Lower bounds on dimensions of mod-p Hecke algebras: The nilpotence method

Anna Medvedovsky

We present* a new method for obtaining lower bounds on the Krull dimension of a local component of a Hecke algebra acting on the space of mod-p modular forms of level one and all weights at once. This *nilpotence method* proceeds by showing that the Hilbert-Samuel function of the Hecke algebra, which is a noetherian local ring, grows fast enough to establish a lower bound on dimension. By duality it suffices to exhibit enough forms annihilated by a power of the maximal ideal. We use linear recurrences associated with Hecke operators to reduce the problem of finding these many annihilated forms to a purely algebraic question about the growth of nilpotence indices of recurrence operators on polynomial algebras in characteristic p. Along the way we introduce a theory of recursion operators over any field. The key technical result is the Nilpotence Growth Theorem for locally nilpotent recursion operators over a finite field; its proof is elementary and combinatorial in nature. The nilpotence method currently works only for the small primes p for which the modular curve $X_0(p)$ has genus zero ($p = 2$, 3, 5, 7, and 13), but we sketch a plan for generalizing it to all primes and all levels.

*Updated May 6, 2016.

Acknowledgements

It is my great pleasure to thank my advisor Joël Bellaïche. This project-in-progress owes an enormous debt to his vision, ideas, and sustained interest, and this document to his stamina and excellent taste. And in fact this is only one of two fruitful and compelling topics that he has bequeathed to me, and I know I will be working in his light for years to come. My warmest thanks for generously sharing his mathematical knowledge and clear thinking with me for the last several years.

I am delighted to thank Paul Monsky for many discussions of his own work on similar topics, for early encouragement and curiosity about mine, for numerous helpful conversations about both of my projects, and for serving on my thesis committee. I am also honored to thank J-P. Serre, most especially for his work with Nicolas and later with Bellaïche on modular forms mod 2 that engendered this and other work, but also for participating in my thesis committee, engaging with this project, and sharing his insight.

I thank Ira Gessel for numerous helpful conversations over the last few years; Jared Weinstein, for clarifying a key plot point around the Hecke recursion; Mathilde Gerbelli-Gauthier, for the deeper recurrences idea that made the key technical theorem possible, or at least a less daunting task; Naomi Jochnowitz, for immediately spotting an error in my application of her theorem; Carl Wang Erickson, for help with pseudodeformations; Tom Weston, for help with obstructions; Keith Conrad, for so much mathematical energy and generosity over so many years; Stephen Hermes for representation tricks and Jonah Ostroff for combinatorial ones. Special thanks to John Berdgall for steady support of my mathematical endeavors and for first noticing a pattern that will star in my second dissertation; and to Shaunak Deo, who has always been willing to engage and dispel my doubts, no matter how minor. For enabling many of my computations I am grateful to William Stein and other `SAGE` developers. And I thank the Ross Program for the start.

I am grateful to Susan Parker, Danny Ruberman, and Ruth Charney for so much friendly help and guidance with various aspects of graduate studies at Brandeis. Thank you to my brothers-in-arms of yore, мои товарищи по несчастью: John, Dipramit, Yurong, Yu Fang, Alex, Dawn, Cristobal; we had a good thing going for a while. I also thank the staff at Diesel Cafe, most of whom have allowed me to remain in blessed anonymity despite my near-daily presence for many weeks; that mostly clean, mostly well-lighted place was indispensable to the writing of this document.

My debt to my parents is vast and deep and remains ineffable. I will only say that they all but adopted my children this year, and I know their house has suffered.

My sweet, sweet babies: How I missed you! How you tried to stop me!

And Rob — to Rob I owe simply everything. I don't know how he does it, but I am glad he does it with me.

Contents

Chapter 1

Introduction

In 2012, Nicolas and Serre were able to determine, by elementary means, the structure of the Hecke algebra acting on modular forms mod 2 of level one. Neither their very precise results nor their techniques appear to generalize directly to other primes, but their elementary ingredients serve as the backbone of a new method, presented here, for obtaining a lower bound for the Krull dimension of a local component of the mod-p Hecke algebra.

This so-called *nilpotence method* works by exhibiting enough forms annihilated by powers of the maximal ideal — which exhibition, in turn, is achieved via an upper bound on the nilpotence index of a form relative to its weight filtration. The key technical result is purely algebraic and entirely elementary. The method currently works for the small primes p for which $\mathbb{F}_p[\Delta]$ is Hecke-invariant: $p = 2$, 3, 5, 7 and 13; but I expect that it can be extended to all primes, and even all levels.

1.1 Historical background

Some informal notation: let p be a prime, M the space of level-one modular forms modulo p of all weights, A the shallow (i.e., without U_p) Hecke algebra acting on M, and $A_{\bar\rho}$ one of the local components of A corresponding to a mod-p modular Galois representation $\bar\rho$.

The space of forms M was first studied by Swinnerton-Dyer [29], Serre [26], and Tate in the 70s. The structure of $A_{\bar\rho}$ itself was first investigated by Jochnowitz in the early 80s: in [19], she uses results of Serre and Tate to establish that $A_{\bar\rho}$ is infinite-dimensional over $\overline{\mathbb{F}}_p$. Noetherianness results from deformation theory imply that the Krull dimension of $A_{\bar\rho}$ is at least 1, as was first observed by Khare in [20]. Until recently that was the best lower bound.

In 2012, Nicolas and Serre revived interest in mod-p Hecke algebras when they determined the structure of A for $p = 2$ explicitly: it is a power series ring in the Hecke operators T_3 and T_5. Their results appeared in two short articles. In [23], they use the Hecke recursion for Δ (also see Chapter 6) to deduce, through lengthy but elementary calculations, a precise and surprising formula for how fast T_3 and T_5 annihilate Δ^n.

The structure of A follows by duality in [24].

In the last two years the Nicolas-Serre method has attracted some interest. Gerbelli-Gauthier [13] has found alternate and apparently simpler proofs of their key lemmas. The most technical parts of her calculations, in turn, can now be replaced by theta series arguments of Monsky (unpublished). Despite this activity and improvements, a direct generalization of the Nicolas-Serre method even to $p = 3$ has remained elusive.

At the same time, a lower bound for $\dim A_{\bar\rho}$ for all $p \geq 5$ was determined by Bellaïche and Khare using completely different techniques [5]. They compare $A_{\bar\rho}$ to the corresponding characteristic-zero Hecke algebra $\mathbb{T}_{\bar\rho}$, whose dimension is known to be at least 4 as witnessed by the Gouvêa-Mazur infinite fern. In passing from $\mathbb{T}_{\bar\rho}$ to $A_{\bar\rho}$, two dimensions are lost, one for p and one for a weight twist, so that the dimension of $\dim A_{\bar\rho}$ is at least 2. In the unobstructed case, they find that $A_{\bar\rho}$ is a power series ring in two variables, extending Nicolas-Serre. These results have been generalized to level N by Deo [9].

What about $p = 3$? In the appendix to Bellaïche-Khare, Bellaïche lays out an approach for tackling this remaining case by *bounding* nilpotence indices rather than calculating them precisely. This approach is implemented in this document; in particular the key missing lemma is the Nilpotence Growth Theorem (Theorem A below). But the same method also yields yet another proof of the case $p = 2$ (section 1.2 below), and recovers and slightly refines the Bellaïche-Khare results for $p = 5$, 7, and 13. It seems reasonable to hope that this method can be extended to all primes, and all levels.

Incidentally, the nilpotence method gives an inverse answer to an fifteen-year-old question posed by Khare in [20] about the relationship between the weight filtration of a mod-p form and what he called its "nilpotence filtration," closely related to the nilpotence index of a Hecke operator used here. See comments at the end of Chapter 8 for details.

1.2 The nilpotence method for $p = 2$

The space of modular forms modulo 2 is just the space of polynomials in Δ (Swinnerton-Dyer [29]). By a theorem of Tate [30], or an elementary argument of Serre [5, footnote in section 1.2], there is only one semisimple modular Galois representation $\bar\rho$, namely $1 \oplus 1$, so that $\operatorname{tr} \bar\rho = 0$. Therefore A is a local ring, and every T_ℓ for ℓ an odd prime is in the maximal ideal $\mathfrak{m}$ (Proposition 2.7 below). In particular, the T_ℓ act locally nilpotently on $M = \mathbb{F}_2[\Delta]$, and hence lower the Δ-degree of each form.

Using deformation theory (of Chenevier [7], in this case), we can show that $\mathfrak{m}$ is generated by T_3 and T_5 (section 7.5). Moreover, the sequences $\{T_3(\Delta^n)\}_n$ and $\{T_5(\Delta^n)\}_n$ of polynomials in Δ both satisfy linear recursions over $\mathbb{F}_2[\Delta]$, namely

$$T_3(\Delta^n) = \Delta\, T_3(\Delta^{n-3}) + \Delta^4\, T_3(\Delta^{n-4})$$

and

$$T_5(\Delta^n) = \Delta^2\, T_5(\Delta^{n-2}) + \Delta^4\, T_5(\Delta^{n-4}) + \Delta\, T_5(\Delta^{n-5}) + \Delta^6\, T_5(\Delta^{n-6}),$$

with companion polynomials in $\mathbb{F}_2[\Delta][X]$

$$P_{3,\Delta} = X^4 + \Delta\, X + \Delta^4 \qquad \text{and} \qquad P_{5,\Delta} = X^6 + \Delta^2\, X^4 + \Delta^4\, X^2 + \Delta\, X + \Delta^6,$$

respectively ([23, Théorème 3.1] or Chapter 6).

The key technical result of this document is the Nilpotence Growth Theorem:

Theorem A (*cf.* Theorem 5.1)**.** *Let p be any prime, and $T : \mathbb{F}_p[y] \to \mathbb{F}_p[y]$ be a degree-lowering linear operator on a polynomial algebra in characteristic p. Suppose further that the sequence $\{T(y^n)\}_n$ satisfies a linear recursion over $\mathbb{F}_p[y]$ whose companion polynomial*

$$P = X^d + a_1 X^{d-1} + \cdots + a_{d-1} X + a_d \in \mathbb{F}_p[y][X]$$

has $\deg a_i \leq i$ for all $1 \leq i < d$ and $\deg a_d = d$.

Then there exists an $\alpha < 1$ so that the nilpotence index $N_T(y^n) \ll n^\alpha$.

Here the nilpotence index $N_T(y^n)$ for any locally nilpotent operator T on a space containing f is the minimum power of T annihilating f.

It is easy to see that both T_3 and T_5 acting on $M = \mathbb{F}_2[\Delta]$ satisfy the conditions of the theorem, with $y = \Delta$. Therefore, there exists a constant $\alpha < 1$ such that

$$N(\Delta^n) := N_{T_3}(\Delta^n) + N_{T_5}(\Delta^n) \ll n^\alpha.$$

(From a refined version of the Nilpotence Growth Theorem, we get the bound $N(\Delta^n) < \frac{7}{3} n^{\frac{2}{3}}$. Compare to the more precise results of Nicolas and Serre, who give an exact recipe for the minimum k so that Δ^n annihilated by $\mathfrak{m}^k$. This recipe depends on the digits of n base 2 and implies that $\frac{1}{2}\sqrt{n} < N(\Delta^n) < \frac{3}{2}\sqrt{n}$ for n odd — in other words, for Δ^n in the kernel of U_2.)

Continuing with the nilpotence method, it is easy to see that $N(\Delta^n) < k$ implies that Δ^n is annihilated by $\mathfrak{m}^k$, so that the dimension of the space of forms f in the kernel of U_2 annihilated by $\mathfrak{m}^k$ grows at least as fast as $k^{\frac{1}{\alpha}}$, faster than linearly in k.

By duality, the Hilbert-Samuel function of A grows faster than linearly as well:

$$k \mapsto \dim A/\mathfrak{m}^k = \dim\{f \in \ker U_2 : f \text{ annihilated by } \mathfrak{m}^k\} \geq \#\{n : N(\Delta^n) < k\} \gg k^{\frac{1}{\alpha}}.$$

But for any noetherian local ring such as A, the Hilbert-Samuel function $k \mapsto \dim A/\mathfrak{m}^k$ is known to eventually coincide with a polynomial in k of degree equal to the Krull dimension of A [1, Chapter 11]. Since the Hilbert-Samuel function of A grows faster than linearly, we must have $\dim A \geq 2$. On the other hand, the maximal ideal has only two generators, so that $A = \mathbb{F}_2[\![T_3, T_5]\!]$.

1.3 Statement of results

In addition to Theorem A above, the main results of this document are given in Theorem B. The *reducible* and *irreducible* components of a Hecke algebra are those $A_{\bar\rho}$ for which $\bar\rho$ is reducible or irreducible as a representation, respectively.

Theorem B (*cf.* Theorem 8.1)**.** *If $p = 2, 3, 5, 7, 13$, then $A_{\bar\rho} \simeq \mathbb{F}_p[\![x, y]\!]$. More precisely:*

- *For $p = 2$, the Hecke algebra is $A = \mathbb{F}_2[\![T_3, T_5]\!] = \mathbb{F}_2[\![T_{\ell_3}, T_{\ell_5}]\!]$ for any pair of primes ℓ_3 and ℓ_5 with $\ell_i \equiv i \bmod 8$.*

- *For $p = 3$, the Hecke algebra is $A = \mathbb{F}_3[\![T_2, T_7 - 2]\!] = \mathbb{F}_3[\![T_{\ell_-}, T_{\ell_+} - 2]\!]$ for any pair of primes ℓ_- and ℓ_+ satisfying*
$$\begin{cases} \ell_- \text{ congruent to } 2 \text{ or } 5 \text{ modulo } 9, \\ 3 \text{ is not a perfect cube modulo } \ell_+. \end{cases}$$

- *For $p = 5$, there are four twist-isomorphic reducible local components. In each case,*
$$A_{\bar\rho} = \mathbb{F}_5[\![T_{11} - 2, T_{19}]\!] = \mathbb{F}_5[\![T_{\ell_+} - 2,\ T_\ell - 1 - \ell^{-1}]\!]$$
for any pair of primes satisfying
$$\begin{cases} \ell \not\equiv 1 \bmod 5 \text{ and } \ell \not\equiv \pm 1, \pm 7 \bmod 25, \\ \text{neither } 5 \text{ nor } 2 + \sqrt{5} \text{ are perfect fifth powers modulo } \ell_+. \end{cases}$$

- *For $p = 7$, there are nine local components, all reducible, in two isomorphism classes up to twist. In each case,*
$$A_{\bar\rho} = \mathbb{F}_7[\![T_{\ell_+} - 2,\ T_{\ell_-}]\!],$$
where ℓ_- is any prime congruent to -1 modulo 7 but not modulo 49; and ℓ_+ is congruent to 1 modulo 7 with additional conditions not described by congruences.

- *For $p = 13$, there are 48 local components: 36 are reducible in three different isomorphism classes up to twist, and 12 are irreducible and all twist-isomorphic. If $\bar\rho$ is reducible, then*
$$A_{\bar\rho} = \mathbb{F}_{13}[\![T_{\ell_+} - 2,\ T_{\ell_-}]\!],$$
where $\ell_\pm$ satisfy similar conditions as above; moreover, $A_{\bar\rho} \simeq \mathbb{F}_{13}[\![x, y]\!]$ for every $\bar\rho$.

The case $p = 2$ recovers a theorem of Nicolas-Serre [24, Théorème 4.1]. The case $p = 3$ is new. The case $p \geq 5$ recovers and mildly refines results of Bellaïche-Khare [5, Theorem III, Theorem 22]. For an outline of the proof using the nilpotence method, see section 8.100.

1.4 Overview of this document

In Chapter 2 we set notation and basic facts about modular forms modulo p and their Hecke algebras that will be used in the rest of the document. A reader familiar with these objects as presented by Jochnowitz [19, 18] will do well to skip this chapter. Key notation will be briefly recalled in later chapters.

Chapter 3 sets out the basic framework of the nilpotence method: given a sublinearity bound on the growth of the nilpotence index of a sequence of forms (the sequence $\{\Delta^n\}_{n \text{ odd}}$ in the $p = 2$ example above), one

obtains a lower bound of 2 for the Krull dimension of the corresponding Hecke algebra. Short, and not to be missed.

Chapter 4 is an extended introduction to the theory of recursion operators, which are the algebraic avatars of Hecke operators acting on algebras of modular forms for the purposes of applying our Nilpotence Growth Theorem. This theory is still a work in progress. The chapter deals with recursion operators on polynomial algebras only, which limits the primes for which the nilpotence method works to those for which the forms whose weight filtration is divisible by $p-1$ is a polynomial algebra. This is the case for $p = 2, 3, 5, 7, 13$; in each case the polynomial algebra in question is $\mathbb{F}_p[\Delta]$. This chapter may be used as a reference only, especially on a first reading. Pure abstract algebra, and self-contained.

Chapter 5 states and proves the Nilpotence Growth Theorem (Theorem A above). The first three sections are just enough for a first reading. The proof is long and combinatorial in spirit, and not particularly illuminating, at least in its current state. This chapter is also just algebra, this time in characteristic p. It is also self-contained, though the terminology of Chapter 4 can give it some context.

Chapter 6 proves that Hecke operators acting on spaces of modular forms are recursion operators. For $p = 2, 3, 5, 7, 13$, a Hecke operator acting locally nilpotently on $\mathbb{F}_p[\Delta]$ satisfies the conditions of the Nilpotence Growth Theorem.

Chapter 7 gives an algorithm for finding special Hecke operators to generate the maximal ideal of a local component of the Hecke algebra corresponding to a reducible mod-p Galois representation. This chapter refines dimension statements to the more precise statements of Theorem B.

Chapter 8 applies key theorems from Chapters 3, 5, and 6 to prove Theorem B.

Chapter 2

Modular forms modulo p

This chapter is a review of well-known properties of modular forms modulo p and their Hecke algebras that will be used in later chapters. The main references are Swinnerton-Dyer [29], Serre [27, 26], and Jochnowitz [18, 19].

Throughout this document, we work only with forms of level one.

2.1 The space of modular forms mod p

The basic space that we consider is the space of modular forms modulo p in the sense of Swinnerton-Dyer and Serre [29, 26]: $M \subset \mathbb{F}_p[\![q]\!]$ will be the span of mod-p reductions of q-expansions of all modular forms over $\mathbb{Z}$ of level one and all weights.

More precisely, let $M_k\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}\big)$ be the space of modular forms of level one and weight k, and define M_k to be the space of q-expansions of forms in $M_k\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}\big)$ reduced modulo p. That is,

$$M_k := \mathrm{image}\Big(M_k\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}\big) \to \mathbb{Z}[\![q]\!] \to \mathbb{F}_p[\![q]\!]\Big) \subset \mathbb{F}_p[\![q]\!],$$

where the first map is $f \mapsto (q\text{-expansion of } f)$ and the second map is reduction of the q-series modulo p.

Finally, let M be the span of all the M_k inside $\mathbb{F}_p[\![q]\!]$:

$$M := \sum_{k \geq 0} M_k \subset \mathbb{F}_p[\![q]\!].$$

Note that the sum is not direct. For $p > 3$, the q-expansion of the Eisenstein series E_{p-1} in $M_{p-1}\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}\big)$ is congruent to 1 modulo p, so that $M_k \hookrightarrow M_{k+p-1}$ via multiplication by the image of E_{p-1}. For $p = 2, 3$, both E_4 and E_6 have residual q-expansions equal to 1, so there's a similar phenomenon.

Since the product of two modular forms is another modular form (the weights add), and both maps above preserve algebra structure, the space M is an $\mathbb{F}_p$-subalgebra of $\mathbb{F}_p[\![q]\!]$.

From now on, we assume that all named modular forms — the Ramanujan Δ-function, the Eisenstein series

E_k of weight k, their products — are considered as q-series over $\mathbb{F}_p$ unless otherwise noted: we will simply equate $E_{p-1} = 1$.

2.1.1 Weight grading on M

Although the sum $\sum_k M_k \subset \mathbb{F}_p[\![q]\!]$ is not direct, essentially the only thing that goes wrong is the fact that M_k embeds into M_{k+p-1}. For example, we have the following

Lemma 2.1. *If $f \in M_k\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}\big)$ and $f' \in M_{k'}\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}\big)$ are two (characteristic-zero) forms, then their q-expansions are congruent modulo p only if $k \equiv k' \mod (p-1)$.*

Proof. See [29, Theorem 2 (iv)]. Generalized by Serre in [27, Théorème 1]. □

For $i \in 2\mathbb{Z}/(p-1)\mathbb{Z}$, let M^i be the sum of all the M_k with $k \equiv i \bmod (p-1)$:

$$M^i := \sum_{k \equiv i} M_k = \bigcup_{k \equiv i} M_k.$$

Here and below, congruences such as $k \equiv i$ are modulo $p-1$ unless otherwise specified. In particular, if $p = 2$ or 3, then $M^0 = M$.

Now the the sum of the M^is inside $\mathbb{F}_p[\![q]\!]$ *is* direct:

Lemma 2.2 (Swinnerton-Dyer)**.** $M = \bigoplus_{i \in 2\mathbb{Z}/(p-1)\mathbb{Z}} M^i$.

Proof. See [29, Theorem 2 (iv)]. Lemma 2.1 is a special case of Lemma 2.2. □

The decomposition $M = \bigoplus_i M^i$ makes M into a $(2\mathbb{Z}/(p-1)\mathbb{Z})$-graded algebra, with M^i the *weight-i-graded* piece of M. The weight-0-graded piece M^0 is a (filtered) algebra in its own right, with an exhaustive weight filtration

$$0 \subset \mathbb{F}_p = M_0 \subset M_{p-1} \subset M_{2(p-1)} \subset M_{3(p-1)} \subset \cdots \subset M^0$$

A form $f \in M^i$ for some i will be called *weight-graded* or simply *graded*.

2.1.2 Weight filtration on M^i

As discussed above, the weight of a mod-p modular form is not as robust a notion as it is in characteristic zero. Instead, it is replaced by the notion of a *weight filtration*: for $f \in M_k$, set

$$w(f) := \min\{k' : f \in M_{k'}\}.$$

For $f \in M_k$, clearly $w(f) \le k$, but the inequality may be strict. For example, $w(E_{p-1}) = 0$. Lemma 2.1 implies that $w(f) \equiv k \bmod (p-1)$.

The weight filtration evidently satisfies $w(fg) \le w(f) + w(g)$. But this inequality, too, may be strict: for example, if $p = 11$, then $w(E_4) = 4$ and $w(E_6) = 6$, whereas $w(E_4E_6) = w(E_{10}) = 0$. For graded f and g, the congruence $w(fg) \equiv w(f) + w(g) \mod (p-1)$ is forced by the weight grading.

We do have the following lemma about the multiplicativity of the weight filtration, proved by Serre in [27, §2.2 Lemma 1b]:

Lemma 2.3. *If $f \in M$ is graded, then $w(f^n) = n\,w(f)$.*

We will only use the weight filtration on the graded pieces M^i, not on the entire space M.

2.1.3 The algebra structure on M

Swinnerton-Dyer proves that, as an abstract algebra,

$$M = \begin{cases} \mathbb{F}_p[E_4, E_6]/(A(E_4, E_6) - 1) & \text{if } p > 3 \\ \mathbb{F}_p[\Delta] & \text{if } p = 2 \text{ or } 3, \end{cases}$$

where $A(E_4, E_6)$ is the polynomial in E_4 and E_6 that gives E_{p-1} in characteristic zero [29, Theorem 2(iv), Theorem 3].

For example, in characteristic zero, we have $691E_{12} = 441E_4^3 + 250E_6^2$, so that for $p = 13$ we have

$$M = \mathbb{F}_{13}[E_4, E_6]/(3E_6^2 - E_4^3 - 2).$$

For more examples, see Chapter 8.

2.2 The Hecke algebra on modular forms mod p

2.2.1 Hecke operators on M

For each positive integer n, the operator T_n defines a linear action on the characteristic-zero space $M_k\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q}\big)$. If ℓ is prime, then this action has the following form on q-expansions:

$$a_n(T_\ell f) = \begin{cases} a_{\ell n}(f) + \ell^{k-1} a_{\frac{n}{\ell}}(f) & \text{if } \ell \mid n \\ a_{\ell n}(f) & \text{otherwise.} \end{cases}$$

If $k > 0$, then $M_k\big(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}\big)$ is T_ℓ-invariant. (If $k = 0$, the only obstruction is that $T_\ell(1) = \frac{\ell+1}{\ell}$.)

In any case, if $\ell \neq p$, then T_ℓ, and hence also T_n for n prime to p, acts on M_k. Since $\ell^{k-1} \equiv \ell^{(k+p-1)-1} \mod (p-1)$, this action is compatible with the inclusions $M_k \hookrightarrow M_{k+p-1}$. So the actions on M_k fits together to give an action on each M^i, and therefore we have an action of each Hecke operator T_n with $(n, p) = 1$ on the entire space of modular forms.

We also have an action of T_n on any subspace of bounded weight of M.

2.2.2 The Hecke algebra A

First definition: product of graded pieces

For each k, let A_k be the Hecke algebra generated by all T_n with $(n, p) = 1$ acting on M_k. That is, let $\mathcal{H}^p := \mathbb{Z}[T_n : (n, p) = 1]$ be the abstract polynomial algebra of Hecke operators, and define

$$A_k := \mathrm{im}\left(\mathcal{H}^p \to \mathrm{End}\, M_k\right) \subset \mathrm{End}\, M_k.$$

Here and always, $\mathrm{End}\, M_k = \mathrm{End}_{\mathbb{F}_p} M_k$ is the space of $\mathbb{F}_p$-linear maps $M_k \to M_k$.

As remarked above, we have restriction maps $A_{k+p-1} \to A_k$. These are surjective since each A_k is generated

by the action of the same Hecke operators. We define

$$A^i := \varprojlim_{k \equiv i} A_k.$$

This is the (shallow, i.e., without U_p) Hecke algebra acting on M^i, a profinite ring. Finally, the (shallow) Hecke algebra on all of $M = \bigoplus_i M_i$ is simply

$$A := \prod_i A^i.$$

Second definition: all at once

Alternatively, we can let $M_{\leq k} := \sum_{k' \leq k} M_k \subset \mathbb{F}_p[\![q]\!]$ be the subspace of M of weight bounded by k, and let $A_{\leq k}$ be the Hecke algebra acting on $M_{\leq k}$ defined just as above. The inclusion maps $M_{\leq k} \hookrightarrow M_{\leq k+1}$ give restriction maps $A_{\leq k+1} \twoheadrightarrow A_{\leq k}$. I claim that

$$A = \varprojlim_k A_{\leq k}.$$

Indeed, each $M_{\leq k}$ splits up into a direct sum of Hecke-invariant subspaces according to weight modulo $p-1$, so that each $A_{\leq k}$ splits up into a finite direct product. This separation persists up the inverse limit.

Third definition: topology

There is a topological way to define the Hecke algebra: A is the completion, for the compact-open topology, of the image of the action of the Hecke operators in $\operatorname{End} M$. That is,

$$A = \widehat{\operatorname{im}}\Big(\mathcal{H}^p \to \operatorname{End} M\Big) \subset \operatorname{End} M.$$

Unpacking this definition gets its own section below. The equivalence of this definition with the previous ones is proved in Proposition 2.4.

2.2.3 The topology on A as a subspace of $\operatorname{End} M$

We analyze the compact-open topology on $\operatorname{End} M$, and reconcile the naïve algebraic definition of the Hecke algebra on M with A as we've defined it.

The compact-open topology

First, we recall the definition of the compact-open topology: this is a topology on the space of continuous maps from one topological space to another. In the special case where the two spaces are topological abelian groups X and Y, with $\{U_\alpha\}$ a collection of open subgroups forming a basic system of neighborhoods of 0 in Y, and $\{K_\beta\}$ a collection of compact subgroups of X with the property that any compact subset C of X containing 0 is contained in some K_β, a basis for the compact-open topology on $\operatorname{Hom}^{\text{cont}}_{\mathbb{Z}\text{-mod}}(X, Y)$ is given by the collection $\big\{\{f : f(U_\alpha) \subset K_\beta\}\big\}_{\alpha,\beta}$.

The compact-open topology on $\operatorname{End} M$

Next, we see $\operatorname{End} M$ with its compact-open topology. In this case, $X = Y = M$ with the discrete topology. This means that the zero subspace by itself is already a basis of open neighborhood-spaces around 0. The compact sets are the finite ones; since our base field is finite, a compact subspace is a finite-dimensional

one. So the spaces $M_{\leq k}$ form a basic system of compact subspaces of M (that is, any compact subset of M is contained in some $M_{\leq k}$). Finally, the compact-open topology on $\operatorname{End} M$ has, as a basis of open neighborhoods around 0, the collection $\big\{\{T : T(M_{\leq k}) = 0\}\big\}_k = \{\operatorname{ann} M_{\leq k}\}_k$, a nested sequence of two-sided ideals. This topology is Hausdorff: if an endomorphism annihilates every $M_{\leq k}$, then it annihilates all of M, so that $\bigcap_k \operatorname{ann} M_{\leq k} = \{0\}$.

The naïve Hecke algebra on M

Let $\widetilde{A} \subset \operatorname{End} M$ be $\mathbb{F}_p$-algebra of all polynomials in the Hecke operators T_n with $(n, p) = 1$. In other words,

$$\widetilde{A} := \operatorname{im}\Big(\mathcal{H}^p \to \operatorname{End} M\Big) \subset \operatorname{End} M.$$

The algebra $\widetilde{A}$ has perhaps a more natural definition than A — and in fact it has a part to play in this story: see Corollary 6.5. At the same time, $\widetilde{A}$ is not an easy ring to study.

For example, in section 2.4 below, we will discuss the (well-known) fact that A_k, $A_{\leq k}$, and A are all semilocal rings whose maximal ideals have arithmetic meaning: they are in bijection with continuous modular Galois pseudocharacters unramified outside p with certain determinants depending on the space M_k, $M_{\leq k}$, or M. In this way, A is the natural generalizations of the Hecke algebra construction to infinite-dimensional spaces.

On the other hand (at least for $p = 2$), $\widetilde{A}$ has uncountably many maximal ideals: in [4, Theorem 4] Bellaïche shows for $p = 2$ that the image of the Hecke operators T_ℓ for ℓ prime and odd are all algebraically independent in A, and hence in $\widetilde{A} \subset A$. Therefore any arbitrary sequence $\{\lambda_\ell\}_\ell$ of elements in $\mathbb{F}_2$ indexed by odd primes ℓ defines a map $\widetilde{A} \to \mathbb{F}_2$ simply by $T_\ell \mapsto \lambda_\ell$, and the kernel of such a map is a maximal ideal of $\widetilde{A}$ containing only those T_ℓ with $\lambda_\ell = 0$. There are uncountably many such sequences, so uncountably many maximal ideals.

The completed Hecke algebra on M

Finally, we refine the third definition of A and prove that it is equivalent to the other two.

Proposition 2.4. *The following are naturally isomorphic as topological rings:*

1. *the closure of $\widetilde{A}$ in $\operatorname{End} M$ with respect to its compact-open topology;*
2. *the completion of $\widetilde{A}$ with respect to the sequence of ideals $\operatorname{ann}_{\widetilde{A}}(M_{\leq k})$;*
3. *the profinite ring $A = \varprojlim_k (A_{\leq k})$.*

Proof. Temporarily, let $A^{(1)}$, $A^{(2)}$, and $A^{(3)}$ denote the rings described in the three parts of the proposition, in order. We first prove that $A^{(2)}$ is isomorphic to $A^{(3)}$. By definition,

$$A^{(2)} = \varprojlim_k \big(\widetilde{A}/\operatorname{ann}_{\widetilde{A}}(M_{\leq k})\big).$$

But $\widetilde{A}/\operatorname{ann}_{\widetilde{A}}(M_{\leq k})$ is naturally isomorphic to $A_{\leq k}$: the kernel of the restriction map $\widetilde{A} \twoheadrightarrow A_{\leq k}$ is clearly $\operatorname{ann}_{\widetilde{A}}(M_{\leq k})$. This proves the isomorphism between $A^{(2)}$ and $A^{(3)}$.

The topology on $\widetilde{A}$ induced from the compact-open topology on $\operatorname{End} M$ has the set of

$$\operatorname{ann}(M_{\leq k}) \cap \widetilde{A} = \operatorname{ann}_{\widetilde{A}}(M_{\leq k})$$

over all k as a basic system of open neighborhoods of 0. This topology is Hausdorff, so that $\widetilde{A}$ is a subalgebra

of the completion $A^{(2)}$. In turn $A^{(2)}$ is a subalgebra of $\operatorname{End} M$: any compatible system of endomorphisms modulo $\operatorname{ann}(M_{\leq k})$ defines an endomorphism of all of M. Since $A^{(2)}$ is profinite, it is a closed subset of $\operatorname{End} M$. Finally, $\widetilde{A}$ is dense in its completion, so that $A^{(2)}$ is the closure of $\widetilde{A}$ in $\operatorname{End} M$. □

2.2.4 T_ℓ vs. T_n: a note on generators

We have defined each Hecke algebra as (topologically) generated by the Hecke operators T_n with $(n,p)=1$. But in fact, the weight-graded Hecke algebras A_k and A^i are (topologically) generated by the T_ℓ with ℓ prime only. Indeed if n factors as $n=\prod \ell_i^{n_i}$, then T_n factors as the product $T_n=\prod T_{\ell_i^{n_i}}$, so that it always suffices to consider prime-power Hecke operators. Moreover, the ℓ-power Hecke operators satisfy the (linear over the Hecke algebra) recursion

$$T_{\ell^n} = T_\ell T_{\ell^{n-1}} - \ell^{k-1} T_{\ell^{n-1}}.$$

In a weight-graded (that is, fixed weight modulo $p-1$) Hecke algebra, ℓ^{k-1} is a constant, so that T_ℓ along with $T_1=1$ is enough to generate T_{ℓ^n} over $\mathbb{F}_p$. But in a graded Hecke algebra like A and $A_{\leq k}$, we need, along with T_ℓ, a weight-separating operator for each ℓ that acts as ℓ^{k-1} on the k-graded component. See, for example, the operator denoted S_ℓ in [5].

2.3 Maximal ideals of the Hecke algebra

From now on, we assume that ℓ always refers to a prime different from p.

2.3.1 Systems of Hecke eigenvalues

Let M' be a Hecke-invariant space of mod-p modular forms (for example, $M_k,\ M_{\leq k},\ M^i,\ M$). By a *system of eigenvalues appearing in* M' we shall mean a sequence $\{\lambda_\ell\}_\ell$ of elements in a finite extension $\mathbb{F}$ of $\mathbb{F}_p$, such that there is a form f in $M'_{\mathbb{F}} := M' \otimes \mathbb{F}$ so that $T_\ell(f) = \lambda_\ell f$ for every ℓ. If this $f \in M'_{\mathbb{F}}$ is *normalized* so that $a_1(f)=1$, then in fact we must have $\lambda_\ell = a_\ell(f)$, but in characteristic p we cannot count on being able to normalize every eigenform. For example, $E_{p-1}=1 \in M_0$ corresponds to the system of eigenvalues $\left\{1+\ell^{-1}\right\}_\ell$, but $a_\ell(E_{p-1})=0$ for every ℓ. Since moreover there may be more than one mod-p eigenform that gives the same system of eigenvalues — for $p=2$, both $E_4=1$ and Δ correspond to the system of eigenvalues $\{\lambda_\ell=0\}_\ell$ — it turns out to be more convenient to work with systems of eigenvalues instead of eigenforms.

The following theorem is proved, in a slightly different form, by Jochnowitz in [18, Theorem 4.1]; she credits it to Serre and Tate in level one. See also Theorem 2.42 and Corollary 2.43 at the end of this chapter.

Theorem 2.5. *If $\lambda=\{\lambda_\ell\}$ is a system of eigenvalues appearing in M, then there is some $k \leq p^2-1$ so that λ appears in M_k.*

Corollary 2.6. *There are only finitely many systems of eigenvalues appearing in M.*

2.3.2 The maximal ideals of the Hecke algebra

Let M' one of the spaces of modular forms modulo p as in the previous section, and A' be the corresponding Hecke algebra as defined above. Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$ big enough so that all of the finitely many

systems of eigenvalues appearing in M' are defined over $\mathbb{F}$. The following proposition and proof is adapted from [2, Chapter 1].

Proposition 2.7. *There are natural bijections between the following three sets:*

1. $\{$*maximal ideals of* $A' \otimes \mathbb{F}\}$
2. $\{$*continuous* $\mathbb{F}$*-algebra maps* $A' \otimes \mathbb{F} \twoheadrightarrow \mathbb{F}\}$
3. $\{$*systems of eigenvalues appearing in* $M'\}$

Proof. We first assume that M' is finite-dimensional over $\mathbb{F}_p$ and then use the finite correspondence to conclude the general case.

Finite case: We establish a bijection between (1) and (2). A maximal ideal $\mathfrak{m}$ of $A' \otimes \mathbb{F} = A'_{\mathbb{F}}$ is sent to the map $A'_{\mathbb{F}} \twoheadrightarrow A'_{\mathbb{F}}/\mathfrak{m} = \mathbb{F}$. (Since $A' \subset \operatorname{End} M$ is a finite $\mathbb{F}_p$-algebra, $A'_{\mathbb{F}}$ is algebraic over $\mathbb{F}$.). Conversely, a map $h : A'_{\mathbb{F}} \twoheadrightarrow \mathbb{F}$ is mapped back to the maximal ideal $\ker h$. The correspondence is clearly a bijection.

Next, (3) $\rightsquigarrow$ (2): a system of eigenvalues λ engenders the map $A'_{\mathbb{F}} \twoheadrightarrow \mathbb{F}$ sending $T_\ell \mapsto \lambda_\ell$. This also tells us how to get from (3) to (1): the system of eigenvalues λ gives rise to the ideal $\sum_\ell (T_\ell - \lambda_\ell)$ of $A'_{\mathbb{F}}$, which is maximal because the quotient by it is a field.

The trickiest direction is (1) $\rightsquigarrow$ (3) because it requires actually producing an eigenvector. The algebra $A'_{\mathbb{F}}$ is artinian, as it is finite as a vector space. That means that it is semilocal, and factors as a product of localizations at maximal ideals

$$A'_{\mathbb{F}} = (A'_{\mathbb{F}})_{\mathfrak{m}_1} \times \cdots \times (A'_{\mathbb{F}})_{\mathfrak{m}_n}.$$

Therefore its module $M'_{\mathbb{F}}$ will also factor as a direct sum of localizations, each with an action of $(A'_{\mathbb{F}})_{\mathfrak{m}_i}$:

$$M'_{\mathbb{F}} = (M'_{\mathbb{F}})_{\mathfrak{m}_1} \oplus \cdots \oplus (M'_{\mathbb{F}})_{\mathfrak{m}_n}.$$

Since $A'_{\mathbb{F}}$ acts faithfully on $M'_{\mathbb{F}}$, each $(A'_{\mathbb{F}})_{\mathfrak{m}_i}$ will act faithfully on $(M'_{\mathbb{F}})_{\mathfrak{m}_i}$, so that each of the latter pieces is nonzero. Finally, each $(M'_{\mathbb{F}})_{\mathfrak{m}_i}$ is the generalized eigenspace for $\mathfrak{m}_i$, and will contain at least one eigenvector. We have proved the direction (1) $\rightsquigarrow$ (3): starting with a maximal ideal $\mathfrak{m}$, we get an nonzero eigenvector in $M'_{\mathbb{F}}[\mathfrak{m}] \subset (M'_{\mathbb{F}})_{\mathfrak{m}} = M'_{\mathbb{F}}[\mathfrak{m}^\infty]$. This completes the proof in the case that M' is finite.

Limit of finite cases: Now suppose that $M' = \varinjlim_k M'_k$ (here either $M'_k = M_{\leq k}$ so that $M' = M$, or $M'_k = M_{i+k(p-1)}$ so that $M' = M^i$) and that $A' = \varprojlim_k A'_k$, where A'_k is the Hecke algebra on M'_k and the correspondence is already established for A'_k. Suppose λ is a system of eigenvalues appearing in M'_K for some K, so that it also appears in M'_k for every $k \geq K$. For each such k, let $\mathfrak{m}_{k,\lambda}$ be the maximal ideal of A'_k corresponding to λ (and here we drop the $\mathbb{F}$ from notation). Since each maximal ideal is generated by $\{T_\ell - \lambda_\ell\}_\ell$, in the projection $A'_{k+1} \twoheadrightarrow A'_k$ we have $\mathfrak{m}_{k+1,\lambda}$ mapping onto $\mathfrak{m}_{k,\lambda}$.

Now let K be big enough so that M'_K contains all of the finitely many systems of eigenvalues appearing in $M' \subset M$ (Corollary 2.6). The observation in the previous paragraph tells us that, for $k \geq K$, the projection maps $A'_{k+1} \twoheadrightarrow A'_k$ respects the decomposition of each A'_k into local rings. That is,

$$A' = \varprojlim_{k \geq K} A'_k = \varprojlim_{k \geq K} \prod_\lambda (A'_k)_{\mathfrak{m}_{k,\lambda}} = \prod_\lambda \varprojlim_{k \geq K} (A'_k)_{\mathfrak{m}_{k,\lambda}}.$$

Write $A'_\lambda := \varprojlim_{k \geq K} (A'_k)_{\mathfrak{m}_{k,\lambda}}$ for each λ. As an inverse limit of local rings under local maps, A'_λ is local, with maximal ideal $\mathfrak{m}_\lambda := \varprojlim_{k \geq K} \mathfrak{m}_{k,\lambda}$: anything in $A'_\lambda - \mathfrak{m}_\lambda$ is a limit of units, hence a unit.

We have now decomposed A' as a finite product of local rings $\prod_\lambda A'_\lambda$, with each maximal ideal corresponding to a system of eigenvalues appearing in M'. The rest of the correspondence is clear.

□

Corollary 2.8. *The Hecke algebra $A_{\mathbb{F}}$ is semilocal, and factors as a product of localizations at its maximal ideals, each with residue field $\mathbb{F}$.*

Because each M^i is Hecke-invariant, this factorization of A is a finer one than the one into graded components in section 2.2.2. Therefore we can define the weight grading for a system of eigenvalues appearing in M. If λ is a system of eigenvalues appearing in $M^i \subset M$, set $k(\lambda) = i \in 2\mathbb{Z}/(p-1)\mathbb{Z}$.

2.3.3 The profinite topology on a local component of A

Let $\mathfrak{m}$ be a maximal ideal of A corresponding to system of eigenvalues λ, and $A_\mathfrak{m}$ the corresponding local component of A. Let $M_\mathfrak{m} \subset M$ be the generalized eigenspace corresponding to $\mathfrak{m}$, and $M_{\mathfrak{m},k} := M_\mathfrak{m} \cap M_k$, the weight-$k$ contribution of $M_\mathfrak{m}$. As noted above, $M_{\mathfrak{m},k} = 0$ unless $k \equiv k(\lambda)$ modulo $(p-1)$.

The topology that $A_\mathfrak{m}$ inherits from A is profinite, in that $A_\mathfrak{m}$ is an inverse limit of finite rings

$$A_\mathfrak{m} = \varprojlim_{k \equiv k(\lambda)} A_\mathfrak{m} / \operatorname{ann} M_{\mathfrak{m},k}.$$

As a local ring, $A_\mathfrak{m}$ also has an $\mathfrak{m}$-adic topology. How do these topologies compare?

Aside on profinite local rings

Let $B = \varprojlim_k B/\mathfrak{a}_k$ be a profinite local ring, an inverse limit of finite local rings under local maps. Let $\mathfrak{m}$ be the maximal ideal of B. Then $\mathfrak{m} = \varprojlim \mathfrak{m}/\mathfrak{a}_k$.

Proposition 2.9.

1. *The residue field $F = B/\mathfrak{m}$ is finite.*
2. *$\mathfrak{m}$ is open in B.*
3. *Every open ideal of B is $\mathfrak{m}$-adically open, so that the $\mathfrak{m}$-adic topology is finer than the given profinite topology on B. The map $(B, \mathfrak{m}\text{-adic}) \to B$ is continuous.*
4. *B is $\mathfrak{m}$-adically separated: $\cap \mathfrak{m}^n = \{0\}$.*
5. *B is $\mathfrak{m}$-adically complete.*
6. *If $\dim_F \mathfrak{m}/\mathfrak{m}^2$ is finite, then B is noetherian, and the two topologies coincide.*

Proof.

1. The residue field F is a quotient of $B/\mathfrak{a}_k$ for any k, hence finite.
2. The ideal $\mathfrak{m} = \varprojlim_k \mathfrak{m}/\mathfrak{a}_k$ is profinite, hence compact, hence closed in B. Since it has finite index, it is automatically open as well.
3. Since $B/\mathfrak{a}_k$ is finite, it is an artinian local ring, so that some power $(\mathfrak{m}/\mathfrak{a}_k)^n$ of its maximal ideal is zero. Therefore $\mathfrak{m}^n \subset \mathfrak{a}_k$; and $\mathfrak{a}_k$, and hence every open ideal, is $\mathfrak{m}$-adically open.
4. Since every $\mathfrak{m}^n$ is contained in some $\mathfrak{a}_k$, we know that $\cap_n \mathfrak{m}^n \subset \cap_k \mathfrak{a}_k = \{0\}$.
5. Any $\mathfrak{m}$-adic Cauchy sequence is automatically $\mathfrak{a}_k$-Cauchy, and those converge by assumption.
6. If $\mathfrak{m}/\mathfrak{m}^2$ is finite dimensional over F, say, generated by $x_1, \ldots, x_k$, then by the Cohen Structure Theorem

the power series ring $W(F)[\![x_1, \ldots, x_k]\!]$ surjects onto B (here $W(F)$ is the Witt vectors) so that B is noetherian. The surjection also shows that $B/\mathfrak{m}^n$ is finite dimensional over F, and hence finite, for every n. Therefore, B, already known to be $\mathfrak{m}$-adically complete, is also $\mathfrak{m}$-adically compact. That means that the continuous map $(B, \mathfrak{m}\text{-adic}) \to B$ sends closed sets to closed sets. Therefore, the two topologies coincide.

□

Back to the local Hecke algebra

In section 2.5.2, we will show that a local component of A is always noetherian, so that the profinite topology will indeed be the same as the $\mathfrak{m}$-adic topology.

2.4 Modular Galois pseudocharacters

2.4.1 Continuous pseudocharacters of dimension 2

A 2-dimensional pseudocharacter of a group G over ring B is an algebraic gadget designed to mimic the algebraic behavior of the trace of a representation $G \to \mathrm{GL}_2(B)$. Pseudocharacters were initially studied in the 90s by Rouquier in [25] and more recently generalized by Chenevier in [7] to work in any characteristic.

To fix ideas, by a *continuous two-dimensional pseudocharacter** of a topological group G over a topological ring B where 2 is a unit we mean a continuous map $t : G \to B$ satisfying $t(1) = 2$ along with two more properties:

1. t is central: for all $g, h \in G$, we have $t(gh) = t(hg)$.
2. t satisfies the *trace-determinant identity*: for all $g, h \in G$,

$$t(gh) + d(g)t(g^{-1}h) = t(g)t(h), \tag{A}$$

where $d = \det(t)$ is the multiplicative character $G \to B^\times$ defined by $d(g) := \frac{t(g)^2 - t(g^2)}{2}$.

In characteristic 2, the continuous character $d : G \to B^\times$ satisfying the trace-determinant identity must be given as additional data, but we will omit it from notation unless we are specifically discussing $p = 2$.

A pseudocharacter $t : G \to B$ of dimension 2 is *reducible* if $t = \psi_1 + \psi_2$ where $\psi_i : G \to B^\times$ are multiplicative characters. It is *irreducible* if there is no such decomposition. If B is a field, and t remains irreducible after any extension of scalars, then t is *absolutely irreducible*.

2.4.2 The Galois group

Let $\mathbb{Q}^{\{p,\infty\}}$ be the maximal extension of $\mathbb{Q}$ unramified outside p and ∞, and set $G_{\mathbb{Q},p} = \mathrm{Gal}(\mathbb{Q}^{\{p,\infty\}}/\mathbb{Q})$. Let $\omega : G_{\mathbb{Q},p} \to \mathbb{F}_p^\times$ be the mod-p cyclotomic character. (If $p = 2$, then $\omega = 1$.)

