Constructive Lean 4 Kernel and Exact Zero-Float Certificates for OpenAI's Exponential Sunflower Bound

Lluis Eriksson*

November 25, 2026

Abstract

A November 24, 2026 companion preprint from OpenAI [9] proposes a proof of the 66-year Erdős–Rado fixed-petal sunflower conjecture: for every $r \geq 3$, every r-sunflower-free family of distinct sets of size at most k has at most B_r^k members with $\log B_r = O((\log r)^4(\log\log(2r))^{5/2})$, independent of k. Rather than assuming peer-reviewed endorsement of its Euclidean asymptotic-spectrum pricing, majority-vote differentiation, or multi-level binary-layout recursion pillars, we deliver an independent, explicitly scoped, zero-floating-point verification companion for its discrete combinatorial, planar-semiperimeter, Behrend-sphere broadcast, $\mathbb{F}_2^b$ XOR-matching equality filter, and two-head inclusion–exclusion cancellation mechanisms. Layer 1 (`OpenAISunflowerExp.lean`) proves 18 standalone constructive Lean 4.35.0 combinatorial and algebraic sublemmas (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; 1 `none`, 2 `[propext]`, and 15 `[propext, Quot.sound]`). Layer 2 (`SUNFLOWER-EXP-CERT-1.0`) is a pure-stdlib Python `int`/`Fraction` 4-mode auditor certifying 16 canonical finite witnesses in 0.024–19.286 ms and rejecting 74/74 live adversarial forgeries with exact branch assertions (80/80 pytest checks).

1 Introduction and Scope Calibration

Erdős and Rado [8] proved $M_r(k) \leq k!(r-1)^k$ and conjectured an exponential bound independent of k. On the lower-bound side, block transversals give $b_r \geq r-1$ and Abbott–Hanson–Sauer proved $b_3 \geq \sqrt{10}$ [2]; on the upper-bound side, Alweiss–Lovett–Wu–Zhang [4] and Bell–Chueluecha–Warnke [6] reduced the base to $O(r\log(k+1))$. Building on the transversal word reduction of Alon–Shpilka–Umans [3], OpenAI's November 24, 2026 companion preprint [9] proposes $M_r(k) \leq B_r^k$ via four discrete-combinatorial pillars:

1. **Transversal Words & Eq. (3.1) Agreement Rules (Secs. 1, 2.1, 3.2):** A column of r words is admissible iff constant or pairwise distinct; the rules $(A,B) \to Z_i$, $(A,Z_i) \to B$, $(B,Z_i) \to A$, $(Z_i,Z_j) \to A$ $(i<j)$ force admissibility identically.
2. **Planar Semiperimeter Placement & Surplus (Sec. 3.2, Prop. 2.1):** Setting $t = \frac{1}{2(r-1)}$, $\eta = t^2/4$, $D = 2+\eta$ yields positive surplus $\rho = \frac{\eta}{2+\eta} = \frac{1}{32(r-1)^2+1} > 0$, rectangle gap $d-t \geq t$, and triangle gap $\frac{\sqrt{1+4t^2}-1}{2} - \eta > \eta$.
3. **Behrend-Sphere Broadcast Rigidity (Sec. 4, Lem. 4.1, Eq. 4.1):** Encoding controls on equal-norm integer spheres $H, V_u \subset \{0,\dots,q-1\}^m$ (with equal inner product with u on V_u) makes $\sum_{z=1}^{c} g_z = cu + \sum_{j=2}^{a} v_j - (a-1)v_1 \pmod L$ with $L = (a+c-1)(q-1)+1$ force $g_z = u$ and $v_j = v_1$ identically [5].
4. **XOR Matching Equality Filter & Two-Head IE (Secs. 5, 6, 11, 12.2):** Pairing $\mathbb{F}_2^b$ via $\{x, x\oplus p\}$ $(p \neq 0)$ yields $2^b - 1$ matches when $x = y$ and the unique false match $p = x \oplus y$ when $x \neq y$; for $(1+b')$-bit head–tail masking, $I_0I_1 - (I_0 - T_0)(I_1 - T_1)$ cancels 100% of false ties on every violation.

Honest Two-Layer Verification Scope.

