Hidden Subgroup Problem

A Brief Introduction

minxuan mei

2025-11-13

Zhejiang University

Preliminaries

1.1 Basic Notations

1. 量子数据

量子计算机是使用信息的量子力学表示进行计算的设备. 信息存储在量子比特中，其状态可以表示为复向量空间 l_2 范数归一化向量:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x \, |x\rangle,$$

其中系数 $a_x \in \mathbb{C}$ 满足归一化条件 $\sum_x |a_x|^2 = 1$. 基态 $|x\rangle$ 组成的基称为**计算基**.

给定群 G，$|g\rangle$ 为对应于群元素 $g \in G$ 的基态，而

$$|\varphi\rangle = \sum_{g\in G} b_g \, |g\rangle$$

则表示群 G 上的量子态.

均匀叠加态定义为

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle.$$

2. 量子电路

对量子态的操作需要将归一化的态映射到归一化的态上，因此量子操作需要是酉算子，即满足 $U^\dagger U = UU^\dagger = I$ 的线性算子.

3. 测量

量子测量由一组测量算子 $\{M_m\}$ 描述，其作用在被测量系统的状态空间上. 下标 m 对应测量可能的结果. 若测量前系统处于状态 $|\psi\rangle$，那么结果 m 出现的概率为

$$p(m) = \langle\psi|\ M_m^\dagger M_m\ |\psi\rangle.$$

测量后，系统的状态变为

$$\frac{M_m\ |\psi\rangle}{\sqrt{p(m)}}.$$

测量算子满足完备性条件，即

$$\sum_m M_m^\dagger M_m = I.$$

假定对一个处于 $|\psi\rangle$ 的系统进行一次由算子 M_m 描述的测量. 那么结果 m 出现的概率为 $p(m) = \langle\psi|\ M_m^\dagger M_m\ |\psi\rangle$. 定义

$$E_m = M_m^\dagger M_m,$$

可知 E_m 是一个正算子，且满足完备性条件 $\sum_m E_m = I$. E_m 便被称为 POVM 元素，整个 POVM 便被描述为 $\{E_m\}$.

4. 纯态和混合态

纯态是可以用单个态矢量表示的量子态，而混合态则是多个纯态的概率分布. 混合态通常用密度算子 ρ 表示，定义为

$$\rho = \sum_i p_i \ |\psi_i\rangle\langle\psi_i|,$$

其中 p_i 是纯态 $|\psi_i\rangle$ 出现的概率，满足 $\sum_i p_i = 1$.

Theorem 1.1.1: 算子 ρ 为一个和某系综 $\{p_i, |\psi_i\rangle\}$ 对应的密度算子的充分必要条件是:

1. $\mathrm{tr}(\rho) = 1$
2. ρ 是正定的.

1.2 Abstract Algebra

群 G 是一个集合，配备有一个二元运算 $\cdot : G \times G \to G$，满足以下性质：

结合性：对于任意 $g, h, k \in G$，都有 $(g \cdot h) \cdot k = g \cdot (h \cdot k)$；

单位元：存在一个元素 $e \in G$，使得对于任意 $g \in G$，都有 $e \cdot g = g \cdot e = g$；

逆元：对于任意 $g \in G$，存在一个元素 $h \in G$，使得 $g \cdot h = h \cdot g = e$，$h$ 称为 g 的逆元，记作 g^{-1}.

子群的定义类似子空间的定义，主要验证运算满足和封闭性.

设 H 是 G 的一个子群，$a, b \in G$. 若 $ab^{-1} \in H$，则称 a 在模 H 意义下右同余于 b；左同余则是 $a^{-1}b \in H$. 元素 a 模 H 的右同余等价类为集合 $Ha = \{ha : h \in H\}$，称为关于 H 的右陪集；左陪集为 $aH = \{ah : h \in H\}$.

Lagrange 定理指出，有限群 G 的任一子群 H 的阶数 $|H|$ 整除 $|G|$，且陪集的个数为 $|G|/|H|$.

群同态是指两个群之间的映射 $\varphi : G \to G'$，满足对于任意 $g_1, g_2 \in G$，都有

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \odot \varphi(g_2),$$

其中 $\cdot$ 和 $\odot$ 分别是 G 和 G' 上的群运算.