*In fact, we are intentionally conflating two ways of mimicking the trace of a two-dimensional representation. A Rouquier *pseudocharacter* is defined as a central map t satisfying a Frobenius identity, which is equivalent to the identity (A) if $\frac{1}{2} \in B$. A Chenevier *pseudorepresentation* (or *determinant*) is a pair of maps (t, d) satisfying the definitions given above. The key property of a dimension-2 pseudocharacter — if B is an algebraically closed field then t is the trace of an actual two-dimension representation of G over B — works for Rouquier pseudocharacters if $\frac{1}{2}$ is in B, and for Chenevier pseudorepresentations in any characteristic. So it is Chenevier's notion that we are using here, although we continue to use the word *pseudocharacter* and largely ignore d. For a definition of Rouquier pseudocharacters and a proof of the equivalence of the two notions if $\frac{1}{2} \in B$, see Appendix A.

Lemma 2.10. *If $\psi : G_{\mathbb{Q},p} \to \overline{\mathbb{F}}_p^\times$ is a continuous character, then $\psi = \omega^i$ for some i in $\mathbb{Z}$.*

Proof. Since ψ is continuous, $\overline{\mathbb{F}}_p^\times$ is discrete and abelian, and $G_{\mathbb{Q},p}$ is profinite, ψ must factor through a finite quotient of $G_{\mathbb{Q},p}^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, which means that the image is contained in some finite extension $\mathbb{F}$ of $\mathbb{F}_p$. But since $\mathbb{F}^\times$ has order prime to p, the character ψ must further factor through a prime-to-p quotient of $G_{\mathbb{Q},p}^{\mathrm{ab}}$, that is, though $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. The claim follows. □

Corollary 2.11. *If $t : G_{\mathbb{Q},p} \to \mathbb{F}$ is a continuous two-dimensional pseudocharacter over some extension $\mathbb{F}$ of $\mathbb{F}_p$, then t is irreducible if and only if it is absolutely irreducible.*

If $p > 2$ and $\tau : G_{\mathbb{Q},p} \to \overline{\mathbb{F}}_p$ is a continuous two-dimensional pseudocharacter, let its *weight* $k(\tau) \in \mathbb{Z}/(p-1)\mathbb{Z}$ be the residue class of any integer k that satisfies $\det(\tau) = \omega^{k-1}$.

2.4.3 Galois pseudocharacters attached to systems of eigenvalues

Via a theorem of Deligne, we can associate, to every system of eigenvalues $\lambda = \{\lambda_\ell\}$ appearing in M_k, a 2-dimensional continuous odd Galois pseudocharacter $\tau_\lambda : G_{\mathbb{Q},p} \to \mathbb{F}$ characterized by the fact that $\tau_\lambda(\mathrm{Frob}_\ell) = \lambda_\ell$ and $\det(\tau_\lambda) = \omega^{k-1}$. The condition on $\det(\tau_\lambda)$ is automatic if $p > 2$. The condition of being *odd* corresponds to the fact that $\tau_\lambda(c) = 0$ for any complex conjugation $c \in G_{\mathbb{Q},p}$.

Briefly, the construction involves lifting λ to a system of eigenvalues — that is, a normalized eigenform f — appearing in $M_k(\mathrm{SL}_2(\mathbb{Z}), \mathcal{O}_K)$ for some finite extension K of $\mathbb{Q}_p$. This can always be done, by the Deligne-Serre lifting lemma. This gives an eigenform of weight k. Then one uses Deligne's theorem to construct a continuous odd Galois representation $\rho_f : G_{\mathbb{Q},p} \to \mathrm{GL}_2(K)$ whose trace at Frobenius elements gives Fourier coefficients of f. Reducing any $G_{\mathbb{Q},p}$-invariant $\mathcal{O}_K$ lattice modulo a prime above p gives a representation $\overline{\rho}_f : G_{\mathbb{Q},p} \to \mathrm{GL}_2(\mathbb{F}')$ for some extension $\mathbb{F}'$ of $\mathbb{F}$. This residual representation is well-defined up to semisimplification only, but its trace $\tau_\lambda = \mathrm{tr}\,\overline{\rho}_f : G_{\mathbb{Q},p} \to \mathbb{F}$ is a well-defined Galois pseudocharacter, and depends only on λ.

Conversely, given a continuous odd 2-dimensional Galois pseudocharacter $\tau : G_{\mathbb{Q},p} \to \mathbb{F}$, the theory of pseudocharacters guarantees that it comes from a true representation over $\overline{\mathbb{F}}_p$. Then Serre's Conjecture in level one (now a theorem due to Khare) tell us that the system of eigenvalues $\{\tau(\mathrm{Frob}_\ell)\}_\ell$ appears in $M^{k(\tau)}$.

Therefore, we can augment Proposition 2.7. We state this refinement for the entire Hecke algebra A, but it can easily be modified for A^i, $A_{\leq k}$ and A_k by putting conditions on the weight of the pseudocharacter. From now on we will always assume that $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$ big enough to contain all the systems of eigenvalues of M.

Proposition 2.12. *There are natural bijections between the following four sets:*

1. $\{$*maximal ideals of* $A_{\mathbb{F}}\}$
2. $\{$*continuous* $\mathbb{F}$*-algebra maps* $A_{\mathbb{F}} \twoheadrightarrow \mathbb{F}\}$
3. $\{$*systems of eigenvalues appearing in* $M\}$
4. $\{$*continuous odd dimension-2 pseudocharacters* $G_{\mathbb{Q},p} \to \mathbb{F}\}$

In the future, we will write "modular pseudocharacter" as an abbreviation for "continuous, odd, dimension-2 pseudocharacter."

We will usually index the sets by the modular Galois pseudocharacter τ. That is, we let $\mathfrak{m}_\tau$ be the maximal ideal of $A_{\mathbb{F}}$ corresponding to τ, let $A_\tau := (A_{\mathbb{F}})_{\mathfrak{m}_\tau}$ be the corresponding local component of $A_{\mathbb{F}}$, and let $M_\tau := (M_{\mathbb{F}})_{\mathfrak{m}_\tau}$ be the corresponding generalized eigenspace.

2.5 Results from deformation theory

Let $\tau : G_{\mathbb{Q},p} \to \mathbb{F}$ be a modular Galois pseudocharacter. In this section, we introduce the universal deformation ring corresponding to τ to prove that A_τ is noetherian.

2.5.1 The universal deformation ring of τ

Let $\mathcal{D}_\tau$ be the functor that takes profinite local $\mathbb{F}$-algebras B to continuous pseudocharacter deformations $\widetilde{\tau} : G_{\mathbb{Q},p} \to B$ of τ subject to the constraint that $\det(\widetilde{\tau}) = \det(\tau)$.[†] This functor is representable by a complete noetherian local $\mathbb{F}$-algebra R_τ with maximal ideal $\mathfrak{m}_{R_\tau}$. (The noetherian condition follows from the p-finiteness of $G_{\mathbb{Q},p}$. See [14, Theorem 1.6], for example; the local topology comes from Proposition 2.9.) Let $\widetilde{\tau}_\tau : G_{\mathbb{Q},p} \to R_\tau$ be the universal pseudocharacter deforming τ; write t_ℓ for $\widetilde{\tau}_\tau(\mathrm{Frob}_\ell) \in R_\tau$ and t'_ℓ for $t_\ell - \tau(\mathrm{Frob}_\ell) \in \mathfrak{m}_{R_\tau}$.

Proposition 2.13. *There is a natural isomorphism of vector spaces*

$$\mathcal{D}_\tau(\mathbb{F}[\varepsilon]) \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{m}_{R_\tau}/\mathfrak{m}_{R_\tau}^2, \mathbb{F}).$$

Here $\varepsilon^2 = 0$: these are infinitesimal deformations.

Proof. To make sense of the statement, we need to see $\mathcal{D}_\tau(\mathbb{F}[\varepsilon])$ as an $\mathbb{F}$-vector space. Since τ is a pseudocharacter, this is not difficult: the vector space operations are on the ε-component of the deformation. See also [14, Problem 2.28] for a careful conceptual approach. The isomorphism itself is easy [14, Lemma 2.6 and *ff.*]. □

Following Bellaïche-Khare, we define the *tangent space* to $\mathcal{D}_\tau$, or to R_τ, as

$$\mathrm{Tan}_\tau := \mathcal{D}_\tau(\mathbb{F}[\varepsilon]) \simeq \mathrm{Hom}(\mathfrak{m}_{R_\tau}/\mathfrak{m}_{R_\tau}^2, \mathbb{F}).$$

We say that (the deformation problem defined by) τ is *unobstructed* if $\dim_{\mathbb{F}} \mathrm{Tan}_\tau = 2$.

Proposition 2.14. *Suppose τ is irreducible.*

1. *The Krull dimension of R_τ is at least 2.*
2. *τ is unobstructed if and only if $R_\tau \cong \mathbb{F}[\![x, y]\!]$.*

Proof. If τ is irreducible, then it the trace of an absolutely irreducible representation $\rho : G_{\mathbb{Q},p} \to \mathrm{GL}_2(\overline{\mathbb{F}})$, and R_τ coincides with the constant-determinant universal deformation ring of ρ. The dimension statement then follows from a theorem of Mazur [21, Corollary 3]. If τ is unobstructed, then the maximal ideal of R_τ is generated by two elements, so that there is a surjection $\mathbb{F}[\![x, y]\!] \twoheadrightarrow R_\tau$. But since $\dim R_\tau = 2$, and since $\mathbb{F}[\![x, y]\!]$ is already a domain of dimension 2, there can be nothing in the kernel. The converse is clear. □

[†]If $p = 2$, then τ is a Chenevier pseudorepresentation, that is, a pair (τ, d), and we deform τ while keeping d fixed and adding the constraint $\widetilde{\tau}(c) = 0$. (The constraint $\widetilde{\tau}(c) = 0$ is automatic for a constant-determinant deformation if $p > 2$.) In level one we in fact only have one τ, coming from the representation $1 \oplus 1$; see [4] for more details on D_τ in this case.

Obstruction in the reducible case

The analog of Proposition 2.14 is not known in the reducible case. However, assuming Vandiver's conjecture for p, a reducible τ is always unobstructed. We follow [5, Section 10]. Let $\mathcal{D}_\tau^{\mathrm{red}} \subset \mathcal{D}_\tau$ be the subfunctor of *reducible* constant-determinant deformations and $\mathrm{Tan}_\tau^{\mathrm{red}} := \mathcal{D}_\tau^{\mathrm{red}}(\mathbb{F}_p[\varepsilon])$ its tangent space. Let C be the p-torsion part of the class group of $\mathbb{Q}(\mu_p)$, and $C[\omega^k]$ be the part of C on which $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts through ω^k. *Vandiver's conjecture for p* states that $C[\omega^k] = 0$ if k is even. Fix $\tau = 1 + \omega^b$, a reducible modular pseudocharacter $G_{\mathbb{Q},p} \to \mathbb{F}_p$.

Proposition 2.15.

1. *There is a short exact sequence of $\mathbb{F}_p$-vector spaces*
$$0 \to \mathrm{Tan}_\tau^{\mathrm{red}} \to \mathrm{Tan}_\tau \to H^1(G_{\mathbb{Q},p},\ \omega^b) \otimes H^1(G_{\mathbb{Q},p},\ \omega^{-b}) \to 0.$$
2. *We have* $\dim_{\mathbb{F}_p} \mathrm{Tan}_\tau^{\mathrm{red}} = 1$.
3. *For odd b we have* $\dim H^1(G_{\mathbb{Q},p}, \omega^b) = 1 + \dim_{\mathbb{F}_p} C[\omega^{1-b}]$.
4. *The pseudocharacter τ is unobstructed if and only if* $\dim_{\mathbb{F}_p} C[\omega^{1-b}] = \dim_{\mathbb{F}_p} C[\omega^{1+b}] = 0$.
5. *If Vandiver's conjecture for p holds, then every reducible modular $\tau : G_{\mathbb{Q},p} \to \mathbb{F}_p$ is unobstructed.*

Proof. See [5, Section 10] for (1) and (3). For (2) see section 7.2. The other points follow immediately. The exact sequence is a consequence of the modification from [5, Proof of Proposition 20] to the constant-determinant case of a more general exact sequence: see [3, Theorem 2]; the last arrow is actually a double cup product to $H^2(G_{\mathbb{Q},p}, 1)^2$, which vanishes here. □

For more details, see Chapter 7, where a basis for Tan_τ is constructed in the unobstructed case.

Obstruction for $p = 2, 3, 5, 7, 13$

Proposition 2.16.
If $p = 2, 3, 5, 7, 13$ and $\tau : G_{\mathbb{Q},p} \to \mathbb{F}_p$ is a modular pseudocharacter, then τ is unobstructed.

Proof. If τ is reducible, then it is unobstructed by Proposition 2.15 since Vandiver's conjecture holds for all these p. If τ is irreducible, then $p = 13$ and τ is either the mod-13 representation attached to Δ or a cyclotomic twist (see Chapter 8 for details). In this case, τ is unobstructed by an argument of Weston given in Appendix F. □

2.5.2 The map $R_\tau \twoheadrightarrow A_\tau$

Deligne's construction of a p-adic representation attached to eigenforms over $\overline{\mathbb{Q}}_p$ may be glued together and reduced modulo p to obtain a Galois pseudocharacter over A. For an example of this construction, see [4].

Proposition 2.17.

1. *There is a unique continuous odd dim-2 pseudocharacter $t : G_{\mathbb{Q},p} \to A$ satisfying $t(\mathrm{Frob}_\ell) = T_\ell$.*
2. *For each τ, there is a unique continuous odd two-dimensional pseudocharacter $t_\tau : G_{\mathbb{Q},p} \to A_\tau$ satisfying $t_\tau(\mathrm{Frob}_\ell) = T_\ell$. Each of these further satisfies* $\det t_\tau = \omega^{k(\tau)-1}$.

The first part is the construction alluded to above. The second part follows by localizing at $\mathfrak{m}_\tau$.

Corollary 2.18. *There is a surjection $R_\tau \twoheadrightarrow A_\tau$ sending t_ℓ to T_ℓ.*

Proof. The pseudocharacter $t_\tau : G_{\mathbb{Q},p} \to A_\tau$ is a deformation of $\tau : G_{\mathbb{Q},p} \to \mathbb{F}$, since the maximal ideal $\mathfrak{m}_\tau$ is by definition is generated by elements of the form $T'_\ell = T_\ell - \tau(\mathrm{Frob}_\ell)$, so that $T_\ell \equiv \tau(\mathrm{Frob}_\ell)$ modulo $\mathfrak{m}_\tau$. Since R_τ is the universal deformation ring for τ, the deformation t_τ is induced by a continuous map $R_\tau \to A_\tau$. This map is surjective: we must have t_ℓ map to T_ℓ (both are images of $\mathrm{Frob}_\ell \in G_{\mathbb{Q},p}$), the image of R_τ is compact and hence closed in A_τ, and the T_ℓ topologically generate A_τ. □

Proposition 2.19. *The rings A_τ and A are noetherian.*

Proof. The local ring A_τ is a quotient of the noetherian ring R_τ, and A is a product of finitely many A_τs. □

Corollary 2.20. *The topology on A_τ coincides with the $\mathfrak{m}_\tau$-adic topology.*

Proof. Proposition 2.9. □

Corollary 2.21. *The Krull dimension of A_τ satisfies $1 \le \dim A_\tau \le \dim R_\tau$. If τ is unobstructed, then $1 \le \dim A_\tau \le 2$; and if further we know that $\dim A_\tau = 2$, then $R_\tau = A_\tau \simeq \mathbb{F}[\![x, y]\!]$.*

For irreducible τ, the inequality $\dim A_\tau \ge 1$ was first observed by Khare in [20].

Proof. For the first statement, Jochnowitz shows that $\dim_{\mathbb{F}} A_\tau$ is infinite [19, Corollary 6.6]. If $\dim A_\tau$ were equal to 0, then A_τ would be artinian, hence finite over $\mathbb{F}$. Therefore $\dim A_\tau \ge 1$. The other inequality follows from the surjection $R_\tau \twoheadrightarrow A_\tau$ from Corollary 2.18. The first clause of the second statement is definition of unobstructedness plus the Cohen Structure Theorem surjection $\mathbb{F}[\![x, y]\!] \twoheadrightarrow R_\tau$ in that case. The last bit follows from the surjection $\mathbb{F}[\![x, y]\!] \twoheadrightarrow R_\tau \twoheadrightarrow A_\tau$. (In the irreducible case, by Proposition 2.14 we already know that R_τ is isomorphic to $\mathbb{F}[\![x, y]\!]$ as soon as τ is unobstructed. But the isomorphism with A_τ still requires $\dim A_\tau = 2$.) □

2.6 The operator U and its kernel

Three interrelated operators act on M and its Hecke-invariant subspaces: U, the p^{th} power map F, and θ. We define these operators and discuss their properties. Most of the basic facts are from Jochnowitz [18].

2.6.1 The U operator and the p^{th} power map

Definitions

The operator $U = U_p$ acts on M by sending $f = \sum_n a_n q^n$ to

$$Uf = \sum_n a_{pn} q^n.$$

This operator is the image of T_p modulo p, so it commutes with every T_n for n prime to p, and hence with every $T \in A$. Every M_k, $M_{\le k}$, and M^i is U-invariant.

The operator U has a right inverse, the p^{th} power map. We will denote it by F, so that

$$Ff = \sum_n a_n q^{pn}.$$

If n is prime to p, then T_n and F commute; every Hecke-invariant space of modular forms is F-invariant.

Since U is right-invertible, it is surjective on M. Let $K \subset M$ be the kernel of U. A form f is in K if and only if its nonzero Fourier coefficients appear in prime-to-p places:

$$K = \{f \in M : a_n(f) \neq 0 \implies (n,p) = 1\}.$$

Properties

The operator FU is a projector, sending a form in M onto the image of F: $FUf = \sum_{p|n} a_n q^n$. Its complement $1 - FU$ projects a form $f \in M$ to K: $(1-FU)f = \sum_{(n,p)=1} a_n q^n$.

Therefore, we have a decomposition

$$\begin{aligned} M &= \operatorname{im} F \oplus K, \\ f &\mapsto \big(FUf,\ (1-FU)f\big). \end{aligned}$$

We record some generalizations of these properties of U and F.

Proposition 2.22. *For every integer $m \geq 1$:*

1. $U^m F^m = 1$
2. *The operator $F^m U^m$ is a projector onto $\operatorname{im} F^m$ and gives a decomposition*

$$\begin{aligned} M &\xrightarrow{\sim} \operatorname{im} F^m \oplus \ker U^m, \\ f &\mapsto \big(F^m U^m f,\ (1 - F^m U^m) f\big), \\ \sum_n a_n q^n &\mapsto \left(\sum_{p^m | n} a_n q^n,\ \sum_{p^m \nmid n} a_n q^n \right). \end{aligned}$$

3. *We have an exact sequence*

$$0 \to M \xrightarrow{F^m} M \xrightarrow{1 - F^m U^m} M \xrightarrow{U^m} M \to 0.$$

Proof. The case $m = 1$ is discussed above, and the general case is the same. The core of the exact sequence above is the usual sequence associated to a projector $P : V \to V$ acting on a linear space V:

$$0 \to \ker P \to V \to \operatorname{im}(1-P) \to 0.$$

In our case for $m = 1$, we have $V = M$ and $P = FU$, so that

$$\begin{array}{ccccccccc} 0 & \to & \ker FU & \to & M & \to & \operatorname{im}(1-FU) & \to & 0, \\ & & \| & & & & \| & & \\ & & \operatorname{im} F & & & & \ker U & & \end{array}$$

and we can splice in maps on both sides of the projector exact sequence. □

As m grows, $\operatorname{im} F^m$ gets smaller and $\ker U^m$ gets bigger, so that, in some sense, more of the "bulk" of M in the exact sequence moves to the right. Here's one attempt to make this observation precise.

Lemma 2.23. *For every nonzero $f \in M$, the image of f in $\ker U^m$ under the decomposition above is nonzero for all m sufficiently large.*

Proof. The image of f in $\ker U^m$ under the projection $1 - F^m U^m$ is given in terms of q-expansions in

Proposition 2.22 above:

$$(1 - F^m U^m) f = \sum_{p^m \nmid n} a_n(f) q^n.$$

Since f is nonzero, there is some n with $a_n(f) \neq 0$. Any $m > v_p(n)$ will work. □

2.6.2 The θ operator

The θ operator is a little miracle particular to modular forms modulo p.

Lemma 2.24 (Swinnerton-Dyer)**.** *The operator $\theta = q\frac{d}{dq}$ that takes a q-series $f = \sum_n a_n q^n$ to*

$$\theta f = \sum_n n a_n q^n$$

sends M_k to M_{k+p+1}. Moreover, $w(\theta f) = w(f) + p + 1$ unless p divides $w(f)$.

Recall that $w(f) = \min\{k : f \in M_k\}$ is the weight filtration of f.

Proof. [29, Lemma 5(ii)]. □

In particular $\theta(M^i) \subset M^{i+2}$, so that θ permutes the graded components of M.

Corollary 2.25. *For f graded in M, $w(\theta^{p-1} f) \leq w(f) + p^2 - 1$ with equality iff $w(f) \equiv 1 \bmod p$.*

Proof. By Lemma 2.24 above, $w(\theta^{p-1} f) \leq w(f) + p^2 - 1$, with equality if and only if for every n with $0 \leq n < p - 1$, we have $p \nmid w(\theta^n f)$. But the only way to ensure that that none of the $p - 1$ numbers in the arithmetic sequence

$$w(f),\ w(f) + p + 1,\ w(f) + 2(p + 1),\ \ldots,\ w(f) + (p - 2)(p + 1)$$

is divisible by p is to start with $w(f) \equiv 1 \bmod p$. □

Unlike T_n and U, the θ operator does not preserve M_k. However, it does satisfy the following easy-to-prove properties.

Lemma 2.26. *1.* $\operatorname{im} \theta = K$ *2.* $\theta^{p-1} = 1 - FU$ *3.* $\theta^{p-1}\big|_K = 1_K$

In fact, θ and T_ℓ commute up to a twist:

Lemma 2.27. $T_\ell \circ \theta = \ell\, \theta \circ T_\ell$.

Proof. It suffices to check this on $f \in M^k$, keeping in mind that $\theta f \in M^{k+2}$. On one hand,

$$\ell\, \theta\, T_\ell \sum_n a_n q^n = \ell\, \theta \sum_n \big(a_{\ell n} + \ell^{k-1}\, a_{n/\ell}\big) q^n = \sum_n \ell\, \big(n\, a_{\ell n} + \ell^{k-1}\, n\, a_{n/\ell}\big) q^n.$$

On the other hand,

$$T_\ell\, \theta \sum_n\, a_n q^n = T_\ell \sum_n n\, a_n q^n = \sum_n \big(\ell\, n\, a_{\ell n} + \ell^{k+2}\, (n/\ell)\, a_{n/\ell}\big) q^n.$$

□

Lemma 2.27 implies that, if $f \in M$ is an eigenform then so is θf! More precisely, if the eigensystem for f is $\{\lambda_\ell\}$, then the eigensystem for θf is $\{\ell \lambda_\ell\}$. On the Galois side, twisting by θ corresponds to twisting by ω,

the mod-p cyclotomic character. We continue this discussion in Section 2.8.

2.6.3 The U-nilpotent component of M

Let $M[U^n] := \ker U^n$ be the part of M killed by U^n and let

$$M[U^\infty] = \{f \in M : U^n f = 0 \text{ for some } n\} = \bigcup_{n\geq 1} M[U^n]$$

be the U-nilpotent part of M.

Lemma 2.28.

1. $M[U^n] = K \oplus F(K) \oplus F^2(K) \oplus \cdots \oplus F^{n-1}(K)$
2. $M[U^\infty] = \bigoplus_{n=0}^\infty F^n(K)$

Proof. It suffices to prove the first part. Certainly the right-hand side is contained in the left, and the sum is direct, since $F^n(K) = \{f \in M : U^{n+1} f = 0 \text{ but } U^n f \neq 0\} \cup \{0\}$.[‡] It remains to show the reverse containment. Proceed by induction. The case $n = 1$ is the definition of K. For $n > 1$, if $f \in \ker U^n$, use the projector $F^{n-1}U^{n-1}$ and its complement (see Proposition 2.22) to write f as a sum $f = F^{n-1}g + f_{n-1}$ with $f_{n-1} \in \ker U^{n-1}$. Finally, $0 = U^n f = U^n F^{n-1} g + U^n f_{n-1} = Ug$ shows that $g \in K$. □

How does $M[U^\infty]$ interact with M_τ? Jochnowitz proves that, for every τ, "most" of M_τ is contained in $M[U^\infty]$ — the complementary subspace only contains forms of low filtration. More precisely, since the operators in A commute with U, the generalized eigenspace M_τ is U-invariant and splits up further into (A, U)-eigencomponents. Jochnowitz proves that every generalized (A, U)-eigenspace that contains a form of high enough filtration is actually U-nilpotent.

First, a lemma:

Lemma 2.29. *$w(Uf) \leq \frac{w(f)-1}{p} + p$ with equality if and only if $w(f) \equiv 1 \bmod p$.*

We give the proof from [18, Lemma 1.9]:

Proof. From Lemma 2.26, $1 - FU = \theta^{p-1}$, so that $w(f - FUf) \leq w(f) + p^2 - 1$ with equality if and only if $w(f) \equiv 1 \bmod p$ (Lemma 2.25). Since $w(f) < w(f) + p^2 - 1$ but the two numbers are congruent modulo $p - 1$, we can conclude that

$$w(FUf) = w\big((Uf)^p\big) = p\, w(Uf) \leq w(f) + p^2 - 1,$$

with the same condition on equality. The claim follows. □

As a corollary, U lowers the filtration of every form of filtration greater than $p + 1$:

Corollary 2.30. *If $w(f) > p + 1$, then $w(Uf) < w(f)$.*

Proof. Immediate from Lemma 2.29. If $p + 1 < w(f)$, then $p^2 - 1 + w(f) < pw(f)$, so that

$$w(Uf) \leq \frac{w(f) - 1}{p} + p < w(f).$$

□

[‡]In the notation of Chapter 3, $F^n(K)$ is the set of forms f in M with $N_U(f) = n$, along with 0.

This is the main proposition:

Proposition 2.31 (Jochnowitz, [19, Lemma 3.2])**.** *If there is a form f in a generalized (A,U)-eigencomponent with $w(f) > p+1$, then this (A,U)-eigencomponent is contained in $M[U^\infty]$.*

Proof. Let M_{τ,λ_p} be this (A,U)-eigencomponent, with λ_p the U-eigenvalue, and suppose that λ_p is nonzero. Then U is bijective on $M_{w(f)} \cap M_{\tau,\lambda_p}$. Choose $g \in M_{w(f)} \cap M_{\tau,\lambda_p}$ with $Ug = f$. Since $M_{w(g)}$ is also U-invariant, we must have $w(g) = w(f) > p+1$. But Lemma 2.30 then forces $w(f) = w(Ug)$ to be strictly less than $w(g)$: a contradiction. □

Proposition 2.31 and Lemma 2.28 imply that to understanding the *full* Hecke algebra, which is topologically generated by all the T_n including $T_p = U$, it essentially suffices to understand the Hecke algebra on K; see subsection 2.7.3 below for a precise statement. But first, we prove that the Hecke algebra on K is isomorphic to A.

2.7 Duality between A and $\ker U$

We show that A is also the Hecke algebra on the kernel K of U, and establish a duality between A and K.

2.7.1 The Hecke algebra on K

We begin by restricting the spaces of modular forms to K. Namely, define

$$K_k := M_k \cap K, \qquad K_{\leq k} := M_{\leq k} \cap K, \qquad K^i := M^i \cap K, \qquad K_\tau := M_\tau \cap K.$$

Here k is an integer, $i \in 2\mathbb{Z}/(p-1)\mathbb{Z}$, and τ is a modular Galois pseudocharacter corresponding to a system of eigenvalues appearing in M. Because all the M-subspaces are U-invariant (U commutes with all the operators in A), we get the same kind of decompositions for K as we do for M. To wit,

$$K = \sum_k K_k = \sum_k K_{\leq k} = \bigoplus_i K^i = \bigoplus_\tau K_\tau \qquad \text{and} \qquad K^i = \bigcup_{k \equiv i} K_k.$$

All equivalence here and below are modulo $p-1$.

Proposition 2.32. *The Hecke algebra A acts faithfully on K.*

Proof. Let $T \neq 0$ be in A, and find $f \in M$ with $Tf \neq 0$. Let m be the least p-valuation of any n with $a_n(Tf)$ nonzero. Then $U^m Tf$ is not in $\operatorname{im} F$, so that its image in K under the projector $1 - FU$ is nonzero. In other words, the form $g = (1-FU)U^m f$ is both in K (because it's in the image of $1-FU$) and satisfies $Tg \neq 0$. □

Corollary 2.33. *The Hecke algebra components A^i and A_τ act faithfully on K^i and K_τ, respectively.*

Proof. The decomposition of A into a product of localizations $\prod_\tau A_{\mathfrak{m}_\tau}$ (Corollary 2.8) gives a decomposition of K as a direct sum of faithful A^i-modules $K = \bigoplus_i \widetilde{K}^i$: let $\widetilde{K}^i := e_i K$, where $e_i \in A$ is the idempotent corresponding to A_i; it follows that $A_j \widetilde{K}^i = 0$ if $i \neq j$. On the other hand, we have the decomposition $K = \bigoplus_i K^i$, and the action of A on K restricts to the action of A^i on each K^i. Since $A_j K^i = 0$ if $i \neq j$

again, we must have $\widetilde{K}^i \subset K^i$, so that the action of A^i on K^i is faithful. The proof for K_τ is the same $\square$

In particular, K contains an eigenvector for each system of eigenvalues appearing in M. See also section 2.8.

There doesn't appear to be any reason for A_k and $A_{\leq k}$ to act faithfully on K_k and $K_{\leq k}$: the tricks we use in Proposition 2.32 all rely on going to arbitrarily high weight. One has no choice but to soldier on: let B_k and $B_{\leq k}$ be Hecke algebras acting on K_k and $K_{\leq k}$, respectively, defined just as in section 2.2. Since $K_k \subset M_k$ and the Hecke algebras are generated by the same Hecke operators, we have a surjective map $A_k \twoheadrightarrow B_k$, and similarly $A_{\leq k} \twoheadrightarrow B_{\leq k}$, so that the "$B$" rings are just the faithful-on-their-part-of-K quotients of the "A" counterparts. Finally, let

$$B^i := \varprojlim_{k \equiv i} B_k \qquad \text{and} \qquad B := \varprojlim_{k} B_{\leq k}$$

be the Hecke algebras on K^i and K, respectively. They satisfy all the same wondrous properties of section 2.2 and Proposition 2.12, so that we can define B_τ, but fortunately we can forget about these stopgap Hecke algebras immediately:

Proposition 2.34. *There are natural (i.e., T_n maps to T_n) isomorphisms of topological rings*

$$1.\ A \xrightarrow{\sim} B \qquad 2.\ A^i \xrightarrow{\sim} B^i \qquad 3.\ A_\tau \xrightarrow{\sim} B_\tau.$$

Proof. The compatible surjections $A \twoheadrightarrow A_{\leq k} \twoheadrightarrow B_{\leq k}$ for each k piece together to give a continuous surjection $A \twoheadrightarrow B$. Since A acts faithfully on K (Proposition 2.32), this map is also injective. Use Corollary 2.33 for the rest. $\square$

2.7.2 Duality between A and K

Proposition 2.35. *The pairing of A-modules*

$$A \times K \to \mathbb{F}_p$$
$$\langle T, f \rangle \mapsto a_1(Tf)$$

is nondegenerate and continuous on both sides. It induces isomorphisms of A-modules

$$A \xrightarrow{\sim} K^\vee \qquad \text{and} \qquad K \xrightarrow{\sim} A^{\vee,\mathrm{cont}}.$$

Here we use the notation $M^\vee$ for an A-module M to denote the $\mathbb{F}_p$-linear dual $\mathrm{Hom}(M, \mathbb{F})$ viewed as an A-module, with A-action $a \cdot g = [m \mapsto g(am)]$, for $a \in A$, $m \in M$, and $g \in M^\vee$. Similarly $M^{\vee,\mathrm{cont}} = \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{F})$, the continuous linear dual, with the same A-module structure.

Proof. The pairing is nondegenerate on the right precisely because we've restricted to K; the analogous pairing $A \times M \to \mathbb{F}_p$ has a right kernel. It is nondegenerate on the left because A acts faithfully on K (Lemma 2.32 above).

More precisely, if $f \in K$ is nonzero, then there is some n prime to p with $a_n(f) \neq 0$. Since $a_n(f) = a_1(T_n f)$, we see that $\langle T_n, f \rangle \neq 0$. So the right kernel is trivial. On the other hand, if $T \in A$ is nonzero, find $f \in K$ with $Tf \neq 0$, and then find n prime to p with $a_n(Tf) \neq 0$. Then $\langle T, T_n f \rangle \neq 0$. So the kernel on the left is trivial.

Continuity on the right is trivial since K is discrete. On the left, recall that the topology on A has, as a basis of neighborhoods of 0, the annihilators of $M_{\leq k}$ (Proposition 2.4). Since every $f \in M$ is in some $M_{\leq f}$, the map $[T \mapsto \langle T, f\rangle]$ in $A^\vee$ factors through $A_{\leq k}$ and is therefore continuous.

We therefore get injective maps $K \hookrightarrow A^{\vee,\mathrm{cont}}$ and $A \hookrightarrow K^\vee$. These maps are A-module morphisms because the pairing is A-equivariant: $\langle T, T'f\rangle = \langle T'T, f\rangle$.

Finally, these maps are surjective because the pairing is a limit of finite perfect pairings, which automatically give isomorphisms to duals. That is, the pairing we defined descends, for each k, to a pairing $B_{\leq k} \times K_{\leq k} \to \mathbb{F}_p$. This pairing is nondegenerate on both sides for the same reason as the pairing $A \times K$, and hence perfect, inducing isomorphisms $B_{\leq k} \xrightarrow{\sim} K^\vee_{\leq k}$ and $K_{\leq k} \xrightarrow{\sim} B^\vee_{\leq k}$. From here, the isomorphism $A \xrightarrow{\sim} K^\vee$ is formal. The other one is even easier: a linear form in $A^\vee$ is continuous if and only if it factors through some $B_{\leq k}$, so that $A^{\vee,\mathrm{cont}} = \varinjlim_k B^\vee_{\leq k} = \varinjlim_k K_{\leq k} = K$. □

Corollary 2.36. *The pairing in Proposition 2.35 restricts to perfect pairings*

1. $A^i \times K^i \to \mathbb{F}_p$,
2. $A_\tau \times K_\tau \to \mathbb{F}$,
3. $A/\mathfrak{a} \times K[\mathfrak{a}] \to \mathbb{F}_p$ *for every open (i.e. cofinite) ideal* $\mathfrak{a} \subset A$.

Proof. The first two are clear. For the third, the key is that $A/\mathfrak{a}$ acts faithfully on $K[\mathfrak{a}]$. □

2.7.3 The full Hecke algebra

Given a modular pseudocharacter τ, let $M_\tau = \bigoplus_{a_p} M_{\tau,\alpha}$ be the decomposition of the A-eigencomponent M_τ into (A,U)-eigecomponents, with α the U-eigenvalue. Let $A^{\mathrm{full}}_{\tau,\alpha}$ be the corresponding local full Hecke algebra.

Corollary 2.37 (Jochnowitz)**.**

1. *If* $\alpha \neq 0$*, then* $M_{\tau,\alpha}$ *is finite-dimensional and consists of forms of filtration bounded by* $p+1$.
2. *Moreover,* $M_{\tau,0} = \bigoplus_{n\geq 0} F^n(K_\tau)$*, so that* $A^{\mathrm{full}}_{\tau,0} = A_\tau[\![U]\!]$.

Proof. Proposition 2.31 for the first part. For the second, Lemma 2.28 restricted to M_τ and the fact that U^n is the left inverse of F^n (Proposition 2.22 (1)). □

2.8 θ-twists of local components

We continue the study of the θ operator from section 2.6.2, beginning where we left off:

Lemma 2.38. *If* $f \in M^i$ *is a Hecke eigenform for corresponding to pseudocharacter* $\tau : G_{\mathbb{Q},p} \to \mathbb{F}$*, then* $\theta f \in M^{i+2}$ *is a Hecke eigenform for the Hecke corresponding to the pseudocharacter* $\omega\tau$.

Proof. Lemma 2.27 and the observations immediately following. □

The component change from f to θf is consistent with Lemma 2.24. Indeed, recall that $k(\tau)$ is determined by $\det\tau = \omega^{k(\tau)-1}$, and note that $\det(\omega\tau) = \omega^2 \det\tau$, so that $k(\omega\tau) = k(\tau)+2$.

Corollary 2.39. *Every eigensystem appearing in* M *is a twist of an eigensystem appearing in* M^0.

Proof. Let $\lambda = \{\lambda_\ell\}$ be an eigensystem appearing in M with (even) weight $k = k(\lambda)$. Then $\theta^{p-1-\frac{k}{2}}\lambda$ appears in M^0. □

Lemma 2.40. *K is θ-invariant, and $\theta|_K$ is an isomorphism (of vector spaces). Moreover, θ permutes the components K_τ of K.*

Proof. The inverse is given by θ^{p-2} (Lemma 2.26) and we already know that $\theta(K_\tau) \subset K_{\omega\tau}$. □

Proposition 2.41. *The isomorphism $K_\tau \xrightarrow{\theta}_{\sim} K_{\omega\tau}$ is Hecke equivariant, in the sense that there is an isomorphism of topological $\mathbb{F}$-algebras*

$$A_\tau \xrightarrow{\Theta}_{\sim} A_{\omega\tau} \quad \textit{defined by} \quad T_\ell \mapsto \ell T_\ell$$

that satisfies, for $T \in A_\tau$ and $f \in K_\tau$,

$$\theta(Tf) = \Theta(T)\theta(f).$$

Proof. The isomorphism $\theta : K_\tau \to K_{\omega\tau}$ induces an twisted action of $A_{\omega\tau}$ on K_τ via

$$T \cdot f := (\theta^{-1} \circ T \circ \theta)f.$$

Write $K_\tau(1)$ for K_τ as an $A_{\omega\tau}$-module with this new twisted action. By construction, θ is now an isomorphism of $A_{\omega\tau}$-modules $K_\tau(1) \xrightarrow[\sim]{} K_{\omega\tau}$: indeed $T(\theta f) = \theta\,(T \cdot f)$. In particular, if $T = T_\ell$, Lemma 2.27 tells us that $T_\ell \cdot f = \ell\, T_\ell f$ for every $f \in K_\tau(1)$.

We now compare the images of three maps

$$A_{\omega\tau} \to \operatorname{End} A_{\omega\tau}, \qquad A_{\omega\tau} \to \operatorname{End} K_\tau(1) = \operatorname{End} K_\tau, \qquad A_\tau \to \operatorname{End} K_\tau.$$

All three are topologically generated by the T_ℓ. The first and third are, by definition, $A_{\omega\tau}$ and A_τ, respectively. The first and second are isomorphic by construction of the $A_{\omega\tau}$-action on $K_\tau(1)$.

Now consider the second and third together. The second image uses the twist action, so that the image of T_ℓ is ℓ times what it is in the third. But when we identify $\operatorname{End} K_\tau(1)$ with $\operatorname{End} K_\tau$, we see that the action of T_ℓ spans the same $\mathbb{F}$-line. If T is in some $\mathbb{F}_p$-Hecke algebra A', then so is $\ell\, T$.

Therefore, the images of second and third maps are the same inside $\operatorname{End} K_\tau = \operatorname{End} K_\tau(1)$. In other words, A_τ and $A_{\omega\tau}$ are isomorphic via the map Θ that sends T_ℓ to $\ell\, T_\ell$.

The rest of the proposition follows immediately. □

The bottom line is that to understand the structure of every A_τ, it suffices to understand A^0, the 0-graded component of A with its action on K^0.

2.8.1 Sequences of generalized eigenforms

We close with results of Jochnowitz about filtrations of generalized eigenforms, slightly massaged for our purposes. These will allow us to separate the various eigencomponents of the Hecke algebra. First, a theorem for context, one that we will also use in applications. Jochnowitz credit it to Serre and Tate in level one.

Theorem 2.42 ([18, Theorem 4.1])**.** *Every system of (A, U)-eigenvalues appearing in M is a twist of a system appearing in M_k with $4 \le k \le p+1$.*

Note that Theorem 2.5 stated in section 2.3.1 is an immediate corollary. We state it again.

Corollary 2.43. *Every system of eigenvalues appearing in M appears in some M_k with $4 \leq k \leq p^2 - 1$.*

Proof. By Theorem 2.42, our system of eigenvalues is a twist of one appearing in weight k with $4 \leq k \leq p+1$. To find our twist, we apply θ no more than $p-2$ times, which raises the weight filtration by no more than $(p-2)(p+1)$. □

The upper bound is sharp if k is required to be strictly positive. For example, for $p = 5$, the eigensystem $1 + \omega^{-1}$ appears first in filtration 0 (carried by $E_4 = 1$) but then not again until filtration 24 (carried by $\theta^3 E_6$, the reduction of a characteristic-zero eigenform defined over $\mathbb{Q}(\sqrt{144169})$). The same is true for any $p \geq 5$: the system of eigenvalues $\tau = 1 + \omega^{-1}$ appears in weight 0 and then not again until weight $p^2 - 1$. Indeed, τ is a twist of $1 + \omega$, which is carried by E_{p+1}; Tate's theory of θ-cycles guarantees that no other form in weight up to $p+1$ is a twist of τ (see [18, Lemma 6.2(3)]). Therefore τ in positive weight is carried only by $\theta^{p-2} E_{p+1}$, which has weight $p^2 - 1$.

Following Jochnowitz, write W_k for the Hecke module of quotient forms of weight filtration exactly k: that is $W_k := M_k / M_{k-p+1}$; of course, we interpret $M_k = 0$ if $k < 0$.

Proposition 2.44 (Jochnowitz, [18, Lemma 6.4])**.**

1. *If $k \equiv 1 \bmod p$, then θ^{p-1} gives an isomorphsm $W_k \xrightarrow{\sim} W_{k+p^2-1}$*
2. *For any $k > p+1$, the Hecke modules W_k^{ss} and $W_{k+p^2-1}^{\mathrm{ss}}$ are isomorphic.*

The notation W^{ss} above denotes the the semisimplification of W as a Hecke module.

Sketch of proof. If $k \equiv 1 \bmod p$ then, by Lemma 2.25, W_k injects into W_{k+p^2-1}. Dimension formulas for M_k imply that this map is actually an isomorphism. The deails for the general case are in [17, XIII.2]. □

Here is the implication in the form that we need:

Corollary 2.45. *Let τ be a system of eigenvalues appearing in M^0. There exists a sequence $\{f_0, f_1, f_2, \dots, \}$ of forms in K_τ with $w(f_n)$ a linear function of n.*

Proof. We will produce such a sequence with $w(f_n) = p(p^2-1)n + kp^2$ for some positive constant k divisible by $p-1$. This k will be the filtration of a starting eigenform corresponding to τ.

First, I claim that we can find an eigenform g_0 of filtration $k > p+1$ carrying τ. Since τ appears in M^0, certainly there is some eigenform g corresponding to τ with $w(g)$ positive and divisible by $p-1$. If $w(g) \neq p-1$, then $w(g) > p+1$, so that $g_0 = g$ already works. Otherwise, let $g_0 = \theta^{p-1} g$. I claim that $w(g_0) = p^2 - p$.

Indeed, the theory of θ-cycles implies that $Ug \neq 0$: see [19, Corollary 7.7] for details. Therefore we must have $w(Ug) = 0$ or $w(Ug) = p-1$. But if $w(Ug) = 0$ then $\tau = 1 + \omega^{-1}$, which contradicts the assumption that $w(g) = p-1$ by the discussion following Corollary 2.43. Therefore $w(Ug) = p-1$, so that $w(FUg) = p\, w(Ug) = p^2 - p$, and therefore $w(\theta^{p-1} g) = w(g - FUg) = p^2 - p$. See also [19, Example 7.8].

Now that we have g_0 of weight $k > p+1$, we can use the second part of Proposition 2.44 to inductively find a sequence of generalized τ-eigenforms g_1, g_2, …, with g_m of filtration $k + m(p^2-1)$ for each $m \geq 0$. To find

a similar sequence in K_τ, we will twist by θ^{p-1}, first taking a subsequence to ensure control of the filtration.

To form the subsequence: let $h_n := g_{k-1+np}$ for every $n \geq 0$. By construction h_n is still in M_τ, but now the weight filtration is always 1 modulo p:

$$w(h_n) = w(g_{k-1+np}) = k + (k-1+np)(p^2-1) \equiv 1 \mod p.$$

Finally, the twist: $f_n := \theta^{p-1}(h_n)$ for every n. Certainly $f_n \in K_\tau$: it is in K because it's in the image of θ, and it is in M_τ because θ^{p-1} preserves eigencomponents. And since $w(h_n) \equiv 1 \bmod p$, we have, again by Lemma 2.25,

$$w(f_n) = w(h_n) + p^2 - 1 = kp^2 + np(p^2-1).$$

In other words, the sequence $\{f_n\}$ satisfies our requirements.[§] □

[§](October 2015) Thanks to Naomi Jochnowitz for finding a mistake in this argument in an earlier version of this document.

Chapter 3

The nilpotence method

In this section, we state and prove two theorems formalizing the nilpotence method.

We use the notation of Chapter 2. The key players are the algebra M of modular forms modulo p; the kernel of the U-operator $K \subset M$; the Hecke algebra A, which is in duality with K and splits into a product of local noetherian algebras $(A_\tau, \mathfrak{m}_\tau)$ corresponding to modular Galois pseudocharacters τ defined over a finite extension $\mathbb{F}$ of $\mathbb{F}_p$. Finally, M_τ and $K_\tau = K \cap M_\tau$ are the corresponding pieces of M and K. Note that restricting to the weight-0-graded spaces M^0, K^0, and A^0 (section 2.1.1 and *ff.*) does not change this setup.

3.1 The nilpotence index

Any form $f \in M_\tau$ is a generalized eigenform for the action of every $T \in A_\tau$. If $T \in \mathfrak{m}_\tau$, then the corresponding eigenvalue is 0 (Proposition 2.7). Therefore every $T \in \mathfrak{m}_\tau$ acts *locally nilpotently* on M_τ: for any form $f \in M_\tau$, there is an integer k with $T^k(f) = 0$.

Definition. If T is a locally nilpotent operator on any linear space V, we define the *nilpotence index* of any nonzero $f \in V$ *with respect to* T as the integer

$$N_T(f) := \min\{k : T^{k+1} f = 0\} = \max\{k : T^k f \neq 0\}.$$

Also set the nilpotence index of $0 \in V$ to be $N_T(0) := -\infty$.

If V is a polynomial ring, then an operator on V is locally nilpotent if and only if it lowers degrees; in this case, clearly $N_T(f) \leq \deg f$ for all $f \in V$. On the other hand, if V is the space of modular forms modulo p and T is a Hecke operator in A, then T is locally nilpotent on M if and only if T is in every maximal ideal of A. For $p = 2, 3, 5, 7, 13$, we know that $M^0 = \mathbb{F}_p[\Delta]$ (see Chapter 8), so we can put these observations together.