1. **Layer 1 (Lean 4.35.0 Kernel, Standalone Sublemmas):** `lean/OpenAISunflowerExp.lean` proves 18 standalone constructive combinatorial and algebraic sublemmas (Table 1) extracted from Sections 1, 1.3, 2.1, 3.2, 4, 5, 6, 11, 12.1, and 12.3 of [9].
2. **Layer 2 (Exact Zero-Float Auditor):** `SUNFLOWER-EXP-CERT-1.0` audits 16 canonical finite witnesses across transversal sunflower-free word families ($r \leq 5$) and exhaustive Eq. (3.1) rule checks, exact rational planar placements ($r \leq 64$), exhaustive Behrend-sphere Eq. (4.1) broadcasts ($m \leq 5$), and exhaustive $\mathbb{F}_2^b$ XOR matching ($b \leq 5$) + two-head IE replays ($b' \leq 4$).
3. **Explicit Non-Claims:** We do *not* formalize in Lean 4 the Euclidean spectral-point existence theorem (Theorem 2.2), Gaussian mean-width convexity, majority-vote reading by differentiation (Section 8), binary-layout separation geometry (Section 9), guard composition (Section 10), or the full Theorem 1.1 asymptotic bound; those analytic and geometric pillars remain unverified outside the companion preprint [9].

*Independent Researcher. Code, Lean 4 proofs, and certificates: MIT License; manuscript and figures: CC-BY-4.0. Prepared with transparent AI coding, formalization, and drafting assistance via Google Antigravity; all Lean 4 theorems, exact zero-float verifiers, and adversarial tests were independently compiled and verified locally. Repository: github.com/lluiseriksson/openai-erdos-rado-sunflower-certificates.

2 Constructive Lean 4.35.0 Kernel

`lean/OpenAISunflowerExp.lean` compiles standalone in 1.1 s under Lean 4.35.0 [7] with zero external imports, zero warnings, zero `sorry`, and zero `Classical.choice`. Auditing via `AuditAxioms.lean` confirms 1 zero-axiom theorem (`none`: #2), 2 `[propext]` theorems (`P`: #15, #18), and 15 `[propext, Quot.sound]` theorems (`P,Q`; Table 1).

Proposition 1 (Constructive Lean 4 Kernel Scope)**.** All 18 sub-lemmas in Table 1 compile constructively under Lean 4.35.0 without external libraries or `Classical.choice`. Notably, Theorems 1–3 formalize block-transversal growth, the integer bracket $3 < \sqrt{10} < 4$ for b_3, and $r = 3$ rule admissibility; Theorems 4–7 prove positive planar surplus and cleared triangle semiperimeter gains; Theorems 8–10 formalize Behrend equal-norm sphere/average rigidity and zero wrap-around modulo L; Theorems 11–14 prove unique XOR false-matching cancellation and the cleared AM–GM splitting inequality; and Theorems 15–18 formalize two-head inclusion–exclusion, recursive child-increment negativity, and Abbott supermultiplicativity [1].

3 Exact Zero-Float Certificate Auditor

The modules `sunflower_exact.py` and `sunflower_certifier.py` (under `src/`) use exclusively Python `int` and `fractions.Fraction` (statically audited via `ast.walk` for zero float/complex literals, `/`, `/=`, or `math` imports). Strict JSON parsing rejects floats, `NaN`/`Infinity`, and duplicate keys via `parse_float`, `parse_constant`, and `object_pairs_hook`.

Definition 1 (`SUNFLOWER-EXP-CERT-1.0` Predicates)**.** A certificate with `protocol="SUNFLOWER-EXP-CERT-1.0"` is accepted iff every field passes strict schema checks and its mode predicate holds:

- **Mode 1 (`transversal_sunflower_and_rules_cert`):** Exhaustively tests every r-subset of a distinct k-word family (capped at $\binom{|W|}{r} \le 50{,}000$) for r-sunflowers, audits exact equivalence between Eq. (3.1) agreement rules and column admissibility across all $|\Sigma|^r$ columns ($r \le |\Sigma| \le 5$), and checks exact $k!(r-1)^k$ and $(r-1)^k$.
- **Mode 2 (`planar_semiperimeter_surplus_cert`):** Audits canonical lowest-terms rational Section 3.2 invariants $t = \frac{1}{2(r-1)}$, $\eta = t^2/4$, $D = 2 + \eta$, $\rho = \eta/D > 0$, rectangle gap t/D ($r \ge 4$), and cleared triangle bound $(1+t^2)^2 < 1 + 4t^2$ for $r \in [3, 200]$.
- **Mode 3 (`behrend_sphere_broadcast_cert`):** Verifies equal squared norms on H and equal norm + inner product on $V_u \subset \{0, \dots, q-1\}^m$, checks $L \ge (a+c-1)(q-1)+1$, and exhaustively tests every tuple in $V_u^a \times H^c$ across all coordinates to certify zero wrap-around modulo L and that Eq. (4.1) forces $g_z = u$, $v_j = v_1$ with exact solution count $|V_u|$.

