kappa_v$. The counting behind it is elementary, and we prove it in a model; the covering lemma that feeds it is stated.

Throughout, $\mathfrak{o}$ is a complete discrete valuation ring with uniformizer ϖ and valuation v, and $p \in \mathfrak{o}$ is a nonzero nonunit; in the application $v(p) = 2$. Modules are finitely generated, and rk is the rank of a free $\mathfrak{o}$-module.

41.1. Covering up to a few vectors

Let M be a free $\mathfrak{o}$-module and $P \subseteq M$ a submodule. For an integer $E \geq 0$ and a real $g \geq 0$ we say that $p^E M \subseteq P$ *up to* g *vectors* if there is a set $C \subseteq M$ with at most g elements and $p^E M \subseteq P + \mathfrak{o}C$. If P has full rank, write $P = \bigoplus_i \varpi^{\varepsilon_i}\mathfrak{o}h_i$ for a basis (h_i) of M, with exponents ε_i.

Problem 41.1.1. Let P have full rank. Then $p^E M \subseteq P$ up to g vectors exactly when $\#\{i : \varepsilon_i > Ev(p)\} \leq g$.

Problem 41.1.2. Let P have full rank and $\tau \geq 0$. Then $P \cap p^\tau M = \bigoplus_i \varpi^{\max(\varepsilon_i, \tau v(p))}\mathfrak{o}h_i$, so $\operatorname{length}(M/(P \cap p^\tau M)) = \sum_i \max(\varepsilon_i, \tau v(p))$.

Problem 41.1.3. Let P have full rank, let $\tau \geq 0$ and $S \geq 1$ be integers, and suppose that $p^{\tau+\beta S} M \subseteq P$ up to g_β vectors for every $\beta \geq 0$. Then

$$\operatorname{length}\bigl(M/(P \cap p^\tau M)\bigr) \leq v(p)\Bigl(\tau \operatorname{rk} M + S \sum_{\beta \geq 0} g_\beta\Bigr).$$

41.2. Elementary symmetric functions

For real numbers $\kappa_v \geq 0$, $v \in \mathcal{V}$, let $e_j(\kappa) = \sum_{U \subseteq \mathcal{V},\, |U| = j} \prod_{v \in U} \kappa_v$.

Problem 41.2.1. $e_j(\kappa) \leq (\sum_v \kappa_v)^j / j!$ for every $j \geq 0$.

Problem 41.2.2. For $0 \leq \Sigma \leq 1$, $\sum_{\beta \geq 0} \Sigma^{\beta+1}/(\beta+1)! = e^\Sigma - 1 \leq 2\Sigma$. The inequality $e^\Sigma - 1 \leq 2\Sigma$ fails for $\Sigma = 1.26$.

Problem 41.2.3. Let $m \geq 1$ and $\Sigma = m \sum_v \kappa_v \leq 1$. In Problem 41.1.3 suppose $g_\beta \leq \operatorname{rk} M \, m^{\beta+1} e_{\beta+1}(\kappa)$ for every β. Then

$$\operatorname{length}\bigl(M/(P \cap p^\tau M)\bigr) \leq v(p) \operatorname{rk} M \, (\tau + 2S\Sigma).$$

Date: November 26, 2026.

41.3. Hecke operators on a tensor product

Here is the mechanism in a model. Let $\mathcal{V}$ be a finite set, M_v free $\mathfrak{o}$-modules for $v \in \mathcal{V}$, and $M = \bigotimes_{v\in\mathcal{V}} M_v$. Let Y_v be an endomorphism of M_v, and y_v the endomorphism of M acting by Y_v on the factor M_v and by the identity on the others. Suppose that for each v there are an integer $E_v \geq 0$ and a real $\kappa_v \geq 0$ with

$$p^{E_v} M_v \subseteq Y_v M_v \quad \text{up to } \kappa_v \operatorname{rk} M_v \text{ vectors.}$$

Problem 41.3.1. For $m \geq 1$, $p^{mE_v} M_v \subseteq Y_v^m M_v$ up to $m\kappa_v \operatorname{rk} M_v$ vectors.

