arXiv:2304.08376v1 [quant-ph] 17 Apr 2023

零和子序列与隐藏子群

Muhammad Imran，布达佩斯科技与经济大学代数系，Egry J´ozsef u. 1，H-1111 布达佩斯，匈牙利。电子邮件：muh.imran716@gmail.com

G´abor Ivanyos，计算机与自动化研究所，E¨otv¨os Lor´and 研究网络，Kende u. 13-17，H-1111 布达佩斯，匈牙利。电子邮件： Gabor.Ivanyos@sztaki.hu

2023年4月18日

摘要

我们提出一种求解幂零群中隐藏子群问题的方法。其主要思想是，沿着中心列的各个成员，迭代地将隐藏子群变换为其在相应商群中的像，最终得到它在原群的交换商群中的像；然后使用阿贝尔隐藏子群算法确定该像。获知这个像后，即可继续向下归约到一个真子群，除非隐藏子群就是整个群。该变换依赖于在有限素域上的向量序列中寻找足够长的零和子序列。对于域大小为常数的情形，我们提出了一种针对后一个问题的新型确定性多项式时间算法。由此可得一种多项式时间精确量子算法，用于求解幂零类为常数、且其阶的素因子均有常数上界的幂零群中的隐藏子群问题。

关键词：隐藏子群问题、幂零群、零和子序列、精确量子算法。

致谢。第二作者的研究得到了匈牙利创新与技术部国家研究、发展与创新办公室在人工智能国家实验室计划框架内的支持。

1 引言

隐藏子群问题（简称 HSP）的标准版本如下：给定群 $G \to \{0,1\}^r$ 上的一个函数 f，满足存在一个子群 H，使得 $f(x) = f(y)$ 当且仅当 x 和 y 属于 H 的同一个左陪集，求子群 H。Kitaev 可能是第一个注意到，Shor 的因式分解和离散对数算法可以推广到有限阿贝尔群（以及某些无限交换群）中的 HSP，并在多项式时间内求解该问题的人。对于非交换群中该问题的复杂度，人们所知甚少。最一般的结果归功于 Ettinger、Hoyer 和 Knill。他们在 [EHK04] 中证明，有限的、未必为阿贝尔群的群中，该问题的查询复杂度是多项式级的。关于时间复杂度，Kuperberg 亚指数时间量子算法 [Kup05] 在二面体群及非常相似的群中求解 HSP，或许是目前已知的最佳结果。Alagic、Moore 和 Russell 在 [AMR07] 中将其显著推广到某个特殊的 HSP，该 HSP 所涉及的群类包括非可解群。有一些群类中的 HSP 可以在多项式时间内求解。关于这类早期结果，参见 Lomont 的综述论文 [Lom04] 以及 Wang 的综述论文 [Wan10] 。Lomonaco 和 Kauffman 的论文 [LK07b] 提出了 Shor-Kiteav 算法的有趣衍生算法和推广。Horan 和 Kahrobaei 的论文 [HK18] 讨论了 HSP 的密码学方面，并且还介绍了较新的研究成果。阿贝尔群上的隐藏移位问题（以及相关半直积群上的 HSP）似乎在后量子密码学中颇受关注，例如参见 Castryck 和 Vander Meeren 的论文 [CM23] ，以及 Alagic 和 Russell 的论文 [AR17] 。在 [BL21], 中，Bae 和 Lee 提出了一种在多项式时间内求解隐藏移位问题连续版本的方法。

若量子过程在最终测量后以概率 1 返回正确输出，则称其为精确量子过程。除了可以将精确量子算法视为确定性经典方法的对应物之外，无测量版本还可以作为更大型酉过程的组成部分。 [EHK04] 的方法存在一个精确版本，因此自然会问：哪些群类中的隐藏子群问题可以由多项式时间精确量子算法求解? Brassard 和 Hoyer [BH97] 提出了一种适用于 $\mathbb{Z}_2^n$ 的多项式时间精确方法。在 [CQ18], 中，Cai 和 Qiu 为 Simon 问题（隐藏子群问题的一个特殊实例，尽管它可能是最难的实例）提出了一种更简单、高效的精确方法。Bonnetain 在 [Bon21] 中，以及 Wu 等人 在 [WQT+22] 中，分别独立提出了针对 $\mathbb{Z}_2^n$ 中隐藏子群问题、具有最优查询复杂度的高效精确算法。Mosca 和 Zalka 在 [MZ03] 中提出了一个高效的精确算法，用于求解已知阶循环群上的离散对数问题。最近， [II22], 提出了适用于一般 m 的 $\mathbb{Z}_{m^k}^n$ 隐藏子群问题精确量子算法；在已知群的阶的素因子的某个倍数这一假设下，该算法解决了阿贝尔群的情形。

本文提出一种方法，用于求解幂零类为 $O(1)$ 的幂零群中的隐藏子群问题。我们的主要结果是：对于阶的素因子也均为 $O(1)$ 的此类群，存在一个多项式时间精确量子算法，可求解其中的隐藏子群问题

。我们假设群G 以具有唯一编码的黑盒群形式给出。该算法的主要策略本质上是将问题归约为 G 的子群之商群中的隐藏子群问题实例。我们选择了一种适用于此类归约的输入模型。

在标准版本中，输入由一个预言机给出，该预言机是一个酉映射，用于计算 $|x\rangle|f(x)\rangle$ ，其来源是 $|x\rangle|0\rangle$。通常的隐子群算法首先使用预言机计算叠加态 $\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|f(x)\rangle$ ，其中大多数算法会忽略保存 f 值的第二个寄存器，后续仅处理陪集叠加态 $|xH\rangle = \frac{1}{\sqrt{|H|}}\sum_{y\in H}|xy\rangle$ ，例如参见 [LK07b]。正如 [Kup05]，中所指出的，这些方法同样适用于这样的情形：假设预言机生成的是陪集叠加态混合态的多个副本。特别是， [II22] 提出的精确阿贝尔隐藏子群算法也适用于这种情形。

具体而言，为了得到一个酉预言机，我们将状态 $\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|f(x)\rangle$ 视为混合态 $\Xi_{G,\ H} = \frac{1}{|G|:\ H|}\sum_{x\in X}|xH\rangle\langle xH|$ 的纯化，其中 X 是 G 中 H 的任意左横截集。状态 $\Xi_{G,\ H}$ 称为（隐藏）子群态。我们假设，隐藏子群 H 由一个酉映射（称为预言机）给出，该映射在零输入时返回子群态 $\Xi_{G,\ H}$ 的任意（但固定的）纯化副本。

引入隐藏子群问题（HSP）的一个子任务将很有用，即计算模去 G的交换子子群后的隐藏子群，也就是子群 HG' ，其中 H 是隐藏子群。我们将这个问题简称为 HSMC。为了说明 HSMC 在幂零群中的威力，请注意，它自然涵盖了 HSP 的交换情形；而且，在计算出子群 HG' 后，如果它是 G 的真子群，那么我们就可以将其作为目标，继续计算 H；而如果 $HG' = G$ ，那么 $H = G$ ，因为在幂零群中，每个极大子群都包含交换子子群。

我们给出一种用于求解幂零群某一类中 HSMC 问题的策略概述。如果某个群 G 满足：对于某个素数 p ， G 是一个p-群，且 G/G' 是初等阿贝尔群，那么我们称该群为半初等群。在半初等群 G中，我们通过反复执行以下程序，来计算模掉交换子后的隐藏子群。假设 L是一个包含于 G中心的初等阿贝尔子群。那么，我们便可利用群 G中对应于 H 的子群态的足够多份拷贝，在商群G/L 中创建一份对应于 HL/L 的子群态。我们将这一程序（以及一些更简单的程序）称为子群态转换。这种转换基于从 L的足够长的元素序列中寻找零和子序列。最终，经过 $c-1$ 轮迭代后，其中 c 是 G的幂零类，我们便能计算出一份在 G中对应于HG'/G' 的子群态。（半初等性质确保存在一个长度为 c 、其因子均为初等阿贝尔群的标准中心列。）最后，利用这类子群态的足够多份拷贝，我们便能通过第 [II22] 节中的精确阿贝尔隐藏子群算法计算出 HG'/G' 。幸运的是，半初等

