基于两次量子搜索的K子集和问题求解

叶天语，吴恒，甘志刚
（浙江工商大学信息与电子工程学院，浙江 杭州 310018）

摘　要：针对K子集和问题，提出了一种基于两次量子搜索的高效量子算法。第一次量子搜索通过变异Grover算子生成包含所有元素个数为K的子集的量子叠加态；具体地，首先通过Oracle算子进行相位翻转标记所有含K个元素的子集，然后通过扩散算子放大标记的目标子集的概率幅值。第二次量子搜索则通过另一个变异Grover算子从所有元素个数为K的子集中找到K个元素和等于目标值的子集；具体地，首先通过特定的和校验Oracle算子标记所有的元素和等于目标值且只含K个元素的子集，然后通过扩散算子放大标记子集的概率幅值。仿真实验结果表明，所提方法准确率大于或等于89%，较现有方法准确率更高。

关键词：K子集和问题；Grover量子搜索算法；布尔可满足性问题；量子线路
中图分类号：TP301.6
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025132

Solving the K-subset summation problem based on twice quantum searching

YE Tianyu, WU Heng, GAN Zhigang
College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

Abstract: An efficient quantum algorithm based on twice quantum searching was proposed to solve the K-subset summation problem. In the first quantum searching, a varied Grover operator was utilized to generate the quantum superposition containing all subsets of K elements. Specifically, an Oracle operator was used to accomplish the phase flip to mark all subsets of K elements, followed by a diffusion operator for amplifying the probability amplitudes of marked target subsets. In the second quantum searching, another varied Grover operator was employed to find the subsets whose summation of K elements equalled to the target value from all subsets of K elements. In detail, a specially designed sum-checking Oracle operator was used to mark all subsets of K elements whose summation of K elements equalled to the target value, followed by a diffusion operator for amplifying the probability amplitudes of marked subsets. Simulation experimental results turn out that the proposed method achieves an accuracy of no less than 89%, which is higher than that of existing methods.

Keywords: K-subset summation problem, Grover quantum searching algorithm, Boolean satisfiability problem, quantum circuit

0　引言

子集和问题[1]是计算机科学中一个经典的非确定性多项式（NP, nondeterministic polynominal）完全问题，被广泛应用于密码学、资源分配和组合优化等领域。子集和问题在理论上具有重要的研究价值，但由于其计算复杂度随问题规模呈指数级增

收稿日期：2025–03–31；**修回日期：**2025–07–10
通信作者：叶天语，yetianyu@zjgsu.edu.cn
基金项目：国家自然科学基金资助项目（No.62071430）
Foundation Item：The National Natural Science Foundation of China (No.62071430)

长，传统的经典算法在处理大规模子集和问题时会面临巨大的挑战。

量子计算作为一门新兴的计算技术，正在引领计算机科学的变革，在航空、金融等多个行业均已出现了实际应用[2-3]。与传统计算机依赖于经典比特运算不同，量子计算利用量子力学的基本原理，通过量子比特运算来实现信息的存储和处理。量子比特具有叠加性和纠缠性等特性，使量子计算能够在某些特定问题上展现出远超经典计算的潜力，如因子分解、组合优化等问题。例如，HHL（Harrow-Hassidim-Lloyd）算法[4]、量子近似优化算法（QAOA, quantum approximate optimization algorithm）[5]和量子退火算法[6]已经在线性方程组求解问题、组合优化问题和经典NP问题上分别展现出超越经典算法的潜力。

近年来，Wurtz等[7]研究了变分量子算法在子集和问题上的经典最优性，发现该算法在特定输入下能够表现出超越经典算法的优势。Zheng等[8]提出了一种针对子集和问题的量子算法，该算法结合振幅放大技术显著减少了量子比特的使用并实现了平方加速。Biesner等[9]将子集和问题转化为二次无约束二进制优化问题，再利用量子退火技术去解决它。Zheng等[10]提出了一种新的基于量子伊辛模型的变分量子优化方法，该方法通过条件风险值优化策略为子集和问题提供更有效的解法。Lancellotti等[11]介绍了一种基于量子行走线路的子集和问题解决方法，并研究构建了适用于NP完全问题的通用量子线路，该方法在特定条件下比经典方法具有更快的速度。Nüblein等[12]研究了量子方法在子集和问题中的应用，提出了一种基于量子启发式方法的框架。Benoit等[13]提出了一种针对子集和问题的量子Oracle优化方法，专注于减少所需的量子比特数和量子门数。

