# 隐含子群问题的研究现状

戴文静 袁家斌

(南京航空航天大学计算机科学与技术学院 南京 211106)

**摘 要** 在Shor发现大整数因子分解问题的有效量子算法之后,量子计算迫使我们重新审视现有的密码系统。隐含子群问题是量子计算在群结构上的推广,它暗示通过考虑不同的群和函数来解决更困难的问题,以期找到新的指数倍快于其经典对应物的量子算法。有限交换群隐含子群问题的研究已有相对固定的研究框架和方法,而非交换群隐含子群问题的研究一直很活跃。研究表明,二面体群隐含子群问题的有效解决可能攻破基于格的唯一最短向量问题的密码体制,图同构问题可以转化为对称群隐含子群问题。文中对隐含子群问题的研究现状进行综述,希望能够吸引更多研究者对隐含子群问题的注意。最后为隐含子群问题未来的研究方向提出参考意见。

**关键词** 量子计算,隐含子群问题,交换群,二面体群,唯一最短向量问题,对称群

**中图法分类号** TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.06.001

## Survey on Hidden Subgroup Problem

DAI Wen-jing YUAN Jia-bin

(College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 211106, China)

**Abstract** After Shor has presented an effective quantum algorithm for factoring of large integer, quantum computation forces us to re-examine the existing cryptosystems. Hidden subgroup problem is the generalization of quantum computation in group structure, it implicits that more difficult problems might be solved by considering various groups and functions to find new algorithms which are exponentially faster than their classical counterparts. The abelian hidden subgroup problem research has formed a relatively unified framework, while the non-abelian hidden subgroup problem research is always alive. The dihedral hidden subgroup problem may break the cryptosystems of the unique shortest vector problem based on the lattice and the graph isomorphism problem can be reduced to the symmetric hidden subgroup problem. The hidden subgroup problem was summarized to attract more researchers. Finally, this paper provided a suggestion for the direction of future research.

**Keywords** Quantum computation, Hidden subgroup problem, Abelian group, Dihedral group, Unique shortest vector problem, Symmetric group

## 1 引言

现代密码学将密码体制分为对称密码体制和公钥密码体制。1976年,美国密码学专家Diffie和Hellman发表的文献[1]奠定了公钥密码体制的基石。公钥密码的安全性基于数学问题的计算困难性,最具代表性的公钥密码是RSA,ElGamal和ECC。RSA[2]是一种基于大整数因子分解问题的公钥密码系统;ElGamal[3]基于离散对数问题的困难性;ECC[4],即椭圆曲线密码体制,基于椭圆曲线有限域上的离散对数问题的计算困难性。

量子计算是量子力学与计算机科学的交叉学科。利用量子算法对各种NP问题进行求解是量子计算的研究重点。Shor算法[5]和Grover量子搜索算法[6]是目前最著名的两种量子算法。Shor算法用于求解大整数因子分解问题(Factoring)和离散对数问题(Discrete Logarithm Problem),其相比经典算法达到了指数级加速;Grover量子搜索算法用于在无序数据库中搜索若干特定的目标,对许多启发式搜索经典算法起到了二次加速的作用。Shor算法可以对RSA,ElGamal,ECC公钥密码进行有效攻击,说明在量子计算环境下RSA,ElGamal,ECC公钥密码体制将不再安全。Grover算法的应用范围广泛,可用于密码分析,具有加速搜索密码系统密钥的潜在用途,可有效破译DES密码体系[7]。

量子计算对密码体制的威胁以必须使用"大规模的量子计算机"为前提。然而,量子计算机并不能有效攻击所有的现有密码。基于量子计算机不擅长计算的那些问题构造密码,就可以抵抗量子计算的攻击,抗量子计算密码应运而生。

到稿日期:2017-05-09 返修日期:2017-08-11 本文受基于GPU集群的大规模量子线路仿真理论与方法研究(61571226),国家自然科学基金青年基金(61701229),江苏省自然科学基金青年基金(BK20170802)资助。

**戴文静**(1992-),女,硕士生,主要研究方向为量子密码、量子计算,E-mail:jing@nuaa.edu.cn;**袁家斌**(1968-),男,博士后,教授,CCF高级会员,主要研究方向为信息安全、量子密码、高性能计算,E-mail:jbyuan@nuaa.edu.cn(通信作者)。

由于运算具有线性特性，因此基于格(Lattice)的公钥密码体制比 RSA 等经典公钥密码体制具有更快的实现效率，且该类密码体制的安全性基于 NP-Hard 或者 NP-C 问题。以上优势使得格密码体制成为抗量子攻击密码体制中最核心的研究领域。最短向量问题(Shortest Vector Problem，SVP)是格中重要的 NP-C 问题。2002 年，Regev[8] 率先注意到量子计算与格之间的联系，提出利用量子算法求解格的唯一最短向量问题(Unique Shortest Vector Problem，uSVP)的归约方法。文献[9]从问题归约角度详细阐述了该联系，这在一定程度上反映了利用量子计算来求解某些格的困难问题的可能性。

隐含子群问题(Hidden Subgroup Problem，HSP)是量子计算在群结构上的推广。已有研究表明，格的唯一最短向量问题可转化为二面体群隐含子群问题(Dihedral Hidden Subgroup Problem，DHSP)，图同构问题可以转化为对称群隐含子群问题(Symmetric Hidden Subgroup Problem，SHSP)。进一步地，有效地求解 DHSP 可能攻破基于格的唯一最短向量问题的公钥密码体制，并且 SHSP 的解决将会针对图同构问题产生一种有效的量子算法[10]。因此，HSP 成为量子计算最突出的主题之一。

## 2 量子算法与隐含子群问题

很多研究将量子算法推广到 HSP，HSP 与量子算法密切相关。

Deutsch 算法[11]是第一个被明确定义的量子算法。文献[12]给出求解 Simon 问题的量子算法。1994 年，Shor 把大整数因子分解问题和离散对数问题转化为一类周期寻找问题(Period Finding Problem)，并且对其进行了有效的求解[5]。

Kitaev[13]于 1995 年给出了一个求解交换群稳定子问题(Abelian Stabilizer Problem)的多项式量子算法，并证明该算法可以将大整数因子分解问题和离散对数问题作为特殊情况来求解[14]。Kitaev 证明阶寻找问题(Order Finding Problem)可被归约为特征值估计问题(Eigenvalue Estimation Problem)，然后再被归约为相位估计问题(Phase Estimation Problem)。而量子 Fourier 变换是相位估计的关键，并且 Fourier 变换与群表示相关，$Z_n$ 即为描述该问题的隐含子群(Hidden Subgroup)，隐含子群问题随即诞生。

1995 年，Dan 和 Lipton 率先注意到量子算法和 HSP 的联系，并给出了一个解隐含线性函数问题的量子算法[15]。1997 年，Brassard 和 Høyer 将 Simon 问题推广到 HSP[16]。同年，Jozsa 给出了 Deustch-Jozsa 算法、Simon 算法和 Shor 算法在 HSP 形式下的统一描述[17]。