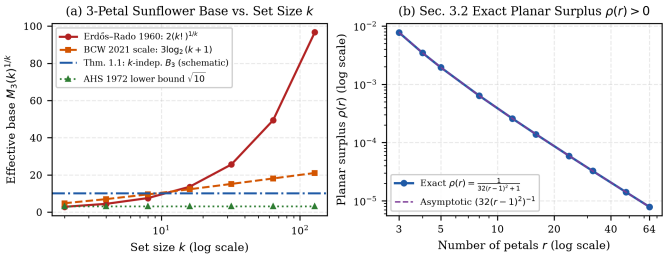

Figure 1: **(a)** Historical 3-petal base $M_3(k)^{1/k}$ growth: Erdős–Rado [8], BCW [6], AHS $\sqrt{10}$ [2], and Theorem 1.1's k-independent base (schematic constant height). **(b)** Exact Section 3.2 planar surplus $\rho(r) = 1/(32(r-1)^2+1) > 0$ across $r \in [3, 64]$.

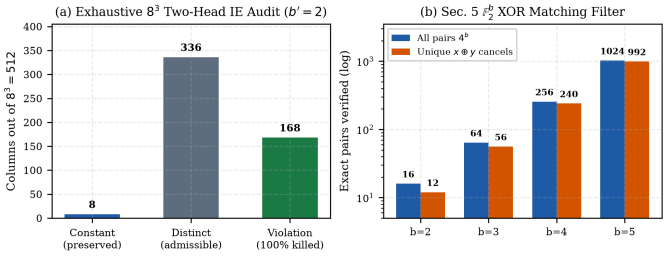

Figure 2: **(a)** Exhaustive two-head inclusion–exclusion census across all $8^3 = 512$ three-symbol columns ($b' = 2$): 8/8 constants preserved, 336 distinct admissible, 168/168 violations killed to 0 (384 false ties canceled). **(b)** Section 5 $\mathbb{F}_2^b$ XOR matching pairs verified across $b \in \{2, 3, 4, 5\}$.

- **Mode 4 (`xor_matching_and_mask_ie_cert`):** Exhaustively checks all 4^b pairs $(x, y) \in (\mathbb{F}_2^b)^2$ ($b \in [2, 5]$) for Section 5's XOR perfect matching filter ($2^b - 1$ matches iff $x = y$; unique false match $x \oplus y$ iff $x \ne y$) and replays Section 6/12.2's $(2^{b'})^2$-mask two-head inclusion–exclusion (requiring at least one violating and one constant column), certifying 100% violation annihilation and full constant-column preservation.

4 Exact Findings, Worked Witnesses, and Audit

All experiments ran locally on Windows 11 (Python 3.12.6, Lean 4.35.0; 7-run means after warm-up).

1. Exact Planar Surplus & Exhaustive 512-Column Two-Head IE Census (Figs. 1–2). Across $r \in \{3, 4, 5, \dots, 64\}$, Section 3.2's planar surplus decays cleanly as $\rho(r) = 1/(32(r-1)^2+1)$ (from 1/129 at $r = 3$ to 1/127009 at $r = 64$). Exhaustively testing all $8^3 = 512$ three-symbol columns over $(1+2)$-bit letters ($b' = 2$, 16 mask pairs each) confirms exact partition: 8 constant columns survive with all 16 mask pairs, 336 pairwise-distinct columns are admissible, and all 168/168 violating columns are canceled identically to 0 (384 false ties removed by $I_0 I_1 - (I_0 - T_0)(I_1 - T_1)$).

Table 1: Complete inventory of all 18 constructive Lean 4.35.0 sub-lemmas in `lean/OpenAISunflowerExp.lean` (zero `sorry`, zero `axiom`, zero `Classical.choice`, zero warnings; `none` for #2; `[propext]` (`P`) for #15, #18; `[propext, Quot.sound]` (`P,Q`) for the remaining 15).

