The Sharp Exponential Constant for 6-Regular Circulant Matrices

Yair Lavi

24 September 2026

Abstract

We prove that, for every integer $n \geq 6$ and six-element set $S \subseteq \mathbb{Z}_n$, the binary circulant $C_n(S) = (1_{\{j-i \in S\}})_{i,j \in \mathbb{Z}_n}$ satisfies

$$\operatorname{per} C_n(S) \geq \left(\frac{3125}{1296} e^{7/250000}\right)^n.$$

For every integer $d \geq 2$, we also identify the optimal uniform base as the limit of an explicit sequence of circulants:

$$\inf_{n \geq d} \inf_{\substack{S \subseteq \mathbb{Z}_n \\ |S|=d}} \operatorname{per} C_n(S)^{1/n} = \lim_{q \to \infty} \operatorname{per} C_{q^{d-1}}(\{0, 1, q, \ldots, q^{d-2}\})^{1/q^{d-1}},$$

where q runs through integers at least 2. In degree six this base is at most $163812873663198^{1/35}$. The lower bound strictly improves the sharp uniform base $3125/1296$ for unrestricted binary 6-regular matrices. This resolves the surviving circulant lower-bound question in Minc's Problem 10; its proposed full upper bound fails even for circulants.

Keywords. Permanent; binary circulant; matching measure; regular bipartite graph; matching entropy.
2020 Mathematics Subject Classification. 15A15 (primary), 05C70, 05C50 (secondary).

1 Introduction

Let Λ_n^d denote the set of $n \times n$ binary matrices having every row sum and every column sum equal to d. Two classical exponential bounds are

$$\left(\frac{(d-1)^{d-1}}{d^{d-2}}\right)^n \leq \operatorname{per} A \leq (d!)^{n/d}, \qquad A \in \Lambda_n^d.$$

Schrijver and Valiant conjectured the lower inequality and established its asymptotic optimality [4]; Schrijver proved it [5]. Brègman proved the upper inequality [13] (see also Schrijver's short proof [3]). Both bases are asymptotically best possible in the unrestricted class. At degree six they are

$$\frac{5^5}{6^4} = \frac{3125}{1296} \quad \text{and} \quad (6!)^{1/6} = 2.9937951\ldots.$$

Minc's earlier work studied permanents of circulants [1, 2]. His 1983 survey [14] restates Problem 10 from his 1978 monograph [15], explicitly giving both the unrestricted and circulant scopes. After the correction recorded by Cheon and Wanless, the problem asks for

$$2.31^n < m^n \le \operatorname{per} A \le M^n < 2.99^n$$

for every $A \in \Lambda_n^6$ and all sufficiently large n, or alternatively for every circulant in that class and all sufficiently large n [14, Problem 10, p. 246]; [6, Problem 10, p. 336]. The 1983 display actually prints 2.29 at the final endpoint; Cheon and Wanless explicitly identify this as a typographical error for 2.99 [6, p. 336].

The 2.31 threshold belongs to Minc's 1978 formulation [15]. It predates Schrijver and Valiant's 1980 conjecture of the stronger 3125/1296 lower base [4] and Schrijver's 1998 proof of that bound [5]. Minc asked for some $m > 2.31$; he did not assert that 2.31 was the optimal base.

For $S \subseteq \mathbb{Z}_n$, put $C_n(S) = \sum_{s\in S} P^s$, where $P_{ij} = 1$ exactly when $j - i = 1$ in $\mathbb{Z}_n$. Equivalently, $C_n(S)_{ij} = 1$ exactly when $j - i \in S$.

The full corrected chain is impossible even for circulants. For $n = 6k$, the support $S = \{0, k, 2k, 3k, 4k, 5k\}$ gives k all-one 6×6 blocks after row and column permutations, so $\operatorname{per} C_n(S) = 720^k$ and its root rate $\operatorname{per} C_n(S)^{1/n}$ is $720^{1/6} = 2.9937951\ldots > 2.99$, with the last inequality equivalent to $720 \cdot 100^6 > 299^6$. Cheon and Wanless therefore isolate the sole surviving component: can the sharp unrestricted lower base be improved for 6-regular circulants? We answer that question and identify the optimal base. Put

$$m_{\mathrm{circ},d} = \inf_{n\ge d} \inf_{\substack{S\subseteq\mathbb{Z}_n\\ |S|=d}} \operatorname{per} C_n(S)^{1/n}.$$

This infimum is also the optimal asymptotic base if a fixed positive multiplicative prefactor is allowed: every finite circulant can be repeated as a disjoint circulant lift, so such a prefactor disappears after taking roots.

Let $e_1, \ldots, e_{d-1}$ be the standard basis of $\mathbb{Z}^{d-1}$ and put $D_d = \{0, e_1, \ldots, e_{d-1}\}$. The bipartite graph Γ_d has left vertices L_x, right vertices R_x for $x \in \mathbb{Z}^{d-1}$, and edges L_xR_{x+s} for $s \in D_d$. To specify the entropy in our answer, let $m_k(G)$ count the k-edge matchings of a finite balanced bipartite graph G with m vertices in each color class. Its matching polynomial is $\sum_{k=0}^m (-1)^k m_k(G) z^{2m-2k}$, and its normalized matching-root measure ρ_G gives mass $1/(2m)$ to each root, with multiplicity. Let ρ_{Γ_d} be the weak limit of these measures for the bipartite graphs of $C_{q^{d-1}}(\{0, 1, q, \ldots, q^{d-2}\})$ as integer $q \to \infty$. We define the perfect-matching entropy per vertex by

$$\lambda_{\Gamma_d}(1) = \int \log|x| \, d\rho_{\Gamma_d}(x).$$

Sections 2–4 establish that this limit exists and that the integral is finite.

