THE MAIN INEQUALITY

Prerequisites. Hadamard's inequality for positive definite Hermitian matrices [HJ, §7.8]. Dirichlet L-functions: $L(1,\chi) \neq 0$ for χ nonprincipal, induced and primitive characters, and the functional equation [Dav, Ch. 4, Ch. 5, Ch. 8, Ch. 9]. From Chapter 1 the remainder $R_{d,q}$, written R_q here for fixed d, the one-sided criterion and the prime number theorem in progressions; from Chapter 3 the identity for the total remainder; from Chapter 33 the data and Problem 33.6.3; from Chapter 34 the objects and the target lattice (Definition 34.11.1); and the statements of Theorems A, B and C (Chapters 42, 36 and 54). The problems in Section 35.1 use no earlier chapter.

Theorems A and B supply many independent target forms, with upper bounds for the lengths of their untwisted lifts and for the index of the family; Theorem C bounds the covolume plus twice the index of such a family from below by the main amount, times the dimension, less a small error. How do the three statements give the theorem? Comparing the two bounds gives the main inequality for the total remainder rem. The identity of Theorem 3.2.1 then gives an upper bound for the prime-sum remainder $R_{q_0}(x)$. We first do the comparison in a lattice, then state the main inequality, and finally pass to the one-sided bound and to the theorem. Parts VII, VIII and IX state and deduce Theorems B, A and C.

35.1. The comparison in a lattice

Let $N \geq 1$ be an integer, and give $\mathbb{C}^d$ the Hermitian form $\langle v, w\rangle := N\,\bar{v}^{\mathsf{T}} w$. For $y_1, \dots, y_n \in \mathbb{Q}^d$ write $\mathrm{Gram}(y) := \det(\langle y_i, y_j\rangle)_{i,j\leq n}$, and let $H := \log N$.

Problem 35.1.1. If $\langle y_i, y_i\rangle \leq e^u$ for $i = 1, \dots, n$, then $\mathrm{Gram}(y) \leq e^{nu}$; if the y_i are linearly independent, $\log \mathrm{Gram}(y) \leq nu$.

The comparison itself is an inequality between real numbers. Suppose that a family of n vectors in a space of dimension $d \geq 1$ satisfies a lower bound and two upper bounds,

$$d(H - 3F) \leq c + 2\delta, \qquad c \leq n(H - \rho + F), \qquad \delta \leq dI,$$

for real numbers H, F, I, ρ, c, δ. The upper exponent per vector is $H - \rho + F$, including the error F.

Problem 35.1.2. If moreover $H + F \geq 0$ and $d/2 \leq n \leq d$, then $n\rho \leq d(4F + 2I)$, and $\rho \leq 2(4F + 2I)$ when $4F + 2I \geq 0$.

Problem 35.1.3. In the comparison of real numbers above, after dropping the hypothesis $H + F \geq 0$ one can satisfy all three bounds and $d/2 \leq n \leq d$ while $n\rho > d(4F + 2I)$. (Here H is any real number, not necessarily $\log N$.)

In this lattice the main amount sits in the metric. In Chapter 54 it enters through the height of the family $\iota \mapsto Z(1)/Z(\theta_\iota)$, where the twist θ_ι is chosen for each pair (ℓ, ι) (Problem 54.2.4).

Date: November 26, 2026.

35.2. The main inequality

Let rem be the total remainder of Chapter 33, $U = fa\log^3 b$ the unit of the errors and $F := U\log b$. Theorems A and B (Chapters 42 and 36) concern the ramified source forms S_{ram}, the integral ones $S^{\mathrm{int}}_{\mathrm{ram}}$, the finite group $\bar G$, and the normalized translates $A_s\colon S_{\mathrm{ram}} \to T$ of the Poincaré map, $s \in \bar G$. For $v \in T$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$, $\|v\|^2_\sigma$ is the squared length of Definition 34.11.1, computed from the σ-conjugate coordinates of the untwisted lift $\Theta_1 v$. Theorems A, B and C are proved in Parts VIII, VII and IX (Chapters 42, 36 and 54); here we use only their statements, in the following form.

