# Sharp $T$-Count Lower Bounds and Symplectic-Gram Decompositions for Unary-Tracked Unitary Synthesis and Wide Fredkin Gates

Lluis Eriksson*

November 26, 2026

**Abstract**

We resolve both open questions posed by Sun [1] (`arXiv:2611.34740v1`) regarding unary-tracked unitary synthesis and Wide Fredkin decompositions, and establish exact closed-form resource bounds for the associated space-depth volume construction.

First (Theorem 6, refuting Open Question 1), we prove that *every* computational-basis tracker encoding $E : \{0,1\}^n \to \mathbb{F}_2^m$ supporting universal zero-$T$ CNOT+$X$ Boolean lookups is affinely independent over $\mathbb{F}_2$ (requiring $m \geq 2^n - 1$), and that for *any* mixing subset $M \subseteq \{0,1\}^{n-1}$ of size $K_j = |M| \geq 2$, a four-term affine-dependence obstruction forces the exact stabilizer-nullity jump $\Delta\nu(K_j) = \nu(|\psi_{\text{out}}(M)\rangle) - \nu(|\phi_{\text{in}}(M)\rangle)$ to equal 3 for $K_j = 2$ and $K_j$ for all $K_j \geq 3$. By stabilizer-nullity monotonicity, *every* Clifford+$T$ (or Clifford + arbitrary single-qubit diagonal $R_z(\theta)$) circuit—even with arbitrary clean ancillas and arbitrary adaptive mid-circuit Pauli measurements—maintaining $E$ across a single multiplexed Clifford layer with $K_j$ mixing branches requires at least $K_j$ non-Clifford gates (and $\geq 3$ for $K_j = 2$), ruling out any poly$(n)$-$T$ tracker update whenever $K_j = \omega(\text{poly}(n))$.

Second (Theorem 9, resolving Open Question 2), for the full-space $m$-pair Wide Fredkin gate $W_m = \prod_{z=1}^{m} \text{CSWAP}(c; a_z, b_z)$, we prove via Clifford reduction to $\prod_{z=1}^{m} \text{CCZ}(c, a_z, b_z)$ and a discrete quadratic-derivative theorem that $|\,\text{Stab}(U_{\text{CCZ},m}|+\rangle^{\otimes(2m+1)})| = 1$, yielding the universal lower bound $T(W_m) \geq 2m + 1$ for all $m \geq 1$ (ruling out any $o(m)$ decomposition). Conversely, we introduce an explicit *symplectic-Gram* factorization $V_m V_m^\top = H_m \in \mathbb{F}_2^{2m\times 2m}$ using the provably minimal $k_{\min} = 2m+1$ rank-1 factors, giving an *ancilla-free, measurement-free* Clifford+$T$ circuit for full-space $W_m$ with exact $T$-count $4m+3$ and $12m-2$ CNOTs—a 1.75× asymptotic reduction over independent Fredkin gates ($7m$), matching the optimal 7 at $m = 1$, achieving 11 vs. 14 at $m = 2$, and lying within 2× of our universal lower bound.

Third (Theorem 10), exploiting the unary-subspace invariant $A_{z,0}A_{z,1} = 0$, we cut Sun's per-factor tracker update from $14K_j$ to $8K_j$ $T$-gates (1.75×) measurement-free with zero extra ancillas via an $S^\dagger$-corrected 4-$T$ relative-phase router, and to $4K_j$ (3.50×) with *zero extra ancillas* when adaptive measurements are permitted (Step 1 un-routing takes *exactly* 0 *$T$-gates*, matching the exact sign asymmetry $\Delta\nu = -K_j \leq 0$ vs. $+K_j$ for $K_j \geq 3$, and $\pm 3$ at $K_j = 2$). Fourth (Theorem 12), we derive exact closed-form depth and space-depth volume laws for Sun's Theorem 1.2, proving strict volume monotonicity in the power-of-two block size $B = 2^k$, eliminating a 2× budget-charged sawtooth penalty, and identifying an exact leading-order discontinuity between full-unary ($B = N$) and sub-$N$ QSD-hybrid regimes ($n \ll B \ll N$). All core universal algebraic lemmas and scaling identities are constructively formalized in Lean 4.35.0 (15/15 theorems, 0 `sorry`, 0 `Classical.choice`, 0 warnings) and cross-checked by an AST-audited zero-float exact $\mathbb{Q}(\zeta_8)$ verifier (16/16 SHA-256 certificates, 67/67 tests).

*Independent Researcher. Manuscript and figures licensed under CC-BY-4.0; Lean 4 formalization, exact $\mathbb{Q}(\zeta_8)$ verification scripts, and SHA-256 certificates licensed under MIT. Source repository: https://github.com/lluiseriksson/unary-tracker-t-count-lower-bounds.

Table 1: Exact $T$-count hierarchy resolving Open Questions 1 and 2 of Sun [1]. Lower bounds hold for arbitrary adaptive Clifford+$T/R_z(\theta)$ circuits with arbitrary clean ancillas and mid-circuit Pauli measurements. All upper bounds are exact over $\mathbb{Q}(\zeta_8)$ and require zero extra ancillas unless explicitly noted.

| **Problem / Construction** | **Exact $T$** | **Anc.** | **Meas.** | **Status / Ratio vs. [1]** |
|---|---|---|---|---|
| *Open Question 1: Single CSD factor tracker update ($K_j$ mixing branches)* | | | | |
| Universal LB (any affine-indep. $E$, $K_j \geq 3$) | $\geq K_j$ (3 at 2) | arb. | arb. | **Thm. 6 (refutes** poly$(n)$**)** |
| Sun [1] (2 Fredkins/branch) | $14K_j$ | 0 | No | Baseline |
| Ours: $S^\dagger$-corrected 4-$T$ router (Step 1+3) | $8K_j$ | 0 | No | **Thm. 10 (1.75× exact)** |
| Ours: 0-$T$ Step 1 + 4-$T$ Step 3 | $4K_j$ | 0 | Yes | **Thm. 10 (3.50× exact)** |
| *Open Question 2: Full-space $m$-pair Wide Fredkin $W_m = \prod_{z=1}^{m} \mathrm{CSWAP}(c; a_z, b_z)$* | | | | |
| Universal LB (all $m \geq 1$) | $\geq 2m+1$ | arb. | arb. | **Thm. 9(a) (refutes** $o(m)$**)** |
| Sun [1] (independent Fredkins) | $7m$ | 0 | No | Baseline |
| Naive shared-$c$ phase polynomial | $6m + (m \bmod 2)$ | 0 | No | Shares $T(c)$ across pairs |
| **Ours: Symplectic-Gram ($V_m V_m^\top = H_m$)** | $\mathbf{4m+3}$ | **0** | **No** | **Thm. 9(b) (1.75×, $12m-2$ CNOT)** |
| Gidney temporary-AND [3] | $4m$ | 1 | Yes | Saves 3 $T$-gates over $4m+3$ |

# 1 Introduction and Summary of Results

In a recent preprint [1], Sun introduced a unary-tracking architecture for fault-tolerant unitary synthesis in the Clifford+$T$ gate set. By maintaining an $N$-qubit unary (one-hot) register $A$ coherently tracking the computational-basis label of an $n$-qubit data register $D$ ($N = 2^n$),

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle_D |e_x\rangle_A, \tag{1}$$

any classically specified Boolean lookup $f : \{0,1\}^n \to \{0,1\}^w$ executes using only CNOT gates (0 $T$-gates). Across the $N-1$ multiplexed single-qubit factors of a cosine-sine decomposition (CSD), Sun's Theorem 1.1 achieves $T$-count $O(K + NL)$ using $N + O(L)$ clean ancillas (where $L = n + \log(1/\epsilon)$ and $K = \sum_{j=1}^{N-1} K_j$ is the total number of mixing branches across all CSD factors), paying two Fredkin (CSWAP) gates—14 $T$-gates ancilla-free—per mixing branch. In a second construction (Theorem 1.2), Sun combines unary-wire parallel execution with the quantum Shannon decomposition (QSD) using at most $a$ ancillas ($n \leq a \leq N$) to obtain depth $D = O(N^2/a)$ and space-depth volume $V = (n+a)D = O(N^2)$.

Section 5 of [1] leaves two explicit open questions as the central obstacles to reaching $\widetilde{O}(2^n)$ general unitary synthesis via unary tracking:

1. **Open Question 1 (Tracker update barrier):** *Can the per-factor tracker update cost $O(K_j)$ $T$-gates be reduced to* poly$(n)$ *$T$-gates, possibly via a different tracker encoding or a collective update, while preserving zero-$T$ Boolean lookups and exact cleanup?*
2. **Open Question 2 (Wide Fredkin decomposition):** *All $m$ Fredkin gates within a CSD factor share a single control qubit $c$ while acting on disjoint target pairs $(a_z, b_z)$. Does this "Wide Fredkin" gate $W_m = \prod_{z=1}^{m} \mathrm{CSWAP}(c; a_z, b_z)$ admit a more $T$-efficient decomposition than implementing each Fredkin gate independently ($7m$ $T$-gates)?*

We completely resolve both questions—proving exact matching-scale lower bounds and new constructive upper bounds—and sharpen Sun's Theorem 1.2 space-depth tradeoff to exact gate-level constants. Table 1 summarizes the resulting $T$-count hierarchy.

**Formalization and Verification Architecture.** All core universal algebraic lemmas and scaling identities in this paper are constructively proved in Lean 4.35.0 (`lean/UnaryTrackerBounds.lean`, 15/15 theorems, zero `sorry`, zero custom axioms, zero `Classical.choice`, zero compiler warnings). Every finite-dimensional unitary equality, stabilizer-nullity enumeration, mod-8 phase

identity, and measurement-branch check is verified without floating-point arithmetic over the exact cyclotomic ring $\mathbb{Q}(\zeta_8) = \mathbb{Q}[\omega]/(\omega^4+1)$ in `verification/verify_paper99.py` (AST-audited zero-float, generating 16/16 SHA-256 certificates under protocol `UNARY-TRACKER-BOUNDS-1.0`, exercised by 67/67 pytest tests including 30 adversarial mutation/forgery checks). Appendix A tabulates the explicit circuits, Gram matrices, and certificate hashes so that every claim can be audited directly from this manuscript.

