NONDEGENERACY AT AN EDGE

Prerequisites. Chapter 19: sources of a lattice (Problem 19.1.1), the integral forms $H(L) = \mathrm{Sym}^d(L^\vee)$ and their equivariance (Problem 19.1.2), and elementary divisors with witnesses and tests (Problems 19.2.1 and 19.2.2). Theorem 37.4.1 of Chapter 37, which states the nondegeneracy property in the form of [Adr, Thm. 12.11]. The Frobenius orbits and the classes of inert primes of Section 53.4. Unramified extensions of $\mathbb{Q}_p$, their Frobenius, and Teichmüller representatives [SeL, Ch. II, §§4–5]. Gaussian binomial coefficients.

In Chapter 19 the Hecke image at a vertex of the tree was computed directly. In the proof the vertex lies in the building of GL_k over a large unramified extension, and the image is controlled by a condition on one edge at a time. This chapter states that condition as the Lean formalization [Lean] has it, checks its formal properties in the smallest model, and shows why it can only hold thanks to the Frobenius twist. The theorems that establish it are stated at the end; their proofs are large and are not developed here.

40.1. Edges and their midpoints

Fix a prime $p \geq 5$ and an integer $\nu \geq 1$. Let W be the ring of integers of the unramified extension K of $\mathbb{Q}_p$ of degree ν, with residue field $\mathbb{F}_Q$, $Q = p^\nu$, and Frobenius σ. In the application ν is the length n_p of a Frobenius orbit, Section 53.4, and the formalization requires ν to be even. Let $\mathfrak{o} \supset W$ be a complete discrete valuation ring with a uniformizer ϖ such that $\varpi^2 = p$; in the formalization its residue field is $\mathbb{F}_{Q^2}$. We write v for the valuation of $\mathfrak{o}$, so $v(p) = 2$. For a W-lattice L we write $L_\mathfrak{o} = \mathfrak{o}L$.

Fix integers $k \geq 2$ and $1 \leq r < k$. For W-lattices $L'' \subset L$ in K^k, the pair $e = (L'' \subset L)$ is an *r-edge* if $pL \subset L''$ and $L/L'' \cong \mathbb{F}_Q^r$; its *source* is L'' and its *target* is L. Its *midpoint* is the $\mathfrak{o}$-lattice $M(e) = L''_\mathfrak{o} + \varpi L_\mathfrak{o}$.

Problem 40.1.1. The r-edges into L correspond to the subspaces of codimension r of L/pL, and the r-edges out of L'' to the r-dimensional subspaces of $p^{-1}L''/L''$. Each set has $\binom{k}{r}_Q \geq Q^{r(k-r)}$ elements. For $k = 2$, $r = 1$ this is $Q + 1$; for $k = 4$, $r = 2$, $Q = 5$ it is $806 \geq 625$.

Problem 40.1.2. $L''_\mathfrak{o} \subset M(e) \subset L_\mathfrak{o}$, and both quotients $M(e)/L''_\mathfrak{o}$ and $L_\mathfrak{o}/M(e)$ have length r over $\mathfrak{o}$. If L'' has a basis $g_1, \ldots, g_k$ with $L = L'' + Wp^{-1}g_1 + \cdots + Wp^{-1}g_r$, then $M(e)$ has the basis $\varpi^{-1}g_1, \ldots, \varpi^{-1}g_r, g_{r+1}, \ldots, g_k$.

40.2. Integral forms on an edge

To each lattice L the construction attaches an $\mathfrak{o}$-lattice $H(L)$ in a finite-dimensional representation V of $\mathrm{GL}_k(K)$ over the fraction field of $\mathfrak{o}$, with $H(gL) = gH(L)$. In the formalization V is a tensor product, over the positions $i \in \mathbb{Z}/\nu$, of dual Weyl modules of a dominant weight, twisted by σ^i; at the odd

Date: November 26, 2026.

positions the dual weight is used [Lean]. We work in the following model, for $k = 2$ and $r = 1$, which keeps the twist and drops the duals.

