Hidden parabolic subgroups of GL_n over finite chain rings

Muhammad Imran
School of Computer Science, University of Birmingham
CISITS Lab, Department of Mathematics, Universitas Indonesia
e-mail: m.imran.2@bham.ac.uk; m.imran@sci.ui.ac.id

October 20, 2026

Abstract

We give a bounded-error quantum polynomial-time algorithm for finding hidden parabolic subgroups of $\mathrm{GL}_n(R)$ over any effectively presented finite chain ring R. We call auxiliary group elements or subgroups used to extract information through oracle queries *probes*. For chain length at least two, elementary abelian socle probes first recover the complete flag modulo the maximal ideal. When the residue field has size $q \geq 3$, we reconstruct the flag recursively, lifting rank-one terminal members one digit at a time. The intermediate digits reduce to abelian hidden subgroup problems, while the final digit is a finite-field multiple-shift problem solved using learning from subset and Fourier sampling. For $q = 2$, where distinct flags can have the same stabilizer, we instead lift the conjugate parabolic subgroup through the congruence filtration. A final linear system determines it modulo normalizer directions. The algorithm outputs generators with probability at least $1 - \epsilon$ in time $\mathrm{poly}(n, \log |R|, \log(1/\epsilon))$. Consequences include $\mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ for every $N \geq 2$ and, with an explicit maximal-order presentation, $\mathrm{GL}_n(\mathcal{O}_K/N\mathcal{O}_K)$ for number fields K.

1 Introduction

The hidden subgroup problem (HSP) asks for generators of a subgroup $H \leq G$ from coherent access to a function f constant exactly on its left cosets. It is efficiently solvable on quantum computers for finite abelian groups [Kit96, BL95], but general non-abelian groups remain substantially harder. Efficient algorithms are known for selected group families [IMS01, ISS07, ISS12, II22, II24] and selected classes of hidden subgroups. Among the latter, Denney–Moore–Russell and Ivanyos treated Borel stabilizers over finite fields [DMR10, Iva12], and Decker–Ivanyos–Kulkarni–Qiao–Santha (DIKQS) solved the parabolic HSP in $\mathrm{GL}_n(\mathbb{F}_q)$ for arbitrary parabolic type [DIK+14].

We extend the finite field result to finite commutative chain rings $R \supsetneq \mathfrak{m} = (\pi) \supsetneq \cdots \supsetneq \mathfrak{m}^t = 0$ where $\mathfrak{m}$ is the maximal ideal of R. Write $k = R/\mathfrak{m} \cong \mathbb{F}_q$ and $V = R^n$. A parabolic subgroup is the stabilizer of a flag of free direct summands of V. Examples of R include $\mathbb{Z}/p^t\mathbb{Z}$, Galois rings, $\mathbb{F}_q[x]/(x^t)$, and prime-power quotients of rings of integers.

Theorem 1.1 (Parabolic HSP over finite chain rings)**.** *Let R be a finite chain ring in the effective presentation of Section 2.2. Given access to an oracle hiding a parabolic subgroup $H \leq \mathrm{GL}_n(R)$ and $0 < \epsilon < 1$, a quantum algorithm outputs generators of H with probability at least $1 - \epsilon$ in time $\mathrm{poly}(n, \log |R|, \log(1/\epsilon))$. The type of the hidden flag is not part of the input.*

Algorithms. For $t = 1$ we use DIKQS. Assume $t \geq 2$. Our common first step is to recover the reduced flag in $V/\mathfrak{m}V \cong k^n$. For a unimodular functional $\mu : V \to R$, the socle group

$$S_\mu = \{I + \pi^{t-1} a\mu : a \in V\} \cong (k^n, +)$$

is elementary abelian. Its intersection with H identifies a member of the reduced flag. Sampling functionals successively in annihilators recovers the entire chain and its type (Proposition 3.7).

For $q \geq 3$, a parabolic determines its flag (Theorem 2.12). If the smallest nonzero member T has rank at least two, an abelian intersection probe produces a nonzero free direct summand $W \subseteq T$, and we recurse on a complement. Rank-one terminal members require a new lifting routine: each non-final digit is an abelian HSP over $k^{n-1} \times k$, whereas the last digit yields the family $F(w - cs)$ with $c \in k^\times$. For small q, a Fourier projection produces an instance of learning from subset with support $\{0, 1\}$, solved by [IPS18]; for large q, direct Fourier sampling suffices. This gives polynomial time uniformly in q and n.

For $q = 2$, the last rank-one shift has only one copy, and distinct flags can have the same stabilizer. We therefore recover the subgroup directly. After standardizing the reduction, write $H = gPg^{-1}$ with P known and $g \equiv I \pmod{\mathfrak{m}}$. Two-copy socle shifts, each an elementary abelian HSP, strip successive digits of g modulo the block triangular algebra. At the final layer, linear equations determine the remaining conjugator modulo precisely the directions that normalize P. This ambiguity does not change H.

Why direct transport is insufficient. The Frobenius duality and constant-density estimates behind the DIKQS Fourier procedures extend to R, but one transported rank-one procedure has repetition factor $(1 - 1/q)^{-(n-1)}$. There is also a limitation on a different probe family: an algorithm seeing only uniformly sampled pairs $(\lambda, H \cap N_\lambda)$ can require $\Omega(q^{t-1})$ probes to distinguish terminal lines in their last digit. This is a restricted transcript lower bound, not a lower bound for the HSP or for adaptively chosen probes. The new lifting procedures avoid both limitations.

Motivation and organization. The pSIDH attack of [CII+23] uses hidden Borel subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. As isogeny-based cryptography shifts to higher-dimensional abelian varieties, the problem in higher-dimensional matrix groups $\mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ might be a useful cryptanalytic tool. Work relating Hawk to a quaternion principal ideal problem [CME+25], and the directions discussed in [AEJS26], also motivate the case of number-field quotient rings; no reduction of those problems to the parabolic promise is claimed here. Sections 2–3 establish the algebraic setting and reduced-flag algorithm. Sections 4–5 give rank-one lifting and full reconstruction for $q \geq 3$; Section 6 handles $q = 2$. Section 7 completes the main proof and gives the arithmetic consequences. Supporting algebra, transported procedures, and arithmetic preprocessing appear in Appendices A–C.

Roadmap of the proof. The proof of Theorem 1.1 has three stages; the first is common to all q.

(1) *Reduced flag* (Section 3). Socle probes S_μ turn the oracle into elementary abelian HSPs whose answers are members of $\bar{\mathcal{F}}$. Iterating in annihilators recovers $\bar{\mathcal{F}}$ and the type (Proposition 3.7).

(2) *Case* $q \geq 3$ (Sections 4–5). Here H determines $\mathcal{F}$ (Theorem 2.12), so we reconstruct the flag from the bottom. A nonzero split free $W \subseteq T$ is found either by an abelian intersection probe when $\operatorname{rank} T \geq 2$ (Proposition 3.4), or by lifting the π-adic digits of T one at a time when $\operatorname{rank} T = 1$ (Theorem 4.8). The candidate is certified (Lemma 5.1) and we recurse on a complement (Lemma 5.2, Theorem 5.3).

(3) *Case* $q = 2$ (Section 6). The flag is no longer determined, so we recover the subgroup. Writing $H = gPg^{-1}$ with $g \equiv I \pmod{\mathfrak{m}}$, two-copy socle shifts strip the digits of g one layer at a time (Proposition 6.5). A final linear system over $\mathbb{F}_2$ fixes g modulo directions that normalize P (Proposition 6.6, Theorem 6.7).

One mechanism underlies all three stages. Each probe is chosen so that the unknown π-adic digit is multiplied into the socle $\pi^{t-1}R \cong k$, where only its residue modulo $\mathfrak{m}$ survives. The oracle restricted to such probes is then an abelian hidden subgroup or hidden shift problem over k.

2 Algebraic setting and computational model

2.1 Chain rings and split flags

Definition 2.1. A finite chain ring is a finite commutative local ring whose ideals are linearly ordered by inclusion. Fix a generator π of its maximal ideal $\mathfrak{m}$, let t be the least positive integer with $\mathfrak{m}^t = 0$, and put $k = R/\mathfrak{m} = \mathbb{F}_q$. For a field we take $\pi = 0$ and $t = 1$.

The ideals are $\pi^j R$ for $0 \leq j \leq t$; each nonzero successive quotient has size q, so $|R| = q^t$. Write $v(x) = j$ when $x \in \pi^j R \setminus \pi^{j+1}R$, with $v(0) = t$, and $v(\pi^j R) = j$. Then

$$R^\times = R \setminus \mathfrak{m}, \qquad \operatorname{Ann}(\pi^j) = \pi^{t-j}R, \qquad \operatorname{soc}(R) = \pi^{t-1}R.$$

For $U \leq V = R^n$, write $\bar{U} = (U + \mathfrak{m}V)/\mathfrak{m}V \leq \bar{V} = k^n$.

Definition 2.2. A submodule is *split free* if it is a free direct summand of V. A flag of type $(n_1, \ldots, n_m)$, with $n_i \geq 1$ and $\sum_i n_i = n$, is a chain $\mathcal{F} : V = U_0 > U_1 > \cdots > U_m = 0$ of split free submodules with $\operatorname{rank} U_i = \sum_{j>i} n_j$. Its stabilizer $G_{\{\mathcal{F}\}}$ is called *parabolic*. The standard flag $\mathcal{F}_0$ consists of $U_i = \langle e_{n_1+n_2+\cdots+n_i+1}, \ldots, e_n \rangle$ where e_i is the i-th standard basis vector; its stabilizer P, the *standard parabolic* of that type, is block lower triangular.

Lemma 2.3. *The stabilizers of flags of a fixed type are exactly the conjugates of the standard parabolic of that type.*

Proof. Each quotient U_i/U_{i+1} is a direct summand of the free module V/U_{i+1}, hence is free over the local ring R. Lifting bases of these quotients gives an adapted basis, in which the stabilizer is P. Conversely, gPg^{-1} stabilizes $g\mathcal{F}_0$, whose members remain split free of the same ranks. □

Lemma 2.4 (Nakayama's lemma)**.** *If M is a finitely generated R-module and $M = N + \mathfrak{m}M$, then $M = N$.*

Lemma 2.5 (Splitting criterion)**.** *For $U \leq V$ the following are equivalent:*

(a) U is split free of rank r;

(b) U is generated by r elements with linearly independent reductions in $\bar{V}$;

(c) U is pure ($U \cap \pi^j V = \pi^j U$ for all j) and $\dim_k \bar{U} = r$.

In that case $\operatorname{rank} U = \dim_k \bar{U}$*, every complement is split free, and every split free $U' \leq U$ is a direct summand of U. In particular a nonzero split free submodule is not contained in $\mathfrak{m}V$.*

A proof, including the purity criterion, is given in Appendix A.

Lemma 2.6. *$\bar{\mathcal{F}}$ is a flag in $\bar{V}$ of the same length and type as $\mathcal{F}$, with $\dim_k \bar{U}_i = \operatorname{rank} U_i$. In particular the type of $\mathcal{F}$, and hence $d = \operatorname{rank} U_{m-1}$, is determined by $\bar{\mathcal{F}}$.*

Proof. For split free U, $U/\mathfrak{m}U \cong \bar{U}$ and $\dim_k \bar{U} = \operatorname{rank} U$. The positive rank gaps in the flag therefore remain positive after reduction. □

Lemma 2.7. *If $U \leq V$ is split free and $0 \leq j \leq t$ then for $x \in V$, $\pi^j x \in U \iff x \in U + \pi^{t-j} V$.*

Proof. Fix $V = U \oplus C$ and write $x = u + c$; then $\pi^j x \in U$ iff $\pi^j c = 0$ iff $c \in \pi^{t-j} C$. □

In words, multiplying by π^j hides any error in $\pi^{t-j}V$. So the condition $\pi^j x \in U$ tests membership $x \in U$ only to precision $t - j$. This is how the valuations $v(\lambda(U_i))$ enter the probe formulas of Section 3.

Lemma 2.8 (Densities)**.** *Write $c_q(m) = \prod_{i=1}^{m}(1 - q^{-i})$ and $c_\infty = \prod_{i \geq 1}(1 - 2^{-i}) > 0.288$, so $c_q(m) \geq c_\infty$.*

(i) A uniform $X \in \mathrm{M}_m(R)$ is invertible with probability $c_q(m)$.

(ii) A uniform $X \in \mathrm{M}_{m \times l}(R)$, $l \geq m$, is surjective with probability $\prod_{i=l-m+1}^{l}(1 - q^{-i}) \geq c_\infty$.

(iii) $l \geq m$ uniform elements of a free module of rank m generate it with probability $\geq c_\infty$.

In particular none of these probabilities depends on the length t.

Proof. Invertibility is detected by the determinant modulo $\mathfrak{m}$; generation and surjectivity are detected modulo $\mathfrak{m}$ by Lemma 2.4. Reduction has equal fibres, and the assertions follow by counting full-rank matrices over k. □

2.2 Computational model

The ring is supplied by additive coordinates and multiplication structure constants over $\mathbb{Z}/p^e\mathbb{Z}$, where $p^e = \operatorname{char} R$, together with π, t and $q = p^\ell$. We assume a presentation of size polynomial in $\log |R|$ supporting ring arithmetic, valuation, additive cyclic decomposition, residue-field arithmetic, and a section $\sigma : k \to R$ with $\sigma(0) = 0$, all in time $\mathrm{poly}(\log |R|)$. We apply σ coordinatewise to vectors and matrices over k: for $a \in k$ we write $\widehat{a} = \sigma(a)$, and call it the *standard lift* of a. We also use polynomially many generators of $R^\times$. Appendix A describes the unit generators and the module algorithms used below. The parameters e, t, ℓ are independent: $|R| = p^{\ell t}$ and $1 \leq e \leq t$; $(R, +)$ need not be homocyclic.

