Hidden Subgroup Minicourse - PGM

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006

Contents

POVM

Positive operator valued measurement

- $F_1, \ldots, F_r$ $n \times n$ matrices. $\sum_{i=1}^{r} F_i^\dagger F_i = I$.
- The measurement: on mixed state M, $Prob(i) = Tr(F_i M F_i^\dagger)$, collapsed state $M' = \frac{1}{Tr(F_i M F_i^\dagger)} F_i M F_i^\dagger$.
- $Prob(i) = Tr(F_i M F_i^\dagger) = Tr(F_i^\dagger F_i M) = Tr(E_i M)$, where $E_i = F_i^\dagger F_i$.
- $E_1, \ldots, E_r$ pos. semidef. self-adjoint, $n \times n$. $\sum_{i=1}^{r} E_i = I$.
- $Prob(i) = Tr(E_i M)$ depend on E_i, not on F_i.
- collapsed state may depend on F_i.

Neumark's theorem 1.

POVM as "standard" measurement on a larger system.

- $F_1, \ldots, F_m$ $n \times n$
- Add an m dimensional ancilla register: work in $C^{mn} = C^n \otimes C^m$. The ancilla will contain the index i of F_i.
- $V = \sum_{i=1}^{m} F_i \otimes e_i$, $mn \times n$ where e_i is the ith standard basis vector of $\mathbb{C}^m$.

$$V = \begin{pmatrix} F_1 \\ \vdots \\ F_m \end{pmatrix}.$$

- $V^\dagger V = \sum_{i=1}^{m} F_i^\dagger F_i = I_{n \times n}$, i.e, the columns of V are pairwise orthogonal unit vectors. (V embeds C^n into C^{mn} orthogonally.)

Neumark's theorem 2.

- Let $\{P_i = I_{n\times n} \otimes e_i^\dagger e_i | i = 1, \ldots m\}$ projective measurement. Standard measurement of the ancilla. Measures the the m-dimensional part of the system.

$$P_i = \begin{pmatrix} \ddots & & \\ & I_{n\times n} & \\ & & \ddots \end{pmatrix}$$

- $VXV^\dagger = \sum_{j=1}^{n} F_j X F_j^\dagger \otimes e_j e_j^\dagger$, so

$$P_i VXV^\dagger P_i = \begin{pmatrix} \ddots & & \\ & F_i X F_i^\dagger & \\ & & \ddots \end{pmatrix}$$

Neumark's theorem 3.

- Probability of i as at the POVM.
  $Tr(P_i V X V^\dagger P_i) = Tr(F_i X F_i^\dagger)$
- Collapsed state as at the POVM.
  $Tr_m(P_i V X V^\dagger P_i) = F_i X F_i^\dagger$
- Implementation: $|x\rangle|0\rangle \rightarrow \sum_{i=1}^m |F_i(x)\rangle|i\rangle$
- Difficulty: in general, does not go through $|x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{m}} \sum_{i=1}^m |x\rangle|i\rangle$

Pretty good measurement (PGM)

- $M_1, \ldots, M_m$ mixed states (density matrices) over $\mathbb{C}^n$.
- Want a POVM $E_1, \ldots, E_m$ that measures i on M_i with sufficiently high probability.
- Pretty good measurement (least square measurement) often optimal, more often works quite well.

$$E_i = M^{-1/2} M_i M^{-1/2}, \text{ where } M = \sum_{i=1}^{m} M_i.$$

- $Prob(\text{identifying } i) = Tr(E_i M_i)$
- Warning: this is a POVM on the subspace generated by the columns of $M_1, \ldots, M_m$.
- In our case M_i will be a rank one matrix: $M_i = |z_i\rangle\langle z_i|$.
- $E_i = |M^{-1/2} z_i\rangle\langle M^{-1/2} z_i|$.

.

PGM - implementation

- In our case M_i will be of rank one: $M_i = |z_i\rangle\langle z_i|$.
- $E_i = |w_i\rangle\langle w_i|$, where $w_i = M^{-1/2} z_i$.
- Can take $F_i = |0\rangle\langle w_i|$ where $|0\rangle \in \mathbb{C}^n$ unit vector.
- $V = \sum_{i=1}^m F_i \otimes |i\rangle = \sum_{i=1}^m |0,i\rangle\langle w_i|$
- $V = (w_1, 0 \ldots, 0, w_2, 0, \ldots, 0, \ldots, w_m, 0, \ldots, 0)^\dagger$, after rearranging columns: $V = (W, 0, \ldots, 0)^\dagger$, where $W = (w_1, \ldots, w_m) = \sum_{i=1}^m |w_i\rangle\langle i|$.
- Implementation of the POVM amounts to implementing $W^\dagger = \sum_{i=1}^m |i\rangle\langle w_i|$.
- More precisely, we need a unitary $nm \times nm$ matrix U s.t. $\langle 0, i|U|w_{i'}, 1\rangle = \delta_{i,i'}$

  (This expresses that W is the appropriate submatrix of U.)

