Exact Coset Sampling for Quantum Lattice Algorithms

Yifan Zhang
Princeton University
yifzhang@princeton.edu

October 24, 2025*

Abstract

We give a simple replacement for the contested "domain-extension" in Step 9 of a recent windowed-QFT lattice algorithm with complex-Gaussian windows [Chen, 2024]. As acknowledged by the author, the reported issue is due to a periodicity/support mismatch when extending only the first coordinate in the presence of offsets, which breaks the intended $\mathbb{Z}_P$-fiber. Our new subroutine replaces domain extension by a pair-shift difference that cancels unknown offsets exactly and synthesizes a uniform cyclic subgroup (a zero-offset coset) of order P inside $(\mathbb{Z}_{M_2})^n$. We adopt a gate-level access model and run a short prepass that measures the designated outcome registers (Chen's Steps 1, 3, and 5), fixing $E = (y', z', h^*)$. We then identify a concrete program point $t^\star$ at which an index wire $J \in \mathbb{Z}_P$ is preserved and the coordinate block equals $\mathbf{X}(j) \equiv 2D^2 j\,\mathbf{b}^* + \mathbf{v}^* \pmod{M_2}$. A compute-copy-uncompute sandwich on the prefix up to $t^\star$ yields a reversible evaluator that we call only on basis inputs $j = 0, 1$ to harvest $V = \mathbf{X}(0)$ and $\Delta = \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\mathbf{b}^*$ within the same run. We never invert a measurement, and we do not claim the circuit suffix after $t^\star$. The default Step 9† uses only Δ (no foreknowledge of $\mathbf{b}^*$): set $\mathbf{Z} \leftarrow -T \cdot \Delta \pmod{M_2}$ for uniform $T \in \mathbb{Z}_P$ and erase T coherently primewise by modular inversion and CRT.

Project Page: https://github.com/yifanzhang-pro/quantum-lattice

1 Introduction

Fourier Sampling-based quantum algorithms for lattice problems typically engineer a structured superposition whose Fourier transform reveals modular linear relations. A recent proposal of a windowed quantum Fourier transform (QFT) with complex-Gaussian windows by Chen [2024] follows this paradigm and, after modulus splitting and CRT recombination, arrives at a joint state whose n coordinate registers (suppressing auxiliary workspace) are of the explicit affine form

$$|\phi_8.f\rangle = \sum_{j\in\mathbb{Z}} \alpha(j)\,\big|\,2D^2 j\,b_1^*\,\big|\,2D^2 j\,\boldsymbol{b}^*_{[2..n]} + \boldsymbol{v}^*_{[2..n]} \mod M_2\big\rangle, \tag{1.1}$$

*Updates. We adopt a concrete gate-level access model with a short prepass that measures Chen's Step 1, 3, and 5 outcomes $E = (y', z', h^*)$ and specialize the preparation to E. We isolate a prefix $\mathcal{Q}_E$ at a concrete frontier $t^\star$ where an index wire $J \in \mathbb{Z}_P$ is preserved and $\mathbf{X}(j) \equiv 2D^2 j\,\boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$ is already written. A compute-copy-uncompute sandwich yields a basis-callable evaluator used only at $j = 0, 1$ to harvest (V, Δ).

where $M_2 := D^2 P$ with $P = \prod_{\eta=1}^{\kappa} p_\eta$ the product of distinct odd primes, $\gcd(D, P) = 1$, $\alpha(j) = \exp\big(\frac{2\pi i}{M_2}(aj^2 + bj + c)\big)$ is a known quadratic envelope from the windowed-QFT stage,[1] $\boldsymbol{b}^* = (b_1^*, \ldots, b_n^*) \in \mathbb{Z}^n$ (with $b_1^* = p_2 \cdots p_\kappa$ in the concrete pipeline of Chen [2024]), and the offset vector $\boldsymbol{v}^* \in \mathbb{Z}^n$ has unknown entries (often $v_1^* = 0$ by upstream normalization). The algorithmic goal is to sample a vector $\boldsymbol{u} \in \mathbb{Z}_{M_2}^n$ satisfying the modular linear relation

$$\langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \;\equiv\; 0 \pmod{P}, \tag{1.2}$$

from which the hidden information is recovered by standard linear algebra over the CRT factors.

Phase envelope persists. In Chen's derivation, Eq. (35) shows the quadratic envelope in j; Step 8 applies a reversible gadget and then returns to $|\varphi_7\rangle$, so this j-dependent envelope persists. We track it abstractly as $\alpha(j)$ and never disturb it downstream.

The published Step 9 of Chen [2024] seeks to implement Eq. (1.2) by a "domain extension" applied only to the first coordinate, justified by a periodicity-of-amplitude heuristic. However, the domain-extension lemma invoked there presupposes global P-periodicity of the amplitude, while the presence of offsets $\boldsymbol{v}^*$ breaks this premise: extending one coordinate alone changes the support and misaligns it with the intended $\mathbb{Z}_P$-fiber. As acknowledged by the author, the resulting state does not enforce Eq. (1.2) once offsets are present.

In this work, we give a simple, reversible subroutine that substitutes Step 9 and enforces the desired relation by subgroup structure rather than amplitude-periodicity. The core idea is a pair-shift difference that cancels offsets exactly and synthesizes a uniform cyclic coset of order P inside $(\mathbb{Z}_{M_2})^n$; a plain QFT then enforces Eq. (1.2) by character orthogonality. Formally, we prepare a uniform label $T \in \mathbb{Z}_P$, realize the difference register using the harvested finite difference

$$\Delta \;:=\; \mathbf{X}(1) - \mathbf{X}(0) \;\equiv\; 2D^2\, \boldsymbol{b}^* \pmod{M_2},$$

and set

$$\mathbf{Z} \;\leftarrow\; -T \cdot \Delta \pmod{M_2},$$

then (coherently) erase T primewise and by CRT. This produces an exactly uniform superposition over a cyclic subgroup of size P contained in the $\mathbb{Z}_P$-component of $(\mathbb{Z}_{M_2})^n$. Applying $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ to $\mathbf{Z}$ yields outcomes exactly supported on Eq. (1.2) and uniform over that set; the quadratic phase $\alpha(j)$ and the offsets $\boldsymbol{v}^*$ play no role in the support.

We require a residue-accessibility condition: for each prime $p_\eta \mid P$, some coordinate of $\boldsymbol{b}^*$ is nonzero modulo p_η. Equivalently, the map $T \mapsto T\,\boldsymbol{b}^* \pmod{P}$ is injective. This assumption is used solely to erase T coherently; no amplitude periodicity is assumed anywhere. When it fails, our procedure does not enforce Eq. (1.2) with constant probability (see Section 4).

Finally, our access model matters. We assume the windowed-QFT pipeline of Chen [2024] is available at the gate list level so that a prepass can condition on measured outcomes E and we can isolate a concrete prefix $\mathcal{Q}_E$ (Section 2.3). If only a black-box state oracle were available, the prefix isolation and compute–copy–uncompute evaluator would in general be impossible to realize (see Section 2.1).

[1] The sum over j is effectively finite due to the upstream window; we omit a global normalization constant, which plays no role in our arguments.

Organization. Section 2 fixes notation and access model, isolates the prefix $\mathcal{Q}_E$ and index wire J, states offset coherence, and derives a basis-callable evaluator via compute–copy–uncompute. Section 3 makes the default J-free Step $9^\dagger$ primary, cleanly separates cleanup, and proves exact correctness; the re-evaluation variant appears afterward. Section 4 records gate counts, complexities, and variants. Appendix B gives the frontier and input-lifting proofs. Appendix C explains offset cancellation, the cyclic coset, and the orthogonality check. Appendix E proves state factorization; Appendix F lists a gate-level skeleton; Appendix G details run-local determinism.

2 Background and Access Model

Notation and standing assumptions. For $q \in \mathbb{N}$, we write $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ with representatives in $(-\frac{q}{2}, \frac{q}{2}]$. Vectors are bold; inner product is $\langle \cdot, \cdot \rangle$. All modular arithmetic on registers is modulo $M_2 = D^2 P$ unless noted. We write $\boldsymbol{x}_{[2..n]} := (x_2, \ldots, x_n)$ for coordinate slices. For convenience, we write

$$\Delta \;:=\; \mathbf{X}(1) - \mathbf{X}(0) \;\equiv\; 2D^2\, \boldsymbol{b}^* \pmod{M_2}.$$

Throughout, for each prime $p_\eta \mid P$ we let $i(\eta)$ denote the lexicographically first index $i \in \{1, \ldots, n\}$ with $\Delta_i \not\equiv 0 \pmod{p_\eta}$ (equivalently, $b_i^* \not\equiv 0 \pmod{p_\eta}$ since $2D^2$ is a unit). This choice is fixed once and for all and is implementable by a reversible priority encoder (see Step $9^\dagger$.4).

Parameter identification from Chen [2024]. In Chen's notation, $M = 2(t^2+u^2)$ and $x = Db$, so that $P := M/(2D^2)$ is odd and $M_2 = D^2 P$. After modulus splitting and the parity measurement (Chen's Steps 5–8), the coordinate block takes the affine form $\mathbf{X}(j) \equiv 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$ with $\boldsymbol{v}^*$ independent of j. Consequently $\Delta = \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2 \boldsymbol{b}^* \pmod{M_2}$; see Lemma 2.7.

2.1 Assumptions and scope

A1. We assume a uniform, gate-level description of the windowed-QFT pipeline specialized to measured outcomes $E = (y', z', h^*)$ (we never invert those measurements). Prefix isolation at a frontier $t^\star$ uses only the given gate list. If only a black-box state oracle is available, the compute–copy–uncompute evaluator $U_{\mathrm{coords},E}$ cannot, in general, be realized.

A2. After modulus splitting and parity measurement (Chen's Steps 5–8), all coordinates share the same affine offset across j: $\mathbf{X}(j) \equiv 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$ with $\boldsymbol{v}^*$ independent of j (cf. Lemma 2.7). We treat this as an assumption about the compiled pipeline, supported by Chen's expressions (see Section 2.2), and do not claim it holds for arbitrary implementations.

A3. We assume $P = \prod_{\eta=1}^{\kappa} p_\eta$ is given together with its (pairwise-distinct, odd) prime factors, consistent with Chen [2024]. Our cleanup uses per-prime modular inversions and a reversible CRT.

A4. For each prime $p_\eta \mid P$, some coordinate $b_i^* \not\equiv 0 \pmod{p_\eta}$ (Section 3). This is necessary and sufficient for coherent erasure of T (Section 3.2). When it fails, Step $9^\dagger$ cannot enforce $\langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \equiv 0 \pmod{P}$ without postselection (Section 4).

A5. P is odd; any 2-power factors are absorbed into D^2, so 2 is a unit modulo P.

A6. Phase envelope persistence. After Step 8 in Chen [2024] the state equals $|\varphi_7\rangle$, hence the j-dependent envelope $\alpha(j)$ produced upstream is present throughout our Step $9^\dagger$. All

superposition-time operations in our construction are classical reversible (no QFT-based adders), so this envelope is preserved exactly.