周期寻找问题可以通过 $Z_n$ 上的量子 Fourier 变换进行有效求解，其中$(Z_n,+)$是 $n$ 阶循环群。$n$ 阶循环群对应的 HSP 被称为有限循环群 HSP，其具体定义为：设 $G$ 是一个有限生成群，$K\leqslant G$，给定一个函数 $f:G\to X$，其中 $X$ 为任意有限集合。该函数 $f$ 在子群 $K$ 的(左)陪集上是固定常数，且在每个不同的陪集上函数值都不同。HSP 是给定一个对 $g\in G,h\in X$ 和适当选取的 $X$ 上的二元运算$\oplus$，执行酉变换 $U|g\rangle|h\rangle=|g\rangle|h\oplus f(g)\rangle$的量子黑箱，求子群 $K$ 的一个生成集。求阶、求周期、离散对数问题和许多其他问题都是 HSP 的实例[14]。

隐含子群问题是量子计算在群结构上的推广，它暗示通过考虑不同的群 $G$ 和函数 $f$ 来解决更困难的问题，以期找到新的指数倍快于其经典对应物的量子算法。隐含子群问题遵循“有限循环群隐含子群问题－交换群隐含子群问题－非交换群隐含子群问题－一般隐含子群问题”的发展脉络。

## 3 交换群隐含子群问题

2001 年，Jozsa 分析了 Shor 算法的基本要素，对交换群 HSP 进行统一概括[18]。文献[19-20]介绍了更一般的交换群 HSP，给出了量子 Fourier 变换求解交换群 HSP 的量子算法。Fourier 抽样，即 Fourier 变换和测量，是求解 HSP 的主要工具之一。当相关的群是有限交换群时，良好的群论性质能够保证 HSP 被求解。而 HSP 并不总是直接适用于这类群，不同的方法被用来证明 HSP 是可解的[10]。交换群 HSP 关注的主要是有限交换群。

有限交换群同构于模算术中整数加法群的积，即 $G\cong Z_{p_1^{m_1}}\times Z_{p_1^{m_2}}\times\cdots\times Z_{p_t^{m_t}}$，其中 $p_i$ 是素数，$m_i$ 是正整数，$Z_{p_i^{m_i}}=\{0,1,\cdots,p_i^{m_i}-1\}$是整数模 $p_i^{m_i}$ 加法群。文献[21]给出有限交换群分解的量子算法。文献[19,22]给出有限交换群 HSP 量子算法的详细介绍。迄今为止，有限交换群 HSP 的研究已形成相对固定的统一研究框架和方法，如算法 1 所示。

**算法 1** 有限交换群 HSP 的量子算法

输入：HSP 的函数 $f:G\to X$ 和算符 $U_{f(Xe_j)}$

要求：G 是一个有限交换群，X 为任意有限集合，$|x\rangle U_{f(Xe_j)}|f(y)\rangle=|x\rangle f(y+xe_j)\rangle$

输出：子群 $K\leqslant G$

具体步骤：

Step 1 制备初态；

Step 2 对第一寄存器做量子 Fourier 变换；

Step 3 对第一寄存器执行酉变换 $U_{f(Xe_j)}$，将结果存储到最后一个寄存器；

Step 4 对第一寄存器做量子 Fourier 变换；

Step 5 测量第一寄存器，根据测量结果可得子群 K 的生成元，进而得到隐含子群 K。

第一寄存器由 $l$ 个量子寄存器组成，每个寄存器的量子比特数是$\lceil\log(p^{m_i})\rceil$，量子 Fourier 变换为 $F_G=F_{p^{m1}}\times F_{p^{m2}}\times\cdots\times F_{p^{ml}}$，即对每个寄存器都做量子 Fourier 变换。该量子算法的框架适用于与循环群直积同构的有限交换群。循环群一定是交换群，但交换群不一定是循环群，这是 HSP 的重要推广。

## 4 非交换群隐含子群问题

1998 年，Ekert 和 Jozsa 对 Abel 快速 Fourier 变换算法和非 Abel 快速 Fourier 变换算法的量子算法的加速效果进行了研究[23]，该研究很富启发性。1999 年，Cleve 证明了在一台有界误差概率经典计算机上求一个置换的阶的问题需要指数次计算[24]。Ettinger 等[25]，Röetteler 等[26]，Püschel 等[27]，Beals 等[28]及 Ettinger 等[29]都试图将这种方法推广到交换群以外。其中，Beals 等[28]还描述了对称群量子 Fourier 变换的构造。这些研究表明，到目前为止，对于求解非交换群的 HSP，存在仅需 $O(\log|G|)$次 Oracle 调用的量子算法，但该操作是否可

以在多项式时间内实现尚不清楚[14]。对于非交换群 HSP，主要的公开问题是寻找非交换群 HSP 的有效量子算法。

二面体群和对称群是两种结构最简单的非交换群，但 DHSP 和 SHSP 都未能得到有效解决。目前，Kuperberg 的亚指数级量子算法及其改进算法是解决 DHSP 最好的量子算法，而量子 Fourier 变换仍然是解决该问题的重要手段。已有研究表明，如果在群上的 Fourier 变换是有效的，且能够计算表示集合的交，则当隐含子群是正规子群时，非交换群 HSP 就能得到解决。这是交换群 HSP 的直接一般化情况，因为交换群的每个子群都是正规的[10,30]。

亚指数级 DHSP 量子算法的提出点燃了攻破基于格的唯一最短向量问题的公钥密码系统的希望，而 SHSP 的解决将会为图同构问题带来一种有效的量子算法。因此，对于非交换群 HSP，重点关注 DHSP 和 SHSP。

### 4.1　二面体群隐含子群问题

DHSP 本身就是基于非交换群 HSP 寻找有效的量子算法的天然候选者。这主要是由于：1)它是结构最简单的非交换群，相对于其他非交换群更容易解决；2)$\langle(1,d)\rangle_{0\leqslant d\leqslant N-1}$ 具有指数级数量的子群，并且子群的阶很小，经典的暴力猜测算法对其不适用[31]。二面体群是正 $N(N\geqslant 3)$ 边形的对称群，将其记作 $D_N$。若用 $\sigma$ 表示绕正 $N$ 边形中心以 $\frac{2\pi}{N}$ 为旋转角度的旋转，用 $\tau$ 表示关于正 $N$ 边形的某条对称轴的反射，则 $D_N=\langle\sigma,\tau|\sigma^N=\tau^2=I,\tau\delta\tau=\tau^{-1}\rangle$。$D_N$ 同构于 $Z_N$ 和 $Z_2$ 的半直积，记为 $D_N\cong Z_N\rtimes Z_2$，$D_N$ 中的每个元素可以表示为 $\tau^s\sigma^t$，$s\in Z_2$，$t\in Z_N$，记作$(s,t)$，其中 $Z_N=\{0,1,\cdots,N-1\}$。