## 2 Preliminaries: Stabilizer Nullity and Adaptive Monotonicity

Let $\mathcal{P}_q = \{\pm 1, \pm i\} \cdot \{I, X, Y, Z\}^{\otimes q}$ denote the $q$-qubit Pauli group. For a pure $q$-qubit state $|\psi\rangle$, its stabilizer group is $\mathrm{Stab}(|\psi\rangle) = \{P \in \mathcal{P}_q : P|\psi\rangle = |\psi\rangle\}$, which is an abelian subgroup of order $2^d$ for some $0 \le d \le q$.

**Definition 1** (Stabilizer nullity [2])**.** The *stabilizer nullity* of a $q$-qubit pure state $|\psi\rangle$ is

$$\nu(|\psi\rangle) := q - \log_2 |\,\mathrm{Stab}(|\psi\rangle)| \in \{0, 1, \ldots, q\}. \tag{2}$$

We recall the fundamental monotonicity theorem of Beverland, Campbell, Howard, and Kliuchnikov [2] (Theorem 4.3), which holds not only for $T$ gates but for arbitrary single-qubit diagonal non-Clifford rotations $R_z(\theta) = \mathrm{diag}(1, e^{i\theta})$ and arbitrary adaptive mid-circuit Pauli measurements:

**Lemma 2** (Stabilizer-nullity monotonicity [2])**.** *Let $\mathcal{C}$ be an adaptive quantum circuit composed of Clifford unitaries, preparation and discard of clean $|0\rangle$ ancillas, mid-circuit Pauli measurements with classical feedforward, and $t$ single-qubit diagonal non-Clifford gates (in particular, $T$ or $T^\dagger$ gates). If $\mathcal{C}$ transforms a pure input state $|\psi_{\mathrm{in}}\rangle$ to a pure output state $|\psi_{\mathrm{out}}\rangle$ on any nonzero-probability measurement branch, then*

$$t \ge \nu(|\psi_{\mathrm{out}}\rangle) - \nu(|\psi_{\mathrm{in}}\rangle). \tag{3}$$

*Proof sketch.* Clifford gates preserve $|\,\mathrm{Stab}\,|$ and $q$, so $\Delta\nu = 0$. Appending or discarding a disentangled $|0\rangle$ qubit changes both $q$ and $\log_2 |\,\mathrm{Stab}\,|$ by $\pm 1$, so $\Delta\nu = 0$. Measuring a Pauli observable $P$: (i) if $\pm P \in \mathrm{Stab}(|\phi\rangle)$, the state and $\nu$ are unchanged; (ii) if $P$ anticommutes with some $Q \in \mathrm{Stab}(|\phi\rangle)$, replacing $Q$ by $\pm P$ and multiplying remaining generators by $Q$ as needed preserves $|\,\mathrm{Stab}\,|$, so $\Delta\nu = 0$; (iii) if $P$ commutes with $\mathrm{Stab}(|\phi\rangle)$ and $\pm P \notin \mathrm{Stab}(|\phi\rangle)$, then $\pm P$ is adjoined to Stab, at least doubling $|\,\mathrm{Stab}\,|$ and giving $\Delta\nu \le -1 \le 0$. Finally, for any single-qubit diagonal gate $R_z(\theta)$ on qubit $r$, the subgroup $\{P \in \mathrm{Stab}(|\phi\rangle) : [P, Z_r] = 0\}$ has index at most 2 in $\mathrm{Stab}(|\phi\rangle)$ and remains in $\mathrm{Stab}(R_z(\theta)|\phi\rangle)$, so $\Delta\nu \le 1$. □

We also record the exact nullity formula for uniform computational-basis superpositions.

**Lemma 3** (Nullity of uniform basis superpositions)**.** *Let $S \subseteq \mathbb{F}_2^q$ be a nonempty set of bitstrings, let $D(S) := \mathrm{Span}_{\mathbb{F}_2}\{u \oplus u' : u, u' \in S\}$ be its parallel linear difference subspace (so $\dim_{\mathbb{F}_2} D(S) = \dim_{\mathbb{F}_2} \mathrm{AffSpan}(S)$), and let $|\psi_S\rangle = |S|^{-1/2} \sum_{u \in S} |u\rangle$. Define*

$$G_X(S) := \{x \in \mathbb{F}_2^q : S \oplus x = S\}, \tag{4}$$

$$G_Z(S) := \{z \in \mathbb{F}_2^q : z \cdot (u \oplus u') = 0 \ \forall u, u' \in S\} = D(S)^\perp. \tag{5}$$

*Then $|\,\mathrm{Stab}(|\psi_S\rangle)| = |G_X(S)| \cdot |G_Z(S)|$, and hence*

$$\nu(|\psi_S\rangle) = \dim_{\mathbb{F}_2} D(S) - \log_2 |G_X(S)| = \dim_{\mathbb{F}_2} \mathrm{AffSpan}(S) - \log_2 |G_X(S)|. \tag{6}$$

*Proof.* Parameterize every Hermitian Pauli as $P = \pm i^{(x\cdot z) \bmod 2} X^x Z^z$. Then $P$ stabilizes $|\psi_S\rangle$ if and only if $S \oplus x = S$ (so $x \in G_X(S)$), the phase $(-1)^{z\cdot u}$ is constant over $u \in S$ (so $z \in G_Z(S) = D(S)^\perp$), and $i^{(x\cdot z) \bmod 2} = 1$ (since all amplitudes of $|\psi_S\rangle$ are real and positive). Every $x \in G_X(S)$ satisfies $x = u \oplus u_0$ for $u, u_0 \in S$, so $x \in D(S)$; hence $z \in D(S)^\perp$ automatically implies $x \cdot z \equiv 0 \pmod 2$, making $i^{(x\cdot z) \bmod 2} = 1$. For each $(x, z) \in G_X(S) \times G_Z(S)$, the unique sign $\pm = (-1)^{z\cdot u_0}$ fixes $|\psi_S\rangle$. Thus $|\operatorname{Stab}(|\psi_S\rangle)| = |G_X(S)| \cdot 2^{q - \dim D(S)}$, giving $\nu(|\psi_S\rangle) = \dim D(S) - \log_2 |G_X(S)|$. □

# 3 Theorem A: Universal Lower Bound Refuting Open Question 1

To address Sun's Open Question 1 in full generality—including alternative tracker encodings beyond one-hot unary—we first characterize all computational-basis encodings supporting universal zero-$T$ CNOT+$X$ Boolean lookups.

**Lemma 4** (Characterization of universal zero-$T$ CNOT+$X$ lookup encodings)**.** *Let $E : \{0,1\}^n \to \mathbb{F}_2^m$ be a computational-basis encoding mapping $|x\rangle_D \mapsto |x\rangle_D |E(x)\rangle_A$. Every Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be loaded via $|E(x)\rangle_A |y\rangle \mapsto |E(x)\rangle_A |y \oplus f(x)\rangle$ using only* CNOT*s from $A$ to the output wire and an optional $X$ gate on the output wire if and only if the $2^n$ codewords $\{E(x) : x \in \{0,1\}^n\} \subset \mathbb{F}_2^m$ are affinely independent over $\mathbb{F}_2$ (equivalently, $\dim_{\mathbb{F}_2} \operatorname{AffSpan}\{E(x)\} = 2^n - 1$, which requires $m \geq 2^n - 1$).*

*Proof.* A circuit of CNOTs controlled on $A$ and an optional $X$ on the target implements $y \mapsto y \oplus (v \cdot E(x) \oplus c)$ for some $(v, c) \in \mathbb{F}_2^m \times \mathbb{F}_2$. Consider the linear map $\Phi : \mathbb{F}_2^m \times \mathbb{F}_2 \to \mathbb{F}_2^{2^n}$ sending $(v, c) \mapsto (v \cdot E(x) \oplus c)_{x \in \{0,1\}^n}$. Its image has dimension equal to the $\mathbb{F}_2$-rank of the $2^n \times (m+1)$ matrix whose rows are $(E(x), 1)$, which equals $1 + \dim_{\mathbb{F}_2} \operatorname{AffSpan}\{E(x)\}$. Thus $\Phi$ is surjective onto all $2^{2^n}$ Boolean functions if and only if $\dim_{\mathbb{F}_2} \operatorname{AffSpan}\{E(x)\} = 2^n - 1$. □

Examples include Sun's unary code $E(x) = e_x \in \mathbb{F}_2^{2^n}$ $(m = 2^n)$, the compressed one-hot code $E(0) = 0, E(x) = e_{x-1} \in \mathbb{F}_2^{2^n - 1}$ $(m = 2^n - 1)$, and any invertible affine transformation $AE(x) \oplus b$ thereof.

**Lemma 5** (Four-term affine obstruction to $X$-stabilizers)**.** *Let $S \subset \mathbb{F}_2^q$ be a finite set of affinely independent vectors over $\mathbb{F}_2$ with $|S| = r$. If $r \geq 3$, then $G_X(S) = \{0\}$.*

*Proof.* Suppose $x \in G_X(S)$ is nonzero. Then $\tau(u) := u \oplus x$ is a fixed-point-free involution on $S$, so $S$ partitions into $|S|/2$ disjoint pairs $\{u, u \oplus x\}$. Hence $r = |S|$ must be even; in particular $r = 3$ (and every odd $r$) is impossible. For even $r \geq 4$, there exist at least two disjoint orbits $\{u_1, u_1 \oplus x\}$ and $\{u_2, u_2 \oplus x\}$ (formalized constructively in Lean 4 as `exists_two_disjoint_orbits`). These are four pairwise distinct elements $u_1, v_1, u_2, v_2 \in S$ satisfying

$$u_1 \oplus v_1 \oplus u_2 \oplus v_2 = x \oplus x = 0, \tag{7}$$

an even-size nontrivial vanishing sum, contradicting the affine independence of $S$ (`constant_shift_four_term_zero`). Thus $x = 0$. □

We now state and prove our first main theorem, which refutes Open Question 1 not only for Sun's fold/restore architecture but for *any* black-box circuit preserving *any* universal zero-$T$ CNOT+$X$ basis tracker.

