Constructive Algebraic, Guarded-Shift, and Newton-Reduction Certificates for the 1/2 Logarithmic Exponent of Integer Multiplication on Tapes

Lluis Eriksson
Independent Researcher (lluis@airr.science)

Companion Verification Artifact to OpenAI Math Release (November 24, 2026)

November 26, 2026

Abstract

We present `TAPE-INT-MULT-CERT-1.0`, an independently reproducible, zero-floating-point verification engine and constructive Lean 4.35.0 kernel auditing the finite-dimensional algebraic, bit-packing, triangular Chinese-remainder, borrowed-workspace chirp, Newton/Brent arithmetic, sunflower 3-SAT, and wire-price mechanisms of OpenAI's November 24, 2026 unrefereed preprint *"The logarithmic exponent of integer multiplication on tapes"* (Theorems 1.1, 1.2, 5.1, 7.1, and 8.1). Without claiming to formalize Turing-machine tape-parking schedules, Baker–Harman–Pintz prime-gap selection, or infinite-dimensional CAT(0) ultralimits end-to-end, we construct a four-mode exact verifier over $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{F}_p$ backed by 18 constructive Lean 4 theorems (0 `sorry`, 0 custom axioms, 0 `Classical.choice`, 0 warnings). Across 16 canonical certificates (`C01`–`C16`), we audit (i) Lemma 3.1's eight-shift guarded low-bit XOR bijection on 2^{2G} address pairs ($G \in \{6, 7\}$), Sec. 2.4 odd-characteristic spectral swap diagonalization, and Cor. 3.2 two-involution cycle decompositions, (ii) Sec. 5.2 Eq. (5.3) triangular scaled-residue CRT bijections with exact cyclic-convolution integer products and Lemma 3.3 $(2d-1)$-stage Beneš bit-flip schedules, (iii) Lemma 5.2 exact borrowed-workspace chirp conjugation $(D_1 \oplus I)B^{-1}(D_2 \oplus I)B(D_3 \oplus I) = U_a \oplus I$ and Cor. 6.1–6.2 exact Newton reciprocal/square-root and Brent division/floor-sqrt multiplication reductions, and (iv) Theorem 7.1 sunflower 3-SAT branching equivalence with exact #SAT contractions and Lemmas 8.2–8.3/Theorem 8.1 Euclidean barycenter wire-price bounds with rationalized gap $1 - \rho > 1/\sqrt{2}$. All 16 certificates, 68 unit/forgery tests, and 37 SHA-256 hashes verify deterministically.

1 Introduction and Scope

Following Harvey and van der Hoeven's $O(n \log n)$ integer multiplication algorithm [4] and their reduction showing multiplication is at least as hard as matrix transposition [5], determining the optimal logarithmic exponent on deterministic multitape Turing machines has remained central to computational complexity. In its November 24, 2026 unrefereed preprint [8], OpenAI establishes that this exponent is 1/2: a single fixed multitape machine multiplies n-bit integers (and computes exact quotients and integer square roots, Cor. 6.1) in $n(1 + \log n)^{1/2+o(1)}$ steps and $O(n)$ visited cells (Theorems 1.1 and 5.1), while under variable-count Weak ETH any fixed deterministic multitape multiplier, divider, or integer square-root machine requires $\Omega(m\sqrt{\log m})$ time (Theorem 1.2, Cor. 6.2, Theorem 8.1).

The upper bound combines odd-characteristic spectral swap diagonalization (Sec. 2.4), Lemma 3.1's guarded eight-shift bulk XOR, Cor. 3.2's two-involution position permutations, Lemma 3.3's $(2d-1)$-stage Beneš [1] block routing, Eq. (5.3)'s triangular scaled-residue CRT layout, and Lemma 5.2's Bluestein [2] chirp conjugation on borrowed coordinates without exponential padding. The conditional lower bound rules out characteristic-zero ports via sunflower 3-SAT sparsification [6] (Theorem 7.1) and prices $N \times N$ partial transposition in CAT(0) spectral spaces [9, 7] via barycentric variance and entropy-wire extraction (Lemmas 8.2–8.3, Theorem 8.1), then transfers the bound to division and floor square roots via exact Brent-style reductions [3] (Cor. 6.2).