The model. Fix degrees $d_0, \dots, d_{\nu-1} \geq 0$. Let V be the space of functions $F(u_0, \dots, u_{\nu-1})$ on $(K^2)^\nu$, with values in the fraction field of $\mathfrak{o}$, that are homogeneous polynomials of degree d_i in u_i. For a lattice $L \subset K^2$ put

$$H(L) = \bigotimes_{i \in \mathbb{Z}/\nu} \operatorname{Sym}^{d_i}\big((\sigma^i L)^\vee\big) \otimes_W \mathfrak{o},$$

where $\sigma^i L$ is the image of L under σ^i applied to coordinates and Sym^{d_i} acts on the variable u_i. For $\nu = 1$ this is $\operatorname{Sym}^d(L^\vee) \otimes \mathfrak{o}$, as in Chapter 19. The *normalizing exponent* is $A = \sum_i d_i$. For $F \in V$ and $u \in K^2$, the *twisted value* is $F^\sigma(u) = F(u, \sigma u, \dots, \sigma^{\nu-1}u)$. The group $\mathrm{GL}_2(K)$ acts on V by $(gF)(u_0, \dots, u_{\nu-1}) = F((\sigma^0 g)^{-1}u_0, \dots, (\sigma^{\nu-1}g)^{-1}u_{\nu-1})$, where $\sigma^i g$ is g with σ^i applied to its entries, and on $V^\vee$ by the contragredient action.

For an edge e, put

$$R(e) = \varpi^{-A} H\big(M(e)\big), \qquad R'(e) = \varpi^{-A} H\big(M(e)\big)^\vee, \qquad \langle F, G\rangle = G(p^A F),$$

where $H(M(e)) = \bigotimes_i \operatorname{Sym}^{d_i}\big(((\sigma^i L'')_\mathfrak{o} + \varpi(\sigma^i L)_\mathfrak{o})^\vee\big)$, the duals now taken over $\mathfrak{o}$, $^\vee$ is the dual lattice in the dual space $V^\vee$, and $F \in V$, $G \in V^\vee$. Let $e = (L'' \subset L)$ be an edge, let g, g' be a basis of L'' with $L = L'' + Wp^{-1}g$, and let η, ξ be the dual basis of $L''^\vee$, so that $\eta(g) = 1$ and $\xi(g) = 0$. Let η_i, ξ_i be the corresponding basis of $(\sigma^i L'')^\vee$, and for $J = (j_0, \dots, j_{\nu-1})$ with $0 \leq j_i \leq d_i$ put $x_J = \prod_i \eta_i^{j_i} \xi_i^{d_i - j_i}$.

Problem 40.2.1. In the basis x_J,

$$H(L'') = \bigoplus_J \mathfrak{o}\, x_J, \qquad H(M(e)) = \bigoplus_J \varpi^{|J|}\mathfrak{o}\, x_J, \qquad H(L) = \bigoplus_J p^{|J|}\mathfrak{o}\, x_J,$$

with $|J| = \sum_i j_i$. Hence $R(e) = \bigoplus_J \varpi^{|J|-A}\mathfrak{o}\, x_J$.

Problem 40.2.2. $R(e)$ and $R'(e)$ are dual to each other under $\langle\ ,\ \rangle$: an element G lies in $R'(e)$ exactly when $\langle F, G\rangle \in \mathfrak{o}$ for every $F \in R(e)$, and conversely. In the basis dual to (x_J), $R'(e) = \bigoplus_J \varpi^{-A-|J|}\mathfrak{o}\, x_J^*$.

Problem 40.2.3. $H(L'') \subset R(e) \subset p^{-A}H(L)$, and $H(L)^\vee \subset R'(e)$.

Problem 40.2.4. Write $F \in V$ as $\sum_J f_J x_J$. The coefficient of the top monomial $\prod_i \eta_i^{d_i}$ is the twisted value $F^\sigma(g)$. Consequently, if $F \in \varpi^c R(e)$, then $v(F^\sigma(g)) \geq c$.

So $R(e)$ lies halfway between H of the source and $p^{-A}H$ of the target, and the top coefficient, which is the twisted value at the direction g in which the edge expands, is the one that $R(e)$ does not enlarge. In the formalization these are the lemmas on dual bases, inclusions and perfectness, proved for every dominant weight.