Problem 41.3.2. For submodules $A_v, B_v \subseteq M_v$, the image of $\bigotimes_v (A_v + B_v)$ in M is the sum, over $U \subseteq \mathcal{V}$, of the images of $\bigotimes_{v\notin U} A_v \otimes \bigotimes_{v\in U} B_v$.

Fix $m \geq 1$, integers $0 \leq S_v \leq S$, and put

$$N = \sum_{U\subseteq\mathcal{V}} \Big(\prod_{v\notin U} y_v^m\Big)\Big(p^{\sum_{v\in U} S_v} M\Big), \qquad \tau = m\sum_v E_v.$$

So N is spanned by the images of products of Hecke operators, where each orbit not used is replaced by a scalar p^{S_v}.

Problem 41.3.3. For every $\beta \geq 0$, $p^{\tau+\beta S} M \subseteq N$ up to $\operatorname{rk} M\, m^{\beta+1} e_{\beta+1}(\kappa)$ vectors. Also $p^{\sum_v S_v} M \subseteq N$.

Problem 41.3.4. If $M = \bigoplus_c M^{(c)}$ is a direct sum of such tensor products, with the same $\mathcal{V}$, E_v, κ_v, m and S_v, and y_v acts on each summand as above, then Problem 41.3.3 holds for M.

Problem 41.3.5. Let $\mathfrak{o} = \mathbb{Z}_p$, $\mathcal{V} = \{1, 2\}$, $M_v = \mathbb{Z}_p^4$, $Y_v = \operatorname{diag}(1, 1, 1, p^5)$, $E_v = 0$, $\kappa_v = 1/4$, $m = 1$ and $S_v = 2$. Then the exponents of N in M are 0 (nine times), 2 (six times) and 4 (once), so $\operatorname{length}(M/N) = 16$. The bounds of Problem 41.3.3 are 8 for $\beta = 0$ and 1 for $\beta = 1$; Problem 41.1.3 gives $\operatorname{length}(M/N) \leq 18$, and Problem 41.2.3, with $\Sigma = 1/2$, gives 32.

The count $\operatorname{rk} M\, m^{\beta+1} e_{\beta+1}(\kappa)$ is the number of basis vectors that are bad at $\beta+1$ orbits at once. A vector bad at only β orbits is rescued by the scalars p^{S_v} there, at the cost βS in depth.

41.4. Forms on a class set

At one prime p, let $\mathcal{V}$ be a finite set of Frobenius orbits. For each $v \in \mathcal{V}$ take the data of Chapter 40: W_v, K_v, a rank k, a type r of edges, a representation V_v with lattices $H_v(L)$ for W_v-lattices $L \subset K_v^k$, and the normalizing exponent A_v, with $p^{A_v} H_v(L'') \subseteq H_v(L)$ for every edge (Problem 40.2.3). A *tuple* is a family $L = (L_v)_v$ of lattices, and $H(L) = \bigotimes_v H_v(L_v)$. Let Γ be a group acting on tuples through homomorphisms $\Gamma \to \mathrm{GL}_k(K_v)$, and $\chi\colon \Gamma \to \mathfrak{o}^\times$ a character. A *form* is a function F on tuples with $F(L) \in H(L)$ and $F(\gamma L) = \chi(\gamma)\,\gamma F(L)$; write M for the $\mathfrak{o}$-module of forms. Assume that Γ has finitely many orbits on tuples, with representatives $L^{(1)}, \ldots, L^{(h)}$, and that the stabilizer in Γ of every tuple is trivial.

Problem 41.4.1. $F \mapsto (F(L^{(c)}))_c$ is an isomorphism $M \cong \bigoplus_c H(L^{(c)})$. Hence M is free of rank $h \prod_v \dim V_v$.

The normalized Hecke operator at v is

$$(y_v F)(L) = p^{A_v} \sum_{L''} F(L_{v \to L''}),$$

the sum over the r-edges ($L'' \subset L_v$), where $L_{v\to L''}$ is L with L_v replaced by L''. For $\mathcal{V}$ a single orbit, $k = 2$, $r = 1$ and $\nu = 1$, this is the operator $Y = p^k T$ of Chapter 19, with k there the degree.