Our main result is the following.

Theorem 1.1 (Sharp circulant constant)**.** *For every integer $d \ge 2$,*

$$\boxed{m_{\mathrm{circ},d} = h_d := \exp\big(2\lambda_{\Gamma_d}(1)\big),}$$

with Γ_d and $\lambda_{\Gamma_d}(1)$ as defined above. Moreover, for integers $q \ge 2$, the bipartite graphs of the connected cyclic quotients (the circulants below, whose bipartite graphs are connected because 1 is in their support)

$$C_{q^{d-1}}\big(\{0, 1, q, \ldots, q^{d-2}\}\big)$$

have, for every fixed radius, the same rooted neighborhoods as Γ_d when q is sufficiently large, and their permanent root rates converge to h_d.

Every finite circulant quotient has root rate at least this limit. The proof combines the coefficientwise matching inequality for bipartite 2-lifts [9] with local continuity and endpoint convergence of matching entropy [7, 8].

For degree six we obtain the strict factor $e^{7/250000}$ over the unrestricted lower base.

Theorem 1.2 (Certified degree-six bracket)**.** *For every $n \geq 6$ and every six-element $S \subseteq \mathbb{Z}_n$,*

$$\operatorname{per} C_n(S) \geq \left[\frac{3125}{1296} \exp\left(\frac{7}{250000}\right)\right]^n .$$

Consequently

$$\boxed{\frac{3125}{1296} e^{7/250000} \leq m_{\mathrm{circ},6} = h_6 \leq 163812873663198^{1/35}.}$$

The numerical certificate uses only exact integers and rational intervals; decimal numbers in this paper are for presentation. The upper endpoint is the exact permanent of the 35-circulant with support $\{0, 1, 3, 7, 16, 24\}$.

We further prove a finite-degree convergence modulus, give a convergent two-sided moment scheme for evaluating h_6, and report an exact finite census through order 31. These results separate what is now settled from what remains: the optimal exponent is proved, while a closed form, many-digit evaluation, strict nonattainment by finite quotients, and a stability theorem for near minimizers are still open.

2 Matching entropy and the quotient model

2.1 Bipartite graphs and matching measures

The matrix $C_n(S)$ is the bipartite adjacency matrix of the graph with left and right color classes both indexed by $\mathbb{Z}_n$, with

$$L_x \sim R_y \iff y - x \in S.$$

Thus its permanent is the number of perfect matchings of this graph.

For a finite balanced bipartite graph G with $m \geq 1$ vertices in each color class and a perfect matching, let $m_k(G)$ be the number of k-edge matchings and put

$$M(G,t) = \sum_{k=0}^{m} m_k(G) t^k, \qquad P_G(t) = \frac{1}{2m} \log M(G,t).$$

Give a matching M probability $t^{|M|}/M(G,t)$. Its expected size divided by m is

$$p_G(t) = \frac{tM'(G,t)}{mM(G,t)}.$$

Because G has a perfect matching, $p_G(t)$ increases continuously from 0 to 1 as t runs from 0 to infinity. For $0 < p < 1$, the matching entropy is

$$\lambda_G(p) = P_G(t) - \frac{p}{2} \log t, \qquad p = p_G(t).$$

Equivalently, $\lambda_G(p) = \inf_{t>0}[P_G(t) - (p/2)\log t]$: as a function of $\log t$, $P_G(t)$ is convex and its derivative is $p_G(t)/2$.

Set $\lambda_G(0) = 0$ by continuity.

At the perfect-matching endpoint,

$$\lambda_G(1) = \frac{1}{2m} \log \mathrm{pm}(G),$$

where $\mathrm{pm}(G) = m_m(G)$ is the number of perfect matchings. The matching polynomial and its normalized root measure, recalled from the introduction, are explicitly

$$\mu_G(z) = \sum_{k=0}^{m} (-1)^k m_k(G) z^{2m-2k}, \qquad \rho_G = \frac{1}{2m} \sum_{\mu_G(\xi)=0} \delta_\xi,$$

with roots counted according to multiplicity. The measure's support is contained in $[-2\sqrt{d-1}, 2\sqrt{d-1}]$ when G has maximum degree $d \geq 2$ [10]. The basic integral identities are

$$P_G(t) = \frac{1}{2} \int \log(1 + tx^2)\, d\rho_G(x), \qquad \lambda_G(1) = \int \log|x|\, d\rho_G(x).$$

The self-avoiding-walk tree of a graph rooted at v has one vertex for each simple path starting at v, with two paths adjacent when one extends the other by one edge. For a transitive infinite graph L, local convergence of finite transitive graphs means that, for every fixed radius, their rooted neighborhoods eventually agree with a rooted neighborhood of L. The matching measure ρ_L is the weak limit of their matching-root measures. Define

$$P_L(t) = \frac{1}{2} \int \log(1 + tx^2)\, d\rho_L(x), \qquad p_L(t) = 2tP_L'(t) = \int \frac{tx^2}{1 + tx^2}\, d\rho_L(x),$$

$\lambda_L(p) = \inf_{t>0}[P_L(t) - (p/2)\log t]$ for $0 < p < 1$, and $\lambda_L(1) = \lim_{p\uparrow 1} \lambda_L(p)$. The function $\tau \mapsto P_L(e^\tau)$ is convex with derivative $p_L(e^\tau)/2$; therefore the infimum defining $\lambda_L(p_L(t))$ is attained at t.