群经常作为幂零群的子群的因子群出现，因此可以将隐藏子群问题归约到 HSMC 的特殊情形，详见命题 1。我们得到的主要结果如下。

定理 1. 假设 G 是一个类受常数限制的幂零群，且 $|G|$ 的素因子也受常数限制。我们假设G 是一个黑盒群，其元素由 ℓ位字符串唯一编码。那么，存在一种精确量子算法，使用 poly(ℓ) 次操作以及 poly(log$|G|$) 次对G中子群态制备预言机及其逆的调用，即可解决隐藏子群问题。

相关结果。在精确情形下， [II22] 可以高效解决阿贝尔情形，且不受 $|G|$的素因子限制。已有不少相关的非精确多项式时间算法。其中， [FIM$^+$14]的结果或许与定理 1 最为接近；该结果解决了导出列和指数均受常数限制的可解群中的隐藏子群问题。此类群涵盖了本结果适用的群，但不包括指数被小素数的大次幂整除的群。不过，值得注意的是，这些群的情形可以通过结合命题 1 的归约与 [FIM$^+$14]的算法来高效处理。我们指出，使隐藏子群问题等价于在$\mathbb{Z}_{2^k}^n$ 上的隐藏移位问题的半直积群，是一个类为 k的幂零群。Bonnetain 和 Naya-Plasencia [BNP18]提出了一种非精确方法，其主要组成部分可以看作是将 Kuperberg筛法与利用线性代数在 $\mathbb{Z}_2^n$中寻找零和子序列相结合。

对于幂零类至多为二的情形， [ISS12], 的非精确方法能够高效处理，且对$|G|$的素因子大小没有任何限制。值得一提的是，就技术内容而言， [ISS12] 可以视为与本文最为接近的相关工作。将隐藏子群问题归约为 HSMC 的思路源自该文，归约中的许多要素也都出现在那篇论文中。此外， [ISS12], 的关键工具——使用多个陪集叠加态以及中心子群的量子傅里叶变换——也可以视为某种子群态转换形式，尽管这种形式不那么直观。然而，在二阶情形中，有一种更强大的工具可以消去子群的特征：还可以利用群的某些良好自同构进行扭转，而这些自同构不会过多改变隐藏子群。遗憾的是，一般而言，幂零类大于二的幂零群中不存在这样的自同构。

[DHIS14, IS17] 的方法能够高效解决某些高阶幂零群中的隐藏子群问题，这些群的阶同样可能含有较大的素因子。这些群具有一个正规子群，其阿贝尔商群属于受限类型（例如循环群）。这些方法以及 [FIM$^+$14] 的方法都具有很强的非精确性。或许经过一些努力，可以将 [DHIS14] 的技术改造为精确方法。

有限阿贝尔群A的达文波特常数 $S(A)$ 是满足以下条件的最小数：群 A中任意由 s 个元素组成的序列 A 都包含一个非空子序列，其元素之和为零元。这个名称源自 H. Davenport

提出了在 A 为某个数域的理想类群时求出 $S(A)$，并将其作为衡量该数域整数因子分解不唯一性的指标。这个一般问题已成为加法组合学中的著名问题。Olson [Ols69] 求出了 p群的达文波特常数的精确值；特别地，对于 $\mathbb{Z}_p^n$，其值为 $1+n(p-1)$。我们要寻找的是一种“有效”达文波特常数：对于 A中的任意一个由 S' 个元素构成的序列，算法 $\mathcal{B}$ 能在多项式时间内找到一个非空零和子序列所需的最小数 $S' = S^{\mathcal{B}}(A)$ 是多少？这里的多项式时间是相对于 $S'\log|A|$ 而言的（大致上，这是输入序列的比特长度）。本文给出一种运行时间为 poly(n) 的确定性算法 $\mathcal{B}$；对于 $p = O(1)$，给定 $\mathbb{Z}_p^n$中的一个包含 $S^{\mathcal{B}}(\mathbb{Z}_p^n) =$ poly(n) 个向量的序列，该算法返回一个零和子序列。

本文其余部分的结构如下。第 2 节介绍一些背景材料，包括精确量子过程、幂零黑盒群及其相关计算、（隐藏）子群态及其纯化，并介绍将整个群中的子群态转换为子群中的子群态，以及在某些非常简单的情况下转换为商群中的子群态的方法。第 3 节证明命题 1，即存在一种从一般幂零群中的隐藏子群问题归约到半初等群中的 HSMC 问题的精确多项式时间归约。第 4 节介绍如何将半初等群中若干个子群态转换为该群阿贝尔因子中的一个子群态。作为该技术的应用，我们证明命题 2：如果能够在时间 poly($n\log\ p$) 内，从由 $\mathbb{Z}_p^n$ 中的 poly($n\log\ p$) 个向量组成的序列中找到零和子序列，那么对于幂零类为常数的半初等 p-群，我们就能通过多项式时间精确量子算法解决 HSMC 问题。第 5 节证明定理 2，说明当 p 有界于某个常数时，可以高效地解决后一任务。命题 1 和命题 2 连同定理 2 立即推出定理 1。第 6 节是结语。

2 预备知识

2.1 关于精确量子计算

为获得足够一般的中间结果，我们采用 Nishimura 和 Ozawa [NO05]所描述的一致电路族模型。这是因为 [II22] 中的一些精确方法以及我们的主要转换技术，都基于这样的假设：模 $|G|$ 的素因子的量子傅里叶变换及其逆变换可以被精确实现。正如 [NO02], 中所指出的，使用固定的有限门集无法完成这一任务。为清晰起见，我们使用关于量子傅里叶变换可用性的假设，而不是关于其精确实现所需门的假设，来陈述我们的中间结果。（参见 Mosca 和 Zalka [MZ03]提出的模一般整数的傅里叶变换实现方法。）不过请注意，对于我们的定理 1，由于假设这些素数被某个常数所界定，因此只需常数数量的门，因而，

根据 [NO09], , 该定理在 Bernstein 和 Vazirani [BV97]的量子图灵机模型中仍然成立。

2.2 群

关于群论中的标准记号和概念，例如子群、正规子群、陪集、共轭元、交换子、交换子子群、中心等，请读者参阅相关教材，例如 [Rob95]。对于 G 的子集 U 和 V，我们用 UV 表示集合 $\{uv\colon\ u \in U, v \in V\}$。如果 U 和 V 都是子群，且 U 或 V 是 G 的正规子群，那么 UV 是一个子群。对于子群 U,V，我们用 $[U,V]$ 表示由交换子 $[u,v]$ $(u \in U, v \in V)$ 生成的子群。回顾一下，有限群 G 的下中心列是由正规子群 $G_i \lhd G$ 构成的序列 $G = G_0 > G_1 > \ldots > G_c$，其递归定义为 $G_i = [G, G_{i-1}]$。这里我们假设 c 是满足 $G_i = [G, G_i]$ 的最小指标 i。如果 $G_c = \{1\}$，则群 G 是幂零群，而 c 称为 G 的（幂零）类。有限群是幂零群，当且仅当它是其 Sylow 子群的直积。

为了获得足够一般的结果，我们研究元素具有唯一编码的黑盒群。这一概念涵盖了各种“真实”群，例如置换群以及有限域上的矩阵群。黑盒群的元素由长度为 ℓ 的二进制串表示，群运算则由预言机提供；此外，群的生成集作为输入给出。子群也将以生成元集合的形式给出。可以使用 [II22] 的精确多项式时间量子成员测试，将生成集的大小缩减到至多 $\log|G|$。

在本部分其余内容中，我们假设 G 是一个类为 c 的幂零黑盒群，并且已知 $|G|$ 的素因子。

对于 G 的正规子群 N，子群 $[G,N]$ 是包含于 N 的 G 的正规子群。若 Γ 和 Δ 分别是 G 和 N 的生成元集合，则可通过取交换子 $[x,y]$（其中 $x \in \Gamma$、$y \in \Delta$），再与 Γ 中的元素构成迭代交换子，直至这些元素生成的子群稳定，从而得到 $[G,N]$ 的生成集。要检验是否稳定，可以使用 [II22] 的精确量子子群成员判定算法。由此可得到一种多项式时间精确方法，尤其可用于计算下中心列。