1.3 Representation and Character

1. 表示

   设 V 是一复线性空间，$\mathrm{GL}(V)$ 是 V 的自同构组成的群. 显然若 V 有一组有 n 个元素的基 (e_i) 时，每个线性映射 $a \in \mathrm{GL}(V)$ 都可以用一个 n 阶的可逆矩阵 $\left(a_{ij}\right)$ 表示.

   设 G 是有限乘法群，G 在 V 上的一个线性表示是指从群 G 到 $\mathrm{GL}(V)$ 的一个群同态 $\rho : G \to \mathrm{GL}(V)$，满足

   $$\rho(st) = \rho(s)\rho(t), s, t \in G.$$

   也经常简记 $\rho(s)$ 为 ρ_s.

2. 特征标

   $\rho : G \to \mathrm{GL}(V)$ 是有限群 G 在 V 上的线性表示. 对任一 $s \in G$，定义

$$\chi_{\rho(s)} = \mathrm{tr}(\rho(s)),$$

这样定义得到的复值函数 $\chi_\rho : G \to \mathbb{C}$ 被称为表示 ρ 的特征标. 其有以下性质

- $\chi\left(s^{-1}\right) = \overline{\chi(s)}, \forall s \in G$
- $\chi\left(tst^{-1}\right) = \chi(s), \forall s, t \in G$

1.4 Quantum Fourier Transform

经典的离散傅里叶变换满足

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}.$$

对应的量子傅里叶变换满足

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} \ |k\rangle.$$

而如果扩展到阿贝尔群，并以酉算子的形式写出，则有以下定义：

$$F_G = \frac{1}{\sqrt{|G|}} \sum_{x \in G} \sum_{y \in \hat{G}} \chi_y(x) \ |y\rangle\langle x|.$$

其中 $\hat{G}$ 是 G 的完备特征标集合，$\chi_y(x)$ 表示 G 的第 y 个特征标在元素 x 处的取值.

The hidden subgroup problem

2.1 The hidden subgroup problem

Example: $G = \langle g \rangle$ 为 g 生成的循环群，而给定 $x \in G$，其相对于 g 的离散对数 $\log_g x$ 定义为满足 $g^\alpha = x$ 的最小非负整数 α. 而离散对数问题就是：给定 g 和 x，求出 $\log_g x$.

如上的离散对数问题实际上是**隐藏子群问题**的一个特例. 在隐藏子群问题中，会给定一个黑盒函数 $f : G \to S$，其中 G 是一个已知群，而 S 是一个有限集合. 函数 f 满足如下性质：

对于一个未知的 $H \leq G$，$f(x) = f(y)$ 当且仅当 $x^{-1}y \in H$，也即存在 $h \in H$ 使得 $y = xh$.

所以函数 f 隐藏了子群 H，目标也就是找出这个子群 H.

此外，f 在陪集 $gH = \{gh : h \in H\}$ 上是常数，而在不同陪集上取不同值.

Theorem 2.1.1: 设群 G 有一个由 N 个子群构成的集合 $\mathcal{H} = \{H_1, H_2, ..., H_N\}$，且 $\cap_{i=1}^{N} = \{e\}$. 那么任何经典确定性算法都需要 $\Omega\left(\sqrt{N}\right)$ 次查询才能解决隐藏子群问题.

Proof: 假设谕示机并没有事先隐藏某个子群，而是采取对抗的行为，行为如下：

在第 l 次查询时，算法查询了 g_l，不失一般性假设其与 $g_1, g_2, ..., g_{l-1}$ 都互异. 如果存在子群 $H \in \mathcal{H}$ 使得对任意 $1 \leq j < k \leq l$ 都有 $g_k \notin g_j H$，也就是说，谕示机仍可以将 g_l 分配到一个尚未查询的陪集上，那么谕示机就简单的返回 l；否则，谕示机认输并输出一个与目前查询结果相容的子群的生成集.

现在考虑一个迫使谕示机认输前进行了 t 次查询的算法，算法只能得到 $1, 2, ..., t$ 作为查询结果. 但不管查询了哪 t 个群元素，最多只能得到 $t(t-1)$ 个非单位元的 $g_k g_j^{-1}$，而总共有 N 个子群，若想要覆盖所有子群，必须有 $t(t-1) \geq N$，所以 $t = \Omega\left(\sqrt{N}\right)$.