Sato等[14]提出利用两次量子搜索去解决旅行商问题，其中第一步量子搜索高效地生成所有可行解的均匀叠加态，第二步量子搜索从第一步生成的叠加态中放大最优解，将第一步输出直接作为第二步输入以减少开销，优化路径成本。然而，由于旅行商问题的约束为路径唯一性，而K子集和问题需同时满足子集元素唯一性和有效性、子集大小固定、和等于目标值3个约束，文献[14]的第二步搜索依赖路径成本相位标记，无法直接适配子集和校验。受文献[14]的启发，本文提出一种基于两次量子搜索的高效量子算法用于解决K子集和问题。首先，为K个元素的二进制数值实现高效的编码设计。其次，第一次量子搜索使用了一种变异的Grover算子生成包含所有元素个数为K的子集的量子叠加态，保障子集中K个元素的有效性和唯一性；具体地，先由Oracle算子对所有含K个元素的子集施加相位翻转标记，再经扩散算子来放大目标子集的概率幅值。然后，第二次量子搜索创建了和校验Oracle，通过另一个变异Grover算子从所有元素个数为K的子集中筛选K个元素和等于目标值的子集，满足了和约束条件；具体地，该过程通过特定的和校验Oracle算子标记所有的元素和等于目标值且只含K个元素的子集，并利用扩散算子放大标记子集的概率幅值。对本文算法进行量子线路设计及仿真实验，仿真实验结果表明，本文算法在解决K子集和问题时能以大于或等于89%的概率得到目标解。

1　K子集和问题和Grover量子搜索算法

1.1　K子集和问题

K子集和问题是一个著名的NP完全问题[15]，其目标是从集合$S=\{s_1,s_2,\cdots,s_{\text{num}}\}$中找出$K$（子集的大小）个元素，使其和等于目标值，其中集合$S$中$T$的元素各不相同且$0<K\leqslant \text{num}$。例如，假设存在一个集合$S_1=\{0,1,2\}$，要从中找出2个元素使它们的和等于目标值2，这就是一个简单的2子集和问题。显然，这个2子集和问题所要找出的2个元素为0和2。

1.2　Grover量子搜索算法

Grover在1996年提出的量子搜索算法是量子计算领域的一种重要算法，利用量子并行计算来加速未排序数据库的数据搜索[16]。传统计算机在最坏情况下需$O(N)$次查询才能找到目标项，而Grover算法可将这个搜索时间复杂度降低到$O\left(\sqrt{N}\right)$，其中N为数据库的数据大小。接下来详细介绍Grover量子搜索算法[16-18]。

将初始态定义为$|\psi\rangle=\sqrt{\dfrac{N-M}{N}}|\alpha\rangle+\sqrt{\dfrac{M}{N}}|\beta\rangle$，其中，$M$为目标态的个数，$N=2^n$为所有状态的总

个数，$|\alpha\rangle$为非目标态，$|\beta\rangle$为目标态。令$\sqrt{\frac{M}{N}}=\sin\frac{\theta}{2}$，$\sqrt{\frac{N-M}{N}}=\cos\frac{\theta}{2}$，则有$|\psi\rangle=\cos\frac{\theta}{2}|\alpha\rangle+\sin\frac{\theta}{2}|\beta\rangle$。

步骤1　初始化。

制备n个量子比特都处于$|0\rangle$，对它们都施加Hadamard门变换以产生量子叠加态$|\mu\rangle$，即有

$$|0\rangle^{\otimes n}\xrightarrow{H^{\otimes n}}|\mu\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle \tag{1}$$

步骤2　Grover迭代。

定义Oracle算子为

$$\boldsymbol{O}=\boldsymbol{I}-2|\beta\rangle\langle\beta| \tag{2}$$

其作用是只将目标态的相位翻转，即存在

$$\boldsymbol{O}|\mu\rangle=\frac{1}{\sqrt{N}}\sum_{x=0\&x\neq\beta}^{N-1}|x\rangle-\frac{1}{\sqrt{N}}|\beta\rangle \tag{3}$$

定义Grover扩散算子为

$$\boldsymbol{U}=2|\mu\rangle\langle\mu|-\boldsymbol{I} \tag{4}$$

其中，$\boldsymbol{I}$为单位矩阵，则Grover迭代算子为$\boldsymbol{G}=\boldsymbol{UO}$。对$|\psi\rangle$进行一次Grover迭代后会产生

$$|\psi_1\rangle=\boldsymbol{G}|\psi\rangle=\cos\frac{3\theta}{2}|\alpha\rangle+\sin\frac{3\theta}{2}|\beta\rangle \tag{5}$$

对$|\psi\rangle$进行k次Grover迭代后会产生

$$|\psi_k\rangle=\boldsymbol{G}^k|\psi\rangle=\cos\frac{(2k+1)\theta}{2}|\alpha\rangle+\sin\frac{(2k+1)\theta}{2}|\beta\rangle \tag{6}$$

步骤3　量子测量。

每次Grover迭代都会增加目标项的概率幅度。在经过大约$\left\lfloor\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rfloor$次Grover迭代后，对量子态进行$\{|0\rangle,|1\rangle,\cdots,|N-1\rangle\}$基测量，可得到目标项。

2　基于两次量子搜索的K子集和问题求解算法

假设集合$\{s_1,s_2,\cdots,s_{\text{num}}\}$的元素各不相同，且其数值最大的元素为$s_{\max}$。为从集合$S$中找出$K$个元素使其和等于目标值$T$，其中$0<K\leqslant\text{num}$，本文提出基于两次量子搜索的K子集和问题求解算法，该求解算法的量子线路如图1所示。