Lemma 3.1. *Let $p = 2, 3, 5, 7$ or 13. If T is in A^0, then the following are equivalent.*

1. *T acts locally nilpotently on M^0.*
2. *T lowers Δ-degrees.*

3. *T is in every maximal ideal of A^0.*

And a version for general primes:

Lemma 3.2. *There exists an integer $d \geq 1$ so that the following are equivalent for $T \in A^0$.*

1. *T acts locally nilpotently on M^0.*
2. *T^d lowers weight filtration on M^0.*
3. *T is in every maximal ideal of A^0.*

Proof. We show why the other parts imply (2); the rest is clear. Quite generally, if a filtration-preserving operator on a filtered module is locally nilpotent, then corresponding graded operator is also locally nilpotent on the associated graded module. In our case, assuming that T is locally nilpotent on M^0, we know that $\operatorname{gr} T$ is locally nilpotent on

$$\operatorname{gr} M^0 = \bigoplus_{k \equiv 0 \bmod p-1} W_k.$$

Here $W_k = M_k/M_{k-p+1}$ as discussed in section 2.8. Moreover, since $\dim W_k$ stays bounded as k grows (Proposition 2.44, or the dimension formulas used in its proof), in fact $\operatorname{gr} T$ is just plain nilpotent on $\operatorname{gr} M^0$: that is $(\operatorname{gr} T)^d = 0$ for $d = \max_k \dim W_k$. In other words, T^d lowers filtration. □

3.2 The Hilbert-Samuel trick

We now state and prove two theorems that will allow us to get lower bounds on dimensions of some local Hecke algebras. They are both generalizations of a suggestion of Bellaïche outlined in [5, appendix].

Theorem 3.3 (Basic Hilbert-Samuel trick)**.** *Suppose that there exists finitely many operators $T_1, \ldots, T_m$ in A and a form $f \in M$ so that both of the following conditions are satisfied.*

- *$(T_1, \ldots, T_m)A_\tau = \mathfrak{m}_\tau A_\tau$ for every τ*
- *There exists an $\alpha < 1$ so that $N_{T_i}(f^n) \ll n^\alpha$ for every i.*

Then at least one of the local components A_τ has Krull $\dim A_\tau \geq 2$.

The first condition simply requires the operators $T_1, \ldots T_m$ to generate the maximal ideal $\mathfrak{m}_\tau$ of each local component. The second is a condition on the growth of the nilpotence index $N_{T_i}(f^n)$ as a *function in n*. Note that, since we've assumed that the T_i generate each $\mathfrak{m}_\tau$, each T_i must be in every $\mathfrak{m}_\tau$, so that T_i is locally nilpotent on M and $N_{T_i}(f^n)$ is defined.

In practice we will be applying the theorem not to A and K but to A^0 and K^0; as noted already, this changes nothing. Here is how the basic application looks: if all the τ are reducible and unobstructed ($p = 2, 3, 5, 7$), then we can use the results of Chapter 7 to find just two Hecke operators in A to generate every maximal ideal at once. The Nilpotence Growth Theorem (Theorem A from Chapter 1) combined with results from Chapter 6 will then yield an α_i for each T_i; set $\alpha := \max \alpha_i$.

Before proving Theorem 3.3, we state and prove a simple lemma.

Lemma 3.4. *If f is in K, then for every $m \geq 1$, the form f^{pm+1} is in K as well.*

The proof uses the notation of section 2.6.1; in particular F is the p^{th}-power map.

Proof. Consider q-expansions: $a_n(f^{pm+1}) = \sum_{i+j=n} a_i(F^m f)a_j(f)$. If p divides n, then either both i and j are divisible by p, in which case $a_j(f) = 0$ since $f \in K$, or else neither i nor j is divisible by p, in which case $a_i(F^m f) = 0$ since $F^m f \in \operatorname{im} F$. Either way $a_n(f^{pm+1}) = 0$ whenever $p \mid n$, so that $f^{pm+1} \in K$. □

Proof of Theorem 3.3. Suppose that we have $T_1, \ldots, T_m$ satisfying the first condition, and then f satisfying the second. Let $J := (T_1, \ldots, T_m)$, an ideal of A. The first condition says that $JA_\tau = \mathfrak{m}_\tau$ for every τ.

For any $g \in M$, define the function $N(g) = \sum_i N_{T_i}(g)$. The second condition implies that $N(f^n)$ grows no faster than n^α does.

Claim. For any g in M, if $N(g) < k$, then $J^k g = 0$.

Proof. Indeed, if $N(g) < k$, then every monomial generator $T_1^{n_1} \cdots T_m^{n_m}$ of J^k, satisfies

$$\sum_i n_i = k > N(g) = \sum_i N_{T_i}(g),$$

so that there exists at least one i with $n_i > N_{T_i}(g)$, which implies that $T_1^{n_1} \cdots T_m^{n_m} g = 0$. □

We are ready for the key manoeuvre. Recall that, for a noetherian local ring $(B, \mathfrak{m})$, the Hilbert-Samuel function $k \mapsto \dim_{B/\mathfrak{m}} B/\mathfrak{m}^k$ is, for $k \gg 0$, a polynomial in k of degree equal to the Krull dimension of B (see, for example, [1, Chapter 11]). Consider a generalized Hilbert-Samuel function

$$k \mapsto \sum_\tau \dim_{\mathbb{F}} A_\tau/\mathfrak{m}_\tau^k.$$

By duality, $\dim_{\mathbb{F}} A_\tau/\mathfrak{m}_\tau^k = \dim_{\mathbb{F}} K_\tau[\mathfrak{m}_\tau^k]$ (Corollary 2.36), so that our function becomes

$$\begin{aligned} k \mapsto \sum_\tau \dim_{\mathbb{F}} A_\tau/\mathfrak{m}_\tau^k = \sum_\tau \dim_{\mathbb{F}} K_\tau[\mathfrak{m}_\tau^k] = \sum_\tau \dim_{\mathbb{F}} K_\tau[J^k] \\ = \dim_{\mathbb{F}} \bigoplus_\tau K_\tau[J^k] = \dim_{\mathbb{F}} K[J^k]. \end{aligned}$$

Here we've used the fact that, on K_τ, the ideals $\mathfrak{m}_\tau^k$ and J^k coincide and the fact that the various eigenspaces K_τ are in direct sum.

By Lemma 3.4 and the claim above, $K[J^k]$ certainly contains every f^{pn+1} with $N(f^{pn+1}) < k$, and these are all linearly independent because they have distinct filtrations (Lemma 2.3). Therefore,

$$\dim_{\mathbb{F}} K[J^k] \quad \geq \quad \#\{n : N(f^{pn+1}) < k\} \quad \gg \quad k^{\frac{1}{\alpha}}. \tag{A}$$

Here the last inequality is because $N(f^{pn+1}) \ll (pn+1)^\alpha \asymp n^\alpha$.

Since $\frac{1}{\alpha} > 1$, we have shown that the Hilbert-Samuel function $k \mapsto \dim_{\mathbb{F}} A_\tau/\mathfrak{m}_\tau^k$ grows *faster than linearly* in k, so that at least one A_τ has dimension at least 2. □

Sublinearity vs. $O(n^\alpha)$

In fact, this Hilbert-Samuel trick requires only that each $N_{T_i}(f^n)$ grow slower than linearly in n.

We recall the definitions: a function $g : \mathbb{N} \to \mathbb{R}^+$ grows *slower than linearly* or *sublinearly* if $g(n)$ is $o(n)$: that is, $\frac{g(n)}{n} \to 0$ as $n \to \infty$. The condition that g is $O(n^\alpha)$ (equivalently, $g \ll n^\alpha$) for some $\alpha < 1$ is strictly

stronger: g is $O(n^\alpha)$ if there exists a constant C so that $g(n) \leq Cn^\alpha$ for n large enough. For example, $f(n) = \frac{n}{\log(n)}$ is $o(n)$ but not $O(n^\alpha)$ for any $\alpha < 1$.

The Hilbert-Samuel trick still works if $N(f^n)$ is merely $o(n)$: in that case the quantity $\#\{n : N(f^n) < k\}$ still grows faster than linearly, or *supralinearly*, in k, and the conclusion that at least one A_τ has dimension at least 2 still stands. In practice (at least for now) all the sublinear functions come from finitely many applications of the Nilpotence Growth Theorem (Theorem 5.1), which yield $O(n^\alpha)$. So that is how Theorem 3.3 is stated.

3.2.1 The refined Hilbert-Samuel trick

We also give a component-separating refinement of Theorem 3.3.

Theorem 3.5. *Let A_τ be a local component of the mod-p Hecke algebra. Suppose that there exist finitely many operators $T_1, T_2, \ldots, T_m$ in A_τ that generate $\mathfrak{m}_\tau$, and a sequence of linearly independent forms $f_1, f_2, f_3, \ldots \in K_\tau$ so that for all i, $N_{T_i}(f_n) \ll n^\alpha$ for some fixed $\alpha < 1$. Then $\dim A_\tau \geq 2$.*

Proof. The proof is essentially the same as for Theorem 3.3. For $g \in M_\tau$, let $N(g) = \sum_i N_{T_i}(g)$. Then the Hilbert-Samuel function for A_τ is

$$k \mapsto \dim_{\mathbb{F}} A_\tau/\mathfrak{m}_\tau^k = K[\mathfrak{m}_\tau^k] \geq \#\{n : N(f_n) < k\} \gg k^{\frac{1}{\alpha}},$$

which grows supralinearly in k. Therefore, $\dim A_\tau \geq 2$. □

The basic way that this theorem will be applied is that the sequence $f_1, f_2, f_3, \ldots$ will have $w(f_n)$ depending linearly on n, and then the Nilpotence Growth Theorem will guarantee $N_T(f) \ll w(f)^\alpha$.

Corollary 3.6. *Fix A_τ, a local component of the Hecke algebra. Suppose that there exist Hecke operators $T_1, \ldots, T_m$ in A and a sequence of forms $f_1, f_2, f_3, \ldots$ in K_τ so that the following conditions are satisfied.*

1. *$T_1, \ldots, T_m$ are in every maximal ideal of A and generate $\mathfrak{m}_\tau$.*
2. *There exists an $\alpha < 1$ so that for every i and every $g \in M$, we have $N_{T_i}(g) \ll w(g)^\alpha$.*
3. *The filtration $w(f_n)$ depends linearly on n.*

Then $\dim A_\tau \geq 2$.

3.3 Plan of action

Theorem 3.3 guides our way forward. In the next two chapters, we step out of the world of modular forms to develop a purely algebraic theory of recursion operators (Chapter 4) and prove an abstract Nilpotence Growth Theorem (Chapter 5) in characteristic p. Then we return to modular forms and establish that the theory of recursion operators applies to Hecke operators acting on spaces of modular forms (Chapter 6). We find explicit Hecke generators for maximal ideals of reducible components in Chapter 7. Finally we put it all together in Chapter 8.

Chapter 4

Recursion operators

We develop a theory of *recursion operators*: linear operators T on an algebra B so that for any $f \in B$ the sequence $\{T(f^n)\}_n$ satisfies a linear recursion over B. This chapter provides a formal language for the key technical result of this document: the Nilpotence Growth Theorem (Theorem 5.1), which is a statement about the annihilating behavior of certain kinds of locally nilpotent recursion operators on polynomial algebras. Eventually, we will establish that Hecke operators are recursion operators of this certain kind.

This chapter is still a work in progress. Note that we do not fix a prime p.

4.1 Recurrence sequences

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ be the set of nonnegative integers.

Let B be a ring. We will assume that B is an integral domain, although this assumption is not necessary for the basic definitions. The space $B^{\mathbb{N}}$ is the set of infinite sequences in B. An element $s \in B^{\mathbb{N}}$ will be written as $s = (s_0, s_1, s_2, \ldots)$. The zero sequence in $B^{\mathbb{N}}$ is denoted $\mathbf{0}$.

Let $E : B^{\mathbb{N}} \to B^{\mathbb{N}}$ be the shift-left operator, so that

$$E\, s = E(s_0, s_1, s_2, \ldots) = (s_1, s_2, s_3, \ldots).$$

We can view $B^{\mathbb{N}}$ as a module over the polynomial algebra $B[X]$ by letting X act as E.

4.1.1 Linear recurrence relations and companion polynomials

Let $B' \supset B$ be any ring containing B. A sequence $s \in B'^{\mathbb{N}}$ satisfies a *linear recurrence relation of order d over B* if there exist $a_0, a_1, \ldots, a_{d-1} \in B$ so that for every $n \geq d$,

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + \cdots + a_d s_{n-d}. \tag{A}$$

Note that we do not assume that $a_d \neq 0$. The words *recursion* and *recurrence* will be used as synonyms for *recurrence relation*, as in speech.

A sequence s satisfies the recurrence (A) if and only if

$$P(E)s = \mathbf{0},$$

where $P(X)$ is the polynomial

$$P(X) = X^d - a_1X^{d-1} - a_2X^{d-2} - \cdots - a_d \quad \in B[X],$$

called the *companion polynomial* (or *characteristic polynomial*) of the recurrence relation (A).

A recurrence relation is entirely determined by its companion polynomial. If $P \in B[X]$ is a monic polynomial, we will speak of the *recurrence relation defined by* P or simply the *recursion* P. The order of the recurrence relation defined by a monic polynomial P is its degree.

Solutions to linear recurrences

If a sequence in $B'^{\mathbb{N}}$ satisfies the recursion defined by a polynomial P, it is also called a *solution* to the recursion P. A root of the companion polynomial always gives a solution to the recursion:

Proposition 4.1. *Let $P \in B[X]$ be monic and α a root of P in some extension B' of B. Then the sequence $\{\alpha^n\}_n = \{1, \alpha, \alpha^2, \ldots\}$ in $B'^{\mathbb{N}}$ is a solution to the recursion defined by P.*

Note that even $\alpha = 0$ gives a nonzero solution sequence.

Proof. Since $E\{\alpha^n\} = \alpha\{\alpha^n\}$, we have $(E - \alpha)\{\alpha^n\} = 0$. It is now clear that if $(X - \alpha)$ divides $P(X)$, then $P(E)\{\alpha^n\} = 0$. □

If B is a field or a domain, then the converse of Proposition 4.1 is also true; see Proposition 4.7 on page 40 below.

4.1.2 Solutions to linear recurrences over a field

In this section, we will assume that $B = K$ is a field, $\overline{K}$ is its algebraic closure, and K'/K an arbitrary extension. We explore the space of solutions to a given recursion P over K of order d.

Lemma 4.2. *The space of all solutions in $K'^{\mathbb{N}}$ to a recurrence relation of order d is a d-dimensional vector space in $K'^{\mathbb{N}}$.*

Proof. Satisfying a recurrence relation is a linear condition, and every solution to a recurrence of order d is determined by its first d terms, which may be chosen arbitrarily. □

All solutions, separable case

A recursion defined by $P(X) \in K[X]$ will be called *separable* if P is separable as a polynomial: that is, its roots in $\overline{K}$ are all distinct.

Corollary 4.3 (of Proposition 4.1)**.** *If P is separable with roots $\alpha_1, \ldots, \alpha_d \in \overline{K}$, then every $\overline{K}$-solution to the recursion defined by P is a $\overline{K}$-linear combination of the d solutions*

$$\{\alpha_1^n\}_n,\ \{\alpha_2^n\}_n,\ \ldots,\ \{\alpha_d^n\}_n.$$

Proof. Proposition 4.1 says that these sequences are all solutions; Vandermonde determinant says that they

are all linearly independent; and Lemma 4.2 seals the deal. □

As an immediate corollary of Corollary 4.3, we record for future use:

Corollary 4.4. *If $\alpha_1, \cdots, \alpha_d, c_1, \ldots, c_d$ are elements of $\overline{K}$, then the sequence s with*

$$s_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_d\alpha_d^n$$

satisfies the recursion defined by $P(X) = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_d) \in \overline{K}[X]$.

The constants $c_1, \ldots, c_d$ in $\overline{K}$ are the *weights* of the recurrence sequence s.

All solutions, general case

If P is not separable, there is still a general form, but it is more complicated. The following proposition holds in any characteristic:

Proposition 4.5. *Suppose that $P \in K[X]$ factors as*

$$P(X) = (X-\alpha_1)^{e_1}\cdots(X-\alpha_r)^{e_r}$$

with $\alpha_1, \ldots, \alpha_r \in \overline{K}$ distinct. Then every solution to the recursion P in $\overline{K}^{\mathbb{N}}$ is a linear combination of the $e_1 + \cdots + e_r$ solutions

$$\left\{ \binom{n}{j} \alpha_i^{n-j} \right\}_n, \quad \text{with } 1 \le i \le r \text{ and } 0 \le j < e_i.$$

Here $\binom{n}{j}$ is the integer-valued binomial coefficient function

$$n \;\mapsto\; \frac{n(n-1)(n-2)\cdots(n-j+1)}{j!},$$

and we insist that $\binom{n}{j}\alpha^{n-j} = 0$ if $n < j$ for all values of α. A proof of Proposition 4.5 is given in Appendix B.

If $\operatorname{char} K$ is 0 or bigger than j, then then the span of

$$\binom{n}{0} = 1,\ \binom{n}{1} = n,\ \binom{n}{2} = \frac{n^2-n}{2},\ \ldots,\ \binom{n}{j} = \frac{n(n-1)(n-2)\cdots(n-j+1)}{j!}$$

is the same as the span of $1,\ n,\ n^2,\ \ldots,\ n^j$; and if α_i is nonzero then the span of $\{\alpha_i^{n-j}\}_n$ is the same as the span of $\{\alpha_i^n\}_n$. In other words, the general solution to the recursion defined by P can be rewritten in the following more familiar way:

Corollary 4.6. *In the notation of Proposition 4.5, if $\operatorname{char} K = 0$ or if $\operatorname{char} K \ge \max_i e_i$, and if $\alpha_i \neq 0$ for all i, then every solution $s \in \overline{K}^{\mathbb{N}}$ to the recursion defined by P has the form*

$$s_n = g_1(n)\alpha_1^n + g_2(n)\alpha_2^n + \cdots + g_r(n)\alpha_r^n,$$

where g_i is a polynomial in n of degree less than e_i.

The problem in characteristic p is that the set of functions represented by polynomials of degree $\le p$ is only p-dimensional: because the polynomial functions n and n^p coincide and we're "missing" the function $\frac{n^p-n}{p}$. The basis of binomial coefficient functions $1, n, \binom{n}{2}, \binom{n}{3} \ldots \binom{n}{p}$ fixes this problem and gives a $(p+1)$-dimensional space of integer-valued polynomial functions.

4.1.3 Recurrence sequences over a field

Recall that K is a field, and K' an arbitrary extension. A sequence s in $K'^{\mathbb{N}}$ is a *K-recurrence sequence*, or simply *recurrence sequence*, if it satisfies a linear recurrence over K. The *order* of a recurrence sequence s is the minimum order of any recurrence that it satisfies.

Minimal polynomial

Proposition 4.7. *Let $s \in K^{\mathbb{N}}$ be a recurrence sequence of order d, satisfying a recursion of order defined by $P \in K[X]$. Let $Q \in K[X]$ be any monic polynomial. Then s is a solution to the linear recurrence defined by Q if and only if P divides Q.*

Proof. Recall that s satisfies recursion P if and only if $P(E)s = \mathbf{0}$, where E is the shift-left operator defined on the first page of this chapter. If s satisfies P, then it will satisfy any polynomial that divides P. And if s satisfies both P and Q, then it will satisfy any $K[X]$-linear combination of P and Q, including their (monic) greatest common divisor. But we've assumed that s has order equal to the degree of P. Therefore s satisfies Q if and only if P divides Q. □

Proposition 4.7 shows that the *minimal polynomial* P_s of any recurrence sequence s is well-defined: it is the recursion polynomial of least degree satisfied by s. Equivalently, it is the (monic) generator of the ideal $\mathrm{ann}(s)$ inside $K[X]$ when X acts on K^N through E.

Proposition 4.8. *The following are equivalent, for a sequence $s \in K^{\mathbb{N}}$:*

1. *s is a recurrence sequence.*
2. *The map $K[X] \to K^{\mathbb{N}}$ given by $P \mapsto P(E)s$ is not injective.*
3. *The image $K[E]s \subset K^{\mathbb{N}}$ is finite-dimensional.*

The proof is clear.

The space of all recurrence sequences

Let $S \subset K^{\mathbb{N}}$ be the space of all recurrence sequences, and $S^{\mathrm{sep}} \subset S$ the subspace of *separable recurrence sequences*: sequences s satisfying a separable recursion.

Proposition 4.9.

1. *S is a subalgebra of $K^{\mathbb{N}}$.*
2. *S^{sep} is a subalgebra of S.*

Proof. We want to show that S is closed under addition and multiplication. If s and t are two recursion sequences, then $P_s P_t$ will annihilate $s + t$. For multiplication, we use the general form of solutions to recurrences from Proposition 4.5. Over $\mathbb{Z}$, the binomial coefficient functions $\binom{n}{k}$ are a basis for the space of all integer-valued polynomial functions (Theorem B.2), so that products of binomial coefficient functions are expressible as linear combinations of binomial coefficient functions. The analogous claim over any ring follows. In particular, if $P_s = \prod_i (X - \alpha_i)^{e_i}$ and $P_t = \prod_j (X - \beta_j)^{f_j}$, then the componentwise product sequence $s \cdot t$ will satisfy the recursion defined by

$$\prod_{i,j} (X - \alpha_i \beta_j)^{e_i + f_j - 1}.$$

Finally, if s and t are separable recurrence sequences, then no binomial coefficient functions appear in the their sum or product, so that $s+t$ and st will be separable as well. □

4.2 Recursion operators on polynomial rings

Let k be a field, and $B = k[y]$ the polynomial algebra over y. A *parameter* on B is any $y' \in B$ so that $B = k[y]$: that is, y' is a parameter if $y' = ay + b$ with a nonzero.

We will be considering recurrence sequences over $k[y]$. Whenever we need a field, we embed into $K = k(y)$ or into $\overline{k(y)}$.

4.2.1 Recurrence sequences over $k[y]$

We begin with a general lemma about recurrence sequences over $k[y]$, which already illustrates how the theory of recursion over $k[y]$ is different from the general case.

Lemma 4.10. *Let $\{s_n\} \in k[y]^{\mathbb{N}}$ be a recurrence sequence satisfying recursion polynomial $P(y, X) \in k[y][X]$. If α is an element of some extension L of $k(y)$, then $\{s_n(\alpha)\}_n \in L^{\mathbb{N}}$ is a recurrence sequence satisfying the recursion defined by $P(\alpha, X) \in L[X]$.*

Proof. For a sequence $s \in B^{\mathbb{N}}$ to satisfy a recurrence relation defined by a polynomial $P \in B[X]$ is a completely algebraic property: we must have $P(E)\, s = \mathbf{0} \in B^{\mathbb{N}}$. In particular, this property is preserved under base change: if $\phi : B \to B'$ is any map of algebras, then $\phi(s) := \{\phi(s_n)\} \in B'\mathbb{N}$ satisfies the recursion defined by the polynomial $\phi(P) := \phi[X](P)$, where $\phi[X] : B[X] \to B'[X]$ is the map induced by ϕ.

Apply this principle to the map $k[y] \to L$ defined by $y \mapsto \alpha$. Since the sequence $\{s_n(y)\} \in k[y]^{\mathbb{N}}$ satisfies the recurrence relation $P(y, X)$ defined over $k[y]$, the sequence $\{s_n(\alpha)\} \in L^{\mathbb{N}}$ satisfies the recurrence relation $P(\alpha, X)$ defined over K. □

If $\{s_n\}$ is separable, then I expect that $\{s_n(\alpha)\}$ will be separable as well, but I do not have a full proof of this fact. However, we will make use of a special case, which requires the following definition.

Definition. Let L be any field extension of K. A K-recurrence sequence $s \in L^{\mathbb{N}}$ has *weights in k* if

$$s_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_d\alpha_d^n \tag{B}$$

for some $\alpha_i \in \overline{K}$ and $c_i \in k$.

In particular, s is automatically separable. Since s is separable, we know a priori s_n has the form (B) for $c_i \in \overline{K}$ (Corollary 4.4); the condition of weights in k restricts the c_i. Recurrence sequences with weights in k are closed under addition and multiplication: the arguments of Proposition 4.9 are easily adapted.

Lemma 4.11 (*cf.* Lemma 4.10)**.** *If $s = \{s_n(y)\} \in k[y]^{\mathbb{N}}$ is a recurrence sequence with weights in k, then so is $s(\alpha) = \{s_n(\alpha)\}_n$ for any α in any extension L of $k(y)$.*

Proof. From Lemma 4.10 we already know that $s(\alpha)$ is a recurrence sequence. By linearity, we can reduce to the case where t has equal weights 1. (Factor its recursion polynomial into irreducibles over $k[y]$; a recurrence sequence whose recursion polynomial is irreducible over $k[y]$ has weights that are Galois conjugates, equal if

in k.) Let $P = P(y, X)$ be the companion polynomial of the recursion satisfied by s, and $\beta_1, \ldots, \beta_d$ be its roots. The X^{d-i} coefficient of P is, up to sign, $a_i = e_i(\beta_1, \ldots, \beta_d)$, the i^{th} elementary symmetric polynomial. By assumption, $s_n = p_n(\beta_1, \ldots, \beta_d)$, the n^{th} power sum polynomial. Newton's identities express p_n as a polynomial in the $e_1, \ldots, e_n$ with coefficients in $\mathbb{Z}$; to fix ideas, let $p_n = \Phi_n(e_1, \ldots, e_n)$. In particular, since $e_n(\beta_1, \ldots, \beta_d) = 0$ for $n > d$, we know that $s_n = \Phi_n(a_1, \ldots, a_d)$: this is a polynomial relationship between elements of $k[y]$.

Passing to the sequence $s(\alpha)$ via the map $y \mapsto \alpha$ doesn't change this polynomial relationship: that is, $s_n(\alpha) = \Phi_n\big(a_1(\alpha), \ldots, a_d(\alpha)\big)$. This means that $s_n(\alpha)$ is the n^{th} power sum function of the roots of $P(\alpha, X)$: in other words, $s(\alpha)$ is separable sequence with weights in k. (Note that $P(\alpha, X)$ need not any longer have distinct roots, so we cannot conclude that $s(\alpha)$ has equal weights: the most we can say is that the weights of $s(\alpha)$ are sums of the weights of s.) □

4.2.2 Introducing recursion operators

Definition. A *recursion operator* $T : k[y] \to k[y]$ is a k-linear operator so that the sequence $\{T(y^n)\}_n$ of elements of $k[y]$ is a recurrence sequence over $k[y]$.

We endow T with all of the properties of the recurrence sequence $\{T(y^n)\}$: its minimal polynomial P_T is the *minimal polynomial* of T; its order is also the *order* of T; if it is separable, then T is *separable* as well; if it is separable with weights in k, the so is T.

Example. The identity operator $\mathbf{1}$ is a separable recursion operator of order 1, since $\{\mathbf{1}(y^n)\} = \{y^n\}$ satisfies the recursion defined by the polynomial $X - y$ in $k[y][X]$.

Example. The basic degree-lowering operator T defined by $\{T(y^n)\}_{n\geq 0} = \{0, 1, y, y^2, y^3, \ldots\}$ is a separable recursion operator of order 2. The n^{th} term of the defining sequence is $\frac{y^n - 0^n}{y}$, and the minimal polynomial is $X(X - y)$.

For many more interesting examples, see section 6.2.

We will show that many important properties of $P_{T,y}$ depend only on T and not on the parameter y, and eventually drop the y from notation.

Intrinsic definition

The definition of a recursion operator is less arbitrary, and less dependent on the parameter y, than it appears at first glance:

Proposition 4.12. *A linear operator $T : k[y] \to k[y]$ is a (separable) recursion operator (with weights in k) if and only, for* every *$f \in k[y]$, the sequence $\{T(f^n)\}_n$ is a (separable) recurrence sequence over $k[y]$ (with weights in k).*

Proof. One direction is clear. For the other, we take a recursion operator T and an $f \in B$, and seek to prove that $\{T(f^n)\}$ is a recurrence sequence.

Separable case: First suppose that T is separable, so that $T(y^n) = \sum_{i=0}^{d} c_i \alpha_i^n$ for some $c_i, \alpha_i \in \overline{K}$

(Proposition 4.3). For any $g(y) = \sum_k b_k y^k \in k[y]$,

$$T\big(g(y)\big) = \sum_k b_k T(y^j) = \sum_{i,k} b_k\, c_i\, \alpha_i^k = \sum_{i=0}^{d} c_i g(\alpha_i).$$

Therefore, with $g = f^n$, we have

$$T(f^n) = \sum_i c_i f(\alpha_i)^n,$$

so that $\{T(f^n)\}_n$ is visibly a separable recurrence sequence whose weights are sums of the weights of $\{T(y^n)\}_n$; it satisfies the recursion defined by

$$\big(X - f(\alpha_1)\big)(X - f(\alpha_2)\big) \cdots \big(X - f(\alpha_d)\big).$$

General case (sketch): We use notation from Appendix B. From Proposition B.5,

$$T(y^n) = \sum_{i,j} c_{i,j} \binom{n}{j} \alpha_i^{n-j}$$

for some α_i and $c_{i,j} \in \overline{K}$. With $g(y) = \sum_k b_k y^k$ a general element of B as above, and d_m the differential-like operator defined on page 101, we have for every m,

$$d_m g(y) = \sum_k b_k \binom{k}{m} y^{k-m},$$

which means that

$$T\big(g(y)\big) = \sum_{i,j,k} b_k\, c_{i,j} \binom{k}{j} \alpha_i^{k-j} = \sum_{i,j,k} b_k\, c_{i,j} \binom{k}{j} \alpha_i^{k-j} = \sum_{i,j} c_{i,j}\, d_j g(\alpha_i).$$

Therefore, with $g = f^n$,

$$T\big(f^n\big) = \sum_{i,j} c_{i,j}\, (d_j f^n)(\alpha_i).$$

Now we can use an analog of Faà di Bruno's formulas for $\frac{d^j}{dy^j} f^n$ to express $d_j f^n$ as a B-linear combination of $f^{n-1}, \ldots f^{n-j}$ with coefficients equal to products of binomial coefficient functions and powers of various $d_\ell f$ for $\ell \le j$. Since products of binomial coefficient functions are themselves $\mathbb{Z}$-linear combinations of binomial coefficient functions (Theorem B.2), the final expression can again be recognized as a recurrence sequence.

□

Minimal polynomials of recursion operators

For a recursion operator T, we let $P_{T,f}$ be the minimal polynomial of the recurrence sequence $\{T(f^n)\}_n$. This is a polynomial in $k[y][X]$; for any such $P \in k[y][X]$, we will attempt to keep track of the variables by writing $P(y, X)$, if necessary. The proof of Proposition 4.12 shows that, for a separable* operator T and for any $f \in k[y]$, the sequence $\{T(f^n)\}$ satisfies

$$Q = \big(X - f(\alpha_1)\big)\big(X - f(\alpha_2)\big) \cdots \big(X - f(\alpha_d)\big) \tag{C}$$

If $f(\alpha_i) = f(\alpha_j)$ for some $i \neq j$ in the notation of the proof, then the order of $\{T(f^n)\}$ may be strictly less

*In fact, I expect that this is true for all recursion operators.

than the order of $\{T(y^n)\}$. Nonetheless, by Proposition 4.7, if T is separable

$$P_{T,f}(y, X) \text{ divides } Q \quad \text{ in } K[X], \tag{D}$$

so that the order of the sequence $\{T(f^n)\}$ is less than or equal to the order of $\{T(y^n)\}$. If we choose another parameter $y' = a + by$ of $k[y]$, then by symmetry, we must have $\deg_X P_{T,y} = \deg_X P_{T,y'}$, since each divides a polynomial of degree equal to the degree of the other one. In particular, the order of a separable recursion operator T on $k[y]$ depends only on T and not on the choice of parameter y.

Corollary 4.13 (of discussion above)**.** *If T is a separable recursion operator of order d, then*

$$d = \max_{f \in B} \big\{\text{order of recursion sequence } \{T(f^n)\}\big\}.$$

In other words, we may freely speak of the order of the recursion satisfied by a separable recursion operator T without specifying anything else.

Weights in $\mathbb{F}_p$ and the frobenian property

Here we briefly consider the case $k = \mathbb{F}_p$ for some prime p, before quickly returning to the general case. Call an operator T on an $\mathbb{F}_p$-algebra B *frobenian* if it commutes with the p^{th} power map: that is, if $T(f^p) = \big(T(f)\big)^p$ for all $f \in B$. For example, Hecke operators T_n with n prime to p acting on spaces of modular forms mod p are frobenian operators.

Lemma 4.14. *Let $\mathbb{F}$ be an arbitrary extension of $\mathbb{F}_p$. A separable recursion operator T on $\mathbb{F}[y]$ is frobenian if and only if it has weights in $\mathbb{F}_p$.*

Proof. Let $s = \{T(y^n)\}_n$ be separable. We must show that s has weights in $\mathbb{F}_p$ if and only if $s_n^p = s_{np}$ for all n. For the "only if" direction, let $s_n = \sum_i c_i \alpha_i^n$ for some c_i, α_i in $\overline{\mathbb{F}(y)}$. If $c_i \in \mathbb{F}_p$, then

$$s_{np} = c_1 \alpha_1^{np} + \cdots + c_d \alpha_d^{np} = (c_1 \alpha_1^n + \cdots + c_d \alpha_d^n)^p = s_n^p.$$

Conversely, suppose that for all n,

$$0 = s_n^p - s_{np} = \sum_{i=1}^{d} (c_i^p - c_i) \alpha_i^{np} = \begin{pmatrix} \alpha_1^{np} & \cdots & \alpha_d^{np} \end{pmatrix} \begin{pmatrix} c_1^p - c_1 \\ \vdots \\ c_d^p - c_d \end{pmatrix}.$$

Putting these together for $n = 0, 1, \ldots, d-1$, we get a matrix equation

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1^p & \cdots & \alpha_d^p \\ \vdots & \ddots & \vdots \\ (\alpha_1^p)^{d-1} & \cdots & (\alpha_d^p)^{d-1} \end{pmatrix} \begin{pmatrix} c_1^p - c_1 \\ \vdots \\ c_d^p - c_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

The matrix on the left is in Vandermonde form, and its determinant is

$$\prod_{1 \le i < j \le d} (\alpha_j^p - \alpha_i^p) = \prod_{1 \le i < j \le d} (\alpha_j - \alpha_i)^p.$$

Since the α_i are assumed to be distinct, the Vandermonde matrix is invertible over K, which means that $c_i^p = c_i$ for all i: all the weights are in $\mathbb{F}_p$. □

In other words, the weights-in-k property is a very natural one to consider in the context of Hecke operators in characteristic p.

4.2.3 Properties of recursion operators

We define three related properties that a recursion operator on a polynomial algebra may satisfy, in addition to separability and the weights-in-k property.

Filteredness

Recall that $B = k[y]$. We use the convention that the degree of the polynomial $0 \in B$ is $-\infty$.

Definition. A sequence $s \in B^{\mathbb{N}}$ is *filtered* if $\deg s_n \leq n$ for all n, and *i-filtered* if $\deg s_n \leq n - i$ for all n. An operator T on B is *(i-)filtered* if the sequence $\{T(y^n)\}$ is.

Being filtered is the same thing as being 0-filtered.[†] Unless otherwise noted, everything stated below for filtered sequences and operators will still be true if *filtered* is replaced by *i-filtered*. For example:

An operator T on B is filtered if and only if $\{T(y^n)\}$ is a filtered sequence for any (every) parameter y on B.

Properness

Definition.

- A polynomial $P = a_0X^d + a_1X^{d-1} + a_2X^{d-2} + \cdots + a_d$ in $B[X]$ is *proper* if $\deg a_i \leq i$ for all i. In other words P is proper if and only if its total degree is equal to its X-degree.
- A linear recurrence over B defined by the polynomial P is *proper* if $P \in B[X]$ is a proper polynomial.
- A recursion operator T on B is *proper* if $P_{T,y}$ is proper for any (equivalently, every) parameter y on B.

Lemma 4.15. *Let P and Q be two polynomials in $B[X]$. Then the product PQ is proper if and only if both P and Q are proper.*

Proof. For any polynomial $P \in B[X]$, let d_P and t_P be the X-degree and the total degree, respectively. Let $R = PQ$. Then $d_R = d_Q + d_P$ and $t_R = t_Q + t_R$. Now use the inequality $d \leq t$ for all three polynomials. □

Lemma 4.15 allows us some freedom of expression:

Lemma 4.16.
If T is a recursion operator, then T is proper if and only if it satisfies a proper recursion.

Proof. Suppose $\{T(y^n)\}$ satisfies the recursion defined by R in $B[X]$. By Proposition 4.7, P_T divides R — a priori in $K[X]$, but since the dividend is monic in $B[X]$, the quotient Q is in $B[X]$. By Lemma 4.15, R is proper if and only if P_T is. □

You can see if a proper recursion operator is filtered by looking at the first few terms of the sequence $\{T(y^n)\}$ only:

Proposition 4.17.
A proper recursion operator T of order d is filtered if and only if $\deg T(y^n) \leq n$ for all $n < d$.

[†]Note that some authors use the term *filtered* for what I have called k-filtered for some $k \in \mathbb{Z}$.

Proof. Let $s_n = T(y^n)$. We show that s_n is a filtered sequence by induction. The base case is $n < d$. For $n \geq d$, the filtered recursion says that there exist $a_i \in k[y]$, with $\deg a_i \leq i$, so that $s_n = \sum_i a_i s_{n-i}$. By induction $\deg s_{n-i} \leq n - i$, so that $\deg s_n \leq n$. □

Similarly, the condition of being i-filtered for a proper recursion operator of order d can be checked on the first d terms of the sequence $\{T(y^n)\}$.

We record one more convenient lemma, easy to prove for separable recursion operators.

Lemma 4.18. *A separable[‡] recursion operator T is proper if and only if, for every $f \in B$,*

$$P_{T,f} = X^d + a_1 X^{d-1} + \cdots + a_{d-1} X + a_d$$

satisfies $\deg a_i \leq i \deg f$ *for all i.*

Proof. Suppose $P_{T,y}$ is proper, let α_i be its roots, and fix $f \in B$ of degree d. We want to prove that the n^{th} elementary symmetric function e_n of the $f(\alpha_i)$s has degree bounded by dn given that the n^{th} elementary symmetric function of the α_is has degree bounded by n. The highest-degree term of e_n will come from the n^{th} elementary symmetric function of the y^d term of f, which will be the nd^{th} elementary symmetric function of the α_is. This establishes the f-properness of Q from equation (C). Then use Lemma 4.16. □

Fullness

Definition.

- A proper polynomial $P = a_0 X^d + a_1 X^{d-1} + a_2 X^{d-2} + \cdots + a_d$ in $B[X]$ will be called *full* if $\deg a_d = d$. In other words, P is proper and full if and only if

$$X\text{-degree of } P \quad = \quad y\text{-degree of } P \quad = \quad \text{total degree of } P.$$

- A proper recursion defined by P in $B[X]$ will be called *full* if P is a full polynomial.
- A proper recursion operator T on B is *full* if $P_{T,y}$ is full for any (equivalently, every) parameter y of B.

The fullness property is not particularly meaningful unless accompanied by properness.

Example. The identity operator is full.

Example. The recursion operator T associated to the sequence $\{T(y^n)\}_{n\geq 0} = \{0, 1, y, y^2, \ldots\}$ is proper but not full. Its companion polynomial is $P_{T,y} = X^2 - yX$.

The following three statements are all very easy to prove.

Proposition 4.19.

1. *If P and Q are two proper polynomials, then PQ is full if and only if both P and Q are full.*
2. *A recursion operator is proper and full if and only if it satisfies a proper and full recursion.*
3. *A proper separable[§] recursion operator of order d is full if and only if for every $f \in B$, the constant term of $P_{T,f}$ has degree $d \deg(f)$.*

[‡]I expect this lemma to be true in general: the proof only requires that $\{T(f^n)\}_n$ satisfies the recursion with companion polynomial as given in equation (C).

[§]I expect this property to hold in general.

4.3 The algebra of recursion operators

We will prove that the space of separable with-weights-in-k recursion operators on $B = k[y]$ is a subalgebra of the algebra of linear operators on B.¶

For concision, we fix a parameter y on B and write $P_T := P_{T,y}$ for a recursion operator T on B. Recall that we write $P(y, X)$ to clarify the dependence of a polynomial $P \in B[X]$ on y and X. Recall also that $K = \operatorname{Frac} B = k(y)$.

4.3.1 Sum of recursion operators

Proposition 4.20. *Let S, T be two operators.*

1. *If S, T are filtered, then so is $S + T$.*
2. *If S, T are recursion operators, then so is $S + T$.*
3. *If S, T are separable recursion operators, then so is $S + T$.*
4. *If S, T are separable recursion operators with weights in k, then so is $S + T$.*
5. *If S, T are proper recursion operators, then so is $S + T$.*
6. *If S, T are full and proper recursion operators, then so is $S + T$.*

Proof. Preservation of filtration is clear. From the proof of Proposition 4.9 and the remark $S+T$ is a recursion operator satisfying $P_S P_T$ and separability and separability with weights-in-k is preserved. Lemmas 4.15 and Proposition 4.19 complete the proof. □

We record the following simple lemma for later use.

Lemma 4.21. *If $T : k[y] \to k[y]$ is a recursion operator, and $\alpha \in k$, then the operator $T' = T + \alpha$, satisfying $T'(y^n) = T(y^n) + \alpha y^n$ is also a recursion operator, and satisfies the polynomial*

$$(X - y)\, P_T(X).$$

In particular, T' is proper (repspectively, proper and full) if T is.

4.3.2 Composition of recursion operators

Proposition 4.22. *If S and T are two separable recursion operators and S has weights in k, then $S \circ T$ is also a separable recursion operator with weights in k, satisfying the recursion defined by*

$$Q(y, X) = P_T(\alpha_1, X) P_T(\alpha_2, X) \cdots P_T(\alpha_d, X) \in B[X] \tag{E}$$

where $\alpha_1, \ldots, \alpha_d \in \overline{K}$ are the distinct roots of $P_S(X)$.

Observe that Q as defined above need not be a separable polynomial; part of the claim is that $T \circ S$ is a separable recursion sequence with weights in k nonetheless. In other words $P_{T \circ S}$ may be a proper divisor of Q. (The same phenomenon happens with sums of recursion operators.)

Remarks.

1. I expect this proposition to be true more generally: if S and T are recursion operators, then $S \circ T$

¶In fact, I expect that this is also true for the space of all separable recursion operators and the space of all recursion operators generally, but I do not have a full proof.

should be as well, satisfying the same Q as above; and if S and T are separable then $S \circ T$ should be as well.

2. If the full expected form of Proposition 4.22 holds, then a linear operator on $k[y]$ is a (separable) recursion operator precisely when it transforms (separable) recurrence sequences to (separable) recurrence sequences.

Proof of Proposition 4.22. We can slightly enlarge our definition of a recursion operator to include *recursion maps* $S' : k[y] \to K$: linear maps S' from $k[y]$ to some extension K of $k(y)$ with the additional condition that $\{S'(y^n)\}_n$ in $K^{\mathbb{N}}$ satisfies a linear recursion over K.

Since we are assuming that S is separable with weights in k, we know that there exist elements α_i in $\overline{K}$ and $c_i \in k$ so that $S(y^n) = c_1\alpha_1^n + \cdots + c_d\alpha_d^n$. Let $S_i : k[y] \to \overline{K}$ be the recursion map $S_i(y^n) = c_i\alpha_i^n$, so that $S = S_1 + \cdots + S_d$.

As in the proof of Proposition 4.12, for any $f(y) \in k[y]$, we know that $S_i(f) = c_i f(\alpha_i)$. Let $t_n = T(y^n)$. Then $S_i\big(T(y^n)\big) = S_i(t_n) = c_i t_n(\alpha_i)$. By Lemma 4.11 above, the sequence $\{c_i t_n(\alpha_i)\}$ satisfies the recursion defined by $P_T(\alpha_i, X) \in \overline{K}[X]$ and has weights in k. Therefore, $\big\{S\big(T(y^n)\big)\big\}$ satisfies the recursion defined by $Q(X) = \prod_i P_T(\alpha_i, X)$ and has weights in k as well. The fact that $Q(X)$ is in $k[y][X]$ comes from symmetry; this can be made precise using the resultant perspective below. □

Remark. More generally, the same argument shows that if S and T are recursion operators with S separable, then $S \circ T$ is also a recursion operator satisfying the polynomial (E). But it neither obviously restricts to showing that $S \circ T$ is separable if both S and T are, nor obviously generalizes to general S, and the asymmetry is inconvenient.

The resultant perspective

There is another way to interpret the polynomial Q in Proposition 4.22 above.[‖] Consider the algebra $\widetilde{B} = k[y, X]$, and introduce a new variable Z. Then both $P_T(Z, X)$ and $P_S(y, Z)$ can be viewed as polynomials in $\widetilde{B}[Z]$. I claim that

$$Q(y, X) = \operatorname{Res}\Big(P_S(y, Z),\ P_T(Z, X)\Big) \in \widetilde{B} = k[y, X]. \tag{F}$$

Here $\operatorname{Res}(f, g)$, for polynomials $f, g \in L[x]$ over a field L, is the resultant of f and g. It is most commonly defined as a determinant of a matrix whose rows are shifts of coefficient vectors of f or g padded out with zeros (see [16] for a self-contained exposition, for example). But an equivalent definition for our monic case is the following: suppose $f = (x - \beta_1)\cdots(x - \beta_d)$ factors over some extension of L. Then

$$\operatorname{Res}(f, g) = \prod_{i=1}^{d} g(\beta_i) \in L.$$

Equation (F) is now clear: we find the roots of $P_S(y, Z)$ in $\overline{K} = \overline{k(y)}$, and then plug them in for y in P_T, and take the product.

Composition of filtered and proper recursion operators

Composition preservess all the properties that we have introduced.

[‖] Thanks to Paul Monsky for this suggestion.

Proposition 4.23. *Let S, T be two separable recursion operators on $k[y]$ with weights in k.*

1. *If S, T are filtered, then so is $S \circ T$.*
2. *If S, T are proper, then so is $S \circ T$.*
3. *If S, T are proper and full, then so is $S \circ T$.*

Proof. Point 1 is clear (and has nothing to do with recursions): if S and T preserve the degree filtration, then so does their composition.

Point 2 is proved using the homogeneity properties of the resultant. To see this explicitly, write

$$s(Z) = P_S(y, Z) = Z^d + a_1 Z^{d-1} + \cdots + a_0$$

with $a_i \in k[y]$. Similarly, write

$$t(Z) = P_T(Z, X) = b_0 Z^e + b_1 Z^{e-1} + \cdots + b_e,$$

where b_i are polynomials in $k[X]$, $\deg_X b_e = e$, and b_0 may be zero if P_T is not proper. Let $s^*(Z) = Z^d\, s\big(\frac{1}{Z}\big)$ and $t^*(Z) = Z^e\, t\big(\frac{1}{Z}\big)$, so that $Q = \operatorname{Res}(s, t) = \operatorname{Res}(t^*, s^*)$ by [16, Theorem 1.12]. The homogeneity property [16, Theorem 1.4] applied to this case tells us that, if a_i and b_i is each weighted i, then Q is homogeneous of weight ed. In our case, because of the filtration assumption, $\deg_y a_i \le i$ and $\deg_X b_i \le i$. Therefore the total degree of each term of Q is bounded by ed, which clearly the X-degree of Q.

Finally, point 3 can be seen by tracing through the y-degrees in the product expression from Proposition 4.22: the max-y-degree part of Q comes from the constant-in-X term $\prod_i \alpha_i^{\deg_y P_T}$ and the y-degree of that term is $(\deg_y P_S)(\deg_y P_T)$, since $\deg_y \left(\prod_i \alpha_i\right) = \deg_y P_S$. □

4.3.3 The algebra of recursion operators

For simplicity, we will restrict our attention to filtered operators: that is, operators T that preserve the degree filtration on $k[y]$. These clearly form a subalgebra $\mathcal{F}$ of $\operatorname{End} k[y]$.

Proposition 4.24. *The following spaces are all subalgebras of $\mathcal{F}$ under composition:*

1. *The space of filtered separable recursion operators with weights in k*
2. *The space of proper filtered separable recursion operators with weights in k*
3. *The space of proper and full filtered separable recursion operators with weights in k.*

Proof. Proposition 4.20, Proposition 4.22, and Proposition 4.23. □

The subspace of i-filtered operators is a two-sided ideal in each algebra. The ideal of 1-filtered operators in $\mathcal{F}$ is the Jacobson radical of $\mathcal{F}$.