如果对抗性谕示机在 t 次查询后仍没有认输，这就表明存在两个或更多的标准谕示机在 t 次查询后无法被区分开来. □

2.2 Shor's algorithm

简单起见假设 $N := |G|$ 是已知的. 离散对数问题可以被视作群 $\mathbb{Z}_N \times \mathbb{Z}_N$ 上的隐藏子群问题. 定义函数 $f : \mathbb{Z}_N \times \mathbb{Z}_N \to G$ 为

$$f(\alpha, \beta) = x^\alpha g^\beta = g^{\alpha \log_g x + \beta}.$$

所以 f 在线

$$L_\lambda := \left\{(\alpha, \beta) \in \mathbb{Z}_N^2 : \alpha \log_g x + \beta = \lambda\right\}$$

上是常数. 所以 f 隐藏了子群

$$H = L_0 = \left\{(0, 0), \left(1, -\log_g x\right), \left(2, -2\log_g x\right), ..., \left(N-1, -(N-1)\log_g x\right)\right\}.$$

陪集形式为 $(\gamma, \delta) + H, \gamma, \delta \in \mathbb{Z}_N$. 但 δ 取遍 $\mathbb{Z}_N$ 时,

$$(0,\delta)+H=\left\{\left(\alpha,\delta-\alpha\log_g x\right):\alpha\in\mathbb{Z}_N\right\}=L_\delta,$$

给出了陪集的完整表示.（因此 $\{0\}\times\mathbb{Z}_N$ 是 H 在 $\mathbb{Z}_N\times\mathbb{Z}_N$ 中的一个**横截**（transversal）.）

首先从 $\mathbb{Z}_N\times\mathbb{Z}_N$ 上的均匀叠加态开始，而后计算隐藏函数：

$$|\mathbb{Z}_N\times\mathbb{Z}_N\rangle:=\frac{1}{N}\sum_{\alpha,\beta\in\mathbb{Z}_N}|\alpha,\beta\rangle\mapsto\frac{1}{N}\sum_{\alpha,\beta\in\mathbb{Z}_N}|\alpha,\beta,f(\alpha,\beta)\rangle.$$

然后丢弃第三个寄存器. 概念上可以想象成实际上测量了第三个寄存器，测量得到 $f(\alpha,\beta)=g^\delta,\delta\in\mathbb{Z}_N$，对应的 (α,β) 落在陪集 L_δ 上，也就得到了陪集态

$$|(0,\delta)+H\rangle=|L_\delta\rangle=\frac{1}{\sqrt{N}}\sum_{\alpha\in\mathbb{Z}_N}|\alpha,\delta-\alpha\log_g x\rangle.$$

但实际上进行的是丢弃，丢弃会使得整个系统处于由陪集态系综描述的混合态中，δ 均匀分布在 $\mathbb{Z}_N$ 上. 进而执行 $\mathbb{Z}_N \times \mathbb{Z}_N$ 上的 QFT：

$$\frac{1}{N^{3/2}} \sum_{\alpha,\mu,\nu\in\mathbb{Z}_N} \omega_N^{\alpha\mu+(\delta-\alpha\log_g x)\nu} \left|\mu,\nu\right\rangle = \frac{1}{N^{3/2}} \sum_{\mu,\nu\in\mathbb{Z}_N} \omega_N^{\delta\nu} \sum_{\alpha\in\mathbb{Z}_N} \omega_N^{\alpha(\mu-\nu\log_g x)} \left|\mu,\nu\right\rangle.$$

利用式子 $\sum_{\alpha\in\mathbb{Z}_N} \omega_N^{\alpha\beta} = N\delta_{\beta,0}$，上式化简为

$$\frac{1}{\sqrt{N}} \sum_{\nu\in\mathbb{Z}_N} \omega_N^{\delta\nu} \left|\nu\log_g x,\nu\right\rangle.$$

此时测量便会得到某个对 $\left(\nu\log_g x,\nu\right)$，如果 ν 在模 N 下有乘法逆元，那么直接相除即可；否则重复上述步骤直到得到的 ν 有逆元为止. 每次尝试成功的概率为 $\varphi(N)/N = \Omega(1/\log\log N)$，所以不需要太多次尝试.