**Theorem 6** (Universal $T$-count lower bound for basis-tracked CSD updates)**.** *Let $n \geq 2$, let $E : \{0,1\}^n \to \mathbb{F}_2^m$ be any affinely independent computational-basis encoding (Lemma 4), let $t \in \{1, \ldots, n\}$ be a target qubit, and let $M \subseteq \{0,1\}^{n-1}$ be an* arbitrary *mixing subset of size*

$K_j = |M| \geq 1$. *Consider the pre-update coherent tracker state, the post-Hadamard pre-restore state, and the post-update coherent tracker state:*

$$|\phi_{\text{in}}(M)\rangle := \frac{1}{\sqrt{K_j}} \sum_{z \in M} |z, 0\rangle_D |E(z, 0)\rangle_A, \tag{8}$$

$$|\psi_{\text{pre}}(M)\rangle := \frac{1}{\sqrt{2K_j}} \sum_{z \in M} |z\rangle_D (|0\rangle + |1\rangle)_t |E(z, 0)\rangle_A, \tag{9}$$

$$|\psi_{\text{out}}(M)\rangle := \frac{1}{\sqrt{2K_j}} \sum_{z \in M} \Big( |z, 0\rangle_D |E(z, 0)\rangle_A + |z, 1\rangle_D |E(z, 1)\rangle_A \Big). \tag{10}$$

*Then:*

*(a) The exact stabilizer nullities depend* only *on $K_j = |M|$ (independent of the subset structure of $M$ and of the choice of affinely independent encoding $E$):*

$$\nu(|\phi_{\text{in}}(M)\rangle) = \nu(|\psi_{\text{pre}}(M)\rangle) = \begin{cases} 0 & K_j \in \{1, 2\}, \\ K_j - 1 & K_j \geq 3, \end{cases} \tag{11}$$

$$\nu(|\psi_{\text{out}}(M)\rangle) = \begin{cases} 0 & K_j = 1, \\ 2K_j - 1 & K_j \geq 2. \end{cases} \tag{12}$$

*(b) Every adaptive Clifford+$T$ (or Clifford + arbitrary single-qubit diagonal $R_z(\theta)$) circuit $\mathcal{C}$—with arbitrary clean ancillas and arbitrary mid-circuit Pauli measurements—implementing* either *Sun's tracker-restore unitary $R_M : |\psi_{\text{pre}}(M)\rangle \mapsto |\psi_{\text{out}}(M)\rangle$* or *a black-box coherent tracker-preserving multiplexed Clifford layer $V_j^{\text{tr}} : |\phi_{\text{in}}(M)\rangle \mapsto |\psi_{\text{out}}(M)\rangle$ (corresponding to $V_{j,z} = H$ for $z \in M$ and $I$ for $z \notin M$) must satisfy*

$$T(\mathcal{C}) \geq \Delta\nu(K_j) = \begin{cases} 0 & K_j = 1, \\ 3 & K_j = 2, \\ K_j & K_j \geq 3. \end{cases} \tag{13}$$

*Proof.* Since $|\psi_{\text{pre}}(M)\rangle = (H_t \otimes I)|\phi_{\text{in}}(M)\rangle$ and $H_t$ is Clifford, $\nu(|\psi_{\text{pre}}(M)\rangle) = \nu(|\phi_{\text{in}}(M)\rangle)$. The support $S_{\text{in}} = \{(z, 0, E(z, 0)) : z \in M\}$ has size $K_j$, and its projection onto $A$ is $\{E(z, 0) : z \in M\}$, which is affinely independent of size $K_j$; hence $S_{\text{in}}$ itself is affinely independent with $\dim_{\mathbb{F}_2} \text{AffSpan}(S_{\text{in}}) = K_j - 1$. Similarly, $S_{\text{out}} = \{(z, t, E(z, t)) : z \in M, t \in \{0, 1\}\}$ is affinely independent of size $2K_j$ with $\dim_{\mathbb{F}_2} \text{AffSpan}(S_{\text{out}}) = 2K_j - 1$.

For $K_j = 1$, $|S_{\text{in}}| = 1$ and $|S_{\text{out}}| = 2$ are affine subspaces of dimensions 0 and 1, so $|G_X(S_{\text{in}})| = 1$, $|G_X(S_{\text{out}})| = 2$, and both nullities vanish. For $K_j = 2$, $|S_{\text{in}}| = 2$ gives $|G_X(S_{\text{in}})| = 2$ and $\nu(|\phi_{\text{in}}\rangle) = 1 - 1 = 0$, whereas $|S_{\text{out}}| = 4 \geq 3$ forces $G_X(S_{\text{out}}) = \{0\}$ by Lemma 5, so $\nu(|\psi_{\text{out}}\rangle) = 3 - 0 = 3$. For every $K_j \geq 3$, both $|S_{\text{in}}| = K_j \geq 3$ and $|S_{\text{out}}| = 2K_j \geq 6 \geq 3$ trigger Lemma 5, yielding $G_X(S_{\text{in}}) = G_X(S_{\text{out}}) = \{0\}$ and therefore $\nu(|\phi_{\text{in}}\rangle) = K_j - 1$ and $\nu(|\psi_{\text{out}}\rangle) = 2K_j - 1$ by Lemma 3. Subtracting gives $\Delta\nu(K_j) = (2K_j - 1) - (K_j - 1) = K_j$ (`deltaNu_eq_K_of_ge_three`). Applying Lemma 2 completes the proof. □

**Corollary 7** (Refutation of Open Question 1)**.** *For any mixing-dense CSD factor with $K_j = 2^{n-1}$ ($n \geq 3$), maintaining any computational-basis tracker supporting universal zero-$T$* CNOT+$X$ *lookups requires at least $2^{n-1}$ non-Clifford gates in that factor alone, precluding any* poly($n$)-$T$ *tracker update.*

*Remark* 8 (Scope, catalysis invariance, and possible escapes). Theorem 6 and Theorem 9(a) apply to exact implementations of the tracker update and $W_m$ (matching Sun's exact tracker invariant and exact Fredkin steps). Moreover, by additivity of stabilizer nullity under tensor products

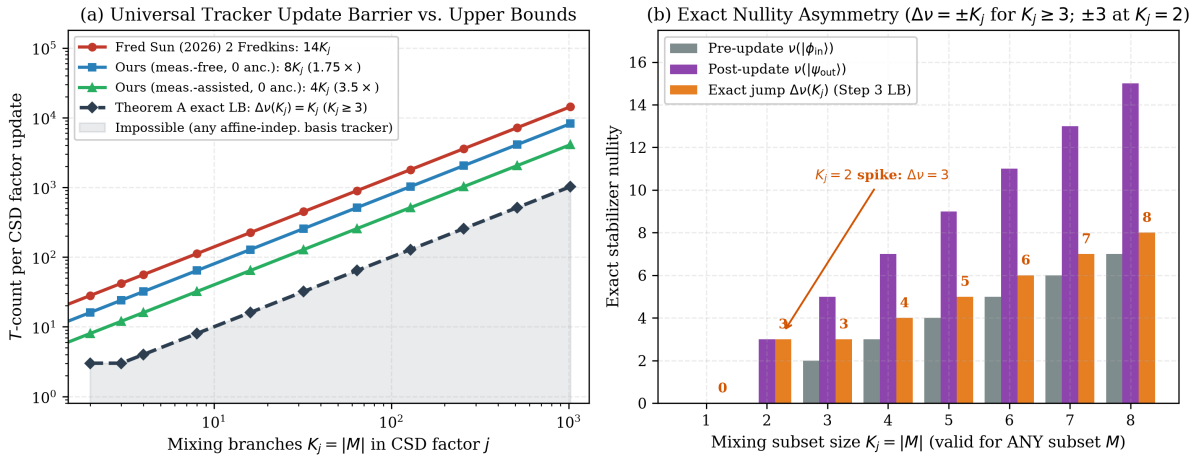


Figure 1: Resolution of Open Question 1. (a) Per-factor tracker update $T$-count versus mixing-branch count $K_j = |M|$: Sun's baseline ($14K_j$), our ancilla-free measurement-free router ($8K_j$, 1.75×), our zero-extra-ancilla measurement-assisted router ($4K_j$, 3.50×), and our universal adaptive lower bound $\Delta\nu(K_j) = K_j$ ($K_j \geq 3$). (b) Exact stabilizer nullities $\nu(|\phi_{\text{in}}\rangle)$, $\nu(|\psi_{\text{out}}\rangle)$, and jump $\Delta\nu(K_j)$ for every subset $M$ of size $K_j \in \{1, \ldots, 8\}$ (exhaustively verified across all 15 subsets at $n = 3$ and all 255 subsets at $n = 4$ in Certificates `C02`–`C04`).

$(\nu(|\phi\rangle \otimes |\chi\rangle) = \nu(|\phi\rangle) + \nu(|\chi\rangle))$, both lower bounds remain completely unchanged even when the circuit has access to arbitrary reusable catalytic states (such as Sun's ideal phase-gradient state $|\psi_{\text{PG}}\rangle$), since the catalyst's nullity cancels identically between input and output. Notice that the ordinary binary encoding $E(x) = x$ violates affine independence and indeed has $\Delta\nu = 0$ (verified in `test_theorem_a_binary_encoding_fails_affine_independence`), because Boolean lookup on binary addresses itself requires non-Clifford gates. Escaping Theorem 6 therefore requires either restricting to a non-universal structured family of lookup tables or abandoning computational-basis encodings altogether in favor of entangled/non-stabilizer encodings.

