Hidden Subgroup Minicourse - Noncommutative Fourier

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006

Contents

Projection to coset states

Lemma

$K, H \leq G$, T left transversal of K, $u \in G$. Then

$$\sum_{t \in T} |\langle tK | uH \rangle|^2 = \frac{|K \cap H|}{|K|} \begin{cases} = 1 & \text{if } K \leq H \\ \leq \frac{1}{2} & \text{otherwise.} \end{cases}$$

Proof.

$\sum_{t \in T} |\langle tK | uH \rangle|^2 = \sum_{t \in T : tK \cap uH \neq \emptyset} \frac{|tK \cap uH|^2}{|K||H|} = \ldots$
Claim: $tK \cap uH \neq \emptyset$ for $|H : K \cap H|$ elements $t \in T$ and in that case $|(tK \cap uH)| = |K \cap H|$. From claim:
$\ldots = \frac{|K:K \cap H||K \cap H|^2}{|K||H|} = \frac{|K \cap H|}{|K|}$ □

Proof of claim

- If $tK \cap uH \neq \emptyset$ choose $z_t \in tK \cap uH$. Then $z_t^{-1} \in Kt^{-1} \cap Hu^{-1}$ and hence $|(tK \cap uH)| = |z_t^{-1}(tK \cap uH)| = |K \cap H|$.
- $y_t = z_t^{-1}u \in H \cap Kt^{-1}u$, whence for different t and t' the elements y_t and $y_{t'}$ are in different right cosets of K and in different cosets of $K \cap H$. Thus $tK \cap uH \neq \emptyset$ for at most $|K : K \cap H|$ t's.
- Equality: $|H| = |uH| = \sum_t |tK \cap uH| \leq |K : K \cap H||K \cap H| = |H|$.

Test for $K \leq H$

- Let $P_K = \sum_{t \in T} |tK\rangle\langle tK|$, the subgroup state of K, considered as a linear transformation of $\mathbb{C}G$.
- $\langle tK||g\rangle = \begin{cases} \frac{1}{\sqrt{|K|}} & \text{if } g \in tK \ (\Leftrightarrow tK = gK) \\ 0 & \text{otherwise} \end{cases}$
- $P_K|g\rangle = \sum_{t \in T} |tK\rangle\langle tK||g\rangle = \frac{1}{\sqrt{|K|}}|gK\rangle = \frac{1}{|K|}\sum_{x \in K} gx.$
- $P_K^2 = P_K$ so P_K is a projection.
- $U_K = \begin{pmatrix} I - P_K & P_K \\ P_K & I - P_K \end{pmatrix}$ is a unitary operation on $\mathbb{C}G \otimes \mathbb{C}^2$.
- $U_K|y\rangle|0\rangle = (I - P_K)|y\rangle|0\rangle + P_K|y\rangle|1\rangle.$

Test for $K \leq H$ 2.

- $P_K = \sum_{t \in T} |tK\rangle\langle tK|$.
- $U_K|y\rangle|0\rangle = (I - P_K)|y\rangle|0\rangle + P_K|y\rangle|1\rangle$.
- $P_K|uH\rangle = \sum_{t \in T}(\langle tK||uH\rangle)|tK\rangle$,
- $\{|tK\rangle | t \in T\}$ is orthonormal
- $|P_K|uH\rangle|^2 = \sum_{t \in T} |\langle tK||uH\rangle|^2 \begin{cases} = 1 & \text{if } K \leq H \\ \leq \frac{1}{2} & \text{otherwise} \end{cases}$.
- After application of U_K to $|uH\rangle$, we always measure 1 in the ancialla if $K \leq H$
- Otherwise measure 1 with prob. $\leq \frac{1}{2}$.

The HSP algorithm.

- Starting state: $|u_1H\rangle|0\rangle|u_2H\rangle|0\rangle\dots|u_\ell H\rangle|0\rangle$
- List the cyclic subgoups of G. Unmark all. $K =$ first in the list.