Lemma 2.9 (Effective operations)**.** *Membership, equality, sums, intersections, splitness, and bases and complements of split free submodules are computable in classical time polynomial in $n, \log |R|$ and the total encoding length of their generators. From a split free flag or submodule W, one can also compute polynomial-size generating sets of $G_{\{\mathcal{F}\}}$ and $\{X \in \mathrm{GL}_n(R) : (X - I)V \subseteq W\}$.*

Proof. The algorithms and group generators are detailed in Appendix A. □

The HSP oracle $f : G \to S$ is coherent and satisfies $f(x) = f(y) \iff x^{-1}y \in H$. Thus $f(xh) = f(x)$ for $h \in H$. Its restriction to any known subgroup A hides $H \cap A$. Inversion converts it to a right-coset oracle with one query and polynomial matrix arithmetic. Output encodings and one oracle call have polynomial size in the stated input parameters.

Convention 2.10 (Error and running time)**.** Quantum polynomial time means bounded running time $\mathrm{poly}(n, \log|R|, \log(1/\epsilon))$ and success probability at least $1-\epsilon$. All loops have explicit caps; malformed outputs or timeouts cause a failure return. For at most N adaptive calls with valid promises before the first error, assigning error δ/N to each bounds the probability of a first erroneous call by δ. Any additional sampling failure is analyzed in the corresponding ideal execution with exact subroutine answers. Approximate QFTs and state preparations are given a separate error budget: if at most B are used, their individual operator errors are at most $O(\epsilon/B)$, so the complete computation changes by at most $O(\epsilon)$ in trace distance. Constant-factor budget divisions are chosen so that the total is at most ϵ.

Problem 2.11 (Parabolic HSP)**.** Given the above presentation of R and a coherent oracle hiding a parabolic subgroup $H \le \mathrm{GL}_n(R)$ of unknown type, output generators of H.

2.3 Faithfulness

The distinction between flag and subgroup recovery is governed by

$$\text{there exists } b \in R^\times \text{ with } b-1 \in R^\times \iff q \ge 3. \tag{2.1}$$

Equivalently, $q \ge 3$ exactly when k has an element other than 0 and 1. For $q = 2$ every unit is $\equiv 1 \pmod{\mathfrak{m}}$, so no unit b can make $b-1$ a unit.

Theorem 2.12 (Faithfulness for $q \ge 3$)**.** *Suppose $q \ge 3$. If $\mathcal{F}$ and $\mathcal{F}'$ are flags in $V = R^n$ with $G_{\{\mathcal{F}\}} \subseteq G_{\{\mathcal{F}'\}}$, then every member of $\mathcal{F}'$ is a member of $\mathcal{F}$. In particular $G_{\{\mathcal{F}\}} = G_{\{\mathcal{F}'\}}$ implies $\mathcal{F} = \mathcal{F}'$, and the parabolic subgroup determines the flag.*

The proof is in Appendix A. At $q = 2$ the conclusion can fail already in dimension two: over $\mathbb{Z}/4\mathbb{Z}$, the distinct lines Re_1 and $R(e_1 + 2e_2)$ have the same stabilizer (Example A.3). Proposition A.2 describes these fibres over every binary chain ring of length at least two. The algorithm must therefore target the subgroup rather than a unique flag.

Definition 2.13 (Congruence filtration)**.** Put $K_j = I + \pi^j \mathrm{M}_n(R)$ for $j \ge 1$, with $K_j = \{I\}$ for $j \ge t$. These are the kernels of reduction modulo π^j, hence normal subgroups of G. We use the commutator convention $[x, y] = xyx^{-1}y^{-1}$.

For $t \ge 2$ the deepest nontrivial layer is abelian. Since $\pi^{2t-2} = 0$, we have $(I + \pi^{t-1}A)(I + \pi^{t-1}B) = I + \pi^{t-1}(A + B)$, and $I + \pi^{t-1}Y \mapsto \bar{Y}$ identifies K_{t-1} with $(\mathrm{M}_n(k), +)$. All probes in Sections 3 and 6 live in this socle layer, which is why the HSPs they produce are elementary abelian.

3 Recovering the reduced flag

Throughout this section $t \geq 2$ and $H = G_{\{\mathcal{F}\}}$, with $\mathcal{F} : V = U_0 > \cdots > U_m = 0$, terminal member $T = U_{m-1}$ and terminal rank $d = \operatorname{rank} T$. For the one-block flag, $T = V$. We first compute intersections with rank-one matrix families, then use their socle restrictions to recover $\bar{\mathcal{F}}$.

3.1 Intersection probes

For a unimodular functional $\lambda \in V^* = \operatorname{Hom}_R(V, R)$, meaning $\lambda(V) = R$, put $P_\lambda = \ker \lambda$ and

$$G_\lambda = \{I + a\lambda : 1 + \lambda(a) \in R^\times\}, \qquad N_\lambda = \{I + a\lambda : a \in P_\lambda\} \cong (R^{n-1}, +).$$

The product is $(I + a\lambda)(I + b\lambda) = I + (a + b + \lambda(b)a)\lambda$. Consequently G_λ is a group, N_λ is its abelian normal subgroup, and $G_\lambda/N_\lambda \cong R^\times$. Thus N_λ consists of the transvections with fixed "row" λ. Its parameter a is a vector, and $I + a\lambda$ moves each $u \in V$ by $\lambda(u)a$. Restricting the oracle to N_λ gives an abelian HSP.

Lemma 3.1 (Filtered stabilizer formula)**.** *Let $\lambda \in V^*$ be unimodular and set $v_i = v(\lambda(U_i))$ for $0 \leq i \leq m$, so that $0 = v_0 \leq v_1 \leq \cdots \leq v_{m-1} \leq v_m = t$. Put*

$$D_\lambda \;:=\; \bigcap_{i=0}^{m} \big(U_i + \pi^{\,t-v_i} V\big) \;=\; \bigcap_{i=1}^{m-1} \big(U_i + \pi^{\,t-v_i} V\big),$$

the terms $i = 0$ and $i = m$ both being equal to V. Then

(i) $H \cap N_\lambda = \{I + a\lambda :\ a \in P_\lambda \cap D_\lambda\}$ and $H \cap G_\lambda = \{I + a\lambda :\ a \in D_\lambda,\ 1 + \lambda(a) \in R^\times\}$;

(ii) D_λ, and hence each of the two intersections, is a function of λ, of the valuations $v_0, \ldots, v_m$, and of the residues $U_i \bmod \pi^{\,t-v_i} V$ alone.

The integer v_i measures how deep $\lambda(U_i)$ lies in the chain of ideals of R. A member with $v_i = 0$ (λ surjective on U_i) imposes the exact condition $a \in U_i$. A member with $0 < v_i < t$ imposes it only modulo $\pi^{t-v_i}V$, and a member with $v_i = t$ imposes nothing. So $H \cap N_\lambda$ sees each U_i only to precision $t - v_i$, and part (ii) says that it sees nothing more.

Proof. (i) For $X = I + a\lambda$ and $u \in U_i$ we have $Xu = u + \lambda(u)a$, so $XU_i \subseteq U_i$ iff $\lambda(U_i)a \subseteq U_i$, i.e. $\pi^{v_i} a \in U_i$, i.e. $a \in U_i + \pi^{\,t-v_i}V$ by Lemma 2.7; and $XU_i \subseteq U_i$ forces $XU_i = U_i$ because X is invertible and U_i is finite. Intersect over i and impose $a \in P_\lambda$, respectively invertibility of $I + a\lambda$, which by $\det(I + a\lambda) = 1 + \lambda(a)$ is the stated unit condition. For the two trivial terms, $v_0 = 0$ gives $U_0 + \pi^t V = V$ and $v_m = t$ gives $0 + \pi^0 V = V$. (ii) is immediate, since $U_i + \pi^{\,t-v_i}V$ depends on U_i only through its class modulo $\pi^{\,t-v_i}V$. □

Call λ *transverse* if $\lambda(T) = R$. Equivalently, $\bar{\lambda}$ does not vanish on $\bar{T}$. Then every v_i with $i < m$ is 0, so the smallest member T determines D_λ by itself.

Corollary 3.2. *If λ is transverse then $D_\lambda = T$, so*

$$H \cap N_\lambda = \{I + a\lambda : a \in T \cap P_\lambda\} \cong T \cap P_\lambda,$$

which is split free of rank $d-1$, and

$$H \cap G_\lambda = \{I + a\lambda : \ a \in T, \ 1 + \lambda(a) \in R^\times\},$$

a subgroup of G_λ whose coefficient set has R-span T provided $q \geq 3$.

Proof. Since $\lambda(T) = R$ and $T \subseteq U_i$ for $i < m$, we have $\lambda(U_i) = R$, so $v_i = 0$ for all $i < m$ and $D_\lambda = T$. Because $\lambda(T) = R$, we may fix $\tau \in T$ with $\lambda(\tau) = 1$. Then $r \mapsto r\tau$ splits $\lambda|_T \colon T \to R$, and

$$T = (T \cap P_\lambda) \oplus R\tau, \qquad a = \big(a - \lambda(a)\tau\big) + \lambda(a)\tau.$$

The first assertion follows from the additive product on N_λ. For the second, note that the coefficient set $\{a \in T : 1 + \lambda(a) \in R^\times\}$ contains $T \cap P_\lambda$. If $q \geq 3$, choose $c \in R^\times$ with $1 + c \in R^\times$. Then $c\tau$ also lies in the coefficient set, since $1 + \lambda(c\tau) = 1 + c$. As c is a unit, the R-span of the coefficient set is $(T \cap P_\lambda) + R\tau = T$. □

Lemma 3.3 (Transversality is generic)**.** *For λ uniform among unimodular elements of V^*,*

$$\Pr[\lambda \text{ not transverse}] = \frac{q^{-d} - q^{-n}}{1 - q^{-n}} = q^{-d} \cdot \frac{1 - q^{d-n}}{1 - q^{-n}} \ < \ q^{-d} \ \leq \ \frac{1}{q}.$$

Proof. In coordinates adapted to T, nontransversality says that the first d coefficients of λ lie in $\mathfrak{m}$. Before conditioning on unimodularity this has probability q^{-d}; the excluded event that all n coefficients lie in $\mathfrak{m}$ has probability q^{-n}. □

Proposition 3.4 (Terminal rank at least two)**.** *Suppose* $\operatorname{rank} T \geq 2$ *and draw λ uniformly among unimodular elements of V^*. An abelian HSP in $N_\lambda \cong (P_\lambda, +) \cong R^{n-1}$ returns $H \cap N_\lambda$ in time* $\mathrm{poly}(n, \log |R|)$*. With probability*

$$1 - \frac{q^{-d} - q^{-n}}{1 - q^{-n}} \ > \ 1 - q^{-d} \ \geq \ 1 - q^{-2} \ \geq \ \frac{3}{4}$$

the draw is transverse, and in that case

$$\sum_{X \in H \cap N_\lambda} (X - I)V \ = \ T \cap P_\lambda$$

is a nonzero split free submodule of T, of rank $d-1$.

Proof. P_λ is split free of rank $n-1$ because $V/P_\lambda \cong R$ is free, so $(N_\lambda, +) \cong (R^{n-1}, +)$ is a finite abelian group of known structure and the abelian HSP applies at the stated cost; only the fact that f restricted to a subgroup hides the intersection is used, so normality of N_λ is not needed. The probability is Lemma 3.3. For a transverse draw, Corollary 3.2 gives $H \cap N_\lambda = \{I + a\lambda : a \in T \cap P_\lambda\}$, and $(I + a\lambda - I)V = a\lambda(V) = aR$ since λ is unimodular, so the sum is $T \cap P_\lambda$, of rank $d - 1 \geq 1$. □

The Frobenius duality and constant-density estimates behind the DIKQS [DIK+14] Fourier procedures extend to R, but one transported rank-one procedure has repetition factor $(1 - 1/q)^{-(n-1)}$ (Appendix B). The new lifting procedures avoid this.

3.2 Socle probes

Definition 3.5 (Socle layers)**.** Let $t \geq 2$ and let $\mu \in V^*$ be unimodular. Put

$$S_\mu = \{\, I + \pi^{t-1} a\mu \;:\; a \in V \,\} \;\leq\; G.$$

Lemma 3.6 (Socle layers)**.** *Let $t \geq 2$ and let $\mu \in V^*$ be unimodular, and write $q = p^\ell$. Then:*

(i) $S_\mu = G_\mu \cap K_{t-1}$, and $a \mapsto I + \pi^{t-1} a\mu$ induces a group isomorphism $(\bar{V}, +) \xrightarrow{\sim} S_\mu$; in particular $S_\mu \cong (\mathbb{Z}/p\mathbb{Z})^{\ell n}$ is elementary abelian of order q^n, and it is generated by the ℓn explicitly computable elements

$$I + \pi^{t-1}\sigma(b_r) e_a \mu, \qquad 1 \leq a \leq n,\ 1 \leq r \leq \ell,$$

where $b_1, \ldots, b_\ell$ is an $\mathbb{F}_p$-basis of k and $e_1, \ldots, e_n$ is the standard basis of V;

(ii) let $i_0(\mu)$ be the largest index i with $\mu(U_i) = R$. It is well defined, and $\mu(U_i) = R$ iff $\bar{U}_i \not\subseteq \ker \bar{\mu}$, so $i_0(\mu)$ depends only on $\bar{\mu}$. Moreover

$$H \cap S_\mu = \{\, I + \pi^{t-1} a\mu : \bar{a} \in \bar{U}_{i_0(\mu)} \,\} \;\cong\; \bar{U}_{i_0(\mu)}.$$

The socle probe is the depth-$(t-1)$ version of G_μ. Because its coefficients are multiplied by π^{t-1}, only $\bar{a}$ and $\bar{\mu}$ matter. The intersection with H is therefore governed by the reduced flag alone. It returns the smallest reduced member $\bar{U}_{i_0(\mu)}$ on which $\bar{\mu}$ is not identically zero.