The abelian HSP

3.1 The abelian HSP

阿贝尔群通常使用加法记号，所以隐藏条件写作 $f(x) = f(y) \Leftrightarrow x - y \in H$.

解决策略和离散对数算法很相近，首先从群上的均匀叠加态开始，然后计算函数：

$$|G\rangle := \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x, f(x)\rangle.$$

丢弃第二个寄存器以获得 H 在 G 上的某个随机选择的陪集 $x + H := \{x + h \mid h \in H\}$ 的均匀叠加态：

$$|x + H\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle,$$

该状态被称为**陪集态**（coset state）. 因为陪集是未知且均匀随机的，所以丢弃后的状态可以用密度算子表示为

$$\rho_H := \frac{1}{|G|}\sum_{x\in G}|x+H\rangle\langle x+H|.$$

对陪集态施加 QFT，有

$$|\widehat{x+H}\rangle := F_G\ |x+H\rangle = \frac{1}{\sqrt{|H|\cdot|G|}}\sum_{y\in\hat{G}}\sum_{h\in H}\chi_y(x+h)\ |y\rangle = \sqrt{\frac{|H|}{|G|}}\sum_{y\in\hat{G}}\chi_y(x)\chi_y(H)\ |y\rangle,$$

其中

$$\chi_y(H) := \frac{1}{|H|}\sum_{h\in H}\chi_y(h).$$

接下来证明 ρ_H 是 G-不变的，它与 G 的正则表示对易，即对于满足 $U(x)|y\rangle = |x+y\rangle$ 的酉矩阵 $U(x)$，有

$$\begin{aligned} U(x)\rho_H &= \frac{1}{|G|}\sum_{y\in G}|x+y+H\rangle\langle y+H| \\ &= \frac{1}{|G|}\sum_{z\in G}|z+H\rangle\langle z-x+H| \\ &= \rho_H U(-x)^\dagger \\ &= \rho_H U(x). \end{aligned}$$

所以 $\hat{\rho}_H := F_G \rho_H F_G^\dagger$ 是对角化的，因而可以无损测量.

再考虑将 χ_y 限制到子群 H 上. 显然若 $\chi_y(h) = 1, \forall h \in H$，则 $\chi_y(h) = 1$. 否则，χ_y 在 H 上是非平凡的，即存在 $h' \in H$ 使得 $\chi_{y(h')} \neq 1$. 而 $h' + H = H$，所以

$$\begin{aligned}\chi_y(h) &= \frac{1}{|H|} \sum_{h \in h'+H} \chi_y(h) \\ &= \frac{1}{|H|} \sum_{h \in H} \chi_y(h' + h) \\ &= \chi_y(h')\chi_y(h),\end{aligned}$$

也就是说 $\chi_y(h) = 0$. 这也能从 H 的特征标正交性关系

$$\frac{1}{|H|}\sum_{x\in H}\chi_y(x)\chi_{y'}(x)^* = \delta_{y,y'}$$

得到，选取 y' 为平凡特征标即可. 所以有

$$|\widehat{x+H}\rangle = \sqrt{\frac{|H|}{|G|}}\sum_{y:\chi_y(h)=1}\chi_{y(x)}\ |y\rangle,$$

以及混合态:

$$\hat{\rho}_H = \frac{|H|}{|G|^2}\sum_{x\in G}\sum_{y,y':\chi_y(h)=\chi_{y'}(H)=1}\chi_y(x)\chi_{y'}(x)^*\ |y\rangle\langle y'| = \frac{|H|}{|G|}\sum_{y:\chi_y(h)=1}|y\rangle\langle y|.$$

在计算基下测量便会得到某个在隐藏子群 H 上平凡的特征标 χ_y，此时便可以将范围缩小，考虑满足 $\chi_y(g)=1$ 的 $g\in G$，记为 χ_y 的核 $\ker\chi_y=\{g\in G:\chi_y(g)=1\}$，显然其是 G 的子群，且包含 H. 重复上述过程，并计算核的交集. 可以证明在多项式步后便会以高概率得到 H.