(*) Apply $U_K^{\otimes \ell}$

- If we see $|*\rangle|1\rangle\dots|*\rangle|1\rangle$ then mark K.
- reverse U^K
- take next K, go to (*).
- For constant error probability, $\ell = O(\log|G|)$

Contents

Recall: Inverse Fourier Transform

- **Inverse Fourier transform** linear extension of

$$E_{ij}^{\rho} \mapsto \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \sum_{g \in G} \overline{\rho(g)_{ij}} g$$

- Properties:
  - Unitary bijective linear map between

$$\mathbb{C}G \text{ and } R = \bigoplus_{\rho \in \hat{G}} M_{d_\rho}(\mathbb{C})$$

  - (with "natural" scalar products.)
- **Fourier transform:** linear extension of

$$g \mapsto \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \sum_{i,j=1}^{d_\rho} \rho(g)_{ij} E_{ij}^{\rho}$$

Noncommutative Fourier transform

Linear extension of $|x\rangle \mapsto \sum_{\rho\in\hat{G}} \sqrt{\frac{d_\rho}{|G|}} \sum_{i,j\leq d_\rho} \rho(x)_{ij}|\rho,i,j\rangle$.

$$\sum_{x\in G} \alpha(x)|x\rangle \mapsto \sum_{\rho\in\hat{G}} \sum_{i,j\leq d_\rho} \hat{\alpha}(\rho,i,j)|\rho,i,j\rangle,$$

$$\hat{\alpha}(\rho,i,j) = \sqrt{\frac{d_\rho}{|G|}} \sum_{x\in G} \alpha(x)\rho(x)_{ij}.$$

$$\hat{\alpha}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{x\in G} \alpha(x)\rho(x) \quad (d_\rho \times d_\rho \text{ matrix}).$$

Noncommutative Fourier transform of coset states

$$|yH\rangle = \frac{1}{\sqrt{|H|}} \sum_{x \in H} |yx\rangle \mapsto \sum_{\rho \in \hat{G}} \sqrt{\frac{d_\rho}{|G|}} |\rho(yH)\rangle,$$

where

$$|\rho(yH)\rangle = \sum_{i,j \le d_\rho} \rho(yH)_{ij} |\rho, i, j\rangle = \frac{1}{\sqrt{|H|}} \sum_{x \in H} \sum_{i,j \le d_\rho} \rho(yx)_{ij} |\rho, i, j\rangle.$$

$$Prob(\rho) = \frac{d_\rho}{|G|} |\rho(yH)|^2,$$

where $|\rho(yH)|$ is the Frobenius norm of $\rho(yH)$: $\sqrt{\sum_{i,j} |\rho(yH)_{ij}|^2}$.

Properties of $\rho(yH)$

- $\rho(yH) = \rho(y) \cdot \rho(H)$
- $|\rho(yH)|^2 = |\rho(H)|^2$

  $\rho(y)$ unitary etc.....
- $\rho(H)$ is $\sqrt{|H|}$ times an orthogonal projection $\pi_H = \frac{1}{\sqrt{|H|}}|H\rangle = \frac{1}{|H|}\sum_{h \in h}|h\rangle$ is an "orthogonal projection" in $\mathbb{C}G$: $\pi_H^2 = \pi_H^\dagger = \pi_H$, and ρ is a $\dagger$-preserving homomorphism from $\mathbb{C}G$ into $M_{d_\rho}(\mathbb{C})$. (On $\mathbb{C}G$, $\dagger$ is the extension of $g \mapsto g^{-1}$.)
- $|\rho(H)|^2 = |H|\mathrm{rk}\rho(H) = \sum_{h \in H} Tr(\rho(h))$.

  $|\rho(H)|^2 = |H|\mathrm{rk}\rho(H) = |H|Tr(|H|^{-1/2}\rho(H)) = \sum_{h \in H} Tr(\rho(h))$

Weak Fourier sampling on coset states

probability of ρ

$$Prob(\rho|yH) = \frac{d_\rho}{|G|} \sum_{h \in H} \chi_\rho(h)$$

If $H \lhd G$

$$\sum_{h \in H} \chi_\rho(h) = \begin{cases} |H| d_\rho & \text{if } H \leq \ker(\rho) \\ 0 & \text{otherwise} \end{cases}$$

- Proof. $\rho_{|H} = \sigma_1 \oplus \cdots \oplus \sigma_r$, σ_i irred.
- $\frac{1}{|H|} \sum_{h \in H} \chi_\rho(h) = \sum_{i=1}^r \sum_{h \in H} \chi_{\sigma_i}(h) = |H| \sum_{i=1}^r (\chi_{\sigma_i}, 1_H)$
- $= |\{i | \sigma_i = 1_H\}|$ (Orthogonality of σ_i and 1_H.)

