Harmonic dyadic shifts and short sums of factorial divisors

Will Howe, Grant Huffman, Jensen Kohlmeyer, Liam Kruer

Unpublished draft - 1 November 2026

hexagon:2611.00748v1

Abstract

Let $h(N)$ be the maximum, over $1 \le R \le N$, of the least number of distinct positive divisors of a practical integer N whose sum is R. We prove

$$h(n!) = O((\log n)^9).$$

The main ingredient is a finite entropy lemma: a law modulo 2^k with entropy at least $gL \log 2$ in every L-bit lower prefix becomes supported on more than half the group after $O(g^{-2}(\log k)^2)$ independent copies, each multiplied by an independently chosen power of two. The shift distribution is harmonic. A divisor-digit construction supplies $g \asymp 1/\log k$ at linear factorial index. Positive quotient recursion, binary carrying, and a factorial radix then give the stated bound.

1. Statement, conventions, and source overlap

All unmarked logarithms are natural; $\log_2$ has base two. A sum of no terms is zero. Local modular representations may repeat divisors. The final representations use distinct positive divisors.

For a practical $N \ge 1$, define

$$h(N) = \max_{1 \le R \le N} \min\{|D| : D \text{ is a set of positive divisors of } N,\ \sum_{d \in D} d = R\}.$$

The original question often uses $R < N$. For $N \ge 2$ the two conventions agree: the smaller range already requires at least one term, while N itself is a one-term divisor sum. For $N = 1$, the inclusive convention gives $h(1) = 1$. We use the inclusive convention throughout.

Theorem 1. There are absolute constants $C_h > 0$ and n_0 such that

$$h(n!) \le C_h(\log n)^9 \qquad (n \ge n_0).$$

Consequently the strict-power version of Erdős 18(c) holds with exponent 10.

The divisor-block construction and the positive quotient/radix framework are adapted from Kohlmeyer-Kruer, Section 3 and Sections 5-6. Plasma AI's author-recorded L63 already gives an overlapping quantitative interface from short dyadic representatives to factorial divisor sums. We give the complete transfer argument for the parameters used here, and credit those earlier transfer mechanisms.

The separated-digit entropy obstruction L64 excludes a **fixed positive** entropy rate at this factorial scale. Our input rate tends to zero, and the harmonic **additive** shift lemma has polynomial cost in its reciprocal. The final law sums overlapping shifted inputs; it is not a single separated-digit family covered by that support bound. The source's displayed multiplicative block expansion is also not used. The related L66 records a vanishing-rate residue estimate for the full odd-divisor law and a conditional multiplicative mixing criterion. That multiplicative criterion is not assumed here. Novelty of the harmonic additive argument remains to be assessed externally.

The use of entropy in additive combinatorics has a substantial prior history; see Tao, Green-Manners-Tao, and the multiscale convolution theorems of Hochman. Weighted sums over cyclic groups also appear in Abbe-Li-Madiman. We do not claim these general ideas as new. The proposed contribution here is the specific harmonic-shift estimate in Lemma 2, uniform as the lower-prefix entropy rate tends to zero, and its application to factorial divisors. A separate novelty report records the scope of the source comparisons; no global priority certification is claimed.

2. Harmonic shifts from lower-prefix entropy

For a finite random variable Y, let $H(Y)$ denote Shannon entropy in natural units. Conditional probabilities on zero-probability events can be chosen arbitrarily.