We do not assume amplitude periodicity, we do not assume postselection or interaction, and we do not assume any oracle that maps $\mathbf{X}(j)$ to $\mathbf{X}(j+T)$ across runs.

Failure modes.

- If **A4** fails for some p_η, coherent cleanup of T is impossible solely from $(\mathbf{Z}, \Delta)$; Fourier sampling on $\mathbf{Z}$ is then uniform over $(\mathbb{Z}_{M_2})^n$ (Prop. 3.2) and does not enforce Eq. (1.2).
- If only black-box access is available (violating **A1**), the prefix isolation and evaluator $U_{\mathrm{coords},E}$ cannot be constructed, so the proposed "harvest Δ at $j = 0, 1$ within the same run" procedure is unavailable.

Why single-coordinate domain extension fails under offsets. For readers comparing to Chen [2024], here is a concrete two-dimensional counterexample illustrating the periodicity/support mismatch. Let $P = 15$, $M_2 = D^2 P$, $\boldsymbol{b}^* = (5, 1)$, and $\boldsymbol{v}^* = (1, 2)$. The intended $\mathbb{Z}_P$-fiber is $\{(2D^2 j \cdot 5,\ 2D^2 j \cdot 1 + 2)\} \bmod M_2$. Extending only the first coordinate by a factor $C > 1$ produces states supported on $\{(2D^2(j + C\widetilde{j}) \cdot 5,\ 2D^2 j + 2)\}$; the second coordinate still depends on the unextended j, so the support no longer projects to a uniform cyclic subgroup in the P-part. The offsets prevent the amplitude from being P-periodic in all coordinates, violating the hypothesis of the domain-extension lemma used in Chen [2024]. Our construction avoids this pitfall by working directly with subgroup cosets in $(\mathbb{Z}_{M_2})^n$.

2.2 Concrete index-wire exposure inside Chen's pipeline

We now make explicit the concrete index rail that controls the write into the first coordinate. This matches the access model above and will be used only to build a basis-callable evaluator. The lemma below is a program-analysis statement about any fixed uniform gate list; it is not a black-box claim.

Lemma 2.1 (Concrete exposure via the first-coordinate rail)**.** Fix the measured outcomes $E = (y', z', h^*)$ of Chen's Steps 1, 3, and 5 and unitarize the remainder (deferred measurement). In any uniform gate-level implementation of the portion between just-after Step 5 and just-before the small operations of Step 8, there exists a named control wire $J_{\mathrm{ctl}} \in \mathbb{Z}_P$ and a program point $t^\star$ immediately after the last gate that writes X_1 and before any subsequent gate that modifies J_{ctl} such that the circuit prefix $U_{\le t^\star}$ satisfies

$$U_{\le t^\star} :\ |j\rangle_{J_{\mathrm{ctl}}} |0\rangle_X |0\rangle_A \ \longmapsto\ |j\rangle_{J_{\mathrm{ctl}}} |\mathbf{X}(j)\rangle_X |\gamma_{j,E}\rangle_A ,$$

with $\mathbf{X}(j) = 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$ and J_{ctl} preserved at $t^\star$.

The existence of such a J_{ctl} follows from the gate dependencies that drive the write into X_1; however, in highly optimized or obfuscated implementations, locating the first occurrence of j may require full access to the compilation artifacts. This is why Assumption **A1** in Section 2.1 is necessary.

Proof sketch. Since X_1 is ultimately a deterministic function of a single cyclic parameter $j \in \mathbb{Z}_P$, some last gate writes X_1 using a control that carries j. Take J_{ctl} to be the first occurrence of that

value along the dependency DAG; place $t^\star$ just after the last write into X and before any subsequent modification of J_{ctl}. Offset coherence (Theorem 2.7) implies all coordinates follow the same affine rule in j, so the stated form holds. □

Basis COPY and input lifting. Insert a single basis COPY $(J_{\mathrm{ctl}}, J) \mapsto (J_{\mathrm{ctl}}, J_{\mathrm{ctl}}+J)$ to materialize a fresh J that is preserved up to $t^\star$. Decompose the prefix as $U_{\mathrm{rest}} \circ U_{\text{prep-}J}$, where $U_{\text{prep-}J}$ prepares the internal (possibly nonuniform) superposition on J_{ctl}. By linearity (input-lifting; Theorem 2.5), replacing $U_{\text{prep-}J}$ by the identity and feeding an *external* basis input $|j\rangle$ on J yields the branchwise action $|j\rangle\,|0\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ without changing phases or touching any measurement.

2.3 Access model and outcome-conditioned determinism

We work in the standard gate-level access model: the preparation is a uniform circuit family built from QFTs, windows, and arithmetic. We run a short prepass that executes Chen's Steps 1, 3, and 5 and actually measures the designated registers, obtaining $E = (y', z', h^*)$, which are henceforth treated as classical controls (we never invert these measurements). Specializing to E, there exists a concrete program point $t^\star$ such that a circuit prefix $\mathcal{Q}_E$ preserves a computational-basis index wire $J \in \mathbb{Z}_P$ and deterministically writes

$$\mathbf{X}(j) \;\equiv\; 2D^2 j\,\boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$$

on the coordinate block; see Lemmas 2.4, 2.5, 2.7 and Theorem 2.10 below.

Assumption 2.2 (Run-local determinism and phase discipline)**.** Within a single run, the basis outputs $\mathbf{X}(0)$ and $\mathbf{X}(1)$ are reproducible. We harvest $V := \mathbf{X}(0)$ and $\Delta := \mathbf{X}(1) - \mathbf{X}(0)$ by basis calls to the prefix-based evaluator (defined below), then treat (V, Δ) as read-only basis data. All superposition-time arithmetic thereafter uses classical reversible (Toffoli/Peres) adders/multipliers only, introducing no data-dependent phases.

2.4 Prefix isolability and evaluator synthesis

We use two standard primitives throughout: $\mathrm{QFT}_{\mathbb{Z}_q}$ (in $\mathrm{poly}(\log q)$ gates) and classical reversible modular arithmetic. Our construction separates two clean roles:

- **Prefix-based coordinate evaluator.** From the prefix at $t^\star$ we synthesize

  $$U_{\mathrm{coords},E} \;:=\; \mathcal{Q}_E^\dagger \;\circ\; \mathrm{COPY}_X \;\circ\; \mathcal{Q}_E,$$

  which maps $|j\rangle\,|0\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ on basis inputs $j \bmod P$ and is called only at $j = 0, 1$ to harvest (V, Δ).
- **Arithmetic evaluator.** A separate phase-free reversible circuit U_{prep} that, with read-only access to (V, Δ), computes $V + j\Delta$ via double-and-add and modular adds. It is never used to re-enter the state-preparation path and imprints no data-dependent phases.

Lemma 2.3 (Existence of a basis-callable coordinate evaluator)**.** Fix a gate-level implementation of Chen's pipeline that produces Eq. (1.1). Execute a short prepass that performs Chen's Steps 1, 3,

and 5 and measures the designated registers, obtaining outcomes $E = (y', z', h^*)$ which are henceforth used as classical controls. There exists a concrete program point $t^\star$ and a circuit prefix $\mathcal{Q}_E$ such that

$$\mathcal{Q}_E : \ |j\rangle\,|0\rangle_X\,|0\rangle_A \longmapsto |j\rangle\,|\mathbf{X}(j)\rangle_X\,|\gamma_{j,E}\rangle_A\,,$$

with an index wire $J \equiv j \pmod P$ preserved up to $t^\star$ and $\mathbf{X}(j) \equiv 2D^2 j\,\boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$. Defining

$$U_{\text{coords},E} \ := \ \mathcal{Q}_E^\dagger \ \circ \ \text{COPY}_X \ \circ \ \mathcal{Q}_E,$$

we have $U_{\text{coords},E} : |j\rangle\,|0\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ for every basis $j \bmod P$, with all work reset. No measurement is inverted. We call $U_{\text{coords},E}$ only on $j = 0, 1$ to harvest (V, Δ).

2.5 Frontier and input-lifting

We formalize two auxiliary facts used in Lemma 2.3.

Lemma 2.4 (Frontier lemma for index preservation)**.** In any uniform gate list, let X be the coordinate block and J an index rail used to write X and later modified. There exists a frontier $t^\star$ after the last write into X and before any subsequent modification of J such that the prefix up to $t^\star$ has the form $U_{\le t^\star} : |j\rangle_J\,|0\rangle_X\,|0\rangle_A \mapsto |j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A\,.$

Lemma 2.5 (Input-lifting (clarified))**.** Let $U = U_{\text{rest}} \circ U_{\text{prep-}J}$ be a unitary such that $U_{\text{prep-}J}$ prepares $\sum_j \alpha(j)\,|j\rangle_J$ on a register J, and the suffix U_{rest} acts *branchwise* as

$$U_{\text{rest}} : \ |j\rangle_J\,|0\rangle_X\,|0\rangle_A \ \longmapsto \ |j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A \quad \text{for every basis } j.$$

Define $\widetilde{\mathcal{Q}} := U_{\text{rest}}$ and replace $U_{\text{prep-}J}$ by the identity, treating J as an external input. Then, for every basis j,

$$\widetilde{\mathcal{Q}} : \ |j\rangle_J\,|0\rangle_X\,|0\rangle_A \ \longmapsto \ |j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A\,,$$

and, by linearity, for any amplitude profile $(\beta(j))_j$,

$$\widetilde{\mathcal{Q}}\left(\sum_j \beta(j)\,|j\rangle_J\,|0\rangle_X\,|0\rangle_A\right) = \sum_j \beta(j)\,|j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A\,.$$

Corollary 2.6 (Controlledness and linearity)**.** With $\mathcal{Q}_E$ as in Theorem 2.10 and Lemma 2.5, the prefix acts in a controlled manner by J and, for any amplitudes $\beta(j)$,

$$\mathcal{Q}_E\Big(\sum_{j\in\mathbb{Z}_P} \beta(j)\,|j\rangle_J\Big)\,|0\rangle_X\,|0\rangle_A \ = \ \sum_{j\in\mathbb{Z}_P} \beta(j)\ |j\rangle_J\,|F(j)\rangle_X\,|\gamma_{j,E}\rangle_A\,. \tag{2.1}$$

Equivalently, the prefix decomposes as a block-diagonal (controlled) sum

$$\mathcal{Q}_E \ = \ \sum_{j\in\mathbb{Z}_P} |j\rangle\langle j|_J \ \otimes \ V_{j,E}, \qquad V_{j,E}\,|0\rangle_X\,|0\rangle_A \ = \ |F(j)\rangle_X\,|\gamma_{j,E}\rangle_A\,.$$

Proof. By Lemma 2.5, for each basis j, $\mathcal{Q}_E\,|j\rangle_J\,|0\rangle_X\,|0\rangle_A = |j\rangle_J\,|F(j)\rangle_X\,|\gamma_{j,E}\rangle_A$. Theorem 2.10 ensures J is preserved up to $t^\star$, so $\mathcal{Q}_E$ is block-diagonal in the computational basis of J. Linearity yields (2.1) for arbitrary superpositions of $|j\rangle$. □

Lemma 2.7 (Offset coherence)**.** In the deferred-measurement unitary of Chen [2024], after modulus splitting and the parity measurement, and for each fixed outcome E, the coordinate block equals $\mathbf{X}(j) \equiv 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$, with $\boldsymbol{v}^*$ independent of j. Hence $\Delta \equiv 2D^2\, \boldsymbol{b}^* \pmod{M_2}$.

