Explicit non-Gorenstein R=T via rank bounds II: Computation

Catherine M. Hsu

Swarthmore College

Fifteenth Algorithmic Number Theory Symposium
University of Bristol
August 2022

Joint with Preston Wake and Carl Wang-Erickson

Review of prime level

Let $p \geq 5$, N be primes. We consider weight 2 modular forms of level $\Gamma_0(N)$:

- ◇ $E_{2,N} = E_2(z) - E_2(Nz)$, weight 2 Eisenstein series of level $\Gamma_0(N)$
- ◇ $\mathcal{I} = \mathrm{Ann}(E_{2,N}) = \langle T_\ell - \ell - 1 : \ell \text{ prime}, \ell \neq N \rangle$
- ◇ $\mathbb{T}$ = the completion of the Hecke algebra at $(\mathcal{I}, p)$
- ◇ $\mathbb{T}^0$ = the cuspidal quotient of $\mathbb{T}$
- ◇ $\mathcal{I}^0$ = the image of $\mathcal{I}$ in $\mathbb{T}^0$

Theorem (Mazur, '77). Assume that $p \neq N$. Then,

1. $\mathbb{T}^0 \neq 0 \iff p$ divides the numerator of $\frac{N-1}{12}$
2. $\mathbb{T}^0$ is Gorenstein
3. $\mathcal{I}^0$ is a principal ideal, and $T_\ell - \ell - 1$ generates $\mathcal{I}^0$ if and only if $\ell \not\equiv 1 \pmod{p}$ and ℓ is not a pth power mod N

Review of prime level (cont.)

Question (Mazur): What is the rank of $\mathbb{T}^0$ as a $\mathbb{Z}_p$-module? What is the arithmetic significance of rank 1 vs. rank > 1?

Some results:

(i) Merel, ∼'96:

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{T}^0) > 1 \iff \prod_{i=1}^{\frac{N-1}{2}} i^i \text{ is a } p\text{th power mod } N$$

(ii) Calegari-Emerton, ∼'05:

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{T}^0) > 1 \implies \dim_{\mathbb{F}_p}\Big((Cl(\mathbb{Q}(\sqrt[p]{N}))[p]\Big) > 1$$

(iii) Wake–Wang-Erickson, ∼'20:

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{T}^0) > 1 \iff \text{some cup product in Galois cohomology vanishes}$$

$R = \mathbb{T}$ via Wiles' numerical criterion

An "$R = \mathbb{T}$ Theorem" relates the arithmetic data of the following objects:

R : a universal Galois deformation ring ⇠ ⇢ $\mathbb{T}$: a Hecke algebra acting on modular forms

In particular, there is a standard argument to construct a surjection

$$R \twoheadrightarrow \mathbb{T}.$$

To conclude $R = \mathbb{T}$, Calegari–Emerton and Wake–Wake-Erickson apply Wiles' numerical criterion, which requires $\mathbb{T}$ to be a local complete intersection (LCI) ring.

Today's Goal: Outline a computational approach for counting rank of R directly in order to establish $R = \mathbb{T}$ when $\mathbb{T}$ is **not** LCI

Our setup: Ribet's newform setting (RNS)

With $p \geq 5$ prime, we consider the following setting:

- $N = \ell_0 \ell_1$, with ℓ_i primes satisfying
  - $\ell_0 \equiv 1 \pmod p$ and $\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{T}^0_{\ell_0}) = 1$
  - $\ell_1 \not\equiv \pm 1 \pmod p$ but ℓ_1 is a pth power modulo ℓ_0
- $E^{\varepsilon}_{2,N}$ = the weight 2 Eisenstein series of level $\Gamma_0(N)$ with Atkin-Lehner signature $(-1, -1)$.