Proof. Since $\pi^{2t-2} = 0$,

$$(I + \pi^{t-1} a\mu)(I + \pi^{t-1} b\mu) = I + \pi^{t-1}(a+b)\mu.$$

A unit coordinate of μ shows that the kernel of the parameter map $V \to S_\mu$ is $\mathfrak{m}V$, and that $G_\mu \cap K_{t-1} = S_\mu$. This proves (i), including the generators obtained from the $\mathbb{F}_p$-basis $\{b_r e_a\}$ of k^n.

For (ii), $i_0(\mu)$ exists because $\mu(V) = R$, and $\mu(U_i) = R$ exactly when $\bar{\mu}$ is nonzero on $\bar{U}_i$. An element $I + \pi^{t-1} a\mu$ preserves U_i exactly when $\pi^{t-1}\mu(U_i) a \subseteq U_i$. If $\mu(U_i) \subseteq \mathfrak{m}$ this is automatic; otherwise Lemma 2.7 makes it equivalent to $\bar{a} \in \bar{U}_i$. Intersecting these nested conditions yields $\bar{a} \in \bar{U}_{i_0(\mu)}$. □

Proposition 3.7. *Let R be a finite chain ring of length $t \geq 2$ and let $0 < \epsilon < 1$. There is a quantum algorithm running in time $\mathrm{poly}(n, \log|R|, \log(1/\epsilon))$ which, for every q and every n and with no further hypotheses, outputs the reduced flag*

$$\bar{V} = \bar{U}_0 > \bar{U}_1 > \cdots > \bar{U}_m = 0$$

in $\bar{V} = k^n$, together with its type $(n_1, \ldots, n_m)$, with failure probability at most ϵ.

Idea. The flag is built from the bottom. Suppose $W = \bar{U}_{j+1}$ has been found, and take μ with $\bar{\mu}$ vanishing on W. By Lemma 3.6(ii) the answer is a member containing $\bar{U}_j$, and with probability at least $1/2$ it is $\bar{U}_j$ itself. Intersecting r such answers gives $\bar{U}_j$ unless every draw also vanishes on $\bar{U}_j$.

Proof. Let $r = \lceil \log_2(2n/\epsilon) \rceil$. Maintain a recovered subspace W, initially 0. While $W \neq \bar{V}$, sample r independent nonzero functionals uniformly from the annihilator $W^\circ := \{\lambda \in \bar{V}^* : \lambda|_W = 0\}$ of W in $\bar{V}^*$, lift each to a unimodular μ, and solve the abelian HSP in S_μ with error at most $\epsilon/(2nr)$. Convert each answer to the k-span of its coefficient vectors and let W_{new} be the intersection of those spans. Require $W < W_{\text{new}} \leq \bar{V}$, append W_{new}, and continue. Stop after at most n rounds, reporting failure if strict progress or termination fails. Reverse the resulting list to obtain the flag and read its type from dimension gaps.

Analyze first the ideal execution with exact intersection answers. If the current member is $W = \bar{U}_{j+1}$, every sampled functional kills W, and Lemma 3.6 returns a flag member containing $\bar{U}_j$. It equals $\bar{U}_j$ unless it also kills $\bar{U}_j$. For a uniform nonzero element of W°, the latter probability is at most $q^{-(\dim \bar{U}_j - \dim W)} \leq 1/2$. Thus the next member is missed with probability at most 2^{-r}. Every ideal round makes strict progress, even if it skips a member, so there are at most n rounds and the probability of any omission is at most $n2^{-r} \leq \epsilon/2$.

Couple the actual and ideal executions up to the first incorrect HSP answer. Before that error they have the same history, so each call has its stated promise and error bound. At most nr calls give discrepancy probability at most $\epsilon/2$; adding the ideal sampling error proves the result. This argument does not condition probe distributions on future success events. The caps bound all execution paths. Each query forms a matrix over R, giving the claimed $\text{poly}(n, \log|R|, \log(1/\epsilon))$ gate cost. □

A successful call also supplies a basis change making the reduced flag standard. Lemma 6.2 then gives $H = gPg^{-1}$ with $g \in K_1 = I + \pi \, \mathrm{M}_n(R)$ and P the known standard parabolic. The following sections recover the remaining digits.

4 Rank-one lifting

Assume $t \geq 2$, $q \geq 3$, and that the reduced terminal line is known. Write $l = n - 1$ in this section. After a known basis change the terminal member has the unique normalized form

$$T = R(e_1 + y), \qquad y \in \mathfrak{m}R^l. \tag{4.1}$$

Since $\sigma(k)$ is a set of representatives containing 0, y has a unique expansion $y = \sum_{i=1}^{t-1} \pi^i \sigma(s_i)$ with $s_i \in k^l$. For $1 \leq j \leq t$ write

$$y_{<j} = \sum_{i=1}^{j-1} \pi^i \sigma(s_i), \tag{4.2}$$

so that $y \equiv y_{<j} \pmod{\pi^j R^l}$. Once the digits $s_1, \ldots, s_{j-1}$ are known, conjugating by $C_j = \left(\begin{smallmatrix} 1 & 0 \\ -y_{<j} & I_l \end{smallmatrix}\right)$ maps T to

$$T_j = R(e_1 + \pi^j z_j), \qquad z_j \in R^l, \quad s_j = \bar{z}_j \in k^l, \qquad 1 \leq j < t. \tag{4.3}$$

Write H_j, f_j for the conjugated subgroup and oracle.

Standing notation for this section. Here $l = n - 1$, and matrices are written in blocks of sizes 1 and l. The terminal line is $T = R(e_1 + y)$ with π-adic digits $s_1, \ldots, s_{t-1} \in k^l$. At stage j the digits $s_1, \ldots, s_{j-1}$ are known and have been conjugated away. The current line is $T_j = R(e_1 + \pi^j z_j)$, its unknown leading digit is $s_j = \bar{z}_j$, and H_j, f_j are the subgroup and oracle after this conjugation. The section σ and the notation $\widehat{a} = \sigma(a)$ are from Section 2.2.

4.1 One lifting layer

Use the fixed section σ coordinatewise, writing $\widehat{a} = \sigma(a)$. For $x \in k^l$ and $a \in k$, define the query matrix

$$G_j(x,a) = \begin{pmatrix} 1+\pi^{t-1-j}\widehat{a} & 0 \\ \pi^{t-1}\widehat{x} & I_l \end{pmatrix}. \tag{4.4}$$

Think of $x \in k^l$ as a test vector and $a \in k$ as a scalar. The diagonal entry has depth $t-1-j$, chosen so that its product with the unknown $\pi^j z_j$ (depth j) lands exactly in the socle $\pi^{t-1}R$. There it is compared with the lower-left block $\pi^{t-1}\widehat{x}$. The section need not preserve addition or multiplication. These matrices need not form a group; the HSP below is on their parameter group. For the coset calculations use the containing group

$$Q = \left\{ M(\beta,c) = \begin{pmatrix} \beta & 0 \\ \pi^{t-1}\widehat{c} & I_l \end{pmatrix} : \beta \in R^\times,\ c \in k^l \right\},$$

whose operations are

$$\begin{aligned} M(\beta,c)M(\beta',c') &= M(\beta\beta', c\bar{\beta}' + c'), \\ M(\beta,c)^{-1} &= M(\beta^{-1}, -c\bar{\beta}^{-1}). \end{aligned} \tag{4.5}$$

For $1 \le r < t$ the well-defined map

$$b_r : 1+\pi^r R \to (k,+), \qquad b_r(1+\pi^r u) = \bar{u} \tag{4.6}$$

is a surjective homomorphism: the cross term in a product contributes $\pi^r uu' \in \mathfrak{m}$. Separately put

$$b_0 : R^\times \to k, \qquad b_0(\beta) = \bar{\beta} - 1. \tag{4.7}$$

Unlike b_r for $r \ge 1$, this last map is not an additive homomorphism.

Lemma 4.1 (Membership)**.** *Let $1 \le j \le t-1$ and let s_j be as in (4.3).*

(i) If $j < t-1$, then $G_j(x,a) \in \mathrm{GL}_n(R)$ for every $a \in k$. If $j = t-1$, it is invertible exactly when $a \neq -1$.

(ii) More generally, put $r = t-1-j$ and let $M(\beta,c) \in Q$, where $\beta \in 1+\pi^r R$ if $r \ge 1$ and $\beta \in R^\times$ if $r = 0$, and $c \in k^l$. Then

$$M(\beta,c) \in H_j \iff c = b_r(\beta)\, s_j, \tag{4.8}$$

with b_r as in (4.6) for $r \ge 1$ and as in (4.7) for $r = 0$. In particular, for admissible a, $G_j(x,a) \in H_j$ if and only if $x = a\, s_j$.

Formula (4.8) says that $M(\beta,c)$ fixes T_j exactly when its lower-left block $\pi^{t-1}\widehat{c}$ matches the socle term $(\beta-1)\pi^j z_j = \pi^{t-1}uz_j$. Here $\beta = 1+\pi^r u$ with $\bar{u} = b_r(\beta)$, and $s_j = \bar{z}_j$. The membership condition is therefore the bilinear relation $c = (\text{digit of } \beta)\cdot s_j$ over k.

Proof. The determinant of $G_j(x,a)$ is $1+\pi^{t-1-j}\widehat{a}$, proving (i). For (ii), write $\beta = 1+\pi^r u$, with $u = \beta - 1$ if $r = 0$, and put $v_j = e_1 + \pi^j z_j$. The first coordinate of $M(\beta,c)v_j$ is β, so $M(\beta,c)$ stabilizes T_j exactly when $\pi^{t-1}\widehat{c} = (\beta-1)\pi^j z_j = \pi^{t-1}uz_j$. Since $\mathrm{Ann}(\pi^{t-1}) = \mathfrak{m}$, this is $c = \bar{u}s_j = b_r(\beta)s_j$. It is also sufficient for membership in the full flag stabilizer, because then

$$M(\beta,c) - I = (\pi^r u v_j)e_1^*, \tag{4.9}$$

so $(M-I)V \subseteq T_j$, which is contained in every nonzero flag member. □

Lemma 4.2 (Intermediate layers)**.** *Let $1 \le j < t-1$ and put $F_j(x) = f_j(G_j(x,0))$. Then $\{G_j(x,0) : x \in k^l\}$ is a subgroup isomorphic to k^l, the function F_j is injective, and for every $a \in k$ and $x \in k^l$*

$$f_j\big(G_j(x,a)\big) = F_j\big(x - a\, s_j\big). \tag{4.10}$$

The shift parameter a ranges over all of k.

In other words, $(x,a) \mapsto f_j(G_j(x,a))$ is constant exactly on cosets of the line $\{(as_j, a) : a \in k\}$ in $(k^l \times k, +)$, which is an abelian HSP. The point is that for $r = t-1-j \ge 1$ the digit map b_r is additive, so composing two queries adds their scalars a.

Proof. Since $\sigma(0) = 0$ we have $G_j(x,0) = M(1,x)$, so (4.5) gives $G_j(x,0)G_j(x',0) = G_j(x + x', 0)$ and $G_j(x,0)^{-1} = G_j(-x,0)$: this family is a subgroup isomorphic to k^l. Write $r = t-1-j$, $\alpha = 1 + \pi^r \widehat{a}$ and $\alpha' = 1 + \pi^r \widehat{a'}$, and note $\bar{\alpha} = \bar{\alpha'} = 1$ because $r \ge 1$. Then (4.5) gives

$$G_j(x,a)^{-1} G_j(x',a') = M\big(\alpha^{-1}\alpha',\, x' - x\big).$$

Here $\alpha^{-1}\alpha'$ lies in the group $1 + \pi^r R$, and since $r \ge 1$ the map b_r of (4.6) is a homomorphism, so $b_r(\alpha^{-1}\alpha') = -b_r(\alpha) + b_r(\alpha') = a' - a$. By Lemma 4.1(ii) this matrix lies in H_j if and only if $x' - x = (a'-a)s_j$. Taking $a' = 0$ and $x' = x - as_j$ shows that $G_j(x,a)$ and $G_j(x - as_j, 0)$ lie in the same left coset of H_j, which is (4.10); taking $a = a' = 0$ shows $G_j(x,0)^{-1}G_j(x',0) \in H_j$ iff $x = x'$, which is injectivity of F_j. □

Lemma 4.3 (Final layer)**.** *Let $j = t-1$, write $h = \bar{\beta}$ for $\beta \in R^\times$, so that the admissible query coefficients are $h = 1 + a$ with $a \ne -1$, and abbreviate $s = s_{t-1}$, $\Gamma = Q$. Then:*

(i) Γ is a subgroup of $\mathrm{GL}_n(R)$ and $M(\beta, c) \mapsto (c, \bar{\beta})$ is a surjective homomorphism $\Gamma \to k^l \rtimes k^\times$, the target having the product $(x,h)(x',h') = (xh' + x',\, hh')$. Moreover $\Gamma \cap H_{t-1} = \{M(\beta,c) : c = (\bar{\beta} - 1)s\}$ is the full preimage of $\{(x,h) : x = (h-1)s\}$, so all coset computations may be carried out in $k^l \rtimes k^\times$;

(ii) two elements of Γ lie in the same left coset of $\Gamma \cap H_{t-1}$ if and only if they have the same value of $h^{-1}(x + s) \in k^l$;

(iii) consequently, setting $\Phi(w) = f_{t-1}(G_{t-1}(w - s, 0))$, the function Φ is injective and for all $w \in k^l$, $h \in k^\times$

$$f_{t-1}\big(G_{t-1}(hw,\, h-1)\big) = \Phi\big(w + h^{-1}s\big). \tag{4.11}$$

Equivalently, writing $c = -h^{-1}$, the family $\{\, w \mapsto f_{t-1}(G_{t-1}(hw, h-1))\,\}$ is of the form $\Phi(w - c\,s)$ with c ranging over $k^\times$.

