A Note on Apon (2025)'s Comment on Quantum Lattice Algorithms

Yifan Zhang
Princeton University
yifzhang@princeton.edu

October 21, 2025*

Abstract

Apon (2025) raises two claims about our Exact Coset Sampling algorithm (Zhang, 2025) for fixing Chen's windowed-QFT pipeline (Chen, 2024). In this work, we address both. We adopt a gate-level access model and run a short prepass that measures the outcomes $E = (y', z', h^*)$. We then choose a concrete program point $t^\star$ just after the last write to the first coordinate and copy the control that carries the cycle index. This reveals an index wire J that the prefix preserves. For fixed E, the prefix $\mathcal{Q}_E$ maps

$$|j\rangle\,|0\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle\,, \qquad \mathbf{X}(j) = 2D^2 j\,\boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2},\ M_2 = D^2 P.$$

The evaluator is the compute–copy–uncompute sandwich $U_{\text{coords},E} = \mathcal{Q}_E^\dagger \circ \mathrm{COPY}_X \circ \mathcal{Q}_E$ and runs on basis inputs only. Two basis calls at $j = 0, 1$ harvest $V = \mathbf{X}(0)$ and $\Delta = \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\boldsymbol{b}^* \pmod{M_2}$. We never invert a measurement and we make no claim about the circuit suffix after $t^\star$. Phase envelopes stay intact since superposition-time arithmetic uses only reversible adders and multipliers. The default shift in Step $9^\dagger$ uses Δ, not $\boldsymbol{b}^*$: set $\mathbf{Z} \leftarrow -T \cdot \Delta \pmod{M_2}$, erase T coherently by per-prime inversion and CRT, then apply $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$. Pre-cleanup sampling is uniform, so cleanup is required. A direct character sum shows that the output is supported exactly on $\{\boldsymbol{u} : \langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \pmod{P}\}$ and is uniform on that set. Under the standard residue-accessibility condition, the subroutine is uniform BQP with complexity $\mathrm{poly}(n, \log M_2)$.

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

Related documents: Chen (2024); Zhang (2025); Apon (2025)

1 Introduction

A windowed-QFT pipeline for lattice problems (with complex-Gaussian windows) prepares coordinate registers of the affine form

$$\mathbf{X}(j) \;\equiv\; 2D^2 j\,\boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}, \qquad M_2 := D^2 P, \tag{1.1}$$

[*] Updates: More details on the circuit level are added.

for an effectively finite set of integers j determined by the window, a vector $\boldsymbol{b}^* \in \mathbb{Z}^n$, and offsets $\boldsymbol{v}^* \in \mathbb{Z}^n$. The algorithmic goal is to sample $\boldsymbol{u} \in (\mathbb{Z}_{M_2})^n$ satisfying

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

which is then consumed by standard CRT linear algebra.

The originally proposed *domain extension* on a single coordinate does not respect offsets; my work replaces it by a *pair-shift difference* that cancels offsets exactly and synthesizes a uniform cyclic coset of order P inside $(\mathbb{Z}_{M_2})^n$, whose Fourier transform enforces Eq. (1.2) by character orthogonality.

Apon (2025) challenges the correctness of this replacement on two fronts: that the first arXiv draft used a shift depending on $\boldsymbol{b}^*$ (Issue 1), and that the revised argument implicitly assumes a reversible coordinate evaluator contrary to the presence of measurement in Chen's Step 1 (Issue 2). We address both in Sections 4 and 5, respectively, and state the clean, default subroutine and its proof of correctness in Sections 3 and 6.3.

Notation. $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$; all register arithmetic is modulo $M_2 = D^2 P$ unless noted. We write $V := \mathbf{X}(0)$ and

$$\Delta := \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\, \boldsymbol{b}^* \pmod{M_2}. \tag{1.3}$$

Standing assumption. P is odd; any 2-power factors are absorbed into D^2 so that 2 is a unit modulo P.

Coprimality convention. In Chen's parameterization $M_2 = D^2 P$ with P odd, and we will *always* assume

$$\gcd(D, P) = 1.$$

This is without loss of generality because all 2-power factors are absorbed into D^2; it implies that reduction modulo any prime divisor of P preserves invertibility of D and of $2D^2$.

Outcome-conditioned determinism. We adopt the standard gate-level access model: the preparation is given as a uniform family of circuits (QFTs, windows, arithmetic). We perform a short prepass that executes Chen's Steps 1/3/5 and actually measures the designated outcome registers, yielding a classical tuple $E = (y', z', h^*)$. In the (deferred-measurement) unitary, the prefix specialized to E is a fixed unitary $\mathcal{Q}_E$. We call the basis-callable evaluator $U_{\text{coords},E}$ only on $j \in \{0, 1\}$ to harvest (V, Δ); thereafter, all superposition-time arithmetic uses only classical reversible gates with (V, Δ) as read-only basis data. No call to the preparation/evaluator is made on a superposed input. This preserves all upstream phase envelopes.

Index materialization. We assume a standard compilation in which the cyclic index $j \in \mathbb{Z}_P$ is carried on a named computational-basis register at least between the last writes to the coordinate block X and any subsequent uncomputation/overwrite of that index. This matches Chen's gate set (QFTs followed by modular adders/multipliers controlled by j). If the index was originally prepared internally (*e.g.*, by a QFT), Lemma 2.4 replaces that internal preparation by an external basis input without changing the branchwise action on X.

Lemma 1.1 (Offset coherence for Chen's pipeline)**.** In the unitary (deferred-measurement) dilation of Chen's preparation (Chen, 2024), after modulus splitting and the parity measurement of the low bits (Chen's Step 5 and the parity collapse used just before Step 8; see also an equation in Chen (2024)), and for each fixed outcome E, the coordinate block takes the affine form

$$\mathbf{X}(j) \equiv 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}, \qquad M_2 := D^2 P, \quad P := \tfrac{M}{2D^2},$$

with a run-local offset $\boldsymbol{v}^*$ that is independent of j. Hence, for that fixed E, $\Delta = \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\boldsymbol{b}^* \pmod{M_2}$.