40.3. The condition

For an integer $t \geq 0$, a lattice L'' and a lattice L, put

$$N_t^{\mathrm{src}}(L'') = \varpi^{-t}H(L'') \cap \bigcap_{e \text{ out of } L''} R(e), \qquad N_t^{\mathrm{tgt}}(L) = \varpi^{-t}H(L)^\vee \cap \bigcap_{e \text{ into } L} R'(e).$$

Let $D \geq 0$ and $c_* \geq 0$ be integers and $0 \leq \kappa \leq 1$. The condition $\mathrm{LP}(r; t, D, \kappa, c_*)$ is: $c_* \geq 4(D+1)$, and for every lattice L there are

(i) r-edges $e_1, \dots, e_M$ into L, with sources $L_1'', \dots, L_M''$, and vectors $F_l \in N_t^{\mathrm{src}}(L_l'')$;
(ii) such that each F_l is *isolated*: $F_l \in \varpi^{c_*} R(e')$ for every edge $e' \neq e_l$ out of L_l'';
(iii) and an integer $n \geq (1-\kappa)\dim V$, an $\mathfrak{o}$-linear map $u\colon \mathfrak{o}^n \to N_t^{\mathrm{tgt}}(L)$ and an $n \times M$ matrix (μ_{jl}) over $\mathfrak{o}$, with $\sum_l \mu_{jl}\langle F_l, u(z)\rangle = p^D z_j$ for all $z \in \mathfrak{o}^n$ and all j.

This is the definition of [Adr, Def. 12.6], recalled before Theorem 37.4.1, in the form of the formalization. The parameter t is the *depth*, D the *denominator*, κ the *defect* and c_* the *isolation order*.

Problem 40.3.1. $R(ge) = gR(e)$, $R'(ge) = gR'(e)$, $N_t^{\mathrm{src}}(gL'') = gN_t^{\mathrm{src}}(L'')$ and $N_t^{\mathrm{tgt}}(gL) = gN_t^{\mathrm{tgt}}(L)$ for $g \in \mathrm{GL}_2(K)$, and $\langle gF, gG\rangle = \langle F, G\rangle$. Hence if (i)–(iii) hold for one lattice L, they hold for every lattice.

Problem 40.3.2. If $c_* \geq 4(D+1)$, then $\mathrm{LP}(r; t, D, 1, c_*)$ holds. If $\mathrm{LP}(r; t, D, \kappa, c_*)$ holds and $\kappa \leq \kappa' \leq 1$, then so does $\mathrm{LP}(r; t, D, \kappa', c_*)$. The set of κ for which $\mathrm{LP}(r; t, D, \kappa, c_*)$ holds is $[\kappa_0, 1]$ for some κ_0 in $\{1 - n/\dim V : 0 \leq n \leq \dim V\}$.

Problem 40.3.3. Given $F_1, \dots, F_M$, let $\Phi\colon N_t^{\mathrm{tgt}}(L) \to \mathfrak{o}^M$ be the map $G \mapsto (\langle F_l, G\rangle)_l$. Then (iii) holds with a given n exactly when at least n elementary divisors of Φ have valuation at most $2D$.

Problem 40.3.4. If $\mathfrak{o}' \supset \mathfrak{o}$ is a complete discrete valuation ring, finite over $\mathfrak{o}$, and $\mathrm{LP}(r; t, D, \kappa, c_*)$ holds over $\mathfrak{o}$ with ϖ, then it holds over $\mathfrak{o}'$ with the same ϖ, for the lattices $H(L) \otimes_{\mathfrak{o}} \mathfrak{o}'$.

The formalization defines the defect it uses at the primes of class I as the least κ for which the condition holds; by Problem 40.3.2 this least value exists and is attained. So the condition itself is never in doubt. What has content is how small its least defect is, and that is a statement about the isolated vectors.