Theorem (Ribet): There is a newform $f \in S_2(\Gamma_0(N))$ such that

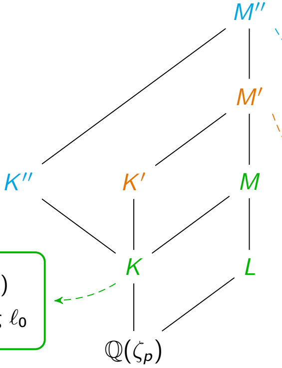
$$f \equiv E^{\varepsilon}_{2,N} \pmod p.$$

This means that $\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{T}) \geq 3$ since we have:

- the Eisenstein series $E^{\varepsilon}_{2,N}$
- the cusp form of level ℓ_0
- the newform f of level N

We can check computationally that $\mathbb{T}$ is **not** LCI.

Main result



- $\diamond$ $M''/\mathbb{Q}$ is Galois
- $\diamond$ M''/M' is ω-isotypic, conductor*
- $\diamond$ primes over ℓ_0 split in M''/M'

- $\diamond$ $M'/\mathbb{Q}$ is Galois
- $\diamond$ M'/M is ω^0-isotypic, unramified
- $\diamond$ primes over ℓ_0 split in M'/M

- $\diamond$ $K = \mathbb{Q}(\zeta_p, \ell_1^{1/p})$
- $\diamond$ L defined using ℓ_0

Theorem (H-W-WE): For (p, ℓ_0, ℓ_1) satisfying the RNS assumptions,

$\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{T}) > 3 \implies$

(i) all primes of K over ℓ_1 split in K'/K,

(ii) there exists some prime of K over ℓ_0 that splits in both K'/K and K''/K.

If either condition fails, the surjection $R \twoheadrightarrow \mathbb{T}$ is an isomorphism.

$R = \mathbb{T}$ via rank bounds

Following work of Wake–Wang-Erickson, we study a deformation ring R of Galois pseudorep'ns of $\overline{\rho} = \omega \oplus 1$. The input for this machinery is:

1. For (p, ℓ_0, ℓ_1) satisfying our RNS assumptions, we fix two cocycles:
   - ◇ $b^{(1)}$ represents the Kummer class of ℓ_1 in $H^1(G_{\mathbb{Q}}, \mathbb{F}_p(1))$
   - ◇ $c^{(1)}$ represents a class in $H^1(G_{\mathbb{Q}}, \mathbb{F}_p(-1))$ ramified only at ℓ_0
2. Since $b^{(1)} \cup c^{(1)} = 0$, there exists a cochain $a^{(1)}$ satisfying
$$-\delta a^{(1)} = b^{(1)} \smile c^{(1)}.$$
3. With $d^{(1)} = b^{(1)} c^{(1)} - a^{(1)}$, we check for a cochain $b^{(2)}$ satisfying
$$-\delta b^{(2)} = a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)}.$$

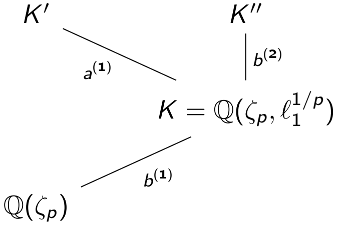
Main Theoretical Output from HWWE Part I: For (p, ℓ_0, ℓ_1) as above,

$\dim_{\mathbb{F}_p}(R/pR) > 3 \iff$ (i) $a^{(1)}(\mathrm{Fr}_{\ell_1}) \in \mathbb{F}_p$ vanishes
(ii) a special invariant $\alpha^2 + \beta \in \mathbb{F}_p(2)$ vanishes

Going from theory to computation

The key idea is to compute S-units that correspond to $a^{(1)}|_{G_K}$ and $b^{(2)}|_{G_K}$ via Kummer theory. We take a two-step approach to this computation:

1. Find candidate cochains that solve differential equations for $a^{(1)}$ and $b^{(2)}$
2. Make local adjustments so candidate solutions satisfy local conditions



Using this construction, we prove

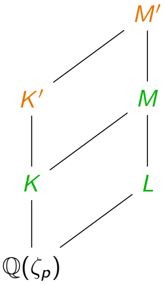
(i) $a^{(1)}(\mathrm{Fr}_{\ell_1}) = 0 \iff$ all primes of K over ℓ_1 split in K'/K