假设在计算过程中，核的交集为 $K\le G$ 且 $K\neq H$. 因为 $H<K$，根据 Lagrange 定理，必然有 $|K|\ge 2|H|$. 因为 G 的特征 χ_y 满足 $\chi_y(h)=1$ 的概率为 $|H|/|G|$，而满足 $K\le\ker\chi_y$ 的概率为

$$\frac{|H|}{|G|}\cdot\left|\left\{y\in\hat{G}:K\le\ker\chi_y\right\}\right|.$$

而满足这样条件的 y 的个数为 $|G|/|K|$，因为假如 K 是被隐藏的子群，那么得到这些 y 的概率为 $|K|/|G|$. 因而得到一个满足 $K\le\ker\chi_y$ 的 y 的概率实际上为 $|H|/|K|\le 1/2$. 若

测量得到 $K \not\leq \ker \chi_y$，那么有 $\left|K \cap \ker \chi_y\right| \leq |K|/2$. 也就是说每次测量都有至少 $1/2$ 的概率将 K 的大小缩小至少一半，重复 $O(\log|G|)$ 次便能以高概率得到 H.

Quantum query complexity of the HSP

4.1 The nonabelian HSP and its applications

图自同构问题：

对于给定的 n 个顶点的图 Γ，确定是否存在非平凡的自同构映射 π，即是否存在非平凡置换 $\pi \in S_n$ 使得 $\pi(\Gamma) = \Gamma$. Γ 的全体自同构构成一个群 $\mathrm{Aut}\ \Gamma \leq S_n$，如果 $\mathrm{Aut}\ \Gamma$ 是平凡的，那么称 Γ 是**刚性**（rigid）的. 通过函数 $f(\pi) = \pi(\Gamma)$ 来归约为 S_n 上的 HSP，f 隐藏的就是 $\mathrm{Aut}\ \Gamma$.

图同构问题：

Definition 4.1.1：设 A 为一群，H 是左作用在集合 X 上的群. 群 A 的直积 A^X 中的元素为序列 $\bar{a} = (a_x)_{x\in X}$，由 X 索引，运算为逐点乘法. H 在 X 上的作用可以通过重新索引扩展到 A^X 上，即定义

$$h \cdot (a_x)_{x\in X} = (a_{h^{-1}x})_{x\in X}.$$

所以 A 被 H 在 X 上的**无限制圈积**（unrestricted wreath product）$A \wr_X H$ 定义为半直积 $A^X \rtimes H$，A^X 被称为该圈积的**底群**（base group）.

限制圈积（restricted wreath product）$A\mathrm{wr}_X H$ 定义与无限制圈积类似，但底群使用的是直和. 当 X 是有限集时，两者相同.

最常见的情况下，$X = H$，H 通过左平移作用在自身上，称为**正规圈积**（restricted wreath product）.

给出两个 n 个顶点的图 Γ, Γ', 判断是否存在置换 $\pi \in S_n$ 使得 $\pi(\Gamma) = \Gamma'$, 如果存在则称 Γ 和 Γ' 同构. 该问题可以归约为 $S_n \wr S_2 \leq S_{2n}$ 上的 HSP. 将 $S_n \wr S_2$ 上的元素记作 (π, τ, b), 其中 $\pi, \tau \in S_n$, $b \in \{0, 1\}$ 决定是否交换两个图. 定义函数

$$f(\pi, \tau, b) = \begin{cases} (\pi(\Gamma), \tau(\Gamma')) & b = 0 \\ (\pi(\Gamma'), \tau(\Gamma)) & b = 1 \end{cases}$$

这个函数隐藏的是 Γ 和 Γ' 不交并的自同构群, 如果 Γ 和 Γ' 同构, 那么隐藏子群中会有一个非平凡元素对应于交换两个图的置换. 最难的情况是 Γ 和 Γ' 都是刚性的, 如果它们不同构, 那么隐藏子群就是平凡的; 否则隐藏子群会包含一个满足 $\pi(\Gamma) = \Gamma'$ 的元素 $(\pi, \pi^{-1}, 1)$.

4.1 The nonabelian HSP and its applications

格问题：

n 维格 Λ 是 $\mathbb{R}^n$ 中由 n 个线性无关向量的所有整数线性组合构成的离散子群. 在**最短向量问题**（shortest vector problem, SVP）中，需要找到 Λ 中的非零最短向量.