Local-limit facts used below [7, 8]. If bounded-degree finite graphs G_j with perfect matchings converge locally to L, their matching measures converge weakly [7, Theorem 2.7], each moment is the average number of closed walks from a uniform root in its self-avoiding-walk tree [7, Theorem 2.2], and both $P_{G_j}(t) \to P_L(t)$ for $t > 0$ and $\lambda_{G_j}(p) \to \lambda_L(p)$ for $0 \leq p < 1$ [7, Theorem 3.3]. This limit definition of $\lambda_L(p)$ agrees with the infimum above by the integral formulas [8, Remark 2.7]. If the G_j are also vertex-transitive, d-regular and bipartite, then $\lambda_{G_j}(1) \to \lambda_L(1)$ [8, Theorem 1.8].

For $L = \Gamma_d$, Section 4 proves $\rho_L([-s, s]) \leq C_d s$. Thus $\rho_L(\{0\}) = 0$ and $p_L(t) \uparrow 1$. Splitting the integral for $1 - p_L(t)$ at $|x| = t^{-1/3}$ shows it is $O(t^{-1/3})$. Since

$$P_L(t) - \tfrac{1}{2}\log t = \tfrac{1}{2} \int \log(x^2 + 1/t)\, d\rho_L(x),$$

the root-mass bound permits passage to the limit $t \to \infty$ in this integral. The term $(1 - p_L(t))\log t$ vanishes, so the Legendre formula gives $\lambda_L(1) = \int \log|x|\, d\rho_L(x)$, as used in the introduction.

2.2 Every circulant is a lattice quotient

Translate a d-element support so that it is

$$S = \{0, s_1, \ldots, s_{d-1}\} \subseteq \mathbb{Z}_n.$$

Let $H \leq \mathbb{Z}_n$ be the subgroup generated by the s_i, and define

$$\psi : \mathbb{Z}^{d-1} \longrightarrow H, \qquad e_i \longmapsto s_i.$$

Its kernel Λ is a full-rank lattice. Write $A_\Lambda = \mathbb{Z}^{d-1}/\Lambda$ and let G_Λ have left vertices L_x, right vertices R_x for $x \in A_\Lambda$, and edges $L_x R_{x+s}$ for $s \in D_d$. Each connected component of the circulant bipartite graph is isomorphic to this quotient graph, whose edges retain their labels in D_d.

All components are isomorphic. If $|H| = m$, there are n/m components and

$$\operatorname{per} C_n(S)^{1/n} = \operatorname{pm}(G_\Lambda)^{1/m} = \exp\bigl(2\lambda_{G_\Lambda}(1)\bigr).$$

The graph $G_0 = \Gamma_d$ is a common cover of all these labelled quotients.

3 Proof of the sharp constant

3.1 Unwrapping finite quotients by 2-lifts

A 2-lift of a graph G is a graph equipped with a projection to G such that every vertex has two preimages and the edges above each edge of G form a perfect matching between its two vertex fibers. We use the following theorem of Csikvári [9].

Bipartite 2-lift inequality. If $\widetilde{G}$ is a bipartite 2-lift of a finite bipartite graph G, then for every k,

$$m_k(\widetilde{G}) \le m_k(G \sqcup G).$$

The coefficientwise inequality gives $M(\widetilde{G}, t) \le M(G, t)^2$ for every $t > 0$. Taking pressure per vertex and then the infimum formula from Section 2.1 gives, with entropy normalized per vertex,

$$\lambda_{\widetilde{G}}(p) \le \lambda_G(p), \qquad 0 \le p \le 1.$$

The endpoints follow by continuity of the finite-graph entropies.

For a full-rank lattice $\Lambda \le \mathbb{Z}^{d-1}$, the quotient $\Lambda/2\Lambda$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{d-1}$. Choose a composition series between Λ and 2Λ. For an index-two inclusion $\Lambda' \subset \Lambda$, every vertex fiber of $G_{\Lambda'} \to G_\Lambda$ has two elements, and each edge label $s \in D_d$ maps that fiber bijectively to the fiber of its neighboring vertex. Thus each successive labelled quotient is a bipartite 2-lift. The labels remain distinct in every refinement because they are distinct modulo Λ. Hence

$$\lambda_{G_\Lambda}(p) \ge \lambda_{G_{2\Lambda}}(p) \ge \lambda_{G_{4\Lambda}}(p) \ge \cdots.$$

Every nonzero lattice vector in $2^j\Lambda$ has length tending to infinity with j. Therefore

$$G_{2^j\Lambda} \longrightarrow \Gamma_d$$

locally. Finite-activity continuity of matching entropy gives

$$\lambda_{G_\Lambda}(p) \ge \lambda_{\Gamma_d}(p), \qquad 0 \le p < 1.$$

The quotient G_Λ has a perfect matching, for example the matching formed by all edges carrying the label 0. Thus its finite endpoint is well-defined and $\lambda_{G_\Lambda}(p) \to \lambda_{G_\Lambda}(1)$ as $p \uparrow 1$. Letting $p \uparrow 1$ therefore yields

$$\lambda_{G_\Lambda}(1) \ge \lambda_{\Gamma_d}(1).$$

By the component calculation in Section 2.2,

$$\operatorname{per} C_n(S)^{1/n} \ge h_d.$$

This proves $m_{\mathrm{circ},d} \ge h_d$.