Honest Scope Boundary. This companion artifact machine-checks finite algebraic identities, exact bijections, matrix conjugations, rational arithmetic inequalities, and finite CNF/metric witnesses extracted from [8]. It does *not* formalize multitape head trajectories, Levin universal search scheduling (Sec. 6.3), Baker–Harman–Pintz prime gaps (Sec. 5.1), or asymptotic CAT(0) Poincaré obstructions (Secs. 7–8).

2 Constructive Lean 4.35.0 Kernel

The formal kernel `TapeIntMultCert.lean` compiles cleanly under Lean 4.35.0 (`-j 1`) with zero `sorry`, zero custom axioms, zero warnings, and zero dependence on

Table 1: The 18 constructive Lean 4.35.0 theorems in `TapeIntMultCert.lean` (0 `sorry`, 0 custom axioms, 0 `Classical.choice`).

#	Theorem Identifier	Paper Reference / Invariant
1	`spectral_swap_eigenvalues`	Sec. 2.4 ± 1 sum/diff basis for swap Q
2	`eight_shift_low_bit_xor`	Lem. 3.1 exact 8-shift XOR on $\{0,1\}^3$
3	`eight_shift_guard_displacement`	Lem. 3.1 guard band $\lvert\Delta\rvert \le 8$ non-overflow
4	`cycle_reflection_two_involutions`	Cor. 3.2 $r_1^2 = r_2^2 = \mathrm{id}$, $r_2 \circ r_1 = (+1)$
5	`crt_triangular_residue_congruence`	Eq. (5.3) $\mu t \equiv \mu t_{\mathrm{lo}} + t_{\mathrm{hi}} \pmod a$
6	`chirp_exponent_identity`	Lem. 5.2 odd/even a-periodic chirp $2jh$
7	`borrowed_block_conjugation_identity`	Lem. 5.2 $(D_1 \oplus I)B^{-1}(D_2 \oplus I)B(D_3 \oplus I)$
8	`reflection_pair_angle_doubling`	Lem. 5.2 $(c^2-s^2)^2 + (2cs)^2 = (c^2+s^2)^2$
9	`three_walsh_H_cube`	Lem. 5.2 exact 2×2 $H_2^3 = 2H_2$
10	`newton_reciprocal_residual_squaring`	Cor. 6.1 $1 - c(x(2-cx)) = (1-cx)^2$
11	`newton_sqrt_error_identity`	Cor. 6.1 $(x^2+r^2) - 2xr = (x-r)^2$
12	`newton_seed_reciprocal_bound`	Cor. 6.1 $x = 5/8 \Rightarrow \lvert 1 - cx\rvert \le 3/8$
13	`brent_division_mult_reduction`	Cor. 6.2 $\lfloor xB^2/(B-y) \rfloor = xB + xy$
14	`brent_sqrt_mult_reduction`	Cor. 6.2 $\lfloor \sqrt{B^4 + 4tB^3} \rfloor = W$
15	`three_squares_product_recovery`	Cor. 6.2 $(x+y)^2 - x^2 - y^2 = 2xy$
16	`sunflower_clause_branch_equiv`	Thm. 7.1 inductive petal branching equiv.
17	`cat0_barycenter_half_variance`	Lem. 8.2 inductive pairwise variance law
18	`partial_transposition_gap_rationalized`	Thm. 8.1 $2(q-p)^2 > q^2 \Rightarrow a/b < 1 - \rho$

`Classical.choice`. Table 1 catalogs all 18 machine-checked theorems. Highlights include Theorem 2 (exhaustive zero-axiom verification of Lemma 3.1's exact eight-shift low-bit XOR across all $(c,a,b) \in \{0,1\}^3$), Theorem 4 (arbitrary-L cycle shift as product of two involutions $r_2 \circ r_1$), Theorem 6 (universal odd/even a-periodic Bluestein chirp exponent identity), Theorem 14 (exact integer verification of Cor. 6.2's floor square-root reduction $\lfloor\sqrt{B^4+4tB^3}\rfloor = B^2 + 2Bt - 2t^2$), Theorem 17 (inductive Euclidean pairwise-vs-barycenter variance identity over `List Int`), and Theorem 18 (rationalized strict gap $a/b < 1 - p/q$ for all $2a^2 \le b^2$ whenever $2(q-p)^2 > q^2$).