(A1) (Theorem 42.3.2(a), which writes $\|\Theta_1 A_s\varphi\|_\sigma$ for the length used here and $fa\log^4 b$ for F.) S_{ram} is spanned by the set S_{short} of $\varphi \in S^{\mathrm{int}}_{\mathrm{ram}}$ with $\|A_s\varphi\|^2_\sigma \le \exp(h_{\mathrm{main}} - m\,\mathrm{rem} + F)$ for every $s \in \bar G$ and every σ.

(A2) (Theorem 42.3.2(b), which writes $2fa\log^3 b$ for $2U$.) If $J \subseteq \bar G$ is finite and every y_i lies in $A_s(S^{\mathrm{int}}_{\mathrm{ram}})$ for some $s \in J$, then $y_1, \dots, y_n$ has index at most $2\,\#J \dim S_{\mathrm{ram}} \cdot U$.

(B) (Consequence of Theorem 36.4.2: there the maps $e_0\rho(s)\mathcal{P}$ on S_{ram} have the same ranges as the A_s.) $d_T > 0$, and there is a finite $J \subseteq \bar G$ with $\#J \dim S_{\mathrm{ram}} \le 5d_T \log(1+2b^2)$ and $\dim \sum_{s\in J} A_s(S_{\mathrm{ram}}) \ge (1 - 4/b^2)d_T$.

Theorem C (Theorem 54.2.1), in full, is the lower bound: if $y_1, \dots, y_n$ are linearly independent target forms with $(1-4/b^2)d_T \le n$, of index at most δ and covolume at most c, then

$$d_T(h_{\mathrm{main}} - 3fa\log^4 b) \le c + 2\delta;$$

index and covolume are those of the target lattice (Definition 34.11.1).

The upper bound for the covolume is Hadamard's inequality: if $\|z_i\|^2_\sigma \le e^u$ for $i = 1, \dots, n$ and every σ, then $z_1, \dots, z_n$ has covolume at most nu.

Problem 35.2.1. For J as in (B), the span of $\bigcup_{s\in J} A_s(S_{\mathrm{short}})$ is $\sum_{s\in J} A_s(S_{\mathrm{ram}})$. Hence that space has a basis $y_1, \dots, y_n$ with each $y_i \in A_s(S_{\mathrm{short}})$ for some $s \in J$, and $(1-4/b^2)d_T \le n \le d_T$.

Problem 35.2.2. This family has covolume at most $n(h_{\mathrm{main}} - m\,\mathrm{rem} + F)$ and index at most $d_T \cdot 10\log(1+2b^2)\,U$.

Problem 35.2.3. $n\,m\,\mathrm{rem} \le d_T\big(4F + 20\log(1+2b^2)\,U\big)$.

Problem 35.2.4. $n \ge d_T/2$, and $8F + 40\log(1+2b^2)\,U \le fa\log^5 b$. Hence $m\,\mathrm{rem} \le fa\log^5 b$.

Theorem 35.2.1 (Main inequality)**.** $m\,\mathrm{rem} \le fa\log^5 b$.

The errors per dimension are: F from the size in Theorem A, $20\log(1+2b^2)\,U$ from the index in Theorems A and B (counted twice, as it enters as 2δ), and $3F$ from Theorem C.