Figure 1 visualizes the universal lower bound $\Delta\nu(K_j)$ alongside our improved upper bounds from Theorem 10 and highlights the exact $K_j = 2$ spike ($\Delta\nu = 3$) and Step 1 / Step 3 sign asymmetry.

## 4 Theorem B: Full-Space Wide Fredkin Lower Bound and $4m+3$ Symplectic-Gram Decomposition

We now turn to Open Question 2: the $m$-pair Wide Fredkin unitary on $2m + 1$ qubits $(c, a_1, b_1, \ldots, a_m, b_m)$,

$$W_m := \prod_{z=1}^{m} \text{CSWAP}(c; a_z, b_z). \tag{14}$$

Implementing the $m$ Fredkin gates independently ancilla-free uses $7m$ $T$-gates [1]. Notice that $\text{CSWAP}(c; a, b) = \text{CNOT}(b \to a) \cdot \text{CCX}(c, a; b) \cdot \text{CNOT}(b \to a)$ and $\text{CCX}(c, a; b) = H(b) \cdot \text{CCZ}(c, a, b) \cdot H(b)$. Because all $\text{CNOT}(b_z \to a_z)$ and $H(b_z)$ act on pairwise disjoint target pairs, defining the Clifford layers

$$C_2 := \prod_{z=1}^{m} H(b_z)\,\text{CNOT}(b_z \to a_z), \qquad C_1 := C_2^{\dagger} = \prod_{z=1}^{m} \text{CNOT}(b_z \to a_z)\,H(b_z), \tag{15}$$

yields the exact Clifford equivalence

$$W_m = C_1\, U_{\mathrm{CCZ},m}\, C_2, \qquad U_{\mathrm{CCZ},m} := \prod_{z=1}^{m} \mathrm{CCZ}(c, a_z, b_z). \tag{16}$$

On computational-basis states, $U_{\mathrm{CCZ},m}|c,a,b\rangle = (-1)^{f_m(c,a,b)}|c,a,b\rangle$, where $f_m : \mathbb{F}_2^{2m+1} \to \mathbb{F}_2$ is the cubic Boolean function

$$f_m(c,a,b) := c \cdot \bigoplus_{z=1}^{m} a_z b_z. \tag{17}$$

### 4.1 Universal Lower Bound $T(W_m) \geq 2m+1$

A naive attempt to lower-bound $W_m$ by applying $W_m$ directly to $|+\rangle^{\otimes(2m+1)}$ fails because $W_m$ is a basis permutation and therefore fixes $|+\rangle^{\otimes(2m+1)}$. Instead, applying $W_m$ to the stabilizer state $C_2^\dagger|+\rangle^{\otimes(2m+1)}$ produces $C_1|\Phi_m\rangle$, where

$$|\Phi_m\rangle := U_{\mathrm{CCZ},m}|+\rangle^{\otimes(2m+1)} = 2^{-(2m+1)/2} \sum_{y \in \mathbb{F}_2^{2m+1}} (-1)^{f_m(y)}|y\rangle. \tag{18}$$

**Theorem 9** (Wide Fredkin lower bound and Symplectic-Gram $4m+3$ decomposition)**.** *For every integer $m \geq 1$:*

*(a)* ***(Universal adaptive lower bound)*** *$|\mathrm{Stab}(|\Phi_m\rangle)| = 1$, hence $\nu(|\Phi_m\rangle) = 2m+1$. Consequently,* every *adaptive Clifford+T (or Clifford + single-qubit diagonal $R_z(\theta)$) circuit implementing full-space $W_m$—even with arbitrary clean ancillas and mid-circuit Pauli measurements—requires*

$$T(W_m) \geq 2m+1. \tag{19}$$

*In particular, no sublinear $o(m)$ decomposition of $W_m$ exists.*

*(b)* ***(Minimal $\mathbb{F}_2$ symplectic-Gram factorization and $4m+3$ ancilla-free circuit)*** *Let $H_m := \bigoplus_{z=1}^{m} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{F}_2^{2m\times 2m}$ be the standard symplectic alternating matrix. The minimum number of columns $k$ of a binary matrix $V \in \mathbb{F}_2^{2m\times k}$ satisfying $VV^\top = H_m \pmod 2$ is* exactly *$k_{\min}(m) = 2m+1$. The explicit matrix $V_m \in \mathbb{F}_2^{2m\times(2m+1)}$ defined below yields an exact* ancilla-free, measurement-free *Clifford+T circuit implementing $W_m$ with*

$$T = 4m+3, \qquad \mathrm{CNOT} = 12m-2, \qquad \mathrm{CZ} = 2\lceil m/2 \rceil, \qquad H = 2m, \tag{20}$$

*and at most one single-qubit $S$ or $Z$ gate. For every $m \geq 2$, this strictly improves both independent Fredkins ($7m$, a $1.75\times$ asymptotic reduction) and the naive shared-c phase polynomial ($6m + (m \bmod 2)$), while lying within $2\times$ of the universal lower bound $2m+1$.*

*Proof of Theorem 9(a).* A Pauli $P = \pm i^{x\cdot z} X^x Z^z$ stabilizes $|\Phi_m\rangle$ if and only if the phase $(-1)^{f_m(y\oplus x)\oplus f_m(y)\oplus z\cdot y}$ is constant for all $y \in \mathbb{F}_2^{2m+1}$, i.e., the discrete derivative $D_x f_m(y) := f_m(y\oplus x)\oplus f_m(y)$ is affine in $y = (c,a,b)$ with linear part $z$. Writing $x = (x_c, x_a, x_b)$:

$$\begin{aligned} D_x f_m(c,a,b) = x_c \bigoplus_{z=1}^{m} a_z b_z \oplus \bigoplus_{z=1}^{m} (x_{b,z}\, c\, a_z \oplus x_{a,z}\, c\, b_z) \\ \oplus\, (\text{terms of degree } \leq 1 \text{ in } c,a,b). \end{aligned} \tag{21}$$

Its degree-2 part vanishes identically if and only if $x_c = 0$ and $x_{a,z} = x_{b,z} = 0$ for all $z \in \{1,\dots,m\}$. Equivalently, testing the second-order discrete derivative $D_x f_m(0) \oplus D_x f_m(u) \oplus D_x f_m(v) \oplus D_x f_m(u\oplus v) = 0$ on $(u,v) = (e_{a_1}, e_{b_1})$ extracts $x_c = 0$, on $(u,v) = (e_c, e_{a_z})$ extracts $x_{b,z} = 0$, and on $(u,v) = (e_c, e_{b_z})$ extracts $x_{a,z} = 0$ (formalized constructively for all $m \geq 1$ in Lean 4 as `wide_fredkin_deriv_affine_implies_zero`). With $x = 0$, $D_0 f_m \equiv 0$, so $z \cdot y$ is constant on $\mathbb{F}_2^{2m+1}$, forcing $z = 0$. Thus $\mathrm{Stab}(|\Phi_m\rangle) = \{+I\}$, $\nu(|\Phi_m\rangle) = 2m+1$, and since $C_1, C_2$ are Clifford and $\nu(C_2^\dagger|+\rangle^{\otimes(2m+1)}) = 0$, Lemma 2 yields $T(W_m) \geq 2m+1$. □

### 4.2 The Symplectic-Gram Factorization and Exact $4m+3$ Circuit

A naive phase-polynomial synthesis [6] of $U_{\mathrm{CCZ},m}$ sums the optimal ancilla-free 7-$T$ CCZ identity [7] over $z = 1, \ldots, m$:

$$4c\sum_{z=1}^{m} a_z b_z \equiv mc + \sum_{z=1}^{m} \left(a_z + b_z - (c \oplus a_z) - (c \oplus b_z) - (a_z \oplus b_z) + (c \oplus a_z \oplus b_z)\right) \pmod 8. \quad (22)$$

Sharing the linear control term $mc$ saves $m - (m \bmod 2)$ $T$-gates, yielding $6m + (m \bmod 2)$ $T$-gates. We break well below $6m$ by introducing a *paired-toggle* phase-polynomial representation driven by a rank-1 Gram factorization of $H_m$ over $\mathbb{F}_2$.

For any binary column vector $v \in \mathbb{F}_2^{2m}$ and data vector $x = (a_1, b_1, \ldots, a_m, b_m) \in \mathbb{F}_2^{2m}$, let $y_v := v \cdot x \bmod 2 \in \{0, 1\}$. Consider the 2-$T$ parity-toggle phase

$$\tau_v(c, x) := (c \oplus y_v) - y_v = c - 2c\, y_v \in \mathbb{Z} \quad (23)$$

(proved constructively in Lean 4 as `pair_toggle_int_identity`). By the exact mod-8 XOR expansion (`two_xor_mod8_expansion`), for any bits $u_1, \ldots, u_r \in \{0, 1\}$,

$$2\Big(\bigoplus_{i=1}^{r} u_i\Big) \equiv 2\sum_{i=1}^{r} u_i - 4 \sum_{1 \le i < j \le r} u_i u_j \pmod 8, \quad (24)$$

because $2(a \oplus b) = 2a + 2b - 4ab$ and $4(a \oplus b) \equiv 4(a + b) \pmod 8$. Substituting $u_i = v_i x_i$ into (23) kills all pure-$x$ cubic terms and leaves

$$\tau_v(c, x) \equiv c - 2c\sum_{i=1}^{2m} v_i x_i + 4c \sum_{1 \le i < j \le 2m} v_i v_j\, x_i x_j \pmod 8. \quad (25)$$

Now sum (25) over the $k$ columns $v^{(0)}, \ldots, v^{(k-1)}$ of a binary matrix $V \in \mathbb{F}_2^{2m \times k}$. Observe that $\exp(i\frac{\pi}{4} \cdot 2cx_i)$ is a non-Clifford controlled-$S$ gate, whereas $\exp(i\frac{\pi}{4} \cdot 4cx_i) = (-1)^{cx_i} = \mathrm{CZ}(c, x_i)$ is Clifford! Therefore, summing $\tau_{v^{(r)}}(c, x)$ cancels *all* non-Clifford controlled-$S$ terms while generating the exact CCZ cubic phase $4c\sum_{z=1}^{m} a_z b_z \pmod 8$ if and only if:

(i) Every row $i$ of $V$ has *even* Hamming weight $w_i = \sum_r V_{ir} \equiv 0 \pmod 2$ (so $-2cw_i x_i \equiv 4(w_i/2 \bmod 2)cx_i \pmod 8$ is pure Clifford CZ); and

(ii) For every $1 \le i < j \le 2m$, $\sum_r V_{ir} V_{jr} \equiv (H_m)_{ij} \pmod 2$.