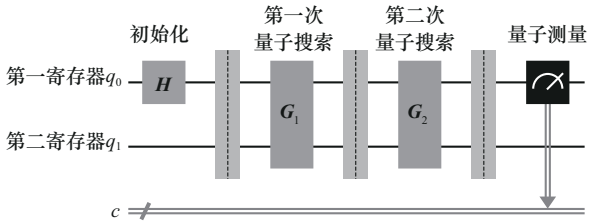

图1　基于两次量子搜索的K子集和问题求解算法的量子线路

步骤1　初始化。

制备n'个量子比特都处于$|0\rangle$，对它们都施加Hadamard门变换以产生叠加态$|\psi_0\rangle=|+\rangle^{\otimes n'}$，其中$n'=Km=K\lceil\text{lb}(s_{\max}+1)\rceil$。

步骤2　第一次量子搜索。

$\boldsymbol{G}_1$的量子线路如图2所示，$\boldsymbol{G}_1$是第一次量子搜索的变异Grover算子，即存在

$$\boldsymbol{G}_1=\boldsymbol{D}_1\boldsymbol{R}_1 \tag{7}$$

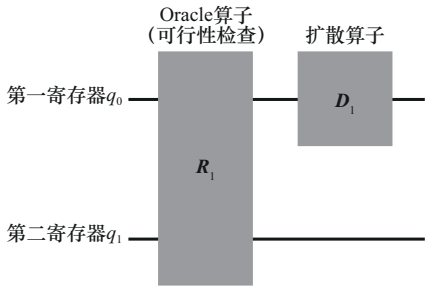

图2　$\boldsymbol{G}_1$的量子线路

其作用是生成包含所有元素个数为K的子集的量子叠加态。其中，$\boldsymbol{R}_1$为第一次量子搜索的Oracle算子，被定义为

$$\boldsymbol{R}_1=\boldsymbol{I}-2\sum_{x'}|x'\rangle\langle x'| \tag{8}$$

其作用是利用相位翻转来标记所有含K个元素的子集，即存在

$$\boldsymbol{R}_1|x\rangle=\begin{cases}-|x\rangle, x=x'\\ |x\rangle, x\neq x'\end{cases} \tag{9}$$

其中，x'为S的含K个元素子集中所有元素的二进制表示；$\boldsymbol{D}_1$是第一次量子搜索的扩散算子，被定义为

$$\boldsymbol{D}_1=2|\psi_0\rangle\langle\psi_0|-\boldsymbol{I} \tag{10}$$

其作用是放大标记的目标子集的概率幅值。

步骤3　第二次量子搜索。

$\boldsymbol{G}_2$的量子线路如图3所示，$\boldsymbol{G}_2$是第二次量子搜索的变异Grover算子，即存在

$$\boldsymbol{G}_2 = \boldsymbol{D}_2\boldsymbol{R}_2 \tag{11}$$

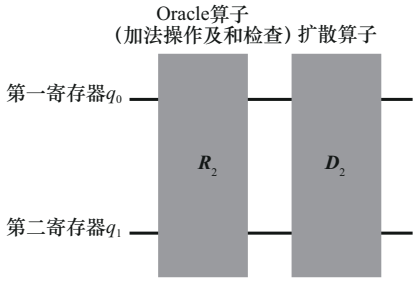

图 3　$\boldsymbol{G}_2$的量子线路

其作用是找到S的元素和等于T且元素个数为K的子集。其中，$\boldsymbol{R}_2$为第二次量子搜索的Oracle算子，被定义为

$$\boldsymbol{R}_2 = \boldsymbol{I} - 2\sum_{x''}|x''\rangle\langle x''| \tag{12}$$

其作用是标记所有的元素和等于T且只含K个元素的子集，即存在

$$\boldsymbol{R}_2|x\rangle = \begin{cases} -|x\rangle, x = x'' \\ |x\rangle, x \neq x'' \end{cases} \tag{13}$$

其中，x''为和等于T的K个元素的二进制表示；$\boldsymbol{D}_2$是第二次量子搜索的扩散算子，被定义为

$$\boldsymbol{D}_2 = 2\boldsymbol{G}_1|\psi_0\rangle\langle\psi_0|\boldsymbol{G}_1{}^{\dagger} - \boldsymbol{I} \tag{14}$$

其作用是放大标记子集的概率幅值。

步骤4　量子测量。

经过两次量子搜索后，对量子态进行$\{|0\rangle,|1\rangle,\cdots,|2^{n'}-1\rangle\}$基测量，可得到标记子集。

3　线路设计

首先将本文算法所需实现的功能转换成对应的布尔操作，然后使用对应于不同布尔操作的不同量子门进行线路设计[19-20]。

3.1　布尔可满足性问题

布尔可满足性问题[21]是计算机科学中的一个经典问题，也是第一个被证明出来的NP完全问题。布尔可满足性问题的目标是根据给定的布尔公式判断是否存在一种使公式为真的变量赋值。例如，对于$a \wedge b = 1$这个布尔公式，当a和b都为1时这个公式才为真，其中∧表示“与”操作。

3.2　K子集和问题转换成布尔可满足性问题

1) 元素有效性转换成布尔可满足性问题

对集合进行量子编码有时会额外生成不在集合中的元素，为了减少计算成本，需将其剔除。因此，需将在集合中的元素和额外生成的不在集合中的元素进行区分，可将这种区分转化为布尔可满足性问题进行实现。

