THE LAGUERRE GRAM MATRIX OF GONÇALVES' SHARPENED STRICHARTZ INEQUALITY: A CLOSED FACTORISATION, AND THE SPECTRAL CONJECTURE THROUGH $S = 60$

KOREA SUPERINTELLIGENCE LABS

Abstract. Let L_n be the Laguerre polynomial normalised by $L_n(0) = 1$, so that the L_n are orthonormal for $e^{-x}\,dx$ on $(0,\infty)$, and let

$$Q(a,b,c,d) = \int_0^\infty L_a(x/2)L_b(x/2)L_c(x/2)L_d(x/2)\,e^{-x}\,dx,$$

and let $Q_S = \big[\,Q(a,S-a,c,S-c)\,\big]_{a,c=0}^{S}$. Gonçalves introduced Q_S to prove a sharpened Strichartz inequality for radial data in $\mathbb{R}^2$, showed that it is positive semi-definite, doubly stochastic and strictly positive, and closed his paper with two numerical conjectures about it: that the eigenvalues of Q_S are exactly $\lambda(n) = \binom{2n}{n}^2 16^{-n}$ for $n \le \lfloor S/2 \rfloor$, each simple, together with 0 of multiplicity $\lceil S/2 \rceil$; and that the least entry of Q_S is $Q(\lfloor S/2 \rfloor, \lceil S/2 \rceil, S, 0)$. He reports verifying both for $S \le 30$. No formula for $Q(a,b,c,d)$ is given there, and we have found none in the literature. We give one on the diagonal slice: writing $\mathbf{X}_S[a,j] = \binom{S-2j}{a-j}$, $\mathbf{H}_S[i,j] = \binom{2(S-i-j)}{S-i-j}$ and $\mathbf{\Delta}_S = \operatorname{diag}\big((-4)^i\binom{S-i}{i}\big)$ for $0 \le i,j \le \lfloor S/2 \rfloor$,

$$2^{2S}\,Q_S \;=\; \mathbf{X}_S\,\mathbf{\Delta}_S\mathbf{H}_S\mathbf{\Delta}_S\,\mathbf{X}_S^{\top},$$

an identity we derive from the two-variable generating function of the Laguerre linearisation coefficients. It compresses the characteristic polynomial to $\operatorname{char}_{Q_S}(X) = X^{\lceil S/2 \rceil}\cdot\operatorname{char}_{4^{-S}\mathbf{M}_S^2}(X)$ with $\mathbf{M}_S = \mathbf{\Delta}_S\mathbf{H}_S$, so that Gonçalves' eigenvalue conjecture at S becomes a statement about a matrix of half the size whose eigenvalues are the square roots $(-1)^n\binom{2n}{n}2^{S-2n}$. Instances of the identity and of the compression are machine-checked, and so is the eigenvalue conjecture in full, with multiplicities, for every S with $31 \le S \le 60$, thirty values beyond the range reported in the source; likewise the minimum-entry conjecture over the same range, together with the observation — stated nowhere, and not new mathematics — that the minimum is attained exactly on the 4- or 8-element symmetry orbit of $(\lfloor S/2 \rfloor, 0)$. Every statement below is formally verified in Lean 4 except where the text says otherwise.

1. Introduction

1.1. **The matrix.** Let $L_n = L_n^0$ denote the Laguerre polynomial normalised by $L_n(0) = 1$; explicitly

$$L_n(x) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{x^k}{k!}, \qquad \int_0^\infty L_m(x)L_n(x)\,e^{-x}\,dx = \delta_{mn}, \tag{1}$$

which is Szegő [8, (5.1.6) and (5.1.1)] at parameter $\alpha = 0$. Following Gonçalves [1], put

$$Q(a,b,c,d) = \int_0^\infty L_a(x/2)L_b(x/2)L_c(x/2)L_d(x/2)\,e^{-x}\,dx, \tag{2}$$

and for an integer $S \geq 0$ let

$$Q_S = \big[\, Q(a, S-a, c, S-c) \,\big]_{a,c=0,\dots,S}, \tag{3}$$

an $(S+1)\times(S+1)$ matrix of rational numbers. Setting $f_a(x) = L_a(x/2)L_{S-a}(x/2)$, the matrix Q_S is the Gram matrix of $f_0, \dots, f_S$ in $L^2\big((0,\infty), e^{-x}dx\big)$, which is why we call it the *Laguerre Gram matrix*. Since $f_a = f_{S-a}$, the list of Gram vectors has at most $\lfloor S/2 \rfloor + 1$ distinct members, a remark we return to in §3.

The matrix arises as follows. Gonçalves proves in [1, Theorems 1 and 3] a sharpened form of the sharp Strichartz estimate $\|u\|_{L^4(\mathbb{R}^2\times\mathbb{R})} \leq 2^{-1/2}\|f\|_{L^2(\mathbb{R}^2)}$ for radial data, the deficit being a constant $\gamma > 0$ times a squared $L^2(\mathbb{R}^4)$ distance to the radial functions — the first of the two theorems is the estimate for radial $f \in L^2(\mathbb{R}^2)$, the second the version for $g \in L^2(\mathbb{R}^2\times\mathbb{R}^2)$ radial in each variable, from which the first follows with the same γ. The proof expands in Laguerre polynomials and reduces to a spectral gap estimate for a doubly stochastic operator $\mathcal{Q}$ on $\ell^2(\mathbb{Z}^2_{\geq 0})$ which decomposes as $\bigoplus_{S\geq 0} Q_S$. Writing $\mathrm{sg}(A) = \sigma_1(A) - \sigma_2(A)$ for the gap between the two largest eigenvalue moduli, the constant obtained is $\gamma = \inf_{S\geq 1} \mathrm{sg}(Q_S)$, and the lower bound proved there is $\mathrm{sg}(Q_S) \geq 4/\pi^2$ for every $S \geq 1$. The structural input is [1, Theorem 6]:

> *for any $S \geq 0$ the matrix Q_S … is a positive semi-definite doubly stochastic matrix with strictly positive entries.*

1.2. **The two conjectures.** The final section of [1] reports numerical experiments and states two conjectures, both quoted here verbatim. Numbering throughout this paper, for [1], is that of the e-print arXiv:1709.08100v2; the two conjectures below are its Conjectures 4 and 3, and the theorem quoted above is its Theorem 6. The published version appears to carry the same numbers: [2], citing the journal version, refers to its Theorem 3 and its Conjectures 1 and 2, and those are Theorem 3 and Conjectures 1 and 2 of the e-print as well. The first conjecture is about the spectrum.