Lemma 2 (harmonic dyadic shifts). Let $k, r \geq 1$, let $0 < g \leq 1$, and let X be a law on $\mathbb{Z}/2^k\mathbb{Z}$. Suppose

$$H(X \bmod 2^L) \geq gL \log 2 \qquad (1 \leq L \leq k). \tag{2.1}$$

Put

$$\mathcal{L}_k = \sum_{a=0}^{k-1} \frac{1}{a+1}.$$

Take mutually independent pairs (A_i, X_i), $1 \leq i \leq r$, such that A_i and X_i are independent within each pair, X_i has law X, and

$$\mathbb{P}(A_i = a) = \frac{1}{(a+1)\mathcal{L}_k}, \qquad 0 \leq a < k.$$

For

$$S = \sum_{i=1}^{r} 2^{A_i} X_i \pmod{2^k},$$

one has

$$H(S) \geq k \log 2 \left(1 - \exp\left[-\frac{r g^2 (\log 2)^2}{2\mathcal{L}_k}\right]\right). \tag{2.2}$$

In particular, if

$$r \geq \frac{2\mathcal{L}_k \log(2k)}{g^2 (\log 2)^2}, \tag{2.3}$$

then $B = \operatorname{supp} S$ satisfies $|B| > 2^{k-1}$, and $B + B = \mathbb{Z}/2^k\mathbb{Z}$.

Proof. Write residues using their canonical k binary digits, indexed from position zero. Given the lower t bits of X, let p_t be the conditional probability that bit t is one. Define

$$u_t = \mathbb{E}[2 \min(p_t, 1 - p_t)].$$

For binary entropy $\mathcal{H}(p) = -p \log p - (1-p)\log(1-p)$,

$$\mathcal{H}(p) \leq 2\sqrt{\min(p, 1-p)}.$$

Indeed, for $0 \leq p \leq 1/2$,

$$-p \log p \leq (2/e)\sqrt{p}, \qquad -(1-p)\log(1-p) \leq p \leq \sqrt{p},$$

and $1 + 2/e < 2$; use symmetry on the other half. Thus

$$\mathbb{E}\mathcal{H}(p_t) \leq \sqrt{2u_t}.$$

The entropy chain rule and Cauchy-Schwarz give

$$gL\log 2 \le \sum_{t<L} \mathbb{E}\mathcal{H}(p_t) \le \sqrt{2L\sum_{t<L} u_t}.$$

Consequently, with $c_g = g^2(\log 2)^2/2$,

$$\sum_{t<L} u_t \ge c_g L. \tag{2.4}$$

Fix $0 \le j < k$. Let $\mathbf{A} = (A_1, \dots, A_r)$, and condition on

$$\mathcal{G}_j = \sigma\Big(\mathbf{A},\ X_i \bmod 2^{\max(j-A_i,0)} :\ 1 \le i \le r\Big).$$

On any positive-probability atom, first fix $\mathbf{A} = \mathbf{a}$. The remaining conditioning specifies one lower-prefix event for each separate input. Independence of the input pairs therefore preserves independence of the current input bits on that atom.

Let ℓ_i be the least nonnegative residue of $2^{A_i}X_i$ modulo 2^j. These residues, and hence the carry

$$C_j = \left\lfloor \frac{\sum_i \ell_i}{2^j} \right\rfloor,$$

are $\mathcal{G}_j$-measurable. For $j = 0$ all ℓ_i and the carry are zero. A carry may exceed one; only its known parity is used.

If $A_i \le j$, the current bit of the i-th summand is bit $j - A_i$ of X_i. If $A_i > j$, it is zero. Thus, writing $\gamma_{i,j}$ for the conditional sign-bias of that bit given its own lower prefix, and setting $\gamma_{i,j} = 1$ when $A_i > j$,

$$\mathbb{E}[(-1)^{S_j} \mid \mathcal{G}_j] = (-1)^{C_j} \prod_i \gamma_{i,j}. \tag{2.5}$$

No independence of carries or output bits is asserted.