$g(n)$-唯一最短向量问题（$g(n)$-unique shortest vector problem）要求格 Λ 存在唯一的最短非零向量 v，并且比任何其他非平行向量都要短 $g(n)$ 倍. 如果 $g(n)$ 足够大，那么该问题可以用经典算法在多项式时间内解决；而如果 $g(n) = O(1)$，那么就是 NP-难的. 而中间情况知之甚少，即使 $g(n) = \mathrm{poly}(n)$，也被怀疑是经典计算机难以解决的. 但基于标准方法的用于解决二面体隐藏子群问题的高效量子算法可以解决这一问题.

4.2 The standard method

首先制备群元素的均匀叠加态：

$$|G\rangle := \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle,$$

然后在辅助寄存器中计算 f，得到状态：

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle.$$

最后丢弃辅助寄存器，如果结果是 $s \in S$，那么主寄存器的状态将投影到所有满足 $f(g) = s$ 的 $g \in G$ 的均匀叠加态上，而依据 f 的定义，这些 g 构成某个左陪集 gH，因此主寄存器的状态变为陪集态：

$$|gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h\in H} |gh\rangle.$$

所以最终结果应该为混合态

$$\rho_H := \frac{1}{|G|} \sum_{g\in G} |gH\rangle\langle gH|,$$

称为隐藏子群状态. 在标准方法中，会去使用隐藏子群的样本来确定 H. 换言之，在给定 $\rho_H^{\otimes k}$，其中 $k = \mathrm{poly}(\log|G|)$ 的情况下，寻找 H 的一个生成元集合.

4.3 Query complexity of the HSP

理解 HSP 量子计算复杂度的第一步是考虑对 f 的查询复杂度，如果证明需要指数次查询才能确定 H，那么便不存在高效的量子算法来解决该问题.

前人证明只需要 $\mathrm{poly}(\log|G|)$ 次查询便能确定 H，也在标准方法的框架下证明了 $\rho_H^{\otimes\,\mathrm{poly}(\log|G|)}$ 包含足够的信息来恢复 H.

为了证明隐藏子群问题的查询复杂度是多项式的，只需证明单副本的隐藏子群态是两两统计可区分的，度量标准为量子保真度：

$$F(\rho_H,\rho_{H'})=\mathrm{tr}\left|\sqrt{\rho}\sqrt{\rho'}\right|.$$

其中 $|A|:=\sqrt{A^\dagger A}$.

Theorem 4.3.1: 设 ρ 是从系综 $\{\rho_1, ..., \rho_N\}$ 中抽取的，每个 ρ_i 的概率为固定的 p_i. 那么存在一个量子测量，能够以至少

$$1 - N\sqrt{\max_{i \neq j} F(\rho_i, \rho_j)}$$

的概率正确识别 ρ. 而实际上, 依据极小极大定理, 即使不假设系综的先验概率分布, 这一结论依然成立.

给定隐藏子群态的一个副本, 上式只能给出一个平凡界; 但通过获取多个隐藏子群态的副本，便可以确保整体态之间是近似正交的，因而可区分. 特别地，如果使用 ρ 的 k 个副本，便存在一种测量能够以至少

$$1 - N\sqrt{\max_{i\neq j} F\left(\rho_i^{\otimes k}, \rho_j^{\otimes k}\right)} = 1 - N\sqrt{\max_{i\neq j} F\left(\rho_i, \rho_j\right)^k}$$

的概率正确识别 ρ.（保真度在张量积下是乘性的.）令该表达式为 $1-\varepsilon$，并求解 k，便得到只要使用

$$k \geq \lceil \frac{2(\log N - \log \varepsilon)}{\log\left(1/\max_{i\neq j} F\left(\rho_i, \rho_j\right)\right)} \rceil$$

个 ρ 的副本，就能实现任意小的错误概率 ε.