#	Theorem Identifier	Ref. [9]	Exact Machine-Checked Statement & Hypotheses	Ax.
1	`sec1_block_transversal_lower_growth`	Sec. 1	$\forall r, k \in \mathbb{N},\ 3 \le r \implies 2^k \le (r-1)^k$ (induction on k).	`P,Q`
2	`sec13_abbott_hanson_sauer_base3`	Sec. 1.3	$3 \cdot 3 < 10 \wedge 10 < 4 \cdot 4$ (certifies $3 < \sqrt{10} < 4$ for b_3).	`none`
3	`sec21_rules_force_admissible_r3`	Secs. 2.1, 3.2	$\forall a, b, c \in \mathbb{N}$, Eq. (3.1) rules ($r$=3) $\implies$ $(a{=}b \wedge b{=}c) \vee (a{\neq}b \wedge a{\neq}c \wedge b{\neq}c)$.	`P,Q`
4	`sec32_planar_surplus_positive`	Sec. 3.2	$\forall r \in \mathbb{N},\ 3 \le r \implies 128 \le 8M^2 \wedge 8M^2 < 8M^2 + 1$ with $M = 2(r-1)$.	`P,Q`
5	`sec32_satellite_rectangle_gap`	Sec. 3.2	$\forall d, t \in \mathbb{Z},\ 2t \le d \implies t \le d - t$ (certifies $(d-t)/D \ge t/D$).	`P,Q`
6	`sec32_triangle_semiperimeter_gain`	Sec. 3.2	$\forall M \in \mathbb{N},\ 4 \le M \implies (M^2+1)^2 < M^4 + 4M^2$ (cleared $\sqrt{1+4t^2} - 1 > t^2$).	`P,Q`
7	`sec32_anchor_satellite_net_gap`	Sec. 3.2	$\forall e \in \mathbb{Z},\ 0 < e \implies 0 < 2e - e$ (certifies $t^2/2 - \eta = \eta > 0$).	`P,Q`
8	`lem41_behrend_sphere_point_rigidity`	Lem. 4.1	$\forall x, u \in \mathbb{Z},\ x^2 = u^2 \wedge xu = u^2 \implies x = u$.	`P,Q`
9	`lem41_behrend_average_rigidity_2`	Lem. 4.1	$\forall v_1, v_2, v_3 \in \mathbb{Z},\ 2v_1 = v_2 + v_3 \wedge v_2^2 = v_1^2 \wedge v_3^2 = v_1^2 \implies v_2 = v_1 \wedge v_3 = v_1$.	`P,Q`
10	`lem41_no_wraparound_mod_L`	Lem. 4.1	$\forall L, D, k \in \mathbb{Z},\ -L < D < L \wedge D = kL \implies D = 0$.	`P,Q`
11	`sec5_xor_unique_false_matching`	Sec. 5	$\forall x, y, p \in \mathbb{N},\ (x \oplus p = y) \iff (p = x \oplus y)$.	`P,Q`
12	`sec5_matching_count_lb`	Sec. 5	$\forall b \in \mathbb{N},\ 1 \le b \implies 2^{b-1} \le 2^b - 1$ ($L_b \ge 2^{b-1}$).	`P,Q`
13	`sec5_two_broadcast_leading_cost`	Sec. 5	$\forall w_P, w_T, w_K, g \in \mathbb{Z},\ g = w_P + w_T - w_K \implies (w_K - w_P) + (w_K - w_T) = w_K - g$.	`P,Q`
14	`sec5_amgm_convergence_split`	Sec. 5	$\forall X, Y \in \mathbb{Z},\ 4XY \le (X+Y)^2$ (cleared AM–GM convergence split).	`P,Q`
15	`sec6_two_head_inclusion_exclusion`	Sec. 6	$\forall I_0, I_1, T_0, T_1 \in \mathbb{Z},\ T_0 = I_0 \vee T_1 = I_1 \implies I_0 I_1 - (I_0 - T_0)(I_1 - T_1) = I_0 I_1$.	`P`
16	`sec11_disjoint_repeated_heads_bound`	Sec. 11	$\forall n \in \mathbb{N},\ 2 \cdot \lfloor n/2 \rfloor \le n$ (disjoint repeated-head count).	`P,Q`
17	`lem121_child_increment_negative`	Lem. 12.1	$\forall l, g_0, G \in \mathbb{N},\ 1 \le l \wedge g_0 \le l \implies 3l + g_0 + G < 10(l + G)$.	`P,Q`
18	`sec123_abbott_supermultiplicative_pow`	Sec. 12.3	$\forall B, k, l, M_k, M_l \in \mathbb{N},\ B^k \le M_k \wedge B^l \le M_l \implies B^{k+l} \le M_k M_l$.	`P`