Problem 41.4.2. y_v maps M into itself, and $y_u y_v = y_v y_u$ for all $u, v \in \mathcal{V}$.

In this setting the forms are not a tensor product over the orbits on which the y_v act factorwise, since y_v moves a tuple to its neighbours. The formalization proves the covering of Section 41.3 directly.

Theorem 41.4.1 (colength of the Hecke image)**.** *In the setting above, let $\mathcal{V}' \subseteq \mathcal{V}$, let $m \geq 1$, $D \geq 0$, $c_* \geq 0$, integers $t_v \geq 0$ and $0 \leq S_v \leq S$, and reals $0 \leq \kappa_v \leq 1$, and suppose that $\mathrm{LP}(r; t_v, D, \kappa_v, c_*)$ holds at every $v \in \mathcal{V}'$. Put*

$$N = \sum_{U \subseteq \mathcal{V}'} \Big(\prod_{v \in \mathcal{V}' \setminus U} y_v^m \Big) \Big(p^{\sum_{v \in U} S_v} M \Big), \qquad \tau = m \sum_{v \in \mathcal{V}'} (t_v + D + 1), \qquad \Sigma = m \sum_{v \in \mathcal{V}'} \kappa_v.$$

(a) *For every $\beta \geq 0$, $p^{\tau + \beta S} M \subseteq N$ up to $\lfloor \mathrm{rk}\, M \, m^{\beta+1} e_{\beta+1}(\kappa) \rfloor$ vectors, and $p^{\sum_v S_v} M \subseteq N$.*

(b) *If $\Sigma \leq 1/2$, then $\mathrm{length}(M/(N \cap p^\tau M)) \leq v(p)\, \mathrm{rk}\, M\, (\tau + 2S\Sigma)$. If $M' \subseteq M$ is a saturated submodule, then $N \cap p^\tau M \cap M' \subseteq p^\tau M'$, and $\mathrm{length}(M'/(N \cap p^\tau M \cap M'))$ satisfies the same bound.*

Status: proved in the Lean formalization [Lean]. The proof of (a) first covers p^{D+1} times a depth-t lattice of forms by Hecke images at the orbits of any U, up to $\prod_{v \in U} \kappa_v \, \mathrm{rk}\, M$ vectors. For this it uses the isomorphism of Problem 41.4.1, the isolated vectors of the condition LP, which make y_v of a form concentrated at a source almost concentrated at one target, and the witnesses and tests of (iii) there. It then counts as in Section 41.3. We have not followed the proof of this covering lemma. Part (b) follows from (a) by the problems below. The corresponding statement in [Adr] is [Adr, Thm. 12.18], recalled in Theorem 37.4.2.

Problem 41.4.3. Part (a) of Theorem 41.4.1 implies the length bound in part (b).

Problem 41.4.4. Let $M' \subseteq M$ be saturated, that is, $M \cap (M' \otimes \mathrm{Frac}\, \mathfrak{o}) = M'$. Then $p^\tau M \cap M' = p^\tau M'$, and $M'/(Q \cap M')$ injects into M/Q for every submodule $Q \subseteq M$.

The formalization uses two integral structures, $M \subseteq M^{\mathrm{na}}$, on the forms at a prime; Theorem 41.4.1 is proved for M^{na} and transferred.

Problem 41.4.5. Let $p^s M^{\mathrm{na}} \subseteq M \subseteq M^{\mathrm{na}}$, both stable under the y_v, and write $N(\cdot)$ for the module N built from each. If $p^E M^{\mathrm{na}} \subseteq N(M^{\mathrm{na}})$ up to g vectors, then $p^{E+s} M \subseteq N(M)$ up to g vectors. Hence Theorem 41.4.1 holds for M with τ replaced by $\tau + s$.

