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 objections to the Exact Coset Sampling subroutine (Zhang, 2025) that replaces the contested domain extension in a windowed-QFT lattice algorithm (Chen, 2024): (1) the first arXiv version allegedly presupposes knowledge of the target vector $\boldsymbol{b}^*$ to perform a shift; and (2) the revised version allegedly relies on a coordinate evaluator that "cannot exist" because Chen's pipeline uses measurement.

We clarify both points and state the minimal invariants needed for correctness. First, the default Step 9† uses the harvested finite difference $\Delta := \mathbf{X}(1) - \mathbf{X}(0) \equiv 2D^2\,\boldsymbol{b}^* \pmod{M_2}$ and realizes the shift as $\mathbf{Z} \leftarrow -T \cdot \Delta$; it never assumes $\boldsymbol{b}^*$ is known. The constant-adder variant that adds $2D^2T\,\boldsymbol{b}^*$ is explicitly marked as optional. Second, by the deferred-measurement principle there is an equivalent unitary preparation of the coordinate block; a standard compute-copy-uncompute construction yields a basis-callable evaluator U_{coords} without any mid-circuit measurement (Nielsen and Chuang, 2000). Superposition-time arithmetic is delegated to a separate phase-free reversible evaluator U_{prep} with read-only (V, Δ); U_{coords} is never applied to a superposition, so the upstream phase envelope is preserved.

We restate the residue-accessibility injectivity needed for coherent cleanup, prove that pre-cleanup Fourier sampling is uniform (hence cleanup is necessary), and give the exact orthogonality calculation showing that the uniform coset Fourier-samples to the annihilator $\{\boldsymbol{u} : \langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \,(\operatorname{mod} P)\}$, independent of offsets and amplitude windows. The subroutine lies in uniform BQP with $\operatorname{poly}(n, \log M_2)$ complexity.

`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

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

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 3 and 4, respectively, and state the clean, default subroutine and its proof of correctness in Section 2and Section 5.3.

Notation. $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$; all register arithmetic is modulo $M_2 = D^2P$ 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.

Run-local Determinism. Within a single coherent execution ("run") of the preparation, fix the classical randomness and call a basis-callable evaluator only on $j \in \{0,1\}$ to harvest (V,Δ) once; 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 the upstream envelope on j and avoids any data-dependent phase.

2 Summary of the replacement (Step $9^\dagger$)

Prepare a uniform label $T \in \mathbb{Z}_P$, form the difference register

$$\mathbf{Z} \;\leftarrow\; -T\cdot\Delta \;\equiv\; -2D^2T\,\boldsymbol{b}^* \pmod{M_2}, \tag{2.1}$$

erase T coherently via per-prime modular inversion and CRT using only ($\mathbf{Z}$ mod P,Δ), and apply $\mathrm{QFT}^{\otimes n}_{\mathbb{Z}_{M_2}}$ to $\mathbf{Z}$. The offsets $\boldsymbol{v}^*$ never enter $\mathbf{Z}$, and the phase envelope on j remains in disjoint registers. Section 5.3 proves that the measurement distribution is *exactly* supported on (1.2) and uniform on that set.

Algorithm 1 Step $9^\dagger$ (default, J-free)

Require: Coordinate block $\mathbf{X}(j)$ as in (1.1); harvested Δ from (1.3).

1: Prepare $\dfrac{1}{\sqrt{P}}\sum_{T\in\mathbb{Z}_P}|T\rangle$.
2: Compute $\mathbf{Z} \leftarrow -T\cdot\Delta \pmod{M_2}$ by double-and-add with read-only Δ.
3: **Cleanup (injectivity required):** For each $p_\eta \mid P$, choose the least index $i(\eta)$ with $\Delta_{i(\eta)} \not\equiv 0 \pmod{p_\eta}$ and compute $T_\eta \equiv -\Delta^{-1}_{i(\eta)} Z_{i(\eta)} \pmod{p_\eta}$. Recombine the residues via reversible CRT to obtain $T' \in \mathbb{Z}_P$, update $T \leftarrow T - T' \pmod{P}$, then uncompute the CRT and inversions (erasing T') using only ($\mathbf{Z}$ mod P,Δ).
4: Apply $\mathrm{QFT}^{\otimes n}_{\mathbb{Z}_{M_2}}$ to $\mathbf{Z}$ and measure $\boldsymbol{u}$.