(ii) $\alpha^2 + \beta = 0 \iff$ there exists some prime of K over ℓ_0 that splits in both K'/K and K''/K

Computing an S-unit in $K^\times$ for $a^{(1)}|_{G_K}$

Any cochain $a^{(1)}$ satisfying $-\delta a^{(1)} = b^{(1)} \smile c^{(1)}$ gives a degree $p^3(p-1)$ twisted-Heisenberg extension of $\mathbb{Q}$, cut out by

$$\begin{pmatrix} \omega & b^{(1)} & \omega a^{(1)} \\ 0 & 1 & \omega c^{(1)} \\ 0 & 0 & \omega \end{pmatrix} : G_{\mathbb{Q}} \to GL_3(\mathbb{F}_p).$$



Sharifi's theory gives the explicit formula

$$a^{(1)}_{\mathrm{cand}}|_{G_K} = D^1_\sigma(\gamma) \in K^\times,$$

where

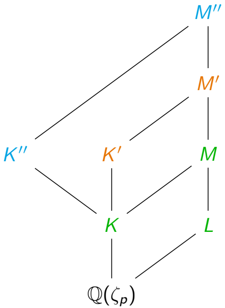
- $\gamma \in K^\times$ satisfies $\mathrm{Nm}_{K/\mathbb{Q}(\zeta_p)}(\gamma) = c^{(1)}$, and
- $D^1_\sigma = \sum_{i=0}^{p-1} i\sigma^i$ denotes a first-order Kolyvagin derivative operator.

The local adjustment can be written $a^{(1)}_{\mathrm{adj}} = \zeta_p^j a_0^k$.

Computing an S-unit in $K^\times$ for $b^{(2)}|_{G_K}$

Similarly, a cochain $b^{(2)}$ satisfying $-\delta b^{(2)} = a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)}$ gives a degree $p^4(p-1)$ twisted-Heisenberg extension of $\mathbb{Q}$, cut out by

$$\begin{pmatrix} \omega & b^{(1)} & \omega a^{(1)} & b^{(2)} \\ 0 & 1 & \omega c^{(1)} & d^{(1)} \\ 0 & 0 & \omega & b^{(1)} \\ 0 & 0 & 0 & 1 \end{pmatrix} : G_{\mathbb{Q}} \to GL_4(\mathbb{F}_p).$$



Expressing the differential equation for $b^{(2)}$ in terms of the triple Massey product $(b^{(1)}, c^{(1)}, b^{(1)})$ gives

$$b^{(2)}_{\mathrm{cand}}|_{G_K} = (D^2_\sigma(\gamma) D^1_\sigma(\xi))^{-2} a^{(1)}|^{-1}_{G_K} \in K^\times,$$

where

- $\xi \in K^\times$ satisfies $\mathrm{Nm}_{K/\mathbb{Q}(\zeta_p)}(\xi) = a^{(1)}_{\mathrm{adj}}$, and
- $D^2_\sigma = \sum_{i=0}^{p-1} \binom{i}{2} \sigma^i$.

The local adjustment can be written $b^{(2)}_{\mathrm{adj}} = p^m \ell_0^n$.

Computational evidence for $R = \mathbb{T}$

We have attempted to verify whether the conditions in our main result hold for the triples (p, ℓ_0, ℓ_1) in the following ranges:

- $(5, \ell_0, \ell_1)$ with $\ell_0 \leq 100$ and $\ell_1 \leq 1000$,
- $(7, \ell_0, \ell_1)$ with $\ell_0 \leq 50$ and $\ell_1 \leq 500$.

To summarize, every example for which our algorithm completed is consistent with our conjecture that $R = \mathbb{T}$. Specifically, we either:

- compute that (i) and (ii) of our main result are satisfied, and hence

$$\dim_{\mathbb{F}_p}(R/pR) > 3,$$

  and independently compute that $\mathrm{rk}_{\mathbb{Z}_p}(\mathbb{T}) > 3$, or
- compute that (ii) is not satisfied, and hence $R = \mathbb{T}$.