This matches the explicit affine form presented just before Step 8 in Chen [2024] (see also Section 2.2). Our analysis relies on this affine computational-basis content; if a different implementation breaks offset coherence, the harvesting step must be reworked. Proofs are presented in Appendix B.

Proof sketch. We work in Chen's notation recalled in Section 2 ("Parameter identification from Chen [2024]"). In Chen [2024], immediately before Step 8, the prepared register block has computational-basis contents of the form)

$$\big|\, 2Dj\, \boldsymbol{x} \;+\; \boldsymbol{v}' \;+\; \tfrac{M}{2}\boldsymbol{k} \mod M \big\rangle,$$

for a loop index $j \in \mathbb{Z}$, an auxiliary label $\boldsymbol{k} \in 0\,|\,\mathbb{Z}^{n-1}$ orthogonal to $\boldsymbol{x}$, and some vector $\boldsymbol{v}'$ determined by earlier measurement outcomes $E = (y', z', h^\star)$. Using the parameter identification $P := M/(2D^2)$ and $M_2 := D^2 P = M/2$, reduce the above register modulo $M_2 = M/2$. The $\frac{M}{2}\boldsymbol{k}$ term vanishes mod M_2, leaving

$$\big|\, 2Dj\, \boldsymbol{x} \;+\; \boldsymbol{v}' \mod M_2 \big\rangle.$$

Defining $\boldsymbol{b}^* := \boldsymbol{x}/D$ (note D is odd and $\gcd(D, P) = 1$, so division is well-defined modulo P) and $\boldsymbol{v}^* := \boldsymbol{v}' \bmod M_2$, we obtain

$$\mathbf{X}(j) \;\equiv\; 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}.$$

The offset $\boldsymbol{v}^*$ depends only on the fixed outcomes E and is independent of j, since $\boldsymbol{v}'$ is determined before the j-controlled update. Consequently, $\Delta = \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\, \boldsymbol{b}^* \pmod{M_2}$. This proves the claimed affine form. □

Remark 2.8 (Black-box limitation)**.** If only a state-preparation oracle for $\sum_j \alpha(j)\,|\mathbf{X}(j)\rangle$ is available, constructing $U_{\mathrm{coords},E}$ (and harvesting V, Δ without disturbing phases) is no longer possible: the oracle might imprint unknown j-dependent phases, and its inverse is unavailable. Our route therefore requires gate-level access as stated in Section 2.1.

Remark 2.9. From a single transformation $|0\rangle_J\,|0\rangle_X \mapsto \sum_j \alpha(j)\,|j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A$ of an arbitrary unitary one cannot conclude a decomposition $U = U_{\mathrm{rest}} \circ U_{\mathrm{prep}\text{-}J}$ with the branchwise property above. Our input-lifting applies only after the frontier cut (Lemma 2.4) has established that the prefix acts as $|j\rangle\,|0\rangle \mapsto |j\rangle\,|F(j)\rangle\,(\cdot)$ on basis inputs. Absent this structure, the concern that such a Q may not exist would be valid.

The unitary $(x, y) \mapsto (x, x{+}y)$ permutes the computational basis, so copying X by modular addition never violates the no-cloning/no-broadcasting theorems; it produces entanglement unless the input is basis [Wootters and Zurek, 1982, Dieks, 1982, Barnum et al., 1996].

Theorem 2.10 (Prefix isolability and index-wire preservation)**.** In the (deferred-measurement) unitary dilation of Chen's windowed-QFT pipeline and for any fixed outcome tuple $E = (y', z', h^*)$, there exists a concrete program point $t^\star$ and a uniform compilation such that:

1. a computational-basis register $J \in \mathbb{Z}_P$ (obtained by a one-gate basis COPY from the control that writes X_1) is preserved up to $t^\star$;

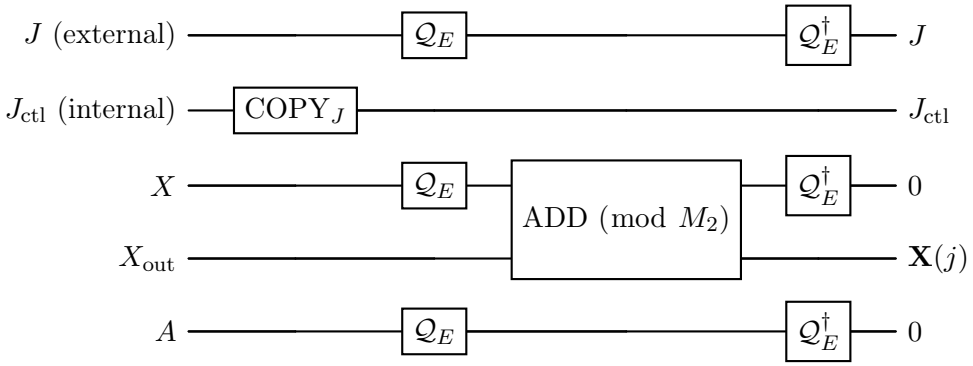

Figure 1: Compute–copy–uncompute evaluator $U_{\text{coords},E}$ built from the *prefix* specialized to outcomes E. Only basis inputs ($j = 0, 1$) are ever used to harvest (V, Δ).

2. the circuit prefix $\mathcal{Q}_E := \big(\text{preparation} \restriction_{\le t^\star}\big)$ deterministically writes $\mathbf{X}(j) = 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^*(E) \pmod{M_2}$ on X as a function of J;
3. even if J is internally prepared, input-lifting (Lemma 2.5) makes J an external basis input with the same branchwise action on (J, X);
4. no claim is made about the suffix beyond $t^\star$; it may freely touch X.

Because we cut before any gate that changes J, J is preserved; in particular, the prefix decomposes as $\mathcal{Q}_E = \sum_{j \in \mathbb{Z}_P} |j\rangle\langle j|_J \otimes V_{j,E}$ acting on (X, A), which is the controlledness used in Corollary 2.6. Consequently, the basis-callable evaluator

$$U_{\text{coords},E} \;:=\; \mathcal{Q}_E^\dagger \;\circ\; \text{COPY}_X \;\circ\; \mathcal{Q}_E$$

maps $|j\rangle\,|0\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ for every basis $j \bmod P$, with all work reset.

2.6 Two-pass harvest

Algorithm 1 Constructing $U_{\text{coords},E}$ and harvesting (V, Δ)

1: **Prepass.** Execute Chen's Steps 1, 3, and 5 and measure the designated registers to obtain $E = (y', z', h^*)$ (we never invert this measurement).
2: **Prefix.** Using Lemmas 2.4 and 2.5, identify a frontier $t^\star$ and define $\mathcal{Q}_E$ as the input-lifted prefix up to $t^\star$.
3: **Evaluator.** Define $U_{\text{coords},E} := \mathcal{Q}_E^\dagger \circ \text{COPY}_X \circ \mathcal{Q}_E$.
4: **Harvest.** Call $U_{\text{coords},E}$ on $j = 0$ and $j = 1$ to obtain $V := \mathbf{X}(0)$ and $\Delta := \mathbf{X}(1) - \mathbf{X}(0)$; treat (V, Δ) as read-only basis data thereafter.

Security/indistinguishability note. If an external oracle were to return $\mathbf{X}(j+T)$ from $\mathbf{X}(j)$ for arbitrary T with the same offset, then, as in LWE with reused noise, subtracting two outputs would reveal the offset-free difference and compromise indistinguishability. Our construction never assumes such an oracle. All calls to $U_{\text{coords},E}$ are intra-run basis calls that reuse the very arithmetic that prepared Eq. (1.1); across runs, upstream randomness need not preserve the same offset.

Implementation note. (i) Harvest (V, Δ) within the same run before any superposition-time step, and keep them as read-only basis data. The coordinate evaluator U_{coords} is never applied to a superposed input. (ii) The evaluator U_{prep} is implemented with classical reversible (Toffoli/Peres) adders/multipliers only; we do not use QFT-based adders, ensuring no data-dependent phase is introduced on superpositions.

Lemma 2.11 (Phase discipline)**.** If all superposition-time arithmetic in Step $9^\dagger$ is realized by classical reversible circuits (no QFT-based adders) and $U_{\text{coords},E}$ is never applied on a superposed input, then no additional data-dependent phase is imprinted beyond the fixed quadratic envelope $\alpha(j)$ produced upstream.

Proof. Classical reversible adders/multipliers implement permutations of the computational basis; thus they preserve amplitudes and phases. Avoiding U_{coords} on superpositions prevents reintroduction of state-preparation phases. □

Remark. QFT-based adders would, in general, introduce data-dependent phases through controlled rotations; these are precisely the kind of envelope phases one must avoid in the windowed-QFT regime that produced $\alpha(j)$ upstream. In our construction, $U_{\text{coords},E}$ is never applied to a superposed input, and all superposition-time arithmetic is phase-free. Linearity implies that if one did feed $\sum_j \beta(j)\,|j\rangle$ to Q then Q would act branchwise, but we explicitly avoid such calls.

Within a single run, one could measure the harvested basis registers $V = \mathbf{X}(0)$ and $\Delta = \mathbf{X}(1) - \mathbf{X}(0)$ and hence recover $\mathbf{v}^*$ and $2D^2\mathbf{b}^*$ classically. Our default path simply does not require such measurement; we retain (V, Δ) as basis data to maintain phase discipline. If an implementation is willing to expose $\mathbf{b}^*$ classically, the constant-adder variant applies verbatim and further simplifies cleanup. No indistinguishability claim is made or needed here.

Arithmetic evaluator and finite difference Δ. Let U_{prep} be the reversible arithmetic evaluator of $\mathbf{X}(\cdot)$ as above, and define

$$\Delta \;:=\; \mathbf{X}(1) - \mathbf{X}(0) \pmod{M_2},$$

harvested once via basis calls $j = 0, 1$. Because $\mathbf{X}(j)$ depends only on $j \bmod P$, this same Δ equals $\mathbf{X}(J{+}1) - \mathbf{X}(J)$ for any classical J, but we do not recompute it; Δ is treated as read-only basis data. In all cases, $\Delta \equiv 2D^2\,\mathbf{b}^* \pmod{M_2}$. We will use Δ to compute T from $\mathbf{Z}$ without any classical knowledge of $\mathbf{b}^*$.