Hidden complements of abelian normal subgroups

- $G = A \rtimes B$, A Abelian, $B \cong \mathbb{Z}_r$. $A \cap H = \{1\}$, $AH = G$.
- $T = A$ a nice transversal: every element of A acts diagonally in the so-called A-adapted bases of the irreps of G.
- Irrep+row measurement of a coset state will give the image of $|H\rangle$ up to a scalar factor:
  $|yH\rangle \to \rho(y)\rho(H)_i = \rho(y)_{ii}\rho(H)_i$.
- After measuring irrep and row, the hidden subgroup state becomes $\rho(H)_i\rho(H)_i^\dagger$ $(= |\rho(H)_i\rangle\langle\rho(H)_i|)$.

Hidden complements of abelian normal subgroups 2

- Diagonalness of A remains true for the "partial" Fourier of G (Fourier of A on the A-part):
- elements of G: $|ab^j\rangle \sim |a\rangle|j\rangle$
- $|a\rangle|j\rangle \mapsto \frac{1}{\sqrt{|A|}} \sum_{\chi \in \hat{A}} \chi(a)|\chi\rangle|j\rangle$
- after measuring χ, the coset states will be the same (up to scalar factors).
- The density matrix of the hidden subgroup state will be of rank one.

Hidden subgroups

Hidden subgroups

$H = H_a = \langle ab \rangle = \{(ab)^t | t \in \mathbb{Z}_r\}$ for some $a \in A$.

Powers of ab

$$(ab)^t = \left(\prod_{i=0}^{t-1} b^i a b^{-i} \right) b^t.$$

Proof.

- $(ab)^t = a_t b^t$ for some $a_t \in A$: $(ab)^t = b^t$ modulo A.
- $a_1 = a$. $(ab)^{t+1} = (ab)^t ab = a_t b^t ab = a_t b^t ab^{-t} b^{t+1}$,
- $a_{t+1} = a_t b^t ab^{-t}$.

Hidden subgroup states

$$|H\rangle = |H_a\rangle = \frac{1}{\sqrt{r}} \sum_{t \in \mathbb{Z}_r} |(ab)^t\rangle$$

$$\sim \frac{1}{\sqrt{r}} \sum_{t \in \mathbb{Z}_r} |B_t(a)\rangle |t\rangle, \text{ where } B_t(a) = \prod_{i=0}^{t-1} b^i a b^{-i}.$$

B_t is an endomorphism of A: $B_t(a_1 a_2) = B_t(a_1) B_t(a_2)$.
B_t^* endomorphism of A s.t. $\chi_{B_t^*(x)}(y) = \chi_x(B_t(y))$.

Examples for B_t

Warning: additive notation in A:

- $G = A \times Z_r$, $u^b = u$.
  - $B_t(u) = \sum_{i=0}^{t-1} u = t \cdot u$. $B_t^* = B_t$.
- $G = \mathbb{Z}_n \rtimes \mathbb{Z}_r$, $\mathbb{Z}_n$, $u^b = \beta \cdot u$,
  - where the multiplicative order of β is r (so $r \mid \phi(n)$).
  - Spec. case: affine group.
  - $B_t(u) = \sum_{i=0} t - 1\beta^i u$ $(= \frac{\beta^t - 1}{\beta - 1} u$ if $\beta - 1 \in Z_n^*)$.
  - dihedral group D_n: $\beta = -1$, $r = 2$:
    - $B_0(u) = u$, $B_1(u) = 0$.
- $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_r$, $u^b = Bu$,
  - where B is an $n \times n$ invertible matrix over $\mathbb{Z}_p$.
  - $B_t = \sum_{i=0}^{t-1} B^i$, $B_t^* = B_t^T$
  - $B_t = (B - 1)^{-1}(B^t - 1)$ if 1 is not an eigenvalue of B.