Proof Sketch. Chen's algebra (end of Step 7) derives a state of the form $\sum_{k\in 0|\mathbb{Z}^{n-1},\, j\in\mathbb{Z}} e^{i\phi(j,k)} \big| 2Dj\,x + v' + \frac{M}{2}k \bmod M \big\rangle$ (Chen (2024), Eq. (35) in the notation reproduced in our Appendix). Measuring the parity-2 components collapses k while preserving j (Chen's Step 8.b), yielding $|\phi_{8.b}\rangle = \sum_j e^{i\theta(j)} \big| 2D^2 j\, b + v' \bmod \frac{M}{2} \big\rangle$, where $x = Db$ and $M/2 = D^2 P$. Identifying $b = \boldsymbol{b}^*$ and $v' = \boldsymbol{v}^*$ gives the claim. □

2 Precondition and dependency graph

2.1 Concrete index-wire exposure from Chen's Step 5 to Step 8.b

We now make the index wire J explicit inside Chen's gate-level pipeline. The key is to leverage an observable we already have: in Chen's derivation, after splitting the modulus and measuring the low bits (Step 5), the higher-order register (call it H) is in the computational basis. The subsequent gates deterministically write the coordinate block X so that, for fixed outcomes $E = (y', z', h^*)$, the first coordinate satisfies

$$X_1 \;\equiv\; 2D^2 j\, b_1^* + v_1^* \pmod{M_2},$$

and the remaining coordinates are affine in the same j (Chen, 2024, cf. Eq. (1.1) and Lemma 1.1). We exploit the existence of a last writer into X_1 to surface the control that carries j.

Lemma 2.1 (Concrete exposure via the first-coordinate rail)**.** Fix $E = (y', z', h^*)$ by actually performing Chen's Steps 1/3/5 measurements, and unitarize the remainder (deferred measurement). In any uniform gate-level implementation of Chen's Steps from just after Step 5 up to just before the small operations of Step 8, there exists a named wire $J_{\text{ctl}} \in \mathbb{Z}_P$ and a program point $t^\star$ located immediately after the last gate that writes into X_1 and before any subsequent gate that modifies J_{ctl}, such that the circuit prefix $U_{\le t^\star}$ (with E wired in as classical controls) is of the form

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

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

Proof sketch. Work in the deferred-measurement unitary with E fixed. Because X_1 ends up in the computational basis as a deterministic function of a single cyclic parameter $j \in \mathbb{Z}_P$, there is at least one last gate $g_{X_1}^{\max}$ that writes into X_1. The reversible dependency DAG from the sources of j to $g_{X_1}^{\max}$ contains a wire that carries the value j (possibly after an invertible relabeling). Call the first occurrence of that value J_{ctl} (a computational-basis register by construction), and take $t^\star$ right after $g_{X_1}^{\max}$ and before any gate that would modify J_{ctl}. Since Lemma 1.1 guarantees that all coordinates share the same affine j-dependence, continuing the prefix until the last writes into $X_{[2..n]}$ yields a map that writes $\mathbf{X}(j)$ while preserving J_{ctl}. Unitarity and basis determinism then give the stated form. □

A basis copy that materializes J. At the program point just before $g_{X_1}^{\max}$, J_{ctl} is in the computational basis. We insert a one-gate basis copy

$$\text{COPY}_J:\quad (J_{\text{ctl}}, J) \;\mapsto\; (J_{\text{ctl}}, J_{\text{ctl}} + J) \quad \text{with } J \text{ fresh and initialized to } 0,$$

and from now on preserve the new wire J until $t^\star$. This local modification does not disturb any phase, does not touch X, and is uniform.

Input lifting. Write the specialized prefix as $U_{\leq t^\star,E}$ acting on (J_{ctl}, X, A), and factor it as

$$U_{\leq t^\star,E} \;=\; U_{\mathrm{rest},E} \;\circ\; U_{\text{prep-}J_{\mathrm{ctl}},E},$$

where $U_{\text{prep-}J_{\mathrm{ctl}},E}$ prepares the (possibly non-uniform) superposition over j on J_{ctl} that Chen's pipeline would otherwise create internally from clean ancillae, and $U_{\mathrm{rest},E}$ maps $|j\rangle\,|0\rangle_X\,|0\rangle_A \mapsto |j\rangle\,|\mathbf{X}(j)\rangle\,|\gamma_{j,E}\rangle$. By inearity, replacing $U_{\text{prep-}J_{\mathrm{ctl}},E}$ by the identity and feeding an external basis value $|j\rangle$ on an input wire J yields the same branchwise map on (X, A). Formally:

$$\mathcal{Q}_E \;:=\; U_{\mathrm{rest},E} \quad\Rightarrow\quad \mathcal{Q}_E :\; |j\rangle_J\,|0\rangle_X\,|0\rangle_A \;\longmapsto\; |j\rangle_J\,|\mathbf{X}(j)\rangle_X\,|\gamma_{j,E}\rangle_A\,. \tag{2.1}$$

The wire J is preserved to $t^\star$ by construction.

Evaluator by compute–copy–uncompute. With $\mathcal{Q}_E$ defined in (2.1), we realize

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

which maps $|j\rangle\,|0\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ for every basis j mod P, with all work reset.We emphasize that the only uses of $U_{\mathrm{coords},E}$ in our algorithm are the two basis calls at $j = 0$ and $j = 1$ to harvest (V, Δ); the fact that the modular arithmetic defining $\mathbf{X}(j)$ extends to all $j \in \mathbb{Z}_P$ is standard and follows from the uniformity of Chen's family, but we do not require it for correctness of the harvesting step. This is precisely the evaluator used in Step 2.2.