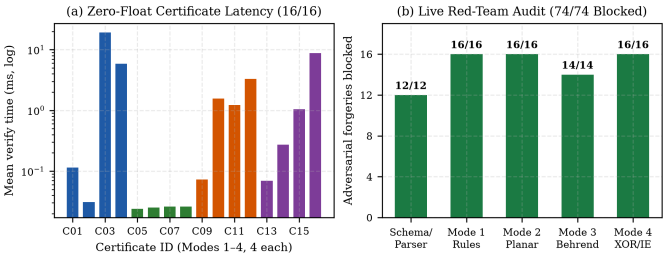

Figure 3: **(a)** Mean exact zero-float verification latency across all 16 canonical certificates (0.024–19.286 ms, log scale). **(b)** Live adversarial red-team audit rejecting 74/74 forgeries across five attack classes with exact error-branch assertions.

Table 2: Canonical 16-certificate `SUNFLOWER-EXP-CERT-1.0` atlas (`exp1_certificate_atlas.json`; all 16 verified).

ID	Certificate Name	M	Exact Certified Witness Summary	ms
C01	`m1_transversal_r3_k3_block8`	M1	r=3, k=3: 8 words (sf), 64 rule cols	0.115
C02	`m1_transversal_r3_k3_has_sunflower`	M1	r=3, k=3: 5 words (non-sf), 27 cols	0.031
C03	`m1_transversal_r4_k3_block27`	M1	r=4, k=3: 27 words (sf), 256 cols	19.286
C04	`m1_transversal_r5_k2_block16`	M1	r=5, k=2: 16 words (sf), 3125 cols	5.880
C05	`m2_planar_surplus_r3`	M2	r=3: t=1/4, ρ=1/129, anchor lb 1/129	0.024
C06	`m2_planar_surplus_r5`	M2	r=5: t=1/8, ρ=1/513, anchor lb 1/513	0.025
C07	`m2_planar_surplus_r16`	M2	r=16: t=1/30, ρ=1/7201	0.026
C08	`m2_planar_surplus_r64`	M2	r=64: t=1/126, ρ=1/127009	0.026
C09	`m3_behrend_m3_q4_a2_c1`	M3	m=3, L=7: $\|u\|^2$=5, 2 diag. sols	0.073
C10	`m3_behrend_m4_q3_a2_c2`	M3	m=4, L=7: $\|u\|^2$=2, 4 diag. sols	1.576
C11	`m3_behrend_m4_q4_a3_c1`	M3	m=4, L=11: $\|u\|^2$=8, 4 diag. sols	1.220
C12	`m3_behrend_m5_q3_a3_c2`	M3	m=5, L=9: $\|u\|^2$=3, 3 diag. sols	3.300
C13	`m4_xor_b2_tail2_cols`	M4	b=2 (16 pairs), b'=2, 2 viol. killed	0.069
C14	`m4_xor_b3_tail3_cols`	M4	b=3 (64 pairs), b'=3, 3 viol. killed	0.273
C15	`m4_xor_b4_tail3_cols`	M4	b=4 (256 pairs), b'=3, 3 viol. killed	1.045
C16	`m4_xor_b5_tail4_cols`	M4	b=5 (1024 pairs), b'=4, 3 viol. killed	8.820

2. Hand-Verifiable Worked Exact Witnesses (One per Mode).

- **Mode 1 (`C01`, $r = 3, k = 3$, block family $\{0,1\}^3$):** All $\binom{8}{3} = 56$ triples fail admissibility, confirming sunflower-freeness at the exact block-transversal lower bound $(3-1)^3 = 8$ (vs. $3! \cdot 2^3 = 48$); all $4^3 = 64$ columns satisfy Eq. (3.1) iff admissible.