2.7 Where $\mathbf{X}(j)$ comes from

In Chen's nine-step pipeline, after modulus splitting P and CRT recombination, the state is denoted $|\varphi_7\rangle$ (and the discussion immediately before Step 8 there) contains a coordinate block of the explicit affine form

$$\left(2D^2 j\, b_1^* \;\middle|\; 2D^2 j\, \boldsymbol{b}^*_{[2..n]} + \boldsymbol{v}^*_{[2..n]}\right) \pmod{M_2},$$

up to an orthogonal $\frac{M_2}{2}$–coset index k and a global quadratic phase in j (the "Karst-wave" envelope). Step 8 in Chen [2024] reverses its temporary manipulations and returns to $|\varphi_7\rangle$, so this envelope persists; we denote it by $\alpha(j)$ and ensure it is not perturbed by our phase-free arithmetic. If we retain just this coordinate block (suppressing k), rename the surviving (effectively finite) loop variable as j, and ignore global phases, we obtain exactly Eq. (1.1). In the notation used throughout our paper,

$$\mathbf{X}(j) \;:=\; V + j\Delta \;\equiv\; 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2},$$

with $V = \boldsymbol{v}^*$ and $\Delta = 2D^2\boldsymbol{b}^*$ harvested once via basis calls $j = 0, 1$ to the preparation/evaluator block $U_{\text{coords},E}$ (Prop. 2.12). The optional label $J \equiv j \pmod P$ that we carry in Section 3 is precisely the CRT-reduced index present after Chen's Step 8. No periodicity-of-amplitude assumption is used here, only the affine computational-basis content of the coordinate registers.

2.8 Explicit construction of U_{prep}

We now give a stand-alone construction of the reversible arithmetic evaluator $U_{\text{prep}} : |j\rangle\,|\mathbf{0}\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ that does not require any classical knowledge of $\boldsymbol{b}^*$ or $\boldsymbol{v}^*$.

Proposition 2.12 (Harvest-on-basis & arithmetic re-evaluation)**.** Let $U_{\text{coords},E}$ be the coordinate evaluator from Lemma 2.3. Invoke it once each on the basis inputs $j = 0$ and $j = 1$ (with all ancillas restored to $|0\rangle$) to obtain two program registers in the computational basis:

$$V := \mathbf{X}(0) = \boldsymbol{v}^* \pmod{M_2}, \qquad \Delta := \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\,\boldsymbol{b}^* \pmod{M_2}.$$

This harvest occurs within the same run, before any superposition-time step, and uses no mid-circuit measurement. Now define a separate reversible arithmetic evaluator U_{prep} that acts on $|j\rangle\,|\mathbf{0}\rangle$ (with read-only access to V, Δ) by computing

$$|j\rangle\,|\mathbf{0}\rangle \;\mapsto\; |j\rangle\,|\,V + j\cdot\Delta \mod M_2\,\rangle\,.$$

This evaluator performs no phase kickback (Toffoli/Peres-style arithmetic; no QFT adders) and never invokes U_{coords} again; hence any quadratic phases created during the windowed–QFT stage remain unaffected. The multiplication $j \cdot \Delta$ is implemented reversibly by a standard double-and-add routine that treats Δ as data (not as a hard-coded constant) without mutating it: if $j = \sum_\ell j_\ell 2^\ell$ in binary, perform for each bit ℓ the controlled update "if j_ℓ=1 then add R_ℓ", where $R_0 := \Delta$ and $R_\ell := 2R_{\ell-1} \pmod{M_2}$ is maintained in a scratch register; Δ itself remains unchanged and the R_ℓ ladder is uncomputed at the end. Finally add $V \pmod{M_2}$.

Lemma 2.13 (Efficiency and independence from classical secrets)**.** Construction 2.12 realizes a unitary U_{prep} with gate complexity $O(n \log P \cdot \text{poly}(\log M_2))$. It uses only reversible modular additions/doublings and treats (V, Δ) as basis registers obtained from U_{coords}; no classical description of $\boldsymbol{b}^*$ or $\boldsymbol{v}^*$ is required. The reversible double-and-add uses one scratch register R to hold R_ℓ and uncomputes it at the end; Δ is never modified. Computing per-prime modular inverses during cleanup via a reversible extended Euclidean algorithm costs $O((\log p_\eta)^2)$ gates per p_η (or $\widetilde{O}(\log p_\eta)$ with half-GCD). Re-evaluating $\mathbf{X}(\cdot)$ at $J{+}T$ therefore consists of invoking the arithmetic evaluator on the input label $J{+}T$, without imprinting any additional phases.

Proof. The schoolbook double-and-add uses $O(\log P)$ additions per coordinate, each in $\text{poly}(\log M_2)$ gates; n coordinates contribute the stated factor. All operations are on computational-basis registers (V, Δ) and do not assume knowledge of their numeric values. As $U_{\text{coords},E}$ is the known reversible subroutine already used to produce Eq. (1.1), preparing (V, Δ) once is efficient; after preparation, U_{prep} can be called repeatedly at different inputs (e.g., $J{+}T$ in Step $9^\dagger$.2). *Note.* Multiplication by the data vector Δ via double-and-add performs $O(\log P)$ controlled additions per coordinate, never mutates Δ, and uncomputes the scratch ladder R_ℓ exactly. □

Remark 2.14. If a classical description of $\boldsymbol{b}^* \bmod P$ happens to be available, one may replace the data-multiplication by a constant adder using $2D^2T\,\boldsymbol{b}^*$; this is optional and not used in our default path.

2.9 Uniformity and complexity containment

For clarity and to preempt complexity-theoretic misunderstandings, we spell out the uniformity and model assumptions used throughout the superposition-time part of Step 9†:

(1) All classical constants (CRT parameters for (p_η), modular inverses, mixed-radix digits, etc.) are computed on the fly by uniform reversible algorithms in time $\mathrm{poly}(\log M_2, \kappa)$; no nonuniform advice is assumed.

(2) We never assume an oracle that, given $\mathbf{X}(j)$, returns $\mathbf{X}(j{+}T)$ with the same hidden offsets for arbitrary T. The only calls to the preparation block $U_{\mathrm{coords},E}$ are the basis inputs $j = 0, 1$ used once to harvest (V, Δ) within the same run; superposition-time arithmetic thereafter uses the separate, phase-free evaluator U_{prep}.

(3) The cleanup erases T because T is a deterministic function of $(\mathbf{Z} \bmod P, \Delta)$ under residue accessibility (Definition 2.17); it is implemented by reversible computation and CRT, not by conditioning on rare events.

(4) QFTs are implemented by standard, uniform approximations with operator-norm error at most ε_1 per register; by a telescoping bound the n-fold error is at most $n\varepsilon_1$ (Remark after Theorem 3.5). No exact irrational rotations or nonuniform gate sets are required.

Lemma 2.15 (Uniform BQP containment of Step 9†)**.** The transformation that maps the input state of Eq. (1.1) to a Fourier sample $\boldsymbol{u} \in (\mathbb{Z}_{M_2})^n$ supported on Eq. (1.2) is implementable by a uniform family of quantum circuits of size $\mathrm{poly}(n, \log M_2, \kappa)$, assuming Section 2.1. In particular, Step 9† resides in BQP.

Proof. Phase discipline (Lemma 2.11) ensures that all superposition-time arithmetic is a permutation of basis states. The evaluator U_{prep} is realized by reversible modular additions and doublings with read-only (V, Δ) (Prop. 2.12). Cleanup computes T' from $(\mathbf{Z}, \Delta)$ by per-prime modular inversions and a reversible CRT (Lemma 3.1); these are uniform classical computations lifted to reversible form with $\mathrm{poly}(\log M_2, \kappa)$ overhead. The final $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ is a standard BQP primitive with uniform approximations and tracked error (Remark after Theorem 3.5). No postselection, interaction, or nonuniform advice is used. Hence the whole procedure is in uniform BQP. □

Lemma 2.16 (Affine register form)**.** For all j in the implicit finite window (from the windowed-QFT stage), the coordinate registers immediately before Step 9 have the exact affine form

$$\mathbf{X}(j) \equiv 2D^2 j\, \mathbf{b}^* + \mathbf{v}^* \pmod{M_2},$$

and the window affects only the amplitudes $\alpha(j)$, not the computational-basis contents. In particular, $\mathbf{X}(j{+}1) - \mathbf{X}(j) \equiv \Delta \pmod{M_2}$ for all j, hence $\mathbf{X}(j) \equiv V + j\Delta \pmod{M_2}$.

Default J-free realization. If one prefers to avoid carrying J, the construction can be simplified as follows: after harvesting Δ as basis data, skip the re-evaluation of $\mathbf{X}(j{+}T)$ and directly allocate $\mathbf{Z}$ and set

$$\mathbf{Z} \;\leftarrow\; -T \cdot \Delta \;\equiv\; -2D^2 T\, \boldsymbol{b}^* \pmod{M_2}. \tag{2.2}$$

by a double-and-add with read-only access to Δ. The subsequent cleanup (computing T' from $\mathbf{Z}$ and uncomputing it) proceeds unchanged. This variant removes the need for $\mathbf{Y}$ and J entirely and is the default Step 9† used throughout. Note that while 2 is a unit modulo P (since P is odd), we still require residue accessibility (Section 3.2) to recover T from $(\mathbf{Z}, \Delta)$.

Injectivity condition. We will use the following natural assumption, which enables coherent coset synthesis by allowing us to uncompute the shift parameter T from the difference register. Without it, T cannot be erased from the rest of the state, and Fourier sampling on $\mathbf{Z}$ alone becomes uniform over $\mathbb{Z}_{M_2}^n$ (i.e., it does not enforce Eq. (1.2) with constant success probability).

Definition 2.17 (Residue accessibility)**.** For each prime $p_\eta \mid P$, there exists a coordinate $i(\eta) \in \{1, \ldots, n\}$ such that the entry $b^*_{i(\eta)}$ is not a multiple of p_η, i.e., $b^*_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$.

This condition holds with overwhelming probability for the lattice instances considered in [Chen, 2024]; any given instance can be checked efficiently, and coordinates can be permuted if necessary. Importantly, this assumption is needed only for the cleanup that erases T coherently. If the cleanup is skipped, then regardless of whether Definition 2.17 holds, applying QFT to $\mathbf{Z}$ alone yields the uniform distribution on $\mathbb{Z}_{M_2}^n$ (the T-branches remain orthogonal and do not interfere). When Definition 2.17 holds, T is a function of $\mathbf{Z}$ mod P, enabling coherent erasure and the interference that enforces Eq. (1.2). It implies that the map $T \mapsto T\,\boldsymbol{b}^* \pmod{P}$ from $\mathbb{Z}_P$ to $(\mathbb{Z}_P)^n$ is injective. To see this, if $T\,\boldsymbol{b}^* \equiv \mathbf{0} \pmod{P}$, then for each η, the condition $b^*_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$ (equivalently, $\Delta_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$ since $\Delta \equiv 2D^2\mathbf{b}^*$ and $2D^2$ is a unit mod p_η) forces $T \equiv 0 \pmod{p_\eta}$. By the Chinese Remainder Theorem, this implies $T \equiv 0 \pmod{P}$. Conversely, if Definition 2.17 fails for some p_η, then $b^*_i \equiv 0 \pmod{p_\eta}$ for all i, so every T multiple of p_η lies in the kernel of $T \mapsto T\,\boldsymbol{b}^* \bmod P$; hence injectivity fails. Thus, Definition 2.17 is equivalent to the injectivity of this map and to the recoverability of T from $\mathbf{Z}$ mod P.