2) 元素独特性转换成布尔可满足性问题

假设集合中的元素都是不相同的，那么需要对所有的元素都进行两两比较来确保元素的独特性。元素的独特性可用“异或”（即⊕）来验证。例如，若$S' = \{a,b,c\}$且S'中的元素均为单比特，那么$a \oplus b = 1$表示a和b不相同，单比特的独特性转换为布尔可满足性问题真值表如表1所示，$(a \oplus b) \wedge (a \oplus c) \wedge (b \oplus c) = 1$表示集合$S'$中没有重复的元素；若$S' = \{a,b,c\}$的元素均为双比特且用$a_1a_2$、$b_1b_2$和$c_1c_2$分别表示$a$、$b$和$c$，那么$a \oplus b = (a_1 \oplus b_1) \vee (a_2 \oplus b_2) = 1$表示$a$与$b$不相同，$((a_1 \oplus b_1) \vee (a_2 \oplus b_2)) \wedge ((a_1 \oplus c_1) \vee (a_2 \oplus c_2)) \wedge ((b_1 \oplus c_1) \vee (b_2 \oplus c_2)) = 1$表示集合$S'$中没有重复的元素，其中∨表示“或”操作。因为异或不属于基本布尔操作，所以需将异或转换为基本布尔操作。例如，$a \oplus b = (\bar{a} \wedge b) \vee (a \wedge \bar{b})$，$a \oplus b \oplus c = (a \wedge \bar{b} \wedge \bar{c}) \vee (\bar{a} \wedge b \wedge \bar{c}) \vee (\bar{a} \wedge \bar{b} \wedge c) \vee (a \wedge b \wedge c)$。

表1　单比特的独特性转换为布尔可满足性问题真值表

a	b	输出
0	0	0
0	1	1
1	0	1
1	1	0

3)元素求和转换成布尔可满足性问题

单比特全加器的输入为2个单比特，它的输出为1个和位及1个进位。表2为单比特全加器真值表，其中输出为$C_{\text{in}}P$。和位P的逻辑表达式为

$$P = a \oplus b \tag{15}$$

进位C_{in}的逻辑表达式为

$$C_{\text{in}} = a \wedge b \tag{16}$$

双比特全加器的输入为2个双比特，对它们进行求和需要2个和位及2个进位；双比特全加器的输出为2个和位及1个最终的进位。表3为双比特全加器真值表，其中输出为$C_{\text{in2}}P_2P_1$。第一个和位P_1的逻辑表达式为

表2 单比特全加器真值表

a	b	P	C_{in}	输出
0	0	0	0	00
0	1	1	0	01
1	0	1	0	01
1	1	0	1	10

$$P_1 = a_0 \oplus b_0 \tag{17}$$

第一个进位C_{in1}的逻辑表达式为

$$C_{\text{in1}} = a_0 \wedge b_0 \tag{18}$$

第二个和位P_2的逻辑表达式为

$$P_2 = a_1 \oplus b_1 \oplus C_{\text{in1}} \tag{19}$$

第二个进位C_{in2}的逻辑表达式为

$$C_{\text{in2}} = \left(a_1 \wedge b_1\right) \vee \left(a_1 \wedge C_{\text{in1}}\right) \vee \left(b_1 \wedge C_{\text{in1}}\right) \tag{20}$$

表3 双比特全加器真值表

a_1a_0	b_1b_0	P_1	C_{in1}	P_2	C_{in2}	输出
00	00	0	0	0	0	000
00	01	1	0	0	0	001
00	10	0	0	1	0	010
00	11	1	0	1	0	011
01	01	0	1	1	0	010
01	10	1	0	1	0	011
01	11	0	1	0	1	100
10	10	0	0	0	1	100
10	11	1	0	0	1	101
11	11	0	1	1	1	110

如果全加器输入的比特位数大于2位，可参照上面的方法利用布尔关系式将元素求和转化为对应的布尔可满足性问题。

3.3 第一次量子搜索的线路设计

以$S_1=\{0,1,2\}$和$S_2=\{0,1,2,3\}$为例对本文算法进行量子线路设计。

第一次量子搜索需首先实现2种功能：一是检测元素是否存在于集合S中，可将元素有效性转换成布尔可满足性问题进行验证；二是检测是否有元素在集合S中重复出现，可将元素独特性转换成布尔可满足性问题进行验证。

当K子集和问题的集合为S_1且K为2时，初始化及$\boldsymbol{G}_1$的量子线路如图4所示。这里需用$n_1'=2\lceil \text{lb}(2+1)\rceil=4$个量子比特来表示从$S_1=\{0,1,2\}$中选择出的2个不重复的数，即$q_1q_0$和$q_3q_2$。在图4中，第一条虚线的左侧部分为初始化操作；第二条虚线的左侧部分用于确保生成的元素存在于集合中，尤其是需删除因输入为4位而在初始化阶段不可避免产生的量子态$|11\rangle$；第三条虚线的左侧部分用于确保元素的独特性；第四条虚线的左侧部分用于检测是否满足式(8)的Oracle算子的输入条件；第五条虚线的左侧部分为有效性和独特性检测的逆操作，其目的为输入量子比特进行复原；最后一条虚线的右侧部分的作用是运用式(10)的扩散算子来增加标记态的概率幅值。