Unconditionally, each $\gamma_{i,j}$ is a function of its own independent pair. Therefore

$$\mathbb{E}\left|\mathbb{E}[(-1)^{S_j} \mid \mathcal{G}_j]\right| = (1-\beta_j)^r, \quad \beta_j = \frac{1}{\mathcal{L}_k}\sum_{a=0}^{j} \frac{u_{j-a}}{a+1}.$$

Equation (2.4) gives

$$\beta_j \ge \frac{\sum_{t=0}^{j} u_t}{(j+1)\mathcal{L}_k} \ge \frac{c_g}{\mathcal{L}_k}. \tag{2.6}$$

A binary law with absolute sign-bias z has entropy at least $(1-z)\log 2$, by concavity. The output's lower j bits and the full shift vector are measurable under $\mathcal{G}_j$, so

$$\begin{aligned} H(S_j \mid S \bmod 2^j, \mathbf{A}) &\ge H(S_j \mid \mathcal{G}_j) \\ &\ge \log 2\left[1 - (1-\beta_j)^r\right] \\ &\ge \log 2\left[1 - e^{-rc_g/\mathcal{L}_k}\right]. \end{aligned}$$

This entropy comparison does not assume independence after conditioning only on the output prefix. Summing over j, using the chain rule conditioned on the **same full vector A**, and then $H(S) \ge H(S \mid \mathbf{A})$, proves (2.2).

Under (2.3), $H(S) \ge (k - \frac{1}{2})\log 2$. Entropy is at most log support size, hence

$$|B| \ge 2^k/\sqrt{2} > 2^{k-1}.$$

For every residue x, the sets B and $x - B$ intersect; thus $B + B$ is the whole group. □

The proof first bounds $H(S \mid \mathbf{A})$. Randomness in the unobserved shifts is therefore not being used as a hidden entropy source.

3. Divisor digits at linear factorial index

Fix

$$C_0 = e^{100}, \qquad k_0 = \lceil e^{1000} \rceil.$$

For every integer $k \geq k_0$, put

$$m = \lceil C_0 k \rceil, \quad c = \frac{8}{\log m}, \quad g = \frac{c}{4} = \frac{2}{\log m}, \quad b_0 = \lfloor \log_2 m \rfloor.$$

These choices satisfy

$$c \leq \tfrac{1}{3}, \quad g \leq \tfrac{1}{2}, \quad 2 \leq b_0 < k, \quad b_0 \geq 4/c, \quad \frac{1}{\log k} \leq g \leq \frac{2}{\log k}. \tag{3.1}$$

For example, $\log m \leq \log k + 101 \leq 2 \log k$; $b_0 \geq \log m - 1 \geq \frac{1}{2} \log m = 4/c$; and $\log_2 m \leq \frac{3}{2}(\log k + 101) < k$ in this range.

For $1 \leq \ell \leq k$, define

$$D_\ell = \{0\} \cup \{d : d \mid m!,\ 1 \leq d < 2^\ell\}.$$

Lemma 3. Uniformly for $k \geq k_0$ and $1 \leq \ell \leq k$,

$$|D_\ell| \geq 2^{c\ell}. \tag{3.2}$$

Proof. We use the elementary bound

$$\pi(m) \geq \frac{m}{2 \log m} \qquad (m \geq 100). \tag{3.3}$$

To verify it, the central binomial coefficient is at least $2^m/(m+1)$. In its valuation at a prime p, each prime-power term is zero or one, so the prime's whole contribution is at most $p^{\lfloor \log_p m \rfloor} \leq m$. Hence

$$2^m/(m+1) \leq \binom{m}{\lfloor m/2 \rfloor} \leq m^{\pi(m)}.$$

Since $\log 2 > 2/3$ and $m/6 > \log(m+1)$ for $m \geq 100$, this proves (3.3).

Write $a = \log_2 m$. If $\ell \leq 2a + 2$, all integers through m divide $m!$, so

$$|D_\ell| \geq \min(m+1, 2^\ell) \geq 2^{\ell/3} \geq 2^{c\ell};$$

here $a \geq 2$ ensures $2a + 2 \leq 3a$.