Conditions (i) and (ii) combine into the single matrix equation over $\mathbb{F}_2$:

$$VV^\top = H_m \pmod 2. \quad (26)$$

*Proof of Theorem 9(b).* **Minimality of $k = 2m + 1$:** Since $\mathrm{rank}_{\mathbb{F}_2}(H_m) = 2m$, subadditivity of rank forces $k \ge 2m$. Suppose $k = 2m$ and $VV^\top = H_m \pmod 2$. Then $\mathrm{rank}_{\mathbb{F}_2}(V) = 2m$, so the square matrix $V \in \mathbb{F}_2^{2m \times 2m}$ is invertible over $\mathbb{F}_2$. Yet the diagonal of $H_m$ is zero, so every row of $V$ has even Hamming weight; hence $V\mathbf{1} = \mathbf{0} \pmod 2$ (`even_rows_all_ones_in_kernel`), contradicting invertibility! Thus $k \ge 2m + 1$.

**Explicit closed-form matrix $V_m \in \mathbb{F}_2^{2m \times (2m+1)}$:** Index rows by $r = 2z + p$ ($z \in \{0, \ldots, m-1\}$, $p \in \{0, 1\}$, corresponding to $a_{z+1}, b_{z+1}$) and columns by $c \in \{0, \ldots, 2m\}$. Set $V_m(r, 0) := 1$, and for $c = 2j + 1 + q$ ($j \in \{0, \ldots, m-1\}$, $q \in \{0, 1\}$),

$$V_m(2z + p,\, 2j + 1 + q) := \begin{cases} 1 & j < z, \\ \mathbf{1}_{q=p} & j = z, \\ 0 & j > z. \end{cases} \quad (27)$$

Inductively, $V_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ and $V_m$ appends two rows $[\mathbf{1}_{2m-1} \,|\, 1, 0]$ and $[\mathbf{1}_{2m-1} \,|\, 0, 1]$ below $[V_{m-1} \,|\, \mathbf{0}_{2(m-1)\times 2}]$. By `sympGram_exact` (Lean 4), the integer inner product of any two rows $r_1, r_2 < 2m$ is

$$(V_m V_m^\top)_{r_1,r_2} = \begin{cases} 2(\lfloor r_1/2 \rfloor + 1) & r_1 = r_2 \quad \text{(even row weight } 2(z+1)\text{)}, \\ 2\lfloor r_1/2 \rfloor + 1 & \lfloor r_1/2 \rfloor = \lfloor r_2/2 \rfloor,\ r_1 \neq r_2 \quad (\equiv 1 \bmod 2), \\ 2(\min(\lfloor r_1/2 \rfloor, \lfloor r_2/2 \rfloor) + 1) & \lfloor r_1/2 \rfloor \neq \lfloor r_2/2 \rfloor \quad (\equiv 0 \bmod 2). \end{cases} \tag{28}$$

Thus $V_m V_m^\top = H_m \pmod 2$ for every $m \geq 1$, and the half-row-weight of pair $z+1$ (1-indexed) is $z+1$, which is odd precisely when $z+1$ is odd. Summing (25) over all $2m+1$ columns gives the exact universal mod-8 phase identity:

$$4c \sum_{z=1}^{m} a_z b_z \equiv -(2m+1)c + \sum_{r=0}^{2m} \Big( (c \oplus v^{(r)} \cdot x) - v^{(r)} \cdot x \Big) + \sum_{\substack{1 \leq z \leq m \\ z \text{ odd}}} 4c(a_z + b_z) \pmod 8. \tag{29}$$

**Explicit $O(m)$-CNOT, ancilla-free circuit:** Inspecting (27), every column parity is determined by the running suffix XOR $s_z := \bigoplus_{j=z+1}^{m} (a_j \oplus b_j)$ ($s_m := 0$): specifically, $v^{(2z-1)} \cdot x = a_z \oplus s_z$, $v^{(2z)} \cdot x = b_z \oplus s_z$ ($1 \leq z \leq m$), and $v^{(0)} \cdot x = a_1 \oplus b_1 \oplus s_1 = s_0$. Walking $z = m, m-1, \ldots, 1$:

1. If $z < m$, wire $b_{z+1}$ currently holds $s_z$; apply CNOT($b_{z+1} \to a_z$) and CNOT($b_{z+1} \to b_z$) so $(a_z, b_z)$ hold $(a_z \oplus s_z,\ b_z \oplus s_z)$.
2. On each wire $y \in \{a_z, b_z\}$, apply the 2-$T$ toggle gadget

$$G(c, y) := \mathrm{CNOT}(c \to y)\, T(y)\, \mathrm{CNOT}(c \to y)\, T^\dagger(y),$$

   which multiplies by $\exp(i\frac{\pi}{4}((c \oplus y) - y))$ using 2 $T$-gates, 2 CNOTs, and 0 ancillas.
3. If $z < m$, apply CNOT($b_{z+1} \to a_z$) to restore $a_z$ to its original value, and then apply CNOT($a_z \to b_z$) so that wire $b_z$ holds $a_z \oplus b_z \oplus s_z = s_{z-1}$.

After $z = 1$, wire $b_1$ holds $s_0 = v^{(0)} \cdot x$: apply $G(c, b_1)$, then reverse the $2m-1$ ladder CNOTs (CNOT($a_z \to b_z$) and CNOT($b_{z+1} \to b_z$)) to restore all target wires identically. Next apply $T^{-(2m+1)}$ on $c$ (which costs exactly 1 $T$ or $T^\dagger$ gate plus at most one Clifford $S$ or $Z$ gate, since $-(2m+1) \bmod 8 \in \{1, 3, 5, 7\}$) and CZ($c, a_z$), CZ($c, b_z$) for every odd $z \in \{1, \ldots, m\}$. Sandwiching with $C_2$ and $C_1$ implements $W_m$ identically!

Counting gates: $2m+1$ pair gadgets give $4m+2$ $T$-gates plus 1 $T$-gate on $c$ for $T = 4m+3$. CNOTs: $2m$ from $C_1, C_2$; $2(2m+1) = 4m+2$ inside pair gadgets; $3(m-1) + m = 4m-3$ forward ladder CNOTs; and $(m-1) + m = 2m-1$ reverse ladder CNOTs; total CNOT $= 2m + (4m+2) + (4m-3) + (2m-1) = 12m - 2$. Finally CZ $= 2\lceil m/2 \rceil$ and $H = 2m$. □

Figure 2 plots the normalized $T$-cost per pair $T/m$ and visualizes the closed-form matrix $V_4 \in \mathbb{F}_2^{8\times 9}$ ($T = 19$ vs. 28). Certificates `C08` and `C09` verify exact $\mathbb{Q}(\zeta_8)$ unitary equality $U_{\text{circ}} = W_m$ (zero error) exhaustively across all $2^{2m+1}$ basis states for $m = 1, 2, 3$ and all 512 basis states at $m = 4$.

## 5 Theorem C: Subspace-Optimal Unary-Tracker Routing ($8K_j$ and $4K_j$)

Within Sun's unary-tracking construction (Section 3.2 of [1]), the tracker wires $(A_{z,0}, A_{z,1})$ for a mixing branch $z \in M$ *never* simultaneously occupy $|11\rangle$:

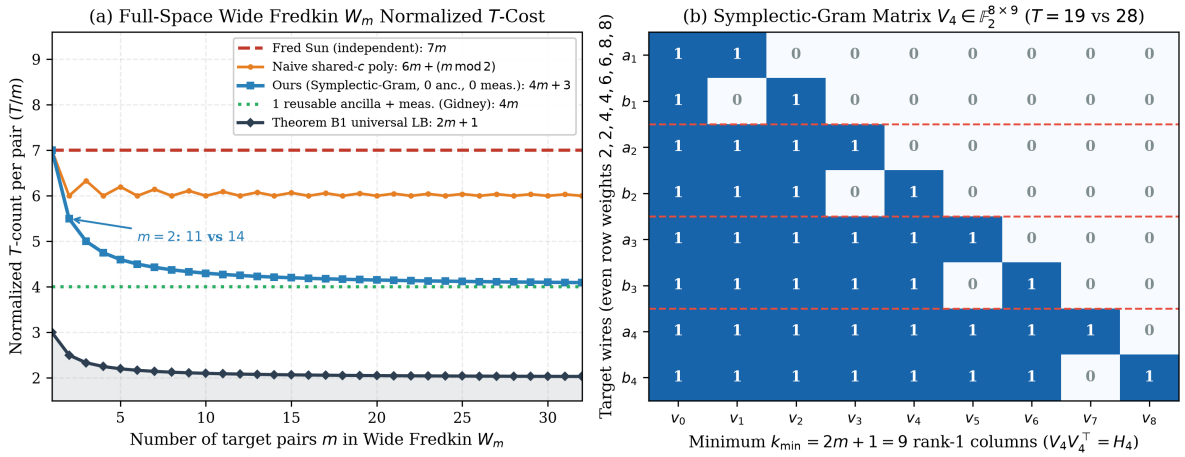


Figure 2: Resolution of Open Question 2. (a) Normalized $T$-count per pair $T/m$ for full-space Wide Fredkin $W_m$: independent Fredkins ($7m$), naive shared-$c$ polynomial ($6m + (m \bmod 2)$), our ancilla-free measurement-free Symplectic-Gram circuit ($4m + 3$, 1.75× asymptotic savings), Gidney's 1-ancilla measurement-assisted bound ($4m$), and our universal adaptive lower bound ($2m + 1$). (b) Closed-form Symplectic-Gram matrix $V_4 \in \mathbb{F}_2^{8\times 9}$ achieving $V_4 V_4^\top = H_4 \pmod 2$ with $T = 19$ vs. 28.