Overview of implementation in Sage

- Our program for checking the conditions in our main result, available online at `https://github.com/cmhsu2012/RR3`, is written for Sage Version 9.2 and uses the unit/S-unit interface, written by John Cremona, to the unit/S-unit groups computed in PARI/GP.

- All computations were carried out on the Strelka Computer Cluster or the SMP Cluster with an allotted computing time of 3 days per example.

- A particularly interesting computational observation is that condition (i) in our main result, i.e., $a^{(1)}(\mathrm{Fr}_{\ell_1}) = 0$, has been satisfied in every example computed to date.

- When translating the abstract conditions on Galois cochains into implementable computations in number fields, a particularly challenging aspect was determining which Kummer extension of $\mathbb{Q}(\zeta_p)$ to use.

Example: $p = 5, \ell_0 = 11, \ell_1 = 23$

$c = (3, 4, 4, 4, 1, 1)$
$\gamma = (2, 0, 1, 4, 0, 4, \ldots, 0)$

$a^{(1)}_{\mathrm{cand}} = (4, 1, 2, 1, 3, 0, \ldots, 1)$
$b^{(2)}_{\mathrm{cand}} = (2, 3, 2, 0, 2, 3, \ldots, 0)$

$a^{(1)}_{\mathrm{adj}} = \zeta_p^0 a_0^1$
$= (2, 2, 0, 2, 1, 3, \ldots, 4)$

$a^{(1)} = a^{(1)}_{\mathrm{cand}} + a^{(1)}_{\mathrm{adj}}$
$= (1, 3, 2, 3, 4, 3, \ldots, 0)$

$a^{(1)}|_{\ell_1} = 0$,
Condition (*i*) holds

$\xi = (2, 0, 2, 1, 0, 0, \ldots, 0)$
with $\mathrm{Nm}(\xi) = a^{(1)}_{\mathrm{adj}}$

$\tilde{b}^{(2)}_{\mathrm{cand}} = (1, 1, 2, 2, 2, 3, \ldots, 2)$

$b^{(1)}_{\mathrm{adj}} = p^3 \ell_0^4$
$= (0, 1, 2, 0, 3, 3, \ldots, 4)$

$b^{(2)} = \tilde{b}^{(2)}_{\mathrm{cand}} + b^{(2)}_{\mathrm{adj}}$
$= (1, 2, 4, 2, 0, 1, \ldots, 1)$

$\alpha^2 + \beta \neq 0$,
Condition (*ii*) does not hold

Examples: $p = 5, \ell_0 = 11$

primes			β difficulty factors		adjustments to $a^{(1)} \rightsquigarrow \alpha$		adjustments to $b^{(2)} \rightsquigarrow \beta$		conclusion	Hecke rank
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\|_p$	ζ_p^i	a_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?	$\mathrm{rk}(\mathbb{T})$
5	11	23	wild	$\neq 0$	0	1	3	4	no	3
5	11	43	tame	$\neq 0$	3	2	0	4	yes	≥ 4
5	11	67	wild	$\neq 0$	0	0	1	3	no	3
5	11	197	wild	$\neq 0$	0	2	1	4	yes	≥ 4
5	11	263	wild	$= 0$	0	2	4	3	no	3
5	11	307	tame	$= 0$	1	3	0	0	no	3
5	11	373	wild	$\neq 0$	0	4	0	3	no	3
5	11	397	wild	$\neq 0$	0	4	2	3	no	3
5	11	593	tame	$= 0$	0	3	0	2	no	3
5	11	683	wild	$= 0$	0	4	3	0	yes	≥ 4
5	11	727	wild	$\neq 0$	0	1	1	3	yes	≥ 4
5	11	857	tame	$\neq 0$	2	0	0	4	no	3
5	11	967	wild	$\neq 0$	0	0	2	2	no	3
5	11	1013	wild	$\neq 0$	0	3	3	1	no	3

Thanks for listening!