Remark 2.18 (Random-instance bound)**.** Because $b^*_1 = p_2 \cdots p_\kappa$, we have $b^*_1 \not\equiv 0 \pmod{p_1}$ and $b^*_1 \equiv 0 \pmod{p_\eta}$ for all $\eta \geq 2$. If, for each prime p_η, the remaining coordinates $(b^*_2, \ldots, b^*_n) \bmod p_\eta$ are close to uniform over $(\mathbb{Z}_{p_\eta})^{n-1}$ (as in typical reductions), then for $\eta = 1$ the accessibility condition holds deterministically, while for each $\eta \geq 2$ we have

$$\Pr[\, b^*_i \equiv 0 \text{ for all } i \bmod p_\eta\,] \;=\; \Pr[\, b^*_2 \equiv \cdots \equiv b^*_n \equiv 0 \bmod p_\eta\,] \;=\; p_\eta^{-(n-1)}.$$

A union bound therefore yields

$$\Pr[\text{residue accessibility fails for some } p_\eta] \;\leq\; \sum_{\eta=2}^{\kappa} p_\eta^{-(n-1)},$$

which is negligible once $n \geq 2$ and the p_η are moderately large (for $n = 2$, the sum still decays with the prime sizes).

3 The new Step $9^\dagger$

Precondition. Run the prepass to fix E, synthesize $U_{\text{coords},E}$, and basis-call it only at $j = 0, 1$ to harvest $V := \mathbf{X}(0)$ and $\Delta := \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\boldsymbol{b}^* \pmod{M_2}$. Treat (V, Δ) as read-only basis data thereafter (Assumption 2.2); $U_{\text{coords},E}$ is never applied to a superposition.

3.1 Default realization

The default route avoids carrying the preparation's index and directly synthesizes the subgroup coset on $\mathbf{Z}$ from Δ alone. It does *not* assume any classical knowledge of $\boldsymbol{b}^*$ and does not re-enter the preparation path.

Algorithm 2 Step 9† — *Default J-free route*

Require: Harvested $\Delta = \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\boldsymbol{b}^* \pmod{M_2}$.

1: Prepare $T \in \mathbb{Z}_P$ in $\frac{1}{\sqrt{P}} \sum_{t\in\mathbb{Z}_P} |t\rangle$ (e.g., per-prime $\mathrm{QFT}_{\mathbb{Z}_{p_\eta}}$ + CRT wiring).

2: **Form the difference register:** set $\mathbf{Z} \leftarrow -T \cdot \Delta \pmod{M_2}$ by reversible double-and-add with read-only Δ. (Eq. (2.2))

3: **Auxiliary cleanup (mandatory):** compute T' from $(\mathbf{Z}, \Delta)$ by per-prime modular inversion and reversible CRT (Lemma 3.1); set $T \leftarrow T - T'$ so $T = 0$; uncompute T' from $\mathbf{Z}$ by inverting its computation. (Sec. 3.2)

4: Apply $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ to $\mathbf{Z}$ and measure $\boldsymbol{u} \in \mathbb{Z}_{M_2}^n$.

5: **return** $\boldsymbol{u}$ (uniform over solutions to $\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \pmod{P}$ by Theorem 3.5).

Interpretation. Eq. (2.2) shows that $\mathbf{Z}$ is a uniform superposition over the cyclic subgroup generated by $-2D^2\boldsymbol{b}^*$ in the $\mathbb{Z}_P$-component of $(\mathbb{Z}_{M_2})^n$; offsets $\boldsymbol{v}^*$ never enter. Cleanup is needed to erase the label T coherently; otherwise Fourier sampling on $\mathbf{Z}$ alone is uniform on $(\mathbb{Z}_{M_2})^n$ (Prop. 3.2).

3.2 Cleanup and necessity

Under residue accessibility (Def. 2.17), for each $p_\eta \mid P$ select the lexicographically first index $i(\eta)$ with $\Delta_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$ and compute

$$T_\eta \;\equiv\; -\,\Delta_{i(\eta)}^{-1}\, Z_{i(\eta)} \pmod{p_\eta},$$

then recombine by a reversible CRT to obtain the unique $T' \in \mathbb{Z}_P$ (Lemma 3.1). Updating $T \leftarrow T - T'$ zeros T; inverting the construction of T' from $\mathbf{Z}$ erases T' without touching $\mathbf{Z}$.

Lemma 3.1 (Recovering T from $\mathbf{Z}$)**.** Under Definition 2.17 and Eq. (2.2), let $\Delta = \mathbf{X}(1) - \mathbf{X}(0)$. For each p_η, fix $i(\eta)$ with $\Delta_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$ and let $c_\eta := \Delta_{i(\eta)}^{-1} \bmod p_\eta$. Then $T \equiv -c_\eta\, Z_{i(\eta)} \pmod{p_\eta}$ for all η, and the unique $T \in \mathbb{Z}_P$ is obtained by CRT recombination.

Proposition 3.2 (Pre-cleanup Fourier sample is uniform)**.** Let $\rho_{\mathbf{Z}} = \frac{1}{P} \sum_{T\in\mathbb{Z}_P} |-2D^2T\,\boldsymbol{b}^*\rangle\langle -2D^2T\,\boldsymbol{b}^*|$ be the classical mixture obtained by tracing out non-$\mathbf{Z}$ registers prior to cleanup. For any such convex mixture of basis states, applying $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ and measuring yields the uniform distribution on $(\mathbb{Z}_{M_2})^n$. Hence auxiliary cleanup is necessary to enforce Eq. (1.2).

3.3 Optional re-evaluation variant

When it is convenient to retain the preparation's index $J \equiv j \bmod P$, one may realize a pair-evaluation shift and explicit difference. This variant is functionally equivalent to the default path and still uses only (V, Δ).

Algorithm 3 Step $9^\dagger$ — *Re-evaluation route*

Require: Label $J \equiv j \pmod P$, harvested (V, Δ).

1: Prepare $T \in \mathbb{Z}_P$ uniformly.
2: Copy $\mathbf{X}$ into $\mathbf{Y}$ by modular adds. (no-cloning is not violated; only basis is copied [Wootters and Zurek, 1982, Dieks, 1982, Barnum et al., 1996, Nielsen and Chuang, 2010])
3: Evaluate U_{prep} at $J + T$ into $\mathbf{Y}$ to get $\mathbf{X}(j{+}T)$ (without imprinting phases).
4: Set $\mathbf{Z} \leftarrow \mathbf{X} - \mathbf{Y} \pmod{M_2}$ so $\mathbf{Z} \equiv -2D^2 T\, \boldsymbol{b}^*$.
5: Cleanup as in Sec. 3.2: compute T' from $(\mathbf{Z}, \Delta)$; update $\mathbf{Y} \leftarrow \mathbf{X}(j{+}T{-}T')$; set $T \leftarrow T - T'$; uncopy $\mathbf{Y}$; uncompute T' from $\mathbf{Z}$.
6: Apply $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ to $\mathbf{Z}$ and measure $\boldsymbol{u}$; **return** $\boldsymbol{u}$.

Reversibility note. CRT recombination can be implemented (i) by a reversible Garner mixed-radix scheme in $O(\kappa^2)$ modular operations, or (ii) by a reversible remainder/product-tree CRT in $O(\kappa \log \kappa)$ modular operations; both use constants depending only on (p_η) and are reversible when the ancilla trail is retained, so the subsequent uncomputation is exact. After these actions, the global state factorizes with a coherent superposition on $\mathbf{Z}$.[2]
After Step $9^\dagger$.4 we have the factorized state

$$\left(\sum_j \alpha(j)\ |\mathrm{junk}(j)\rangle \right) \otimes \frac{1}{\sqrt{P}} \sum_{T \in \mathbb{Z}_P} \Big| -2D^2 T\, \boldsymbol{b}^* \mod M_2 \Big\rangle_{\mathbf{Z}}. \tag{3.1}$$

Fourier sampling. Apply $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ to the entire $\mathbf{Z}$-register block and measure $\boldsymbol{u} \in \mathbb{Z}_{M_2}^n$. The outcome distribution is analyzed next.

3.4 Exact correctness

Lemma 3.3 (Cyclic embedding)**.** Under Definition 2.17, the map $\phi : \mathbb{Z}_P \to (\mathbb{Z}_{M_2})^n$ given by $\phi(T) = -2D^2 T\, \boldsymbol{b}^* \pmod{M_2}$ is an injective group homomorphism. By the CRT decomposition $\mathbb{Z}_{M_2} \cong \mathbb{Z}_{D^2} \times \mathbb{Z}_P$, the image lies in the $\mathbb{Z}_P$ component and has order exactly P. Hence the state in Eq. (3.1) is uniform over a subgroup-coset of size P.

Proof. Homomorphism is immediate. For injectivity, reduce modulo P: if $\phi(T) \equiv \mathbf{0}$, then $2D^2 T\, \boldsymbol{b}^* \equiv \mathbf{0} \pmod P$. Since $2D^2$ is a unit modulo P and by Definition 2.17 some coordinate of $\boldsymbol{b}^*$ is a unit modulo each p_η, we must have $T \equiv 0 \pmod{p_\eta}$ for all η. The Chinese Remainder Theorem gives $T \equiv 0 \pmod P$. Moreover, under the CRT decomposition $\mathbb{Z}_{M_2} \cong \mathbb{Z}_{D^2} \times \mathbb{Z}_P$, the image of ϕ lies entirely in the $\mathbb{Z}_P$-component (the $\mathbb{Z}_{D^2}$ projection is 0), and residue accessibility guarantees that, for each p_η, some coordinate has order p_η. Hence the subgroup has order exactly $\prod_\eta p_\eta = P$. □

Lemma 3.4 (Exact orthogonality from a CRT-coset)**.** Consider the uniform superposition over the CRT-coset generated by $\boldsymbol{b}^*$:

$$|\Psi\rangle = \frac{1}{\sqrt{P}} \sum_{T \in \mathbb{Z}_P} |-2D^2 T\, \boldsymbol{b}^* \mod M_2\rangle\,.$$

[2] This cleanup is necessary for correctness; see Prop. 3.2 and Prop. 3.6.