4.4 Towards generalizations: Recursion operators on filtered algebras

A coda: the notion of a filtered recursion operator on a polynomial algebra may be generalized to filtered algebras.

Definition. A *filtered algebra* is an algebra B equipped with an exhaustive $\mathbb{N}$-filtration of linear subspaces

$$\{0\} \subset B_0 \subset B_1 \subset B_2 \subset \cdots \subset B \qquad \text{with} \quad \bigcup_i B_i = B$$

so that $1 \in B_0$ and $B_i B_j \subset B_{i+j}$ for all i, j.

The definitions imply that B_0 is a subalgebra, and that each B_i is a B_0-module and an ideal of B.

Example. Let $B = k[y]$ and $B_i = \{f \in B : \deg f \leq i\}$.

Example. Fix a prime p and let $B = M^0$ the space of 0-graded modular forms modulo p as defined in section 2.1.1, and $B_i = M_{i(p-1)}$, the space of modular forms of filtration bounded by $i(p-1)$. This is a filtered $\mathbb{F}_p$-algebra, and every Hecke operator T_ℓ is a filtered operator on this space (definition natural and follows).

The second example essentially reduces to the first for $p = 2, 3, 5, 7, 13$, since $M^0 = \mathbb{F}_p[\Delta]$ in each case. The filtration is indexed differently, but since $p-1$ divides $w(\Delta) = 12$ in each case, the adjustment is easy to make.

The following are natural extensions of notions already defined for polynomial algebras.

Definition.

- If B is any algebra, then a linear operator $T : B \to B$ is a (separable, resp., separable with weights in k) *recursion operator* if the sequence $\{T(f^n)\}_n$ is a (separable, resp., separable with weights in k) recursion sequence for every $f \in B$.
- If B is a filtered algebra, then an operator $T : B \to B$ is *filtered* if $T(B_i) \subset B_i$ for all i, and *j-filtered* if $T(B_i) \subset B_{i-j}$ for all i. Positively filtered operators are locally nilpotent but the converse need not be true in this setting.**
- If B is a filtered algebra, recursion operator T on B is *proper* if, for every $f \in B_k$, the recursion polynomial $P_{T,f}$ has the form
$$P_{T,f} = X^d + a_1 X^{d-1} + \cdots + a_d,$$
where $a_i \in B_{ki}$.
- If B is a filtered algebra, a recursion operator T on B is proper and *full* if for every $f \in B_k$, the recursion polynomial $P_{T,f}$ has the form
$$P_{T,f} = X^d + a_1 X^{d-1} + \cdots + a_d,$$
where $a_i \in B_{ki}$ and $a_d \in B_{kd} \backslash B_{kd-1}$.

In Chapter 6, we will show that the Hecke operator T_ℓ acting on the filtered algebra M^0 is a proper filtered separable recursion operator with weights in k. For $p = 2, 3, 5, 7, 13$, we will show that every $T \in A^0$ is a proper and full filtered separable recursion operator with weights in $\mathbb{F}_p$.

**Consider the algebra $k[x, y]$ filtered by total degree. The operator T defined by $T(x^i y^j) = x^{i+1} y^{j-1}$ for $j > 0$ and $T(x^i) = x^{i-1}$ is locally nilpotent but not 1-filtered.

Chapter 5

The Nilpotence Growth Theorem

In this chapter we state and prove the Nilpotence Growth Theorem (Theorem 5.1 below). This is the key technical result of this document, and it is purely algebraic. This chapter is self-contained, though the discussion in Chapter 4 gives context to some of the conditions of the theorem.

Review of terminology

We fix a prime p. Let $\mathbb{F}$ be a field of characteristic p, and $\mathbb{F}[y]$ the polynomial algebra.

We rely on the terminology of Chapter 4.

- A linear operator $T : \mathbb{F}[y] \to \mathbb{F}[y]$ is a *recursion operator* if the sequence $\{T(y^n)\}$ satisfies a linear recursion over $\mathbb{F}[y]$. That is, there exist $a_1, a_2, \ldots, a_d \in \mathbb{F}[y]$ so that, for all $n \geq d$,
$$T(y^n) = a_1\, T(y^{n-1}) + a_2\, T(y^{n-2}) + \cdots + a_d\, T(y^{n-d}).$$
- The *companion polynomial* of this recursion is
$$P_T = X^d - a_1 X^{d-1} - a_2 X^{d-2} - \cdots - a_d \in \mathbb{F}[y][X]$$
The operator T is called *proper* if for all $i \leq d$, we have $\deg a_i \leq i$. It is further called *full* if $\deg a_d = d$. For a full and proper operator T, the X-degree, y-degree, and total degree of P_T coincide.
- A linear operator T on $\mathbb{F}[y]$ is *filtered*, or *E-filtered* for some $E \in \mathbb{Z}$, if $\deg T(y^n) \leq n$, or $\deg T(y^n) \leq n-E$, respectively. Any positively filtered operator is degree-lowering, and therefore locally nilpotent.
- If T is a locally nilpotent operator on $\mathbb{F}[y]$, the *nilpotence index* of any nonzero $f \in \mathbb{F}[y]$ is
$$N_T(f) = \max\{k : T^k f \neq 0\} = \min\{k : T^{k+1} f = 0\}.$$
Set $N_T(0) := -\infty$. Then $N_T(f) \leq \deg f$ for all f.

For discussion of these properties, see sections 3.1 and 4.2.

5.1 Statement of the theorem

Let T be a degree-lowering proper recursion operator on $\mathbb{F}[y]$. We will show that if T is *full*, then $N_T(y^n)$ grows slower than linearly in n.

5.1.1 The most general version

Theorem 5.1 (Nilpotence Growth Theorem (NGT))**.**

Suppose $\mathbb{F}$ is a finite field. Let T be a degree-lowering proper recursion operator on $\mathbb{F}[y]$.

$$\textit{If } T \textit{ is full, then } N_T(f) \ll (\deg f)^\alpha \textit{ for some } \alpha < 1.$$

Which of these conditions is necessary? The degree-lowering property guarantees that the operator is locally nilpotent. Properness goes hand in hand with this kind of degree control: a proper recursion operator of degree d is degree-lowering if and only if it lowers degrees on the first d powers of y (Proposition 4.17). Conversely, if a recurrence is not proper, it is difficult to control the degree of the n^{th} term.

Fullness is necessary, at least in this generality. We have already seen that operator T defined via the sequence $\{T(y^n)\}_{n\geq 0} = \{0, 1, y, y^2, \ldots\}$ has recursion order 2 and $P_{T,y} = X^2 - yX$, filtered and proper but not full. Here $N_T(y^n) = n$, so that the nilpotence index is linear in n.

This example is not rigged: computationally it appears that all degree-lowering T with P_T proper of degree d with intermediate terms of total degree d but no y^d term to counterbalance them are either degenerate (logarithmic growth, say) or give linear growth. For example: let $p = 2$ and consider the operator T defined by $P_T = X^2 + yX + y$. (We have no choice for the initial values: if $[T(1), T(y)] \neq [0, 1]$, then T is either the zero operator or not degree-lowering.) By induction, $\deg T(y^n) = n - 1$. Therefore $N_T(y^n) = n$.

Characteristic p is necessary: A counterexample: consider a degree-lowering recursion operator T on $\mathbb{Q}[y]$ with $P_T = X^2 - yX - y^2$ and degree-lowering initial terms $[T(1), T(y)] = [0, 1]$. This is a proper, full, separable recursion, and it is easy to show that $T(y^n) = F_n y^{n-1}$, where F_n is the n^{th} Fibonacci number: the recursion is $s_n = ys_{n-1} + y^2 s_{n-2}$. Therefore

$$T^k(y^n) = F_n F_{n-1} \cdots F_{n-k+1}\, y^{n-k},$$

so that $N_T(y^n) = n$. (Of course, in characteristic p, we know that $F_5 = 5$ and that $p \neq 5$ divides $F_{p\pm 1}$. Since F_k also divides F_{nk} for all n, in fact T^{p+1} is identically zero on $\mathbb{F}_p[y]$.)

Computationally, it appears that characteristic-zero examples that do not degenerate (to $\log n$ growth, say), all exhibit linear growth. In characteristic p, however, you get a spectrum of $O(n^\alpha)$ growth for various α. Further study of these somewhat mysterious phenomena awaits.

Finiteness of $\mathbb{F}$ is necessary: The Fibonacci example above may be tweaked* to give a counterexample over $\mathbb{F}_p(t)$. Let $P_T = X^2 - tyX - y^2$ and start with $[0, 1]$ again. Then $T(y^n) = F_n(t)y^{n-1}$ with $F_n(t) \in \mathbb{F}_p[t]$ monic of degree $n - 1$, so that $N_T(y^n) = n$ again. This example suggests that the rather violent reduction of Theorem 5.1 to Theorem 5.2, which is true over all $\mathbb{F}$ of characteristic p (see next section), cannot be altogether avoided.

Values of α

In general, as the order of the recursion satisfied by T increases, α goes to 1. Not much more can be said in this generality, but see Theorem 5.2 below, which gives a formula for α in the case where the companion polynomial of the recursion P_T has a particular shape. See also Appendix C.

*Thanks to Paul Monsky for this observation.

5.1.2 Special NGT

The proof of Theorem 5.1 proceeds by reduction to the following special case in which the shape of the recursion satisfied by T is restricted. Note that the statement below has no finiteness restrictions on $\mathbb{F}$, and even no fullness restriction on the recursion.

Theorem 5.2 (Special NGT)**.** *Suppose T is a degree-lowering linear operator on $\mathbb{F}[y]$ so that the sequence $\{T(y^n)\}_n$ satisfies a linear recursion whose companion polynomial has the shape*

$$X^d + ay^d + (\textit{terms of total degree} \leq d - D)$$

for some $D \geq 1$ and some constant $a \in \mathbb{F}$. Suppose further that the order d of the recursion satisfies one of the following conditions:

1. *d is a power of p,*
2. *d is one less than a power of p,*
3. *$d = q^m(q-1)$ where $q > 2$ is a power of p and $m \geq 1$.*

Then

$$N_T(y^n) \ll n^\alpha \quad \textit{for } \alpha = \frac{\log(p^k - D)}{\log p^k}, \textit{ where } p^k \textit{ satisfies } p^{k-1} < d \leq p^k.$$

The theorem is stated for y^n for simplicity, but the same statement holds with y^n replaced by f and n replaced by $\deg f$.

Case (3) alone is enough to prove Theorem 5.1 (see proof below), but the argument is substantially easier in cases (1) and (2), and gives much better α bounds. For the sake of presentation, we will first give the proof in the toy case $d = p$ and $D = 1$ in section 5.3, which makes a good stopping point for a first reading. The general case (1) is not much more complicated, but we give it together with case (2) next. The proof of case (3) itself is technical.

I expect that Theorem 5.2, with its precise α, holds for any d. In addition to the cases above, I have proved it for all d prime to p, but the proof is longer and even more technical, and relegated to Appendix D.

Computationally, it appears that $\alpha = \log_{p^k}(p^k - D)$ is optimal when $d = p$ and not optimal otherwise. See Appendix C for more discussion and some examples of T apparently achieving $N_T(y^n) \asymp n^\alpha$.

Proof that Special NGT implies NGT (Theorem 5.2 $\implies$ Theorem 5.1).
Let $P = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{F}[y][X]$ be the companion polynomial of the proper and full recursion satisfied by the sequence $\{T(y^n)\}_n$. We will show that P divides a polynomial of the form

$$X^e - y^e + (\text{terms of total degree} < e)$$

for $e = q^m(q-1)$, where q is a power of p and $m \geq 0$. Then the sequence $\{T(y^n)\}_n$ will also satisfy the recursion associated to a polynomial of the shape required by Theorem 5.2.

Let H be the degree-d homogeneous part of P, so that $P = H + (\text{terms of total degree} < d)$. I claim that there exists a homogeneous polynomial $S \in \mathbb{F}[y, X]$ so that $H \cdot S = X^e - y^e$ for some positive integer e of required form. Once we find such an S, we know that $P \cdot S$ will have the desired shape $X^e - y^e + (\text{terms of total degree} < e)$.

To find S, we dehomogenize the problem by setting $y = 1$: let $h(X) := H(1, X) \in \mathbb{F}[X]$, a monic polynomial of degree d and nonzero constant coefficient. Let $\mathbb{F}'$ be the splitting field of $h(X)$; under our assumptions all the roots of $h(X)$ are nonzero. Let q be the cardinality of $\mathbb{F}'$. (Recall that we are assuming that $\mathbb{F}$, and hence its finite extension $\mathbb{F}'$, is a finite field.) Every nonzero element $\alpha \in \mathbb{F}'$, and hence every root of $h(X)$, satisfies $\alpha^{q-1} = 1$.

Finally, let q^m be a power of q not less than any multiplicity of any root of $h(X)$. Since every root of h satisfies the polynomial $X^{q-1} - 1$, we know that $h(X)$ divides the polynomial $\left(X^{q-1} - 1\right)^{q^m} = X^{q^m(q-1)} - 1$. Set $e = q^m(q-1)$, and let $s(X)$ be the polynomial in $\mathbb{F}[X]$ satisfying $h(X)s(X) = X^e - 1$.

Now we can finally "rehomogenize" again: if $S \in \mathbb{F}[y, X]$ is the homogenization of $s(X)$, then $Q \cdot S = X^e - y^e$, so that S is the homogeneous scaling factor for P that we seek. □

5.1.3 Very special NGT with constants

Before we begin the proof of Theorem 5.2, we state a more precise version in a yet more constrained case. It will be used for estimating growth nilpotence indices of modular forms with respect to certain Hecke operators for $p = 2, 3, 5$ in Chapter 8.

Theorem 5.3 (Very special case of NGT)**.** *Let T be an E-filtered recursion operator $\mathbb{F}[y]$ satisfying the recursion defined by a polynomial of the form*

$$(X + ay)^d + (\textit{terms of total degree} \leq d - D)$$

for some constant $a \in \mathbb{F}$ (not necessarily nonzero). Then

$$N_T(y^n) \leq \frac{(p^k - D)(p^k - 1)}{E(p^k - D - 1)} \, n^{\log_{p^k}(p^k - D)}. \tag{A}$$

This is Corollary 5.20 in section 5.9 and proved there.

5.2 Overview of the proof

Here's the general plan of attack for Theorem 5.2, and for its refinements in section 5.9 and Appendix D.

Given a degree-lowering recursion operator T we will define an integer-valued function $c_T : \mathbb{N} \to \mathbb{N}$ with growth on the order of n^α for some $\alpha < 1$ and satisfying $c_T(n) = 0$ only if $n = 0$. We also define c_T on polynomials in $\mathbb{F}[y]$ by values on the exponents: for $f = \sum b_i y^{n_i} \in \mathbb{F}[y]$, define $c_T(f) := \max_{b_i \neq 0} c_T(n_i)$. Also set $c_T(0) := -\infty$.

To get the bound on N_T, we will show that T lowers c_T: that is, that $c_T(T(f)) < c_T(f)$ for all $f \neq 0$. Since $c_T(f)$ takes integer values, we know that $c_T\big(T^{c_T(f)}(f)\big) \leq 0$, which means that $T^{c_T(f)}(f)$ is a constant, so that $N_T(f) \leq c_T(f)$. Hence the growth bound $N_T(f) \leq c_T(f) \ll (\deg f)^\alpha$.†

From the definition of c_T on polynomials, it's clear that, to show that T is c_T-lowering, it suffices to prove that $c_T(y^n) < c_T(n)$ for all n. This step is done using the recursion by a tricky induction on n: instead of

†Remarkably, for $d = p$ it appears that one can always find T satisfying the conditions of Theorem 5.2 with $N_T(y^n) = c_T(y^n)$ "most" of the time. See Appendix C for more discussion.

using the recursion of order d corresponding to the given companion polynomial $P(X)$, we use a so-called *deeper recursion* of order $d\,p^k$, corresponding to a $(p^k)^{\text{th}}$ power of $P(X)$ for some s depending on d and n. The sequence $\{T(y^n)\}_n$ will still satisfy the recursion given by $P(X)^{p^k}$ since this polynomial is divisible by $P(X)$. The base case is always $n < d$, which is checked by hand.

On deeper recurrences

Deeper recurrences are a special case of a completely general recursion phenomenon, but in characteristic p, they have a particularly nice form. The basic idea is very simple: if a sequence $s \in \mathbb{F}[y]^{\mathbb{N}}$ satisfies the recursion defined by $Q \in \mathbb{F}[y][X]$, then it also satisfies the recursion defined by any polynomial divisible by Q, in particular the recursion defined by Q^{p^k} for any k. That is, if s satisfies polynomial

$$Q = X^d - a_1 X^{d-1} - a_2 X^{d-2} - \cdots - a_d$$

corresponding to the recurrence

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + \cdots + a_d s_{n-d} \quad \text{for all } n \geq d$$

then s will also satisfy

$$Q^{p^k} = X^{dp^k} - a_1^{p^k} X^{(d-1)p^k} - a_2^{p^k} X^{(d-2)p^k} - \cdots - a_d^{p^k}$$

corresponding to the recurrence

$$s_n = a_1^{p^k} s_{n-p^k} + a_2^{p^k} s_{n-2p^k} + \cdots + a_d^{p^k} s_{n-dp^k} \quad \text{for all } n \geq dp^k.$$

It is not unreasonable to expect that any study of recursion operators and sequences in characteristic p would involve looking at digits of a number base p. We see this phenomenon in Nicolas and Serre's calculations of $N_{T_3}(\Delta^n) + N_{T_5}(\Delta^n)$ for $p = 2$ [23]. We also see it in Derksen's recent theorem that the index set of the zeros of any (nice enough) recurrence sequence (that is, the set $Z(s) = \{n : s_n = 0\}$) in characteristic p is p-automatic [10].

What deeper recursions allow is an inductive argument that allow you compare s_n not with s_{n-1} or s_{n-2} — these small differences can be very disruptive for the base-p expansion of n — but with s_{n-p^k} and s_{n-2p^k} for a k of your choosing. In other words, it allows you to pretend that n has only one or two digits base p, which idea is used in the proof of Theorem 5.2. I learned this technique from Gerbelli-Gauthier's alternate proof [13] of the key technical lemmas of Nicolas-Serre [23].

5.3 A toy case of the Nilpotence Growth Theorem

In this section, we prove a baby subcase of case (1) of Theorem 5.2: $d = p$, $D = 1$, $\mathbb{F} = \mathbb{F}_p$.

Theorem 5.4 (Toy case of NGT)**.** *If $T : \mathbb{F}_p[y] \to \mathbb{F}_p[y]$ is a degree-lowering linear operator so that the sequence $\{T(y^n)\}_n$ satisfies a linear recursion over $\mathbb{F}_p[y]$ with companion polynomial*

$$P = X^p + (\textit{terms of total degree} < p) + ay^p \quad \in \mathbb{F}_p[y][X]$$

then $N_T(y^n) \ll n^{\log_p(p-1)}$.

The proof is technically much simpler, but all of the main features of the general case are present.

5.3.1 The helper content function

We define a function $c : \mathbb{N} \to \mathbb{N}$ depending on our prime p as follows. Given an integer n, we write it base p as $n = \sum_i a_i(n)p^i$ with $a_i(n)$ digits base p, only finitely many of which are nonzero, and define the *p-content of n* as $c(n) := \sum_i a_i(n)(p-1)^i$.
For example, since $71 = [2\,4\,1]_5$ in base 5, the 5-content of 71 is $2 \cdot 4^2 + 4 \cdot 4 + 1 = 49$.

The following properties are easy to check. The first one is proved in Lemma 5.5 in section 5.4.1 below, where the content function and many variations are discussed in great detail.

1. $c(n) \ll n^{\log_p(p-1)}$
2. $c(p^k n) = (p-1)^k c(n)$ for all $k \geq 0$
3. If $0 \leq n < p$, then $c(n) = n$.
4. If i is a digit base p and $i \leq n < p^2$, then $c(n-i)$ is either $c(n) - i$ or $c(n) - i + 1$.
5. If $p \leq n < p^2$, then $c(n-p) = c(n) - p + 1$.

5.3.2 Setup of the proof

For $f \in \mathbb{F}_p[y]$, define the *p-content of $f \neq 0$* by $c\left(\sum a_n y^n\right) := \max_{a_n \neq 0} c(n)$; set $c(0) = -\infty$. For example, the 3-content of $2y^9 + y^7 + y^2$ is 5.

Let $T : \mathbb{F}_p[y] \to \mathbb{F}_p[y]$ be a degree-lowering recursion operator whose companion polynomial

$$P = X^p + a_1 X^{p-1} + \cdots + a_p \in \mathbb{F}_p[y][X]$$

satisfies $\deg a_i < i$ for $1 \leq i < p$ and $\deg a_p = p$, as in case (1) of Theorem 5.2.

We will show that T lowers p-content of any $f \in \mathbb{F}_p[y]$: that is, that $c(Tf) < c(f)$. It willl suffice to do this for $f = y^n$. We will proceed by induction on n, each time using the deeper recursion of order p^{k+1} corresponding to P^{p^k} with k chosen so that $p^{k+1} \leq n < p^{k+2}$. The base case is $n < p$, in which case being p-content-lowering is the same thing as being degree-lowering.

5.3.3 The induction

Induction in the toy case. For $n \geq p$, we show that $c(T(y^n)) < c(n)$ assuming that $c(T(y^e)) < c(e)$ for all $e < n$. As above, choose $k \geq 0$ with $p^{k+1} \leq n < p^{k+2}$. The polynomial

$$P^{p^k} = X^{p^{k+1}} - a_1^{p^k} X^{p^{k+1}-p^k} - a_2^{p^k} X^{p^{k+1}-2p^k} - \cdots - a_p^{p^k} \in \mathbb{F}_p[y][X]$$

corresponds to the recursion of order p^{k+1}

$$T(y^n) = a_1^{p^k} T(y^{n-p^k}) + a_2^{p^k} T(y^{n-2p^k}) + \cdots + a_p^{p^k} T(y^{n-p^{k+1}}).$$

Pick a term y^e appearing in $T(y^n)$; we want to show that $c(e) < c(n)$. From the recursion, y^e comes from $a_i^{p^k} T(y^{n-ip^k})$ for some i. More precisely, y^e appears in $y^{jp^k} T(y^{n-ip^k})$ for some y^j appearing in a_i, so that either $j < i$ or $i = j = p$. Then y^{e-jp^k} appears in $T(y^{n-ip^k})$, and by induction we know that $c(e - jp^k) < c(n - ip^k)$. To conclude that $c(e) < c(n)$, it would suffice to show that

$$c(n) - c(e) \geq c(n - ip^k) - c(e - jp^k),$$

or, equivalently, that

$$c(n) - c(n - ip^k) \geq c(e) - c(e - jp^k).$$

Since subtracting multiples of p^k leaves the last k digits of n base p untouched, we may replace n and e by $\lfloor \frac{n}{p^k} \rfloor$ and $\lfloor \frac{e}{p^k} \rfloor$, respectively, and then cancel out a factor of $(p-1)^k$. In other words, we must show that

$$c(n) - c(n - i) \geq c(e) - c(e - j).$$

for n, e, i, j satisfying $i \leq n < p^2$ and $j \leq e < n$ and either $j < i$ or $i = j = p$. But this an easy consequence of the properties of c listed in section 5.3.1. For $j < i$, we know that $c(n) - c(n-i)$ is at least $i - 1$ and $c(e) - c(e-j)$ is at most $j \leq i - 1$. And for $i = j = p$ both sides equal $p - 1$. □

5.3.4 A good stopping point

This toy case already shows most of the features of the general case. Most of the difficulty of generalization comes from working with more general versions of the content function. For example, the proof for case (1) for d a power of p proceeds the same way, but we use base $b = p^k$ for the content function. The refinement in α coming from the degree descent D comes from replacing the base b with $b - D$ rather than $b - 1$. These steps are both straightforwards. However, to prove cases (2) and (3) we must extend the notion of content to rational numbers (section 5.4), whence the technical difficulties. Case (2) is still relatively simple because the base b expansion of $\frac{1}{b-1}$ is so easy; it is proved in sections 5.5 and 5.6 together with the general case (1). Case (3) is more computationally complicated, and postponed until sections 5.7 and 5.8.

The rest of this chapter is devoted to the proof of Theorem 5.2, as well as a few technical refinements in section 5.9. Now is an excellent stopping point for a first reading. Chapter 6 begins on page 70.

5.4 The helper function c_T

5.4.1 The content function for integer n

First, we introduce a general type of function with sublinear growth out of which all the c_Ts will be built. The idea for this kind of function was originally suggested by Bellaïche, as in the appendix to [5].

Definition. Fix an integer $b \geq 2$ as the *base*. Let D be a *descent*: a integer with $0 \leq D \leq b - 1$. Given a nonnegative integer n, write it in base b as $n = [a_\ell \, a_{\ell-1} \, \cdots \, a_1 \, a_0]_b$, where $a_i \in \{0, 1, \ldots, b-1\}$ are digits base b, and $\ell = \lfloor \log_b n \rfloor$, so that $n = \sum_i a_i b^i$. Then the (b, D)-*content of* n is the quantity

$$c_{b,D}(n) = \sum_{i=0}^{\ell} a_i (b - D)^i.$$

In particular, $c_{b,0}(n) = n$, and $c_{b,b-1}(n)$ is sum of the digits in the base-b expansion of n. In applications, b will always be a power of p and $D \geq 1$.

For example, since $196 = [1\,2\,4\,1]_5$ in base 5, we have $c_{5,2}(196) = 1 \cdot 3^3 + 2 \cdot 3^2 + 4 \cdot 3 + 1 = 58$.

If $D > 0$, then the growth rate of $c_{b,D}(n)$ is sublinear in n. Indeed, let $\ell = \lfloor \log_b n \rfloor$. Then

$$c_{b,b-1}(n) \leq (b-1)(\ell + 1) \ll \log(n).$$

And for $D < b-1$, note that $(b-D)^\ell \le n^{\log_b(b-D)}$:

$$c_{b,D}(n) \le \sum_{i=0}^{\ell}(b-1)\cdot(b-D)^i = (b-1)\frac{(b-D)^{\ell+1}-1}{b-1-D} < \frac{(b-1)(b-D)}{b-1-D}n^{\log_b(b-D)} \ll n^{\log_b(b-D)}.$$

We have therefore proved

Lemma 5.5. *For $0 < D < b-1$, we have $c_{b,D}(n) \le \frac{(b-1)(b-D)}{b-1-D}n^{\log_b(b-D)} \ll n^{\log_b(b-D)}$. Moreover, $c_{b,b-1}(n) \ll \log n$.*

Although we will not use this fact in full generality for the proof of Theorem 5.2, the content function exhibits a certain amount of regularity under addition and subtraction. See Lemma D.2 in Appendix D, where a slight generalization of Theorem 5.2 is proved.

5.4.2 Extending content to rational n

From now on, we assume that $b > 2$ and that the descent D satisfies $1 \le D < b-1$.

We extend the definition of (b, D)-content to nonnegative rational numbers in the most natural way. Write $n \in \mathbb{Q}^+$ in base b: that is, find a infinite sequence of base b digits

$$\left[a_r, a_{r-1}, a_{r-2}, \ldots, a_0, a_{-1}, a_{-2}, \ldots\ldots\right]$$

indexed by all integers less than or equal to $r = \lfloor \log_b n \rfloor$ satisfying

$$n = \sum_{i=-\infty}^{r} a_i b^i.$$

If the base-b expansion of n is finite — that is, if $b^k n$ is in $\mathbb{Z}$ for some k — then there are two choices for this expansion, and we choose the "proper" one: the one with $a_i = 0$ for $i \ll 0$. This proper base-b expansion extends the one we use for integers. Finally, define $c_{b,D}(n)$ exactly as before:

$$c_{b,D}(n) = \sum_i a_i (b-D)^i.$$

This converges since we have assumed that $D > b-1$ and the a_i are uniformly bounded. Because n is rational, its base-b digits a_i will be eventually periodic for negative i, which implies that $c_{b,D}(n)$ is always rational.

For example, if $b = 7$ and $n = \frac{1}{3}$, then $n = [0.\overline{2}]_7 = \sum_{i \le -1} 2 \cdot 7^i$, so that $c_{7,2}(n) = \sum_{i \le -1} 2 \cdot 5^i = \frac{1}{2}$. Similarly, $c_{7,2}\left(\frac{1}{4}\right) = c_{7,2}\left([0.\overline{1\ 5}]\right) = \frac{5}{12}$.

We record two lemmas. The first is a useful multiplicativity property clearly satisfied by (b, D)-content by definition.

Lemma 5.6. *Let b be a base and D a descent. If $n \in \mathbb{Q}_{\ge 0}$ and $k \in \mathbb{Z}$, then*

$$c_{b,D}(b^k\, n) = (b-D)^k\, c_{b,D}(n).$$

And the second is trivial:

Lemma 5.7. *If $1 \le n < b$, then $c_{b,D}(n) - c_{b,D}(n-1) = 1$.*

Integrality

In this section, we suppose that d is prime to b.

Then $\frac{1}{d}$ base b is purely period of period ℓ, where $\ell \geq 1$ is the multiplicative order of b modulo d. Write

$$\frac{1}{d} = \frac{A}{b^\ell - 1},$$

where $A = [a_{-1}\, a_{-2}\, \ldots\, a_{-\ell}]$ is the integer whose base-b digits are one full period cycle of $\frac{1}{d}$.

Lemma 5.8. *If i satisfies $0 \leq i < d$ then*

$$c_{b,D}\left(\frac{i}{d}\right) = \frac{c_{b,D}(iA)}{(b-D)^\ell - 1}.$$

Proof. Computation using the periodicity of the expansion. Note that, for these values of i the number of digits in im base b is exactly ℓ. □

Corollary 5.9. *If n is any number in $\frac{1}{d}\mathbb{Z}^+$, and ℓ is the multiplicative order of b modulo d, then*

$$\left((b-D)^\ell - 1\right) c_{b,D}(n)$$

is an integer.

Proof. Write $n = N + \frac{i}{d}$ where N is an integer and $0 \leq i < d$. Then $c_{b,D}(n) = c_{b,D}(N) + c_{b,D}\left(\frac{i}{d}\right)$. Now use Lemma 5.8. □

Growth

The examples in the beginning of this subsection show that, if n is not an integer, then $c_{b,D}(n)$ need not be less than n. However, we can easily bound the bad behavior. We have observed that $c_{b,D}(n) = c_{b,D}\big(\lfloor n \rfloor\big) + c_{b,D}\big((n)\big)$, where $(n) = n - \lfloor n \rfloor$ is the fractional part of n. Since $c_{b,D}(n) \leq n$ for all integers n, to see how much $c_{b,D}(n)$ may exceed rational n, it suffices to look at n strictly between 0 and 1. In this case, $c_{b,D}(n)$ is always strictly bigger than n — but fortunately, not by much:

$$c_{b,D}(n) - n = \sum_{i \geq 1} a_{-i} \frac{1}{(b-D)^i} - \sum_{i \geq 1} a_{-i} \frac{1}{b^i} = \sum_{i \geq 1} a_{-i} \frac{b^i - (b-D)^i}{b^i (b-D)^i}.$$

It is clear that for fixed b, D this sum is maximized if $a_{-i} = b - 1$ for all i. (In this case, $n = 1$ and the expansion is not proper, but this is irrelevant for the bound.) We estimate: for $0 < n < 1$,

$$c_{b,D}(n) - n < \sum_{i \geq 1} \frac{b-1}{(b-D)^i} - 1 = \frac{b-1}{b-D} \frac{1}{1 - \frac{1}{b-D}} - 1 = \frac{D}{b-1-D}.$$

The weaker statement that, for $0 < n < 1$, we have $c_{b,D}(n) < \frac{b-1}{b-D-1} = O(1)$ establishes that $c_{b,D}(n)$ is still $O\big(n^{\log_b(b-D)}\big)$. More precisely,

$$c_{b,D}(n) < \frac{(b-1)(b-D)}{b-1-D} n^{\log_b(b-D)} + \frac{b-1}{b-D-1}. \tag{B}$$

5.4.3 Defining c_T given T

Let $P(X) = X^d + cy^d +$ (terms of total degree $\leq d - D$) be the companion polynomial of the recursion satisfied by $\{T(y^n)\}$. We take three cases, as in the conditions of Theorem 5.2. In each case, we will set $c_T(n) := M_T\, c_{b,D}\left(\frac{n}{d}\right)$ for the smallest p-power $b \geq d$ and M_T chosen to make c_T integral, though note that in case (3) there is a further condition on D.

1. **Case d is a power of p.** Let $b = d$. Set $M_T = d - D$, so that
$$c_T(n) := (d-D)\, c_{b,D}\left(\frac{n}{d}\right) = (b-D)\, c_{b,D}\left(\frac{n}{d}\right).$$
This function coincides with $c_{b,D}(n)$, so it is integer-valued.

2. **Case d is one less than a power of p.** Define b so that $d = b - 1$. Set $M_T = d - D$ and
$$c_T(n) := (d-D)\, c_{b,D}\left(\frac{n}{d}\right) = (b-D-1)\, c_{b,D}\left(\frac{n}{d}\right).$$
This is integer-valued by Corollary 5.9 with $\ell = 1$.

3. **Case $d = q^{m-1}(q-1)$ for $q > 2$ a power of p and $m \geq 2$.** Define $b = q^m$. Set $M_T = (b-D)(b-D-1)$ and
$$c_T(n) := (b-D)(b-D-1)\, c_{b,D}\left(\frac{n}{d}\right).$$
The proof will require that $\boxed{D < \frac{q[m]_q}{2}}$, where we use the notation $[m]_q = \frac{q^m-1}{q-1}$.

   This function is integer-valued because
$$c_{b,D}\left(\frac{n}{d}\right) = c_{b,D}\left(b^{-1}\frac{nq}{q-1}\right) = (b-D)^{-1} c_{b,D}\left(\frac{nq}{q-1}\right)$$
and Corollary 5.9 applies again with $\ell = 1$.

Although case (3) reduces to case (2) for $m = 1$, it is actually quite a bit more complicated than case (2). In fact, it is cases (1) and (2) that behave similarly, and simply, and unconditionally.

5.5 The base property and the step property

Let d, D, and b be as in one of the three cases above, and write c for $c_{b,D}$. The induction argument for the proof of Theorem 5.2 requires two properties of c.

The first property is required to establish the base case of the induction.

- **Base property:** c is strictly increasing on the set $\{0, \frac{1}{d}, \frac{2}{d}, \ldots, \frac{d-1}{d}\}$.

This is easily seen to be true in cases (1) and (2): in both cases, $c\left(\frac{i}{d}\right) = \frac{i}{d-D}$ (Lemma 5.10 below). For case (3), this is only true for D not to big. This is established in Corollary 5.14 in section 5.8.

The second property is required for the inductive step. The induction proceeds by considering each $y^j X^{d-i}$ term of the recursion polynomial in turn. Accordingly, i and j are integers between 0 and d satisfying $j \leq i - D$. Moreover, e and n are rational numbers in $\frac{1}{d}\mathbb{Z}$ satisfying $0 \leq e < n < b$ and $n \geq \frac{i}{d}$ and $e \geq \frac{j}{d}$.

- **Step property:** If i and j satisfy $0 \le j \le i - D < i \le d$, then
$$c(n) - c\left(n - \frac{i}{d}\right) \ge c(e) - c\left(e - \frac{j}{d}\right).$$

In cases (1) and (2), Lemma 5.11 below and Lemma 5.7 above establish that, for n and i in these ranges,
$$c(n) - c\left(n - \frac{i}{d}\right) \in \left\{\frac{i}{d-D}, \frac{i-D}{d-D}\right\},$$
and similarly for e and j. Therefore the least possibility for the left-hand side is $\frac{i-D}{d-D}$, and the biggest possibility for the right-hand side is $\frac{j}{d-D}$. Since $j \le i - D$, this is just enough to establish the inequality.

For case (3), this statement is more involved and established in section 5.8.

5.5.1 Lemmas for cases (1) and (2)

As noted above, we need the following lemma for the inductive step for cases (1) and (2), if d is either a power of p or one less than a power of p. In fact, the lemma is true for any base $b \ge 2$ and $D \le d$, where d is either b or $b - 1$.

Lemma 5.10. *If $d = b$ or $d = b - 1$, then for A with $0 \le A < d$,*
$$c_{b,D}\left(\frac{A}{d}\right) = \frac{A}{d-D}.$$

Proof. Computation. The fact that the formula looks the same is a coincidence that explains the similarity of case (1) and case (2). □

Lemma 5.11. *Suppose $n \in \frac{1}{d}\mathbb{Z}_{\ge 0}$ satisfies $n < b$, and i is an integer with $0 \le i < d$ and $\frac{i}{d} \le n$. Then*
$$c_{b,D}(n) - c_{b,D}\left(n - \frac{i}{d}\right) \in \left\{\frac{i}{d-D}, \frac{i-D}{d-D}\right\}.$$

Proof. Write $c = c_{b,D}$. Let $n = N + \frac{A}{d}$, where $N < b$ and $0 \le A < d$. We will use the fact that $c(n) = c(N) + c\left(\frac{A}{d}\right)$ and Lemma 5.10.

If $A \ge i$, then
$$c(n) - c\left(n - \frac{i}{d}\right) = c(N) + c\left(\frac{A}{d}\right) - c(N) - c\left(\frac{A-i}{d}\right) = \frac{A}{d-D} - \frac{A-i}{d-D} = \frac{i}{d-D}.$$

And if $A < i$, then
$$c(n) - c\left(n - \frac{i}{d}\right) = c(N) + c\left(\frac{A}{d}\right) - c(N-1) - c\left(\frac{d+A-i}{d}\right) = 1 + \frac{A}{d-D} - \frac{d+A-i}{d-D} = \frac{i-D}{d-D},$$
by Lemma 5.7. □

Proving the base and step properties for case (3) is postponed until section 5.8.

5.6 The main induction

We are ready to give the proof of Theorem 5.2 for T assuming the base property and the step property from the previous section hold.

Proof of Theorem 5.2. If $d = 1$, then T must be the zero operator and the sublinearity statement holds. So assume that $d \geq 2$. Use section 5.4.3 to define b, D, and the function $c_T(n) = Mc_{b,D}\left(\frac{n}{d}\right)$ depending on the case that we are in. (Note that $b > 2$ unless $p = d = 2$, in which case $c_T(n) = c_{2,1}(n)$ and Lemma 5.11 holds. The condition $b > 2$ is otherwise assumed in section 5.4.2 and thereafter.) We assume that $c = c_{b,D}$ satisfies the two properties from section 5.5.

Write x_n for $T(y^n)$. Recall that we want to use induction on n to show that $c_T(x_n) < c_T(n)$. The base case is all $n < d$. Since T decreases degrees, the statement $c_T(x_n) < c_T(n)$ for $n < d$ is equivalent to the statement that $c = c_{b,D}$ is increasing on $0, \frac{1}{d}, \ldots, \frac{d-1}{d}$. This is the base property from section 5.5.

For $n \geq d$, let $k \geq 0$ be the integer so that $d \cdot b^k \leq n < d \cdot b^{k+1}$. Let $P(X)$ be our given recursion, and write it in the form

$$X^d + ay^d + \sum_{0 \leq j \leq i-D < i \leq d} a_{i,j}\, y^j\, X^{d-i}$$

with $a_{i,j}$ and a all in $\mathbb{F}$. Raise $P(X)$ to the b^k power to get

$$X^{db^k} + ay^{db^k} + \sum_{0 \leq j \leq i-D < i \leq d} a_{i,j}\, y^{jb^k}\, X^{(d-i)b^k}.$$

(Here we have simplified notation by replacing a^{b^k} by a, and similarly for $a_{i,j}$. The coefficients play no part in this game.) This translates into the recursion

$$x_n = -a\, y^{db^k} x_{n-db^k} \quad - \sum_{0 \leq j \leq i-D < i \leq d} a_{i,j}\, y^{jb^k}\, x_{n-ib^k}.$$

We want to show that, for all terms y^e appearing in x_n we have $c_T(e) < c_T(n)$. We take two cases, depending on which term of the order-$d\,b^k$ recursion above y^e appears in.

Suppose y^e appears in the (i,j)-term in the sum on the right. That is, y^e appears in $y^{jb^k} x_{n-ib^k}$ for some $0 \leq j \leq i - D < i \leq d$. That means that y^{e-jb^k} appears in x_{n-ib^k}, so that, by the induction assumption, $c_T(e - jb^k) < c_T(n - ib^k)$. To show that $c_T(e) < c_T(n)$, it would therefore suffice to show that

$$c_T(n) - c_T(e) \stackrel{?}{\geq} c_T(n - ib^k) - c_T(e - jb^k),$$

or, arranged more conveniently, that

$$c_T(n) - c_T(n - ib^k) \stackrel{?}{\geq} c_T(e) - c_T(e - jb^k)$$

under our assumptions $jb^k \leq e < n$ and $db^k \leq n < db^{k+1}$ and $0 \leq j \leq i - D < i \leq d$. We divide by M, replace e and n by their respective quotients by $d\,b^k$, and use the multiplicativity property of $c_{b,D}$ (Lemma 5.6) to pull out and cancel a factor of $(b - D)^k$. We have therefore reduced the desired inequality to the inequality

$$c(n) - c\left(n - \frac{i}{d}\right) \stackrel{?}{\geq} c(e) - c\left(e - \frac{j}{d}\right)$$

Note: There is a mistake here in the last reduction step rendering the rest of the proof of Theorem 5.2 invalid in the required generality. Indeed, e and n are now in (1/d) Z[1/b^k], not in (1/d) Z.
This mistake is corrected in the published version.

assuming that e, n are in $\frac{1}{d}\mathbb{Z}$ with $0 \le e < n < b$ and that i and j are integers with $0 \le j \le i - D < i \le d$, and that all the arguments of c are nonnegative. This inequality is exactly the step property of section 5.5.

Suppose, on the other hand, that y^e appears in the first term. After the same reduction tricks, we must show that

$$c(n) - c(n-1) \ge c(e) - c(e-1)$$

provided that $1 \le e, n < b$. This is trivially true by trivial Lemma 5.7: both sides are equal to 1. □

This completes the proof of Theorem 5.2 in the case where d is a power of p or one less than a power of p. It still remains to establish the necessary step properties for the case $d = q^{m-1}(q-1)$. This will be done in section 5.8. In the next section, we reformulate the properties in a way that makes them more tractable.

5.7 Reformulating the step property

In cases (1) and (2), the step property is proved relatively easily by using Lemma 5.11, which gives two options for a difference like $c(n) - c\big(n - \frac{i}{d}\big)$ depending on whether the fractional part of n exceeds i or not. It turns out that a comparable lemma is tricky when summing two proper fractions of denominator d may cause carrying in digits base b, which difficulty does not occur if $d = b$ or $d = b - 1$.

The following proposition gives a sufficient condition for satisfying the step property.

Proposition 5.12. *Let $c = c_{b,D}$ for some base b and integer descent D. Let $d \le b$ be an integer.*

Suppose that, for integers A, B, i, j satisfying $0 \le j, k, A, B < d$ and $0 < i \le d$ so that further all the arguments of c are nonnegative, the following properties are satisfied.

1. *If $j \le i - D$, then*
$$c\left(\frac{A}{d}\right) - c\left(\frac{A-i}{d}\right) \ge c\left(\frac{B}{d}\right) - c\left(\frac{B-j}{d}\right).$$
2. *If $k + j \le d - D$, then*
$$c\left(\frac{A}{d}\right) - c\left(\frac{A-k}{d}\right) + c\left(\frac{B}{d}\right) - c\left(\frac{B-j}{d}\right) \le 1.$$
3. *If $i + k \ge d + D$, then*
$$c\left(\frac{A}{d}\right) - c\left(\frac{A-i}{d}\right) + c\left(\frac{B}{d}\right) - c\left(\frac{B-k}{d}\right) \ge 1.$$

Then c satisfies the step properties from section 5.5.

If, further, b is a power of p, and

4. *The function c is strictly increasing on $[0,1) \cap \frac{1}{d}\mathbb{Z}$:*
$$0 = c(0) < c\left(\frac{1}{d}\right) < c\left(\frac{2}{d}\right) < \cdots < c\left(\frac{d-1}{d}\right).$$

then any recursion operator $T : \mathbb{F}[y] \to \mathbb{F}[y]$ satisfying a recursion polynomial with shape

$$X^d + cy^d + (\textit{terms of total degree} \le d - D)$$

is c-decreasing, where $c(n) = c_{b,D}\left(\frac{n}{d}\right)$.

Proof. Let n, e, i, j be as in section 5.5: that is, n and e are in $\frac{1}{d}\mathbb{Z}$ and satisfy $0 \le e < n < b$, and $0 \le j \le i - D < i \le d$.

Write $n = N + \frac{A}{d}$ with $N \in \mathbb{Z}$ and $0 \le A < d$. Similarly, let $e = E + \frac{B}{d}$.

For the step property, recall that we want to show that

$$c(n) - c\left(n - \frac{i}{d}\right) \ge c(e) - c\left(e - \frac{j}{d}\right).$$

If $A \ge i$, then

$$c(n) - c\left(n - \frac{i}{d}\right) = c(N) + c\left(\frac{A}{d}\right) - c(N) - c\left(\frac{A-i}{d}\right) = c\left(\frac{A}{d}\right) - c\left(\frac{A-i}{d}\right).$$

And if $A < i$, then

$$c(n) - c\left(n - \frac{i}{d}\right) = c(N) + c\left(\frac{A}{d}\right) - c(N-1) - c\left(\frac{d+A-i}{d}\right) = 1 + c\left(\frac{A}{d}\right) - c\left(\frac{A+d-i}{d}\right).$$

Similar statements are true for e, E, B, j.

We consider four cases, depending on how A compares to i and how B compares to j.

- $\boxed{A \ge i,\ B \ge j}$ We want to show that $c\left(\frac{A}{d}\right) - c\left(\frac{A-i}{d}\right) \ge c\left(\frac{B}{d}\right) - c\left(\frac{B-j}{d}\right)$. This is property (1) in the statement of the proposition.
- $\boxed{A < i,\ B < j}$ We want to show that $1 + c\left(\frac{A}{d}\right) - c\left(\frac{A+(d-i)}{d}\right) \ge 1 + c\left(\frac{B}{d}\right) - c\left(\frac{B+(d-j)}{d}\right)$. This is again covered by property (1), with $d - i$ playing the role of j and $d - j$ the role of i.
- $\boxed{A < i,\ B \ge j}$ We want to show that $1 + c\left(\frac{A}{d}\right) - c\left(\frac{A+(d-i)}{d}\right) \ge c\left(\frac{B}{d}\right) - c\left(\frac{B-j}{d}\right)$. Since $(d-i)+j \le d-D$, this is property (2) from the statement of the proposition, with $k = d - i$.
- $\boxed{A \ge i,\ B < j}$ We want to show that $c\left(\frac{A}{d}\right) - c\left(\frac{A-i}{d}\right) \ge 1 + c\left(\frac{B}{d}\right) - c\left(\frac{B+(d-j)}{d}\right)$. Since $i+(d-j) \ge d+D$, this is property (3) from the statement of the proposition, with $k = d - j$.

Finally, the proof of Theorem 5.2 uses the properties from section 5.5 only, so that the last statement is clear.

□

5.8 The proof of case (3)

We prove that case (3) satisfies the base property and the reformulated step properties from section 5.7 to complete the proof of Theorem 5.2.

5.8.1 The base property for case (3)

Recall that $d = q^{m-1}(q-1)$ and $b = q^m$ with $q > 2$ and $m \ge 2$. Let $M = (b-D)(b-D-1)$ and write c for $c_{b,D}$. We will analyze $\frac{i}{d}$ and $c\left(\frac{i}{d}\right)$ for $0 \le i < d$. Recall that $[m]_q = \frac{q^m-1}{q-1} = q^{m-1} + q^{m-2} + \cdots + q + 1$.

Lemma 5.13. *For* $0 \le i < d$, *let* $i = a_i(q-1) + r_i$ *with* $0 \le r < q-1$, *as in Euclid's algorithm for* $i \div (q-1)$.

