hexagon:2611.00395v1

CERTIFIED LOWER BOUNDS FOR THE FIRST AND THE SIGNED THIRD AUTOCORRELATION CONSTANTS

TEJASVI SINGH TOMAR

ABSTRACT. Let C_1 be the largest constant such that $\sup_{|t|\le 1/2}\int f(t-x)f(x)\,dx \ge C_1\big(\int_{-1/4}^{1/4} f\big)^2$ for every nonnegative function f on the real line. We prove $C_1 \ge 1.337$, improving the bound 1.2937 of Kim and Pilanci, by a spatial branch-and-bound over the masses of f on equal bins. Consequently, for every large g, every g-Sidon set in $\{1,\dots,N\}$ has fewer than $1.2231\sqrt{gN}$ elements once N is large enough in terms of g. For real-valued f supported in $[-1/4,1/4]$, let C_3 and C_3' be the analogous constants for the essential suprema of $|f*f|$ and of $f*f$; no lower bound better than the trivial bound 1 was recorded for them. We prove $C_3 \ge C_3' \ge 4/3$ with the argument principle. Both proofs are computer-assisted, and both theorems are also proved in Lean 4.

1. INTRODUCTION

For $f\colon \mathbb{R}\to[0,\infty]$ write $(f*f)(t)=\int_{\mathbb{R}} f(t-x)f(x)\,dx\in[0,\infty]$. Following [1], we call the largest constant C such that

$$\sup_{-1/2\le t\le 1/2}(f*f)(t)\ \ge\ C\Big(\int_{-1/4}^{1/4} f(x)\,dx\Big)^2 \tag{1.1}$$

for all measurable $f\colon\mathbb{R}\to[0,\infty]$ the *first autocorrelation constant* C_1 (the name is customary, although $f*f$ is the autoconvolution of f). It is Problem 6.2 of [8]. Restricting f to $[-1/4,1/4]$ does not increase the left side, so C_1 is also the infimum of $\sup(f*f)/(\int f)^2$ over nonnegative f supported in $[-1/4,1/4]$. Schinzel and Schmidt [26] studied this quantity and conjectured that $C_1=\pi/2$.

The constant comes from additive combinatorics. A set $A\subseteq\{1,\dots,N\}$ is a g-Sidon set if $|\{(a,b)\in A\times A : a+b=m\}|\le g$ for all m. Cilleruelo, Ruzsa and Vinuesa [3] proved that the largest g-Sidon set in $\{1,\dots,N\}$ has between $\underline{\sigma}(g)\sqrt{gN}(1-o(1))$ and $\overline{\sigma}(g)\sqrt{gN}(1+o(1))$ elements as $N\to\infty$, where $\underline{\sigma}(g)$ and $\overline{\sigma}(g)$ both tend to a constant σ as $g\to\infty$. They also expressed σ through the continuous problem, and in our normalization $\sigma^2=2/C_1$ [4, Section 1.2].

Explicit step functions give the best upper bounds for C_1. Matolcsi and Vinuesa [18] found $C_1\le 1.5098$, which disproved the conjecture of Schinzel and Schmidt. Computer searches [1, 8] and later programs [5, 11] have lowered the bound below 1.5028. Lower bounds, however, have moved slowly. Cloninger and Steinerberger list the earlier ones [4, Section 1.2], which end with the bound $C_1\ge 1.2748$ of Matolcsi and Vinuesa [18] (quoted as 1.2749 in [4]). Cloninger and Steinerberger reduced the problem to a finite min-max over mass vectors, replaced the simplex of mass vectors by a lattice, and proved $C_1\ge 1.28$ by a large enumeration. Ivanisvili and Xie [10] sharpened an error term of that computation to obtain 1.2802. Piterbarg, Bajaj and Vincent report $C_1\ge 1.292$ [21]. Kim and Pilanci [14] proved $C_1\ge 1.2937$ with a semidefinite relaxation, and they checked its dual solution in interval arithmetic.

2020 *Mathematics Subject Classification.* 42A85, 11B83; 30C15, 90C57, 68V05.

Key words and phrases. Autoconvolution, autocorrelation inequality, Sidon sets, branch and bound, argument principle, computer-assisted proof.

Theorem 1.1. $C_1 \geq \frac{1337}{1000}$. *That is,* (1.1) *holds with* $C = 1.337$ *for every measurable* $f\colon \mathbb{R} \to [0,\infty]$.

The proof also gives the inequality with the essential supremum in place of the supremum.

Corollary 1.2. *In the notation above,* $\sigma \leq \sqrt{2000/1337} < 1.2231$.

The method. Cloninger and Steinerberger observed that the masses $p_i = \int_{B_i} f$ of f on n equal bins B_i already force $f * f$ to be large somewhere. If $c_1 \leq i + j \leq c_2$, then $B_i + B_j$ lies in one interval J of length $(c_2 - c_1 + 2)/(2n)$, the same for all such i, j, so $\sup_J f * f$ is at least the averaged mass $q_{c_1 c_2}(p)$ of (2.1). Hence $C_1 \geq V_n$, where V_n is the minimum over the simplex of the largest of these averages (Lemma 2.1). The inequality $C_1 \geq V_n$ has no error term, and since we work on the continuous simplex, the lattice error that limited [4] does not arise. We prove $V_{39} \geq \frac{1337}{1000}$ (Theorem 2.2). Section 5 explains the choice of n.

The function $p \mapsto \max_{c_1 \leq c_2} q_{c_1 c_2}(p)$ is a maximum of indefinite quadratic forms, and any convex relaxation of its minimization over the simplex that replaces pp^T by a matrix variable and admits all points (p, pp^T) with $p \in \Delta_n$ gives no lower bound above 1: the uniform mixture of the n vertices of Δ_n has second moment matrix $\frac{1}{n} I$, and for this matrix all averaged forms are at most 1. We therefore split the simplex into regions, following the multiscale idea of [4], and bound the maximum from below on each region by a linear relaxation, tightened where necessary by linearized inequalities $(v_0 + v \cdot p)^2 \geq 0$ that a semidefinite relaxation supplies. The dual vector of the linear program certifies the bound on the region (Sections 3 and 4).

Signed functions. Problem 6.4 of [8] asks the question of Problem 6.2 for functions that may take negative values. If f takes negative values, then $f * f$ can be negative as well. For an integrable function $f\colon \mathbb{R} \to \mathbb{R}$ that vanishes almost everywhere outside $[-1/4, 1/4]$, the function $f * f$ is integrable and vanishes almost everywhere outside $[-1/2, 1/2]$. Let C_3 and C_3' be the largest constants such that

$$\operatorname*{ess\,sup}_{t\in\mathbb{R}} |(f*f)(t)| \geq C_3 \Big(\int f\Big)^2 \quad \text{and} \quad \operatorname*{ess\,sup}_{t\in\mathbb{R}} (f*f)(t) \geq C_3' \Big(\int f\Big)^2 \tag{1.2}$$

for all such f; Section 6 compares this with the formulation of [8]. The notation C_3 follows [1], and the repository of optimization constants [20] calls C_3 the signed third autocorrelation constant. Clearly $C_3' \leq C_3$, and $C_3 \leq C_1$ since nonnegative integrable f are admissible in (1.2) and for them $\operatorname{ess\,sup} |f * f| \leq \sup f * f$. Averaging $f * f$ over $[-1/2, 1/2]$ gives $C_3' \geq 1$. The problem list [8] gives no lower bound for either constant, and [20] gives only this trivial bound for C_3. Step functions give $C_3 \leq 1.4631$ [20], and a step function with 600 cells gives $C_3 \leq 1.4603$ [7]; we checked the value 1.4603 in exact rational arithmetic. A step function with 800 cells is reported to give $C_3 \leq 1.4579$ [13], and a step function that gives an upper bound of about 1.4489 for C_3' is reported in [11]. Earlier upper bounds are listed in [8] and [2, Table 1 and Appendix A.5].

Theorem 1.3. *Let* $f\colon \mathbb{R} \to \mathbb{R}$ *be integrable, vanish almost everywhere outside* $[-1/4, 1/4]$*, and satisfy* $\int f \neq 0$. *Then*

$$\operatorname*{ess\,sup}_{t\in\mathbb{R}} |(f*f)(t)| \geq \operatorname*{ess\,sup}_{t\in\mathbb{R}} (f*f)(t) > \tfrac{4}{3} \Big(\int f\Big)^2.$$

Consequently $C_3 \geq C_3' \geq \frac{4}{3}$.

We prove Theorem 1.3 in Section 6. Since $C_3 \leq C_1$, it also gives $C_1 \geq 4/3$, which Theorem 1.1 improves by a different method. For the proof, let $\int f = 1$ and let M be the essential supremum of $f * f$; then $\hat{f}(z)^2 = M\big(S(z) - \hat{w}(z)\big)$ for complex z, where $S(z) = \sin(\pi z)/(\pi z)$ and $w =$

$\mathbf{1}_{[-1/2,1/2]} - (f*f)/M$ is nonnegative almost everywhere with $\int w = 1 - 1/M$. So all zeros of $S - \hat{w}$ have even order, whereas S has simple zeros, and the argument principle gives a point of a circle around the zero 1 of S at which $S = \lambda\hat{w}$ for some $\lambda \in (0,1]$. If $M \le \frac{4}{3}$, that is, $\int w \le 1/4$, such a point cannot lie on part of the circle, and on the rest of the circle it confines the values of $\hat{w}$; under these constraints an argument of the same kind on further ellipses shows that $S - \hat{w}$ has a zero of odd order, which is impossible (Section 6 outlines the argument before the proof).

For each theorem, two separately written checkers accept the certificate. Both theorems themselves, not only their certificates, are also proved in Lean 4 [15] with Mathlib [16], each in two ways: with finite checks evaluated by compiled code, and by Lean's kernel alone. For Theorem 1.1 the checkers check that the leaves of the search tree cover the simplex, up to the symmetry $p_i \mapsto p_{n-1-i}$, and evaluate the bound of Lemma 3.1 exactly at every leaf, so no solver needs to be trusted (Section 4.2); for Theorem 1.3 they work in ball arithmetic (Appendix B). Appendix A describes the formal proofs. The two parts of the paper are independent: Sections 2 to 5 concern Theorem 1.1 and Corollary 1.2, and Section 6, with Appendix B, proves Theorem 1.3.

2. Reduction to a finite problem

Fix $n \ge 1$ and put $h = 1/(2n)$. For $0 \le i < n$ let $B_i = [-\frac{1}{4} + ih,\ -\frac{1}{4} + (i+1)h)$, and let

$$\Delta_n = \Big\{ p \in \mathbb{R}^n :\ p_i \ge 0,\ \textstyle\sum_i p_i = 1 \Big\}.$$

For $0 \le c_1 \le c_2 \le 2n-2$ and $p \in \Delta_n$ define

$$q_{c_1 c_2}(p) = \frac{2n}{c_2 - c_1 + 2} \sum_{c_1 \le i+j \le c_2} p_i p_j, \tag{2.1}$$

where the sum runs over ordered pairs $(i,j) \in \{0,\dots,n-1\}^2$. Let $F_n(p) = \max_{c_1 \le c_2} q_{c_1 c_2}(p)$ and $V_n = \min_{p \in \Delta_n} F_n(p)$.

