The circuit size of $[x_1 + \cdots + x_6 \equiv 1 \pmod 3]$: closing the $n = 6$ case of Knuth's mod-3 conjecture

machine-assisted (Claude, Anthropic, as autonomous research agent)

22 August 2026

Abstract

Let $\mathrm{MOD}_n^{3,r}(x) = [x_1 + \cdots + x_n \equiv r \pmod 3]$ and let $\mathrm{C}(f)$ be the minimum number of binary gates (any of the 16 operations) in a circuit for f. Knuth (TAOCP 7.2.2.2, answer to exercise 480) computed $\mathrm{C}(\mathrm{MOD}_n^{3,r})$ for $n \le 5$, proved $\mathrm{C}(\mathrm{MOD}_6^{3,0}) = 12$ with a SAT solver, conjectured $\mathrm{C}(\mathrm{MOD}_n^{3,r}) = 3n-5-[(n+r) \equiv 0 \bmod 3]$, and wrote that the case $n = 6$, $r \neq 0$ "lies tantalizingly close to the limits of today's solvers [and] is still unknown." Kulikov, Pechenev and Slezkin proved the conjectured upper bound for all n. We report on a machine-checked attack on the remaining cell $\mathrm{C}(\mathrm{MOD}_6^{3,1})$ $(= \mathrm{C}(\mathrm{MOD}_6^{3,2}))$: an explicit 13-gate circuit, verified in the Lean 4 kernel; a DRAT-certified proof that no circuit of 11 or fewer gates exists, obtained from Knuth's encoding strengthened by a gate-elimination lemma that is itself proved inductively with DRAT certificates at $n = 4, 5$; and a DRAT-certified cube-and-conquer proof that no 12-gate circuit exists. Hence $\mathrm{C}(\mathrm{MOD}_6^{3,1}) = \mathrm{C}(\mathrm{MOD}_6^{3,2}) = 13$, and Knuth's conjecture holds for $n = 6$. The same machinery, fed with these values, reproduces $\mathrm{C}(\mathrm{MOD}_6^{3,0}) = 12$ and settles a cell at $n = 7$: $\mathrm{C}(\mathrm{MOD}_7^{3,2}) = 15$ (conjectured value), with $\mathrm{C}(\mathrm{MOD}_7^{3,0}), \mathrm{C}(\mathrm{MOD}_7^{3,1}) \in \{15, 16\}$. Nothing here bears on P vs NP; the contribution is one exact value at the finite base of the circuit-lower-bound programme.

1 Statement and prior status

A *Boolean chain* on $x_1, \ldots, x_n$ is a sequence $x_i = x_j \circ_i x_k$ $(n < i \le n + s,\ 1 \le j < k < i)$ with $\circ_i$ any binary operation; its cost is s. $\mathrm{C}(f)$ is the least cost of a chain having f as some step; $\mathrm{C}(f) = \mathrm{C}(\neg f)$ and *normal* chains (all operations send $(0, 0) \mapsto 0$) suffice (Knuth 7.1.2). Known values: $\mathrm{C}(\mathrm{MOD}_3^{3,r}) = (3, 4, 4)$, $\mathrm{C}(\mathrm{MOD}_4^{3,r}) = (7, 7, 6)$, $\mathrm{C}(\mathrm{MOD}_5^{3,r}) = (10, 9, 10)$ for $r = 0, 1, 2$, and $\mathrm{C}(\mathrm{MOD}_6^{3,0}) = 12$ (Knuth); $\mathrm{C}(\mathrm{MOD}_n^{3,r}) \le 3n - 5 - [(n + r) \equiv 0 \bmod 3]$ (KPS, Thm 1). Open: $\mathrm{C}(\mathrm{MOD}_6^{3,1}) \in \{?, \ldots, 13\}$. Complementing all inputs shows $\mathrm{C}(\mathrm{MOD}_6^{3,1}) = \mathrm{C}(\mathrm{MOD}_6^{3,2})$.

2 Method

Encoding. We use Knuth's CNF of answers 477–478 (after Kojevnikov–Kulikov–Yaroslavtsev): variables x_{it} (truth tables of steps), s_{ijk} (operand pairs), f_{ipq} (operation bits), g_{hi} (outputs). Our generator reproduces Knuth's published counts exactly (full adder: 82 variables / 942 clauses at $r = 4$, 115/1662 at $r = 5$). A second, structurally different encoding (one-hot left/right operands, one-hot over five operations, lex instead of colex ordering) agrees with the first on every calibration cell.