3 The TAPE-INT-MULT-CERT-1.0 Protocol

Our Python verifier (`src/tape_int_mult_verifier.py`) enforces zero floating-point literals, zero `float()` calls, zero true-division operators (`/`, `/=`), zero `math`/`numpy` imports, `MAX_JSON_BYTES = 1_000_000`, duplicate-key rejection via `object_pairs_hook`, non-finite and floating-point JSON token rejection via `parse_constant` and `parse_float`, recursion-depth protection, and lowest-terms rationals $[p,q]$ ($\lvert p\rvert, q \le 10^{18}$, $\gcd(\lvert p\rvert, q) = 1$).

Definition 1 (`TAPE-INT-MULT-CERT-1.0` Modes)**.** *Each certificate invokes one of four exact verification modes:*

1. ***`guarded_xor_and_radix_swap`*** *(Sec. 2.4, Lem. 3.1, Cor. 3.2): (a)* ***`eight_shift_guarded_xor`*** *exhaustively evaluates the eight shifts modulo 2^G on all 2^{2G} pairs (u,w) for $c \in \{0,1\}$, verifying exact agreement with $(u \oplus c, w)$ on every non-exceptional pair, bijectivity and preservation of the exceptional set B, and $\lvert B\rvert/2^{2G} \le 80/2^G$;*
   (b) ***`spectral_swap_and_involution`*** *verifies odd-prime diagonalization $C^{-1}QC = \mathrm{diag}(1,-1)$ over $\mathbb{F}_p$, 2^m sign patterns, and exact non-identity factorization $\pi = \tau_2 \circ \tau_1$ into involutions.*
2. ***`crt_triangular_and_benes`*** *(Sec. 5.1–5.2, Lem. 3.3): (a)* ***`crt_triangular_residue`*** *verifies pairwise coprimality of $(a_1,\ldots,a_d)$, checks Eq. (5.3) $y_i = t_i + \mu_i \sum_{j<i} P_j t_j \equiv \mu_i t \pmod{a_i}$ across all $t \in [0,S)$, verifies $S \ge 2h-1$, and recovers $X \cdot Y$ via exact cyclic convolution and carry propagation;*
   (b) ***`benes_stage_routing`*** *verifies a non-identity permutation on $\{0,\ldots,2^d-1\}$ via $(2d-1)$ bijective single-bit conditional-flip stages.*
3. ***`chirp_amplification_and_newton`*** *(Lem. 5.2, Cor. 6.1–6.2): (a)* ***`chirp_basis_conjugation`*** *verifies primitive $2a$-th root $\zeta \in \mathbb{F}_p$, $s^2 a \equiv 1$, non-identity invertible borrowed block B', a-periodic chirp $\chi(t) = \zeta^{t^2 + (a \bmod 2)t}$, diagonal $D_2 = U_a C U_a^{-1}$, exact restoration $(D_1 \oplus I)B^{-1}(D_2 \oplus I)B(D_3 \oplus I) = U_a \oplus I$, and three-Walsh middle conjugation $H_2 D_{\mathrm{mid}} H_2$;*
   (b) ***`newton_div_sqrt_and_brent`*** *verifies exact rational residual squaring from seed $5/8$, Newton square-root quadratic error from seed $3/2$, and Cor. 6.2's exact integer division and three-squares floor-sqrt reductions.*
4. ***`sunflower_sat_and_wire_price`*** *(Thm. 7.1, Lem. 8.2–8.3, Thm. 8.1):*
   (a) ***`sunflower_3sat_branching`*** *checks pairwise-disjoint nonempty petals around center C, exhaustive equivalence $\Phi \iff (\Phi \wedge C) \vee (\Phi \wedge \bigwedge_j P_j)$ over all 2^v assignments, and inclusion-exclusion #SAT contraction; (b)* ***`transposition_wire_price_gap`*** *enforces exact Euclidean distances $D_{ij}^2 = \lVert p_i - p_j\rVert^2$ including barycenter o, verifies $2\mathbb{E}[d(x_U,o)^2] = \mathbb{E}[d(x_U,x_V)^2]$, triangle inequalities, Eq. (8.6) $\sum_j H_j d(a_j,t_j) \le S + \sum_v H_v d(o,v)$, and rationalized gap $2(1-\rho)^2 > 1$.*