35.3. From the main inequality to the theorem

Let $q_0 \ge 1$ and d be the parameters of the data, so that $18480 \mid q_0$ and d is a prime with $d \equiv q_0/2 - 1 \pmod{q_0}$; then d is odd and prime to q_0. Recall that, for $q \ge 1$ prime to d, $R_q(y) = \sum_{n\le y} \lambda(n)(1/n - 1/y) - \log y/\varphi(q) - c_q$, with $\lambda(n) = \Lambda(n)(1 - (n/d))$ for $n \equiv 1 \pmod q$ and $\lambda(n) = 0$ otherwise, where (n/d) is the Legendre symbol and c_q is the constant for which $R_q(y) \to 0$; these are $R_{d,q}$

and $c_{d,q}$ of Chapter 1. When d varies we write $R_q^{(d)} = R_{d,q}$. We use the identity of Theorem 3.2.1,

$$\text{rem} = a\big(\#\Phi_b\,(R_{q_0}(x) - R_{q_0}(x_1)) + \#\Phi_a\,R_1(x_1)\big)$$

for the sets Φ_a and Φ_b of a-places and b-places, together with $f = \#\Phi_a\,\varphi(q_0)$ and $0 < \#\Phi_a \le \#\Phi_b \log b$ (Chapter 33).

Problem 35.3.1. $R_{q_0}(x) \le \varphi(q_0)\log^6 b/m + |R_{q_0}(x_1)| + \log b\,|R_1(x_1)|$.

Two further inputs. By the prime number theorem in progressions, for every prime $d \ne 2$, every $q \ge 1$ prime to d and every integer $B \ge 0$, one has $|R_q(y)| \le (\log y)^{-B}$ for all large y (Chapter 1). And for $0 < \varepsilon < 1/100$ and every large integer x there are data with this x, with $\log b \le 2x^{\varepsilon}$, $m \ge \sqrt{x}$ and $\log x_1 \ge x^{\varepsilon/12}$ (Problem 33.6.3).

Problem 35.3.2. Let $\varepsilon > 0$. For all large integers x and every real y with $\log y \ge x^{\varepsilon/12}$, one has $|R_{q_0}(y)| \le x^{-2}$ and $|R_1(y)| \le x^{-2}$.

Problem 35.3.3. Let $0 < \varepsilon < 1/100$. For all large integers x, $R_{q_0}(x) \le (64\varphi(q_0) + 3)\,x^{-1/2+6\varepsilon}$.

Problem 35.3.4. For $q \ge 1$ prime to d and real $y \ge 2$, $R_q(y) - R_q(\lfloor y\rfloor) \le 3/y$. For $-1 \le u \le 0$, $\lfloor y\rfloor^u \le 2y^u$.

Problem 35.3.5. Let $\varepsilon > 0$. For all large real y, $R_{q_0}(y) \le y^{-1/2+\varepsilon}$.

Theorem 35.3.1 (One-sided bound)**.** *Let $q_0 \ge 1$ be a multiple of* 18480*, let $d \equiv q_0/2 - 1 \pmod{q_0}$ be a prime, and let $\varepsilon > 0$. Then $R_{q_0}(y) \le y^{-1/2+\varepsilon}$ for all large real y.*

The criterion of Chapter 1 reads: let $q_0 \ge 1$ be a multiple of 8, let $d_0 \ge 0$ be an integer with $d_0 \equiv 7 \pmod 8$ and prime to q_0, and let $\beta > \frac12$; if for every prime $d \equiv d_0 \pmod{q_0}$ one has $R_{q_0}^{(d)}(y) \le y^{\beta-1}$ for all large y, then $L(\rho,\psi) \ne 0$ for every character ψ modulo q_0 and every $\rho \ne 1$ with $\operatorname{Re}\rho > \beta$.

Problem 35.3.6. For $q \ge 1$, $q_0 := 18480q$ and $d_0 := 9240q - 1$: $d_0 \equiv 7 \pmod 8$, $\gcd(d_0, q_0) = 1$, and $d_0 = q_0/2 - 1$.

Problem 35.3.7. Let $q \ge 1$, let χ be a character modulo q, and let χ' be the character modulo $q_0 = 18480q$ that it induces. If χ is nonprincipal or $s \ne 1$, then $L(s,\chi') = L(s,\chi)\prod_{p\mid q_0}(1 - \chi(p)p^{-s})$, so $L(s,\chi') \ne 0$ implies $L(s,\chi) \ne 0$.

Problems 35.3.6 and 35.3.7, Theorem 35.3.1, the criterion and $L(1,\chi) \ne 0$ for χ nonprincipal prove the following.