3.2 Explicit cyclic quotients attain the limit

For an integer $q \geq 2$, put

$$n_q = q^{d-1}, \qquad S_q = \{0, 1, q, q^2, \ldots, q^{d-2}\} \subseteq \mathbb{Z}_{q^{d-1}}.$$

Let G_q be the bipartite graph of $C_{n_q}(S_q)$. The support generates $\mathbb{Z}_{n_q}$ because it contains 1. The lattice describing this quotient is the kernel of

$$\phi_q : \mathbb{Z}^{d-1} \longrightarrow \mathbb{Z}_{q^{d-1}}, \qquad (a_0, \ldots, a_{d-2}) \longmapsto \sum_{j=0}^{d-2} a_j q^j.$$

Fix R. If $q > R$, $\sum_j |a_j| \leq R$, and $\phi_q(a) = 0$, then

$$\left| \sum_j a_j q^j \right| \leq R q^{d-2} < q^{d-1}.$$

The congruence is therefore an equality in the integers. Reduction modulo q gives $a_0 = 0$; division by q and induction give $a = 0$. Hence the shortest nonzero vector of $\ker \phi_q$ tends to infinity, and

$$G_q \longrightarrow \Gamma_d$$

locally.

These finite graphs are vertex-transitive: translations act transitively on each color class, and $L_x \mapsto R_{-x}$, $R_y \mapsto L_{-y}$ exchanges the classes. Endpoint convergence for vertex-transitive bipartite graphs [8] now gives

$$\lim_{q \to \infty} \operatorname{per} C_{q^{d-1}}(S_q)^{1/q^{d-1}} = \exp\bigl(2\lambda_{\Gamma_d}(1)\bigr) = h_d.$$

Thus $m_{\mathrm{circ},d} \leq h_d$, completing the proof of Theorem 1.1.

4 A quantitative quotient-convergence theorem

The preceding proof is qualitative. A shortest-lattice-vector parameter gives an explicit rate. Throughout this section, $\Lambda \leq \mathbb{Z}^{d-1}$ is full-rank and the images of $0, e_1, \ldots, e_{d-1}$ in $\mathbb{Z}^{d-1}/\Lambda$ are distinct.

These assumptions make G_Λ a finite d-regular bipartite graph, and it is vertex-transitive. Translations act transitively within each color class, while $L_x \mapsto R_{-x}$ and $R_y \mapsto L_{-y}$ exchange the two classes and preserve adjacency.

For $a = (a_1, \ldots, a_{d-1}) \in \mathbb{Z}^{d-1}$, define

$$p(a) = \sum_i \max(a_i, 0), \qquad n(a) = \sum_i \max(-a_i, 0),$$

$$\|a\|_D = 2 \max\{p(a), n(a)\}, \qquad \sigma(\Lambda) = \min_{0 \neq a \in \Lambda} \|a\|_D.$$

The norm has a direct graph meaning:

$$\operatorname{dist}_{\Gamma_d}(L_0, L_a) = \|a\|_D.$$

Indeed, a path of length $2k$ expresses a as a sum of k elements of D_d minus another such sum, giving the lower bound; listing the positive and negative coordinate units and padding the shorter list with zeros gives equality.

Put

$$B_d = 2\sqrt{d-1}, \qquad C_d = \frac{2\sqrt{d-1}}{d}.$$

For a finite transitive d-regular bipartite graph on $2m$ vertices, write its squared positive matching roots as $0 < \gamma_1 \le \cdots \le \gamma_m$. Csikvári's ordered-root estimate [8] states that

$$\gamma_k \ge \frac{d^2k^2}{4(d-1)m^2}.$$

The matching-polynomial roots are $\pm\sqrt{\gamma_k}$, each with mass $1/(2m)$. Therefore, if j of the γ_k are at most s^2, then $j/m \le 2\sqrt{d-1}s/d$, and so

$$\rho_G([-s,s]) \le C_d s \qquad (s \ge 0).$$

The same estimate passes to every bounded-degree local limit of such graphs. Indeed, if $G_j \to L$ locally, then their matching measures converge weakly. For any $\eta > 0$, the portmanteau theorem applied to $(-s-\eta, s+\eta)$ gives

$$\rho_L([-s,s]) \le \rho_L((-s-\eta, s+\eta)) \le \liminf_{j\to\infty} \rho_{G_j}((-s-\eta, s+\eta)) \le C_d(s+\eta);$$

letting $\eta \downarrow 0$ gives the asserted bound for ρ_L.

Theorem 4.1 (Finite-degree modulus)**.** *Let $d \ge 2$ and $N \ge 1$ be integers with $2N < \sigma(\Lambda)$. For $\varepsilon > 0$, set*

$$u = \frac{\varepsilon}{B_d}, \qquad r = (\sqrt{1+u^2} - u)^2.$$

Then

$$\boxed{0 \le \lambda_{G_\Lambda}(1) - \lambda_{\Gamma_d}(1) \le \frac{2r^{N+1}}{(N+1)(1-r)} + \frac{\pi C_d}{2}\varepsilon.}$$

Proof. The covering map $\Gamma_d \to G_\Lambda$ is injective on every rooted ball of radius N, since two lifts of one ball vertex would be at distance at most $2N < \sigma(\Lambda)$. It also preserves every edge between ball vertices: an edge from the chosen lift of one endpoint reaches a lift of the other at distance at most $2N+1$ from its chosen lift. Because $\sigma(\Lambda)$ is even, $2N < \sigma(\Lambda)$ implies $2N+1 < \sigma(\Lambda)$, so these lifts coincide. Thus the rooted N-balls are isomorphic. The kth matching-measure moment counts length-k closed walks in the self-avoiding-walk tree, which remain inside radius $\lfloor k/2 \rfloor$. Hence the matching measures of G_Λ and Γ_d have equal moments through degree $2N$.