1998 年，Ettinger 和 Høyer 率先开始研究 DHSP[25]，将二面体群分为旋转和反射两个子群，并分别寻找各子群的隐含子群。研究发现，只要求出反射子群的隐含子群的生成元，就足以求解 DHSP。2001 年，Murphy 将二面体群 $D_N$ 的两个子群与二面体群 $D_{N/2}$ 的同构性质引入到 DHSP 中，提出只要求解出生成元的最低有效位，就可求解 DHSP[32]。次年，Regev 发现格的唯一最短向量问题与 DHSP 之间的联系，指出如果能够有效解决 DHSP，则格的唯一最短向量问题也可得到有效求解[8]。2003 年，Kuperberg 提出第一个亚指数级 DHSP 的量子算法[33]，即 Kuperberg 算法。2004 年，Regev 将 Kuperberg 的筛分法思想(sieve)经典抽象为管道(pipeline)，将原算法的量子空间复杂度降低为多项式级，但是时间复杂度仍为亚指数级[34]。2011 年，Kuperberg 改进原算法和 Regev 的多项式空间算法，提出另一个亚指数级 DHSP 的量子算法[35]。改进算法的时间复杂度略有降低，但是在最坏的情况下，算法即为 Regev 算法。尽管这 3 个亚指数级的 DHSP 量子算法没有提供加速的经典格算法，但是它们依然是目前最重要的 DHSP 量子算法。

二面体群问题是当前 HSP 的研究热点，更是研究难点。目前已知的求解 DHSP 效果最佳的算法是亚指数级时间复杂度、多项式空间复杂度的量子算法，寻找能够有效求解 DHSP 的多项式级量子算法依然是主要的研究方向。

### 4.2　二面体群隐含子群问题与格问题的联系

DHSP 与格问题之间的联系主要表现为 DHSP 和 SVP 之间的联系。研究表明，$poly(n)$-unique SVP 可以归约为两点问题(Two Point Problem)，两点问题可以归约为二面体陪集问题(Dihedral Coset Problem，DCP)[9]。因为 DCP 存在多项式时间的有效量子算法[25]，并且陪集抽样对于 DHSP 是充分的，DHSP 可以转化为 DCP，所以如果 DHSP 利用陪集抽样的标准方法是有效可解的，那么 $f(n)$-uSVP 对于某些多项式有界函数存在有效的算法。

归约定义为：问题 $A$ 可归约到问题 $B$，表明求解问题 $A$ 可以转化为求解问题 $B$，即只要找到求解问题 $B$ 的方法，就找到了问题 $A$ 的求解方法[9]。

解决 SVP 的一种主要方法是 Regev 在文献[8]中提到的 DHSP 方法。在这种方法中，陪集态用函数来表示。在交换的情况下，Fourier 抽样，即计算 Fourier 变换和测量结果，足以解决这个问题。二面体群是非交换群，尽管尚不知怎样有效地获取二面体群的隐含子群，但是通过测量和分享子群所包含的陪集态信息可近似地看作是可交换的 HSP[10]。

下面简要介绍亚指数级 DHSP 的量子算法。假设输入尺寸为 $\log N$，即二面体群 $D_N$ 满足 $N=2^n$，$n=kl+1$，$k=O(\sqrt{n/\log n})$。$N\neq 2^n$ 的情形在文中未涉及，参见文献[33,36]。

#### 4.2.1　Kuperberg 的亚指数级量子算法

对于二面体群 $D_N$，子群为 $H=\langle\sigma\sigma^d\rangle$，DHSP 可归结为求解 $d$ 的问题。Kuperberg 提出了第一个亚指数级的 DHSP 量子算法，其计算复杂度、时间复杂度和空间复杂度都是 $2^{O(\sqrt{\log N})}=2^{O(\sqrt{n})}$。Kuperberg 算法的思想如下：

1)通过给定的 Oracle 黑箱获得 $d$ 的最低有效位。若 $d=0$，则 $f':D_{N/2}\rightarrow X$，其中 $f'(a,b)=f(a,2b)$。函数隐藏了 $D_{N/2}$ 的子群$\{(0,0),(1,d/2)\}$。若 $d=1$，则 $f'':D_{N/2}\rightarrow X$，其中$f''(a,b)=f(a,2b+1)$。函数隐藏了 $D_{N/2}$ 的子群$\{(0,0),(1,(d-1)/2)\}$。这样，就得到了 $d$ 的第一个最低有效位。

2)Oracle 黑箱调用 $f'$ 或者 $f''$。这样，就得到了 $d$ 的第二个最低有效位。

3)重复执行以上步骤，最终得到 $d$ 的所有比特位。

可得出结论：二面体群 $D_N$ 包含子群 $K_{2,0}$($d$ 为偶数)或 $K_{2,1}$($d$ 为奇数)，而且 $K_{2,0}\cong D_{N/2}$，$K_{2,1}\cong D_{N/2}$。

Kuperberg 算法的一般叙述请见文献[22,33,36]，具体算法如算法 2 所示。

**算法 2**　Kuperberg 算法

输入：HSP 的一个例子 $f:Z_N\rtimes Z_2\rightarrow X$

输出：1-qubit 量子态

Step 1　制备初态。

$$|\psi_0\rangle=\sum_{x=0}^{N-1}\sum_{y=0}^{1}|x\rangle|y\rangle|f(x,y)\rangle,x\in Z_2,y\in Z_N$$

Step 2　测量第三寄存器，则第一、第二寄存器相应地坍缩为陪集态。

$$|\psi_1\rangle=\frac{1}{2}(|x\rangle|0\rangle+|x+d \bmod N\rangle|1\rangle)$$

Step 3　对第一寄存器应用量子 Fourier 变换。

Step 4　测量第一寄存器。忽略全局相位和第一寄存器，则第二寄存器坍缩。

$$|\psi_{z_0}\rangle=\frac{1}{\sqrt{2}}(|0\rangle+e^{\frac{2\pi i z_0 d}{N}}|1\rangle)$$

Kuperberg 算法的目的在于找到 d 的最低位(最不重要位),因此最终目的是制备状态$|\psi_{2n-1}\rangle$。

Step 5 运用 Kuperberg 的筛分法(筛选出最低位相同的量子态),对$|\psi_z\rangle$不断进行"结合"操作,最终得到目标量子态。

$|\psi_{2n-1}\rangle=(|0\rangle+(-1)^d|1\rangle)$

Step 6 运用 Hadamard 门,得 $H|\psi_{2n-1}\rangle=(\frac{1+(-1)^d}{2}|0\rangle+\frac{1-(-1)^d}{2}|1\rangle)$。

Step 7 测量第二寄存器,若测得 0,则 d 为偶数;若测得 1,则 d 为奇数。

经过以上步骤,可以找到 $d$ 的最低有效位。因为 $D_N\cong D_{N/2}$,所以下一轮可以在 $D_{N/2}$ 上运用该算法。Kuperberg 算法的核心是 Kuperberg 的筛分法。

