POSITIVE TYPE AND THE BOOTSTRAP: THE SECOND MOMENT

Prerequisites. Hermitian forms and inner products are linear in the first variable; norms of operators are Hilbert–Schmidt norms. Additive characters of a finite field and their orthogonality [LN, Ch. 5, §1]. From Chapter 9: Problem 9.2.2. From Chapter 36: the Bessel subgroup and the vectors $v_1, \dots, v_\varrho$, z (Section 36.1; they belong to the lattice basis of Definition 36.4.1), the scaled Poincaré map $\mathcal{P}^\circ$, the Gram operators $\mathcal{K}_s$ and the covolume ν (Definition 36.4.1), the group $\bar{R}_0$ and ρ_{Bes} (Definition 36.4.2), and admissible fillings (Section 36.4). From Chapter 37: Theorem 37.3.2, the sizes $D_{\mathrm{id}} = \#\bar{R}_0 \cdot D_X$ and D_{main} (Definition 37.3.2), Problems 37.4.3, 37.4.4 and 37.4.5. From Chapter 38: frame products and their leading minors $\langle s \rangle_j$ (Definition 38.2.1), meeting and the meet norm mt (Definition 38.2.5), open reductions (Definition 38.2.6), fixers (Definition 38.2.7), scalar cosets (Definition 38.2.4), second moments and link second moments (Definition 38.3.1), Theorems 38.3.1, 38.3.2 and 38.3.3. From Chapter 39: Theorem 39.3.3.

Chapter 36 deduces Theorem B from three estimates for the Gram operators $\mathcal{K}_s = \mathcal{P}^{\circ *}\rho(s)\mathcal{P}^\circ$, $s \in \bar{G}$. This sheet proves the second-moment estimate $\sum_{s\in\bar{G}} \|\mathcal{K}_s\|^2 \le (1 + 9b^{-4}) D_{\mathrm{main}}$. Chapter 39 bounds the open reductions that fix given frame vectors; the others, where a leading minor of the frame products vanishes, are many (three sevenths of $\mathrm{GL}_3(\mathbb{F}_2)$ in the toy below). How can one show that they carry little of $s \mapsto \|\mathcal{K}_s\|^2$ without knowing that this function is spread evenly over $\bar{G}$?

40.1. Positive type and singular minors

In this sheet a real function Θ on a finite group G is *of positive type* if there are vectors u_a, $a \in G$, of a complex inner product space with $\langle u_a, u_b \rangle = \Theta(a^{-1}b)$ for all a, b. A subset of G *carries* the sum of Θ over it. By Problem 9.2.2, if ρ is a unitary representation of G and L a linear map into its space, then $s \mapsto \|L^*\rho(s)L\|^2$ is of positive type, with $u_a = \rho(a)LL^*\rho(a)^*$ in the Hilbert–Schmidt inner product.

Problem 40.1.1. Let Θ be of positive type on G, with vectors u_a. (a) $\Theta(s^{-1}) = \Theta(s)$ and $|\Theta(s)| \le \Theta(1) = \|u_a\|^2$ for all s, a. (b) For a subgroup $\Gamma' \subseteq G$, $\sum_{s\in\Gamma'} \Theta(s) = \|\sum_{a\in\Gamma'} u_a\|^2/\#\Gamma' \ge 0$, and the restriction of Θ to Γ' is of positive type.

Let ψ be a nontrivial additive character of $\mathbb{F}_q$; vectors are columns, y^t is a transpose and g^{-t} the inverse transpose of $g \in \mathrm{GL}_n(\mathbb{F}_q)$.

Problem 40.1.2. For a $j \times j$ matrix Z over $\mathbb{F}_q$, $\#\{y \in \mathbb{F}_q^j : y^t Z = 0\} = q^{-j} \sum_{y,v\in\mathbb{F}_q^j} \psi(y^t Z v)$, and this number is at least q if $\det Z = 0$.