At the last digit ($r = 0$) the diagonal entry ranges over all of $R^\times$, and b_0 is no longer additive. The relevant group is the affine group $k^l \rtimes k^\times$, acting on k^l by $w \cdot (x,h) = wh + x$. Part (i) says that $\Gamma \cap H_{t-1}$ is the stabilizer of the point $-s$, since $-sh + x = -s$ iff $x = (h-1)s$. Part (ii) labels its cosets by the image of that point. The hidden subgroup is thus a nonabelian point stabilizer, and part (iii) recasts it as $q-1$ shifted copies of a single injective function.

Proof. (i) The product law is (4.5), and the displayed map is a homomorphism onto $k^l \rtimes k^\times$ because $\beta \mapsto \bar{\beta}$ is one. The intersection is Lemma 4.1(ii) with $r = 0$, where $b_0(\beta) = \bar{\beta} - 1$. Its description shows that the kernel $\{M(\beta,0) : \beta \in 1 + \mathfrak{m}\}$ of the map is contained in H_{t-1}, so $\Gamma \cap H_{t-1}$ is the full preimage of $\{(x,h) : x = (h-1)s\}$ and descends to the quotient.

(ii) From (i), $(x,h)^{-1} = (-xh^{-1}, h^{-1})$, so

$$(x,h)^{-1}(x',h') = \big(x' - xh^{-1}h',\ h^{-1}h'\big),$$

which lies in $\Gamma \cap H_{t-1}$ iff $x' - xu = (u-1)s$ with $u = h^{-1}h'$, i.e. iff $x' + s = u(x+s)$, i.e. iff $h'^{-1}(x'+s) = h^{-1}(x+s)$.

(iii) By (ii) the value $f_{t-1}(G_{t-1}(x, h-1))$ is an injective function of $h^{-1}(x+s)$; at $h=1$, $x = w-s$ this function is Φ, so Φ is injective. Substituting $x = hw$ gives $h^{-1}(hw+s) = w+h^{-1}s$, which is (4.11). As h ranges over $k^\times$ so does h^{-1}, hence so does $c = -h^{-1}$. □

Remark 4.4. For $F_0(x) = f_{t-1}(G_{t-1}(x,0))$, the final-layer identity is $f_{t-1}(G_{t-1}(x,a)) = F_0((1+a)^{-1}(x-as))$. The substitution $x = hw$ and $\Phi(w) = F_0(w-s)$ produce genuine shifts of one common injective function, as in (4.11).

4.2 Recovering an intermediate digit

Proposition 4.5 (Intermediate lifting)**.** *Let $1 \le j < t-1$. Given the first $j-1$ digits of the rank-one terminal member, the next digit $s_j \in k^l$ can be recovered in quantum time* $\mathrm{poly}(n, \log|R|)$.

Proof. Lemma 4.2 makes $(x,a) \mapsto f_j(G_j(x,a)) = F_j(x - as_j)$ an oracle for

$$L_{s_j} = \{(as_j, a) : a \in k\} \le (k^l \times k, +).$$

An abelian HSP returns additive generators of this subgroup. Any nonzero returned element has the form (as_j, a) with $a \neq 0$; divide its first component by a to recover s_j. The group computations are over k, and the query matrices are computed over R, giving the stated gate cost. □

4.3 The final digit

Lemma 4.3 reduces the remaining task to $q-1$ shifted copies indexed by $k^\times$. We work directly over the additive space k^l, including when q is not prime.

Proposition 4.6 (Finite-field $(q-1)$-shift)**.** *Let $k = \mathbb{F}_q$ with $q \ge 3$, let $F : k^l \to S$ be injective, and suppose we have quantum oracle access to*

$$\Psi_s(w,c) = F(w - c\,s), \qquad w \in k^l, \quad c \in k^\times, \tag{4.12}$$

for an unknown $s \in k^l$. Then s can be recovered in quantum time $\mathrm{poly}(l, \log q)$.

Proof. Choose distinct $c_0, c_1 \in k^\times$. Injectivity of F gives the exact verifier

$$z = s \quad \Longleftrightarrow \quad \Psi_s(0,c_0) = \Psi_s((c_1-c_0)z, c_1). \tag{4.13}$$

First test $z = 0$, and henceforth assume $s \neq 0$.

Fix a nontrivial additive character χ of k. Querying on a uniform superposition of $(w,c) \in k^l \times k^\times$ and measuring the output leaves $(q-1)^{-1/2}\sum_{c\neq 0}|y+cs\rangle|c\rangle$. (The measured value

$F(y)$ fixes $y = w - cs$ by injectivity of F.) Fourier transform the first register and measure it. The outcome $u \in k^l$ is uniform, and the remaining state, up to a global phase, is

$$\mu_{\ell(u)} = \frac{1}{\sqrt{q-1}} \sum_{c \neq 0} \chi(c\ell(u))|c\rangle, \qquad \ell(u) = u \cdot s. \tag{4.14}$$

The unknown s now enters only through the scalar $\ell(u)$. It therefore suffices to learn the nonzero linear form $\ell : k^l \to k$, and the two regimes below differ only in how $\ell(u)$ is extracted from $\mu_{\ell(u)}$. Note that μ_θ is the Fourier state κ_θ defined below with its $c = 0$ term removed.

Small q: $q \leq (l+1)^2$. Put $\kappa_\theta = q^{-1/2} \sum_{c \in k} \chi(c\theta)|c\rangle$. Project the remaining register onto the known unit vector

$$\eta = \frac{\kappa_0 - \kappa_1}{\sqrt{2}} = \frac{1}{\sqrt{2q}} \sum_{c \in k} (1 - \chi(c))|c\rangle. \tag{4.15}$$

It is supported on $k^\times$ and can be prepared by a QFT applied to $(|0\rangle - |1\rangle)/\sqrt{2}$; reversing that preparation implements the projection. Character orthogonality gives

$$|\langle \eta, \mu_\theta \rangle|^2 = \begin{cases} q/(2(q-1)), & \theta \in \{0, 1\}, \\ 0, & \text{otherwise.} \end{cases}$$

Since $\ell \neq 0$, acceptance has probability $1/(q-1)$, and the accepted u is uniform on $\ell^{-1}(\{0, 1\})$. So the projection postselects on $\ell(u) \in \{0, 1\}$. Learning ℓ from uniform samples of the preimage of a fixed subset of k, here of size $d = 2$, is the problem of learning a linear function from subset [IPS18]. This is an LFS$(q, l, 2)$ instance. The algorithm of [IPS18, Thms. 1.3 and 3.2] uses polynomially many samples and polynomial expected time, and recovers ℓ up to nonzero scalar with probability at least $1/2$. Its LFS theorem applies to prime-power q with $2 \leq d \leq q - 1$, so $d = 2$ is valid for every $q \geq 3$. Enumerate the at most $q - 1$ scalar multiples of its output and apply (4.13).

For bounded running time, let $M = \text{poly}(l, \log q)$ be the prescribed sample count and use $B = C(q-1)(M+1)$ raw trials. For a suitable absolute C, a binomial tail bound makes the probability of fewer than M acceptances at most $1/16$. Use the first M accepted samples, whose joint conditional distribution is the required independent LFS distribution; the acceptance indicators are independent of their accepted values. Also cap the randomized LFS postprocessing at eight times a polynomial upper bound for its expected running time. Markov's inequality bounds timeout probability by $1/8$. One capped attempt therefore succeeds with probability at least $1/2 - 1/16 - 1/8 > 1/4$. Its cost is polynomial because $q \leq (l+1)^2$.

Large q: $q > (l+1)^2$. An inverse QFT on (4.14) returns $\ell(u)$ with probability $(q-1)/q$, independently of u, because μ_θ differs from κ_θ only by the missing $c = 0$ term. With m independent samples, the probability that all reported values are correct and the u's are linearly independent is

$$\left(\prod_{i=1}^{l} (1 - q^{-i}) \right) (1 - 1/q)^l \geq c_\infty (1 - l/q) \geq c_\infty / 2.$$

Solve the resulting linear system and verify its candidate by (4.13); singular systems count as failed attempts.

In either regime, $O(\log(1/\epsilon))$ independent capped attempts reduce the ideal failure probability to $\epsilon/2$, with no false acceptance. Implementing the QFTs and preparations so that the

entire bounded computation has trace-distance error at most $\epsilon/2$ proves the stated bound. This includes the rejected trials and thus requires no separate conditioning estimate for approximate postselection. □

Remark 4.7. The chosen threshold is convenient rather than sharp. Direct Fourier recovery has constant success for $q = \Omega(l)$ and inverse-polynomial success for $q = \Omega(l/\log l)$, with the corresponding repetition overhead. The LFS branch is polynomial whenever $q = \mathrm{poly}(l)$.

4.4 Completing the lift

Theorem 4.8 (Rank-one lifting over finite chain rings)**.** *Let R be a finite chain ring of length $t \geq 2$ with residue field $k = \mathbb{F}_q$, $q \geq 3$. Given the reduced terminal line of a hidden parabolic subgroup of $\mathrm{GL}_n(R)$ whose terminal member T has rank one, T can be recovered exactly in quantum time $\mathrm{poly}(n, \log|R|)$.*

Proof. After moving the known reduction to ke_1, initialize $y_{<1} = 0$. Suppose $y - y_{<j} \in \pi^j R^l$ where $y_{<j}$ is as in (4.2). Conjugation by $C_j = \begin{pmatrix} 1 & 0 \\ -y_{<j} & I_l \end{pmatrix}$ puts the terminal line in the form (4.3). The digit s_j is well defined: any two choices of z_j differ by $\pi^{t-j}R^l$, whose reduction is zero. Use Proposition 4.5 for $j < t-1$, and Lemma 4.3 with Proposition 4.6 for $j = t-1$. Set $y_{<j+1} = y_{<j} + \pi^j \sigma(s_j)$. Then $y - y_{<j+1} \in \pi^{j+1}R^l$, and after $t-1$ stages it is zero.

Give each stage error $\epsilon/(t-1)$. A first-error union bound is valid because every stage has its stated promise before the first incorrect digit. Since $t \leq \log_2|R|$ and every stage has bounded polynomial time, the total satisfies Convention 2.10. Intermediate candidates can also be checked by $f_j(G_j(z,1)) = f_j(I)$; the last digit uses (4.13). □

Remark 4.9 (Length two and the binary exception). For $R = \mathbb{Z}/p^2\mathbb{Z}$ with p odd, the only unknown digit is $\mathrm{HMS}(p, n-1, p-1)$ with shift set $\mathbb{F}_p^\times$. For $q = 2$, that set has one element, so the final query family alone contains no shift information. Section 6 instead uses shifts indexed by elements of the whole reduced parabolic.

5 Full flag reconstruction for $q \geq 3$

We combine the reduced-flag and rank-one routines with a verified recursion. The following criterion ensures that every accepted reduction of dimension is legitimate.

Lemma 5.1 (Checking: [DIK+14, Lem. 10])**.** *Assume $q \geq 3$. Let $0 < W < V$ be split free with complement W' and put $\mathcal{L} = \{X \in G : (X-I)V \subseteq W\}$ and $\mathcal{L}' = \{X \in G : (X-I)V \subseteq W', (X-I)W' = 0\}$. Then $W \subseteq T$ iff $\mathcal{L} \subseteq H$; and if $W \subseteq T$ then $W = T$ iff $H \cap \mathcal{L}' = \{I\}$.*

Recall that T is the terminal member of the hidden flag. $\mathcal{L}$ consists of the elements moving every vector by an element of W, and it lies in every stabilizer of a flag whose members all contain W. The first criterion is a containment test, checkable on the generators of Lemma 2.9. The second detects whether W already exhausts T.

Proof. If $W \subseteq T$, every $X \in \mathcal{L}$ preserves each flag member. Conversely, choose $w \in W \setminus T$, a unimodular $\tau \in T$, and $\ell \in V^*$ with $\ell(\tau) = 1$. For a unit c, the map $X_c = I + cw\ell$ has

image deviation in W and $X_c\tau = \tau + cw \notin T$. Its determinant is $1 + c\ell(w)$. This is a unit automatically when $\ell(w) \in \mathfrak{m}$; otherwise choose $\bar{c} \neq -\overline{\ell(w)}^{-1}$, possible because $q \geq 3$.

