The generalized Riemann hypothesis for Dirichlet L-functions

27 November 2026 · Edition 930

Volume II

Strict local conditions and Selmer groups of twists

Abstract

We impose the strict local conditions on both conjugation eigenspaces. Tame inertia and auxiliary twists give tests for the Selmer groups, whose lengths are compared with critical values over a common interval.

The guide in Volume I lists all twenty-seven volumes.

Contents

II Strict local conditions and Selmer groups of twists 1
11 Strict local conditions and conjugation . . . 3
11.1 A uniform bound for one conjugation eigenspace . . . 3
11.1.1 From strict classes to special values . . . 3
11.1.2 One integral determinant for all odd primes . . . 4
11.1.3 The integral group ring at primes dividing the degree . . . 4
11.2 Both signs at finite level and the exceptional twists at two . . . 6
11.2.1 One dyadic module for the whole interval . . . 7
11.3 The remaining twists on a common power interval . . . 9
11.3.1 The implication still needed for Dirichlet GRH . . . 11
11.4 The full local-length bound at the prime two . . . 11
11.5 Local cohomology at the primes of the theta tests . . . 14
11.6 The remaining local estimate in terms of finite group orders . . . 16
11.7 The strict local condition at every coefficient level . . . 19
11.8 Finite odd cocycles and the strict local condition . . . 22
11.9 A cyclotomic annihilator at all coefficient primes . . . 24
11.10 One integer for the full length of the odd cocycle module . . . 26
12 Selmer groups and marked local conditions . . . 29
12.1 Dual Selmer classes and relations on tame inertia . . . 29
12.2 Auxiliary primes for the tame values of even cocycles . . . 33
12.3 The cost of the auxiliary primes on a period interval . . . 36
12.4 Scalar cocycles after the paired inertia and Frobenius tests . . . 39
12.5 Crystalline cocycles at the spherical coefficient primes . . . 41
12.6 One anticyclotomic twist for simultaneous integral tests . . . 44
12.7 Integral minors for the Selmer groups of the twists . . . 47
12.8 The primary and dual terms for a polarized marked summand . . . 50
12.9 Reducing the Selmer groups by local conditions at split pairs . . . 53
12.10 Short Selmer groups for genuine twists of the main summands . . . 57
13 Critical values and Selmer lengths on a common interval . . . 60
13.1 Critical Hecke values at the twists used for Selmer groups . . . 60
13.2 The local cohomology loss on a fixed interval of weights . . . 64
13.3 The critical-value comparison at primes dividing the discriminant or old conductor . . . 68

13.4 Heights of the critical factors in the chain of lifts 72
13.5 Local lifting with a separate weight interval at each embedding 74
13.6 The sum of the marked Selmer lengths on a common interval 77
14 References 80

11 Strict local conditions and conjugation

11.1 A uniform bound for one conjugation eigenspace

Fix the primitive character ψ of conductor F. For this section use the primes, fields and interval of Proposition 6.4. At a given x, write $g = [E : \mathbb{Q}]$, $G = \mathrm{Gal}(E/\mathbb{Q})$, $c \in G$ for complex conjugation, and $t = \lfloor x^{401} \rfloor$. The integer

$$N = 2^{l+2} F q d$$

is a cyclotomic modulus for E. The letter d here denotes the second auxiliary prime. The field E is CM, since it is abelian and contains the imaginary quadratic field $\mathbb{Q}(\sqrt{-q})$. For an odd prime ℓ and $n = r + 1 \geq 2$, put $e_n = (1 + (-1)^n c)/2 \in \mathbb{Z}_\ell[G]$. We shall bound $e_n \mathcal{S}_{\ell,r}(E)$ for all odd primes at once. The sign depends on the twist.

Theorem 11.1 (The contribution with sign $(-1)^{r+1}$)**.** *Fix $0 < \varepsilon < 1/52$. For all sufficiently large Y, take the single pair q, d of Proposition 6.4. At every $2Y \leq x \leq (2Y)^{3/2}$ its fields satisfy*

$$\sum_{\ell > 2 \text{ prime}} (\log \ell) \sum_{1 \leq r < t} \mathrm{length}_{\mathbb{Z}_\ell} \left(e_{r+1} \mathcal{S}_{\ell,r}(E) \right) \leq C_{F,\varepsilon} x^{812} \leq \tfrac{1}{4} \exp(x^\varepsilon / 2). \tag{11.1}$$

Every group in the sum is finite, and for fixed x only finitely many terms are nonzero.

11.1.1 From strict classes to special values

Put $S_0 = \{\infty\} \cup \{p : p \mid N\}$, $U_\ell = \mathrm{Spec}\, \mathcal{O}_E[1/(N\ell)]$, and $C_\ell = H^2_{\mathrm{et}}(U_\ell, \mathbb{Z}_\ell(n))$. Let $\Theta_n \in \mathbb{Q}[G]$ be the equivariant special value characterized by

$$\chi(\Theta_n) = L_{S_0}(1 - n, \chi^{-1}) \qquad (\chi \in \widehat{G}).$$

On the right the Euler factors at $p \mid N$ are removed. This is the value of the Dirichlet function of the character induced to modulus N. The Bernoulli formula below also constructs Θ_n over $\mathbb{Q}$. Complex conjugation acts on all cohomology groups through the natural action of the field automorphism.

Lemma 11.2 (The relevant Fitting ideal)**.** *There is a G-equivariant injection $\mathcal{S}_{\ell,r}(E)^\vee \hookrightarrow C_\ell$, where the dual has the contragredient action. If a positive integer W kills $H^0(E, \mathbb{Q}_\ell/\mathbb{Z}_\ell(n))$, then $e_n W \Theta_n$ belongs to the zeroth Fitting ideal of $e_n C_\ell$ over $R_\ell = e_n \mathbb{Z}_\ell[G]$.*

Proof. Poitou–Tate duality pairs the strict kernel in degree one for $\mathbb{Q}_\ell/\mathbb{Z}_\ell(1-n)$ with the strict kernel in degree two for its Tate dual $\mathbb{Z}_\ell(n)$ on $\mathrm{Spec}\, \mathcal{O}_E[1/\ell]$. One obtains this form of duality by taking direct and inverse limits of the finite-coefficient duality sequence. The finite-level groups are finite, so the inverse systems satisfy the Mittag–Leffler condition. On the discrete side vanishing at the finitely many local places can be tested in the direct limit. The pairing is preserved by field automorphisms, and the archimedean degree-one local terms vanish for these odd primes. Thus the dual embeds into global degree two. Inverting the extra primes above N gives an injection in degree two by the localization sequence, since the preceding terms at $w \nmid \ell$ are $H^0(\kappa_w, \mathbb{Z}_\ell(n-1)) = 0$. Indeed multiplication by $(Nw)^{n-1} - 1$ has zero kernel in $\mathbb{Z}_\ell$. This proves the injection. We use continuous étale cohomology and the usual identification with Galois cohomology on rings of S-integers where ℓ is invertible. [1, 2]

We use the refined Coates–Sinnott theorem of Greither and Popescu. For an abelian extension of the totally real base $\mathbb{Q}$, a set S_0 containing the infinite and ramified primes, $n \geq 2$, and $\ell > 2$, it identifies

$$\mathrm{Ann}_{\mathbb{Z}_\ell[G]} \left(H^1_{\mathrm{et}}(U_\ell, \mathbb{Z}_\ell(n))_{\mathrm{tors}} \right) \Theta_n = e_n \, \mathrm{Fitt}_{\mathbb{Z}_\ell[G]}(C_\ell).$$

The hypothesis on the cyclotomic μ-invariant holds by the Ferrero–Washington theorem, because the maximal CM subfield of $E(\mu_\ell)$ is abelian over $\mathbb{Q}$. The torsion group in the formula is $H^0(E, \mathbb{Q}_\ell/\mathbb{Z}_\ell(n))$. This follows from the coefficient sequence for $\mathbb{Z}_\ell(n) \subset \mathbb{Q}_\ell(n)$, since $H^0(E, \mathbb{Q}_\ell(n)) = 0$. Projecting the equality to the direct factor R_ℓ and using base change for Fitting ideals proves the assertion. [2, Thm. 6.11 and Lem. 6.9][3] □

11.1.2 One integral determinant for all odd primes

Choose two distinct fixed rational primes $P_1, P_2 \nmid 2F$. For large Y these differ from q, d, so E is unramified at both. Put

$$W = (P_1^{gn} - 1)(P_2^{gn} - 1), \qquad A = W\, nN(n+1)!.$$

For each ℓ choose $P_i \neq \ell$. At a place of E over P_i, the cyclotomic character takes arithmetic Frobenius to P_i^f, where the residue degree f divides g. Consequently $P_i^{gn} - 1$ kills $H^0(E, \mathbb{Q}_\ell/\mathbb{Z}_\ell(n))$. This proves the required annihilation by a single W independent of ℓ.

Lemma 11.3 (Integrality, nonvanishing and size)**.** *The element $A\Theta_n$ lies in $\mathbb{Z}[G]$. The integer*

$$D_n = \prod_{\substack{\chi \in \widehat{G} \\ \chi(c) = (-1)^n}} A\, L_{S_0}(1-n, \chi^{-1})$$

is nonzero and satisfies $\log |D_n| \ll_F gn\{g + \log(2Nn)\}$.

Proof. The standard special-value formula for residue classes, obtained from the Hurwitz zeta function at $1-n$, is

$$L_{S_0}(1-n, \chi^{-1}) = -\frac{N^{n-1}}{n} \sum_{\substack{1 \le a \le N \\ (a,N)=1}} \chi^{-1}(a) B_n(a/N).$$

Here $B_n(z) = \sum_{j=0}^{n} \binom{n}{j} B_j z^{n-j}$. The recurrence $\sum_{j=0}^{m} \binom{m+1}{j} B_j = 0$ for $m \ge 1$, with $B_0 = 1$, gives $(m+1)!B_m \in \mathbb{Z}$ by induction. Hence $nN(n+1)!$ clears every rational coefficient in the last display. Replacing each $\chi^{-1}(a)$ with the inverse of the cyclotomic Artin symbol of a in G, constructs the asserted integral group-ring element. [4]

For the indicated parity, $1-n$ is not a trivial zero. Writing $\chi(-1) = (-1)^a$ with $a \in \{0, 1\}$, the gamma argument $(1 - n + a)/2$ is a half-integer for this parity. The completed functional equation relates the value to that of the conjugate character at $n > 1$, where the Euler product is nonzero. For the trivial character the same conclusion follows from the zeta functional equation. Every removed factor of a primitive unramified character has the form $1 - \chi^{-1}(p)p^{n-1}$, which is nonzero. The displayed product is Galois-invariant because conjugation permutes its characters. Each factor is an algebraic integer by the first assertion, proving that D_n is a nonzero rational integer.

On the circle $|z| = 1$, the generating function $ze^{vz}/(e^z - 1)$ is bounded uniformly for $0 \le v \le 1$. Cauchy's estimate gives $|B_n(v)| \ll n!$. The special-value formula therefore bounds each absolute value by $O(N^n n!)$ before multiplication by A. Since $\log W \ll_F gn$, $\log((n+1)!) \ll n \log(2n)$, and the number of factors is at most g, the stated logarithmic estimate follows. □

11.1.3 The integral group ring at primes dividing the degree

Write $M_\ell = e_n C_\ell$ and $b_\ell = e_n A\Theta_n$. The finitely generated $\mathbb{Z}_\ell$-module R_ℓ is free. On $R_\ell \otimes \overline{\mathbb{Q}}_\ell$, multiplication by b_ℓ is diagonal with eigenvalues indexed by the characters of the indicated

parity. Its determinant is D_n. Thus $R_\ell/b_\ell R_\ell$ has $\mathbb{Z}_\ell$-length $v_\ell(D_n)$ by the elementary divisor theorem. Lemma 11.2 puts b_ℓ in the zeroth Fitting ideal of M_ℓ, which annihilates M_ℓ.

If $\ell \nmid g$, R_ℓ is a product of rings of integers of unramified extensions of $\mathbb{Q}_\ell$. Indeed the cyclic group-ring factors are defined by $X^m - 1$ with m prime to ℓ, whose reduction has distinct roots. The abelian group ring and its direct factors are therefore finite étale over $\mathbb{Z}_\ell$. In each discrete valuation ring the valuation of the zeroth Fitting ideal equals the length of the module. Membership of b_ℓ bounds that length by the valuation of the corresponding component of b_ℓ. Weighting by the residue degrees and summing gives

$$\operatorname{length}_{\mathbb{Z}_\ell} M_\ell \le v_\ell(D_n).$$

For the other odd primes, $\ell \mid g$ implies $\ell \mid o$, where o is the fixed order of ψ. To see this, $[K_\psi C_l : \mathbb{Q}] = o\,2^l/[K_\psi \cap C_l : \mathbb{Q}]$, and adjoining the two quadratic fields multiplies this by four. We bound the number of $\mathbb{Z}_\ell$-generators of C_ℓ. Its reduction modulo ℓ injects into $H^2_{\text{et}}(U_\ell, \mathbf{F}_\ell(n))$ by the coefficient sequence. Put $K = E(\mu_\ell)$ and pass to $\operatorname{Spec} \mathcal{O}_K[1/(N\ell)]$. Restriction is injective on the latter cohomology by trace, since the finite étale cover has degree dividing $\ell - 1$. Over K choose an isomorphism of $\mathbf{F}_\ell(n)$ with μ_ℓ. Kummer theory bounds this degree-two dimension by the sum of the dimensions of the class group modulo ℓ and the ℓ-torsion in the Brauer group of the open ring. Its class group is a quotient of $\mathrm{Cl}(K)$. By the global invariant sequence for the Brauer group, its ℓ-torsion injects into the local ℓ-torsion at the missing finite places. Each such place contributes dimension at most one, and there are at most $[K : \mathbb{Q}](1 + \log_2 N)$ of them. [1, 5]

Writing $a = [K : \mathbb{Q}]$, we have $a \le (\ell - 1)g$ and $|\operatorname{disc} K| \le (N\ell)^a$ by the abelian conductor–discriminant formula. Minkowski’s bound represents each ideal class by an integral ideal of norm at most $B = 2^a |\operatorname{disc} K|^{1/2}$. The number of such ideals is at most $B^2 \zeta_K(2) \le B^2 \zeta(2)^a$, the last inequality following from the Euler factors. Thus $\log |\mathrm{Cl}(K)| \ll_F g \log(2N)$. Nakayama’s lemma now bounds the number of $\mathbb{Z}_\ell$-generators of C_ℓ, hence of its summand M_ℓ, by $C_F g \log(2N)$. Finite generation here is the standard finiteness theorem for continuous étale cohomology of an open ring of integers. [2]

These generators also generate over R_ℓ. As $b_\ell M_\ell = 0$, a direct sum of that many copies of $R_\ell/b_\ell R_\ell$ surjects onto M_ℓ. Its length is therefore at most $C_F g \log(2N) v_\ell(D_n)$. This argument includes the primes at which the group ring has nonsemisimple reduction.

Proof of Theorem 11.1. The injection of Lemma 11.2 preserves the sign on complex conjugation, since $c^{-1} = c$ on the dual. Every term in the sum of lengths for fixed r is now finite. Combining the two cases above and summing $v_\ell(D_n) \log \ell$ gives

$$\sum_{\ell > 2} (\log \ell) \operatorname{length}_{\mathbb{Z}_\ell}(e_n \mathcal{S}_{\ell,r}(E)) \ll_F (1 + g \log(2N))\, gn\{g + \log(2Nn)\}.$$

The sum of valuations over all primes is $\log |D_n|$, so the estimate also gives finite support. On the stated family $g \ll_F x^3$ and $\log(2Nt) \ll_{F,\varepsilon} x$, uniformly, by the bounds on $q, d, 2^l$ and $Y \le x$. When $n \le t$ the right side is $O_{F,\varepsilon}(x^{10} n)$. Finally $\sum_{2 \le n \le t} n \le t^2 \le x^{802}$. This even gives $O_{F,\varepsilon}(x^{812})$, and any fixed power of x is $o(\exp(x^\varepsilon/2))$. □

The complementary eigenspace has $\chi(c) = (-1)^{n-1}$. Its primitive L-function has a trivial zero at $1 - n$, as follows from the pole of the gamma factor there and the functional equation. The determinant in Lemma 11.3 would vanish on this component. Controlling its local lengths requires a different arithmetic estimate.

11.2 Both signs at finite level and the exceptional twists at two

Continue with the same $\psi, \varepsilon, Y, q, d$, and with the fields of Proposition 6.4. Write $t(x) = \lfloor x^{401} \rfloor$ and $I_Y = [2Y, (2Y)^{3/2}]$. We first establish finiteness of the full sum in (L) at each x. We then give uniform estimates which also see the complementary sign.

Proposition 11.4 (Finiteness of the full sum)**.** *For every $x \in I_Y$ and $r \geq 1$ one has*

$$\sum_{\ell} (\log \ell) \operatorname{length}_{\mathbb{Z}_\ell} \mathcal{S}_{\ell,r}(E) \leq \log |K_{2r}(\mathcal{O}_E)| < \infty.$$

Here K_i denotes Quillen's algebraic K-group. In particular the supremum in (L) *is a finite sum at each x.*

Proof. The Poitou–Tate argument of Lemma 11.2, before the extra primes are inverted, embeds the dual of the strict group into $H^2_{\mathrm{et}}(\mathcal{O}_E[1/\ell], \mathbb{Z}_\ell(r+1))$. It applies at two as well because E contains an imaginary quadratic field and has no real places. In the duality sequence the modified local groups at complex places are zero. [1]

Use the number-field Quillen–Lichtenbaum comparison in even degree. For a ring of S-integers with all primes over ℓ inverted it identifies the ℓ-adic completion of K_{2r} with $H^2_{\mathrm{et}}(-, \mathbb{Z}_\ell(r+1))$, for $r \geq 1$ and odd ℓ, and also for $\ell = 2$ in the totally imaginary case. In the descent spectral sequence the only other possible term in this degree is $H^0(-, \mathbb{Z}_\ell(r))$, which vanishes because the cyclotomic image over a number field is open and $r > 0$. The cohomological dimension is at most two under these hypotheses. [6, Ch. VI, Sec. 8][7, Thm. 1]

In Quillen's localization sequence for $\mathcal{O}_E \subseteq \mathcal{O}_E[1/\ell]$ the groups surrounding the map in degree $2r$ are the sums, over $v \mid \ell$, of $K_{2r}(\kappa_v) = 0$ and $K_{2r-1}(\kappa_v)$, respectively. The latter are cyclic of order $|\kappa_v|^r - 1$, prime to ℓ. Thus the map is an isomorphism after tensoring with $\mathbb{Z}_\ell$. The group $K_{2r}(\mathcal{O}_E)$ is finite by Quillen's finite generation theorem and Borel's rank theorem in positive even degree. Its ℓ-part therefore bounds the order of the strict group. Taking logarithms and summing proves the claim. There are finitely many indices $r < t(x)$ at a fixed x. [6] □

Theorem 11.5 (A uniform range for both signs)**.** *Let $P = \exp(x^{\varepsilon}/12)$ and $b_0 = \lfloor \exp(x^{\varepsilon}/8) \rfloor$. For every sufficiently large Y and every $x \in I_Y$,*

$$\sum_{\ell \leq P} (\log \ell) \sum_{1 \leq r < t(x)} \operatorname{length}_{\mathbb{Z}_\ell} \Big(\mathcal{S}_{\ell,r}(E)[\ell^{b_0}] \Big) \leq \exp(x^{\varepsilon}/3).$$

The sum is over rational primes, including two. The bracket denotes the subgroup killed by the indicated power.

Proof. Write $g = [E : \mathbb{Q}]$ and $N = 2^{l+2} F q d$ as before. Let $d_{\ell,r}$ be the dimension of $\mathcal{S}_{\ell,r}(E)[\ell]$ over $\mathbf{F}_\ell$. The multiplication-by-ℓ sequence on $\mathbb{Q}_\ell/\mathbb{Z}_\ell(-r)$ maps $H^1(G_{E,S_\ell}, \mathbf{F}_\ell(-r))$ onto the ℓ-torsion of the ambient degree-one group. Therefore $d_{\ell,r}$ is at most the dimension of this finite-coefficient cohomology.

Put $K = E(\mu_\ell)$, $a = [K : \mathbb{Q}] \leq g\ell$. Restriction to K is injective on the finite-coefficient group by corestriction, since $[K : E]$ divides $\ell - 1$ and the extension is unramified outside ℓ. The module becomes isomorphic to μ_ℓ. Let S_K be the primes over ℓ and $R_K = \mathcal{O}_K[1/\ell]$. The Kummer sequence gives

$$0 \longrightarrow R_K^\times / (R_K^\times)^\ell \longrightarrow H^1(G_{K,S_K}, \mu_\ell) \longrightarrow \mathrm{Cl}(R_K)[\ell] \longrightarrow 0.$$

Dirichlet's S-unit theorem bounds the first dimension by $a + |S_K| \leq 2a$, including roots of unity. The last dimension is at most $\log |\mathrm{Cl}(K)| / \log \ell$. The conductor of K divides $N\ell$. The

same Minkowski and ideal-count argument as in Section 11.1 gives $\log|\mathrm{Cl}(K)| \ll a\log(2N\ell)$ with an absolute constant. We obtain $d_{\ell,r}\log\ell \ll g\ell\log(2N\ell)$ for every twist.

In a finite abelian ℓ-group with $d_{\ell,r}$ cyclic summands, the subgroup killed by ℓ^{b_0} has length at most $b_0 d_{\ell,r}$. Sum over $r < t(x)$ and use $\sum_{\ell\le P}\ell \le P(P+1)$. The result is $O(t(x)b_0 gP^2\log(2NP))$. The factors $t(x), g, \log(2NP)$ are bounded by fixed powers of x on this family. Since $1/8 + 2/12 = 7/24 < 1/3$, the claimed bound follows throughout I_Y. □

11.2.1 One dyadic module for the whole interval

Put $k_\infty = K_\psi(\mu_{2^\infty})$, $B = K_\psi(\sqrt{-q}, \sqrt{-d})$, and $L_\infty = B(\mu_{2^\infty})$. For every $x \in I_Y$ one has $E_x = BC_l$ and $E_x(\mu_{2^\infty}) = L_\infty$. In this subsection the symbol B refers to this base field. Let M be the Galois group over L_∞ of its maximal everywhere unramified abelian pro-2 extension.

Lemma 11.6 (A uniform generator bound)**.** *The compact $\mathbb{Z}_2$-module M can be generated by at most R elements, for a constant R depending only on ψ, independently of q, d, Y.*

Proof. The fixed field k_∞ is the cyclotomic $\mathbb{Z}_2$-extension of $K_\psi(i)$. The latter contains μ_4, so its cyclotomic image is an open subgroup of $1 + 4\mathbb{Z}_2 \simeq \mathbb{Z}_2$. Iwasawa's class module theorem identifies the maximal everywhere unramified abelian pro-2 Galois group over k_∞ with the inverse limit of the dyadic ideal class groups in this tower. It is a finitely generated torsion module over the one-variable Iwasawa algebra. Its μ-invariant vanishes by Ferrero–Washington, since $K_\psi(i)/\mathbb{Q}$ is abelian. The structure theorem over $\mathbb{Z}_2[[T]]$ then gives finite generation over $\mathbb{Z}_2$. Indeed, its distinguished polynomial factors give finite free $\mathbb{Z}_2$-modules before taking powers and its pseudo-isomorphism contributes only finite groups. Denote by r_0 the dimension of its quotient modulo two. This number is independent of Y. [8, 3]

The number of primes above q, d in k_∞ is bounded independently of these primes. In $\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}$ the decomposition group of an odd prime p is the closure of $\langle p\rangle$ in $\mathbb{Z}_2^\times$, since the extension is unramified there and Frobenius acts by p. Put $a = v_2(p^2-1)$. For $q \equiv 3 \bmod 8$ one has $a = 3$, and for $d \equiv 7 \bmod 16$ one has $a = 4$. The powers of p^2 generate $1 + 2^a\mathbb{Z}_2$ topologically by the dyadic logarithm. Thus the index of each decomposition group is at most $2^{a-1} \le 8$. Passing to k_∞ multiplies the number of primes by at most $o = [K_\psi : \mathbb{Q}]$. In total there are at most $16o$ such places.

Let $\mathcal{P}$ be the maximal pro-2 Galois group over k_∞ unramified away from these places. Its maximal elementary abelian quotient is its Frattini quotient, obtained by killing squares and commutators and taking the closure. On additionally killing all inertias above q, d, this quotient has dimension r_0. At a place of odd residue characteristic p, the dyadic image of inertia is procyclic. Indeed wild inertia is pro-p and the pro-2 quotient of tame inertia is procyclic. Here the cyclotomic tower over the finite base is unramified at q, d, so the absolute inertia groups can equally be computed over that finite base. Conjugation has no effect in the elementary abelian quotient. Each of the at most $16o$ places thus contributes at most one further generator. The pro-2 basis theorem gives at most $r_0 + 16o$ topological generators for $\mathcal{P}$.

The extension L_∞/k_∞ has degree at most four, and is unramified away from q, d, by the quadratic discriminants. It corresponds to a subgroup of $\mathcal{P}$ of index at most four. Every finite unramified abelian 2-extension of L_∞ lies in the corresponding maximal extension: its finitely many conjugates over k_∞ have compositum a Galois 2-extension of k_∞ unramified away from q, d. Therefore M is a quotient of that subgroup. The Schreier generator bound for an index-e subgroup of a d-generated pro-2 group is $1+e(d-1)$. It follows by choosing coset representatives along a spanning tree in the coset graph and taking the remaining Schreier generators, then taking the closure. We may take $R = 1 + 4(r_0 + 16o)$. □

Theorem 11.7 (A common set of exceptional twists at two)**.** *There is a constant $R = R(\psi)$ such that, for each sufficiently large Y and the single chosen pair q, d, there exists one set $\mathcal{R}_Y$ of at most R positive integers with*

$$\operatorname{length}_{\mathbb{Z}_2} \mathcal{S}_{2,r}(E_x) \ll_{\psi,\varepsilon} \log(2x) \qquad (x \in I_Y,\ 1 \le r < t(x),\ r \notin \mathcal{R}_Y).$$

In particular the contribution of all these twists at two to (L) *is $O_{\psi,\varepsilon}(t(x)\log(2x))$.*

Proof. The group $\Gamma_* = \mathrm{Gal}(L_\infty/B(i))$ acts on M by conjugation. The action is well-defined because the maximal unramified abelian extension is invariant and M is abelian. The cyclotomic character embeds Γ_* as an open subgroup of $1 + 4\mathbb{Z}_2$. Choose a topological generator γ and write $u = \kappa(\gamma)$, $e_* = v_2(u-1)$. Its index in $1+4\mathbb{Z}_2$ is 2^{e_*-2} and is at most $[B(i):\mathbb{Q}] \le 8o$, by intersecting $B(i)$ with the cyclotomic extension. In particular e_* is uniformly bounded.

Take a minimal surjection $\pi : \mathbb{Z}_2^D \to M$, so $D \le R$ and its reduction modulo two is an isomorphism onto $M/2M$. If $D = 0$, Proposition 6.5 already bounds every length by one. Otherwise lift the images under γ of these D generators to columns of a matrix A over $\mathbb{Z}_2$. Then $\pi A = \gamma\pi$ and A is invertible since its reduction is. This also handles finite torsion in M. The image of the pro-2 group Γ_* on $M/2M$ is a finite 2-group, so the reduction of A is unipotent. Fix $h_* = \lceil \log_2 R \rceil + 1$. In characteristic two, $(I+U)^{2^k} = I + U^{2^k}$ for a nilpotent D-by-D matrix U. Consequently $A^{2^{h_*-1}} \equiv I \bmod 2$. Squaring gives $A' = A^{2^{h_*}} \equiv I \bmod 4$.

The subgroup $\mathrm{Gal}(L_\infty/E_x(i))$ is generated topologically by $\gamma^{2^{h_x}}$, where

$$2^{h_x} = [B(i)C_l : B(i)] = [C_l : C_l \cap B(i)].$$

Thus $2^l/(8o) \le 2^{h_x} \le 2^l$. Throughout I_Y, $h_x \ge h_*$ for large Y and $h_x \ll_\psi \log(2x)$. The module $X_2'(E_x)$ in Section 6.4 is a quotient of M. Its defining extensions over L_∞ are unramified outside two and split completely above two, hence are everywhere unramified. The quotient map respects the action of this subgroup. On imposing the specialization relations of Proposition 6.5 we therefore have a surjection

$$\operatorname{coker}\Bigl(A^{2^{h_x}} - u^{-r2^{h_x}} I\Bigr) \longrightarrow X_r'.$$

Imposing one generator relation suffices for this surjection because all the relations defining X_r' are imposed in its target.

Let $\alpha_1, \dots, \alpha_D$ be the eigenvalues of A', with multiplicity, in $\overline{\mathbb{Q}}_2$, normalizing $v_2(2) = 1$. Each satisfies $v_2(\alpha_i - 1) \ge 2$, since $(A' - I)/4$ is an integral matrix. Put $b_r = u^{-r2^{h_*}}$, also congruent to one modulo four. At each squaring step $v_2(a+b) = 1$ for two such units, so $v_2(a^2 - b^2) = v_2(a-b) + 1$. The expression also holds with infinite valuation at equality. Applying this to each eigenvalue, without any diagonalizability assumption, gives

$$v_2 \det\Bigl(A^{2^{h_x}} - u^{-r2^{h_x}} I\Bigr) = D(h_x - h_*) + \sum_{i=1}^{D} v_2(\alpha_i - b_r).$$

Put $T_Y = \lfloor (2Y)^{(3/2)^{401}} \rfloor$, $J_Y = \lceil \log_2(T_Y + 1) \rceil$. For distinct $1 \le r, s \le T_Y$,

$$v_2(b_r - b_s) = e_* + h_* + v_2(r-s) \le e_* + h_* + J_Y.$$

The equality is the principal-unit binomial identity proved in Lemma 6.6. Consequently, for each α_i, at most one integer $1 \le r \le T_Y$ has $v_2(\alpha_i - b_r) > e_* + h_* + J_Y$. Otherwise the ultrametric inequality would contradict the last display. Collect these integers in $\mathcal{R}_Y$. The choices of A', u, and T_Y precede the choice of x. The same $\mathcal{R}_Y$ thus works throughout I_Y.

For every remaining twist the determinant is nonzero and its valuation is at most $D(h_x + e_* + J_Y)$. This is $O_{\psi,\varepsilon}(\log(2x))$, since $x \geq 2Y$. The elementary divisor theorem bounds the length of X_r' by that valuation. Proposition 6.5 adds at most one for the kernel of restriction, proving both conclusions. □

The exceptional set gives a precise limitation of the spacing argument. Even a unit α arbitrarily close to a single b_r satisfies all of the pairwise spacing inequalities. Proposition 11.4 proves finiteness at that twist. Theorem 11.5 bounds its subgroup of bounded exponent. Sections 11.3 and 11.4 combine a shorter interval, descent, and an effective bounded-degree estimate to handle their full lengths. At odd primes the missing terms are the complementary sign from Section 11.1 beyond the prime or exponent cutoff of Theorem 11.5.

11.3 The remaining twists on a common power interval

The proof of Theorem 11.7 leaves at most $R(\psi)$ dyadic twists. We now descend their full local lengths to a field of bounded degree and choose one interval on which every such twist that actually occurs is small. Both conclusions concern the groups in (L) themselves.

Proposition 11.8 (Descent without a torsion error)**.** *Use $B, L_\infty, \Gamma_*, h_*, h_x$ from Section 11.2. There is a field $F_* \subset L_\infty$ containing $B(i)$, of degree bounded solely in terms of ψ, such that for every $r \geq 1$ and every sufficiently large x with $h_x \geq h_*$,*

$$\operatorname{length}_{\mathbb{Z}_2} \mathcal{S}_{2,r}(E_x) \leq 1 + R(\psi)(h_x - h_*) + \operatorname{length}_{\mathbb{Z}_2} \mathcal{S}_{2,r}(F_*).$$

Moreover $\log(2|\operatorname{disc} F_*|) \ll_\psi \log(2Fqd)$.

Proof. Take F_* to be the fixed field of $\gamma^{2^{h_*}}$, meaning the closed subgroup it generates in Γ_*. Its index over $B(i)$ is 2^{h_*}, hence its degree is bounded. The cyclotomic image of this subgroup is $1 + 2^{e_*+h_*}\mathbb{Z}_2$. Thus $F_* = B(i, \mu_{2^{e_*+h_*}})$ and its conductor divides $2^{e_*+h_*}Fqd$. The bounds for e_*, h_* and the conductor–discriminant formula give the discriminant estimate.

Let X be the maximal abelian unramified pro-2 Galois group over L_∞ on which all decomposition groups over two vanish. This is an intrinsic quotient of M from Lemma 11.6. It is the group X_2' in Section 6.4 for each of the base fields F_*, E_x. To see this, at any $v \nmid 2$ the cyclotomic extension of either base is unramified, so its absolute inertia subgroup at v is unchanged on passage to L_∞. An extension cut out by a quotient defining X, together with all its conjugates over that base, kills these inertia subgroups. It is therefore contained in the base field's maximal extension unramified away from two. Conversely, the extensions defining X_2' are unramified there and split over two. These descriptions give the same quotient and conjugation action.

Both F_* and its dyadic completions contain i. Their cyclotomic Galois groups are open subgroups of $1 + 4\mathbb{Z}_2$, hence are procyclic and isomorphic to $\mathbb{Z}_2$. The degree-one inflation and degree-two obstruction in Proposition 6.5 then vanish, exactly as in its procyclic calculation. Locally the same holds at every prime over two. Consequently, with $b_r = u^{-r2^{h_*}}$,

$$\mathcal{S}_{2,r}(F_*)^\vee \simeq X/(\gamma^{2^{h_*}} - b_r)X.$$

For E_x the length of its strict group is at most one plus the length of $X/(\gamma^{2^{h_x}} - u^{-r2^{h_x}})X$, since the relations from the full cyclotomic Galois group include this one.

Apply the minimal-generator construction in Theorem 11.7 to X itself. Write $\pi : \mathbb{Z}_2^D \to X$ for the surjection and A for a lift of γ. Now $D \leq R$, and $A' = A^{2^{h_*}} \equiv I \bmod 4$ as before. Let

$a = h_x - h_*$. Factoring a difference of 2^a-th powers gives

$$(A')^{2^a} - b_r^{2^a} I = 2^a (A' - b_r I) \prod_{j=0}^{a-1} \frac{(A')^{2^j} + b_r^{2^j} I}{2}.$$

Every factor in the product is an integral matrix congruent to I mod 2, hence invertible over $\mathbb{Z}_2$. Its product therefore maps the entire free cover onto itself. After applying π, the image of the left hand side is exactly $2^a Z$ with $Z = (\gamma^{2^{h_*}} - b_r)X$. This uses equality of images on a free cover and holds even if X has finite torsion. Now Z has at most D generators since it is an image of X. The kernel of $X/2^a Z \to X/Z$ is $Z/2^a Z$ of length at most aD. The length of X/Z is finite by Proposition 11.4 and its proof, which applies to the totally imaginary field F_*. This proves the proposition, including $D = 0$. □

Theorem 11.9 (Small exceptional twists on the interval used for the count)**.** *Fix $0 < \eta < 401$. For arbitrarily large Z there exist primes q, d, a field F_* as above, a real $V \geq Z$, and at most $R(\psi)$ exceptional integers such that, simultaneously for every $V \leq x \leq V^{3/2}$, the following hold.*

1. *The fields, characters, and integral prime-sum weights satisfy conditions 1–3. The odd-prime bound of Theorem 11.1 and the finite-exponent bound of Theorem 11.5 hold there.*
2. *At two the length is $O_{\psi,\varepsilon,\eta}(\log(2x))$ for each nonexceptional $r < t(x)$. Every exceptional $r < t(x)$ satisfies $r \leq x^\eta$ and the bound of Proposition 11.8 with this single F_*.*

Proof. Put $c_0 = 401$, $b_1 = c_0/\eta$, $R = R(\psi)$, and fix $K = 2(2b_1)^R$ before choosing Z, q, d. Choose the primes by Theorem 5.1 with initial scale Z and power $K + 1$. In the range $Z \leq x \leq Z^K$ the field is $E_x = BC_l$ with the same q, d, and $\log(qd) \ll Z^{\varepsilon/5}(\log Z)^2$. All conductor, degree, and dyadic generator bounds used in Sections 11.1–11.2 are consequently uniform in this larger range. In Theorem 11.7 make the single replacement $T_Y = \lfloor Z^{Kc_0} \rfloor$. Its proof produces at most R exceptional integers for this entire range. The inequality $J_Y \ll_{\psi,\varepsilon,\eta} \log(2x)$ follows from $x \geq Z$.

Here is the interval selection in detail. Starting with $U = K \log Z$, attach to each exceptional integer r the point $a_r = (\log r)/c_0$. If none lies in $(U/(2b_1), U]$, take $v = U/2$. For $v \leq u \leq 2v$ and $a_r \leq u$, one then has $b_1 a_r \leq v \leq u$. Otherwise discard one point in that half-open interval, replace U by $U/(2b_1)$, and repeat. A discarded point exceeds every future upper endpoint. After at most R divisions the procedure terminates. For the resulting v, $v \geq K \log Z/(2(2b_1)^R) = \log Z$ and $2v \leq K \log Z$. Take $V = e^v$. On $[V, V^2]$ this gives

$$r \leq x^{401} \implies r \leq x^\eta \qquad (r \text{ exceptional}).$$

Use the subinterval $[V, V^{3/2}]$.