Otherwise put $v = \lfloor (\ell - 1)/a \rfloor$. Then

$$\ell/(2a) \leq v \leq k/a.$$

Every product of v distinct primes at most m divides $m!$ and is at most $m^v \leq 2^{\ell-1}$. Distinct prime subsets give distinct integers. With $P = \pi(m)$, (3.3) yields

$$P/v \geq C_0/(2 \log 2), \qquad \log(P/v) > 40.$$

In particular $P \geq v$. Since $\binom{P}{v} \geq (P/v)^v$,

$$\log_2 |D_\ell| \geq v \log_2(P/v) \geq \frac{20\ell}{\log m} \geq c\ell.$$

□

Digit convention. Start at endpoint b_0. Define successive endpoints

$$b_{s+1} = \min(2b_s, k)$$

until $b_L = k$, and let $\ell_s = b_{s+1} - b_s$. Choose an initial digit d_0 uniformly among the odd integers in $[1, 2^{b_0})$. Independently choose d_{s+1} uniformly from D_{ℓ_s}, and set

$$U = d_0 + \sum_{s=0}^{L-1} 2^{b_s} d_{s+1}.$$

The number $J = L + 1$ **includes the initial digit**. A zero digit contributes no divisor term. Before the final block the endpoint doubles, so $J \le 2 + \log_2 k$, giving the count below. Because all digits are below their block radices, there are no carries between blocks and

$$1 \le U < 2^k, \qquad U \text{ is odd}, \qquad J + 1 \le 3 \log k. \tag{3.4}$$

Each initial digit divides $m!$. Every later nonzero term divides $2^k m!$, and

$$2^k m! \mid (m + 2k)!.$$

Thus U is a positive sum of at most J divisors of $M!$, where $M = m + 2k$.

For $2 \le j \le b_0$, $U \bmod 2^j$ is uniform among odd residues, giving maximum mass $2^{1-j} \le 2^{-gj}$. For $j > b_0$, let b be the last completed block endpoint at or below j. If j cuts a block, that block has length at most b, so $b \ge j/2$; at $j = k$, take $b = k$. Fixing a residue fixes every completed digit. Independence and (3.2) give

$$\begin{aligned} \max_a \mathbb{P}(U = a \bmod 2^j) &\le 2^{-(b_0-1)} \prod_{\text{completed appended blocks}} |D_\ell|^{-1} \\ &\le 2^{1-cb} \le 2^{1-cj/2} \le 2^{-cj/4} = 2^{-gj}. \end{aligned} \tag{3.5}$$

The last inequality uses $j > b_0 \ge 4/c$.

Take an independent uniform $E \in \{0, 1\}$, and let $V = U + E$ be the **actual positive integer**; let $X = V \bmod 2^k$ be its residue. Then

$$1 \le V \le 2^k,$$

and V is a sum of at most $J + 1$ divisors of $M!$. The possible integer value $V = 2^k$ supplies a positive witness for residue zero.

Parity of an output residue determines the unique compatible value of E, since U is odd. Equation (3.5), and uniform parity at $j = 1$, therefore imply

$$\max_a \mathbb{P}(X = a \bmod 2^j) \le 2^{-gj} \qquad (1 \le j \le k). \tag{3.6}$$

In particular $H(X \bmod 2^j) \ge gj \log 2$, as required in Lemma 2.

4. Short positive representatives of every dyadic residue

Apply Lemma 2 to this X, taking

$$r = \left\lceil 20(\log k)^4 \right\rceil.$$

This satisfies (2.3): $\mathcal{L}_k \le 2 \log k$, $\log(2k) \le 2 \log k$, $g^{-1} \le \log k$, and $\log 2 > 2/3$, so the right side of (2.3) is at most $18(\log k)^4$.