Date: November 26, 2026.

The toy. In this sheet let J be the permutation matrix exchanging e_1 and e_3 and fixing e_2, the Gram matrix of the symmetric bilinear form $(x, x') \mapsto x^t J x'$ on $\mathbb{F}_p^3$. Take the frame (e_1, e_2): e_1 is isotropic and paired with e_3. The only proper leading minor of the frame products of $s \in \mathrm{GL}_3(\mathbb{F}_p)$ is $e_1^t J s e_1 = s_{31}$, so the open elements are those with $s_{31} \neq 0$. An element may fix a frame vector x in two ways: $sx = x$, or $s^{-t}(Jx) = Jx$, that is, s fixes the linear form $x' \mapsto x^t J x'$; for $x = e_1$ the second is $e_3^t s = e_3^t$.

Problem 40.1.3. By machine: in $\mathrm{GL}_3(\mathbb{F}_p)$ the group, the set $\{s_{31} = 0\}$, the fixer of e_1 and the fixer $\{s : e_3^t s = e_3^t\}$ of the form e_3^t have $168, 72, 24, 24$ elements for $p = 2$ and $11232, 3456, 432, 432$ for $p = 3$. Both fixers lie in $\{s_{31} = 0\}$.

So a weight concentrated on a fixer lives entirely where the minor vanishes. The next two problems show that this is the only obstruction: a vanishing minor is detected by characters, and the character sums are bounded by the weight of stabilizers.

Problem 40.1.4. Let $\pi \colon G \to \mathrm{GL}_n(\mathbb{F}_q)$ be a homomorphism, Θ of positive type on G, $y, v \in \mathbb{F}_q^n$ and Y real. If the s with $\pi(s)v = v$, and the s with $\pi(s)^{-t} y = y$, each carry at most Y, then

$$\Big| \sum_{s \in G} \Theta(s)\, \psi\big(y^t \pi(s) v\big) \Big| \leq q^{n/2} Y.$$

Problem 40.1.5. Let π be as in Problem 40.1.4, $\Theta \geq 0$ of positive type, A_0, A_1 two $n \times j$ matrices over $\mathbb{F}_q$ and $Y \geq 0$. Suppose that for every $v \in \mathbb{F}_q^j \smallsetminus 0$ the s with $\pi(s)A_0 v = A_0 v$, and the s with $\pi(s)^{-t} A_1 v = A_1 v$, each carry at most Y. Then

$$q \sum_{\det(A_1^t \pi(s) A_0) = 0} \Theta(s) \leq 2 \sum_{s \in G} \Theta(s) + q^j q^{n/2}\, Y.$$

Problem 40.1.6. In the toy take $j = 1$, $A_0 = e_1$, $A_1 = J e_1 = e_3$, so that $\det(A_1^t s A_0) = s_{31}$. (a) For $\Theta \equiv 1$ and Y the order of a fixer in Problem 40.1.3, Problem 40.1.5 reads $144 \leq 471.764\ldots$ for $p = 2$ and $10368 \leq 29198.213\ldots$ for $p = 3$. (b) For $p = 2$ the indicator Θ of the fixer of e_1 is of positive type; all of its mass 24 lies in $\{s_{31} = 0\}$, the least admissible Y is 24, and Problem 40.1.5 reads $48 \leq 183.764\ldots$.

For the uniform weight the elements with $s_{31} = 0$ are a proportion $3/7$ of $\mathrm{GL}_3(\mathbb{F}_2)$; for the weight of (b) they are everything. The function $s \mapsto \|\mathcal{K}_s\|^2$ is neither, and the proof never replaces its non-open part by a proportion for the uniform measure. It chooses a subgroup on which stabilizers carry little, and then Problem 40.1.5 makes the singular part small. In the toy the lemma gains almost nothing: for $p = 2$ its right side $471.7\ldots$ exceeds the trivial bound $2 \cdot 168$, and for $p = 3$ it is $29198.2\ldots$ against $3 \cdot 11232 = 33696$. It gains when $q^{j+n/2}\, Y$ is small against $q \sum \Theta$; for the data this is Problem 40.2.1 with $Y = b^{-6k} H$.