Conjecture 1.1 (the eigenvalue conjecture of [1])**.** Let $\lambda(n) = \binom{2n}{n}^2 16^{-n}$. Then $\mathrm{Eig}(Q_S) = \{\lambda(0), \lambda(1), \dots, \lambda(\lfloor S/2 \rfloor), 0\}$. Moreover, each non-zero eigenvalue has multiplicity 1 and the zero eigenvalue has multiplicity $\lceil S/2 \rceil$.

Since $\lambda(0) = 1$ and $\lambda(1) = 1/4$, Conjecture 1.1 would give $\mathrm{sg}(Q_S) = \lambda(0) - \lambda(1) = 3/4$ for every $S \geq 2$, hence $\gamma = 3/4$, which [1] notes is best possible. The paper's own verification is described there as follows: "*The Laguerre polynomials expand in monomials with rational coefficients whenever the parameter ν is rational, therefore using rational arithmetic one can compute the coefficients $Q(a,b,c,d)$ explicitly … Using this procedure we confirmed the conjecture above for $S \leq 30$.*"

The second conjecture is about the smallest entry.

Conjecture 1.2 (the minimum-entry conjecture of [1])**.** Let $a + b = c + d = S$. Then $Q(a,b,c,d) \geq Q(\lfloor S/2 \rfloor, \lceil S/2 \rceil, S, 0)$. That is, the minimal element of Q_S lies in the first column with the middle row.

Together with the elementary evaluation and bound recorded in [1],

$$Q(a,b,a+b,0) = \binom{2a}{a}\binom{2b}{b}4^{-(a+b)} \;\geq\; \frac{2}{\pi(a+b+1)},$$

Conjecture 1.2 would give $\gamma = 2/\pi$, better than the proved $4/\pi^2$ but weaker than the $3/4$ that Conjecture 1.1 would give. Neither conjecture has, to the best of our knowledge, been proved in print; §1.4 records what the closest published work does and does not say, and it says more than one might expect.

1.3. **Results.** The source gives no formula for $Q(a,b,c,d)$; it says only that the numbers are rational and computable. Our main result is a closed formula on the diagonal slice (3), in the form of a factorisation through a space of dimension $\lfloor S/2 \rfloor + 1$. Fix S and write $r = \lfloor S/2 \rfloor$. Define, for $0 \le a \le S$ and $0 \le i, j \le r$,

$$\begin{aligned} \mathbf{X}_S[a,j] &= \binom{S-2j}{a-j}, \qquad \mathbf{H}_S[i,j] = \binom{2(S-i-j)}{S-i-j}, \\ \boldsymbol{\Delta}_S &= \operatorname{diag}\Big((-4)^i \tbinom{S-i}{i} \Big)_{0 \le i \le r}, \end{aligned} \tag{4}$$

with the convention that $\binom{m}{k} = 0$ unless $0 \le k \le m$, so that $\mathbf{X}_S[a,j] = 0$ outside $j \le a \le S - j$. Put $\mathbf{W}_S = \boldsymbol{\Delta}_S \mathbf{H}_S \boldsymbol{\Delta}_S$ and $\mathbf{M}_S = \boldsymbol{\Delta}_S \mathbf{H}_S$, that is

$$\begin{aligned} \mathbf{W}_S[i,j] &= (-4)^{i+j} \binom{S-i}{i} \binom{S-j}{j} \binom{2(S-i-j)}{S-i-j}, \\ \mathbf{M}_S[i,j] &= (-4)^{i} \binom{S-i}{i} \binom{2(S-i-j)}{S-i-j}. \end{aligned} \tag{5}$$

The factorisation (Proposition 3.2, and Theorem 3.3 for the machine-checked instances) is

$$2^{2S}\, Q_S = \mathbf{X}_S\, \mathbf{W}_S\, \mathbf{X}_S^{\top}, \tag{6}$$

equivalently, entry by entry,

$$\begin{aligned} 2^{2S}\, Q(a, S-a, c, S-c) = \sum_{i,j=0}^{\lfloor S/2 \rfloor} (-4)^{i+j} \binom{S-i}{i} \binom{S-j}{j} \binom{2(S-i-j)}{S-i-j} \\ \times \binom{S-2i}{a-i} \binom{S-2j}{c-j}. \end{aligned} \tag{7}$$

It is derived in §3 from the two-variable generating function

$$\sum_{a,b \ge 0} p_m(a,b)\, t^a s^b = \frac{2\,(t+s-2ts)^m}{(2-t-s)^{m+1}}, \tag{8}$$

where the $p_m(a,b)$ are the linearisation coefficients of the Laguerre polynomials, defined by $L_a(x/2) L_b(x/2) = \sum_m p_m(a,b) L_m(x)$; a diagonal coefficient extraction and two Vandermonde convolutions then finish the derivation.

Two consequences are recorded. The first is a compression of the characteristic polynomial: $\mathbf{X}_S^{\top} \mathbf{X}_S = \mathbf{H}_S$, so (6) gives

$$\operatorname{char}_{Q_S}(X) = X^{\lceil S/2 \rceil} \cdot \operatorname{char}_{4^{-S} \mathbf{M}_S^2}(X). \tag{9}$$

The second is what (9) does to Conjecture 1.1. Setting

$$\theta(S,n) = (-1)^n \binom{2n}{n} 2^{S-2n}, \qquad \text{so that} \qquad 4^{-S} \theta(S,n)^2 = \lambda(n), \tag{10}$$

the zero eigenvalue of multiplicity at least $\lceil S/2 \rceil$ — half of Conjecture 1.1 — drops out of the shape of (6), and the surviving half becomes a statement about the $(\lfloor S/2 \rfloor + 1)$-square *integer* matrix $\mathbf{M}_S$ of (5): it holds as soon as the eigenvalues

of $\mathbf{M}_S$ are the $\lfloor S/2 \rfloor + 1$ values $\theta(S, n)$ (Corollary 3.6). That is a problem of half the size, over $\mathbb{Z}$ rather than $\mathbb{Q}$, and about square roots rather than squares. We emphasise that the rank bound alone is not new information: $f_a = f_{S-a}$ already gives $\operatorname{rank}(Q_S) \le \lfloor S/2 \rfloor + 1$ in one line. What (6) adds is the identification of the surviving block.