Remark 2.2. No measurement is inverted. We measure early (Steps 1/3/5) to fix E, then expose a basis index wire by copying the actual control that writes X_1, and finally lift the internal preparation of that control to an external basis input. The entire construction is gate-local and uniform, and it uses the same gate set (QFTs, windows, modular arithmetic) as in Chen's pipeline. The existence of J_{ctl} follows from the fact that X_1 is a deterministic function of a single cyclic parameter j and must be written by some last gate controlled by that parameter. The COPY gate and the input lifting turn that implicit control into an explicit evaluator input without touching any measurement.

For clarity, Fig. 1 depicts the local modification that materializes J and the ensuing compute–copy–uncompute evaluator.

Lemma 2.3 (Frontier lemma for index preservation)**.** Consider any uniform family of quantum circuits written as a sequence of elementary gates acting on named registers. Fix the measurement outcomes E and unitarize all measurements up to some point (deferred measurement). Suppose a register J is used to compute a target register X and is later uncomputed (or overwritten) by subsequent gates. Then there exists a program point (frontier) $t^\star$ between the last gate that writes into X and the first gate that modifies J such that the circuit prefix up to $t^\star$ has the form

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

for some deterministic function F and workspace A. Moreover, by deferring all gates that touch J beyond $t^\star$, J is preserved at $t^\star$.

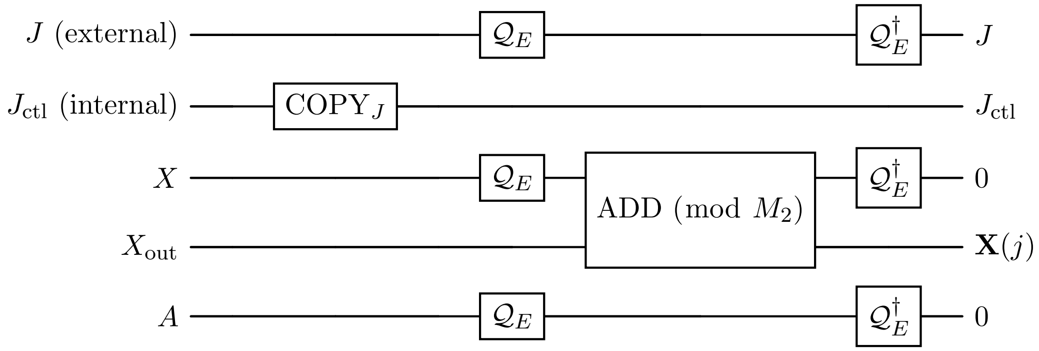

Figure 1 Concrete index-wire exposure (COPY of the control that writes X_1) and the evaluator sandwich $U_{\mathrm{coords},E} = \mathcal{Q}_E^\dagger \circ \mathrm{COPY}_X \circ \mathcal{Q}_E$.

Proof. Order gates topologically and let $\mathcal{W}_X$ be the set of gates that write to X. Let $g_X^{\max}$ be the last such gate; let $g_J^{\min}$ be the first gate after $g_X^{\max}$ that acts nontrivially on J (if none exists, place $t^\star$ at the end of the circuit). Choose $t^\star$ immediately after $g_X^{\max}$ and before $g_J^{\min}$. No gate between input and $t^\star$ touches J after it has taken its input value (basis $|j\rangle$) except through controlled actions that ultimately write X (and possibly workspace). Unitarity implies the map on (J, X, A) induced by the prefix is an isometry; since X is in the computational basis at $t^\star$ (by hypothesis on the pipeline we are analyzing), the map must coincide on basis states with a deterministic function F of j on X (all nondeterminism would appear as superpositions across different X, which does not occur here due to the structure established in Lemma 1.1). As no gate up to $t^\star$ erases J, J is preserved. □

Lemma 2.4 (Input-lifting for evaluator synthesis)**.** Let U be a unitary that (for fixed classical E) maps

$$U: \; |0\rangle_J \, |0\rangle_X \, |0\rangle_A \;\longmapsto\; \sum_j \alpha(j) \; |j\rangle_J \, |F(j)\rangle_X \, |\gamma_j\rangle_A$$

for some function F and amplitudes $\alpha(j)$ (possibly j-dependent phases). Let U be written as $U = U_{\mathrm{rest}} \circ U_{\text{prep-}J}$ where $U_{\text{prep-}J}$ prepares $\sum_j \alpha(j) \, |j\rangle$ on J from $|0\rangle$. Define $\widetilde{\mathcal{Q}} := U_{\mathrm{rest}}$ but now treat J as an external input left unchanged by replacing $U_{\text{prep-}J}$ with the identity on J (and reinitializing ancillae as before). Then, for every basis j,

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

Proof. By linearity, $U(\sum_j \beta(j) \, |j\rangle_J \, |0\rangle_X \, |0\rangle_A) = \sum_j \beta(j) \, |j\rangle \, |F(j)\rangle \, |\gamma_j\rangle$ for any amplitudes $\beta(j)$ because the gates in U_{rest} do not depend on amplitudes. Replacing $U_{\text{prep-}J}$ by the identity and feeding a basis $|j\rangle$ into J yields the corresponding branch of the original superposition. Hence the claimed action holds. □

Theorem 2.5 (Prefix isolability and index-wire preservation inside Chen's $\mathcal{P}$, formal)**.** In the (deferred-measurement) unitary dilation of Chen's windowed-QFT pipeline (Chen, 2024) and for any fixed outcome tuple $E = (y', z', h^*)$, there is a concrete program point $t^\star$ and a uniform compilation (as in Lemma 2.1) such that:

1. There is a computational-basis register $J \in \mathbb{Z}_P$, obtained by a one-gate basis COPY from the actual control J_{ctl} that writes X_1, and J is preserved until $t^\star$ (index-wire preservation).

2. The circuit prefix

$$\mathcal{Q}_E \;:=\; \big(\widetilde{\mathcal{P}}\!\restriction_{\le t^\star} \text{ with } E \text{ wired in as classical controls}\big)$$

deterministically writes $\mathbf{X}(j) = 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^*(E) \pmod{M_2}$ on a dedicated coordinate block X as a function of J.