筛分法主要包括结合和筛分两个过程。

过程 1 结合操作

1)选定两个样本$|\psi_k\rangle=\frac{1}{\sqrt{2}}(|0\rangle+e^{\frac{2\pi ikd}{2^n}}|1\rangle)$,$|\psi_l\rangle=\frac{1}{\sqrt{2}}(|0\rangle+e^{\frac{2\pi ild}{2^n}}|1\rangle)$。

2)作$|\psi_k\rangle$,$|\psi_l\rangle$的张量积。

3)以第一个量子比特为控制位,应用受控非门。

4)测量第二寄存器,则第一寄存器坍缩为$|\psi_{k\pm l}\rangle$。最终的量子态是 $k+l$ 和 $k-l$ 之间无偏的随机选择(成功的概率同为 50%)。如此,便可以通过迭代过程得到最佳的量子态。

过程 2 筛分思想

1)二面体陪集采样黑箱均衡地随机选取许多量子态的新样本$|\psi_k\rangle$。

2)在每一个程序 $j(j=1,\cdots,k)$中,程序 $j$ 存储着大量的量子态$|\psi_k\rangle$样本。在过程中找出$(i-1)k+1,\cdots,ik$ 位为 0 的量子态,如果不存在,则程序 $j$ 重新生成样本;如果存在,则对新生成的样本和匹配的样本执行结合操作。将程序 $j$ 的输出作为 $j+1$ 阶段的输入。

3)重复多次,最后的程序序号为 $2^{n-1}$,即得到量子态$|\psi_{2^n-1}\rangle$。

#### 4.2.2 Regev 的多项式空间的量子算法

Regev 的多项式空间的 DHSP 量子算法将筛分法(Sieve)经典抽象为管道(Pipeline)思想,运用不同的结合操作,提出多项式空间的 DHSP 量子算法,改进了 Kuperberg 算法。该改进虽然使算法的空间复杂度从 $2^{O(\sqrt{n})}$ 降为多项式级 $O(\sqrt{n\log n})$,但是时间复杂度从 $2^{O(\sqrt{n})}$ 增加到了 $2^{O(\sqrt{n\log n})}$。

在 Regev 管道算法的管道节点中接收到 $l+4$ 个量子态时,执行结合操作(每个量子态的最低 $l$ 个量子位为 0),把 $l+4$ 个量子寄存器整合成一个大的量子寄存器,然后做张量积运算。即 Regev 的多项式空间的量子算法与 Kuperberg 算法相比,仅在步骤 5(运用 Kuperberg 的筛分法筛选出最低位相同的量子态)不同,其他步骤与 Kuperberg 的亚指数级算法一致。详细过程请参见文献[37]。

#### 4.2.3 Kuperberg 的改进 DHSP 量子算法

2011 年,Kuperberg 提出了另一个亚指数级 DHSP 的量子算法。算法的运行时间包括 $e^{O(\sqrt{\log N})}$ 的量子时间和 $e^{O(\sqrt{\log N})}$ 的经典空间,但是只需要 $O(\sqrt{\log N})$ 的量子空间。该算法在量子可寻址的经典空间中比在完全经典空间中运行得更快。可以通过两个参数扩展算法,以经典空间和经典时间来换取量子时间。在极端节省空间时,算法就变成 Regev 的多项式空间的 DHSP 量子算法。如果算法允许具有量子随机存取的经典存储器,则对于经典时间和量子时间的权衡是可行的。该算法进一步改进了所需量子比特数的渐近缩放比例。

Regev 建立了某些格问题到 DHSP 的归约。Kuperberg 算法适用于求解该归约问题,但是尚未发现这些实例的量子加速。因为 Regev 是将 DHSP 归约为 SVP,所以 DHSP 可能比相关的格问题更加困难,而且 Kuperberg 算法的主要功能是使 DHSP 与量子计算机上的格问题大致相当。Kuperberg 算法和 Regev 算法都试图有效地求解 DHSP,而不是以任何有意义的方式停留在群的表示理论上。因此,进一步探索其他隐含结构问题的非表示方法是有趣的。

### 4.3 对称群隐含子群问题

对称群是除二面体群以外,结构最简单的非交换群。对称群的定义为:当 $\Omega$ 为有限集合时,到自身的一个双射叫做 $\Omega$ 上的一个置换(Permutation)。设 $\Omega$ 含有 $n$ 个元素,此时 $\Omega$ 上的一个置换被称为 $n$ 元置换(permutation on $n$ letters),并且 $\Omega$ 上的全变换构成的群被称为 $n$ 元对称群,记作 $S_n$。

对称群隐含子群问题(SHSP)的定义为:基础群为对称群 $S_n$ 的 HSP,SHSP 的有效算法要求算法的复杂度为多项式级 $poly(n)$。由 Cayley 定理可知,任何一个群同构于一个变换群,任意一个有限群同构于一个置换群,而置换群是一种特殊的变换群,因此群 $G$ 同构于 $S_{|G|}$ 的子群。求解 $G$ 的子群 $H$ 可被看作是求解 SHSP 相应的 $S_{|G|}$ 的子群。

2007 年,Lomonaco 和 Kauffman 证明 Grover 算法可被看作是一个求解非交换群 HSP 的量子算法[38],并且可以被重新定义为求解对称群 $S_N$ 上的非交换群 HSP 的量子算法,但是标准的非交换群 HSP 的量子算法不能求解 Grover 隐含子群问题。这无疑是 HSP 的重要推广。

1997 年,Beals 给出对称群上 Fourier 变换的多项式时间的量子算法[39]。2005 年,Moore,Russell 和 Schulman 指出 Fourier 抽样技术在多项式时间内不能解决图同构问题,且它不足以用多项式次的量子测量解决问题,基于陪集态的任何量子测量都必须通过对多个陪集态使用纠缠测量来偏离原始框架[40]。2006 年,Hallgren,Moore 和 Russell 证明了当图同构问题被归约到非交换群 HSP 时,受限制的 Fourier 抽样不能解决图同构问题,但是说明多项式个副本的联合测量是必要的[41]。2013 年,Kawano 和 Sekigawa 提出了一种对称群上的量子 Fourier 变换算法[42],其速度是同类量子 Fourier 变换算法中最快的。该算法可被用于构建 HSP 的标准算法。

图同构问题是确定两个给定的图在 $n$ 个顶点标号的某个置换下是否相同。这些置换可以描述为对称群 $S_n$ 中的变换,并且在这些群上进行快速 Fourier 变换的算法是存在的。然而,图同构问题是众所周知长期悬而未决的 NP-Hard 问题,目前尚没有有效的求解算法[14],但图同构问题可以转化为 SHSP,SHSP 的有效算法将会给出图同构问题的某种解决方案,这是 SHSP 最激动人心的应用。