Lemma 2.1 (Cloninger–Steinerberger)**.** *$C_1 \ge V_n$ for every $n \ge 1$.*

Proof. Let f be measurable and nonnegative, and let $g = f\mathbf{1}_{[-1/4,1/4)}$. Then $g*g \le f*f$ pointwise and $\int g = \int_{-1/4}^{1/4} f$. If this integral is zero there is nothing to prove. If it is infinite, then $\int_{-1/2}^{1/2} g*g = (\int g)^2 = \infty$ by Tonelli's theorem, so the left side of (1.1) is infinite. Otherwise we scale so that $\int g = 1$. We write $g = \sum_i g_i$ with $g_i = g\mathbf{1}_{B_i}$ and put $p_i = \int g_i$, so that $p \in \Delta_n$. All terms of $g*g = \sum_{i,j} g_i * g_j$ are nonnegative, and $g_i * g_j$ vanishes outside $B_i + B_j \subseteq [-\frac{1}{2} + (i+j)h, -\frac{1}{2} + (i+j+2)h]$. For $c_1 \le c_2$ let $J = [-\frac{1}{2} + c_1 h, -\frac{1}{2} + (c_2+2)h] \subseteq [-\frac{1}{2}, \frac{1}{2}]$. If $c_1 \le i+j \le c_2$, then $B_i + B_j \subseteq J$, and $\int_J g_i * g_j = p_i p_j$ by Tonelli's theorem. Hence

$$|J| \sup_J g*g \ \ge\ \int_J g*g \ \ge \sum_{c_1 \le i+j \le c_2} p_i p_j,$$

and $\sup_{|t| \le 1/2} g*g \ge q_{c_1 c_2}(p)$ because $|J| = (c_2 - c_1 + 2)h$. We take the maximum over $c_1 \le c_2$ and obtain $\sup g*g \ge F_n(p) \ge V_n$. The same argument works with the essential supremum on J, which also bounds $|J|^{-1} \int_J g*g$ from above. □

The reversal $p_i \mapsto p_{n-1-i}$ maps the pair (c_1, c_2) to $(2n-2-c_2, 2n-2-c_1)$ and preserves $c_2 - c_1$, so it preserves F_n. One of p and its reversal satisfies $\sum_i (2i - n + 1)p_i \le 0$. Therefore

$$V_n = \min\Big\{ F_n(p) :\ p \in \Delta_n,\ \textstyle\sum_i (2i-n+1)p_i \le 0 \Big\}. \tag{2.2}$$

Theorem 2.2. $V_{39} \ge \frac{1337}{1000}$.

Theorem 1.1 follows from Lemma 2.1 and Theorem 2.2, and Corollary 1.2 follows from Theorem 1.1 and $\sigma^2 = 2/C_1$; by the remark after Theorem 1.1, it holds in either normalization. We prove Theorem 2.2 in Section 4.

3. Regions and their relaxations

3.1. **Regions.** Let $\mathcal{T}$ be the balanced binary tree of bin intervals. Its root is $\{0, \dots, n-1\}$, an interval with more than one bin has its two halves as children (the left half has $\lfloor \cdot/2 \rfloor$ bins), and its leaves are the single bins. For a block $D \in \mathcal{T}$ put $m_D = \sum_{i \in D} p_i$. A *region* is a set

$$R = \Big\{ p \in \Delta_n : \; L_D \le m_D \le U_D \; (D \in \mathcal{T}), \; \textstyle\sum_i (2i - n + 1) p_i \le 0 \Big\}$$

with rational bounds. The root region has $L_D = 0$ and $U_D = 1$. A region is split at a block D and a rational s with $L_D < s < U_D$ into the regions with U_D replaced by s and with L_D replaced by s. After a split the bounds are tightened by the rules $m_D = m_{D_1} + m_{D_2}$ for the children D_1, D_2 of D and $m_{\text{root}} = 1$, applied until they no longer change. A region whose tightened bounds cross is empty.

3.2. **The relaxation.** For p in a region R we consider the point $x(p)$ with the following coordinates: m_D for $D \in \mathcal{T}$; $Z_{ij} = p_i p_j$ for $i \le j$, where Z_{ji} stands for Z_{ij}; $Z_{DE} = m_D m_E$ for pairs of non-root blocks that are not both single bins (for two single bins, Z_{DE} stands for the corresponding Z_{ij}); the band masses $P_c = \sum_{i+j=c} p_i p_j$ over ordered pairs and their partial sums $G_c = P_0 + \cdots + P_c$ for $0 \le c \le 2n-2$; and $t = F_n(p)$. This point satisfies the following constraints.

(i) Window constraints $\frac{2n}{c_2 - c_1 + 2}(G_{c_2} - G_{c_1 - 1}) - t \le 0$ for $0 \le c_1 \le c_2 \le 2n-2$, with $G_{-1} = 0$.
(ii) Band, tree and product constraints: the definitions of P_c and G_c, the identities $m_D = m_{D_1} + m_{D_2}$, and the identities $Z_{DE} = Z_{D_1 E} + Z_{D_2 E}$ (or $Z_{DD} = Z_{D_1 D_1} + 2Z_{D_1 D_2} + Z_{D_2 D_2}$).
(iii) Simplex constraints $\sum_j Z_{ij} = p_i$ for each i, which hold because $\sum_j p_j = 1$. These are reformulation-linearization constraints in the sense of Sherali and Adams [23].
(iv) The symmetry constraint $\sum_i (2i - n + 1) p_i \le 0$.
(v) McCormick constraints [17]: for each pair of non-root blocks D, E, the four inequalities that state $(m_D - L_D)(m_E - L_E) \ge 0$, $(U_D - m_D)(U_E - m_E) \ge 0$, $(m_D - L_D)(U_E - m_E) \ge 0$ and $(U_D - m_D)(m_E - L_E) \ge 0$ after $m_D m_E$ is replaced by Z_{DE}.
(vi) Square constraints, in the spirit of Sherali and Fraticelli [24]: for distinct non-root blocks $D_1, \dots, D_k$ and integers $v_0, v_1, \dots, v_k$, the inequality obtained from $(v_0 + v_1 m_{D_1} + \cdots + v_k m_{D_k})^2 \ge 0$ by expanding the square and replacing the products of block masses by the corresponding variables Z.
(vii) The bounds $L_D \le m_D \le U_D$, $0 \le Z, P, G \le 1$ and $0 \le t \le 3$, the last one whenever $F_n(p) \le 3$.

Lemma 3.1. *Write finitely many of these constraints as $\ell_r \le a_r \cdot x \le u_r$ with $\ell_r, u_r \in \mathbb{Q} \cup \{\pm\infty\}$, and the bounds as $b^- \le x \le b^+$. Let y be a rational vector with $y_r \le 0$ whenever $\ell_r = -\infty$ and $y_r \ge 0$ whenever $u_r = \infty$, and put $\rho = e_t - \sum_r y_r a_r$. If*

$$\mathrm{LB}(y) = \sum_{y_r > 0} y_r \ell_r + \sum_{y_r < 0} y_r u_r + \sum_c \min(\rho_c b_c^-, \rho_c b_c^+) \;\ge\; \lambda$$

for some $\lambda \le 3$, then $F_n(p) \ge \lambda$ for every $p \in R$.

Proof. Suppose $p \in R$ and $F_n(p) < \lambda$. Then $x = x(p)$ satisfies all constraints and bounds, and $t = \rho \cdot x + \sum_r y_r (a_r \cdot x) \ge \mathrm{LB}(y) \ge \lambda$, a contradiction. □

The quantity $\mathrm{LB}(y)$ is the safe dual bound of Neumaier and Shcherbina [19], valid for any y with the stated signs, optimal or not.

4. The computation

4.1. **The search.** Throughout this section $n = 39$ and $\lambda = \frac{1337}{1000}$. We solved the linear programs with the open-source solver HiGHS [9] in double precision. At $n = 39$ the relaxation without square constraints has 17,085 rows and 3,158 columns. Window and McCormick constraints enter the linear programs lazily, when the current solution violates them. We obtain square constraints for pairs of blocks from an eigenvector of the matrix $\begin{pmatrix} 1 & m_D & m_E \\ m_D & Z_{DD} & Z_{DE} \\ m_E & Z_{DE} & Z_{EE} \end{pmatrix}$ for its smallest eigenvalue at the current solution, scaled and rounded to integers.

If the linear program does not close a node but its value is close to λ, we also solve Shor's semidefinite relaxation [25] with the interior-point solver Clarabel [6]. It keeps the equality rows of the linear program and those of its inequality rows that are nearly active at the solution, and it adds the condition that the matrix $M = \begin{pmatrix} 1 & p^T \\ p & Z \end{pmatrix}$, where $Z = (Z_{ij})$ is the matrix of the bin products, be positive semidefinite. The variables P_c, G_c and Z_{DE} for pairs of blocks that are not both single bins keep no bounds there: the checkers complete the multipliers of the rows that define these variables so that their reduced costs vanish, and a dual solution that used bounds on them would lose that part of its bound. If the value of this relaxation is at least λ, its dual solution gives multipliers for the rows and a positive semidefinite matrix S, which multiplies the condition $\langle S, M\rangle \geq 0$. Let $u = (u_0, u')$, with $u_0 \in \mathbb{R}$ and $u' \in \mathbb{R}^n$, be a unit eigenvector of S whose eigenvalue σ exceeds 10^{-7} times the largest one. The term $\sigma\, u^T M u$ of $\langle S, M\rangle$ is σ times the linearization of $(u_0 + u' \cdot p)^2$. We round $2^{20}u/\|u\|_\infty$ to an integer vector $v = (v_0, v')$ and replace this term by a multiple of the square constraint for $(v_0 + v' \cdot p)^2 \geq 0$; the terms with smaller eigenvalues, or with $v' = 0$, are dropped. With the multipliers of the rows, these square constraints give a dual vector of the linear relaxation. The search stores it like the dual vectors of the linear programs (see below), and if the floating-point check fails, it splits the node. These square constraints never enter the linear programs.

When neither program closes a node, we give every block D the score $\sum_E |Z_{DE} - m_D m_E|\,(1 + 20\, w_{DE}/\max w)$, where w_{DE} is the sum of the absolute duals of the pair's McCormick constraints. We split the block with the largest score at its mass in the optimal solution, clipped to the middle half of its interval. Splits are made at multiples of 2^{-30}, so that the search propagates bounds exactly in floating point, in agreement with the rational propagation in the checkers.

We distributed the tree over subtrees, which we call *jobs*; each job is stored as one log file. We call these files the *search logs*. Together with a file that fixes n, λ and the rows and columns, they form the certificate. The root job expands the tree to depth 9 and delegates the 330 open nodes there as new jobs. Every other job is processed depth-first by one worker, which delegates the unexplored nodes as new jobs once it has processed its budget of nodes. The budget only decides where jobs are cut. At most leaves (Table 1) the search stored a compressed dual vector, as in the certificates with stored dual vectors of Section 5, with the keys of the square constraints that it uses: the blocks and the integers $v_0, \ldots, v_k$. Its entries on most rows and on the square constraints are integers divided by a power of 2, and the checkers complete the remaining entries as the format in the repository specifies. The search stored such a vector only if it passed a floating-point check. Each of the other leaves is recorded without data; the search records a leaf in this way only if its floating-point bound is at least $\lambda + 10^{-7}$. The format also has a record for a leaf with an uncompressed dual vector, which no leaf needed. Unlike the archived certificate for $V_{39} \geq 267/200$ (Section 5), this certificate keeps the dual vectors: the linear programs of the checkers use square constraints for pairs of blocks only.