Partially transformed hidden subgroup states

$$
\begin{aligned}
|H_a\rangle &\mapsto \frac{1}{\sqrt{|A|}}\sum_{u\in A}|u\rangle\frac{1}{\sqrt{r}}\sum_{t\in Z_r}\chi_u(B_t(a))|t\rangle \\
&= \frac{1}{\sqrt{|A|}}\sum_{u\in A}|u\rangle\frac{1}{\sqrt{r}}\sum_{t\in Z_r}\chi_{B_t^*(u)}(a)|t\rangle
\end{aligned}
$$

- Multiple coset state: $|y_1H_a,\ldots,y_kH_a\rangle = |yH_a^k\rangle$, where $y=(y_1,\ldots,y_k)\in A^k$
- A^k good transversal for H^k: $y\in A^k$ diagonal in the partial Fourier of G^k.
- after measuring the character of A^k, state $\sim |H_a^k\rangle$.

Transformed subgroup states 2.

- Single register

$$|H_a\rangle \quad \mapsto \quad \frac{1}{\sqrt{|A|}} \sum_{u\in A} |u\rangle \frac{1}{\sqrt{r}} \sum_{t\in Z_r} \chi_{B_t^*(u)}(a)|t\rangle$$

- Multiregister

$$\begin{aligned} |H_a^k\rangle \quad &\mapsto \quad \frac{1}{\sqrt{|A|^k}} \sum_{u\in A^k} |u\rangle \frac{1}{\sqrt{r^k}} \sum_{t\in \mathbb{Z}_r^k} \prod_{i=1}^{k} \chi_{B_{t_i}^*(u_i)}(a)|t\rangle \\ &= \quad \frac{1}{\sqrt{|A|^k}} \sum_{u\in A^k} |u\rangle \frac{1}{\sqrt{r^k}} \sum_{t\in \mathbb{Z}_r^k} \chi_{B_t^{**}(u)}(a)|t\rangle \end{aligned}$$

$$\text{where } B_t^{**}(u) = \prod_{i=1}^{k} B_{t_i}^*(u_i)$$

Transformed subgroup states 3.

$$
\begin{aligned}
|H_a^k\rangle &\mapsto \frac{1}{\sqrt{|A|^k}} \sum_{u\in A^k} |u\rangle \frac{1}{\sqrt{r^k}} \sum_{t\in\mathbb{Z}_r^k} \chi_{B_t^{**}(u)}(a)|t\rangle \\
&\quad \text{measure } |u\rangle \\
&\to \frac{1}{\sqrt{r^k}} \sum_{t\in Z_r^k} \chi_{B_t^{**}(u)}(a)|t\rangle \\
&= \frac{1}{\sqrt{r^k}} \sum_{v\in A} \chi_v(a) \sum_{\substack{t\,\in\,\mathbb{Z}_r^k \\ B_t^{**}(u)\,=\,v}} |t\rangle
\end{aligned}
$$

Transformed subgroup states 4.

$$
\begin{aligned}
|H_a^k\rangle &\mapsto \frac{1}{\sqrt{r^k}} \sum_{v \in A} \chi_v(a) \sum_{\substack{t \in \mathbb{Z}_r^k \\ B_t^{**}(u) = v}} |t\rangle \\
&= \frac{1}{\sqrt{r^k}} \sum_{v \in A} \chi_v(a) \sqrt{s_{uv}} |S_{uv}\rangle
\end{aligned}
$$

where $|S_{uv}\rangle = \frac{1}{\sqrt{s_{uv}}} \sum_{t \in S_{uv}} |t\rangle$

and $\quad S_{uv} = \{t \in \mathbb{Z}_r^k \mid B_t^{**}(u) = v\}$ and $s_{uv} = |S_{uv}|$.

convention: $|\emptyset\rangle = 0$.

The PGM

- $|z_a^u\rangle = \frac{1}{\sqrt{r^k}} \sum_{v \in A} \chi_v(a) \sqrt{s_{uv}} |S_{uv}\rangle$
- $|z_a^u\rangle = \sum_{v \in A} |z_a^{uv}\rangle$, where $|z_a^{uv}\rangle = \chi_v(a) \frac{\sqrt{s_{uv}}}{\sqrt{r^k}} |S_{uv}\rangle$
- $M_a^u = \frac{1}{r^k} \sum_{v,v' \in A} \chi_v(a) \overline{\chi_{v'}(a)} \sqrt{s_{uv} s_{uv'}} |S_{uv}\rangle\langle S_{uv'}|$.
- $M^u = \sum_{a \in A} M_a^u = \chi_v(a) \overline{\chi_{v'}(a)} \frac{\sqrt{s_{uv} s_{uv'}}}{|G|^k} |S_{uv}\rangle\langle S_{uv'}|$