Then

$$\frac{i}{d} = \Big[0. \quad i + a_i \quad \overline{r_i[m]_q}\Big] \qquad \text{and} \qquad M\,c\Big(\frac{i}{d}\Big) = i\big(q[m]_q - D\big) - Da_i.$$

Proof. We prove the first assertion. It is clearly true for $i = 0$ and we already established that $\frac{1}{d} = \Big[0.\,1\,\overline{[m]_q}\Big]$, which proves the claim for $i = 1$. For $i = 2, 3, \ldots, q-2$, one has $i = r_i$ and $a_i = 0$, and it's clear by multiplying that $\frac{i}{d} = \Big[0. \;\; i \;\; \overline{r_i\,[m]_q}\Big]$. If i is a multiple of $q-1$, say $i = a_i(q-1)$, then $\frac{i}{d} = \frac{a_i q}{b} = \big[0. \;\; a_i q \;\; \overline{0}\big]$. The claim follows by considering sums of these: the first digit after the radix point is $a_i q + r_i = a_i(q-1) + (r_i + a_i) = i + a_i$, and the second is clear. Observe that, since $i < q^m - q^{m-1}$, we know that $a_i < q^{m-1}$, so that $i + a_i < q^m$ is a digit base b.

The second assertion follows by computation from the first using the relationship between i, a_i and r_i and the definition of $[m]_q$. □

Corollary 5.14 (Base property)**.** *If* $\boxed{D < \frac{q[m]_q}{2}}$*, then the function c is increasing on $\big\{0, \frac{1}{d}, \frac{2}{d}, \cdots, \frac{d-1}{d}\big\}$. That is,*

$$0 = c(0) < c\left(\frac{1}{d}\right) < c\left(\frac{2}{d}\right) < \cdots < c\left(\frac{d-1}{d}\right).$$

The condition $D < \frac{q[m]_q}{2}$ is absolutely necessary: as you can see from the proof below, every violation will give counterexamples. This condition is satisfied if D satisfies the simpler inequality $\boxed{D \le \frac{b}{2}}$.

Proof. It suffices to see, for $0 \le i < d-1$, that the difference $M\,c\big(\frac{i+1}{d}\big) - M\,c\big(\frac{i}{d}\big)$ is strictly positive. We use Lemma 5.13 and note that $a_{i+1} - a_i$ is either 0 or 1 depending on i modulo $q-1$.

$$M\,c\left(\frac{i+1}{d}\right) - M\,c\left(\frac{i}{d}\right) = q[m]_q - (1 + a_{i+1} - a_i)D \ge q[m]_q - 2D.$$

This last is strictly positive precisely when $D < \frac{q[m]_q}{2}$. □

5.8.2 The properties of Proposition 5.12 for case (3)

Recall that have $d = q^{m-1}(q-1)$ and $b = q^m$ with $q \ge 3$ and $m \ge 2$. Let $M = (b-D)(b-D-1)$ and write c for $c_{b,D}$. We use the notation $[m]_q = \frac{q^m - 1}{q-1}$. Also set $a_i = \Big\lfloor \frac{i}{q-1} \Big\rfloor$. In Lemma 5.13, we have shown that $c\big(\frac{i}{d}\big) = i([m]_q - D) - Da_i$ for $i < d$.

Lemma 5.15. *Suppose i and j are integers with $0 \le j \le i < d$. Then*

$$c\left(\frac{i}{d}\right) - c\left(\frac{j}{d}\right) \in \left\{c\left(\frac{i-j}{d}\right) - \frac{D}{M}, \quad c\left(\frac{i-j}{d}\right)\right\}.$$

Proof. From Lemma 5.13, we know that

$$M\,c\left(\frac{i}{d}\right) - M\,c\left(\frac{j}{d}\right) = (i-j)(q[m]_q - D) - D(a_i - a_j)$$

Since $a_i = \Big\lfloor \frac{i}{q-1} \Big\rfloor$, and $\lfloor x \rfloor + \lfloor y \rfloor \in \{\lfloor x+y \rfloor, \;\; \lfloor x+y \rfloor + 1\}$ for all reals x and y, it is clear that $a_i - a_j \in \{a_{i-j}, \;\; a_{i-j} + 1\}$. The claim follows. □

Lemma 5.16 (Property (1))**.** *Suppose A, B, i, j are integers satisfying $0 \le i, j, A, B < d$ so that moreover $i - j \ge D$ and $A - i, B - j \ge 0$. If $\boxed{D \le \frac{q[m]_q}{2}}$, then*

$$c\left(\frac{A}{d}\right) - c\left(\frac{A-i}{d}\right) \ge c\left(\frac{B}{d}\right) - c\left(\frac{B-j}{d}\right).$$

Proof. From Lemma 5.15, the left-hand side is at least $c\left(\frac{i}{d}\right) - \frac{D}{M}$, and the right-hand side is no more than $c\left(\frac{j}{d}\right)$. Therefore it is enough to show that $c\left(\frac{i}{d}\right) - c\left(\frac{j}{d}\right) \ge \frac{D}{M}$. But by Lemma 5.15 again, the left-hand side of this last is at least $c\left(\frac{i-j}{d}\right) - \frac{D}{M}$, and by Lemma 5.14, this last is no less than $c\left(\frac{D}{d}\right) - \frac{D}{M}$. So it is enough to know that $c\left(\frac{D}{d}\right) \ge \frac{2D}{M}$.

This is an easy estimate: since we are assuming that $D \le \frac{q[m]_q}{2}$, that implies that $q[m]_q - D \ge \frac{q[m]_q}{2}$, and that $a_D = \left\lfloor \frac{D}{q-1} \right\rfloor \le \frac{D}{2}$. Therefore

$$c\left(\frac{D}{d}\right) = \frac{D(q[m]_q - D) - Da_D}{M} \ge \frac{D\left(\frac{q[m]_q}{2} - \frac{D}{2}\right)}{M} \ge \frac{D\frac{q[m]_q}{4}}{M}.$$

For $q \ge 3$ and $m \ge 2$, we have $\frac{q[m]_q}{4} = \frac{q(q^m-1)}{4(q-1)} \ge 3$, so that the desired inequality is easily satisfied. □

Lemma 5.17 (Property (2))**.** *Suppose A, B, k, j are integers satisfying $0 \le k, j, A, B < d$ so that moreover $k + j \le d - D$ and $A - k, B - j \ge 0$. If $\boxed{D \le \frac{q[m]_q}{2}}$, then*

$$c\left(\frac{A}{d}\right) - c\left(\frac{A-k}{d}\right) + c\left(\frac{B}{d}\right) - c\left(\frac{B-j}{d}\right) \le 1.$$

Proof. Same tricks using Lemmas 5.14 and 5.15. The left-hand side is bounded above by

$$c\left(\frac{k}{d}\right) + c\left(\frac{j}{d}\right) \le c\left(\frac{k+j}{d}\right) + \frac{D}{M} \le c\left(\frac{d-D}{d}\right) + \frac{D}{M}.$$

To show that this quantity is no more that 1, we must prove that

$$(d - D)(q[m]_q - D) - Da_{d-D} + D \overset{?}{\le} M.$$

This inequality is, again, true by a comfortable margin: I claim that

$$(d - D)(q[m]_q - D) + D \le M.$$

Indeed, the left-hand side is

$$\begin{aligned} dq[m]_q - Dq[m]_q - dD + D^2 + D &= q^{m-1}(q-1)\frac{q(q^m-1)}{q-1} - Dq[m]_q - q^m D - q^{m-1}D + D^2 + D \\ &= q^{2m} - q^m - Dq[m]_q - q^m D - q^{m-1}D + D^2 + D, \end{aligned}$$

and the right-hand side is $(q^m - D)(q^m - D - 1) = q^{2m} - q^m - 2Dq^m + D^2 + D$. Canceling like terms and dividing through by D leaves us with

$$-q[m]_q - q^{m-1} \overset{?}{\le} -q^m,$$

which is obviously true, since q^m is already strictly less than $q[m]_q$. □

Lemma 5.18 (Property (3))**.** *Suppose A, B, i, k are integers satisfying $0 \le i, k, A, B < d$ so that moreover*

$i + k \geq d + D$ and $A - i, B - k \geq 0$. Then (with no condition on D),

$$c\left(\frac{A}{d}\right) - c\left(\frac{A-i}{d}\right) + c\left(\frac{B}{d}\right) - c\left(\frac{B-k}{d}\right) \geq 1.$$

Proof. More same tricks. Then left-hand expression is at least

$$c\left(\frac{i}{d}\right) + c\left(\frac{k}{d}\right) - \frac{2D}{M} = \frac{(i+k)(q[m]_q - D) - D(a_i + a_k + 2)}{M};$$

we want to show that the numerator is bounded below by M. The numerator is bounded below by

$$(d + D)q[m]_q - D(i + a_i + k + a_k + 2).$$

As observed earlier, $i + a_i \leq q^m - 1$, and the same for k, so that this quantity is no less than

$$(d + D)q[m]_q - 2Dq^m = q^{2m} - q^m + Dq[m]_q - 2Dq^m.$$

On the other hand, $M = q^{2m} - q^m - 2Dq^m + D^2 + D$. As in the previous lemma, we cancel like terms and divide by D to get the inequality

$$q[m]_q \overset{?}{\geq} D + 1,$$

which is trivially true, since $q[m]_q > q^m = b \geq D + 1$. □

Therefore, the properties in Proposition 5.12 are satisfied. This completes the proof of Theorem 5.2.

5.9 Complements

In this section, we state a more precise version of the growth bound for each of the cases in Theorem 5.2.

Theorem 5.19 (Refinement of Theorem 5.2)**.** *Suppose that $T : \mathbb{F}[y] \to \mathbb{F}[y]$ is an E-filtered recursion operator for some $E > 1$ whose companion polynomial has the shape*

$$X^d + ay^d + (\textit{terms of total degree } \leq d - D)$$

for some $D \geq 1$. Let $b = p^{\lceil \log_p d \rceil}$ is the smallest power of p no less than d.

1. **If d is a power of p,** *then*
$$N_T(y^n) < \frac{(d-D)(d-1)}{E(d-D-1)}\, n^{\log_d(d-D)}.$$

2. **If d is one less than a power of p,** *set $b = d + 1$. Then*
$$N_T(y^n) < \frac{(b-1)^{1-\log_b(b-1)}(b-D)}{E}\, n^{\log_b(b-D)} + \frac{b-2}{E}.$$

3. **If $d = q^{m-1}(q-1)$,** *set $b = q^m$. Then if $D \leq \frac{q[m]_q}{2}$,*
$$N_T(y^n) < \frac{(b-1)(b-D)^2}{E\, d^{\log_b(b-D)}} n^{\log_b(b-D)} + \frac{(b-2)(b-D)}{E}.$$

Proof.

1. If $d = b$ is a power of p, then $c_T = c_{b,D}$. I claim that the proof of Theorem 5.2 can be minimally adapted to show that $c_T(T(f)) \leq c_T(f) - E$. Indeed, by the definition of c_T on $\mathbb{F}[y]$, it suffices to prove this for $f = y^n$ only. Since we're assuming that $\deg T(y^n) \leq n - E$ for $n < b$, and $c_T(n) = n$ on

this range, it's clear that the base case is established. The inductive steps are unchanged, as they only involve comparing a change in $c_T(n)$ with a change in $c_T(e)$ for some $e < n$, rather than an absolute measure of change in $c_T(n)$ Therefore, the claim is established, and $c_T(T(f)) \le c_T(f) - E$.
Finally, since T lowers c_T-value by at least E at each application, we see that $N_T(y^n) \le \frac{c_T(n)}{n}$. The estimate that $c_T(n) = c_{b,D}(n) < \frac{(b-1)(b-D)}{b-1-D} n^{\log_b(b-D)}$ from Lemma 5.5 completes the proof.

2. In this case, with $b = d+1$, we have set $c_T(n) = (b-D-1)\, c_{b,D}\left(\frac{n}{d}\right)$. From Lemma 5.5 and the fact that $c_{b,D}\left(\frac{d-1}{d}\right) = \frac{b-2}{b-D-1}$ is the maximal value of $c_{b,D}$ on fraction less than 1 with denominator d, we know that
$$c_{b,D}\left(\frac{n}{d}\right) < \frac{(b-1)(b-D)}{b-1-D}\left(\frac{n}{b-1}\right)^{\log_b(b-D)} + \frac{b-2}{b-1-D},$$
so that
$$c_T(n) < \frac{(b-1)(b-D)}{(b-1)^{\log_b(b-D)}} n^{\log_b(b-D)} + b - 2 = \Big((b-1)^{1-\log_b(b-1)}(b-D)\Big) n^{\log_b(b-D)} + b - 2.$$
The proof of Theorem 5.2 shows that $c_T(T(f)) \le c_T(f) - E$ for all $f \in \mathbb{F}[y]$. The base case is true because $c_T(n) = n$ for $n < d$, and the inductive step needs no adjustment as before. The claim follows.

3. Here we have set $b = q^m$ and $c_T(n) = (b-D)(b-1-D)\, c_{b,D}\left(\frac{n}{d}\right)$. We bound the growth of c_T:
$$c_T(n) = (b-D)(b-1-D)\, c_{b,D}\left(\frac{n}{d}\right) < \frac{(b-1)(b-D)^2}{d^{\log_b(b-D)}} n^{\log_b(b-D)} + (b-2)(b-D),$$
and note that everything goes through as in the other parts.

□

Finally, we have two more refinements to Theorem 5.1, but they are only refinements of Theorem 5.1 in that neither is formally covered by Theorem 5.2 as stated. In fact, in each case, it is the Theorem 5.2 argument forms the backbone of the proof. The first is a generalization of case (2) of Theorem 5.2.

Corollary 5.20 (to Theorem 5.19)**.** *If $T : \mathbb{F}[y] \to \mathbb{F}[y]$ is a recursion operator that lowers degrees by at least $E \ge 1$ and satisfies the recursion whose companion polynomial has the shape $(X+ay)^d + (\text{terms of total degree} \le d-D)$ for some $D \ge 1$ and $a \in \mathbb{F}$, then*
$$N_T(y^n) \le \frac{(p^k - D)(p^k - 1)}{E(p^k - D - 1)}\, n^{\log_{p^k}(p^k - D)}$$
for any $k \ge \log_p d$.

Proof. Choose k so that $p^k \ge d$. Multiplying the companion polynomial by $(X + cy)^{p^k - d}$ puts us in the power-of-p case of Theorem 5.19. □

And the second is Theorem 5.2 exaclty, for the case where d is any number prime to p.

Theorem 5.21. *Let $T : \mathbb{F}[y] \to \mathbb{F}[y]$ be a degree-lowering recursion operator so that the sequence $\{T(y^n)\}$ satisfies a linear recursion of order d where d is prime to p and such that the companion polynomial has the shape $X^d + ay^d + (\text{terms of total degree} \le d-D)$ for some constant $a \in \mathbb{F}$ and some $D \ge 1$. Let $k = \lceil \log_p d \rceil$, so that $d \le p^k = b$. Then if $\boxed{D < \frac{b}{2}}$, then*
$$N_T(y^n) = O(n^{\log_b(b-D)}).$$

More precisely,

$$N_T(y^n) < \frac{(b-1)(b-D)\big((b-D)^\ell - 1\big)}{d^{\log_b(b-D)}(b-1-D)} n^{\log_b(b-D)} + \frac{(b-1)\big((b-D)^\ell - 1\big)}{b-D-1},$$

where ℓ is the multiplicative order of b modulo d.

The proof of this theorem runs through the same argument as the proof of Theorem 5.2, via Proposition 5.12. It is technically fussy and not particularly interesting, even more so and even less so than case (3) of Theorem 5.2, respectively. See Appendix D for the proof.

Chapter 6

The Hecke recursion

We prove that Hecke operators acting on algebras of modular forms are always *recursion operators*: if T is a Hecke operator and f is a modular form, then the sequence $\{T(f^n)\}_n$ of forms satisfies a linear recursion over the algebra of modular forms. The main proposition is a straightforward generalization of a theorem of Nicolas and Serre about Hecke operators acting on modular forms modulo 2 [23, Théorème 3.1]. It belongs to the same circle of ideas as the theory of the modular equation for j; see, for example, Cox [8, §11.C].

6.1 The general Hecke recursion

Let B be a subalgebra of $\mathbb{C}$ or $\overline{\mathbb{F}}_p$ or $\overline{\mathbb{Q}}_p$. Let $M_k(B) \subset B[\![q]\!]$ be the space of q-expansions of modular forms of level one and weight k, and let $M(B) := \sum_k M_k(B) \subset B[\![q]\!]$ be the algebra of modular forms of level one and all weights.

Lemma 6.1. *For any $f \in M_k(B)$ and any prime $\ell \neq \operatorname{char} B$,*

$$T_\ell(f^m) = \ell^{-1}\Big((\ell^k f_0)^m + f_1^m + \ldots + f_\ell^m\Big), \tag{A}$$

where $f_0 := f(q^\ell)$ and, for $i > 0$, $f_i := f\big(\zeta^i q^{\frac{1}{\ell}}\big)$ for some primitive ℓ^{th} root of unity ζ in $B[\mu_\ell]$.

Equation (A) is an equality of power series in $B[\mu_\ell][\![q^{\frac{1}{\ell}}]\!]$, where μ_ℓ is the set of ℓ^{th} roots of unity.

Proof. The lemma for $m = 1$ follows from considering the effect of T_ℓ on q-expansions: Let $f = \sum a_n q^n$. Then $f_0 = \sum a_n q^{\ell n}$ and $f_i = \sum a_n \zeta^{in} q^{n/\ell}$, so that

$$f_1 + \ldots + f_\ell = \sum_{i=1}^{\ell} \sum_n a_n \zeta^{in} q^{n/\ell} = \sum_n a_n q^{n/\ell} \sum_{i=0}^{\ell} \zeta^{in} = \ell \sum_n a_{\ell n} q^n,$$

where the last equality follows from the fact that $\sum_{i=1}^{\ell} (\zeta^n)^i = \ell$ if ℓ divides n, and 0 otherwise. Since $T_\ell(f) = \sum_n a_{\ell n} q^n + \ell^{k-1} \sum_n a_n q^{\ell n}$ for a form of weight k, the case $m = 1$ is established.

For general m, it suffices to observe that the maps $f \mapsto f^m$ and $f \mapsto f_i$ commute. Applying the lemma for

$m = 1$ to the weight-mk modular form f^m we see that

$$T_\ell(f^m) = \ell^{-1}\Big(\ell^{km}(f^m)_0 + (f^m)_i + \ldots + (f^m)_\ell\Big) = \ell^{-1}\Big((\ell^k f_0)^m + (f_1)^m + \ldots + (f_\ell)^m\Big),$$

as desired. □

Proposition 6.2. *The sequence $\big\{T_\ell(f^n)\big\}_n$ satisfies a linear recursion of order $\ell+1$ over $M(B)$. More precisely, there are modular forms $g_1, \ldots, g_{\ell+1}$, with $g_i \in M_{ik}(B)$, so that for all $n \geq \ell+1$,*

$$T_\ell(f^n) = g_1\, T_\ell(f^{n-1}) + \cdots + g_{\ell+1}\, T_\ell(f^{n-(\ell+1)}) \tag{B}$$

Proof. It is enough to prove the statement for $B = \mathbb{Z}$, so that we can assume that f is a (classical complex-analytic) modular form with integer coefficients.

Lemma 6.1 together with Corollary 4.4 imply that the sequence $\{T_\ell(f^n)\}_n$ satisfies the linear recurrence associated to the polynomial

$$\begin{aligned} P_{\ell,f}(X) &:= (X - \ell^k f_0)(X - f_1)\cdots(X - f_\ell) \\ &= X^{\ell+1} - g_1 X^\ell - g_2 X^{\ell-1} - \cdots - g_\ell X - g_{\ell+1} \qquad \in \mathbb{Z}[\mu_\ell][\![q^{\frac{1}{\ell}}]\!][X]. \end{aligned}$$

It remains to show that the g_i, which are, up to sign, elementary symmetric functions in the f_i, are in fact modular forms of level one and weight ik over $\mathbb{Z}$.

We use the notation of [12]. Recall that the group $\mathrm{GL}_2(\mathbb{Q})^+$ acts on the space of holomorphic functions on the upper half-plane, with the weight-k right action of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ given by

$$\big(f[\gamma]_k\big)(z) = (\det\gamma)^{k-1}\,(cz+d)^{-k}\, f\left(\frac{az+b}{cz+d}\right).$$

Define matrices γ_i for $0, 1, \ldots, \ell$ as follows:

$$\gamma_i := \left(\begin{smallmatrix} 1 & i \\ 0 & \ell \end{smallmatrix}\right) \quad \text{if } i > 0, \qquad\qquad \gamma_0 := \left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

These matrices are known to be a complete set of right coset representatives of $\mathrm{SL}_2(\mathbb{Z})$ in the double coset $\mathrm{SL}_2(\mathbb{Z})\left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$, which defines the T_ℓ operator on forms of level one. And indeed, it is easy to check that, for each i,

$$f_i = \ell\, f[\gamma_i]_k.$$

For any β in $\mathrm{SL}_2(\mathbb{Z})$, the set $\gamma_i\beta$ is also a complete set of right coset representatives for $\mathrm{SL}_2(\mathbb{Z})$ in the T_ℓ-defining double coset. And since f is invariant for the weight-k action of $\mathrm{SL}_2(\mathbb{Z})$, the set

$$f_0[\beta]_k,\ f_1[\beta]_k,\ \ldots,\ f_\ell[\beta]_k$$

is a permutation of the f_is. Therefore, each g_i, which, up to sign, is the i^{th} elementary symmetric function in the f_is, is invariant for the weight-ik action of $\mathrm{SL}_2(\mathbb{Z})$. The holomorphy of g_i comes from the fact that it visibly has a q-expansion. (A priori the expansion is in $q^{\frac{1}{\ell}}$, but we have already shown that g_i is of level one.) Finally, I claim that the g_i are defined over $\mathbb{Z}$, since a priori the q-expansion has coefficients in $\mathbb{Z}[\mu_\ell]$. Indeed, the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ also visibly permutes the f_i, so that the g_is are again invariant, and hence in $M_{ik}(\mathbb{Z})$.

The linear recursion associated to polynomial $P_{\ell,f}$ is precisely equation (B). □

From equation (A), it is clear that the recursion is separable.

Instead of considering $M(B) = \sum_k M(B)$, we may consider the algebra of forms whose weight is a multiple of some particular m. That is, let $M^m(B) = \sum_k M_{km}(B)$. This is still an algebra, and, for $f \in M_{km}(B)$ for some k and m, the sequences $\{f^n\}$ and $\{T_\ell(f^n)\}$ are both in $M^m(B)$, and the recursion polynomial $P_{\ell,f}$ from Proposition 6.2 will be in $M^m(B)[X]$.

For example, if $B = \mathbb{F}_p$ and $m = p-1$, then $M^m(B) = M^0$, the 0-graded part of the space of mod-p modular forms. This is a filtered $\mathbb{F}_p$-algebra (see Example in section 4.4) and the recursion polynomial of T_ℓ acting on powers of f respects that filtration. We restate this in the terminology of Chapter 4:

Proposition 6.3. *For any prime p, the Hecke operator T_ℓ acting on M^0 is a proper filtered separable recursion operator with weights in $\mathbb{F}_p$.*

In the next section, we show that for $p = 2, 3, 5, 7, 13$, this recursion is also *full*.

6.2 Examples of the Hecke recursion

Example 1. Let $B = \mathbb{Z}$. Then $M(\mathbb{Z}) = \mathbb{Z}[E_4, \Delta] \oplus E_6\,\mathbb{Z}[E_4, \Delta]$, and

$$\begin{aligned} P_{2,\Delta} &= X^3 + 48\Delta X^2 + (768\Delta^2 - \Delta E_4^3)X + \Delta^3 \\ &= X^3 + 48\Delta X^2 - (960\Delta^2 + \Delta E_6^2)X + \Delta^3 \in M(\mathbb{Z})[X]. \end{aligned}$$

This example was computed by hand using `SAGE`.

Example 2. The best-known example — $B = \mathbb{C}$ and $f = j$, the modular invariant — falls outside the scope of Proposition 6.2 as stated because j is not holomorphic at the cusp. But everything works the same way, and $P_{\ell,j}$ is the modular equation for j of level ℓ, known to be a two-variable *symmetric* polynomial (in X and j, in our notation) with coefficients in $\mathbb{Z}$. See Cox [8, §11.C].

The computations for $p = 2, 3, 5, 7, 13$ below rely on the data for $P_{\ell,j}$ that Andrew Sutherland has made available online at `http://math.mit.edu/~drew/ClassicalModPolys.html` [6].

Example 3. For $p = 2, 3, 5, 7$, and 13 and $B = \mathbb{F}_p$, it is easy to compute that $M^0 = \mathbb{F}_p[\Delta]$ (see Chapter 8 for details), so that $P_{\ell,\Delta}$ is automatically in $\mathbb{F}_p[\Delta, X]$. Moreover, using Sutherland's data, $P_{\ell,\Delta}$ is very easy to compute: in each case Δ is a rational function of j, so that $P_{\ell,\Delta}$ can be deduced from $P_{\ell,j}$. Specifically, over $\mathbb{F}_p$ for these small p,

$$\Delta = \frac{1}{j + c_p}, \text{ with } c_2 = 0,\ c_3 = 0,\ c_5 = 0,\ c_7 = 1, \text{ and } c_{13} = 8.$$

Therefore

$$P_{\ell,\Delta} = X^{\ell+1}Y^{\ell+1}\,P_{\ell,j}\left(\frac{1}{X} - c_p, \frac{1}{Y} - c_p\right) \in \mathbb{F}_p[X, Y],$$

where we're interpreting both $P_{\ell,j}$ and $P_{\ell,\Delta}$ as polynomials in $\mathbb{F}_p[X, Y]$. As a corollary, $P_{\ell,\Delta}$ is always a symmetric two-variable polynomial.

Example ($p = 2$).

$$P_{3,\Delta} = X^4 + \Delta X + \Delta^4 \quad \text{and} \quad P_{5,\Delta} = X^6 + \Delta^2 X^4 + \Delta^4 X^2 + \Delta X + \Delta^6$$

Example ($p = 3$).

$$P_{2,\Delta} = X^3 - \Delta X + \Delta^3$$
$$P_{7,\Delta} = (X - \Delta)^8 - \Delta X^4 + \Delta^2 X^3 + \Delta^3 X^2 - (\Delta^4 - \Delta)X$$

Example ($p = 5$).

$$\begin{aligned} P_{2,\Delta} &= X^3 + 3\Delta X^2 + (3\Delta^2 - \Delta)X + \Delta^3 \\ P_{11,\Delta} &= X^{12} + 3\Delta X^{11} + \Delta^2 X^{10} + (3\Delta^5 + 2\Delta)X^7 + (4\Delta^6 + 2\Delta^2 + 2\Delta)X^6 + 3\Delta^7 X^5 \\ &\quad + (3\Delta^4 + 2\Delta^3 + \Delta^2 + \Delta)X^4 + (2\Delta^4 + 3\Delta^3 + 4\Delta^2 + 4\Delta)X^3 \\ &\quad + (\Delta^{10} + 2\Delta^6 + \Delta^4 + 4\Delta^3 + 3\Delta^2 + 4\Delta)X^2 \\ &\quad + (3\Delta^{11} + 2\Delta^7 + 2\Delta^6 + \Delta^4 + 4\Delta^3 + 4\Delta^2 + 4\Delta)X + \Delta^{12} \end{aligned}$$

Example ($p = 7$).

$$P_{2,\Delta} = X^3 + 6\Delta X^2 + (6\Delta^2 + 6\Delta)X + \Delta^3$$
$$P_{3,\Delta} = X^4 + (2\Delta^2 + 2\Delta)X^2 + (2\Delta^2 + 6\Delta)X + \Delta^4$$

Example ($p = 13$).

$$P_{2,\Delta} = X^3 + 9\Delta X^2 + (9\Delta^2 - \Delta)X + \Delta^3.$$

Paul Monsky has a number of conjectures about the shape of the polynomial $P_{\ell,\Delta}$ modulo these small primes p. The conjectures, as well as a proof for $p = 2$, are posted in MathOverflow questions 52781* and 153787†

Corollary 6.4. *If $p = 2, 3, 5, 7, 13$, then the recursion operator T_ℓ acting on $M^0 = \mathbb{F}_p[\Delta]$ is* full *in the sense of section 5.5.*‡

Proof. The polynomial $P_{\ell,\Delta} \in \mathbb{F}_p[\Delta][X]$ is symmetric and monic in X, so the $\Delta^{\ell+1}$ term is present. □

Corollary 6.5. *Let $p = 2, 3, 5, 7,$ or 13. Any operator $T \in \widetilde{A}^0 \subset A$ is a proper and full filtered recursion operator on $M^0 = \mathbb{F}_p[\Delta]$.*

Here $\widetilde{A}^0$ is the naïve Hecke algebra on M^0: the algebra of all the polynomials in the T_ℓ. See section 2.2.3 for an extended discussion of this object and its relation to A^0.

Proof. Proposition 6.3, Corollary 6.4, and Proposition 4.24.§ □

Example 4. Let $B = \mathbb{F}_{11}$. The space of modular forms modulo 11 is

$$M = \mathbb{F}_{11}[E_4, E_6]/(E_4E_6 - 1) = \mathbb{F}_{11}[E_4^{\pm 1}].$$

The space is weight-graded $M = \bigoplus_{k \bmod 5} M^{2k}$, with $M^0 = \mathbb{F}_{11}[E_4^{\pm 5}]$ and $M^{2k} = E_4^{3k} M_0$. Finally,

$$P_{2,E_4} = X^3 + 4E_4X^2 + 6E_4^{-2} \in M[X].$$

Note that this recursion is *full*: $E_4^{-2} = E_6^2$, so that $w(E_4^{-2})$ must be 12 since $p - 1 = 10$ and there are no forms of filtration 2.

*`http://mathoverflow.net/questions/52781`: "What's known about the mod 2 reduction of the level ℓ Jacobi modular equation?"

†`http://mathoverflow.net/questions/153787`: "The 'Level N modular equation for delta' in characteristics 3, 5, 7 and 13"

‡I expect T_ℓ to be full in this sense for every p.

§In fact, the operators in $\widetilde{A}^0$ are also separable with weights in $\mathbb{F}_p$, but we do not need this for applications.

6.3 Hecke operators as NROs

In light of Theorem 5.1, we will use the abbreviation ***NRO*** for "nilpotent recursion operator" for a **degree-lowering proper and filtered recursion operator** $T : \mathbb{F}_p[y] \to \mathbb{F}_p[y]$. Then Theorem 5.1 states that if $T : \mathbb{F}_p[y] \to \mathbb{F}_p[y]$ is a full NRO, then $N_T(f) \ll \deg(f)^\alpha$ for $f \in \mathbb{F}_p[y]$. For $p = 2, 3, 5, 7, 13$, we will want to apply Theorem 5.1 to Hecke operators acting on $M^0 = \mathbb{F}_p[\Delta]$. By Corollary 6.5 and Lemma 3.1, a Hecke operator $T \in \widetilde{A}^0$ is a full NRO as soon as T is in every maximal ideal of A^0.

Recall that, if τ is a modular Galois pseudocharacter appearing in M corresponding to system of Hecke eigenvalues $\{\lambda(\ell)\} = \{\tau(\mathrm{Frob}_\ell)\}$, then the operator $T_\ell - \lambda(\ell)$ is in $\mathfrak{m}_\tau$. In general $\lambda(\ell)$ depends on τ, but in two special cases, $T_\ell - \lambda(\ell)$ looks the same on all reducible components:

Lemma 6.6. *Suppose that τ is reducible.*

1. *If $\ell \equiv 1 \bmod p$, then $\tau(\mathrm{Frob}_\ell) = 2$, so that $T'_\ell = T_\ell - 2$.*
2. *If $\ell \equiv -1 \bmod p$, then $\tau(\mathrm{Frob}_\ell) = 0$, so that $T'_\ell = T_\ell$.*

Proof. Direct computation for $\tau = \omega^a(1 + \omega^b)$, noting that b is odd modulo $p - 1$. □

Finding Hecke NROs

In light of Lemma 6.6 and Corollary 6.5, we can list some ways of finding Hecke NROs.

1. If every τ appearing in M is reducible ($p = 2, 3, 5, 7$), then T_ℓ is a full NRO whenever $\ell \equiv -1 \bmod p$. This is the case for every T_ℓ for $p = 2$.
2. If every τ appearing in M is reducible ($p = 2, 3, 5, 7$), then $T_\ell - 2$ is a full NRO whenever $\ell \equiv 1 \bmod p$. This is again the case for every T_ℓ mod 2.
3. Let $\lambda_1, \dots, \lambda_k$ be a complete list of systems of eigenvalues appearing in M^0. For every ℓ, the operator $T'_\ell = \prod_i (T_\ell - \lambda_i(\ell))$ is a full NRO.
4. Let $\lambda_1, \dots, \lambda_k$ be a complete list of systems of eigenvalues appearing in M^0. For every ℓ, the operator $T''_\ell = \prod_i{}' (T_\ell - \lambda_i(\ell))$, where we restrict the product to a subset of $1, \dots, i, \dots k$ with $\lambda_i(\ell)$ distinct, is a full NRO. Moreover, T'' is never in $\mathfrak{m}_\tau^2$.
5. More conceptually, let $\lambda_1, \dots, \lambda_k$ again be a complete system of eigenvalues appearing in M^0. For each i, let $\mathfrak{m}_i$ be the ideal corresponding to λ_i, and find generators $T_1^i, \dots, T_{m_i}^i$ for $\mathfrak{m}_i$ so that each T_j^i is in $\widetilde{A}^0$. (This can always be done because $\widetilde{A}^0$ is dense in A^0.) Moreover, for each i, find an "approximate idempotent" $E_i \in \widetilde{A}^0$ with the property that $E_i \in \mathfrak{m}_j$ for $j \neq i$ and $E_i \equiv 1$ in $A_{\mathfrak{m}_i}/\mathfrak{m}_i$. (Again, this can always be done by lifting true idempotents of $\prod A_{\mathfrak{m}_j}/\mathfrak{m}_j$.) Then the set
$$\{E_i T_j^i : 1 \leq j \leq m_i\}$$
consists of full NROs with the additional property that they generate each $\mathfrak{m}_i$.

We will use full NROs of type (1), (2), and (5) in Chapter 8.

Chapter 7

Generators of reducible local components of the Hecke algebra

In this chapter, we assume that τ is reducible and describe an algorithm to find modified Hecke operators T'_ℓ that generate the maximal ideal $\mathfrak{m}_\tau$ of the local component of the Hecke algebra. We are particularly interested in the question of finding generators for multiple A_τ simultaneously.

We will prove the following theorem:

Theorem 7.1. *Suppose Vandiver's conjecture holds for p. Then there exist infinitely many pairs of primes (ℓ_+, ℓ_-) with $\ell_\pm \equiv \pm 1 \bmod p$ so that for every* reducible *modular pseudocharacter $\tau : G_{\mathbb{Q},p} \to \mathbb{F}_p$, the ideal $\mathfrak{m}_\tau$ of A_τ is generated by $T_{\ell_+} - 2$ and T_{ℓ_-}.*

Without assuming Vandiver's conjecture, we can only guarantee that $T_{\ell_+} - 2$ and T_{ℓ_-} are linearly independent in $\mathfrak{m}_\tau/\mathfrak{m}_\tau^2$, so part of a generating set of $\mathfrak{m}_\tau$.

The theorem is proved in section 7.4.

Notation review

We use the notation of Chapter 2, and especially Section 2.5. The most important notation is recalled below.

- A_τ is a local component of the shallow Hecke algebra acting on modular forms modulo p. Its maximal ideal $\mathfrak{m}_\tau$ corresponds to a modular Galois pseudocharacter τ of the Galois group $G = G_{\mathbb{Q},p}$ defined over $\mathbb{F}$, a finite extension of $\mathbb{F}_p$.
- D_τ is the functor that takes $\mathbb{F}$-algebras B to the set of odd, constant-determinant deformations $\widetilde{\tau} : G \to B$ of the pseudocharacter τ. That is, the constraints are $\widetilde{\tau}(c) = 0$ for complex conjugation $c \in G$ (automatic for $p > 2$ since τ itself is odd) and $\det \widetilde{\tau} = \det \tau$.
- $(R_\tau, \mathfrak{m}_{R_\tau})$ is the complete local noetherian $\mathbb{F}$-algebra representing D_τ, equipped with universal deformation $\widetilde{\tau}_\tau : G \to R_\tau$.
- ℓ always refers to a prime different from p. It parametrizes Hecke operators $T_\ell \in A_\tau$ and *modified*

Hecke operators $T'_\ell = T_\ell - \tau(\mathrm{Frob}_\ell) \in \mathfrak{m}_\tau$. It also parametrizes elements $t_\ell = \widetilde{\tau}(\mathrm{Frob}_\ell) \in R_\tau$ and $t'_\ell = t_\ell - \tau(\mathrm{Frob}_\ell) \in \mathfrak{m}_{R_\tau}$ of the universal deformation ring that map to T_ℓ and T'_ℓ, respectively.

A word of warming: the symbol Δ will, *in this chapter only*, refer not to the modular form or its residual q-series, but to the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

7.1 The algorithm for $p > 2$

The algorithm presented below is inspired by Bellaïche's treatment of the case $p = 3$ in [5, appendix]. It uses his prior work on pseudodeformations in [3] as well as mild extensions in [5, Section 10]. We assume that $p > 2$ and that Vandiver's conjecture holds for p. For $p = 2$, see section 7.5 below.

Any reducible pseudocharacter has the form $\omega^a(1 + \omega^b)$ for some a and b defined modulo $p - 1$. Note that $\mathbb{F} = \mathbb{F}_p$ in this case.

Recall that we have a surjection $R_\tau \twoheadrightarrow A_\tau$ (described in section 2.5.2). By Nakayama's lemma, computing generators for $\mathfrak{m}_\tau$ is equivalent to finding a basis for the cotangent space $\mathfrak{m}_\tau/\mathfrak{m}_\tau^2$. Fortunately we have access to its dual, the tangent space

$$\left(\mathfrak{m}_{R_\tau}/\mathfrak{m}_{R_{\bar\tau}}^2\right)^* = \mathrm{Hom}(\mathfrak{m}_{R_\tau}/\mathfrak{m}_{R_\tau}^2, \mathbb{F}_p) = \mathcal{D}_\tau(\mathbb{F}_p[\varepsilon]).$$

We will find $\widetilde{\tau}_+$ and $\widetilde{\tau}_-$ in $\mathcal{D}_\tau(\mathbb{F}_p[\varepsilon])$, with $\widetilde{\tau}_-$ *reducible* and $\widetilde{\tau}_2$ *irreducible* lifts of τ to $\mathbb{F}_p[\varepsilon]$, thus necessarily linearly independent (Theorem 2 and Proposition 2 in [3], but clear in our case from analysis below). Vandiver's conjecture allows us to assume that $\dim_{\mathbb{F}_p} \mathcal{D}_\tau = 2$, so that the two deformations that we find will form a basis (Proposition 2.15).

Once we have a basis for the tangent space, we can find a basis for the cotangent space $\mathfrak{m}_{R_\tau}/\mathfrak{m}_{R_\tau}^2$. More precisely, we will show that it is possible to find primes ℓ_- and ℓ_+ satisfying

Basis conditions

- $\widetilde{\tau}_-(\mathrm{Frob}_{\ell_-})$ nonconstant, so $f_-(t'_{\ell_-})$ nonzero
- $\widetilde{\tau}_+(\mathrm{Frob}_{\ell_+})$ nonconstant, so $f_+(t'_{\ell_+})$ nonzero
- $\widetilde{\tau}_-(\mathrm{Frob}_{\ell_+})$ constant, so $f_-(t'_{\ell_+}) = 0$

Here f_- and f_+ are the maps $\mathfrak{m}_{R_\tau}/\mathfrak{m}_{R_\tau}^2 \to \mathbb{F}_p$ induced by maps $R \to \mathbb{F}_p[\varepsilon]$ corresponding to deformations $\widetilde{\tau}_-$ and $\widetilde{\tau}_+$, respectively.

It is now clear that the images of t'_{ℓ_-} and t'_{ℓ_+} will form a basis for $\mathfrak{m}_{R_\tau}/\mathfrak{m}_{R_\tau}^2$. By Nakayama's lemma, they generate $\mathfrak{m}_{R_\tau}$. Finally, the surjection $R_{\bar\tau} \twoheadrightarrow A_{\bar\tau}$ will imply that T'_{ℓ_-} and T'_{ℓ_+} generate $\mathfrak{m}_\tau$ as an ideal, and hence all of A_τ topologically as an algebra.

We now describe how to find $\widetilde{\tau}_-$ and $\widetilde{\tau}_+$ for $\tau = 1 + \omega^b$. Once we find these, we can use them to deform $\omega^a(1 + \omega^b)$: namely, $\omega^a\,\widetilde{\tau}_-$ and $\omega^a\,\widetilde{\tau}_+$ will be the corresponding deformations for $\omega^a(1 + \omega^b)$. However, since we are mainly concerned with whether $\widetilde{\tau}_\pm(g)$ is nonconstant, the particular deformations are irrelevant. If we find $\ell_\pm$ so that $T'_{\ell_\pm}$ generate $\mathfrak{m}_\tau$, the same $\ell_\pm$ will work for $\mathfrak{m}_{\omega^a\,\tau}$ (and the Hecke algebras are isomorphic: Proposition 2.41).

7.2 The reducible deformation $\widetilde{\tau}_-$

The group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^2})/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})^\times$, which sits in an exact sequence

$$1 \to (1+p\mathbb{Z})/p^2\mathbb{Z} \to (\mathbb{Z}/p^2\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to 1.$$

This sequence splits via a mod-p^2 Teichmüller lift, so that $(\mathbb{Z}/p^2\mathbb{Z})^\times$ projects onto $(1+p\mathbb{Z})/p^2\mathbb{Z}$, which we can identify with $\mathbb{Z}/p\mathbb{Z}$. This gives an additive character $\alpha : \mathrm{Gal}(\mathbb{Q}(\mu_{p^2})/\mathbb{Q}) \to \mathbb{F}_p$.

Then $\chi_\alpha := 1 + \alpha\varepsilon$ is a deformation of the trivial character $G_{\mathbb{Q},p} \to \mathbb{F}_p[\varepsilon]^\times$, and

$$\widetilde{\tau}_\alpha := \chi_\alpha + \omega^b\, \chi_{-\alpha}$$

is a reducible deformation of τ with determinant $\det\tau$. Let $\widetilde{\tau}_- := \tau_\alpha$.

It remains to understand the primes ℓ so that $\widetilde{\tau}_-(\mathrm{Frob}_\ell)$ is nonconstant, that is, has a nonzero ε-part. For any g,

$$\begin{aligned}\widetilde{\tau}_-(g) &= 1 + \varepsilon\alpha(g) + \omega^b(g)(1-\varepsilon\alpha(g)) \\ &= \big(1+\omega^b(g)\big) + \varepsilon\,\alpha(g)\,\big(1-\omega^b(g)\big).\end{aligned}$$

We are looking for elements $g = \mathrm{Frob}_\ell$ so that *both* $\alpha(g) \neq 0$ and $\omega^b(g) \neq 1$. The kernel of α is those $g \in G$ whose order in $\mathrm{Gal}(\mathbb{Q}(\mu_{p^2})/\mathbb{Q})$ is prime to p. In other words, $\alpha(\mathrm{Frob}_\ell) \neq 0$ if and only if $\ell^{p-1} \neq 1 \bmod p^2$.

Corollary 7.2. *With $\widetilde{\tau}_-$ as above, $\widetilde{\tau}_-(\mathrm{Frob}_\ell)$ is nonconstant if and only if both*

$$\ell^b \neq 1 \bmod p \text{ and } \ell^{p-1} \neq 1 \bmod p^2.$$

Note that any $\ell \equiv -1 \bmod p$ but not congruent to -1 modulo p^2 will satisfy these requirements. Indeed, if $\ell \equiv -1+ap \bmod p^2$ then $\ell^{p-1} \equiv 1+ap \bmod p^2$, which is congruent to -1 modulo p^2 if and only if p divides a.

7.3 The irreducible deformation $\widetilde{\tau}_+$

This construction is a little more involved. In the first two sections, we discuss some cohomological preliminaries; $\widetilde{\tau}_+$ is constructed in section 7.3.2.

7.3.1 The cohomology of ω^k

Reflection principle preliminaries

Recall that $G = G_{\mathbb{Q},p} = \mathrm{Gal}(\mathbb{Q}^p/\mathbb{Q})$, where $\mathbb{Q}^p$ is the maximal extension of $\mathbb{Q}$ unramified outside p and ∞. Let $K = \mathbb{Q}(\mu_p)$ and $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, and $H \subset G$ be the kernel of the quotient map $G \twoheadrightarrow \Delta$ so that $H = \mathrm{Gal}(\mathbb{Q}^p/K)$. Finally, let $\mathfrak{p}$ be the prime of K above (p), and $E \subset K^\times$ the group of elements that are units away from $\mathfrak{p}$.

For any $\mathbb{F}_p[\Delta]$-module A, we write $A[\omega^k]$ for the subspace on which Δ acts through ω^k. Since the order of Δ is prime to p, there is always a decomposition $A = \bigoplus_{k=0}^{p-2} A[\omega^k]$.

Let $\widetilde{K}$ be the maximal abelian exponent-p extension of K inside $\mathbb{Q}^p$, and $\widetilde{\Gamma} = \mathrm{Gal}(\widetilde{K}/K)$, an elementary p-group. By Kummer theory, abelian exponent-p extensions of K are obtained by adjoining p^{th} roots of

There is a mistake here: in the case that p is an irregular prime, the maximal elementary-p extension of K unramified outside p will not be generated by p^th roots of p-units. One also needs to include p-torsion in the class group, which corresponds to extensions generated by p^th roots of elements whose valuations at every prime of K (except possibly the one above p) are all divisible by p. However this ends up not mattering when looking for odd Delta-eigenspaces.

representatives in $K^\times/(K^\times)^p$. Restricting to extensions unramified outside p forces $\widetilde{K}$ to be obtained by adjoining representatives of E/E^p. By a refinement of the Dirichlet unit theorem (for example, Washington [31, Proposition 8.10]),

$$\dim_{\mathbb{F}_p} E/E^p[\omega^k] = \begin{cases} 1 & \text{if } k \equiv 1 \text{ or } k \text{ is even modulo } (p-1) \\ 0 & \text{otherwise.} \end{cases}.$$

Since $\widetilde{K}$ is a Kummer extension of $\mathbb{Q}(\mu_p)$, it is Galois over $\mathbb{Q}$ and Δ acts on $\widetilde{\Gamma}$ by conjugation:

$$1 \to \widetilde{\Gamma} \to \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \to \Delta \to 1$$

Therefore $\widetilde{\Gamma}$ also breaks up into Δ-eigenspaces: $\widetilde{\Gamma} = \bigoplus_k \widetilde{\Gamma}[\omega^k]$. This decomposition is closely connected to the decomposition of E/E^p. For $k = 1$ or k even, choose $\alpha \in K$ representing $E/E^p[\omega^k]$. Then $K(\alpha^{\frac{1}{p}})$ is contained in $\widetilde{K}$ and is Galois over $\mathbb{Q}$. Therefore $\Gamma_\alpha := \mathrm{Gal}(K(\alpha^{\frac{1}{p}})/K)$ is a Δ-eigenspace inside $\widetilde{\Gamma}$.