假设子群 G 的数量不太多，并且不同隐藏子群态之间的保真度不是太接近 1，这便表明使用多项式数量的 ρ_H 副本就足以解决 HSP. G 的子群总数为 $2^{O(\log^2|G|)}$，原因如下：任何群 K 都可以用至多 $\log_2|K|$ 个生成元指定，而因为任何冗余的生成元都会使得群大小至

少增加一倍，所以 G 的每个子群都可以由最多 $\log_2|G|$ 个 G 中的元素构成的子集指定，所以 G 的子群总数的上界为 $|G|^{\log_2|G|} = 2^{O(\log^2|G|)}$. 进而取 $\log N = \mathrm{poly}(\log|G|)$ 即可，那么只要最大保真度和 1 的差距至少为 $1/\mathrm{poly}(\log|G|)$，利用 $k = \mathrm{poly}(\log|G|)$ 个隐藏子群态的副本便能以常数概率识别 H.

为了给出两个态 ρ 和 ρ' 之间保真度的上界，考虑投影到 ρ 的支撑集或其正交补集上的二结果测量. 回忆量子保真度和经典保真度之间的关系：

$$F(\rho,\sigma) = \min_{\{E_m\}} F(\{p_m\},\{q_m\}),$$

其中最小化遍历所有 POVM 测量 $\{E_m\}$，$p_m = \mathrm{tr}\ E_m\rho$，$q_m = \mathrm{tr}\ E_m\sigma$. 因此：

$$F(\rho,\rho') \le \sqrt{\operatorname{tr}\ \Pi_\rho \rho\ \operatorname{tr}\ \Pi_\rho \rho'} + \sqrt{\operatorname{tr}\ \left(1-\Pi_\rho\right)\rho\ \operatorname{tr}\ \left(\left(1-\Pi_\rho\right)\rho'\right)}$$
$$= \sqrt{\operatorname{tr}\ \Pi_\rho \rho'}.$$

现在考虑两个不同子群 $H, H' \le G$ 对应的态 ρ_H 和 $\rho_{H'}$ 之间的保真度. 不失一般性，假设 $|H| \ge |H'|$. 定义 T_H 为 H 在 G 中的左陪集的一个代表元的集合，那么可以将 ρ_H 重写为

$$\rho_H = \frac{1}{|G|}\sum_{g\in G}|gH\rangle\langle gH| = \frac{|H|}{|G|}\sum_{g\in T_H}|gH\rangle\langle gH|.$$

又因为右侧实际上是 ρ_H 的谱分解式，所以

$$\Pi_{\rho_H} = \sum_{g\in T_H}|gH\rangle\langle gH| = \frac{1}{|H|}\sum_{g\in G}|gH\rangle\langle gH|.$$

进而有

$$
\begin{aligned}
F(\rho_H, \rho_{H'})^2 &\leq \operatorname{tr} \Pi_{\rho_H} \rho_{H'} \\
&= \frac{1}{|H||G|} \sum_{g,g' \in G} |\langle gH | g'H' \rangle|^2 \\
&= \frac{1}{|H||G|} \sum_{g,g' \in G} \frac{|gH \cap g'H'|^2}{|H||H'|} \\
&= \frac{1}{|G| \cdot |H|^2 \cdot |H'|} \sum_{g,g' \in G} |gH \cap g'H'|^2.
\end{aligned}
$$

而

$$
\begin{aligned}
|gH \cap g'H'| &= |\{(h,h') \in H \times H' : gH = g'h'\}| \\
&= \left|\{(h,h') \in H \times H' : hh' = g^{-1}g'\}\right| \\
&= \begin{cases} |H \cap H'| & g^{-1}g' \in HH' \\ 0 & g^{-1}g' \notin HH' \end{cases}.
\end{aligned}
$$

所以

$$
\begin{aligned}
\sum_{g,g' \in G} |gH \cap g'H'|^2 &= |G| \cdot |HH'| \cdot |H \cap H'|^2 \\
&= |G| \cdot |H| \cdot |H'| \cdot |H \cap H'|.
\end{aligned}
$$

最终有

$$
\begin{aligned}
F(\rho_H, \rho_{H'})^2 &\leq \frac{|G| \cdot |H| \cdot |H'| \cdot |H \cap H'|}{|G| \cdot |H|^2 \cdot |H'|} \\
&= \frac{|H \cap H'|}{|H|} \\
&\leq \frac{1}{2},
\end{aligned}
$$

$F(\rho_H, \rho_{H'}) \leq 1/\sqrt{2}$，所以 HSP 的查询复杂度是 $\mathrm{poly}(\log|G|)$.