当K子集和问题的集合为S_2且K为2时，初始化及$\boldsymbol{G}_1$的量子线路如图5所示。这里仍需$n_2'=2\lceil \text{lb}(3+1)\rceil=4$个量子比特来表示从$S_2=\{0,1,2,3\}$中选择出的2个不重复的数，即$q_1q_0$和$q_3q_2$。在图5中，由于初始化过程产生的所有元素均存在于$S_2$中，后续就不需要进行元素有效性验证；其他剩余部分的量子线路与图4的相似。

第一次量子搜索用到的量子比特共为$n'+a_{\text{valid}}+a_{\text{unique}}+1$个。其中，$n'=Km=K\lceil \text{lb}(s_{\max}+1)\rceil$表示

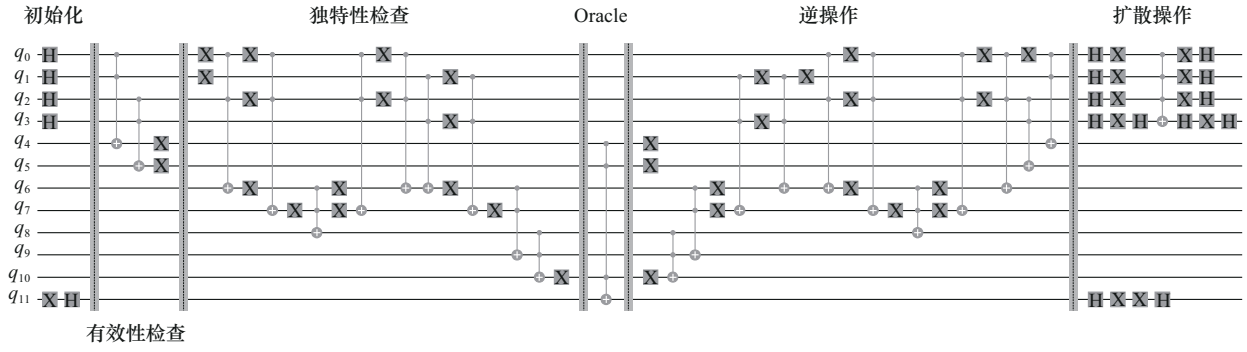

图4 当K子集和问题的集合为S_1且K为2时，初始化及$\boldsymbol{G}_1$的量子线路

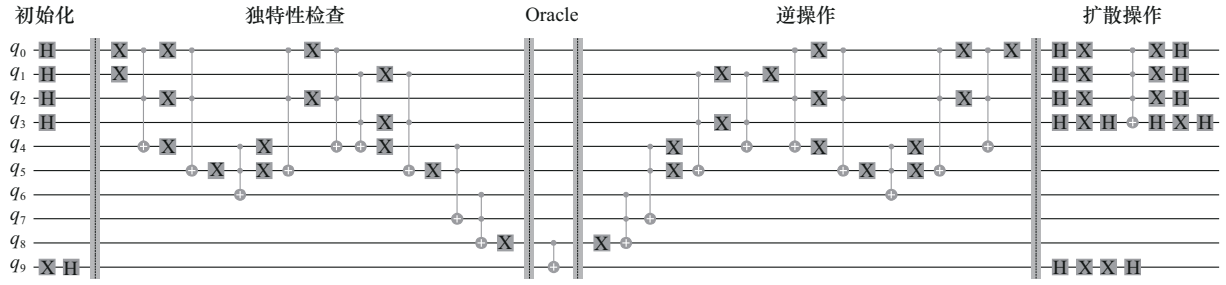

图 5　当K子集和问题的集合为S_2且K为2时,初始化及$\boldsymbol{G}_1$的量子线路

输入的量子比特数：$a_{\text{valid}}=K\left(2^m-|S|\right)=K\left(2^{\lceil \text{lb}\,(s_{\max}+1)\rceil}-|S|\right)$表示元素有效性检测所需的辅助量子比特数，$|S|$表示$S$的元素总个数；$a_{\text{unique}}=C_K^2(m+3)=C_K^2(\lceil \text{lb}\,(s_{\max}+1)\rceil+3)$表示元素重复性检测所需的量子比特数；最后的+1表示用一个辅助比特来标记满足的解的状态。

3.4　第二次量子搜索的线路设计

第二次量子搜索需首先计算K个元素的和值以及验证和值是否与目标值一致，然后提高和值为T的子集的概率。

当K子集和问题的集合为S_1、K为2且T为2时，$\boldsymbol{G}_2$的量子线路如图6所示。在图6中，第一条虚线的左侧部分表示求和操作；第二条虚线的左侧部分用于标记所有和满足目标值的量子态；第三条虚线的左侧部分为逆操作，其目的是恢复输入比特的状态；第三条虚线的右侧部分为扩散操作，其中$\boldsymbol{G}_1$的量子线路见图4，$\boldsymbol{G}_1{}^{\dagger}$为$\boldsymbol{G}_1$的厄米共轭，其量子线路如图7所示。