### 4.4　有效可解非交换群隐含子群问题

二面体群 $D_N$ 与半直积群 $Z_N \rtimes Z_2$ 的同构性质为求解 DHSP 提供了思路。尽管尚未找到解决 DHSP 的有效量子算法，但是一些半直积群的 HSP 有效可解，这类问题即为有效可解的非交换群 HSP。

1998 年，Röetteler 和 Beth 给出圈积 $Z_2^n \wr Z_2$ 的算法[26]。2003 年，Ivanyos，Magniez 和 Santha 将其扩展到一般情形，即 $G=Z_2^n \rtimes K$，并且给出通过使用经典的技术和量子的技术把非交换群情形归约为交换群情形的实例[43]。同年，Friedl，Ivanyos 和 Magniez 给出在恒定素数 $p$ 的 $Z_p^n \rtimes Z_2$ 上和带有光滑可解换位子群的群上解决 HSP 的方法[44]。该方法成功求解了 $Z_p^n$ 上的隐含转换问题（Hidden Translation Problem），并且将其进一步推广到光滑可解群上。

2004 年，Inui 和 Gall 将群 $Z_{p^n} \rtimes Z_q$ 划分为 5 种情形：群 $Z_{p^n} \rtimes Z_p$、$q$ 面体群、二面体群 $D_{2^n} \cong Z_{2^n} \rtimes Z_2$、拟二面体群 $QD_{2^n} \cong Z_{2^n} \rtimes Z_2$ 以及群 $P_{p,n} \cong Z_{p^n} \rtimes Z_p$，其中 $p$ 和 $q$ 是素数，$n$ 是整数；并且给出了求解 $Z_{p^r}^m \rtimes Z_q$ 上非交换群 HSP 的多项式时间量子算法[45-46]。同年，Moore，Rockmore 和 Russell 等给出利用非交换群 Fourier 变换的强 Fourier 抽样来求解 $q$ 面体群 HSP 的有效量子算法[48]。使用良好表示 $Z_p \rtimes Z_q$ 的基，使得在多项式时间内重构隐含子群成为可能。

2005 年，Bacon，Childs 和 Dam 通过在陪集态上执行最佳测量（Optimal Measurement）来解决 HSP[47]。对于可以表示为交换群和循环群的半直积群，证明好的测量（the Pretty Good Measurement）是最佳的。在 $Z_p^r \rtimes Z_p$ 上，对于给定的 $r$，提出非交换群 HSP 多项式时间的量子算法。特别地，当 $r=2$ 时，其为海森堡群。这种方法的特点是，能够在 $r$ 陪集态上使用纠缠测量来求解隐含子群[10]。

2007 年，Moore，Rockmore 和 Russell 等解决了 $Z_q \rtimes Z_p$，$q|(p-1)$ 上的 HSP，特别是仿射群 $A_p \cong Z_{p-1} \rtimes Z_p$[48]。

2011 年，Goncalves 和 Portugal 给出了 $Z_{p^r} \rtimes Z_{q^s}$ 上的非交换群 HSP 多项式时间的量子算法[49]，其中 $p$ 和 $q$ 是任意奇素数，$r$ 和 $s$ 是任意正整数。该算法利用交换群上的量子 Fourier 变换和归约过程将问题简化为找出循环子群的问题，以寻找隐含子群。表 1 总结了半直积群 HSP 的研究现状[31]。

表 1　半直积形式非交换群 HSP 的研究现状

Table 1　Research status of non-abelian hidden subgroup problem in semidirect form

| 群 $G$ | 说明 | 量子算法 |
|---|---|---|
| $Z_N \rtimes Z_2$ | 同构于二面体群 $D_N$，与唯一最短向量问题相关，其中 $D_{2^n}=Z_{2^n} \rtimes Z_2$ | 亚指数时间算法 |
| $Z_N^n \rtimes Z_2$ | 广义 DHSP | 未解决 |
| $Z_p \rtimes Z_{p-1}$ | 仿射群 $Aff(1,p) \cong Z_p \rtimes Z_{p-1}$ | 未解决 |
| $Z_{p^n} \rtimes Z_q$ | 5 种情形：群 $Z_{p^n} \times Z_q$、$q$ 面体群 $Z_N \rtimes Z_q$、二面体群 $D_{2^n} \cong Z_{2^n} \rtimes Z_2$、拟二面体群 $QD_{2^n} \cong Z_{2^n} \rtimes Z_2$、群 $P_{p,n} \cong Z_{p^n} \rtimes Z_p$ | 未完全解决 |
| $Z_{p^n} \rtimes Z_p$ | $Z_{p^n} \rtimes Z_q$ 中的一类 | 存在 |
| $Z_{2p^n} \rtimes Z_p$ | $p$ 为奇数，存在唯一可能的非平凡半直积群 | 存在 |
| $Z_N \rtimes Z_p$ | $N=\prod_{i=1}^{n} p_i^{r_i}$，$p \nmid (p_i-1)$，$p$ 为奇数 | 存在 |
| $Z_N \rtimes Z_{p^2}$ | $N=\prod_{i=1}^{n} p_i^{r_i}$（$r_i>4$），$p \nmid (p_i-1)$，并且 $p$ 为奇数 | 存在 |
| $Z_p^k \rtimes Z_p$ | $k=2$ 时，即 $Z_p^2 \rtimes Z_p$ 为海森堡群 | 存在 |
| $Z_{p^s}^n \rtimes Z_2$ | 黑箱求解 | 存在 |
| $Z_{p^m}^n \rtimes Z_p$ | 黑箱求解 | 存在 |
| $(Z_2^n \times Z_2^n) \rtimes Z_2$ | $G=Z_2^n \wr Z_2=(Z_2^n \times Z_2^n) \rtimes Z_2$ 圈积 | 存在 |
| $Z_p^n \rtimes Z_2$ | $p$ 是固定素数，$Z_{p^s}^n \rtimes Z_2$ 的特例 | 存在 |
| $Z_p^r \rtimes Z_p$ | $r$ 是常数，陪集态上纠缠测量 | 存在 |
| $Z_{p^r} \rtimes Z_q$ | 最佳测量 | 存在 |
| $Z_{p^r} \rtimes Z_{q^s}$ | 交换群上的量子 *Fourier* 变换和归约过程将问题简化为寻找循环子群的问题 | 存在 |
| $A \rtimes Z_N$ | $A \cong Z_{N_1} \times Z_{N_2} \times \cdots \times Z_{N_n}$ 是交换群 | 未解决 |
| $S_n$ | 对称群，与图同构问题相关；$G=S^n \wr Z_2=(S_n \times S_n) \rtimes Z_2$，圈积 | 困难性证明 |

非交换群 HSP 是 HSP 的一般推广，比交换群 HSP 具有更强的一般性以及更广泛的应用范围，主要任务是理解非交换 HSP 和相关群的表示理论。有效求解 DHSP 可能攻破基于格的唯一最短向量问题的公钥密码体制，SHSP 的解决将会为图同构带来一种有效的量子算法。二面体群隐含子群问题和对称群隐含子群问题是当前非交换群 HSP 研究的两大挑战。因此，DHSP 和 SHSP 是非交换群 HSP 研究的重点。