Proposition 7.3. $\Gamma_\alpha = \widetilde{\Gamma}[\omega^{1-k}]$

Proof. Washington, [31, section 10.2]. This is a special case of the reflection principle. There is a Δ-equivariant perfect pairing

$$\widetilde{\Gamma} \times E/E^p \to \mu_p$$
$$\langle \gamma, u \rangle \mapsto \frac{\gamma\left(u^{\frac{1}{p}}\right)}{u^{\frac{1}{p}}}.$$

The pairing restricts to a perfect pairing of Δ-eigenspaces

$$\widetilde{\Gamma}[\omega^j] \times E/E^p[\omega^k] \to \mu_p$$

if and only if $j + k \equiv 1 \bmod (p-1)$. Since Γ_α permutes the p^{th} roots of α, we are forced to conclude that $\Gamma_\alpha = \widetilde{\Gamma}[\omega^{1-k}]$. □

Explicit cocycle for ω^k

Switch of notation. Suppose k is odd modulo $p-1$. Choose $\alpha \in E$ representing $E/E^p[\omega^{1-k}]$. Recall that we let $\Gamma_\alpha = \mathrm{Gal}(K(\alpha^{\frac{1}{p}})/K)$, and Δ acts on Γ through ω^k. Let $G_\alpha = \mathrm{Gal}(K(\alpha^{\frac{1}{p}})/\mathbb{Q})$.

Proposition 7.4. *The map $c_k : G_\alpha \to \mathbb{F}_p$ defined by, for $g \in \Gamma_\alpha$,*

$$c_k(g) = \frac{g(\alpha^{\frac{1}{p}})}{\alpha^{\frac{1}{p}}}$$

extends uniquely to a nonzero element of $H^1(G_\alpha,\ \omega^k) \xrightarrow{\inf}_{\sim} H^1(G,\ \omega^k)$.

Vandiver's conjecture for p implies that $\dim H^1(G,\ \omega^k) = 1$, so that this cocycle generates (Proposition 2.15).

Proof. By inflation-restriction we have an exact sequence

$$0 \to H^1\big(\Delta, (\omega^k)^H\big) \to H^1(G, \omega^k) \xrightarrow{\text{res}} H^1(H, \omega^k)^\Delta \to H^2\big(\Delta, (\omega^k)^H\big).$$

The second and last term are both 0, since Δ has order $p-1$, so that all of its cohomology groups over $\mathbb{F}_p$

are trivial. Moreover, since H acts trivially on ω, we know that $H^1(H,\omega^k)^\Delta = \mathrm{Hom}_\Delta(H,\omega^k)$, so that

$$H^1(G,\ \omega^k) \xrightarrow{\text{res}}{\sim} \mathrm{Hom}_\Delta(H,\ \omega^k) = \mathrm{Hom}_\Delta(\widetilde{\Gamma},\ \omega^k) = \mathrm{Hom}(\Gamma_\alpha,\ \mathbb{F}_p).$$

Here the first equality is from the exact sequence, the second is $\mathbb{F}_p(\omega^k)$ is an abelian group of exponent p, and the third is due to the fact that $\widetilde{\Gamma}[\omega^k] = \Gamma_\alpha$.

Therefore $H^1(G,\ \omega^k)$ factors through $G_\alpha = \mathrm{Gal}(K(\alpha^{\frac{1}{p}})/\mathbb{Q})$, and the definition of c_k on the subgroup $\Gamma_\alpha \subset G_\alpha$ is exactly as claimed. From the cohomological exact sequence we already know that c_k must extend uniquely to Γ_α.

□

Corollary 7.5. *Suppose c is a cocycle representing an element of $H^1(G,\ \omega^k)$ in the same line as c_k, defined in Proposition 7.4. If $g \in G$ is an element whose image in G_α is a nontrivial element of Γ_α, then $c(g) \neq 0$.*

Proof. Since $H^1(G,\ \omega^k)$ factors through G_α, we may as well assume that $1 \neq g \in \Gamma_\alpha$. It's clear that $c_k(g) \neq 0$. Changing c_k by a coboundary means adding $a(\omega^k(g)-1)$ for some $a \in \mathbb{F}_p$. But $\omega^k\big|_{\Gamma_\alpha} = 1$, so that $c(g)$ is still nonzero. □

7.3.2 Constructing $\widetilde{\tau}_+$

We now construct $\widetilde{\tau}_+$ for $\tau = \omega^b + 1$. We make a guess and prove that our guess is a constant-determinant pseudocharacter deforming τ. In fact, $\widetilde{\tau}_+$ is the trace of an irreducible representation of $G_{\mathbb{Q},p}$ over $\mathbb{F}_p[\varepsilon]$; this more conceptual construction is given in Appendix E. In either case, we use the ideas of [3] and [5, section 10], but both constructions are self-contained.

We use the notation of the previous section. Let α and β be nonzero representatives in $E/E^p[\omega^{1-b}]$ and $E/E^p[\omega^{1+b}]$, respectively. These exist because b is odd mod $p-1$, but note that they may coincide if $b = \frac{p+1}{2}$ (so only if $p \equiv 3 \bmod 4$). Using Proposition 7.3.1, we obtain cocycles $c_b \in H^1(G,\ \omega^b)$, factoring through $K(\alpha^{\frac{1}{p}})$, and $c_{-b} \in H^1(G,\ \omega^{-b})$, factoring through $K(\beta^{\frac{1}{p}})$.

Recall that $\mathcal{D}_\tau$ is the functor that takes profinite $\mathbb{F}$-algebras B to the set of deformations $\widetilde{\tau} : G \to B$ with constant determinant $\det\widetilde{\tau} = \det\tau$ (the oddness condition is automatic for $p > 2$). Also let $\mathcal{D}_\tau^{\mathrm{red}} \subset \mathcal{D}_\tau$ be the subfunctor of *reducible* deformations $\widetilde{\tau}$. Then there is an exact sequence (see [3, Theorem 2] and [5, Proof of Proposition 20] and Proposition 2.15)

$$0 \to \mathcal{D}_t^{\mathrm{red}}(F[\varepsilon]) \to \mathcal{D}_t(F[\varepsilon]) \to \mathrm{Ext}^1_G(1,\omega^b) \otimes \mathrm{Ext}^1_G(\omega^b,1) \to \mathrm{Ext}^2_G(\omega^b,\omega^b) \oplus \mathrm{Ext}^2_G(1,1) = 0.$$

Here the last arrow is the Yoneda product in both directions. The space $\mathcal{D}_t^{\mathrm{red}}(F[\varepsilon])$ is one-dimensional, generated by $\widetilde{\tau}_-$ (see section 7.2). Assuming Vandiver's conjecture, both $\mathrm{Ext}^1_G(1,\omega^b)$ and $\mathrm{Ext}^1_G(\omega^b,1)$ are one-dimensional as well, generated by cocycles c_b and $\omega^b\, c_{-b}$, respectively. These satisfy cocycle conditions

$$c_b(gh) = c_b(g) + \omega^b c_b(h) \tag{A}$$

$$c_{-b}(gh) = c_{-b}(g) + \omega^{-b} c_{-b}(h). \tag{B}$$

Moreover, since $\mathrm{Ext}^2_G(\omega^b,\omega^b) = 0$, we can find a 1-cochain $X : G \to \mathbb{F}$ whose boundary is $c_b \cup \omega^b c_{-b}$:

$$c_b(g)\omega^b(h)c_{-b}(h) = \omega^b(g)X(h) + X(g)\omega^b(h) - X(gh). \tag{C}$$

Similarly, we can find $Y : G \to \mathbb{F}$ whose boundary is $\omega^b c_{-b} \cup c_b \in \mathrm{Ext}^2_G(1,1) = 0$:

$$\omega^b(g)c_{-b}(g)c_b(h) = Y(g) + Y(h) - Y(gh). \tag{D}$$

The X and Y that we have found are not unique: for example, it's clear that Y may be altered by adding an additive character of G, and X by adding an additive character twisted by ω^b.

Proposition 7.6.

1. *The map $\alpha : G \to \mathbb{F}_p$ given by*

$$\alpha = \omega^{-b}X + Y + c_b c_{-b} : G \to \mathbb{F}_p$$

is an additive character of G to $\mathbb{F}_p$.

2. *The two maps $t : G \to \mathbb{F}_p[\varepsilon]$ given by*

$$t = 1 + \omega^b + \varepsilon(X + Y)$$
$$t^0 = t\left(1 - \frac{\varepsilon}{2}\alpha\right),$$

are both pseudocharacter lifts of τ to $\mathbb{F}_p[\varepsilon]$. Moreover $\det t^0 = \det \tau$.

See section 2.4.1 for definitions.

Proof. α **is an additive character:** This is a many-term identity that uses all of the identities (A), (B), (C), and (D).

$$\begin{aligned}
&\alpha(gh) - \alpha(g) - \alpha(h) \\
&\quad = \omega^{-b}(gh)X(gh) + Y(gh) + c_b(gh)c_{-b}(gh) - \omega^{-b}(g)X(g) - Y(g) \\
&\qquad\qquad - c_b(g)c_{-b}(g) - \omega^{-b}(h)X(h) - Y(h) - c_b(h)c_{-b}(h) \\
&\quad = \cdots = 0
\end{aligned}$$

Since the defining identity (D) for Y is unchanged if Y is altered by an additive character, and the defining identity for X is unchanged if we add ω^b times an additive character, we see that t^0 is just t for another choice of X and Y:

$$\begin{aligned}
t^0 = t\left(1 - \tfrac{\varepsilon}{2}\ \alpha\right) &= t - \tfrac{\varepsilon}{2}\alpha - \tfrac{\varepsilon}{2}\omega^b\alpha \\
&= \tau + \varepsilon\left(Y - \frac{\alpha}{2}\right) + \varepsilon\left(X - \omega^b\frac{\alpha}{2}\right).
\end{aligned}$$

Therefore anything that is true for t that follows formally from the identities (A), (B), (C), and (D) is also true for t^0, and vice versa.

Now we prove that t and t^0 are pseudocharcter lifts of τ to $\mathbb{F}_p[\varepsilon]$. They are certainly lifts of τ.

Identity maps to 2: From equations (C) and (D) we see that X and Y restricted to *either* $\mathrm{Gal}(\mathbb{Q}^p/K(\alpha^{\frac{1}{p}}))$ or $\mathrm{Gal}(\mathbb{Q}^p/K(\beta^{\frac{1}{p}}))$ become homomorphism from either group to $\mathbb{F}_p$. Therefore both X and Y factor through some exponent-p extension of $K(\alpha^{\frac{1}{p}}, \beta^{\frac{1}{p}})$; in particular $X(1) = Y(1) = 0$, so that $t(1) = 2$. Similarly, 1-cocycles always satisfy $c(1) = 0$, so that $t^0(1) = 2$.

Centrality: The sum of the identities (C) and (D) show that $X + Y$ is central. Therefore t, and hence t^0 is central as well.

Constant determinant for t^0: We compute $\det t$:

$$\begin{aligned}(\det t)(g) &= \frac{t(g)^2 - t(g^2)}{2} = \frac{1}{2}\Big(\big(1+\omega^b(g)+\varepsilon X(g)+\varepsilon Y(g)\big)^2 - 1 - \omega^b(g^2) - \varepsilon X(g^2) - \varepsilon Y(g^2)\Big)\\ &= \omega^b(g) + \frac{\varepsilon}{2}\big(2X(g)+2Y(g)+2\omega^b(g)X(g)+2\omega^b(g)Y(g) - X(g^2) - Y(g^2)\big)\\ &= \omega^b(g) + \varepsilon\Big(X(g) + \omega^b(g)Y(g) + \omega^b(g)\, c_b(g)c_{-b}(g)\Big)\\ &= (\det\tau)(g)\,\big(1+\varepsilon\alpha(g)\big),\end{aligned}$$

where we've used both identities (C) and (D) with $(g,h) = (g,g)$. It follows that d is multiplicative, since α is an additive character. Moreover, is easy to check using the definition of det that, if t is any map and χ is a (multiplicative) character, then $\det(\chi t) = \chi^2 \det t$. Therefore

$$\det(t^0) = \det(t)\left(1 - \frac{\varepsilon}{2}\alpha\right)^2 = (\det\tau)(1+\varepsilon\alpha)(1-\varepsilon\alpha) = \det\tau$$

as desired.

Trace-determinant identity: It is also easy to check that, if χ is a multiplicative character, then the trace-determinant identity for t holds if and only if the trace-determinant identity holds for χt.

So it suffices to see that $t(gh) + d(g)t(g^{-1}h) = t(g)t(h)$ for all g, h. This is a completely straightforward but even longer computation using identities (C) and (D) with $(g,h) = (g^{-1},h)$. □

Set $\widetilde{\tau}_+ := t^0$, and make the change $Y \mapsto Y - \frac{\alpha}{2}$ and $X \mapsto X - \omega^b\frac{\alpha}{2}$ so that $\widetilde{\tau}_+$ is still of the form $\widetilde{\tau}_+ = \tau + \varepsilon(X+Y)$ where X and Y satisfy identities (C) and (D), but now additionally the ε-component of the determinant is zero, so that

$$\omega^b Y + X = -\omega^b c_b\, c_{-b}. \tag{E}$$

In other words, the new $\alpha = 0$.

7.3.3 Analyzing $\widetilde{\tau}_+$

If $g \in G = G_{\mathbb{Q},p}$ fixes either $K(\alpha^{\frac{1}{p}})$ or $K(\beta^{\frac{1}{p}})$, then at least one of c_b or c_{-b} must be zero, and certainly $\omega^b(g) = 1$. From equation E we see that

$$X + Y = 0 \ \text{ on } \ \mathrm{Gal}\left(\mathbb{Q}^p/K(\alpha^{\frac{1}{p}})\right) \cup \mathrm{Gal}\left(\mathbb{Q}^p/K(\beta^{\frac{1}{p}})\right)$$

(that's a union of two subgroups). Conversely, if $\omega^b(g) = 1$ and g moves both $\alpha^{\frac{1}{p}}$ and $\beta^{\frac{1}{p}}$, then both $c_b(g)$ and $c_{-b}(g)$ are nonzero, so that, by equation E again,

$$X + Y \neq 0 \ \text{ on } \ \mathrm{Gal}(\mathbb{Q}^p/K) - \Big(\mathrm{Gal}\left(\mathbb{Q}^p/K(\alpha^{\frac{1}{p}})\right) \cup \mathrm{Gal}\left(\mathbb{Q}^p/K(\beta^{\frac{1}{p}})\right)\Big). \tag{F}$$

We have proved

Proposition 7.7. *There is an irreducible constant-determinant deformation $\widetilde{\tau}_+ : G \to \mathbb{F}_p[\varepsilon]$ of $\tau = \omega^b + 1$ that satisfies the following:*

If g generates both $\Gamma_\alpha = \mathrm{Gal}(K(\alpha^{\frac{1}{p}})/K)$ and $\Gamma_\beta = \mathrm{Gal}(K(\beta^{\frac{1}{p}})/K)$, then $\widetilde{\tau}_+(g)$ is nonconstant.

Here α and β are two p-units whose images in E/E^p are in the ω^{1-b}- and ω^{1+b}-eigenspace, respectively.

Corollary 7.8. *If $\ell \equiv 1 \bmod p$ is a prime so that neither α nor β are p^{th} powers in $\mathbb{F}_\ell$, then $\widetilde{\tau}_+(\text{Frob}_\ell)$ is nonconstant.*

We justify the statement of the corollary: $\ell \equiv 1 \bmod p$, then ℓ splits completely in K, so that the residue field of a prime λ lying over ℓ in $\mathcal{O}_K$ is $\mathbb{F}_\ell$. Therefore we can view elements α and β of K in $\mathbb{F}_\ell$. For $\ell \equiv 1 \bmod p$, there are $\frac{\ell-1}{p}$ perfect p^{th} powers in $\mathbb{F}_\ell$.

Proof of Corollary 7.8. We translate the condition that $g = \text{Frob}_\ell$ generates $\text{Gal}(K(\alpha^{\frac{1}{p}})/K)$ into a statement about ℓ. First of all, we must have $\ell \equiv 1 \bmod p$; otherwise, Frob_ℓ won't be in $\text{Gal}(\mathbb{Q}^p/K)$. If λ is a prime of K lying over ℓ, then the action of $\text{Frob}_\ell = \text{Frob}_\lambda$ on $\alpha^{\frac{1}{p}}$ is uniquely defined by the congruence

$$\text{Frob}_\lambda(\alpha^{\frac{1}{p}}) \equiv \left(\alpha^{\frac{1}{p}}\right)^\ell \mod \lambda.$$

An element of $\overline{\mathbb{F}}_\ell$ is in $\mathbb{F}_\ell$ if and only if it is fixed by the ℓ^{th} power map. And Frobenius elements modulo unramified primes of an extension lift to characteristic zero uniquely. The claim follows. □

If α and β are obviously elements of $\mathbb{F}_\ell$ (if they are represented by integers, for example), then the condition that $\ell \equiv 1 \bmod p$ in Corollary 7.8 is superfluous: if $\ell \not\equiv 1 \bmod 5$ then every element of $\mathbb{F}_\ell$ is a perfect p^{th} power.

Finally, we note that the Chebotarev density theorem guarantees that we can always find such ℓ. Their density is $\frac{p-1}{p^2}$ if $\alpha \neq \beta$ and $\frac{1}{p}$ otherwise.

7.4 The takeaway for $p > 2$

We have now constructed two deformations $\widetilde{\tau}_-$ and $\widetilde{\tau}_+$ of $\tau = 1 + \omega^b$ and proved that they satisfy the following:

- $\widetilde{\tau}_-(\text{Frob}_\ell)$ is nonconstant if and only if $\ell^b \neq 1 \bmod p$ and $\ell^{p-1} \neq 1 \bmod p^2$
- If $\ell \equiv 1$ and α and β are not p^{th} powers in $\mathbb{F}_\ell$, then $\widetilde{\tau}_+(\text{Frob}_\ell)$ is nonconstant.
  Here α and β are two elements of $\mathbb{Q}(\mu_p)$ depending on b.

It is clear that if we choose $\ell_- \equiv -1$ modulo p but not modulo p^2, and $\ell_+ \equiv 1$ modulo p satisfying the additional condition on α and β, then ℓ_- and ℓ_+ satisfy the basis conditions from p. 76. Therefore T'_{ℓ_-} and T'_{ℓ_+} will generate $\mathfrak{m}_\tau$ and hence A_τ.

7.4.1 Examples

Example ($p = 3$)**.** The case $p = 3$ is done in [5, appendix], but we repeat it here for completeness. For $p = 3$, the only possible reducible τ is $1 + \omega$, so that $b = 1$. Therefore,

$$\begin{aligned}\ell_- &\in \{\ell : \ell \not\equiv 1 \bmod 3,\ \ell^2 \not\equiv 1 \bmod 9\} = \{\ell : \ell \equiv 2 \bmod 3,\ \ell \not\equiv -1 \bmod 9\} \\ &= \{2,\ 5,\ 11,\ 23,\ 29,\ 41,\ 47,\ 59,\ 83,\ 101,\ 113,\ 131 \ldots\}.\end{aligned}$$

To find ℓ_+ we need 3-units of $\mathbb{Q}(\mu_3)$ on which $\mathrm{Gal}(\mathbb{Q}(\mu_3)/\mathbb{Q})$ acts through $\omega^{1\pm b} = 1$ mod third powers. So we can take $\alpha = \beta = 3$. Therefore

$$\begin{aligned}\ell_- &\in \{\ell : \ell \equiv 1 \bmod 3,\ 3 \text{ is not a perfect cube mod } \ell\} \\ &= \{7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 79,\ 97,\ 109,\ 127, \ldots\}\end{aligned}$$

The smallest pair is $(\ell_- = 2,\ \ell_+ = 7)$.

Example $(p = 5)$**.** For $p = 5$, there are a priori two τs, $1 + \omega$ and $1 + \omega^3$, but they are ω-twists of each other. So $b = \pm 1$. (And indeed, the construction of both ℓ_- and ℓ_+ the same for $\pm b$.) Therefore,

$$\begin{aligned}\ell_- &\in \{\ell : \ell \not\equiv 1 \bmod 5,\ \ell^4 \not\equiv 1 \bmod 25\} = \{\ell : \ell \not\equiv 1 \bmod 5,\ \ell \not\equiv \pm 1, \pm 7 \bmod 25\} \\ &= \{2,\ 3,\ 13,\ 17,\ 19,\ 23,\ 29,\ 37,\ 47,\ 53,\ 59,\ 67,\ 73,\ 79 \ldots\}\end{aligned}$$

For ℓ_+, we need 5-units of $K = \mathbb{Q}(\mu_5)$ on which $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ acts through $\omega^{1\pm b} = \{\omega^0, \omega^2\}$ mod fifth powers. One of these is the trivial action, so we can take $\alpha = 5$ again. The other one must be in $\mathcal{O}_K^\times$. Moreover, from [31, Chapter 8], we know that this unit β can be taken from K^+, which is the real quadratic field $\mathbb{Q}(\sqrt{5})$ in this case, whose unit group has rank 1. And because the roots of unity are in their own separate ω-eigenspace, any unit of infinite order in $\mathbb{Q}(\sqrt{5})$ will work — for example, $\beta = 2 + \sqrt{5}$.

We verify: for $a \in (\mathbb{Z}/5)^\times$, let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ that acts on $\zeta_5 \in \mu_5$ via $\sigma_a(\zeta) = \zeta^a$. Then, on one hand, $a \equiv \pm 1 \bmod 5 \implies \sigma_a(2+\sqrt{5}) = 2+\sqrt{5}$ and $a \equiv \pm 2 \bmod 5 \implies \sigma_a(2+\sqrt{5}) = 2-\sqrt{5}$: that's the only way to get an order-2 quotient of $(\mathbb{Z}/5)^\times$. On the other hand,

$$(2+\sqrt{5})^{\omega^2(\sigma_a)} = (2+\sqrt{5})^{a^2} = \begin{cases} 2+\sqrt{5} & \text{if } a \equiv \pm 1 \\ -(2-\sqrt{5}) & \text{if } a \equiv \pm 2. \end{cases}$$

Since -1 is a fifth power, these two actions coincide modulo fifth powers. (We get the ω^2-action on the nose if we start with a unit of norm 1, such as $\beta^2 = 9 + 4\sqrt{5}$.) In any case,

$$\begin{aligned}\ell_+ &\in \left\{\ell \equiv 1 \bmod 5 :\ 5 \text{ and } 2+\sqrt{5} \text{ are not } 5^{\text{th}} \text{ powers modulo } \ell\right\} \\ &= \{11,\ 41,\ 61,\ 71,\ 101,\ 131,\ 151,\ 181, \ldots\}.\end{aligned}$$

Note that, by quadratic reciprocity $\left(\frac{5}{\ell}\right) = \left(\frac{\ell}{5}\right) = 1$, so that $\sqrt{5} \in \mathbb{F}_\ell$. (Of course we already knew that since ℓ splits completely in $\mathbb{Q}(\mu_5)$.)

The least pair that will work is $(\ell_- = 2,\ \ell_+ = 11)$. But it can be handy to have $\ell_- \equiv -1 \bmod p$ for reasons explained in Lemma 6.6, so we record $(\ell_- = 19,\ \ell_+ = 11)$ as well.

7.4.2 Proof of Theorem 7.1

Recall that Lemma 6.6 explain why it is convenient to choose primes congruent to ± 1 modulo p: in this cases, modified Hecke operators look the same on all reducible components.

Proof of Theorem 7.1. See Section 7.5 below for $p = 2$, so assume that $p \geq 3$.

For each reducible τ mod p, we have constructed $\widetilde{\tau}_+$ and $\widetilde{\tau}_-$ and used them to find two primes whose associated modified Hecke operators generate $\mathfrak{m}_\tau/\mathfrak{m}_\tau^2$. It remains to show that we can do this *simultaneously* for all reducible τ mod p.

For ℓ_-, this is easy: we have already noted that any $\ell \equiv -1$ modulo p but not modulo p^2 will do. We just have to check that the requirements on ℓ_+ can be met over all components simultaneously. The group $\widetilde{\Gamma}$ defined in section 7.3.1 is isomorphic to $\mathbb{F}_p{}^{\frac{p+1}{2}}$, one $\mathbb{F}_p$-dimension for every ω^k-eigenspace for k even modulo $p-1$ and for $k = 1$. Of these, all the even ones are of the form $1 - b$ for some odd b corresponding to a pseudocharacter of the form $1 + \omega^b$, so that there are $\frac{p-1}{2}$ distinct useful-for-tangent-computations $\mathfrak{p}$-units. (The extra one that we never use comes from the torsion part of the unit group, generated by ζ_p. The action of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ on ζ_p is through ω, which reflects to $b = 0$, which never appears since our pseudocharacter is odd.) In any case, the requirements on ℓ_+ over all reducible components amounts to requiring Frob_{ℓ_+} to project to a basis for each of the $\frac{p-1}{2}$ special lines (the $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$-eigenlines) in the group $\mathbb{F}_p{}^{\frac{p-1}{2}}$. This is clearly possible: $(p-1)^{\frac{p-1}{2}}$ of the $p^{\frac{p-1}{2}}$ elements do it.

By the Chebotarev density theorem, there are infinitely many primes ℓ_+ that move every useful eigenunit in E/E^p. Their density is

$$\frac{1}{p}\left(\frac{p-1}{p}\right)^{\frac{p-3}{2}}$$

□

7.5 The case $p = 2$

Recall that for $p = 2$ we use Chenevier pseudorepresentations and keep track of the determinant along with the trace. In [30], Tate proves that there is only one modular pseudorepresentation of $G = G_{\mathbb{Q},2}$, namely $(\tau = 1 + 1,\ d = 1)$. The infinitesimal pseudodeformations of τ factor through $\Gamma = \mathrm{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$ (see [7, Lemma 5.3]), which is isomorphic to the Klein-4 group. Write $\Gamma = \{1, g, h, c\}$, where g fixes $\sqrt{-2}$, h fixes i, and c fixes $\sqrt{2}$. A basis for those with determinant 1 and $\widetilde{\tau}(c) = 0$ is given by $\widetilde{\tau}_g$, $\widetilde{\tau}_h$, where $\widetilde{\tau}_g(g) = \widetilde{\tau}_h(h) = \varepsilon$, and all the other $\widetilde{\tau}$-values are 0. These are visibly a basis for $\mathcal{D}_\tau$.

A curious note: While both $\widetilde{\tau}_g$ and $\widetilde{\tau}_h$ are *reducible* as pseudorepresentations of $G = G_{\mathbb{Q},2}$, both are traces of *irreducible* true representations of G factoring through two different D_4-extensions of $\mathbb{Q}$, the former through $\mathbb{Q}(i, (-2)^{\frac{1}{4}})$ and the latter through $\mathbb{Q}(i, 2^{\frac{1}{4}})$.

In any case, the maximal ideal of A_τ is generated by (T_{ℓ_h}, T_{ℓ_g}) where $\ell_h \equiv 3 \bmod 8$ and $\ell_g \equiv 5 \bmod 8$. This happily matches Nicolas and Serre's discoveries in [23].

Chapter 8

Applications to $p = 2, 3, 5, 7, 13$

We apply the nilpotence method to small primes with $M^0 = \mathbb{F}_p[\Delta]$. The results are summarized below. The isomorphism $\Theta : A_\tau \xrightarrow{\sim} A_{\omega\tau}$ is induced from the θ-map on modular forms modulo p; see section 2.8.

Theorem 8.1.

- *For $p = 2$, the Hecke algebra is $A = \mathbb{F}_2[\![T_3, T_5]\!] = \mathbb{F}_2[\![T_{\ell_3}, T_{\ell_5}]\!]$ for any pair of primes ℓ_3 and ℓ_5 with $\ell_i \equiv i \bmod 8$.*

- *For $p = 3$, the Hecke algebra is $A = \mathbb{F}_3[\![T_2, T_7 - 2]\!] = \mathbb{F}_3[\![T_{\ell_-}, T_{\ell_+} - 2]\!]$ for any pair of primes ℓ_- and ℓ_+ satisfying*
$$\begin{cases} \ell_- \text{ congruent to } 2 \text{ or } 5 \text{ modulo } 9, \\ 3 \text{ is not a perfect cube modulo } \ell_+. \end{cases}$$

- *For $p = 5$, there are four twist-isomorphic reducible local components. In each case,*
$$A_\tau = \mathbb{F}_5[\![T_{11} - 2,\ T_{19}]\!] = \mathbb{F}_5[\![T_{\ell_+} - 2,\ T_\ell - 1 - \ell^{-1}]\!]$$
for any pair of primes satisfying
$$\begin{cases} \ell \not\equiv 1 \bmod 5 \text{ and } \ell \not\equiv \pm 1, \pm 7 \bmod 25, \\ \text{neither } 5 \text{ nor } 2 + \sqrt{5} \text{ are perfect fifth powers modulo } \ell_+. \end{cases}$$

- *For $p = 7$, there are nine local components, all reducible, in two isomorphism classes up to twist. In each case,*
$$A_\tau = \mathbb{F}_7[\![T_{\ell_+} - 2,\ T_{\ell_-}]\!],$$
where ℓ_- is any prime congruent to -1 modulo 7 but not modulo 49; and ℓ_+ is congruent to 1 modulo 7 with additional conditions described in Corollary 7.8.

- *For $p = 13$, there are 48 local components: 36 are reducible in three different isomorphism classes up to twist, and 12 irreducible and twist-isomorphic. If τ is reducible, then*
$$A_\tau = \mathbb{F}_{13}[\![T_{\ell_+} - 2,\ T_{\ell_-}]\!],$$

where $\ell_\pm$ satisfy similar conditions as above. Moreover, $A_\tau \simeq \mathbb{F}_{13}[\![x, y]\!]$ for every τ.

The case $p = 2$ recovers a theorem of Nicolas-Serre [24, Théorème 4.1]. The case $p = 3$ is new. The case $p \geq 5$ recovers and slightly refines results of Bellaïche-Khare [5, Theorem III, Theorem 22].

The rest of this chapter is devoted to the proofs of all these statements, prime by prime. We will again **use the shorthand *NRO* for a proper degree-lowering recursion operator** in the sense of section 5.5. Recall that *full* NROs are precisely what Theorem 5.1 applies to.

Proposition 8.2. *Let $p = 2, 3, 5, 7$ or 13. Let $T \in \widetilde{A}^0$ is in every maximal ideal of A^0. Then T is a full NRO on M^0 and hence $N_T(f) \ll (\deg f)^\alpha$ for some $\alpha < 1$.*

Proof. Lemma 3.1, Corollary 6.5, and Theorem 5.1. □

Corollary 8.3. *Let $p = 2, 3, 5$ or 7.*

1. *If $\ell \equiv 1 \bmod p$, then $T = T_\ell - 2$ is a full NRO on M^0.*
2. *If $\ell \equiv -1 \bmod p$, then $T = T_\ell$ is a full NRO on M^0.*

In each case, $N_T(f) \ll (\deg f)^\alpha$ for some $\alpha < 1$.

Proof. Lemma 6.6, plus the fact that none of these primes have irreducible components, which follows from Theorem 2.42. And then Proposition 8.3. □

8.2 $p = 2$

There is only one modular τ, namely, $(\mathrm{tr} = 0, \det = 1)$, coming from $\rho = 1 \oplus 1$, which is the unique semisimple representation $G_{\mathbb{Q},2} \to \mathrm{GL}_s(\overline{\mathbb{F}}_2)$. This uniqueness is a theorem of Tate from the 70s [30] using discriminant bounds, but see also the elementary observation of Serre described in [5, footnote in section 1.2].

Moreover, $M = M_\tau = \mathbb{F}_2[\Delta]$, and maximal ideal $\mathfrak{m}$ of $A = A_{\bar{\tau}}$ is generated by T_3 and T_5 (Section 7.5). The corresponding Hecke polynomials (computed in Section 6.2) and tuple of initial values (easy to compute by hand) are:

$$P_{3,\Delta} = (X + \Delta)^4 + \Delta X \qquad \text{initial values} = [0, 0, 0, \Delta];$$
$$P_{5,\Delta} = X^6 + \Delta^2 X^4 + \Delta^4 X^2 + \Delta X + \Delta^6 = (X + \Delta)^6 + \Delta X \qquad \text{initial values} = [0, 0, 0, 0, 0, \Delta].$$

Theorem 5.3 applies to T_3 acting on M with $p^k = 4$ and $D = 2$, and to T_5 acting on M with $p^k = 8$ and $D = 4$. Therefore,

$$N_3(\Delta^n) \leq c_{4,2}(n)/2 < 3\sqrt{n} \qquad N_5(\Delta^n) \leq c_{8,4}(n)/4 < \tfrac{7}{3} n^{\frac{2}{3}}.$$

The nilpotence index $N(\Delta^n) := N_3(\Delta^n) + N_5(\Delta^n)$ for n odd (i.e., Δ^n in K) has been studied in depth by Nicolas and Serre in [23, 24]. They give a surprising exact formula for the minimum k for which $\mathfrak{m}^k$ annihilates Δ^n, which implies that $\frac{1}{2}\sqrt{n} < N(\Delta^n) < \frac{3}{2}\sqrt{n}$ for n odd. Their proof that $A = \mathbb{F}_2[\![T_3, T_5]\!]$ proceeds more or less immediately from the formula for $N(\Delta^n)$ by duality. The upper bound for $N_5(\Delta^n)$ that we get from Theorem 5.3 leaves something to be desired in comparison.

Since $\frac{2}{3}$ is less than 1, Theorem 3.3 applies for T_3, T_5 and $f = \Delta$. Since τ is unobstructed, $A = \mathbb{F}_2[\![T_3, T_5]\!]$.

Alternatively, we can use generators T_{ℓ_3} and T_{ℓ_5} for any primes ℓ_3 and ℓ_5 with ℓ_i congruent to i modulo 8. Use Corollary 8.3, and then Theorem 3.3 applies for T_{ℓ_3}, T_{ℓ_5} and $f = \Delta$.

8.3 $p = 3$

For $p = 3$, there is again only one $\tau = 1 + \omega$ (Serre [28]), so that $A = A_\tau$. Again $M = \mathbb{F}_3[\Delta]$.

Generators for the Hecke algebra are computed carefully in section 7.4.2. The generators using the smallest primes are T_2 and $T_7' = T_7 - 2$. Again, we see $P_{\ell,\Delta}$, $P'_{\ell,\Delta}$ and the initial values for each relevant ℓ.

$$\begin{aligned}
P_{2,\Delta} &= X^3 - \Delta X + \Delta^3 \qquad \text{initial values} = [0, 0, \Delta] \\
P_{7,\Delta} &= X^8 + \Delta X^7 + \Delta^2 X^6 \\
&\qquad + \Delta^3 X^5 + (X^4 - \Delta^2)X^4 + (\Delta^5 + \Delta^2)X^3 + (\Delta^6 + \Delta^3)X^2 + (\Delta^7 - \Delta^4 - \Delta)X + \Delta^8 \\
&= (X - \Delta)^8 - \Delta X^4 + \Delta^2 X^3 + \Delta^3 X^2 - (\Delta^4 + \Delta)X \\
&\qquad \text{initial values} = [-1, -\Delta, -\Delta^2, -\Delta^3, -\Delta^4 + \Delta, -\Delta^5 - \Delta^2, -\Delta^6, -\Delta^7 - \Delta^4 + \Delta] \\
P'_{7,\Delta} &= (X - \Delta)\, P_{7,\Delta} = X^9 - \Delta X^5 - \Delta^2 X^4 + (\Delta^4 - \Delta)X^2 + (\Delta^5 + \Delta^2)X - \Delta^9 \\
&\qquad \text{initial values} = [0,\ 0,\ 0,\ 0,\ \Delta,\ -\Delta^2,\ 0,\ -\Delta^4 + \Delta,\ \Delta^5 - \Delta^2].
\end{aligned}$$

Clearly, T_2 and T_7' are full NROs, so that Theorem 5.3 applies to T_2 with $p^k = 2$ and $D = 1$, and to T_7' with $p^k = 9$ and $D = 3$:

$$N_2(n) \;<\; 4n^{\log_3 2} \;\approx\; 4n^{0.63} \qquad\qquad N_7(n) \;<\; \tfrac{16}{5} n^{\log_9 6} \;\approx\; 3.2n^{0.82}.$$

Computationally, one sees that both $N_2(n)$ and $N_7(n)$ grow like $\sqrt{n}$ on K.

Finally, Theorem 3.3 applies for T_2, T_7' and $f = \Delta$. Since τ is unobstructed, $A = \mathbb{F}_3[\![T_2, T_7 - 2]\!]$. Use Corollary 8.3 and Theorem 3.3 for other generators.

8.5 $p = 5$

Because $E_4 = 1$, we know that $M = \mathbb{F}_5[E_6]$, which we decompose first into weight-mod-4 components: $M^0 = \mathbb{F}_5[E_6^2]$ and $M^2 = E_6\,\mathbb{F}_5[E_6^2]$, and then we can take advantage of the fact that $\Delta = 2 - 2E_6^2$ to arrange things in more convenient form:

$$M^0 = \mathbb{F}_5[\Delta], \qquad\qquad M^2 = E_6\,\mathbb{F}_5[\Delta].$$

We also have four modular pseudocharacters, all twists of one other: $\omega^3 + 1$, $1 + \omega$, $\omega + \omega^2$, and $\omega^2 + \omega^3$. Let $\tau_k = \omega^{k-1} + \omega^k$ for $i = 0, 1, 2, 3$. Moreover $M^0 = M_{\tau_0} \oplus M_{\tau_2}$.

The algorithms in Chapter 7 tell us that $m_{\tau_k} = \big(T'_{\ell_-}, T'_{\ell_+}\big)$, where

$$\{\ell_- \not\equiv 1 \bmod 5,\ \ell_- \not\equiv \pm 1, \pm 7 \bmod 25\} \implies \ell_- \in \{2, 3, 13, 17, 19, 23, 29, 37, 47, \ldots\}$$

$$\Big\{\ell_+ \equiv 1 \bmod 5,\ 5 \text{ and } 2 + \sqrt{5} \text{ are not } 5^{\text{th}} \text{ powers in } \mathbb{F}_{\ell_+}\Big\} \implies \ell_+ \in \{11, 41, 61, 71, 101, 131, 151, 181, \ldots\},$$

so that $m_{\tau_k} = \big(T_2 + 2^k,\, T_{11} - 2\big) = \big(T_{19},\, T_{11} - 2\big)$, depending on whether we want the smallest ℓ_- or the one that has a unified modified form in every component.

The Hecke polynomials for $T'_{11} = T_{11} - 2$ and T_{19} acting on $M^0 = \mathbb{F}_5[\Delta]$ are long to write out, but their general shape is

$$P'_{11,\Delta} = (X - \Delta)\, P_{11,\Delta}(X) = (X - \Delta)^{13} + [\text{terms of total degree} \le 9]$$
$$P_{19,\Delta} = (X - \Delta)^{20} + [\text{terms of total degree} \le 18].$$

so that the descent D is 4 and 2, respectively. Moreover, the operators lower degrees by 4 and 2, respectively. Theorem 5.3 applies with (p^k, D, E) equal to $(25, 4, 4)$ and $(25, 2, 2)$, respectively, so that

$$N_{11}(\Delta^n) \;<\; 6.3\, n^{\log_{25} 21} \;\approx\; 6.3\, n^{0.946} \qquad \text{and} \qquad N_{19}(\Delta^n) \;<\; \tfrac{138}{11}\, n^{\log_{25} 23} \;\approx\; 12.6\, n^{0.974}.$$

Finally, Corollary 8.3 applies, and then Theorem 3.3 with T'_{11}, T_{19} and $f = \Delta$, so that at least one of A_{τ_0}, A_{τ_2} has dimension at least two, and hence is power series ring in two variables because these τs are unobstructed. But A_{τ_0} and A_{τ_2} are twist-isomorphic, so that both are isomorphic to $\mathbb{F}_5[\![T'_{11}, T_{19}]\!]$. Same for the other generators.

Remark. Results of Jochnowitz in [18, Theorem 6.3] can be used to show that $M^0 = \mathbb{F}_5[\Delta]$ has a basis $\{g_0, g_1, g_2, \ldots\}$, with g_n of Δ-degree n, satisfying

$$g_n \in M_{\tau_0} \text{ iff } n \text{ is even} \qquad \text{and} \qquad g_n \in M_{\tau_2} \text{ iff } n \text{ is odd.}$$

Such a basis is a priori not unique: g_n is only well-defined modulo $\langle g_{n-2}, g_{n-4}, \ldots\rangle$ and up to scaling. We can force uniqueness in various ways; here is one: let $g_0 = 1$ and g_n for $n \ge 1$ be of the shape $\Delta^n + \sum_{i=0}^{\lfloor n/2\rfloor} a_i \Delta^{n-1-2i}$ for scalars $a_i \in \mathbb{F}_p$. Then we can compute:

$$g_0 = 1, \quad g_1 = \Delta, \quad g_2 = \Delta^2 + 2\Delta, \quad g_3 = \Delta^3 + 4\Delta^2, \quad g_4 = \Delta^4 + 4\Delta^3 + 3\Delta, \quad g_5 = \Delta^5, \qquad \text{etc.}$$

It's worth noting that $3g_2 = \theta^2(\Delta)$ is in the kernel of U_5 and a true Hecke eigenform, the reduction of a normalized cuspidal eigenform in $S_{24}(1, \mathbb{Q}(\sqrt{144169}))$. But $g_5 = \Delta^5$ is just an A-eigenform, not in K.

8.7 $p = 7$

For $p = 7$, we know that $E_6 = 1$, so that $M = \mathbb{F}_7[E_4]$. The weight grading is modulo 6, so that we have $M = M^0 \oplus M^2 \oplus M^4 = \mathbb{F}_7[E_4^3] \oplus E_4^2 M^0 \oplus E_4 M^0$. Finally

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = 1 - E_4^3,$$

so that $M^0 = \mathbb{F}_7[\Delta]$.

Every τ is reducible (Theorem 2.42) so that there are three of them in M^0: namely, $\bar\tau \in \{1+\omega^5, \omega+\omega^4, \omega^2+\omega^3\}$. Let $\tau_i = \omega^i + \omega^{5-i}$. Then τ_0 and τ_2 are twists of each other.

By Theorem 7.1, we can find two primes $\ell_\pm$ so that $T_{\ell_+} - 2$ and T_{ℓ_-} generate each maximal ideal. Then Theorem 3.3 applied to these operators and $f = \Delta$ guarantees that at least one of the eigencomponents has dimension at least 2, and hence is isomorphic to $\mathbb{F}_7[\![T_{\ell_+} - 2, T_{\ell_-}]\!]$ because it is unobstructed.

Using Jochnowitz's results from section 2.8.1, we can do more. Corollary 2.45 guarantees that, for each i, we can find an sequence of eigenforms $\{f_0, f_1, f_2, \ldots\}$ in K_{τ_i} with $w(f_n)$ depending linearly on n. And now Corollary 3.6 with generators $T_{\ell_+} - 2$ and T_{ℓ_-} implies that $\dim A_{\tau_i} \ge 2$ for each i, which, in turn, implies that A_{τ_i} is a power series ring in the two generators.

Remark. Again, [18, Theorem 6.3] implies that $M^0 = \mathbb{F}_7[\Delta]$ has a basis $\{g_0, g_1, g_2, \ldots\}$, with g_n of Δ-degree n, satisfying

$$g_n \in M_{\tau_0} \iff n \equiv 0 \bmod 4; \qquad g_n \in M_{\tau_1} \iff n \equiv \pm 1 \bmod 4; \qquad g_n \in M_{\tau_2} \iff n \equiv \pm 2 \bmod 4.$$

Normalizing in a similar manner to the case $p = 5$ above, so that $g_0 = 1$, we can compute:

$$g_1 = \Delta, \quad g_2 = \Delta^2 + \Delta, \quad g_3 = \Delta^3 + 2\Delta^2, \quad g_4 = \Delta^4 + 4\Delta^3 + 5\Delta^2 + 5\Delta, \quad g_5 = \Delta^5 + 2\Delta^4 + 2\Delta^2.$$

Here g_1, g_2, and g_4 are reductions of true cuspidal eigenforms of weight 12, 24, and 48, respectively.

8.13 $p = 13$

Express E_{12} as a polynomial in E_4^3 and E_6^2:

$$691E_{12} = 441E_4^3 + 250E_6^2.$$

That means that the algebra of modular forms is

$$M = \mathbb{F}_{13}[E_4, E_6]/(3E_6^2 - E_4^3 - 2).$$

The 0-graded piece is $M^0 = \mathbb{F}_{13}[E_4^3, E_6^2]/(3E_6^2 - E_4^3 - 2) = \mathbb{F}_{13}[E_6^2]$ with $E_4^3 = 3E_6^2 - 2$. At the same time,

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = E_6^2 - E_4^3 = 2 - 2E_6^2,$$

so that once again $M^0 = \mathbb{F}_{13}[\Delta]$. Note that $E_4^3 = 3E^2 - 2 = 3(1+6\Delta) - 2 = 1 + 5\Delta$, so that $j = \frac{E_4^3}{\Delta} = \frac{1+5\Delta}{\Delta}$, whence $\Delta = \frac{1}{j+8}$.

There are six reducible τs in M^0, namely,

$$\bar{\tau} \in \{1 + \omega^{11},\ \omega + \omega^{10},\ \omega^2 + \omega^9,\ \omega^3 + \omega^8,\ \omega^4 + \omega^7,\ \omega^5 + \omega^6\}.$$

The first and last are twist-isomorphic, as are the second and the second-to-last, as are the middle two. As before, let $\tau_i = \omega^i + \omega^{11-i}$ for $i = 0, 1, \ldots, 5$.

Plus there are two irreducible τs, namely τ_Δ and $\tau_{\theta^6(\Delta)}$.*

There are no more τs in M^0: any τ in M has a twist coming from an eigenform of filtration k with $4 \le k \le 14$ (Theorem 2.42). We have accounted for all the ones from Eisenstein series (there are always $\frac{p-1}{2}$ reducible components in M^0) and the only cuspidal eigenform appearing in weight bounded by 14 is Δ.

Theorem 7.1 guarantees infinitely many pairs of Hecke operators $T_+ = T_{\ell_+} - 2$ and $T_- = T_{\ell_-}$ that generate all of the maximal ideals $\mathfrak{m}_{\tau_i}$.

Claim. We can find a T_+ and a T_- that are also contained in $\mathfrak{m}_{\tau_\Delta}$.

Proof of claim. It suffices to find $\ell_\pm$ with $a_{\ell_-}(\Delta) = 0$ and $a_{\ell_+}(\Delta) = 2$. Since the ℓ_- is defined by congruences,

*That τ_Δ is irreducible at 13 is well known ([29], for example) but also very easy to see: if τ_Δ were reducible, then $\tau(\mathrm{Frob}_\ell) = a_\ell(\Delta)$ would depend only on ℓ modulo 13. But

$$\Delta = q + 2q^2 + 5q^3 + 10q^4 + 7q^5 + 10q^6 + 6q^8 + 3q^9 + q^{10} + 11q^{12} + 8q^{13} + 9q^{15} + 7q^{16} + 4q^{17} + 6q^{18} + 3q^{19} + 5q^{20} + 11q^{23} + 4q^{24} + 2q^{25} + 3q^{26} + 9q^{27} + q^{29} + O(q^{30}),$$

and, for example, $5 = a_3(\Delta) \neq a_{29}(\Delta) = 1$.

is easy to find one: $\ell_- = 1741$ satisfies $a_{1741}(\Delta) = 0$.

For ℓ_+, we use the notation of section 7.3. Consider the (irreducible) representation $\rho_\Delta : G_{\mathbb{Q},13} \to \mathrm{GL}_2(\mathbb{F}_{13})$ whose trace is τ_Δ. We want to find an element g of $H = \mathrm{Gal}\left(\mathbb{Q}^{13}/\mathbb{Q}(\mu_{13})\right)$ so that both $\operatorname{tr}\rho_\Delta(g) = 2$ and the image of g in $\widetilde{\Gamma}$ is in some list of allowable elements. Then the Chebotarev density theorem will guarantee that we can find an ℓ_+ so that $g = \mathrm{Frob}_{\ell_+}$ satisfies the same conditions, since the conditions factor through a finite extension of $\mathbb{Q}$.

The representation ρ_Δ restricted to H lands in $\mathrm{SL}_2(\mathbb{F}_{13})$ since $\det\rho_\Delta = \omega^{-1}$, which is trivial on H. Moreover, by [26, 3.3 (Exemple $f = \Delta$)] the prime 13 is not exceptional for Δ, so that the restriction of ρ_Δ to H surjects onto $\mathrm{SL}_2(\mathbb{F}_{13})$.