At its left endpoint it is convenient to choose $a_t = \lceil bx \rceil$ in Proposition 7.2. This makes $x \leq a_t/b \leq x + 1/b$, so the character estimates apply even if $V = Z$. At the upper endpoint $a_t/b \leq Z^K + 1 \leq Z^{K+1}$. The proof for integral weights, including its derivative bound, applies to this rounding. All the size, count-weight, and cohomology deductions cited in the statement now hold on this one interval. The primes and F_* were chosen before restricting the interval. □

In particular, the dyadic remainder in this construction can be bounded by the sum of at most $R(\psi)$ orders on a bounded-degree field, counted logarithmically. Explicitly, putting $v_2(2) = 1$, one obtains uniformly

$$\sum_{1 \leq r < t(x)} \operatorname{length}_{\mathbb{Z}_2} \mathcal{S}_{2,r}(E_x) \ll_{\psi,\varepsilon,\eta} t(x) \log(2x) + \sum_{\substack{r \text{ exceptional} \\ 1 \leq r \leq x^\eta}} v_2(|K_{2r}(\mathcal{O}_{F_*})|)\,.$$

This follows by summing Proposition 11.8 and applying Proposition 11.4 at F_*. The dependence on $\operatorname{disc} F_*$ still matters here because the field changes with the chosen auxiliary primes.

11.3.1 The implication still needed for Dirichlet GRH

The prime sum itself detects whether a period comparison on this family would finish the proof. Take $T_2 = A_0$, $m = \lfloor \sqrt{x} \rfloor$, $a_E = xb$, $k = xm$, the integral weights of Proposition 7.2, and $a_t = \lceil bx \rceil$ for all t. These are the numerical choices in Theorem 11.9. An interval in the following proposition always uses one pair q, d.

Proposition 11.10. *With $Q = hmb$ and $\delta = 1/o$, at each x on the selected interval and for every translate u one has*

$$\frac{2\Delta_u}{Q\delta} = \mathcal{G}_\psi(x) + O_{\psi,\varepsilon}(x^{1/2+\varepsilon/2}).$$

Consequently, to prove Main Theorem 1.1 it suffices to establish (6.3) *for these counts on arbitrarily distant selected intervals for every primitive ψ and arbitrarily small $\varepsilon > 0$. Conversely, Main Theorem 1.1, if established, would imply* (6.3) *for these numerical choices on every sufficiently distant selected interval.*

Proof. Every distinguished set L_u is the same because $T_2 = A_0$. The idealized contribution for each translate therefore equals its average in Lemma 6.2. The exact coset proportions of Proposition 6.4 give the weights of $\mathcal{G}_\psi(y)$ on the retained characters, with $y = \lceil bx \rceil / b$. The other $3o$ surviving characters have weights of modulus at most one after normalizing the sum over T. Their total is at most $3o\, y^{1/2+\varepsilon/2}$ by Theorem 5.1. The comparison of actual and idealized weights in condition 3 costs at most $4/(\delta x)$ after multiplication by $2/(Q\delta)$. Finally $0 \le y - x \le 1/b$, and the slope bound in the proof of Proposition 6.3 gives $|\mathcal{G}_\psi(y) - \mathcal{G}_\psi(x)| \ll_\psi (1 + \log^2(2x))/b$. This proves the formula.

The sufficiency statement is Proposition 6.3 followed by Theorem 1.2. In the other direction, the critical-line assertion would give $|\mathcal{G}_\psi(x)| \ll_\psi \sqrt{x}$ by Theorem 3.3. Since $\mathcal{B}/Q \ge ha_E/(hmb) = x/m \ge \sqrt{x}$, the formula in the proposition would yield $\Delta_u \le x^{5\varepsilon}\mathcal{B}$ for every large x on those intervals. □

Even for the primitive character of conductor one, the retained term here is the smoothed prime sum for the Riemann zeta function. A proof of (6.3) must bound that term independently of its zeros. In the proposed theta argument the local divisibility must measure the Frobenius-weighted count for the specified projected period maps, and the norm and index estimates must hold for the same maps. The endpoint comparison in Theorem 7.3 and the local length estimates above establish parts of this argument. The required upper bound for these projected periods and the remaining part of (L) have not been derived. Section 11.4 completes the dyadic part of the local cohomology estimate.

11.4 The full local-length bound at the prime two

We now bound the exceptional twists of Theorem 11.9. The necessary input is an estimate in terms of the degree and discriminant of F_*. Its degree is bounded before the auxiliary primes are chosen. Write $D_L = |\operatorname{disc} L|$ for any number field L.

Lemma 11.11 (A dyadic bound at bounded degree)**.** *Fix $d_0 \ge 2$. If L is totally imaginary of degree $d \le d_0$, then for all $r \ge 1$*

$$\operatorname{length}_{\mathbb{Z}_2} \mathcal{S}_{2,r}(L) \le \exp\Big(C_{d_0}(r+2)^8 \log(2(r+2)D_L)\Big).$$

Proof. Set $i = 2r$, $n = 2i + 8$, $\Gamma = \mathrm{GL}_n(\mathcal{O}_L)$, and $D = dn^2$. We first bound an integer annihilating the torsion in $H_i(\Gamma, \mathbb{Z})$. Use the contractible well-rounded retract W of Ash for the free lattice $\mathcal{O}_L^n$. Its cells are indexed by the sets of shortest nonzero vectors for positive archimedean Hermitian metrics, normalized to have squared trace minimum one. A face has a larger set of shortest vectors than a cell containing it, with equality only for the same cell. Stabilizers are finite. The metrics form an open cone in a real vector space of dimension at most D. The well-rounded condition is that the shortest vectors span L^n over L. [9, Sec. 2.3]

Bayer-Fluckiger, Emery and Houriet give a finite set $\Phi \subset \mathcal{O}_L^n$ into which some $\gamma \in \Gamma$ simultaneously moves all shortest vectors of any one well-rounded form. Their Corollary 5.2 applies to free lattices of rank at least five over a field other than $\mathbb{Q}$, as here. Its explicit estimate implies

$$\log(2 + |\Phi|) \le C_{d_0}(n+1)^3 \log(2nD_L).$$

We use this assertion about shortest vectors, which has no restriction on the residue characteristic. [9, Cor. 5.2]

We count chains of incident cells. For a vector v, the equation that it has squared trace length one is affine linear in the metric. For the shortest-vector set of any cell, the corresponding simultaneous affine equations are consistent and are implied by at most $D+1$ of them, by linear algebra. Such a choice from its shortest vectors determines the cell among cells for which it spans the simultaneous equations. Indeed, if two cells yield the same choice, every shortest vector of either has length one for a form in the other. Normalization then makes their full shortest-vector sets equal. In a chain of cells take its smallest face and move its shortest vectors into Φ. After this single move, every shortest-vector set in the chain is contained in Φ. Each member can therefore be encoded by a list of at most $D+1$ vectors from Φ. A strict chain has at most $D+1$ cells by dimension. Allow a padding symbol in the lists and for missing cells. The number of Γ-orbits of simplices of the barycentric subdivision of W is at most $(2 + |\Phi|)^{(D+2)^2}$. This argument permits arbitrary incidences among the shortest-vector equations.

Let Γ_3 be the kernel of reducing the underlying $\mathbb{Z}$-linear action on $\mathcal{O}_L^n$ modulo three. Its index J is at most $3^{(dn)^2}$ and it is torsion-free by the binomial argument in Theorem 7.3. Thus it acts freely on the contractible subdivided retract. Its quotient computes integral group homology. This quotient has at most

$$C = J(2 + |\Phi|)^{(D+2)^2}$$

oriented simplices when one orientation is chosen for each simplex. Indeed a Γ-orbit splits into at most J orbits under the subgroup. Equivalently one may use the quotient as a simplicial cell complex, allowing face identifications. Each column of the boundary in degree $i+1$ has sum of absolute entries at most $i+2$, from the alternating sum of its faces. If the boundary matrix has rank $k > 0$, the order of the torsion in its cokernel divides the absolute value of any nonzero k-rowed minor by Smith normal form. Hadamard’s inequality bounds such a minor by $(i+2)^k$. The rank-zero case contributes order one. Homology embeds in the cokernel. Consequently $T = |H_i(\Gamma_3, \mathbb{Z})_{\mathrm{tors}}|$ satisfies $\log T \le C \log(i+2)$. Transfer followed by inclusion is multiplication by J on the homology of Γ. It follows that JT kills every torsion class in $H_i(\Gamma, \mathbb{Z})$. In particular

$$\log(JT + 1) \le \exp\Bigl(C'_{d_0}(n+1)^7 \log(2nD_L)\Bigr),$$

since $D = dn^2$.

Homological stability for general linear groups over a Dedekind ring identifies $H_i(\Gamma, \mathbb{Z})$ with $H_i(\mathrm{GL}(\mathcal{O}_L), \mathbb{Z})$ in this range. The stable range $n \ge 2i+1$ used for rings of integers in Section

3.1 of the cited paper suffices. Quillen's plus construction gives the same integral homology for the connected space $B\,\mathrm{GL}(\mathcal{O}_L)^+$ and identifies its i-th homotopy group with $K_i(\mathcal{O}_L)$. [9, Sec. 3.1][6]

We also need the Hurewicz kernel at two. Mathew's Theorem 1.3(a) says that $2^{\lceil i/2\rceil+3}$ kills the dyadic part of the kernel of the stable Hurewicz map of any connective spectrum in positive degree i. Apply it to the connective algebraic K-theory spectrum. The space $B\,\mathrm{GL}(\mathcal{O}_L)^+$ is its basepoint component in the infinite loop space. The adjunction map from the suspension spectrum of that component to the K-theory spectrum takes its ordinary Hurewicz image to the stable Hurewicz image. Indeed both are obtained from a representative sphere map by applying integral homology, followed in the second case by this adjunction map. Hence a dyadic homotopy class killed by ordinary Hurewicz is killed by 2^{r+3}. As $K_{2r}(\mathcal{O}_L)$ is finite, its ordinary Hurewicz image is torsion. We have proved that $2^{r+3}JT$ annihilates its dyadic part. [10, Thm. 1.3(a)]

By the duality and comparison in the proof of Proposition 11.4, the same integer kills the strict group. To bound its length from its exponent, its dimension modulo two, equivalently its dimension of elements killed by two, is also needed. The Kummer argument of Theorem 11.5 at $\ell = 2$ applies directly to L, since $\mu_2 \subset L$. Dirichlet's unit theorem bounds the unit contribution by $2d$. Minkowski's bound and the estimate $\zeta_L(2) \le \zeta(2)^d$ bound $\log|\mathrm{Cl}(L)|$ by $O(d + \log(2D_L))$, including for nonabelian L. The number of cyclic summands is therefore $O_{d_0}(\log(2D_L))$. Multiplying this by $r + 3 + \log_2(JT)$ bounds the length. Since $n = 4r + 8$, the asserted exponent eight absorbs the last factors. □

Theorem 11.12 (All dyadic twists on the common interval)**.** *For every fixed primitive ψ and $0 < \varepsilon < 1/52$, there are arbitrarily distant intervals $[V, V^{3/2}]$ and a single pair of auxiliary primes on each interval for which, at every x therein,*

$$(\log 2) \sum_{1\le r<t(x)} \mathrm{length}_{\mathbb{Z}_2}\, \mathcal{S}_{2,r}(E_x) \le \tfrac{1}{4}\exp(x^{\varepsilon}/2).$$

On these same fields and intervals the bound (11.1) holds at every odd prime after summing the specified eigenspace, and the integral prime-sum weights satisfy conditions 1–3.

Proof. Use Theorem 11.9 with $\eta = \varepsilon/64$. The degree of F_* is bounded in terms of ψ. Its discriminant satisfies $\log(2D_{F_*}) \ll_\psi \log(2Fqd) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$ throughout the selected interval by Proposition 11.8 and the bounds for q, d. For an exceptional $1 \le r < t(x)$, the interval choice gives $r \le x^{\eta}$. The exponent in Lemma 11.11 is then at most $C_{\psi,\varepsilon}x^{3\varepsilon/8}$, using $8\eta = \varepsilon/8$. Apply the lemma to the strict group over F_* in Proposition 11.8. The descent contributes $O_\psi(\log(2x))$ for each such twist. There are at most $R(\psi)$ of them. For every other twist Theorem 11.9 gives $O_{\psi,\varepsilon}(\log(2x))$ directly. Thus the sum before its factor $\log 2$ is bounded by

$$C_{\psi,\varepsilon}\Big(t(x)\log(2x) + \exp(C_{\psi,\varepsilon}x^{3\varepsilon/8})\Big).$$

As $t(x) \le x^{401}$ and $3\varepsilon/8 < \varepsilon$, this gives the stated quarter of the allowance for all sufficiently large V. All the other assertions were included in the selection theorem. □

The full dyadic term in (L) and the odd part in (11.1) now use at most half its allowance. The remaining cohomological task is to bound the $(-1)^r$-eigenspace for odd primes beyond the ranges in Theorem 11.5. The geometric task is to prove (6.3) for the projected integral theta periods on the same interval. Proposition 11.10 shows why that estimate, if established, would imply the intended main theorem.

11.5 Local cohomology at the primes of the theta tests

Write $E = E_x$, $F = E^+$, $f = [F : \mathbb{Q}]$, and $d = [E : \mathbb{Q}] = 2f$ for the common family of Section 6.6. Let N be the cyclotomic modulus there. The two split prime ideals $\mathfrak{p}, \mathfrak{q}$ in the theta construction represent the narrow classes of the absolute different $\mathfrak{d}_F$ and the ideal $\mathfrak{a}_0$ below $(\sqrt{-d_0})$. We shall use the strict cohomology groups of the original field throughout. The auxiliary class fields below enter only in the choice of the two primes.

Proposition 11.13 (Split primes above a prescribed threshold)**.** *Let R_0 be the product of the distinct rational primes dividing $2Ng_1g_2T$. For every real $Y \geq 2$, the two prime ideals may be chosen above distinct rational primes $\ell_1, \ell_2 > Y$, outside R_0, which split completely in E. With an absolute implied constant,*

$$\log \ell_1 + \log \ell_2 \ll f^2(1 + \log |D_F| + \log(2Y) + \log(2R_0)(1 + \log(2f))).$$

In particular their logarithmic sizes are polynomial in x uniformly whenever $\log(2Y)$ is so bounded.

Proof. First consider one of the two classes. Write U for the set of rational primes to avoid, initially those dividing R_0. Put $R_U = \prod_{p \in U} p$. Take $M = \prod_{p \in U} p^{k_p}$ as in Proposition 72.23, with k_p the least positive integer such that $\varphi(p^{k_p}) > f$. Thus $\log M \leq \log R_U + |U| \log(2f)$. The extension $L_0 = H^+(F)F(\zeta_M)$ is abelian over F and ramifies above all the excluded primes.

Choose any prime $l \mid (R_U + 1)$, so $l \notin U$, $l \nmid N$, and $\log l \leq \log(2R_U)$. Let $a \geq 1$ be least such that $l^a > Y + 1$. Then $\log(l^a) \leq \log(Y + 1) + \log l$. At every place of F above l the field F is unramified over $\mathbb{Q}_l$. The totally ramified local cyclotomic extension $\mathbb{Q}_l(\zeta_{l^a})/\mathbb{Q}_l$ remains totally ramified of full degree after this unramified base change. Hence $F(\zeta_{l^a})/F$ has the entire group $(\mathbb{Z}/l^a\mathbb{Z})^\times$ as its inertia there. The extension L_0/F is unramified at l since the narrow Hilbert class field is unramified at finite places and $l \nmid M$. Their intersection is F, since every nontrivial subextension of $F(\zeta_{l^a})/F$ is ramified there. Thus we may prescribe a lift of the narrow class on L_0 and prescribe $-1 \bmod l^a$ independently on $F(\zeta_{l^a})$.

The finite conductor norm of any character on the composite is at most $(Ml^a)^f$, by the character extension and local norm calculation in Proposition 72.23. The unconditional theorem of Thorner and Zaman, Theorem 1.1 gives an unramified degree-one prime of F in the prescribed Frobenius class, with

$$\log \ell \ll 1 + \log |D_F| + f(\log M + \log(l^a) + \log(2f)).$$

Here ℓ is its rational prime norm. The action on roots of unity forces $\ell \equiv -1 \pmod{l^a}$, so $\ell > Y$. The rational prime avoids U, and in particular N, hence is unramified in $E/\mathbb{Q}$. The chosen narrow class restricts trivially to E/F, by Lemma 72.18. The prime of F therefore splits in E. As $E/\mathbb{Q}$ is Galois, the existence of one prime there of absolute residue degree one proves complete splitting of ℓ.

For the second class add ℓ_1 to U and repeat. At this step $\log R_U = \log R_0 + \log \ell_1$ and $|U| \leq 1 + \log R_0 / \log 2$. Substitution of the first bound into the second yields the displayed estimate. All original family parameters on its right have logarithms or degrees polynomially bounded as asserted. □

For a number field K, a finite place w and a coefficient prime p, put $A_{p,r} = (\mathbb{Q}_p/\mathbb{Z}_p)(-r)$ for $r \geq 1$. Write G_w and I_w for the local Galois and inertia groups. Use arithmetic Frobenius and write $q_w = Nw$. Say that a local class is unramified when its restriction to I_w vanishes. Impose the original archimedean conditions in every group. In our application E is totally imaginary.

Lemma 11.14 (Local restrictions at a negative twist)**.** *If $w \nmid p$, the unramified part of $H^1(K_w, A_{p,r})$ is zero and the whole local group is cyclic of order $p^{v_p(q_w^{r+1}-1)}$. At $w \mid p$, writing $e_w = e(K_w/\mathbb{Q}_p)$, the unramified part has logarithmic order at most*

$$(2 + v_p(r) + v_p(e_w)) \log p.$$

At $K_w = \mathbb{Q}_p$ with p odd and $p - 1 \nmid r$, this unramified group is zero.

Proof. Away from p the coefficient is unramified. The quotient of the decomposition group by inertia is procyclic, of p-cohomological dimension one. Inflation–restriction computes its degree-one term as $A_{p,r}/(q_w^{-r} - 1)A_{p,r}$. The multiplier is a nonzero p-adic integer and the module is divisible, so this group vanishes. The full local cohomology is thus $\mathrm{Hom}_{\mathrm{cont}}(I_w, A_{p,r})^{\mathrm{Frob}_w}$. The wild inertia and prime-to-p factors of tame inertia contribute zero. On the pro-p factor $\mathbb{Z}_p(1)$, Frobenius acts as multiplication by q_w. The induced action on its homomorphisms to $A_{p,r}$ is therefore multiplication by q_w^{-r-1}. Its fixed group is the torsion killed by $q_w^{r+1} - 1$ in $\mathbb{Q}_p/\mathbb{Z}_p$, giving the stated cyclic group.

At $w \mid p$, unramified cohomology is a quotient of $A_{p,r}^{I_w}$, by the same procyclic computation. The image of the local cyclotomic character on inertia over $\mathbb{Q}_p$ is all of $\mathbb{Z}_p^\times$, since the p-power cyclotomic extensions are totally ramified. Its image on I_w has finite index h dividing e_w. Indeed the index of I_w in the absolute inertia of $\mathbb{Q}_p$ is e_w, and passing to images gives a divisor of that index. For odd p, the element $(1+p)^h$ belongs to the image. Invariance implies annihilation by $(1+p)^{rh} - 1$, of valuation $1 + v_p(rh)$. At two use 5^h and valuation $2 + v_2(rh)$. These valuations follow by binomial expansion, first at an exponent prime to p and then at each successive multiplication of the exponent by p. The order of the unramified quotient has the asserted upper bound. If $K_w = \mathbb{Q}_p$ and $p - 1 \nmid r$, a Teichmüller root of unity in inertia acts on the coefficient by a scalar whose difference from one is a unit. There are then no inertia invariants. □

Let R be any squarefree product of rational primes and let W consist of all places of E over its divisors. Write $\mathcal{S}_{p,r}(E)$ for the usual strict group. Its classes are unramified away from p and vanish on every decomposition group above p. This is the local condition in `Formalism/GaloisCohomology/Statement.lean`, line 75. Define $\mathcal{S}_{p,r}^W(E)$ by allowing the full local group at $w \in W$, $w \nmid p$, and unramified classes at $w \in W$, $w \mid p$. Keep the strict conditions at all other places.

Theorem 11.15 (The cost of the finite test places at every twist)**.** *For each integer $t \geq 2$ one has*

$$0 \leq \sum_{1 \leq r < t} \sum_{p} \log |\mathcal{S}_{p,r}^W(E)/\mathcal{S}_{p,r}(E)| \ll d\, t^2 \log(2Rdt). \tag{11.2}$$

Every original strict class already restricts to zero at every finite place. At odd primes the same upper bound holds for the total increase in the logarithmic orders after applying the sign $(1 + (-1)^r c)/2$ and the operators $p^{k_{p,r}}(1 - \pi_{p,r})$ of equation 19.15.

Proof. Away from p a strict local class is unramified and hence zero by the lemma. At p it is zero by definition. Embed the global quotient in the direct sum of its allowed local groups at W by restriction. The kernel consists exactly of the original strict classes. The quotient is finite since these local groups are finite. For a fixed $w \in W$ the sum over coefficient primes different from its residue characteristic is at most $(r+1)\log q_w$, by factoring the positive integer $q_w^{r+1} - 1$. The sum of $\log q_w$ over all W is at most $d \log R$, by the residue degree formula. The resulting contribution over all twists is at most $d(t-1)(t+2)\log R/2$.

For the coefficient primes equal to the residue characteristic use the second part of the lemma. For each rational prime there are at most d places, all with the same ramification index dividing d, since $E/\mathbb{Q}$ is Galois. Consequently at a single r the remaining sum is at most $d(2\log R + \log r + \log d)$, by factoring r and d. This proves (11.2), including the coefficient prime two. In particular all prime sums for these quotients are finite.

Both global groups are stable under $\mathrm{Gal}(E/\mathbb{Q})$, since W contains whole rational fibers. The sign and the indicated averaging projectors are integral group-ring operators at the coefficient primes where they are used. For any such combined endomorphism T_0, the map from the quotient of the two groups onto the quotient of their images under T_0 is surjective, by applying T_0 to representatives. The order of the latter quotient is therefore bounded by the former. Additivity of the logarithmic order gives the last assertion. □

Corollary 11.16 (The cohomological and theta choices on the same interval)**.** *Take $t = \lfloor x^{401} \rfloor$, $b = \exp(x^{\epsilon})$, and Y at least $t+2$ and the largest prime-power cutoff in the count of Section 6.6. The two auxiliary primes can be chosen above this Y with logarithmic norms polynomial in x if $\log(2Y)$ is bounded by a power of x. Such a threshold exists on the original intervals. For $R = R_0\ell_1\ell_2$ the left side of (11.2) is $O_{\psi,\epsilon}(x^C)$, hence $o(b^{1/2})$, there. The last real integral comparison of Theorem 104.9, and its finite-depth construction continue to use these very fields and intervals.*

Proof. Each cutoff is of the form a_j/w with positive prescribed weight w. The weights in the construction are eventually at least one and its numerators are $O(xb)$, so one may take $Y \geq \max(t+2, Cxb)$ for a sufficiently large fixed C. Its logarithm is bounded by a power of x. The prime selection gives the original narrow classes, so the separately unramified oscillator data, the bounded generators of Theorem 104.2, and the ensuing theta calculations all apply. The two new rational primes split completely and exceed the cutoffs. At their own coefficient characteristics the relaxed unramified group is zero since $p > t+2$. The original exceptional primes and both auxiliary primes enter the cohomological estimate through $\log R$. This quantity, d, and t are all polynomially bounded in x. This proves the corollary. □

The estimate bounds the change of local conditions at all these primes. The classes already satisfying the original strict conditions lie in the kernel of their restriction to this entire set. Their remaining total order is the global quantity in equation 19.15.

11.6 The remaining local estimate in terms of finite group orders

Keep the pair of auxiliary primes and fields on the intervals of Section 6.6. Write $E = E_x$, $F_+ = E^+$, $n_E = [E : \mathbb{Q}]$, and $t = \lfloor x^{401} \rfloor$. Let N be the cyclotomic modulus of the field construction, so that each character of $\mathrm{Gal}(E/\mathbb{Q})$ has conductor dividing N. For a finite abelian group B, write $|B|_{\mathrm{odd}} = |B|/2^{v_2(|B|)}$. Consider the following sum of logarithmic orders of finite groups.

$$\begin{aligned}\mathcal{A}(E,t) = &\sum_{1\leq 2j<t} \log |K_{4j}(\mathcal{O}_{F_+})|_{\mathrm{odd}} \\ &+ \sum_{\substack{j\geq 1 \\ 2j-1<t}} \log \frac{|K_{4j-2}(\mathcal{O}_E)|_{\mathrm{odd}}}{|K_{4j-2}(\mathcal{O}_{F_+})|_{\mathrm{odd}}}.\end{aligned} \tag{11.3}$$

Here j is an integer and K_i denotes Quillen's algebraic K-group. All the quotients inside the logarithms are positive integers, as the next theorem shows.

Theorem 11.17 (The odd group orders required on the common interval)**.** *Write $\mathcal{L}(x)$ for the left side of* (L) *and put $\mathcal{L}_2(x) = \sum_{1\le r<t} \log|\mathcal{S}_{2,r}(E)|$. On the intervals of Section 6.6 one has*

$$|\mathcal{L}(x) - \mathcal{A}(E,t) - \mathcal{L}_2(x)| \ll n_E^2 t^2 \log(4n_E tN).$$

In particular, uniformly on those intervals as their left endpoints tend to infinity,

$$\frac{\mathcal{L}(x) - \mathcal{A}(E,t)}{\exp(x^{\varepsilon}/2)} \longrightarrow 0. \tag{11.4}$$

Thus any fixed $\delta > 0$ with $\mathcal{A}(E,t) \le (1-\delta)\exp(x^{\varepsilon}/2)$ throughout arbitrarily distant such intervals suffices for (L)*.*

Proof. At an odd prime the action of complex conjugation on a finite group splits into its two eigenspaces by the idempotents $(1+c)/2$ and $(1-c)/2$. At every $r \ge 1$, restriction identifies the plus eigenspace of $K_{2r}(\mathcal{O}_E)$ at odd primes with $K_{2r}(\mathcal{O}_{F_+})$ at those primes. The hypotheses for this descent are satisfied because E/F_+ is unramified at finite places by Theorem 94.9. The descent proof and the comparison with restricted Galois cohomology are in Sections 25.1–25.2. In particular the ratio of the two odd orders is the order of the minus eigenspace. The sign $(-1)^r$ is plus for $r = 2j$ and minus for $r = 2j-1$. Adding its logarithmic orders produces exactly (11.3).

For clarity write $U(E,t)$ for the sum of the logarithmic orders of the opposite eigenspaces, with sign $(-1)^{r+1}$, at odd primes. Let $C_{\mathrm{odd}}(E,t)$ be the sum over $r<t$, $r\ge 1$ and odd ℓ of

$$\sum_{v|\ell} \log|H^0(E_v, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r))| - \log|H^0(E, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r))|.$$

The exact order formula of Theorem 25.1, gives the identity

$$\mathcal{L}(x) = \mathcal{A}(E,t) + \mathcal{L}_2(x) + U(E,t) - C_{\mathrm{odd}}(E,t).$$

Theorem 25.5, bounds $U(E,t)$ by $O(n_E t^2 \log(4n_E tN))$, and Corollary 25.3 bounds $C_{\mathrm{odd}}(E,t)$ by $O(n_E^2 t^2 \log(4n_E t))$. Both terms are nonnegative. This proves the first bound.

On the selected intervals one has $n_E \ll_\psi x^3$ and $\log(2N) \ll_{\psi,\varepsilon} x$. Hence the right side is a polynomial bound in x. In the proof of Theorem 11.12, the full dyadic term on these intervals is at most

$$C_{\psi,\varepsilon}(t\log(2x) + \exp(C_{\psi,\varepsilon} x^{3\varepsilon/8})).$$

The interval selection in Volume IV retains this bound. Since $3\varepsilon/8 < \varepsilon$, division by $\exp(x^{\varepsilon}/2)$ sends it and each fixed polynomial in x to zero uniformly as x increases. This proves (11.4) and the last assertion. □

Corollary 11.18 (The summand from the rational integers)**.** *For every $j \ge 1$ and odd $\ell \nmid n_E$, the group $K_{4j}(\mathbb{Z})\{\ell\}$ embeds as a direct summand of the dual of the actual strict group $\mathcal{S}_{\ell,2j}(E)$. Its image lies in the complementary sign at twist $2j$. For the primitive character of conductor one, this holds at every odd prime. On each of its prescribed fields one consequently has*

$$\sum_{1\le 2j<t} \log|K_{4j}(\mathbb{Z})|_{\mathrm{odd}} \;\le\; \mathcal{L}(x).$$

Proof. For $\mathbb{Q}$ at odd ℓ, the finite-coefficient Poitou–Tate argument of Theorem 25.1, applies with the one real place. Its modified cohomology at this place vanishes because two is a unit on all the coefficients. The cyclotomic characters of $\mathbb{Q}$ and $\mathbb{Q}_\ell$ both have image $\mathbb{Z}_\ell^\times$. Indeed $\Phi_{\ell^a}(1+X)$ is Eisenstein at ℓ for every $a \ge 1$, so that the full global degree is already obtained in

the completion. At twist $-2j$ the global invariant subgroup therefore equals the local one. Its restriction map is the identity under these identifications. In the duality sequence the map from the local degree-two group to the dual of the global invariants is consequently an isomorphism. Thus every class of $K_{4j}(\mathbb{Z})\{\ell\}$ has zero localization at ℓ.

Under extension of scalars to $\mathcal{O}_E$ the number-ring comparison commutes with restriction. Each localization above ℓ is the restriction of the zero localization just proved. The image is therefore in the kernel identified with $\mathcal{S}_{\ell,2j}(E)^\vee$. It is fixed by c, because it comes from $\mathbb{Z}$. This is sign $(-1)^{2j}$.

For the splitting, follow extension of scalars by the transfer that forgets the $\mathcal{O}_E$-module structure. The ring $\mathcal{O}_E$ is free of rank n_E over $\mathbb{Z}$. After a choice of integral basis the composite functor on finitely generated projectives over $\mathbb{Z}$ is naturally isomorphic to the direct sum of n_E copies of the identity. Additivity of algebraic K-theory gives multiplication by n_E on $K_{4j}(\mathbb{Z})$. This multiplication is invertible on the finite ℓ-primary subgroup. Composing its inverse with transfer therefore retracts the strict subgroup onto the indicated copy. For the character of conductor one, E is the compositum of a real cyclotomic field of two-power degree and two quadratic fields. Its degree is a power of two. The splitting applies to all odd primes, and summing the logarithms proves the inequality. □

Proposition 11.19 (The rational summand modulo an odd prime)**.** *Let ℓ be an odd prime, $L=\mathbb{Q}(\zeta_\ell)$, $L^+=L\cap\mathbb{R}$, and $\Delta=\mathrm{Gal}(L/\mathbb{Q})$. Denote the character describing its action on μ_ℓ by $\omega:\Delta\to\mathbb{F}_\ell^\times$. Let $V_\ell=\mathrm{Cl}(L^+)/\ell\,\mathrm{Cl}(L^+)$, with the action of Δ through restriction to L^+. For every $j\geq 1$,*

$$\dim_{\mathbb{F}_\ell} K_{4j}(\mathbb{Z})/\ell K_{4j}(\mathbb{Z}) = \dim_{\mathbb{F}_\ell} V_\ell^{\omega^{-2j}},$$

where the superscript denotes the character eigenspace. Consequently, on the intervals for the character of conductor one, if $J=\lfloor (t-1)/2\rfloor$, then

$$\mathcal{L}(x) \;\geq \sum_{\ell>2 \text{ prime}} \left\lfloor \frac{2J}{\ell-1} \right\rfloor (\log \ell)\dim_{\mathbb{F}_\ell} V_\ell.$$

In particular the rational summands at a fixed ℓ vanish for every j exactly when ℓ does not divide the ordinary class number of L^+.

Proof. Jordan, Klagsbrun, Poonen, Skinner and Zaytman give the rational class-group formula in [11, Thm. 5.1]. We derive its even-character case from the same strict groups used in the interval bound. Write $r=2j$, $M=(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r)$, and $A=M[\ell]=\mathbb{F}_\ell(-r)$. The strict group over $\mathbb{Q}$ is the Pontryagin dual of $K_{4j}(\mathbb{Z})\{\ell\}$ by the first paragraph of the preceding proof. Its ℓ-torsion therefore has the dimension on the left of the first formula. Multiplication by ℓ on M gives the exact row

$$0\longrightarrow H^0(M)/\ell H^0(M)\longrightarrow H^1(A)\longrightarrow H^1(M)[\ell]\longrightarrow 0$$

in global restricted cohomology, and also in local cohomology at ℓ. Restriction on the left is an isomorphism by equality of the global and local cyclotomic images. The kernels of the two other vertical maps are consequently isomorphic by the snake lemma. Thus the ℓ-torsion of the strict group is computed exactly using the finite coefficient A, including when A is a trivial character.

On L the action on A is trivial. The extension $L/\mathbb{Q}$ is unramified away from ℓ and infinity. Its degree $\ell-1$ is a unit in $\mathbb{F}_\ell$, so inflation–restriction and averaging identify global classes with Δ-equivariant continuous homomorphisms to A over L, unramified outside ℓ. The identical inflation–restriction argument works at ℓ, whose decomposition group in Δ is all of Δ. Hence

a strict homomorphism is trivial on the full decomposition group above ℓ. It is unramified everywhere, and the prime above ℓ splits completely in the extension it defines. By the Hilbert class field theorem its source is the ideal class group of L modulo the class of that prime. The prime is principal, generated by $1-\zeta_\ell$. We have thus obtained $\mathrm{Hom}_\Delta(\mathrm{Cl}(L),\mathbb{F}_\ell(-r))$.

The group algebra of Δ over $\mathbb{F}_\ell$ splits into its character eigenspaces, since Δ is cyclic of order $\ell-1$. An equivariant homomorphism to A is an arbitrary linear functional on the ω^{-r}-eigenspace of $\mathrm{Cl}(L)/\ell$ and vanishes on the others. As r is even, complex conjugation acts by $+1$ on that eigenspace. Ideal extension and norm between L^+ and L have composites 2 and $1+c$, respectively. Division by two on the odd-primary groups identifies the plus part with the class group of L^+ at ℓ, equivariantly for Δ. This proves the dimension formula.

In every $(\ell-1)/2$ consecutive values of j, the characters ω^{-2j} run once through all even characters of Δ. Their dimensions sum to $\dim V_\ell$. Every copy of $\mathbb{F}_\ell$ in the indicated reduction gives at least $\log\ell$ to the logarithm of the order of the corresponding finite group. Apply Corollary 11.18 and retain only complete blocks of $j\le J$ for each prime. The displayed sum is finite since its floors vanish for $\ell>2J+1$. A finite ℓ-group is zero exactly when its reduction modulo ℓ is zero, which gives the last assertion. □

The estimates above express the remaining cohomology bound using global orders on the specified fields. Equation (11.3) still needs a uniform upper bound of the size in Theorem 11.17. On the same intervals Corollary 87.3 still leaves the height of the arithmetically normalized theta-period map to be controlled.

11.7 The strict local condition at every coefficient level

At the prime in the coefficients, a class which is zero with divisible coefficients can have a nonzero finite lift. We compute the permitted lifts over the field cut out by the finite character. This also treats coefficient primes ramifying in the original field.

Let K be a number field, let p be an odd prime and let O be the ring of integers of a finite unramified extension J of $\mathbb{Q}_p$. Fix $r\ge1$ and a continuous character η of $G_K=\mathrm{Gal}(\overline{K}/K)$ of finite order prime to p with values in $O^\times$. Write

$$\theta=\eta\kappa_p^{-r},\qquad D=(J/O)(\theta),\qquad A_j=D[p^j]\simeq(O/p^j)(\theta_j)\quad(j\ge1),$$

where κ_p is the cyclotomic character and θ_j is the reduction of θ modulo p^j. The displayed identification sends the class of $p^{-j}a$ to a mod p^j. Let $S_K(\theta)\subset H^1(K,D)$ consist of classes zero on inertia at all finite $v\nmid p$ and zero on G_{K_v} at every $v\mid p$. All cohomology and homomorphisms from Galois groups are continuous. Set

$$F_j=\overline{K}^{\ker\theta_j},\qquad \Gamma_j=\mathrm{Gal}(F_j/K),\qquad R_j=O/p^j.$$

Lemma 11.20 (Restriction to the field of the character)**.** *For each subgroup $H\subset\Gamma_j$ the groups $H^1(H,A_j)$ and $H^2(H,A_j)$ vanish. Thus restriction gives*

$$H^1(K,A_j)\ \simeq\ \mathrm{Hom}_{\Gamma_j}(G_{F_j}^{\mathrm{ab}},A_j).$$

The same assertion holds on decomposition groups, with their own finite images and local fields.

Proof. The finite image is contained in the product of the cyclic Teichmüller group of the residue field of O and the image of $1+p\mathbb{Z}_p$ modulo p^j. The second group is cyclic by the p-adic logarithm, and the two orders are coprime. In particular H is cyclic. For a generator acting by u, with group order n, put $T=1+u+\cdots+u^{n-1}$. The cyclic resolution has alternate

maps $u-1, T$. If $u-1$ is a unit it is exact in positive degrees. If H is trivial the conclusion also follows. In the remaining case u lifts to a rational principal unit with $a = v_p(u-1)$ satisfying $1 \le a < j$. Its exact order modulo p^j is p^{j-a}, since $v_p(u^{p^i}-1) = a+i$. The latter identity follows by the binomial theorem and induction for odd p. Hence $v_p(T) = j-a$. On R_j the kernel of $u-1$ is $p^{j-a}R_j = TR_j$, and the kernel of T is $p^a R_j = (u-1)R_j$. This proves both vanishings. The inflation–restriction sequence and the trivial action over F_j give the two assertions. □

For $v \mid p$ with $\bar{\theta}|_{G_{K_v}} = 1$, define the integer $h_v \ge 1$ by $\theta(G_{K_v}) = 1 + p^{h_v}\mathbb{Z}_p$. Indeed the residual condition cancels the Teichmüller part, leaving the principal part of κ_p^{-r}. The image of κ_p is open in $\mathbb{Z}_p^\times$ because $K_v/\mathbb{Q}_p$ is finite, so this principal image is open. At each $w \mid v$ of F_j use local reciprocity to define

$$\lambda_{w,j}(z) = p^{-\max(h_v,j)} \log \theta(\mathrm{rec}_{F_{j,w}} z) \pmod{p^{\min(h_v,j)}}, \qquad z \in F_{j,w}^\times. \tag{11.5}$$

The formula uses the restriction of the global character to the local abelian Galois group. Either choice of sign for reciprocity gives the same kernel.