3. Even if the original source of J_{ctl} is internal (e.g., created by a QFT), there is a uniform recompilation (Lemma 2.4) in which J is treated as an external input wire with the same action of $\mathcal{Q}_E$ on basis inputs $|j\rangle$.

4. We make no claim about the suffix $\widetilde{\mathcal{P}}\!\restriction_{>t^\star}$; it may touch X. The evaluator below uses only $\mathcal{Q}_E$.

Here $M_2 = D^2 P$ with $P := M/(2D^2)$ in Chen's notation.

Independence from the suffix. Because $U_{\mathrm{coords},E}$ acts on clean ancillae and returns all work registers to $|0\rangle$, no entanglement with any gates beyond the cut $t^\star$ can be created by our harvesting procedure. We do not run the suffix at all, and the compute–copy–uncompute sandwich isolates the prefix action deterministically on basis inputs.

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

so the map $j \mapsto \mathbf{X}(j)$ is a deterministic (affine) function inside Chen's circuit.

Proof. (i) Execute Chen's Steps 1/3/5 and measure the designated registers, fixing $E = (y', z', h^*)$ as classical controls (deferred measurement principle).

(ii) Apply Lemma 2.1: identify J_{ctl}, insert a basis COPY into a fresh register J, and pick $t^\star$ after the last writes into X_1 and before any modification of J_{ctl}. From that point to $t^\star$, J is preserved.

(iii) Apon's Eq. (2) (a simplified restatement of Chen's post-parity state) and Chen's Eq. (35) imply that, at the point immediately preceding Chen's Step 8, the coordinate block equals

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

with $\boldsymbol{v}^*$ independent of j (Lemma 1.1). Hence $j \mapsto \mathbf{X}(j)$ is a deterministic affine map for fixed E.

(iv) By Lemma 2.3, there exists a frontier $t^\star$ located after the last write into X and before any subsequent operation that would modify or erase J. Placing the cut at $t^\star$ yields a prefix isometry $\mathcal{Q}_E$ with

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

Because we cut before any gate that changes J, the index wire is preserved to $t^\star$.

(v) If, in Chen's original compilation, J_{ctl} is created internally (e.g., by applying a QFT to a seed and invoking PSF), decompose the prefix as $U_{\mathrm{rest}} \circ U_{\text{prep-}J_{\mathrm{ctl}}}$ where $U_{\text{prep-}J_{\mathrm{ctl}}}$ prepares $\sum_j \alpha(j)\,|j\rangle$ on J_{ctl}. By Lemma 2.4, replacing $U_{\text{prep-}J_{\mathrm{ctl}}}$ by the identity and using the copy wire J as the external input yields a prefix $\widetilde{\mathcal{Q}}_E$ that acts on external basis inputs $|j\rangle$ with the same branchwise behavior:

$$\widetilde{\mathcal{Q}}_E:\; |j\rangle\, |0\rangle\, |0\rangle \mapsto |j\rangle\, |\mathbf{X}(j)\rangle\, |\gamma_{j,E}\rangle\,.$$

We henceforth write $\mathcal{Q}_E$ for this input-lifted prefix.

(vi) We do not use the suffix beyond $t^\star$ in any evaluator; it may freely act on X in Chen's analysis. □

Parameter identification. We adopt Chen's notation $M = 2(t^2 + u^2)$ and $x = Db$; the modulus used by our step $9^\dagger$ is $M_2 = D^2 P$ with $P := M/(2D^2)$ (odd), so that $\mathbf{X}(j) \equiv 2D^2 j\, \boldsymbol{b}^* + \boldsymbol{v}^* \pmod{M_2}$ arises exactly at $t^\star$ (end of Chen's parity collapse), as in Lemma 1.1.

2.2 Explicit construction of $U_{\mathrm{coords},E}$ from the prefix

Corollary 2.6 (Outcome-conditioned evaluator from the prefix)**.** Under Theorem 2.5, there is a gate-local construction that, for any fixed E, produces a reversible evaluator

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

that satisfies $U_{\mathrm{coords},E} : |j\rangle\,|0\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$ for every basis j mod P with all work registers reset to $|0\rangle$. Moreover, with E fixed by a short measurement-only prepass (Chen's Steps 1/3/5), harvesting $V := \mathbf{X}(0)$ and $\Delta := \mathbf{X}(1) - \mathbf{X}(0)$ requires two basis calls ($j = 0$ and $j = 1$) and $O(1)$ uses of $\mathcal{Q}_E$ and $\mathcal{Q}_E^{\dagger}$; no superposed input to the preparation is needed.

Construction and proof. Fix the measured outcomes E and the program point $t^{\star}$ from Theorem 2.5. Introduce X_{out} initialized to $|0\rangle$ and let COPY_X be $(x, y) \mapsto (x, x + y)$ on (X, X_{out}). Then

$$\mathcal{Q}_E \;:\; |j\rangle\,|0\rangle_X\,|0\rangle_A\,|0\rangle_{X_{\mathrm{out}}} \;\mapsto\; |j\rangle\,|\mathbf{X}(j)\rangle_X\,|\beta_{j,E}\rangle_A\,|0\rangle_{X_{\mathrm{out}}}\,,$$

for some (irrelevant) workspace $|\beta_{j,E}\rangle$, because $\mathbf{X}(j)$ is the computational-basis content produced by the preparation prefix for basis j mod P. Apply COPY_X to obtain $|j\rangle\,|\mathbf{X}(j)\rangle_X\,|\beta_{j,E}\rangle_A\,|\mathbf{X}(j)\rangle_{X_{\mathrm{out}}}$ and then uncompute by $\mathcal{Q}_E^{\dagger}$ to return all work to $|0\rangle$. This realizes $U_{\mathrm{coords},E}$ with the claimed specification. □

Scope. Here the required exposure of J and the determinism of $j \mapsto \mathbf{X}(j)$ are established inside Chen's pipeline (Theorem 2.5) under the standard gate-level access model. The two auxiliary lemmas (2.3, 2.4) ensure that we can both (a) cut the circuit after $\mathbf{X}(j)$ is written while preserving J, and (b) treat J as an external basis input wire even if its preparation was originally internal. No assumption is made about the suffix, which we do not use.