After $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$, the amplitude of $\boldsymbol{u} \in \mathbb{Z}_{M_2}^n$ is

$$A(\boldsymbol{u}) \;=\; \frac{1}{\sqrt{M_2^n}} \cdot \frac{1}{\sqrt{P}} \sum_{T=0}^{P-1} \exp\Big(\tfrac{2\pi i}{M_2} \left\langle -2D^2 T\, \boldsymbol{b}^*,\, \boldsymbol{u} \right\rangle\Big) \;=\; \frac{1}{\sqrt{M_2^n}} \cdot \frac{1}{\sqrt{P}} \sum_{T=0}^{P-1} \big(\exp(\tfrac{2\pi i}{P} \cdot (-2)\, \langle \boldsymbol{b}^*, \boldsymbol{u} \rangle)\big)^T,$$

Only the $\mathbb{Z}_P$-component of $\boldsymbol{u}$ influences the sum over T (the $\mathbb{Z}_{D^2}$ projection cancels since $M_2 = D^2 P$). Because P is odd, 2 is invertible modulo P. Hence $A(\boldsymbol{u}) = 0$ unless $\langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \equiv 0 \pmod P$, in which case $|A(\boldsymbol{u})| = \sqrt{P}/M_2^{n/2}$ (up to a global phase). Consequently, the measurement outcomes are exactly supported on Eq. (1.2) and are uniform over that set; indeed,

$$\#\{\boldsymbol{u} \in (\mathbb{Z}_{M_2})^n :\; \langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \equiv 0 \pmod P\} \;=\; \frac{M_2^n}{P}.$$

Since each feasible $\boldsymbol{u}$ occurs with probability P/M_2^n and there are M_2^n/P of them, the total probability sums to 1.

Proof. Let $r := \exp\big(\frac{2\pi i}{M_2} \cdot (-2D^2)\, \langle \boldsymbol{b}^*, \boldsymbol{u} \rangle\big) = \exp\big(-\frac{2\pi i}{P} \cdot 2\, \langle \boldsymbol{b}^*, \boldsymbol{u} \rangle\big)$. Because P is odd, 2 is a unit modulo P, and only the $\mathbb{Z}_P$-component of the phase contributes to the sum over T (the $\mathbb{Z}_{D^2}$-component cancels since $M_2 = D^2 P$). Note also that $r^P = \exp\big(-\frac{2\pi i}{M_2}\, 2D^2 P\, \langle \boldsymbol{b}^*, \boldsymbol{u} \rangle\big) = 1$ for all $\boldsymbol{u}$, so the geometric sum over $T \in \mathbb{Z}_P$ always collapses to either 0 or P. Since $M_2 = D^2 P$, we have $\frac{-2D^2}{M_2} \equiv -\frac{2}{P} \pmod 1$, i.e., only the P-component of the phase matters in the sum over T; this is exactly why the base of the geometric progression is $e^{\frac{2\pi i}{P}(-2)\langle \boldsymbol{b}^*, \boldsymbol{u} \rangle}$. Because P is odd, 2 is invertible mod P. Thus $r = 1$ iff $\langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \equiv 0 \pmod P$. The sum $\sum_{T=0}^{P-1} r^T$ is P if $r = 1$ and 0 otherwise; multiplying by the prefactor $M_2^{-n/2} P^{-1/2}$ gives the stated amplitude magnitude. □

At each prime p_η, Definition 2.17 guarantees that the linear form $\boldsymbol{u} \mapsto \langle \boldsymbol{b}^*, \boldsymbol{u} \rangle$ has rank 1 over $\mathbb{Z}_{p_\eta}$, so the solution set on $(\mathbb{Z}_{p_\eta})^n$ has size p_η^{n-1}. By CRT this gives P^{n-1} solutions on the $\mathbb{Z}_P$-part, while the $\mathbb{Z}_{D^2}$-parts are unconstrained and contribute $(D^2)^n$, yielding a total of $(D^2)^n P^{n-1} = M_2^n/P$.

Group-theoretic perspective. For a finite abelian group G and a subgroup $H \le G$, the QFT on the uniform superposition over any coset of H produces uniform support on the annihilator $H^\perp \subseteq \widehat{G}$. Taking $G = (\mathbb{Z}_{M_2})^n$, $H = \langle -2D^2 \boldsymbol{b}^* \rangle$, and identifying $\widehat{G} \cong G$ via the standard pairing, we recover Lemma 3.4 with $H^\perp = \{\boldsymbol{u} :\; \langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \equiv 0 \pmod P\}$. The overall sign is immaterial since -1 is a unit modulo P.

Theorem 3.5 (Step $9^\dagger$ is correct)**.** Assume Assumption 2.2 and Definition 2.17. Starting from Eq. (1.1) (specialized to measured outcomes E by a short prepass), after executing either (i) the default J-free route (Algorithm 2), or (ii) the re-evaluation route (Algorithm 3), the state factors as in Eq. (3.1). In all cases, $U_{\mathrm{coords},E}$ is never applied to superpositions. Applying $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ to the $\mathbf{Z}$-register and measuring yields $\boldsymbol{u} \in \mathbb{Z}_{M_2}^n$ uniformly distributed over the solutions of Eq. (1.2). The offsets $\boldsymbol{v}^*$ and the quadratic phases $\alpha(j)$ do not affect the support or uniformity of the measured $\boldsymbol{u}$.

Proof. Eq. (2.2) shows $\mathbf{Z}$ depends only on T, not on j or $\boldsymbol{v}^*$. Under Definition 2.17, Step $9^\dagger$.4 erases T and yields the factorization Eq. (3.1); the part carrying $\alpha(j)$ is in registers disjoint from $\mathbf{Z}$. By Lemma 3.4, Fourier sampling of $\mathbf{Z}$ yields Eq. (1.2) uniformly. Neither $\boldsymbol{v}^*$ nor $\alpha(j)$ enters that calculation. □

Proposition 3.6 (Cleanup necessity and consequence)**.** Let $|\Phi_3\rangle$ be the joint state immediately after forming $\mathbf{Z}$ (Eq. (2.2)) but before auxiliary cleanup. If T remains entangled with $\mathbf{Z}$, then Fourier sampling on $\mathbf{Z}$ alone is uniform over $(\mathbb{Z}_{M_2})^n$, irrespective of $\boldsymbol{v}^*$ and the phases $\alpha(j)$. Under Definition 2.17, T is a function of $\mathbf{Z}$ mod P and can be erased coherently; the resulting pure state factors as in Eq. (3.1), enabling interference that enforces Eq. (1.2).

Proof. Tracing out $(\mathbf{X}, \mathbf{Y}, T)$ before cleanup leaves the mixture $\rho_{\mathbf{Z}} = \frac{1}{P}\sum_{t\in\mathbb{Z}_P} |-2D^2 t\boldsymbol{b}^*\rangle\langle -2D^2 t\boldsymbol{b}^*|$, whose Fourier sample is uniform by linearity since each basis input has a flat spectrum under $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$. When Definition 2.17 holds, t is a CRT-function of $\mathbf{Z}$ mod P; computing t reversibly from $\mathbf{Z}$, zeroing T, restoring auxiliary registers (if present), and uncomputing yields the factorization (3.1). See Appendix E. □

Remark 3.7 (Approximate QFTs and leakage)**.** If a single-register QFT implementation $\widetilde{U}$ satisfies $\|U - \widetilde{U}\|_{\mathrm{op}} \le \varepsilon_1$, then $\left\|U^{\otimes n} - \widetilde{U}^{\otimes n}\right\|_{\mathrm{op}} \le n\varepsilon_1$, so any measurement's total-variation leakage is at most $n\varepsilon_1$. The annihilator support is unchanged; only small leakage mass appears.

Remark 3.8. (i) No amplitude periodicity is used anywhere. (ii) The offsets $\boldsymbol{v}^*$ cancel exactly by construction; no knowledge of their residues is required. (iii) Residue accessibility (Definition 2.17) is operationally necessary for coherent cleanup. (iv) Edge case $n = 1$: with $b_1^* = p_2 \cdots p_\kappa$, accessibility cannot hold (it vanishes modulo every p_η for $\eta \ge 2$), consistent with upstream requirements that $n \ge 2$. (v) The factor 2 in $-2D^2\, T\, \boldsymbol{b}^*$ is inessential; any fixed unit modulo P yields the same annihilator.

Connection back to Chen [2024]. Under the CRT viewpoint, Step 9† replaces domain extension on one coordinate with a coset synthesis agnostic to offsets. Conceptually, we embed $\mathbb{Z}_P$ into $(\mathbb{Z}_{M_2})^n$ via $T \mapsto -2D^2 T\boldsymbol{b}^*$, average uniformly over the orbit, and then read off the annihilator by QFT. This directly yields the intended linear relation modulo P without invoking amplitude periodicity across heterogeneous coordinates.

4 Complexity and variants

Complexity. Copying registers and reversible modular adders and multipliers over $\mathbb{Z}_{M_2}$ use $O(\mathrm{poly}(\log M_2))$ gates. The shift $\mathbf{Z} \leftarrow \mathbf{Z} - 2D^2 T\, \boldsymbol{b}^*$ costs $O\big(n\,\mathrm{poly}(\log M_2)\big)$. Computing $\mathbf{Z} = \mathbf{X} - \mathbf{Y}$ is linear in n. Uncomputing T needs κ modular reductions and inverses in $\mathbb{Z}_{p_\eta}$ and one CRT recombination. A reversible extended Euclid for one inverse costs $O\big((\log p_\eta)^2\big)$ gates, or $\widetilde{O}(\log p_\eta)$ with half-GCD. CRT recombination works with either a Garner mixed-radix scheme in $O(\kappa^2)$ modular steps, or a remainder and product tree in $O(\kappa \log \kappa)$ steps. Word sizes stay in $\mathrm{poly}(\log P)$, and we keep all intermediate digits for clean uncomputation. The transform $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ costs $O\big(n\,\mathrm{poly}(\log M_2)\big)$.

The subroutine matches the time and success bounds of Chen [2024]. No amplitude amplification is needed. The support on the target coset is exact and uniform.

All dependence on j and on $\boldsymbol{v}^*$ stays in registers disjoint from $\mathbf{Z}$ and does not affect the Fourier sample (see also the discussion preceding Lemma 3.3). In particular, the D^2-components of $\boldsymbol{u}$ remain unconstrained, while the P-components satisfy Eq. (1.2).

If residue accessibility fails. If Definition 2.17 fails for some prime p_η, the map $T \mapsto T\,\boldsymbol{b}^* \pmod P$ has a nontrivial kernel. Then T is not a function of $\mathbf{Z} \bmod P$. Coherent erasure of T is not possible. Fourier sampling on $\mathbf{Z}$ alone becomes uniform over $\mathbb{Z}_{M_2}^n$ and does not force Eq. (1.2). Two paths remain:

1. Enforce the condition modulo $P' = \prod_{\eta\in\mathcal{I}} p_\eta$, where accessibility holds. Handle the missing primes by adding one or more auxiliary directions or by a short unimodular re-basis so that each missing prime is accessible in at least one coordinate. Then rerun the coset step for those primes. The measured $\boldsymbol{u}$ then obeys $\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \pmod{P'}$ exactly and is free modulo the other primes. Downstream linear algebra can consume this partial set and repeat after fixing the rest.
2. Use a postselection fallback. First unshift $\mathbf{Y}$ by the known T, that is, apply $\mathbf{Y} \leftarrow \mathbf{Y} - 2D^2 T\,\boldsymbol{b}^*$. Then apply QFT^{-1} to T and keep the zero frequency. The outcome is a coherent uniform coset on $\mathbf{Z}$ without computing T from $\mathbf{Z}$. The zero frequency appears with probability $1/P$. Amplitude amplification raises this rate to $\Theta(1)$ at a cost of $\Theta(\sqrt{P})$ queries.