Regularize the endpoint logarithm by

$$\phi_\varepsilon(x) = \frac{1}{2}\log(x^2 + \varepsilon^2).$$

If $F(s) = \rho([-s,s]) \le C_d s$, a layer-cake calculation gives

$$0 \le \int (\phi_\varepsilon(x) - \log|x|)\, d\rho(x) \le \frac{\pi C_d}{2}\varepsilon.$$

On $[-B_d, B_d]$, the Chebyshev expansion has the form

$$\phi_\varepsilon(x) = A_0 + \sum_{k\geq 1} \frac{(-1)^{k+1} r^k}{k} T_{2k}(x/B_d).$$

Truncation after $k = N$ has uniform error at most $r^{N+1}/((N+1)(1-r))$.

The two measures integrate the truncated polynomial equally, so their regularized logarithmic integrals differ by at most twice this error. The two regularization losses lie in the same interval; comparing them costs one copy of its length. The lower inequality is the finite-abelian-quotient argument of Section 3.1. Combining the estimates proves the claim. □

Choosing parameters explicitly gives a closed form.

Corollary 4.2. *Put $M = N + 1 \geq 2$ and suppose $2(M-1) < \sigma(\Lambda)$. Then*

$$\boxed{0 \leq \lambda_{G_\Lambda}(1) - \lambda_{\Gamma_d}(1) \leq \frac{\pi(d-1)}{d} \frac{\log M}{M} + \frac{4e^{1/100}}{M \log M}.}$$

To obtain this, take $\varepsilon = B_d \log M/(2M)$, so $u = \log M/(2M)$ and $r = e^{-2 \operatorname{arsinh} u}$. The inequalities $\operatorname{arsinh} u \geq u - u^3/6$ and

$$\frac{(\log M)^3}{24M^2} \leq \frac{1}{100}$$

for $M \geq 2$ give $r^M \leq e^{1/100}/M$. Also $u \leq 1/(2e) < 1/5$, whence

$$1 - r = 2u(\sqrt{1+u^2} - u) \geq u.$$

Thus the Chebyshev term in Theorem 4.1 is at most $4e^{1/100}/(M \log M)$; its smoothing term is $\pi(d-1)\log M/(dM)$, as displayed.

For the radix lattice, one has exactly

$$\sigma(\ker \phi_q) = 2q.$$

If $\max\{p(a), n(a)\} < q$, the positive and negative weighted base-q sums are separately smaller than q^{d-1}. Their congruence therefore makes them equal as integers, and reduction modulo q followed by induction forces $a = 0$. Conversely, $q(0, \ldots, 0, 1)$ lies in $\ker \phi_q$ and has D_d-norm $2q$. This proves the displayed equality. Taking $N = q - 1$ yields

$$0 \leq \lambda_{G_q}(1) - \lambda_{\Gamma_d}(1) \leq \frac{\pi(d-1)}{d} \frac{\log q}{q} + \frac{4e^{1/100}}{q \log q}.$$

For $d = 6$, if

$$H_q = \operatorname{per} C_{q^5}(\{0, 1, q, q^2, q^3, q^4\})^{1/q^5},$$

then

$$1 \leq \frac{H_q}{h_6} \leq \exp\left(\frac{5\pi}{3} \frac{\log q}{q} + \frac{8e^{1/100}}{q \log q}\right).$$

5 Explicit lower bounds in degree six

5.1 A symbolic strict improvement

The generic lattice description already implies strict improvement over the Schrijver base. In fact, any three distinct support elements s, t, u in a binary circulant give the simple 6-cycle

$$L_0 \to R_s \to L_{s-t} \to R_{s-t+u} \to L_{u-t} \to R_u \to L_0.$$

The three left vertices and three right vertices are pairwise distinct within their respective color classes because s, t, u are distinct.

For $0 \le p \le 1$, define

$$\mathbb{G}_d(p) = \frac{1}{2}\left[p \log \frac{d}{p} + (d-p)\log\left(1 - \frac{p}{d}\right) - 2(1-p)\log(1-p)\right],$$

with the endpoint values understood continuously. Csikvári's short-cycle gap theorem [8] says that, for a transitive d-regular bipartite graph containing an ℓ-cycle,

$$\lambda_G(1) - \mathbb{G}_d(1) \ge \int_0^1 \left(\frac{1}{4d}\min\{x, (1-x)^2\}\right)^{\ell} dx,$$

where

$$\mathbb{G}_d(1) = \frac{1}{2}\log\frac{(d-1)^{d-1}}{d^{d-2}}.$$

For $d = 6$ and $\ell = 6$, put

$$I_6 = \int_0^1 \left(\frac{1}{24}\min\{x, (1-x)^2\}\right)^6 dx.$$

Writing $\varphi = (1+\sqrt{5})/2$, one obtains

$$I_6 = \frac{1}{24^6}\left(\frac{\varphi^{-14}}{7} + \frac{\varphi^{-13}}{13}\right) = \frac{457}{2173796352} - \frac{545\sqrt{5}}{5796790272} > 0.$$

Thus, without computation,

$$\operatorname{per} C_n(S) \ge \left(\frac{3125}{1296}e^{2I_6}\right)^n.$$

Call S *Sidon modulo* n if the ordered differences $a - b$ for distinct $a, b \in S$ are pairwise distinct modulo n. If S is not Sidon, a repeated ordered difference gives a 4-cycle and the same argument replaces I_6 by

$$I_4 = \frac{727}{29859840} - \frac{65\sqrt{5}}{5971968} = 9.307059668\ldots \times 10^{-9}.$$

Every six-set is non-Sidon for $n \le 30$, since its 30 nonzero ordered differences cannot all be distinct in $\mathbb{Z}_n$.