Beyond the factorisation the paper records machine-checked instances. Theorem 4.2 is Conjecture 1.1 in full, with multiplicities, for every S with $31 \le S \le 60$ — thirty values past the $S \le 30$ that [1] reports checking, and past every verified range we have found in the literature; on what [2] asserts about all S, see §1.4. Theorem 5.1 is Conjecture 1.2 over the same range, together with the exact minimiser set, which turns out to be the full symmetry orbit of $(\lfloor S/2 \rfloor, 0)$ and nothing else: four positions when S is even, eight when S is odd. Neither of these is new mathematics — at $S = 60$ the underlying arithmetic is seconds of exact rational computation, and anyone who asks the question can redo it — and we state them as extensions of a verified range, not as theorems that were hard to obtain. What they add over an unaudited computation is the certificate shape of §4.1.

1.4. **Provenance, and what is classical.** Identity (7) follows from standard Laguerre linearisation, and an expert in orthogonal polynomials may well regard it as routine; we have not, however, found it written down, and we have not found the reduction (9) at all. The classical literature on quartic Laguerre integrals evaluates $Q(a, b, c, d)$ combinatorially rather than by a product formula: Even and Gillis [4] read the integral as a count of derangements of a multiset, Askey, Ismail and Koornwinder [3] attach it to weighted permutation problems, Gillis and Zeilberger [5] give a direct combinatorial proof of a positivity result for it, Foata and Zeilberger [6] extend the evaluation to an arbitrary Laguerre parameter α by weighted derangements, and Ismail, Kasraoui and Zeng [7, §4] recover the Foata–Zeilberger results by separation of variables. None gives an elementary product formula for a general $Q(a, b, c, d)$. Our own searches are described in §6.

One published tool comes very close to Conjecture 1.1, and the paper that carries it says so in a sentence that has to be quoted rather than paraphrased. Gonçalves and Zagier [2] prove a criterion for a "special" power series F under which the matrix R_S read off the coefficients of F has eigenvalues $e_0, \dots, e_S$ with each e_n independent of S and computable as $e_n = [x^n y^n](H)$ for a second series H [2, (3.3) and (3.6), numbering of the journal version]. The matrix Q_S is of that shape. Discussing the quadratic form behind Q_S — their Q_2 under the constraint that $f(x_1, x_2, x_3, x_4)$ depends only on $x_1^2 + x_2^2$ and $x_3^2 + x_4^2$ — [2] writes: "*using the method of Section 3 one can reprove Theorem 3 in* [1] *(with $\gamma = 3/4$ as it was conjectured; we omit the details)*", where the reference inside the quotation is theirs, renumbered to the bibliography of this paper. Since the constant in [1, Theorem 3] is $\gamma = \inf_{S \ge 1} \operatorname{sg}(Q_S)$, that sentence amounts to $\operatorname{sg}(Q_S) \ge 3/4$ for every $S \ge 1$ — the consequence Conjecture 1.1 was raised to give, and the one [1] calls best possible. The details are omitted there, and neither Conjecture 1.1 nor Conjecture 1.2 is stated, named or proved in [2]; what [2] does cite of [1] by number is its Conjectures 1 and 2, about the exponents $(6, 6, 1)$ and $(4, 8, 1)$, proving a generalised form of the first. We do not carry out the verification for Q_S either; we record it in §7 as the natural route to a proof for all S. Nothing in the present paper bears on the constant γ, and the record on γ is this: $\gamma \ge 4/\pi^2$ is proved in [1], $\gamma = 3/4$ is asserted without details in [2], and $\gamma \ge 2/\pi$ would follow from Conjecture 1.2.

1.5. **Verification.** All statements below are formally verified in Lean 4 against *Mathlib* [10], with two marked exceptions: Propositions 3.1 and 3.2, the all-S forms of (8) and (6), are proved here by hand and are outside the formal development, because *Mathlib* has no Laguerre polynomials, and their consequences Corollaries 3.5–3.6 inherit that status; what *is* machine-checked about the factorisation is the family of instances Theorem 3.3. Section 6 says which claims rest on exhaustive computation and how large each search is. Computed data carrying no theorem is labelled as such where it appears.

2. The matrix in rational form

Because *Mathlib* has no Laguerre polynomials, the formal development works with Q_S through the closed rational formula that [1] itself points at. We record it, and we record the check that licenses it.

Lemma 2.1 (Rational form)**.** *For integers $S \geq 0$ and $0 \leq a, i \leq S$ put*

$$u(S,a,i) = \sum_p \binom{i}{p}\binom{a}{p}\binom{S-a}{i-p} \in \mathbb{Z}.$$

Then $L_a(x/2)L_{S-a}(x/2) = \sum_{i=0}^{S}(-1)^i\, u(S,a,i)\, x^i/(2^i\, i!)$, and consequently

$$2^{2S}\, Q(a,S-a,c,S-c) = \sum_{i,j=0}^{S} (-1)^{i+j}\, 2^{\,2S-i-j} \binom{i+j}{i}\, u(S,a,i)\, u(S,c,j). \tag{11}$$

In particular $A_S := 2^{2S}Q_S$ is an integer matrix, $A_S = UNU^{\top}$ with $U[a,i] = u(S,a,i)$ and $N[i,j] = (-1)^{i+j}2^{\,2S-i-j}\binom{i+j}{i}$.