4.2. **The check.** We call the two programs the first checker and the second checker. At a leaf with a stored dual vector, the first checker completes the vector, builds each square constraint from the integers of its key, and evaluates $\mathrm{LB}(y)$ exactly; if this value is below λ, it rejects the

certificate. For a leaf without data, the first checker solves the relaxation of its region, with window and McCormick constraints added when they are violated. If this does not give a bound of at least λ, it adds square constraints for pairs of blocks, built from eigenvectors as in the search and rounded to integers, for a bounded number of rounds. It rounds the duals that it found to dyadic rationals and evaluates $\mathrm{LB}(y)$ exactly in integer arithmetic; the parameters of these steps, which do not affect correctness, are in the repository.

Proof of Theorem 2.2. We check each job separately: we recompute its root region from the splits on its path, follow its depth-first record, and recompute the child regions. Every node of a job receives exactly one record, a split, a delegation or a leaf, and no record is left over. A child whose tightened bounds cross would be empty and need no leaf, but no such child occurs. At a leaf recorded without data the checker first computes a dual vector y as described above. At every leaf it evaluates $\mathrm{LB}(y)$ exactly and finds $\mathrm{LB}(y) \geq \frac{1337}{1000}$, so Lemma 3.1 gives $F_{39} \geq \frac{1337}{1000}$ on the leaf region. The smallest value of $\mathrm{LB}(y)$ that it finds (Table 1) exceeds λ by about 10^{-8}. A final pass confirms three facts: every delegated subtree is the root of exactly one job, all jobs are reachable from the root job, and the delegation graph has no cycles. Because a delegated region and the root region of its job are recomputed from the same path, they coincide. The two children of a split cover their parent, so the leaf regions cover the region (2.2), and (2.2) gives $V_{39} \geq \frac{1337}{1000}$. The first checker performed these steps on the search logs. The Lean checker repeats the region, record, bound and partition checks on these logs, completed as described in Appendix A. □

The second checker differs from the first in the following respects.

(a) It evaluates $\mathrm{LB}(y)$ in rational arithmetic. It rounds the duals that it finds to multiples of 2^{-50}; for a square inequality, whose linear program carries a rescaled copy of the row, it rounds the dual of that copy and undoes the scaling. A stored dual vector is evaluated as stored.
(b) Its linear programs manage their rows differently and restart with other settings when they stall, and an exact Farkas test, never needed at any leaf, handles infeasible leaf programs.
(c) It recomputes the regions and checks the records of each job before it solves any linear program for that job, and its final step identifies every job file by its SHA-256 and then checks the partition as the first checker does.
(d) It tests a stored dual vector, which it first completes if it is stored in compressed form, before it searches for its own.

We ran it on the search logs. It accepted every leaf: at the leaves with a stored dual vector, this vector passed the test in (d), and at the leaves without data the second checker accepted the leaf with a dual vector that it found. The smallest bound $\mathrm{LB}(y)$ with which it accepted a leaf agrees with that of the first checker in all printed digits.

Table 1. The certificate of Theorem 2.2.

Bins n and bound λ	39, $\frac{1337}{1000}$
Nodes of the search tree	179,347,419
Leaves	89,673,710 (89,671,264 with a stored dual vector, 2,446 without data)
Smallest exact leaf bound	$1.33700001000\ldots$

5. Remarks

Limits of the reduction. We list in Table 2 upper bounds for V_n, each from an explicit mass vector found by a local search from random starting points and evaluated exactly. Independent runs agree on all digits shown. We release such vectors for $2 \le n \le 24$, for $n = 26, 28, \dots, 36$ and for $n = 39$. For $2 \le n \le 19$ the value is below 1.2937, and $V_1 = 1$, so the reduction needs at least 20 bins to improve on [14]. Since $V_{39} \le 1.349505$, Theorem 2.2 is within 0.0126 of the best bound available at $n = 39$.

Table 2. Upper bounds for V_n from explicit mass vectors, rounded up.

n	$V_n \le$	n	$V_n \le$	n	$V_n \le$	n	$V_n \le$
12	1.243365	19	1.292579	23	1.308665	30	1.331221
16	1.271793	20	1.294443	24	1.312492	32	1.335788
17	1.281014	21	1.299660	26	1.320130	34	1.338779
18	1.283145	22	1.304949	28	1.325596	36	1.342202
						39	1.349505

Further certificates. We also checked six further certificates, for $V_{39} \ge 267/200$, $V_{36} \ge 133/100$, $V_{30} \ge 33/25$, $V_{28} \ge 131/100$, $V_{24} \ge 13/10$ and $V_{20} \ge 32/25$, with between 113,761 and 527,163,006 leaves; the first three use square constraints. Both checkers of Theorem 2.2 accepted the first two, a checker for certificates that store the dual vector of every leaf accepted the third, and a third checker, for certificates without square constraints, the other three. The certificate for $V_{39} \ge 267/200$ comes from a search as in Section 4 with $\lambda = 267/200$, a root job of depth 8 and no semidefinite step. Its archived form keeps only the search tree, and the first checker accepted it in this form, finding its own dual vector at every leaf except two. For $V_{36} \ge 133/100$, a search of the same kind as in Section 4 was run, with $n = 36$ and $\lambda = 133/100$ and without compressed dual vectors; one leaf of its certificate carries a dual vector and 21 square constraints. The certificate for $V_{30} \ge 33/25$ stores the dual vector of every leaf, for most leaves in compressed form. The certificate for $V_{20} \ge 32/25$ gives an independent proof of the bound $C_1 \ge 1.28$ of [4]. With the same branching rule, the square constraints reduced the number of leaves by a factor of 2.5 at $n = 20$ and 2.3 at $n = 24$.

6. The signed third autocorrelation constant

In this section, which does not depend on Sections 2 to 5, we prove Theorem 1.3. We reduce it to a statement about the zeros of $S - \hat{\mu}$ for the measures μ of a class, outline the certificates, prove the lemmas behind multi-level certificates (Lemmas 6.1–6.5 and Proposition 6.7) and nested certificates (Lemmas 6.9 and 6.10 and Proposition 6.12), and then prove the theorem. The problem list [8] states the constants C_3 and C_3' with the maximum over $|t| \le 1/2$ and with $|\max_t (f*f)(t)|$ on the left of the second inequality. For $f \in L^2$ the function $f*f$ is continuous, so the maximum exists and equals the essential supremum. The absolute value in the second inequality of [8] does not matter, because $\operatorname{ess\,sup}(f*f) \ge \int_{-1/2}^{1/2} f*f = (\int f)^2$. For integrable f, the supremum of $f*f$ over any set of full measure on which it is defined is at least its essential supremum, so lower bounds for the constants in (1.2) hold for either reading.

Let f be as in the theorem. Replacing f by $f/\int f$ multiplies $f*f$ by the positive number $(\int f)^{-2}$, so we may assume $\int f = 1$. Let $g = f*f$. Then g is integrable, it vanishes almost everywhere outside $[-1/2, 1/2]$, and $\int g = 1$ by Fubini's theorem. In the *one-sided case* let $M = \operatorname{ess\,sup} g$, and in the *two-sided case* let $M = \operatorname{ess\,sup} |g|$. If $M = \infty$ there is nothing to

prove, so let $M < \infty$. Since $g \le M$ almost everywhere on $[-1/2, 1/2]$ and $\int_{-1/2}^{1/2} g = 1$, we have $M \ge 1$. Let $w = \mathbf{1}_{[-1/2,1/2]} - g/M$. After a change on a null set, $w \ge 0$, w vanishes outside $[-1/2, 1/2]$, and $\int w = 1 - 1/M$. In the two-sided case $g \ge -M$ almost everywhere, and we may also assume $w \le 2$.

For $z \in \mathbb{C}$ and $t \in \mathbb{R}$ let

$$F(z) = \hat{f}(z) = \int f(x) e^{-2\pi i x z}\, dx, \qquad K_t(z) = e^{-2\pi i t z}, \qquad S(z) = \int_{-1/2}^{1/2} K_t(z)\, dt = \frac{\sin \pi z}{\pi z},$$

with $S(0) = 1$. For a finite Borel measure μ on $[-1/2, 1/2]$ let $\hat{\mu}(z) = \int K_t(z)\, d\mu(t)$ and $G_\mu = S - \hat{\mu}$. We identify an integrable function ρ on $[-1/2, 1/2]$ with the measure $\rho(t)\, dt$. The functions F, $\hat{\mu}$ and G_μ are entire. Since $\iint |f(x) f(y) K_{x+y}(z)|\, dx\, dy \le \|f\|_1^2 e^{\pi |\operatorname{Im} z|}$, Fubini's theorem gives $\int g(t) K_t(z)\, dt = F(z)^2$, and therefore

$$F(z)^2 = M\, G_w(z), \qquad z \in \mathbb{C}. \tag{6.1}$$

The zeros of S are the nonzero integers, and they are simple because $S'(n) = (-1)^n/n$. Since $F(0) = \int f = 1$, the function F is not identically zero, and by (6.1) every zero of G_w has even order.

For $\tau > 0$ let $\mathcal{A}_\tau$ be the set of nonnegative Borel measures on $[-1/2, 1/2]$ of total mass at most τ, and let $\mathcal{A}_\tau^2$ be the set of measurable functions $\rho\colon [-1/2, 1/2] \to [0, 2]$ with $\int \rho \le \tau$. Both sets are convex and closed under multiplication by numbers in $[0, 1]$, and $\mathcal{A}_\tau^2 \subseteq \mathcal{A}_\tau$. We call $\mathcal{A}_\tau$ the class of the one-sided case and $\mathcal{A}_\tau^2$ the class of the two-sided case. If $1 - 1/M \le \tau$, then w belongs to the class of its case (for the same τ). The certificates below rule this out, because they show that G_μ has a zero of odd order for every μ in the class (Propositions 6.7 and 6.12).

The certificates work in levels. On an ellipse T_1 around the zero 1 of S, every measure μ of the class has a crossing unless G_μ has an odd number of zeros inside T_1: for some $\lambda \in (0, 1]$, the function $S - \lambda\hat{\mu}$ vanishes at a point z of T_1 (Lemma 6.1 below). At this point, $S(z)$ lies in a convex set whose size is proportional to τ. If τ is small, a line separates $S(z)$ from this set on part of T_1 (Lemma 6.2). On the rest, the crossing confines the value of $\hat{\mu}$ at a nearby point to a thin neighbourhood of a ray (Lemma 6.5). Under this constraint an argument of the same kind on a second ellipse, a tile around the zero 3 of S, shows that G_μ has a zero of odd order (Lemmas 6.3 and 6.4). Where this second step fails on part of a tile, a crossing there confines $\hat{\mu}$ further (Lemma 6.9), and the argument is repeated under the new constraint, with further tiles near 3, 4.5 and 6.4.