5.2 Exact moments of the generic lattice

The stronger bound in Theorem 1.2 comes from the matching measure ρ_{Γ_6}. Its moment $\mu_k = \int x^k \, d\rho_{\Gamma_6}(x)$ is the number of length-k closed walks from the root of the self-avoiding-walk tree of Γ_6 [7]. Odd moments vanish. Exact enumeration gives:

$2j$	μ_{2j}	$2j$	μ_{2j}
0	1	18	15356334036
2	6	20	268021382436
4	66	22	4731256843176
6	876	24	84316269917196
8	12786	26	1514802320358216
10	197796	28	27404472908976936
12	3183036	30	498786397086170496
14	52710216	32	9126710952996738306
16	892040706		

For completeness, the recursion is as follows. In the symmetric model put $A = \mathbb{Z}^d/\mathbb{Z}(1,\dots,1)$ and join L_a to R_{a+e_i} for $0 \le i < d$. Coordinate sum modulo d is well-defined on A, and the differences $e_i - e_j$ generate its sum-zero kernel. Hence the symmetric graph has exactly d components. The **component** with left coordinate sum 0 and right coordinate sum 1 modulo d is Γ_d: each class in that component has a unique representative in $\mathbb{Z}^d$ of coordinate sum 0 or 1, respectively, and dropping the last coordinate gives exactly the edge displacements D_d. In one fixed color class, two such representatives coincide modulo the diagonal only if their coordinate tuples coincide literally, since a diagonal difference would change their common coordinate sum by a multiple of d. This is the collision test in the recursion.

Canonically relabel edge directions in a rooted self-avoiding path by order of first occurrence. If r labels have already appeared, a new label has multiplicity $d-r$. For a path state Q, let $w(Q,R)$ count the edge labels that lead to the same canonical child state R. The forward self-avoiding-walk subtree has formal Green function

$$H_Q(x) = \frac{1}{1 - x\sum_{R \text{ child of } Q} w(Q,R) H_R(x)}.$$

The coefficient of x^j at the empty path is μ_{2j}. Through $j = 16$ the recursion visited 294779635 canonical states; at $d = 3$ it reproduces the published honeycomb moments through order 48 [7].

5.3 The fixed-activity rational certificate

Let

$$P_L(t) = \frac{1}{2}\int \log(1 + tx^2)\, d\rho_L(x)$$

be pressure per vertex. Since $x^2 = y \in [0, 20]$ for $L = \Gamma_6$, put $z = y/10 - 1 \in [-1, 1]$. For rational $t > 0$, write

$$1 + ty = a + bz, \qquad a = 1 + 10t, \qquad b = 10t,$$
$$s = \sqrt{1 + 20t}, \qquad r = \frac{a - s}{b}, \qquad C = \frac{a + s}{2}.$$

Uniformly for $z \in [-1, 1]$,

$$\log(a+bz) = \log C + 2\sum_{k\geq 1} \frac{(-1)^{k+1} r^k}{k} T_k(z).$$

Truncation after N terms, where $N \geq 0$ is an integer, has uniform error at most $2r^{N+1}/((N+1)(1-r))$.

The integrals of $T_k(z)$ for $k \leq 16$ are exact rational combinations of the moments above. Square roots are enclosed by dyadic rationals and logarithms by the identity

$$\log x = 2\,\mathrm{artanh}\,\frac{x-1}{x+1}$$

after exact range reduction. Every series remainder is bounded by a rational geometric tail.

At $t = 29/50$ and $N = 16$, outward rational decimal enclosures give

$$0.609450453043169353759817 < P_{\Gamma_6}(t) < 0.609464645905759970546275.$$

For the 6-regular tree $\mathbb{T}_6$, the matching density is the smaller solution of

$$t(1-p)^2 = \frac{p}{6}\left(1 - \frac{p}{6}\right),$$

and its pressure is

$$P_{\mathbb{T}_6}(t) = \mathbb{G}_6(p) + \frac{p}{2}\log t.$$

The same rational interval arithmetic gives

$$0.609436394248973464942208 < P_{\mathbb{T}_6}(29/50) < 0.609436394248973464942209,$$

and certifies exactly that

$$\boxed{P_{\Gamma_6}(29/50) - P_{\mathbb{T}_6}(29/50) > \frac{7}{500000}.}$$

To convert pressure to perfect-matching entropy, let $g_L(p) = \lambda_L(p) - \mathbb{G}_6(p)$. Csikvári proved that g_G is nondecreasing for every finite vertex-transitive 6-regular bipartite graph G [8]. This passes to Γ_6: along the radix quotients $G_q \to \Gamma_6$, finite-activity continuity gives $g_{G_q}(p) \to g_{\Gamma_6}(p)$ for every $p < 1$, so the pointwise limit is nondecreasing on $[0,1)$. Since $\lambda_{\Gamma_6}(1)$ is defined as the limit as $p \uparrow 1$ and $\mathbb{G}_6$ is continuous there, this extends the monotonicity to $p = 1$.

The pressure comparison converts the certificate into a lower bound on $g_{\Gamma_6}(1)$. Put $p = p_{\Gamma_6}(t)$. The attained infimum in Section 2.1 gives $\lambda_{\Gamma_6}(p) = P_{\Gamma_6}(t) - (p/2)\log t$. Also $\lambda_{\mathbb{T}_6}(p) = \mathbb{G}_6(p)$ [9, Theorem 2.15], while the infimum definition gives

$$P_{\mathbb{T}_6}(t) \geq \mathbb{G}_6(p) + \frac{p}{2}\log t.$$

Subtracting these relations gives

$$g_{\Gamma_6}(p_{\Gamma_6}(t)) \geq P_{\Gamma_6}(t) - P_{\mathbb{T}_6}(t).$$

Therefore

$$\lambda_{\Gamma_6}(1) \geq \mathbb{G}_6(1) + \frac{7}{500000}.$$

Since $e^{2\mathbb{G}_6(1)} = 3125/1296$, Theorem 1.1 gives

$$h_6 \geq \frac{3125}{1296} e^{7/250000} = 2.41133294847608906899\ldots.$$

This proves the lower half of Theorem 1.2.