Theorem 35.3.2. *Let $q \ge 1$, let χ be a Dirichlet character modulo q, and let $s \in \mathbb{C}$ with $\operatorname{Re} s > \frac12$, where $s \ne 1$ if χ is principal. Then $L(s,\chi) \ne 0$.*

Problem 35.3.8. Every zero s of a Dirichlet L-function with $0 < \operatorname{Re} s < 1$ has $\operatorname{Re} s = \frac12$.

Theorem 35.3.2 is the half-plane form of the generalized Riemann hypothesis for Dirichlet L-functions. Thus Theorems A, B and C give the main inequality, from which the one-sided bound and the criterion of Chapter 1 yield Theorem 35.3.2.

In the Lean formalization. In the Lean proof [GL], Theorem 35.2.1 is `New.star_inequality`, in `grh/src/New/Reduction/MainInequality.lean`; Problem 35.3.1, Theorem 35.3.1 and Theorem 35.3.2 are `New.Data.primeRemainder_le`, `New.eventually_primeRemainder_le_rpow` and `New.grh`, in `grh/src/New/Reduction/OneSidedBound.lean`. Hadamard's inequality for the covolume is `New.TwistedLattice.covolumeLe_of_normSqAt_le`, and Problems 35.2.1–35.2.4 follow the proof of `New.star_inequality`. Problems 35.3.2 and 35.3.3 are `New.eventually_abs_primeRemainder_exp_le` and `New.eventually_primeRemainder_natCast_le`. For the first bound of Problem 35.3.4 the proof uses `New.primeRemainder_sub_primeRemainder_floor_le`, which gives $26/y$ in place of $3/y$, for every prime d and every $q \geq 1$; the sharper bound is an exercise here. The second bound is `New.natFloor_rpow_le_two_mul_rpow`. Problem 35.3.8 is `New.zeros_on_line`, in `grh/src/New/Main.lean`, applied to `New.grh`.

Hints

§35.1.

35.1.1: Apply Hadamard's inequality to the Gram matrix.

35.1.2: Insert the upper bounds into the lower bound; then use $n(H+F) \leq d(H+F)$.

35.1.3: Take $d = 2$, $n = 1$, $F = I = \delta = 0$ and $H = -1$.

§35.2.

35.2.1: Images of a spanning set span the image.

35.2.2: Hadamard's inequality with $u = h_{\mathrm{main}} - m\,\mathrm{rem} + F$; (A2) and the bound for $\#J \dim S_{\mathrm{ram}}$ in (B).

35.2.3: Compare the two bounds for $c + 2\delta$, using $n \leq d_T$ and $h_{\mathrm{main}} + F \geq 0$.

35.2.4: $\log(1 + 2b^2) \leq 3 \log b$, and $\log b \geq 128$.

§35.3.

35.3.1: Solve the identity for $R_{q_0}(x)$, and divide Theorem 35.2.1 by $ma\#\Phi_b$.

35.3.2: Take $B \geq 24/\varepsilon$; d is odd and prime to q_0.

35.3.3: Use Problem 35.3.1 for the data at x and Problem 35.3.2 with $y = x_1$.

35.3.4: The two sums differ by $(1/\lfloor y \rfloor - 1/y) \sum_{n \leq y} \lambda(n)$; use $0 \leq \lambda \leq 2\Lambda$ and $\psi(\lfloor y \rfloor) < 1.04 \lfloor y \rfloor$ [RS, Thm. 12].

35.3.5: Problem 35.3.3 with $\min(\varepsilon/7, 1/200)$ in place of ε, and Problem 35.3.4.

35.3.7: Compare Euler products for $\mathrm{Re}\, s > 1$, then continue analytically.

35.3.8: Reduce to a primitive character; then the functional equation and Theorem 35.3.2.

References

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Grad. Texts in Math. 74, Springer, 2000.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HJ] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge Univ. Press, 2013.

[RS] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.