Lemma 11.21 (The permitted local homomorphisms)**.** *At $v \mid p$ with nontrivial residual character the finite lift of a strict class must restrict to zero over $F_{j,w}$. At a place with trivial residual character, the allowed homomorphisms on $G_{F_{j,w}}^{\mathrm{ab}}$, viewed by local reciprocity on $F_{j,w}^\times$, are precisely the homomorphisms that factor through $\lambda_{w,j}$. This map is onto $\mathbb{Z}/p^{\min(h_v,j)}$. At $v \nmid p$ the finite local condition is vanishing on inertia over $F_{j,w}$.*

Proof. For any of the local groups G, the kernel of $H^1(G, A_j) \to H^1(G, D)$ is the image of $D^G/p^j D^G$ under the connecting homomorphism. At $v \nmid p$ apply this to inertia. Its image under θ is finite of order prime to p. Thus its invariants are either zero or all of D, and the kernel vanishes. Restriction to inertia over $F_{j,w}$ is injective on the cohomology of inertia downstairs by Lemma 11.20 and inflation–restriction. At $v \mid p$ with nontrivial residual character the full local invariants vanish, which gives the first assertion in the same way.

At the other places over p, put $h = h_v$, $s = \max(h,j)$ and $k = \min(h,j)$. The local invariants of D are $p^{-h}O/O$. A lift of $p^{-h}a$ under multiplication by p^j is $p^{-h-j}a$. Over $F_{j,w}$ its boundary in A_j is the homomorphism

$$g \longmapsto a\,\frac{\theta(g)-1}{p^h} \equiv a\,p^{s-h}\frac{\log\theta(g)}{p^s} \pmod{p^j}.$$

The image of θ over this field is exactly $1+p^s\mathbb{Z}_p$, the kernel of reduction modulo p^j on its local image. If $z \in p^s\mathbb{Z}_p$, then $\log(1+z) - z \in p^{2s}\mathbb{Z}_p$, term by term since $(n-2)s \ge v_p(n)$ for $n \ge 2$ and p odd. As $2s-h \ge j$, the congruence follows. The logarithm maps this principal unit group onto $p^s\mathbb{Z}_p$. Local reciprocity therefore gives all values modulo p^k in (11.5). A homomorphism from $\mathbb{Z}/p^k$ to R_j may send 1 to any element of $p^{j-k}R_j$, and $j-k = s-h$. These are exactly the boundaries just computed. The local restriction is injective by Lemma 11.20, so the condition on the restricted homomorphism is sufficient as well. □

Let Σ be the primes of F_j above p. Define B_j to be the p-primary part of the following idele class quotient of F_j. Divide by $F_j^\times$, the full factors at infinity, and the local unit groups away from Σ. At $w \in \Sigma$ divide by all of $F_{j,w}^\times$ when $\bar{\theta}|_{G_{K_v}} \ne 1$, and by $\ker\lambda_{w,j}$ otherwise. These subgroups are carried to one another by Γ_j, since the global character is invariant under conjugation. If Σ_0 consists of the latter primes, then

$$\mathcal{O}_{F_j,\Sigma}^\times \longrightarrow \bigoplus_{w\in\Sigma_0} \mathbb{Z}/p^{\min(h_v,j)} \longrightarrow B_j \longrightarrow \mathrm{Cl}(\mathcal{O}_{F_j,\Sigma})\{p\} \longrightarrow 0. \tag{11.6}$$

Indeed on removing the full factors at Σ the quotient becomes the ideal class group of the ring of Σ-integers. Retaining the indicated local factors adds the displayed finite groups, modulo the images of principal ideles which are units outside Σ. These come from the global Σ-units. The quotient is finite, and taking primary parts gives the sequence.

Theorem 11.22 (The finite class group formula at every level)**.** *With no restriction on the ramification of p in K, there is an exact sequence*

$$0 \longrightarrow D^{G_K}/p^j D^{G_K} \longrightarrow \mathrm{Hom}_{O[\Gamma_j]}(B_j \otimes_{\mathbb{Z}_p} O, R_j(\theta_j)) \longrightarrow S_K(\theta)[p^j] \longrightarrow 0. \tag{11.7}$$

In particular, when $O = \mathbb{Z}_p$,

$$\log |S_K(\theta)[p^j]| \;\le\; \log |\,\mathrm{Cl}(F_j)| + (\log p) \sum_{w \in \Sigma_0} \min(h_v, j). \tag{11.8}$$

Proof. Multiplication by p^j on D is onto, so every class killed by p^j in $H^1(K, D)$ has a lift in $H^1(K, A_j)$. Under Lemma 11.20 the lifts with image in the strict group correspond to the equivariant homomorphisms with the local conditions of Lemma 11.21. Global Artin reciprocity, with its compatibility with local reciprocity, identifies these with the homomorphisms from the idele class quotient just defined. The targets are p-primary, so passage to B_j and extension of scalars give the middle term of (11.7). The archimedean local factors have no nontrivial finite quotient of odd order. This application uses local and global class field theory. [12]

The kernel on global cohomology is the boundary of $D^{G_K}/p^j D^{G_K}$. Every such boundary meets all the local conditions since its divisible-coefficient class is zero. This proves exactness. For $O = \mathbb{Z}_p$, the number of homomorphisms from a finite abelian p-group B to $\mathbb{Z}/p^j$ is at most $|B|$, by cyclic decomposition. Dropping equivariance, applying (11.6) and using the surjection of the ordinary class group onto the Σ-class group proves (11.8). □

Corollary 11.23 (Recovering successive orders)**.** *Let γ generate Γ_j, and form the finite module*

$$C_j = (B_j \otimes_{\mathbb{Z}_p} O)/(p^j, \gamma - \theta_j(\gamma))(B_j \otimes_{\mathbb{Z}_p} O).$$

Any lift to O of the scalar $\theta_j(\gamma)$ gives the same quotient. Put $a_j = \mathrm{length}_O C_j - \mathrm{length}_O(D^{G_K}/p^j D^{G_K})$ and $a_0 = 0$. Then $a_j = \mathrm{length}_O S_K(\theta)[p^j]$. Equality $a_{j+1} = a_j$ implies $S_K(\theta) = S_K(\theta)[p^j]$. The subtracted term is zero for a nontrivial global residual character. For a trivial global residual character it equals $\min(j, h_K)$, with $\theta(G_K) = 1 + p^{h_K}\mathbb{Z}_p$.

Proof. Equivariance on a cyclic group imposes precisely the displayed relation on the source. The length of $\mathrm{Hom}_O(C_j, R_j)$ is $\mathrm{length}_O C_j$, by cyclic decomposition. Theorem 11.22 proves the length identity. If there were an element of order greater than p^j, a multiple of it would have order p^{j+1}, contradicting equality of the successive finite orders. Finally a nontrivial residual value has unit difference from one. In the trivial residual case the global cyclotomic image is open, as K is finite over $\mathbb{Q}$, and the same invariant calculation as over K_v gives $D^{G_K} = p^{-h_K} O/O$. □

For $K = \mathbb{Q}$ and $\eta = \alpha^{-1}$ as in Section 24.7, this gives a finite class computation also above $1 + v_p(r)$. For the period field $K = K_\psi C_{l'}(\sqrt{-q}, \sqrt{-d_0})$ and $\eta = 1$ it applies directly to the entire strict group on the period field, including the primes dividing its degree or conductor.

11.8 Finite odd cocycles and the strict local condition

Let E be a CM number field in a fixed algebraic closure of $\mathbb{Q}$, stable under the chosen complex conjugation c. Fix a prime ℓ and an integer $r \geq 1$. Write $G_E = \mathrm{Gal}(\overline{\mathbb{Q}}/E)$, $A = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r)$, $A_\nu = A[\ell^\nu]$, and let κ be the ℓ-adic cyclotomic character. Thus g acts by $\kappa(g)^{-r}$. For $\eta \in \{+1, -1\}$, let $Z^\eta_\nu(E, r)$ consist of the continuous cocycles $z : G_E \to A_\nu$ satisfying the following conditions.

1. They vanish on every inertia group away from ℓ.
2. At every place above ℓ they vanish on $D_v \cap \ker \kappa$, for every choice of the decomposition group D_v in G_E.
3. They satisfy $z(cgc) = \eta z(g)$.

Here a cocycle is the function itself. Its image in $H^1(G_E, A)$ is obtained by including A_ν in A and then passing to the class modulo coboundaries. The sign -1 is the positive-weight module called `shaOdd` in the second source archive. Write $\mathcal{S}_{\ell,r}(E)$ for the strict group of Section 11.1, and a superscript in parentheses for the eigensubgroup under the natural action of c on cohomology.

Theorem 11.24 (Comparison at every coefficient level for odd primes)**.** *For $\ell > 2$, including primes dividing $[E : \mathbb{Q}]$, the class map gives*

$$\begin{aligned} Z^-_\nu(E, r) &\simeq \mathcal{S}_{\ell,r}(E)^{((-1)^{r+1})}[\ell^\nu], \\ Z^+_\nu(E, r)/\delta(A)[\ell^\nu] &\simeq \mathcal{S}_{\ell,r}(E)^{((-1)^{r})}[\ell^\nu], \end{aligned}$$

where $(\delta a)(g) = (\kappa(g)^{-r} - 1)a$. The group divided out in the second line is cyclic of order ℓ^ν. The first isomorphism in particular describes the whole finite odd cocycle module, including its elementary divisors.

Proof. Set $\Gamma_v = \kappa(D_v)$. This is an open subgroup of $\mathbb{Z}_\ell^\times$, since $E_v/\mathbb{Q}_\ell$ is finite and the cyclotomic image over $\mathbb{Q}_\ell$ is $\mathbb{Z}_\ell^\times$. Put $\Gamma'_v = \Gamma_v \cap (1 + \ell\mathbb{Z}_\ell)$. It is procyclic and torsion-free. A topological generator γ acts on A by $\gamma^{-r} \neq 1$. Multiplication by $\gamma^{-r} - 1$ on A is surjective. Thus any continuous cocycle on Γ'_v agrees with a coboundary at γ, hence on its dense cyclic subgroup and everywhere by continuity. The quotient Γ_v/Γ'_v has order prime to ℓ. Averaging annihilates its positive cohomology with ℓ-primary coefficients. Inflation and restriction now give $H^1(\Gamma_v, A) = 0$.

By the second local condition, the restriction of z to D_v factors through Γ_v. Its class with coefficients in A is therefore zero. The first condition lets z descend to the Galois group unramified away from ℓ. Indeed the inertia groups there act trivially on its target, and z vanishes on their closed normal span. Its class is strict. The natural action of c on a class represented by z is represented by $g \mapsto (-1)^r z(cgc)$, since c also acts on the coefficients. This gives the signs in the two formulas.

Conversely take a strict class killed by ℓ^ν in the eigensubgroup of sign $\eta(-1)^r$. Represent it by a cocycle y on the unramified-outside-ℓ group. Write $\ell^\nu y = \delta a$ and choose $b \in A$ with $\ell^\nu b = a$. Subtracting δb makes y A_ν-valued. At each $v \mid \ell$ strictness means $y|_{D_v} = \delta a_v$ in A, so y vanishes on $D_v \cap \ker \kappa$. This holds for every conjugate decomposition group. The cocycle $g \mapsto (y(g) + \eta y(cgc))/2$ has all three stated properties and represents the same class, by its assumed eigenvalue.

Finally every coboundary with values in A is unchanged by $g \mapsto cgc$, since the action on coefficients is cyclotomic. For the negative sign this forces a coboundary to vanish. For the

positive sign the kernel is precisely $\delta(A)[\ell^\nu]$. The kernel of $\delta : A \to Z^1(G_E, A)$ is finite, because the global cyclotomic image is open and $r \geq 1$. A quotient of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ by a finite subgroup is isomorphic to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, as multiplication by the order of that subgroup shows. This gives the stated kernel order. □

Proposition 11.25 (The defect at two)**.** *Let $s_2(E)$ be the number of dyadic places of E. For $\ell = 2$ and $\nu \geq 1$, the kernel of the class map on $Z_\nu^-(E, r)$ has order two. Its image modulo its intersection with $\mathcal{S}_{2,r}(E)$ has order at most $2^{s_2(E)}$. The image contains $2\big(\mathcal{S}_{2,r}(E)^{((-1)^{r+1})}[2^\nu]\big)$. In particular,*

$$\operatorname{length}_{\mathbb{Z}_2} Z_\nu^-(E, r) \leq 1 + s_2(E) + \operatorname{length}_{\mathbb{Z}_2} \mathcal{S}_{2,r}(E)[2^\nu].$$

Proof. A dyadic coboundary is invariant under $g \mapsto cgc$, so it satisfies the odd relation exactly when it is killed by two. The preceding computation of $\delta(A)$ then gives one subgroup of order two in the kernel. Its elements satisfy both local conditions and take values in $A[2]$, giving equality. Now take $\Gamma_v' = \Gamma_v \cap (1 + 4\mathbb{Z}_2)$. The generator argument in the theorem still gives $H^1(\Gamma_v', A) = 0$. The quotient Γ_v/Γ_v' has order at most two. It acts on the finite cyclic group $A^{\Gamma_v'}$. Its first cohomology is a subquotient of that cyclic group by evaluation at a generator, and is killed by the group order. Consequently $H^1(\Gamma_v, A)$ has order at most two by inflation and restriction. Localizing the image at all dyadic places bounds its quotient by the strict part as asserted. The construction with $y - \delta b$ in the theorem also gives a finite-valued representative y_0 of any strict class in the displayed eigensubgroup. The cocycle $g \mapsto y_0(g) - y_0(cgc)$ satisfies the odd relation and represents twice the given class. This proves the inclusion and the length bound. □

Corollary 11.26 (The total of the finite odd cocycle lengths on the period fields)**.** *On the polynomial-conductor intervals of Theorem 19.15 take $E = E_x$. One may choose $\nu_{\ell,r} \geq 0$ separately at each prime, weight and node. One may also use any finite extension of $\mathbb{Q}_\ell$ with integer ring $\mathcal{O}_{\ell,r}$ and ramification index $e_{\ell,r}$ for the coefficient module $(\mathcal{O}_{\ell,r}/\ell^{\nu_{\ell,r}})(-r)$. With that coefficient ring understood on the left,*

$$\sum_\ell \log \ell \sum_{1 \leq r < t(x)} \frac{\operatorname{length}_{\mathcal{O}_{\ell,r}} Z_{\nu_{\ell,r}}^-(E_x, r)}{e_{\ell,r}} = o_{\psi,\varepsilon}(\exp(x^\varepsilon/2))$$

uniformly on the selected intervals.

Proof. The finite coefficient module is the original one tensored with $\mathcal{O}_{\ell,r}$ over $\mathbb{Z}_\ell$. In a finite free integral basis all the cocycle, parity and local conditions are coordinatewise. Thus the new solution module is the original one tensored with this ring, compatibly with its scalar action. A cyclic factor of length a becomes $\mathcal{O}_{\ell,r}/\ell^a$ and has length $e_{\ell,r}a$. It suffices to use $\mathbb{Z}_\ell$.

For odd primes the first isomorphism of the theorem bounds the sum by the critical-sign estimate of Theorem 11.1. Indeed its proof gives a polynomial bound in the field degree, the maximum weight and the logarithm of the conductor. All are polynomial on these fields. At two the overhead in the proposition is $O(t(x)(1 + [E_x : \mathbb{Q}]))$ after summing over r. The full dyadic lengths on these same fields are bounded by $O_{\psi,\varepsilon}(t(x)\log(2x) + \exp(C_{\psi,\varepsilon}x^{3\varepsilon/8}))$ by the interval selection in Theorem 19.15 and the proof of Theorem 11.12. These bounds are $o(\exp(x^\varepsilon/2))$. The zero coefficient level contributes zero. This proves the assertion uniformly in all the choices. □

For odd primes the unestimated sign in (L) is the second line of Theorem 11.24. A bound for the odd cocycles alone therefore supplies the first line. The even cocycles modulo the stated coboundaries still enter the original length estimate.

11.9 A cyclotomic annihilator at all coefficient primes

Fix an integer $N \geq 3$, put $G_N = (\mathbb{Z}/N\mathbb{Z})^\times$, and let E be any CM subfield of $\mathbb{Q}(\mu_N)$. For $r \geq 1$ put $n = r + 1$. Write $B_n(X)$ for the Bernoulli polynomial with generating series $te^{Xt}/(e^t - 1)$. In the integral quotient ring

$$R_n = \mathbb{Z}[G_N]/([-1] - (-1)^n[1])$$

form the element and its integer determinant

$$T_n = \sum_{j \in G_N} (n+1)!\, N^n B_n(j/N)[j], \qquad d_n = \det(T_n : R_n \longrightarrow R_n).$$

Every j occurring as an integer denotes its representative in $[1, N-1]$. Choose $b_1 = 1+2N$, $b_2 = 1 + 2Nb_1$. They are coprime to one another, each is congruent to one modulo N, and both exceed one.

Lemma 11.27 (Moments of the integral Stickelberger coefficients)**.** *Fix a prime ℓ and one of b_1, b_2 prime to ℓ, denoted by b_0. For $M = N\ell^L$ let*

$$S_j(L) = \sum_{\substack{1 \leq a < M,\ (a,M)=1 \\ a \equiv j \bmod N}} a^{\,n-1} \lfloor b_0 a/M \rfloor.$$

In $\mathbb{Q}_\ell[G_N]$ the following limit holds, also at $\ell = 2$. In the formula for T_n on the right use its displayed representative in the full group ring.

$$\lim_{L \to \infty} n b_0^{n-1} N (n+1)! \sum_{j \in G_N} S_j(L)[j] = (b_0^n - 1) \begin{cases} T_n, & \ell \mid N, \\ (1 - \ell^{\,n-1}[\ell])T_n, & \ell \nmid N. \end{cases}$$

Proof. Multiplication by b_0 modulo M permutes the units in each class j mod N. Its representative is $a' = b_0 a - M\lfloor b_0 a/M \rfloor$. Expanding $(a')^n$, summing, and using $\sum (a')^n = \sum a^n$, gives

$$n b_0^{n-1} S_j(L) - \frac{b_0^n - 1}{M} \sum_{\substack{a \equiv j \bmod N \\ 1 \leq a < M,\ (a,M)=1}} a^n \ \in\ M\mathbb{Z}.$$

For $v = \ell^L$, first include every $a = j + Nh$, $0 \leq h < v$. The normalized n-th power sum is

$$\frac{1}{Nv} \sum_{h=0}^{v-1} (j + Nh)^n = \frac{N^{n-1}}{n+1} \frac{B_{n+1}(j/N + v) - B_{n+1}(j/N)}{v}.$$

This follows by summing the polynomial finite-difference formula $B_{n+1}(y+1) - B_{n+1}(y) = (n+1)y^n$. As v tends to zero in $\mathbb{Q}_\ell$, the quotient tends to $B'_{n+1}(j/N) = (n+1)B_n(j/N)$. For $\ell \mid N$ the condition $(a, M) = 1$ is automatic. Otherwise the excluded terms have $a = \ell a_0$ with $a_0 \equiv \ell^{-1} j \bmod N$, $1 \leq a_0 < M/\ell$. After division by M their limit is ℓ^{n-1} times the corresponding limit at $\ell^{-1}j$. Combining these computations gives the group-ring formula. □

Theorem 11.28 (One integer annihilates the odd cocycles at every prime)**.** *The positive integer*

$$J_{N,r} = 2(b_1^n - 1)(b_2^n - 1)|d_n|$$

annihilates $Z_\nu^-(E, r)$ for every prime ℓ, every $\nu \geq 0$ and every such E. It satisfies $\log J_{N,r} \ll Nn \log(2Nn)$ with an absolute constant.

Proof. The coefficients of T_n are integers. Indeed $B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}$ and $(i+1)!B_i \in \mathbb{Z}$. The latter follows inductively from $\sum_{j=0}^{i} \binom{i+1}{j} B_j = 0$ for $i \geq 1$, since $i!\binom{i+1}{j}$ is divisible by $(j+1)!$ for $j < i$. The ring R_n is free over $\mathbb{Z}$, with basis represented by one member of each pair $\{j, -j\}$. Over $\mathbb{C}$ its characters are precisely those with $\chi(-1) = (-1)^n$. The Bernoulli formula for $L(1-n, \chi)$ identifies the eigenvalue of T_n at each such character as $-n(n+1)!NL(1-n, \chi)$, using the character as induced to modulus N. It is nonzero by the functional equation and the Euler product at $n > 1$. Each removed Euler factor is $1 - \chi^*(p)p^{n-1} \neq 0$ when $\chi^*(p) \neq 0$. This proves $d_n \neq 0$. On $0 \leq y \leq 1$ the generating series on $|t| = 1$ gives $|B_n(y)| \leq Cn!$ by Cauchy's inequality with an absolute constant. Each eigenvalue of T_n has modulus at most $CN(n+1)!N^n n!$. There are at most N eigenvalues and $b_2 \ll N^2$. Their product gives the stated logarithmic bound.

Fix a cocycle $z \in Z_\nu^-(E, r)$, taking $\nu > 0$. Put $K_M = \mathbb{Q}(\mu_M)$, $M = N\ell^L$. For $L \geq \nu$ the restriction of z to G_{K_M} is a homomorphism, since that group acts trivially on A_ν. For all sufficiently large L it is unramified everywhere. Away from ℓ this follows from the first local condition. At each $v \mid \ell$ the second condition makes $z|_{D_v}$ a continuous function of κ vanishing at one. Its target is finite, so this function vanishes for $\kappa \equiv 1 \bmod \ell^L$ when L is sufficiently large. One L works for representatives of the finitely many v's. For their conjugates the cocycle identity gives $z(shs^{-1}) = \kappa(s)^{-r} z(h)$ when h acts trivially on A_ν, which proves the same vanishing. Class field theory now gives a homomorphism $\phi_L : \mathrm{Cl}(K_M) \to A_\nu$ representing the restriction.

Write σ_a for the automorphism of K_M raising roots of unity to their a-th powers. On these homomorphisms put $P_a\phi(x) = \phi(\sigma_a^{-1}x)$, using the natural action on ideal classes. Set $U_a = a^{-r}P_a$, with the factor read modulo ℓ^ν. If $a \equiv 1 \bmod N$, a lift s of σ_a fixes E. On G_{K_M} the identity $z(s^{-1}hs) = \kappa(s)^r z(h)$ then gives $U_a\phi_L = \phi_L$ by equivariance of the Artin map. The operators U_a commute. On the module generated by their translates of ϕ_L they therefore give an action of G_N, using surjectivity of reduction from the units modulo M. Moreover $P_{-1}\phi_L = -\phi_L$, by the odd cocycle relation. Thus U_{-1} acts by $(-1)^{r+1} = (-1)^n$ on this module and the action factors through the integral ring R_n, including at two.

Choose b_0 among the two specified integers prime to ℓ. The classical Stickelberger theorem for the full cyclotomic field K_M says that $(b_0 - \sigma_{b_0}) \sum_a (a/M)\sigma_a^{-1}$ annihilates $\mathrm{Cl}(K_M)$, where the sum is over reduced representatives. The hypotheses are $(b_0, M) = 1$ and $K_M = \mathbb{Q}(\mu_M)$, both of which hold here. [13, Ch. 6] The coefficient of σ_a^{-1} in this integral element is exactly $\lfloor b_0 a/M \rfloor$, by the same permutation of representatives used above. Evaluating ϕ_L on its action on arbitrary ideal classes gives $\sum_j S_j(L)U_j\phi_L = 0$.

By Lemma 11.27, for all sufficiently large L the coefficients of the scaled last relation agree modulo ℓ^ν with those of the limit. Only this finite congruence is used, so the class groups may vary with L. If $\ell \nmid N$, the extra factor $1 - \ell^{n-1}U_\ell$ is invertible on a module killed by ℓ^ν, by a finite geometric sum. In either case $(b_0^n - 1)T_n\phi_L = 0$. In the regular representation of R_n, the image ideal T_nR_n contains $d_n[1]$, by the adjugate identity applied to the basis vector of $[1]$. It follows that $(b_0^n - 1)d_n\phi_L = 0$.

The cocycle $(b_0^n - 1)d_n z$ consequently factors through $\mathrm{Gal}(K_M/E)$. Conjugating an element of this quotient by c fixes it, since $K_M/\mathbb{Q}$ is abelian. The descended function is also odd under that conjugation. Its values are therefore killed by two. This proves the asserted annihilation for the one $J_{N,r}$ independent of ℓ, ν, E. □

11.10 One integer for the full length of the odd cocycle module

We now pass from the exponent in Theorem 11.28 to orders. Write $F_N = \mathbb{Q}(\mu_N)$, $g = \varphi(N)$ and choose primes $N < P_1 < 2N < P_2 < 4N$, which exist by Bertrand's postulate for $N \geq 3$. For $n \geq 2$ put $W_n = (P_1^{gn} - 1)(P_2^{gn} - 1)$. Keep d_n and $J_{N,n-1}$ of the preceding subsection. For $t \geq 2$ define the positive integer

$$\mathcal{J}_{N,t} = \prod_{n=2}^{t} J_{N,n-1}^{20N^3} W_n^{g/2} |d_n|.$$

For $t = 0, 1$ use the empty product. Throughout the subsection E is any CM subfield of F_N.

Theorem 11.29 (Uniform orders through all weights and coefficient levels)**.** *For each prime ℓ and each choice of nonnegative integers $\nu_{\ell,r}$, one has*

$$\sum_{1 \leq r < t} \operatorname{length}_{\mathbb{Z}_\ell} Z^-_{\nu_{\ell,r}}(E, r) \leq v_\ell(\mathcal{J}_{N,t}), \qquad \log \mathcal{J}_{N,t} \ll N^4 t^2 \log(2Nt) \quad (t \geq 2).$$

The integer works for all the subfields E at once. To include $r = 0$ with the convention of the second archive, multiply it by h_E, the class number of E. With a finite coefficient ring of integers $\mathcal{O}$ above ℓ, replace a length on the left by its $\mathcal{O}$-length divided by the ramification index. The coefficient ring may vary with the weight.

Proof. First suppose $\ell \mid 2g$. In particular $\ell \leq N$. The ℓ-torsion in the finite-coefficient cocycle module embeds into the space of continuous cocycles of the character $\bar{\kappa}^{-r}$ over $\mathbb{F}_\ell$, unramified outside ℓ. We bound the dimension of that space. Over $K = E(\mu_\ell)$ the action is trivial, so restriction gives homomorphisms unramified outside the places above ℓ. The kernel consists of cocycles on $\mathrm{Gal}(K/E)$. This finite group has order dividing $\ell - 1$, so those cocycles are coboundaries and span a space of dimension at most one. Kummer theory over K, which contains μ_ℓ, bounds the dimension of the homomorphisms by the dimension of the group of units of $\mathcal{O}_K[1/\ell]$ modulo ℓ-th powers plus $\log_\ell h_K$. Indeed a Kummer element has valuation divisible by ℓ away from ℓ. Sending it to the resulting ideal class gives an ℓ-torsion class in the open ring, whose class number divides h_K. The kernel consists of the indicated units modulo powers.

Put $d = [K : \mathbb{Q}] \leq N^2$. The unit contribution is at most $2d$ by the unit theorem including its roots of unity, since there are at most d places above ℓ. The conductor of K divides $N\ell$, so its absolute discriminant is at most $(N\ell)^d$ by the conductor–discriminant formula. Minkowski's bound gives each ideal class an integral representative of norm at most $B = 2^d (N\ell)^{d/2}$. The number of ideals up to that norm is at most $B^2 \zeta_K(2) \leq B^2 \zeta(2)^d$. Hence $\log_2 h_K \leq d(3 + 2\log_2 N)$. Together these estimates give dimension at most $1 + (5 + 2\log_2 N)N^2 \leq 20N^3$. A group of exponent dividing ℓ^ν with finite ℓ-torsion is finite, by induction on ν. Each successive layer has dimension at most the dimension of that torsion, by multiplication by a power of ℓ on the filtration by kernels. Applying Theorem 11.28 bounds the full length at $r = n - 1$ by $20N^3 v_\ell(J_{N,n-1})$.

Now let $\ell \nmid 2g$. By Theorem 11.24 it suffices to bound the strict eigensubgroup with eigenvalue $(-1)^n$. Restriction embeds this group into the corresponding group over F_N. It preserves all strict local conditions and commutes with c, and corestriction after restriction is multiplication by $[F_N : E]$, a unit at ℓ.

Apply the Fitting-ideal argument of Lemma 11.2 to $F_N/\mathbb{Q}$. For clarity, the set of removed primes contains infinity and all finite primes dividing N, the twist has $n \geq 2$, and ℓ is odd. The cyclotomic μ-invariant in the refined Coates–Sinnott theorem vanishes by Ferrero–Washington

for abelian fields. The dual of the indicated strict group embeds in the same sign of degree-two cohomology over $\mathcal{O}_{F_N}[1/(N\ell)]$. In the sign ring $R_n \otimes \mathbb{Z}_\ell$ its ambient module has zeroth Fitting ideal containing $W_n\Theta_n$, where the character values of Θ_n are $L(1-n,\chi^{-1})$ with the Euler factors over N removed. In fact W_n kills the degree-one torsion $H^0(F_N,\mathbb{Q}_\ell/\mathbb{Z}_\ell(n))$ by the action of Frobenius at $P_i \neq \ell$, whose residue degree divides g. A further omitted Euler factor at $\ell \nmid N$ is a unit in the ℓ-adic group ring because $n-1>0$. These are precisely the hypotheses and the Fitting membership in the cited lemma. [2, Thm. 6.11][3]

The ring $R_n \otimes \mathbb{Z}_\ell$ is a product of unramified discrete valuation rings since $\ell \nmid 2g$. On each factor the valuation of an element of the zeroth Fitting ideal bounds the length of the module. Multiplying $W_n\Theta_n$ by the integer $n(n+1)!N$, taking the component valuations with residue-degree weights and adding, gives

$$\operatorname{length}_{\mathbb{Z}_\ell} \mathcal{S}_{\ell,n-1}(F_N)^{((-1)^n)} \le v_\ell(W_n^{g/2}|d_n|).$$

Indeed the absolute determinant of $n(n+1)!N\Theta_n$ on the sign ring is $|d_n|$, by its eigenvalues as computed in Theorem 11.28. Inverting χ permutes the characters of that sign. Duality preserves $\mathbb{Z}_\ell$-length. Multiplying the integer bounds for all n proves the valuation inequality in both prime ranges.

The bound for $\log \mathcal{J}_{N,t}$ follows by summing $\log J_{N,n-1} \ll Nn\log(2Nn)$ and $\log W_n \le 2gn\log(4N)$. For comparison with an explicit size used in the second archive, one also has $\mathcal{J}_{N,t} \le 2^{4(N+t+3)^{27}}$. To see this, put $y = N+t+3$, with $t \ge 2$. In the Cauchy estimate from the preceding theorem one may take $12n!$, since $|e^z-1| \ge 3-e > 1/4$ on $|z|=1$ and $|e^{uz}|<3$ for $0 \le u \le 1$. Thus each eigenvalue has modulus at most $12N(n+1)!N^n n!$. Using $n, N \le y$ gives $\log_2|d_n| \le 5y^3$. Since $b_1 \le 3N$, $b_2 \le 5N^2$, this gives $\log_2 J_{N,n-1} \le 6y^3$, and $\log_2 W_n \le 2y^3$. It follows that $\log_2 \mathcal{J}_{N,t} \le 130y^7 \le 4y^{27}$. The empty product satisfies the same absolute bound.

At weight zero the model is the group of everywhere unramified homomorphisms into $\mathbb{Z}/\ell^\nu$, with no sign condition. It is $\operatorname{Hom}(\mathrm{Cl}(E),\mathbb{Z}/\ell^\nu)$ by class field theory for the totally imaginary field E. Its length is at most $v_\ell(h_E)$. The finite free base-change calculation of Corollary 11.26 proves the assertion for every coefficient ring, including at weight zero. □

Corollary 11.30 (The same integer on the period interval)**.** *On a polynomial-conductor interval $[V, V^{3/2}]$, let N_* be its upper-endpoint cyclotomic modulus and let $t_* = \lfloor V^{1203/2} \rfloor$. For every node x on this interval, every finite coefficient level, and all primes simultaneously, $\mathcal{J}_{N_*,t_*}$ bounds the positive-weight odd cocycle lengths as in the theorem. Its logarithm is bounded by a power of V. On the family in the shorter archive the same theorem supplies the entire odd-cocycle input, including weight zero, with the bound $2^{4(N+t+3)^{27}}h_E$. For that family's fixed q_0, d, writing $J' = h_E\mathcal{J}_{N,t}$, the particular contribution $t\,v_\ell(J')$ to the denominator estimate for the lifts satisfies*

$$\sum_\ell t\,v_\ell(J')\log\ell = t\log J' \ll_{q_0,d} x^{59}\log^5(2x).$$

Proof. In Theorem 19.15 every E_x belongs to $\mathbb{Q}(\mu_{N_*})$, since only the dyadic conductor changes and each layer is contained in the top one. The weights $1 \le r < t(x)$ are below t_*, and both N_*, t_* are polynomial in V. Apply the theorem to this single N_*, t_*.

For the second assertion the shorter construction uses $E = \mathbb{Q}(\sqrt{-d}, \mu_{q_1})$, where $d \equiv 7 \bmod 8$ is prime. The quadratic field has discriminant $-d$ and embeds in $\mathbb{Q}(\mu_d)$, so $E \subseteq \mathbb{Q}(\mu_N)$ for $N = q_1 d$. The field is totally imaginary and abelian over $\mathbb{Q}$. Complex conjugation fixes a totally real subfield of index two, so E is CM. The local conditions and coefficient sign are those specified in Section 11.8, also at the primes dividing N. Apply the theorem and multiply by h_E for the zero weight. The result works without adjoining any character values to the coefficient ring.

To compute its size, the number m of lifts lies between $\sqrt{x}$ and $2\sqrt{x}$, and the tower exponent s satisfies $2^s = m^{22}$. With l_0 the least power of three at least $27s$, the modulus satisfies $q_1 = 3q_0 l_0 2^s$. Thus $l_0 \le 81s$ and $N \ll_{q_0,d} x^{11}\log(2x)$. The weight cutoff is five times a rank of size at most $3x^5$. The class number bound in the proof of the theorem gives $\log h_E \ll N\log(2N)$ by applying the same Minkowski estimate to $E \subseteq \mathbb{Q}(\mu_N)$. Hence $\log J' \ll_{q_0,d} x^{54}\log^5(2x)$. Multiplication by $t \le 15x^5$ and prime factorization of J' prove the asserted bound for this term. □

For the shorter argument this establishes the bound on the odd cocycles used in its first-order congruence calculation. The bounds for the denominators of the projected lifts and for their periods involve further terms. For the original comparison (L), positive-weight cocycles of the other sign still occur as described in Theorem 11.24.

12 Selmer groups and marked local conditions

12.1 Dual Selmer classes and relations on tame inertia

Let E be a CM field, let $F = E^+$ be its maximal real subfield, and put $f = [F : \mathbb{Q}]$. Suppose that E/F is unramified at every finite place. We will verify this hypothesis on both families of period fields at the end of the subsection. Write $G_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ for each field in a fixed algebraic closure. Choose a complex conjugation $c \in G_F$. Let ε be the quadratic character of E/F and κ the ℓ-adic cyclotomic character, for a prime ℓ. The character $\kappa_+ = \kappa\varepsilon$ equals κ on G_E and equals 1 at every real conjugation of F.

Fix an exponent $e \geq 1$ and a coefficient precision $\nu \geq 1$. Put $R_n = \mathbb{Z}/\ell^n\mathbb{Z}$ for $1 \leq n \leq \nu$. Use the two rank-one modules

$$A_n = R_n(\kappa_+^{-e}), \qquad B_n = \mathrm{Hom}(A_n, \mu_{\ell^n}) \simeq R_n(\kappa\kappa_+^e).$$

In this notation $R_n(\chi)$ is the additive group of R_n on which g acts by multiplication by $\chi(g)$. Choose compatible primitive roots ζ_{ℓ^n} for the displayed identifications. The duality pairing in the two coordinates sends (a, b) to $\zeta_{\ell^n}^{ab}$. At level zero use the zero modules. Let X be a finite set of primes of F away from ℓ splitting completely in $E(\mu_{\ell^\nu})/F$. We keep this same X through all the levels $n \leq \nu$.

At a real place or a prime in X prescribe $L_{n,v} = 0$ in $H^1(F_v, A_n)$. At each other prime $v \nmid \ell$ prescribe unramified cohomology, the kernel of restriction to inertia. For $v \mid \ell$ write $\Gamma_v = \kappa_+(G_{F_v})$, using the full ℓ-adic image at every level. Except in the following dyadic case, take for $L_{n,v}$ the inflation of $H^1(\Gamma_v, A_n)$. If $\ell = 2$ and $-1 \in \Gamma_v$, prescribe

$$L_{n,v} = \begin{cases} \inf H^1(\Gamma_v/\{1,-1\}, A_n), & e \text{ even}, \\ 0, & e \text{ odd}. \end{cases}$$

The quotient acts on A_n in the first line. These subgroups define $S_n \subset H^1(F, A_n)$ by inverse image under localization. Define $D_n \subset H^1(F, B_n)$ in the same way using $L_{n,v}^\perp$ for the local Tate pairing at each place. Write $S_0 = D_0 = 0$.