We adopt Definition 2.17. It gives deterministic cleanup with no postselection cost.

Alternative modulus choices. Under Definition 2.17 we can compute the coset label $J = T$ from $\mathbf{Z} \bmod P$. Applying $\mathrm{QFT}_{\mathbb{Z}_P}$ to J produces a flat spectrum over $\mathbb{Z}_P$, but this step alone does not force Eq. (1.2). A safe route is to map J back into $\mathbf{Z}$ by $-2D^2 J\,\boldsymbol{b}^* \pmod{M_2}$ and then apply $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$, identical to the main path. We keep the J-free variant for clarity.

5 Conclusion

We presented a reversible Step $9^\dagger$ that (i) cancels unknown offsets exactly, (ii) synthesizes a coherent, uniform CRT-coset state without amplitude periodicity, and (iii) yields the intended modular linear relation via an exact character-orthogonality argument. The access model and evaluator construction are now fully formal: we fix outcomes by a short prepass, cut at a concrete frontier $t^\star$, lift the internal index to an external basis input, and synthesize a basis-callable evaluator by compute–copy–uncompute on the *prefix* only. The default shift path uses only the harvested Δ (no foreknowledge of $\boldsymbol{b}^*$).

We expect the pair-shift difference pattern to be broadly useful in windowed-QFT pipelines whenever unknown offsets obstruct clean CRT lifting.

Acknowledgment

We are grateful to all who provided constructive discussions and helpful feedback.

References

Howard Barnum, Carlton M Caves, Christopher A Fuchs, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15):2818, 1996.

Yilei Chen. Quantum algorithms for lattice problems. *Cryptology ePrint Archive*, 2024.

DGBJ Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886): 802–803, 1982.

Appendices

A Why single-coordinate domain extension fails under offsets

To concretize the critique, take $n = 2$, $P = 15$, $M_2 = D^2P$, $\boldsymbol{b}^* = (5, 1)$, $\boldsymbol{v}^* = (1, 2)$, and the affine block

$$\mathbf{X}(j) \equiv (2D^2j \cdot 5 + 1,\ 2D^2j + 2) \pmod{M_2}.$$

Extending only the first coordinate by a factor $C > 1$ replaces $2D^2j \cdot 5$ by $2D^2(j + C\widetilde{j}) \cdot 5$ while the second coordinate remains $2D^2j + 2$. The support is then

$$\{(2D^2(j + C\widetilde{j}) \cdot 5 + 1,\ 2D^2j + 2)\},$$

which, modulo the P-part, sweeps the first coordinate over a C-fold extension of a 15-cycle while the second coordinate remains restricted to a single 15-cycle indexed by j. The pair no longer lies in a coherent $\mathbb{Z}_{15}$-coset; there is no subgroup of $(\mathbb{Z}_{M_2})^2$ of order 15 whose coset this support equals. Consequently, a QFT will not enforce $\langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \equiv 0 \pmod{15}$ with constant probability. Our coset-synthesis avoids this by building the subgroup first and only then applying the QFT.

B Details on frontier cuts and input lifting

This appendix gives clean, self-contained proofs of Lemmas 2.4 and 2.5. We make the very mild assumption that the state preparation is realized by a uniform family of straight-line circuits (unitaries with deferred measurements), which covers the pipelines considered in this paper.

Registers and events. Let J denote the (computational-basis) index rail and X the block of n coordinate registers. Let A collect all other ancilla/workspace registers. For a fixed circuit instance (after specializing all classical outcomes E), linearize the circuit into a sequence of elementary gates $g_1, \ldots, g_T$. We say that a gate writes X if one of its targets lies in X, and it modifies J if one of its targets lies in J.[3]

B.1 Proof of Lemma 2.4

Proof. Let $g_X^{\max}$ be the last gate in the sequence whose target intersects X, and let $g_J^{\min}$ be the first subsequent gate whose target intersects J. If no such $g_J^{\min}$ exists, place the frontier at the end of the circuit. Choose the frontier $t^\star$ to be the time slice immediately after $g_X^{\max}$ and strictly before $g_J^{\min}$. By construction:
1. No gate after $t^\star$ ever writes to X (by definition of $g_X^{\max}$).
2. No gate up to and including $t^\star$ modifies J (since $g_J^{\min}$ is the earliest such gate after $g_X^{\max}$).
Therefore the unitary prefix $U_{\le t^\star}$ has the form

$$U_{\le t^\star} :\ |j\rangle_J |0\rangle_X |0\rangle_A \longmapsto |j\rangle_J |F(j)\rangle_X |\gamma_j\rangle_A ,$$

for a deterministic function $F : \mathbb{Z}_P \to (\mathbb{Z}_{M_2})^n$ and some (generally j-dependent) workspace state $|\gamma_j\rangle$. Determinism of F follows because, for any fixed basis input j, the contents of X at $t^\star$ are

[3] This includes controlled operations whose target is in X or J. Controls (on J) do not count as modifying J.

fully determined by the circuit's action; unitarity precludes a superposition of different X-values on the same basis branch $|j\rangle$. Finally, since J is not modified before $t^\star$, it is preserved as a computational-basis wire up to that frontier. This proves the lemma. □

B.2 Proof of Lemma 2.5

Proof. Write the full (deferred-measurement) preparation as $U = U_{\text{rest}} \circ U_{\text{prep}}$, where U_{prep} prepares the (possibly nonuniform) superposition $\sum_j \alpha(j)\,|j\rangle_J$ and U_{rest} applies the remaining gates that act on (J, X, A). By assumption on the circuit (and by Lemma 2.4 applied at the frontier $t^\star$ inside U_{rest}), for every basis j we have a branchwise map

$$U_{\text{rest}} :\ |j\rangle_J\,|0\rangle_X\,|0\rangle_A \longmapsto |j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A\,,$$

for the same function F and some workspace state $|\gamma_j\rangle$. Now, by linearity, on the superposed input prepared by U_{prep},

$$U\big(|0\rangle_X\,|0\rangle_A\big) = \sum_j \alpha(j)\,U_{\text{rest}}\big(|j\rangle_J\,|0\rangle_X\,|0\rangle_A\big) = \sum_j \alpha(j)\ |j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A\,.$$

Consequently, if we replace U_{prep} by the identity and feed an external basis input $|j\rangle$ on J, the same suffix U_{rest} implements the identical branchwise map

$$\widetilde{\mathcal{Q}} := U_{\text{rest}} :\ |j\rangle_J\,|0\rangle_X\,|0\rangle_A \longmapsto |j\rangle_J\,|F(j)\rangle_X\,|\gamma_j\rangle_A\,,$$

because U_{rest} depends only on the value stored in J, not on how that value was prepared nor on the coefficients $\alpha(j)$. In particular, the phases $\alpha(j)$ never enter the computational-basis contents of X. This proves the lemma. □

C Mechanics inside Step $9^\dagger$

Offset cancellation. Write

$$\mathbf{X}(j) = \big(2D^2 j\, b_1^* \;\big|\; 2D^2 j\, \boldsymbol{b}^*_{[2..n]} + \boldsymbol{v}^*_{[2..n]}\big), \qquad \mathbf{X}(j+T) = \big(2D^2 (j+T)\, b_1^* \;\big|\; 2D^2 (j+T)\, \boldsymbol{b}^*_{[2..n]} + \boldsymbol{v}^*_{[2..n]}\big).$$

Then

$$\mathbf{X}(j) - \mathbf{X}(j+T) \equiv -2D^2 T\, \boldsymbol{b}^* \pmod{M_2},$$

so the offset $\boldsymbol{v}^*$ vanishes identically.

Uniform CRT coset on Z. After Step $9^\dagger$.4 we have erased T from the rest. A uniform superposition over $T \in \mathbb{Z}_P$ maps by

$$T \longmapsto -2D^2 T\, \boldsymbol{b}^* \pmod{M_2}$$

to a coherent uniform coset on $\mathbf{Z}$ of length P. No amplitude reweighting appears. The image is cyclic of order P by Lemma 3.3.

Orthogonality check. For any $\boldsymbol{u}$ the phase base is

$$r = \exp\Big(-\tfrac{2\pi i}{M_2}\, 2D^2\, \langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \Big).$$

We have

$$r^P = \exp\Big(-\tfrac{2\pi i}{M_2}\, 2D^2 P\, \langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \Big) = 1,$$

with $M_2 = D^2 P$. So the P-term geometric sum collapses exactly. Equivalently,

$$\frac{-2D^2}{M_2} \equiv -\frac{2}{P} \pmod 1,$$

which makes the reduction to phases modulo P explicit.

D Proof of Lemma 2.3

Proof of Lemma 2.3. Let $\mathcal{P}$ be any fixed gate-level implementation specialized to measured outcomes E that produces the state of Eq. (1.1). Denote by J the (computational-basis) label wire carrying j (or j mod P), by X the block of n coordinate registers, and by A all remaining ancillas/workspace. By construction of Eq. (1.1), for every basis input j the final contents of X equal the deterministic string $\mathbf{X}(j) \in (\mathbb{Z}_{M_2})^n$; the amplitude envelope $\alpha(j)$ resides in phases on J (and/or registers disjoint from X).

Fix a program point $t^\star$ in $\mathcal{P}$ immediately after the last gate that acts nontrivially on X. Then express $\mathcal{P}$ as a composition of a prefix and a suffix:

$$\mathcal{P} = \mathcal{R} \circ \mathcal{Q},$$

where $\mathcal{Q}$ denotes the portion of the circuit up to $t^\star$, and $\mathcal{R}$ denotes the remainder following $t^\star$. By the choice of $t^\star$ there exist states $|\gamma_j\rangle, |\beta_j\rangle$ of A such that, for every basis j,

$$\mathcal{Q}:\ |j\rangle_J |0\rangle_X |0\rangle_A \longmapsto |j\rangle_J |\mathbf{X}(j)\rangle_X |\gamma_j\rangle_A, \qquad \mathcal{R}:\ |j\rangle_J |\mathbf{X}(j)\rangle_X |\gamma_j\rangle_A \longmapsto |j\rangle_J |\mathbf{X}(j)\rangle_X |\beta_j\rangle_A,$$

that is, $\mathcal{R}$ leaves the *value* stored in X unchanged (it may entangle A further, but never overwrites X).