Lemma 6.1 (first level)**.** *Let μ be a finite Borel measure on $[-1/2, 1/2]$, and let Γ be a piecewise smooth Jordan curve that passes through no zero of S and encloses an odd number of them. Then G_μ has no zero on Γ and an odd number of zeros inside Γ, counted with multiplicity, or there are $z \in \Gamma$ and $\lambda \in (0, 1]$ with $S(z) = \lambda\hat{\mu}(z)$.*

Proof. For $0 \le \lambda \le 1$ the function $G_{\lambda\mu} = S - \lambda\hat{\mu}$ is entire, and $G_{\lambda\mu}(z)$ and $G'_{\lambda\mu}(z)$ depend continuously on (λ, z). Suppose that no $G_{\lambda\mu}$ vanishes on Γ. Then $|G_{\lambda\mu}(z)|$ has a positive lower bound on the compact set $[0, 1] \times \Gamma$, so the number of zeros of $G_{\lambda\mu}$ inside Γ, counted with multiplicity,

$$N(\lambda) = \frac{1}{2\pi i} \oint_\Gamma \frac{G'_{\lambda\mu}(z)}{G_{\lambda\mu}(z)}\, dz \qquad (\Gamma \text{ oriented counterclockwise}),$$

depends continuously on λ. As an integer, $N(\lambda)$ is constant. Thus $N(1) = N(0)$, and $N(0)$ is odd because Γ encloses an odd number of zeros of $G_0 = S$ and they are simple. Otherwise $G_{\lambda\mu}(z) = 0$ for some $\lambda \in [0, 1]$ and $z \in \Gamma$, and $\lambda > 0$ because S has no zero on Γ. □

Lemma 6.1 is a homotopy form of Rouché's theorem. We call a point z as in its second alternative a *crossing* for μ. For $\mu = w$ the first alternative contradicts (6.1), so w has a crossing on Γ. The next lemma bounds the real part of $\bar{u}\hat{\mu}(z)$ for the measures of the two classes.

Lemma 6.2. *Let $\phi\colon [-1/2, 1/2] \to \mathbb{R}$ be continuous and $\tau > 0$.*

(a) $\int \phi\, d\mu \le \tau \max(0, \max \phi)$ for every $\mu \in \mathcal{A}_\tau$.

(b) $\int \rho\phi \le \lambda_0 \tau + 2\int \max(\phi - \lambda_0, 0)$ for every $\rho \in \mathcal{A}_\tau^2$ and every $\lambda_0 \ge 0$.

Proof. Part (a) holds because $\phi \le \max(0, \max\phi)$ and μ is nonnegative with mass at most τ. In (b), $\int \rho\phi = \lambda_0 \int \rho + \int \rho(\phi - \lambda_0)$. Here $\lambda_0 \int \rho \le \lambda_0 \tau$ because $\lambda_0 \ge 0$, and $\rho(\phi - \lambda_0) \le \rho \max(\phi - \lambda_0, 0) \le 2\max(\phi - \lambda_0, 0)$. □

In the one-sided case let $B_\tau(\phi) = \tau \max(0, \max\phi)$. In the two-sided case let $B_\tau(\phi) = \lambda_0\tau + 2\int \max(\phi - \lambda_0, 0)$, where $\lambda_0 \ge 0$ is a number that the certificate supplies with ϕ (Definition 6.6). By Lemma 6.2, $\int \phi\, d\mu \le B_\tau(\phi)$ for every μ in the class of the case. If $\mathrm{Re}(\bar{u}S(z)) > B_\tau(\phi)$ for $\phi(t) = \mathrm{Re}(\bar{u}K_t(z))$, then the functional $\zeta \mapsto \mathrm{Re}(\bar{u}\zeta)$ separates $S(z)$ from the convex set of all $\hat{\mu}(z)$ with μ in the class, and no measure of the class has a crossing at z. Where this separation fails, we restrict the values of $\hat{\mu}$ at finitely many points and use witnesses.

Let $\tau' > 0$, $z_c \in \mathbb{C}$, $r \ge 0$, let $p_1, \dots, p_k \in \mathbb{C}$ with $k \ge 0$, and let $Q_1, \dots, Q_k \subset \mathbb{C}$ be closed rectangles with sides parallel to the axes. Let $\mathcal{P} = \mathcal{P}(\tau', z_c, r; p_1, Q_1; \dots; p_k, Q_k)$ be the set of measures ν in the class of the case, with τ' in place of τ, for which some $\sigma \ge 1$ satisfies $|\hat{\nu}(z_c) - \sigma S(z_c)| \le r$ and for which $\hat{\nu}(p_j) \in Q_j$ for $j = 1, \dots, k$. We say that $\mathcal{P}$ pins the values of $\hat{\nu}$ at z_c and at the points p_j. This set is convex: $\nu \mapsto \hat{\nu}(p)$ is linear, discs and rectangles are convex, and convex combinations of the numbers σ preserve the condition at z_c.

Lemma 6.3 (pinned sets)**.** *Let $\mathcal{P}$ be as above, let $v, y_1, \dots, y_k \in \mathbb{C}$, and let $\Lambda(t) = \mathrm{Re}(\bar{v}K_t(z_c)) + \sum_j \mathrm{Re}(\bar{y}_j K_t(p_j))$. In the two-sided case $B_{\tau'}$ may be formed with any $\lambda_0 \ge 0$.*

(a) If $\mathrm{Re}(\bar{v}S(z_c)) \ge 0$ and

$$B_{\tau'}(\Lambda) < \mathrm{Re}(\bar{v}S(z_c)) - |v|r + \sum_j \min_{x \in Q_j} \mathrm{Re}(\bar{y}_j x), \tag{6.2}$$

then $\mathcal{P}$ is empty.

(b) Let $p, u \in \mathbb{C}$ and $\phi_p(t) = \mathrm{Re}(\bar{u}K_t(p)) - \Lambda(t)$. If $\mathrm{Re}(\bar{v}S(z_c)) \le 0$ and

$$\mathrm{Re}(\bar{u}S(p)) - \mathrm{Re}(\bar{v}S(z_c)) - |v|r - \sum_j \max_{x \in Q_j} \mathrm{Re}(\bar{y}_j x) > B_{\tau'}(\phi_p), \tag{6.3}$$

then $G_\nu(p) \ne 0$ for every $\nu \in \mathcal{P}$.

Proof. Let $\nu \in \mathcal{P}$, with σ as in the definition. Then $\mathrm{Re}(\bar{v}\hat{\nu}(z_c))$ differs from $\sigma\,\mathrm{Re}(\bar{v}S(z_c))$ by at most $|v|r$, and $\mathrm{Re}(\bar{y}_j\hat{\nu}(p_j))$ lies between the minimum and the maximum of $\mathrm{Re}(\bar{y}_j x)$ over $x \in Q_j$. Moreover $\int \Lambda\, d\nu = \mathrm{Re}(\bar{v}\hat{\nu}(z_c)) + \sum_j \mathrm{Re}(\bar{y}_j\hat{\nu}(p_j))$. In (a), $\mathrm{Re}(\bar{v}S(z_c)) \ge 0$ and $\sigma \ge 1$ give

$$\int \Lambda\, d\nu \ge \mathrm{Re}(\bar{v}S(z_c)) - |v|r + \sum_j \min_{x \in Q_j} \mathrm{Re}(\bar{y}_j x),$$

which together with (6.2) contradicts Lemma 6.2. In (b), suppose that $G_\nu(p) = 0$. Then $\hat{\nu}(p) = S(p)$, and $\mathrm{Re}(\bar{v}S(z_c)) \le 0$ and $\sigma \ge 1$ give

$$\mathrm{Re}(\bar{u}S(p)) = \int \phi_p\, d\nu + \int \Lambda\, d\nu \le B_{\tau'}(\phi_p) + \mathrm{Re}(\bar{v}S(z_c)) + |v|r + \sum_j \max_{x \in Q_j} \mathrm{Re}(\bar{y}_j x)$$

by Lemma 6.2. This contradicts (6.3). □

Lemma 6.4 (witness covers)**.** *Let μ be a finite Borel measure on $[-1/2, 1/2]$, and let $\mathcal{K}_1, \dots, \mathcal{K}_m$ be convex sets of such measures with $\mu \in \mathcal{K}_1 \cup \dots \cup \mathcal{K}_m$. Suppose that for each j either $\mathcal{K}_j$ is empty, or there are a piecewise smooth Jordan curve T_j and a measure $\nu_j \in \mathcal{K}_j$ such that no G_ν with $\nu \in \mathcal{K}_j$ vanishes on T_j and G_{ν_j} has an odd number of zeros inside T_j, counted with multiplicity. Then G_μ has a zero of odd order.*

Proof. Let μ lie in $\mathcal{K}_j$. Then $\mathcal{K}_j$ is not empty. For $0 \le \theta \le 1$ the measure $\mu_\theta = (1-\theta)\mu + \theta\nu_j$ lies in $\mathcal{K}_j$, and $G_{\mu_\theta} = (1-\theta)G_\mu + \theta G_{\nu_j}$. As in the proof of Lemma 6.1, the number of zeros of G_{μ_θ} inside T_j depends continuously on θ, so it is constant. Hence G_μ has an odd number of zeros inside T_j, and one of them has odd order. □

Lemma 6.5 (localization)**.** *Let $A \subset \mathbb{C}$ be a set with a point $z_c \in A$, and let $U \supseteq A$ be convex. Let d, Y, L, m_S be numbers with $|z - z_c| \le d$ and $|S(z)| \ge m_S > 0$ for $z \in A$, and $|\operatorname{Im}\zeta| \le Y$ and $|S'(\zeta)| \le L$ for $\zeta \in U$. Put $\sigma_{\max} = \tau e^{\pi Y}/m_S$ and $r_\tau = d(\pi\tau e^{\pi Y} + \sigma_{\max} L)$. If $\mu \in \mathcal{A}_\tau$, $z \in A$ and $\lambda \in (0, 1]$ satisfy $S(z) = \lambda\hat{\mu}(z)$, then $\sigma = 1/\lambda \ge 1$ satisfies $|\hat{\mu}(z_c) - \sigma S(z_c)| \le r_\tau$. Moreover $|\hat{\mu}(p)| \le \tau e^{\pi|\operatorname{Im} p|}$ for every $p \in \mathbb{C}$ and every $\mu \in \mathcal{A}_\tau$.*

Proof. We have $\hat{\mu}(z) = \sigma S(z)$. Since the segment from z to z_c lies in U and $|2\pi t K_t(\zeta)| \le \pi e^{\pi|\operatorname{Im}\zeta|}$ for $|t| \le 1/2$, we get $|\hat{\mu}(z) - \hat{\mu}(z_c)| \le \int |K_t(z) - K_t(z_c)|\, d\mu(t) \le \pi\tau d e^{\pi Y}$. Moreover $\sigma = |\hat{\mu}(z)|/|S(z)| \le \tau e^{\pi|\operatorname{Im} z|}/m_S \le \sigma_{\max}$ and $|S(z) - S(z_c)| \le dL$. Hence $|\hat{\mu}(z_c) - \sigma S(z_c)| \le |\hat{\mu}(z_c) - \hat{\mu}(z)| + \sigma|S(z) - S(z_c)| \le r_\tau$. The last claim holds because $|K_t(p)| \le e^{\pi|\operatorname{Im} p|}$ for $|t| \le 1/2$. □

Definition 6.6. Let $0 < \tau < 1$. A *certificate* for τ, in the one-sided or in the two-sided case, consists of the following data.