40.2. The open part and the terminal fixer

We work as the proof does: with an admissible filling (Section 36.4) over a CM field E with Weil data (Chapter 39); the data provide one, the group $\bar{G} = \prod_{w \in \mathcal{M}} \mathrm{GL}_r(k_w)$, $\mathcal{M} = \mathcal{M}_0 \cup \mathcal{M}_1$ the chosen places above p_0 and p_1, a unitary representation ρ of $\bar{G}$ on a finite-dimensional complex inner product space, and a linear

map $\mathcal{P}^\circ$ from the coordinate space with the block identity of Theorem 37.3.2. In this sheet $\mathrm{en}(s) := \|\mathcal{K}_s\|^2$, formed with the full Bessel function. By Problem 37.4.5, en is of positive type, with $u_a = \rho(a)\mathcal{P}^\circ\mathcal{P}^{\circ *}\rho(a)^*$, and $\mathrm{en}(s) \le \mathrm{en}(1)$. The proof also gives $\mathrm{en}(1) = \|\mathcal{K}_1\|^2 \le 2D_X$ in this generality (see the remark), by Theorem 38.3.3 and Problems 37.4.3 and 37.4.4, whose hypotheses ($\mathcal{K}_{st} = \mathcal{K}_s\rho_{\mathrm{Bes}}(t)$ for $t \in \bar{R}_0$, and ρ_{Bes} a unitary representation of $\bar{R}_0$) it states for every admissible filling with the block identity. Of the conditions of admissibility we use: $b \ge 1000$; $b^{10} \le p_0 \le b^{11}$ and $M = p_0p_1 \le b^{23}$; $1000(2\varrho + 2) \le k \le f$ and $\varrho + 1 \le b$; there are f chosen places above each p_i, each with residue field of p_i elements, all distinct, and no conjugate of a chosen place is chosen; $b^{11kf}D_{\mathrm{id}} \le D_{\mathrm{main}}$. The matrices s_w have size $r = k + 2\varrho + 1$.

We recall Definitions 38.2.6, 38.2.7 and 38.2.5 at a chosen place w above p_0, with one abbreviation. In this sheet a *frame vector* at w is a nonzero vector x of the span of the frame modulo w, with a side: s fixes it on the side of w if $s_wx = x$, and on the side of $\bar{w}$ if s_w^{-t} fixes Jx, where J is the Gram matrix of the lattice basis modulo w. The fixer of frame vectors given at a set $\mathcal{D} \subseteq \mathcal{M}_0$ of such places is the subgroup of the s fixing each. An element s is *open* if at some $w \in \mathcal{M}_0$ the leading minors $\langle s\rangle_1, \dots, \langle s\rangle_\varrho$ of its frame products are nonzero. With A_0 the matrix whose columns are the first j vectors $v_1, \dots, v_j$ of the frame and $A_1 = JA_0$, the minor $\langle s\rangle_j$ at w is $\det(A_1^t s_w A_0)$. An element *meets* at w (or at $\bar{w}$) if modulo that place the span of the frame and that of its image share a nonzero vector, and $\mathrm{mt}(s)$ is the product of $\#k_w$ over the places w and $\bar{w}$, $w \in \mathcal{M}$, at which s meets; an element that fixes a frame vector on a side meets at that place. An element of $\bar{R}_0$ fixes v_1 modulo every chosen place: $\mathcal{U}$ and $U(X_0)$ fix v_1 (Section 36.1), and v_1 is a vector of the lattice basis. For $s \notin \bar{R}_0$ we have $\rho_{\mathrm{Bes}}(s) = 0$, and $\mathrm{en}(s)$ is the second moment at s of the terms outside the Bessel subgroup.