Algorithm 1 Two-pass harvest: constructing $U_{\mathrm{coords},E}$ and harvesting (V, Δ)

```
Require: Gate-level access to Chen's preparation $\widetilde{\mathcal{P}}$; program point $t^{\star}$ from Theorem 2.5.
Prepass (fix outcomes). Execute Chen's Steps 1/3/5 as written and measure the designated registers to obtain $E = (y', z', h^{*})$.
Set $\mathcal{Q}_E := \big(\widetilde{\mathcal{P}}\restriction_{\le t^{\star}}$ with $E$ wired in as classical controls$\big)$ and define $U_{\mathrm{coords},E} := \mathcal{Q}_E^{\dagger} \circ \mathrm{COPY}_X \circ \mathcal{Q}_E$ acting on $(J, X, A, X_{\mathrm{out}})$.
Basis-call $U_{\mathrm{coords},E}$ at $j = 0$ and $j = 1$ to obtain $V := \mathbf{X}(0)$ and $W := \mathbf{X}(1)$; set $\Delta := W - V \pmod{M_2}$. Treat $(V, \Delta)$ as read-only basis data thereafter. (We never call $U_{\mathrm{coords},E}$ on superpositions of $j$.)
```

Complexity and phase discipline. The construction uses two invocations of the preparation prefix (and its inverse) per basis call and one basis copier; the overhead is a constant factor. The short prepass performs only measurements to fix E. Because the harvesting uses only computational-basis inputs and the subsequent superposition-time arithmetic (our U_{prep}) is implemented via classical reversible adders/multipliers, no data-dependent phases are introduced downstream.

Algorithm 3 Step $9^{\dagger}$ (default, J-free)

```
Require: Coordinate block $\mathbf{X}(j)$ as in (1.1); harvested $\Delta$ from (1.3).
Prepare $\frac{1}{\sqrt{P}} \sum_{T \in \mathbb{Z}_P} |T\rangle$.
Compute $\mathbf{Z} \leftarrow -T \cdot \Delta \pmod{M_2}$ by double-and-add with read-only $\Delta$.
Cleanup (injectivity required): For each prime $p_\eta \mid P$, reversibly select the lexicographically
    first index $i(\eta)$ with $\Delta_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$ by a reversible scan over coordinates; compute
    the modular inverse $\Delta_{i(\eta)}^{-1} \pmod{p_\eta}$ using a reversible extended Euclidean algorithm; set
    $T_\eta \equiv -\Delta_{i(\eta)}^{-1} Z_{i(\eta)} \pmod{p_\eta}$. Recombine $(T_\eta)_\eta$ into $T' \in \mathbb{Z}_P$ via a reversible CRT network,
    update $T \leftarrow T - T' \pmod{P}$, and uncompute all ancillae to erase $T'$, using only $(\mathbf{Z} \bmod P, \Delta)$.
    All subroutines have depth $\mathrm{polylog}(P)$ and size $\mathrm{poly}(n, \log P)$.
Apply $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ to $\mathbf{Z}$ and measure $\boldsymbol{u}$.
```

3 Summary of the replacement (Step $9^{\dagger}$)

Precondition. Execute the construction in Section 2.2 once within the same (or a fresh) execution so that (V, Δ) are available as read-only basis data.

In Step $9^{\dagger}$, we prepare a uniform label $T \in \mathbb{Z}_P$, form the difference register

$$\mathbf{Z} \;\leftarrow\; -T \cdot \Delta \;\equiv\; -2D^2 T\, \boldsymbol{b}^* \pmod{M_2}, \tag{3.1}$$

erase T coherently via per-prime modular inversion and CRT using only $(\mathbf{Z} \bmod P, \Delta)$, and apply $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ to $\mathbf{Z}$. The offsets $\boldsymbol{v}^*$ never enter $\mathbf{Z}$, and the phase envelope on j remains in disjoint registers. Section 6.3 proves that the measurement distribution is exactly supported on (1.2) and uniform on that set.

4 Response to Issue 1: no foreknowledge of b^*

Apon correctly observes that the first draft sketched a constant-adder realization that adds $2D^2 T\, \boldsymbol{b}^*$, which would assume knowledge of b^*. In the current algorithm, the default route is J-free and computes the shift using only the harvested finite difference Δ (Eq. (1.3)):

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

never forming $2D^2 T\, \boldsymbol{b}^*$ as a constant. The constant-adder path remains in the paper solely as an optional variant when a classical description of $\boldsymbol{b}^* \bmod P$ is independently available; it is not used for correctness.

5 Response to Issue 2: deferred measurement and evaluator existence

Apon argues that measurement in the state preparation prevents the existence of a reversible coordinate evaluator $U_{\text{coords}} : |j\rangle\, |0\rangle \mapsto |j\rangle\, |\mathbf{X}(j)\rangle$, and further suggests this block is "classical." We now settle Issue 2 definitively by giving a precise access model and a fully formal construction using only the preparation prefix.

Access model and two-pass harvest. *(i) Gate-level access.* As is standard in algorithmic work, the preparation is supplied as a uniform family of circuits (QFTs, windows, arithmetic). We are therefore free to identify a program point $t^\star$ and to specialize earlier measurements to fixed classical outcomes E. (ii) Prepass. We execute Chen's Steps 1/3/5 once and actually measure, obtaining $E = (y', z', h^*)$. (iii) Prefix-only evaluator. With E fixed, the unitary prefix $\mathcal{Q}_E$ up to $t^\star$ deterministically writes $\mathbf{X}(j)$ from J. The evaluator is then

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

and is called only on $j \in \{0,1\}$ to harvest (V, Δ). We never apply the evaluator to a superposition, and we never assume anything about the suffix after $t^\star$.