(i) An ellipse T_1, parametrized by $z(s) = c + a\cos 2\pi s + ib\sin 2\pi s$ for $0 \le s \le 1$ with real c and $a, b > 0$, that passes through no zero of S and encloses an odd number of them, and a subdivision of $[0, 1]$ into intervals of two types, E and H.

(ii) For each interval of type E, a number $u \in \mathbb{C}$, and in the two-sided case a number $\lambda_0 \ge 0$ with which B_τ is formed, such that $\operatorname{Re}(\bar{u}S(z)) > B_\tau(\phi)$ for $\phi(t) = \operatorname{Re}(\bar{u}K_t(z))$ at every point z of the arc.

(iii) For each interval $[s_0, s_1]$ of type H: a point $z_c = z(s_c)$ with $s_0 \le s_c \le s_1$; numbers d, Y, L, m_S as in Lemma 6.5 for the arc $z([s_0, s_1])$ and a convex set containing it, and a number $r \ge r_\tau$; points $p_1, \dots, p_k \in \mathbb{C}$ with $k \ge 0$ and numbers $R_j \ge \tau e^{\pi|\operatorname{Im} p_j|}$; and finitely many products $Q = Q_1 \times \dots \times Q_k$ of closed rectangles with sides parallel to the axes, called *leaves*, whose union contains the product of the squares $\{x \in \mathbb{C} : |\operatorname{Re} x|, |\operatorname{Im} x| \le R_j\}$. For $k = 0$ there is a single leaf. Each leaf carries one of the following.

- An *exclusion*: numbers $v, y_1, \dots, y_k \in \mathbb{C}$, and in the two-sided case $\lambda_0 \ge 0$, that satisfy $\operatorname{Re}(\bar{v}S(z_c)) \ge 0$ and (6.2) with $\tau' = \tau$.
- A *witness*, which consists of the following.
  - (a) Numbers $\tau' \ge \tau$ and $r' \ge r_\tau$.
  - (b) An ellipse T, called the tile, parametrized by $p(q) = c_T + a_T\cos 2\pi q + ib_T\sin 2\pi q$ for $0 \le q \le 1$ with complex c_T and $a_T, b_T > 0$, and a subdivision of $[0, 1]$ into intervals that define the tile arcs.
  - (c) For each tile arc, numbers $u, v, y_1, \dots, y_k \in \mathbb{C}$, and in the two-sided case $\lambda_0 \ge 0$, that satisfy $\operatorname{Re}(\bar{v}S(z_c)) \le 0$ and (6.3), with this τ' and with r' in place of r, at every point p of the tile arc.
  - (d) A measure $\nu_{\text{rep}} \in \mathcal{P}(\tau', z_c, r'; p_1, Q_1; \dots; p_k, Q_k)$ such that $G_{\nu_{\text{rep}}}$ has no zero on T and an odd number of zeros inside T, counted with multiplicity.

A certificate whose intervals all have type E is a single-contour certificate, and its correctness rests on Lemmas 6.1 and 6.2 alone. We say that the ellipse T_1 forms the first level, the intervals of type H with $k = 0$ the second level, and those with $k \geq 1$ the third level. A certificate without intervals of the third level is a two-level certificate. On an arc of the second level, a crossing confines $\hat{\mu}(z_c)$ to a disc around a point $\sigma S(z_c)$, and under this constraint G_μ has an odd number of zeros inside the tile. The nested certificate of Theorem 1.3 has no third level in the sense of Definition 6.6: on each of its intervals of type H we have $k = 0$, and the single leaf carries a tree of nodes as in Definition 6.11 below. Its tiles are the following. Seven are ellipses around the zero 3 of S; two of them also enclose the zero 2, and one also encloses the zero 4. A circle of radius 0.45 around $4.55 - 0.25i$ encloses no zero of S. An ellipse around $4.57 + 0.157i$ encloses the zeros 4 and 5, and an ellipse around $6.44 - 0.05i$ encloses the zero 6. Each of these comes with its mirror image. The remaining tile is an ellipse around 6.35, symmetric about $\mathbb{R}$, that encloses the zeros 6 and 7. The lemmas need no condition on the zeros of S inside a tile. The reflection $t \mapsto -t$ maps each class to itself and replaces $\hat{\mu}(z)$ by $\overline{\hat{\mu}(\bar{z})}$, so every condition at a point z has a counterpart at $\bar{z}$; this is why the tiles come in conjugate pairs. The checkers nevertheless do not use this symmetry; the nested certificate of Theorem 1.3 is checked on every interval of $[0, 1]$.

Proposition 6.7 (multi-level certificates)**.** *If a certificate for τ exists, then G_μ has a zero of odd order for every μ in the class of the case.*

Proof. Let μ be in the class. By Lemma 6.1 for $\Gamma = T_1$, either G_μ has an odd number of zeros inside T_1, and then one of them has odd order, or μ has a crossing $z = z(s)$ on T_1 with $S(z) = \lambda\hat{\mu}(z)$ and $\lambda \in (0, 1]$. In the second case let s lie in an interval I of the certificate. If I has type E, then $\lambda\mu$ belongs to the class, and $\operatorname{Re}(\bar{u}S(z)) = \int \phi \, d(\lambda\mu) \leq B_\tau(\phi)$ by Lemma 6.2, which contradicts (ii). So I has type H. By Lemma 6.5, some $\sigma \geq 1$ satisfies $|\hat{\mu}(z_c) - \sigma S(z_c)| \leq r_\tau$, and $|\operatorname{Re}\hat{\mu}(p_j)|, |\operatorname{Im}\hat{\mu}(p_j)| \leq R_j$ for every j. So μ belongs to $\mathcal{P}(\tau, z_c, r_\tau; p_1, Q_1; \ldots; p_k, Q_k)$ for some leaf Q. For a leaf with an exclusion let $\mathcal{K}_Q = \mathcal{P}(\tau, z_c, r; p_1, Q_1; \ldots; p_k, Q_k)$. It contains the former set because $r \geq r_\tau$, and it is empty by Lemma 6.3(a). For a leaf with a witness let $\mathcal{K}_Q = \mathcal{P}(\tau', z_c, r'; p_1, Q_1; \ldots; p_k, Q_k)$. It contains the former set because $\tau' \geq \tau$ and $r' \geq r_\tau$, it contains ν_{rep}, and by Lemma 6.3(b) no G_ν with $\nu \in \mathcal{K}_Q$ vanishes on the tile. Lemma 6.4 with the sets $\mathcal{K}_Q$ gives the claim. □

Corollary 6.8. *Let f be as in Theorem 1.3. If a certificate for τ exists in the one-sided case, then* $\operatorname{ess\,sup}(f * f) > (\int f)^2/(1 - \tau)$. *If one exists in the two-sided case, then* $\operatorname{ess\,sup}|f * f| > (\int f)^2/(1 - \tau)$.

Proof. We may assume $\int f = 1$ and $M < \infty$, as at the beginning of this section. If $1 - 1/M \leq \tau$, then w belongs to the class of its case, and G_w has a zero of odd order by Proposition 6.7. This contradicts (6.1). Hence $1 - 1/M > \tau$, that is, $M > 1/(1 - \tau)$. □

Nested certificates. The certificate behind the bound $\frac{4}{3}$ needs one more step. At a witness, separation may fail on part of the tile. A measure of the leaf's set then has a crossing of a second kind on the tile, and this crossing confines the measure further, so that a failing arc can be treated in the same way as a leaf.

Lemma 6.9 (crossings at a base measure)**.** *Let T be a piecewise smooth Jordan curve, and let ν_0 and μ be finite Borel measures on $[-1/2, 1/2]$. Suppose that G_{ν_0} has no zero on T and an odd number of zeros inside T, counted with multiplicity, and that every zero of G_μ has even order. Then there are $z \in T$ and $\kappa \geq 0$ with $\hat{\mu}(z) = S(z) + \kappa G_{\nu_0}(z)$.*

Proof. For $0 \leq \theta \leq 1$ let $\mu_\theta = (1 - \theta)\nu_0 + \theta\mu$, so that $G_{\mu_\theta} = (1 - \theta)G_{\nu_0} + \theta G_\mu$. If G_μ vanishes at a point of T, take $\kappa = 0$. Otherwise G_μ is not identically zero, and it has an even number of zeros inside T. If no G_{μ_θ} vanished on T, then, as in the proof of Lemma 6.1, the number of

zeros of G_{μ_θ} inside T would not depend on θ; but it is odd for $\theta = 0$ and even for $\theta = 1$. Hence $G_{\mu_\theta}(z) = 0$ for some $\theta \in [0,1]$ and $z \in T$, and $\theta > 0$ because G_{ν_0} has no zero on T. Dividing $(1-\theta)G_{\nu_0}(z) + \theta G_\mu(z) = 0$ by θ gives the claim with $\kappa = (1-\theta)/\theta$. □

Fix $\varepsilon \geq 0$. Let $A = p([q_0, q_1])$ be an arc of a tile T with parametrization $p(q)$, and let ν_0 be a finite Borel measure on $[-1/2, 1/2]$. A measure μ satisfies the *tube condition* (A, ν_0) if there are $z \in A$ and $\kappa \geq 0$ with $|\hat{\mu}(z) - S(z) - \kappa G_{\nu_0}(z)| \leq \varepsilon$. A *node* N below an interval of type H consists of numbers $\tau_N \geq \tau$ and $r_N \geq r_\tau$, where r_τ is formed with some numbers d, Y, L, m_S as in Lemma 6.5 for the arc of T_1 and a convex set containing it, a product $Q_1 \times \cdots \times Q_k$ of closed rectangles and finitely many tube conditions $(A_1, \nu_1), \dots, (A_m, \nu_m)$. In the one-sided case let E_N be the set of measures in $\mathcal{P}(\tau_N, z_c, r_N; p_1, Q_1; \dots; p_k, Q_k)$ that satisfy these tube conditions. This set need not be convex, and we write $\operatorname{conv} E_N$ for its convex hull.

Lemma 6.10 (tubes)**.** *Let N be a node in the one-sided case, let (A_l, ν_l) for $l = 1, \dots, m$ be its tube conditions, and let $v, y_1, \dots, y_k, v_1, \dots, v_m \in \mathbb{C}$.*

(a) Suppose that $\operatorname{Re}(\bar{v} S(z_c)) \geq 0$, that $\operatorname{Re}(\bar{v}_l G_{\nu_l}(\zeta)) \geq 0$ for $\zeta \in A_l$ and every l, and that

$$B_{\tau_N}(\Lambda) < \operatorname{Re}(\bar{v} S(z_c)) - |v| r_N + \sum_j \min_{x \in Q_j} \operatorname{Re}(\bar{y}_j x) + \sum_l \Big(\min_{\zeta \in A_l} \operatorname{Re}(\bar{v}_l S(\zeta)) - |v_l| \varepsilon \Big)$$

for $\Lambda(t) = \operatorname{Re}(\bar{v} K_t(z_c)) + \sum_j \operatorname{Re}(\bar{y}_j K_t(p_j)) + \sum_l \max_{\zeta \in A_l} \operatorname{Re}(\bar{v}_l K_t(\zeta))$. Then E_N is empty.