40.4. Isolation needs the Frobenius twist

Let L'' have the basis $g = e_2$, $g' = e_1$, so that the edge $e = (L'' \subset L'' + Wp^{-1}e_2)$ is one edge out of L''. Let x, y be the coordinates dual to e_1, e_2.

Problem 40.4.1. The edges out of L'' other than e are $e'_\alpha = (L'' \subset L'' + Wp^{-1}(e_1 + [\alpha]e_2))$, for $\alpha \in \mathbb{F}_Q$, where $[\alpha]$ is the Teichmüller representative. The twisted value of a monomial $\prod_i x_i^{d_i - j_i} y_i^{j_i}$ at $e_1 + [\alpha]e_2$ is $[\alpha]^{\sum_i j_i p^i}$.

Problem 40.4.2. Suppose that the exponents $\sum_i j_i p^i$, for $0 \leq j_i \leq d_i$, are distinct and less than Q; this holds if $d_i \leq p-1$ for every i, and also if $d_0 < Q$ and $d_i = 0$ for $i \neq 0$. Then the map sending $F \in H(L'')$ to the function $\alpha \mapsto F^\sigma(e_1 + [\alpha]e_2) \bmod \varpi$ on $\mathbb{F}_Q$ is injective modulo $\varpi H(L'')$.

Problems 40.2.4 and 40.4.2 show that, under the hypothesis of Problem 40.4.2, a vector of $H(L'')$ that lies in $\varpi R(e'_\alpha)$ for every α has its top coefficients at the Q directions divisible by ϖ, and so lies in $\varpi H(L'')$. Pushing this further gives the following, which we state without proof.

Remark 40.4.1. Under the hypothesis of Problem 40.4.2, if $F \in \varpi^{-t} H(L'')$ lies in $\varpi^c R(e'_\alpha)$ for every $\alpha \in \mathbb{F}_Q$, then $F \in \varpi^c H(L'')$. Combined with Problems 40.2.3 and 40.2.2, and $c_* \geq 4(D+1) > 2D$, this shows that every isolated vector pairs into

$\varpi^{c_*}\mathfrak{o}$ with $N_t^{\mathrm{tgt}}(L)$, so that $\mathrm{LP}(1;t,D,\kappa,c_*)$ holds in the model only with $\kappa=1$. This includes the untwisted tree of Chapter 19 with $Q>d$, where Theorem 19.5.1 shows that the Hecke image itself is nondegenerate up to $p^{\lfloor \log_p d\rfloor}$ on all of the rank. *Status*: this observation is ours; it is not in the formalization, and we have not found it in the literature.

So without the twist the edge condition is a much stronger requirement than nondegeneracy of the image: it asks for witnesses at single edges, and a binary form of degree less than Q cannot be small at Q directions without being small everywhere. The twist removes this obstruction as soon as one degree reaches p.

Problem 40.4.3. Let $p=5$, $\nu=2$, $d_0=5$ and $d_1=4$. The form $F=y_0^5y_1^4-x_0^4y_0x_1^4$ lies in $H(L'')$, its twisted values $F^\sigma(e_1+[\alpha]e_2)$ vanish for all 25 elements $\alpha\in\mathbb{F}_{25}$, and $F^\sigma(e_2)=1$.

Thus the top coefficient of F vanishes at all the edges out of L'' except e, and is not small at e. We have not computed whether the full condition, with isolation of order c_*, holds in this example for some depth and denominator. In the formalization the weights at the top positions are of size a, far larger than p, and the orbit length $\nu=n_p$ is at least $x^{\varepsilon/4}$.

40.5. The two theorems

The formalization proves the condition with small defect at the primes of class I, in the two ranges of Theorem 37.4.1: $13\le p<p_*$, with edges of a large type $r\ge 2$, and $p_*\le p<X'$, with $r=1$. We use the notation of Section 37.4: a, b', the rank k, and a parameter $Y\ge 1$. The positions $i\in\mathbb{Z}/\nu$ that carry tops form a set $\mathcal{T}$; a dominant weight $\lambda=(\lambda_i)_{i\in\mathbb{Z}/\nu}$ has *base type* with parameters a_i,b_i and c if, for $i\in\mathcal{T}$, the first entry of λ_i is a_i, the last is $-b_i$, and the others have absolute value at most c, while for $i\notin\mathcal{T}$ every entry has absolute value at most c.