  orthogonality relations for χ_v and χ_v'
- $M^u = \frac{|A|}{r^k} \sum_{v \in A} s_{uv} |S_{uv}\rangle\langle S_{uv}|$
- $(M^u)^{-1/2} = \sum_{v \in A} \sqrt{\frac{r^k}{|A| s_{uv}}} |S_{uv}\rangle\langle S_{uv}|$
- $|w_a^u\rangle = (M^u)^{-1/2} |z_a^u\rangle = \sum_{v \in A} |w_a^{uv}\rangle$,

  where $|w_a^{uv}\rangle = \chi_v(a) \frac{1}{\sqrt{|A|}} |S_{uv}\rangle$.

The PGM 2.

- PGM: $E_a^u = |w_a^u\rangle\langle w_a^u| = \sum_{v,v'\in A} |w_a^{uv}\rangle\langle w_a^{uv'}| = \frac{1}{|A|}\sum_{v,v'\in A}\chi_v(a)\overline{\chi_{v'}(a)}|S_{uv}\rangle\langle S_{uv'}|$.
- Success probability: $Tr(E_a^u M_a^u) = Tr(|w_a^u\rangle\langle w_a^u||z_a^u\rangle\langle z_a^u|)$
  $= \langle w_a^u||z_a^u\rangle Tr(|w_a^u\rangle\langle w_a^u|)$ use $Tr(|x\rangle\langle y| = \langle x||y\rangle$
  $= (\langle w_a^u||z_a^u\rangle)^2$ use that $|S_{uv}\rangle$ is an orthonormal system
  $= \left(\sum_{v\in A}\frac{1}{\sqrt{|A|}}\frac{\sqrt{s_{uv}}}{\sqrt{r^k}}\right)^2 = \frac{1}{r^k|A|}\left(\sum_{v\in A}\sqrt{s_{uv}}\right)^2.$

Overall PGM success probability

$$\frac{1}{r^k|A|^{k+1}}\sum_{u\in A^k}\left(\sum_{v\in A}\sqrt{s_{uv}}\right)^2$$

PGM implementation

- need to implement $W = \sum_{a \in A} |a\rangle\langle w_a^u|$,
  (actually, $W = \sum_{a \in A} |a, 1_B\rangle\langle 1_A, w_a^u|$)
  (need unitary U, s.t. $\langle a', 1_B|U'|1_A, w_a^u\rangle = \delta_{a,a'}$)
- $Q =$ Fourier in the first register:
- $QW = \frac{1}{\sqrt{|A|}} \sum_{a,a' \in A} \chi_{a'}(a)|a'\rangle\langle w_a^u|$
- $|w_a^u\rangle = \sum_{v \in A} |w_a^{uv}\rangle = \sum_{v \in A} \frac{\chi_v(a)}{\sqrt{|A|}} |S_{uv}\rangle$
- $QW = \frac{1}{|A|} \sum_{a,a',v \in A} |a'\rangle \chi_{a'}(a)\overline{\chi_v(a)}\langle S_{uv}|$
  orthogonality relations $\chi_{a'}$ and χ_v
- $QW = \sum_{v \in A} |v\rangle\langle S_{uv}|$

PGM implementation 2.

- $QW = \sum_{v \in A} |v\rangle\langle S_{uv}|$
- actually $QW = \sum_{v \in A} |v, 1_B\rangle\langle 1_A, S_{uv}|$
- $U' = QU$, s.t. $\langle v', 1_B | U' | 1_A, S_{uv}\rangle = \delta_{v,v'}$, whenever $S_{uv} \neq \emptyset$.
- $U'^{\dagger} : |v, 1_B\rangle \mapsto |1_A, S_{uv}\rangle$ whenever $S_{uv} \neq \emptyset$.
- Equivalently, $|v, 1_B\rangle \mapsto |v, S_{uv}\rangle$ whenever $S_{uv} \neq \emptyset$. (v is clear from u and any element of S_{uv})

PGM efficiently implemented, provided that

From u, v one can compute efficiently $|S_{uv}\rangle$ if $S_{u,v} \neq \emptyset$.

Computing S_{uv}

- additive notation in A
- For some $B \in Aut(A)$, $u^b = B(u)$,
- $\chi_x(B(y)) = \chi_{B^*(x)}(y)$ for $B^* \in Aut(A)$.
- $B_t^* = \sum_{i=0}^{t-1} (B^*)^i$
- $t = (t_1, \ldots, t_k)$.
- $B_t^{**} u = \sum_{\ell=1}^{k} B_{t_\ell}^*(u_\ell)$
- If $A = \mathbb{Z}_p^m$ then B is a linear transformation.
- $B_t^{**} u = v$: system of equations for variables $t_1, \ldots, t_k$.