Lemma 12.1 (Change of coefficient level)**.** *Reduction from n to $n-1$ maps $L_{n,v}$ onto $L_{n-1,v}$ at every place. Multiplication by ℓ from A_{n-1} to A_n maps $L_{n-1,v}$ into $L_{n,v}$. At $v \mid \ell$ and $n \geq 1$ one has*

$$\frac{|L_{n,v}|}{|H^0(F_v, A_n)|} = \begin{cases} 1/2, & \ell = 2,\ -1 \in \Gamma_v,\ e \text{ odd}, \\ 1, & \text{otherwise}. \end{cases}$$

Proof. Each Γ_v is open in $\mathbb{Z}_\ell^\times$. Indeed, on the absolute Galois group of the finite local extension E_w of $\mathbb{Q}_\ell$ the character is κ, whose image has finite index in $\mathbb{Z}_\ell^\times$. For odd ℓ an open subgroup of $\mathbb{Z}_\ell^\times$ is a product of a finite group Δ of order dividing $\ell - 1$ and a copy of $\mathbb{Z}_\ell$. This follows from the decomposition into roots of unity and principal units, whose finite quotients have coprime orders. Inflation is injective. Averaging over Δ identifies $H^1(\Gamma_v, A_n)$ with $A_n^\Delta/(\gamma - 1)A_n^\Delta$, for a generator γ of the pro-ℓ factor. Here the usual procyclic formula follows by evaluating a cocycle at the generator. Every value is allowed because the action factors through a finite quotient and the coefficient group is finite of ℓ-power order. Averaging makes reduction on the invariants surjective. Since the kernel and cokernel of an endomorphism of a finite group have the same order, the displayed quotient has order $|A_n^{\Gamma_v}|$.

For $\ell = 2$, the only possible nontrivial torsion subgroup of Γ_v is $\{1, -1\}$, and the quotient by its torsion is isomorphic to $\mathbb{Z}_2$. Indeed, $\mathbb{Z}_2^\times$ is the product of $\{1, -1\}$ and $1 + 4\mathbb{Z}_2 \simeq \mathbb{Z}_2$.

With trivial torsion, or with nontrivial torsion and e even, the same procyclic calculation gives surjectivity and the claimed ratio. For e odd and $-1 \in \Gamma_v$, the local condition is zero. The fixed subgroup of A_n is exactly $A_n[2]$ since -1 acts by -1 and every 2-adic unit fixes $A_n[2]$.

At a finite prime outside X away from ℓ, both ε and κ are unramified. Hence the unramified group is $A_n/(\mathrm{Frob}_v - 1)A_n$, which again reduces surjectively and has order $|H^0(F_v, A_n)|$. At places with zero condition the reduction assertion is immediate. In every case the map from A_{n-1} given by multiplication by ℓ respects the prescribed inflation or zero subgroup. □

Theorem 12.2 (Independent dual classes through every precision)**.** *Put $U = G_{E(\mu_{\ell^\nu})}$. Every $y \in D_\nu$ restricts to a homomorphism $\psi_y : U \longrightarrow R_\nu$ which is independent of the cocycle representative. Let W be the space of their reductions in $\mathrm{Hom}_{\mathrm{cont}}(U, \mathbb{F}_\ell)$. Then*

$$\dim_{\mathbb{F}_\ell} W \;\geq\; \begin{cases} f + |X| - 1, & \ell \text{ odd}, \\ f + |X| - 3, & \ell = 2,\ \mu_4 \subset E, \\ f + |X| - 4, & \ell = 2 \text{ in general}. \end{cases}$$

Each y is unramified at every finite prime outside X and the primes above ℓ. For $a \in G_F$ and $h \in U$ the homomorphism satisfies $\psi_y(aha^{-1}) = (\kappa\kappa_+^e)(a)\psi_y(h)$ in R_ν.

Proof. Use logarithms to base ℓ for the four orders $s_n = \log_\ell |S_n|$, $d_n = \log_\ell |D_n|$, $a_n = \log_\ell |H^0(F, A_n)|$ and $b_n = \log_\ell |H^0(F, B_n)|$. Let k count the places in the first line of the ratio in Lemma 12.1. Put $k_0 = 0$ and $k_n = k$ for $n \geq 1$. For finite dual Galois modules, the Greenberg–Wiles formula gives finiteness and the identity

$$\frac{|S_n|}{|D_n|} = \frac{|H^0(F, A_n)|}{|H^0(F, B_n)|} \prod_v \frac{|L_{n,v}|}{|H^0(F_v, A_n)|}.$$

It applies to continuous cohomology over any number field, with orthogonal conditions for the local cup pairing and the unramified condition at almost all primes. Its displayed factors at real places use ordinary invariants, also at $\ell = 2$. At each real place $\kappa_+ = 1$ on the local group, and at each $v \in X$ both characters are trivial modulo ℓ^ν. These places each contribute ℓ^{-n}. At all remaining places the factors were computed in the lemma. It follows, including at level zero, that

$$d_n - s_n = n(f + |X|) + b_n - a_n + k_n.$$

The formula and the duality conventions used here are those of Darmon, Diamond and Taylor. [14]

The exact coefficient sequence from A_{n-1} to A_n to A_1, with maps multiplication by ℓ and reduction, shows that the kernel of $H^1(F, A_{n-1}) \longrightarrow H^1(F, A_n)$ has order $\ell^{a_1 - a_n + a_{n-1}}$. Indeed, the connecting map has domain $H^0(F, A_1)$ and its kernel is the reduction of $H^0(F, A_n)$, of order $\ell^{a_n - a_{n-1}}$. The lemma maps S_{n-1} into S_n, so $s_n - s_{n-1} \geq -a_1 + a_n - a_{n-1}$. Also $b_n \geq b_{n-1}$ by the injection $B_{n-1} \hookrightarrow B_n$. Subtracting the two cardinality identities gives

$$d_n - d_{n-1} \geq f + |X| - a_1 \geq f + |X| - 1.$$

We need to count classes which survive reduction all the way to B_1. The preimage of D_n under $H^1(F, B_{n-1}) \to H^1(F, B_n)$ is exactly D_{n-1}. Indeed, multiplication by ℓ on the dual coefficients is adjoint under local cup products to reduction $A_n \to A_{n-1}$, and the latter maps every primary local condition onto the preceding one. Therefore the kernel of $D_n \to H^1(F, B_1)$ is the image of D_{n-1}, by the exact sequence for B_{n-1}, B_n, B_1. The image in $H^1(F, B_1)$ has dimension at least $d_n - d_{n-1}$. This argument keeps the classes at their full precision before reducing them.

Finally, U is normal in G_F and acts trivially on B_ν, so restriction kills coboundaries and gives the homomorphisms in the statement. Expanding the cocycle at aha^{-1} proves their equivariance. For $n = \nu$, the kernel of restriction on $H^1(F, B_1)$ is inflated from $H^1(H, B_1)$, where $H = \mathrm{Gal}(E(\mu_{\ell^\nu})/F)$. This group H is abelian, being a subgroup of the product of the quadratic group and the cyclotomic group. For odd ℓ, complex conjugation in H acts by -1 on B_1. If u is a cocycle on H, evaluating it at $cg = gc$ gives $-2u(g) = (g-1)u(c)$. Division by -2 exhibits a coboundary, so restriction loses no dimension.

At two the residual module is trivial, and H embeds by $(\varepsilon, \kappa \bmod 2^\nu)$ in a product of at most three cyclic 2-groups. Any subgroup of such a product is generated by at most three elements, by induction using projection to one cyclic factor and its kernel. This bounds the dimension of $H^1(H, B_1)$ by three. If $\mu_4 \subset E$, then $E = F(i)$. Consequently $\kappa_+(G_F) \subset 1 + 4\mathbb{Z}_2$, since its sign correction is precisely the action on i. The equally faithful pair $(\varepsilon, \kappa_+ \bmod 2^\nu)$ now takes values in a product of at most two cyclic groups. This proves the sharper dyadic assertion.

Outside X and ℓ the unramified local groups for the two unramified modules are exact annihilators. Their cup product vanishes because it inflates from the procyclic unramified quotient, of ℓ-cohomological dimension one. Their orders are the respective invariant orders as in the lemma. For a local field of residual characteristic different from ℓ, the local Euler characteristic formula and local Tate duality give $|H^1(F_v, B_n)| = |H^0(F_v, B_n)|\,|H^0(F_v, A_n)|$. The two unramified groups therefore have the full orders required by orthogonality. This proves the ramification assertion. [1] □

Proposition 12.3 (Reciprocity on the chosen tame generators)**.** *Let Q be another finite set of primes of F, disjoint from X and from ℓ, splitting completely in $E(\mu_{\ell^\nu})/F$. Fix a prolongation of every prime in $X \cup Q$, so that its decomposition group lies in U. At $v \in Q$ take a uniformizer π_v, a lift ϕ_v of arithmetic Frobenius, and a tame inertia element τ_v sending a chosen ℓ^ν-th root of π_v to ζ_{ℓ^ν} times that root.*

Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_\ell$. Let z be a continuous cocycle of G_E with coefficients in $(\mathcal{O}/\ell^\nu\mathcal{O})(\kappa^{-e})$. Suppose $z(cgc^{-1}) = z(g)$, that z is unramified outside ℓ and the primes above Q, and that z vanishes on $\ker\kappa$ in the decomposition groups above ℓ. At each chosen prime over X, assume z vanishes on a Frobenius lift. For every $y \in D_\nu$ one then has

$$\sum_{v \in Q} M\, z(\tau_v)\, \psi_y(\phi_v) = 0 \quad \text{in } \mathcal{O}/\ell^\nu\mathcal{O}.$$

One may take $M = 2$ if ℓ is odd or if every Γ_v for $v \mid 2$ is torsion-free at $\ell = 2$. In all other dyadic cases one may take $M = 4$.

Proof. First take $\mathcal{O} = \mathbb{Z}_\ell$ and put $m = \ell^\nu$. Since $G_F = G_E \rtimes \langle c \rangle$, the formula $\widetilde{z}(gc^j) = z(g)$ for $g \in G_E$, $j = 0, 1$, defines a cocycle for A_ν. Indeed, multiplication conjugates the second G_E-component by c^j, which leaves its z-value unchanged, and $\kappa_+(c) = 1$. At any real conjugation c', its square is 1 and it acts trivially on A_ν. Hence $2\widetilde{z}(c') = 0$. For g in a decomposition group at ℓ with $\kappa_+(g) = 1$, one has $g^2 \in G_E$, $\kappa(g^2) = 1$, and $2\widetilde{z}(g) = z(g^2) = 0$ by the local hypothesis. It follows that $2\widetilde{z}$ descends locally to a cocycle on Γ_v.

At a dyadic place with $-1 \in \Gamma_v$, denote this last cocycle by x. For e even, the torsion involution acts trivially, so $2x$ vanishes on it and descends to the quotient. For e odd, put $t = -1 \in \Gamma_v$. Evaluating at $tg = gt$ gives $2x(g) = (g-1)(-x(t))$, so $2x$ is a coboundary. These are precisely the two exceptional local conditions. Away from ℓ the inertia of F lies in G_E, since E/F is unramified at finite places. Thus $M\widetilde{z}$ satisfies all the primary local conditions outside Q, including at X, where both inertia and a Frobenius lift have zero value.

The global cup product of $M\widetilde{z}$ with y has sum of local invariants zero by the Brauer reciprocity law. Outside Q each invariant is already zero by orthogonality. At $v \in Q$ both modules are locally trivial and y is unramified by Theorem 12.2. Identify μ_m with R_ν using the fixed ζ_m. The Kummer character of π_v takes the value 1 at τ_v. Subtracting $z(\tau_v)$ times that character from z gives an unramified local character. Indeed, wild inertia has no ℓ-quotient, and the maximal exponent-m abelian ℓ-quotient of tame inertia is cyclic of order m, generated by the image of τ_v. The unramified part pairs to zero with y. Local reciprocity pairs the Kummer class of π_v with an unramified character by evaluating that character at arithmetic Frobenius. In the invariant group $\mathbb{Q}/\mathbb{Z}$ this is $\psi_y(\phi_v)/m$, up to the common sign from the ordering of the two cup factors. Thus the sum of the remaining invariants gives the asserted identity in R_ν. The sum is taken over F, so there is one term for each v, with the chosen prolongation fixing both local coordinates. [1]

Finally $\mathcal{O}$ is finite free over $\mathbb{Z}_\ell$. Each coordinate of z in a $\mathbb{Z}_\ell$-basis is an R_ν-valued cocycle satisfying the same hypotheses because the action is scalar. Applying the identity to each coordinate proves it over $\mathcal{O}/\ell^\nu\mathcal{O}$. □

Corollary 12.4 (Dual classes on the fields of the period intervals)**.** *At every node of every sufficiently distant interval of Theorem 19.15, and on each field used in the shorter construction of Corollary 11.30, one has* $\dim W > |X|$*. This holds for every positive weight, every prime and every precision. On the shorter family the reciprocity identity always holds with* $M = 2$*, and on the original intervals it holds with* $M \le 4$*.*

Proof. On the original intervals $E = K_\psi C_J(\sqrt{-q}, \sqrt{-d_0})$ is abelian over $\mathbb{Q}$ and contains two imaginary quadratic fields of coprime discriminants $-q$ and $-d_0$. At any rational prime at least one of these fields is unramified. Inertia in $\mathrm{Gal}(E/\mathbb{Q})$ fixes that field, while complex conjugation acts nontrivially on it. Relative inertia for E/F is the intersection with the subgroup generated by complex conjugation. It is therefore trivial. Moreover F contains the real cyclotomic layer C_J of degree 2^J. The lower bound for $[K_\psi C_J : \mathbb{Q}]$ in Theorem 19.15 and the fixed degree of K_ψ imply $2^J \ge 8$ at every node as soon as V is sufficiently large. Hence even the weakest dimension bound in Theorem 12.2 exceeds $|X|$ on the whole interval.

On the shorter family $E = \mathbb{Q}(\sqrt{-d}, \mu_{q_1})$, the integer d is a prime congruent to 7 mod 8, and $5040 \mid q_1$. For the latter divisibility, $18480 \mid q_0$ and q_1 is a multiple of $3q_0$, with $5040 \mid 3 \cdot 18480$. Here the two imaginary quadratic discriminants -4 and $-d$ are coprime, giving the same unramified conclusion. The inclusion $\mu_{16} \subset E$ gives $f \ge 4$. Since $\mu_4 \subset E$, each dyadic Γ_v lies in the torsion-free group $1 + 4\mathbb{Z}_2$. The sharper bounds in the theorem and proposition apply at every node of this family. □

For example, suppose $k \le |X|$ homomorphisms $U \to R_\nu$ have already been chosen with linearly independent reductions. The corollary gives a dual class whose restriction has reduction outside their span. The resulting $k+1$ homomorphisms together map U onto R_ν^{k+1}. Indeed their image H' surjects onto the reduction of this module, since a proper subspace over $\mathbb{F}_\ell$ has a nonzero annihilating linear form. It follows that R_ν^{k+1}/H' equals its own multiple by ℓ, and iteration ν times gives zero. In particular there is a single element on which the previous homomorphisms vanish at full precision and the new one takes value 1.

The dimension bound counts available relations. To deduce the integral estimate of Section 6.6, one still has to control their evaluations at the primes used in the projection and compare the resulting denominators with the actual theta periods on the same interval.

12.2 Auxiliary primes for the tame values of even cocycles

Keep E, F, ℓ, c, κ as in Corollary 12.4. Fix $t \geq 2$ and $\gamma \in G_E$ such that $u = \kappa(\gamma)$ has infinite order. For $0 \leq e < t$ define the nonzero ℓ-adic integer

$$\Delta_e = \prod_{\substack{0 \leq d < t \\ d \neq e}} (u^e - u^d).$$

Fix $\nu \geq 1$, put $m = \ell^\nu$, $R = \mathbb{Z}/m\mathbb{Z}$, and write $U = G_{E(\mu_m)}$. The word *even* for a cocycle z of weight e means that the action on its coefficients is κ^{-e}, that $z(chc^{-1}) = z(h)$, and that z vanishes on $\ker \kappa$ in all decomposition groups at ℓ. Any finite ramification permitted away from ℓ will be specified separately. We use the multiplier M of Proposition 12.3, so $M = 2$ on the shorter family and $M \leq 4$ on the original period intervals.

Lemma 12.5 (Separation of the weights)**.** *Suppose given continuous homomorphisms $\psi_i : U \to R$ with weights $0 < e_i < t$, satisfying*

$$\psi_i(\gamma h \gamma^{-1}) = u^{e_i+1}\psi_i(h), \qquad \psi_i(chc^{-1}) = -\psi_i(h).$$

Let $\psi : U \to R$ satisfy the same identities with weight e. Suppose the reductions of ψ and of all ψ_i with $e_i = e$ are linearly independent over $\mathbb{F}_\ell$. For each $s \in G_E$ with $\kappa(s) = 1$ there is $g \in U$ such that

$$\psi_i(g) = 0 \quad \text{for all } i, \qquad \psi(g) = 2\Delta_e, \qquad z(g) = 2z(s)$$

for every even cocycle z of weight e with coefficients in $(\mathcal{O}/m\mathcal{O})(\kappa^{-e})$, where $\mathcal{O}$ is any ring of integers finite over $\mathbb{Z}_\ell$. All three identities persist if g is replaced by $\delta^m g$ for any $\delta \in G_E$ with $\kappa(\delta) = 1$.

Proof. The homomorphisms of weight e, including the new one, jointly map U onto the corresponding product of copies of R. Their reductions are independent, so the image is surjective after reduction. The quotient of R^k by that image is then equal to its own multiple by ℓ and hence is zero. Choose $h \in U$ on which the old maps of weight e vanish and the new map takes the value 1.

For each $0 \leq d < t$, $d \neq e$, replace the current h by

$$(\gamma h \gamma^{-1})^a h^b, \qquad a \equiv u^{-1} \pmod m, \quad b \equiv -u^d \pmod m.$$

Take ordinary integer representatives for the exponents. The element stays in U. Its value under a map of weight k is multiplied by $u^k - u^d$. Thus after all replacements the result h' is killed by every old map, and $\psi(h') = \Delta_e$. Set

$$g = s(csc^{-1})h'(ch'c^{-1})^{-1}.$$

The four factors lie in U, on which all the maps are additive. The two terms involving s cancel for the dual maps and add for z. The two terms involving h' add for the dual maps and cancel for z. This proves the formulas. For the last assertion, $\delta \in U$, hence m times its value vanishes under each of the homomorphisms in question, including $z|_U$. □

Theorem 12.6 (A triangular bound at distinct auxiliary primes)**.** *Fix any finite ordered list $(e_j, s_j)_{1 \leq j \leq b}$, with $0 < e_j < t$ and $s_j \in \ker(\kappa|_{G_E})$. There exist primes w_j of E of rational prime norm, with chosen arithmetic Frobenius lifts ϕ_j and normalized tame generators τ_j as in Proposition 12.3. Their underlying rational primes may be chosen pairwise distinct and outside any given finite set. The primes v_j of F below them split completely in $E(\mu_m)/F$, so $Nw_j \equiv 1 \bmod m$. They have these two properties.*

First, every even cocycle of weight e_j unramified outside ℓ satisfies $z(\phi_j) = 2z(s_j)$. Second, allow an even cocycle of weight e_j to ramify at all primes of E over the v_i, as well as at ℓ. If

$$z(\tau_i) = 0 \quad (i < j), \qquad z(\phi_i) = 0 \quad (i < j,\ e_i = e_j),$$

then $2M\Delta_{e_j} z(\tau_j) = 0$. Both assertions hold with the same primes for all coefficient rings $\mathcal{O}/m\mathcal{O}$. In particular the exponent $v_\ell(2M\Delta_{e_j})$ in this bound is independent of ν.

The primes may also obey an additional condition on the pair (w_j, ϕ_j) under the following hypothesis. For every $g \in U$, there is $\delta \in \ker(\kappa|_{G_E})$ such that every open neighborhood of $\delta^m g$ contains Frobenius lifts satisfying the condition at infinitely many degree-one primes of E.

Proof. Choose the primes and dual maps successively. At index j put $e = e_j$ and $X = \{v_i : i < j,\ e_i = e\}$. By Corollary 12.4 the space of residual restrictions of the dual classes at this e, X, ν has dimension greater than $|X|$. Choose a class y_j whose restriction ψ_j is independent modulo ℓ of all the earlier maps of weight e. This also preserves the independence required at the next occurrence of that weight. By Theorem 12.2, y_j is unramified away from X and ℓ, and every map so obtained has the two equivariances of Lemma 12.5. That lemma gives $g \in U$ which kills all the earlier maps, takes the value $2\Delta_e$ under the new one, and has the required evaluations for the even cocycles at s_j.

These equalities are open conditions when imposed on the Frobenius for all the even cocycles unramified outside ℓ. To see this, first use coefficients R. A cocycle gives a continuous homomorphism into the finite affine group $R \rtimes R^\times$ by adjoining its scalar action. Its kernel fixes a Galois extension of bounded degree unramified outside ℓ. There are finitely many such extensions by Hermite–Minkowski finiteness for bounded degree and a fixed ramification set. In this form, finiteness follows by bounding the local discriminants at the permitted primes, where a nonarchimedean local field has finitely many extensions of bounded degree, and then applying the discriminant form of Hermite–Minkowski. Each resulting finite Galois group has finitely many maps to the affine group. This proves finiteness of the cocycles themselves. All their evaluations, together with the finitely many ψ_i and the condition of lying in U, are therefore constant on an open neighborhood of g. For a general coefficient ring take coordinates in a $\mathbb{Z}_\ell$-basis of $\mathcal{O}$. Each coordinate is one of the R-valued cocycles already considered. If the additional condition is imposed, use the same argument around $\delta^m g$, which has the identical prescribed evaluations.

For the unrestricted choice, take a coset of an open normal subgroup of G_E inside the neighborhood of g. The finite Chebotarev theorem gives positive Dirichlet density for the primes with that Frobenius conjugacy class, and a choice of prolongation realizes the chosen representative. The contribution of primes of E of residue degree at least two is bounded as the real variable σ tends to 1 from above, by $[E : \mathbb{Q}] \sum_p p^{-2\sigma}$. Thus there are infinitely many degree-one choices. In the restricted case use the stated neighborhood hypothesis. In either case exclude the rational primes below the previous choices, the given exceptional primes, the divisors of m, and the rational primes ramified in $E(\mu_m)/\mathbb{Q}$. Degree one in E implies residue degree one in E/F, so the prime below w_j splits in that quadratic extension. Its Frobenius also fixes μ_m by the choice of neighborhood. This proves the full splitting assertion. Use the chosen prolongation for τ_j and for ϕ_j. This completes the induction. [15, Theorem 8.31]

For the second assertion, z is unramified at every earlier v_i in the following sense. At the chosen w_i the action is trivial on inertia. Wild inertia has order prime to ℓ in each finite quotient, and the pro-ℓ part of tame inertia is procyclic. Hence $z(\tau_i) = 0$ makes the inertia value zero at w_i. At its conjugate the value also vanishes by evenness. Changing a prolongation preserves vanishing, by the cocycle identity and the trivial action of inertia on the coefficients. The same identity on the whole decomposition group at a split v_i justifies using the Frobenius

lift chosen above. Thus the assumptions give exactly the conditions at X of Proposition 12.3. Apply that proposition to y_j and $Q = \{v_i : i \geq j\}$. All terms with $i > j$ vanish since $\psi_j(\phi_i) = 0$ by construction. The term at j is $2M\Delta_{e_j} z(\tau_j)$, as claimed. □

Corollary 12.7 (A unit determinant at the same primes)**.** *Let $T : G_E \to \mathrm{GL}_r(\mathcal{O}')$ be a continuous representation, where $\mathcal{O}'$ is the ring of integers of a finite extension of $\mathbb{Q}_\ell$. Suppose some element $\eta \in \ker \kappa$ acts modulo the maximal ideal as a scalar α of order greater than r. Then every prime in the theorem can also satisfy* $\det(1 - T(\phi_j)) \in (\mathcal{O}')^\times$.

Proof. For given $g \in U$, the $r+1$ elements $(\eta^a)^m g$, $0 \leq a \leq r$, have residual matrices $\alpha^{am}\overline{T}(g)$. The scalars are distinct because the order of α is prime to ℓ. The polynomial $\det(1 - X\overline{T}(g))$ has constant term 1 and degree at most r, so at some such scalar its value is nonzero. Set $\delta = \eta^a$. Continuity makes the determinant a unit on an open neighborhood of $\delta^m g$. Intersecting with any prescribed smaller neighborhood and applying the same finite Chebotarev argument proves the additional-condition hypothesis. □

The auxiliary primes here are chosen anew at each precision. The annihilator $2M\Delta_e$ is fixed before that choice. A bound on the total loss also requires controlling the size of a family of points s_j that detects all relevant cocycles.

12.3 The cost of the auxiliary primes on a period interval

Let E be one of the period fields in Corollary 12.4 and suppose $E \subseteq \mathbb{Q}(\mu_N)$. Fix an integer $t \geq 2$. Theorem 12.6 allows us to choose one auxiliary prime for each pair consisting of a positive weight less than t and a test point. We now bound how many tests are needed and how the resulting loss varies with ℓ.

For odd ℓ let $K = E(\mu_\ell)$, and choose $\gamma \in G_E$ whose cyclotomic image $u = \kappa(\gamma)$ generates $C = \kappa(G_E)$ topologically. This is possible since C is open in $\mathbb{Z}_\ell^\times$ and is the product of a cyclic group of order prime to ℓ and a copy of $\mathbb{Z}_\ell$, which together are procyclic. At two take $K = E(i)$ and take $\gamma \in G_K$ with u generating $C \cap (1 + 4\mathbb{Z}_2)$, the full cyclotomic image of G_K. This is an open subgroup of $1 + 4\mathbb{Z}_2$. In particular γ generates the whole cyclotomic image at two in the shorter construction.

Lemma 12.8 (Test points independent of precision and weight)**.** *There is a finite set $S_\ell \subseteq \ker(\kappa|_{G_E})$ of size at most $2[K : \mathbb{Q}] + \log_\ell h_K$, where h_K is the ordinary class number. For any weight $e \geq 0$, precision $\nu \geq 1$, and finite coefficient ring of integers $\mathcal{O}$ above ℓ, let z be a cocycle in $(\mathcal{O}/\ell^\nu\mathcal{O})(\kappa^{-e})$ unramified outside ℓ. If $z(\gamma) = 0$ and z vanishes on S_ℓ, then $z = 0$ when ℓ is odd or $i \in E$. In the other dyadic case these vanishing conditions imply $z|_{G_K} = 0$ and $(u^{-e} - 1)z = 0$. Testing also one representative of the nonidentity coset in G_E/G_K then detects z exactly.*

Proof. Let P_K be the Galois group of the maximal pro-ℓ extension of K unramified outside the primes over ℓ. The space of continuous homomorphisms $P_K \to \mathbb{F}_\ell$ has dimension at most $2[K : \mathbb{Q}] + \log_\ell h_K$. Indeed, K contains μ_ℓ, so Kummer theory identifies this space with a subgroup of $K^\times/K^{\times\ell}$. Away from ℓ a representing element has valuation a multiple of ℓ, because an unramified extension has integral value group. Sending the prime-to-ℓ divisor divided by ℓ to the class group of $\mathcal{O}_K[1/\ell]$ gives an ℓ-torsion class. The kernel is represented by units of $\mathcal{O}_K[1/\ell]$. Indeed, a principal divisor at this stage can be removed by an ℓ-th power. The unit theorem, including its roots of unity, bounds the unit dimension modulo ℓ-th powers by $2[K : \mathbb{Q}]$. The open ring class group is a quotient of the ordinary class group, giving the remaining term.

Choose elements $t_1, \ldots, t_d$ in G_K whose images in the maximal elementary abelian quotient of P_K form a basis. Their images generate P_K topologically. For otherwise the closed subgroup they generate would have proper image in some finite ℓ-group quotient, hence lie there in a maximal subgroup of index ℓ. The quotient character would contradict the basis property. For each i choose $h_i \in \overline{\langle\gamma\rangle}$ with $\kappa(h_i) = \kappa(t_i)$. The closed subgroup generated by γ maps onto the closed subgroup generated by u by compactness, and this includes $\kappa(G_K)$ in every case. Take $S_\ell = \{t_i h_i^{-1} : 1 \leq i \leq d\}$.

A cocycle zero at γ is zero on its closed cyclic subgroup by the cocycle identity and continuity. Hence the tests imply $z(t_i) = 0$ for each i. Over K the homomorphism

$$g \longmapsto \left(z(g),\, \kappa(g)^{-e} \bmod \ell^\nu\right)$$

into the group of affine transformations has ℓ-group image. Its translations have ℓ-power order and its linear parts are principal units modulo ℓ^ν. The homomorphism is unramified off ℓ, so it factors through P_K. The images of all the t_i fix zero. They generate the image, whence $z|_{G_K} = 0$. For odd ℓ the quotient $\mathrm{Gal}(K/E)$ is generated by the image of γ. For $\ell = 2$ and $i \in E$ the quotient is trivial. This proves exact detection in both cases. In the remaining case K/E is quadratic. For $a \in G_K,\ g \in G_E$, evaluation at $ag = g(g^{-1}ag)$ gives $\kappa(a)^{-e}z(g) = z(g)$. Take $a = \gamma$. The cocycle identity gives the last assertion on testing one more coset. □

Theorem 12.9 (One integral bound for the tame tests on an interval)**.** *For each ℓ use the above choice of u and put*

$$h_\ell = \max_{1\le a<t} v_\ell(u^a-1), \qquad b_\ell = (t+2)h_\ell, \qquad c_\ell = (2+t|S_\ell|)\, b_\ell.$$

Here $v_\ell(\ell)=1$. In Theorem 12.6 take one prime for every pair (e,s) with $0<e<t$, $s\in S_\ell$, in increasing order of weight and any fixed order within a weight. The resulting exponent needed at each tame generator is at most b_ℓ. For all $0\le e<t$ and all $1\le a<t$, respectively, the following divisibilities hold in $\mathbb{Z}_\ell$, as follows.

$$\Delta_e \mid \ell^{b_\ell}, \qquad 4(u^a-1)^2 \mid \ell^{b_\ell}.$$

The primes may vary with ν while the test points and all the displayed bounds are fixed. If Y is any integer with $N+t<Y$, then $c_\ell \le Y^6 h_\ell$, and $h_\ell = 0$ for $\ell > \max(N,t)$.

In particular suppose a common interval has $E\subseteq\mathbb{Q}(\mu_{N_*})$ and $2\le t\le t_*$ throughout. Put $Y_* = N_* + t_* + 1$, $g_* = \varphi(N_*)$, and choose primes $N_* < P_1 < 2N_* < P_2 < 4N_*$ for $N_*\ge 3$. The positive integer

$$H_* = \prod_{a=1}^{t_*-1} (P_1^{2g_*a}-1)(P_2^{2g_*a}-1)$$

satisfies, at every node,

$$c_\ell \le Y_*^6 v_\ell(H_*), \qquad \sum_\ell c_\ell \log\ell \le Y_*^6 \log H_* \ll Y_*^6 N_* t_*^2 \log(4N_*).$$

Proof. Each difference u^e-u^d, $d\ne e$, is a unit times $u^{|e-d|}-1$, up to sign. Thus every product Δ_e has valuation at most $(t-1)h_\ell$. At odd primes $2M$ is a unit. At two we chose $u\in 1+4\mathbb{Z}_2$, so $h_2\ge 2$ and $v_2(2M)\le 3\le 2h_2$. Consequently $v_\ell(2M\Delta_e)\le b_\ell$, and $v_\ell(4(u^a-1)^2)\le 3h_\ell\le b_\ell$. This proves both divisibilities and the tame bound. There are $(t-1)|S_\ell|$ primes and $|S_\ell|$ kernel test points. The additional two units in $2+t|S_\ell|$ allow for testing γ and the extra coset when it occurs. If $\ell=2$ and that extra coset is omitted, the remaining positive-weight cocycle is killed by ℓ^{h_2}, by Lemma 12.8.

For $\ell>\max(N,t)$, the cyclotomic ℓ-power fields are disjoint from $\mathbb{Q}(\mu_N)$. At every finite level this follows from the Chinese remainder isomorphism of Galois groups at the relatively prime moduli. Thus u mod ℓ generates $\mathbb{F}_\ell^\times$, of order $\ell-1\ge t$. All the factors u^a-1 are units. For the remaining primes the field K lies in a cyclotomic field of modulus $L\le Y^2$, using the modulus $N\ell$ at odd primes and $4N$ at two. Also $d=[K:\mathbb{Q}]\le Y^2$, by the degree bound for this cyclotomic field. The absolute discriminant of K is at most L^d, by the cyclotomic discriminant formula and the relative discriminant formula in a tower. Minkowski's bound gives an integral representative of each ideal class of norm at most $B=2^dL^{d/2}$. Counting ideals by their inverse squared norm bounds their number up to B by $B^2\zeta_K(2)\le B^2\zeta(2)^d$. Therefore $\log_2 h_K\le d(3+2\log_2 Y)$, and the lemma gives $|S_\ell|\le(5+2\log_2 Y)Y^2\le Y^4$ in this prime range. Since $t+2\le Y$ and $2+tY^4\le Y^5$, the cost bound follows. When $h_\ell=0$ the cost is already zero.

To get a single integer at all nodes, the index of $\kappa(G_E)$ in $\mathbb{Z}_\ell^\times$ divides $[E:\mathbb{Q}]$, and this degree divides g_*. The first divisibility follows by taking the preimage of $\kappa(G_E)$ in $G_\mathbb{Q}$ and using the index formula and surjectivity of $\kappa|_{G_\mathbb{Q}}$. For P one of P_1,P_2 different from ℓ, it follows that P^{2g_*} is a limit of powers of u. At two its square exponent also guarantees $P^{2g_*}\equiv 1 \bmod 4$, so it belongs to the group generated by our chosen u there as well. For integer powers u^j, including negative powers, u^a-1 divides $u^{aj}-1$. The principal ideal it generates is closed in $\mathbb{Z}_\ell$. Passing to the limit gives $u^a-1\mid P^{2g_*a}-1$. The primes P_1,P_2 exist by Bertrand's postulate. Taking

valuations proves $h_\ell \le v_\ell(H_*)$, and prime factorization gives the sum bound. The asserted estimate on its logarithm follows by summing $4g_* a \log(4N_*)$ over $a < t_*$. □

Corollary 12.10 (Comparison with the two actual level groups)**.** *On the shorter family, write r for the prescribed rank, $t_0 = 5r$, and p_0, p_1 for its two level primes. At a node put $N = q_1 d$, $f = [E^+ : \mathbb{Q}]$ and*

$$G_0 = \prod_{i=0}^{1} |\mathrm{GL}_{rt_0}(\mathbb{F}_{p_i})|^f.$$

For each $2 \le t \le t_0$ and integer $Y > N + t$, all the tame tests above have $c_\ell \le Y^6 v_\ell(G_0)$. In particular their total weighted cost is at most

$$Y^6 \log G_0 \le Y^6 f (rt_0)^2 \log(p_0 p_1).$$

The detection in Lemma 12.8 is exact at every coefficient prime of this family.

Proof. At a chosen place over $p_i \neq \ell$, arithmetic Frobenius has cyclotomic value p_i, because p_i splits completely in E by Section 130.1. Here u generates the whole cyclotomic image, including at two because $\sqrt{-1}$ belongs to E. Hence $u^a - 1$ divides $p_i^a - 1$ by the closed-ideal argument just used. Counting ordered bases gives

$$|\mathrm{GL}_d(\mathbb{F}_p)| = p^{d(d-1)/2} \prod_{a=1}^{d} (p^a - 1) \le p^{d^2}.$$

For $1 \le a < t \le t_0$, the factor at that a occurs in the group of dimension rt_0. The two level primes are distinct, so there is always a choice different from ℓ. This proves $h_\ell \le v_\ell(G_0)$ and both estimates. □

On the original intervals, Theorem 19.15 and Corollary 11.30 provide the single modulus N_* and weight cutoff t_*, polynomial in V, that the theorem requires. On the shorter family $q_1 = 3q_0 l_0 2^s$, where l_0 is the least power of three at least $27s$. For fixed q_0, d these moduli divide the modulus taken at the largest s on the interval. The bounds on N and t in Corollary 11.30 are polynomial there as well. Thus the tame cost and the previously bounded odd cocycle contribution are available on the same nodes and intervals. The estimate on c_ℓ counts the valuation loss in the cohomological tests. Its use in an integral projection still requires the congruence argument for the Hecke action on the theta lifts.

For the geometric Frobenius convention in that action, apply Theorem 12.6 at s^{-1} for each test point s, and use the inverse of its arithmetic Frobenius. All these elements act trivially on the finite twisted coefficients. Inversion negates the value of a cocycle there, so the test at geometric Frobenius gives $2z(s)$. It changes the sign of the diagonal dual value and leaves its valuation unchanged. Testing γ^{-1} is equivalent to testing γ by the cocycle identity.

12.4 Scalar cocycles after the paired inertia and Frobenius tests

Fix a field E, a prime ℓ, an exponent $0 \le e < t$ and finite precision $\nu \ge 1$ as in Theorem 12.9. Write $A = \mathcal{O}/\ell^\nu\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_\ell$. The coefficient character is $\chi = \kappa^{-e}$. At a prime above ℓ, consider the following elements of the absolute Galois group. For $e > 0$ take the kernel of the full cyclotomic character in its decomposition group. For $e = 0$ take its inertia group. Write L_e for the union of these sets over all places above ℓ and all their prolongations. This set is stable under $g \mapsto cgc^{-1}$.