下面我们介绍一些用于隐子群算法的其他群论任务的高效解法。G 的 p-Sylow 子群可按如下方法计算。设 Γ 是 G的一个生成集。然后，对每个 $g \in \Gamma$，我们计算 g 的阶 o_g，并将 o_g 分解为乘积 $p^\alpha o_g{}'$，其中 $o_g{}'$ 与 p互素。于是，$g^{o_g{}'}$ $(g \in \Gamma)$生成了 G的（唯一） p-Sylow 子群。我们将通过计算隐子群与 Sylow 子群的交，在 G 中计算隐子群。

Kantor 和 Luks 的确定性多项式方法 [KL90]可用于计算 G 的子群的正规化子。该方法最初是为幂零置换群提出的，但也能在任何仅具有小素因子的阶的幂零黑箱群中求出正规化子。

假设 L 是 G的子群。将 G 的元素x 分解为如下形式的乘积会很有用： $\alpha_L(x)\beta_L(x)$，其中 $\beta_L(x) \in L$ 和 $\alpha_L(x)$仅取决于陪集 xL。（因此， α_L 的取值范围是 G中 L 的陪集代表系。）为此，计算一个主列（由正规子群组成、且因子为素数阶循环群的列） $G = K_0 > K_1 > \ldots > K_r = 1$。获得这种列的最简单方法或许是对下中心列进行细化。取子群 K_iL并删除重复元素后，我们得到一个因子为素数阶循环群的次正规列$G = M_0 > M_1 > \ldots > M_s = L$ 。再取元素 $a_i \in M_{i-1} \setminus M_i$，并将 $M_{i-1}/M_i\,(i = 1, \ldots, s)$ 的阶记为 p_i。那么，元素 $a_1^{\gamma_1} a_2^{\gamma_2} \ldots a_s^{\gamma_s}((\gamma_1, \ldots \gamma_s) \in \prod_{i=1}^{s} \mathbb{Z}_{p_i})$ 构成 G中 L 的左横截集。对于元素 $x \in G$，可以按如下方式计算它在该横截集中的陪集代表。首先，通过计算 x 模M_1的底数 a_1 离散对数，找出使得 $xa_1^{-\gamma_1} \in M_1$ 成立的最小非负整数 γ_1。这可以通过在 $\mathbb{Z}_{p_1}^2$中求解一个隐藏子群问题实例来完成。具体而言，我们定义函数 $(\beta, \gamma) \mapsto |x^\gamma\rangle|a_1^{-\beta} M_1\rangle$。借助精确版 [II22] Watrous 方法 [Wat01]计算均匀叠加态 $|M_1\rangle$，即可求出该函数的值。这些值是 p 两两正交的状态，隐藏子群为 $\{(\delta, \gamma) : x^\delta a_1^{-\gamma} \in M_1\}$。我们使用 [II22] 的精确隐藏子群算法来求出该群的一个生成元。由此即可显然地得到 γ_1 。接下来，我们继续处理 $xa_1^{-\gamma_1}$以计算 γ_2，依此类推。令 $\alpha_L(x) = a_1^{\gamma_1} \ldots a_r^{\gamma_r}$，并令 $\beta_L(x) = \alpha_L(x)^{-1} x$。

如果 L 是 G 的正规子群，我们可以用 $\alpha_L(x)$ 对陪集 xL 进行编码。这样一来，商群 G/L 就成为一个黑盒群：其元素由陪集代表系 $\{\alpha(x)$ 的元素编码；$x \in G\}$ 而乘法预言机则可通过将 G 的乘法预言机与函数 α_L 的计算组合而得到。

2.3 子群态与纯化

设 G 是一个有限群， H 是 G 的一个子群。我们将群代数 $\mathbb{C}G$ 中的元素视为纯量子态。（“自然”的内积 $(\sum_x \alpha_x|x\rangle, \sum_y \alpha_y|y\rangle) = \sum \alpha\overline{\beta}xy^{-1}$ 使得 $\mathbb{C}G$ 成为一个希尔伯特空间，其中群元素构成标准正交基。）

H 在 G 中的（左）陪集叠加态是均匀叠加态 $|aH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ah\rangle$，其中 $a \in G$。 H 在 G 中的（左）子群态是一个混合态，其密度矩阵为

$$\Xi_{G,H} = \frac{1}{|G|} \sum_{a \in G} |aH\rangle\langle aH| = \frac{1}{|G : H|} \sum_{a \in X} |aH\rangle\langle aH|,$$

其中， X 是 G中 H的任意左横截集（左陪集的一组代表元）。

$\Xi_{G,\ H}$ 的一个纯化是指任意纯态 $|\psi\rangle \in \mathbb{C}G \otimes V$，其中存在某个希尔伯特空间 V，使得 $\Xi_{G,\ H}$ 是 $|\psi\rangle\langle\psi|$ 关于第二子系统的相对迹。关于混合态纯化的一般事实，尤其是其与施密特分解之间的联系，请参阅第2.5节

[NC10]的。以下引理给出了子群态纯化的刻画。

引理 1. 纯态 $|\psi\rangle \in \mathbb{C}G \otimes V$ 是子群态 $\Xi_{G,\ H}$ 的纯化，当且仅当它可以写成

$$|\psi\rangle = \frac{1}{\sqrt{|G|}} \sum_{x\in G} |x\rangle|v(x)\rangle,$$

其中，状态 $|v\ (x)\ \rangle$ 与 $|v\ (y)\ \rangle$ 在 x 和 y 属于 H 的同一左陪集时相等，否则正交。

证明。“若”部分可由 $|v()\rangle$ 的条件推出 $|\psi\rangle = \frac{1}{\sqrt{k}} \sum_{a\in X} |aH\rangle|v\ (a)\ \rangle$。

为说明“仅若”部分，回顾一下，状态 $|\psi\rangle \in \mathbb{C}G \otimes V$ 的施密特分解形式为 $|\psi\rangle = \sum_{i=1}^{m} \lambda_i |u_i\rangle|v_i\rangle$，其中 $m = |G|$、$|u_1\rangle$、$\ldots$、$|u_m\rangle$ 是 $\mathbb{C}G$ 的任意标准正交基，在该基下，$|\psi\rangle\langle\psi|$ 关于第二子系统的相对迹是对角的（对角元为 λ_1、$\ldots$、λ_m），而与非零特征值 λ_i 对应的向量系 v_i 是 V 中的标准正交系。向量 v_i 取决于基 $|u_i\rangle$（$i = 1$、$\ldots$、m）的选择。注意，$\Xi_{G,\ H}$ 的唯一非零特征值为 $\frac{1}{k}$，其重数为 k，其中 $k = |G\colon\ H|$。陪集叠加态构成相应特征子空间的一组标准正交基。因此，若 $|\psi\rangle$ 是 $\Xi_{G,\ H}$ 的纯化，那么作为 $\Xi_{G,\ H}$ 的纯化的 $|\psi\rangle$ 的施密特分解形式为 $|\psi\rangle = \frac{1}{\sqrt{k}} \sum_{i=1}^{k} |u_i\rangle|v_i\rangle$，其中 $|u_1\rangle$、$\ldots$、$|u_k\rangle$ 是 $\Xi_{G,\ H}$ 的 $\frac{1}{k}$ 特征子空间的任意标准正交基，而 $|v_1\rangle$、$\ldots$、$|v_k\rangle$ 是 V 的标准正交系。特别地，若 $X = \{a_1, \ldots, a_k\}$，则取 $|u_i\rangle = |a_i H\rangle$，并对 $x \in a_i H$ 定义 $|v\ (x)\ \rangle = |v_i\rangle$，即可得到 $|\psi\rangle = \frac{1}{\sqrt{k}} \sum_{a\in X} |aH\rangle|v\ (a)\ \rangle = \frac{1}{\sqrt{|G|}} \sum_{x\in G} |x\rangle|v\ (x)\ \rangle$。 □