Proof (cont.)

- $\frac{1}{|H|}\sum_{h\in H}\chi_\rho(h) = |\{i|\sigma_i = 1_H\}|$
- $|\{i|\sigma_i = 1_H\}| = \dim U$

  where U = fixed points of H in M_ρ.
- $H \lhd G \Rightarrow GU = U$

  $(u \in U, g \in G, h \in H,\ hgu = gg^{-1}hgu = g(h^{(g^{-1})}u) = gu.)$
- ρ irred $\rightarrow$ either $U = 0$ or $U = M_\rho$.
- $|\{i|\sigma_i = 1_H\}| = 0$ or d_ρ.

Weak Fourier sampling for normal hidden subgroups 1

If $H \lhd G$

$$Prob(\rho|yH) \begin{cases} \frac{d_\rho^2}{|G/H|} & \text{if } H \leq \ker(\rho) \\ 0 & \text{otherwise} \end{cases}$$

$H \lhd G$, Conclusion 1.

- Only representations which are trivial on H are sampled.
- These are representations of G/H.
- Probabilities proportional to the $\dim^2$.

Weak Fourier sampling for normal hidden subgroups 2

- $H \lhd G$, $H < N \lhd G$,

$$\begin{aligned} Prob(N \leq \ker \rho) &= \frac{1}{|G/H|} \sum_{N \leq \ker \rho} d_\rho^2 = \frac{1}{|G/H|} \sum_{\rho \in \widehat{G/N}} d_\rho^2 = \\ &= \frac{|G/N|}{|G/H|} \leq \frac{1}{2}. \end{aligned}$$

- If $N = \bigcap_{i=1}^{s-1} \ker(\rho_i) > H$ then $N \cap \ker \rho_s < N$ with prob. at least $\frac{1}{2}$.

$H \lhd G$, Conclusion

When sample size $s = O(\log |G|)$:

$\bigcap_{i=1}^{s} \ker(\rho_i) = H$ with high prob.

More generally

probability of ρ

$$Prob(\rho|yH) = \frac{d_\rho}{|G|}\sum_{h\in H}\chi_\rho(h)$$

For general H

(1) If $N \leq H$, $N \lhd G$ $N \not\leq \ker(\rho)$ then $\sum_{h\in H}\chi_\rho(h) = 0$

- Proof. $\rho_{|H} = \sigma_1 \oplus \cdots \oplus \sigma_r$, σ_i irred.
- $\frac{1}{|H|}\sum_{h\in H}\chi_\rho(h) = |\{i|\sigma_i = 1_H\}|$ as above.
- $|\{i|\sigma_i = 1_H\}| = \dim U \leq \dim V \leq d_\rho$

  where U = fixed points of H in M_ρ.

  and V = fixed points of N in M_ρ, $U \leq V$.

Proof (cont.)

- $|\{i|\sigma_i = 1_H\}| = \dim U \leq \dim V \leq d_\rho$
  where $U =$ fixed points of H in M_ρ.
  and $V =$ fixed points of N in M_ρ, $U \leq V$.
- $N \lhd G \Rightarrow GV = V$
  $(u \in V, g \in G, x \in N,\ xgu = gg^{-1}xgu = g(x^g u) = gu.)$
- ρ irred $\rightarrow$ either $V = 0$ or $V = M_\rho$.
- either $|\{i|\sigma_i = 1_H\}| = 0$ or N trivial on M_ρ.

Weak Fourier sampling and the normal core

$H \lhd G,\ N \lhd G,\ N \not\leq H$

$$
\begin{aligned}
Prob(N \leq \ker(\rho)) &= \sum_{N \leq \ker(\rho)} Prob(\rho) = \sum_{N \leq \ker(\rho)} \frac{d_\rho}{|G|} |\rho(H)|^2 \\
&= \sum_{\rho \in \widehat{G/N}} \frac{d_{\hat\rho}}{|G|} \frac{|H|}{|HN/N|} |\hat\rho(HN/N)|^2 \\
&= \frac{|H|}{|HN|} \sum_{\hat\rho \in \widehat{G/N}} \frac{d_{\hat\rho}}{|G/N|} |\hat\rho(HN/N)|^2 \\
&= \frac{|H|}{|HN|} \sum_{\hat\rho \in \widehat{G/N}} Prob(\hat\rho | HN/N) = \frac{|H|}{|HN|} \leq \frac{1}{2}
\end{aligned}
$$

Weak Fourier sampling and the normal core 2

- $H \lhd G$, $N \lhd G$, $N \not\leq H$ then
  $Prob(N \leq \ker(\rho)) \leq \frac{1}{2}$
- If $N = \bigcap_{i=1}^{s-1} \ker(\rho_i) \not\leq H$ then
  $N \cap \ker \rho_s < N$ with prob. at least $\frac{1}{2}$.