Symmetry breaking (Lemma 1). For a minimum chain of a fully symmetric function depending on all inputs we may assume: nontrivial operations; every step used; no re-application of an operand (Knuth); colex-ordered operand pairs for consecutive independent steps; inputs first used in order $x_1, \ldots, x_n$; distinct truth tables; output last. Proof: take the lexicographically least sequence of operand pairs over all relabellings and topological reorderings. (Full proof in the README.)

Gate elimination (Lemmas 2, 2′, 3, 4). Substituting $x_j := 1$ into a chain of cost s for $\mathrm{MOD}_6^{3,1}$ deletes every step reading x_j and leaves a chain for $\pm\mathrm{MOD}_5^{3,0}$; hence every input has fanout $\varphi_j \le s-10$. At the tight level a step reading x_j cannot collapse to a constant (its consumer would also die). More generally, for each (j, c) we encode the set of steps that provably become constant or read a constant, and require its size to be $\le s - \mathrm{C}(f|_{x_j:=c})$. Finally (Lemma 4), substituting $x_a := x_b$ for two inputs makes a step reading exactly $\{x_a, x_b\}$ unary (the constant 0 if its op has $f_{11} = 0$) and leaves a chain for $h = [2x_b + \sum \mathrm{rest} \equiv 1]$, whose cost we prove to be 10 (chain at 10; UNSAT at 9 by 264 DRAT-checked cubes with a checked cover); so at most $s-10$ steps are deleted, which pins an XOR of two inputs to fanout 1. This lemma is what collapses the hard region of the $s = 12$ search (cubes with two XOR-of-inputs gates among the first three steps, ≈ 2 CPU-hours each without it, well under a second with it). All of these are clause groups added to the CNF; each was validated on every calibration cell (satisfiable cells stay satisfiable). The costs used are Knuth's, *re-proved here* with DRAT certificates ($n = 4$ plain; $n = 5$ plain by encoding B and with the $n = 4$-based bound by encoding A), so the induction is machine-checked at every level.

Certificates. Every satisfiable cell yields a chain checked by an independent 90-line verifier and by a self-contained Lean 4 file (kernel `decide` over all 2^n inputs, with a negative control). Every unsatisfiable cell yields a DRAT proof checked by `drat-trim`; the $s = 12$ case is split into cubes on the first four steps (18 760 cubes; six were split one step further), each cube's proof is checked, and the cube cover is itself proved by a DRAT-checked refutation.

3 Results

claim	status
$\mathrm{C}(\mathrm{MOD}_6^{3,1}) \le 13$	Lean kernel (KPS chain; our own SAT chain)
no chain of cost ≤ 10	Lemma 2 from $\mathrm{C}(\mathrm{MOD}_5^{3,0}) = 10$ (DRAT)
no chain of cost 11	DRAT, 166 s (fanout ≤ 1), 0.6 s (+no-collapse)
no chain of cost 12	DRAT: 18 760 depth-4 cubes (6 refined to 220 depth-5), each checked; co
$\mathrm{C}(\mathrm{MOD}_6^{3,0}) = 12$	DRAT 0.1 s (Lemmas 1–3) + Biere's chain (Lean)
$\mathrm{C}(\mathrm{MOD}_7^{3,2}) = 15$	DRAT 0.4 s at $s = 14$ (fanout ≤ 1 from the $n = 6$ values) + KPS chain (
$\mathrm{C}(\mathrm{MOD}_7^{3,0}), \mathrm{C}(\mathrm{MOD}_7^{3,1}) \ge 15$ (≤ 16)	DRAT 1.2 s / 7.2 s at $s = 14$; KPS chains (Lean)

4 Calibration

Knuth's nine values for $n \le 5$ and the full adder are reproduced (SAT halves verified, UNSAT halves DRAT-checked); his Table 1 distribution of 4-variable costs ($5, 35, 263, 1500, 6812, 18904, 31408$ normal functions of cost $\le s$) is reproduced by an exhaustive non-SAT enumerator; Biere's 12-step chain for $\overline{\mathrm{MOD}_6^{3,0}}$ is transcribed and Lean-verified.

5 What is new and what is quoted

Quoted: the encoding (KKY 2009, Knuth), the 13-gate construction (KPS), all anchor values (Knuth). New and checkable: the value $C(\mathrm{MOD}_6^{3,1}) = 13$ and the value $C(h) = 10$, with their certificate chain; the exhaustive confirmation of Knuth's Table 1. New as statements: Lemma 1 as one proved statement; Lemmas 2–4 (classical gate elimination, here as exact clause groups over machine-checked residue costs). Not reproduced: Knuth's $C(\mathrm{MOD}_6^{3,0}) = 12$ UNSAT half (runs exceeded 12 hours; not used). Every claim in this note is reproduced by `code/verify_all.sh`.