2.4 子群态的基本转换

给定 G 的一个子群 L，通过将 $|x\rangle$ 替换为针对 $x \in G$、按照第 2.2 小节所述方法得到的分解 $|\beta_L(x)\rangle|\alpha_L(x)\rangle$，并“忽略” $|\alpha_L(x)\rangle$（将这部分传递给纯化子系统），即可将子群态 $\Xi_{G,\ H}$ 的一个副本（或其纯化的一个副本）“转换”为 $\Xi_{L,\ H\cap L}$ 的一个副本（或其纯化的一个副本）。为此，设 $\frac{1}{\sqrt{|G|}} \sum_{x\in G} |x\rangle|\psi(x)\rangle$ 是 $\Xi_{G,\ H}$ 的一个纯化，其中

$|\psi(x)\rangle$ 与 $|\psi(y)\rangle$ 相等，当且仅当 $y^{-1}x \in H$；否则正交。然后，代入得到状态 $\frac{1}{\sqrt{|L|}} \sum_{x\in L} |x\rangle \frac{1}{\sqrt{|G:L|}} \sum_{y\in Y} |y\rangle|\psi(yx)\rangle$，其中 $Y = \{\alpha_L(z)\colon\ z \in G\}$。现在，若 x_1、$x_2 \in L$ 来自 $H \cap L$ 的同一个左陪集，那么对于每个 $y \in Y$，都有 $|\psi(yx_1)\rangle = |\psi(yx_2)\rangle$，因此状态 $\frac{1}{\sqrt{|G:L|}} \sum_{y\in Y} |y\rangle|\psi(yx_i)\rangle$ 相等（$i = 1,\ 2$）；而否则它们不重叠，因为对于 y_1、$y_2 \in Y$，要么 $|y_1\rangle$ 与 $|y_2\rangle$ 正交，要么（对于 $y_1 = y_2$）$|\psi(y_1x_1)\rangle$与 $|\psi(y_1x_2)\rangle$ 正交。我们将这个程序称为限制。之所以这样称，是因为在 HSP 的标准版本中，可以

通过将“隐藏函数”限制在 L上，在子群 L 中获得一个 HSP 实例。

类似地，假设 L 是 H中包含于 G 的正规子群。那么，通过将 x 替换为 $|\alpha_L(x)\rangle|\beta_L(x)\rangle$ ，并将$|\beta_L(x)\rangle$ 传递到纯化子系统中，可以把子群态 $\Xi_{G,\ H}$ 的一个副本（纯化后的副本）转换为 $\Xi_{G/L,\ H/L}$ 的一个副本（纯化后的副本）。这对应于 [LK07a, LK07b]中称为“推送”的技术。

3 群论归约

本节证明以下命题。

命题 1. 设 G 是一个类至多为 c的幂零黑盒群，并假设 $|G|$ 的素因子作为输入的一部分给出，且对于每个这样的素数 p ，都能通过高效的精确量子过程实现模 p的倍数的量子傅里叶变换及其逆变换。那么，可以通过一个精确过程，在时间 poly(log ℓ)内，将 G 中的隐藏子群问题归约为 poly(log$|G|$)个实例；这些实例所涉及的是 G的子群的半初等商群上的 HSMC 问题。（假设 G 中的元素均由长度为 ℓ的字符串唯一编码。）

证明。有限幂零群 G 是其 Sylow 子群的直积。因此，任意子群 H 都是其 Sylow 子群的乘积。 H 的 p-Sylow 子群是 $P \cap H$ ，其中 P 是 G的 p-Sylow 子群。 G 的 Sylow 子群可以使用第 2.2 小节中概述的方法计算。可以使用限制将 G 中的子群态转换为 P 中的子群态，参见第 2.4 小节。

在接下来的约化描述中，我们假设 G 是一个 p-群。我们维护 H的一个子群 H_0 。初始时 $H_0 = \{1_G\}$。在算法的外层循环的每一轮中，如果 $H_0 < H$，就增大 H_0 。如果 H_0 已经是G ，那么显然可以停止。我们还会维护 G 的一个子群 K ，使得如果 $H_0 < H$ ，那么甚至 $H_0 < K \cap H$。初始时 $K = N_G(H_0)$ 。这是一个不错的选择，因为在幂零群中，每个真子群的正规化子都严格更大，因此如果 $H_0 < H$ ，那么 $H_0 < N_H(H_0) = H \cap N_G(H_0)$ 。在内层循环中， K 会不断减小，直到 H_0 增大，或者 K 与 H_0相同。后一种情况下，我们可以断定 $H = H_0$ ，并停止整个程序。如果阿贝尔因子 $K/(K'H_0)$ 不是初等阿贝尔群，那么可以按如下方式用一个真子群替换 K 。令 $L > K'H_0$ 为 K 的子群，使得 $L/(K'H_0)$ 包含 $K/(K'H_0)$ 中所有阶为 p 的元素。要计算 L，首先计算 K' 和 $K'H_0$。然后取 K的生成元集合 Γ ，对每个元素 $g \in \Gamma$，计算使得$g^{p^{\alpha_g}} \in K'H_0$成立的最小正整数 α_g 。元素 $g^{p^{\alpha_g - 1}}$ （$g \in \Gamma$）生成 L。如果 L 是 K 的真子群，就用 L 替换 K ，并重复上述步骤。（对此正确性的证明如下：注意到 L/H_0 包含 K/H_0中所有阶为 p 的元素，因此如果 $H \cap K > H_0$ ，那么 $H \cap L > H_0$也成立。）否则，我们便得到 $K/(K'H_0)$ 是初等阿贝尔群。然后我们使用 $(H \cap K)K'/H_0$ 来计算

HSMC。若 $(H \cap K)K' = K$，则 K' 包含于 K的每个极大子群中，因此 $H \cap K = K$。然后，我们可以通过将 H_0 替换为 K 来增加 H_0，并继续外层循环。若 $(H \cap K)K' < K$，我们可以将 K 替换为 $(H \cap K)K'$，并继续内层循环。

根据以上描述，我们将精确算法总结为以下伪代码。

算法 1 归约到 HSMC

```
初始化: H_0 ← 1_G;
当 H_0 < G 时
    K ← N_G(H_0);
    Found ← 假;
    当 Found = 为假时执行
        如果 K/(K'H_0) 是初等的，则
            使用 HSMC 计算 (H ∩ K)K'/H_0;
            如果 (H ∩ K)K' = K，则
                H_0 ← K;
                Found ← 真;
            else
                K ← (H ∩ K)K';
                如果 K = H_0，则
                    返回 H = K。
                结束条件判断
            结束条件判断
        else
            对于每个 g ∈ Γ_K，计算满足 g^{p^{α_g}} 的最小正整数 α_g        ∈ K'H_0;
            计算 L = ⟨g^{p^{α_g − 1}}        | g ∈ Γ_K⟩;
            K ← L;
        结束 if
    结束 while
结束 while
```

如果 $|G| = p^n$，那么外层循环至多执行 n 次，而外层循环的每一轮中，内层循环至多有 n 轮。因此，我们至多需要调用 HSMC 程序 n^2 次，以处理 G 的子群的因子群；此外还需要进行 n^2 次 poly(ℓ) 群运算及其他操作。注意，我们需要应用 HSMC 程序的所有群的类都至多为 c，因为类至多为 c 的幂零群构成的族在取子群和因子群时是封闭的。

□

4 主要转换

设 L 是 G 的中心的一个子群，且同构于 $\mathbb{Z}_p^n$，其中 p 是素数。那么 L 是 G 的正规子群。我们的目标是将子群态 $\Xi_{G,\ H}$ 的一个副本转换为 $\Xi_{G/L,\ HL/L}$ 的一个副本。根据第 2.4 小节所述的第二次转换（“推送”），可以先将其转换为 $\Xi_{G,\ HL}$ 的一个副本。

为此，最好能有一个程序，将陪集叠加态 $|aH\rangle$ 转换为 $|aHL\rangle$。一种可行的方法是，在一个新的寄存器中计算 $|L\rangle = \frac{1}{\sqrt{|L|}} \sum_{z \in L} |z\rangle$，将 $|aH\rangle$ 与其相乘，得到 $\frac{1}{\sqrt{|HL|}} \sum_{z \in L} \sum_{x \in H} |azx\rangle|z\rangle$，然后尝试将 $|z\rangle$ 与 $|azx\rangle$“解纠缠”。