Proof. From (1), $L_n(x/2) = \sum_k (-1)^k \binom{n}{k} x^k/(2^k k!)$. Multiplying the expansions of $L_a(x/2)$ and $L_{S-a}(x/2)$ and collecting the coefficient of x^i gives

$$(-1)^i 2^{-i} \sum_p \frac{1}{p!\,(i-p)!}\binom{a}{p}\binom{S-a}{i-p} = \frac{(-1)^i}{2^i\, i!}\sum_p \binom{i}{p}\binom{a}{p}\binom{S-a}{i-p},$$

which is the first claim. Multiplying the expansions for a and for c and integrating against e^{-x} with $\int_0^\infty x^m e^{-x}\,dx = m!$ turns the pair (i,j) into $(i+j)!/(2^{i+j} i!\, j!) = 2^{-(i+j)}\binom{i+j}{i}$, and multiplying by 2^{2S} clears every denominator because $i, j \leq S$. □

Lemma 2.1 is the one hand computation on which the whole formal development rests, so it is gated against a from-scratch expansion of the *four-fold* product, in which the four Laguerre polynomials are multiplied out in monomials and integrated term by term with no algebra beyond (1) and $\int_0^\infty x^m e^{-x} dx = m!$. That naive evaluation costs $O(S^4)$ per entry, so it is run at small S; that is what a gate is for.

Proposition 2.2 (Compute-first gate)**.** *For $S \in \{3, 6\}$ and all $0 \leq a, c \leq S$, the right-hand side of (11) divided by 2^{2S} agrees with the four-fold monomial expansion of $Q(a, S-a, c, S-c)$. Moreover $Q_6[0,0] = \binom{12}{6}/4^6$.*

Proof. Both sides of each of the $4^2 + 7^2 = 65$ entry comparisons are explicit rational numbers, and the comparison is exhaustive, in exact rational arithmetic. The corner value is $Q(0,6,0,6) = \int_0^\infty L_6(x/2)^2 e^{-x} dx$, whose closed form $\binom{2S}{S}4^{-S}$ is elementary and independent of Lemma 2.1, so it serves as a second anchor. □

Throughout, $A_S = 2^{2S} Q_S$ denotes the integer matrix of Lemma 2.1; statements about positivity, symmetry and row sums are stated for A_S, where they are statements about integers.

Proposition 2.3 ([1, Theorem 6], at $31 \le S \le 60$)**.** *For every S with $31 \le S \le 60$: A_S is symmetric, all its entries are strictly positive, and every row sums to 2^{2S} — that is, Q_S is symmetric, strictly positive and doubly stochastic.*

Proof. These three properties are proved for every S in [1, Theorem 6]; nothing is claimed here beyond the instances. Each is an exhaustive evaluation on A_S: $(S+1)^2$ comparisons for symmetry, $(S+1)^2$ sign tests and $S+1$ row sums, the largest case being $S = 60$ with $61^2 = 3721$ entries. They are the control that the matrix built from Lemma 2.1 is the matrix of [1]: a mis-derived coefficient would have to preserve symmetry, positivity and all $S+1$ row sums simultaneously to escape. Positive semi-definiteness, the fourth assertion of [1, Theorem 6], is not re-checked here. □

3. A closed factorisation

3.1. **The generating function.** Expand the product of two Laguerre polynomials in the orthonormal basis: for $a, b \ge 0$ write

(12)
$$L_a(x/2)L_b(x/2) = \sum_{m \ge 0} p_m(a,b)\, L_m(x), \quad p_m(a,b) = \int_0^\infty L_a(\tfrac{x}{2})L_b(\tfrac{x}{2})L_m(x)e^{-x}dx.$$

The sum is finite: $p_m(a,b) = 0$ for $m > a+b$. Orthonormality of the L_m turns (2) into

$$Q(a, S-a, c, S-c) = \sum_{m \ge 0} p_m(a, S-a)\, p_m(c, S-c), \tag{13}$$

that is, $Q_S = PP^\top$ where P is the $(S+1)$-square matrix $P[a,m] = p_m(a, S-a)$, the entries with $m > S$ all vanishing.

The following two propositions are the only statements in this paper that are proved by hand and are *not* part of the formal development; the reason is that *Mathlib* has no Laguerre polynomials, so the objects of (12) cannot yet be written down there. Their machine-checked instances are Theorem 3.3.

Proposition 3.1 (Linearisation generating function; not formalised)**.** *For every $m \ge 0$,*

$$\sum_{a,b \ge 0} p_m(a,b)\, t^a s^b = \frac{2\,(t+s-2ts)^m}{(2-t-s)^{m+1}}$$

as formal power series in t, s.

Proof. The Laguerre generating function [8, (5.1.9)], at $\alpha = 0$, is

$$\sum_{n \ge 0} L_n(x)\, t^n = \frac{1}{1-t}\, e^{-xt/(1-t)}.$$

Hence

$$\sum_{a,b \ge 0} L_a(x/2)L_b(x/2)\, t^a s^b = \frac{1}{(1-t)(1-s)}\, e^{-\frac{x}{2}\alpha}, \qquad \alpha = \frac{t}{1-t} + \frac{s}{1-s}.$$

Put $w = \alpha/(2+\alpha)$, so that $\alpha/2 = w/(1-w)$ and therefore $e^{-x\alpha/2} = (1-w)\sum_{m\ge 0} L_m(x) w^m$ by the generating function again. A direct computation gives

$$w = \frac{t+s-2ts}{2-t-s}, \qquad 1-w = \frac{2(1-t)(1-s)}{2-t-s},$$

so the prefactor $(1-t)^{-1}(1-s)^{-1}(1-w)$ equals $2/(2-t-s)$ and

$$\sum_{a,b\ge 0} L_a(x/2) L_b(x/2)\, t^a s^b = \sum_{m\ge 0} L_m(x) \cdot \frac{2}{2-t-s}\Big(\frac{t+s-2ts}{2-t-s}\Big)^m.$$

Comparing coefficients of $L_m(x)$, which is legitimate because for each pair (a,b) only finitely many m occur, gives the claim. □

Proposition 3.2 (The factorisation, for every S; not formalised)**.** *For every $S \ge 0$, with $\mathbf{X}_S, \mathbf{H}_S, \mathbf{\Delta}_S, \mathbf{W}_S$ as in* (4) *and* (5)*,*

$$2^{2S}\, Q_S = \mathbf{X}_S\, \mathbf{W}_S\, \mathbf{X}_S^\top = \mathbf{X}_S\, \mathbf{\Delta}_S \mathbf{H}_S \mathbf{\Delta}_S\, \mathbf{X}_S^\top,$$

which written out entry by entry is (7)*. Moreover $\mathbf{X}_S^\top \mathbf{X}_S = \mathbf{H}_S$.*