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

Apon correctly observes that the first draft sketched a constant-adder realization that adds $2D^2T\,\boldsymbol{b}^*$, 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 $2D^2T\,\boldsymbol{b}^*$ as a constant. The constant-adder path remains in the paper solely as an optional variant when a classical description of $\boldsymbol{b}^*$ mod P is independently available; it is not used for correctness.

4 Response to Issue 2: deferred measurement and evaluator existence

Apon argues that measurement in the state preparation prevents the existence of a reversible arithmetic block U_{coords} that maps $|j\rangle\,|\mathbf{0}\rangle \mapsto |j\rangle\,|\mathbf{X}(j)\rangle$, and further suggests this block is "classical." This conflates two distinct facts: (i) projection is non-invertible as a channel; (ii) one may still *unitarize* the whole preparation by the deferred-measurement principle and extract a basis-callable evaluator from that unitary (Nielsen and Chuang, 2000).

Deferred measurement. Any circuit with mid-circuit measurements and classical control has an equivalent unitary implementation (deferred measurement) that postpones measurements to the end while preserving all computational-basis contents. In that unitary model, let $\mathcal{P}$ be a fixed preparation unitary for Eq. (1.1) and write $\mathcal{P} = \mathcal{R}\circ\mathcal{Q}$, where $\mathcal{Q}$ is the prefix up to the last gate that touches the coordinate block X and $\mathcal{R}$ the suffix (which does not overwrite X).

compute-copy-uncompute construction. Let COPY_X be the basis-copy unitary $|x\rangle\,|0\rangle \mapsto |x\rangle\,|x\rangle$ implemented by modular adders. Define

$$U_{\text{coords}} \;:=\; (\mathcal{R}\circ\mathcal{Q})^\dagger \;\circ\; \mathrm{COPY}_X \;\circ\; (\mathcal{R}\circ\mathcal{Q}). \tag{4.1}$$

Then for any basis j,

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

with all workspace restored to $|0\rangle$. This U_{coords} is unitary, efficient whenever $\mathcal{P}$ is, and requires no measurement undoing. In our algorithm it is invoked *only* on basis inputs (e.g., $j = 0, 1$) to harvest (V,Δ); it is *never* applied to a superposition.

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).

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 the upstream amplitude envelope on j is preserved.

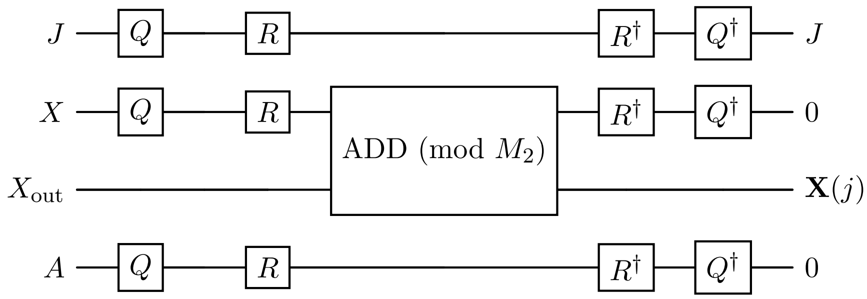

Figure 1 compute-copy-uncompute construction of U_{coords}. The suffix R does not overwrite X.

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

- Observation 1 ("U_{coords} is classical"). The statement is imprecise. U_{coords} is a unitary acting on computational-basis registers; when called on basis inputs it *implements* a classical reversible function. Nothing in our proof requires classical oracle access to $\boldsymbol{b}^*$ or re-running state preparation on a superposition.