## 5　隐含子群问题的求解方法

尽管 DHSP 和 SHSP 都尚未得到有效求解，但是出现了许多创造性地求解 HSP 的方案及技术。量子计算机算法设计存在经典计算机算法设计所没有的本质困难性：人的直觉植根于经典世界，为设计更好的量子算法，必须“关闭”部分的经典直觉，而利用量子效应来达到期望的算法目的；设计出纯粹的量子算法并不一定真正有意义，算法必须超过所有已知的经典算法[14]。因此，这些求解 HSP 的创造性方法是具有非凡意义的尝试，对它们进行总结十分必要，以期为找到有效的量子算法提供启发。

就目前已知的研究成果而言，有限交换群 HSP 已形成相对固定的统一研究方法，而有限非交换群 HSP 的研究重点在于找到 DHSP 和 SHSP 的有效量子算法。已有的求解方法可分为标准方法和一般方法：标准方法主要基于量子 Fourier 变换来解决一般非交换群 HSP，而一般方法则针对性地解决 DHSP。

### 5.1　隐含子群问题的标准方法

几乎所有已知的非交换群 HSP 的算法使用的黑箱基本上与交换群 HSP 所使用的黑箱是相同的。因此，这种方法被称为标准方法（见算法 3）。给定有限群上 HSP 的一个例子，目标是在多项式 $\log|G|$ 步骤内计算出隐含子群 $H$ 的生成元集。

**算法 3**　标准 HSP 方法

输入：HSP 的一个例子 f：G→X

输出：子群 H≤G

Step 1　陪集采样过程获得量子态 $|gH\rangle$；

Step 2　计算量子 Fourier 变换；

Step 3　对寄存器进行测量得到目标量子态；

Step 4　由得到的测量结果计算子群 H。

在 HSP 的标准方法中，步骤 1 产生了一个随机陪集态，

其是一个随机陪集上的均衡叠加态。如果不存在陪集特征，那么取自该陪集态的测量信息足以获得 $H$ 的一个随机元素。正因为每次迭代都会产生随机陪集特征，所以必须进行多次测量[10]。

标准方法的核心过程是陪集采样。陪集采样过程的描述大致如下，详细内容请参见文献[9,36]。

1)准备基础群 $G$ 中所有元素的均衡叠加态。

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

2)在一个辅助寄存器中计算值 $f$，给出状态。

$$|\Phi\rangle=\frac{1}{|G|}\sum_{g\in G}|g\rangle|f(g)\rangle$$

3)测量 $|\Phi\rangle$ 的第二个寄存器，并且丢弃第二个寄存器。假设第二个寄存器坍缩到 $f(g)=s, s\in X, g\in G$，那么第一个寄存器坍缩为陪集态。

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

4)多次重复该过程，直到获得充分的样本。

综上，HSP 可以归约为从这些陪集样本中寻找子群 $H$ 的问题。

若一个群是交换群，量子 Fourier 变换把一个陪集态转换成一个 Fourier 变换的子群态 $|H\rangle$，并伴随一些与陪集相关的相位，这些相位有规范的并且不改变结果的概率分布。因此，这个问题可被归结为对一个子群 Fourier 变换的理解，并且这仅仅是一个群 $G$ 中具有特征$\hat{G}$的子群$\hat{H}$，多项式多次样本统计为$\hat{H}$提供了一组生成元，并且通过这些信息能够有效地采用经典计算产生出 $H$ 的生成元集。若基础群不是有限群或交换群，那么算法将变得更复杂。必须将有限近似法用于群 $G$ 以及函数的求值过程。例如，在原始的群元素上产生一个叠加态是不可能的。若要使用一个有限群和有限群上的 Fourier 变换，它必须满足：所产生的结果分布有足够多的子群信息，且这个过程能被有效计算[10]。

### 5.2 隐含子群问题的一般方法

有限群上的 Fourier 抽样是交换群情形下的自然延伸。对于非交换群 HSP，相关群的性质决定了采用标准算法能否得到足够的信息来解决问题。即便如此，用 Fourier 抽样样本来重构子群，可能也是难于计算的。已有的研究表明，只要能确定隐含子群是平凡的还是二阶的，陪集态就能拥有足够的信息来找出子群，或约束为一个更简单的问题[10]。在此基础上，文献[51]证明，如果一个酉变换能够以任何方式将陪集空间和正交空间的基映射到标准基，则酉变换可以用于求解密度恒大于 1 的随机子集和，而 DHSP 可归约到密度大于 1 的随机子集和。

非交换群 HSP 的主要任务是理解非交换 HSP 和相关群的表示理论，以期找到非交换群 HSP 的有效量子算法。DHSP 是结构最为简单的非交换群 HSP，有理由相信 DHSP 比其他的非交换群 HSP 更容易解决。文献[31]总结了许多求解 DHSP 的方法，包括枚举法、Fourier 抽样、商归约、DCP 归约、群归约、Sieve、Pipeline、最佳测量、弱 Fourier 抽样、强 Fourier 抽样、Oracle 值的叠加。

1982 年，Woottres 和 Zurek 首次提出量子不可克隆定理，并证明无法精确克隆纯态。1996 年，Barnum 等证明无法精确克隆混合态。“量子不可克隆定理”成为量子计算机研究的重要障碍。虽然无法做到精确复制，但是可以独辟蹊径，近似量子克隆或概率量子克隆。文献[37]利用概率量子克隆对 DHSP 展开研究，为成功解决 DHSP 提供了新思路。

文献[52]利用格基规约方法改进了文献[35]提出的算法，但是时间复杂度仍然为亚指数级。总而言之，能够有效解决非交换群 HSP 的方法还有待进一步探索。

值得一提的是，文献[53]给出了 HSP 量子算法的完全图解法，尝试利用高级图示法来研究 HSP，成功证明了交换群 HSP 协议的准确性，并且获得了能够解决特定无限交换群 HSP 的协议。

## 6 一般隐含子群问题

如果一个群除了单位元和其本身以外不存在其他的正规子群，那么称该群是单群(Simple Group)。可将有限单群比喻为搭成有限群的“积木块”，它是有限群结构的基石。有限单群分为四大类：素数 $p$ 阶循环群 $Z_p$、$n\geqslant 5$ 的交错群 $A_n$、李型单群(共 16 族)和 26 个散在的单群。对于一个任意的有限群，组成列是群的子群序列，即 $\{1\}=H_0\lhd H_1\lhd H_2\lhd\cdots\lhd H_n\lhd G$。每个 $H_i$ 是 $H_{i+1}$ 的极大正规子群。整数 $n\approx O(\log|G|)$ 为组成长度。