当K子集和问题的集合为S_2、K为2且T为3时，$\boldsymbol{G}_2$的量子线路如图8所示。在图8中，前四条虚线的左侧部分为求和操作；第五条虚线的左侧部分用于标记和满足目标值的量子态；第六条虚线的左侧部分为逆操作，用于恢复输入比特的状态；第六条虚线的右侧部分为扩散操作，其中$\boldsymbol{G}_1$的量子线路见图5，$\boldsymbol{G}_1{}^{\dagger}$为$\boldsymbol{G}_1$的厄米共轭，其量子线路如图9所示。

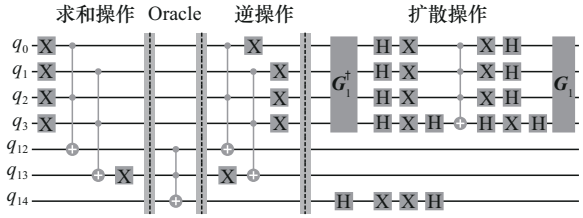

图 6　当K子集和问题的集合为S_1、K为2且T为2时,$\boldsymbol{G}_2$的量子线路

第二次量子搜索用到的量子比特共为$n'+a_{\text{valid}}+a_{\text{unique}}+a_{\text{plus}}+2$个。其中，$n'$仍表示输入的量子比特数；$\boldsymbol{D}_2$算子需用到$\boldsymbol{G}_1$，从而包含了$\boldsymbol{G}_1$中的$a_{\text{valid}}+a_{\text{unique}}+1$个辅助量子比特。当$K=1$时，和位操作不需要辅助量子比特，这时辅助量子比特数为$a_{\text{plus}}=0$；当$K>1$时，和位操作需要的辅助量子比特数为$a_{\text{plus}}=9(K-1)(m-1)+4\sum_{i=1}^{K-1}i$。最后的+1用于判断对应的每位数的数值是否相等。