Let COPY_X denote the computational-basis copying unitary implemented by modular addition on a fresh block X_{out}:

$$\mathrm{COPY}_X:\ |x\rangle_X |0\rangle_{X_{\mathrm{out}}} \longmapsto |x\rangle_X |x\rangle_{X_{\mathrm{out}}}.$$

Define the reversible arithmetic evaluator

$$U_{\mathrm{coords},E} := \big(\mathcal{R}\circ\mathcal{Q}\big)^\dagger \circ \mathrm{COPY}_X \circ \big(\mathcal{R}\circ\mathcal{Q}\big), \tag{D.1}$$

acting on $(J, X, A, X_{\mathrm{out}})$ and initialized with $|0\rangle_X |0\rangle_A |0\rangle_{X_{\mathrm{out}}}$. For any basis j,

$$\begin{aligned} |j\rangle_J |0\rangle_X |0\rangle_A |0\rangle_{X_{\mathrm{out}}} &\xrightarrow{\mathcal{R}\circ\mathcal{Q}} |j\rangle_J |\mathbf{X}(j)\rangle_X |\beta_j\rangle_A |0\rangle_{X_{\mathrm{out}}} \\ &\xrightarrow{\mathrm{COPY}_X} |j\rangle_J |\mathbf{X}(j)\rangle_X |\beta_j\rangle_A |\mathbf{X}(j)\rangle_{X_{\mathrm{out}}} \\ &\xrightarrow{(\mathcal{R}\circ\mathcal{Q})^\dagger} |j\rangle_J |0\rangle_X |0\rangle_A |\mathbf{X}(j)\rangle_{X_{\mathrm{out}}}. \end{aligned}$$

Thus, on the visible pair (J, X_{out}) we obtain exactly

$$U_{\text{coords},E}: \quad |j\rangle\,|0\rangle \;\longmapsto\; |j\rangle\,|\mathbf{X}(j)\rangle\,,$$

with all work registers (X, A) restored to $|0\rangle$. This proves the existence of a reversible arithmetic block implementing $|j\rangle\,|\mathbf{0}\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ inside any unitary that prepares Eq. (1.1).

Remarks on scope and phases. (i) The construction uses only gates already present in the given preparation $\mathcal{P}$ and a basis copy; it does not assume access to an external oracle for $j \mapsto \mathbf{X}(j)$. (ii) When used in our algorithm, $U_{\text{coords},E}$ is called only on basis inputs $j \in \{0, 1\}$ to harvest $V = \mathbf{X}(0)$ and $\Delta = \mathbf{X}(1) - \mathbf{X}(0)$; since $\mathcal{R} \circ \mathcal{Q}$ and COPY_X are permutations of the computational basis, these basis calls imprint no data-dependent phases (cf. Lemma 2.11). We never apply U_{coords} to a superposed J. □

E Proof of State Factorization

For completeness, we show that the state after cleanup (Step $9^\dagger$.4) factors as claimed, and we contrast it with the pre-cleanup mixed state on $\mathbf{Z}$ (this also makes Prop. 3.6 fully formal). Let the joint state after Step $9^\dagger$.2 be

$$|\Phi_2\rangle \;=\; \frac{1}{\sqrt{P}} \sum_{t\in\mathbb{Z}_P} \sum_j \alpha(j)\;\; |\mathbf{X}(j)\rangle_{\mathbf{X}}\,|\mathbf{X}(j) + 2D^2 t\,\boldsymbol{b}^*\rangle_{\mathbf{Y}}\,|t\rangle_T\,.$$

Computing $\mathbf{Z} \leftarrow \mathbf{X} - \mathbf{Y}$ gives

$$|\Phi_3\rangle \;=\; \frac{1}{\sqrt{P}} \sum_{t} \sum_j \alpha(j)\;\; |-2D^2 t\,\boldsymbol{b}^*\rangle_{\mathbf{Z}}\,|\mathbf{X}(j)\rangle_{\mathbf{X}}\,|\mathbf{X}(j) + 2D^2 t\,\boldsymbol{b}^*\rangle_{\mathbf{Y}}\,|t\rangle_T\,.$$

Tracing out $(\mathbf{X}, \mathbf{Y}, T)$ at this point leaves the mixed state

$$\rho_{\mathbf{Z}} \;=\; \frac{1}{P} \sum_{t\in\mathbb{Z}_P} |-2D^2 t\,\boldsymbol{b}^*\rangle\langle -2D^2 t\,\boldsymbol{b}^*|\,,$$

since the different t-branches are orthogonal in the T-register. Under Definition 2.17, Step $9^\dagger$.4 computes t from $\mathbf{Z}$ mod P and uncomputes the original T-register (and $\mathbf{X}, \mathbf{Y}$), yielding the factorized pure state

$$\Big(\sum_j \alpha(j)\,|\text{junk}(j)\rangle\Big) \;\otimes\; \frac{1}{\sqrt{P}} \sum_{t\in\mathbb{Z}_P} |-2D^2 t\,\boldsymbol{b}^*\rangle_{\mathbf{Z}}\,,$$

which is exactly Eq. (3.1). □

F Gate skeleton for the shift and difference

Route map. Items (1), (2), and (4) below are used only in the *re-evaluation route*; the *J-free route* uses item (3) directly to form $\mathbf{Z} \leftarrow -T \cdot \Delta$ and skips copy/difference. Cleanup (item (5)) applies to both routes (with the re-evaluation sub-steps when $\mathbf{Y}$ is present).

Each coordinate uses the same pattern (we suppress the index):

1. Copy: CNOTs (or modular adds) from X into Y.

2. Shift (optional re-evaluation route): add $2D^2b^* \cdot T$ into Y via a controlled modular adder with precomputed $2D^2b^* \pmod{M_2}$.

3. Shift (default J-free): set $Z \leftarrow -T \cdot \Delta \pmod{M_2}$ using double-and-add with Δ as read-only data (no classical access to $\boldsymbol{b}^*$).

4. Difference: set $Z \leftarrow X - Y$ using a modular subtractor; this can overwrite X if desired.

5. Cleanup: use the harvested $\Delta \leftarrow X(1) - X(0)$; compute $T' \leftarrow f(Z, \Delta)$ into an auxiliary by, for each p_η, choosing a coordinate with $\Delta_i \not\equiv 0 \pmod{p_\eta}$, inverting Δ_i modulo p_η, and CRT-recombining; if using the optional route, update $Y \leftarrow Y + \big(X(J+T-T') - X(J+T)\big)$ via the reversible evaluator U_{prep}; set $T \leftarrow T - T'$; if using the optional route, apply the inverse of the copy to clear Y; uncompute T' from Z. (All steps preserve Z.)

Phase discipline. All arithmetic inside U_{prep} uses classical reversible (Toffoli/Peres) adders/multipliers; no QFT-based adders are used. This ensures that applying U_{prep} on superpositions introduces no data-dependent phases.
Determinism across invocations. Basis calls to U_{coords} (such as $0, 1$ or $J, J{+}1$) use fixed classical constants within a single run so that $\mathbf{X}(\cdot)$ is reproducible as computational-basis data.

Variant: pair-evaluation without classical $\boldsymbol{b}^*$. Let U_{prep} denote the arithmetic evaluator that sends $|j\rangle\,|\mathbf{0}\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ using the harvested (V, Δ) (suppressing ancillary work registers). Retain a label $J \equiv j \pmod{P}$. Then implement Step $9^\dagger$.2 as follows:

1. Compute $J + T$ in place (mod P).

2. Run U_{prep} on input $J + T$ into Y to obtain $\mathbf{X}(j + T)$.

3. (Optionally) restore J by subtracting T.

The subsequent difference $Z \leftarrow X - Y$ yields $Z \equiv -2D^2T\,\boldsymbol{b}^* \pmod{M_2}$, with the offsets cancelling identically. This realization needs no classical access to $\boldsymbol{b}^*$ (nor to $\boldsymbol{v}^*$).

Implementation note. In practice, set $\Delta = \mathbf{X}(1) - \mathbf{X}(0)$ (harvested once) and reduce $(\Delta, \mathbf{Z})$ modulo each p_η in parallel. For each prime, choose the lexicographically smallest coordinate $i(\eta)$ with $\Delta_i \not\equiv 0 \pmod{p_\eta}$ (deterministic and reversible), compute $\Delta_{i(\eta)}^{-1} \pmod{p_\eta}$ via a reversible extended Euclidean algorithm, and form $T_\eta \equiv -\Delta_{i(\eta)}^{-1} Z_{i(\eta)} \pmod{p_\eta}$. Recombine the residues by a reversible CRT (e.g., Garner mixed-radix), keeping the mixed-radix digits and running-product moduli so they can be uncomputed exactly in reverse. Since $\gcd(D, P) = 1$ and each p_η is odd, the factors 2 and D^2 are units modulo every p_η, and residue accessibility guarantees the existence of at least one invertible coordinate per prime. Keep T' as a dedicated scratch register that is not modified by any other step until it is uncomputed by inverting its computation from $\mathbf{Z}$. For preparing $\frac{1}{\sqrt{P}} \sum_{t \in \mathbb{Z}_P} |t\rangle$, the per-prime preparation $\bigotimes_\eta \frac{1}{\sqrt{p_\eta}} \sum_{t_\eta \in \mathbb{Z}_{p_\eta}} |t_\eta\rangle$ followed by CRT wiring is exact and avoids approximation issues associated with a monolithic $\mathrm{QFT}_{\mathbb{Z}_P}$; this mirrors the modulus-splitting/CRT bookkeeping already used in Chen [2024]. The unit factor -2 in the generator is immaterial (any fixed unit modulo P yields the same annihilator); we keep it to match Eq. (1.1).

G Run-local determinism

A run is one coherent execution from the start of state preparation up to (and including) Step $9^{\dagger}$. Within a run, the coordinate evaluator U_{coords} uses a fixed set of classical constants (including any classical values obtained by earlier measurements in the same run, such as y', z', h^* in Chen [2024]). Hence, the basis outputs $\mathbf{X}(0)$ and $\mathbf{X}(1)$ are reproducible within that run. We harvest

$$V := \mathbf{X}(0), \qquad \Delta := \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\, \boldsymbol{b}^* \pmod{M_2},$$

once on literal inputs $j = 0, 1$ and then treat (V, Δ) as read-only basis data.

All superposition-time arithmetic (copy/shift/difference/cleanup) is implemented by classical reversible circuits (no QFT-based adders), so it is a permutation of computational-basis states and introduces no data-dependent phase (Lemma 2.11). We never call U_{coords} on a superposed input.

Approximate QFTs may be used for standard transforms; their approximation error is tracked separately (Remark after Theorem 3.5) and is unrelated to determinism of (V, Δ).

Across different runs, the upstream randomness, offsets, and even the arithmetic constants used by U_{coords} may change. Our proofs do not assume that (V, Δ) are identical across runs, nor do they assume any global seeding, device-level determinism, or that the overall global phase is fixed. The only place determinism is needed is to ensure that the single-run harvest (V, Δ) is well-defined and then reused verbatim by U_{prep} in that same run.

Under this scope, the cleanup step can always compute T' from $(\mathbf{Z}, \Delta)$ when Definition 2.17 holds, guaranteeing the factorization in Eq. (3.1). If desired, one may even measure (V, Δ) early and cache them as classical strings; this does not affect correctness or phases because we never feed U_{coords} with a superposition.