Theorem 40.5.1 (small primes)**.** *There is an absolute constant C with the following property. Let $p\ge 13$, $2\le r\le Y$, and let $\mathcal{T}$ satisfy the orbit conditions of the formalization, with parameters L_1,N_1,G', where N_1 is its window count and $N_1^2\le r|\mathcal{T}|$. Let λ have base type with $a+c\le a_i\le 2a-c$ and $0\le b_i\le c_0-2c$. Put $\Lambda=CN_1^2\log a$, and suppose*

$$\Lambda\le k,\quad N_1{+}3r\le k,\quad 256k^2|\mathcal{T}|Y^2\le p^{L_1-1},\quad C|\mathcal{T}|k^2\log_p a\le D,\quad 8(D{+}1)\le c_*,$$

$$Ck^3r^2|\mathcal{T}|p^{5G'}\big(c_*+r|\mathcal{T}|c_0+2r\nu c\big)Y\le a.$$

Then $\mathrm{LP}(r;t,D,C|\mathcal{T}|r^2k/Y,c_*)$ holds for every integer

$$t\ge Cr|\mathcal{T}|\Big(\frac{\Lambda a}{pk}+ap^{-L_1}+c_0+kp^{G'}\Big)+2r\nu c.$$

Status: proved in the formalization. It is used with $r=r_G=\lceil 8(h+2)/\varepsilon\rceil+1$, $h=2+8\varepsilon$; for $\varepsilon=1/100$ this is $r_G=3265$. Its proof rests on the dual-basis and perfectness lemmas of Section 40.2 for general weights, on a model for the weights whose factors are symmetric powers or their duals (in Witt-vector coordinates), on counts of rational planes over $\mathbb{F}_Q$ (Problem 40.1.1), branching and Pieri counts, the extremal projector, and on valuations of digit polynomials along chains of letters. It is a large development which we have not followed. In [Adr] the corresponding statement is Theorem 37.4.1(i), derived there from the engines of [Adr, Hyp. 12.12].

For $p \geq p_*$ the weights vary in a box: $a_i \in [a, a+a/(kY)] \cap \mathbb{Z}$ and $b_i \in [b_l, b_u] \cap \mathbb{Z}$ for $i \in \mathcal{T}$. For a position i let $d(i) \geq 1$ be least with $i - d(i)$ an even position in $\mathcal{T}$.

Theorem 40.5.2 (large primes)**.** *For suitable constants C_0, C_H and C, the first two large enough, the following holds. Put $\Lambda_0 = C_0 N_{\mathrm{gap}}^2 \log a$, where N_{gap} and G_{gap} bound the number of tops between, and the distance between, consecutive even tops. Under the size conditions of the formalization on $p, \nu, k, \mathcal{T}, Y, a, b', b_l, b_u, c, D, c_*$ (among them $k^2Y^2 \leq p < a/b'$, $c_* \geq 8(D+1)$, and that no odd power of p lies within a factor $1 \pm 2\delta$ of a/b' for an explicit $\delta < 1/6$), there is a function $\kappa(a_\bullet, b_\bullet) \geq 0$ on the box such that*

(a) *the mean of κ over the box is at most $C|\mathcal{T}|N_{\mathrm{gap}}/Y$;*
(b) *for every weight of base type with parameters in the box, $\mathrm{LP}(1; t, D, \kappa(a_\bullet, b_\bullet), c_*)$ holds for every integer $t \geq t_I$, where*

$$t_I = \sum_{i \in \mathcal{T},\ i\ odd} \min\Big(b_i,\ \frac{a_{i-d(i)}}{p^{d(i)}}\Big) + E,$$

with an explicit error term E of size $C|\mathcal{T}|N_{\mathrm{gap}}(a/p^2 + b'/p + \Lambda_0 a/(pk) + \Lambda_0 b'/k)$ plus terms in $p^{G_{\mathrm{gap}}}$, k, $\log_p a$, ν, c_* and c.