For the second assertion, $\mathcal{L}' \cong \mathrm{Hom}_R(W, W')$. If $W < T$, the decomposition $T = W \oplus (T \cap W')$ supplies nonzero maps $W \to T \cap W'$ and hence nonidentity elements of $H \cap \mathcal{L}'$. If $W = T$, write $v = w + w'$. An element of $H \cap \mathcal{L}'$ fixes w' and has $Xw - w \in W \cap W' = 0$, so it is the identity. □

The first criterion is checked on generators of $\mathcal{L}$ (Lemma 2.9). It is specific to $q \geq 3$: the two lines in Example A.3 have indistinguishable stabilizers.

Lemma 5.2 (Recursion)**.** *Let $0 < W \subseteq T$ be split free of rank ρ and $V = W \oplus W'$. Embedding $\mathrm{GL}(W')$ by the identity on W, the restricted oracle hides the stabilizer of the induced flag with members $U_i \cap W'$. Remove repeated zero members. Each nonzero member is split free of rank $\operatorname{rank} U_i - \rho$, and*

$$U_i = W \oplus (U_i \cap W') \qquad (i < m).$$

The new ambient rank is $n - \rho < n$, and a query costs one original oracle call and $O(n^3)$ ring operations.

Proof. The decomposition follows from $W \subseteq U_i$. Its second summand is a direct summand of U_i, hence of V and W'. An automorphism fixing W pointwise and preserving W' stabilizes U_i exactly when its restriction stabilizes $U_i \cap W'$. Strict rank gaps persist, except that the terminal member becomes zero when $W = T$. In an adapted basis matrix B, the embedding is $Y \mapsto B \operatorname{diag}(I_\rho, Y)B^{-1}$. □

Theorem 5.3 (Flag reconstruction)**.** *For $q \geq 3$, Problem 2.11 is solvable in bounded-error quantum polynomial time. The algorithm also recovers the hidden flag.*

Proof. For $t = 1$ use [DIK+14]. Otherwise fix $c = \lceil \log_4(2n/\epsilon) \rceil$ and $N = n(c + 2)$. Give each invocation of Proposition 3.7, Proposition 3.4, or Theorem 4.8 error at most $\epsilon/(2N)$. A recursive call on V' with oracle f' proceeds as follows.

1. Recover the reduced flag and its type. If it has one block, propose the trivial flag and proceed to verification in step 4. Otherwise let d be its terminal rank.

2. If $d = 1$, use Theorem 4.8 to obtain a candidate W. If $d \geq 2$, try at most c independent uniform unimodular λ, using Proposition 3.4 to form $M_\lambda = \sum_X (X - I)V'$ from the returned generators. In either case accept a candidate only if it is proper, nonzero, split free, and passes $\mathcal{L} \subseteq H'$ from Lemma 5.1. Reject failed draws; report failure if no candidate is accepted.

3. Put $\rho = \operatorname{rank} W$ and choose $V' = W \oplus W'$. Recurse through Lemma 5.2. Lift each nonzero member U'' of the returned flag to $W \oplus U''$, and append W exactly when $\rho = d$.

4. Check that the candidate is a split free flag of the type returned in step 1. Compute its stabilizer generators and require $f'(X) = f'(I)$ for every generator. Return the flag and generators if all checks pass; otherwise return failure.

All calls have fixed polynomial time limits; propagate failure returns and cap the recursion at n nodes.

Correctness with exact subroutine answers. Step 1 gives the true type. Step 2 certifies $0 < W \subseteq T$, and a transverse draw when $d \geq 2$ passes with $W = T \cap P_\lambda$. For nested split free modules, $\rho = d$ is equivalent to $W = T$. Lemma 5.2 therefore proves the assembly rule and the strict decrease of ambient rank. The verification checks containment of the candidate stabilizer in H'; the correct type gives equal orders by Lemma 2.3, hence equality.

Error and cost. In the ideal recursion with exact answers, each draw at a node with $d \geq 2$ is transverse with probability at least $3/4$. Exhausting its c draws has probability at most 4^{-c}; across at most n nodes this contributes at most $\epsilon/2$. Couple the actual recursion to this ideal execution until its first incorrect subroutine answer. There are at most N invocations, each with a valid promise before that error, so discrepancy contributes at most $\epsilon/2$. The total failure probability is at most ϵ. The bounded recursion and all constituent bounds give $\mathrm{poly}(n, \log|R|, \log(1/\epsilon))$ time on every execution. The containment tests certify accepted W's. □

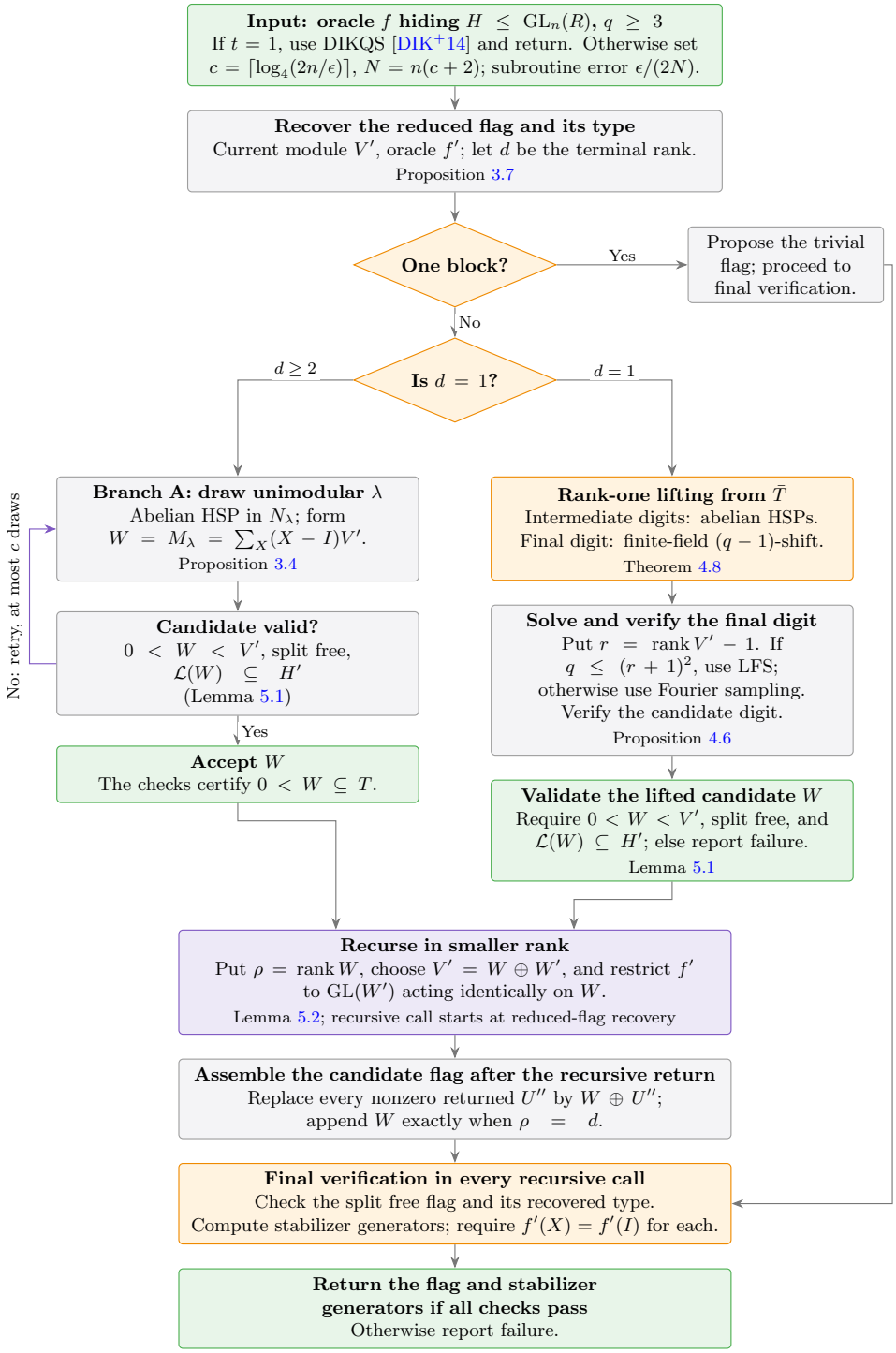


Figure 1: Full reconstruction for $q \geq 3$ (Theorem 5.3). The one-block case also undergoes final verification. Exhausted draws, failed checks, timeouts and recursive failures return failure; all loops are capped and there are at most n recursive nodes. The overall success probability is at least $1 - \epsilon$.

6 Subgroup lifting for binary residue fields

Assume $k = \mathbb{F}_2$ and $t \geq 2$. Let P be the standard parabolic (Definition 2.2) of the recovered type, $\mathfrak{l} \leq \mathrm{M}_n(k)$ its block lower triangular algebra, and $\mathfrak{u}$ the strictly upper-block subspace, so $\mathrm{M}_n(k) = \mathfrak{l} \oplus \mathfrak{u}$. Write $\mathrm{pr}_{\mathfrak{u}}$ for the projection, and put $\varepsilon = \pi^{t-1}$ and

$$\iota(Y) = I + \varepsilon \widehat{Y} \qquad (Y \in \mathrm{M}_n(k) \text{ and } \widehat{Y} = \sigma(Y) \in \mathrm{M}_n(R)).$$

This does not depend on the lift $\widehat{Y}$, since $\varepsilon\mathfrak{m} = 0$; also $\varepsilon^2 = 0$. We recover the conjugate subgroup rather than a uniquely specified flag. In this section ε always denotes π^{t-1}, not the error parameter ϵ. The map ι is the identification $\mathrm{M}_n(k) \cong K_{t-1}$ noted after Definition 2.13. Under it, $P \cap K_{t-1}$ corresponds to $\mathfrak{l}$.

Lemma 6.1 (Congruence commutators)**.** *For $1 \leq a, b \leq t$, $A \in \pi^a \mathrm{M}_n(R)$ and $B \in \pi^b \mathrm{M}_n(R)$, one has $[K_a, K_b] \subseteq K_{a+b}$. If $a + b \geq t - 1$, then*

$$[I + A, I + B] = I + AB - BA.$$

The coefficient depends only on $A \bmod \pi^{t-b}$ and $B \bmod \pi^{t-a}$.

Proof. The exact identity

$$[I + A, I + B] = I + (AB - BA)(I + A)^{-1}(I + B)^{-1}$$

gives the inclusion. When $a + b \geq t - 1$, multiplication of $AB - BA$ by either inverse leaves it unchanged because $\pi^{t-1}\mathfrak{m} = 0$. The two dependence claims follow by multiplying the possible differences. □

This lemma is what makes digit extraction possible. Suppose $g \in K_a$ is known only modulo π^{a+1}, and take $B \in \pi^{t-1-a} \mathrm{M}_n(R)$. Then $[g, I + B]$ already lies in the socle layer K_{t-1}, and it depends only on the leading digit of $g - I$.

6.1 Standardization and the reference oracle

Lemma 6.2 (Standardization after reduction)**.** *Let $\mathcal{F}$ be a split free flag whose reduction modulo $\mathfrak{m}$ is the standard flag $\mathcal{F}_0$ stabilized by P. Then*

$$\mathcal{F} = g\mathcal{F}_0$$

for some $g \in K_1$. Consequently

$$G_{\{\mathcal{F}\}} = gPg^{-1}, \qquad g \in K_1.$$

Proof. Choose a basis of V adapted to $\mathcal{F}$ whose reduction is the standard basis of $\bar{V}$. Such a basis is obtained by lifting, successively along the flag, bases of the quotients $\bar{U}_i/\bar{U}_{i+1}$; the basis-extension property in Lemma 2.5 and Nakayama's lemma show that the lifts form an R-basis. If g is the matrix whose columns are these vectors, then $g \equiv I \pmod{\mathfrak{m}}$, hence $g \in K_1$, and $g\mathcal{F}_0 = \mathcal{F}$. □

Lemma 6.3 (Socle reference oracle)**.** *Suppose*

$$H = gPg^{-1}, \qquad g \in K_1.$$

Then

$$H \cap K_{t-1} = P \cap K_{t-1}.$$

Moreover

$$A_{\mathfrak{u}} := \{\iota(Y) : Y \in \mathfrak{u}\}$$

is an elementary abelian subgroup isomorphic to $(\mathfrak{u}, +)$*, and*

$$F : \mathfrak{u} \longrightarrow S, \qquad F(Y) = f(\iota(Y)),$$

is injective.

Socle elements commute with K_1, so conjugation by the unknown g is invisible on K_{t-1}. There the oracle sees only the known P, and F labels the cosets of $P \cap K_{t-1} \leftrightarrow \mathfrak{l}$ by their $\mathfrak{u}$-component. This gives a reference copy of the oracle against which shifts can be measured.

Proof. The inclusion $[K_1, K_{t-1}] \subseteq K_t = \{I\}$ gives $H \cap K_{t-1} = P \cap K_{t-1}$. The identity $\iota(Y)\iota(Z) = \iota(Y+Z)$ identifies $A_{\mathfrak{u}}$ with $(\mathfrak{u}, +)$. If $f(\iota(Y)) = f(\iota(Z))$, then $\iota(Z-Y) \in P \cap K_{t-1}$, hence $Z - Y \in \mathfrak{l}$. For $Y, Z \in \mathfrak{u}$ this forces $Y = Z$. □

Lemma 6.4 (Two-copy socle shift)**.** *Assume* $H = gPg^{-1}$ *with* $g \in K_1$*, and let* $w \in P$ *satisfy*

$$gwg^{-1}w^{-1} = \iota(C)$$

for some $C \in M_n(k)$*. Put*

$$s = \mathrm{pr}_{\mathfrak{u}}(C).$$

Then the function

$$\Phi_w : \mathfrak{u} \times \mathbb{F}_2 \longrightarrow S$$

defined by

$$\Phi_w(Y, 0) = f(\iota(Y)), \qquad \Phi_w(Y, 1) = f(\iota(Y)w)$$

hides the subgroup

$$L_s = \{(0,0), (s,1)\} \leq \mathfrak{u} \times \mathbb{F}_2.$$

Thus s *is recoverable by an abelian HSP in quantum time* $\mathrm{poly}(n, \log |R|)$.