6 Convergent certified evaluation of the sharp base

The logarithm in $\lambda_{\Gamma_6}(1) = \int \log|x|\, d\rho_{\Gamma_6}(x)$ is singular at zero. The missing endpoint control is supplied by Csikvári's root estimate [8] and its radix-limit extension justified in Section 4:

$$\rho_{\Gamma_d}([-\varepsilon,\varepsilon]) \leq \frac{2\sqrt{d-1}}{d}\varepsilon.$$

For $d = 6$,

$$\rho_{\Gamma_6}([-\varepsilon,\varepsilon]) \leq \frac{\sqrt{5}}{3}\varepsilon < \frac{3}{4}\varepsilon.$$

Let

$$f_\varepsilon(x) = \log\max\{|x|,\varepsilon\}.$$

Integration by parts gives

$$0 \leq \int f_\varepsilon\, d\rho_{\Gamma_6} - \lambda_{\Gamma_6}(1) \leq \frac{3}{4}\varepsilon.$$

Suppose an even polynomial Q satisfies the exactly certified uniform bound

$$\|Q - f_\varepsilon\|_{\infty,[-2\sqrt{5},2\sqrt{5}]} \leq \delta.$$

Writing $I(Q) = \int Q\, d\rho_{\Gamma_6}$, which is exactly computable from finitely many moments, we obtain

$$\boxed{I(Q) - \delta - \frac{3}{4}\varepsilon \leq \lambda_{\Gamma_6}(1) \leq I(Q) + \delta.}$$

Here the approximation can be made explicit. On $[-5,5]$, which contains the root support, f_ε is $1/\varepsilon$-Lipschitz. Rescale this interval to $[0,1]$. Its degree-K Bernstein polynomial has uniform error at most $5/(\varepsilon\sqrt{K})$ by the binomial variance bound. Enclose the finitely many logarithmic node values by rational intervals, choose their precision and K so the total error is at most δ, and symmetrize the resulting rational polynomial. Taking rational $\varepsilon, \delta \to 0$ proves that exact moments produce a convergent sequence of rational two-sided bounds on $\lambda_{\Gamma_6}(1)$ and hence on h_6.

7 Exact finite circulants

7.1 Complete affine census for orders 23–31

Supports related by

$$S \longmapsto uS + c, \qquad u \in \mathbb{Z}_n^\times, \quad c \in \mathbb{Z}_n,$$

give permutation-equivalent matrices. We enumerated all 8148 affine classes of six-subsets for $23 \leq n \leq 31$. The following class is the unique minimizing affine class at each order.

Table 1: Unique minimizing affine classes of six-element supports, orders 23 through 31.

n	affine classes	minimizing support	exact permanent	nth-root rate
23	207	$\{0,1,2,4,7,15\}$	3843409486	2.610518715946044918
24	870	$\{0,1,3,5,13,18\}$	9368913864	2.603077221944179924
25	366	$\{0,1,2,4,12,20\}$	22785392966	2.596009401396219872
26	767	$\{0,1,2,6,10,13\}$	55339674228	2.589367634679046236
27	634	$\{0,1,2,6,9,16\}$	134510172390	2.583307565903801233
28	1252	$\{0,1,4,15,20,22\}$	326803223040	2.577653350057210309
29	598	$\{0,1,2,5,14,23\}$	810203756246	2.574193451167119615
30	2643	$\{0,1,2,5,14,24\}$	1934592438260	2.567751448390291055
31	811	$\{0,1,3,8,12,18\}$	4598378639550	2.561362932953538240

The nine displayed rates are strictly decreasing; this was checked exactly by cross-power comparisons. The order-31 support is a cyclic $(31,6,1)$ difference set: its 30 ordered nonzero differences exhaust $\mathbb{Z}_{31} \setminus \{0\}$. Its translates are the lines of the cyclic projective plane of order 5, and the associated bipartite graph is its incidence graph.

7.2 The order-35 upper certificate

There are three Sidon affine classes at order 35. Their exact permanents are:

canonical support	exact permanent	35th-root rate
$\{0,1,3,7,16,24\}$	163812873663198	2.547558874426894768
$\{0,1,3,7,12,22\}$	164058070108318	2.547667744065163230
$\{0,1,3,7,12,20\}$	164070859106478	2.547673418168322034

This is a complete Sidon-class scan, not a complete scan of all 1998 affine classes at order 35. For the upper bound on h_6, only the first exact evaluation is needed: $h_6 \leq 163812873663198^{1/35}$.

Together with Section 5.3, this completes Theorem 1.2.

The finite computations used two separately implemented exact permanent engines. The primary engine applies Glynn's signed formula [11] with Gray-code updates of the six affected factors; the verifier uses Ryser's all-subsets formula [12]. Both use integer arithmetic, and their absolute-sum bounds fit in signed 128-bit accumulators throughout the certified range. Fresh affine enumeration, support-set comparison, exact cross-powers, and direct cycle checks on reference cases were included in the checks of Section 9. The independent review of v4 recomputed all 8148 census permanents with a separately written Ryser engine on independently enumerated affine classes; every value agrees with the primary Glynn census, and each order has the unique minimizing affine class shown above. It also recomputed all three order-35 Sidon permanents.