Proof. Fix S and m, and read off $[t^a s^{S-a}]$ in Proposition 3.1. Expanding $(2-t-s)^{-(m+1)}$ and $(t+s-2ts)^m$ and keeping the terms of total degree S gives

$$p_m(a, S-a) = 2^{-S} \sum_j (-4)^j \binom{S-j}{m}\binom{m}{j}\binom{S-2j}{a-j}. \tag{14}$$

The factor $\binom{S-j}{m}\binom{m}{j}$ vanishes unless $j \le m \le S-j$, so the sum runs over $0 \le j \le \lfloor S/2 \rfloor$ and (14) says $P = 2^{-S}\mathbf{X}_S Y$ with

$$Y[j,m] = (-4)^j \binom{S-j}{m}\binom{m}{j}.$$

By (13), $2^{2S} Q_S = \mathbf{X}_S\,(YY^\top)\,\mathbf{X}_S^\top$, so it remains to identify $YY^\top$ and $\mathbf{X}_S^\top \mathbf{X}_S$. Both are Vandermonde convolutions. For the second, substituting $p = a - i$,

$$\begin{aligned}(\mathbf{X}_S^\top \mathbf{X}_S)[i,j] &= \sum_{a=0}^{S} \binom{S-2i}{a-i}\binom{S-2j}{a-j} \\ &= \sum_p \binom{S-2i}{p}\binom{S-2j}{p+i-j} = \binom{2(S-i-j)}{S-i-j},\end{aligned}$$

which is $\mathbf{H}_S[i,j]$; here we used $\sum_p \binom{M}{p}\binom{N}{p+k} = \binom{M+N}{N-k}$ with $M = S-2i$, $N = S-2j$ and $k = i-j$. For the first, the trinomial revision $\binom{S-i}{m}\binom{m}{i} = \binom{S-i}{i}\binom{S-2i}{m-i}$ gives

$$(YY^\top)[i,j] = (-4)^{i+j}\binom{S-i}{i}\binom{S-j}{j}\sum_m \binom{S-2i}{m-i}\binom{S-2j}{m-j},$$

and the same convolution turns the remaining sum into $\binom{2(S-i-j)}{S-i-j}$. That is $YY^\top = \mathbf{W}_S = \mathbf{\Delta}_S \mathbf{H}_S \mathbf{\Delta}_S$. □

3.2. **The machine-checked instances.** For each (S, a, c), (7) is an identity between integers, so it can be checked exhaustively at a fixed S. We record three such cells, and the matrix-level form, in which the compression of the characteristic polynomial becomes available.

Theorem 3.3 (Instances of the factorisation)**.** *Let $S \in \{31, 36, 41\}$ and $r = \lfloor S/2 \rfloor$. Then:*

(1) *for all $0 \le a, c \le S$, the integer identity (7) holds;*
(2) *$Q_S = \mathbf{X}_S \cdot \left(2^{-2S}\, \mathbf{W}_S \mathbf{X}_S^\top\right)$ as an identity of $(S+1)$-square matrices over $\mathbb{Q}$, where the two factors have inner dimension $r+1$;*
(3) *consequently*

$$\mathrm{char}_{Q_S}(X) = X^{\lceil S/2 \rceil} \cdot \mathrm{char}_{\,2^{-2S}\mathbf{W}_S \mathbf{X}_S^\top \mathbf{X}_S}(X),$$

the second factor being the characteristic polynomial of an $(r+1)$-square matrix.

Proof. Parts (1) and (2) are exhaustive evaluations: (1) compares $(S+1)^2$ integers, the right-hand side of each comparison being a sum of $(r+1)^2$ products of five binomial coefficients, and (2) compares $(S+1)^2$ rationals. At $S = 41$ this is $42^2 = 1764$ entries against $21^2 = 441$ terms apiece. Part (3) is not a computation: if $Q = EF$ with E of size $(S+1) \times (r+1)$ and F of size $(r+1) \times (S+1)$, then $\mathrm{char}_{EF}(X) = X^{\,S+1-(r+1)} \mathrm{char}_{FE}(X)$, and $S + 1 - (r+1) = S - \lfloor S/2 \rfloor = \lceil S/2 \rceil$. Applying this to the factorisation of (2) gives (3), with $FE = 2^{-2S} \mathbf{W}_S \mathbf{X}_S^\top \mathbf{X}_S$. The step from (2) to (3) is proved by argument, not by evaluation. □

Remark 3.4. The instances stop at $S = 41$ for cost, not for principle: the check of (1) is $O(S^5)$ as implemented, and the run at $S = 60$ was priced at over 30 CPU-minutes and cut, which buys nothing the small instances do not show, since Proposition 3.2 proves the identity for every S. Outside the formal development, (7) was also verified in exact rational arithmetic for $0 \le S \le 62$, with no failure; that is computed data and carries no theorem here.

3.3. **Two consequences.** The first is the structural half of Conjecture 1.1. It is worth being precise about what is and is not new in it.

Corollary 3.5 (Rank; not formalised in the stated generality)**.** *For every $S \ge 0$, $\mathrm{rank}(Q_S) \le \lfloor S/2 \rfloor + 1$; equivalently 0 is an eigenvalue of Q_S of multiplicity at least $\lceil S/2 \rceil$.*

Proof. Immediate from Proposition 3.2, since $\mathbf{X}_S$ has $\lfloor S/2 \rfloor + 1$ columns. The same bound follows in one line without the factorisation, from $f_a = f_{S-a}$: the Gram vectors of Q_S take at most $\lfloor S/2 \rfloor + 1$ distinct values. We state it here only to fix the exponent in (9). □

The second consequence is the one that changes the shape of the problem.

Corollary 3.6 (The half-size problem; not formalised in the stated generality)**.** *For every $S \ge 0$, with $\mathbf{M}_S = \mathbf{\Delta}_S \mathbf{H}_S$ the $(\lfloor S/2 \rfloor + 1)$-square integer matrix of (5) and $\theta(S, n)$ as in (10),*

$$\mathrm{char}_{Q_S}(X) = X^{\lceil S/2 \rceil} \cdot \mathrm{char}_{4^{-S}\mathbf{M}_S^2}(X).$$

Consequently Conjecture 1.1 holds at S if and only if $\operatorname{char}_{\mathbf{M}_S^2}(X) = \prod_{n=0}^{\lfloor S/2\rfloor}\big(X - \theta(S,n)^2\big)$*; in particular it holds at S whenever the spectrum of $\mathbf{M}_S$, with multiplicity, is* $\{\theta(S,0),\dots,\theta(S,\lfloor S/2\rfloor)\}$.