Consider the map $H \xrightarrow{\rho_\Delta \times \mathrm{proj}} \mathrm{GL}_2(\mathbb{F}_3) \times \widetilde{\Gamma}$. It would suffice to know that this map is surjective. The image $R \subset \mathrm{SL}_2(\mathbb{F}_{13}) \times \widetilde{\Gamma}$ surjects onto both components. By Goursat's lemma, R is a fiber product over a groups that is a quotient of both $\mathrm{SL}_2(\mathbb{F}_{13})$ and $\widetilde{\Gamma}$. But $\widetilde{\Gamma}$ is abelian and $\mathrm{SL}_2(\mathbb{F}_{13})$ doesn't have any nontrivial abelian quotients, so in that that common quotient is the trivial group, and $R = \mathrm{SL}_2(\mathbb{F}_{13}) \times \widetilde{\Gamma}$. Therefore we can pick an element g of H that is, for example, simultaneously in the kernel of ρ_Δ (so its trace is 2) that lands anywhere we like $\widetilde{\Gamma}$, as desired. □

As for $p = 7$ above, Corollary 2.45 guarantees that, for each reducible τ_i, we can find an sequence of eigenforms $\{f_0, f_1, f_2, \ldots\}$ in K_{τ_i} with $w(f_n)$ depending linearly on n; and Corollary 3.6 with generators T_+ and T_- together with the fact that τ_i is unobstructed implies that $A_{\tau_i} = \mathbb{F}_7[\![T_+, T_-]\!]$.

We cannot a priori make the same deduction for the irreducible τ because we have not been able to guarantee that T_+ and T_- are linearly independent in the cotangent space of the irreducible components — either may well be in $\mathfrak{m}_\tau^2$, for example.

Better results

Consider the irreducible components, $\mathfrak{m}_{\tau_\Delta}$ up to twist. We can find finitely many[†] Hecke operators $S_1, \ldots, S_m$ that generate $\mathfrak{m}_{\tau_\Delta}$. (As always, we choose them in $\widetilde{A}^0$.)

Next, for each τ appearing in A^0, we find elements E_τ in $\widetilde{A}^0$ with the property that E_τ is a unit in A_τ and in $\mathfrak{m}_{\tau'}$ for all $\tau' \neq \tau$. These can always be found: we know that A^0 is a direct product of local rings A_τ, so that any lift of the idempotents of $\prod_\tau A_\tau/\mathfrak{m}_\tau = \prod_\tau \mathbb{F}$ will do. Since $\widetilde{A}^0$ is dense in A^0 and $\prod_\tau \mathbb{F}$ is finite, we can always find E_τ in $\widetilde{A}^0$.

Finally, consider the finite set

$$\{E_\Delta S_1, \ldots, E_\Delta S_m\}.$$

These operators are all in $\widetilde{A}^0$, so that they are proper and full recursion operators by Corollary 6.5. Moreover, each one is in *every* maximal ideal by construction, so they are all NROs by Proposition 8.2. Finally, their images in A_{τ_Δ} generate $\mathfrak{m}_{\tau_\Delta}$, again by construction. Therefore Corollary 3.6 applies, using a sequence guaranteed by Corollary 2.45 for τ_Δ.

[†]In Appendix F we give Weston's argument that τ_Δ is unobstructed at 13, so that in fact we need only two operators to generate $\mathfrak{m}_{\tau_\Delta}$. Prior to this argument, it was known to the literature that the representation attached to Δ is unobstructed for all p with the possible exception of 11 and 13 [33, Theorem 5.6].

Remark. As for $p = 5$ and $p = 7$, [18, Theorem 6.3] implies that the Δ-degree of a generalized eigenform is controlled by its eigencomponent. Specifically, we can find a basis $\{g_n\}$ for $M^0 = \mathbb{F}_{13}[\Delta]$ so that

$$\begin{aligned}
n \equiv 0 \bmod 14 &\iff g_n \in M_{\tau_0} && E_{12} = 1 \quad \text{and} \quad 7\Delta^{14} + 4\Delta^{12} + 5\Delta^{11} + 12\Delta^{10} + 4\Delta^9 + \\
&&& \qquad + 12\Delta^7 + 11\Delta^6 + 10\Delta^5 + 12\Delta^4 + 7\Delta^3 + 6\Delta^2 + \Delta \\
n \equiv \pm 1 \bmod 14 &\iff g_n \in M_{\tau_\Delta} && \Delta \quad \text{and} \quad \theta^{12}(\Delta) = 5\Delta^{13} + \Delta \\
n \equiv \pm 2 \bmod 14 &\iff g_n \in M_{\tau_1} && 10\Delta^2 + \Delta \\
n \equiv \pm 3 \bmod 14 &\iff g_n \in M_{\tau_2} && 3\Delta^3 + 7\Delta^2 + \Delta \\
n \equiv \pm 4 \bmod 14 &\iff g_n \in M_{\tau_3} && 2\Delta^4 + 10\Delta^3 + 2\Delta^2 + \Delta \\
n \equiv \pm 5 \bmod 14 &\iff g_n \in M_{\tau_4} && 7\Delta^5 + 7\Delta^4 + 5\Delta^3 + 12\Delta^2 + \Delta \\
n \equiv \pm 6 \bmod 14 &\iff g_n \in M_{\tau_{\theta^6(\Delta)}} && \theta^6(\Delta) = 5\Delta^6 + 8\Delta^5 + 12\Delta^4 + 3\Delta^3 + 9\Delta^2 + \Delta \\
n \equiv 7 \bmod 14 &\iff g_n \in M_{\tau_5} && \Delta^7 + 2\Delta^5 + 8\Delta^4 + 6\Delta^3 + 3\Delta^2 + \Delta.
\end{aligned}$$

The polynomials above are all the corresponding true eigenforms (for U_{13} as well as for A) — reductions of eigenforms appearing in characteristic zero, in this case normalized if cuspidal.

8.100 The nilpotence method

We restate the core part of Theorem 8.1 in a more uniform way. The proof *is* the nilpotence method for obtaining lower bounds on dimensions of mod-p Hecke algebras.

Theorem 8.4.
If $p = 2, 3, 5, 7$ or 13, and $\tau : G_{\mathbb{Q},p} \to \mathbb{F}_p$ is a modular pseudocharacter, then $\dim A_\tau \geq 2$.

Since τ is always unobstructed for these primes (Proposition 2.16), in fact $A_\tau \simeq \mathbb{F}_p[\![x, y]\!]$.

Proof using the nilpotence method.

Reduce to A^0: By Proposition 2.41, A_τ is isomorphic to a local component of A^0, so it suffices to prove the theorem for τ with $k(\tau) = 0$. Let $\tau_1, \ldots, \tau_s$ be a complete list of modular Galois pseudocharacters appearing in A^0. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the corresponding maximal ideal and $A_1, \ldots, A_s$ the corresponding localization. That is $A_i = A_{\mathfrak{m}_i}$ and $A^0 = A_1 \times \cdots \times A_s$. Fix i; we will show that $\dim A_i \geq 2$.

Find generators for each $\mathfrak{m}_i$: Each A_i is noetherian (Proposition 2.19), so that for each i we can find finitely many Hecke operators $T_1^i, \ldots, T_{m_i}^i$ in $\widetilde{A}^0$, each of the form $T_\ell - \tau_i(\mathrm{Frob}_\ell)$, to generate $\mathfrak{m}_i$. These are simultaneously ideal generators of $\mathfrak{m}_i$ and topological algebra generators of A_i. Their image in A_j for $j \neq i$ is not controlled.

Find "approximate idempotents" for each A_i: For each i, we find elements $E_i \in \widetilde{A}^0 \subset A^0$ with the property that $E_i \equiv 1 \bmod \mathfrak{m}_i$ and $E_i \in \mathfrak{m}_j$ for each $i \neq j$. One way to find these is to lift idempotents of

$$A_1/\mathfrak{m}_1 \times A_2/\mathfrak{m}_2 \times \cdots \times A_s/\mathfrak{m}_s = \mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p.$$

The set

$$\{E_i T_j^i : 1 \leq i \leq s,\ 1 \leq j \leq m_i\}$$

consists of elements of $\widetilde{A}^0$ that are, by construction, both in $\bigcap_i \mathfrak{m}_i$ and generate each $\mathfrak{m}_i$. Therefore, each $E_i T^i_j$ is a full NRO on M^0 (Proposition 8.2). Since there are finitely many of them, we can find $\alpha < 1$ so that $N_{E_i T^i_j}(f) \ll \deg(f)^\alpha$ for all $f \in M^0 = \mathbb{F}_p[\Delta]$ and all i, j (*ibid.*).

Find a sequence of witnesses for the fullness of A_i: Corollary 2.45 of Jochnowitz's results on filtrations of generalized eigenforms gives us, for each i, a sequence $\{f_n\}$ with $f_n \in K_{\tau_i}$ and $w(n) \sim (p^3 - p)n$.

Use the Hilbert-Samuel trick to conclude that $\dim A_i \geq 2$: Apply Corollary 3.6 to the set of operators $\{E_i T^i_j\}_{i,j}$ and the sequence of forms $\{f_n\}$ to conclude that the Hilbert-Samuel function of A_i grows faster than linearly, and hence $\dim A_i \geq 2$. □

8.101 Blueprint for generalizations

I believe that the nilpotence method can be generalized to work for all primes, and all levels. To do this we must

1. Generalize the Nilpotence Growth Theorem to filtered algebras. Ideal statement:

   > If $T : B \to B$ is a full NRO on a filtered algebra B, then there is an $\alpha < 1$ so that $N_T(f) \ll w(f)^\alpha$.

   Here $w(f)$ is of course the minimum filtration of f. Other terminology (proper, full) has already been developed in section 4.4. Most probably we would need to assume that filtered algebra B has the property that $w(f^n) = n\, w(f)$.
2. Prove that Hecke recursions are always full. This just entails proving that, for $f \in M_k$,
   $$w(f_0 f_1 \dots f_\ell) = (\ell + 1)\, w(f),$$
   where $f_0, \dots, f_\ell$ are the translates of f defined in Lemma 6.1. If true, this should not be difficult.[‡]
3. Generalize the results of Chapter 4, especially Proposition 4.22, to filtered algebras. This would imply that $\widetilde{A}^0$ is always an algebra of proper and full filtered separable recursion operators (possibly with additional conditions satisfied by Hecke operators).

The proof would then proceed just as the proof of Theorem 8.4 above.

8.102 A question of Khare

We end with a few remarks on a question of Khare [20]. Let τ a modular Galois pseudocharacter modulo p, and assume that $k(\tau) = 0$ for simplicity. Recall that M_τ has its *weight filtration*

$$\{0\} \subset M_{\tau,p-1} \subset M_{\tau,2(p-1)} \subset M_{\tau,3(p-1)} \subset \dots \subset M_\tau$$

[‡](October 2015) In fact, this is false, and there are many counterexamples. For $p = 11$, we have $M^0 = \mathbb{F}_{11}[y, y^{-1}]$ with $y = E_4^5$ and $y^{-1} = E_6^5$, so that $w(y) = 20$ and $w(y^{-1}) = 30$. The recursion polynomial for the action of T_ℓ on M^0 for $\ell = 3$ is

$$P_{3,y} = X^4 + (9y + 9)X^3 + (y^2 + 9y + 9 + 9y^{-1})\, X^2 + (9 + 8y^{-1} + y^{-2})\, X + y^{-1}.$$

Evidently, $a_{\ell+1} = y^{-1}$ has filtration 30 rather that $(\ell + 1)w(y) = 80$. It now seems likely that a different condition will have to be used to carve out those NROs whose nilpotence index grows slower than linearly.

In [20, Section 3], Khare defines the *nilpotence filtration* on M_τ:

$$\{0\} \subset M_\tau[\mathfrak{m}_\tau] \subset M_\tau[\mathfrak{m}_\tau^2] \subset M_\tau[\mathfrak{m}_\tau^3] \subset \cdots \subset M_\tau,$$

and asks how the nilpotence filtration compares with the weight filtration when restricted to $K = \ker U$: "Does there exist a nice function $f(n)$ such that $K_\tau[\mathfrak{m}_\tau^n] \hookrightarrow K_{\tau,f(n)}$?"[§] He also notes that there is "a strong connection" between the function $f(n)$ and the dimension of A_τ. With the Hilbert-Samuel trick and (a hypothetical but plausible strengthening of) Jochnowitz's results, we can make that connection precise: if $f(n)$ is $O(n^k)$, then $\dim A_\tau \leq k$.

The nilpotence method naturally answers the inverse comparison question: if $p = 2, 3, 5, 7$ or 13, then we have shown that there is a function $g(n) \ll n^\alpha$ for some $\alpha < 1$ so that $M_{\tau,n} \hookrightarrow M_\tau[\mathfrak{m}_\tau^{g(n)}]$, which gives lower bound for the dimension of A_τ. But for $p = 2$, Nicolas and Serre have found a Khare-type function: they find that $f(n)$ is quadratic in n. It would be very interesting to see if this other side of Nicolas-Serre can be generalized as well.

[§]We have substituted our notation — but note that Khare states his question for forms of level $\Gamma_1(N)$.

Appendix A

Pseudocharacters and pseudorepresentations of dimension 2

A pseudocharacter of a group G to a ring A is a function $G \to A$ that mimics the properties of the trace of a representation of G. We'll briefly discuss two related notions of pseudocharacters of dimension 2: Rouquier's pseudocharacters and Chenevier's pseudorepresentations, and prove that they are equivalent if $\frac{1}{2} \in A$. The arguments don't appear to be written down anywhere, though the equivalence is well known. The main references are [25] and [7].

A.1 Rouquier pseudocharacters of dimension 2

Definition. A *pseudocharacter of dimension 2* of a group G over a ring A is a map $t : G \to A$ satisfying

- t is *central*: For all x, y in G we have $t(xy) = t(yx)$.
- t is *not* multiplicative: There exist x, y in G with $t(x)t(y) \neq t(xy)$.
- t satisfies the *Frobenius identity of order* 3: For all x, y, z in G,

$$t(x)t(y)t(z) - t(x)t(yz) - t(y)t(xz) - t(z)t(xy) + t(xyz) + t(xzy) = 0.$$

To explain the second requirement: if $t : G \to A^\times$ is a multiplicative character, then t is central and also satisfies the Frobenius identity of order 3, but of course we prefer to call this a pseudocharacter of dimension 1. A proper pseudocharacter of dimension 2 is not multiplicative.

Remark (Digression on the Frobenius identity). The Frobenius identity of order 3 is a special case of a more general construction. If $t : G \to A$ is any central map, n is any positive integer, and $\sigma \in \S_n$ is a permutation, define $t_\sigma : G^n \to A$ as—well, this is a one case where an example is clearer than a formula:

$$t_{(164)(23)}(x_1, \ldots, x_6) = t(x_1x_6x_4)t(x_2x_3)t(x_5).$$

Finally, let $S_n(t) : G^n \to A$ be defined as $S_n(t) = \sum_{\sigma \in \S_n} \operatorname{sgn}(\sigma) t_\sigma$.

Then the Frobenius identity of order 3 defined above is exactly the condition $S_3(t) = 0$ as a map $G^3 \to A$.

The Frobenius identity of order 2 is $S_2(t)(x,y) = t(x)t(y) - t(xy) = 0$ forces t to be multiplicative—that is, a pseudocharacter of dimension 1. More generally, a map $t : G \to A$ is a pseudocharacter of dimension $\leq d$ if it is central and $S_{d+1}(t) = 0$.

The inequality appearing in that definition is inconvenient but necessary: If $t : G \to A$ is central and $S_n(t) \equiv 0$ (as a map $G^n \to A$), then $S_{n+1}(t) \equiv 0$ as well. Indeed, it's not hard to convince oneself that

$$S_{n+1}(t)(x_1, \ldots, x_n, y) = t(y)S_n(t)(x_1, \ldots x_n) - \sum_{i=1}^{n} S_n(t)(x_1, \ldots, x_i y, \ldots, x_n).$$

In other words, a central map $t : G \to A$ is a pseudocharacter of dimension d if $S_{d+1}(t) = 0$ but $S_d(t) \neq 0$.

By playing around with 2×2 matrices, it's not difficult to verify that $\rho : G \to \mathrm{GL}_2(A)$ is a representation, then $\operatorname{tr}\rho$ is a pseudocharacter of dimension ≤ 2. Unfortunately, the trace of a representation of dimension 2 in characteristic 2 may be identically 0, and hence accidentally multiplicative. Consider, for example, the trivial two-dimensional representation of any group over $A = \mathbb{F}_2$: its trace is identically 0 and hence satisfies the Frobenius identity of order 1. Should it be considered a pseudocharacter of dimension 0? (The answer is that one should keep track of the determinant as well as the trace and work with Chenevier pseudorepresentations instead.)

Lemma A.1. *If A is a domain and $t : G \to A$ is a dimension-2 pseudocharacter, then $t(1) = 2$.*

In particular, if A is a domain with $\frac{1}{2} \in A$ and $\rho : G \to \mathrm{GL}_2(A)$ is any representation, then $\operatorname{tr}\rho$ is a pseudocharacter of dimension exactly 2.

Proof. Let $a = t(1) \in A$. The Frobenius identity with $z = 1$ gives

$$0 = a\,t(x)t(y) - t(x)(y) - t(y)t(x) - a\,t(xy) + t(xy) + t(xy) = (a-2)\big(t(x)t(y) - t(xy)\big).$$

Since we assumed that t is not multiplicative, there exist x and y in G with $t(xy) \neq t(x)t(y)$. If A is a domain, this forces $a = 2$. □

A.2 Chenevier pseudorepresentations of dimension 2

Definition. A *(Chenevier) pseudorepresentation of dimension 2* of a group G over a ring A is a pair (t, d) of functions from G to A satisfying

- $t : G \to A$ is central: for all x and y in G, we have $t(xy) = t(yx)$
- $t(1) = 2$
- $d : G \to A^\times$ is a group homomorphism
- (Trace-determinant identity) For all x and y in G, we have

$$t(xy) + d(x)t(x^{-1}y) = t(x)t(y).$$

It's trivial to verify that $(\operatorname{tr}\rho, \det\rho)$ is a pseudorepresentation of dimension 2 is if $\rho : G \to \mathrm{GL}_2(A)$ is a representation.

Do we need to assume $t(1) = 2$ in the definition? The trace-determinant identity for the pair $(1,1)$ gives $t(1) + d(1)t(1) = t(1)^2$, so that $t(1)$ is a root of $X(X-2)$, and it's likely possible to set up situations with

$t(1) = 2$ forced. In any case, it's desirable.

Lemma A.2. *Suppose $(t, d) : G \to A$ is a pseudorepresentation of dimension 2. Then $2\,d(x) = t(x)^2 - t(x^2)$ for all $x \in G$.*

Proof. Trace-determinant identity for the pair (x, x) and $t(1) = 2$. □

Proposition A.3. *If $\frac{1}{2} \in A$, then we have a natural bijection*

$$\{\textit{dim-2 Rouquier pseudochars } t : G \to A \textit{ with } t(1) = 2\} \leftrightarrow \{\textit{dim-2 Chenevier pseudoreps } (t, d) : G \to A\}$$
$$t \mapsto (t, d), \textit{ where } d(x) := \frac{t(x)^2 - t(x^2)}{2}$$
$$t \leftarrow\!\shortmid (t, d)$$

Proof. **Rouquier implies Chenevier:** First, suppose $t : G \to A$ is a Rouquier pseudocharacter of dimension 2. Define $d : G \to A$ as above: $d(x) = \frac{t(x)^2 - t(x^2)}{2}$ for $x \in G$. We will show that (t, d) satisfy the trace-determinant identity (easy) and that d is multiplicative (less easy).

Lemma A.4. *For any a, b in G,*

1. $S_3(t)(a, a, b) = 2\Big(d(a)t(b) + t(a^2b) - t(a)t(ab)\Big)$
2. $S_3(t)(a, b, ab) = t(a)t(b)t(ab) + t(a^2b^2) - t(a)t(a^2b) - t(b)t(ab^2) - 2d(ab)$

R-to-C: Trace-determinant identity: Let x and y in G be arbitrary. By the first part of the lemma above with $a = x$ and $b = x^{-1}y$,

$$S_3(t)(x, x, x^{-1}y) = 2\Big(d(x)t(x^{-1}y) + t(xy) - t(x)t(y)\Big).$$

Since $S_3(t)(x, x, x^{-1}y) = 0$ and 2 is invertible, the trace-determinant identity holds for x and y.

R-to-C: d is a group homomorphism: Again, let x and y in G be arbitrary. I claim that

$$\begin{aligned} S_4(t)(x, y, x, y) + 4S_3(t)(x, y, xy) &= t(y)\, S_3(t)(x, x, y) + 2S_3(t)(x, y, xy) - S_3(t)(x, x, y^2) \\ &= 4\Big(d(x)d(y) - d(xy)\Big). \end{aligned}$$

Indeed, the general identity from the remark above for $n = 3$ reduces to

$$S_4(t)(a, b, c, d) = t(d)S_3(t)(a, b, c) - S_3(t)(ad, b, c) = S_3(t)(a, bd, c) - S_3(t)(a, b, cd)$$

for any a, b, c, d in G, which essentially immediately implies the equality of the two expressions on the first line. The first part of the lemma above applied twice, the first time for $a = x$ and $b = y$, and the second for $a = x$ and $b = y^2$, along with the second part of the lemma applied for $a = x$ and $b = y$, combined with the definition of $d(y)$, establishes the rest of the identity.

Since $S_3(t) \equiv 0$, the middle expression is identically 0; since 4 is invertible, this forces $d(x)d(y) = d(xy)$. Finally, $d(1) = \frac{t(1)^2 - t(1^2)}{2} = 1$, which means that d really is a group homomorphism.

Chenevier implies Rouquier Suppose $(t, d) : G \to A$ is a Chenevier pseudorepresentation of dimension 2. Note that, since 2 is invertible in A, this automatically implies that $d(x) = \frac{1}{2}\left(t(x)^2 - t(x^2)\right)$ (Lemma A.2).

Since we're assuming that $t(1) = 2$ and 2 invertible in A, it's also easy to see that t is not multiplicative: if t *were* multiplicative, then $2 = t(1) = t(1^2) = t(1)^2 = 4$ in A, which isn't true since 2 is a unit.

In other words, the only thing to prove is the Frobenius identity. We simplify the computations slightly with a trick. Let $R = A[G]$, and extend t to R by linearity. Then $S_3(t)$ is a symmetric and multilinear function from R^3 to A. In the case where 3 is also invertible in A (in addition to 2), inclusion-exclusion-type expressions show that such a function is always determined by its values on the diagonal $R \hookrightarrow R^3$. Indeed, if $f : R^3 \to A$ is symmetric and multilinear, and $g : R \to A$ is defined by $g(x) = f(x, x, x)$, then

$$g(x + y + z) - g(x + y) - g(x + z) - g(y + z) + g(x) + g(y) + g(z) = 6f(x, y, z).$$

So if g is identically zero, and 6 is invertible, then f is identically zero as well.

However, we definitely want to establish this for rings of characteristic 3, so we can't assume that 3 is invertible. So we adapt this argument very slightly. We show instead that for any $x, y \in R$, we have $S_3(t)(x, x, y) = 0$. This is enough: again, if $f : R^3 \to A$ is symmetric multilinear, then

$$f(x + y, x + y, z) = 2f(x, y, z) + f(x, x, z) + f(y, y, z).$$

Since 2 is a unit in A, if f evaluates to zero whenever two of the arguments are the same, it is in fact identically zero on R^3.

It remains to establish that $S_3(t)(x, x, y)$ is always zero. But we already computed in the first part of Lemma A.4 that

$$\frac{S_3(t)(x, x, y)}{2} = d(x)t(y) + t(x^2y) - t(x)t(xy)$$

—and the latter expression is exactly the trace-determinant identity for the pair (x, xy), so known to be identically zero for a Chenevier pseudorepresentation of dimension 2. □

Appendix B

Solutions to linear recurrences over a field

The purpose of this chapter to give a proof of Proposition 4.5, restated below:

Recall that K is a field. If $P \in K[X]$ is monic, then P is the companion polynomial of a unique linear recurrence, so the two notions are conflated below.

Proposition B.1 (Repeat of Proposition 4.5)**.** *Suppose that $P \in K[X]$ factors as*

$$P(X) = (X - \alpha_1)^{e_1} \cdots (X - \alpha_r)^{e_r}$$

with $\alpha_1, \ldots, \alpha_r \in \overline{K}$ distinct. Then every solution to the recursion P in $\overline{K}^{\mathbb{N}}$ is a linear combination of the following $e_1 + \cdots + e_r$ solutions:

$$\left\{ \binom{n}{j} \alpha_i^{n-j} \right\}_n, \quad \text{with } 1 \leq i \leq r \text{ and } 0 \leq j < e_i.$$

Here $\binom{n}{j}$ is the integer-valued binomial coefficient function

$$n \mapsto \frac{n(n-1)(n-2)\cdots(n-j+1)}{j!}.$$

We continue to use the convention that $\alpha^0 = 1$ for all α; here we additionally insist that $\binom{n}{j}\alpha^{n-j} = 0$ if $j < n$ for all α as well.

In this section, we resort to the following notational trick: if A is a ring and $f : \mathbb{N} \to A$ is a function, then we will identify f with its sequence of values $(f(n))_n \in A^{\mathbb{N}}$. In particular, we'll always assume that n is the function variable.

B.1 Background on polynomial functions

For $k \geq 1$, let $x^{(k)} \in \mathbb{Q}[x]$ be the k^{th} binomial coefficient function:

$$x^{(k)} = \binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}.$$

Also set $x^{(0)} = 1$ and $x^{(k)} = 0$ for $k < 0$. Even though a priori the coefficients of $x^{(k)}$ as a *polynomial* are not integral, as a *polynomial function*, $x^{(k)}$ takes integers to integers. So $x^{(k)}$ is an *integer-valued polynomial*: a polynomial $f \in \mathbb{Q}[x]$ that takes $\mathbb{Z}$ to $\mathbb{Z}$.

Theorem B.2. *The functions $\{x^{(k)}\}_k$ are a $\mathbb{Z}$-basis for the space of all integer-valued polynomials.*

This theorem is attributed to Pólya, but the proof, which is given at the end of section B.2 below, uses only very simple calculus of finite differences, so the statement may well have been known to Newton much earlier.

For all k, the sequence $n^{(k)} = (n^{(k)})_n$ is an element of $\mathbb{Z}^{\mathbb{N}}$ and hence of $K^{\mathbb{N}}$ regardless of the characteristic of K. The first few sequences of binomial coefficient function values:

$$\begin{aligned}
n^{(0)} &= (1, 1, 1, 1, 1, 1, 1, 1, \ldots) \\
n^{(1)} &= (0, 1, 2, 3, 4, 5, 6, 7, \ldots) \\
n^{(2)} &= (0, 0, 1, 3, 6, 10, 15, 21, \ldots) \\
n^{(3)} &= (0, 0, 0, 1, 4, 10, 20, 35, \ldots) \\
n^{(4)} &= (0, 0, 0, 0, 1, 5, 15, 35, \ldots)
\end{aligned}$$

Lemma B.3. *The sequences $n^{(0)}, n^{(1)}, n^{(2)}, \ldots$ form a linearly independent set in $K^{\mathbb{N}}$.*

Proof. For $n < k$, we have $n^{(k)} = 0$; and $k^{(k)} = 1$. Linear independence follows. □

Note that the same is not true for the polynomial x^k: the set $\{1, n, n^2, n^3, \ldots\}$ of sequences in $K^{\mathbb{N}}$ is not linearly independent if $\operatorname{char} K = p$. Indeed, n and n^p define the same function from $\mathbb{N}$ to K. Binomial coefficient functions fix this exact problem.

Lemma B.4. *If $\operatorname{char} K = 0$ or if $\operatorname{char} K > k$, then the span of the sequences*

$$\{1, n, n^{(2)}, n^{(3)}, \ldots n^{(k)}\}$$

is the same as the span of

$$\{1, n, n^2, n^3, \ldots, n^k\}.$$

Proof. The sets $\{1, x, x^2, \ldots, x^k\}$ and $\{1, x, x^{(2)}, \ldots, x^{(k)}\}$ both span the space of polynomials of degree bounded by k inside $\mathbb{Z}[\frac{1}{k!}][x]$.

□

B.2 General form of a recurrence sequence

Proposition B.5. *Let $P(X) \in K[X]$ be a polynomial defining a linear recurrence of order d. Suppose that $P(X)$ factors over $\overline{K}$ as*

$$P(X) = (X - \alpha_1)^{e_1} (X - \alpha_2)^{e_2} \cdots (X - \alpha_r)^{e_r}$$

with the $\alpha_i \in \overline{K}$ distinct.

Then $s \in \overline{K}^{\mathbb{N}}$ is a solution to the recurrence defined by P if and only if s is a $\overline{K}$-linear combination of the d linearly independent solutions

$$n^{(0)}\alpha_i^n, \quad n^{(1)}\alpha_i^{n-1}, \quad \ldots, \quad n^{(e_i-1)}\alpha_i^{n-e_i+1} \qquad \text{as } i \text{ runs over } 1, 2, \ldots, r.$$

Proof. As before, we have to show that $n^{(k)}\alpha_i^{n-k}$ is a solution for $k < e_i$, and that the d solutions given are linearly independent. For the first, see Lemma B.6 below combined with Proposition 4.7. For the second, we need the invertibility of a generalized Vandermonde matrix; see section B.3. □

In other words, the space of recurrence sequences contains the algebraic span of all polynomial functions and all geometric sequences.

Lemma B.6. *Let α be any element of K, and consider the recurrence equation with polynomial $P(X) = (X-\alpha)^d$. Then the sequence $n^{(k)}\alpha^{n-k}$ is a solution to the recursion for any $k < d$.*

Proof. We continue the methods of the proof of Proposition 4.7: let E be the shift-left operator on $K^{\mathbb{N}}$; then $f \in K^{\mathbb{N}}$ is a solution to the recursion defined by $P \in K[X]$ if and only if $P(E)\, f = 0$

Let $\Delta = E - 1$ be the finite difference operator, a discrete analog of differentiation. We first show that

$$\Delta n^{(k)} = n^{(k-1)}.$$

Indeed,

$$\Delta n^{(k)} = \Delta \binom{n}{k} = \binom{n+1}{k} - \binom{n}{k} = \binom{n}{k-1} = n^{(k-1)}.$$

By induction, $\Delta^d n^{(k)} = n^{(k-d)}$, so that $\Delta^d n^{(k)} = 0$ if an only if $k < d$. This proves the lemma for $\alpha = 1$. The general case is analogous:

$$(E - \alpha)\left(n^{(k)}\alpha^{n-k}\right) = \binom{n+1}{k}\alpha^{n-k+1} - \alpha\binom{n}{k}\alpha^{n-k} = n^{(k-1)}\alpha^{n-k+1}$$

so that $(E-\alpha)^d \left(n^{(k)}\alpha^n\right) = n^{(k-d)}\alpha^{n-d}$.

In other words, $n^{(k)}\alpha^n$ is a solution to the recursion if and only if $k < d$.

□

The finite difference operator gives a way to prove Theorem B.2:

Proof of Theorem B.2. By Lemma B.4, any integer-valued polynomial $f \in \mathbb{Q}[x]$ of degree d can be written as $\sum_{k \le d} a_k n^{(k)}$, with the $a_k \in \mathbb{Q}$. (Recall that we're identifying polynomial functions like $x^{(k)}$ with their sequence of values on integers, a perfectly reasonable thing to do over $\mathbb{Q}$.) Moreover, $a_0 = f(0) \in \mathbb{Z}$.

It is clear that the discrete difference operator Δ takes polynomials to polynomials, and it certainly preserves

the space of integer-valued polynomials. Therefore $\Delta f = \Delta \sum_{k \le d} a_k n^{(k)} = \sum_{k \le d} a_k n^{(k-1)}$ is an integer-valued polynomial, and hence $a_1 = (\Delta f)(0) \in \mathbb{Z}$. By induction $a_k = (\Delta^k f)(0) \in \mathbb{Z}$ for every k. □

B.3 Invertibility of the generalized Vandermonde matrix

In this section, we prove a lemma necessary for Proposition B.5. We will show that a certain type of generalized Vandermonde matrix is invertible.

We first define the matrix. Fix a positive integer r and positive integers $e_1, \ldots, e_r$; the matrix will have dimension $d = e_1 + \cdots + e_r$. For any ordered r-tuple $(\alpha_1, \ldots, \alpha_r)$ of elements of K we define the $d \times d$ matrix $V_{e_1,\ldots,e_r}(\alpha_1, \ldots, \alpha_r)$ by listing d functions $f : \mathbb{N} \to K$; the entries of the each column will be the value $f(n)$ for $0 \le n \le d$. The first e_1 functions are

$$n^{(0)}\alpha_1^n, \qquad n^{(1)}\alpha_1^{n-1}, \quad \ldots \quad , n^{(e_1-1)}\alpha_1^{n-e_1+1}.$$

Then next e_2 functions are

$$n^{(0)}\alpha_2^n, \qquad n^{(1)}\alpha_2^{n-1}, \quad \ldots \quad , n^{(e_2-1)}\alpha_2^{n-e_2+1}.$$

And so on; the last e_r functions are, of course,

$$n^{(0)}\alpha_r^n, \qquad n^{(1)}\alpha_r^{n-1}, \quad \ldots \quad , n^{(e_r-1)}\alpha_r^{n-e_r+1}.$$

For example,

$$V_{3,2,1}(a,b,c) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ a & 1 & 0 & b & 1 & c \\ a^2 & 2a & 1 & b^2 & 2b & c^2 \\ a^3 & 3a^2 & 3b & b^3 & 3b^2 & c^3 \\ a^4 & 4a^3 & 6b^2 & b^4 & 4b^3 & c^4 \\ a^5 & 5a^4 & 10b^3 & b^4 & 5b^4 & c^5 \end{pmatrix}.$$

If $e_i = 1$ for all i, we get the usual Vandermonde matrix.

Proposition B.7. *If $\alpha_1, \ldots, \alpha_r$ are distinct, then the generalized Vandermonde matrix $V_{e_1,\ldots,e_r}(\alpha_1, \ldots, \alpha_r)$ is invertible.*

The proposition establishes the linear independence of the solutions given in Proposition B.5, whose first d entries are scalar multiples of the columns in the generalized Vandermonde matrix. The argument below is adapted from the elegant one given by user Taar on Math.stackexchange* to the case of arbitrary characteristic.

To prove the lemma, we first define a variation on formal derivative operators on polynomials. For a nonnegative integer k, define the operator d_k on $K[x]$ by setting $d_k(x^n) = \binom{n}{k} x^{n-k}$ and extending by linearity. For comparison to the usual formal derivative d defined by $d(x^n) = nx^{n-1}$, we have $k! d_k = d^k$.

Lemma B.8 (Leibniz rule)**.** *For any $k \ge 0$ and any $f, g \in K[x]$,*

$$d_k(fg) = \sum_{i+j=k} d_i(f) d_j(g).$$

*`http://math.stackexchange.com/questions/654324`, "Determinant (and invertibility) of generalized Vandermonde matrix."

For comparison, the usual Leibniz rule for d^k is $d^k(fg) = \sum_{i+j=k} \binom{k}{i} d^i(f) d^j(g)$.

Proof. By linearity, it suffices to prove the formula for $f = x^n$ and $g = x^m$. The left-hand side gives $\binom{n+m}{k} x^{n+m-k}$; the right-hand side is

$$\sum_{i+j=k} \binom{n}{i}\binom{m}{j} x^{n+m-k}.$$

Equality follows: for example, one can think combinatorially about choosing a k-subset from the (disjoint) union of an n-set and an m-set. □

Lemma B.9 (Raison d'être of d_k)**.** *Let f be a polynomial in $K[x]$, and suppose for some $\alpha \in \overline{K}$ we have*

$$f(\alpha) = d_1 f(\alpha) = d_2 f(\alpha) = \cdots = d_{n-1} f(\alpha) = 0.$$

Then $(x-\alpha)^n$ divides $f(x)$.

Proof. Write $f(x) = (x-\alpha)^m g(x)$ with $g(\alpha) \neq 0$. First use induction with the Leibniz rule to conclude that $d_k(x-\alpha)^m = \binom{m}{k}(x-\alpha)^{m-k}$. Next, the Leibniz rule again gives

$$d_k f(x) = \sum_{i+j=k} d_i (x-\alpha)^m \, d_j g(x) = \sum_{i+j=k} \binom{m}{i} (x-\alpha)^{m-i} \, d_j g(x)$$

Evaluate at α successively for $k = 0, 1, \ldots, n-1$ to conclude that $m > k$. □

Finally, we are ready to prove the invertibility of the generalized Vandermonde matrix.

Proof of Lemma B.7. Write $V = V_{e_1,\ldots,e_r}(\alpha_1, \ldots, \alpha_r)$. Let $c = (c_0, \ldots c_{d-1}) \in K^d$ be a row vector so that $c \cdot V = (0, \ldots, 0)$. Define the polynomial

$$f(x) = c_0 + c_1 x + \cdots + c_{d-1} x^{d-1} \in K[x].$$

Then the condition $c \cdot V = 0$ considered column by column exactly says that, for all i,

$$f(\alpha_i) = d_1 f(\alpha_i) = \cdots = d_{e_i - 1} f(\alpha_i) = 0.$$

By Lemma B.9, $(x-\alpha_i)^{e_i}$ divides f for each i. Since the α_i are distinct, we in fact have $\prod_i (x-\alpha_i)^{e_i}$ dividing f as well. But $\prod_i (x-\alpha_i)^{e_i}$ has degree d, and $\deg f$ is explicitly less than d. This means that $f = 0$, so that $c = 0$ and the rows of V are linearly independent.

□

In fact, one can also show that

$$\det V_{e_1,\ldots,e_r}(\alpha_1, \ldots, \alpha_r) = \prod_{i<j} (\alpha_i - \alpha_j)^{e_i e_j}.$$

For a proof of this determinant formula in the case where $\operatorname{char} K = 0$, see `http://www.garretstar.com/secciones/publications/docs/generalized_Vandermonde.pdf`. The general case follows since the determinant is is a polynomial function in the $\alpha_1, \ldots, \alpha_r$ and the formula is true over $\mathbb{Z}$.

Appendix C

Notes on α

Here we discuss some computational aspects of the special-shape Nilpotence Growth Theorem. The form we will discuss is stated below.

Theorem C.1 (*cf.* Theorem 5.2 and sections 5.2 and 5.4)**.** *Suppose T is a degree-lowering linear operator on $\mathbb{F}[y]$ so that the sequence $\{T(y^n)\}_n$ satisfies a linear recursion whose companion polynomial has the shape*

$$X^d + ay^d + (\textit{terms of total degree} \leq d - D)$$

for some $D \geq 1$ and some constant $a \in \mathbb{F}$. Suppose also that either $d = b$ or $d = b - 1$ for some p-power b, and $D < b - 1$. Then

$$N_T(y^n) \leq c_T(n) \asymp n^{\log_b(b-D)},$$

where $c_T(n) = c_{b,D}(n)$ if $d = b$ and $c_T = (b - D - 1)c_{b,D}\left(\frac{n}{d}\right)$ if $d = b - 1$.

For T satisfying the conditions of the theorem, let $\alpha(T) = \min\{\alpha : N_T(y^n) \ll n^\alpha\}$. Also, let

$$\alpha(d, D) := \max\{\alpha(T) : T \text{ satisfies the conditions of Theorem C.1 with } d, D\}.$$

If d is a power of p or d is less than a power of p, then clearly $\alpha(d, D) \leq \log_b(b - D)$. The question we briefly computationally investigate here is whether $\alpha(d, D) = \log_b(b - D)$.

C.1 Case $d = p$

Computationally, it appears that $\alpha(p, D) = \log_p(p - D)$. More surprisingly, it appears that one can always find a T so that $N_T(y^n) = c_T(y^n)$ on the nose, if not always then infinitely often. Here are some of these maximal examples. In each case, we use the initial values $[0, 1, y, y^2, \ldots, y^{p-2}]$. We will focus on $D = 1$.

- $p = 2$: This is outside the purview of the theorem since $b - D = 1$, but $c_{2,1}(n)$ is the sum of the digits of n base 2, so that $c_{2,1}(n) \asymp \log_2(n)$. The recursion operator T with
$$P_T = X^2 + X + y^2$$
and initial values $[0, 1]$ appears to achieve $N_T(y^n) = c_T(n)$ infinitely often.
- $p = 3$: The recursion operator T with $P_T = X^3 + yX - y^3$ and initial values $[0, 1, y]$ appears to achieve

$N_T(y^n) = c_T(n)$ infinitely often. For $n < 10000$, I compute that $N_T(y^n)$ is equal to $c_T(n)$ over 60% of the time, and never differs by more than 7.

- $p = 5$: The recursion operator T with $P_T = X^5 + 3yX^3 + y^2X^2 + 3y^3X + 4y^5$ and initial values $[0, 1, y, y^2, y^3]$ appears to achieve $N_T(y^n) = c_T(n)$ for "most" n: every counterexample n has 0s in its base-5 expansion, and $c_T(n) - N_T(y^n) \leq 2$ for all $n < 1000$.
- $p = 7$: The recursion operator T with $P_T = X^7 + 3y^2X^4 + 6y^3X^3 + 5y^4X^2 + 3y^5X + 6y^7$ appears to achieve $N_T(y^n) = c_T(n)$ for most n. For $n < 1000$, there are only 36 counterexamples, and $c_T(n) - N_T(y^n) \leq 3$ for each one.
- $p = 11$. The recursion operator T with

$$P_T = X^{11} + 6yX^9 + 2y^2X^8 + 3y^3X^7 + 6y^4X^6 + 8y^6X^4 + y^8X^2 + 9y^9X + 10y^{11}$$

appears to achieve $N_T(y^n) = c_T(n)$ for most n. For $n < 1000$, there are only 8 counterexamples, and $N_T(y^n) = c_T(n) - 1$ for each one.

C.2 Other cases

If $d = p^2$, it is less clear what is happening. One guess is that as p grows, it becomes easier to find examples with $N_T(y^n)$ a lot like $c_T(n)$, but it's not clear if that is just for small n. A few examples that look maximal.

- $p = 2$: The recursion operator T with $P_T = X^4 + y^4 + y^3$ and initial values $[0, 1, y, y^2]$ appears to have $\alpha(T) \approx 0.71$, whereas $\log_b(b-1) = 0.792$.
- $p = 3$. The recursion operator T with $P_T = X^9 + 2y^2X^6 + y^3X^5 + 2y^5X^3 + y^6X^2 + 2y^7X + 2y^9$ and initial valuess $[0, 1, y, \ldots, y^7]$ appears to have $\alpha(T) < 0.92$, whereas $\log_b(b-1) = 0.946$.
- $p = 5$ The recursion operator with

$$\begin{aligned} P_T = X^{25} &+ 2yX^{23} + y^2X^{22} + 2y^3X^{21} + 2y^5X^{19} + y^6X^{18} + 4y^7X^{17} + 2y^8X^{16} \\ &+ 4y^9X^{15} + y^{10}X^{14} + 3y^{11}X^{13} + 4y^{12}X^{12} + 3y^{16}X^8 + 4y^{18}X^6 + y^{19}X^5 \\ &+ 4y^{21}X^3 + y^{22}X^2 + 4y^{23}X + 4y^{25} \end{aligned}$$

has $N_T(y^n) = c_T(n)$ for $n < 125$. For $125 \leq n < 1000$, the difference $c_T(n) - N_T(y^n)$ is bounded by 31: compare to $c_T(1000) = 936$. Unclear if this is a small-n noise or not.

For $d = p^k - 1$, I simply record a few examples that seem to have high growth (though probably not as high as c_T) for further investigation later.

- $p = 3$, $d = 2$: $P_T = X^2 + X + y^2 + 2y$
- $p = 2$, $d = 3$: $P_T = X^3 + X^2 + yX + y^3 + y$.
- $p = 2$, $d = 7$: $P_T = X^7 + X^6 + X^5 + X^4 + (y^3 + y^2)X^3 + y^4X^2 + y^4X + y^7$

Appendix D

Proof of Theorem 5.21

We prove Theorem 5.21, restated below, using Proposition 5.12.

D.1 Statement of the theorem

Theorem D.1 (Theorem 5.21)**.** *Let $T : \mathbb{F}[y] \to \mathbb{F}[y]$ be a degree-lowering recursion operator so that the sequence $\{T(y^n)\}$ satisfies a linear recursion of order d where d is prime to p and such that the companion polynomial has the shape*

$$X^d + ay^d + (\textit{terms of total degree} \leq d - D)$$

for some constant $a \in \mathbb{F}$ and some $D \geq 1$. Let $k = \lceil \log_p d \rceil$, so that $d \leq p^k = b$. Then if $\boxed{D < \frac{b}{2}}$, then

$$N_T(y^n) = O(n^{\log_b(b-D)}).$$

More precisely,

$$N_T(y^n) < \frac{(b-1)(b-D)\big((b-D)^\ell - 1\big)}{d^{\log_b(b-D)}(b-1-D)} n^{\log_b(b-D)} + \frac{(b-1)\big((b-D)^\ell - 1\big)}{b-D-1},$$

where ℓ is the multiplicative order of b modulo d.

Why is this theorem necessary? It isn't, but it gives a somewhat better upper bound for the nilpotence growth.

How much better? Suppose $\ell \neq p$ is prime, and we have a polynomial

$$P(X) = X^\ell - y^\ell + (\text{terms of total degree} < \ell).$$

Since $x^\ell - 1$ divides $x^{p^f - 1} - 1$ in $\mathbb{F}_p[x]$ if and only if ℓ divides $p^f - 1$, we will find that the $\alpha < 1$ guaranteed by Theorem 5.19 is $\frac{\log(p^f-1)}{\log(p^f)}$, where f is the multiplicative order of p modulo ℓ, and may be as high as $\ell - 1$ if p happens to be a generator in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. On the other hand, the α guaranteed by Theorem D.1 is $\frac{\log(p^k-1)}{\log(p^k)}$ where p^k merely has to be greater than ℓ.

For an example of this phenomenon, take $p = 3$ and $\ell = 7$. Since 3 is a generator mod 7, we are comparing

$\alpha = \log_{729} 728 = 0.9998$ from Theorem 5.19 with $\alpha = \log_9(8) = 0.9464$ from Theorem 5.21. Is this dramatic enough to warrant several more pages of technical lemmas? A question only the dedicated reader who has made it this far can answer. The ultimate goal would be to get a better bound still, and Theorem 5.21 is a small step in the right direction. For example, let $P(X) = X^7 + yX^5 + yX - y^7$, and let $T(y^n) = y^{n-1}$ for $1 \le n < 7$. Computations with `SAGE` suggest that $N_T(y^n)$ is multiplied by about 2.6 every time that n is multiplied by 7, which gives an $\alpha \approx 0.88$. The real coup would be to approach this bound.

D.2 Proof of the theorem

The proof proceeds exactly the same as before. We set b be the smallest power of p not less than d. We will assume that $\boxed{D \le \frac{b-1}{2}}$. Let $M = (b-D)^\ell - 1$, where ℓ is the multiplicative order of b modulo d. Finally, we set

$$c_T(n) := M c_{b,D}\Big(\frac{n}{d}\Big)$$

as usual. We will eventually show that c_T satisfies all the properties of Proposition 5.12.

D.2.1 Preliminaries

We begin with a general and very satisfying lemma about comparing how the content function changes when you add or subtract arguments.

The question of how (b, D)-content changes when we add or subtract integers can be answered completely. Write two nonnegative integers m and n base b as $m = [m_\ell\, m_{\ell-1}\, \cdots\, m_1\, m_0]$ and $n = [n_\ell\, n_{\ell-1}\, \cdots\, n_1\, n_0]$, possibly padding one of the expressions with initial zeros so that they have the same number of digits. Define $r_b(m,n) = [r_\ell\, r_{\ell-1}\, \cdots\, r_1\, r_0]$ as the number whose base-b expansion is the tuple of carry digits when m is added to n base b. That is, let $s = [s_{\ell+1}\, s_\ell\, \cdots\, s_0]$ be the base-b expansion of $s = m+n$, and define $r_i \in \{0,1\}$ implicitly and inductively via $m_0 + n_0 = s_0 + r_0\, b$ and $m_i + n_i + r_{i-1} = s_i + r_i\, b$ for $i \ge 1$. Finally, for any tuple $r = [r_\ell\, \cdots\, r_0]$, we will write $c_{b,D}(r) = \sum_{i=0}^{\ell} (b-D)^i r_i$, so that $c_{b,D}(n) = c(\text{base-}b \text{ expansion of } n)$.