L 的量子傅里叶变换几乎可以完成这项工作：如果我们将它作用于第二个寄存器，就会得到以下状态

$$\frac{1}{\sqrt{|L|}}\sum_{y\in L}\frac{\omega^{(y,z)}}{\sqrt{|HL|}}\sum_{z\in L}\sum_{x\in H}|azx\rangle|y\rangle,$$

其中 $\omega=e^{\frac{2\pi i}{p}}$，我们用 $(,)$ 表示 L 模p上的标准内积。对于 $y\in L$，记将 $|x\rangle$ 映射到$\frac{1}{\sqrt{|L|}}\sum_{z\in L}\omega^{(y,z)}|xz\rangle$的 $\mathbb{C}G$ 上的线性变换为 P_y。采用这一记号，我们可以将当前状态重写为

$$\frac{1}{\sqrt{|L|}}\sum_{y\in L}|P_y(aH)\rangle|y\rangle.$$

利用 L 位于 G的中心这一假设，直接计算可得，对于任意 x_1、$x_2\in G$，都有

$$|P_y(x_1x_2)\rangle=|x_1P_y(x_2)\rangle=|(P_y(x_1)x_2)\rangle. \tag{1}$$

同样容易看出，对于任意 $x\in G$ 和任意 $w\in L$，都有

$$|wP_y(x)\rangle=|P_y(x)w\rangle=\omega^{-(y,w)}|P_y(x)\rangle. \tag{2}$$

我们将 $\mathbb{C}G$ 中元素 $|u\rangle$ 的支撑集定义为：在将 $|u\rangle$ 分解为群元素的线性组合时，系数非零的元素所构成的集合。利用等式 (1) 可以证明，若 x_1 和 x_2 不属于 LH 的同一个左陪集，则状态 $|P_y(aH)x_1^{-1}\rangle$ 与 $|P_y(aH)x_2^{-1}\rangle$ 正交。这是因为 $|P_y(aH)x_i^{-1}\rangle$ 的支撑集包含于 $LHx_i^{-1}=(x_iLH)^{-1}$ $(i=1,2)$ 中。另一方面，若 $x_1H=x_2H$，则 $Hx_1^{-1}=Hx_2^{-1}$，且这两个状态相等。根据引理 1 中给出的刻画可知，对于任意左陪集 aH，状态 $\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|P_0(aHx^{-1})\rangle$ 是 Ξ_G的纯化

当然，要在 $|\overset{,LH\cdot}{P_y}(aH)x_1^{-1}\rangle$中强制实现 $y=0$ 是不可能的。不过，我们可以通过使用若干个子群态，并应用一种能够在 L的足够长元素序列中寻找零和子序列的算法，计算出效果基本相同的状态。假设我们有一个程序：对于某个 $S=S(p,n)$，给定一个元素 $\underline{y}=(y_1,\ldots,y_S)\in L^S$，计算出 $\{1,\ldots,S\}$ 的一个非空子集 $J(\underline{y})$，使得$\sum_{j\in J(\underline{y})}y_j=0$。

那么，对于一个序列 $|a_1H\rangle\ldots|a_SH\rangle$，我们首先计算

$$|L|^{-S/2}\sum_{\underline{y}\in L^S}|\underline{y}\rangle|P_{y_1}(a_1H)\rangle\ldots|P_{y_S}(a_SH)\rangle$$

通过对各个分量分别应用上述傅里叶方法。接下来，我们在一个新的寄存器中计算$\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle$，并在 $j\in J(\underline{y})$ 时乘以$|P_{y_1}a_1H\rangle\ldots|P_{y_S}a_SH\rangle$ 的第 j 个分量 x^{-1}。令 $\chi_{\underline{y}}$：$\{1,\ldots,S\}\to\{0,1\}$ 表示 $J(\underline{y})$ 的特征函数。那么我们得到的状态为$\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|\psi(x)\rangle$,

其中

$$|\psi(x)\rangle = |L|^{-S/2} \sum_{\underline{y}\in L^S} |\underline{y}\rangle |P_{y_1} a_1 H x^{-\chi_{\underline{y}}(1)}\rangle \dots |P_{y_S} a_S H x^{-\chi_{\underline{y}}(S)}\rangle.$$

考虑 $|\psi(x)\rangle$ 中对应任意 $\underline{y}$ 的项。由于 $J(\underline{y})$ 非空，对于不属于 LH 同一左陪集的 x_1、x_2，$|\psi(x_i)\rangle$ 中相应的项彼此正交。由于相应项中也出现了 $|\underline{y}\rangle$，因此 $|\psi(x_i)\rangle$ 也彼此正交。另一方面，如果 x_1、x_2 属于 H 的同一左陪集，那么这些状态逐项相等。最后，对于 $x \in L$，根据 (2，$\underline{y}$ 的项仅因 $\prod_{j\in J}(\underline{y})\omega^{-(y_j,x)} =_{\omega} \Sigma_{j\in J}(\underline{y})(y_j,x) = \omega^0 = 1$ 而发生相位变化，这由 $J(y)$ 的选取所致。因此，如果 x_1 和 x_2 属于 LH 的同一左陪集，那么 $|\phi(x_1)\rangle = |\phi(\overline{x_2}\rangle$。由此可知，我们的状态是 $\Xi_{G,LH}$ 的一个纯化。由于这对 H 的任意固定 S 元左陪集组都成立，根据线性性，如果将该程序应用于 $\Xi_{G,H}$ 的一个纯化的多个副本，我们也能得到 $\Xi_{G,LH}$ 的一个纯化。我们得到了如下结果。

引理 2. 假设我们有一个精确量子过程（例如，一个确定性多项式时间算法），它对于 $\mathbb{Z}_p^n$ 中的任意序列 $y_1, \dots, y_S$ of$S = S(p,n)$ 个元素，能在时间 $T(p,n) \geq S(p,n)$ 内找到 $\{1,\dots,S\}$ 的一个非空子集，使得 $\sum_{j\in J} y_j = 0$。那么，我们有一个精确量子过程，使用 n 次模 p 的量子傅里叶变换，在时间 $T(p,n)$ poly(log $|G|$) 内，将 $\Xi_{G,H}$ 的 $S(p,n)$ 个副本（的一个纯化）转换为 $\Xi_{G/L,HL/L}$ 的一个副本（的一个纯化），其中 L 是 G 中心的一个子群，且与 $\mathbb{Z}_p^n$ 同构。

在迭代中使用该引理，并应用 [II22], 的精确阿贝尔隐藏子群算法，我们可以推出以下结论。

命题 2. 设 G 是一个阶为 p^n、具有唯一编码的半初等黑盒群。假设模 p 的量子傅里叶变换及其逆变换可以通过高效的精确算法实现，并且与引理 2 中一样，我们有一种精确方法，可以在时间 $T(p,n) \geq S(p,n)$ 内，从 $\mathbb{Z}_p^n$ 中由 $S(p,n)$ 个元素构成的序列中找到零和子序列。那么，HSMC 问题可以由一个精确量子算法求解，该算法使用 poly$(T(p,n)^{O(c)}\ell)$ 次初等运算、poly$(T(p,n)^{O(c)}$ log $|G|)$ 次群预言机调用、计算子群态纯化的预言机调用，以及这些调用的逆运算。（假设 G 中的元素均由长度为 ℓ 的字符串唯一编码。）

证明。我们使用第 2.2 小节中介绍的方法计算下中心列 $G = G_0 > G_1 > \dots > G_c = \{1\}$。由于 G/G' 是初等阿贝尔群，因此因子 G_{i-1}/G_i（$i = 1,\dots,c$）也都是初等阿贝尔群。这是因为因子群 G_{i-1}/G_i 是 G/G' 的张量幂（作为 $\mathbb{Z}$-模）的同态像，见 [Rob95] 的定理 5.2.5。此外，使用 [II22] 的方法，可以高效地计算 G_{i-1}/G_i 与 $\mathbb{Z}_p^{n_i}$ 之间的同构。反复应用引理 2，可得到一个程序，将 $\prod_{i=2}^{c} S(n_i)$ 个 $\Xi_{G,H}$ 的纯化副本转换为一个 $\Xi_{G/G',HG'/G'}$ 的纯化副本。将原始程序的多个实例组合起来