(b) Let $p, u \in \mathbb{C}$. Suppose that $\operatorname{Re}(\bar{v} S(z_c)) \leq 0$, that $\operatorname{Re}(\bar{v}_l G_{\nu_l}(\zeta)) \leq 0$ for $\zeta \in A_l$ and every l, and that

$$\operatorname{Re}(\bar{u} S(p)) - \operatorname{Re}(\bar{v} S(z_c)) - |v| r_N - \sum_j \max_{x \in Q_j} \operatorname{Re}(\bar{y}_j x) - \sum_l \Big(\max_{\zeta \in A_l} \operatorname{Re}(\bar{v}_l S(\zeta)) + |v_l| \varepsilon \Big) > B_{\tau_N}(\Phi)$$

for $\Phi(t) = \operatorname{Re}(\bar{u} K_t(p)) - \operatorname{Re}(\bar{v} K_t(z_c)) - \sum_j \operatorname{Re}(\bar{y}_j K_t(p_j)) + \sum_l \max_{\zeta \in A_l} \big(-\operatorname{Re}(\bar{v}_l K_t(\zeta)) \big)$. Then $G_\nu(p) \neq 0$ for every $\nu \in \operatorname{conv} E_N$.

Proof. The arcs A_l are compact, so these extrema exist, and Λ and Φ are continuous. Let $\mu \in E_N$, with σ as in the definition of $\mathcal{P}$, and with points $z_l \in A_l$ and numbers $\kappa_l \geq 0$ for its tube conditions. Then $\operatorname{Re}(\bar{v}_l \hat{\mu}(z_l))$ differs from $\operatorname{Re}(\bar{v}_l S(z_l)) + \kappa_l \operatorname{Re}(\bar{v}_l G_{\nu_l}(z_l))$ by at most $|v_l| \varepsilon$. In (a) let $\lambda(t) = \operatorname{Re}(\bar{v} K_t(z_c)) + \sum_j \operatorname{Re}(\bar{y}_j K_t(p_j)) + \sum_l \operatorname{Re}(\bar{v}_l K_t(z_l))$. As in the proof of Lemma 6.3, the sign conditions give

$$\int \lambda \, d\mu \geq \operatorname{Re}(\bar{v} S(z_c)) - |v| r_N + \sum_j \min_{x \in Q_j} \operatorname{Re}(\bar{y}_j x) + \sum_l \Big(\min_{\zeta \in A_l} \operatorname{Re}(\bar{v}_l S(\zeta)) - |v_l| \varepsilon \Big),$$

while $\int \lambda \, d\mu \leq B_{\tau_N}(\lambda) \leq B_{\tau_N}(\Lambda)$ by Lemma 6.2, because $z_l \in A_l$ gives $\lambda \leq \Lambda$. This contradicts the hypothesis, so E_N is empty. In (b) let $\phi(t) = \operatorname{Re}(\bar{u} K_t(p)) - \operatorname{Re}(\bar{v} K_t(z_c)) - \sum_j \operatorname{Re}(\bar{y}_j K_t(p_j)) - \sum_l \operatorname{Re}(\bar{v}_l K_t(z_l))$. Then $\phi \leq \Phi$, and the sign conditions give

$$\operatorname{Re}(\bar{u} \hat{\mu}(p)) = \int \phi \, d\mu + \operatorname{Re}(\bar{v} \hat{\mu}(z_c)) + \sum_j \operatorname{Re}(\bar{y}_j \hat{\mu}(p_j)) + \sum_l \operatorname{Re}(\bar{v}_l \hat{\mu}(z_l)) \leq \beta,$$

where $\beta = B_{\tau_N}(\Phi) + \operatorname{Re}(\bar{v} S(z_c)) + |v| r_N + \sum_j \max_{x \in Q_j} \operatorname{Re}(\bar{y}_j x) + \sum_l (\max_{\zeta \in A_l} \operatorname{Re}(\bar{v}_l S(\zeta)) + |v_l| \varepsilon)$. The number β does not depend on μ, and $\nu \mapsto \operatorname{Re}(\bar{u} \hat{\nu}(p))$ is linear, so $\operatorname{Re}(\bar{u} \hat{\nu}(p)) \leq \beta$ for every $\nu \in \operatorname{conv} E_N$. If $G_\nu(p) = 0$, then $\operatorname{Re}(\bar{u} S(p)) = \operatorname{Re}(\bar{u} \hat{\nu}(p)) \leq \beta$, which contradicts the hypothesis. □

Definition 6.11. A *nested certificate* for τ in the one-sided case consists of the data of Definition 6.6, except that each leaf Q of an interval of type H carries a finite tree of nodes in place of an exclusion or a witness. The root of the tree has the rectangles of Q and no tube conditions. Each node N has one of the following kinds.

- *Empty*: numbers as in Lemma 6.10(a).
- *Split*: an index j; the four children of N arise from dividing Q_j into four equal rectangles.
- *Arc split*: an index l and a number q_m with $q_0 < q_m < q_1$, where $A_l = p([q_0, q_1])$ and p is the parametrization of the tile of A_l; in the two children of N the arc A_l is replaced by $p([q_0, q_m])$ and by $p([q_m, q_1])$.
- *Witness*: a tile T as in Definition 6.6, a measure $\nu \in E_N$ such that G_ν has no zero on T and an odd number of zeros inside T, counted with multiplicity, and a subdivision of the parameter interval of T into tile arcs. Each tile arc A carries either numbers as in Lemma 6.10(b) for every point p of A, or a child N' whose tube conditions are those of N together with (A, ν).

Each node has its own numbers τ_N and r_N, and except where stated, a child has the rectangles and the tube conditions of its parent. An exclusion of Definition 6.6 is an empty node without tube conditions, and a witness there is a witness node all of whose tile arcs carry separations.

Proposition 6.12 (nested certificates)**.** *If a nested certificate for τ exists in the one-sided case, then G_μ has a zero of odd order for every $\mu \in \mathcal{A}_\tau$.*

Proof. Suppose that every zero of G_μ has even order for some $\mu \in \mathcal{A}_\tau$. As in the proof of Proposition 6.7, μ has a crossing $z(s)$ with $S(z(s)) = \lambda\hat{\mu}(z(s))$ and $\lambda \in (0, 1]$, where s lies in an interval of type H, and $\hat{\mu}(p_j) \in Q_j$ for every j, for some leaf Q of this interval. Every node N below this interval has $\tau_N \geq \tau$ and $r_N \geq r_\tau$, so $\mu \in \mathcal{A}_{\tau_N}$, and by Lemma 6.5 the number $\sigma = 1/\lambda$ satisfies $|\hat{\mu}(z_c) - \sigma S(z_c)| \leq r_N$. Hence $\mu \in E_N$ whenever μ satisfies the rectangles and the tube conditions of N, in particular for the root N of the tree of Q. We show that $\mu \in E_N$ implies $\mu \in E_{N'}$ for some child N' of N. As the tree is finite, this is a contradiction. An empty node has $E_N = \varnothing$ by Lemma 6.10(a). At a split, $\hat{\mu}(p_j)$ lies in one of the four rectangles. At an arc split, a point $z_l \in A_l$ as in the tube condition (A_l, ν_l) for μ lies in one of the two halves of A_l. At a witness, Lemma 6.9 with $\nu_0 = \nu$ gives $z \in T$ and $\kappa \geq 0$ with $\hat{\mu}(z) = S(z) + \kappa G_\nu(z)$. Then $G_{\mu_\theta}(z) = 0$ for $\mu_\theta = (1-\theta)\nu + \theta\mu$ and $\theta = 1/(1+\kappa)$, and $\mu_\theta \in \operatorname{conv} E_N$. By Lemma 6.10(b), z lies on no tile arc with a separation. So z lies on a tile arc A with a child N', and μ satisfies the tube condition (A, ν) with this z and κ, even with $\hat{\mu}(z) - S(z) - \kappa G_\nu(z) = 0$. As μ also satisfies the rectangles and the tube conditions of N, we get $\mu \in E_{N'}$. □

Here the induction runs over E_N and not over $\operatorname{conv} E_N$: a measure in $\operatorname{conv} E_N$ that satisfies a new tube condition need not lie in the convex hull of the measures of E_N that satisfy it.

Corollary 6.13. *Let f be as in Theorem 1.3. If a nested certificate for τ exists in the one-sided case, then* $\operatorname{ess\,sup}(f * f) > (\int f)^2/(1-\tau)$.

Proof. As for Corollary 6.8, with Proposition 6.12 in place of Proposition 6.7. □

The proof of Theorem 1.3 below uses only the one-sided case. The two-sided case enters only the limits at the end of this section.

Proof of Theorem 1.3. The nested certificate of Theorem 1.3 (Table 3) uses for T_1 the circle with $c = 21/20$ and $a = b = 3/5$. Its interior meets $\mathbb{R}$ in the interval $(c-a, c+a) = (0.45, 1.65)$. All zeros of S are real, so T_1 encloses exactly one of them, the zero 1, and passes through none. Its intervals of type H have no pinned points. It is a nested certificate for $\tau = \frac{1}{4}$ in the one-sided case, with $\varepsilon = 10^{-6}$ in the tube conditions. The checks described in Appendix B confirm that its intervals subdivide $[0, 1]$, that the tile arcs of every witness subdivide the parameter interval of its tile, and that the conditions of Definitions 6.6 and 6.11 hold. Since $1/(1-\frac{1}{4}) = \frac{4}{3}$, Corollary 6.13 gives $\operatorname{ess\,sup}(f * f) > \frac{4}{3}(\int f)^2$, and $\operatorname{ess\,sup}|f * f| \geq \operatorname{ess\,sup}(f * f)$. If $\int f = 0$,

the right sides of the inequalities in (1.2) vanish, and the left sides are nonnegative because $\operatorname{ess\,sup}(f*f) \geq \int_{-1/2}^{1/2} f*f = 0$. Hence $C_3 \geq C_3' \geq \frac{4}{3}$. □

TABLE 3. The nested certificate of Theorem 1.3 (one-sided case).

Threshold τ; ε	$\frac{1}{4}$; 10^{-6}
Intervals of type E; of type H (records of type N)	276; 2,182
Nodes: empty; arc split; witness	15,172,398; 15,100,886; 7,924,564
Tube conditions at a node; arc splits in a row	at most 2; at most 8
τ_N of the empty nodes and witnesses	τ, except at 81,508 of them (at most 101/400)

Certificates, checks and formal proofs. Appendix B describes the certificate files and their checks, and Appendix A the formal proofs of Theorem 1.3 and of two weaker bounds. The certificates were found by search programs in the repository, which choose the numbers u, v and y_j by linear programming in floating point; they are not part of the proof.