文献[31]详细介绍了一般 HSP，并给出了一般 HSP 的解决方案以及可能的算法。其中提出了两个一般 HSP 的解决方案：1)如果存在单群 HSP 的有效量子算法，那么一般 HSP 存在解决方案；2)如果对于非单群和正规子群 $\{1\}\subsetneq N\subsetneq G$ 上的 HSP 存在建立 $G/N$ 上的多项式时间 Oracles 函数 $\overline{f}$ 和 $f_{H\cap N}$ 的方法(其中 $N$ 隐含了子群 $\overline{H}$ 和 $H\cap N$)，那么一般 HSP 也存在解决方案。这两个一般 HSP 的解决方案衍生了两个研究方向，即解决单群 HSP 和寻找归约方法。一般 HSP 的可能算法如算法 4 所示。

**算法 4** 一般 HSP 的可能算法

输入：群 G 和 Oracle f:G→X

输出：子群 H≤G

Step 1 若至多使用 k 次陪集测量来确定 H=G 是否成立，且成功概率至少为 $1-2^{-k}$，则返回 G。

Step 2 若存在 G 上的有效 HSP 算法，则执行算法并返回找到的子群 H。

Step 3 若 G 是单群，则确定包含 H 的极大子群 G′，并且使用 G′来运用子群归约法。递归地调用算法并返回 H。

Step 4 运用弱 Fourier 抽样来确定 G 的极大正规子群 H′(H′⊆H)。若 H′是非平凡的，则将 H′运用于商群归约法。递归地调用算法并返回 H。

Step 5 找到一种使用正规子群 N({1}⊊N⊊G)来归约问题的方法。递归地调用算法并返回 H。

HSP 最初是由研究量子 Fourier 变换发展而来的，之后许多学者将量子算法推广到 HSP，这使得 HSP 获得了极大的发展。从群结构的角度来看，HSP 的发展主线是“有限循环群－有限交换群－有限非交换群－无限群”。对于特定情形下的 HSP，量子算法与 HSP 联系紧密，为一些具体的难题

提供了解决方案，甚至产生了一些具有重要意义的应用，如许多重要的数域问题、唯一最短向量问题、图同构问题等。而从研究的角度来看，主要是从特例到一般性的推广，推广已知的量子算法以探索新的量子算法。其他相关的综述文章请见文献[31，36，54]。

**结束语**　本文详细阐述了隐含子群问题的研究现状。目前，国内针对隐含子群问题展开研究的个人或团队比较少；国外对隐含子群问题的研究比较深刻，范围也比较广。交换群隐含子群问题已经形成了固定的模式，因此隐含子群问题的研究已经从交换群的研究转向非交换群的研究。目前的研究重点在于二面体群、对称群等非交换群隐含子群问题，而且研究范围呈不断扩展的趋势。隐含子群问题是今后量子计算领域一个重要的研究难点。

正因为隐含子群问题的研究仍然非常困难，所以我们希望本文能够通过对隐含子群问题的简单介绍吸引更多研究者的注意。下面列出一些可供参考的未来研究方向。

1）进一步扩展隐含子群问题依托的基础群，如非 Abel 群中结构较为复杂的群、有限 P 群中的某些群等。

2）研究一些已知的尚未解决或尚未完全解决的基于特定群特征的隐含子群问题，如 DHSP、SHSP、拟 DHSP、半直积群$A \rtimes Z_N$的 HSP、P 群 HSP、幂零群 HSP、可解群 HSP、交错群 $A_n$ 的 HSP、圈积 HSP、仿射 HSP、李型群 HSP、单群 HSP 以及一般 HSP 等。

3）将 Grover 算法推广到非交换群的隐含子群问题还存在一些问题。

4）Quantum Walk 与 Grover 算法之间的关系以及在 Grover 算法推广到隐含子群问题的前提下，Quantum Walk 和隐含子群问题之间的关系。

5）对解决二面体群和对称群等非 Abel 群的隐含子群问题的方法的探索，如弱/强傅里叶抽样、二面体陪集抽样、量子 Oracle 方法、归约方法、概率克隆机等。

6）在二面体群隐含子群问题和格的唯一最短向量之间的联系的基础上，进一步探索隐含子群问题和基于格的密码体制之间的关系。

7）物理系统及现象具有“对称性”，数学中的群论是研究有某些对称性系统和现象的最适宜的有力工具。隐含子群问题就是量子计算在数学群结构上的推广，因此充分利用量子计算的物理性质和问题本身特殊的数学结构，探索快速的量子算法是今后的工作。

## 参 考 文 献


[1] DIFFIE W，HELLMAN M E. New directions in cryptography [J]. IEEE Transactions on Information Theory，1976，22(6)：644-654.

[2] RIVEST R L，SHAMIR A，ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the Acm，1978，26(2)：96-99.

[3] ELGAMAL T. A Public-Key Cryptosystem and Signature Scheme Based on Discrete Logarithms[J]. IEEE Transactions on Information Theory，1985，31(4)：469-472.

[4] MILLER V S. Use of Elliptic Curves in Cryptography[M]// Advances in Cryptology-CRYPTO'85 Proceedings. Springer Berlin Heidelberg，1986：417-426.

[5] SHOR P W. Algorithms for Quantum Computation：Discrete Log and Factoring[C]// Proceedings of the 35th Symposium on Foundations of Computer Science. 1994：124-134.

[6] GROVER L K. A fast quantum mechanical algorithm for database search[C]// ACM Symposium on the Theory of Computing. 1996：212-219.

[7] WANG H F. Theoretical study on grover quantum search algorithm[D]. Harbin：Harbin Institute of Technology，2010.（in Chinese）
王洪福. Grover 量子搜索算法理论研究[D]. 哈尔滨：哈尔滨工业大学，2010.

[8] REGEV O. Quantum computation and lattice problems[C]// Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science. 2002：520-529.

[9] BRIGHT C. From the Shortest Vector Problem to the Dihedral Hidden Subgroup Problem[J/OL]. https：//cs. uwaterloo. ca/~cbright/reports/cs667proj. pdf.

[10] BERNSTEIN D J，BUCHMANN J，DAHMEN E. 抗量子计算密码[M]. 张焕国，王后珍，杨昌，等译. 北京：清华大学出版社，2015.

[11] DEUTSCH D. Quantum theory，the Church-Turing principle and the universal quantum computer[J]. Proceedings of the Royal Society of London A，1985，400(1818)：97-117.

[12] SIMON D R. On the power of quantum computation[C]// Symposium on Foundations of Computer Science. IEEE Computer Society，1994：116-123.

[13] KITAEV A Y. Quantum measurements and the Abelian stabilizer problem[OL]. https：//arxiv. org/abs/quant-ph/9511026.

[14] NIELSEN M A，CHUANG I L. 量子计算和量子信息（一）--量子计算部分[M]. 赵千川，译. 北京：清华大学出版社，2004.

[15] DAN B，LIPTON R J. Quantum Cryptanalysis of Hidden Linear Functions[C]// International Cryptology Conference on Advances in Cryptology. Springer-Verlag，1995：424-437.