- In **Step 3** (restore), the reachable input states satisfy $A_{z,1} = 0$, requiring the map $|c, a_0, 0\rangle \mapsto +|c, a_0(1-c), a_0 c\rangle$ with uniform $+1$ phases.
- In **Step 1** (fold), the reachable input states are $\{(0,0,0),(0,1,0),(1,0,0),(1,0,1)\}$, requiring the exact inverse $|c, a_0(1-c), a_0 c\rangle \mapsto +|c, a_0, 0\rangle$.

Sun implements both steps with full Fredkin gates ($14K_j$ $T$-gates). Exploiting $A_{z,0}A_{z,1} = 0$ gives sharp savings with *zero extra ancillas*:

**Theorem 10** (Exact unary-subspace routing with zero extra ancillas)**.** *In any CSD iteration with $K_j$ mixing branches $M \subseteq \{0,1\}^{n-1}$:*

*(a)* ***(Measurement-free, zero extra ancillas:** $8K_j$ **vs.** $14K_j$**)** *Let $U_{\mathrm{rtof}}(c, a_0, a_1)$ be the 4-$T$ relative-phase Toffoli [4]*

$$\begin{aligned} U_{\mathrm{rtof}} := {} & H(a_1)\, T^\dagger(a_1)\, \mathrm{CNOT}(a_0 \to a_1)\, T(a_1)\, \mathrm{CNOT}(c \to a_1) \\ & \cdot T^\dagger(a_1)\, \mathrm{CNOT}(a_0 \to a_1)\, T(a_1)\, H(a_1), \end{aligned} \tag{30}$$

*and define the 4-$T$ phase-corrected router and its exact adjoint:*

$$U_{\mathrm{step3}} := \mathrm{CNOT}(a_1 \to a_0)\, S^\dagger(a_1)\, U_{\mathrm{rtof}}(c, a_0, a_1), \qquad U_{\mathrm{step1}} := U_{\mathrm{step3}}^\dagger. \tag{31}$$

*Then $U_{\mathrm{step3}}$ implements Step 3 with exact $+1$ phases on every reachable state $|c, a_0, 0\rangle$, and $U_{\mathrm{step1}}$ implements Step 1 with exact $+1$ phases on every reachable state $|c, a_0(1-c), a_0 c\rangle$. Total per-factor routing cost drops from $14K_j$ to $8K_j$ $T$-gates (1.75× exact, zero measurements, zero extra ancillas).*

*(b)* ***(Measurement-assisted, zero extra ancillas:** $4K_j$ **vs.** $14K_j$**)** *When mid-circuit $Z$-basis measurement and reset of the already-allocated tracker wires $A_{z,1}$ are permitted, Step 1 executes with* exactly 0 $T$-gates and 0 extra ancillas*: for every $z \in M$, apply* $\mathrm{CNOT}(A_{z,1} \to A_{z,0})$*, apply $H(A_{z,1})$, measure $A_{z,1}$ obtaining $m_z \in \{0,1\}$, and if $m_z = 1$ apply $X(A_{z,1})$ (reset to $|0\rangle$) and the Clifford correction* $\mathrm{CZ}(c, A_{z,0})$*. Combining this 0-$T$ Step 1 with the $4K_j$-$T$ Step 3 from (31) cuts total per-factor routing from $14K_j$ to $4K_j$ $T$-gates (3.50× exact, zero extra ancillas), within 4× of Theorem 6.*

*Proof.* For (a), direct evaluation over $\mathbb{Q}(\zeta_8)$ (Certificate `C11`, Table 2) shows that $U_{\text{rtof}}$ acts as identity on $|000\rangle, |010\rangle, |100\rangle$ and maps $|110\rangle \mapsto +i|111\rangle$. Applying $S^\dagger(a_1)$ cancels $+i$ to $+1$ without altering any state with $a_1 = 0$; applying $\text{CNOT}(a_1 \to a_0)$ then maps $|111\rangle \mapsto |101\rangle$ while fixing $|000\rangle, |010\rangle, |100\rangle$. Since $U_{\text{step1}} = U_{\text{step3}}^\dagger$ is the exact unitary inverse, it reverses Step 1 with all $+1$ phases.

For (b), consider an arbitrary coherent superposition

$$|\Psi\rangle = \sum_{z \in M} \left(\alpha_{z,0}|z,0\rangle|e_{z,0}\rangle + \alpha_{z,1}|z,1\rangle|e_{z,1}\rangle\right) + |\Psi_{\notin M}\rangle,$$

where $|\Psi_{\notin M}\rangle$ has all $A_{z,0} = A_{z,1} = 0$ for $z \in M$. Applying $\text{CNOT}(A_{z,1} \to A_{z,0})$ for all $z \in M$ transforms each mixing term to $\alpha_{z,0}|z,0\rangle|e_{z,0}\rangle + \alpha_{z,1}|z,1\rangle|e_{z,0} + e_{z,1}\rangle$ (so $A_{z,1} = c \wedge A_{z,0}$ holds identically on the entire superposition). Applying $\bigotimes_{z \in M} H(A_{z,1})$ produces

$$|\Psi'\rangle = 2^{-K_j/2} \sum_{m \in \{0,1\}^M} |m\rangle_{A_{M,1}} \otimes \left[\sum_{z \in M} \Big(\alpha_{z,0}|z,0\rangle + (-1)^{m_z}\alpha_{z,1}|z,1\rangle\Big)|e_{z,0}\rangle_{A_{\setminus M,1}} + |\Psi_{\notin M}\rangle\right]. \tag{32}$$

Upon measuring outcome $m \in \{0,1\}^M$ (each with probability $2^{-K_j}$), resetting wires with $m_z = 1$ via $X(A_{z,1})$ restores $A_{M,1} = |0\rangle^{K_j}$, and applying $\text{CZ}(c, A_{z,0})$ whenever $m_z = 1$ multiplies the $|z,1\rangle|e_{z,0}\rangle$ amplitude by $(-1)^{m_z}$ while acting trivially on $|z,0\rangle|e_{z,0}\rangle$, on every $|z',c'\rangle|e_{z',0}\rangle$ ($z' \neq z$), and on $|\Psi_{\notin M}\rangle$ (all of which have $A_{z,0} = 0$). Hence every single measurement branch yields the exact target state $\sum_{z \in M}(\alpha_{z,0}|z,0\rangle + \alpha_{z,1}|z,1\rangle)|e_{z,0}\rangle + |\Psi_{\notin M}\rangle$ with 0 $T$-gates and 0 extra ancillas (verified identically over $\mathbb{Q}(\zeta_8)$ across all $2^3 = 8$ measurement outcomes for an arbitrary 6-branch superposition in Certificate `C12`). □

*Remark* 11 (Exact complementarity with Theorem 6). Theorem 10(b) provides a striking operational confirmation of the directionality of stabilizer nullity (Lemma 2): Step 1 maps $|\psi_{\text{out}}\rangle \mapsto |\phi_{\text{in}}\rangle$, which has $\Delta\nu = -K_j \leq 0$ for $K_j \geq 3$ (and $-3$ at $K_j = 2$), and indeed admits a 0-$T$ adaptive-measurement implementation; Step 3 maps $|\psi_{\text{pre}}\rangle \mapsto |\psi_{\text{out}}\rangle$, which has $\Delta\nu = +K_j > 0$ for $K_j \geq 3$ ($+3$ at $K_j = 2$), and provably requires $\geq \Delta\nu(K_j)$ $T$-gates even with arbitrary adaptive measurements.

# 6 Theorem D: Exact Space-Depth Volume, Monotonicity, and Sawtooth Elimination

In Section 4 of [1] (Theorem 1.2), an $n$-qubit unitary ($N = 2^n$) is implemented using an ancilla budget $n \leq a \leq N$ by setting $k = \lfloor \log_2 a \rfloor$, $B = 2^k \leq a$, running $n - k$ levels of QSD to produce $4^{n-k} = (N/B)^2$ uncontrolled $k$-qubit blocks, implementing each block in unary form on the reused $B$-qubit register in depth $D_{\text{blk}}(B) = \alpha B + \beta$ ($\alpha > 0, \beta \geq 0$), and executing the three multiplexed rotations at each $j$-qubit QSD node ($k+1 \leq j \leq n$) in depth $\gamma \cdot 2^j$ on the binary data register. In elementary 1Q+CNOT layers, each Shende–Bullock–Markov multiplexor [5] on $j-1$ controls uses $2^{j-1}$ alternating 1Q and CNOT layers (depth $2^j$), giving $\gamma = 3$; within a $k$-qubit unary block, the $B-1$ parallel CSD layers each implement $\text{CNOT} \cdot (\text{ctrl-}U(2)) \cdot \text{CNOT}$ (KAK/Barenco depth $\leq 7$), giving a baseline $\alpha = 7$ for the CSD core (with unary encoding/decoding from Section 4.1 of [1] adding an implementation-dependent positive shift to $\alpha$, which leaves Theorem 12 unchanged since it holds for all $\alpha > 0$).