子群态制备过程（即对预言机的调用）与该转换相结合，就得到一个制备 $\Xi_{G/G',HG'/G'}$ 的纯化的程序。我们可以将其用作 $\mathbb{Z}_p^{n_1}$ 中 [II22] 的精确隐藏子群算法的预言机输入。对于 $i = 1, \ldots, c$，有 $S(p, n_i) \leq S(p, n)$，且 $T(p, n_i) \leq T(p, n)$，因为 $\mathbb{Z}_p^{n_i}$ 可以作为子群嵌入 $\mathbb{Z}_p^n$。 □

在非精确情形下，基本上相同的证明可得如下结论。

命题 3. 设 G 是一个具有唯一编码且阶为 p^n的半初等黑盒群。假设存在一种量子（或随机化）算法，能够以高概率在时间 $T(p, n) \geq S(p, n)$ 内，找出 $\mathbb{Z}_{p^n}$ 中由 $S(p, n)$ 个元素组成的序列的零和子序列。那么，HSMC 问题可由一种量子算法求解，该算法使用 poly$(T(p, n)^{O(c)}\ell)$ 次初等操作、poly$(T(p, n)^{O(c)}$ log $|G|)$ 次群预言机调用，以及调用用于计算子群态纯化的预言机。

5 $\mathbb{Z}_p^n$中的零和子序列

本节中，我们假设输入是来自 $\mathbb{Z}_p^n$的向量序列。我们还假设 p 是奇素数，因为对于 $p = 2$，可将由 $n + 1$ 个向量构成的零和子序列表示为零线性组合。由于子序列可以表示为指标集的子集，因此将（子）序列称为（子）集也不会造成太大误解。我们的策略是寻找 p 个两两不相交的输入向量子集，使它们的和相等。为此，我们将设计一种方法，找出一对和相等的非平凡子集，然后像在 [IS17], 中那样递归应用该算法，从而得到 4、8、16 个等和的不相交子集。

注意，一对和相等的不相交子集，可以解释为：通过对输入向量作线性组合，并使用非零系数 1 或 -1 only，表示零向量。基于这一点，使用“带符号子集”和“带符号子集和”这两个术语会很方便。集合 S 中的向量的一个带符号子集，形式上是一个从 S 到集合 $\{0, 1, -1\}$ 的函数。此类带符号子集的支撑集，是函数取非零值的元素所组成的集合。稍微不严谨地说，我们使用“带符号子集和”一词，既指带符号子集，也指带符号求和的值。（严格来说，一个带符号子集和可以是一种数据结构，由带符号子集的描述及其值组成。）如果两个或多个子集和的支撑集两两不相交，我们就称它们不相交。基于这一观察：由支撑集两两不相交的子集和所得的向量的带符号子集和，仍然是原始向量的带符号子集和，因此可以从较小的不相交带符号子集和分层构建带符号子集和。平凡的子集和对应于空集，其值为零向量。

一组向量之间的线性关系（简称关系）是一列系数，使相应的线性组合为零向量。通常可以省略系数为零的向量

及其对应的系数。取线性关系中系数相同或相反的向量所组成的带符号子集，就能得到一个关于两两不相交的带符号子集和的线性关系，其中系数为 $\{1,\ldots,\frac{p-1}{2}\}$，且每个系数至多出现一次。我们称这种带符号子集和的关系为标准关系。

我们将构造一系列标准线性关系，其中带符号子集和中的系数逐渐变小（而子集和所涉及的向量越来越多）。关键思路是：首先构造 $(p-1)_4^{\ 2}$ 个两两不同的带符号子集和，将它们排成一个方阵矩阵，使每一行和每一列都满足一个关系；然后用较高一半“垂直”关系之和减去较高一半“水平”关系之和，从而得到一个系数介于 1 和 $\frac{p-1}{4}$ 之间的关系，并迭代这一构造。我们将在下面的引理及其证明中给出细节。（我们给出的版本甚至省去了维持前一半垂直关系的开销。）

引理 3. 设 d 为正整数。假设存在一个确定性过程 $\mathcal{A}$，该过程给定来自 $\mathbb{Z}_p^n$的 $h(d,n)$ 个向量后，能在 $\mathrm{poly}(h(d,n)\log p)$ 时间内，找到输入向量的d 个两两不相交的带符号子集和 v_1，.....，v_d，它们不全为空，且满足 $\sum_{i=1}^{d} iv_i = 0$。那么也存在一个确定性过程：给定 $h(d,n)h(d,\lceil d/2\rceil n)$ 个向量后，能在 $\mathrm{poly}(h(d,n)h(d,\lceil d/2\rceil n)\log p)$ 时间内，找到 w'_1，.....，$w'_{\lfloor d/2\rfloor}$这些两两不相交的带符号子集和，它们不全为空，且满足 $\sum_{i=1}^{\lfloor d/2\rfloor} iw'_i = 0$。

证明。我们将输入集划分为 $h(d,\lceil d/2\rceil n)$个两两不相交的部分，每部分大小为$h(d,n)$。我们在每个部分中应用程序 $\mathcal{A}$ 。这样，对于每个 k =1, . . . , $h(d,\lceil d/2\rceil n)$，我们得到 d 个两两不相交的子集和 $u_{k1},\ldots,u_{kd}$，它们并非全为空，且满足$\sum_{j=1}^{d} ju_{kj} = 0$。对于每个 k，我们考虑向量 $u_{kj}(j=\lfloor d/2\rfloor+1,\ldots,d)$的拼接 u_k。这些是维数为 $\lceil d/2\rceil n$的向量。我们应用程序 $\mathcal{A}$来找出两两不相交的带符号子集 $M_1,\ldots,M_d$，使得 $\sum_{i=1}^{d} iu'_i = 0$，其中 u'_i是与带符号子集 M_i相对应的 u_k的带符号和。现在，对于每个 $1\le i\le d$， u'_i 是向量 $w_{ij}(j=\lfloor d/2\rfloor+1,\ldots,d)$ 的拼接。这里，对于 $1\le i,\ j\le d$， w_{ij} 表示按照带符号子集 M_i 将带符号子集和 u_{kj} 合并后得到的带符号子集和。这些带符号子集和 w_{ij} 两两不相交，并非全为空，且满足以下关系

$$\sum_{i=1}^{d} iw_{ij} = 0 \ \ (j=\lfloor d/2\rfloor+1,\ldots,d)$$

and

$$\sum_{j=1}^{d} jw_{ij} = 0 \ \ (i=1,\ldots,d).$$

我们从第一类 $\lceil d/2\rceil$ （“垂直”）关系之和中减去第二类最后 $\lceil d/2\rceil$ 个（“水平”）关系之和，得到

关系

$$\sum_{i=1}^{\lfloor d/2\rfloor}\sum_{j=\lfloor d/2\rfloor+1}^{d} iw_{ij} - \sum_{i=\lfloor d/2\rfloor+1}^{d}\sum_{j=1}^{\lfloor d/2\rfloor} jw_{ij} + \sum_{i,j=\lfloor d/2\rfloor+1}^{d}(i-j)w_{ij} = 0.$$

注意，对于 $\lfloor d/2\rfloor+1 \le i$、$j \le d$，我们有 $|i-j| \le \lfloor d/2\rfloor$。因此，在适当的位置改变符号，然后将系数相同的带符号子集合并起来，就得到两两不相交的子集和 w'_1、.....、$w'_{\lfloor d/2\rfloor}$，其中 $\sum_{i=1}^{\lfloor d/2\rfloor} iw'_i = 0$。

子集和 w'_i 全都为空，当且仅当在 $i \ne j$ 时每个 w_{ij} 都为空，并且 i 和 j 中至少有一个大于 $\lfloor d/2\rfloor$。假设情况如此。那么，如果存在一个指标 $i > \lfloor d/2\rfloor$，使得 w_{ii} 非空，则 w_{ii} 本身必定是一个非平凡的零子集和，并给出一个单项解。否则，对于 i、$j \le \lfloor d/2\rfloor$ 和 $\sum_{i}^{\lfloor d/2\rfloor},\ _{j=1}\, iw_{ij} = 0$，并非所有 w_{ij} 都为空。 □