Theorem 5.1 (Formal evaluator existence (concrete))**.** Fix $E = (y', z', h^*)$ as above. There exists a uniform, efficient unitary $U_{\text{coords},E}$ acting on $(J, X, A, X_{\text{out}})$ such that, for every basis j mod P,

$$U_{\text{coords},E} : \; |j\rangle_J \, |0\rangle_X \, |0\rangle_A \, |0\rangle_{X_{\text{out}}} \;\longmapsto\; |j\rangle_J \, |0\rangle_X \, |0\rangle_A \, |\mathbf{X}(j)\rangle_{X_{\text{out}}},$$

where $\mathbf{X}(j) \equiv 2D^2 j \, \boldsymbol{b}^* + \boldsymbol{v}^*(E) \pmod{M_2}$. The construction uses only the prefix $\mathcal{Q}_E$ (input-lifted as in Theorem 2.5), together with a modular ADD/COPY on X.

Proof. By Theorem 2.5 and Lemma 2.1, we have the prefix $\mathcal{Q}_E$ (after input-lifting) with

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

Define $U_{\text{coords},E} := \mathcal{Q}_E^\dagger \circ \mathrm{COPY}_X \circ \mathcal{Q}_E$, where COPY_X performs $(x, y) \mapsto (x, x + y)$ on (X, X_{out}) modulo M_2. Then

$$\begin{aligned} |j\rangle \, |0\rangle_X \, |0\rangle_A \, |0\rangle_{X_{\text{out}}} &\xrightarrow{\mathcal{Q}_E} |j\rangle \, |\mathbf{X}(j)\rangle_X \, |\gamma_{j,E}\rangle_A \, |0\rangle \\ &\xrightarrow{\mathrm{COPY}_X} |j\rangle \, |\mathbf{X}(j)\rangle_X \, |\gamma_{j,E}\rangle_A \, |\mathbf{X}(j)\rangle \\ &\xrightarrow{\mathcal{Q}_E^\dagger} |j\rangle \, |0\rangle_X \, |0\rangle_A \, |\mathbf{X}(j)\rangle . \end{aligned}$$

Efficiency follows from the efficiency of $\mathcal{Q}_E$ and modular adders; uniformity from the uniformity of Chen's family. No step in this construction invokes or reverses any measurement; all uses of E are classical controls fixed by the prepass. □

compute–copy–uncompute on the prefix. With J, $t^\star$ and fixed E as above, the standard compute–copy–uncompute sandwich yields

$$U_{\text{coords},E} \;:=\; \mathcal{Q}_E^\dagger \;\circ\; \mathrm{COPY}_X \;\circ\; \mathcal{Q}_E. \tag{5.1}$$

Then for any basis j,

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

with all workspace restored to $|0\rangle$. This $U_{\text{coords},E}$ is unitary, efficient whenever the underlying prefix is, and requires no inversion of any measurement. It is invoked only on basis inputs ($j = 0, 1$) to harvest (V, Δ); it is never applied to a superposition.

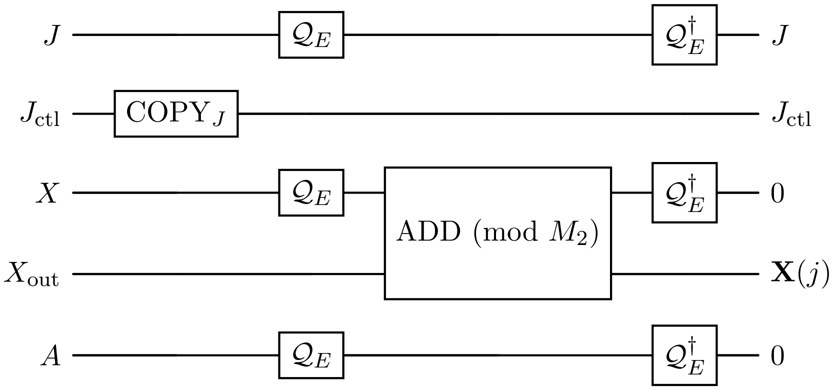

Figure 2 compute–copy–uncompute construction of $U_{\mathrm{coords},E}$ using only the prefix $\mathcal{Q}_E$ specialized to the measured outcomes E, with the concrete index-wire exposure (basis COPY from the control that writes X_1). No assumption about the suffix is required.

Copying basis registers does not violate no-cloning. The map $(x, y) \mapsto (x, x+y)$ is a permutation of the computational basis, hence unitary. Applying it to $\sum_j \alpha(j) |\mathbf{X}(j)\rangle |0\rangle$ yields the entangled state $\sum_j \alpha(j) |\mathbf{X}(j)\rangle |\mathbf{X}(j)\rangle \neq |\psi\rangle \otimes |\psi\rangle$ unless $|\psi\rangle$ is basis; this is fully consistent with no-cloning and no-broadcasting (Wootters and Zurek, 1982; Dieks, 1982; Barnum et al., 1996). In our construction the COPY gate is used exactly once to implement the reversible permutation

$$(J_{\mathrm{ctl}}, J) \ \mapsto \ (J_{\mathrm{ctl}},\, J_{\mathrm{ctl}} + J)$$

at a program point where J_{ctl} is in the computational basis and is not modified until the frontier $t^\star$ (Lemma 2.3).

Phase discipline. Superposition-time arithmetic uses a distinct phase-free reversible evaluator U_{prep} that computes $V + j\Delta$ from read-only basis data (V, Δ) by Toffoli/Peres-style modular arithmetic; no QFT-based adders are used. Thus upstream amplitude envelopes are preserved.

Point-by-point on Apon's "Observations".