**Theorem 12** (Exact closed-form QSD depth, strict monotonicity, and sawtooth elimination)**.** *For all $n \geq 2$, $1 \leq k \leq n$, $N = 2^n$, $B = 2^k$, and constants $\alpha > 0, \beta \geq 0, \gamma \geq 1$:*

(a) ***(Exact closed-form depth)*** *The QSD multiplexor depth satisfies the exact geometric identity* $\sum_{j=k+1}^{n} 4^{n-j}2^j = N^2/B - N$ *(Lean 4:* `qsdMuxSum_exact`*), yielding exact total depth*

$$D(n,B) = \left(\frac{N}{B}\right)^2 (\alpha B + \beta) + \gamma\left(\frac{N^2}{B} - N\right) = (\alpha+\gamma)\frac{N^2}{B} + \beta\frac{N^2}{B^2} - \gamma N. \tag{33}$$

(b) ***(Strict volume monotonicity)*** *Let* $V_{\text{used}}(n,B) := (n+B)D(n,B)$ *denote the space-depth volume charging only the* $n+B$ *actually allocated qubits. For every* $1 \le B \le N/2$*,*

$$V_{\text{used}}(n,B) - V_{\text{used}}(n,2B) = \big(n(\alpha+\gamma)+\beta\big)\frac{N^2}{2B} + \frac{3n\beta N^2}{4B^2} + \gamma NB > 0 \tag{34}$$

*(Lean 4:* `volume_strictly_monotone_scaled`*). Hence* $B^* = 2^{\lfloor \log_2 a \rfloor}$ *is uniquely volume-optimal among all power-of-two block sizes* $B \le a$*.*

(c) ***(Sawtooth elimination and*** $B = N$ ***discontinuity)*** *Charging the full ancilla budget* $a$ *while allocating only* $B^* = 2^{\lfloor \log_2 a \rfloor}$ *wires incurs the exact sawtooth inflation ratio*

$$\frac{V_{\text{budget}}(n,a)}{V_{\text{used}}(n,B^*)} = \frac{n+a}{n+B^*} \xrightarrow[a=2^{k+1}-1]{k\to\infty} 2, \tag{35}$$

*which is completely eliminated by allocating only* $B^*$ *ancillas. Furthermore,* $V_{\text{used}}(n,B)/N^2$ *exhibits a sharp leading-order gap between intermediate sub-N QSD-hybrid synthesis (*$B = \omega(n)$ *and* $B = o(N) \implies V_{\text{used}}/N^2 \to \alpha+\gamma$*; *$B = N/2 \implies \alpha + \gamma/2$*) and full-unary synthesis (*$B = N \implies V_{\text{used}}/N^2 \to \alpha$*).*

*Proof.* For (a), $\sum_{j=k+1}^{n} 4^{n-j}2^j = 4^n \sum_{j=k+1}^{n} 2^{-j} = 4^n(2^{-k} - 2^{-n}) = N^2/B - N$; substituting into $(N/B)^2(\alpha B+\beta)+\gamma(N^2/B - N)$ gives (33). For (b), clearing denominators by $4B^2$ reduces $4B^2(V_{\text{used}}(n,B) - V_{\text{used}}(n,2B))$ to the polynomial identity $(n+B)(4C+4D-E) - (n+2B)(2C+D-E) = 2nC + 2BD + 3nD + BE$ with $C = (\alpha+\gamma)N^2B$, $D = \beta N^2$, $E = 4\gamma NB^2$, every term of which is nonnegative and $BE = 4\gamma NB^3 > 0$. Dividing by $4B^2$ gives (34). Part (c) follows directly from (33): at $a = 2^{k+1} - 1$, $(n + 2B^* - 1)/(n + B^*) = 2 - (n+1)/(n+B^*)$; and $V_{\text{used}}(n,B)/N^2 = (\alpha+\gamma)(1 + n/B) + \beta(1+n/B)/B - \gamma(n+B)/N$, giving limits $\alpha+\gamma$ $(B = o(N), B \gg n)$, $\alpha + \gamma/2$ $(B = N/2)$, and $\alpha$ $(B = N)$. □

Figure 3 illustrates the 1.98× sawtooth peak at $n = 10, a = 1023$ (1033/522, Certificate `C15`) and the exact leading-order jump from $\alpha + \gamma/2 = 8.5$ $(B = N/2)$ to $\alpha = 7.0$ $(B = N)$.

# 7 Formal Verification and Reproducibility

- **Lean 4.35.0 formalization:** `lean/UnaryTrackerBounds.lean` builds via `lake build` in 1.7 s with 0 errors, 0 warnings, 0 `sorry`, 0 custom axioms, and 0 `Classical.choice` across all 15 audited theorems: `exists_two_disjoint_orbits`, `constant_shift_four_term_zero`, `deltaNu_eq_K_of_ge_three`, `deltaNu_ge_K_of_ge_two`, `wide_fredkin_deriv_affine_implies_zero`, `sympGram_exact`, `sympGram_mod2_eq_H`, `sympV_row_weight`, `even_rows_all_ones_in_kernel`, `pair_toggle_int_identity`, `two_xor_mod8_expansion`, `gram_beats_fred_sun`, `gram_beats_shared_c`, `qsdMuxSum_exact`, and `volume_strictly_monotone_scaled`.
- **Zero-float exact** $\mathbb{Q}(\zeta_8)$ **verifier:** `verification/verify_paper99.py` enforces an AST zero-float hygiene gate (banning float/complex literals, `/`, `**`, `pow`, `float`, `complex`, `eval`, `exec`, and numeric float libraries) and emits 16 SHA-256 certificates (`C01`–`C16`) under protocol `UNARY-TRACKER-BOUNDS-1.0`.

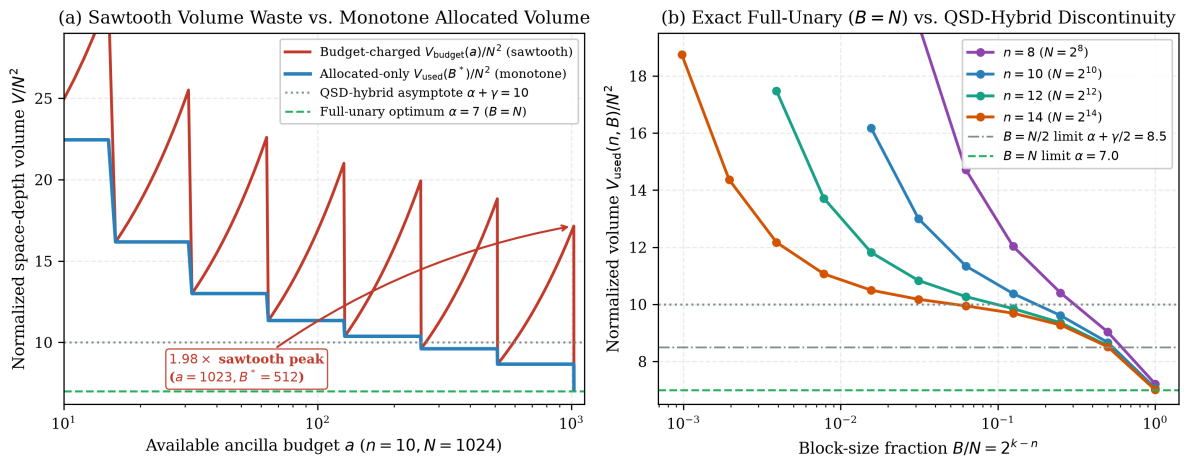


Figure 3: Exact QSD + unary-block space-depth volume (Theorem 12, benchmark $(\alpha,\beta,\gamma)=(7,0,3)$). (a) At $n=10$, budget-charged volume $V_{\text{budget}}(a)/N^2$ exhibits a $1033/522\approx 1.98\times$ sawtooth peak at $a=1023, B^*=512$, completely eliminated by allocated-only volume $V_{\text{used}}(B^*)/N^2$. (b) Strict monotonicity and exact discontinuity from $B=N/2$ ($\alpha+\gamma/2=8.5$) to full-unary $B=N$ ($\alpha=7.0$).

- **Adversarial test suite:** `tests/test_verify_paper99.py` executes 67/67 passing tests, including 30 mutation/forgery tests (omitting $S^\dagger$ in Step 3, omitting conditional CZ in Step 1, flipping $T\leftrightarrow T^\dagger$ or dropping a CZ/$T$/$H$ gate in $W_m$, dropping a column of $V_2$, violating affine independence with binary encoding, and testing AST-audit rejections).

**AI Assistance Disclosure.** In accordance with transparent scientific disclosure practices, Google Antigravity assisted with Lean 4 proof engineering, exact $\mathbb{Q}(\zeta_8)$ verification scripting, figure generation, and LaTeX typesetting. All mathematical definitions, theorems, proofs, formalization checks, and final manuscript claims were reviewed and validated by the sole author, Lluis Eriksson.

# A Self-Contained Verification Tables, Explicit Circuits, and Certificate Ledger

To ensure that every theorem in this manuscript can be audited without executing external code, we tabulate the explicit matrices $V_1, V_2, V_3$, the complete gate-by-gate circuits for $U_{\text{step3}}$ and $W_2$, the exact $T$-count comparison across scales, and the full SHA-256 certificate ledger.

## A.1 Explicit Symplectic-Gram Matrices $V_1, V_2, V_3$

From (27), the first three minimal Gram factors ($k=2m+1$ columns) are:

$$V_1=\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix},\quad V_2=\begin{pmatrix}1&1&0&0&0\\1&0&1&0&0\\1&1&1&1&0\\1&1&1&0&1\end{pmatrix},\quad V_3=\begin{pmatrix}1&1&0&0&0&0&0\\1&0&1&0&0&0&0\\1&1&1&1&0&0&0\\1&1&1&0&1&0&0\\1&1&1&1&1&1&0\\1&1&1&1&1&0&1\end{pmatrix}.$$

Direct multiplication verifies $V_1V_1^\top=\left(\begin{smallmatrix}2&1\\1&2\end{smallmatrix}\right)\equiv H_1$, $V_2V_2^\top=\left(\begin{smallmatrix}2&1&2&2\\1&2&2&3\\2&2&4&3\\2&2&3&4\end{smallmatrix}\right)\equiv H_2$, and $V_3V_3^\top\equiv H_3 \pmod 2$, with even row weights $2,2,4,4,6,6$.