Here w is a known element of the reference parabolic P, and conjugation by the unknown g moves it by the socle element $\iota(C)$. The oracle on $\iota(Y)w$ is therefore the reference oracle F shifted by s, the $\mathfrak{u}$-part of C. In characteristic two, shifting by s while flipping the second coordinate is an involution, so $\{(0,0), (s,1)\}$ is a subgroup. This is the "two-copy" structure, and it replaces the $q-1$ shifted copies available when $q \geq 3$.

Proof. Put $c = \iota(C)$, so $cw = gwg^{-1} \in H$. Right multiplication by $(cw)^{-1}$ gives

$$\Phi_w(Y, 1) = f(\iota(Y)w(cw)^{-1}) = f(\iota(Y - C)).$$

Write $C = C_{\mathfrak{l}} + s$. Since $\iota(-C_{\mathfrak{l}}) \in P \cap K_{t-1} \subseteq H$, we obtain $\Phi_w(Y, 1) = F(Y - s)$ and $\Phi_w(Y, 0) = F(Y)$. Injectivity of F and characteristic two show that collisions are exactly differences in $\{(0,0), (s,1)\}$. □

The HSP here is on the parameter group $\mathfrak{u} \times \mathbb{F}_2$. The query matrices $\iota(Y)w^b$ need not form a subgroup; their multiplication is not used in the reduction.

6.2 Intermediate layers

Proposition 6.5 (One intermediate lifting layer)**.** *Suppose*

$$H_j = g_j P g_j^{-1}, \qquad g_j \in K_j,$$

where $1 \le j < t-1$*. Using* n *abelian HSP instances one can compute an explicit* $c_j \in K_j$ *such that*

$$c_j H_j c_j^{-1} = g_{j+1} P g_{j+1}^{-1}$$

for some $g_{j+1} \in K_{j+1}$*.*

Proof. Write $g_j \equiv I + \pi^j \widehat{X} \pmod{\pi^{j+1}}$ and $x = \mathrm{pr}_{\mathfrak{u}}(X)$. For $a = 1, \dots, n$, use the diagonal element $w_a = I + \pi^{t-1-j} E_{aa} \in P$. Since $g_j \in K_j$ and $w_a \in K_{t-1-j}$, Lemma 6.1 applies with exponents summing to $t-1$. The commutator lies in the socle and depends only on the leading digit X of g_j:

$$[g_j, w_a] = \iota([X, E_{aa}]).$$

The two-copy HSP of Lemma 6.4 therefore returns $s_a = \mathrm{pr}_{\mathfrak{u}}([X, E_{aa}]) = \mathrm{pr}_{\mathfrak{u}}([x, E_{aa}])$. The lower-block component drops out because $\mathfrak{l}$ is an algebra. For every upper-block entry in column a, $[x, E_{aa}]_{ia} = x_{ia}$, so these shifts determine x.

Lift x with support in the upper blocks and put $c_j = I - \pi^j \widehat{x}$. The leading coefficient of $c_j g_j$ lies in $\mathfrak{l}$. Thus for some $p_j \in P \cap K_j$, $g_{j+1} = c_j g_j p_j^{-1} \in K_{j+1}$, and $c_j H_j c_j^{-1} = g_{j+1} P g_{j+1}^{-1}$. Only c_j needs to be computed. □

Updating the oracle by $f_{j+1}(X) = f_j(c_j^{-1} X c_j)$ removes one layer. Iterate for $j = 1, \dots, t-2$.

6.3 The final layer

Now $H_{t-1} = g P g^{-1}$ with $g \in K_{t-1}$. Absorb the $\mathfrak{l}$-component into P and write $g = \iota(X)$ for some $X \in \mathfrak{u}$. Let $\bar{P} = P(k)$.

Proposition 6.6 (Final layer)**.** *The subgroup* H_{t-1} *can be recovered in quantum time* $\mathrm{poly}(n, \log |R|)$*.*

At the last layer the conjugator $g = \iota(X)$ lies in the socle itself, so its commutator with every $w \in P$ is a socle element, not only with diagonal probes. Each generator u_i of $\bar{P}$ gives one linear equation for X over $\mathbb{F}_2$. Here ρ is the action of $\bar{P}$ on $\mathfrak{u} \cong \mathrm{M}_n(k)/\mathfrak{l}$ induced by conjugation. The solution set is X plus the directions D with $\iota(D)$ normalizing P, and these do not change H_{t-1}.

Proof. Choose generators $u_1, \dots, u_\nu$ of $\bar{P}$, using the admissible elementary transvections over $\mathbb{F}_2$; $\nu \le n(n-1)$. Lift them to $w_i \in P$. Since $\varepsilon^2 = 0$,

$$[g, w_i] = \iota(X - u_i X u_i^{-1}),$$

so Lemma 6.4 yields $s_i = \mathrm{pr}_{\mathfrak{u}}(X - u_i X u_i^{-1})$.

Conjugation preserves $\mathfrak{l}$, hence induces the representation

$$\rho(u) Y = \mathrm{pr}_{\mathfrak{u}}(u Y u^{-1}) \quad \text{on } \mathfrak{u} \cong \mathrm{M}_n(k)/\mathfrak{l}.$$

Solve $(I-\rho(u_i))X_0 = s_i$ over $\mathbb{F}_2$. The true X proves consistency. For any solution, $D = X - X_0$ is fixed by the generators and therefore by all of $\bar{P}$. Equivalently, $D - uDu^{-1} \in \mathfrak{l}$ for every $u \in \bar{P}$. For $p \in P$ this gives

$$[\iota(D), p] = I + \varepsilon(\widehat{D} - p\widehat{D}p^{-1}) \in P.$$

Thus $\iota(D)P\iota(D)^{-1} \subseteq P$, and finiteness gives equality. Conversely, if $\iota(D)$ normalizes P, these commutators belong to $P \cap K_{t-1}$; their reduced coefficients are in $\mathfrak{l}$, so $\rho(u)D = D$ for all u. The homogeneous solutions are therefore exactly the socle normalizer directions.

Finally, $\iota(X) = \iota(X_0)\iota(D)$, and hence $H_{t-1} = \iota(X_0)P\iota(X_0)^{-1}$. Conjugating generators of P gives the required output. □

Theorem 6.7 (Binary residue field)**.** *Let R be a finite chain ring with residue field $R/\mathfrak{m} = \mathbb{F}_2$, presented as in Section 2.2. Then Problem 2.11 is solvable in quantum time* $\mathrm{poly}(n, \log|R|)$*, in the sense of Convention 2.10.*

Proof. For $t = 1$ use [DIK+14]. Otherwise set

$$N_0 = 1 + n(t-2) + n(n-1)$$

and give each of the following randomized calls error at most ϵ/N_0. First recover $\bar{\mathcal{F}}$ by Proposition 3.7. Let $\bar{b}$ have columns forming an adapted basis of $\bar{\mathcal{F}}$, and lift it to $b \in \mathrm{GL}_n(R)$. Then $b^{-1}Hb = g_1 P g_1^{-1}$ for some $g_1 \in K_1$ by Lemma 6.2.

Apply Proposition 6.5 for $j = 1, \ldots, t-2$, then Proposition 6.6. The resulting subgroup is CHC^{-1}, where the known product is

$$C = c_{t-2} \cdots c_1 b^{-1}.$$

Conjugate its generators by C^{-1} to obtain generators of H.

Before the first erroneous answer, every call has a valid promise. There are at most N_0 calls, so the first-error union bound gives failure probability at most ϵ. Use the prescribed time caps and return failure on malformed subspaces, inconsistent linear systems, or failed subroutines. Each HSP has an elementary abelian parameter group of dimension at most $n^2 + 1$ over $\mathbb{F}_2$; the remaining work is polynomial linear algebra and matrix arithmetic. Since $t \le \log_2|R|$, the claimed bounded running time follows. For the one-block type, $\mathfrak{u} = 0$ and the same construction simply returns G. □

Remark 6.8 (Even residue fields). The same lifting construction works over $k = \mathbb{F}_{2^f}$. Its two-copy graph is still a subgroup of $\mathfrak{u} \times \mathbb{F}_2$. Generate $\bar{P}$ by admissible $I + b_r E_{ij}$ for an $\mathbb{F}_2$-basis $\{b_r\}$ of k, together with diagonal generators of $k^\times$; there are $O(n^2 \log q)$ such generators. Expand the parameter groups and final linear system over $\mathbb{F}_2$. All costs remain polynomial in $n, \log|R|$. In odd characteristic a nonzero shift does not give a subgroup of $\mathfrak{u} \times \mathbb{F}_2$, so this two-copy reduction is unavailable.

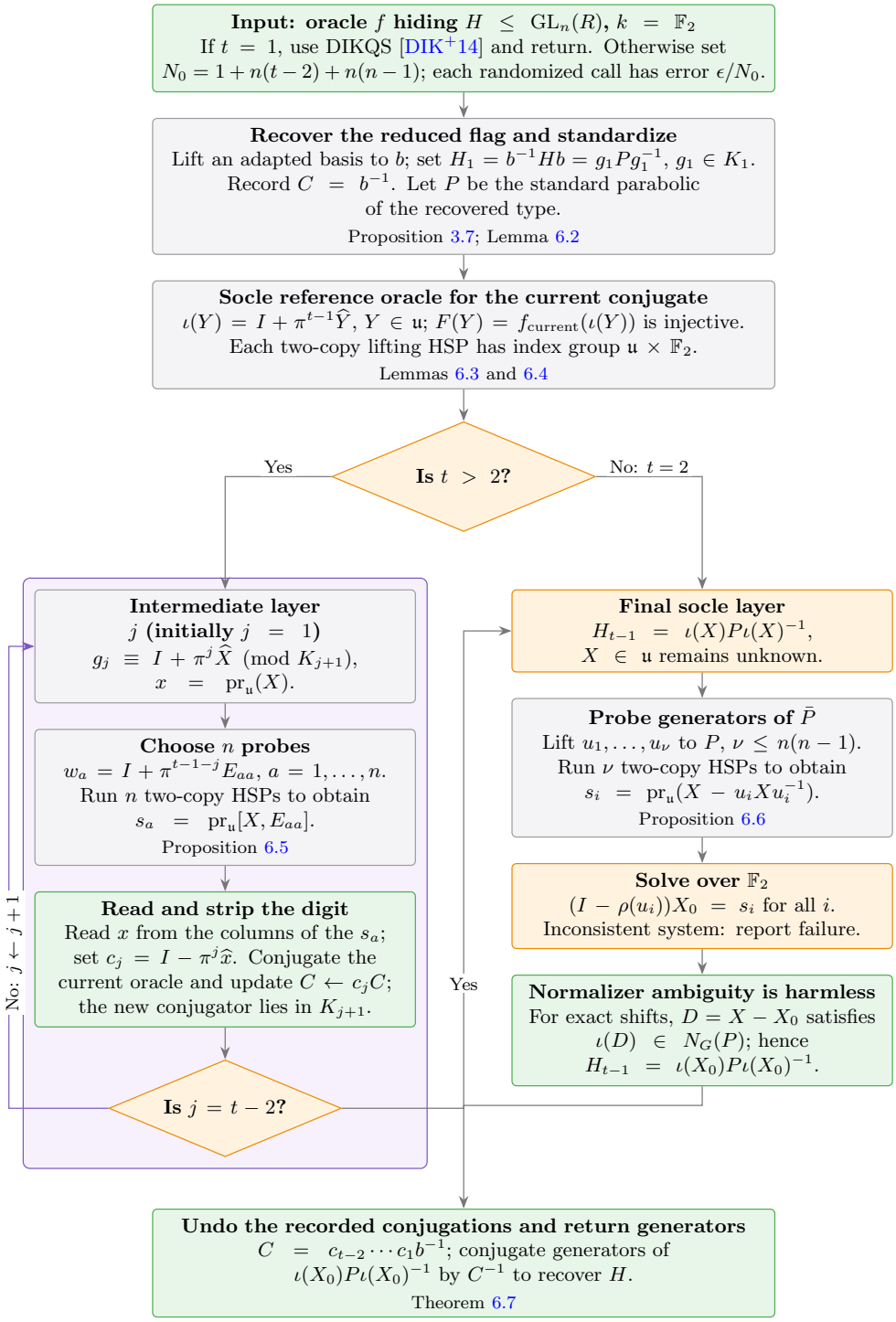


Figure 2: Subgroup reconstruction for $q = 2$ (Theorem 6.7). The intermediate loop is skipped when $t = 2$. All calls have prescribed time caps; malformed outputs and failed subroutines return failure. With probability at least $1-\epsilon$, the returned generators define H; a unique hidden flag is not required. For the one-block type, $\mathfrak{u} = 0$ and the construction returns $\mathrm{GL}_n(R)$.