Normal core

- $Ncore(H) =$ largest normal subgroup of H.
  When sample size $s = O(\log|G|)$:
  $\bigcap_{i=1}^{s} \ker(\rho_i) = Ncore(H)$ with high prob.
  Exercise: $Ncore(H) = \bigcap_{x \in G} H^x$

The hidden subgroup state density matrix M_H

- $M_H = \frac{1}{|G|}\sum_{g\in G}|gH\rangle\langle gH|$ as a lin.trans of $\mathbb{C}G$?
- Map $P_H : \mathbb{C}G \to \mathbb{C}G$ (right averaging over H) defined as $P_H|y\rangle = \frac{1}{|H|}\sum_{h\in H}|yh\rangle = \frac{1}{\sqrt{|H|}}|yH\rangle$.
- P_H orthogonal projection

  $P_H^2 = P_H$,

  self-adjoint: $\langle x|P_H|y\rangle = \frac{1}{|H|}\sum_{h\in H}\langle x||yh\rangle = \frac{1}{|H|}\sum_{h'\in H}\langle xh'||y\rangle = \langle y|P_H|x\rangle$.
- $M_H = \frac{|H|}{|G|}P_H$.

  $\frac{|G|}{|H|}\langle x|M_H|y\rangle = \frac{1}{|H|}\sum_{g\in G}\langle x||gH\rangle\langle gH||y\rangle = \sum_{g\in G}\langle x|P_H|g\rangle\langle g|P_H|y\rangle = \langle x|P_H^2|y\rangle = \langle x|P_H|y\rangle$,

Fourier transform of M_H

- $\Phi(M_H) = \frac{|H|}{|G|}\phi(P_H)$.
- Fourier transform: $\sim \mathbb{C}G \cong \bigoplus_\rho Mat_{d_\rho}(\mathbb{C})$ (componentwise scaling.)
- The rows of Mat_{d_ρ} are invariant under $\Phi(M_H)$
- On each such row, $\phi(M_H)$ acts as multiplication by $\frac{\sqrt{|H|}}{|G|}\rho(H)$ from the right.
- the Fourier transform of M_H:

$$\frac{\sqrt{|H|}}{|G|}\bigoplus_{\rho\in\hat{G}}\bigoplus_{i=1}^{d_\rho}|\rho,i\rangle\langle\rho,i|\otimes\overline{\rho}(H)$$

- $\overline{\rho}$ contragradient representation: transpose of the inverse.

Fourier transform of M_H -conclusion

- the Fourier transform of M_H:

$$\frac{\sqrt{|H|}}{|G|}\bigoplus_{\rho\in\hat{G}}\bigoplus_{i=1}^{d_\rho}|\rho,i\rangle\langle\rho,i|\otimes\rho(H)$$

- block diagonal structure according to ρ and i.
- Measuring $|\rho\rangle$ and $|i\rangle$ (information theoretically) does not hurt $\sim$ working blockwise.
- For every ρ, the sate $\bigoplus_{i=1}^{d_\rho}|\rho,i\rangle\langle\rho,i|\otimes\rho(H)$ is completely mixed in $|i\rangle$.
- No information in $|i\rangle$, we can drop it (but not ρ!).