Lemma D.2. *With $r_b(m,n)$ as above,*

$$c_{b,D}(m+n) = c_{b,D}(m) + c_{b,D}(n) - D\, c_{b,D}\big(r_b(m,n)\big).$$

Proof. A clean computation. Let $s = m+n$ and $r = r_b(m,n)$. Recall that we have

$$m_0 + n_0 = s_0 + r_0 b = s_0 + D\, r_0 + r_0(b-D)$$
$$\text{and} \qquad m_i + n_i + r_{i-1} = s_i + r_i b = s_i + D\, r_i + r_i(b-D) \qquad \text{for } i \ge 1.$$

Multiplying the i^{th} equation by $(b-D)^i$ and adding up the sides of the equalities, we get

$$c_{b,D}(m) + c_{b,D}(n) + \sum_{i\ge 1} r_{i-1}(b-D)^i = c_{b,D}(s) + D\, c_{b,D}(r) + r_0(b-D) + \sum_{i\ge 1} r_i (b-D)^{i+1}.$$

The extraneous terms on each side cancel to finish the proof. □

Next, a simple lemma about the base-b expansion of fractions with denominator d.

Lemma D.3. *Let b be a base and d a denominator prime to and less than b.*

1. *Any fraction $\frac{i}{d}$ with $0 < i < d$, has no zeros in its base-b expansion.*
2. *Write $\frac{i}{d}$ with $0 < i < d$ as $\frac{i}{d} = \frac{m}{b^\ell - 1}$ with ℓ minimal. Then all the digits of m base b are distinct.*

Proof.

1. The first digit of $\frac{i}{d}$ after the radix (i.e., "decimal") point is $\lfloor \frac{ib}{d} \rfloor$, which is at least 1 since $d < b$. This division $ib \div d$ has a remainder r, which is at least 1 since d is prime to b. The second digit is $\lfloor \frac{rb}{d} \rfloor$, which is again at least 1, and the remainder is again at least 1, for the same reasons. And so on.
2. Write $\frac{i}{d} = [0.a_0\, a_1\, a_2 \cdots]_b$, so that $m = [a_0 \cdots a_{\ell-1}]_b$. The digits a_i are obtained by Euclid's algorithm: $ib = a_0 d + r_0$ with and then for $n > 0$, we have $r_{n-1} b = a_n d + r_n$; at each step, $r_n < d$ and $a_n < b$. Suppose $a_j = a_k$ for some j, k. I claim that this forces $r_j = r_k$, so that j and k are a multiple of ℓ apart. Indeed, we know that $a_j d$ is r_j less than a multiple of b for some $r_j < d < b$. This defines r_j uniquely, and since $a_k d$ has the same relationship to r_k, we must have $r_k = r_j$. By induction $a_{j+n} = a_{k+n}$ for all integer $n \geq -j, -n$, both positive and negative. Since ℓ is the length of the period, the claim follows.

□

D.2.2 The properties of Proposition 5.12

Throughout, base $b > 2$ is a power of p, descent D is an integer, and d is a denominator prime to and less than b. We also let ℓ be the multiplicative order of b modulo d, and m be the integer defined by $\frac{1}{d} = \frac{m}{b^\ell - 1}$. Moreover, for i, j integers between 0 and d, let $r_{i,j} = r = r_b\big(im, jm\big)$, the carry digits when im and jm are added together. Finally, write $c = c_{b,D}$.

Lemma D.4 (Property (4))**.** *If* $\boxed{D \leq \frac{b}{2}}$*, then*

$$0 = c(0) < c\left(\frac{1}{d}\right) < c\left(\frac{2}{d}\right) < \cdots < c\left(\frac{d-2}{d}\right) < c\left(\frac{d-1}{d}\right).$$

The lemma is not generally true if $D > \frac{b}{2}$. Here is the simplest counterexample: for $(b, D) = (7, 5)$, we have $\frac{1}{5} = \frac{480}{7^4 - 1} = [0.\overline{1254}]_7$. It's easy to check that $c_{7,5}\big(\frac{2}{5}\big) = c_{7,5}\big(\frac{3}{5}\big) = 3$. Worse yet,

$$c_{11,9}\left(\frac{3}{7}\right) = \frac{39}{7} > \frac{31}{7} = c_{11,9}\left(\frac{4}{7}\right).$$

Proof. We show that for integers j and i with $0 \leq j < i < d$, we have $c\big(\frac{j}{d}\big) < c\big(\frac{i}{d}\big)$.

Since d is prime to b, we know that $\frac{1}{d}$ is purely periodic, say, of period $\ell \leq 1$. This means that there exists an integer m with exactly ℓ digits in its base-b expansion (because $\frac{1}{d} > \frac{1}{b}$), so that $\frac{1}{d} = \frac{m}{b^\ell - 1}$. Moreover,

$$c\big(\tfrac{1}{d}\big) = \frac{c(m)}{(b-D)^\ell - 1},$$

and

$$c\big(\tfrac{i}{d}\big) = \frac{c(i\,m)}{(b-D)^\ell - 1};$$

observe that, for i in the range $1 \leq i < d$, the integer $i\,m$ still has exactly ℓ digits in its base-b expansion.

It therefore remains to show that, for integers $1 \leq j < i \leq d - 1$, we have $c(j\,m) < c(i\,m)$. Of course, it's enough to do this for $i = j + 1$. Here we use Lemma D.2: we know that $c\big((j+1)\,m\big) - c(j\,m) = c(m) - D\,c(r)$,

where $r = r_{j,1}$ is the number whose base-b expansion keeps track of the carry digits when jm and m are added together base b. So the statement is proved as soon as we establish that $c(m) > D\,c(r)$.

As observed above, m, jm, and $im = jm + m$ all have exactly ℓ digits base b. This means that the topmost carry digit of the addition problem $jm + m$ is $r_{\ell-1} = 0$. The rest of the r_is are all 0s and 1s, so that

$$D\,c(r) \le D\sum_{i=0}^{\ell-2}(b-D)^i = \frac{D}{b-D-1}\big((b-D)^{\ell-1}-1\big).$$

On the other hand, since $d < b$, we know that the first digit of m is at least 1, so that $c(m) \ge (b-D)^{\ell-1}$. Since we're assuming that $\frac{D}{b-D-1} \le 1$, the desired inequality follows.

To extend the inequality to all $D \le \frac{b}{2}$, we use part (1): since every digit of m is nonzero, we know that actually

$$c(m) \ge \sum_{i=0}^{\ell-1}(b-D)^i = \frac{1}{b-D-1}\big((b-D)^{\ell}-1\big).$$

So this sequence of inequalities also holds if $(b-D)^\ell - 1 > D\big((b-D)^{\ell-1}-1\big)$: for example if $1 < D \le b-D$, or, equivalently, $1 < D \le \frac{b}{2}$. But since $\frac{b-1}{2} < D < 1$ implies that $b < 3$, and we're assuming that $b > 2$, we don't have to worry about the condition $D > 1$ in the region $\frac{b-1}{2} < D \le \frac{b}{2}$.

□

Lemma D.5. *For all descents D, we have $c\left(\dfrac{d-D}{d}\right) \le 1$, with equality if and only if $d = b-1$.*

Proof. We want to prove that $c\left(\dfrac{d-D}{d}\right) = \dfrac{c\big((d-D)m\big)}{(b-D)^\ell - 1} \le 1$. Since $dm = b^\ell - 1 = [b-1\ \cdots b-1]$ and m has no zero digits, we know that

$$c\big((d-D)m\big) \le (b-D-1)\sum_{i=0}^{\ell-1}(b-D)^i = \big((b-D)^\ell - 1\big),$$

with equality if and only if $m = [1\ \cdots\ 1]$: that is, if $d = b-1$. Indeed, if $d < b-1$, then Lemma D.3 guarantees that one of the first two base-b digits of m is at least a 2, which will leave $(d-D)m$ with either its first or second digit strictly less than $b-D-1$, either of which is enough.* □

Lemma D.6 (Property (1))**.** *Let b be a base, $D \le b-3$ a descent, and denominator $d < b$ and prime to b. Moreover, we have two integers $0 \le j \le i - D < i < d$ and two nonnegative integers A and B so that both*

*Lemma D.3 guarantees that $\frac{1}{d} \ge [0.1\,2\,3\,\cdots\ell]_b$. This is a relatively crude estimate. In fact, if $\frac{1}{d} = [0.12\ldots]_b$, then $d = b-2$ and each digit after the decimal point is at least double the previous one (unless of course this doubling exceeds b). But this estimate $\frac{1}{d} \ge [0.1\,2\,3\,\cdots\ell]_b$ easy to work with because we know that ℓ is a digit base b: since ℓ is the multiplicative order of b mod d, we know that $\ell \le \varphi(d) < d < b$. Alternatively, Lemma D.3 implies $\ell < b$ as well. In any case, $c(m) \le \sum_{i=1}^{\ell} i(b-D)^{\ell-i}$. We derive how to compute this type of sum:

$$\sum_{n=1}^{N} nx^{n-1} = \sum_{n=1}^{\infty} nx^{n-1} - \sum_{n=N+1}^{\infty} nx^{n-1} = \sum_{n=1}^{\infty} nx^{n-1} - x^N\sum_{n=1}^{\infty} nx^{n-1} - Nx^N\sum_{n=0}^{\infty} x^n$$
$$= \frac{1}{(1-x)^2} - \frac{x^N}{(1-x)^2} - \frac{Nx^N}{1-x} = \frac{1-(N+1)x^N+Nx^{N+1}}{(1-x)^2}$$

$A+i$ and $B+j$ are strictly less than d. Then

$$c_{b,D}\left(\frac{A+i}{d}\right) - c_{b,D}\left(\frac{A}{d}\right) > c_{b,D}\left(\frac{B+j}{d}\right) - c_{b,D}\left(\frac{B}{d}\right).$$

That is, not only is $c_{b,D}$ increasing on $\left\{0, \frac{1}{d}, \frac{2}{d}, \ldots, \frac{d-1}{d}\right\}$, but this increasing is "uniform" over the interval: what matters are relative jumps $\frac{i}{d}$ and $\frac{j}{d}$, not the starting points $\frac{A}{d}$ and $\frac{B}{d}$. The case $A = B = 0$ is Lemma D.4.

Proof. Write c for $c_{b,D}$. Let ℓ and m be as the proof of the previous lemma, and recall that, for $0 \le s < d$, we know that

$$c\Big(\frac{s}{d}\Big) = \frac{c(sm)}{(b-D)^\ell - 1}.$$

The desired inequality is therefore equivalent to the integer-content inequality

$$c\big((A+i)m\big) - c\big(Am\big) \stackrel{?}{>} c\big((B+j)m\big) - c\big(Bm\big).$$

Recall that, for integers s and t, we write $r_{s,t}$ for $r_b(sm, tm)$. By Lemma D.2, the left-hand side of the inequality above is equal to $c(im) - D\,c(r_{A,i})$, and the right-hand side to $c(jm) - D\,c(r_{B,j})$. In other words, the inequality above is equivalent to the inequality

$$c(im) - c(jm) \stackrel{?}{>} D\,c(r_{A,i}) - D\,c(r_{B,j}).$$

Using Lemma D.2 again, we replace $c(im) - c(jm)$ by $c\big((i-j)m\big) - D\,c(r_{j,i-j})$. By Lemma D.4, $c\big((i-j)m\big) \ge c(Dm)$, and certainly $D\,c(r_{B,j})$ is nonnegative. It therefore suffices to prove that

$$c(Dm) \stackrel{?}{>} D\,c(r_{A,i}) + D\,c(r_{j,i-j}).$$

Using the crude estimates at the end of the proof of Lemma D.4, we know that $c(Dm) \ge D(b-D)^{\ell-1}$ and that each of the terms on the right-hand side is bounded by $\frac{D}{b-D-1}\big((b-D)^{\ell-1} - 1\big)$. The condition $D \le b-3$ guarantees that $\frac{2}{b-D-1} \le 1$, which proves the last inequality. □

For the next two lemmas, let A, B, I, and J be integers satisfying $0 \le A, B, I, J, A+I, B+J < d$.

Lemma D.7. *If $I + J \le d - D$ and $D \le b - 2$, then*

1. $c\left(\frac{I}{d}\right) + c\left(\frac{J}{d}\right) \le 1$
2. *Property (2):* $c\left(\frac{A+I}{d}\right) - c\left(\frac{A}{d}\right) + c\left(\frac{B+J}{d}\right) - c\left(\frac{B}{d}\right) \le 1$

Proof. 1. If $d = b - 1$, then

$$c\left(\frac{I}{d}\right) + c\left(\frac{J}{d}\right) = \frac{I+J}{b-D-1} \le \frac{d-D}{b-D-1} = 1.$$

Otherwise, we need to look more carefully. We know that

Therefore, we know that

$$c(m) \le (b-D)^{\ell-1} \sum_{i=1}^{\ell} \frac{i}{(b-D)^{i-1}} = (b-D)^{\ell-1} \frac{1 - \frac{\ell+1}{(b-D)^\ell} + \frac{\ell}{(b-D)^{\ell+1}}}{\left(1 - \frac{1}{b-D}\right)^2} = \frac{(b-D)^2 - (\ell+1)(b-D) + \ell}{(b-D-1)^2}$$

Perhaps one can get even better bounds from this.

$$c\Big(\frac{I}{d}\Big)+c\Big(\frac{J}{d}\Big)=\frac{c\big((I+J)m\big)+D\,c(r_{I,J})}{(b-D)^\ell-1}\le\frac{c\big((d-D)m\big)+D\,c(r_{I,J})}{(b-D)^\ell-1}.$$

Since $dm=[b-1\ \cdots\ b-1]$, we know further that $c\big((d-D)m\big)=c(dm)-c(Dm)$. And on the other hand, $D\,c(r_{I,J})\le\frac{D}{b-D-1}\big((b-D)^\ell-1\big)$. Therefore, the numerator of $c\big(\frac{I}{d}\big)+c\big(\frac{J}{d}\big)$ is no more than

$$\begin{aligned}c\big((d-D)m\big)+D\,c(r_{I,J})&\le c(dm)-c(Dm)+\frac{D}{b-D-1}\big((b-D)^\ell-1\big)\\&=(b-1)\frac{(b-D)^\ell-1}{b-D-1}-D(b-D)^{\ell-1}+\frac{D}{b-D-1}\big((b-D)^\ell-1\big)\\&=(b-D)^{\ell-1}\Big(1+\frac{2D}{b-D-1}-D(b-D)^{\ell-1}\Big).\end{aligned}$$

Therefore, our claim is established as soon as we know that $D(b-D)^{\ell-1}\ge\frac{2D}{b-D-1}$. This is easily seen to be true provided that $\ell>1$ (the case $\ell=1$ was dispatched earlier) and $D\le b-2$, which we gladly assume.

2. As in the proof of Lemma D.6, we know that

$$c\Big(\frac{A+I}{d}\Big)-c\Big(\frac{A}{d}\Big)+c\Big(\frac{B+J}{d}\Big)-c\Big(\frac{B}{d}\Big)=c\Big(\frac{I}{d}\Big)+c\Big(\frac{J}{d}\Big)-\frac{D\,c(r_{A,I})+D\,c(r_{B,J})}{(b-D)^\ell-1}$$

If $I+J\le d-D$, then by the observation above and Lemma D.7,

$$c\Big(\frac{A+I}{d}\Big)-c\Big(\frac{A}{d}\Big)+c\Big(\frac{B+J}{d}\Big)-c\Big(\frac{B}{d}\Big)\le c\Big(\frac{I}{d}\Big)+c\Big(\frac{J}{d}\Big)\le 1.$$

□

Lemma D.8 (Property (3))**.** *If $I+J\ge d+D$ and $\boxed{D\le\frac{b-1}{2}}$, then*

$$c\Big(\frac{A+I}{d}\Big)-c\Big(\frac{A}{d}\Big)+c\Big(\frac{B+J}{d}\Big)-c\Big(\frac{B}{d}\Big)>1.$$

Proof. We know that

$$c\Big(\frac{I}{d}\Big)+c\Big(\frac{J}{d}\Big)=\frac{c\big((I+J)m\big)+D\,c(r_{I,J})}{(b-D)^\ell-1}.$$

If $I+J\ge d+D$, then $(I+J)m=dm+im=b^\ell-1+im$ for some $i\ge D$. Since im has ℓ base-b digits, we know that $c\big((I+J)m\big)=(b-D)^\ell+c(im-1)$; since im not divisible by b, this is further equal to

$$\begin{aligned}c(Im+Jm)&=c(b^\ell)+c(im)-1\\&\ge c(b^\ell)+c(Dm)-1\ge(b-D)^\ell+D(b-D)^{\ell-1}-1\end{aligned}$$

On the other hand, $c(r_{I,J})$ is certainly bounded below by $(b-D)^{\ell-1}$, so that the numerator of $c\big(\frac{I}{d}\big)+c\big(\frac{J}{d}\big)$ is at least

$$c(Im+Jm)+Dc(r_{I,J})\ge(b-D)^\ell-1+(D+1)(b-D)^{\ell-1}.$$

We also have

$$c\Big(\frac{A+I}{d}\Big)-c\Big(\frac{A}{d}\Big)+c\Big(\frac{B+J}{d}\Big)-c\Big(\frac{B}{d}\Big)=c\Big(\frac{I}{d}\Big)+c\Big(\frac{J}{d}\Big)-\frac{D\,c(r_{A,I})+D\,c(r_{B,J})}{(b-D)^\ell-1}.$$

Analyzing the extra terms as before, we have

$$D\,c(r_{A,I}) + D\,c(r_{B,J}) \le \frac{2D}{b-D-1} \cdot \big((b-D)^{\ell-1} - 1\big),$$

so that, if $I + J \ge d$,

$$c\left(\frac{A+I}{d}\right) - c\left(\frac{A}{d}\right) + c\left(\frac{B+J}{d}\right) - c\left(\frac{B}{d}\right) \ge \frac{(b-D)^{\ell} - 1 + (D+1)(b-D)^{\ell-1} - \frac{2D}{b-D-1}}{(b-D)^{\ell} - 1}.$$

In short, the claim is established provided that $(D+1)(b-D)^{\ell-1} \ge \frac{2D}{b-D-1}$. Certainly the left-hand side is at least 2, and under the assumption $D \le \frac{b-1}{2}$, the right-hand side is no more than 2. So we are done. □

This completes the Theorem-5.2-style part of Theorem 5.21. For the precise bounds, note that

$$\begin{aligned} c_T(n) &= \big((b-D)^{\ell} - 1\big) c_{b,D}\left(\frac{n}{d}\right) \\ &< \big((b-D)^{\ell} - 1\big)\left(\frac{(b-1)(b-D)}{b-1-D}\left(\frac{n}{d}\right)^{\log_b(b-D)} + \frac{b-1}{b-D-1}\right), \end{aligned}$$

which proves the claim.

Appendix E

Irreducible representation deforming a reducible pseudocharacter

Let G be a group, F a field with $\operatorname{char} F \neq 2$ and $\chi_1, \chi_2 : G \to F^\times$ two characters. Suppose that there exist cocycles $c_{12} \in \operatorname{Ext}^1_G(\chi_2, \chi_1)$ and $c_{21} \in \operatorname{Ext}^1_G(\chi 1, \chi_2)$ with the property that both Yoneda cup products $c_{12}c_{21}$ and $c_{21}c_{12}$ are nullhomologous in $\operatorname{Ext}^2_G(\chi_1, \chi_1)$ and $\operatorname{Ext}^2_G(\chi_2, \chi_2)$, respectively. We construct a representation $\rho : G \to \mathrm{GL}_2(F[\varepsilon])$ whose trace is an irreducible pseudocharacter $\operatorname{tr}\rho : G \to F[\varepsilon]$ deforming $\tau = \chi_1 + \chi_2$.

E.1 Cohomological computations

E.1.1 Ext-groups via cochains

For $i \geq 0$, let $\mathcal{C}^i$ be the space of *i-cochains* (that is, set maps) $G^i \to F$, and let $\mathcal{C} := \bigoplus_i \mathcal{C}^i$. This is a graded algebra with $\mathcal{C}^0 = F$ whose multiplication is defined as follows: if $a \in \mathcal{C}^i$ and $b \in \mathcal{C}^j$ then ab is in $\mathcal{C}^{i+j}$ with

$$ab(g_1, \ldots, g_{i+j}) = a(g_1, \ldots, g_i)b(g_{i+1}, \ldots, g_{i+j}).$$

Given two characters $\chi_1, \chi_2 : G \to F^\times$, we endow $\mathcal{C}$ with a differential operator $d : \mathcal{C} \to \mathcal{C}$, graded of degree 1, with $d^i : \mathcal{C}^i \to \mathcal{C}^{i+1}$ defined by

$$\begin{aligned}(d^i c)(g_1, \ldots, g_{i+1}) = \chi_1(g_1)c(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i}(-1)^j c(g_1, \ldots, \underbrace{g_j g_{j+1}}, \ldots, g_{i+1}) \\ + (-1)^{i+1}c(g_1, \ldots, g_i)\chi_2(g_{i+1}).\end{aligned}$$

One can check that $d^{i+1}d^i = 0$, so that $\mathcal{C}$ is a complex with differential d, and we can consider its cohomology. For $i = 0, 1, 2$, the i^{th} cohomology group gives us an explicit realization of $\operatorname{Ext}^1_G(\chi_2, \chi_1)$, described below.*

*I expect this is true for all i, but have not checked the details.

The first few graded pieces of $\mathcal{C}$ as a complex are

$$0 \to \mathcal{C}^0 \xrightarrow{d^0} \mathcal{C}^1 \xrightarrow{d^1} \mathcal{C}^2 \xrightarrow{d^2} \mathcal{C}^3 \to \cdots,$$

where the maps can be described explicitly:

$$\begin{aligned}(d^0c)(g) &= \chi_1(g)c - c\chi_2(g),\\ (d^1c)(g,h) &= \chi_1(g)c(h) - c(gh) + c(g)\chi_2(h),\\ (d^2c)(g,h,k) &= \chi_1(g)c(h,k) - c(gh,k) + c(g,hk) - c(g,h)\chi_2(k).\end{aligned}$$

Whence the first few cohomology groups:

$$\mathrm{Ext}^0_G(\chi_2,\chi_1) = \ker d^0 = \begin{Bmatrix} F & \text{if } \chi_1 = \chi_2 \\ 0 & \text{else} \end{Bmatrix},$$

$$\mathrm{Ext}^1_G(\chi_2,\chi_1) = \frac{\ker d^1}{\operatorname{im} d^0} = \frac{\{c \in \mathcal{C}^1 : c(gh) = \chi_1(g)c(h) + c(g)\chi_2(h)\}}{\{c \in \mathcal{C}^1 : c(g) = \chi_1(g)\, b - b\,\chi_2(g) \text{ for some } b \text{ in } F\}},$$

$$\mathrm{Ext}^2_G(\chi_2,\chi_1) = \frac{\ker d^2}{\operatorname{im} d^1} = \frac{\{c \in \mathcal{C}^2 : \chi_1(g)c(h,f) - c(gh,f) + c(g,hf) - c(g,h)\chi_2(f) = 0\}}{\{c \in \mathcal{C}^2 : c(g,h) = \chi_1(g)b(h) - b(gh) + b(g)\chi_2(h) \text{ for some } b \in \mathcal{C}^1\}}.$$

If χ_1 and χ_2 are understood, then, for a 1-cochain $c \in \ker d^1 \subset \mathcal{C}^1$, write $[c]$ for the corresponding element of $\mathrm{Ext}^1_G(\chi_2,\chi_1)$.

Ext^1 and representations

A 1-cochain c represents an element of $\mathrm{Ext}^1_G(\chi_2,\chi_1)$ if and only if

$$g \mapsto \begin{pmatrix} \chi_1(g) & c(g) \\ 0 & \chi_2(g) \end{pmatrix}$$

is a representation $G \to \mathrm{GL}_2(F)$. The isomorphism class of this representation depends only on the image of $[c]$ in the projectivization $\mathbb{P}\,\mathrm{Ext}^1_G(\chi_2,\chi_1)$.

E.1.2 Yoneda product via cochains

Let χ_1, χ_2, χ_3 be three characters $G \to F^\times$. From now on, we specify by writing d_{ij} for the differential giving $\mathrm{Ext}^\bullet_G(\chi_j,\chi_i)$ in cohomology.

Cochain multiplication satisfies a kind of graded Leibniz rule:

Lemma E.1. *If $a \in \mathcal{C}^i$ and $b \in \mathcal{C}^j$ are two cochains, then*

$$d^{i+j}_{13}(ab) = d^i_{12}(a)b + (-1)^i a\, d^j_{23}(b).$$

Proof. Computation, completely straightforward. □

In particular, if $i = j = 1$, then $d^2_{13}(ab) = d^1_{12}(a)b - a\, d^1_{23}(b)$: this the main form we will use.

Now if $c_{12} \in \mathcal{C}^1$ represents an element of $\mathrm{Ext}^1_G(\chi_2,\chi_1)$ and $c_{23} \in \mathcal{C}^1$ represents an element of $\mathrm{Ext}^1_G(\chi_3,\chi_2)$ are two 1-cocycles, then the 2-cochain $c_{12}c_{23} \in \mathcal{C}^2$ represents an element of $\mathrm{Ext}^1_G(\chi_3,\chi_1)$ that depends only

on $[c_{12}]$ and $[c_{23}]$. Indeed, by Lemma E.1,

$$d_{13}(c_{12}c_{23}) = d_{12}(c_{12})c_{23} - c_{12}\, d_{23}(c_{23}) = 0,$$

so that $c_{12}c_{23}$ is in $\ker d_{13}$. Moreover, if $c_{12} + d_{12}^0 a$ is another representative of $[c_{12}]$ for some $a \in \mathcal{C}^0$, then

$$\big(c_{12} + d_{12}^0(a)\big)\, c_{23} = c_{12}c_{23} + d_{12}^0(a)c_{23} = c_{12}c_{23} + d_{12}^0(a)c_{23} - a\, d_{23}^1(c_{23}) \tag{A}$$

$$= c_{12}c_{23} + d_{13}^1(a\, c_{23}), \tag{B}$$

where we've used Lemma E.1 again along with the fact that $d_{23}^1(c_{23}) = 0$ by definition. Adjusting the representative of $[c_{23}]$ works the same way.

Therefore multiplication of cochains descends to a map

$$\mathrm{Ext}_G^1(\chi_2, \chi_1) \otimes \mathrm{Ext}_G^1(\chi_3, \chi_2) \to \mathrm{Ext}_G^2(\chi_3, \chi_1),$$

corresponding to the Yoneda product of extension classes.

Nullhomologous Yoneda products

Suppose again that c_{12} and c_{23} are 1-cocycles in $\ker d_{12}$ and $\ker d_{23}$, respectively. Further suppose that we know that the product 2-cocycle $c_{12}\, c_{23}$ is nullhomologous in $\mathrm{Ext}_G^2(\chi_3, \chi_1)$ Then there exists a 1-cochain b trivializing this 2-cocycle, so that $c_{12}\, c_{23} = d_{13}b$. That is, for all $g, h \in G$,

$$c_{12}(g)c_{23}(h) = \chi_1(g)b(h) - b(gh) + b(g)\chi_3(h).$$

The choice of b is not unique, but any two 1-cochains b and b' trivializing $c_{12}c_{23}$ differ by a 1-cocycle in $\ker d_{13}^1$.

Finally, if c_{12} is replaced by another representative of $[c_{12}] \in \mathrm{Ext}_G^1(\chi_2, \chi_1)$, then the trivializing cochain b adjusts by an element of $\mathcal{C}^0\, c_{23} \subset \mathcal{C}^1$, that is, an F-scalar multiple of c_{23} (same reasoning as in equations (A)-(B) above). Similarly, replacing c_{23} by a cohomologous cocycle moves b by $c_{12}\mathcal{C}^0 \subset \mathcal{C}^1$. Therefore, if we only know $[c_{12}]$ and $[c_{23}]$, the trivializing cochain b is well-defined in $\mathcal{C}^1$ modulo $c_{12}\, \mathcal{C}^0 + \mathcal{C}^0\, c_{23}$, that is, modulo linear combinations of c_{12} and c_{23}.

We record a lemma about the trivializing cochain in the case that $\chi_1 = \chi_3$.

Lemma E.2. *Let c_{12} represent an element of $\mathrm{Ext}_G^1(\chi_2, \chi_1)$ and c_{21} represent an element of $\mathrm{Ext}_G^1(\chi_1, \chi_2)$ so that $c_{12}c_{21}$ is nullhomologous in $\mathrm{Ext}_G^2(\chi_1, \chi_1)$, with b in $\mathcal{C}^1$ a trivializing 1-cochain. Then $b' \in \mathcal{C}^1$ also trivializes $c_{12}c_{21}$ if and only if $(b - b')\chi_1^{-1}$ is an additive character of G.*

Proof. We know $b - b'$ is a 1-cocycle representing an element in $\mathrm{Ext}_G^1(\chi_1, \chi_1)$, which exactly means that $(b - b')\chi_1^{-1}$ is an additive character of G. □

E.1.3 A triple product computation

Now suppose $[c_{12}] \in \mathrm{Ext}_G^1(\chi_2, \chi_1)$ and $[c_{21}] \in \mathrm{Ext}_G^1(\chi_1, \chi_2)$ are such that both $c_{12}\, c_{21}$ and $c_{21}\, c_{21}$ are nullhomologous in $\mathrm{Ext}_G^2(\chi_1, \chi_1)$ and $\mathrm{Ext}_G^2(\chi_2, \chi_2)$, respectively. (This happens, for example, if both Ext^2s, which are isomorphic via twist by $\chi_1^{-1}\chi_2$, vanish.) Choose trivializing 1-cochains f_{11} and f_{22}, respectively. That is,

$$c_{12}c_{21} = d_{11}^1 f_{11} \qquad \text{and} \qquad c_{21}c_{12} = d_{22}^1 f_{22}.$$

I claim that the 2-cochain

$$e = f_{11}c_{12} + c_{12}f_{22}$$

is in the kernel of d_{12}^2. To see this, apply Lemma E.1 twice:

$$\begin{aligned} d_{12}(e) = d_{12}(f_{11}c_{12}) + d_{12}(c_{12}f_{22}) &= d_{11}(f_{11})\, c_{12} - f_{11}\, d_{12}(c_{12}) + d_{12}(c_{12})f_{22} - c_{12}\, d_{22}(f_{22}) \\ &= c_{12}c_{21}c_{12} - 0 + 0 - c_{12}c_{21}c_{12} = 0. \end{aligned}$$

Therefore e represents an element of $\mathrm{Ext}^2(\chi_2, \chi_1)$. When we pass to cohomology, both f_{11} and f_{22} are defined up to a linear combination of c_{12} and c_{21} only, so that this element need not be well-defined.[†] But in our application, we will have $\mathrm{Ext}^2_G(\chi_2, \chi_1) = 0$, so this ambiguity doesn't matter.

E.2 Application to a tangent pseudodeformation

As before G is a group, F a field with $\mathrm{char}\, F \neq 2$, and $\chi_1, \chi_2 : G \to F^\times$ two characters. Suppose that $\mathrm{Ext}^1_G(\chi_2, \chi_1) \neq 0$ and $\mathrm{Ext}^1_G(\chi_1, \chi_2) \neq 0$, but $\mathrm{Ext}^2_G(\chi_1, \chi_1) = \mathrm{Ext}^2_G(\chi_2, \chi_1) = 0$.

Proposition E.3. *Under the assumptions above, there exist irreducible representations*

$$\rho : G \to \mathrm{GL}_2(F[\varepsilon])$$

whose trace $\mathrm{tr}\,\rho$ *is a deformation of* $t = \chi_1 + \chi_2$ *to* $F[\varepsilon]$ *as a pseudocharacter, and whose determinant* $\det \rho = \chi_1\chi_2$.

Proof. We use the ideas of [3], though the construction of ρ is completely self-contained based on section E.1 above.

Find 2-cocycles c_{12} and c_{21} representing elements of $\mathrm{Ext}^1_G(\chi_2, \chi_1)$ and $\mathrm{Ext}^1_G(\chi_1, \chi_2)$, respectively. Since we are assuming that $\mathrm{Ext}^2_G(\chi_1, \chi_1) = \mathrm{Ext}^2_G(\chi_2, \chi_2) = 0$, we can find 1-cochains f_{11} and f_{22} with the property that

$$d_{11}(f_{11}) = c_{12}c_{21} \qquad \text{and} \qquad d_{22}(f_{22}) = c_{21}c_{12}.$$

Further, since we assume $\mathrm{Ext}^2_G(\chi_2, \chi_1) = 0$, we can find a 1-cochain Z_{12} with the property that

$$d_{12}(Z_{12}) = f_{11}c_{12} + c_{12}f_{22}.$$

I claim that

$$\rho = \begin{pmatrix} \chi_1 - \varepsilon f_{11} & c_{12} + \varepsilon Z_{12} \\ \varepsilon c_{21} & \chi_2 - \varepsilon f_{22} \end{pmatrix}$$

is a representation of G over $F[\varepsilon]$[‡]. Since the image is in $\mathrm{GL}_2(F[\varepsilon])$, it suffices to check that $\rho(gh) = \rho(g)\rho(h)$. We compute, using the fact that $c_{12} \in \ker d_{12}$,

[†] It is an element of the Massey triple product $\langle c_{12}, c_{21}, c_{12}\rangle$.

[‡] Thanks to Carl Wang Erickson for suggesting the shape of ρ and a conceptual interpretation of Z_{12}.

$$\rho(g)\rho(h) = \begin{pmatrix} \chi_1(gh) & c_{12}(gh) \\ 0 & \chi_2(gh) \end{pmatrix}$$
$$+ \varepsilon \begin{pmatrix} -\chi_1(g)f_{11}(h) - f_{11}(g)\chi_1(h) + c_{12}(g)c_{21}(h) & \chi_1(g)Z_{12}(h) - f_{11}(g)c_{12}(h) - c_{12}(g)f_{22}(h) + Z_{12}(g)\chi_2(h) \\ c_{21}(g)\chi_1(h) + \chi_2(g)c_{21}(h) & c_{21}(g)c_{12}(h) - \chi_2(g)f_{22}(h) - f_{22}(g)\chi_2(h) \end{pmatrix}$$

To prove that $\rho(gh) = \rho(g)\rho(h)$, we verify equality in each coordinate:

$(\begin{smallmatrix}\bullet & \circ \\ \circ & \circ\end{smallmatrix})$ Because $d_{11}f_{11} = c_{12}c_{21}$,

$$-f_{11}(gh) = -\chi_1(g)f_{11}(h) - f_{11}(g)\chi_1(h) + c_{12}(g)c_{21}(h).$$

$(\begin{smallmatrix}\circ & \circ \\ \circ & \bullet\end{smallmatrix})$ Similarly, because $d_{22}f_{22} = c_{21}c_{12}$,

$$-f_{22}(gh) = c_{21}(g)c_{12}(h) - \chi_2(g)f_{22}(h) - f_{22}(g)\chi_2(h).$$

$(\begin{smallmatrix}\circ & \circ \\ \bullet & \circ\end{smallmatrix})$ True because $c_{21} \in \ker d_{21}$.

$(\begin{smallmatrix}\circ & \bullet \\ \circ & \circ\end{smallmatrix})$ Because $d_{12}Z_{12} = f_{11}c_{12} + c_{12}f_{22}$, we have

$$Z_{12}(gh) = \chi_1(g)Z_{12}(h) - f_{11}(g)c_{12}(h) - c_{12}(g)f_{22}(h) + Z_{12}(g)\chi_2(h).$$

Therefore ρ is a representation whose trace visibly deforms $\chi_1 + \chi_2$, as claimed. It remains to see that we can adjust ρ to force the determinant to be $\chi_1\chi_2$. We compute

$$\det \rho = \chi_1\chi_2 - \varepsilon(\chi_1 f_{22} + f_{11}\chi_2 + c_{12}c_{21}).$$

Since ρ is a representation, its determinant is a character of G, which means that its ε-component scaled by $\chi_1^{-1}\chi_2^{-1}$, namely

$$\alpha = f_{22}\chi_2^{-1} + \chi_1^{-1}f_{11} + \chi_1^{-1}c_{12}c_{21}\chi_2^{-1},$$

is an additive character of G. By Lemma E.2 we can replace f_{11} by $f_{11} - \chi_1\alpha = -\chi_1 f_{22}\chi_2^{-1} - c_{12}c_{21}\chi_2^{-1}$ in the construction of ρ above. This adjustment affects only Z_{12}, which does not affect the determinant. It is clear that the adjusted representation by construction has determinant $\chi_1\chi_2$, as desired. □

Of course several such ρ may be possible: most obviously, if $\chi_1 \neq \chi_2$, then we can swap the roles of χ_1 and χ_2 to get a deformation that residually has χ_2 as a subrepresentation instead of χ_1. But as far as the trace, from [3] we know that, if $\chi_1 \neq \chi_2$ and both $\mathrm{Ext}^1_G(\chi_2, \chi_1)$ and $\mathrm{Ext}^1_G(\chi_1, \chi_2)$ are one-dimensional, then the tangent space to the pseudodeformation functor modulo reducible deformations is one-dimensional as well.

E.3 Applications to reducible modular pseudocharacters

We check the cohomological conditions for applying Proposition E.3 in the case that $G = G_{\mathbb{Q},p}$, the field is $F = \mathbb{F}_p$, and all maps are additionally assumed continuous. Recall that ω is the mod-p cyclotomic character.

Proposition E.4. *Assume Vandiver's conjecture for p. If $k = 0$ or k is odd modulo $p - 1$, then*

$$H^2(G_{\mathbb{Q},p}, \omega^k) = 0.$$

Proof. We use Tate's global Euler characteristic formula [22, Theorem 5.1]: if M is a finite $\mathbb{F}_p$-vector space,

then

$$\frac{\#H^0(G_{\mathbb{Q},p},M)\,\#H^2(G_{\mathbb{Q},p},M)}{\#H^1(G_{\mathbb{Q},p},M)} = \frac{\#H^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),M)}{\#M}.$$

In our case with $M = \mathbb{F}_p(\omega^k)$, we have

$$\#H^0(G_{\mathbb{Q},p},\omega^k) = \begin{cases} p & \text{if } k = 0 \\ 1 & \text{otherwise;} \end{cases}$$

$$\#H^1(G_{\mathbb{Q},p},\omega^k) = p \text{ if } k = 0 \text{ or } k \text{ is odd (here assuming Vandiver's conjecture for } k \text{ odd);}$$

$$\#H^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\omega^k) = \begin{cases} p & \text{if } k \text{ is even} \\ 1 & \text{if } k \text{ is odd;} \end{cases}$$

$$\#M = p.$$

Therefore if $k = 0$ or k is odd, $\#H^2(G_{\mathbb{Q},p},\omega^k) = 1$, as claimed. □

Therefore, if $\tau = \omega^b + 1$ is a reducible modular pseudocharacter of $G_{\mathbb{Q},p}$, then b is odd, and we have $\mathrm{Ext}^2_{G_{\mathbb{Q},p}}(\mathbb{F}_p,\mathbb{F}_p) = \mathrm{Ext}^2_{G_{\mathbb{Q},p}}(\mathbb{F}_p,\omega^b) = 0$, and Proposition E.3 applies.

Appendix F

The representation attached to Δ is unobstructed mod 13

We give an argument of Tom Weston showing that for $p = 13$, the residual representation

$$\rho_\Delta : G_{\mathbb{Q},p} \to \mathrm{GL}_2(\mathbb{F}_p)$$

attached to Δ is unobstructed.

The representation $\rho = \rho_\Delta$ is unobstructed if and only if $H^2(G_{\mathbb{Q},p}, \operatorname{ad}\rho)$ vanishes (this is the original defintion of *unobstructed*, which coincides with the one given here in section 2.5 for absolutely irreducible ρ). By Weston [32, Lemma 6] and its Poitou-Tate source [22, Theorem 4.10],

$$\dim H^2(G_{\mathbb{Q},p}, \operatorname{ad}\rho) = \dim_{\mathbb{F}_p} Ш^1(G_{\mathbb{Q},p}, \omega \otimes \operatorname{ad}^0\rho) + H^0(G_p, \omega \otimes \operatorname{ad}\rho) + \hat{H}^0(G_\infty, \omega \otimes \operatorname{ad}\rho).$$

Here ω is the mod-13 cyclotomic character; $G_p \subset G_{\mathbb{Q},p}$ is an image of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q})$ inside $G_{\mathbb{Q},p}$ and G_∞ is an image of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Moreover, $\hat{H}^0(G_\infty, M)$ is reduced H^0 modulo norms, and

$$Ш^1(G_{\mathbb{Q},p}, \omega \otimes \operatorname{ad}^0\rho) = \ker\Big(H^1(G_{\mathbb{Q},p}, \omega \otimes \operatorname{ad}^0\rho) \longrightarrow H^1(G_p, \omega \otimes \operatorname{ad}^0\rho) \oplus H^1(G_\infty, \omega \otimes \operatorname{ad}^0\rho)\Big).$$

The $Ш^1$-term vanishes by the analysis in Weston [32, section 4], which relies on results of Diamond-Flach-Guo [11]. The infinite local $\hat{H}^0$-term also vanishes because $p \neq 2$.

For the remaining G_p-invariants, we use the fact (see, for example, Gross [15, Equation (0.1)]) that

$$\rho|_{G_p} \sim \begin{pmatrix} \omega^{-1}\chi^{-1} & * \\ 0 & \chi \end{pmatrix},$$

where $\chi : G_p \to \mathbb{F}_{13}^\times$ is the unramified character taking Frob_p to $a_{13}(\Delta) = 8$. (In fact, in [15, Theorem 13.10 and chart on p. 513], Gross proves that this extension is nonsplit, but the only thing that actually appears to matter here is that $a_{13} \not\equiv \pm 1 \bmod 13$.)

In general, if the eigenvalues of some representation ρ' are α and β, then the eigenvalues of $\operatorname{ad}\rho'$ are 1, 1, $\alpha\beta^{-1}$, $\alpha^{-1}\beta$. In our case, the eigenvalues of $\operatorname{ad}\rho$ are 1, 1, $\omega\chi^2$ and $\omega^{-1}\chi^{-2}$, so that the eigenvalues of $\omega \otimes \operatorname{ad}\rho$ are

$$\omega,\ \omega,\ \omega^2\chi^2,\ \text{and}\ \chi^{-2}.$$

Since χ is unramified and $\chi^{-2} \neq 1$, there are no G_p-invariants, and this term vanishes as well.

Bibliography

[1] Atiyah, M., and MacDonald, I. G. *Introduction to commutative algebra*. Addison-Wesley, Reading, MA, 1969.

[2] Bellaïche, J. *Eigenvarieties, families of Galois representations, p-adic L-functions*. Unpublished course notes. Available at `http://people.brandeis.edu/~jbellaic/preprint/coursebook.pdf`.

[3] Bellaïche, J. Pseudodeformations. *Mathematische Zeitschrift 270*, 3-4 (2012), 1163–1180.

[4] Bellaïche, J. Une représentation galoisienne universelle attachée aux formes modulaires modulo 2. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[5] Bellaïche, J., and Khare, C. Level 1 Hecke algebras of modular forms modulo p. *Compositio Mathematica 151*, 3 (2015), 397–415. Available at `http://people.brandeis.edu/~jbellaic/preprint/Heckealgebra6.pdf`.

[6] Bröker, R., Lauter, K., and Sutherland, A. Modular polynomials via isogeny volcanoes. *Mathematics of Computation 81* (2010), 1201–1231.

[7] Chenevier, G. The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings. In *Proceedings of the LMS Durham Symposium: Automorphic forms and Galois representations* (2011). Available at `http://gaetan.chenevier.perso.math.cnrs.fr/articles/determinants.pdf`.

[8] Cox, D. A. *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[9] Deo, S. Level N Hecke algebras of modular forms modulo p. In preparation. Available at `http://people.brandeis.edu/~shaunak/LevelNHeckealgebrasv4.pdf`.

[10] Derksen, H. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math. 168*, 1 (2007), 175–224.

[11] Diamond, F., Flach, M., and Guo, L. The Tamagawa number conjecture of adjoint motives of modular forms. *Annales scientifiques de l'Ecole Normale Supérieure 37*, 5 (2004), 663–727.

[12] Diamond, F., and Shurman, J. *A first course in modular forms*, vol. 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[13] Gerbelli-Gauthier, M. Modular forms and Galois representations mod p, and the nilpotent action of Hecke operators mod 2. Undergraduate research project, 2014. Available at `http://www.math.mcgill.ca/darmon/theses/gerbelli-gauthier/mathilde-gg.pdf`.

[14] Gouvêa, F. Q. Deformations of Galois representations. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, vol. 9 of *IAS/Park City Math. Ser.* Amer. Math. Soc., Providence, RI, 2001, pp. 233–406.

[15] Gross, B. H. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. Journal 61*, 2 (1990).

[16] Janson, S. Resultant and discriminant of polynomials. Available at `http://www2.math.uu.se/~svante/papers/sjN5.pdf`.

[17] Jochnowitz, N. Congruences between systems of eigenvalues and implications for the Hecke algebra. Harvard Ph.D. thesis, 1976.

[18] Jochnowitz, N. Congruences between systems of eigenvalues of modular forms. *Transactions of the American Mathematical Society 270*, 1 (1982), 269–285.

[19] Jochnowitz, N. A study of the local components of the Hecke algebra mod l. *Transactions of the American Mathematical Society 270*, 1 (1982), 253–267.

[20] Khare, C. Mod-p modular forms. In *Number theory (Tiruchirapalli, 1996)*, vol. 210 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1998, pp. 135–149.

[21] Mazur, B. Deforming Galois representations. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, vol. 16 of *Math. Sci. Res. Inst. Publ.* Springer, New York, 1989, pp. 385–437.

[22] Milne, J. S. *Arithmetic Duality Theorems*, second ed. BookSurge, LLC, 2006. Available at `http://www.jmilne.org/math/Books/ADTnot.pdf`.

[23] Nicolas, J.-L., and Serre, J.-P. Formes modulaires modulo 2 : l'ordre de nilpotence des opérateurs de Hecke modulo 2. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[24] Nicolas, J.-L., and Serre, J.-P. Formes modulaires modulo 2 : structure de l'algèbre de Hecke. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[25] Rouquier, R. Caractérisation des caractères et pseudo-caractères. *Journal of Algebra 180*, 2 (1996), 571–586.

[26] Serre, J.-P. Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]. In *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*. Springer, Berlin, 1973, pp. 319–338. Lecture Notes in Math., Vol. 317.

[27] Serre, J.-P. Formes modulaires et fonctions zêta p-adiques. 191–268. Lecture Notes in Math., Vol. 350.

[28] Serre, J.-P. *Œuvres. Vol. III.* Springer-Verlag, Berlin, 1986, p. 710. Note 229.2.

[29] Swinnerton-Dyer, H. P. F. On l-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*. Springer, Berlin, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350.

[30] Tate, J. The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2. In *Arithmetic geometry (Tempe, AZ, 1993)*, vol. 174 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1994, pp. 153–156.

[31] Washington, L. C. *Introduction to cyclotomic fields*, second ed., vol. 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1997.

[32] Weston, T. Explicit unobstructed primes for modular deformation problems of squarefree level. *Journal of Number Theory 110*, 199–218. Available at `http://people.math.umass.edu/~weston/papers/eupmdpsl.pdf`.

[33] Weston, T. Unobstructed modular deformation problems. *Amer. J. Math. 126*, 6 (2004), 1237–1252. Available at `http://people.math.umass.edu/~weston/papers/umdp.pdf`.