Each residue in the support B of the shifted sum has an actual positive witness formed from r shifted integers V_i. Expanding their divisor representations gives at most $r(J+1)$ terms. If $d \mid M!$ and $0 \le a < k$, then

$$2^a d \mid 2^k M! \mid (M+2k)!.$$

All terms therefore divide the **single common factorial**

$$F(k)! = (m+4k)!, \qquad F(k) \le A_0 k, \quad A_0 = C_0 + 5. \tag{4.1}$$

Its index does not multiply by the number of additive copies.

As $B + B$ covers the group, every residue modulo 2^k has a positive integer representative S which is a sum, with repetition allowed, of at most

$$2r(J+1) \le 200(\log k)^5 \tag{4.2}$$

divisors of $F(k)!$. Uniformly over the chosen residue,

$$S \le \lceil 200(\log k)^5 \rceil \, F(k)!. \tag{4.3}$$

There is also the smaller bound $S \le r2^{2k}$, but (4.3) suffices for the exponent proved below.

This is the local representative interface overlapping L63. With the coarse height (4.3), the factorial index is linear, the count exponent is five, and the binary logarithmic height has one logarithmic overhead. The next sections independently give the corresponding transfer.

5. Exact positive lifting and distinct divisors

Lemma 4 (binary repetition removal). A sum of $w \ge 1$ positive divisors of an integer N is a sum of at most w distinct positive divisors of

$$2^{\lfloor \log_2 w \rfloor} N$$

with the same value.

Proof. Write $N = 2^v N_{\mathrm{odd}}$. Group the terms according to their odd part $d \mid N_{\mathrm{odd}}$. In a group, the total is dA_d, where A_d is a sum of at most w powers 2^a, $0 \le a \le v$, hence $A_d \le w2^v$. Its binary expansion has largest exponent at most $v + \lfloor \log_2 w \rfloor$. Each surviving digit gives an allowed divisor. Binary carrying reduces term count. The terms within a group are distinct; terms in different groups have different odd parts. □

Lemma 5 (one exact integer). For every sufficiently large integer $R > 0$, put $T = \lceil \log_2(R+1) \rceil$. Then R is a sum of $O((\log T)^7)$ distinct divisors of $(4T)!$.

Proof. Fix an absolute $D \ge 16A_0/\log 2$. For a current positive integer R_i with bit length T_i, take

$$k_i = \left\lfloor \frac{T_i}{D \log(T_i + 2)} \right\rfloor.$$

Fix a threshold T_0 so that, for every $T_i \ge T_0$,

- $k_i \ge k_0$ and $k_i \ge T_i/[2D \log(T_i+2)] \ge 2$;
- $F(k_i) \le T_i$;
- the upper bound in (4.3) is at most $2^{T_i/2}$.

These are compatible eventual conditions. For the height condition, use

$$\log(F(k_i)!) \le A_0 k_i \log(A_0 k_i)$$

and, eventually, $\log(A_0 k_i) \le 2 \log T_i$. The factorial contribution is at most $2A_0 T_i/D$; the logarithm of the count in (4.3) is $O(\log \log T_i)$. Our fixed choice of D, followed by a fixed sufficiently large T_0, leaves ample margin below $(T_i/2) \log 2$. All constants and thresholds are independent of the target R.

Choose the positive representative $S_i \equiv R_i \pmod{2^{k_i}}$ from Section 4. Since $R_i \ge 2^{T_i - 1}$,

$$0 < S_i \le 2^{T_i/2} < R_i.$$

Thus

$$R_i = S_i + 2^{k_i} R_{i+1}, \qquad 0 < R_{i+1} < R_i / 2^{k_i}. \tag{5.1}$$

Its bit length satisfies $T_{i+1} \le T_i - k_i$. Continue while $T_i \ge T_0$, and represent the final bounded integer by a bounded number of copies of 1.