反复应用引理 3 的方法，可得以下结果。

命题 4. 给定来自 $\mathbb{Z}_p^n$ 的 $S_\pm(p,n) = p^{O(p\log p)}n^{O(p)}$ 个向量，可以在 poly($S_\pm(p,n)$) 确定性时间内找到一个表示零向量的非平凡带符号子集和。

证明. 令 $d_0 = \frac{p-1}{2}$，$h_0(n) = n+1$，并递归定义 $d_i = \lfloor d_{i-1}/2\rfloor$ 和 $h_i(n) = h_{i-1}(n)h_{i-1}(\lceil d_{i-1}/2\rceil n)$，其中 $i = 1,\dots,\lfloor \log d_0\rfloor$。由于从 $\mathbb{Z}_p^n$ 中任取 $h_0(n)=n+1$ 个向量，都可以在 poly($n\log p$) 时间内找到一个非平凡线性关系，因此递归应用引理 3 可知，在 $h_{\lfloor \log d_0\rfloor}(n)$ 个向量中，可以在 poly($h_{\lfloor \log d_0\rfloor}(n)\log p$) 时间内找到一个非平凡带符号子集和（即仅含非零系数±1 的线性关系）。我们用归纳法证明

$$h_i(n) \le \left(\prod_{j=0}^{i-1}\lceil d_j/2\rceil\right)^{2^{i-1}} (n+1)^{2^i}. \tag{3}$$

对于 $i=0$，两边均等于 $n+1$。假设该不等式对$0 \le i < \lfloor \log d_0\rfloor$成立。那么我们还有

$$h_i(\lceil d_i/2\rceil n) \le \left(\prod_{j=0}^{i-1}\lceil d_j/2\rceil\right)^{2^{i-1}} (\lceil d_i/2\rceil n+1)^{2^i}.$$

利用 $\lceil d_i/2\rceil n + 1 \le \lceil d_i/2\rceil(n+1)$，我们得到

$$h_i(\lceil d_i/2\rceil n) \le \lceil d_i/2\rceil^{2^{i-1}} \left(\prod_{j=0}^{i}\lceil d_j/2\rceil\right)^{2^{i-1}} (n+1)^{2^i}. \tag{4}$$

将不等式 (3) 和 (4) 相乘，并利用 $h_{i+1}(n) = h_i(n)h_i(\lceil d_i/2\rceil n)$，得到

$$h_{i+1}(n) \le \left(\prod_{j=0}^{i}\lceil d_j/2\rceil\right)^{2^i} (n+1)^{2^{i+1}},$$

这就是将 i 替换为 $i+1$ in 后的不等式 (3)。利用 $d_j \le d_0/2^j \le d_0 = \frac{p-1}{2}$，针对 $i = \lfloor \log d_0 \rfloor$ 的不等式 (3) 得到

$$h_{\lfloor \log d_0 \rfloor} \le \left(\prod_{j=0}^{\lceil \log \frac{p-1}{2} \rceil - 1} \left\lceil \frac{p-1}{4} \right\rceil \right)^{2^{\lceil \log \frac{p-1}{2} \rceil - 1}} (n+1)^{2^{\lceil \log \frac{p-1}{2} \rceil}}$$

$$= \left\lceil \frac{p-1}{4} \right\rceil^{\lceil \frac{p-1}{4} \rceil \lceil \log \frac{p-1}{2} \rceil} (n+1)^{\lceil \frac{p-1}{2} \rceil}.$$

因此，我们有

$$h_{\lfloor \log d_0 \rfloor}(n) = p^{O(p \log p)} n^{O(p)}.$$

□

我们将非空的零和带符号子集解释为两个不相交子集和之间的非平凡碰撞。（非平凡是指这两个子集中至多有一个为空。）我们将这样的一对子集简称为碰撞。下面给出如下结果。

命题 5. 假设存在一个算法 $\mathcal{B}$，它能在给定来自 $\mathbb{Z}_p^n$ 的一个大小为 $S_\pm(p,n)$ 的向量集合时找到一次碰撞。那么，存在一个确定性过程，它在给定 $S_\pm(p,n)^{\lceil \log p \rceil}$ 个向量时，能够找到一个非平凡零和子集，且使用该算法 $\mathcal{B}$ 的次数少于 $S_\pm^{\lceil \log p \rceil}$ 次，其他操作的次数为 $\mathrm{poly}((S_\pm(p,n))^{\lceil \log p \rceil})$。

证明. 令 $S = S_\pm(p,n)$，并令 $\ell = \lceil \log p \rceil$。首先，使用算法$\mathcal{B}$在前 S 个向量中找到一次碰撞（H_1^+,H_1^-），其和为 w_1。接着处理后续的 S 个输入向量，找到一次碰撞（H_2^+,H_2^-），其和为 w_2，依此类推。然后，取前 S 个子集和 $w_1, \ldots, w_S$，并在 $\{1, \ldots, S\}$ 中找出两个不相交的子集（K^+, K^-），它们不全为空，且满足 $\sum_{i \in K^+} w_i = \sum_{i \in K^-} w_i = w$。输入向量的四个子集 $L^{++} = \bigcup_{i \in K^+} H_i^+$、$L^{+-} = \bigcup_{i \in K^+} H_i^-$、$L^{-+} = \bigcup_{i \in K^-} H_i^+$ 和 $L^{--} = \bigcup_{i \in K^-} H_i^-$ 两两不相交、不全为空，并且和相同，均为 w。重复这一过程，最终至少得到 p 个两两不相交、和相等的子集（不全为空）。如果其中一个集合为空，那么共同的和就是零，我们可以任选一个非空子集。否则，前 p 个子集的并集和为零。碰撞查找算法 $\mathcal{B}$总共调用 $S^{\ell-1} + \ldots + S + 1 < S^\ell$ 次。

□

命题 4 和命题 5，加上关于情形 $p = 2$ 的注释，立即得出以下结论。

定理 2。存在一种确定性算法，对于来自 $\mathbb{Z}_p^n$ 的 $S(p,n) = p^{O(p \log^2 p)} n^{O(p \log p)}$ 向量序列，可在 $\mathrm{poly}(S(p,n))$ 时间内找到一个非平凡零和子序列。

我们指出，在 [IS17]，中给出了一种用于更一般任务的算法。该任务是将零向量表示为输入向量的线性组合，并且系数为 d 次幂，从而得到一种非平凡表示。我们的问题是它在 $d = p - 1$ 情形下的特例。 [IS17] 中针对 $d = p - 1$ 的算法会给出 $S(p, n) = p^{O(p^2 \log p)} n^{O(p \log p)}$，其参数比我们在定理 2 中的参数稍差，不过对于 $p = O(1)$，它对 n 仍是多项式的。 [IS17] 中用于寻找碰撞的方法比本文的方法更复杂：它基于收集按 d 维超立方体组织的关系，而非正方形。（碰撞倍增法与命题 5 中所述的方法基本相同。）

6 结论

我们已经证明，对于幂零类 G 有常数上界的幂零群，只要存在一种多项式时间（即时间复杂度为 poly($n$log p)）的精确方法，能够在由 poly 个元素组成的序列中查找 $\mathbb{Z}_p^n$ 的零和子序列，其中 p 是 $|G|$的素因子，就可以通过精确量子算法在多项式时间内求解隐藏子群问题。对于 $p = O(1)$，我们已经拥有这样一种方法。根据 Olson 定理 [Ols69], ，存在零和子序列查找算法时，其最短长度约为 np，而该算法不一定需要在多项式时间内运行。

我们提出如下问题，供进一步研究：是否存在一种 poly(np) 时间算法，能够从长度为（np）^{d} 的序列中查找零和子序列，其中 d 为充分大的常数。肯定的回答将意味着：当 $|G|$为光滑阶时，存在精确的多项式时间量子算法；也就是说， $|G|$ 的素因子的大小均被 log$|G|$的某个多项式所界定。即使是非精确方法（例如随机化算法）也将极具意义，因为根据命题 3，这将为非精确情形带来一个新结果：对于阶为光滑阶且幂零类由 $O(1)$界定的幂零群，存在一种高效的“概率”量子隐藏子群算法。即使结果稍差一些，也可能带来比已知算法更快的量子隐藏子群算法。