- Observation 2 ("measurement makes Step 1 non-reversible"). Projection is not invertible, but by deferred measurement one may push all measurements to the end, obtain a unitary preparation, and isolate a compute-copy-uncompute block that realizes U_{coords}. Our algorithm never attempts to invert a measurement; it only uses the existence of a prefix that *writes* $\mathbf{X}(j)$ coherently.

Lemma 4.1 (Evaluator existence via deferred measurement)**.** Let $\mathcal{P}$ be any unitary that, on basis input $|j\rangle\,|0\rangle$, prepares a state whose coordinate block equals $\mathbf{X}(j)$ as in Eq. (1.1). Then the unitary U_{coords} defined in Eq. (4.1) satisfies $U_{\text{coords}}\,|j\rangle\,|0\rangle = |j\rangle\,|\mathbf{X}(j)\rangle$ with all work registers reset to $|0\rangle$. In particular, a basis-callable evaluator exists and is efficient whenever $\mathcal{P}$ is.

A detailed proof is given in the appendix; it is the standard compute-copy-uncompute argument.

5 Discussions

5.1 Residue accessibility and coherent cleanup

Definition 5.1 (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.

Under Eq. (2.1) 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

$$T \;\equiv\; -\Delta^{-1}_{i(\eta)}\,Z_{i(\eta)} \pmod{p_\eta} \quad \text{for all } \eta. \tag{5.1}$$

Recombination via CRT gives $T \in \mathbb{Z}_P$, which we erase coherently. If Definition 5.1 fails, then T is not a function of $\mathbf{Z}$ mod P and cannot be erased; Section 5.2 formalizes the resulting failure mode (uniform Fourier sample).

5.2 Pre-cleanup necessity

Proposition 5.2 (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 $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ 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).

5.3 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 5.1 the $\mathbb{Z}_P$ projection has size P; thus $|H| = P$.

Lemma 5.3 (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 $\mathrm{QFT}_{\mathbb{Z}_{M_2}}^{\otimes n}$ 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 $\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \pmod P$. Hence the outcomes are exactly supported on (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 $\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \pmod P$ (the factor 2 is a unit since P is odd), and equals 0 otherwise. □

5.4 Complexity and uniformity

All superposition-time arithmetic (copy, double-and-add, modular inversion per prime, CRT) is classical reversible and costs $\mathrm{poly}(\log M_2, \kappa)$ gates per coordinate. The n-fold QFT over $\mathbb{Z}_{M_2}$ costs $O\big(n\,\mathrm{poly}(\log M_2)\big)$. Basis harvesting of (V, Δ) is done once per run via U_{coords} on $j \in \{0,1\}$; U_{coords} is never applied to a superposition. The entire transformation from Equation (1.1) to a Fourier sample supported on Equation (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) U_{coords} is called only on basis inputs to harvest (V, Δ) within the same run (Fig. 1). 4) Pre-cleanup Fourier sampling is uniform (Prop. 5.2); injectivity (Def. 5.1) ensures coherent erasure of T. 5) Orthogonality yields support exactly on $\langle \boldsymbol{b}^*, \boldsymbol{u}\rangle \equiv 0 \pmod P$ (Lemma 5.3); offsets $\boldsymbol{v}^*$ and window phases never enter.

6 Conclusion

The objections in Apon (2025) target (i) an optional constant-adder variant not used in the default path, and (ii) a misunderstanding of evaluator existence in the presence of measurement. 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.

Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

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 the evaluator lemma (compute-copy-uncompute)

Fix a unitary preparation $\mathcal{P}$ for Eq. (1.1) in the deferred-measurement model and write $\mathcal{P} = \mathcal{R} \circ \mathcal{Q}$, where after $\mathcal{Q}$ the coordinate block equals $\mathbf{X}(j)$ on basis input j, and $\mathcal{R}$ no longer touches that block. Define U_{coords} by Eq. (4.1). For basis j,

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

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_{coords} 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 Edge cases and variants

When Definition 5.1 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.