Proof. By Proposition 3.2 we have $2^{2S}Q_S = EF$, where $E = \mathbf{X}_S$ and $F = \mathbf{W}_S\mathbf{X}_S^{\top}$, so $\operatorname{char}_{EF}(X) = X^{\lceil S/2\rceil}\operatorname{char}_{FE}(X)$ as in the proof of Theorem 3.3, and, using $\mathbf{X}_S^{\top}\mathbf{X}_S = \mathbf{H}_S$,

$$FE = \mathbf{W}_S\mathbf{X}_S^{\top}\mathbf{X}_S = \mathbf{\Delta}_S\mathbf{H}_S\mathbf{\Delta}_S\mathbf{H}_S = \mathbf{M}_S^2.$$

Rescaling by 2^{-2S} gives the displayed identity. For the equivalence, the values $\lambda(0) > \lambda(1) > \cdots > \lambda(\lfloor S/2\rfloor) > 0$ are distinct, and $4^{-S}\theta(S,n)^2 = \binom{2n}{n}^2 2^{-4n} = \lambda(n)$. So Conjecture 1.1, which is exactly the statement that $\operatorname{char}_{Q_S}(X)$ equals $X^{\lceil S/2\rceil}\prod_n(X-\lambda(n))$, is equivalent to $\operatorname{char}_{4^{-S}\mathbf{M}_S^2}(X) = \prod_n(X-\lambda(n))$, i.e. to the stated identity for $\mathbf{M}_S^2$. The last sentence is the special case in which the squares are attained with the signs $\theta(S,n)$. □

Remark 3.7. Corollary 3.6 is not merely a reduction in size. The conjectured eigenvalues of $\mathbf{M}_S$ are integers, where those of Q_S are rationals with denominator 16^n; and the multiplicity clause of Conjecture 1.1, the part a numerical eigenvalue computation cannot see, becomes the statement that $\mathbf{M}_S$ has $\lfloor S/2\rfloor + 1$ distinct eigenvalues, hence is diagonalisable for free. The certificates of §4.1 are built out of $\mathbf{M}_S$ for exactly this reason.

4. The spectrum for $31 \le S \le 60$

4.1. **The certificate.** Conjecture 1.1 at a fixed S is a statement about the characteristic polynomial of an explicit rational matrix, and the following elementary lemma is what turns it into two matrix identities. It is the only reasoning step used, and it is proved by argument.

Lemma 4.1 (Orthogonal eigenbasis)**.** *Let A, V be n-square matrices over a field K and let $d, l\colon \{1,\dots,n\} \to K$ satisfy*

$$AV = V\operatorname{diag}(d), \qquad V^{\top}V = \operatorname{diag}(l), \qquad l_i \neq 0 \text{ for all } i.$$

Then V is invertible and $\operatorname{char}_A(X) = \prod_i (X - d_i)$.

Proof. Taking determinants in $V^{\top}V = \operatorname{diag}(l)$ gives $(\det V)^2 = \prod_i l_i \neq 0$, so $\det V \neq 0$. Then $A = V\operatorname{diag}(d)\,V^{-1}$, and the characteristic polynomial is invariant under conjugation, so it equals that of $\operatorname{diag}(d)$. □

The point of the hypothesis $V^{\top}V = \operatorname{diag}(l)$ is that invertibility of a large V comes from a *diagonal* determinant: no determinant of an $(S+1)$-square matrix is ever evaluated, and at $S = 60$ such an evaluation is not feasible at all.

The certificate at a given S is the matrix V whose columns are

- for $0 \le n \le \lfloor S/2\rfloor$: the vector $\mathbf{X}_S\, w_n$, where $w_n = \prod_{m\neq n}\big(\mathbf{M}_S - \theta(S,m)I\big)e_0$ with $\mathbf{M}_S$ and θ as in (5) and (10), each intermediate vector divided by the gcd of its entries;
- for $0 \le a < \lceil S/2\rceil$: the kernel vector $e_a - e_{S-a}$, which lies in the kernel because $f_a = f_{S-a}$ makes rows a and $S-a$ of Q_S equal.

Nothing about this construction is proved or needs to be: V is a witness, produced from Corollary 3.6, and Lemma 4.1 takes only the two identities it satisfies. In particular V is computed from the definitions rather than stored as numerical data, so no list of eigenvector coordinates appears anywhere.

Theorem 4.2 (Conjecture 1.1 for $31 \le S \le 60$)**.** *For every integer S with $31 \le S \le 60$,*

$$\operatorname{char}_{Q_S}(X) = X^{\lceil S/2 \rceil} \prod_{n=0}^{\lfloor S/2 \rfloor} \big(X - \lambda(n)\big), \qquad \lambda(n) = \binom{2n}{n}^2 16^{-n}.$$

Equivalently, the eigenvalues of Q_S are exactly $\lambda(0), \dots, \lambda(\lfloor S/2 \rfloor)$, each of multiplicity 1, together with 0 of multiplicity $\lceil S/2 \rceil$: Conjecture 1.1 holds at every such S, multiplicities included.

Proof. Fix S, let V be the certificate above, let l_k be the squared Euclidean norm of the k-th column of V, and let d be the vector whose entries are $\lambda(0), \dots, \lambda(\lfloor S/2 \rfloor)$ followed by $\lceil S/2 \rceil$ zeros. Three facts are established by exhaustive evaluation in exact rational arithmetic:

$$Q_S V = V \operatorname{diag}(d), \qquad V^\top V = \operatorname{diag}(l), \qquad l_k \neq 0 \ \text{ for all } k,$$

costing $(S+1)^2$ entry comparisons, $(S+1)^2$ entry comparisons and $S+1$ tests respectively, each entry being a sum of $S+1$ products. Lemma 4.1 then gives $\operatorname{char}_{Q_S}(X) = \prod_k (X - d_k)$, and splitting that product at $k = \lfloor S/2 \rfloor$ — a polynomial identity, proved by argument — gives the displayed form. Over the thirty values $31 \le S \le 60$ this is 90 exhaustive evaluations; the largest single one is $S = 60$, where the two matrix identities compare $2 \times 61^2 = 7442$ rational numbers, each a sum of 61 products. □

Proposition 4.3 (Inside the source's own range)**.** *The conclusion of Theorem 4.2 also holds at $S = 4$, $S = 10$, $S = 20$ and $S = 30$. Moreover $\lambda(0) - \lambda(1) = 3/4$.*

Proof. The same certificate and the same three evaluations, at four values inside the range $S \le 30$ that [1] reports having verified. The mathematics is the source's; what is added is that the check is now machine-checked rather than reported. The last assertion is $1 - \frac{1}{4} = \frac{3}{4}$, and it is the value of $\operatorname{sg}(Q_S)$ that Conjecture 1.1 would force for every $S \ge 2$. □

Proposition 4.3 is a control, not a result: a definition that had drifted from (2) would have to reproduce the source's own spectrum at four independent sizes to survive it.