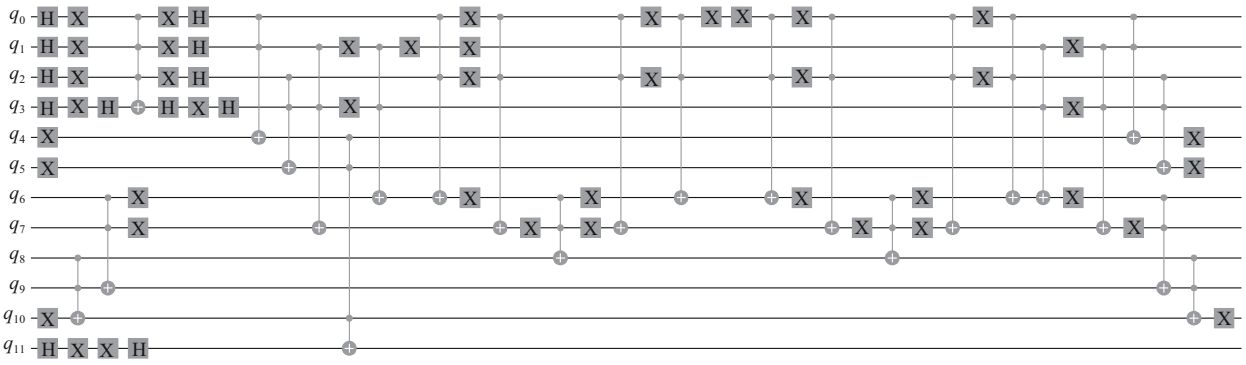

图 7　当K子集和问题的集合为S_1且K为2时,$\boldsymbol{G}_1{}^{\dagger}$的量子线路

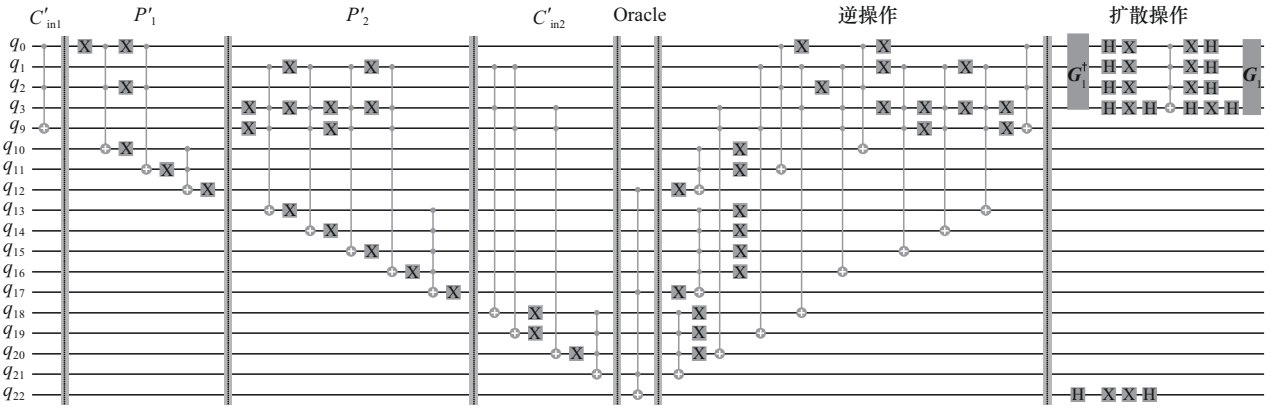

图8　当K子集和问题的集合为S_2、K为2且T为3时，$\boldsymbol{G}_2$的量子线路

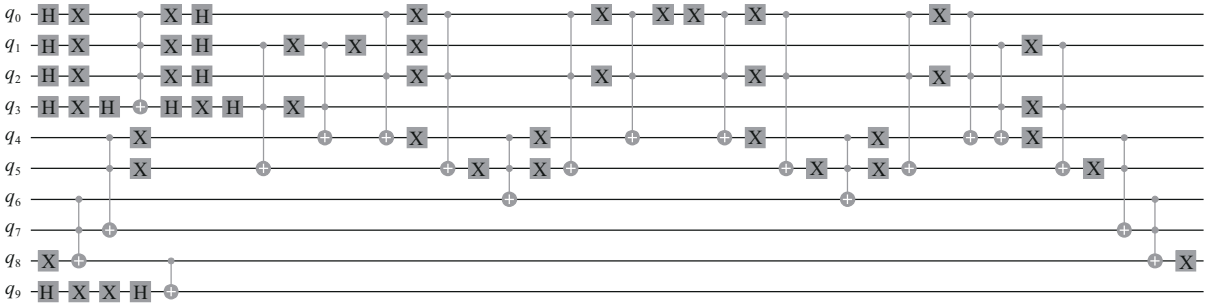

图9　当K子集和问题的集合为S_2且K为2时，$\boldsymbol{G}_1{}^{\dagger}$的量子线路

4　仿真实验结果

使用IBM Qiskit对所设计的量子线路进行仿真，以验证本文算法的性能，仿真的次数为10 240次。

从S_1中选出2个元素构成子集使子集和为2的次数分布实验结果如图10所示。从图10可以看出，子集0010和1000的次数分别为4 716和4 792，而这2个子集都是正确子集。从S_1中选出2个元素构成子集使子集和为2的概率分布实验结果如图11所示，其中实验结果准确率达到92.85%。

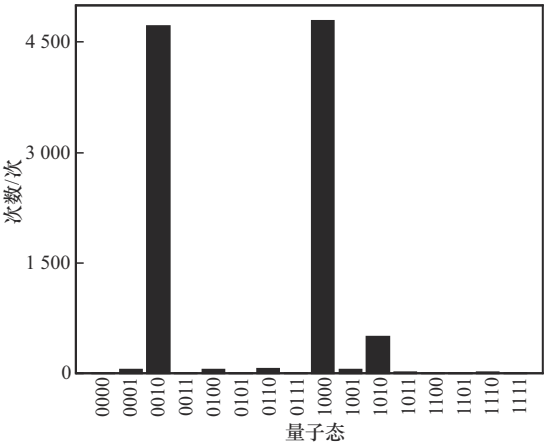

图10　从S_1中选出2个元素构成子集使子集和为2的次数分布实验结果

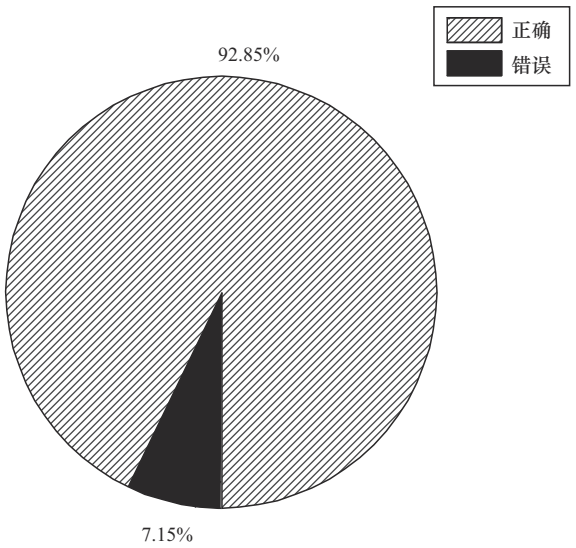

图11　从S_1中选出2个元素构成子集使子集和为2的概率分布实验结果

从S_2中选出2个元素构成子集使子集和为3的次数分布实验结果如图12所示。从图12可以看出，子集0011、0110、1001、1100的次数分别为2 241、2 352、2 258和2 310，而这些子集都是正确子集。从S_2中选出2个元素构成子集使子集和为3的概率分布实验结果如图13所示，其中实验结果准确率达到89.46%。