7 Arithmetic consequences

Proof of Theorem 1.1. Apply Theorem 5.3 when $q \geq 3$ and Theorem 6.7 when $q = 2$, with the common input and error model. □

Corollary 7.1. *For every integer $N \geq 2$, the parabolic HSP in $\mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ is solvable in quantum time $\mathrm{poly}(n, \log N)$.*

Proof. Factor N using Shor's algorithm [Sho97] and apply CRT: $\mathbb{Z}/N\mathbb{Z} \cong \prod_{p^a \| N} \mathbb{Z}/p^a\mathbb{Z}$. A split free flag decomposes componentwise, as does its stabilizer. The embedding of one matrix-group factor with identities in the others therefore restricts the oracle to a component parabolic. Apply Theorem 1.1 to each component and combine generators by CRT. This includes all powers of two. There are at most $\log_2 N$ factors and their logarithmic sizes sum to $\log N$. Assign error $\epsilon/2$ to integer factorization and split the remaining budget among the component calls. □

Definition 7.2 (Number-field input)**.** A number field K is supplied by a monic irreducible $g \in \mathbb{Z}[x]$, an integral basis of its maximal order $\mathcal{O}_K$ expressed in the power basis of $K = \mathbb{Q}[x]/(g)$, and its multiplication table. Let L_K be the total bit length of this data.

The maximal-order basis is part of the input; computing it is not assumed free. Arithmetic modulo N is polynomial in $L_K, \log N$.

Corollary 7.3. *Let K be a number field given in standard form and let $N \geq 2$. Then the parabolic HSP in*

$$\mathrm{GL}_n(\mathcal{O}_K/N\mathcal{O}_K)$$

is solvable in quantum time $\mathrm{poly}(n, L_K, \log N, \log(1/\epsilon))$ with probability at least $1 - \epsilon$.

Proof. After factoring N, write $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e_\mathfrak{p}}$ and set $a_\mathfrak{p} = e_\mathfrak{p} v_p(N)$. Then

$$\mathcal{O}_K/N\mathcal{O}_K \cong \prod_{\mathfrak{p}|N} \mathcal{O}_K/\mathfrak{p}^{a_\mathfrak{p}},$$

and each factor is a finite chain ring. Appendix C constructs the required effective presentations in bounded randomized classical polynomial time once the factorization of N is available. Restrict the oracle to each factor as in Corollary 7.1, apply Theorem 1.1, and recombine. The logarithmic factor sizes sum to $[K : \mathbb{Q}] \log N$. Splitting the error budget between factorization, preprocessing, and the component calls preserves the stated bound. □

Declaration on the use of AI tools

The author used Claude Opus 5.5 to assist with LaTeX formatting, checking grammatical errors, and exploring proof strategies. All mathematical results, proofs and claims were verified by the author, who takes full responsibility for the content of this paper.

Acknowledgment

The author is supported by EPSRC through grant number EP/V011324/1. The author also thanks Gábor Ivanyos for reading an earlier version of this manuscript and for helpful comments.

References

[AEJS26] Gorjan Alagic, Simona Etinski, Stacey Jeffery, and Rainer Steinwandt. Quantum cryptanalysis (Dagstuhl seminar 25431). *Dagstuhl Reports*, 15(10):105–118, 2026. Working group "Quantum cryptanalysis of non-abelian group actions", p. 113.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, MA, 1969.

[BL95] Dan Boneh and Richard J. Lipton. Quantum cryptanalysis of hidden linear functions. In *CRYPTO 1995*, volume 963 of *LNCS*, pages 424–437, 1995.

[CII+23] Mingjie Chen, Muhammad Imran, Gábor Ivanyos, Péter Kutas, Antonin Leroux, and Christophe Petit. Hidden stabilizers, the isogeny to endomorphism ring problem and the cryptanalysis of pSIDH. In *ASIACRYPT 2023*, volume 14440 of *LNCS*, pages 99–130, 2023.

[CME+25] Clémence Chevignard, Guilhem Mureau, Thomas Espitau, Alice Pellet-Mary, Heorhii Pliatsok, and Alexandre Wallet. A reduction from Hawk to the principal ideal problem in a quaternion algebra. In *EUROCRYPT 2025*, 2025. eprint 2025/287.

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer, Berlin, 1993.

[DIK+14] Thomas Decker, Gábor Ivanyos, Raghav Kulkarni, Youming Qiao, and Miklos Santha. An efficient quantum algorithm for finding hidden parabolic subgroups in the general linear group. In *MFCS 2014*, pages 226–238, 2014. arXiv:1406.6511.

[DMR10] Aaron Denney, Cristopher Moore, and Alexander Russell. Finding conjugate stabilizer subgroups in PSL(2;q) and related problems. *Quantum Information & Computation*, 10:282–291, 2010.

[Geo16] Nevyana Georgieva. Basic algorithms for manipulation of modules over finite chain rings. *Serdica Journal of Computing*, 10(3–4):285–297, 2016.

[II22] Muhammad Imran and Gábor Ivanyos. An exact quantum hidden subgroup algorithm and applications to solvable groups. *Quantum Information & Computation*, 22(9–10):770–789, 2022.

[II24] Muhammad Imran and Gábor Ivanyos. Zero sum subsequences and hidden subgroups. *Quantum Information Processing*, 23(1):14, 2024.

[IMS01] Gábor Ivanyos, Frédéric Magniez, and Miklos Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. In *Proceedings of the Thirteenth Annual ACM Symposium on Parallel Algorithms and Architectures*, pages 263–270, 2001.

[IPS18] Gábor Ivanyos, Anupam Prakash, and Miklos Santha. On learning linear functions from subset and its applications in quantum computing. In *ESA 2018*, volume 112 of *LIPIcs*, pages 66:1–66:14, 2018.

[ISS07] Gábor Ivanyos, Luc Sanselme, and Miklos Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 586–597. Springer, 2007.

[ISS12] Gábor Ivanyos, Luc Sanselme, and Miklos Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. *Algorithmica*, 63:91–116, 2012. Preliminary version in LATIN 2008, pp. 759–771.

[Iva12] Gábor Ivanyos. Finding hidden borel subgroups of the general linear group. *Quantum Information & Computation*, 12:661–669, 2012.

[Kit96] A Kitaev. Quantum measurements and the abelian stabilizer problem. *Electronic Colloquium on Computational Complexity (ECCC)*, 3(3):1, 1996.

[McD74] Bernard R. McDonald. *Finite Rings with Identity*, volume 28 of *Pure and Applied Mathematics*. Marcel Dekker, New York, 1974.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997.

[Woo99] Jay A Wood. Duality for modules over finite rings and applications to coding theory. *American journal of Mathematics*, 121(3):555–575, 1999.

A Supporting algebra and effective operations

A.1 Split submodules and faithfulness

Proof of Lemma 2.5. Given generators with independent reductions, extend those reductions to a basis of k^n and lift the additional vectors. The resulting square matrix has unit determinant, so it is an R-basis of V; this proves (b)⇒(a). If $V = U \oplus C$, then $U \cap \pi^j V = \pi^j U$, proving purity and $\bar{U} \cong U/\mathfrak{m}U$; hence (a)⇒(c). Under (c), lifts of a basis of $\bar{U} \cong U/\mathfrak{m}U$ generate U by Nakayama, proving (b).

A complement of a free direct summand is a finitely generated projective module over the local ring R, hence free [AM69, McD74]. If $U' \leq U$ is split free with $V = U' \oplus D$, then $U = U' \oplus (U \cap D)$. Finally $\operatorname{rank} U = \dim_k \bar{U}$ implies that a nonzero split free module cannot lie in $\mathfrak{m}V$. □

Lemma A.1 (Invariant subspaces of a parabolic over a field)**.** *Let $q \geq 3$, let $\bar{\mathcal{F}} : k^n = \bar{U}_0 > \bar{U}_1 > \cdots > \bar{U}_m = 0$ be a flag of subspaces of k^n and let $\bar{P} \leq \mathrm{GL}_n(k)$ be its stabilizer. Then the $\bar{P}$-invariant subspaces of k^n are exactly the members $\bar{U}_0, \ldots, \bar{U}_m$.*

Proof. Use the block decomposition $k^n = \bigoplus_{j=1}^m B_j$ with $\bar{U}_i = \bigoplus_{j>i} B_j$. Choose $\alpha \in k^\times \setminus \{1\}$. Scaling only block j by α shows that any invariant subspace $\bar{W}$ contains each block component of each of its vectors. Thus $\bar{W} = \bigoplus_j (\bar{W} \cap B_j)$. The block group $\mathrm{GL}(B_j)$ is transitive on nonzero vectors, so every intersection is 0 or B_j. Lower-block transvections force the selected blocks to be a terminal segment, giving exactly the stated flag members. □

Proof of Theorem 2.12. The idea is as follows. Reducing modulo $\mathfrak{m}$ pins $\bar{W}$ down to a reduced member $\bar{U}_i$. A block scalar $X_\alpha \in H$ with $\alpha - 1$ a unit, available exactly because $q \geq 3$, then splits W along $U_i \oplus C_i$, and Nakayama's lemma finishes the argument.

Write $H = G_{\{\mathcal{F}\}}$ for $\mathcal{F} : V = U_0 > \cdots > U_m = 0$, and let W be a member of $\mathcal{F}'$, so W is split free and H-invariant. We show $W = U_i$ for some i.

Fix an adapted basis for $\mathcal{F}$ and let C_i be the span of the basis vectors outside U_i, so $V = U_i \oplus C_i$ and $U_j = U_i \oplus (U_j \cap C_i)$ for $j < i$. Reduction modulo $\mathfrak{m}$ maps H onto the parabolic subgroup $\bar{P}$ of $\mathrm{GL}_n(k)$ stabilizing $\bar{\mathcal{F}}$ (block triangular matrices lift to block triangular matrices), whose invariant subspaces are exactly the $\bar{U}_i$ by Lemma A.1. Hence $\bar{W} = \bar{U}_i$ for some i.

For $\alpha \in R^\times$ let X_α act as α on U_i and as the identity on C_i. Then X_α preserves every U_j, so $X_\alpha \in H$. For $w = u + c \in W$ with $u \in U_i$, $c \in C_i$ we get $X_\alpha w - w = (\alpha - 1)u \in W$. By (2.1) we may choose α with $\alpha - 1 \in R^\times$, whence $u \in W$ and $c \in W$. Thus $W = (W \cap U_i) \oplus (W \cap C_i)$, and $W \cap C_i$ is a direct summand of W, hence split free in V by Lemma 2.5. But $\overline{W \cap C_i} \subseteq \bar{W} \cap \bar{C}_i = \bar{U}_i \cap \bar{C}_i = 0$, so $W \cap C_i \subseteq \mathfrak{m}V$, which forces $W \cap C_i = 0$ by the last sentence of Lemma 2.5. Therefore $W \subseteq U_i$, and $\bar{W} = \bar{U}_i$ gives $U_i = W + \mathfrak{m}U_i$, so $W = U_i$ by Lemma 2.4. □

Proposition A.2 (Failure for $q = 2$)**.** *Let $q = 2$, $t \geq 2$, $n = 2$, and let $S = Rv$ be a free cyclic submodule of $V = R^2$. Then for a free cyclic $S' = Rv'$,*

$$G_{\{S'\}} = G_{\{S\}} \quad \Longleftrightarrow \quad v' \equiv uv \pmod{\pi^{t-1}V} \text{ for some } u \in R^\times,$$

so the fibre of $\mathcal{F} \mapsto G_{\{\mathcal{F}\}}$ through S has exactly $q = 2$ elements. In particular the oracle of Problem 2.11 does not determine the last π-adic digit of S.

Proof. Choose $S = Re_1$; its stabilizer consists of $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $a, d \in R^\times$. If a unimodular (x, y) spans an invariant line and y is a unit, varying b gives a contradiction. Normalize therefore to $(1, y)$ with $y \in \mathfrak{m}$. Invariance is equivalent to

$$(d - a)y - by^2 = 0 \qquad (a, d \in R^\times,\ b \in R).$$

Since $R^\times = 1 + \mathfrak{m}$, the differences $d - a$ run through $\mathfrak{m}$. Thus $\mathfrak{m}y = 0$, or $y \in \pi^{t-1}R$. Conversely this condition also gives $y^2 = 0$ for $t \geq 2$, so it is sufficient. There are exactly $q = 2$ choices of y. We have proved containment of stabilizers; both stabilize split lines, so they are conjugate and have equal order. Containment is therefore equality. □

Example A.3. Over $\mathbb{Z}/4\mathbb{Z}$, the lines $R(1, 0)$ and $R(1, 2)$ are distinct but have the same stabilizer. Indeed an upper triangular invertible matrix sends $(1, 2)$ to $(a + 2b, 2d) = (a + 2b)(1, 2)$, since a, d are odd.

A.2 Unit generators and module algorithms

Let $b_1, \ldots, b_f$ be an $\mathbb{F}_p$-basis of k, and let γ lift a generator of $k^\times$. Then

$$\gamma, \qquad 1 + \pi^i \sigma(b_r) \quad (1 \leq i < t,\ 1 \leq r \leq f)$$

generate $R^\times$. Their images generate the residue units and every quotient $(1+\mathfrak{m}^i)/(1+\mathfrak{m}^{i+1}) \cong (k, +)$; induction through the filtration proves the claim. There are $1 + (t - 1)f = O(\log |R|)$ generators.

A certified primitive residue element can be found in quantum polynomial time by factoring $q - 1$ with Shor's algorithm and testing orders. For randomized classical preprocessing, use instead h independent uniform elements of $k^\times$. The cyclic group has one maximal subgroup for each prime $\ell \mid q - 1$, so failure to generate has probability at most

$$\sum_{\ell \mid q-1} \ell^{-h} \leq (\log_2 q) 2^{-h}.$$

Thus $h = O(\log \log q + \log(1/\delta))$ suffices with error δ. Lift these elements and add the principal-unit generators above. This avoids factoring $q - 1$.