Lemma 12.11 (The local crystalline evaluation equations)**.** *At a place $v \mid \ell$, each integral crystalline cocycle of $\mathcal{O}(-e)$ vanishes on L_e in its chosen local group. The same evaluation equations hold for a finite coefficient cocycle satisfying all integral linear relations among the evaluations of the local crystalline cocycles. For a global cocycle, the equations at one prolongation of each v imply the equations at all prolongations.*

Proof. Write $K = E_v$. The Bloch–Kato computation gives $H^1_f(K, \mathbb{Q}_\ell(-e)) = 0$ for $e > 0$. At $e = 0$ this group consists of the unramified homomorphisms. In particular the computation is over the actual completion K, with arbitrary absolute ramification. Scalar extension to the fraction field of $\mathcal{O}$ preserves these descriptions by taking coordinates in a $\mathbb{Q}_\ell$-basis. For $e > 0$ the integral cocycle is therefore of the form $g \mapsto (\chi(g) - 1)a$ over the fraction field and has value zero when $\kappa(g) = 1$. For $e = 0$ it is zero on inertia. The integral lattice embeds in its fraction space, giving these equalities integrally. [16, Corollary 3.8.4 and Example 3.9]

Each such single evaluation with coefficient one is itself an integral linear relation. Finally the cocycle identity gives

$$z(hgh^{-1}) = \chi(h)z(g) + (1 - \chi(g))z(h).$$

The elements being tested have $\chi(g) = 1$, proving the assertion for the conjugate prolongations as well. □

Use the primes of Theorem 12.9 and put $I_e = \{j : e_j = e\}$, so I_0 is empty. For any auxiliary element a put $a' = (cac^{-1})^{-1}$. Write $C = \ell^{b_\ell}$. Let Z be an $\mathcal{O}$-module of continuous $A(\chi)$-valued cocycles unramified outside ℓ and the pairs $w_j, \bar{w}_j$. Write Z_L for those vanishing on L_e, and let Z_f consist of the members of Z satisfying the local crystalline relations in the lemma at every $v \mid \ell$. All lengths below are over $\mathcal{O}$. These modules are finite. Indeed the bounded-degree and finite-ramification-set argument in the proof of Theorem 12.6 applies to the affine group of $A(\chi)$.

Theorem 12.12 (Loss of length after the paired tests)**.** *For $j \in I_e$, let $z \in Z_L$ satisfy $z(\tau_i) = z(\tau_i')$ for all $i < j$ and $z(\phi_i) = z(\phi_i')$ for all $i < j$ in I_e. Then*

$$C\big(z(\tau_j) - z(\tau_j')\big) = 0.$$

Now let $S \subseteq Z_L$ be any submodule whose members vanish at every τ_j, τ_j' and agree at ϕ_j, ϕ_j' for $j \in I_e$. Write $\overline{S}$ for its image in $H^1(G_E, A(\chi))$. Let O_e denote the strict odd cocycles $Z^-_\nu(E, e)$ with coefficients $\mathcal{O}$ if $e > 0$. For $e = 0$ put $O_0 = \mathrm{Hom}(\mathrm{Cl}(E), A)$. Then

$$\mathrm{length}(Z/Z_L) + \mathrm{length}(C\overline{S}) \;\le\; \mathrm{length}(Z/Z_f) + \mathrm{length}\, O_e.$$

The same inequality holds with CS in place of $C\overline{S}$ if $e = 0$, or if every $z \in S$ satisfies $(u^{-e} - 1)z(\gamma) = 0$, with u, γ as in Lemma 12.8.

Proof. Write $z^c(g) = z(cgc^{-1})$. This is a cocycle for the same character since $\kappa(cgc^{-1}) = \kappa(g)$. At every τ_i and ϕ_i the action on A is trivial. The identity for inverses then gives

$$z(a) - z(a') = (z + z^c)(a) \qquad (a = \tau_i, \phi_i).$$

For $j \in I_e$ one has $e > 0$. Thus $z + z^c$ is even, has the allowed ramification, and vanishes on L_e. The earlier equalities in the theorem are exactly the vanishing conditions of Theorem 12.6. Its multiplier $2M\Delta_e$ divides C by Theorem 12.9. This proves the first assertion.

Each member of S is unramified away from ℓ. At either member of an auxiliary pair inertia acts trivially on the coefficients, so the cocycle on inertia is a homomorphism. Wild inertia and the prime-to-ℓ factors of tame inertia map to zero. A generator of the remaining procyclic factor and its conjugate inverse have both been tested. This proves unramifiedness at the pair. In weight zero the condition on L_0 now gives an everywhere unramified homomorphism. Class field theory for the totally imaginary field E embeds S into O_0, and its coboundaries are zero.

Suppose $e > 0$. Sending z to $z^c - z$ maps S to O_e, by the ramification and local conditions just checked. It sends every coboundary to zero because χ is invariant under conjugation by c. Thus it induces a map $\overline{S} \to O_e$. An element in its kernel has a representative $z \in S$ with $z^c = z$ as functions. For each $s \in S_\ell$, the reading prime for (e, s) therefore gives

$$4z(s) = 2(z + z^c)(s) = (z + z^c)(\phi_j) = 0.$$

Put $D = u^{-e} - 1$. To handle an arbitrary representative define the cocycle

$$z_*(g) = Dz(g) - (\chi(g) - 1)z(\gamma).$$

It is unramified outside ℓ, has $z_*(\gamma) = 0$, and $4z_*$ vanishes at every $s \in S_\ell$, since $\chi(s) = 1$. Lemma 12.8 now yields $4Dz_* = 0$ in all cases. At the places of exact detection one already has $4z_* = 0$. In cohomology $[z_*] = D[z]$, so $4D^2[z] = 0$. If $Dz(\gamma) = 0$ holds initially, one may apply the same test lemma directly to $4Dz$, giving $4D^2 z = 0$ as a function. Since $4D^2$ divides C in $\mathcal{O}$ by Theorem 12.9, the corresponding kernel is killed by C. Multiplication by C consequently factors through the image of the map to O_e, and the length of its image is at most $\operatorname{length} O_e$. Finally Lemma 12.11 gives $Z_f \subseteq Z_L$, which proves the displayed bound. □

Corollary 12.13 (The scalar costs on the period fields)**.** *For weights $0 \le e < t$ allow different coefficient rings $\mathcal{O}_e$, with ramification indices a_e, and different precisions. Use a common set of auxiliary primes at the largest precision. With $E \subseteq \mathbb{Q}(\mu_N)$, the sum over e of*

$$\frac{\operatorname{length}(Z/Z_L) + \operatorname{length}(C\overline{S}) - \operatorname{length}(Z/Z_f)}{a_e}$$

is at most $v_\ell(h_E \mathcal{J}_{N,t})$. The cocycle version with CS holds under the corresponding normalization hypotheses of the theorem. When N, t vary on the period interval, the bounds of Corollary 11.30 apply.

Proof. For precision $\nu' < \nu$ the map of coefficient modules $a \bmod \ell^{\nu'} \mapsto \ell^{\nu-\nu'} a \bmod \ell^{\nu}$ is an equivariant injection. Hence all evaluations and the triangular annihilation at precision ν hold at ν'. The primes can simultaneously satisfy the determinant condition of Corollary 47.37 for its prescribed representation. Apply Theorem 11.29 to the bounds of Theorem 12.12 and sum. □

The estimate singles out the local crystalline colength $\operatorname{length}(Z/Z_f)$ in the congruence calculation. Its contribution for the actual families of representations, and the corresponding bound for their higher-rank summands, still enter the integral period comparison.

12.5 Crystalline cocycles at the spherical coefficient primes

The character determinants of Theorem 45.8 contain the index l_e of a local condition inside a module defined by relations among matrices. At coefficient primes in a common Fontaine–Laffaille range, this index is zero at every auxiliary level. We first construct the local extension that realizes a solution of the matrix relations.

Lemma 12.14 (A lattice for the matrix cocycle)**.** *Let G be a profinite group, let $\mathcal{O}$ be the ring of integers of a finite extension $L/\mathbb{Q}_\ell$, and let u_x be a finite family of continuous representations on free $\mathcal{O}$-lattices U_x. Set $D(g) = (u_x(g)-1)_x$. Suppose $z : G \to T/\ell^\nu T$ is a continuous cocycle, where T is a G-stable lattice. Assume that every finite $\mathcal{O}$-linear relation among the $D(g)$ holds among the corresponding $z(g)$. The extension defined by z is the pushout of the reduction of an integral, rationally split extension of $\mathcal{O}$ by a lattice Y. Rationally, Y is a direct sum of copies of the $U_x \otimes L$.*

Proof. Let $W = \bigoplus_x \mathrm{End}_{\mathcal{O}}(U_x)$, with g acting on each matrix by multiplying it on the left by $u_x(g)$. Reading columns gives the asserted direct sum description of W. Let $P \subset W$ be the $\mathcal{O}$-span of the $D(g)$. The identity $hD(g) = D(hg) - D(h)$ makes P stable. The relations define a linear map $b : P \to T/\ell^\nu T$ sending $D(g)$ to $z(g)$. The cocycle identity applied to hg makes b equivariant. By the elementary divisor theorem there is s such that $P \cap \ell^s W \subset \ell^\nu P$. Indeed in a basis in which P has elementary divisors d_i, one can take ℓ^s divisible by every $\ell^\nu d_i$. Thus b extends by zero on $\ell^s W$ to $Y = P + \ell^s W$. Its reduction on $Y/\ell^\nu Y$ is again equivariant.

On $Y \oplus \mathcal{O}v$ put $gv = v + D(g)$. This action is continuous by the lattice topology and the cocycle identity. With $I = (1_{U_x})_x$ one has $D(g) = gI - I$. The vector $v - I$ therefore gives a section over L, since $Y \otimes L = W \otimes L$. Reduction and pushout along b give exactly $gv = v + z(g)$. In particular the torsion extension is a quotient of the direct sum of $(Y \oplus \mathcal{O}v)/\ell^\nu$ and $T/\ell^\nu T$, by the graph of the negative of b. □

Theorem 12.15 (Lifting the local cocycle at full precision)**.** *Suppose $K/\mathbb{Q}_\ell$ is finite unramified, $\ell > 2$, and $G = G_K$. Suppose $T \otimes L$ and all $U_x \otimes L$ are crystalline. Assume that their de Rham filtration jumps at all embeddings, together with 0, lie in one interval of integers $[A, B]$ with $B - A \le \ell - 2$. Use the convention that the cyclotomic character κ has filtration jump -1. Every cocycle in Lemma 12.14 is the reduction of an integral cocycle defining a crystalline extension of the trivial representation by $T \otimes L$.*

Proof. Write $j = -A$. Twist the extensions by κ^{-j}. Their jumps now lie in $[0, B - A]$, and the quotient is the character of jump j. Use the covariant integral Fontaine–Laffaille functor for this interval. It is exact and fully faithful, its essential image on torsion objects is closed under subquotients, and every stable lattice in a crystalline representation with these jumps is in its image. In the filtered description a Tate character κ^{-j} has a generator in degree j fixed by its j-th divided Frobenius. Morphisms are strict for the filtration. These are the integral and torsion comparison theorems, including their versions with coefficients. [17, 18]

Write $S = W(k_K) \otimes_{\mathbb{Z}_\ell} \mathcal{O}$, where k_K is the residue field of K, and $S_\nu = S/\ell^\nu S$. The Frobenius on these rings acts on the Witt vectors and fixes the coefficients. One may enlarge L to contain all embeddings of K. For descent, $\mathcal{O}$ is a direct summand of its finite ring extension as an $\mathcal{O}$-module, since 1 is primitive. After restricting coefficients, project a lifted cocycle back to T using a projection sending 1 to 1. On rational extensions this is a pushout in the category of crystalline representations. It preserves crystallinity because this category is closed under direct sums and quotients.

By the preceding lemma the rational representation behind the graph lattice is a sum of crystalline representations in the given interval. Its reduction and that of T therefore belong to

the Fontaine–Laffaille image after the twist. Closure under quotients puts the pushout in that same image. By full faithfulness and exactness the resulting filtered module is an extension of the rank-one module $S_\nu v_0$, of pure degree j, by the reduction $M_\nu = M/\ell^\nu M$ of the filtered lattice M for $T(\kappa^{-j})$. More explicitly, kernels and images of morphisms in the torsion category are carried to their kernels and images on representations, so the two ends have the specified identifications.

Strictness gives a lift v of v_0 in filtration j. The module splits over S_ν with this choice. In filtration degrees $i \le j$ one adds $S_\nu v$ to $\mathrm{Fil}^i M_\nu$, and in degrees $i > j$ one has precisely $\mathrm{Fil}^i M_\nu$. Thus the only new Frobenius datum is $\phi_j(v) = v + a$, with $a \in M_\nu$. Choose any $\widehat{a} \in M$ reducing to a. On $M \oplus S\widehat{v}$ impose the same split filtration and set

$$\phi_i(\widehat{v}) = \ell^{j-i}(\widehat{v} + \widehat{a}) \qquad (0 \le i \le j),$$

extending semilinearly. These maps satisfy the divided Frobenius relations. Their images generate the module because the images from M generate M and $\phi_j(\widehat{v})$ generates the quotient. This is an integral Fontaine–Laffaille extension, and its reduction with both ends identified is the given extension. Apply the functor and undo the Tate twist. A section of the quotient gives an integral cocycle. If its reduction differs from z by a coboundary, change the section by a lift of the defining element of $T/\ell^\nu T$. The resulting cocycle reduces to z at every group element. □

Corollary 12.16 (Simultaneous vanishing of the scalar colengths)**.** *At a node on the period fields of Corollary 12.4 fix the definite groups, weights and splitting characters in Theorem 45.16 and Corollary 45.17. Let $\ell > 2$ be unramified in $E/\mathbb{Q}$, with hyperspecial level above ℓ, and prime to the finite conductors of the splitting characters. All auxiliary levels used here are away from ℓ. For a group of rank n with algebraic weight $a = (a_{\tau,i})$, let h_α be the largest absolute filtration jump of its normalizing character α. Take the maximum H, over the groups under consideration, of*

$$t - 1, \qquad n + \max_{\tau,i} |a_{\tau,i}| + h_\alpha.$$

If $2H \le \ell - 2$, then $l_e = 0$ for all $0 \le e < t$. The conclusion applies to every auxiliary level and every precision. On any one finite interval the maximum of these bounds over its nodes gives one threshold for the same fields on which the periods are taken.

Proof. We check the local hypotheses for the actual automorphic systems. The base change used in Theorem 45.16 is spherical at a hyperspecial place, including an inert place. Its local parameter is a direct sum of the parameters of its cuspidal norm twists. Since a spherical parameter is trivial on inertia and has zero monodromy, both properties hold for each of these summands. Each normalized cuspidal factor $\pi_{ij} = \rho_i |\det|^s$, $s = j + (a_i - n)/2$ in the notation of that theorem (here a_i denotes the rank of ρ_i), is regular algebraic in its own rank. It is also essentially conjugate self-dual. Indeed the unitary cuspidal center ρ_i of its discrete string satisfies $\rho_i^c = \rho_i^\vee$ by uniqueness of its unitary cuspidal support. The ratio needed to identify $\pi_{ij}^\vee$ with a character twist of π_{ij}^c is $|\det|_E^{-2s}$. This is the pullback of $|\cdot|_F^{-2s}$ by the norm, with value 1 at -1 at each real place.

The spherical case of local-global compatibility for regular algebraic essentially conjugate self-dual cuspidal representations now gives crystallinity for each factor at every $w \mid \ell$. The representations so obtained agree with those in Theorem 45.16 by their good Frobenius polynomials and semisimplicity. In rank one the same assertion is the crystallinity of the local avatar of an algebraic character with unramified smooth part. In particular this applies to α. The Hodge weight formula for the full direct sum in rank n has entries $i - n - a_{\tau,i}$ in Guerberoff's convention. In the opposite sign convention the absolute values are the same. This formula

follows by joining the shifted infinitesimal characters of the cuspidal summands, as in the proof of his Theorem 2.3. It depends only on the algebraic infinity type. Tensoring by α shifts the weights at each embedding by its single filtration jump. The jumps of all the normalized systems hence lie in $[-H, H]$. [19, Thms. 0.1, 2.2 and proof of Thm. 2.3]

The coefficient lattice for weight e is $\mathcal{O}(\kappa^{-e})$ and has jump $e \in [0, H]$. Every cocycle in $\mathcal{Z}_e$ restricts at each $w \mid \ell$ to one obeying all the local matrix relations, since local relations are among the global relations defining $\mathcal{Z}_e$. Apply Theorem 12.15 with $K = E_w$. The resulting integral crystalline lift shows that its reduction satisfies every evaluation relation used in Lemma 12.11. This proves the asserted equality of the two subgroups defining l_e. Auxiliary level away from ℓ changes neither the infinity type nor the hyperspecial local component condition. On a fixed interval there are finitely many fields, nodes and weights, so the common maximum has the stated effect at primes satisfying the indicated local conditions. □

Proposition 12.17 (The main summand at a spherical coefficient prime)**.** *Under the same prime and weight assumptions, let T in Proposition 45.7 be a lattice in a direct summand of one of the normalized representations. Suppose T is unramified at the auxiliary pairs. Let S contain all old places of ramification away from ℓ. Then $\mathcal{V}_T$ injects into the subgroup of $H^1(E, (T \otimes L)/T)$ unramified outside $S \cup \{w \mid \ell\}$ and lying at each $w \mid \ell$ in the image of $H^1_f(E_w, T \otimes L)$. In particular, its length λ_T is bounded by the length of that Selmer group whenever the latter is finite.*

Proof. A continuous cocycle into a discrete torsion module has finite image by compactness, so it takes values in $\ell^{-\nu}T/T$ for some ν. Multiplication by ℓ^ν identifies this with $T/\ell^\nu T$. Its local matrix relations are preserved by this identification. At $w \mid \ell$ the rational summand is crystalline with jumps in the same interval, since subobjects of crystalline representations are crystalline and the de Rham filtration is exact. Lift the resulting local cocycle by Theorem 12.15 and divide by ℓ^ν. This gives a class in $H^1_f(E_w, T \otimes L)$ with the prescribed image.

Away from S, the auxiliary pairs and ℓ, all matrices are trivial on inertia. The corresponding single evaluation equation gives zero for the cocycle on inertia. At an auxiliary place the target is unramified, so the restriction to inertia is a homomorphism to an ℓ-group. It kills wild inertia and factors through the pro-ℓ tame quotient. The chosen tame generator has value zero by the definition of $\mathcal{V}_T$. Finally a coboundary coming from $b \in (T \otimes L)/T$ takes value $(y-1)b$ at the element η in Section 45.3. The same definition requires this value to vanish and $y - 1$ is a unit. Thus $b = 0$, which proves injectivity. □

The local conclusion in Corollary 12.16 is uniform in the precision. For primes below the weight threshold, or ramified in the fields, the torsion comparison used here gives no such bound. A bound for the global Selmer length of the main summand and the integral comparison for the projected periods on these same intervals are also still required by Section 6.6.

12.6 One anticyclotomic twist for simultaneous integral tests

At a new twist prime, the local contribution of a main summand depends on the valuation of a root of unity minus one. The order of this root also affects the values of integral determinants. We construct a single character on the period field for which all its prescribed powers can be used in finitely many such polynomial tests. The order needed for the construction can be chosen before the polynomials are given. The auxiliary characters and the use of cyclotomic radii follow the arguments in the supplied archive, in `AuxiliaryPrimes.lean` and `RootsOfUnity.lean` in its Selmer directory. Throughout this subsection $v(\ell) = 1$ on $\overline{\mathbb{Q}}_\ell$.

Lemma 12.18 (Independent ray characters on the period field)**.** *Let E be one of the CM fields of Corollary 12.4, let c be complex conjugation, and let S be any finite set of finite places containing its conjugates and all places above ℓ. Fix $d, N \geq 1$. There exist d places w_i of distinct rational prime norms outside S, all different from their conjugates, and continuous additive characters $\lambda_i : G_E \to \mathbb{Z}/\ell^N\mathbb{Z}$. They have the following properties. Each satisfies $\lambda_i^c = -\lambda_i$, is trivial on the decomposition groups in S, and is unramified outside w_i, w_i^c. At w_i its value on a suitable tame generator is 1. At w_i^c the conjugate generator has value -1. It is trivial on the decomposition groups at w_j, w_j^c for $j \neq i$. Arithmetic Frobenius lifts at the w_i can be chosen on which all the characters vanish.*

Proof. Enlarge S to a finite conjugation-stable set T whose prime ideal classes generate the class group of E. This is possible by factoring ideals in finitely many generating classes. The ring $\mathcal{O}_{E,T}$ then has trivial class group. The group of its units is finitely generated, including its torsion. Form the extension of E by μ_{ℓ^N} and the ℓ^N-th roots of finitely many generators of these units. It is a finite Galois extension. Enlarge it by the fields of the ray characters already constructed, taking their conjugates as well. Chebotarev supplies completely splitting primes w of E outside all the places used so far. One may choose rational prime norm since the higher residue degree prime ideals of a number field have Dirichlet density zero. Avoid all rational primes ramified in E and all norms previously chosen. An inert place over E^+ would have square norm, so $w \neq w^c$. Write $q = Nw$. Then $\ell^N \mid q - 1$, and every T-unit reduces to an ℓ^N-th power at w. [15]

Choose a surjection from the cyclic residue group $k_w^\times$ onto $\mathbb{Z}/\ell^N\mathbb{Z}$. Via reduction at w this gives a character on

$$D_T = \prod_{v \in T} E_v^\times \times \prod_{v \notin T} \mathcal{O}_v^\times \subset \mathbb{A}_{E,f}^\times.$$

It kills $E^\times \cap D_T = \mathcal{O}_{E,T}^\times$. The equality $\mathbb{A}_{E,f}^\times = E^\times D_T$ follows by taking the ideal of an idele outside T and using the triviality of the T-class group. The local character therefore extends to the finite ideles, kills the principal ideles, and is continuous because D_T is open. Extend it trivially at infinity. By global reciprocity it defines a Galois character ξ. Put $\lambda = \xi - \xi^c$. The character ξ^c is unramified at w, so λ is still onto on its tame inertia. The local components at T are trivial, and at all other places except w, w^c they are unramified. Before repeating the construction put w, w^c in T. Earlier characters vanish at the new decomposition groups by the splitting imposed on the new primes, and the new character vanishes at the earlier groups by the choice of T. At w_i any Frobenius lift may be multiplied by a power of the chosen tame generator to make its value under λ_i zero. All other λ_j vanish on that decomposition group. □

Lemma 12.19 (A uniform range of cyclotomic orders)**.** *Fix a positive real radius in valuation coordinates ρ, a number $B \geq 0$, $0 < \delta < 1$, and a lower exponent $h_* \geq 1$ with $r_{h_*} \leq \rho$, where*

$r_h = 1/\varphi(\ell^h)$. *Choose* $N \ge h_*$ *large enough that*

$$\delta \sum_{h=h_*}^{N} \frac{1}{h+1} > B.$$

For every nonzero polynomial $g(X) = \sum b_i X^i$ *with integral algebraic* ℓ*-adic coefficients and* $v_\rho(g) = \min_i(v(b_i) + i\rho) \le B$*, there is a primitive* ℓ^h*-th root* ζ *with* $h_* \le h \le N$ *such that*

$$v(g(\zeta - 1)) \le v_{r_h}(g) + \delta.$$

Proof. Factor g over $\overline{\mathbb{Q}}_\ell$ and count roots with multiplicity, putting $v(0) = +\infty$. For $u \ge 0$ the Gauss valuation satisfies

$$v_u(g) = v_0(g) + \sum_{\alpha:\, v(\alpha) > 0} \min(v(\alpha), u).$$

Indeed it is multiplicative. For a rational u, substitute a scalar of valuation u times X, divide each factor by a coefficient of least valuation, and reduce modulo the maximal ideal. The product of nonzero reduced polynomials is nonzero. This proves multiplicativity for rational u, and continuity of the finite minima gives it for real u. Applying this to each linear factor proves the formula, also for polynomials with nonintegral roots.

Let R_h be the multiset of roots with $v(\alpha) = r_h$. The r_h are positive and distinct. Since $v_0(g) \ge 0$, $\sum_{h=h_*}^{N} |R_h| r_h \le v_\rho(g)$, so there exists an h for which $|R_h| r_h (h+1) < \delta$. For $\alpha \in R_h$ the polynomial $F_\alpha(Y) = (1 + \alpha + Y)^{\ell^h} - 1$ is integral and monic. Its roots are $\xi - 1 - \alpha$ for all ℓ^h-th roots ξ. They are integral. The coefficient of Y has valuation h, as $1 + \alpha$ is a unit. The same Gauss formula at $u = 1$ shows that

$$\sum_{\xi \text{ primitive of order } \ell^h} \min\bigl(v(\xi - 1 - \alpha), 1\bigr) \le v_1(F_\alpha) \le h + 1.$$

There are $1/r_h$ primitive roots. Averaging this inequality over them and summing over R_h gives one ζ for which the sum of the truncated valuations over R_h is less than $\delta < 1$. Every term consequently equals its untruncated valuation. The identity $v(\zeta - 1) = r_h$ follows from the cyclotomic polynomial at 1, since all the primitive roots are conjugate and their differences from 1 have product of absolute valuation 1. For a root outside R_h, the valuation of $\zeta - 1 - \alpha$ equals $\min(r_h, v(\alpha))$ by the ultrametric inequality. Subtracting the Gauss valuation of the product now gives

$$v(g(\zeta - 1)) - v_{r_h}(g) = \sum_{\alpha \in R_h} \bigl(v(\zeta - 1 - \alpha) - r_h\bigr) < \delta.$$

This includes a constant g, for which the sum is empty. □

Theorem 12.20 (One choice of twist for all powers and polynomials)**.** *Fix* ℓ, E, S, d *as in Lemma 12.18, an integer* $m \ge 1$*, and real numbers* $\rho, \varepsilon, \eta > 0$ *and* $B \ge 0$*. One can choose* N, w_i, λ_i *before the following tests are specified. A test consists of an integral polynomial* P_a *in* d *variables, an integer* s_a *with* $1 \le |s_a| \le m$*, and a witness* $x_a \in \overline{\mathbb{Q}}_\ell^{\,d}$ *with* $v(x_{a,i}) \ge \rho$*. Allow any finite list with* $\sum_a v(P_a(x_a)) \le B$*. There is one finite-order anticyclotomic character* ϑ *trivial on* S*, with tame conductor supported on the selected pairs. Write* γ_i *for the selected tame generator at* w_i *and* $\zeta_i = \vartheta(\gamma_i)$*. Then*

$$v\bigl(P_a((\zeta_i^{s_a} - 1)_i)\bigr) \le v(P_a(x_a)) + \varepsilon \quad \text{for every } a.$$

The same estimate holds for the sum of these valuations, with ε added only once. For every $1 \le |s| \le m$, ϑ^s has nontrivial inertia at all $2d$ selected places and

$$\sum_{w \in \bigcup_{i=1}^{d} \{w_i, w_i^c\}} v(\vartheta^s(\gamma_w) - 1) \le \eta,$$

where the sum ranges over the $2d$ distinct places.

Proof. Put $L = \lfloor \log_\ell m \rfloor$, $\rho' = \rho/m$, and choose $h_* > L$ with $r_{h_*} \le \rho'$ and $2d\ell^L r_{h_*} \le \eta$. Take $\delta = \min(1, \varepsilon)/(d+1)$ and apply Lemma 12.19 with $B+1, \rho', h_*, \delta$ to choose N using divergence of the harmonic series. Now construct the ray characters of this order. Up to this point the polynomial degrees, their number and their witnesses have played no part.

For a test of power $s > 0$, substitute $(1 + X_i)^s - 1$ in each coordinate. For $s = -b < 0$ use $(1 + X_i)^{-b} - 1$ and multiply by $\prod_i (1 + X_i)^{b \deg_{X_i} P_a}$. This gives, in both cases, an integral polynomial Q_a. The extra factors are units whenever $1 + X_i$ is a unit. There are witnesses y_a for these polynomials with $v(y_{a,i}) \ge \rho'$ and $v(Q_a(y_a)) = v(P_a(x_a))$. For $b = |s|$, solve $(1 + Y)^b = 1 + x$ if $s > 0$, and $(1 + Y)^b = (1 + x)^{-1}$ if $s < 0$. All roots in Y are integral because the equation is monic integral. Their product has valuation $v(x)$. Thus some root has valuation at least $v(x)/b$. If $x = 0$ take $Y = 0$.

Replace the witness coordinates successively by common values. At coordinate i, let $g_a(X)$ be Q_a specialized to the current values of its other variables. All coefficients are integral and the unreplaced coordinate of each witness still has valuation at least ρ'. For $g = \prod_a g_a$, multiplicativity gives $v_{\rho'}(g) \le \sum_a v(Q_a(\text{current witness}))$. Inductively this last sum is at most $B + (i - 1)\delta < B + 1$. Choose a primitive root of an allowed order by the preceding lemma. For each factor $v(g_a(\zeta_i - 1)) - v_{r_h}(g_a) \ge 0$ by the ultrametric inequality, and the sum of these excesses is at most δ. Since $v_{r_h}(g_a) \le v_{\rho'}(g_a)$ and the latter is at most its previous witness valuation, each increase and the increase of the sum are bounded by δ. After d coordinates the total allowance is $d\delta \le \varepsilon$.

Finally take $\vartheta(g) = \prod_i \zeta_i^{\lambda_i(g)}$, well defined since each order divides ℓ^N. At a chosen tame generator its value is ζ_i, or ζ_i^{-1} at the conjugate. For $0 < |s| \le m$ its value there has order $\ell^{h_i - v_\ell(s)} > 1$. The valuation of its difference from 1 is therefore $\ell^{v_\ell(s)} r_{h_i}$. Summing proves the ramification bound. □

Corollary 12.21 (Selmer conditions at the new twist places)**.** *Suppose $T_1, \dots, T_b$ are fixed Galois lattices on E. Include all their ramified places outside ℓ in S. For every T_j of rank r_j, and every $0 < |s| \le m$, imposing the finite local conditions at the new pairs on the divisible coefficient Selmer group for $T_j \otimes \vartheta^s$ costs at most $r_j\eta$ in normalized length. The character may satisfy the polynomial conclusions of Theorem 12.20 at the same time.*

Proof. Extend coefficients to contain the character values. At each new place inertia acts by the single nontrivial scalar $u = \vartheta^s(\gamma_w)$. Proposition 45.25 applies with determinant $(1 - u)^{r_j}$. Thus the length divided by the absolute ramification index of the coefficient ring is at most $r_j v(1 - u)$ locally. The quotient of the group with relaxed conditions by the group with finite conditions injects into the direct sum of the local quotients. The sum in Theorem 12.20 proves the claim. Triviality on S ensures that all local representations at the coefficient places are unchanged by this twist. □

This result controls the local cost of adding twist primes on a fixed period field. To bound the global Selmer length by specializing minors, one needs witnesses with a quantitative bound B for the actual relation matrices, and compatible witnesses for the ratios of the Hecke values entering the periods.

12.7 Integral minors for the Selmer groups of the twists

We describe the polynomials needed for the main summand at a fixed precision. In one case a witness can be constructed at the untwisted point, with no enlargement of the group from relaxing ramification. This gives a bound for one twist and all its powers in terms of a group at the original level.

Fix a CM period field E, a coefficient ring $\mathcal{O}$ with fraction field L, a finite conjugation-stable set S containing the coefficient places, and a rank-r lattice T unramified outside S. Specify linear evaluation equations on cocycles, with coefficients in $\mathcal{O}$. Each equation involves a finite sum of coordinates of values at specified elements of G_E. For the application include $z(\eta) = 0$ at the marked element of Section 45.3 and all equations satisfied by local integral crystalline cocycles at the coefficient places. The list of equations itself may be infinite. Extend the coefficients of the equations when extending scalars. We use normalized length, ordinary length divided by the absolute ramification index of the coefficient ring, and the valuation $v(\ell) = 1$.

Proposition 12.22 (A finite set of sharp integral minors)**.** *Let W be a finite set of additional places disjoint from S, and let $\lambda_i : G_E \to \mathbb{Z}/\ell^N\mathbb{Z}$, $1 \le i \le d$, be characters unramified outside $S \cup W$. Fix $M \ge 1$. There is a finite matrix $D(X)$ over $\mathcal{O}[X_1, \dots, X_d]$, of full column rank after every specialization in characteristic zero, with the following property. For any extension of coefficient rings $\mathcal{O}'/\mathcal{O}$ and any ℓ^N-th roots $\zeta_i \in \mathcal{O}'$, let $\chi = \prod_i \zeta_i^{\lambda_i}$. The minimum of the valuations of the maximal column-size minors of $D((\zeta_i - 1)_i)$ equals the normalized length of the cocycles into $(T \otimes \mathcal{O}'/\ell^M)(\chi)$ unramified outside $S \cup W$ and satisfying the given equations. Here and below the tensor with $\mathcal{O}'/\ell^M$ is over $\mathcal{O}$.*

Proof. Let G be the Galois group of the maximal extension unramified outside $S \cup W$, and H the common kernel of T mod ℓ^M and the λ_i in G. It is open and normal. Put

$$\Gamma = G/\overline{[H, H]H^{\ell^M}}.$$

This is a finite group. Indeed the fixed field K of H is a number field. The abelian quotient of H of exponent ℓ^M is unramified outside the finite set over $S \cup W$. By local reciprocity its characters there kill $(K_v^\times)^{\ell^M}$, which contains an open subgroup of the local units. At $v \nmid \ell$ this follows on sufficiently deep principal units by Hensel's lemma, and at $v \mid \ell$ by the logarithm on deep units. Choose a modulus with these local exponents. Global class field theory makes the abelian quotient a quotient of the finite ray class group of that modulus. The possible residue characters at infinity are trivial since K is totally imaginary. This proves finiteness of Γ.

The action of each of the indicated twists modulo ℓ^M is trivial on H. A cocycle restricts on H to a continuous homomorphism killing commutators and ℓ^M-th powers, and hence their closure. The cocycle consequently factors through Γ. Conversely inflation from Γ gives all these cocycles. Take r variables for the value Z_g at each $g \in \Gamma$. Lift the entries of the fixed matrices $T(g)$ mod ℓ^M to $\mathcal{O}$, writing $\widetilde{T}(g)$ for a choice of lift. Let $[b] \in [0, \ell^N - 1]$ be the integer representative of $b \in \mathbb{Z}/\ell^N\mathbb{Z}$. Use the rows of the polynomial linear equations

$$Z_{gh} - Z_g - \widetilde{T}(g) \prod_i (1 + X_i)^{[\lambda_i(g)]}\, Z_h = 0 \qquad (g, h \in \Gamma).$$

At the specified roots of unity these are exactly the cocycle equations over $\mathcal{O}'/\ell^M$. Evaluation equations map to constant rows by projecting their indexing group elements to Γ. The span of these rows in the finite free $\mathcal{O}$-module of all rows is finitely generated. Include any finite generating list. This constructs a matrix $A(X)$ with $b = r|\Gamma|$ columns. Adjoin the rows of $\ell^M I_b$ to form $D(X)$.

At a specialization the desired module is the kernel of A on $(\mathcal{O}'/\ell^M)^b$. By diagonalizing A over the valuation ring its normalized length is $\sum_{j=1}^{b} \min(v(a_j), M)$ for the diagonal entries, filling with zeros when necessary and putting $v(0) = +\infty$. This is also the length of the quotient of the integral row lattice by the row conditions, that is, of $(\mathcal{O}')^b/\operatorname{rowspan} D$. Its zeroth Fitting ideal is generated by the column-size minors of D, giving the claimed minimum. The adjoined rows alone have nonzero determinant. □

Lemma 12.23 (Detection at a single precision)**.** *For any fixed twist over $\mathcal{O}'$, consider cocycles with values in $(T \otimes L')/(T \otimes \mathcal{O}')$, where L' is the fraction field of $\mathcal{O}'$, subject to the same equations and outside ramification condition. If the normalized length at precision ℓ^M in Proposition 12.22 is strictly less than M, it equals the normalized length with these divisible coefficients.*

Proof. The subgroup killed by ℓ^M is identified with the finite precision cocycles by multiplying their values by ℓ^M on $\ell^{-M}(T \otimes \mathcal{O}')/(T \otimes \mathcal{O}')$. Every individual cocycle has bounded order, by compactness of the Galois group and discreteness of the target. If the module contained an element not killed by ℓ^M, the cyclic submodule it generates would have an ℓ^M-torsion subgroup of normalized length M, by the ideal classification in a discrete valuation ring. This would contradict the strict inequality. □

Theorem 12.24 (An auxiliary pair preserving the original Selmer bound)**.** *Assume T has a marked element η in inertia at a place of S away from ℓ, acting by a scalar y whose reduction is different from 1. Assume also that $T^c \otimes L \simeq T^\vee \otimes L(\kappa^a)$ for some integer a. Fix $M, m \geq 1$ and $\varepsilon, \eta_0 > 0$. Let b_M be the normalized length at precision ℓ^M for the untwisted lattice over $\mathcal{O}$, with ramification permitted only in S and the chosen evaluation equations. There exist a single pair w, w^c and a character ϑ of the type constructed in Theorem 12.20, trivial on all decomposition groups in S, for which the following hold for every $0 < |s| \leq m$.*

1. *The normalized length of the group of cocycles for $T \otimes \vartheta^s$, with ramification permitted at the pair and subject to the same equations, is at most $b_M + \varepsilon$ at precision ℓ^M. If $b_M + \varepsilon < M$, the same bound holds with divisible coefficients.*
2. *The two normalized local costs of imposing the finite conditions at w, w^c have sum at most $r\eta_0$.*

If the untwisted group with the specified equations modulo the maximal ideal of $\mathcal{O}$ is zero, the corresponding groups with divisible coefficients are zero for every ℓ-power twist of the form above on the selected pair, for all its powers.