More conclusion

More generally

- Decompose $\mathbb{C}G$ into $\bigoplus$ of irreducible left submodules (minimal left ideals).
- Project the state onto these submods
- Measuring the submod index does not hurt.
- Information only in the isomorphism class of the i and the projected image, not in which of the isomorphic instances of isomorphic modules.
- Generalizable to "partial" decompositions

The affine group $A_1(p)$

$A_1(p) = \{\text{affine linear function } M_{a,b} : x \mapsto ax + b \text{ on } \mathbb{Z}_p\}$,
$M_{a_1,b_1} \circ M_{a_2,b_2} = M_{a_1 a_2, b_1 + a_1 b_2}$
In matrix form $\sim$ action on vectors $\begin{pmatrix} x \\ 1 \end{pmatrix}$:
$A_1(p) = \left\{ M_{a,b} | a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p \right\}$, where $M_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$
$A_1(p) = \mathbb{Z}_p \rtimes Z_{p-1}$, where $Z_{p-1} \cong Z_p^*$ acts on the additive group $\mathbb{Z}_p$ by multiplication. (The automorphism group of the additive group $\mathbb{Z}_p$ is this $\mathbb{Z}_{p-1}$.)

Irreps of the affine group $A_1(p)$

- $p-1$ 1-dim reps of $A_1(p)$: Irreps of $A_1(p)/\mathbb{Z}_p \cong \mathbb{Z}_{p-1}$
- Rep given on the two subgroups as:
  $M_{1,b} \mapsto diag(\omega^b, \ldots, \omega^{(p-1)b})$
  $M_{a,0} \mapsto$ perm. matrix of multiplication by a on $\mathbb{Z}_p^*$.
  $$\rho(M_{a,b})_{ij} = \begin{cases} \omega^{bi} & \text{if } j = ai \\ 0 & \text{otherwise} \end{cases} \quad (i,j = 1 \in \mathbb{Z}_p^*)$$
- $\chi_\rho(M_{a,b}) = \begin{cases} \sum_{i=1}^{p-1} \omega^{bi} & \text{if } a = 1 \\ 0 & \text{if } a \neq 1 \end{cases}$
- $= \begin{cases} p-1 & \text{if } a = 1,\ b = 0 \\ -1 & \text{if } a = 1,\ b \neq 0 \\ 0 & \text{if } a \neq 1. \end{cases}$
- $(\chi_\rho, \chi_\rho) = \frac{1}{p(p-1)} \sum_{(a,b)} |\chi(a,b)|^2 = \frac{(p-1)^2+(p-1)}{p(p-1)} = 1$, so ρ irred.
- $(p-1) + d_\rho^2 = (p-1) + (p-1)^2$, so there are no more irreps.

Non-normal subgroups of the affine group $A_1(p)$

- $\langle M_{a,\beta}\rangle$ $a \in \mathbb{Z}_p \setminus \{0,1\}, \beta \in \mathbb{Z}_p$.
- $M(1,b)^{-1}M_{a,1}M_{1,b} = M_{a,(a-1)b}$ for $b \in \mathbb{Z}_p$,
- so the non-normal subgroups are:
  $H_{a,b} = M_{1,b}^{-1}\langle M_{a,0}\rangle M_{1,b} = \{M_{a^\ell,(a^\ell-1)b} \mid \ell \in \mathbb{Z}_{p-1}\}$,
  where $a \in \mathbb{Z}_p^* \setminus \{1\}, b \in \mathbb{Z}_p$

Subgroup states

- $\rho(M_{a,b})_{ij} = \begin{cases} \omega^{bi} & \text{if } j = ai \\ 0 & \text{otherwise} \end{cases} \quad (i, j = 1 \in \mathbb{Z}_p^*)$
- $H_{a,b} = M_{1,b}^{-1}\langle M_{a,0}\rangle M_{1,b} = \{M_{a^\ell,(a^\ell-1)b} \mid \ell \in \mathbb{Z}_{p-1}\}$,
- $\rho(H_{a,b})_{ij} = \begin{cases} \frac{1}{\sqrt{|H_{a,b}|}}\omega^{(a^\ell-1)bi} & \text{if } j = a^\ell i \text{ for some } \ell \\ 0 & \text{otherwise} \end{cases}$

$$\rho(H_{a,b})_{ij} = \begin{cases} \frac{1}{\sqrt{|H_{a,b}|}}\omega^{b(j-i)} & \text{if } j = a^\ell i \text{ for some } \ell \\ 0 & \text{otherwise} \end{cases}$$