Three statements are used, for sets $\mathcal{B} \subseteq \bar{G}$. Theorem 38.3.1: if z_0 is a positive integer with $z_0 \le \mathrm{mt}(s)$ for all $s \in \mathcal{B}$, the link second moment of the terms with disc $\ne 0$ over $\mathcal{B}$ is at most

$$(b^{2f}/z_0)^k\, D_{\mathrm{main}}\, \nu^2.$$

Theorem 38.3.2: if $\mathcal{B}$ avoids the scalar cosets and that link second moment is at most $C_0\nu^2$, $C_0 \ge 0$, then the second moment over $\mathcal{B}$ of the terms outside the Bessel subgroup, for the full Bessel function, has square root at most

$$\sqrt{C_0} + b^{-15}\sqrt{D_{\mathrm{id}}}.$$

Theorem 39.3.3: for a set $\mathcal{D}$ of h chosen places above p_0 with a frame vector at each, the link second moment of the terms with disc $\ne 0$ over the open elements of their fixer is at most

$$(1 + b^{-4})\, b^{-6kh}\, D_{\mathrm{main}}\, \nu^2.$$

In this sheet $y_h := b^{-6kh}D_{\mathrm{main}}$ for $0 \le h \le f$; since $b^{11kf}D_{\mathrm{id}} \le D_{\mathrm{main}}$, we have $b^{5kf}D_{\mathrm{id}} \le y_h$.

Problem 40.2.1. $p_0^j\sqrt{p_0^r} \le b^{6k}$ for $0 \le j \le \varrho$.

Problem 40.2.2. Let $\Gamma' \subseteq \bar{G}$ be a subgroup, $H := \sum_{s\in\Gamma'} \mathrm{en}(s)$ (in this sheet), and w a chosen place above p_0. Suppose that for every frame vector at w, on either side, the elements of Γ' fixing it carry at most $b^{-6k}H$. Then the elements of Γ' that are not open carry at most $b^{-4}H$.

Problem 40.2.3. If $s_w v_1 \in k_w v_1$ at a chosen place w above p_0, then $\langle s\rangle_1 = 0$ at w. Hence no $s \in \bar{G}$ with $s_w = \zeta_w t_w$ for every $w \in \mathcal{M}$, for some $t \in \bar{R}_0$ and some integral finite adele ζ with residues ζ_w, is open; in particular the open elements avoid the scalar cosets and lie outside $\bar{R}_0$.

Problem 40.2.4. Let Γ' be the fixer of frame vectors at a set of h chosen places above p_0. The open elements of Γ' carry at most $(1 + 4b^{-4})\, y_h$.

The terminal case fixes vectors at all f places above p_0.

Problem 40.2.5. (a) $(b^{2f}/p_0^f)^k\, D_{\mathrm{main}} \le y_f/8$. (b) $8M^f D_{\mathrm{id}} \le y_f$. (c) At most $M^f \# \bar{R}_0$ elements of $\bar{G}$ have the form $s_w = \zeta_w t_w$ of Problem 40.2.3.

Problem 40.2.6. Let Γ' be the fixer of frame vectors at all f chosen places above p_0. Then $\mathrm{mt}(s) \ge p_0^f$ for $s \in \Gamma'$, and Γ' carries at most y_f.

40.3. The bootstrap

Problem 40.2.2 needs a subgroup on which stabilizers carry little, and fixing a vector costs a factor b^{-6k} in Problem 40.2.4. For a set $\mathcal{D}$ of chosen places above p_0 and frame vectors at its places, let $\Gamma_{\mathcal{D}}$ be their fixer (the vectors understood); $\Gamma_{\varnothing} = \bar{G}$. The proof maximizes the *objective* $b^{6k\#\mathcal{D}} \sum_{s\in\Gamma_{\mathcal{D}}} \mathrm{en}(s)$ over the finitely many choices, the empty one included.