The potential $(\log T_i)^2$ drops by an absolute positive amount at each large stage. Indeed $k_i/T_i \gg 1/\log T_i$, and

$$(\log T_i)^2 - (\log T_{i+1})^2 \ge (k_i/T_i) \log T_i \gg 1.$$

There are $O((\log T)^2)$ stages. Each uses $O((\log T)^5)$ terms, so the total count before merging is

$$w = O((\log T)^7). \tag{5.2}$$

Every unscaled term divides the original $T!$, since $F(k_i) \le T_i \le T$; the terminal copies of 1 do also. Let $e_i = \sum_{s<i} k_s$ be a lifting exponent. Positivity in (5.1) implies

$$R \ge 2^{e_i} R_i \ge 2^{e_i},$$

so $e_i \le T$, including the terminal stage. Every lifted term therefore divides $2^T T!$.

Apply Lemma 4 with $b = \lfloor \log_2 w \rfloor = O(\log \log T)$. The distinct resulting divisors divide $2^{T+b} T!$. Increase the fixed starting threshold to $T_1 \ge T_0$ so that $b \le \lfloor T/2 \rfloor$. Among the $3T$ integers after T, at least $\lfloor 3T/2 \rfloor$ are even. Hence

$$2^{T+b} T! \mid (4T)!.$$

The sum and the count (5.2) are preserved. □

This proof includes all finitely many stopping cases by a fixed terminal constant. It never invokes the local cover at a zero k_i or below k_0.

6. Factorial radix and the global bound

First, factorials are practical with the inclusive convention. Let $\mathsf{H}(n) = h(n!)$. For $n = 1$, $\mathsf{H}(1) = 1$. Given $0 \le R \le n!$, write

$$R = na + r, \qquad 0 \le r < n, \qquad 0 \le a \le (n-1)!.$$

Use the empty representation if $a = 0$; otherwise scale an inclusive divisor representation of a by n. Every scaled divisor divides $n!$ and is at least n. If $r > 0$, the integer r itself divides $n!$ and is smaller than all scaled terms. Thus distinctness is preserved, and, for example, $\mathsf{H}(n) \le n$ is a valid finite base bound.

Fix

$$c_0 = \frac{\log 2}{16}, \qquad \ell = \left\lfloor \frac{c_0 n}{\log n} \right\rfloor, \qquad m' = n - \ell, \qquad Q = \frac{n!}{m'!}.$$

Choose a fixed n_* so that $\ell \geq c_0 n/(2\log n) \geq 1$, $m' \geq 1$, and all following eventual bounds hold for $n \geq n_*$.

For any $0 \leq R \leq n!$, write

$$R = aQ + r, \qquad 0 \leq r < Q, \qquad 0 \leq a \leq m'!.$$

A sufficiently large positive remainder has bit length

$$T(r) = \lceil \log_2(r+1) \rceil \leq \log_2 Q + 1 \leq \frac{\ell \log n}{\log 2} + 1 \leq n/16 + 1.$$

Thus $4T(r) < n$ eventually. Lemma 5 represents r by $O((\log n)^7)$ distinct divisors of $(4T(r))!$, hence of $n!$. The finitely many remainders outside Lemma 5's range are themselves divisors once n exceeds that fixed finite set; $r = 0$ uses the empty sum. This is uniform over all $r < Q$.

Scale a distinct inclusive representation of a by Q. Each high term is a divisor of $n!$ and is at least Q. Every positive low term is smaller than Q, because its whole positive sum is $r < Q$. The families do not overlap. Therefore

$$\mathsf{H}(n) \leq \mathsf{H}(n-\ell) + O((\log n)^7). \tag{6.1}$$

The endpoint $R = n!$ is included: it has $a = m'!$, $r = 0$, and also has its direct one-term representation.