Limits of the method. The following limits are numerical observations, not proved statements. For single-contour certificates, whatever the contour, the largest admissible τ appears to be about 0.16557 in the one-sided case and about 0.1694 in the two-sided case, which corresponds to about 1.1984 for C_3' and 1.2039 for C_3. For two-level certificates with the ellipse T_1 of the certificate with $\tau = 7/30$ (Appendix A) and, as tiles, one axis-parallel ellipse around the zero 3 together with its mirror image, the corresponding values appear to be about 1.277 for C_3' and 1.282 for C_3. For a third level with pinned points near $\frac{153}{50} - \frac{3}{5}i$ and $\frac{159}{50} + \frac{6}{25}i$, the value for C_3' appears to be at most about 1.31 with that ellipse and at most about 1.32 with the circle T_1 of the nested certificate. With this circle, trees of nodes as in Definition 6.11 go past these values and give the bound of Theorem 1.3.

APPENDIX A. PROGRAMS AND FORMAL PROOFS

Independent audits rebuilt or re-checked the Lean proofs of both theorems and of the weaker signed bounds, some in full and some in samples. The repository records the runs behind Sections 4 to 6, their costs and the hashes of their inputs, and what each audit covered.

Programs. The README of the repository maps the programs of Sections 4 to 6 to its files and records, for each pair of checkers, what the two have in common and how the second was written. The first checker of Theorem 2.2 shares with the search the constraint definitions of the checker for certificates without square constraints (Section 5), which the first checker extends. The second checker shares no code with the first checker or with the search; an earlier version of it, which did not read compressed dual vectors, checked the certificate for $V_{36} \geq 133/100$. Both checkers use HiGHS.

The Lean proofs of Theorem 1.1. We formalized the reduction, the reversal symmetry and the soundness of a checker in Lean 4 with Mathlib. The formal theorem states (1.1) with $C = 1337/1000$ for measurable $f\colon \mathbb{R} \to [0,\infty]$ with lower Lebesgue integrals. We also derive in Lean the statement with the essential supremum, and a version for measurable $f\colon \mathbb{R} \to \mathbb{R}$ that is nonnegative and vanishes outside $[-1/4, 1/4]$, stated with Mathlib's convolution and the L^∞ norm on $[-1/2, 1/2]$. The Lean checker re-implements the constraints of Section 3 and proves them valid. It reads the search logs, in which a variant of the first checker, with identical acceptance logic, has filled in the dual vectors of the 2,446 leaves without data; any filled certificate that the Lean checker accepts gives the theorem. An exporter translates the

filled logs into Lean source. Since no formal theorem mentions the certificate, the exporter need not be trusted; the same holds for the exporters of the Lean proofs of Section 6.

Lean accepts the certificate in two ways. In the first, `native_decide` evaluates the checks by compiled code, which adds the compiler to the trusted base; each auxiliary axiom of the final theorem records the result of a compiled evaluation, one for each generated module (a module checks a group of jobs) and one for the root region. In the second, a checker evaluated by Lean's kernel alone checks the segments of the depth-first records of all jobs in generated modules, and group modules and the final modules compose these checks. An audit found the three final statements of this proof equal to the reviewed statements with $\lambda = 1337/1000$ and confirmed that they depend only on the standard axioms `propext`, `Classical.choice` and `Quot.sound`.

The Lean proofs of Theorem 1.3 and of two weaker bounds. Two multi-level certificates give weaker bounds. The first, for $\tau = 6/25$, uses the circle T_1 of the nested certificate and has 270 intervals of type E, 672 of the second level and 1,432 of the third level, which pin the values of $\hat{\mu}$ at $\frac{153}{50} - \frac{3}{5}i$ and $\frac{159}{50} + \frac{6}{25}i$ or at their mirror images; it gives $C_3 \geq C_3' \geq 25/19$. The second, for $\tau = 7/30$, in which T_1 is the ellipse with $c = 53/50$, $a = 39/100$ and $b = 21/50$, has 2,626 intervals and gives $C_3 \geq C_3' \geq 30/23$. Both checkers of multi-level certificates accept both certificates.

The formalization of the argument for multi-level certificates counts zeros by winding numbers and uses neither the argument principle nor the Jordan curve theorem. A checker written in Lean re-derives the conditions of Definition 6.6 from the definitions and is proved sound. It is extended to nested certificates, with the node sets and tube conditions of Definition 6.11, and proved sound again; it checks the 1,229 arcs of the nested certificate in the upper half of T_1, and a proved symmetry gives the arcs in the lower half, which are their mirror images. For each of the three bounds $\frac{4}{3}$, 25/19 and 30/23, the formal theorems state that for every f as in Theorem 1.3 each real number M with $f*f \leq M$ almost everywhere satisfies $M > b(\int f)^2$, where b is the bound, the same inequality for the essential supremum in the extended reals together with $\operatorname{ess\,sup} f * f \leq \operatorname{ess\,sup} |f * f|$, and $C_3 \geq C_3' \geq b$. The precision of the interval enclosures of the Lean checker is part of the generated data, 80 bits for the certificate with $\tau = 6/25$ and 64 bits for that with $\tau = 7/30$, and the soundness proof holds for every precision.

Each of the three bounds is proved in two ways. In the first, `native_decide` evaluates the finite certificate checks, one for each interval of T_1 in the certificate with $\tau = 6/25$ and one for the global checks, 2,375 in all; 207,572 for the nested certificate; and 2,627 for the certificate with $\tau = 7/30$. In the second, a version of the checker written for evaluation by the kernel, which is proved to compute the same results as the checker above on every input, checks the certificate in generated modules by `decide +kernel`. The check of each interval of type H is split into piece theorems small enough for the kernel, and further modules assemble them. For the nested certificate, the proof has the same 207,572 finite certificate checks and an assembly with the same statements as the proof by `native_decide`, but it derives each check from the corresponding check of the kernel version; the check of a tree of nodes is split into theorems for single nodes, for small subtrees and, at witnesses with many tile arcs, for runs of consecutive tile arcs, a further theorem shows that these theorems cover the tree, and the largest checks are split over several generated modules. An audit confirmed that the three theorems of this proof state the same as those of the proof by `native_decide` and use no axioms beyond the standard ones.

The Lean proofs of the further certificates. The Lean checker accepted all six further certificates of Section 5 through `native_decide`, and the checker that runs in the Lean kernel alone accepted those for $V_{20} \geq 32/25$, $V_{28} \geq 131/100$ and $V_{36} \geq 133/100$. For that checker, the duals of the rows of these three certificates were rounded to multiples of 2^{-64}, and the duals of

the square constraints of the certificate for $V_{36} \geq 133/100$ were rounded down to nonnegative multiples of 2^{-94}; every leaf was checked again exactly with the rounded duals.

Summary. Each of the bounds $C_1 \geq 1337/1000$, $C_3 \geq C_3' \geq \frac{4}{3}$, $C_3 \geq C_3' \geq 25/19$ and $C_3 \geq C_3' \geq 30/23$ has a proof whose finite checks are evaluated by compiled code, with 124,632, 207,572, 2,375 and 2,627 such checks and one auxiliary axiom for each of them besides Lean's three standard axioms, and a proof by Lean's kernel alone, which depends only on the standard axioms.

Appendix B. Certificates and checkers of Section 6

A certificate is a JSON file. It contains τ, the parameters c, a, b of T_1, the tiles by their centres and semi-axes, and the intervals of $[0,1]$ with their types, all as rational numbers. An interval of type E carries the real and imaginary parts of u. An interval of type H of the second level carries s_c and a witness without numbers y_j and without a stored τ', which is τ. One of the third level carries s_c, its two pinned points p_1, p_2 with the numbers R_1, R_2, and a tree of leaves, obtained from the squares $\{x : |\operatorname{Re} x|, |\operatorname{Im} x| \leq R_j\}$ by repeatedly dividing one of the current squares into four equal squares. A leaf carries its squares Q_j and either an exclusion, given by v and the numbers y_j, or a witness. A witness consists of τ', the name of its tile, ν_{rep}, a number σ_{rep} and the tile arcs. The number σ_{rep} plays the role of σ in the definition of $\mathcal{P}$ for ν_{rep}, and each tile arc is given by an interval of the parameter q of the tile and by u, v and the numbers y_j. The measures ν_{rep} are sums of point masses. The repository specifies the format in full. In a nested certificate an interval of type H is stored as a record of type N, which carries the record of its tree. A node record is an empty node, with v, the numbers y_j and one number v_l for each tube condition; a split, with the index j; an arc split, with the index l of a tube condition and the number q_m; or a witness, with the data of a witness above, whose tile arcs carry either the numbers u, v, y_j and v_l or the record of a child, which names the kind of its new tube condition. For each tube condition (A_l, ν_l) a witness also lists a point q_r of the parameter interval of A_l and a number $\kappa_r \geq 0$, and the checkers prove $|\hat{\nu}(p(q_r)) - S(p(q_r)) - \kappa_r G_{\nu_l}(p(q_r))| \leq \varepsilon$ for its measure ν. Empty nodes and witnesses may store τ_N, which is τ otherwise, and the header holds ε.

Multi-level certificates (Definition 6.6), such as the certificate for $\tau = 6/25$ that the Lean proofs of Appendix A read, are checked by two programs. Both checkers read all numbers exactly. They confirm that the intervals of T_1 and the arcs of each tile subdivide the respective parameter interval $[0,1]$, that $(c-a, c+a)$ contains exactly one nonzero integer, that $c \pm a$ is not a nonzero integer and that $R_j \geq \tau e^{\pi |\operatorname{Im} p_j|}$ for every pinned point p_j. To establish that the leaves cover the product of the two squares, the first checker compares each leaf with its position in the tree, and the second checks that the leaves lie in it, have pairwise disjoint interiors and have total volume $\prod_j (2R_j)^2$. Each checker also verifies $\tau' \geq \tau$ and computes bounds $r \geq r_\tau$ for each interval of type H, together with the numbers d, Y, L, m_S, rather than reading them from the file. For a witness, r' is computed in the same way with τ' in place of τ, that is, $r' = r_{\tau'}$ rounded up (for the second checker, the larger of its two values), so that $r' \geq r_\tau$. Both checkers bound $|S'|$ locally on each arc. With a bound for $|S'|$ on a whole horizontal strip, the value of r in the first checker would be up to about 2.3 times larger, and at least twice as large on 426 of the 2,104 intervals of type H. In a floating-point evaluation 1,574 of the 66,632 exclusions of the certificate for $\tau = 6/25$ would then fail. With the local bounds, the smallest slack of an exclusion in this evaluation is about $2.5 \cdot 10^{-5}$. For each witness the checkers verify in exact arithmetic that ν_{rep} has nonnegative masses at points of $[-1/2, 1/2]$ with total mass at most τ' and that $\sigma_{\mathrm{rep}} \geq 1$, and they prove the inequality $|\hat{\nu}_{\mathrm{rep}}(z_c) - \sigma_{\mathrm{rep}} S(z_c)| \leq r'$ and the conditions $\hat{\nu}_{\mathrm{rep}}(p_j) \in Q_j$ with enclosures. The zeros of $G_{\nu_{\mathrm{rep}}}$ inside the tile are counted by the argument

principle. The checkers divide the tile into pieces on which the values of $G_{\nu_{\mathrm{rep}}}$ provably lie in a disc whose radius is less than half the distance from its centre to 0, and they add the changes of the argument over the pieces and require the sum to be within $\pi/2$ of an odd multiple of 2π.