Example PGM: $\mathbb{Z}_p \rtimes \mathbb{Z}_r$

- $A = \mathbb{Z}_p$, $u^b = \beta u$, $\beta \in Z_p$ of mult. order r. $B_t^*(u) = \frac{\beta^t - 1}{\beta - 1} u$.
- $|H_a\rangle \mapsto \frac{1}{\sqrt{r}} \sum_{v \in \mathbb{Z}_n} \omega^{va} \sqrt{s_{uv}} |S_{uv}\rangle$ $(\omega = \sqrt[n]{1})$
- $S_{uv} = \{t \in \mathbb{Z}_r \mid (\beta^t - 1)u = (\beta - 1)v\}$
  $= \{t \in \mathbb{Z}_r \mid \beta^t = (\beta - 1)vu^{-1} + 1\}$ if $u \neq 0$
- $s_{uv} = |S_{uv}| = 1$ if $(\beta - 1)vu^{-1} + 1$ is a power of β, otherwise 0
- If u, v uniformly random from $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$ then $(\beta - 1)vu^{-1} + 1$ uniformly random from $Z_p \setminus \{1\}$.
- $s_{uv} = 1$ for at least $(p-1)r$ pairs (u, v).
- $Prob(\text{success}) \frac{1}{p^2} |\{(u, v) \mid s_{uv} = 1\}| \geq \frac{(p-1)r}{p^2} \sim \frac{r}{p}$.
- computing S_{uv} form uv: discrete log
  Similar for $\mathbb{Z}_n \rtimes \mathbb{Z}_r$, (if r prime), exercise.

Heisenberg HSP

- p odd prime, $G = \mathbb{Z}_p^2 \rtimes Z_p$, $A = \mathbb{Z}_p^2$, $r = p$, $u^b = Bu$, where

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, B^* = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$B^{*i} = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}, B_t^* = \begin{pmatrix} t & \frac{t(t-1)}{2} \\ 0 & t \end{pmatrix},$$

- $v \begin{pmatrix} \alpha \\ \gamma \end{pmatrix}$, $u_i = \begin{pmatrix} \alpha_i \\ \gamma_i \end{pmatrix}$ $(i = 1, \ldots, k)$.

$$B_t^{**} u = \begin{pmatrix} \sum_{i=1}^k \left(t_i \alpha_i + \frac{t_i(t_i-1)}{2} \gamma_i \right) \\ \sum_{i=1}^k t_i \gamma_i \end{pmatrix}$$

Heisenberg HSP 2.

$$t \in S_{u,v} \Longleftrightarrow \begin{cases} \sum_{i=1}^{k} \left(\alpha_i t_i + \gamma_i \frac{t_i(t_i-1)}{2}\right) = \alpha \\ \text{and} \\ \sum_{i=1}^{k} \gamma_i t_i = \gamma \end{cases}$$

- Take $k = 2$.
- If $\gamma_1 \neq 0$, $\gamma_2 \neq 0$, $\gamma_2 \neq -\gamma_1$, then substituting $t_2 = \frac{\gamma - \gamma_1 t_1}{\gamma_2}$ into the first equation $\rightarrow$
- For fixed $\gamma, \alpha_1, \alpha_2, \gamma_1, \gamma_2$, a quadratic equation in t_1 with degree 0 uniformly random coefficient α.
- For approx. the half of the choices of u and v

Heisenberg HSP 3.

- For fixed $\gamma, \alpha_1, \alpha_2, \gamma_1, \gamma_2$, a quadratic equation for t_1 with degree 0 uniformly random coefficient α.
- For any fixed u, $\approx$ for the half of the choices for v there are two solutions: $s_{uv} = 2$

  and $\approx$ the health of the choices for v there are no solutions $s_{uv} = 0$.
- PGM success probability:

$$\frac{1}{p^8} \sum_{u \in A^2} \left(\sum_{v \in A} \right) \approx \frac{1}{p^8} p^4 \left(\frac{p^2}{2} \sqrt{2} \right)^2 = \frac{1}{2}$$

- S_{uv} computed by solving the quadratic equation

Generalizable to HSP in $\mathbb{Z}_p^k \rtimes \mathbb{Z}_p$ (k constant)