Proposition 4.4 (Negative controls)**.** *Each of the following holds.*

1. The certified list is not a prefix of a longer one. *No entry of the spectrum certified at $S = 20$ equals $\lambda(11)$; with Proposition 4.3 this says $\lambda(\lfloor S/2 \rfloor + 1)$ is not an eigenvalue of Q_{20}.*
2. The certificate is not satisfied vacuously. *Every column of the certificate V at $S = 20$ has strictly positive squared norm, so Lemma 4.1 is applied with a genuine basis.*
3. The statement is not about a rank-one object. *Q_{20} is not a constant matrix: $Q_{20}[0,0] \neq Q_{20}[0,1]$.*
4. The zero eigenvalue does not have multiplicity $\lceil S/2 \rceil + 1$. *At $S = 20$ the certified eigenvalue $\lambda(10)$ is non-zero.*

(5) The scaling is load-bearing. *The first row of the integer matrix A_4 does not sum to* 1*: double stochasticity is a property of Q_S, not of $A_S = 2^{2S}Q_S$.*

Proof. Each item is one exhaustive evaluation over a set of size at most 21, or a single comparison of two explicit rationals. □

5. The smallest entry

Conjecture 1.2 has the same status in [1] as Conjecture 1.1: verified there for $S \le 30$, open in general. Note that the integrand in (2) is symmetric in its four arguments, so $Q(\lfloor S/2\rfloor, \lceil S/2\rceil, S, 0)$ is the entry $Q_S[\lfloor S/2\rfloor, 0]$ of (3), and Conjecture 1.2 is the assertion that this entry is the least one in the matrix.

Theorem 5.1 (Conjecture 1.2 for $31 \le S \le 60$, with its minimiser set)**.** *Let $31 \le S \le 60$. Then for all $0 \le a, c \le S$,*

$$Q(\lfloor S/2\rfloor, \lceil S/2\rceil, S, 0) \;\le\; Q(a, S-a, c, S-c),$$

and equality holds precisely when (a, c) belongs to

$$\Big\{(a,c) : a \in \{\lfloor S/2\rfloor, \lceil S/2\rceil\},\ c \in \{0, S\}\Big\} \cup \Big\{(a,c) : c \in \{\lfloor S/2\rfloor, \lceil S/2\rceil\},\ a \in \{0, S\}\Big\},$$

a set of 4 positions when S is even and 8 when S is odd.

Proof. Both halves are exhaustive comparisons on the integer matrix A_S: the inequality is $(S+1)^2$ comparisons against the entry $A_S[\lfloor S/2\rfloor, 0]$, and the equality clause is $(S+1)^2$ two-way implications, one per position. Over the thirty values this is 60 exhaustive evaluations, the largest being $S = 60$ with 3721 positions. No structure is used; the statement is a computation once it is asked for. □

Remark 5.2. The set in Theorem 5.1 is exactly the orbit of $(\lfloor S/2\rfloor, 0)$ under the three symmetries $a \mapsto S - a$, $c \mapsto S - c$ and $(a, c) \mapsto (c, a)$, all of which preserve Q_S — the first two because $f_a = f_{S-a}$, the third because Q_S is symmetric. So the content of the second half of Theorem 5.1 is that the minimum is attained on *no* position outside the orbit that the symmetries force. [1] states only the inequality, locating the minimum "in the first column with the middle row"; the exactness of the minimiser set is not stated there and we have not found it stated elsewhere. It is not new mathematics — it is an $(S+1)^2$ comparison — but it is the natural sharp form of the conjecture, which a proof of Conjecture 1.2 would be expected to produce.

Remark 5.3. Outside the formal development, both conjectures were also verified in exact rational arithmetic for every S with $0 \le S \le 62$, in a separate implementation written before the formal one. That is computed data and carries no theorem here; the machine-checked range is the one stated in Theorems 4.2 and 5.1 together with Proposition 4.3.

6. Verification

Every theorem, proposition, lemma and corollary above has been formally verified in Lean 4 against *Mathlib* [10], except Propositions 3.1 and 3.2 and their consequences Corollaries 3.5 and 3.6, which are proved by hand here and lie outside the formal development because *Mathlib* has no Laguerre polynomials, so that L_n and $p_m(a, b)$ cannot yet be written down there; what is machine-checked about the factorisation is Theorem 3.3, its instances at $S \in \{31, 36, 41\}$ and the compression (9)