Problem 40.3.1. In the toy with $p = 2$, $\Theta \equiv 1$, one place, and the factor b^{6k} replaced by c: every frame vector, on either side, has a fixer of 24 elements, and the objective at (no place, the place) is $(168, 24c)$; it is $(168, 96)$ for $c = 4$ and $(168, 192)$ for $c = 8$. Either choice can be the maximum.

Problem 40.3.2. Let $\mathcal{D}$ with its frame vectors maximize the objective, $h := \#\mathcal{D}$ and $H := \sum_{s\in\Gamma_{\mathcal{D}}} \mathrm{en}(s)$. If $h < f$ and $w \notin \mathcal{D}$ is a chosen place above p_0, then the elements of $\Gamma_{\mathcal{D}}$ fixing a frame vector at w, on either side, carry at most $b^{-6k}H$, and

$$H \le (1 + 4b^{-4})\, y_h + b^{-4}H.$$

Problem 40.3.3. If $H \le (1 + 4\delta)Y + \delta H$ with $0 \le \delta \le 1/10$ and $Y \ge 0$, then $H \le (1 + 9\delta)Y$. For $\delta = 1/16$: $(1 + 4\delta)/(1 - \delta) = 4/3 \le 25/16 = 1 + 9\delta$.

Problem 40.3.4. With $\mathcal{D}$ as in Problem 40.3.2, $H \le (1 + 9b^{-4})\, y_h$; hence $\sum_{s\in\bar{G}} \mathrm{en}(s) \le (1 + 9b^{-4})\, D_{\mathrm{main}}$.

Problems 40.1.1, 40.1.2, 40.1.4, 40.1.5 and 40.2.1–40.3.4, with Theorems 38.3.1, 38.3.2 and 39.3.3 and the two properties of en recalled in Section 40.2 (positive type, and $\mathrm{en}(1) \le 2D_X$), prove the following.

Theorem 40.3.1 (the second moment)**.** *Let an admissible filling over a CM field with Weil data be given, ρ a unitary representation of $\bar{G}$ on a finite-dimensional complex inner product space, and $\mathcal{P}^\circ$ a linear map from the coordinate space satisfying the block identity of Theorem 37.3.2. Then*

$$\sum_{s\in\bar{G}} \|\mathcal{K}_s\|^2 \le (1 + 9b^{-4})\, D_{\mathrm{main}}.$$

In particular this holds for the data, with $\mathcal{P}^\circ$ the scaled Poincaré map and ρ the representation of Chapter 36.

In the Lean formalization. In the Lean proof [GL] the theorem is `Filling.HasAmplitudeBlocks.sum_hilbertSchmidtNorm_sq_le`, and for the data `Data.sum_hilbertSchmidtNorm_scaledPoincare_sq_le`; it is deduced from `Filling.sum_secondMoment_le`, which bounds the sum over $\bar{G}$ of the second moments at s of all terms, for an admissible filling with Weil data, assuming that this function of s is of positive type and at most $2D_X$ at $s = 1$, by the maximization of Section 40.3. The bound $\mathrm{en}(1) \le 2D_X$ under the block identity, for any representation, is `Filling.HasAmplitudeBlocks.hilbertSchmidtNorm_adjoint_comp_sq_le`. Problem 40.1.5 is `card_mul_sum_det_eq_zero_le`, whose proof bounds only the real part of the sum of Problem 40.1.4; Problem 40.2.2 is the case en of `Filling.sum_not_isOpenElement_le`, stated there for every function ≥ 0 of positive type; the second sentence of Problem 40.2.3, up to "in particular", is `Filling.InScalarCoset.not_isOpenElement`; Problem 40.2.4 is `Filling.secondMoment_fixer_isOpenElement_le`; the bound for the fixer in Problem 40.2.6 is `Filling.secondMoment_fixer_univ_le`, which assumes $\mathrm{en} \le 2D_X$; the first sentence of Problem 40.3.3 is `Filling.le_one_add_nine_mul_of_le_add`.