For $n \geq n_*$,

$$(\log n)^2 - (\log(n-\ell))^2 \geq (\ell/n)\log n \geq c_0/2.$$

There are $O((\log n)^2)$ radix steps down to the fixed base. Summing the uniform cost in (6.1) proves

$$h(n!) = O((\log n)^9),$$

as claimed in Theorem 1. □

7. Strict-power target and the other two questions

The pinned Formal Conjectures statement uses the inclusive endpoint $1 \leq R \leq N$ and asks for a positive real C with

$$\mathrm{practicalH}(n!) < (\log n)^C$$

for all sufficiently large natural n. A set of divisors whose sum is R witnesses its subset-sum condition directly; its infimum/minimum convention therefore has the upper bound proved here. Factorials are practical by Section 6, so no empty representation family is involved.

Choose $C_h \geq 1$ and $n_0 \geq 3$ as in Theorem 1. For

$$n \geq \max\{n_0, \lceil e^{C_h+1} \rceil\},$$

one has $\log n > C_h$, and consequently

$$\mathrm{practicalH}(n!) \leq C_h(\log n)^9 < (\log n)^{10}.$$

Thus $C = 10 > 0$ gives the formal strict-power quantifiers, including the endpoint $n!$. Reading the statement for this comparison is not a formalization or a Lean verification.

Corollary 6 (the three questions together). Theorem 1 implies affirmative answers to all three questions of Erdős Problem 18: (c) with strict exponent 10, (b) for every positive exponent, and (a) with strict exponent 10 along the factorials.

Proof. The implication for (c) was proved above. For (b), fix $\varepsilon > 0$ and write $x = \log n$. The exponential series gives

$$n^{\varepsilon} = e^{\varepsilon x} \geq \frac{(\varepsilon x)^{10}}{10!} > C_h x^9$$

once $x > 10! C_h \varepsilon^{-10}$.

For (a), the elementary factorial estimate $(n+1)! \geq 2^n$ gives

$$\log\log((n+1)!) \geq \log n + \log\log 2.$$

Consequently $\log(n+1) \leq 4 \log\log((n+1)!)$ for all sufficiently large n. Set $y = \log\log((n+1)!)$. Theorem 1 yields

$$h((n+1)!) \leq C_h 4^9 y^9 < y^{10}$$

once $y > C_h 4^9$. Factorials are practical and form an unbounded sequence, so this supplies infinitely many witnesses for (a). □

Part (b) was proved earlier by Kohlmeyer and Kruer KK; see also the accepted part-(b) source record. The implication above does not claim a new discovery of (b). For (a), the earlier work of GPT-5.6 Sol Pro, prompted and posted by Liam Price, and the explicit account of Wouter van Doorn and GPT-6 Astra Pro VD give the stronger square-log-log bound on a suitable sequence of practical numbers. Our factorial corollary does not improve that general-sequence bound. The proposed new result is the bound at every large factorial in (c); it is not obtained by logically combining the statements of (a) and (b). The earlier greedy factorial bound of Hughes Hughes also does not supply a fixed polylogarithm.

8. Acknowledgments and AI assistance

The author list is Will Howe, Grant Huffman, Jensen Kohlmeyer, and Liam Kruer. No institutional affiliations are asserted. This manuscript was developed with Codex assistance. AI systems proposed mathematical arguments and performed informal checks, including separate checks of the entropy and arithmetic parts. AI review is not represented as external peer review or formal verification. The accompanying Lean development independently proves the quantitative bound and the three original statements. Its compiler receipts and axiom audits are provided with this draft; this is local verification, not sponsor acceptance.

We credit the divisor-digit construction and the positive lifting and factorial radix methods to Kohlmeyer and Kruer KK. The overlapping quantitative transfer criterion is recorded by Plasma AI L63. Its separated-digit obstruction L64 and multiplicative criterion L66 delimit, rather than supply, the new mixing step. The arguments required here are proved in the text.

9. Formal verification

The accompanying Lean 4.34.0 project proves the unconditional theorem Erdos18c.ninthPowerB ound and the exact original statements Erdos18.erdos_18a, Erdos18.erdos_18b, and Erdos18.erdo s_18c. It uses mathlib commit 5ed2965256430c3649e86755f9576b54eca72435. The printed axiom dependencies are `propext`, `Classical.choice`, and `Quot.sound`; no unproved problem-specific assumptions are introduced.