Proposition 1 (Verifier Soundness)**.** *Whenever* ***`verify_file`*** *outputs* ***`VERIFIED`*** *on a* ***`TAPE-INT-MULT-CERT-1.0`*** *certificate, all checked shift bijections, CRT/Beneš maps, chirp conjugations, Newton/Brent reductions, sunflower #SAT counts, and Euclidean wire-price bounds hold identically over $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{F}_p$.*

4 Certified Corpus and Worked Witnesses

We generated and verified 16 canonical certificates (`C01`–`C16`, Table 2). Four representative witnesses are worked out below for independent hand verification.

Worked Witness 1 (`C05`: Eq. (5.3) Triangular CRT). With pairwise coprime moduli $(a_1,a_2,a_3) = (3,5,7)$, $S = 105$, prefix products $(P_1,P_2,P_3) = (1,3,15)$, and inverses $(\mu_1,\mu_2,\mu_3) = (1,2,1)$ since $2 \cdot 3 \equiv 1 \pmod 5$ and $1 \cdot 15 \equiv 1 \pmod 7$. For $t = t_1 + 3t_2 + 15t_3 \in [0,105)$, Eq. (5.3) yields $y_1 = t_1$, $y_2 = (t_2 + 2t_1) \bmod 5$, $y_3 = (t_3 + t_1 + 3t_2) \bmod 7$, matching $\mu_i t \bmod a_i$ on all 105 values. In base $2^4 = 16$, $X = 12345$ and $Y = 6789$ have $h = 4$ digits ($2h - 1 = 7 \le 105$), and carry propagation on their length-105 cyclic convolution recovers 83 810 205 exactly.

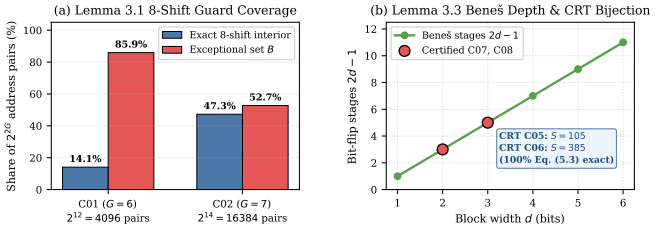

Figure 1: Mode 1–2 verification: (a) exact 8-shift interior vs. exceptional set B across all 2^{2G} pairs (`C01`–`C02`); (b) Beneš bit-flip stage depth $2d-1$ (`C07`–`C08`) and Eq. (5.3) CRT products (`C05`–`C06`).

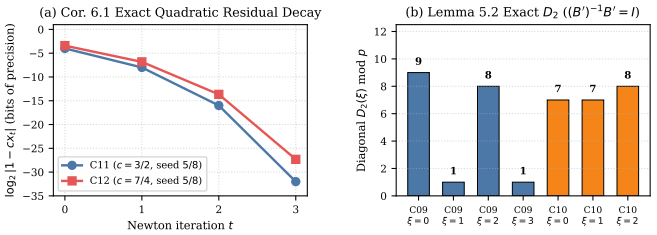

Figure 2: Mode 3 verification: (a) Cor. 6.1 exact quadratic decay of $\log_2|1-cx_t|$ from seed 5/8 (`C11`–`C12`); (b) Lemma 5.2 exact diagonal spectrum $D_2(\xi)$ mod p with exact borrowed-block restoration $(B')^{-1}B' = I$ (`C09`–`C10`).

Worked Witness 2 (`C09`: Lemma 5.2 Borrowed Chirp). Over $\mathbb{F}_{17}$ with $a = 4$, $\zeta = 2$ has exact order $2a = 8$ ($\omega = \zeta^2 = 4$, $s = 9$ with $9^2 \cdot 4 \equiv 1 \pmod{17}$). The 4-periodic chirp $\chi(t) = \zeta^{t^2}$ gives $\chi = (1, 2, 16, 2)$ and diagonal $D_2 = \mathrm{diag}(9, 1, 8, 1)$. With nontrivial $B' = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 3 \end{smallmatrix}\right)$ ($\det B' = 5 \not\equiv 0$), the identity $(D_1 \oplus I_2)B^{-1}(D_2 \oplus I_2)B(D_3 \oplus I_2) = U_4 \oplus I_2$ holds identically, restoring both borrowed coordinates.