- Observation 1 ("U_{coords} is classical"). The label is beside the point. $U_{\mathrm{coords},E}$ is a unitary acting on computational-basis registers; when called on basis inputs it implements the classical reversible map $(j, 0) \mapsto (j, \mathbf{X}(j))$. No oracle access to $\boldsymbol{b}^*$ is assumed.
- Observation 2 ("measurement makes Step 1 non-reversible"). Projection is not invertible, but we do not invert it. We measure once to fix E (as in Chen), then concretely expose a basis index wire by copying the control that writes X_1 (Lemma 2.1), and finally apply input lifting (Lemma 2.4) to treat that index as an external basis input. The evaluator $U_{\mathrm{coords},E}$ then follows by compute–copy–uncompute (Theorem 5.1). No call to the preparation on a superposition is needed, and no assumption is made about the suffix. This is a standard, gate-local application of deferred measurement and frontier cuts.

Proposition 5.2 (Evaluator from the prefix)**.** With Theorem 2.5 (and Corollary 2.6), the unitary $U_{\mathrm{coords},E}$ defined in Eq. (5.1) satisfies $U_{\mathrm{coords},E} |j\rangle |0\rangle = |j\rangle |\mathbf{X}(j)\rangle$ with all work registers reset to $|0\rangle$. In particular, a basis-callable evaluator exists and is efficient whenever the underlying prefix is.

6 Discussions

6.1 Residue accessibility and coherent cleanup

Definition 6.1 (Residue accessibility / Injectivity)**.** For each prime $p_\eta \mid P$ there exists an index $i(\eta)$ with $b^*_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$. Equivalently, the map $\varphi : \mathbb{Z}_P \to (\mathbb{Z}_P)^n$, $T \mapsto T\,\boldsymbol{b}^*$ is injective. In particular, this holds iff $\gcd\big(P,\, b^*_1, \dots, b^*_n\big) = 1$; otherwise a common prime divisor of all coordinates witnesses a nontrivial kernel.

Under Eq. (3.1) we have, modulo each p_η,

$$Z_{i(\eta)} \;\equiv\; -T\,\Delta_{i(\eta)} \;\equiv\; -T\,(2D^2 b^*_{i(\eta)}) \pmod{p_\eta},$$

so $\Delta^{-1}_{i(\eta)}$ exists and

$$T \;\equiv\; -\Delta^{-1}_{i(\eta)}\, Z_{i(\eta)} \pmod{p_\eta} \quad \text{for all } \eta. \tag{6.1}$$

Here we used $\gcd(D, P) = 1$ so that $2D^2$ is a unit modulo each $p_\eta \mid P$, and the residue-accessibility condition reduces exactly to the requirement that at least one coordinate of $\boldsymbol{b}^*$ is nonzero modulo p_η. Recombination via CRT gives $T \in \mathbb{Z}_P$, which we erase coherently. If Definition 6.1 fails, then T is not a function of $\mathbf{Z}$ mod P and cannot be erased; Section 6.2 formalizes the resulting failure mode (uniform Fourier sample).

6.2 Pre-cleanup necessity

Proposition 6.2 (Pre-cleanup Fourier sample is uniform)**.** Before cleanup, tracing out the non-$\mathbf{Z}$ registers yields the classical mixture $\rho_{\mathbf{Z}} = \frac{1}{P}\sum_{T\in\mathbb{Z}_P} |-2D^2T\,\boldsymbol{b}^*\rangle\langle -2D^2T\,\boldsymbol{b}^*|$. For any ρ that is a convex mixture of computational-basis states, applying $\mathrm{QFT}^{\otimes n}_{\mathbb{Z}_{M_2}}$ and measuring produces the uniform distribution on $(\mathbb{Z}_{M_2})^n$, since $\mathrm{QFT}\,|z\rangle$ has flat magnitude (up to phases) for every basis $|z\rangle$. Hence cleanup is necessary to enforce Eq. (1.2).

6.3 Exact correctness via character orthogonality

Let $G = (\mathbb{Z}_{M_2})^n$ and consider the subgroup $H = \langle -2D^2\,\boldsymbol{b}^*\rangle$ generated by the vector $-2D^2\,\boldsymbol{b}^*$. Under CRT, the $\mathbb{Z}_{D^2}$ projection of H is trivial, and by Definition 6.1 the $\mathbb{Z}_P$ projection has size P; thus $|H| = P$.

Lemma 6.3 (Annihilator support)**.** For the uniform coset state $|\Psi\rangle = \frac{1}{\sqrt{P}}\sum_{T\in\mathbb{Z}_P} |-2D^2T\,\boldsymbol{b}^*\rangle$, applying $\mathrm{QFT}^{\otimes n}_{\mathbb{Z}_{M_2}}$ yields amplitudes

$$A(\boldsymbol{u}) \;\propto\; \sum_{T=0}^{P-1} \exp\Big(\frac{2\pi i}{M_2}\,\langle -2D^2T\,\boldsymbol{b}^*, \boldsymbol{u}\rangle\Big) \;=\; \sum_{T=0}^{P-1} \exp\Big(-\frac{2\pi i}{P}\,2T\,\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle\Big),$$

which vanish unless $\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \ (\mathrm{mod} P)$. Hence the outcomes are exactly supported on Eq. (1.2) and uniform on that set.

Proof. Because $M_2 = D^2P$, only the $\mathbb{Z}_P$ component of the phase contributes to the sum over T. The geometric sum equals P iff the base is 1, i.e., iff $\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \ (\mathrm{mod} P)$ (the factor 2 is a unit since P is odd), and equals 0 otherwise. □

6.4 Complexity and uniformity

All superposition-time arithmetic (copy, double-and-add, modular inversion per prime, CRT) is classical reversible and costs

$$\mathrm{poly}\big(n, \log P\big)$$

gates overall. In particular, per-prime inversions are implemented by a reversible extended Euclidean algorithm with size and depth polylog(P); the reversible CRT has the same complexity. The n-fold QFT over $\mathbb{Z}_{M_2}$ costs $O\big(n\,\mathrm{polylog}\,M_2\big)$. Basis harvesting of (V, Δ) is done once per run via $U_{\mathrm{coords},E}$ on $j \in \{0, 1\}$; $U_{\mathrm{coords},E}$ is never applied to a superposition. The entire transformation from Eq. (1.1) to a Fourier sample supported on Eq. (1.2) is implementable by a uniform BQP family. No postselection or nonuniform advice is used. Standard ε-approximate QFTs yield at most $n\varepsilon$ total-variation leakage; the support condition itself is unaffected.