[16] BRASSARD G，HØYER P. An Exact Quantum Polynomial-Time Algorithm for Simon's Problem[C]// Israel Symposium on the Theory of Computing Systems. IEEE Computer Society，1997：12.

[17] JOZSA R. Quantum algorithms and the Fourier transform[C]// Proceedings of the Royal Society of London A：Mathematical，Physical and Engineering Sciences. 1997：323-337.

[18] JOZSA R. Quantum Factoring. Discrete Logarithms，and the Hidden Subgroup Problem[J]. Computing in Science & Engineering，2001，3(2)：34-43.

[19] MOSCA M. Quantum computer algorithms[D]. Oxford：University of Oxford，1999.

[20] MOSCA M，EKERT A. The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer[M]// Quantum Computing and Quantum Communications. Springer Berlin Heidelberg，1999：174-188.

[21] CHEUNG K K H，MOSCA M. Decomposing Finite Abelian Groups[J]. Quantum Information & Computation，2001，1(3)：26-32.

[22] SUN J. Dihedral Hidden Subgroup problem Based on Quantum

Computing Algorithms[D]. Nanjing:Nanjing University of Aeronautics and Astronautics,2012. (in Chinese)
孙静. 基于量子计算的二面体群隐含子群问题研究[D]. 南京:南京航空航天大学,2012.

[23] EKERT A,JOZSA R. Quantum Algorithms:Entanglement Enhanced Information Processing[J]. Philosophical Transactions Mathematical Physical & Engineering Sciences,1998,356(1743):1769-1782.

[24] CLEVE R. The query omplexity of order-finding[C]// 15th Annual IEEE Conference on Computational Complexity. IEEE,2000:54-59.

[25] ETTINGER M,HØYER P. On Quantum Algorithms for Noncommutative Hidden Subgroups[J]. Advances in Applied Mathematics,1998,25(3):239-251.

[26] RÖETTELER M,BETH T. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups[OL]. https://arxiv.org/abs/quant-ph/9812070.

[27] PÜSCHEL M,RÖTTELER M,BETH T. Fast Quantum Fourier Transforms for a Class of Non-abelian Groups[J]. Transactions of the American Mathematical Society,1999,362(2):1009-1045.

[28] BEALS R,BUHRMAN H,CLEVE R,et al. Quantum Lower Bounds by Polynomials[C]// Symposium on Foundations of Computer Science. IEEE Computer Society,1998:352.

[29] ETTINGER M,HOYER P,KNILL E. Hidden Subgroup States are Almost Orthogonal[OL]. https://arxiv.org/abs/quant-ph/9901034.

[30] BERNSTEIN D J,BUCHMANN J,DAHMEN E. Post Quantum Cryptography[M]. Berlin:Springer Berlin Heidelberg,2008.

[31] WANG F. The Hidden Subgroup Problem[OL]. https://arxiv.org/abs/1008.0010.

[32] MURPHY J N. Analysing the quantum fourier transform for finite groups through the hidden subgroup problem[D]. Québec:McGill University,2001.

[33] KUPERBERG G. A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem[J]. Siam Journal on Computing,2003,35(1):170-188.

[34] REGEV O. A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space[J]. Proceedings of Annual Symposium on the Foundations of Computer Science,2004,64(1):124-134.

[35] KUPERBERG G. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem[OL]. https://arxiv.org/abs/1112.3333.

[36] KOBAYASHI H,GALL F L. Dihedral Hidden Subgroup Problem:A Survey(Quantum Computation and Information)[J]. Information & Media Technologies,2006,1(10):470-477.

[37] JIN G L,YUAN J B. Quantum Cloning-based Quantum Algorithm for Dihedral Hidden Subgroup Problem[J]. Computer Science,2014,41(8):183-185. (in Chinese)
金广龙,袁家斌. 基于量子克隆的二面体群隐含子群问题量子算法的研究[J]. 计算机科学,2014,41(8):183-185.

[38] LOMONACO S J,KAUFFMAN L H. Is Grover's Algorithm a Quantum Hidden Subgroup Algorithm? [J]. Quantum Information Processing,2007,6(6):461-476.

[39] BEALS R. Quantum computation of Fourier transforms over symmetric groups[C]// Twenty-Ninth ACM Symposium on the Theory of Computing. 1997:48-53.

[40] MOORE C,RUSSELL A,SCHULMAN L J. The Symmetric Group Defies Strong Fourier Sampling[C]// IEEE Symposium on Foundations of Computer Science. IEEE Computer Society,2005:479-490.

[41] HALLGREN S,MOORE C,RUSSELL A,et al. Limitations of quantum coset states for graph isomorphism[C]// ACM Symposium on Theory of Computing. Seattle,Wa,USA,2006:604-617.

[42] KAWANO Y,SEKIGAWA H. Quantum fourier transform over symmetric groups[C]// International Symposium on Symbolic and Algebraic Computation. ACM,2013:227-234.

[43] IVANYOS G,MAGNIEZ F,SANTHA M. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem[J]. International Journal of Foundations of Computer Science,2003,14(5):723-739.

[44] FRIEDL K,IVANYOS G,MAGNIEZ F,et al. Hidden translation and orbit coset in quantum computing[C]// Proceedings of the thirty-fifth annual ACM symposium on Theory of computing. ACM,2003:1-9.

[45] INUI Y,GALL F L,et al. Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups[J]. Quantum Information & Computation,2004,7(5):559-570.

[46] MOORE C,ROCKMORE D,RUSSELL A,et al. The power of basis selection in Fourier sampling:Hidden subgroup problems in affine groups[C]// Fifteenth Acm-Siam Symposium on Discrete Algorithms(SODA 2004). New Orleans,Louisiana,USA,2004:1113-1122.

[47] BACON D,CHILDS A M,DAM W V. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups[C]// IEEE Symposium on Foundations of Computer Science,2005(FOCS 2005). IEEE Xplore,2005:469-478.

[48] MOORE C,ROCKMORE D,RUSSELL A,et al. The power of strong Fourier sampling:Quantum algorithms for affine groups and hidden shifts[J]. SIAM Journal on Computing,2007,37(3):938-958.

[49] GONCALVES D N,PORTUGAL R. Solution to the Hidden Subgroup Problem for a Class of Noncommutative Groups[OL]. https://arxiv.org/abs/1104.1361.

[50] CHIA N H,HALLGREN S. How hard is deciding trivial versus nontrivial in the dihedral coset problem? [OL]. https://arxiv.org/abs/1608.02003.

[51] LI F,BAO W,FU X. A quantum algorithm for the dihedral hidden subgroup problem based on lattice basis reduction algorithm[J]. Chinese Science Bulletin,2014,59(21):2552-2557.

[52] GOGIOSO S,KISSINGER A. Fully graphical treatment of the quantum algorithm for the Hidden Subgroup Problem[OL]. https://arxiv.org/abs/1701.08669.

[53] CHILDS A M. Lecture notes on quantum algorithms[OL]. https://www.cs.umd.edu/~amchilds/qa.