Probability of ρ

- $Prob(\rho|yH_{a,b}) = \frac{d_\rho}{|G|}|\rho(yH_{a,b})|^2 = \frac{d_\rho}{|G|}|\rho(H_{a,b})|^2$
  abs. value of an entry of $\rho(H_{a,b})$ is 0 or $\frac{1}{\sqrt{|H_{a,b}|}}$
  in each row, there are $|H_{a,b}|$ nonzero entries.
  $|\rho(H_{a,b})|^2 = (p-1)|H_{a,b}|\frac{1}{|H_{a,b}|} = p-1.$
- $Prob(\rho|yH_{a,b}) = \frac{p-1}{p(p-1)} \cdot (p-1) = 1 - \frac{1}{p}$

Row vectors of subgroup states

- $q = |H_{a,b}| = |H_{a,0}| =$ order of a.
- $\rho(H_{a,b})_{ij} = \frac{1}{\sqrt{q}} \begin{cases} \omega^{b(j-i)} & \text{if } j = a^\ell i \text{ for some } \ell \in \mathbb{Z}_q \\ 0 & \text{otherwise} \end{cases}$
- after "measuring" row index i: state $\sum_{j=1}^{p-1} \rho(H_{a,b})_{ij} |j\rangle$

$$\rho(H_{a,b})_{ij} = \begin{cases} \frac{1}{\sqrt{|H_{a,b}|}} \omega^{b(a^\ell - 1)i} & \text{if } j = a^\ell i \text{ for some } \ell \in \mathbb{Z}_q \\ 0 & \text{otherwise} \end{cases}$$

- state $\sum_{\ell \in \mathbb{Z}_q} \frac{\omega^{b(a^\ell - 1)i}}{\sqrt{q}} |a^\ell i\rangle$

Row vectors of nice coset states

- If $y = M_{1,c}$ then $\rho(y) = diag(\omega^c, \omega^{2c}, \ldots, \omega^{(p-1)c})$,
- so $\rho(yH_{a,b})_{ij} = \rho(y)_{ii}\rho(H_{a,b})_{ij} = \omega^{ci}\rho(H_{a,b})_{ij}$, so
- from $|yH_{a,b}\rangle$ we obtain state
  $|\rho_i(yH_{a,b})\rangle = \omega^{(c-b)i} \cdot \frac{1}{\sqrt{q}} \sum_{\ell \in \mathbb{Z}_q} \omega^{ba^\ell i} |a^\ell i\rangle$
- Nice coset state $yH_{a,b}$ obtained by sampling the value of the hiding function f on the subgroup $\langle \mathbb{Z}_p, H_{a,b}\rangle = \langle \mathbb{Z}_p, H_{a,0}\rangle$.
- State $\frac{1}{\sqrt{q}} \sum_{\ell \in \mathbb{Z}_q} \omega^{ba^\ell i} |a^\ell i\rangle \sim \frac{1}{\sqrt{p}} \sum_{k \in \mathbb{Z}_p} \omega^{bk} |k\rangle$
- "almost" the Fourier transform of $|b\rangle$.

Two states

- $u = \frac{1}{\sqrt{q}} \sum_{\ell \in \mathbb{Z}_q} \omega^{ba^\ell i} |a^\ell i\rangle$
  $v = \frac{1}{\sqrt{p}} \sum_{k \in \mathbb{Z}_p} \omega^{bk} |k\rangle$
- $u \cdot v = q \frac{1}{\sqrt{pq}} = \sqrt{\frac{q}{p}}$, $u = \sqrt{\frac{q}{p}} v + v'$, where $v' \perp v$
- $\Phi^{-1}(u) = \frac{q}{p}|b\rangle + w'$, where $w' \perp |b\rangle$ and Φ is Fourier of $\mathbb{Z}_p$
- Measuring $\Phi^{-1}(u)$ (in the standard basis) gives $|b\rangle$ with probability $\frac{q}{p}$.

The algorithm

1. Guess $H_{a,0}$: guess q. If q is promised to be $p/poly\log(p)$ then $poly \log p$ possibilities.
2. Get nice state form $\rangle H_{a,0}, \mathbb{Z}_p \rangle$.
3. Fourier of $A_1(p)$, measure irrep. type and row index.
4. If irrep is not ρ, go back to 2.
5. Inverse Fourier of $\mathbb{Z}_p$ (or $\mathbb{Z}_{p-1}$) (on column index).
6. Measure and try b: compare $f(M_{1,b})$ and $f(M_{1,0})$.
7. Return $H_{a,b}$ if OK. Retry $O(p/q)$ times, if not.