What has been proved is the second moment over the whole group, from the link bound and the cut, which Chapter 38 reads from the proof, and the open-cell bound, whose steps Chapter 39 models with statements read from the proof. With the count of Theorem 41.3.1 it gives the hypothesis of Theorem 9.3.1 on the second moment (Problem 41.3.6); the other hypothesis, the near isometry of the projected map, is Theorem 41.2.2.

Hints

§40.1.

40.1.1: $\langle u_a, u_a\rangle = \Theta(1)$ and Cauchy–Schwarz. Expand $\|\sum_a u_a\|^2$ and group the pairs (a, b) by $a^{-1}b$.

40.1.2: $\sum_v \psi(z^t v)$ is q^j if $z = 0$ and 0 otherwise; a nonzero y in the kernel gives a line.

40.1.3: Run through the p^9 matrices.

40.1.4: Write the sum as an inner product of two vectors of $\mathbb{C}^{\mathbb{F}_q^n} \otimes \mathrm{span}(u_a)$, one built from point masses, the other from the normalized characters $\xi \mapsto q^{-n/2}\psi(z^t\xi)$; then Cauchy–Schwarz.

40.1.5: Bound q times the indicator of $\det Z_s = 0$, $Z_s := A_1^t \pi(s) A_0$, by Problem 40.1.2; sum against Θ. Separate the pairs with $y = 0$ or $v = 0$, and use $y^t Z_s v = (A_1 y)^t \pi(s)(A_0 v)$ for the others.

40.1.6: For (b), $u_a := \delta_{ae_1}$.

§40.2.

40.2.1: Show $11(2j{+}r) \le 12k$, using $p_0 \le b^{11}$, $r = k{+}2\varrho{+}1$, $1000(2\varrho{+}2) \le k$.

40.2.2: A non-open element has $\langle s\rangle_j = 0$ at w for some $1 \le j \le \varrho$. For each j, Problem 40.1.5 for Γ', $\pi(s) = s_w$, $\Theta = \mathrm{en}$ and $Y = b^{-6k}H$: $A_0 v$ and $A_1 v = J(A_0 v)$ are a frame vector and its form. Then Problem 40.2.1 and $\varrho + 1 \le b$.

40.2.3: v_1 is isotropic.

40.2.4: By Problem 40.2.3, Theorems 39.3.3 and 38.3.2 apply to the open elements of Γ'. Then $\sqrt{1+\epsilon} \le 1+\epsilon/2$, $b^{-15} \le b^{-4}/2$ and $D_{\mathrm{id}} \le y_h$.

40.2.5: (a) $p_0 \ge b^{10}$. (b) $23f+1 \le 5kf$. (c) Only the residues of ζ at the $2f$ chosen places matter.

40.2.6: The pairs (place, side) at which the fixed vectors sit are distinct places above M. Split Γ' into the elements of Problem 40.2.5(c) and the rest; use $\mathrm{en} \le 2D_X$, Theorems 38.3.1 with $z_0 = p_0^f$ and 38.3.2, and $(\sqrt{C}+\sqrt{C'})^2 \le 2C+2C'$.

§40.3.

40.3.1: A nonzero vector of $\mathbb{F}_2^3$, or a nonzero form, has 7 images.

40.3.2: Adding w with one frame vector replaces $\Gamma_{\mathcal{D}}$ by its intersection with the fixer of that vector; compare the objectives. Then Problems 40.1.1(b), 40.2.2 and 40.2.4.

40.3.3: $(1-\delta)(1+9\delta) - (1+4\delta) = \delta(4-9\delta)$.

40.3.4: If $h = f$, Problem 40.2.6; otherwise $\delta = b^{-4}$. Then compare with $\mathcal{D} = \varnothing$.

References

[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/`.

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1997.