Effective operations in Lemma 2.9. Standard-form algorithms over finite chain rings compute submodule membership, sums, intersections, and relations [Geo16]. Their arithmetic is effective in the presentation of Section 2.2; linear equations in additive coordinates may also be solved by Smith normal form. Splitness requires the full criterion of Lemma 2.5, not just the dimension of the reduction. For a split free module, extending a reduced basis and lifting produces a complement and quotient coordinates.

In an adapted basis, a parabolic is generated by admissible elementary transvections $I + a_r E_{ij}$, where the a_r additively generate R, and diagonal matrices from generators of $R^\times$. Elementary elimination over the local ring proves generation of each diagonal GL block; the lower blocks are generated by the remaining transvections. For $V = W \oplus W'$ the group $(X - I)V \subseteq W$ has matrices $\left(\begin{smallmatrix} A & B \\ 0 & I \end{smallmatrix}\right)$, and the same generators in the permitted positions apply. There are polynomially many generators, and basis conjugation is polynomial. All costs include the total encoding length of the supplied module generators. □

B Transported Fourier procedures

These procedures explain the relation with [DIK+14]; they are not used in the proof of Theorem 1.1. A finite ring is Frobenius if it admits an additive character whose kernel contains no nonzero ideal [Woo99].

B.1 Duality and sampling

Lemma B.1. *Let R be a finite chain ring. Then R is a Frobenius ring, and there is a character $\chi : (R,+) \to \mathbb{C}^\times$ whose kernel contains no nonzero ideal, computable from the presentation of R. The pairing*

$$\langle A, B\rangle = \chi\big(\mathrm{tr}(AB)\big), \qquad A, B \in L := \mathrm{M}_n(R),$$

is a perfect, symmetric, conjugation-invariant pairing of $(L,+)$ with itself. Consequently, for every subgroup $W \le (L,+)$ one has $|W|\,|W^\perp| = |L|$ and $W^{\perp\perp} = W$.

Proof. Every nonzero ideal contains the simple socle $\pi^{t-1}R$. Choose a character χ nontrivial on that socle; it kills no nonzero ideal. It is computable from additive cyclic coordinates: choose a nonzero coordinate of π^{t-1} and use that coordinate character. If $\chi(\mathrm{tr}(AB)) = 1$ for all B, take $B = cE_{ji}$ to see that $\chi(cA_{ij}) = 1$ for every c. Hence (A_{ij}) lies in the kernel and $A_{ij} = 0$. Symmetry and conjugation invariance follow from cyclicity of trace. The annihilator identities are finite abelian duality. The pairing identification and its inverse are computable by linear algebra in additive coordinates, in $\mathrm{poly}(n, \log|R|)$ time. □

Lemma B.2 (Coset sampling)**.** *Let $W \le (L,+)$, let $\emptyset \neq W' \subseteq W$ and $v_0 \in L$. Applying the abelian QFT of $(L,+)$ to $|v_0 + W'\rangle = \frac{1}{\sqrt{|W'|}} \sum_{v\in W'} |v_0 + v\rangle$ and measuring yields each $u \in W^\perp$ with probability exactly $\frac{|W'|}{|W|} \cdot \frac{1}{|W^\perp|}$, and hence an element of $W^\perp$ with probability $|W'|/|W|$. Moreover, if W' is a union of cosets of a subgroup $K \le W$, then every measurement outcome lies in $K^\perp$.*

Proof. The amplitude at u is $\chi(\mathrm{tr}(v_0 u))|W'|^{-1/2}|L|^{-1/2} \sum_{v\in W'} \langle v, u\rangle$. For $u \in W^\perp$ each summand is 1, giving squared amplitude $|W'|/|L|$, and $|L| = |W||W^\perp|$ by Lemma B.1. For the last claim, suppose $W' = \bigcup_j (a_j + K)$ is a union of cosets of $K \le W$. Then $\sum_{v\in W'} \langle v, u\rangle = \sum_j \langle a_j, u\rangle \sum_{k\in K} \langle k, u\rangle$. If $u \notin K^\perp$, then $k \mapsto \langle k, u\rangle$ is a nontrivial character of K, and hence $\sum_{k\in K} \langle k, u\rangle = 0$. Therefore the amplitude at u vanishes, so every measurement outcome lies in $K^\perp$. □

Uniform states over $\mathrm{GL}_n(R)$ can be prepared by testing invertibility of uniform matrices, with success at least c_∞. Capping this preparation and using approximate abelian transforms implements the following sampling routines within their allocated error budgets.

B.2 Maximal parabolics and complements

Proposition B.3 (Maximal parabolics; cf. [DIK+14, Prop. 6])**.** *Let $q \ge 3$ and let $\mathcal{H} = \{G_{\{U\}} : U \le V$ split free, $0 < U < V\}$. Then $\mathrm{HSP}(\mathrm{GL}_n(R), \mathcal{H})$ is solvable in quantum time $\mathrm{poly}(n, \log|R|)$.*

Proof. Let $H = G_{\{U\}}$, $\operatorname{rank} U = n - d$, and $W = \{X \in \mathrm{M}_n(R) : XU \subseteq U\}$. Then $H = W \cap G$, $|H|/|W| = c_q(d)c_q(n-d) \geq c_\infty^2$, and

$$W^\perp = \{X : XV \subseteq U,\ XU = 0\} \cong \operatorname{Hom}_R(V/U, U).$$

A left coset state $|AH\rangle$ is supported in AW. Lemma B.2 gives a uniform element $u = XA^{-1} \in W^\perp A^{-1}$ with probability $|H|/|W|$. If $\operatorname{rank} U \leq d$, the induced map $V/U \to U$ is surjective with probability at least c_∞, and $uV = XV = U$. For a right coset state $|HA\rangle$, the corresponding good sample is $u = A^{-1}X$. If $d \leq \operatorname{rank} U$, that induced map is injective with split image with probability at least c_∞, giving $\ker u = U$.

At each trial run both the left-coset/image and right-coset/kernel procedures, since the rank is unknown. Require a candidate U' to be proper, nonzero, and split free, and test $G_{\{U'\}} \subseteq H$ on generators. Theorem 2.12 forces $U' = U$, so accepted candidates are correct. A constant success probability and $O(\log(1/\epsilon))$ trials suffice. □

Proposition B.4 (Complements; cf. [DIK+14, Prop. 7])**.** *Let $q \geq 3$, and let $\mathcal{H}$ be the family of complements $\mathcal{H}_\tau = \{I + c\tau\lambda : 1 + c \in R^\times\}$ of N_λ in G_λ, for $\tau \in V$ with $\lambda(\tau) = 1$. Then $\mathrm{rHSP}(G_\lambda, \mathcal{H})$ is solvable by a quantum algorithm with $O((1-1/q)^{-(n-1)})$ expected repetitions of a $\mathrm{poly}(n, \log|R|)$-time procedure, returning $R\tau$ at full precision.*

Proof. Identify $L_\lambda = \{a\lambda : a \in V\}$ with V and use the perfect coordinate pairing $\chi(\sum_i a_i b_i)$, rather than the possibly degenerate restriction of the matrix trace pairing. Put $W = R\tau\lambda$ and $W' = \{c\tau\lambda : 1 + c \in R^\times\}$. For $A = I + a\lambda$ and $\alpha = 1 + \lambda(a) \in R^\times$, subtracting I from a right coset $\mathcal{H}_\tau A$ gives $(A - I) + W'\alpha \subseteq (A - I) + W$, with density $1 - 1/q$. By Lemma B.2, $n - 1$ Fourier outcomes all lie uniformly in $W^\perp$ with probability $(1-1/q)^{n-1}$; conditioned on that, they generate this free module with probability at least c_∞. Compute their R-span, then its annihilator and the corresponding candidate line.

Require the candidate to be split free of rank one with λ surjective on it, and normalize its generator τ' by $\lambda(\tau') = 1$. Generate $\mathcal{H}_{\tau'}$ from $R^\times$ and test its generators against the oracle. All such complements have order $|R^\times|$, so containment certifies equality. Since $q \geq 3$, an admissible coefficient c is a unit, and equality of the complements determines the line. This proves the expected repetition bound. A fixed multiple of $(1-1/q)^{-(n-1)}\log(1/\epsilon)$ trials gives the corresponding bounded-error version. □

Remark B.5. The restriction $q \geq 3$ is necessary. Over $\mathbb{Z}/4\mathbb{Z}$ with $\lambda(x, y) = x$, the vectors $(1, 0)$ and $(1, 2)$ give the same complement $\{I, \mathrm{diag}(3, 1)\}$. For $t = 1, q = 2$, every such complement is trivial.

Proposition B.6 (Branch B: $d = 1$)**.** *Suppose $\operatorname{rank} T = 1$ and $q \geq 3$, and draw λ uniformly among unimodular elements of V^*. With probability $> 1 - 1/q$ the draw is transverse, and then $H \cap G_\lambda$ is a complement of N_λ in G_λ ($G_\lambda \cong N_\lambda \rtimes (H \cap G_\lambda)$), so Proposition B.4 returns T at full precision. The expected cost is $\mathrm{poly}(n, \log|R|) \cdot (1-1/q)^{-(n-1)}$; bounded error adds a $\mathrm{poly}(\log(1/\epsilon))$ factor.*

Proof. For a transverse λ, choose $\tau \in T$ with $\lambda(\tau) = 1$. Corollary 3.2 gives $H \cap G_\lambda = \mathcal{H}_\tau$, so the preceding procedure applies. Lemma 3.3 gives the claimed transversality probability. Cap each trial of the complement procedure and check its candidate line against the full oracle using Lemma 5.1. Thus nontransverse draws cannot cause unbounded runs or false acceptance. □

Remark B.7. The repetition overhead $(1-1/q)^{-(n-1)}$ is polynomial in n when $n/q = O(\log n)$; at fixed q it is exponential. Theorem 4.8 replaces this shortcut in the main algorithm.

C Number-field quotient presentations

We justify the preprocessing in Corollary 7.3. The supplied maximal-order basis and multiplication table have total bit length L_K, and $d = [K : \mathbb{Q}]$. Once N is factored, the following steps use randomized classical polynomial time in $L_K, \log N$.

Prime ideals. For each $p \mid N$, work in the finite $\mathbb{F}_p$-algebra $A = \mathcal{O}_K/p\mathcal{O}_K$ from the supplied multiplication table. Compute its nilradical, decompose the reduced algebra into residue fields, and take the inverse images of the component kernels to obtain the primes above p. The standard prime-decomposition algorithms then give $p\mathcal{O}_K = \prod_{\mathfrak{p}\mid p} \mathfrak{p}^{e_\mathfrak{p}}$; see [Coh93, §6.2]. The randomized step is finite-field polynomial factorization, for which Las Vegas expected polynomial time suffices. An order-computation algorithm is unnecessary because the maximal order is already supplied. Factoring the defining polynomial modulo p is a valid shortcut when p does not divide the index of its power order; that condition, rather than absence of ramification, is the relevant one.

Local rings and CRT. Compute the ideal lattices $\mathfrak{p}^{a_\mathfrak{p}}$ with $a_\mathfrak{p} = e_\mathfrak{p} v_p(N)$. Hermite and Smith normal forms [Coh93, §2.4] give quotient coordinates, additive cyclic decompositions, and effective CRT maps. Multiplication is inherited from the table of $\mathcal{O}_K$. The identity $N\mathcal{O}_K \subseteq \mathfrak{p}^{a_\mathfrak{p}}$ bounds the quotient lattice indices by N^d; the ideal and normal-form computations have polynomial bit complexity. An element of $\mathfrak{p} \setminus \mathfrak{p}^2$, found by lattice arithmetic, maps to a uniformizer when $a_\mathfrak{p} \geq 2$. If $a_\mathfrak{p} = 1$, the quotient is a field and we take uniformizer zero. Residue reduction and a section are computed in these coordinates. Valuation and exact division by powers of the uniformizer are ideal membership and linear-equation computations.

Units and error bounds. Use the principal-unit generators of Appendix A.2, together with random lifts generating the residue units with the desired high probability. No factorization of $q - 1$ is needed. Cap each Las Vegas preprocessing run at a constant multiple of a known polynomial expectation bound and repeat a logarithmic number of times, returning failure if all runs time out. Completed runs have correct output; irreducibility and field decompositions can be checked by finite-field arithmetic. Split the preprocessing error budget among these timeouts and the random unit generating sets. This produces the promised effective presentations with bounded polynomial time and arbitrarily small error.

For $R = \mathcal{O}_K/\mathfrak{p}^a$, distinguish the ramification index $e_{\mathrm{ram}} = v_\mathfrak{p}(p)$, the length $t = a$, and the characteristic exponent

$$e_{\mathrm{char}} = \lceil a/e_{\mathrm{ram}} \rceil.$$

Here $a = e_{\mathrm{ram}} v_p(N)$, so $e_{\mathrm{char}} = v_p(N)$. The length and characteristic exponent agree when $e_{\mathrm{ram}} = 1$; the ramification index is a separate parameter. Finally,

$$\sum_{\mathfrak{p}\mid N} a_\mathfrak{p} \log |\mathcal{O}_K/\mathfrak{p}| = \sum_{p\mid N} v_p(N) \log p \sum_{\mathfrak{p}\mid p} e_\mathfrak{p} f_\mathfrak{p} = d \log N.$$

There are at most $d \log_2 N$ factors. Together with the error allocation in Corollary 7.3, this proves the stated overall complexity. The dependence is on the actual input length L_K, not on degree alone.