Status: proved in the formalization; we have not reproduced its full list of size conditions. Its proof combines a detection theorem for twisted Fock pairings, a rank theorem for systems of columns, and mean bounds for the shares of bad segments. These are presumably the three engines of [Adr, Hyp. 12.12], but we have not checked the correspondence. We have not followed the proof. In [Adr] the corresponding statement is Theorem 37.4.1(ii).

Problem 40.5.1. Let $\kappa_0(a_\bullet, b_\bullet)$ be the least defect of Problem 40.3.2 for the depth $\lceil t_I \rceil$. Under Theorem 40.5.2, κ_0 also has mean at most $C|\mathcal{T}|N_{\mathrm{gap}}/Y$, and the proportion of the box on which $\kappa_0 > \eta$ is at most $C|\mathcal{T}|N_{\mathrm{gap}}/(Y\eta)$.

Problem 40.5.2. Let $\nu = 6$, $\mathcal{T} = \{0, 1, 3\}$, $p = 13$, $a_0 = a_1 = a_3 = 10^6$, $b_1 = 10^5$ and $b_3 = 10^3$. Then $d(1) = 1$, $d(3) = 3$, and the main term of t_I is $10^6/13 + 10^6/13^3$, about 77378.

The main term of t_I is a sum over the odd tops: each pays the smaller of its own bottom weight and the weight of the nearest even top behind it, divided by p to the distance. The defect, not the depth, is what the edge theorems control on average; Chapter 37 turns depth, denominator and defect into the colength of the Hecke image.

In the Lean formalization. In [Lean] the condition is `LPprime`, at one lattice `LPprimeAt`, with `IsEdge`, the midpoint `LeAt`, the lattices `HL`, `Re`, `Re'`, the pairing `be`, the depth lattices `Nsrc`, `Ntgt`, and `GoodRankK` for (iii). The setting is `HidaSetting` and `UnramifiedQuadraticSetting`. Section 40.2 is `DualHeightBasis`, `DualHeightInclusion` and `BePerfect`; Problem 40.3.1 is `LPOneEvery`; Problem 40.3.2 is `one_mem_kapISet`, `LPprime_mono_kappa` and `KapIDef`; Problem 40.3.4 is `lpBaseChange`; Problem 40.1.1 is `rational_planes_count`. Theorem 40.5.1 is `tableLineDegreeFive.aux_3`, from `second_theorem_absolute_constant`; Theorem 40.5.2 is `flipOneThree.Conclusion2`, from `first_theorem_threshold_functions`. Section 40.4 is not in the formalization.

Hints

§40.1.

40.1.1: Count bases of subspaces of $\mathbb{F}_Q^k$; for the lower bound compare the factors of the Gaussian binomial one by one.

40.1.2: Choose a basis of L'' adapted to the edge by the elementary divisor theorem.

§40.2.

40.2.1: Problem 40.1.2 for each $\sigma^i L''$; write the coordinate functions of each lattice in terms of η_i, ξ_i.

40.2.2: Compute $\langle \varpi^{-A} h, \varpi^{-A} h' \rangle$ for $h \in H(M(e))$ and $h' \in H(M(e))^\vee$.

40.2.3: Compare exponents in Problem 40.2.1.

40.2.4: Evaluate x_J at $(\sigma^i g)_i$.

§40.3.

40.3.1: Problem 19.1.2; $\mathrm{GL}_2(K)$ acts transitively on lattices.

40.3.2: Consider the least possible n.

40.3.3: Problem 19.2.2, applied to the image of Φ inside its saturation in $\mathfrak{o}^M$, with $p^D = \varpi^{2D}$.

40.3.4: Keep the same edges, vectors, u and (μ_{jl}).

§40.4.

40.4.1: Problem 40.1.1; $\sigma[\alpha] = [\alpha^p]$.

40.4.2: A polynomial of degree less than Q that vanishes on $\mathbb{F}_Q$ is zero.

40.4.3: Problem 40.4.1; Teichmüller representatives are multiplicative.

§40.5.

40.5.1: Markov's inequality.

References

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

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

[SeL] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer, 1979.