The formal proof realizes the harmonic mixing estimate using convolution and order-two translation differences. It then constructs the divisor digits and positive modular representatives. For the integer lifting and factorial recurrence it uses logarithmic potentials, with different absolute

constants from the exposition. It obtains the same ninth-power conclusion. The code adapts credited infrastructure from Kohlmeyer and Kruer's 18(b) source, whose SHA-256 is 4d6ee896174152 88e9f127beb3c0e0211c011f891889fcb43d0e16373bd14088.

The final statement file reproduces only the definitions and target types from the pinned Formal Conjectures source, and proves their equivalence to the internal definitions. It does not import the unproved conjectures. Build instructions, the source correspondence, and limitations of the local verification are recorded in the accompanying verification report.

References

1. J. Kohlmeyer and L. Kruer, *Short sums of factorial divisors and Erdős Problem 18(b)*, manuscript dated 16 September 2026. Author-hosted PDF. The cited version has SHA-256 f89f4f46b9535c5c990a29bf0ddf1eb305123429a3b89dfb508e95c8cc9b2d6a.
2. Plasma AI, *Polylogarithmic dyadic representatives imply short factorial sums*, L63, updated 14 October 2026. Statement; proof. Author-recorded conditional result; accessed 1 November 2026.
3. Plasma AI, *Subexponential support of short factorial divisor blocks*, L64, updated 14 October 2026. Statement; proof. Accessed 1 November 2026.
4. Plasma AI, *Full-divisor residue spread and a quantitative mixing criterion*, L66, updated 14 October 2026. Statement; proof. Accessed 1 November 2026.
5. T. F. Bloom, *Erdős Problem 18*, problem record and proof-claim record, accessed 1 November 2026. These are problem/status sources, not proof inputs.
6. P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de L'Enseignement Mathématique 28, Université de Genève, 1980. Historical problem reference; no theorem from this book is used without proof here.
7. The Formal Conjectures Authors, *Erdős Problem 18*, Lean statements, commit a64e959c32c2 70df4dd0d96d2027481f15750534, Apache-2.0.
8. T. Tao, *Sumset and inverse sumset theory for Shannon entropy*, Combinatorics, Probability and Computing 19 (2010), 603-639, DOI 10.1017/S0963548309990642. arXiv:0906.4387. Background, not a quantitative input to Lemma 2.
9. B. Green, F. Manners and T. Tao, *Sumsets and entropy revisited*, Random Structures & Algorithms 66 (2025), e21252, DOI 10.1002/rsa.21252. arXiv:2306.13403. Background on entropic doubling and homomorphisms.
10. E. Abbe, J. Li and M. Madiman, *Entropies of weighted sums in cyclic groups and an application to polar codes*, Entropy 19 (2017), 235, DOI 10.3390/e19090235. arXiv:1512.00135. Related weighted-sum and source-polarization context.
11. M. Hochman, *On self-similar sets with overlaps and inverse theorems for entropy*, Annals of Mathematics 180 (2014), 773-822, DOI 10.4007/annals.2014.180.2.7. Published paper, especially Theorems 2.7-2.9. Background, not an input to Lemma 2.
12. W. van Doorn and GPT-6 Astra Pro, *Practical numbers and Egyptian fractions*, source manuscript, commit 56b455ae6949b76f41292d35829034ebb8663241, September 2026. The source credits *Sparse Divisor Sums* by GPT-5.6 Sol Pro, prompted and posted by Liam Price. No new priority for (a) is claimed here.
13. S. D. Hughes, *Sums of distinct divisors of factorials*, arXiv:2609.10902v1, 9 September 2026.
14. Conjectures.io, *Erdős 18(b)*, accepted result record, accessed 1 November 2026. Records acceptance for (b); no local replay is implied by citing the record.