对于“概率型”量子隐藏子群算法而言，即使一种方法只能“平均地”找到零和子序列，也就是说，对于至少占所有可能序列的 $1/\text{poly}(np)$ 的序列，它都能找到零和子序列，这也足够了。然而，正如下面这个简单的最坏情况到平均情况归约所示，至少在随机化的情形下，所获改进不可能超过多项式级别。假设经典随机化算法 $\mathcal{A}$ 能在时间 $T = T(p, n)$ 内，以至少 δ 的概率，从一个由 $\mathbb{Z}_p^n$ 中的向量构成、长度为 $S = S(p, n)$ 的随机序列中找到一个子序列。这里，概率是针对向量数组与 $\mathcal{A}$ 的随机比特的联合均匀分布而言的。于是我们可以这样做：从任意一个由 $\frac{1}{\delta} \cdot S^2$ 个输入向量组成的序列开始，为每个输入向量各抽取一个均匀随机向量。然后将输入序列划分为若干个长度为 S 的组，并将相应的随机向量加到每个输入向量上。在每一组内，我们应用程序

$\mathcal{A}$。由于这些和是随机向量，每一组中，程序 $\mathcal{A}$ 至少以 δ 的概率成功；而且，$\mathcal{A}$ 至少以$_1$ $_2$的概率在至少S 组中成功。若如此，我们就选取 S 个“幸运”组，并在每一组中对与零和子序列成员对应的随机向量求和。我们对这些 S 个和应用算法 $\mathcal{A}$。它至少以 δ的概率找到一个非平凡零和子序列。最后，我们取相应子序列的并集。这样便得到一个程序，它能以至少 $\delta/2$的概率，在时间 poly($T + \frac{1}{\delta} \cdot ST$) 内从每个长度为 $\frac{1}{\delta} \cdot S^2$ 的序列中找到一个非平凡零和子序列。

参考文献

[AMR07] G. Alagic、C. Moore 和 A. Russell。《一般群上的 Simon 问题量子算法》。载于第十八届 ACM-SIAM 离散算法研讨会论文集，第 1217–1224 页，2007 年。[AR17] G. Alagic 和 A. Russell。《基于隐藏平移的量子安全对称密钥密码学》。载于《密码学进展——EUROCRYPT 2017：第 36 届密码技术理论与应用国际会议》，法国巴黎，2017 年 4 月 30 日至 5 月 4 日，论文集第三部分，第 65–93 页。施普林格，2017 年。[BH97] G. Brassard 和 P. Høyer。《Simon 问题的精确量子多项式时间算法》。载于 ISTCS 97，第 12–23 页，1997 年。[BL21] E. Bae 和 S. Lee。《基于 ε-随机线性不等式的连续隐藏平移问题量子算法》。Quantum Inf. Process.，20(10):347，2021 年。[BNP18] X. Bonnetain 和 M. Naya-Plasencia。《隐藏平移量子密码分析及其影响》。载于《密码学进展——ASIACRYPT 2018：第 24 届密码学与信息安全理论及应用国际会议》，澳大利亚昆士兰州布里斯班，2018 年 12 月 2–6 日，论文集第一部分 24，第 560–592 页。施普林格，2018 年。[Bon21] X. Bonnetain。《Simon 算法的紧确界》。载于 LATINCRYPT 2021，第 2–23 页，2021 年。[BV97] E. Bernstein 和 U. Vazirani。《量子复杂性理论》。SIAM J. Comput.，26:1411–1473，1997 年。[CM23] W. Castryck 和 N. Vander Meeren。《关于向量化问题的两点说明》。载于《密码学进展——INDOCRYPT 2022：第 23 届印度密码学国际会议》，印度加尔各答，2022 年 12 月 11–14 日，论文集，第 658–678 页。施普林格，2023 年。

[CQ18] G. Cai 和 D. Qiu。《Simon 问题精确查询复杂度的最优分离》。J. Comput. Syst. Sci.，97:83–93，2018 年。[DHIS14] T. Decker、P. Høyer、G. Ivanyos 和 M. Santha。《若干双变量隐藏多项式问题的多项式时间量子算法》。Quantum Inf. Comput.，14(9-10):790–806，2014 年。[EHK04] M. Ettinger、P. Høyer 和 E. Knill。《隐藏子群问题的量子查询复杂度是多项式级的》。Inf. Process. Lett.，91:43–48，2004 年。[FIM+14] K. Friedl、G. Ivanyos、F. Magniez、M. Santha 和 P. Sen。《量子计算中的隐藏平移与平移陪集》。SIAM J. Comput.，43(1):1–24，2014 年。初步版本发表于 STOC 2003。[HK18] K. Horan 和 D. Kahrobaei。《隐藏子群问题与后量子群密码学》。载于《数学软件——ICMS 2018：第六届国际会议》，美国印第安纳州南本德，2018年7月24日至27日，论文集 6，第 218–226 页。施普林格，2018 年。[II22] M. Imran 和 G. Ivanyos。《一种精确的量子隐藏子群算法及其在可解群中的应用》。Quantum Inf. Comput.，22(9&10):770–789，2022 年。[IS17] G. Ivanyos 和 M. Santha。《在有限域上求解对角多项式方程组》。Theor. Comput. Sci.，657:73–85，2017 年。[ISS12] G. Ivanyos、L. Sanselme 和 M. Santha。《二步幂零群中隐藏子群问题的高效量子算法》。Algorithmica，62(1-2):480–498，2012 年。[KL90] W. M. Kantor 和 E. M. Luks。《商群中的计算》。载于 STOC 1990，第 524–534 页，1990 年。[Kup05] G. Kuperberg。《求解二面体隐藏子群问题的亚指数时间量子算法》。SIAM J. Comput.，35(1):170–188，2005 年。[LK07a] S. Jr. Lomonaco 和 L. H. Kauffman。《Grover算法是量子隐藏子群算法吗？》Quantum Inf. Process.，6:461–476，2007 年。[LK07b] S. Jr. Lomonaco 和 L. H. Kauffman。《量子隐藏子群算法：算法工具包》。载于《量子计算与量子技术数学》，第 21–64 页。Chapman and Hall/CRC，纽约，2007 年。[Lom04] C. Lomont。《隐藏子群问题：综述与开放问题》。技术报告 quant-ph/0411037，arXiv，2004 年。

[MZ03] M. Mosca 和 C. Zalka。精确量子傅里叶变换与离散对数算法。Int. J. Quantum Inf., 02:91–100, 2003。[NC10] M. A. Nielsen 和 I. K. Chuang。《量子计算与量子信息》。剑桥大学出版社，剑桥，10 周年纪念版，2010。[NO02] H. Nishimura 和 M. Ozawa。一致量子电路族与量子图灵机的计算复杂性。Theor. Comput. Sci., 276:147–181, 2002。[NO05] H. Nishimura 和 M. Ozawa。无误差算法的量子电路族一致性。Theor. Comput. Sci., 332:487–496, 2005。[NO09] H. Nishimura 和 M. Ozawa。量子图灵机与有限生成的一致量子电路族之间的完美计算等价性。Quantum Inf. Process., 8:13–24, 2009。[Ols69] J. E. Olson。有限阿贝尔群上的一个组合问题，I。J. Number Theory, 1(1):8–10, 1969。[Rob95] D. Robinson。《群论教程》。施普林格，伊利诺伊州厄巴纳，第 2 版，1995。[Wan10] F. Wang。隐藏子群问题。技术报告 quant-ph/1008.0010，arXiv，2010。[Wat01] J. Watrous。可解群的量子算法。载于 STOC 2001，第 60–67 页，2001。[WQT+22] Z. Wu、D. Qiu、J. Tan、H. Li 和 G. Cai。广义 Simon 问题的量子与经典查询复杂性。Theor. Comput. Sci., 924:171–186, 2022。