### A.2 Complete Explicit Gate Sequences for $U_{\text{step3}}$ and $W_2$

Table 2: Exact action of $U_{\text{rtof}}$ and $U_{\text{step3}} = \text{CNOT}(a_1 \to a_0)\, S^\dagger(a_1)\, U_{\text{rtof}}(c, a_0, a_1)$ (4 $T$-gates, 0 ancillas) on all 4 reachable unary-subspace inputs $|c, a_0, 0\rangle$ (Certificate `C11`).

| Input $\lvert c, a_0, a_1\rangle$ | After $U_{\text{rtof}}$ | After $S^\dagger(a_1)$ | After CNOT$(a_1 \to a_0)$ | Expected Step 3 |
|---|---|---|---|---|
| $\lvert 0,0,0\rangle$ | $+\lvert 0,0,0\rangle$ | $+\lvert 0,0,0\rangle$ | $+\lvert 0,0,0\rangle$ | $+\lvert 0,0,0\rangle$ |
| $\lvert 0,1,0\rangle$ | $+\lvert 0,1,0\rangle$ | $+\lvert 0,1,0\rangle$ | $+\lvert 0,1,0\rangle$ | $+\lvert 0,1,0\rangle$ |
| $\lvert 1,0,0\rangle$ | $+\lvert 1,0,0\rangle$ | $+\lvert 1,0,0\rangle$ | $+\lvert 1,0,0\rangle$ | $+\lvert 1,0,0\rangle$ |
| $\lvert 1,1,0\rangle$ | $+i\lvert 1,1,1\rangle$ | $+\lvert 1,1,1\rangle$ | $+\lvert 1,0,1\rangle$ | $+\lvert 1,0,1\rangle$ |

**Explicit 11-$T$, 22-CNOT ancilla-free circuit for $W_2$ (qubits $0{=}c, 1{=}a_1, 2{=}b_1, 3{=}a_2, 4{=}b_2$):** Let $G(c, y) := \text{CNOT}(c{\to}y)\, T(y)\, \text{CNOT}(c{\to}y)\, T^\dagger(y)$ (applied right-to-left in algebraic notation, i.e., $T^\dagger$ first in time order). Reading gates strictly in *time order* (left to right):

1. **Pre-Clifford $C_2$:** CNOT(2→1), $H(2)$, CNOT(4→3), $H(4)$. (2 CNOT, 2 $H$)
2. **Pair $z = 2$ $(v^{(3)}, v^{(4)})$:** $G(0,3)$, $G(0,4)$, CNOT(3→4). (Wire 4 holds $s_1 = a_2 \oplus b_2$; 4 $T$, 5 CNOT)
3. **Pair $z = 1$ $(v^{(1)}, v^{(2)})$:** CNOT(4→1), CNOT(4→2), $G(0,1)$, $G(0,2)$, CNOT(4→1), and CNOT(1→2), leaving $s_0 = a_1 \oplus b_1 \oplus a_2 \oplus b_2$ on wire 2 (4 $T$, 8 CNOT).
4. **Column $v^{(0)}$ & uncompute ladder:** $G(0,2)$, CNOT(1→2), CNOT(4→2), CNOT(3→4). (2 $T$, 5 CNOT)
5. **Control phase ($-5 \equiv 3 \bmod 8$) & odd-pair CZs:** $T(0)$, $S(0)$, CZ(0,1), CZ(0,2). (1 $T$, 1 $S$, 2 CZ)
6. **Post-Clifford $C_1$:** $H(2)$, CNOT(2→1), $H(4)$, CNOT(4→3). (2 CNOT, 2 $H$)

Total: $T = 4 + 4 + 2 + 1 = 11$ (vs. 14 independent), CNOT $= 2 + 5 + 8 + 5 + 2 = 22$, CZ $= 2$, $H = 4$, $S = 1$, ancillas $= 0$. Certificate `C08` verifies exact identity on all 32 basis states over $\mathbb{Q}(\zeta_8)$.

### A.3 Unified Numerical Scaling Table and SHA-256 Certificate Ledger

Table 3: Exact $T$-count comparison across $m, K_j \in \{1, 2, 3, 4, 16, 64, 256, 1024\}$ (Certificate `C16`).

| | **Open Q1: Tracker Update ($K_j$)** | | | | **Open Q2: Wide Fredkin ($W_m$)** | | | |
|---|---|---|---|---|---|---|---|---|
| $K_j, m$ | Thm. 6 LB | $4K_j$ (meas.) | $8K_j$ (MF) | Sun $14K_j$ | Thm. 9 LB | Gram $4m{+}3$ | Shared-$c$ | Sun $7m$ |
| 1 | 0 | 4 | 8 | 14 | 3 | 7 | 7 | 7 |
| 2 | 3 | 8 | 16 | 28 | 5 | 11 | 12 | 14 |
| 3 | 3 | 12 | 24 | 42 | 7 | 15 | 19 | 21 |
| 4 | 4 | 16 | 32 | 56 | 9 | 19 | 24 | 28 |
| 16 | 16 | 64 | 128 | 224 | 33 | 67 | 96 | 112 |
| 64 | 64 | 256 | 512 | 896 | 129 | 259 | 384 | 448 |
| 256 | 256 | 1024 | 2048 | 3584 | 513 | 1027 | 1536 | 1792 |
| 1024 | 1024 | 4096 | 8192 | 14336 | 2049 | 4099 | 6144 | 7168 |

## References


[1] F. Sun, *Unitary Synthesis with a Unary Tracker*, arXiv:2611.34740v1 [quant-ph], November 2026.

Table 4: Verified SHA-256 certificate ledger under protocol `UNARY-TRACKER-BOUNDS-1.0` (manifest hash `c1e3e176a7ec...68d`).

| ID | Verified Claim | SHA-256 Prefix |
|---|---|---|
| C01 | Exact cyclotomic ring $\mathbb{Q}(\zeta_8)$ unit and Hadamard identities | 973a1756670f49ab |
| C02 | Thm. 6 exhaustive nullity for $n = 3$ (all 15 nonempty subsets) | f5d74364f9c26875 |
| C03 | Thm. 6 exhaustive nullity for $n = 4$ (all 255 nonempty subsets, $K = 1..8$) | 87a1c03eb40190ba |
| C04 | Thm. 6 invariance across compressed, dense, affine-shifted $\mathbb{F}_2$ codes | 232efba4bdcf17ea |
| C05 | Thm. 9(a) exact full-space $W_m$ nullity $\nu = 2m + 1$ ($m = 1..4$) | 0b17b4c5314f82fe |
| C06 | Thm. 9(b) exact symplectic Gram identity $V_m V_m^\top = H_m \pmod 2$ ($m = 1..16$) | ca03dbafe6e808f3 |
| C07 | Thm. 9(b) exhaustive exact mod-8 phase-polynomial identity ($m = 1..4$) | bf402ef5b88c986c |
| C08 | Thm. 9(b) exact $\mathbb{Q}(\zeta_8)$ full unitary verification of $(4m{+}3)$-$T$ $W_m$ ($m = 1..3$) | d57926addbbbaf7c |
| C09 | Thm. 9(b) exhaustive $\mathbb{Q}(\zeta_8)$ verification of all 512 states of 19-$T$ $W_4$ | 3026ad92bdfdb727 |
| C10 | Thm. 9(b) minimality $k_{\min} = 2m + 1$ ($V\mathbf{1} = \mathbf{0}$ kernel obstruction) | e28c388d1dde1c2c |
| C11 | Thm. 10(a) exact $\mathbb{Q}(\zeta_8)$ all-$+1$ phase check of 4-$T$ Step 3 & Step 1 | 05b34ae5c548adeb |
| C12 | Thm. 10(b) exact $\mathbb{Q}(\zeta_8)$ 0-$T$ meas.-assisted Step 1 ($K = 3$, all 8 outcomes) | 6f845d7b4de841ed |
| C13 | Thm. 12(a) exact QSD geometric sum & closed-form depth ($n = 2..14$) | 942d701317333b2f |
| C14 | Thm. 12(b) strict volume monotonicity $V_{\text{used}}(n, B) - V_{\text{used}}(n, 2B) > 0$ | 409caa26794cc746 |
| C15 | Thm. 12(c) exact sawtooth penalty (1033/522 at $n = 10$) & $B = N/2$ vs. $N$ gap | ca9aeb2cf8c12b3e |
| C16 | Unified exact $T$-count hierarchy across Open Questions 1 and 2 ($m, K = 1..1024$) | c5fce82216bb724c |


[2] M. Beverland, E. Campbell, M. Howard, and V. Kliuchnikov, *Lower bounds on the non-Clifford resources for quantum computations*, Quantum Science and Technology **5**(3), 035009, 2020.

[3] C. Gidney, *Halving the cost of quantum addition*, Quantum **2**, 74, 2018.

[4] D. Maslov, *Advantages of using relative-phase Toffoli gates with an application to multiple control Toffoli optimization*, Physical Review A **93**(2), 022311, 2016.

[5] V. V. Shende, S. S. Bullock, and I. L. Markov, *Synthesis of quantum-logic circuits*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **25**(6), 1000–1010, 2006.

[6] M. Amy and M. Mosca, *T-count optimization and Reed–Muller codes*, IEEE Transactions on Information Theory **65**(8), 4771–4784, 2019.

[7] D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo, *An algorithm for the T-count*, Quantum Information and Computation **14**(15–16), 1261–1276, 2014.