8 What the result settles

The unrestricted degree-six exponential bases were already known. Problem 10's corrected full chain is impossible in both the unrestricted and circulant scopes because its upper target is too small. Its sole surviving component was to improve the lower base for circulants. Theorem 1.1 goes further: it identifies the best possible circulant base, proves that every finite circulant has root rate at least it, and supplies an explicit connected cyclic family approaching it. Theorem 1.2 gives an explicit strict numerical improvement, while Section 6 proves that the entropy description admits arbitrarily sharp exact rational evaluation in principle.

Several finer questions remain.

1. Obtain a high-precision numerical value, or a closed form, for h_6.
2. Determine whether every nontrivial finite quotient satisfies a strict inequality above h_6.
3. Characterize near-minimizing sequences. The natural expectation is that every bounded-length lattice vector must disappear, equivalently that the graphs must converge locally to Γ_6.
4. Sharpen the quantitative modulus using lattice-specific information or a quantitative defect in the 2-lift inequality.

These do not affect the sharp exponential constant itself.

9 Reproducibility statement

The structural proofs are independent of computation. The computer-assisted part consists of exact finite recursions and rational interval certificates. The self-contained file *supplement-v7.tar.gz*, distributed as ancillary material with this article, contains the source and data needed for the calculations. Its README gives exact run commands and a SHA-256 manifest.

The package includes the primary Python moment recursion and rational Chebyshev certifier, their stored order-32 output, a separately written C++ moment implementation and its fresh output, the Glynn and Ryser permanent engines, all 8148 raw affine-census records for orders 23 through 31, and all three order-35 Sidon records. It also includes the independent review's separately written moment, rational-certificate, affine-enumeration, and permanent programs, together with its complete census rerun records. A quick standard-library check reconstructs the rational pressure interval from stored moments, verifies $P_{\Gamma_6}(29/50) - P_{\mathbb{T}_6}(29/50) > 7/500000$, checks affine support coverage and minima, and compares all 8148 original permanent values with the independent rerun after affine canonicalization.

The original Python *verify_certificate.py* is a fresh rerun using the same moment and arithmetic modules as the primary driver; it is not a separate implementation. The C++ moment source is separate from the Python moment recursion. The separate v4 review independently reimplemented the rational arithmetic and reran the full census with its own Ryser engine; its raw values and comparison report are in the supplement. The order-35 upper-certificate permanent was also independently recomputed. All certificate decisions use exact integers or rational intervals, while displayed decimals are only for presentation.

Acknowledgments

The author acknowledges substantial assistance from OpenAI Codex GPT-5.6 Sol and Astra and Anthropic Claude Fable 5 and Fable 5.1 in developing and checking the arguments, exact computations, and manuscript. Responsibility for the final text rests with the author.

References

[1] H. Minc, "Permanents of $(0, 1)$-circulants," *Canadian Mathematical Bulletin* **7** (1964), 253–263. doi:10.4153/CMB-1964-023-3

[2] H. Minc, "On permanents of circulants," *Pacific Journal of Mathematics* **42** (1972), 477–484. doi:10.2140/pjm.1972.42.477

[3] A. Schrijver, "A short proof of Minc's conjecture," *Journal of Combinatorial Theory, Series A* **25** (1978), 80–83. doi:10.1016/0097-3165(78)90036-5

[4] A. Schrijver and W. G. Valiant, "On lower bounds for permanents," *Indagationes Mathematicae (Proceedings)* **83** (1980), 425–427. doi:10.1016/1385-7258(80)90043-8

[5] A. Schrijver, "Counting 1-factors in regular bipartite graphs," *Journal of Combinatorial Theory, Series B* **72** (1998), 122–135. doi:10.1006/jctb.1997.1798

[6] G.-S. Cheon and I. M. Wanless, "An update on Minc's survey of open problems involving permanents," *Linear Algebra and its Applications* **403** (2005), 314–342. doi:10.1016/j.laa.2005.02.030

[7] M. Abért, P. Csikvári and T. Hubai, "Matching measure, Benjamini–Schramm convergence and the monomer–dimer free energy," *Journal of Statistical Physics* **161** (2015), 16–34. doi:10.1007/s10955-015-1309-7 arXiv:1405.6740

[8] P. Csikvári, "Matchings in vertex-transitive bipartite graphs," *Israel Journal of Mathematics* **215** (2016), 99–134. doi:10.1007/s11856-016-1375-9

[9] P. Csikvári, "Lower matching conjecture, and a new proof of Schrijver's and Gurvits's theorems," *Journal of the European Mathematical Society* **19** (2017), 1811–1844. doi:10.4171/JEMS/706

[10] O. J. Heilmann and E. H. Lieb, "Theory of monomer-dimer systems," *Communications in Mathematical Physics* **25** (1972), 190–232.

[11] D. G. Glynn, "The permanent of a square matrix," *European Journal of Combinatorics* **31** (2010), 1887–1891.

[12] H. J. Ryser, *Combinatorial Mathematics*, Carus Mathematical Monographs 14, Mathematical Association of America, 1963.

[13] L. M. Brègman, "Some properties of nonnegative matrices and their permanents," *Soviet Mathematics Doklady* **14** (1973), 945–949.

[14] H. Minc, "Theory of permanents 1978–1981," *Linear and Multilinear Algebra* **12** (1983), 227–263. doi:10.1080/03081088308817488

[15] H. Minc, *Permanents*, Encyclopedia of Mathematics and its Applications, vol. 6, Addison-Wesley, Reading, Massachusetts, 1978.