Proof. Choose the order bound ℓ^N using the proof of Theorem 12.20 with $d = 1$, any fixed $\rho > 0$, and $B = 2mb_M$. The untwisted group is finite by the finite quotient argument above with W empty. We refine the prime choice in Lemma 12.18. Write K_0 for the splitting field over E of the roots of the selected S'-units of that proof, with μ_{ℓ^N} included. Here S' denotes its enlarged generating set of places. Since η is in inertia away from ℓ, it fixes μ_{ℓ^N}. On each chosen radical it acts by multiplication by an ℓ^N-th root of unity. Thus $g = \eta^{\ell^N}$ fixes K_0. Apply Chebotarev in the compositum of K_0 with the field of the residual representation of T. Choose a prime of rational prime norm with Frobenius the conjugacy class of g, outside S' and outside the finite ramification of this compositum. The new prime splits in K_0, as required for the ray character. Its residue cardinality q is $1 \bmod \ell^N$. The residual Frobenius of T there is the scalar $\bar{y}^{\ell^N} \neq 1$, since the multiplicative group of the coefficient residue field has order prime to ℓ. At the conjugate place the polarization identifies its eigenvalues with the inverses times

q^a, so they too differ from 1 in the residue field. The equality of characteristic polynomials used here holds over L and hence holds on reduction for any invariant lattice. In particular $T(\phi_v) - qI$ is invertible over $\mathcal{O}$ at both new places.

For the untwisted lattice, allowing ramification at these places does not add any cocycles. Indeed inertia acts trivially on the target of an untwisted cocycle there. Its restriction factors through pro-ℓ tame inertia, and at a tame generator the Frobenius identity is $(T(\phi_v) - qI)z(\gamma_v) = 0$. Invertibility implies that this value is zero at every precision, also after any coefficient extension. At $X = 0$, the matrix of Proposition 12.22 on the enlarged set of places thus has minimum minor valuation exactly b_M. Select one minor P attaining that minimum. For each of the $2m$ signed powers use this same polynomial and its witness $x = 0$. The polynomial argument of Theorem 12.20 uses only the prescribed order bound and the independent ray character at the chosen pair. It applies to the refined choice of prime and gives $v(P(\zeta^s - 1)) \le b_M + \varepsilon$ simultaneously. The actual length is at most that valuation. Lemma 12.23 and Corollary 12.21 prove the first two assertions.

For the last assertion the residual normalized cocycle space remains zero at the enlarged set of places by the same tame calculation. Every finite ℓ-power root of unity reduces to 1. Thus after any such twist the residual equations are exactly the untwisted residual equations. Extending the residue field preserves their zero kernel, by linear algebra on the finite quotient, or by taking coordinates in a residue field basis. A nonzero cocycle with divisible coefficients has finite order. If the smallest power of a uniformizer killing it is the j-th power, multiplying by the $(j-1)$-st power gives a nonzero cocycle killed by the uniformizer. That multiple would give a nonzero solution of the residual equations. This proves vanishing. □

For a main summand with the squarefree marked type and polarization of Section 47.12, the scalar hypothesis holds for every ℓ at one of its two original level primes. At coefficient primes covered by Corollary 12.16, every member of $\mathcal{V}_T$ for the corresponding twisted family satisfies the local crystalline equations, provided the actual family has the hyperspecial coefficient level and the common weight interval of that corollary. This follows from Theorem 12.15 at each coefficient place, with the twist trivial there. Taking the equations at η and at the coefficient places thus gives a finite minor bound for these cocycles whenever the untwisted test gives $b_M + \varepsilon < M$. For a large untwisted group the construction above preserves its bound. A quantitative reduction of such groups under twisting is still needed for the common interval estimate.

12.8 The primary and dual terms for a polarized marked summand

Let T be a lattice over a discrete valuation ring $\mathcal{O}$ finite over $\mathbb{Z}_\ell$, with uniformizer π, fraction field L and $v_\pi(\pi) = 1$. Write $V = T \otimes L$, $G = G_E$, $r = \operatorname{rank} T$, $A_a = \mathcal{O}/\pi^a$, and $W_a = T/\pi^a T$. We use the $\mathcal{O}$-linear Tate dual $W_a^* = \operatorname{Hom}_{\mathcal{O}}(W_a, L/\mathcal{O})(1)$. It identifies with the usual character dual with the Tate twist after choosing a generator of the inverse different of $\mathcal{O}/\mathbb{Z}_\ell$ and using the trace to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Lengths and local orthogonal complements in the statements below are independent of this choice.

Theorem 12.25 (The global congruence term at every precision)**.** *Suppose the $\mathcal{O}$-span of $T(G)$ is $M_r(\mathcal{O})$ and $V^c \simeq V^\vee(1-t)$, with $t \geq 1$. Let $I_t \subset \mathcal{O}$ be the ideal generated by*

$$(1 - \kappa(g)^t) \operatorname{tr} T(g), \qquad g \in G.$$

Then $\operatorname{Hom}_{A_a[G]}(W_a, (W_a^*)^c)$ is cyclic and has ordinary $\mathcal{O}$-length $\min(a, v_\pi(I_t))$, where the valuation of the zero ideal is $+\infty$. The ideal may be computed using good Frobenius elements on any set of primes of Dirichlet density one. It is unchanged by every finite-order anticyclotomic twist after extension to a ring containing the character values, with the original ideal extended to that ring.

Proof. Every G-stable full lattice in V is homothetic to T. Indeed it is stable under every integral matrix, since those matrices are spanned by the action of G. The coordinate idempotents split it into fractional ideals on the coordinate axes, and the off-diagonal matrix units identify those ideals. The same argument applies after a scalar character twist by units. The rational polarization identifies $(V^\vee)^c(1)$ with $V(t)$, so the corresponding integral lattices can be identified equivariantly after a scalar rescaling. With a choice of π^{-a} for the finite coefficient dual this identifies the homomorphism group in the theorem with $\operatorname{Hom}_{A_a[G]}(W_a, W_a(t))$.

The residual representation is absolutely irreducible by the full matrix span. Homomorphisms between it and its residual twist have residue dimension at most one, by Schur's lemma. In the finite-level homomorphism group the subgroup killed by π is exactly this residual homomorphism space, by dividing all entries by π^{a-1}. The structure theorem over a discrete valuation ring therefore makes the group cyclic. A homomorphism of order ideal (π^s), $s > 0$, has entries divisible by π^{a-s}. After that division its reduction to precision s has at least one unit entry. Its residual map between the irreducible modules is nonzero, so it is invertible modulo π, hence modulo π^s. Conversely an isomorphism at precision $s \leq a$, multiplied by π^{a-s}, supplies a homomorphism of precisely that order at precision a.

For completeness, at precision s equality of traces at every g suffices for an isomorphism. Write $B = \mathcal{O}/\pi^s$, $u = T \bmod \pi^s$ and $u' = \kappa^t u$. Both maps $B[G] \to M_r(B)$ are onto, since twisting multiplies each spanning matrix by a unit. The trace pairing on $M_r(B)$ is perfect, as one sees from the matrix units. Equality of traces on G gives equality on $B[G]$, hence equality of the two kernels by testing each element against every right multiplier. We obtain a B-algebra automorphism of $M_r(B)$ carrying $u(g)$ to $u'(g)$. To see that it is inner, let F_{ij} be the images of the standard matrix units. The projections F_{ii} split B^r into r isomorphic projective summands, each free of rank one since B is local. Choose a basis of the first summand and transport it to the others by F_{i1}. In this basis all F_{ij} are the standard units. Thus the two actions are isomorphic. Trace equality is precisely $I_t \subset (\pi^s)$. This proves the length formula. Reduction modulo any π^s makes the trace test a finite union of Frobenius conjugacy conditions, proving the density-one assertion by Chebotarev. A character twist multiplies each displayed generator of I_t by a unit. Anticyclotomicity preserves the polarization with the same t. □

Corollary 12.26 (Uniform size on the two marked level primes)**.** *Suppose the main summand is as in Theorem 47.36 with $1 \leq r \leq r_0$, $t \leq t_0$, on the shorter period field. For each ℓ pick*

$p_i \neq \ell$ with a marked place of the prescribed primitive type, or its indicated rank-one type. Then the supremum over a of the normalized length in Theorem 12.25 is at most $v_\ell(p_i^{rt}-1)$. For $G_0 = \prod_i |\mathrm{GL}_{r_0t_0}(\mathbb{F}_{p_i})|^f$ of Corollary 12.10, the sum of these suprema with weights $\log \ell$ is at most $(\log G_0)/f$.

Proof. By the theorem on the marked local matrices, $g = \phi_w^r$ acts by a unit scalar and $\kappa(g) = p_i^r$. Any isomorphism modulo π^s from T to $T(t)$ intertwines that scalar with p_i^{rt} times itself, implying $p_i^{rt} \equiv 1 \bmod \pi^s$. Use the isomorphism criterion in the proof of the preceding theorem. The integer $p_i^{rt}-1$ divides $|\mathrm{GL}_{r_0t_0}(\mathbb{F}_{p_i})|$, since $rt \leq r_0t_0$. Thus even when the choice of i depends on ℓ, the bound follows by taking valuations of the product of the two orders. The same scalar argument applies to any unramified twist at the chosen place, and Theorem 12.25 covers arbitrary anticyclotomic twists. □

Lemma 12.27 (Integral equations for a Bloch–Kato local condition)**.** *Let $K/\mathbb{Q}_\ell$ be a finite extension at which V is de Rham. Let Z_f be the integral cocycles $G_K \to T$ whose rational class lies in $H^1_f(K,V)$. At precision π^a, the solutions to all coordinate evaluation relations on Z_f are exactly the reductions of Z_f. Write $\mathcal{L}_K$ for their image in $H^1(K,W_a)$. Then*

$$\operatorname{length}_{\mathcal{O}} \mathcal{L}_K - \operatorname{length}_{\mathcal{O}} H^0(K,W_a) = a \dim_L(D_{\mathrm{dR}}(V)/\mathrm{Fil}^0).$$

Proof. The rational space of finite-condition raw cocycles has dimension $r+\dim_L(D_{\mathrm{dR}}(V)/\mathrm{Fil}^0)$. The Bloch–Kato local fundamental exact sequence gives $\dim H^1_f = \dim H^0 + \dim D_{\mathrm{dR}}/\mathrm{Fil}^0$; the coboundaries have dimension $r - \dim H^0$. [16, Cor. 3.8.4] Integral-valued cocycles form a full lattice in this space. In fact rational cocycles have bounded denominators by compactness, and a finite set of coordinate evaluations bounds the lattice from above, since coordinate evaluations separate the rational vectors and span their dual. Moreover the reductions of all evaluation functionals separate $Z_f/\pi Z_f$. A cocycle all of whose values are divisible by π can itself be divided by π in Z_f. By finite-dimensional duality followed by Nakayama's lemma the evaluations therefore span $Z_f^\vee$ integrally. Assigning coordinate values in A_a and obeying every integral relation is consequently exactly the same as assigning a linear map $Z_f^\vee \to A_a$, which is an element of $Z_f/\pi^a Z_f$. This proves the reduction assertion. Every raw coboundary at precision a lifts integrally. Their length is $ar - \operatorname{length} H^0(K,W_a)$. Subtract it from the length of $Z_f/\pi^a Z_f$ to obtain the formula. □

Theorem 12.28 (Comparison with the orthogonal Selmer group)**.** *Assume the hypotheses of Theorem 12.25, that V is de Rham above ℓ, and that an inertia element away from ℓ acts by yI_r with $y-1$ a unit. At the coefficient places use the conditions of Lemma 12.27. At a finite set S_0 away from ℓ, including all other ramified places, allow arbitrary local classes. At any additional unramified places v where W_a and μ_{ℓ^k} are trivial as local modules for some ℓ^k killing A_a, choose a normalized tame generator τ_v, an arithmetic Frobenius lift ϕ_v, and impose $z(\tau_v) = s_v z(\phi_v)$, $s_v \in A_a$. Use the unramified condition elsewhere. Denote these conditions by $\mathcal{L}$ and their local Tate annihilators on W_a^* by $\mathcal{L}^\perp$. Then*

$$\operatorname{length} H^1_{\mathcal{L}}(E,W_a) \leq \operatorname{length} H^1_{\mathcal{L}^\perp}(E,W_a^*) + \sum_{w\in S_0} \operatorname{length} H^0(E_w,W_a^*).$$

At an original marked place with no eigenvalue 1 on full tame inertia, the summand on the right is at most $v_\pi(\det(1-T(\sigma_w)))$. All lengths in this assertion are ordinary $\mathcal{O}$-lengths.

Proof. The equality of local orders in the Greenberg–Wiles formula, obtained by taking orders in Poitou–Tate duality, gives the difference of the two Selmer lengths as

$$\operatorname{length} H^0(E,W_a) - \operatorname{length} H^0(E,W_a^*) + \sum_v (\operatorname{length} \mathcal{L}_v - \operatorname{length} H^0(E_v,W_a)).$$

At an infinite place $\mathcal{L}_v$ has order one. Both global invariant groups are zero since the marked element acts by scalars y, y^{-1} on the two modules. At a finite unramified place with unramified condition, the local contribution is zero by the kernel and cokernel formula for Frobenius on a finite module. At an extra place with the indicated linear constraint, the cocycle is a homomorphism and its two local coordinates are independently arbitrary in W_a. Indeed the tame relation is $(q_v - 1)z(\tau_v) = 0$, automatic under the hypothesis. The graph of multiplication by s_v has length $ar = \operatorname{length} H^0(E_v, W_a)$. At the places of S_0, the finite local Euler characteristic formula gives precisely $\operatorname{length} H^0(E_w, W_a^*)$. [1]

Let $f = [E^+ : \mathbb{Q}]$. After coefficient extension to split all embeddings, the dimension in Lemma 12.27 counts negative de Rham filtration jumps at the embeddings belonging to the place. Extension of scalars does not change that dimension over the coefficient field. Under the polarization, a jump u at an embedding τ is paired with $t - 1 - u$ at its conjugate embedding. Since $t - 1 \geq 0$, each of the fr such pairs contributes at most one negative jump. Thus the total positive contribution above ℓ is at most afr. The f complex places each contribute $-ar$, giving the inequality. At the specified marked places, the dual invariant group is contained in the kernel of $T(\sigma_w)^{-\mathsf{t}} - 1$ on the finite coefficient dual. Over L this matrix is invertible, and its determinant has the same valuation as $\det(1 - T(\sigma_w))$. Elementary divisors bound its kernel length as claimed. □

The term in Theorem 12.25 is the size of a space of equivariant homomorphisms. In Theorem 12.28 the remaining term is a dual Selmer group of global cohomology classes. To use the first bound in the second inequality one needs a proof that the relevant dual classes inject into that homomorphism space after choosing the auxiliary local conditions.

12.9 Reducing the Selmer groups by local conditions at split pairs

We now construct the local conditions required at the end of Section 12.8. The construction works for finitely many polarized lattices at once. It is important that the number of primes can be bounded before specifying the orders of the ray characters. We give the argument for the prime selection and the global duality pairing in detail. The commutator argument and the descent by lengths are drawn from the supplied archive's `Mirror.lean` and `Descent.lean`.

Lemma 12.29 (Varying a linear condition over a finite valuation ring)**.** *Let C be a finite module over $\mathcal{O}$, with two linear maps $u, v : C \to (\mathcal{O}/\pi^a)^b$. Outside at most b residues of d in the residue field, one has*

$$\operatorname{length} \ker(du - v) \le \operatorname{length}\big(\ker u \cap v^{-1}(u(C))\big).$$

Proof. Let C' be the sum in C of all $\ker(xu - v)$ for $x \in \mathcal{O}$. Then $v(C') \subset u(C')$. Choose finitely many generators of C', and lift the columns of their u- and v-values to integral matrices U, V. The length of the image generated by U in $(\mathcal{O}/\pi^a)^b$ is ab minus the minimum k of the valuations of the b-rowed minors of $[U\ \pi^a I_b]$, by elementary divisors. Choose a minor attaining k. The corresponding determinant of $[XU - V\ \pi^a I_b]$ is a polynomial of degree at most b whose leading coefficient is the selected determinant, by multilinearity in the columns. Its least coefficient valuation is therefore at most k. Divide by that common uniformizer power and reduce. This gives a nonzero polynomial of degree at most b. Outside its residue roots the image length of $du - v$ on C' is at least that of u on C'. Subtract from the length of C', observing that $\ker(du - v) \subset C'$ and that $\ker(u|_{C'}) \subset \ker u \cap v^{-1}(u(C))$. □

Theorem 12.30 (Paired conditions with bounded primary length)**.** *Over the same field E, take finitely many lattices T_i satisfying Theorem 12.28, of ranks r_i and polarizing parameters $t_i \ge 1$. For each i require an element η_i of inertia away from ℓ with scalar value y_i such that $y_i^2 - 1$ is a unit. Fix S, closed under conjugation and containing all ramification of the lattices, the marked places, and the coefficient places. Use the finite local conditions of Lemma 12.27 above ℓ, unrestricted conditions at the other places in S, and unramified conditions elsewhere.*

Fix a precision $a_0 \ge 1$ in powers of π. Enlarge the residue field by an unramified coefficient extension until its order exceeds $1 + 2a_0 \max_i r_i$. There is a bound d_0, depending on these data and a_0, with the following property for every N such that $\pi^{a_0} \mid \ell^N$ in $\mathcal{O}$. One can find at most d_0 places J of distinct rational prime norms, outside S and disjoint from their conjugates, with a first place $w_0 \in J$. Each carries an anticyclotomic additive ray character $\lambda_j : G_E \to \mathbb{Z}/\ell^N\mathbb{Z}$, trivial at the coefficient places, of tame conductor supported on j, j^c, with a chosen tame generator τ_j mapping to 1. At each later place j the chosen arithmetic Frobenius ϕ_j satisfies

$$\lambda_{w_0}(\phi_j) = 1, \qquad \lambda_k(\phi_j) = 0 \quad (k \in J,\ k \ne w_0).$$

The first Frobenius may be prescribed in any given neighborhood of an inertia element at an old place away from ℓ. There are slopes $s_{ij} \in \mathcal{O}$, zero at the first place. At a later place impose the two conditions

$$z(\tau_j) = s_{ij} z(\phi_j), \qquad z((\tau_j^c)^{-1}) = s_{ij} z((\phi_j^c)^{-1}), \qquad g^c = cgc^{-1}.$$

A zero slope means the unramified condition at both places. Whenever $s_{ij} \ne 0$, the decomposition groups at the pair act trivially on $W_{i,a_0} = T_i/\pi^{a_0}T_i$ and on μ_{ℓ^N}. For the resulting Selmer group at each $1 \le a \le a_0$ one has

$$\operatorname{length} \operatorname{Sel}_J(W_{i,a}) \le v_\pi(I_{t_i}) + \sum_{\substack{v \in S \\ v \nmid \ell}} \sup_{1 \le b \le a_0} \operatorname{length} H^0(E_v, W_{i,b}^*).$$

A member of the Selmer group is represented throughout by the unique cocycle vanishing at η_i.

Proof. The unique normalization follows since $y_i - 1$ is a unit. The local conditions are conditions on cohomology classes, including the two displayed equations when the local actions are trivial.

Choose w_0, λ_{w_0} by the idele construction of Lemma 12.18. To prescribe its Frobenius near an old inertia element, invert the coefficient places and choose the class-group generating primes away from that old place and its conjugate. The Kummer extension of the resulting units is unramified there, as verified below. The inertia element fixes the extension, so Chebotarev in a compositum with the finite quotient specifying the neighborhood gives the required prime. Multiplication of its Frobenius by tame inertia at the new prime preserves this finite quotient and can make the new character zero on that Frobenius. Avoid the finite set of primes ramified in the compositum when making the choice. Impose the unramified condition there for every i. Its addition does not change any of the original Selmer groups. The sum D of their ordinary lengths over i and $1 \le a \le a_0$ is finite by Proposition 12.22, or its proof with a uniformizer power. The local finite conditions are given by integral equations by Lemma 12.27. We shall take $d_0 = 1 + D$.

Fix one lattice for the moment and omit i. Let H be the closed subgroup generated by $[g, \eta]$ and $[g, \eta^c]$, $g \in G_E$, with $[g, h] = ghg^{-1}h^{-1}$. Normality follows because a conjugate of $[g, \eta]$ by b is $[bg, \eta][b, \eta]^{-1}$, and the same holds for η^c. It is stable under c. The actions of T at η, η^c are the scalars y, y^{-1} by polarization and $\kappa(\eta) = 1$. Hence H acts trivially on T, its Tate dual and all the abelian characters. For a normalized cocycle z into W_a,

$$z([g, \eta]) = (1 - y)z(g).$$

Indeed $g\eta g^{-1} = [g, \eta]\eta$ and evaluating both sides gives the formula. In particular, if some value of z has a unit coordinate, the span of $z(H)$ is all of W_a. That span is stable under $T(G)$ by the cocycle conjugation identity on H. It contains a vector with a unit coordinate and is therefore the whole module by the full matrix span.

We record which new primes can be used. For every $h \in H$ and every neighborhood of $\tau_{w_0} h$ in G_E, there is a new prime w with arithmetic Frobenius lift in this neighborhood, with $T \bmod \pi^{a_0}$ and μ_{ℓ^N} locally trivial. The old character values at its Frobenius are 1 for w_0 and 0 for the others. It supplies a ray character as in the statement that vanishes on the decomposition groups at all earlier places except possibly the first pair. Here is the prime construction. In the idele argument of Lemma 12.18, take the set of inverted primes to include all coefficient places and all earlier nonfirst pairs. Require it to avoid the two places of the first pair and the marked places carrying η, η^c. One may still make the open class group trivial. Every ideal class has a representative prime outside a specified finite set by Chebotarev in the Hilbert class field. Adjoin such primes for generators and their conjugates. The resulting Kummer extension of the units is unramified at the omitted places, since ℓ is invertible there and extracting ℓ^N-th roots of units gives finite étale algebras over their valuation rings. Consequently $\tau_{w_0} h$ fixes this entire extension, since h is generated by commutators with inertia at omitted places. Its image under every old character on H is zero, and its image at τ_{w_0} is the stated one. Both T and κ are trivial on $\tau_{w_0} h$. Impose all the specified conditions in one finite Galois quotient, including a coset inside the given neighborhood, $T \bmod \pi^{a_0}$ at this element and its conjugate, and the Kummer and character fields. Chebotarev gives a new degree-one prime with a prolongation realizing the exact group element in this finite quotient. Avoid the ramified primes of the quotient. The idele construction at the new prime then applies. Multiplying the new Frobenius lift by a power of its tame generator makes the new character zero there, without changing its

image in that quotient. This proves the assertion. In particular every step in the construction is available for arbitrarily large N.

For an available w, let C be the primary Selmer cocycles with ramification relaxed at w, w^c but with all previous conditions. Take $u(z) = (z(\tau_w), z((\tau_w^c)^{-1}))$ and $v(z) = (z(\phi_w), z((\phi_w^c)^{-1}))$. These are linear maps to W_a^2. Their common domain is finite, and $\ker u$ is exactly the old Selmer group, since inertia acts trivially and its homomorphisms factor through the cyclic pro-ℓ tame quotient. If some old class has $v(z) \notin u(C)$, Lemma 12.29 permits a nonzero residue d with a strict decrease for this precision and a weak decrease at all precisions up to a_0. In fact the union of their bad residue sets has at most $2ra_0$ members. Set $s_{iw} = d^{-1}$ using any unit lift of the chosen residue. Give all other lattices slope zero, retaining exactly their old groups. Append this place whenever a failure $v(z) \notin u(C)$ occurs for some lattice, precision and available place. Each step lowers the total length by an integer at least one. After at most D such steps, every old class at every precision has its two Frobenius values in the image of the relaxed pair of tame evaluations at every available new place.

It remains to bound the lengths at this stopping point. Fix i, a. If the group is nonzero, let π^b, $1 \le b \le a$, be its exponent. Multiplying by π^{a-b} identifies the group at precision b with the subgroup at precision a killed by π^b, hence with the entire group. This follows directly on raw cocycles from the fixed linear equations, including those above ℓ, and the normalization. In precision b choose a class z of full order. Some coordinate of one of its values is a unit, so $z(H)$ spans W_b.

Let y' be a cocycle representing any class in the dual Selmer group at this precision, normalized by $y'(\eta) = 0$. Write $\langle\, , \,\rangle : W_b \times W_b^* \to \pi^{-b}\mathcal{O}/\mathcal{O}(1)$ for evaluation, identifying the root-of-unity factor using compatible primitive roots when computing local invariants. On $H \times H$ put

$$B(h,k) = \langle z(h), y'(k)\rangle - \langle z(k^c), y'(h^c)\rangle.$$

We first prove $B(h,h) = 0$. At the first pair both classes are unramified, since the unramified conditions at a place away from ℓ are exact annihilators for unramified modules. As inertia there acts trivially, both cocycles vanish on its tame inertia, including its conjugate. Thus the diagonal expression takes the same value at $\tau_{w_0}h$ and at h. Finite precision makes it locally constant. Choose an available w whose Frobenius ϕ has that same value. The stopping property supplies z' in the relaxed group with

$$z'(\tau) = z(\phi), \qquad z'((\tau^c)^{-1}) = z((\phi^c)^{-1}) = -z(\phi^c).$$

For the reciprocity calculation choose τ normalized on a uniformizer radical using the fixed primitive roots. This can be done by choosing at each new prime the residue logarithm in the ray character so that this generator has character value 1. Then $(\tau^c)^{-1}$ is the corresponding normalized generator at the conjugate place, since c inverts the roots of unity. An arithmetic Frobenius there is ϕ^c.

Apply Brauer reciprocity to z' and y'. All local pairings away from the new pair vanish by the old orthogonal conditions. At the new pair y' is unramified. The local invariant of the cup product is evaluation of its Frobenius value on the tame value of z', up to the same sign at both primes. This follows by subtracting the unramified part and using the Kummer character of a uniformizer as in Proposition 12.3, coordinate by coordinate. Thus the two remaining terms give $B(\phi,\phi) = 0$. For ramified coefficients the numerical invariant uses a trace to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Reciprocity for every scalar multiple of z' then gives vanishing in the coefficient-valued pairing by trace duality with the inverse different. This proves $B(h,h) = 0$.

The restrictions of both cocycles to H are homomorphisms. Expansion at hk consequently gives $B(h,k) + B(k,h) = 0$. If h is conjugated by η in the first argument, $B(h,k)$ is multiplied

by y through the actions of η on W_b and η^c on W_b^*, both equal to y. The same substitution in the second argument multiplies $B(k,h)$ by y^{-1}. Using the antisymmetry twice gives $(y^2-1)B(h,k)=0$, whence $B=0$.

There is now a unique linear map $F : W_b \to (W_b^*)^c$ taking $z(h)$ to $y'(h^c)$. Indeed any linear relation among the $z(h)$ gives the same relation among the $y'(h^c)$, after pairing with every $z(k^c)$, by $B=0$. These vectors span W_b and evaluation is perfect. Conjugating h by elements of G_E shows that F is equivariant. It depends linearly on the normalized dual cocycle. If $F=0$, the latter vanishes on H, and the commutator formula for the dual with scalar y^{-1} forces the normalized cocycle to vanish everywhere. This embeds the dual Selmer group into the homomorphism group computed in Theorem 12.25. Its length is at most $v_\pi(I_t)$. Theorem 12.28 now bounds the primary group as stated. At auxiliary pairs of zero slope the unramified condition contributes zero even when Frobenius acts nontrivially. This completes the proof at all precisions and for all the lattices. □

On the marked field of Corollary 12.10, suppose the only ramified places of the untwisted lattices away from ℓ are the places of the two original levels, with the marked types of Section 47.12. Take S to consist of these and the coefficient places. The results on the two determinants then bound the right side of Theorem 12.30, normalized by $v_\pi(\ell)$, by

$$(2r_i+1)v_\ell(G_0).$$

In fact Corollary 12.26 bounds the global term, and the last estimate of Section 45.8 bounds the sum of the local dual invariant lengths by the same determinant valuations used there. This applies at the spherical coefficient primes of Corollary 12.16 for the indicated main summands, with their prescribed polarization. The slopes just chosen give extra local equations for the original lattice. The passage from these equations to specializations by genuine finite-order characters requires an estimate for dropping the equations after a deformation.

12.10 Short Selmer groups for genuine twists of the main summands

The local equations at the split pairs of Theorem 12.30 apply first to the untwisted representation. Here we remove those equations and obtain a bound for an actual twist, using the same character for all the summands and all its prescribed powers. Write $v(\ell) = 1$. All lengths in this subsection are divided by the absolute ramification index of the coefficient ring.

Lemma 12.31 (Tame inertia along a line of characters)**.** *Use the prime pairs of Theorem 12.30 at precision ℓ^M for one lattice T. Write s_j for its slopes. Let $0 < \rho \le 1$, $N\rho \ge M$, and let y be an integral algebraic ℓ-adic number with $v(y) \ge \rho$. Set*

$$x_{w_0} = y, \qquad x_j = s_j y \quad (j \ne w_0), \qquad \psi_x(g) = \prod_j (1 + x_j)^{[\lambda_j(g)]}.$$

Here the brackets mean representatives modulo ℓ^N as in Proposition 12.22. Modulo ℓ^M this is a character. For any cocycle z of the resulting action on T/ℓ^M, after coefficient extension to contain y, at each later pair the two quantities $z(\tau) - s_j z(\phi)$ are killed by

$$(1 + y)T(\phi) - I.$$

Use $(\tau, \phi) = (\tau_j, \phi_j)$ and $((\tau_j^c)^{-1}, (\phi_j^c)^{-1})$, respectively. At $y = 0$, the two tame values at the first pair are killed by $T(\phi) - I$ for the corresponding Frobenius elements.

Proof. If $v(b) \ge \rho$, the sum $\sum_{h=0}^{\ell-1}(1 + b)^h$ has valuation at least $\min(1, (\ell - 1)v(b)) \ge \rho$. This follows by expanding it as $\sum_{d=1}^{\ell} \binom{\ell}{d} b^{d-1}$. Also $(1 + b)^\ell - 1$ has valuation at least ρ. Factoring the longer geometric sum into N sums of length ℓ gives

$$v\left(\sum_{h=0}^{\ell^N - 1} (1 + b)^h\right) \ge N\rho \ge M.$$

In particular $(1+b)^{\ell^N} \equiv 1 \bmod \ell^M$. Each power in ψ_x thus defines a character modulo ℓ^M. At a selected twist place the underlying T is unramified and the linear inertia action of the twist is scalar. The affine action $u \mapsto z(g) + T(g)\psi_x(g)u$ is trivial on wild inertia, since there the action on the lattice is trivial and a continuous homomorphism from a pro-residue-characteristic group to an ℓ-primary group vanishes. On the chosen tame generator its ℓ^N-th power is the identity because the translation part is multiplied by the geometric sum just estimated, and the scalar part has ℓ^N-th power one. The norm is 1 mod ℓ^N, so the tame Frobenius relation makes the affine actions of ϕ and τ commute, also for the conjugate inverses.

At a later place those two linear actions are $D = (1 + y)T(\phi)$ and $(1 + s_j y)I$, since only the first ray character takes value 1 on ϕ. At the conjugate inverses the ray-character values are identical by anticyclotomicity. Commutation of affine actions gives $(D - I)z(\tau) = s_j y z(\phi)$. When $s_j \ne 0$, one has $T(\phi) = I \bmod \ell^M$. When $s_j = 0$ the right side vanishes. Both cases give the asserted equation. At $y = 0$ all character values are one and the same affine relation at the first place gives $(T(\phi) - I)z(\tau) = 0$. □

Theorem 12.32 (Simultaneous twists with bounded divisible Selmer groups)**.** *Use the lattices T_i, field E, set S and integral coefficient-place evaluation equations of Theorem 12.30. Suppose there is an inertia element g_* at a place of S away from ℓ such that $\det(1 - T_i(g)) \ne 0$ for $g = g_*, (g_*^c)^{-1}$ and every i. Define*

$$B_i = v(I_{t_i}) + \sum_{\substack{w \in S \\ w \nmid \ell}} \sup_{b \ge 1} \operatorname{len}_{\mathrm{norm}} H^0(E_w, W_{i,b}^*) + \sum_{g \text{ in } (g_*, (g_*^c)^{-1})} v(\det(1 - T_i(g))).$$

Assume each B_i is finite. Given $m \geq 1$ and $\varepsilon, \eta_0 > 0$, there exists a finite-order anticyclotomic character ϑ, trivial on all decomposition groups above ℓ, ramified at a finite set of new split pairs, such that for every i and $0 < |s| \leq m$ the following holds. The cocycles for $T_i \otimes \vartheta^s$ with divisible coefficients, normalized to vanish at η_i, obeying the coefficient-place equations and unramified outside S and the new pairs, have normalized length at most $B_i + \varepsilon$. The sum of the normalized valuations of $\vartheta^s(\gamma) - 1$ at normalized tame generators of the new places is at most η_0. All conclusions hold after further finite coefficient extensions.

Proof. Choose $M > \max_i B_i + \varepsilon + 1$ integral. Write $a_0 = M v_\pi(\ell)$ and make the unramified coefficient extension of Theorem 12.30. This leaves the normalized bounds unchanged. For the invariant groups it follows by flat base change in the kernels of the action equations, with π still a uniformizer. The trace ideal and determinants extend by scalars. That theorem bounds the number of prime pairs by an integer d_0 depending on the untwisted data and a_0, independently of N. Choose a rational $0 < \rho \leq 1$ so small that $2(\max_i r_i) d_0 \rho < \min(1, \varepsilon/2)$.

We choose N before constructing any new primes. Require $N\rho \geq M$, and choose it also at least as large as the cyclotomic exponent in Theorem 12.20 for at most d_0 variables, witness coordinate bound ρ, signed powers up to m, tolerance $\varepsilon/2$, tame bound η_0, and sum-of-values bound $2m \sum_i (B_i + 1)$. Its proof gives the same exponent for every smaller number of variables by using the bounds for d_0 throughout. Now choose the pairs, ray characters and slopes by Theorem 12.30. Prescribe the first Frobenius sufficiently close to g_* for the two determinant valuations in B_i to agree at both selected Frobenius elements, for all i. This is an open condition because the finitely many specified determinants are nonzero.

For a fixed T_i, form the polynomial matrix of Proposition 12.22, allowing ramification at all the pairs, retaining the normalization and the fixed coefficient-place equations. Make a second matrix with the equations of Theorem 12.30 at the later pairs only. Both matrices represent the indicated cocycles also at the points of Lemma 12.31. Indeed, the actions there are genuine modulo ℓ^M and trivial on the same group H used to form the finite quotient in Proposition 12.22. Its proof including the elementary divisor calculation applies verbatim.

At the origin the length for the second matrix is at most B_i. With all the equations it has the bound from Theorem 12.30. Dropping the equations at the first pair adds at most the sum of the two normalized determinant valuations there, by Lemma 12.31 at $y = 0$. Indeed the quotient injects through its two tame values into the two matrix kernels on the finite coefficient modules, each of length bounded by its determinant valuation. Select a column-size minor of the second matrix attaining its length at the origin. Restrict this polynomial to the line $X_{w_0} = Y$, $X_j = s_{ij} Y$ and call it $P^0(Y)$. It has $v(P^0(0)) \leq B_i$. Define

$$P^1(Y) = \prod_{j \neq w_0} \prod_{\phi = \phi_j, (\phi_j^c)^{-1}} \det((1+Y)T_i(\phi) - I).$$

Each factor has degree r_i with unit leading coefficient. Hence $v_\rho(P^1) \leq 2 r_i d_0 \rho$, and $v_\rho(P^0) \leq v(P^0(0))$. There is a single algebraic y with $v(y) = \rho$ at which both polynomials attain their Gauss valuations. To see this, write $Y = \varpi_\rho U$ with $v(\varpi_\rho) = \rho$, divide each polynomial by a coefficient of least valuation, and avoid the finitely many roots of the two resulting nonzero residue polynomials and zero in $\overline{\mathbb{F}}_\ell$. A unit lift of the selected residue gives the required y.

At this point on the line, forgetting the later equations increases the length by at most $v(P^1(y))$. The quotient injects by their left sides into the kernels of the matrices in Lemma 12.31, and each kernel has normalized length at most its determinant valuation. The group still satisfying the equations has length at most $v(P^0(y))$ by its chosen minor. Choose a column-size minor P_i of the first matrix attaining its length at this point x_i. We have proved

$$v(x_{i,j}) \geq \rho, \qquad v(P_i(x_i)) \leq B_i + 2 r_i d_0 \rho.$$

These are witnesses for the actual common prime set. For each signed power use the same witness and polynomial for that lattice.

Apply the polynomial specialization argument of Theorem 12.20. It depends on the inertia coordinates and their orders and does not require the earlier characters to vanish at the later Frobenius elements. The characters constructed here have exactly the required inertia coordinates, since each ramifies only at its own pair and takes value 1 at its chosen tame generator. We obtain roots ζ_j and one character $\vartheta = \prod_j \zeta_j^{\lambda_j}$. The first matrix at the point $(\zeta_j^s - 1)_j$ therefore has normalized kernel length at most $B_i + \varepsilon < M$ for the cocycle equations modulo ℓ^M. Here kernel length refers to the equations before adjoining $\ell^M I$, as in Proposition 12.22. Lemma 12.23 gives the divisible-coefficient assertion. The same minor works over every further finite coefficient extension, since its normalized valuation is unchanged. The inertia estimate is the last calculation of Theorem 12.20. □

Corollary 12.33 (The higher-rank part of the trace bound at spherical primes)**.** *On the shorter family of Corollary 12.10, take finitely many untwisted marked main summands as above, of rank r_i and with the specified squarefree or rank-one local types at the two old level primes. Assume their ramification away from ℓ is confined to those levels. Take a spherical coefficient prime in the common range of Corollary 12.16. At this node one twist and its first m powers and inverses give, for each main summand, the estimates in the notation of Theorem 45.11*

$$l_e = 0 \quad (0 \le e < t_i), \qquad \frac{\lambda_{T_i \otimes \vartheta^s}}{v_\pi(\ell)} \le (4r_i + 1) v_\ell(G_0) + \varepsilon.$$

Here the trace families have the hyperspecial level and fixed infinity type of Corollary 12.16 and contain the selected twisted main summand. The estimate is independent of the later auxiliary primes and their precision. For each ℓ one may take $\varepsilon = 2^{-\ell}$.