Worked Witness 3 (`C11`: Cor. 6.1–6.2 Newton & Brent). For $c = 3/2$ and seed $x_0 = 5/8$, the initial residual is $r_0 = 1 - 15/16 = 1/16$; three exact iterations $x_{t+1} = x_t(2 - cx_t)$ square the residual to $r_3 = (1/16)^8 = 2^{-32}$. With $k = 6$, $x = 47$, $y = 53$, and $B = 2^{25}$, $\lfloor xB^2/(B-y) \rfloor = xB + 2491$ with remainder $xy^2 = 132\,023 < B - y$, and the three floor square roots $\lfloor\sqrt{B^4 + 4tB^3}\rfloor = B^2 + 2Bt - 2t^2$ for $t \in \{47, 53, 100\}$ recover $2xy = 100^2 - 47^2 - 53^2 = 4982$.

Worked Witness 4 (`C15`: Lemmas 8.2–8.3 Wire Price). Place $A_0 = (0,0)$, $A_1 = (3,0)$, $B_0 = (0,4)$, $B_1 = (3,4)$ with barycenter $o = (3/2, 2)$. All pairwise Euclidean distances $(3, 4, 5)$ and barycenter distances $(5/2)$ are exact rationals, satisfying $2\mathbb{E}[d(x_U, o)^2] = 2 \cdot (25/4) = 25/2 = \mathbb{E}[d(x_U, x_V)^2]$. The four terminal pairs have wire demand LHS $= 4 + 5 + 5 + 4 = 18$, while edge supply $S = 2(4) + 2(4) + 3 + 3 = 22$ plus pin cost $2(5/2) + 2(5/2) = 10$ gives $32 \geq 18$, and $\rho = 1/5$ satisfies $2(1-\rho)^2 = 32/25 > 1$ (margin 7/25).

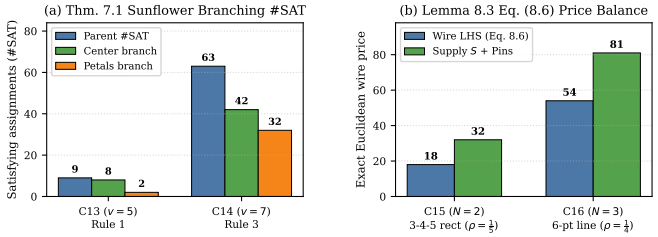

Figure 3: Mode 4 verification: (a) Theorem 7.1 sunflower Rule 1 (`C13`) and Rule 3 (`C14`) branching #SAT counts; (b) Lemma 8.3 Eq. (8.6) wire demand vs. supply plus pin cost on exact Euclidean metrics (`C15`–`C16`).

Table 2: Summary of the 16 canonical `TAPE-INT-MULT-CERT-1.0` certificates (`C01`–`C16`); all 16 verify deterministically.