at those S, and Remarks 3.4 and 5.3 report computations outside the development and are labelled as such. The development contains no `sorry` and declares no axiom of its own; Lemma 4.1, the compression $\mathrm{char}_{EF} = X^{n-k}\mathrm{char}_{FE}$ of Theorem 3.3(3) and the rearrangement of $\prod_k (X - d_k)$ in Theorem 4.2 are proved by argument with no evaluation and depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`. Everything else is exhaustive evaluation over an explicitly bounded finite set, on exact integers and exact rationals — never on floating point — carried out by Lean's `native_decide`, which delegates a decidable proposition to compiled code and records one axiom per invocation, so that the trusted base for the evaluations (and only for them) extends by the Lean compiler; the searches are exactly those counted in the proofs above: 65 entry comparisons plus one corner value for Proposition 2.2; 30 cells $\times 3$ evaluations over at most 61^2 positions for Proposition 2.3; 3 cells $\times 2$ evaluations, the largest comparing 42^2 entries of 441 terms each, for Theorem 3.3; 34 cells $\times 3$ evaluations, the largest comparing 2×61^2 rationals of 61 terms each, for Theorem 4.2 and Proposition 4.3; 30 cells $\times 2$ evaluations over $(S+1)^2$ positions for Theorem 5.1; and five evaluations over sets of size at most 21 for Proposition 4.4 — in total well under one CPU-hour and under 8 GB of memory. Two independent implementations were run before any formal proof was written: Q_S was built from (11) and from the four-fold expansion separately, and both conjectures were checked in exact rational arithmetic for $S \le 62$ (Remark 5.3). The searches behind §1.4 were a full-text pass over an arXiv corpus of 881,145 papers, in which the string `1709.08100` occurs in exactly two papers (the source and the bibliography of one other) and the conjunction of *Laguerre*, *Strichartz* and *doubly stochastic* returns exactly four, none carrying (7); a reading of all nine recorded citing contexts of [1], of which exactly one, [2], engages with the material of §1.4 at all — it cites [1]'s Conjectures 1 and 2, which are not the two treated here, and asserts without details that its own method yields $\gamma = 3/4$, as quoted in §1.4 — while none of the nine states Conjecture 1.1 or Conjecture 1.2 or carries (7); and OEIS queries on the numerators and denominators of $\lambda(n)$ and on the phrasings of both conjectures. We record that the sentence quoted from [2] in §1.4 is present in the published version and in arXiv:2011.02187v2, and absent from arXiv:2011.02187v1, which is what a search run against a mirror of the first e-print version will show. The repository is private; repository reference to be added at submission.

7. Questions

Question 7.1. Does the criterion of Gonçalves and Zagier [2] apply to Q_S? It concerns a "special" power series F and a matrix read off its coefficients, whose eigenvalues are then independent of S; Q_S is of that shape, and [2] states that its Section 3 method reproves [1, Theorem 3] with $\gamma = 3/4$ while omitting the details and without stating Conjecture 1.1 (§1.4). The missing step, in public, is the explicit generating function of $Q(a, b, c, d)$ under the restriction $d = a + b - c$, and the verification that it satisfies the hypothesis; note that Conjecture 1.1 asserts more than $\gamma = 3/4$ does, namely the whole spectrum with multiplicities, and that the criterion of [2], if it applies, delivers exactly that. This is the route to a proof for all S, and it is not attempted here.

Question 7.2. Prove directly that the integer matrix $\mathbf{M}_S$ of (5), of order $\lfloor S/2 \rfloor + 1$, has the eigenvalues $(-1)^n \binom{2n}{n} 2^{S-2n}$, $0 \le n \le \lfloor S/2 \rfloor$. By Corollary 3.6 this implies

Conjecture 1.1 at S, and it is a question about a matrix of half the size, over $\mathbb{Z}$, with integer eigenvalues.

Question 7.3. Is there a formula, or even a lower bound, for a general entry $Q(a,b,c,d)$ off the diagonal slice $b = S-a$, $d = S-c$? Identity (7) covers only the slice, which is what Q_S needs; the combinatorial evaluations of [4, 3, 5, 6, 7] cover the general case but are not product formulas. A lower bound of the right shape would attack Conjecture 1.2, which is at present supported only by computation: [1]'s for $S \le 30$ and ours for $31 \le S \le 60$.

Remark 7.4. The conjectured eigenvalues have a classical closed form that neither [1] nor any of its citing papers records: since $K(k) = \frac{\pi}{2}\sum_{n\ge 0}\binom{2n}{n}^2 16^{-n}k^{2n}$ is the standard series for the complete elliptic integral of the first kind, $\lambda(n) = [k^{2n}]\,\frac{2}{\pi}K(k)$. In lowest terms the numerators of $\lambda(n)$ are OEIS [9] A038534, "*Numerators of coefficients of EllipticK/Pi*", whose comments record that these are equally the numerators of the coefficients of $\frac{2}{\pi}K(k) = {}_2F_1(\frac{1}{2},\frac{1}{2};1;k^2)$ in powers of k^2; the denominators are A056982, "$a(n) = 4^{A005187(n)}$. *The denominators of the Landau constants*", and not the A038533 that OEIS pairs with A038534, which is the denominator sequence for K/π and hence exactly twice ours. The integers $16^n\lambda(n) = \binom{2n}{n}^2$ are A002894, "$a(n) = \text{binomial}(2n,n)^2$". Whether this identification is a route to a proof of Conjecture 1.1 is unexplored.

References

[1] F. Gonçalves, *A sharpened Strichartz inequality for radial functions*, J. Funct. Anal. **276** (2019), no. 6, 1925–1947; arXiv:1709.08100v2, the version quoted throughout.

[2] F. Gonçalves and D. Zagier, *Strichartz estimates with broken symmetries*, Rev. Mat. Iberoam. **38** (2022), no. 5, 1709–1722; arXiv:2011.02187v2. The sentence quoted in §1.4 is absent from arXiv:2011.02187v1.

[3] R. Askey, M. Ismail and T. Koornwinder, *Weighted permutation problems and Laguerre polynomials*, J. Combin. Theory Ser. A **25** (1978), no. 3, 277–287.

[4] S. Even and J. Gillis, *Derangements and Laguerre polynomials*, Math. Proc. Cambridge Philos. Soc. **79** (1976), no. 1, 135–143.

[5] J. Gillis and D. Zeilberger, *A direct combinatorial proof of a positivity result*, European J. Combin. **4** (1983), no. 3, 221–223.

[6] D. Foata and D. Zeilberger, *Laguerre polynomials, weighted derangements, and positivity*, SIAM J. Discrete Math. **1** (1988), no. 4, 425–433.

[7] M. E. H. Ismail, A. Kasraoui and J. Zeng, *Separation of variables and combinatorics of linearization coefficients of orthogonal polynomials*, J. Combin. Theory Ser. A **120** (2013), no. 3, 561–599; arXiv:1112.0970.

[8] G. Szegő, *Orthogonal polynomials*, 4th ed., Amer. Math. Soc. Colloq. Publ., vol. XXIII, Providence, RI, 1975.

[9] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`; entries A002894, A005187, A038533, A038534, A056982.

[10] The mathlib Community, *The Lean mathematical library*, in: Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381.