Proof. At one of the old level primes different from ℓ, take for g_* a full tame generator. At any place of the prescribed type the inertia spectrum excludes 1. The same holds at the conjugate inverse, by polarization and trivial cyclotomic inertia. Section 47.12 bounds each determinant valuation by $r_i v_\ell(G_0)$. All other old local invariant contributions in B_i have total normalized length at most $2r_i v_\ell(G_0)$, as in Theorem 12.30. The global congruence term has normalized length at most $v_\ell(G_0)$ by Corollary 12.26. The marked scalar and matrix hypotheses follow from Theorem 47.36. Together these verify the hypotheses and give the asserted uniform upper bound for B_i.

For the trace cocycles in $\mathcal{V}_{T_i \otimes \vartheta^s}$, the normalization is the same, because the twist is unramified at the original marked inertia element. Its local components are trivial above ℓ, so the fixed crystalline evaluation equations at these places are precisely those of the untwisted summand. They hold for the trace cocycles by the lattice lifting argument of Theorem 12.15, after choosing some finite precision for each such cocycle and scaling back to divisible coefficients. At the later auxiliary places of the trace construction the target is unramified and the cocycles vanish on the chosen tame generators, so they are unramified there. Thus the trace cocycles belong to the group bounded by Theorem 12.32. The scalar colengths vanish by Corollary 12.16. Finally the added errors are summable with weights $\log \ell$, since $\sum_{n \ge 2} 2^{-n} \log n < \infty$. □

This treats the Selmer length for the chosen twists in the indicated coefficient range. To obtain the integral period bound of Section 6.6 the twist must also control the ratios of the Hecke values in those same periods. At coefficient primes outside the common Fontaine–Laffaille range one still needs the quantitative comparison with the crystalline local equations.

13 Critical values and Selmer lengths on a common interval

13.1 Critical Hecke values at the twists used for Selmer groups

Fix a CM field E of Corollary 12.4 and write c for its conjugation. Use arithmetic Frobenius for ideal characters. Fix a complex embedding of the algebraic numbers and an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Write $v(\ell) = 1$. A character u in this subsection is a unitary algebraic Hecke character of E with $u^c = u^{-1}$. Its conductor $\mathfrak{f}_0$ is nontrivial, prime to ℓ, and invariant under c. At the integer $z \geq 1$ we require that the two ideal exponents of $\alpha(\mathfrak{a}) = u(\mathfrak{a})(N\mathfrak{a})^{-z}$ at each conjugate pair of embeddings are, in some order, $k_\sigma - z, -k_\sigma - z$, with $k_\sigma \geq z$. These are precisely the exponents obtained from the norm-one characters of weight $-k_\sigma$ and their inverses by pulling back along $x \mapsto x/\bar{x}$ and multiplying by N^{-z}. In particular α is critical at zero. In the notation $\beta - \alpha'$ for a critical infinity type, the exponents on the negative side have $\alpha' \geq 1$, and the others have $\beta \geq 0$.

For a set J of split primes containing at most one prime of each conjugate pair, disjoint from $\mathfrak{f}_0\ell$, put $\mathfrak{f}_J = \mathfrak{f}_0 \prod_{j \in J} jj^c$. The notation $L_{\mathfrak{f}}(z, u)$ omits all primes dividing $\mathfrak{f}$. Our ratio for a finite-order anticyclotomic character ψ of conductor dividing $\prod_{j \in J} jj^c$ is

$$R_J(u, z, \psi) = \frac{L_{\mathfrak{f}_J}(z, u\psi)}{L_{\mathfrak{f}_0}(z, u)}.$$

For use with a Galois character we identify its finite-order values with complex roots of unity using ι. We first construct integral coefficients on the ray class groups whose evaluations give these ratios up to one constant.

Lemma 13.1 (Keeping additional places split in the ray characters)**.** *In Theorem 12.30 fix any finite conjugation-stable set V of primes disjoint from S. The ray characters can all be taken trivial on the decomposition groups at V, with the same bound d_0 on the number of pairs.*

Proof. At each use of the idele construction in that theorem include V among the inverted primes T, and choose all the new pairs outside V. The extra local factors $E_v^\times$ of D_T are killed by the defining residue character. The Kummer generators are still units at the distinguished old inertia place in the first step. In each later step they are units at the first pair and at the old marked pair used in that step. Extracting their ℓ^N-th roots is unramified at those places. Hence the prescribed Frobenius elements still fix the Kummer extension in the proof of Theorem 12.30. Chebotarev permits the same choices with the extra finite exclusions. The primary Selmer conditions used to count the steps involve the original S. Inverting primes in the idele construction adds no allowed ramification to those Selmer groups. Their initial lengths and the bound d_0 are consequently the same. □

Proposition 13.2 (An integral distribution at all selected tame levels)**.** *Suppose $\ell \nmid |D_E|$. Fix an integral prime ideal $\mathfrak{c}$ away from $\mathfrak{f}_0\ell$ such that $A = N\mathfrak{c}\,\alpha(\mathfrak{c}) \neq 1$. For any of the collections $(\lambda_j)_{j \in J}$ constructed above with $\mathfrak{c}, \mathfrak{c}^c$ split in their character fields, put $H_J = (\mathbb{Z}/\ell^N\mathbb{Z})^J$. There is a constant $C \neq 0$ independent of J, N and integral elements $\Theta_J \in \overline{\mathbb{Z}}_\ell[H_J]$ such that, for every character ψ of H_J,*

$$\psi(\Theta_J) = \iota(CL_{\mathfrak{f}_J}(z, u\psi)). \tag{*}$$

On the right, ψ is pulled back to ideals through the λ_j. The argument of ι in this formula is algebraic. In particular $\Theta_\varnothing = CL_{\mathfrak{f}_0}(z, u)$ after applying ι to the product, and this value is nonzero.

Proof. We use the partial ray-class form of the Kings–Sprang integrality theorem. We spell out its hypotheses because a denominator depending on the auxiliary level would affect the

choice of N. For a critical ideal character χ of nonunit conductor $\mathfrak{f}$, let $L_{\mathfrak{f}}(\chi, 0, b)$ denote the partial value for a ray class b, including the values of χ in the sum over ideals. For the CM type determined by the negative exponents, fix the CM abelian variety with Betti lattice $\mathcal{O}_E$ and bases of the eigendifferentials on it and its dual. The theorem supplies the period factor D from these bases and the infinity type. For each integral representative $\mathfrak{b}$ of b, prime to $\mathfrak{f}\mathfrak{c}\ell$, it gives integrality at ι of

$$D\left(N\mathfrak{c}\,\chi(\mathfrak{c})L_{\mathfrak{f}}(\chi, 0, b) - L_{\mathfrak{f}}(\chi, 0, b[\mathfrak{c}])\right). \tag{1}$$

Such representatives exist by the ray class theorem. The only localizations in the partial-value formula beyond its base ring are at the modulus and at primes dividing $N(\mathfrak{b}\mathfrak{c})$. All are units at the specified coefficient place. This is Corollary 4.13 in the cited version of the paper. [20]

For clarity, the CM data for D can be fixed before varying $\mathfrak{f}$. The existence theorem of complex multiplication defines the CM variety for the indicated lattice and CM type over a number field after choosing a polarization. It has good reduction at the selected place after a finite extension. Indeed semistable reduction gives a toric part whose rational character group, if nonzero, would carry a unital action of E. Its dimension is at most $[E : \mathbb{Q}]/2$, too small for a nonzero E-module. The action comes from extension of endomorphisms to the Néron model. Good reduction follows. After also containing the embeddings of E, the eigendifferentials split over the local integer ring since $\ell \nmid D_E$. Each eigensummand for the CM type, and each dual eigensummand of the appropriate type, is free of rank one. Choose bases there once. For each new level extend the ring to define the required prime-to-ℓ torsion sections. The old bases remain bases. Thus the nonzero complex scalar D used in (1) is identical at every level. This statement concerns a fixed coefficient place. Its scalar need not be bounded as E varies.

Apply (1) with $\mathfrak{f} = \mathfrak{f}_J$. To ensure an exact conductor, let ψ_0 be primitive of order ℓ^N in every coordinate, and take $\chi = \alpha\psi_0$. At each new prime only its own coordinate ramifies, with tame conductor exponent one. At every old prime ψ_0 is unramified. The conductor is therefore exactly $\mathfrak{f}_J$, including for $J = \varnothing$ with $\psi_0 = 1$. The infinity type is unchanged. On a ray class b a partial value of $\alpha\psi_0$ is the partial value of α times $\psi_0(b)$, first by the convergent series and then by continuation. Removing the common root of unity $\psi_0(b[\mathfrak{c}])$ from (1) shows that

$$d_b = D\left(AL_{\mathfrak{f}_J}(\alpha, 0, b) - L_{\mathfrak{f}_J}(\alpha, 0, b[\mathfrak{c}])\right)$$

is algebraic and integral at ι. Map each ray class b to $\lambda(b) = (\lambda_j(b))_j$ by reciprocity. Set $\Theta_J = \sum_b \iota(d_b)[\lambda(b)]$. Evaluating and reindexing the second sum gives $D(A - \psi(\mathfrak{c})^{-1})L_{\mathfrak{f}_J}(\alpha\psi, 0)$. The finite local character at $\mathfrak{c}$ is trivial by construction. Since $\alpha = uN^{-z}$, this proves (*) with $C = D(A - 1)$. The proof involves no division by the size of a ray class group.

It remains to verify nonvanishing and the interpretation of the absolute value. For real $s > 1$, conjugate unramified Euler factors in $L_{\mathfrak{f}_J}(s, u\psi)$ have positive product. At a conjugation-fixed prime the value is 1 or -1, so its factor is positive as well. The product converges absolutely. At $s = 1$ the classical analytic continuation of Hecke L-functions makes both $L_{\mathfrak{f}_J}(s, u\psi)$ and $L_{\mathfrak{f}_J}(s, (u\psi)^2)$ holomorphic there, since their nonzero angular infinity types rule out a norm character. For $s > 1$ the product of $\zeta_{E,\mathfrak{f}_J}(s)^3$, $|L_{\mathfrak{f}_J}(s, u\psi)|^4$, and $|L_{\mathfrak{f}_J}(s, (u\psi)^2)|$ is at least one. Its logarithm is a sum over prime powers with numerators $3 + 4\cos t + \cos(2t) = 2(1 + \cos t)^2$. A zero of the first Hecke value at one would force that product to tend to zero, since the zeta function has a simple pole. The value at one is thus positive by continuity. In particular the ratios R_J agree with the ratios of absolute values at every integer in question. □

Lemma 13.3 (The Euler factors along the first ray character)**.** *Suppose an old inertia element g_* away from ℓ has $u_\ell(g_*) \neq 1$, where u_ℓ is the avatar with the prescribed ideal values at*

arithmetic Frobenius. Write

$$b = v(\Theta_\varnothing), \qquad d = v(u_\ell(g_*) - 1), \qquad \beta = b + 2d.$$

On a set J from Theorem 12.30, choose the first Frobenius sufficiently close to g_* modulo ℓ^M for u_ℓ. Represent Θ_J by the polynomial

$$P_J(X) = \sum_{h \in H_J} (\Theta_J)_h \prod_{j \in J} (1 + X_j)^{[h_j]}, \qquad 0 \le [h_j] < \ell^N.$$

If $0 < \rho \le 1$ is rational and $\beta + 2|J|\rho < M \le N\rho$, this polynomial has a witness x with $v(x_j) \ge \rho$ and $v(P_J(x)) \le \beta + 2(|J| - 1)\rho$.

Proof. Write j_0 for the first prime. At augmentation, omitting j_0, j_0^c multiplies $\Theta_\varnothing$ by $(1 - a_0 q_0^{-z})(1 - a_0^{-1} q_0^{-z})$, with $a_0 = u_\ell(\phi_{j_0})$ and $q_0 = Nj_0$. Since $q_0 \equiv 1 \bmod \ell^N$, these two factors agree modulo ℓ^M with $1 - u_\ell(g_*)^{\pm 1}$. Their valuations are both $d < M$. Thus $P_{\{j_0\}}(0)$ has valuation β.

Put $Z = 1 + Y$ on the j_0-coordinate and put all other $X_j = 0$. For $Z^{\ell^N} = 1$, the value of the corresponding character at arithmetic Frobenius at every later j is Z, by the choice of λ_{j_0}. Removing each pair j, j^c therefore contributes

$$(1 - a_j q_j^{-z} Z)(1 - a_j^{-1} q_j^{-z} Z^{-1}), \qquad a_j = u_\ell(\phi_j), \quad q_j = Nj.$$

This Euler deletion follows from (*) because the scalar there is fixed. Multiply each displayed expression by Z, and take the product $B(Y)$ of the resulting quadratics over the later primes. Each has unit leading coefficient, since a_j, q_j are units. For $h = |J| - 1$, the polynomial

$$Z^h P_J(Y, 0, \dots, 0) - P_{\{j_0\}}(Y) B(Y)$$

vanishes at all the distinct roots of $Z^{\ell^N} - 1$. Division by this monic polynomial has integral quotient and zero remainder.

Use the Gauss valuation at radius $v(Y) = \rho$. The second term has valuation at most $\beta + 2h\rho$, by the constant coefficient of $P_{\{j_0\}}$, the leading coefficient of B, and multiplicativity. The modulus $Z^{\ell^N} - 1$ has Gauss valuation at least $N\rho$. Indeed it factors as Y times the product of the N successive geometric sums of length ℓ, each of valuation at least ρ by the binomial calculation in Lemma 12.31, also valid for the Gauss valuation. The congruence and $v_\rho(Z^h) = 0$ now give $v_\rho(P_J(Y, 0, \dots, 0)) \le \beta + 2h\rho$. Choosing Y of valuation ρ avoiding the finitely many roots of the reduced polynomial on the residue circle attains this valuation, as in Theorem 12.32. □

Theorem 13.4 (One twist for Selmer lengths and critical Hecke values)**.** *In Theorem 12.32 suppose $\ell \nmid D_E$. Fix finitely many (u, z) as above, each with finite conductor prime to ℓ, with $u_\ell(g_*) \ne 1$ at the same old inertia element as in that theorem. For every $m \ge 1$ and $\varepsilon, \eta_0 > 0$, its bounds $B_i + \varepsilon$ for the Selmer groups and η_0 at the new inertia groups hold for one twist ϑ for which, at every $0 < |s| \le m$,*

$$\max\{0, v(\iota(R_J(u, z, \vartheta^s)))\} \le 2v(u_\ell(g_*) - 1) + \varepsilon. \tag{2}$$

Here J is the actual auxiliary prime set of that twist. For the ramified critical pairs on the shorter fields of Corollary 12.33, take a full tame generator of the chosen old place w_* away from ℓ. The right hand side is then at most $2v_\ell(Nw_* - 1) + \varepsilon$.

Proof. Choose one smoothing prime $\mathfrak{c}$ outside S and all old conductors. For each character prescribe Frobenius sufficiently close to g_* for the character $u_\ell\kappa^{1-z}$, where κ is cyclotomic. Its value at g_* is $u_\ell(g_*)$ since the inertia is away from ℓ. Continuity and Chebotarev in a finite common quotient therefore give $A \neq 1$ for every pair at the same $\mathfrak{c}$. Exclude the conjugates of the old places too. Use Lemma 13.1 at $V = \{\mathfrak{c}, \mathfrak{c}^c\}$. The constants b, β for all pairs are now fixed finite numbers, before the order or number of the new characters is chosen.

Take an integer M exceeding every B_i, β by more than $1 + \varepsilon$. At this precision let d_0 be the bound of Theorem 12.30. Choose $0 < \rho \leq 1$ rational such that $2d_0 \max(1, \max_i r_i)\rho < \min(1, \varepsilon/2)$. Choose N with $N\rho \geq M$, large enough for the polynomial specialization in Theorem 12.20 at tolerance $\varepsilon/2$, tame bound η_0, and total witness bound

$$2m \left(\sum_i (B_i + 1) + \sum_{(u,z)} (\beta + 1) \right).$$

Construct the actual pairs with the first Frobenius close enough for every determinant and every u_ℓ. The minor for T_i constructed in Theorem 12.32 has witness valuation at most $B_i + 2r_i d_0 \rho$. For every (u, z), Lemma 13.3 provides on these very pairs a polynomial of witness valuation at most $\beta + 2d_0\rho$. Include each polynomial with every signed exponent s in a single application of the specialization theorem. Its proof uses only the orders and the independent inertia coordinates of the λ_j at this step. It yields one choice of roots ζ_j, hence $\vartheta = \prod_j \zeta_j^{\lambda_j}$, with the required Selmer and tame bounds. Each prescribed power ramifies at every new pair. Moreover the characters λ_j were differences $\xi_j - \xi_j^c$ of idele characters, so the product is pulled back along $x \mapsto x/\bar{x}$ from a finite-order character of the norm-one torus.

At the selected roots the Hecke polynomial is $\vartheta^s(\Theta_J)$, of valuation at most $\beta + \varepsilon$. Equation (*) at J and at the empty level shows that its quotient by $\Theta_\varnothing$ is precisely ιR_J. Subtracting b proves (2). At a chosen old place the given tame character is nontrivial and its order divides $Nw_* - 1$. If $\xi \neq 1$ is such a root, the identity $\prod_{\omega^{Nw_*-1}=1,\ \omega\neq 1}(1-\omega) = Nw_* - 1$ and integrality of every factor give $v(1 - \xi) \leq v_\ell(Nw_* - 1)$. This proves the final assertion. □

In (2) the normalization of the CM periods cancels individually for each field and each critical pair. The choice $\varepsilon = 2^{-\ell}$ is thus available throughout the stated coefficient range. The comparison in Section 6.6 still requires the bound for the full integral projected theta period with its prescribed local tests and the local cohomology loss at coefficient primes outside the common weight range.

13.2 The local cohomology loss on a fixed interval of weights

Let $K/\mathbb{Q}_\ell$ be any finite extension, $L/\mathbb{Q}_\ell$ a finite coefficient field, and $\mathcal{O}$ its integer ring. Fix a G_K-stable free $\mathcal{O}$-lattice T, and write $V = T[1/\ell]$, $A = V/T$. Allow a fixed finite Galois extension K'/K. Assume that V is crystalline over K' with all its filtration jumps in an integer interval I containing zero. The interval bounds the jumps at every embedding, including all coefficient embeddings after restriction of scalars. We obtain a bound independent of the size of an auxiliary family of crystalline lattices and the precision of their torsion quotients.

A finite ℓ-primary $G_{K'}$-module is called torsion crystalline in I if it is a quotient of a lattice in a crystalline $\mathbb{Q}_\ell$-representation with jumps in I. This property is preserved by submodules, quotients and finite direct sums. For submodules, take their preimage in a lattice surjecting onto the given finite module. The preimage has finite index in that lattice and spans the same rational representation.

Write $T_n = T/\ell^n T$, $\mathcal{O}_n = \mathcal{O}/\ell^n\mathcal{O}$. For a raw continuous cocycle $a : G_K \to T_n$ let $U_n(a)$ be the extension on $T_n \oplus \mathcal{O}_n$ with action

$$g(v, t) = (gv + t\, a(g), t).$$

Write C_n for the set of these cocycles for which $U_n(a)$ restricted to $G_{K'}$, considered over $\mathbb{Z}_\ell$, is torsion crystalline in I. Send a into $Z^1(K, A)$ by dividing its values by ℓ^n modulo T. Finally let $Z_f(K, T)$ consist of the integral raw cocycles whose rational classes lie in the Bloch–Kato group $H^1_f(K, V)$.

Theorem 13.5 (Finite error and a criterion using two precisions)**.** *The images of C_n form an increasing union C, an $\mathcal{O}$-submodule of $Z^1(K, A)$, and $C[\ell^n] = C_n$ under the specified identification. Its maximal divisible subgroup is the image C_f of $Z_f(K,T)[1/\ell]$ in $Z^1(K, A)$. In particular $F = C/C_f$ is finite. Let $R = \operatorname{rank}_{\mathbb{Z}_\ell} Z_f(K, T)$. For $n \geq 1$,*

$$\log_\ell |C_{n+1}| - \log_\ell |C_n| = R \quad \Longleftrightarrow \quad \ell^n F = 0.$$

At any such n, $\log_\ell |F| = \log_\ell |C_n| - nR$. All the groups here concern the fixed tuple (K, K', T, I).

Proof. Addition of cocycles uses the direct sum of two extensions, pullback by the diagonal of their quotients, and pushout by addition on the two kernels. Multiplication by $a_0 \in \mathcal{O}$ is pushout by a_0 on the kernel. Each operation uses subquotients of sums of the original modules and of $T_n, \mathcal{O}_n$, so preserves the torsion crystalline condition. To pass from n to $b \geq n$, pull back the extension along $\mathcal{O}_b \to \mathcal{O}_n$ and push out along $T_n \to T_b$, $x \mapsto \ell^{b-n}x$. The resulting cocycle is $\ell^{b-n}a$. This proves the increasing-union assertion. Conversely suppose a member coming from precision b is killed by ℓ^n with $b \geq n$. Its upper right entries at precision b lie in $\ell^{b-n}T_b$. In U_b restrict the first summand to $\ell^{b-n}T_b$, leaving its second summand intact. In this submodule the elements $(0, t)$ with $t \in \ell^n\mathcal{O}_b$ are fixed and form a submodule. Quotienting by it gives exactly U_n for the original cocycle valued in $A[\ell^n]$. This proves the identity $C[\ell^n] = C_n$, including the direction in which the representing precision decreases.

In particular $C[\ell]$ is finite. Indeed there are finitely many raw cocycles into T_1. Each gives a homomorphism to the finite affine group with translation group T_1 and linear group the image of G_K on T_1. Local fields have finitely many extensions of bounded degree inside a fixed algebraic closure. Through each resulting finite quotient there are only finitely many maps. The Pontryagin dual of the discrete ℓ-primary group C is therefore a finitely generated $\mathbb{Z}_\ell$-module. In detail, its quotient modulo ℓ is dual to $C[\ell]$, and lifts of generators generate the compact dual by topological Nakayama. One can see the last assertion by passing to the quotient by the closed span of those lifts. It equals its own ℓ-multiple and has no nonzero finite

ℓ-group quotient, hence is zero. The structure theorem over $\mathbb{Z}_\ell$ now gives a finite group modulo the maximal divisible subgroup of C.

To identify that subgroup take the Tate module $\varprojlim_n C[\ell^n]$ under multiplication by ℓ. In upper right coordinates the transition maps are reductions $T_{n+1} \to T_n$. A compatible family thus gives a continuous integral $z : G_K \to T$, with $U_n(z \bmod \ell^n)$ torsion crystalline in I at K' for every n. The lattice on $T \oplus \mathcal{O}$ defined by z has these reductions. The crystalline limit theorem of Liu, with the proof of Gao and Liu, makes its rational representation crystalline over K'. To apply the theorem, forget to $\mathbb{Z}_\ell$, twist the whole lattice so the interval starts at zero in the Hodge–Tate convention used there, and use the fixed width of the interval at all n. The underlying rank is finite. [21, 22]

Over K' both ends of the extension are crystalline. Exactness of the crystalline period functor on crystalline representations shows that a lift of the quotient generator exists in the invariant periods of the extension. Equivalently, the rational class of z maps to zero over K' with coefficients in $B_{\mathrm{cris}} \otimes_{\mathbb{Q}_\ell} V$. This vanishing descends to K. After subtracting a coboundary, a cocycle zero over $G_{K'}$ factors through $\mathrm{Gal}(K'/K)$ with values in the $G_{K'}$-invariants. Averaging over this finite group in a $\mathbb{Q}_\ell$-vector space gives a coboundary. Hence $z \in Z_f(K, T)$. Conversely such a z splits the extension over B_{cris} already over K. Over K' the two ends have full crystalline periods. The splitting and these periods give full crystalline periods for the middle term. Its jumps remain in I by exactness of the de Rham filtration. Its integral reductions consequently belong to C_n. For coefficients of degree greater than one, the extension over $\mathbb{Q}_\ell$ has one quotient basis vector for each $\mathbb{Q}_\ell$-basis vector of L. Splitting the vector belonging to 1 is equivalent to splitting them all by L-linearity.

We have identified the Tate module with $Z_f(K, T)$, with its maps to $C[\ell^n]$ given by $z \mapsto z/\ell^n \bmod T$. By the structure theorem the images of these projections are exactly the ℓ^n-torsion of the maximal divisible subgroup. Their union is C_f as claimed. The kernel of $Z_f(K, T)[1/\ell] \to Z^1(K, A)$ is $Z_f(K, T)$ itself, since a rational finite cocycle taking integral values lies in that lattice. Write the elementary divisors of F over $\mathbb{Z}_\ell$ as $\ell^{a_1}, \dots, \ell^{a_b}$. The same structure theorem gives

$$\log_\ell |C_n| = nR + \sum_{j=1}^{b} \min(n, a_j).$$

Taking first differences proves the assertion about two precisions. □

Proposition 13.6 (Independence of the coefficient extension)**.** *For a finite extension of coefficient rings $\mathcal{O}'/\mathcal{O}$ the finite quotient for $T' = T \otimes_{\mathcal{O}} \mathcal{O}'$ is $F \otimes_{\mathcal{O}} \mathcal{O}'$. In particular*

$$\Delta(K, K', T, I) = \frac{\mathrm{length}_{\mathcal{O}} F}{v_\pi(\ell)}$$

is invariant under finite coefficient extension, where π is a uniformizer and $v_\pi(\pi) = 1$.

Proof. Choose an $\mathcal{O}$-basis of $\mathcal{O}'$. For an allowed cocycle over $\mathcal{O}'_n$ first pull back its extension to the copy of $\mathcal{O}_n$ generated by 1 in the quotient. This is an injection because $\mathcal{O} \cap \ell^n \mathcal{O}' = \ell^n \mathcal{O}$. Push out the kernel along any coordinate functional $T'_n \to T_n$ in the chosen basis. The resulting extensions belong to the original torsion crystalline class by the subquotient property. Thus each coordinate belongs to C_n. Conversely scalar extending any allowed extension gives, on restriction to $\mathbb{Z}_\ell$, a finite direct sum of copies of the original one, since $\mathcal{O}'$ is free over $\mathcal{O}$. Multiplying by the basis scalars and adding the extensions proves $C'_n = C_n \otimes_{\mathcal{O}} \mathcal{O}'$. Taking the increasing union gives the claim for C. The same basis argument on rational cocycles split over B_{cris} gives the equality for C_f, hence for the quotient by flatness. Both its length and $v_\pi(\ell)$ are multiplied by the relative ramification index. This proves the formula. □

Corollary 13.7 (A bound uniform in the auxiliary levels on a fixed interval)**.** *Consider the matrix families of Theorem 45.11 on an actual period field E. At every $w \mid \ell$ suppose all local members of these families and the target become crystalline over the same fixed finite Galois extension K'_w/E_w with jumps in I_w, where $0 \in I_w$. These choices may depend on the field and the node and are made independently of auxiliary levels away from ℓ. At arbitrary precision one has*

$$\frac{l_e}{v_\pi(\ell)} \le \sum_{w\mid\ell} \Delta(E_w, K'_w, \mathcal{O}(-e), I_w), \qquad 0 \le e < t. \tag{3}$$

For the higher-rank lattices satisfying Theorem 12.32, the length of the trace cocycles for each of its selected twists satisfies

$$\frac{\lambda_{T_i\otimes\vartheta^s}}{v_\pi(\ell)} \le B_i + \varepsilon + \sum_{w\mid\ell} \Delta(E_w, K'_w, T_i, I_w). \tag{4}$$

When the data are spherical as in Corollary 12.16, one can take $K'_w = E_w$ without its numerical condition $2H \le \ell - 2$. The finite bounds then apply on the same fields and the same nodes for weights of any width. On any one finite interval and any fixed finite set of targets, they are uniform over the auxiliary families and precision.

Proof. The graph construction of Lemma 12.14 needs only the matrix relations. At each w its rational lattice for the lifted extension is a sum of the given representations and the trivial quotient. It is crystalline over K'_w in I_w. After reduction and pushout onto the target, the resulting extension is torsion crystalline there, being a subquotient of a finite direct sum with the target lattice. The local raw cocycle thus belongs to C_n. Map its image in $C[\ell^n]$ to F. The kernel consists exactly of reductions of $Z_f(E_w, T)$ at this precision, by the Tate module description in Theorem 13.5. For precision π^j dividing ℓ^n, the same pullback and pushout embed the values into $A[\ell^n]$. A rational finite cocycle whose image is killed by π^j becomes integral when multiplied by π^j, giving the same kernel description at that precision. By Lemma 12.27 these are exactly the integral local evaluation equations. The quotient measuring l_e therefore injects into the direct sum of the indicated finite groups, proving (3).

A divisible-coefficient raw trace cocycle takes values at finite precision by compactness. The same maps to F are compatible with increasing the precision. At all $w \mid \ell$ the selected twists are trivial, so the local groups for the main target are those for T_i, after adjoining coefficient values of the characters. Proposition 13.6 applies. The kernel of all the maps satisfies the coefficient-place equations. The earlier unramified and normalization arguments in Corollary 12.33 apply also here. The kernel lies in the group of Theorem 12.32, proving (4). In the spherical case the local-global compatibility and weight calculation in the proof of Corollary 12.16 precede its use of the Fontaine–Laffaille width and give crystallinity and the bounded interval directly. On a finite interval take the maximum over its finitely many relevant groups for each fixed set of coefficient primes. For primes in the common Fontaine–Laffaille range the original trace loss bound from Corollary 12.16 applies. □

Proposition 13.8 (A nonzero defect for wide intervals)**.** *For $\ell > 2$ and any finite unramified $K/\mathbb{Q}_\ell$, let $T = \mathbb{Z}_\ell$ with trivial action and take $K' = K$. Set $a = (\ell-1)\ell^{m-1}$, $m \ge 1$. If I contains $[-a, 0]$, then F has an element of order ℓ^m.*

Proof. In the crystalline sum $\mathbb{Q}_\ell(\kappa^a) \oplus \mathbb{Q}_\ell$ with basis e_1, e_2, use the lattice spanned by e_1 and $e_2 + \ell^{-m}e_1$. It is stable since every ℓ-adic unit has a-th power congruent to 1 mod ℓ^m. Modulo ℓ^m both diagonal characters are trivial. The upper right entry is the homomorphism

$$g \longmapsto \frac{\kappa(g)^a - 1}{\ell^m} \pmod{\ell^m}.$$

These matrices give a member of C_m, since the displayed lattice has jumps $0, -a$. Inertia over K maps onto $\mathbb{Z}_\ell^\times$ under κ, as the cyclotomic tower is totally ramified and K is unramified. At an inertia element with $\kappa(g) = 1 + \ell$, the upper right entry is a unit. Indeed the binomial theorem gives $v_\ell((1+\ell)^{\ell-1} - 1) = 1$, and raising a principal unit of depth at least one to the ℓ-th power increases its depth by exactly one for odd ℓ. Thus the cocycle in $A[\ell^m]$ has an inertia value of order ℓ^m. Every member of C_f for the trivial target is unramified by Lemma 12.11. Its class in F has the asserted order. □

The numerical loss required in Section 6.6 concerns growth as the period intervals enlarge. The finite group in (3) is independent of precision, but its size can grow with the weight interval, as the last proposition shows. A quantitative estimate at the weights of the theta chain and the full integral projected-period comparison are still required.

13.3 The critical-value comparison at primes dividing the discriminant or old conductor

In constructing a twist we may multiply every partial Hecke value at every auxiliary level by a single nonzero scalar. The constant may depend on the old conductor, the infinity type and the chosen coefficient place. Its valuation disappears on dividing by the untwisted value. We use this freedom to extend Proposition 13.2 to the coefficient places dividing the discriminant of E or one of the two old levels. The argument uses the integral Eisenstein–Kronecker class before its projection to a CM eigenspace.

Lemma 13.9 (A denominator for the moment at a torsion section)**.** *Let B be an abelian scheme over a local integer ring $R \subset \overline{\mathbb{Q}}$ of residue characteristic ℓ. Let x be a section killed by the positive integer n. Use the Poincaré bundle with connection on B and the formal completion of the universal vector extension of its dual at zero. Write $\widehat{\mathcal{P}}^{\natural}$ for its completed coefficient sheaf, and H for the cotangent module of this universal extension at zero. For $b \geq 0$ the characteristic-zero moment of order b at x, multiplied by n^b, defines an integral map*

$$x^*\widehat{\mathcal{P}}^{\natural} \longrightarrow \mathrm{TSym}^b H.$$

Here TSym^b *denotes symmetric tensors, with integral divided powers. The map commutes with automorphisms fixing x.*

Proof. For the endomorphism $[n]$ of B the functoriality of the Poincaré bundle gives, on every finite infinitesimal neighborhood, an integral map $[n]_{\#} : \mathcal{P}^{\natural,(j)} \to [n]^*\mathcal{P}^{\natural,(j)}$. This is Theorem 2.8 of Kings–Sprang. Pulling back at x gives a map to the fiber at zero, since $[n]x = 0$. Compose this integral map with the integral moment mom_0^b at zero of Definition 2.6. On the generic fiber the definition of the torsion splitting in Corollary 2.9 and Definition 2.10 gives the commutative identity

$$\mathrm{mom}_0^b \circ [n]_{\#,x} = \mathrm{TSym}^b(d[n]^*) \circ \mathrm{mom}_x^b = n^b \,\mathrm{mom}_x^b.$$

Indeed the torsion splitting first applies $[n]_{\#,x}$ and then inverts $[n]_{\#,0}$ over the fraction field. The moment at zero is functorial under the induced map on the formal group. Multiplication by n acts as n on its cotangent module. The composite on the left is defined over R even when n is divisible by ℓ. All its maps are functorial for automorphisms fixing x. [20] □

Theorem 13.10 (Integral partial values with fixed old ramification)**.** *In the notation of Section 13.1, allow any coefficient prime ℓ. Assume that the conductor $\mathfrak{f}_0$ of u contains places of two distinct rational residue characteristics. For every J keep all new primes away from ℓ and the old conductor. Take the smoothing prime $\mathfrak{c}$ of Proposition 13.2, with $N\mathfrak{c}$ prime to $\ell N\mathfrak{f}_J$. There is a single nonzero scalar D', independent of J, N and of the ray classes, such that the numbers*

$$D'\left(AL_{\mathfrak{f}_J}(\alpha, 0, b_0) - L_{\mathfrak{f}_J}(\alpha, 0, b_0[\mathfrak{c}])\right), \qquad A = N\mathfrak{c}\,\alpha(\mathfrak{c}),$$

are algebraic and integral at ι for every ray class b_0. Here $\alpha = uN^{-z}$ as before. In particular (*) in Section 13.1 holds with $C = D'(A-1)$ on the same systems of split ray characters.

Proof. Put $\mathfrak{f} = \mathfrak{f}_J$ and choose a representative $\mathfrak{b} \in b_0$ prime to $\ell\mathfrak{f}\mathfrak{c}$, with $N\mathfrak{b}$ prime to $\ell N(\mathfrak{f}\mathfrak{c})$. For example the ray class theorem gives such a prime by excluding the finitely many primes over the latter rational primes. Let $\mathcal{A}$ be the CM abelian variety for the fixed type and lattice $\mathcal{O}_E$. For a fractional ideal $\mathfrak{a}$ let $\mathcal{A}(\mathfrak{a})$ be its Serre tensor by $\mathfrak{a}$, with complex period lattice $\mathfrak{a}\Omega$ in the compatible uniformizations of Kings–Sprang, Section 4.2. Use $B = \mathcal{A}(\mathfrak{f}\mathfrak{b}^{-1})$. The point $x = \Omega \bmod \mathfrak{f}\mathfrak{b}^{-1}\Omega$ has annihilator ideal $\mathfrak{f}$. In fact $ax = 0$ for $a \in \mathcal{O}_E$ means $a\mathfrak{b} \subseteq \mathfrak{f}$, which

is equivalent to $a \in \mathfrak{f}$. After a finite extension, use good models at the coefficient place as in Proposition 13.2 and define the torsion sections there. The ideal isogenies extend over the local integer rings by the Néron mapping property.

Write $D_{\mathfrak{c}} = B[\mathfrak{c}]$. It is finite étale, its order is $N\mathfrak{c}$, and its isogeny and dual isogeny have degree prime to ℓ. The section x is disjoint from $D_{\mathfrak{c}}$ also in the special fiber. Indeed $\mathfrak{f}_0$ has a prime divisor of residue characteristic $p \neq \ell$, and the p-primary component of x is nonzero by its exact annihilator. It stays nonzero under specialization on finite étale p-power torsion. No point of $D_{\mathfrak{c}}$ has such a component. The subgroup $\Gamma = \{e \in \mathcal{O}_E^{\times} : e \equiv 1 \bmod \mathfrak{f}\}$ fixes x and preserves the trace-zero function on $D_{\mathfrak{c}}$ which is $N\mathfrak{c} - 1$ at zero and -1 elsewhere. This is the smoothing function $f_{[\mathfrak{c}]}$ in Section 4.4 of Kings–Sprang. The group Γ is torsion free. Indeed the norm of $1 - \zeta$ for a nontrivial root of unity is either a unit or supported at a single rational prime, by the cyclotomic polynomial at one. The congruences at the two old characteristics exclude such ζ. Dirichlet's unit theorem gives Γ rank $g - 1$ for $g = [E : \mathbb{Q}]/2$. In the evaluation use the subgroup $\Gamma' = \{\epsilon \in \Gamma : \epsilon \equiv 1 \bmod \mathfrak{c}\}$. It fixes each point of $D_{\mathfrak{c}}$ individually. Its index $e_J = [\Gamma : \Gamma']$ divides $|(\mathcal{O}_E/\mathfrak{c})^{\times}| = N\mathfrak{c} - 1$, a number fixed before the auxiliary levels are chosen.