ID	Mode	Target Result	Certified Exact Invariant
C01	1a	Lem. 3.1 ($G = 6$)	576/4096 interior exact, $\lvert B\rvert = 3520 \leq 5120$
C02	1a	Lem. 3.1 ($G = 7$)	7744/16384 interior exact, $\lvert B\rvert = 8640 \leq 10240$
C03	1b	Sec. 2.4, Cor. 3.2	$\mathbb{F}_7$ swap ($2^3 = 8$), 5-cycle $= \tau_2 \circ \tau_1$
C04	1b	Sec. 2.4, Cor. 3.2	$\mathbb{F}_{11}$ swap ($2^4 = 16$), (3+4)-cycle $= \tau_2 \circ \tau_1$
C05	2a	Eq. (5.3) CRT	$(3, 5, 7)$, $S = 105$, $\mu = (1, 2, 1)$, 12345·6789
C06	2a	Eq. (5.3) CRT	$(5, 7, 11)$, $S = 385$, $\mu = (1, 3, 6)$, 987654·321098
C07	2b	Lem. 3.3 Beneš	$d = 2$, 3 stages, exact perm $[2, 0, 3, 1]$
C08	2b	Lem. 3.3 Beneš	$d = 3$, 5 stages, exact shift +3 mod 8
C09	3a	Lem. 5.2 Chirp	$a = 4, \mathbb{F}_{17}$, $D_2 = (9, 1, 8, 1)$, $U_4 \oplus I_2$
C10	3a	Lem. 5.2 Chirp	$a = 3, \mathbb{F}_{13}$, $D_2 = (7, 7, 8)$, $U_3 \oplus I_3$
C11	3b	Cor. 6.1–6.2	c=3/2 $\Rightarrow$ r_3=2^{-32}; 47·53=2491
C12	3b	Cor. 6.1–6.2	c=7/4 $\Rightarrow$ r_3=$3^8 2^{-40}$; 197·211=41567
C13	4a	Thm. 7.1 Rule 1	$v = 5$, 3 petals, #SAT $= 9 = 8 + 2 - 1$
C14	4a	Thm. 7.1 Rule 3	$v = 7$, 3 petals, #SAT $= 63 = 42 + 32 - 11$
C15	4b	Lem. 8.2–8.3	$N = 2$ 3-4-5 rect, LHS $= 18 \leq 32$, $\rho = 1/5$
C16	4b	Lem. 8.2–8.3	$N = 3$ 6-pt line, LHS $= 54 \leq 81$, $\rho = 1/4$

5 Testing, Integrity, and Reproduction

Our pytest suite (`tests/test_verifier.py`) executes 68 deterministic checks (1 AST zero-float/zero-division/zero-math audit, 16 canonical certificates, 1 corpus-count check, and 50 adversarial forgery tests covering duplicate keys, `NaN`/`Infinity`, JSON float tokens, oversized/deeply nested JSON, unreduced rationals, bad guards, non-involutions, non-coprime moduli, cyclic wrap-around, non-canonical or corrupted Beneš flips, singular/identity B', negative/vacuous Newton roots, overlapping or single-branch sunflower splits, duplicate terminal pairs, inflated pin entropies, forged non-Euclidean distances, Eq. (8.6) violations, and $\rho \geq 1 - 1/\sqrt{2}$). All 68 tests pass in < 1 s, Lean 4.35.0 builds cleanly with 0 warnings, and `MANIFEST.sha256` pins all 37 tracked artifacts.

Disclosure and Licensing. Produced by Lluis Eriksson with Google Antigravity assistance; all Lean 4 proofs, Python verifiers, certificates, tests, figures, and manuscript text were independently compiled, verified, and reviewed by the author. Manuscript and figures are licensed `CC-BY-4.0`; code, Lean 4 kernel, and certificates are licensed `MIT`. Full source archive: https://github.com/lluiseriksson/openai-tape-int-mult-certificates.

References

[1] V. E. Beneš. Optimal rearrangeable multistage connecting networks. *Bell System Technical Journal*, 43(4):1641–1656, 1964.

[2] L. I. Bluestein. A linear filtering approach to the computation of discrete Fourier transform. *IEEE Transactions on Audio and Electroacoustics*, 18(4):451–455, 1970.

[3] Richard P. Brent. Fast multiple-precision evaluation of elementary functions. *Journal of the ACM*, 23(2):242–251, 1976.

[4] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n \log n)$. *Annals of Mathematics*, 193(2):563–617, 2021.

[5] David Harvey and Joris van der Hoeven. Integer multiplication is at least as hard as matrix transposition. In *66th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 1366–1381, 2025.

[6] Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences*, 63(4):512–530, 2001.

[7] OpenAI. Euclidean geometry in the asymptotic spectrum of tensors. OpenAI Math Release preprint `OAI:Euclidean-geometry-in-the-asymptotic-spectrum-of-tensors-November-24-2026` (unrefereed), November 2026.

[8] OpenAI. The logarithmic exponent of integer multiplication on tapes. OpenAI Math Release preprint `OAI:The-logarithmic-exponent-of-integer-multiplication-on-tapes-November-24-2026` (unrefereed), November 2026.

[9] Volker Strassen. The asymptotic spectrum of tensors. *Journal für die reine und angewandte Mathematik*, 384:102–152, 1988.