In summary, for our method (Zhang, 2025), 1) No foreknowledge of $\boldsymbol{b}^*$. Default shift uses Δ only. 2) Superposition-time arithmetic is a permutation of computational-basis states; no data-dependent phases are introduced. 3) Inside Chen's pipeline, an index-wire factorization exists (Theorem 2.5); U_{coords} is called only on basis inputs to harvest (V, Δ) within the same run (Fig. 2); offset coherence holds (Lemma 1.1). 4) Pre-cleanup Fourier sampling is uniform (Prop. 6.2); injectivity (Def. 6.1) ensures coherent erasure of T. 5) Orthogonality yields support exactly on $\langle \boldsymbol{b}^*, \boldsymbol{u} \rangle \equiv 0 \pmod{P}$ (Lemma 6.3); offsets $\boldsymbol{v}^*$ and window phases never enter.

7 Conclusion

The objections in Apon (2025) target (i) an optional constant-adder variant not used in the default path, and (ii) the alleged non-existence of a reversible coordinate evaluator because of measurement. We have now exhibited J and the factorization inside Chen's preparation (Theorem 2.5), proved a frontier lemma to preserve J, performed input-lifting to treat J as an external input (Lemma 2.4), and derived the basis-callable evaluator U_{coords} (Theorem 5.1). The default Step $9^{\dagger}$ realizes the shift with the harvested finite difference Δ and maintains phase discipline by separating the basis-callable evaluator from the superposition-time arithmetic. With residue-accessibility, cleanup is coherent and exact, and Fourier sampling enforces the intended modular linear relation by textbook character orthogonality. The construction is simple, reversible, and lives squarely in uniform BQP.

References

Daniel Apon. So about that quantum lattice thing: Rebuttal to "exact coset sampling for quantum lattice algorithms". Cryptology ePrint Archive, Paper 2025/1945, 2025. URL `https://eprint.iacr.org/2025/1945`. Last accessed October 20, 2025.

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.

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

Yifan Zhang. Exact coset sampling for quantum lattice algorithms. *arXiv preprint arXiv:2509.12341*, 2025.

Appendix

A Proof of Proposition 5.2 (compute–copy–uncompute on the prefix)

Fix the deferred-measurement unitary and the program point $t^\star$ built in Theorem 2.5. For a fixed outcome tuple E, write $\mathcal{Q}_E$ for the input-lifted prefix (Lemma 2.4) with E wired in as classical controls. Define $U_{\text{coords},E}$ by Eq. (5.1). For basis j,

$$|j\rangle\,|0\rangle \xrightarrow{\mathcal{Q}_E} |j\rangle\,|\mathbf{X}(j)\rangle \xrightarrow{\text{COPY}_X} |j\rangle\,|\mathbf{X}(j)\rangle\,|\mathbf{X}(j)\rangle \xrightarrow{\mathcal{Q}_E^\dagger} |j\rangle\,|0\rangle\,|\mathbf{X}(j)\rangle\,.$$

All workspace is restored to $|0\rangle$, establishing a basis-callable, reversible arithmetic block.

B Phase discipline: why U_{prep} preserves envelopes

Classical reversible adders/multipliers implement permutations of computational-basis states and imprint no data-dependent phase. Avoiding QFT-based adders prevents controlled-phase kickback. Since $U_{\text{coords},E}$ is only called on basis inputs to harvest (V, Δ), no superposition ever re-enters the state-preparation path; the upstream amplitude envelope on j remains unchanged.

C Note on index-materialization hypothesis

The compilation hypothesis stated near the start—existence of a named computational-basis register that carries the cyclic index j between the last writes to X and any subsequent operations that would modify/erase that index— is satisfied by standard gate-model implementations of Chen's Steps 5–8.b: the coordinate block is written by modular adders/multipliers controlled by a register that holds j; such compilers materialize j in the computational basis for the duration of those arithmetic updates. If a variant compilation creates j internally (for example, by a QFT on a clean seed), our input-lifting lemma (Lemma 2.4) replaces that internal preparation by an external basis input wire without changing the branchwise map $j \mapsto \mathbf{X}(j)$ implemented by the remainder of the prefix. This is the sole place where we appeal to a compilation detail; all other steps (harvesting, cleanup, Fourier sampling) are independent of how j was originally prepared.

D Frontier cuts and input-lifting: formal details

For completeness, we record the two auxiliary facts used in §2. Lemma 2.3 is a straightforward time-slice argument on acyclic gate lists; it ensures a cut exists where X has been deterministically written and J is still intact. Lemma 2.4 follows from linearity: once a unitary U_{rest} implements the branchwise map $j \mapsto \mathbf{X}(j)$ when fed the internally prepared superposition $\sum_j \alpha(j)\,|j\rangle$, it automatically implements the same branchwise map when given an external basis $|j\rangle$, since gate actions do not depend on amplitudes. Both lemmas are independent of Chen's specific arithmetic and hold for any uniform circuit family.

E Edge cases and variants

When Definition 6.1 fails for some p_η, cleanup cannot coherently erase T. Two standard workarounds (outside the default path) are: (i) enforce Eq. (1.2) modulo the accessible subproduct P', fix missing primes by adding directions or re-basing, and repeat; (ii) a postselection fallback that unshifts by the known T and keeps the zero frequency after QFT^{-1} on T, amplifying success to $\Theta(1)$ at $\widetilde{O}(\sqrt{P})$ cost.