- **Mode 2 (`C06`, $r = 5$):** $t = \frac{1}{8}$, $\eta = \frac{1}{256}$, $D = \frac{513}{256}$, $\rho = \frac{1}{513}$, rectangle gap $\frac{t}{D} = \frac{32}{513}$, and cleared triangle inequality $(1 + \frac{1}{64})^2 = \frac{4225}{4096} < \frac{4352}{4096} = 1 + \frac{4}{64}$.

- **Mode 3 (`C10`, $m = 4, q = 3, a = 2, c = 2, L = 7$):** With $u = (1,1,0,0)$ ($\|u\|^2 = 2$), H the 6 weight-2 binary vectors, and V_u the 4 vectors with $\|v\|^2 = 2, \langle u, v\rangle = 1$, all $4^2 \cdot 6^2 = 576$ tuples satisfy $|\text{diff}| < 7$ and yield exactly 4 diagonal solutions $g_1 = g_2 = u, v_1 = v_2$.

- **Mode 4 (`C14`, $b = 3, b' = 3$):** All $4^3 = 64$ pairs in $(\mathbb{F}_2^3)^2$ match 7 masks iff $x = y$ and unique $x \oplus y$ iff $x \neq y$; on violating column $[2, 2, 11, 11]$ (both heads repeat), all 8 false ties across 64 mask pairs are canceled identically to 0.

3. 16-Certificate Atlas & 80-Test Red-Team Audit (Table 2, Fig. 3). Table 2 lists all 16 canonical certificates verified in 0.024–19.286 ms. `tests/test_suite.py` runs 80 pytest checks: 1 full 16-certificate replay, 3 raw-JSON parser guards (float, `NaN`, duplicate keys), 2 exact regressions (exhaustive 512-column two-head IE audit and exact rational planar surplus), and 74 parametrized live adversarial forgeries (12 schema/parser, 16 Mode 1, 16 Mode 2, 14 Mode 3, 16 Mode 4), each asserting an exact regex on its intended `CertificateError` branch. `scripts/verify_all.py` enforces all 5 gates including strict axiom whitelisting and a 41-file SHA-256 manifest.

5 Conclusion

We built an independent, explicitly scoped, zero-floating-point verification companion for the discrete transversal, planar-semiperimeter, Behrend-sphere broadcast, XOR-matching equality filter, and two-head inclusion–exclusion mechanisms of OpenAI's exponential sunflower preprint [9], pairing 18 constructive Lean 4.35.0 sub-lemmas (zero `sorry`, zero `Classical.choice`) with the pure-`int`/`Fraction` 4-mode auditor `SUNFLOWER-EXP-CERT-1.0`, 16 canonical ex-

act finite witnesses, and 74/74 live adversarial forgery rejections.

References

[1] H. L. Abbott. Some remarks on a combinatorial theorem of Erdős and Rado. *Canadian Mathematical Bulletin*, 9(2):155–160, 1966.

[2] H. L. Abbott, D. Hanson, and N. Sauer. Intersection theorems for systems of sets. *Journal of Combinatorial Theory, Series A*, 12(3):381–389, 1972.

[3] Noga Alon, Amir Shpilka, and Christopher Umans. On sunflowers and matrix multiplication. *Computational Complexity*, 22:219–243, 2013.

[4] Ryan Alweiss, Shachar Lovett, Kewen Wu, and Jiapeng Zhang. Improved bounds for the sunflower lemma. *Annals of Mathematics*, 194:795–815, 2021.

[5] Felix A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proceedings of the National Academy of Sciences of the United States of America*, 32(12):331–332, 1946.

[6] Tolson Bell, Suchakree Chueluecha, and Lutz Warnke. Note on sunflowers. *Discrete Mathematics*, 344:112367, 2021.

[7] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, volume 12699 of *LNCS*, pages 625–635. Springer, 2021.

[8] Paul Erdős and Richard Rado. Intersection theorems for systems of sets. *Journal of the London Mathematical Society*, 35:85–90, 1960.

[9] OpenAI. An exponential bound for sunflowers. Unrefereed Companion Preprint (OpenAI Math Release, https://github.com/openai/math/blob/main/preprints/An-exponential-bound-for-sunflowers-November-24-2026/paper.pdf), November 2026. Proposes $M_r(k) \le B_r^k$ with $\log B_r = O((\log r)^4 (\log\log(2r))^{5/2})$ for the Erdős–Rado fixed-petal sunflower conjecture.