The first checker uses the ball arithmetic of Arb [12] through python-flint [22], with a precision of 80 bits. It encloses the points of an arc of T_1 in a complex ball, takes this ball as the convex set of Lemma 6.5, and bounds $|S'|$ from above and $|S|$ from below on it by ball evaluation. It proves the inequalities of (ii), (6.2) and (6.3) on balls for the points of the arcs and on subintervals for t, which it bisects when necessary within fixed limits. The second checker also uses Arb, with a precision of 100 bits, but a different enclosure method. It encloses each arc in a disc around the value at its midpoint and bounds functions on the disc by the value at the centre and a Lipschitz bound. For instance, it bounds $|S'|$ on a disc $D(p_m, \delta)$ by $|S'(p_m)| + \delta(\pi^2/3)e^{\pi Y}$ with $Y = |\operatorname{Im} p_m| + \delta$, which follows from $|S''(\zeta)| \le (\pi^2/3)e^{\pi|\operatorname{Im}\zeta|}$. In t it uses second-order bounds on adaptive cells. For the radius r it computes the bound of Lemma 6.5 twice, once with the disc $D(z_c, d)$ and once, as the first checker does, with a ball containing the arc, and it uses the larger value. Definition 6.6 admits any $r \ge r_\tau$, so this choice is sound. The larger value makes the conditions on the exclusions and on the tile arcs harder and the condition $|\hat{\nu}_{\mathrm{rep}}(z_c) - \sigma_{\mathrm{rep}} S(z_c)| \le r'$ easier. In the certificate for $\tau = 6/25$ the disc-based value would have sufficed for every witness. Both rely on FLINT through python-flint and on the exact rational arithmetic of Python.

Two further programs, the first and the second checker of the nested certificate, check the nested certificate of Theorem 1.3. It is archived in 2,048 parts, files of the same format with the same header that together hold its 2,458 intervals, and the checkers run on each part separately. Both checked all 2,048 parts and accepted every interval of each. A third program checks the SHA-256 hash of every part against a list of the hashes and confirms that the parts have the same header and that their intervals subdivide $[0, 1]$.

The first checker of the nested certificate extends the first checker above to trees of nodes, with the same ball arithmetic at 80 bits, and it checks the intervals of type E as that checker does. At each empty node and each witness it computes r_N from τ_N as it computes r' above and checks the sign conditions and the inequalities of Lemma 6.10. There it bounds the functions of t by second-order Taylor bounds on dyadic cells of $[-1/2, 1/2]$, down to length 2^{-22}, it encloses each term with an arc A_l on four balls that cover A_l, and it bounds the extrema over A_l of the terms with S and G_{ν_l} on 8 or 64 such balls. It checks that the measure of each witness lies in E_N, using the points q_r and the numbers κ_r of the certificate, and it counts the zeros inside the tiles as above. It accepts the record of a child only if the record names the tube condition of Definition 6.11 as its kind.

The second checker of the nested certificate uses ball arithmetic with 128 bits, bounds the extrema over the arcs A_l by second-order Taylor bounds in the parameter of the arc and the functions of t by mean-value bounds on dyadic cells down to length 2^{-34}, and it accepts the records of children under the same rule. For r_N it takes the smaller of two bounds of Lemma 6.5, one with a disc around z_c and one with a box containing the arc of T_1, and at a witness it takes $|\hat{\nu}(z_c) - \sigma S(z_c)|$, for the number σ of the witness, if this is larger; Definition 6.11 admits any $r_N \ge r_\tau$.

Data availability

The certificate of Table 1, the search logs in 178 tar files (1.88 terabytes), is archived by the author and available on request, together with the 2,412 job files that the Lean checker read in filled form; a public location will be added in a later version of this paper. The search programs, the checkers and the Lean formalization are archived at doi:10.5281/zenodo.23715661.

This record also holds the file `meta.json` of the run, the SHA-256 hashes of the job files of each of the 178 tar files and of the 2,412 filled job files, the list of all files that the Lean checker read for this certificate, with their SHA-256 hashes, the SHA-256 hashes of the 124,634 compiled modules of this Lean proof (`c1337_oleans.sha256.gz`) and of their sources (`c1337_sources.sha256.gz`), the SHA-256 hashes of the 5,164,010 compiled check modules of its kernel-only proof (`k1337_check_oleans.sha256.gz`, in two parts), and the certificate for $V_{39} \geq 267/200$ (11.0 gigabytes, compressed) with the corresponding list. That certificate is the copy that the program `search/d2tree.py` of the repository made from its search logs (1.4 terabytes, not archived), and the program `tools/idcheck_tree.py` confirmed that the two have the same tree. The record further holds the certificate for $V_{36} \geq 133/100$ (4.8 gigabytes) with the corresponding list and the SHA-256 hashes of the 2,274,566 compiled modules of its kernel-only proof (`kc36_oleans.sha256.gz`), the certificate for $V_{20} \geq 32/25$ (321 megabytes), and, compressed with gzip, the certificate for $\tau = 6/25$ that the Lean proofs of the bound 25/19 read (2,686 megabytes, 10.64 gigabytes uncompressed) and the certificate with $\tau = 7/30$ that the Lean proofs of the bound 30/23 read (1,300 megabytes), as well as the nested certificate of Theorem 1.3 in 2,048 parts, collected in one tar file (25.2 gigabytes), the hint files that, with it, regenerate the sources of the kernel-only Lean proof of $C_3 \geq C_3' \geq \frac{4}{3}$ (765 megabytes, compressed), and the SHA-256 hashes of the generated sources and compiled modules of that proof; the checkers of this certificate, the program that checks the coverage by its parts and the search programs of Section 6 are in the directory `signed` of the repository snapshot in this record, and the programs that produced the certificate with $\tau = 7/30$ are in that directory of the snapshot archived at doi:10.5281/zenodo.23549127. The certificate for $V_{30} \geq 33/25$ is archived, split into 78 parts, at doi:10.5281/zenodo.23523705. The certificates for $V_{24} \geq 13/10$ and $V_{28} \geq 131/100$, of 11 and 81 gigabytes, are not archived. The programs, the Lean sources and the directory `signed` are also available at `https://github.com/tejasvi/autocorrelation-lower-bounds/tree/v13` (commit `bfabb085b8c4725d2f3f1002341bdeb592cf8979`).

Acknowledgements

Generative AI tools were used to write code, run analyses and draft text; the author directed the work and takes full responsibility for its content.

References

[1] A. Novikov et al., *AlphaEvolve: A coding agent for scientific and algorithmic discovery*, arXiv:2506.13131, 2025.

[2] F. Bianchi, Y. Kwon, A. Pappu and J. Zou, *Harnessing the collective intelligence of AI agents in the wild for new discoveries*, arXiv:2606.10402, 2026.

[3] J. Cilleruelo, I. Z. Ruzsa and C. Vinuesa, *Generalized Sidon sets*, Adv. Math. **225** (2010), 2786–2807.

[4] A. Cloninger and S. Steinerberger, *On suprema of autoconvolutions with an application to Sidon sets*, Proc. Amer. Math. Soc. **145** (2017), 3191–3200.

[5] Together AI, *EinsteinArena state-of-the-art results*, `https://github.com/togethercomputer/EinsteinArena-new-SOTA`, 2026.

[6] P. J. Goulart and Y. Chen, *Clarabel: An interior-point solver for conic programs with quadratic objectives*, arXiv:2405.12762, 2024.

[7] M. German, *C_{1d} upper-bound certificate (600 cells)*, GitHub repository, `https://github.com/steps-re/c1d-certificate`, commit `9a09149`, accessed October 2026.

[8] B. Georgiev, J. Gómez-Serrano, T. Tao and A. Z. Wagner, *Mathematical exploration and discovery at scale*, arXiv:2511.02864, 2025.

[9] Q. Huangfu and J. A. J. Hall, *Parallelizing the dual revised simplex method*, Math. Program. Comput. **10** (2018), 119–142.

[10] P. Ivanisvili and X. Xie, *Grokability in five inequalities*, arXiv:2605.05193, 2026.

[11] P. Jana et al., *MILO: Automated harness discovery via orchestrated multi-agent evolution*, arXiv:2609.38349, 2026.
[12] F. Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), 1281–1292.
[13] A. Kharlamova, J. Kang, B. He and S. Liu, *Certificate for $C_{1d} \leq 1.457854884921989$ (signed third autocorrelation constant)*, Zenodo, doi:10.5281/zenodo.23541324, 2026.
[14] S. Kim and M. Pilanci, *AI-assisted discovery of convex relaxations via dual agents*, Proc. 43rd Int. Conf. Machine Learning, PMLR **306**, 2026; arXiv:2606.31182.
[15] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer, 2021, 625–635.
[16] The mathlib Community, *The Lean mathematical library*, in: Proc. 9th ACM SIGPLAN Int. Conf. Certified Programs and Proofs (CPP 2020), 2020, 367–381.
[17] G. P. McCormick, *Computability of global solutions to factorable nonconvex programs. I. Convex underestimating problems*, Math. Program. **10** (1976), 147–175.
[18] M. Matolcsi and C. Vinuesa, *Improved bounds on the supremum of autoconvolutions*, J. Math. Anal. Appl. **372** (2010), 439–447.
[19] A. Neumaier and O. Shcherbina, *Safe bounds in linear and mixed-integer linear programming*, Math. Program. **99** (2004), 283–296.
[20] D. Davis, P. Ivanisvili, T. Tao and contributors, *Optimization constants in mathematics*, GitHub repository, `https://github.com/teorth/optimizationproblems`, 2026. Constant 1d: `https://teorth.github.io/optimizationproblems/constants/1d.html`, accessed October 2026.
[21] A. Piterbarg, J. Bajaj and D. Vincent, *A new lower bound for the supremum of autoconvolutions*, GitHub repository, `https://github.com/AndreiPiterbarg/sidon-autocorrelation`, commit `1ed5889`, accessed October 2026.
[22] The python-flint developers, *python-flint: Python bindings for FLINT*, version 0.9.0, `https://github.com/flintlib/python-flint`.
[23] H. D. Sherali and W. P. Adams, *A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems*, SIAM J. Discrete Math. **3** (1990), 411–430.
[24] H. D. Sherali and B. M. P. Fraticelli, *Enhancing RLT relaxations via a new class of semidefinite cuts*, J. Global Optim. **22** (2002), 233–261.
[25] N. Z. Shor, *Quadratic optimization problems*, Soviet J. Comput. Systems Sci. **25** (1987), 1–11.
[26] A. Schinzel and W. M. Schmidt, *Comparison of L^1- and L^∞-norms of squares of polynomials*, Acta Arith. **104** (2002), 283–296.

ORCID: `https://orcid.org/0000-0003-4668-3639`