Write the infinity type of α as $\beta - \alpha'$ as in Section 13.1, and let $a = |\alpha'| - g$ and $b = |\beta|$. Apply the general integral construction of Kings–Sprang, Theorem 2.20 and Definitions 2.21–2.24, up to pullback at x of the a-th derivative of the class. Up to this step the construction takes place on an abelian scheme with the finite étale smoothing kernel, and uses its action by Γ', its Poincaré bundle and its connection. The CM idempotents and the moment at x have not entered. Apply Lemma 13.9 with $n = N\mathfrak{f}$, which annihilates x. The resulting integral cohomology class belongs to

$$H^{g-1}(\Gamma', \mathcal{T}(B)), \qquad \mathcal{T}(B) = \mathrm{TSym}^a \omega_B \otimes \mathrm{TSym}^b H_B \otimes \bigwedge^g \omega_B.$$

Here ω_B denotes the invariant differentials. Over the fraction field it is n^b times the unprojected characteristic-zero class in Definition 2.24. This identification uses precisely the moment identity just proved. Its integral coefficient module is finite free over the local integer ring. The valuation $v_\ell(n) = v_\ell(N\mathfrak{f}_0)$ is fixed as J varies. [20]

We next control the projection of this class. Over a number field containing the embeddings of E, make the CM projection of Section 2.4 onto the single prescribed component. It projects H using its rational CM splitting and selects the prescribed symmetric tensors and determinant. Trivialize the resulting line by bases of eigendifferentials and the orientation of the CM type, as in Proposition 2.27. Before evaluating on a group cycle this is a linear functional on $\mathcal{T}(B)$ over the fraction field. It is Γ-equivariant to the trivial module because the selected character of a unit of Γ is trivial. This also follows by evaluating the infinity type of α on any unit congruent to one modulo its conductor.

There is one power ℓ^k making all these linear functionals integral with the compatible period bases of Section 4.3. To see this write $\mathfrak{f} = \mathfrak{f}_\ell \mathfrak{m}$ with $\mathfrak{f}_\ell$ supported above ℓ. It is the fixed ℓ-part of the old conductor. First use the fixed variety $\mathcal{A}(\mathfrak{f}_\ell)$ and choose its rational bases by transport from $\mathcal{A}$. Over a good integral model multiply the single functional on its finite free tensor module by a power ℓ^k so that it is integral. For every new B the diagram

$$\mathcal{A}(\mathfrak{f}_\ell) \xrightarrow{[\mathfrak{b}]} \mathcal{A}(\mathfrak{f}_\ell \mathfrak{b}^{-1}) \xleftarrow{[\mathfrak{m}]} \mathcal{A}(\mathfrak{f}_\ell \mathfrak{b}^{-1} \mathfrak{m}) = B$$

has both degrees prime to ℓ. These arrows induce integral isomorphisms on differentials, on the module H for the universal vector extension, and on the displayed tensor modules. Indeed the inverse is given by an isogeny divided by its prime-to-ℓ degree on the linear modules. The arrows intertwine the action of $\mathcal{O}_E$, its rational projectors, and the transported bases. Over $\mathbb{C}$

they are induced by the inclusions of the corresponding period lattices. Composition with the fixed arrow $[\mathfrak{f}_\ell]$ gives exactly the transport through $[\mathfrak{f}]$ and $[\mathfrak{b}]$ of Section 4.3. Hence the same ℓ^k works, including after all base extensions used for the sections. This proves the denominator bound for the rational projection even at $\ell \mid D_E$.

Apply the scaled functional on cohomology and evaluate on the oriented integral fundamental class of the free abelian group Γ'. This is the top exterior product of an oriented basis of Γ'. Over $\mathbb{C}$ the projected evaluation before multiplication by $n^b\ell^k$ is the smoothed Eisenstein–Kronecker value of Corollary 3.28. We give the orbit count for its conversion to partial values. Write $\mathfrak{a} = \mathfrak{f}\mathfrak{b}^{-1}$. The coset $1 + \mathfrak{c}^{-1}\mathfrak{a}$ is the disjoint union of $1 + t + \mathfrak{a}$ over $t \in \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$. Each coset is Γ'-stable since Γ' fixes x and each smoothing torsion point. The smoothed sum is therefore $N\mathfrak{c}$ times the sum for $1 + \mathfrak{a}$ minus the sum for $1 + \mathfrak{c}^{-1}\mathfrak{a}$, both taken modulo Γ'. The two full cosets in this difference are also Γ-stable and contain no zero, since $\mathfrak{b}\mathfrak{c}$ is prime to $\mathfrak{f}$. Multiplication by units acts freely on their nonzero elements. The summand is invariant under Γ by the infinity type. Each of the two sums modulo Γ' is thus e_J times the corresponding sum modulo Γ. The identities hold first in the region of convergence of the Eisenstein series and then at the critical point by analytic continuation. Formula (4.1.3) and the period computation in Section 4.3 give the resulting scalar, up to the fixed orientation sign, as

$$\frac{e_J D}{\alpha(\mathfrak{b}\mathfrak{c})}\left(AL_{\mathfrak{f}}(\alpha, 0, b_0) - L_{\mathfrak{f}}(\alpha, 0, b_0[\mathfrak{c}])\right).$$

Here $D \neq 0$ is the period factor for the original bases and infinity type, independent of $\mathfrak{f}, \mathfrak{b}$. Indeed formula (4.1.3) weights the first coset by $\alpha(\mathfrak{b})$ and the second by $\alpha(\mathfrak{b}\mathfrak{c})$. It applies to an ideal character defined modulo $\mathfrak{f}$. Equivalently one may twist it by a primitive auxiliary character to give exact conductor, then remove its constant value on each ray class as in Proposition 13.2. All comparisons in this paragraph are over the fraction field or over $\mathbb{C}$. [20]

The multiplier $\alpha(\mathfrak{b}\mathfrak{c})$ is an algebraic ℓ-adic unit. Indeed a positive power of the ideal is principal with generator congruent to one modulo $\mathfrak{f}_0$ and a unit at every place above ℓ. The ideal character on that principal ideal is a product of integral powers of conjugates of the generator. Choose $D' = (N\mathfrak{c} - 1)\ell^{k+b\,v_\ell(N\mathfrak{f}_0)}D$. The quotient of this multiplier by $e_J\ell^k n^b D$ is $(N\mathfrak{c}-1)/e_J$ times a rational ℓ-adic unit. It is integral at ℓ. The integral evaluation just proved gives exactly the assertion about the partial values. Summing the coefficients in $\overline{\mathbb{Z}}_\ell[H_J]$ and evaluating at a character gives (*) by the reindexing in Proposition 13.2. □

Corollary 13.11 (The same critical ratios at all coefficient primes)**.** *The conclusion on $R_J(u, z, \vartheta^s)$ in Theorem 13.4 holds also when ℓ divides D_E or $N\mathfrak{f}_0$, provided the old conductor of each u contains primes in two distinct rational characteristics. Retain the other hypotheses on the lattices and the distinguished old inertia element away from ℓ. In particular for the pairs ramified at both marked levels the cost in (2) is still at most $2v_\ell(Nw_* - 1) + \varepsilon$ for any admissible such w_*.*

Proof. Choose the smoothing prime by the same finite Frobenius conditions away from the finitely many rational primes of the old conductors, and exclude its rational residue characteristic in selecting the new split pairs. Finite exclusions do not change the Chebotarev argument or d_0. By Theorem 13.10 we now have integral polynomials with the same Euler deletion identity. The new augmentation $b = v(\Theta_\varnothing)$ is finite and fixed before M, N. The proof of Lemma 13.3 uses the critical character only at the new primes and at g_*, all away from ℓ. The specialization in Theorem 13.4 applies with this b, and subtracts it on dividing by the original value. No term involving k, n, the conductor or D_E survives this division. At least one of the two old characteristics differs from ℓ, and the asserted inertia cost follows there when the common marking hypotheses hold. □

This extends the control of the critical-value factors in the twisted periods. The two outstanding estimates concern the quantitative size of the local defects as the weights grow and the full projected theta periods of Section 6.6.

13.4 Heights of the critical factors in the chain of lifts

The twists used for integral projections can depend on the coefficient prime and the embedding. This matters when collecting the critical values into a determinant. For a family $y = (y_{\ell,\iota})$ of nonzero algebraic numbers set

$$H_{\mathrm{fin}}(y) = \sum_{\ell} \log \ell \, \sup_{\iota} \max\{0, -v_\ell(\iota y_{\ell,\iota})\}, \qquad v_\ell(\ell) = 1.$$

The sum is the supremum over finite sets of primes. A bound $H_{\mathrm{fin}} \le h$ gives the height bound with multiplier 1 for a family of twisted periods. Indeed the multiplier has absolute value 1 under every complex embedding, and the displayed local suprema are valid exponents for the finite-place inequalities. For algebraic numbers only the restriction of an embedding to $\overline{\mathbb{Q}}$ enters.

Lemma 13.12 (The contribution of a tame generator)**.** *Let ξ have finite order $D > 1$. For every embedding at ℓ,*

$$v_\ell(1-\xi) = b_\ell(D) := \begin{cases} 1/\varphi(\ell^a), & D = \ell^a, \quad a \ge 1, \\ 0, & D \text{ has a prime divisor different from } \ell. \end{cases}$$

Consequently $\sum_\ell b_\ell(D) \log \ell \le \log 2$.

Proof. Reduction is injective on roots of unity of order prime to ℓ, by separability and Hensel's lemma. Roots of ℓ-power order reduce to 1. When D has a nontrivial prime-to-ℓ part, the reduction of ξ therefore differs from 1. If $D = \ell^a$, all the primitive D-th roots give the same valuation. In fact $(1-\xi^j)/(1-\xi) = 1 + \cdots + \xi^{j-1}$ reduces to $j \ne 0$ for $1 \le j \le D$ prime to ℓ. Multiplication over these primitive powers gives $\Phi_{\ell^a}(1) = \ell$, proving the formula. At most one prime contributes, and $\log \ell/\varphi(\ell^a) \le \log \ell/(\ell-1) \le \log 2$. The last inequality follows from $2^{n-1} \ge n$ for integers $n \ge 2$. □

Theorem 13.13 (The height of every ramified critical ratio)**.** *At a node of the shorter family of Corollary 12.10, fix one marked place w_i over each of the two rational level primes p_i, $i = 0, 1$. Take the ramified critical pairs: their tame characters are nontrivial at every marked place, their old conductors are supported on these places and their conjugates, and their integers z satisfy $1 \le z \le t$ and $z \le k_\tau \le 4b$ at each infinite place, in the notation of Section 13.1. For the Hecke character u of such a pair write $D_i(u) > 1$ for its tame order at w_i. Use w_0 when $\ell \ne p_0$ and w_1 when $\ell = p_0$. One may include any of the simultaneous Selmer tests of Theorem 12.32 satisfying its hypotheses for these chosen inertia generators.*

For every $m \ge 1$ and every sequence of positive numbers ϵ_ℓ with $\sum_\ell \epsilon_\ell \log \ell \le \delta$, there is a family $\vartheta_{\ell,\iota}$ with auxiliary modulus prime to ℓ and the prescribed Selmer and new-inertia bounds of Theorem 13.4, with error ϵ_ℓ in the Selmer bounds. Simultaneously for all the pairs and all $0 < |s| \le m$, the inverse of the family $R = R_J(u, z, \vartheta_{\ell,\iota}^s)$ satisfies

$$H_{\mathrm{fin}}(R^{-1}) \le 2 \sum_{\ell \ne p_0} b_\ell(D_0(u)) \log \ell + 2 b_{p_0}(D_1(u)) \log p_0 + \delta \le 4 \log 2 + \delta.$$

If both orders have at least two distinct prime divisors, then $\max(0, v_\ell(\iota R)) \le \epsilon_\ell$ at every place.

Proof. The integers z, the lists of exponents and the tame residue characters range over finite sets. For fixed such data the quotient of two pulled-back Hecke characters is trivial at infinity and on all finite local unit groups, hence factors through the finite ideal class group of E. Thus the list of pairs needed for all ratios is finite. At each (ℓ, ι) fix a tame generator at the selected

w_i. It takes every prescribed residue character to a root of exactly its tame order, since local reciprocity maps tame inertia onto the cyclic residue unit group in the tame abelian quotient. The place is away from ℓ, so the algebraic weight adds no inertia there. The order is preserved by ι. Apply Theorem 13.4 with this generator and the entire list, using Corollary 13.11 at the primes of bad conductor or discriminant. Its proof with an empty list of Selmer tests gives the assertion for the critical pairs alone. The chosen twist works for the whole list at once. Its critical ratio is positive and algebraic, including at $z = 1$, by Section 13.1. With either sign of the twist the same Euler factors at the auxiliary primes are omitted.

The pointwise estimate (2) now gives $\max(0, v_\ell(\iota R)) \le 2b_\ell(D_i(u)) + \epsilon_\ell$. Take the supremum over the embeddings and sum. The bound on each of the two old contributions follows from Lemma 13.12. If both orders have two distinct prime factors then the formula for b_ℓ gives zero for each old contribution at every prime. □

Corollary 13.14 (Arbitrarily small total height for the chain ratios)**.** *On the shorter fields put $Q = (q_0 d)^{h+6}$, where $18480 \mid q_0$ and $2^h = m^{22}$, as in Section 47.12. Use the prescribed residue character ω_w of order Q at each marked place. Consider the characters of the successive lifts in their geometric progression $\nu_j = \nu_0 \xi^j$, $1 \le j \le m$, where ξ has tame part ω_w and angular weight of magnitude $\Delta = 2r^8$ at every infinite place. Write $t = 5r$, with the prescribed $r \ge 2$. For $1 \le i < j \le m$ form the critical factors for $u_{ij} = (\nu_j/\nu_i)^{-1}$. For each (ℓ, ι) put*

$$P_{\ell,\iota} = \prod_{1 \le i < j \le m} \prod_{z=1}^{t} R_J(u_{ij}, z, \vartheta_{\ell,\iota}^{-(j-i)}).$$

Given any $\delta > 0$, the simultaneous twists in Theorem 13.13 can be chosen so that

$$H_{\mathrm{fin}}\Big(\big((N_J^{e/2} P_{\ell,\iota})^{-1} \big)_{\ell,\iota} \Big) \le \delta \qquad (e \in \mathbb{Z}),$$

where N_J is the positive norm of the auxiliary modulus for that twist. The same choice controls the individual critical factors of the main pairs, whose tame parts are ω_w^j for $1 \le j \le m$. The bound δ can be used at every node of each common interval of Corollary 12.4.

Proof. The local character of order Q is obtained by taking the Q-th power of a character of order Q^2 of the cyclic group $\mathbb{F}_{p_i}^\times$, since $Q^2 \mid p_i - 1$. The angular weights of u_{ij} have magnitude $(j-i)\Delta \ge t$, so every displayed integer satisfies the criticality condition. The argument for these factors also follows by adding their finite list directly in Theorem 13.4, which requires no upper cutoff on the magnitudes of the angular weights.

For $1 \le a \le m$, the order of $\omega_w^{\pm a}$ is $Q/\gcd(Q, a)$. Both 2^{h+6} and 3^{h+6} divide Q and both exceed m. Hence 2 and 3 both divide this order. The last assertion of Theorem 13.13 applies at every coefficient prime to every factor of the product, and to every individual main pair. Set $L = t\binom{m}{2}$ and use $\epsilon_\ell = \delta\, 2^{-\ell}/((1+L)(1+\log \ell))$. The positive part of the valuation of a product is at most the sum of the positive parts. Thus the supremum of that positive part for $P_{\ell,\iota}$ is at most $L\epsilon_\ell$, and its weighted sum is at most δ. The norm N_J is an ℓ-adic unit by construction. The positive real square root used in $N_J^{e/2}$ is algebraic, and its valuation at every embedding above ℓ is zero by squaring. This proves the claim also for negative e. The order argument and the choice of the sum bound apply at every node with the same δ. □

The estimate concerns the Hecke values in the chain determinant. The operator clearing the integral projection and the inner products of projected test forms in Section 6.6 require their own estimates on these fields.

13.5 Local lifting with a separate weight interval at each embedding

The automorphic weights need not have the same sign at two embeddings of one completion. The integral lifting argument can use a different shift at each embedding of an unramified local field. This identifies the individual completions contributing to the trace bound even when some other completion above the same coefficient prime has a long interval.

Theorem 13.15 (Lifting at the labelled widths)**.** *Let $K/\mathbb{Q}_\ell$ be unramified, $\ell > 2$, and take the lattices T, U_x of Lemma 12.14 over the ring of integers $\mathcal{O}$ of a finite coefficient field. Suppose that all their rational representations are crystalline. Fix embeddings of the coefficient field and of K in $\overline{\mathbb{Q}}_\ell$. At each $\tau : K \hookrightarrow \overline{\mathbb{Q}}_\ell$ let $[A_\tau, B_\tau]$ contain zero and all labelled filtration jumps of these representations. Suppose*

$$B_\tau - A_\tau \le \ell - 1 \quad \text{for every } \tau, \qquad B_{\tau_0} - A_{\tau_0} \le \ell - 2 \quad \text{for at least one } \tau_0.$$

For any uniformizer π of $\mathcal{O}$ and any $n \ge 1$, every cocycle $z : G_K \to T/\pi^n T$ satisfying the matrix relations of that lemma lifts, as a cocycle, to T with crystalline rational extension. The conclusion also holds for any such cocycle whose extension, with quotient $\mathcal{O}/\pi^n$, is an $\mathcal{O}$-linear subquotient of torsion reductions of crystalline lattices in these same labelled intervals.

Proof. We first enlarge the coefficient field to split K and retain the ideal generated by the original π^n as precision. Put $S = \mathcal{O}_K \otimes_{\mathbb{Z}_\ell} \mathcal{O}$. It is a product of copies of $\mathcal{O}$ indexed by the embeddings τ. The Witt Frobenius permutes the factors cyclically. Denote the next index by $\sigma\tau$. In the convention in which the cyclotomic character has jump -1, we need a crystalline character of jump $j_\tau = -A_\tau$ at each τ. We construct its lattice D.

Set $h = \ell - 1$. In the τ-component of a rank-one Fontaine–Laffaille module take a basis element d_τ of filtration degree j_τ. Thus the filtration contains this whole component through that degree and is zero on it above that degree. Define the divided Frobenius by

$$\phi_i(d_\tau) = \ell^{j_\tau - i} d_{\sigma\tau} \quad (0 \le i \le j_\tau).$$

The relations $\phi_i = \ell\phi_{i+1}$ on the next filtration and generation by the images follow directly. Here $0 \le j_\tau \le B_\tau - A_\tau \le h$, and $j_{\tau_0} < h$. The module belongs to the unipotent category at weight h. To check this, recall that its excluded quotients are the nonzero modules whose whole filtration is in degree h. Our component at τ_0 has zero filtration in that degree. Strictness forces the τ_0-component of any such quotient to be zero. In the quotient the images of ϕ_h generate, since each lower divided Frobenius is a multiple of ϕ_h. Moving around the cyclic permutation of components gives zero in every component. The covariant integral Fontaine–Laffaille comparison therefore gives a rank-one crystalline lattice D with the stated jumps. We use also its exactness, full faithfulness, closure of the torsion image under subquotients, and the lattice comparison in the unipotent weight-$\ell - 1$ range. [18, §2.3]

Tensor the given extension and its presenting lattices with D. All their rational jumps now belong to $[0, h]$, and at τ_0 they are all strictly below h. Each presenting lattice belongs to the comparison category. Indeed its rational representation can have no nonzero quotient that is an unramified representation twisted by the character of constant jump h. Such a quotient would require jump h at τ_0, since the de Rham filtration on crystalline representations is strict on quotients. This verifies the extra hypothesis in the endpoint lattice comparison. For the matrix relations the required presentation is the graph lattice of Lemma 12.14 together with T. In that lemma one may use π^n throughout, by the same elementary divisor argument. Its rational constituents are copies of the given representations and the trivial line. For the more general assertion use the stipulated presentation. Tensoring over $\mathcal{O}$ with the free line preserves subquotients, so the twisted torsion extension is in the comparison image.

Let M be the module corresponding to $T \otimes D$, and put subscripts n on reductions at the chosen precision. The filtered extension of D_n by M_n is strict by exactness in the Fontaine–Laffaille category. Lift $d_\tau \bmod \pi^n$ to v_τ in filtration j_τ in the middle module. This splits its underlying module componentwise. In each filtration degree $i \le j_\tau$, the τ-component is the sum of $\mathrm{Fil}^i(M_n)_\tau$ and the line generated by v_τ. In higher degrees it equals $\mathrm{Fil}^i(M_n)_\tau$, by strictness. Thus $\phi_{j_\tau}(v_\tau) = v_{\sigma\tau} + a_\tau$ for some $a_\tau \in (M_n)_{\sigma\tau}$. Lift a_τ freely to $\widehat{a}_\tau \in M_{\sigma\tau}$. Adjoin an integral generator $\widehat{v}_\tau$ in degree j_τ in each component, with

$$\phi_i(\widehat{v}_\tau) = \ell^{j_\tau - i}(\widehat{v}_{\sigma\tau} + \widehat{a}_\tau) \quad (0 \le i \le j_\tau).$$

The images generate M and project onto every quotient line, so they generate the new module. Its filtration in degree h is zero at τ_0: this holds for M by its labelled jumps and for the added line because $j_{\tau_0} < h$. The preceding quotient argument shows that the new module is unipotent. It reduces to the given filtered extension with both end identifications. Applying the integral comparison, undoing the twist, and adjusting an integral section by a lift of a coboundary gives a cocycle lifting z at every group element.

Finally, for a finite extension $\mathcal{O}'/\mathcal{O}$ of coefficient rings, 1 extends to an $\mathcal{O}$-basis of $\mathcal{O}'$ since its reduction modulo π is nonzero. Project onto this basis vector. Applying the projection to the lifted $T \otimes \mathcal{O}'$-valued cocycle gives an integral lift with values in T. Rationally the operation is restriction of coefficients, pullback on the quotient along the inclusion of the original coefficient field, and pushout on the submodule along the projection. Direct sums and subquotients preserve crystallinity. This gives the claim over the original field. □

Corollary 13.16 (The remaining completions in the trace estimate)**.** *In* (3) *and* (4)*, form* $[A_\tau, B_\tau]$ *separately for each trace family and its target by taking the minimum and maximum of their jumps and zero. At a spherical unramified completion* E_w *of odd residue characteristic, omit the term at* w *if these labelled widths satisfy Theorem 13.15. If every completion above* ℓ *can be omitted, then* $l_e = 0$ *for the scalar targets in question and* $\lambda_{T_i \otimes \vartheta^s}/v_\pi(\ell) \le B_i + \epsilon_\ell$ *for the selected main targets. This holds at every auxiliary level with the prescribed infinity type, for the same twists as in Theorem 13.13.*

Proof. The spherical compatibility and the calculation of the jumps in Corollary 12.16 apply at E_w before any width restriction. Each local matrix relation holds on the restriction of a global trace cocycle. The twists are trivial on G_{E_w}. Apply Theorem 13.15 at this completion. In the maps used to prove (3) and (4) the image there is zero, since all integral crystalline evaluation equations hold on the reduction of an integral crystalline cocycle. The injection into the sum over the other completions consequently has the same kernel as before. The numerical Selmer bound on this kernel was imposed at the same time as the critical-value inequalities. The infinity type determines the overlying lists of jumps independently of the auxiliary level, as in Corollary 12.16. □

Proposition 13.17 (Counting the completions containing a wide label)**.** *Let* $E/\mathbb{Q}$ *be one of the abelian period fields. At an unramified odd spherical prime* ℓ *fix an identification of its complex and* ℓ*-adic embeddings on the algebraic numbers. Write* $\mathcal{B}$ *for the set of embeddings of* E *where the labelled width is greater than* $\ell - 2$*, using the jumps of a given trace family and its target. The contribution to the two inequalities in the corollary is supported at completions whose Frobenius orbits meet* $\mathcal{B}$*. If* f_ℓ *is the order of Frobenius in* $\mathrm{Gal}(E/\mathbb{Q})$*, the sum of the local degrees of these completions is at most* $\min([E : \mathbb{Q}], f_\ell|\mathcal{B}|)$*. An orbit containing a width at most* $\ell - 2$ *and having all widths at most* $\ell - 1$ *can also be omitted.*

In particular, suppose the permitted jumps at a label τ *are in*

$$[-\eta, \eta] \ \cup \ s_\tau[S_\tau, S_\tau + W], \qquad s_\tau \in \{-1, 1\}, \qquad S_\tau, W, \eta \ge 0.$$

One may count only the orbits meeting labels for which $\max(2\eta, \eta + S_\tau + W) > \ell - 2$.

Proof. The decomposition group acts on the embeddings into $\overline{\mathbb{Q}}_\ell$ with one orbit for each completion. Here the orbits are precisely the cycles of the Frobenius permutation, each of size f_ℓ, since the field is Galois and unramified. An orbit disjoint from $\mathcal{B}$ satisfies the lifting theorem. Each remaining orbit contains at least one member of $\mathcal{B}$, so the sum of their sizes has the asserted bound. The endpoint assertion uses the second width condition in Theorem 13.15. For $s_\tau = 1$ the two displayed intervals and zero lie between $-\eta$ and $\max(\eta, S_\tau + W)$. For $s_\tau = -1$ reflect both intervals through zero. The width estimate follows in both cases without combining different signs from different embeddings. □

These omissions apply to the trace cocycles actually entering the determinant. The lengths at the remaining completions, the residual groups in Section 6.6, and the full projected inner products still require quantitative bounds on the common intervals.

13.6 The sum of the marked Selmer lengths on a common interval

The marked representations in the shorter family have odd rank, and the cyclotomic string also has odd length. Taking a determinant in a congruence with a cyclotomic twist exploits both parities. It restricts the primes contributing to the global term even when the trace of an individual matrix is zero. The other terms come from nontrivial roots of unity at the two original levels. We estimate their sum over coefficient primes before taking any new trace levels.

Proposition 13.18 (The determinant restriction on the trace ideal)**.** *Let $E = \mathbb{Q}(\mu_{q_1}, \sqrt{-d})$ be as in Proposition 50.5. Let T be an integral polarized representation as in Theorem 12.25, of odd rank h with odd string length t. For its trace ideal I_t, with $v_\ell(\ell) = 1$, one has*

$$a_\ell(t) \le v_\ell(I_t) \le a_\ell(ht),$$

where a_ℓ is the explicit cyclotomic valuation of Proposition 50.5. In particular $v_\ell(I_t) = 0$ for every $\ell \nmid q_1 d$. The bounds hold at every coefficient embedding and for finite-order anticyclotomic twists.

Proof. Let J_u be the ideal generated by $1 - \kappa(g)^u$, $g \in G_E$, in the coefficient ring $\mathcal{O}$. Integral traces give $I_t \subseteq J_t$. To obtain the other inclusion, write π for a uniformizer and take any $j \ge 1$ such that $I_t \subseteq \pi^j\mathcal{O}$. At this precision T and $T(t)$ have equal traces on the group. They are isomorphic by the full-matrix-span argument in Theorem 12.25. Taking the determinant of the intertwining identity gives

$$\det T(g) \equiv \kappa(g)^{ht} \det T(g) \pmod{\pi^j} \qquad (g \in G_E).$$

The determinants are units. Thus $J_{ht} \subseteq \pi^j\mathcal{O}$ at every such precision. Since $\mathcal{O}$ is a discrete valuation ring, it follows that $J_{ht} \subseteq I_t$, also if I_t is the unit ideal or the zero ideal. The cyclotomic image contains an open group of principal units, so $J_{ht} \ne 0$. The two inclusions and Proposition 50.5, applied to the odd integers t and ht, give the bounds. A character twist multiplies each generator of I_t by a unit. Its anticyclotomicity preserves the polarization. □

Lemma 13.19 (The primes dividing an inertia order)**.** *For an integer $M \ge 1$ and $y = \max(2, \lceil \log M \rceil)$,*

$$\sum_{\ell \mid M} \frac{\log \ell}{\ell - 1} \le 4 \log y + 1.$$

If $\rho \ne 1$ is any root of unity of order dividing M, then $v_\ell(1 - \rho) \le \mathbf{1}_{\ell \mid M}/(\ell - 1)$.

Proof. The second assertion follows from Lemma 13.12. For $\ell \le y$, at least $\lfloor y/\ell \rfloor \ge y/(2\ell)$ factors of $y!$ are divisible by ℓ. Taking valuations and then logarithms gives

$$\sum_{\ell \le y} \frac{\log \ell}{\ell - 1} \le 2 \sum_{\ell \le y} \frac{\log \ell}{\ell} \le \frac{4}{y} \log(y!) \le 4 \log y.$$

Each $\ell > y$ has $\ell - 1 \ge y$, and the product of the distinct primes dividing M divides M. Their remaining contribution is at most $(\log M)/y \le 1$. □

Theorem 13.20 (A uniform bound for the marked Selmer groups in odd rank)**.** *Use the finitely many distinct node data on one shorter period interval of Corollary 12.4. At a node x write $E_x = \mathbb{Q}(\mu_{q_{1,x}}, \sqrt{-d_x})$, $N_x = q_{1,x} d_x$, and $p_{x,0}, p_{x,1}$ for its levels. At each (x, ℓ, ι) take a finite list of untwisted marked main lattices of the following kind. The rational representation V is de Rham at all $w \mid \ell$ and has polarization $V^c \simeq V^\vee(1 - t)$, with odd rank $h \le R$ and odd string length $t \le U$. As in Corollary 12.33, we use the allowed scaled squarefree or rank-one*

spectra excluding 1 *at each of the common old marked places away from* ℓ*, and the primitive or rank-one type at some place above each old level prime for each lattice. All ramification away from* ℓ *is at the marked places. Put*

$$e_* = \max_x [E_x : \mathbb{Q}], \qquad N_* = \operatorname{lcm}_x N_x,$$
$$M_* = \prod_x \prod_{i=0}^{1} \prod_{j=1}^{R} (p_{x,i}^j - 1), \quad y_* = \max(2, \lceil \log M_* \rceil).$$

For a signed exponent $0 < |s| \le m_x$ *let* $b_\ell(T, s)$ *be the normalized length of the divisible Selmer group for* $T \otimes \vartheta_{x,\ell,\iota}^{\,s}$ *with the integral coefficient-place equations and the ramification allowed in Theorem 12.32. For any* $\delta > 0$*, the twists used in the critical ratios can be chosen with*

$$\sum_\ell (\log \ell) \sup_{x,\iota,T,s} b_\ell(T, s) \;\le\; \log\bigl(N_* \operatorname{lcm}(1, \dots, RU)\bigr) + (2e_* + 2)R\,(4 \log y_* + 1) + \delta.$$

The theorem concerns the Selmer groups with the stated integral equations at every coefficient prime. The same bound applies to the raw main trace lengths, normalized by $v_\pi(\ell)$*, over those data for which Corollary 13.16 applies at every coefficient completion, uniformly in the later auxiliary trace levels and precisions.*

Proof. Choose one marked place over each level prime as in Theorem 13.13. For g_* take a full tame generator at the first of these lying away from ℓ. For each lattice a possibly different place of primitive or rank-one type over that same rational prime gives the integral matrix span and a scalar inertia element with $y^2 - 1$ a unit, by Theorem 47.36. The common element g_* has no eigenvalue 1 on any lattice by the hypothesis at every old mark. Its conjugate inverse has the same eigenvalues, by polarization and the triviality of κ on inertia away from ℓ. Thus the common and individual inertia conditions in the twisting theorem hold simultaneously. The unit $y - 1$ makes the normalization of a cocycle at the individual scalar element unique in its cohomology class, since changing it by a coboundary changes its value there by $(y - 1)v$.

At a mark $w \nmid \ell$ above $p_{x,i}$ each scaled inertia eigenvalue ρ has order dividing $p_{x,i}^j - 1$ for some $1 \le j \le h$. Indeed an irreducible residue factor of degree j has its roots in $\mathbb{F}_{p_{x,i}^j}^\times$, since the level prime splits completely in E_x. Multiplication by a residue scalar leaves the root in that group. Naming the roots in characteristic zero preserves their orders. The rank-one character also has order dividing $p_{x,i} - 1$. Therefore for a full tame generator σ_w,

$$v_\ell(\det(1 - T(\sigma_w))) \le \frac{R}{\ell - 1}\, \mathbf{1}_{\ell \mid M_*}.$$

Here we multiplied the factors $1 - \rho$ and applied Lemma 13.19. The same bound holds for the inverse transpose, because the determinant of $T(\sigma_w)$ is a unit. On the finite Tate dual the action of σ_w is this inverse transpose. Its fixed vectors contain the invariants of the full decomposition group. The elementary divisors of the difference from the identity bound their normalized length at every precision by the displayed determinant valuation.

Take S in Theorem 12.32 to consist of the coefficient places and the specified old marked places with their conjugates. At most $2e_*$ old places occur. In the constant B_i of that theorem, their invariant groups and the two distinguished determinants together cost at most $(2e_* + 2)R\mathbf{1}_{\ell \mid M_*}/(\ell - 1)$. The other term of B_i is $v_\ell(I_t)$. By Proposition 13.18 and the explicit cyclotomic formula it is at most

$$v_\ell\bigl(N_* \operatorname{lcm}(1, \dots, RU)\bigr).$$

This follows since $ht \le RU$, and at any prime dividing N_x the conductor part of $a_\ell(ht)$ is at most $v_\ell(N_x)$.

Choose positive ϵ_ℓ with $\sum_\ell \epsilon_\ell \log \ell \le \delta$. At each node and embedding insert its entire finite list in Theorem 13.13. This supplies the same twist for these Selmer groups and the critical ratios. It bounds their normalized lengths by $B_i + \epsilon_\ell$ for all the signed powers. Its tame tolerance can also be chosen as in Corollary 50.10. All the pointwise majorants use the displayed interval data, so they still hold after taking the supremum. Factoring the fixed integer in the cyclotomic bound and applying Lemma 13.19 to M_* proves the inequality. At the indicated spherical coefficient completions, Corollary 13.16 puts the raw normalized main cocycles into this same Selmer group at each precision. This proves the final assertion independently of the later trace levels. □

The argument bounds the congruence and marked-inertia terms using only the fields, ranks and two original levels of the interval. To apply it to all trace cocycles one must also bound their defect in the local integral equations outside the labelled lifting range. The complementary-sign strict groups of Section 6.6 enter a different term of the period comparison.

14 References

[1] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., 2006, Chapters I and II. Book.

[2] C. Greither and C. D. Popescu, *An equivariant main conjecture in Iwasawa theory and applications*, J. Algebraic Geom. **24** (2015), 629–692. Authors' paper.

[3] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395. Original paper.

[4] NIST, *Digital Library of Mathematical Functions*, Section 25.11, formula 25.11.14. Hurwitz zeta function.

[5] J. S. Milne, *Class Field Theory*, version 4.03, 2020, Chapter V, Theorem 3.27. Course notes.

[6] C. A. Weibel, *The K-book*, Grad. Stud. Math. 145, AMS, 2013. Chapter VI, Section 8.

[7] B. Kahn, *The Quillen–Lichtenbaum conjecture at the prime 2*, Theorem 1. Author's paper.

[8] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[9] E. Bayer-Fluckiger, V. Emery and J. Houriet, *Hermitian lattices and bounds in K-theory of algebraic integers*, Doc. Math., Extra Vol. Merkurjev (2015), 71–83. Authors' paper.

[10] A. Mathew, *Torsion exponents in stable homotopy and the Hurewicz homomorphism*, Algebr. Geom. Topol. **16** (2016), 1025–1041. Original paper.

[11] B. W. Jordan, Z. Klagsbrun, B. Poonen, C. Skinner and Y. Zaytman, *Statistics of K-groups modulo p for the ring of integers of a varying quadratic number field*, Tunisian J. Math. **2** (2020). Theorems 2.5 and 5.1.

[12] J. S. Milne, *Class Field Theory*. Local and global Artin reciprocity and the correspondence with idele class quotients.

[13] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, 1997. Chapter 6, Stickelberger's theorem.

[14] H. Darmon, F. Diamond and R. Taylor, *Fermat's Last Theorem*, Theorems 2.17–2.19, especially the number-field formula in Theorem 2.19. Authors' text.

[15] J. S. Milne, *Algebraic Number Theory*, Theorem 8.31 (Chebotarev density theorem). Author's text.

[16] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progress in Mathematics **86**, Birkhäuser, 1990, 333–400, Corollary 3.8.4 and Example 3.9. Published chapter.

[17] J.-M. Fontaine and G. Laffaille, *Construction de représentations p-adiques*, Ann. Sci. École Norm. Sup. (4) **15** (1982), 547–608. Published paper.

[18] T. Gee, F. Herzig, T. Liu and D. Savitt, *Potentially crystalline lifts of certain prescribed types*, Section 2.3. Authors' paper.

[19] L. Guerberoff, *Modularity lifting theorems for Galois representations of unitary type*, Compos. Math. **147** (2011), 1022–1058. Published paper.

[20] G. Kings and J. Sprang, *Eisenstein–Kronecker classes, integrality of critical values of Hecke L-functions and p-adic interpolation*, Ann. of Math. (2) 202 (2025), 1–109. Published paper. Partial ray-class integrality, Corollary 4.13 of the authors' September 2024 text.

[21] T. Liu, *Torsion p-adic Galois representations and a conjecture of Fontaine*, Ann. Sci. Éc. Norm. Supér. (4) 40 (2007), 633–674. Article.

[22] H. Gao and T. Liu, Appendix B to H. Gao, *Breuil–Kisin modules and integral p-adic Hodge theory*, J. Eur. Math. Soc. 25 (2023), 3979–4032. Theorem B.0.1 and its corrected proof.