With $s = e_p$, $D = D_p$, and the real depths t_v of Chapter 37 replaced by $\lceil t_v \rceil$, this is the exponent $\tau(p) = e_p + m \sum_v (\lceil t_v \rceil + D_p + 1)$ of Chapter 37, and $2S\Sigma$, with $S = \max_v S_v$, is the term $\mathrm{io}(p) = 2\Sigma(p) \max_v S_v$ there. In the formalization the local lattice of the source at a served place $w \mid p$ is $N \cap p^{\lceil \tau(p) \rceil} M \cap V^{\mathrm{ram}}$, and Theorem 41.4.1(b), with $M' = M \cap V^{\mathrm{ram}}$, is Theorem 37.4.2.

Problem 41.4.6. Let $P \subseteq M$ have full rank and $p^E M \subseteq P$. Then $\operatorname{length}(M/P) \leq v(p) E \operatorname{rk} M$. Over W, where $v(p) = 1$, with $M = H(L)$ and $P = S(L)$ on the tree of Chapter 19 with $Q > d$, where d is the degree, Theorem 19.5.1 gives $E = \lfloor \log_p d \rfloor$; for $p = d = 5$ and $Q = 25$ the bound is 6, and the true loss is 4.

Problem 41.4.7. Let $\operatorname{rk} M = 8$, $v(p) = 2$, $m = 2$, one served orbit with $\kappa = 1/8$ and $S = 3$. Then $\Sigma = 1/4$, $2S\Sigma = 3/2$, and the bound of Theorem 41.4.1(b) is $16\tau + 24$, as in Problem 37.4.2.

The colength is paid once per prime: it is the price $\tau(p) + \mathrm{io}(p)$ of recording, as a change of lattice, the gain that the chain of lifts makes on N. The gain itself is a separate statement about the lifts.

In the Lean formalization. In [Lean] "$p^E M \subseteq P$ up to g vectors" is `AllButLE`. Theorem 41.4.1 is `SelectionLemmas.Conclusion1`, proved as `LatticeSystems.theta_kernel_expansion` from the covering lemma `RestJ`, itself built from `JDelta` and `JRank` (Problem 41.4.1), `JSmith` (the condition LP at one orbit), `JStep1` (isolation) and `JLocal` (the product over orbits). The module N is `prodIdeal`, and y_v is `GAtP.yv`. Problem 41.2.3 is `floor_scaled_esymmOn_le_sum_pow` with the summation in `core`; Problem 41.4.5 is `core` and `coreT`; the version at a place is `FormalGroupSystem.LemmaVVolumeGeneral`, proved by `stmt6G`, and it gives the lattice clause of `LinkG`.

Hints

§41.1.

41.1.1: For one direction take C among the h_i; for the other, count the generators of $(p^E M + P)/P$.
41.1.2: $p^\tau M$ is diagonal in every basis of M.
41.1.3: Problems 41.1.1 and 41.1.2; count each exponent by the levels $\tau + \beta S$ it exceeds.

§41.2.

41.2.1: Expand $(\sum_v \kappa_v)^j$.
41.2.2: Convexity of $e^\Sigma - 1 - 2\Sigma$.
41.2.3: Problems 41.2.1 and 41.2.2.

§41.3.

41.3.1: Induction on m, keeping the vectors $Y_v^i C$.
41.3.3: Problems 41.3.1 and 41.3.2 with $A_v = Y_v^m M_v$; treat the terms by the size of U.
41.3.5: Work in the basis $e_i \otimes e_j$; each of the four generators of N is diagonal.

§41.4.

41.4.1: Trivial stabilizers make the extension from the representatives well defined.
41.4.2: γ maps the edges into L_v to the edges into γL_v; for integrality use Problem 40.2.3.
41.4.3: Problems 41.1.3 and 41.2.3; if $S = 0$, then $N = M$.
41.4.5: $p^s N(M^{\mathrm{na}}) \subseteq N(M)$.
41.4.6: Problems 41.1.1 and 41.1.2, and Problem 37.4.1.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[La] S. Lang, *Algebra*, revised 3rd ed., Graduate Texts in Mathematics 211, Springer, 2002.

[Lean] The Lean community, *riemann-hypothesis*, a Lean formalization of Alpöge's argument, `https://github.com/leanprover-community/riemann-hypothesis`.