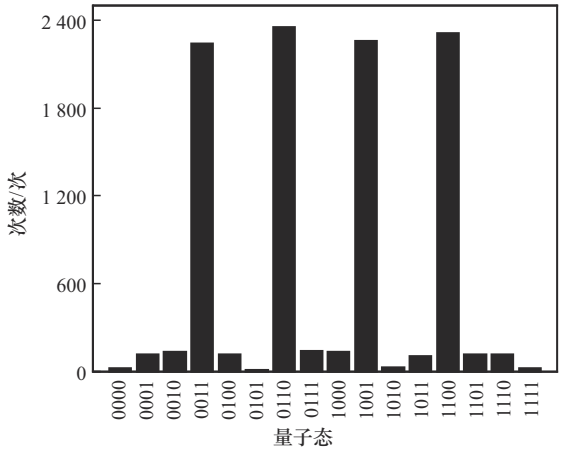

图 12　从S_2中选出2个元素构成子集使子集和为3的次数分布实验结果

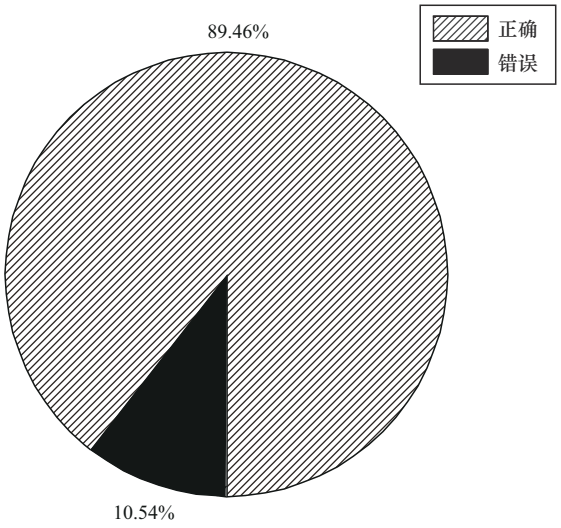

图 13　从S_2中选出2个元素构成子集使子集和为3的概率分布实验结果

当从S_1中选出2个元素构成子集使子集和为2时，本文算法与QAOA[5]和多角度量子近似优化算法（MA-QAOA, multi-angle quantum approximate optimization algorithm）[22]的实验结果准确率对比如图14所示，其中P为演化步数。图15为从S_2中选出2个元素构成子集使子集和为3时，本文算法与QAOA[5]和MA-QAOA[22]的实验结果准确率对比。从图14和图15可以看出，当P = 1~3时，本文算法比QAOA[5]和MA-QAOA[22]在实验结果准确率上表现更为优异。

虽然本文算法在解决K子集和问题时具有较高的准确率，但由于一些因素的干扰仍然会产生求解不成功的情形。首先，量子搜索算法的最优搜索次数随着问题规模增大而增大，且理论上可能不为整数，但仿真的过程中只能将搜索次数取为有限的整数，从而不可避免地影响准确率。其次，使用Qiskit对量子线路进行仿真模拟存在噪声、有限样本等不可控因素，实验结果准确率会出现小幅度的波动。

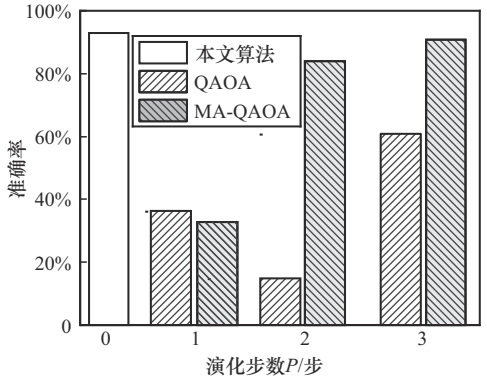

图 14　当从S_1中选出2个元素构成子集使子集和为2时，本文算法与QAOA和MA-QAOA的实验结果准确率对比

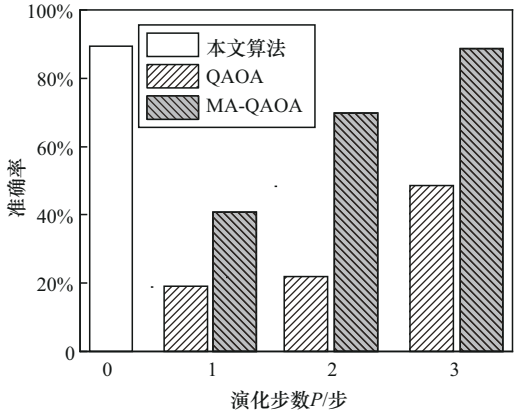

图 15　从S_2中选出2个元素构成子集使子集和为3时，本文算法与QAOA和MA-QAOA的实验结果准确率对比

5　结束语

本文提出一种基于两次量子搜索的高效量子算法，用于解决K子集和问题。第一次量子搜索采用一种变异的Grover算子生成所有元素个数为K的子集的量子叠加态，保障子集中K个元素的有效性和唯一性；具体地，先由Oracle算子对所有含有K个元素的子集施加相位翻转标记，再经扩散算子来放大目标子集的概率幅值。继而执行的第二次量子搜索创建了和校验Oracle，通过另一变异Grover算子从所有元素个数为K的子集中找到元素和等于目标值的子集，满足了和约束的条件；具体地，通过特定的和校验Oracle算子标记元素和等于目标值且只含K个元素的子集，并利用扩散算子放大标记子集的概率幅值。为本文算法设计了相应的量子线路并

进行了仿真。仿真实验结果表明，该算法在解决K子集和问题时准确率大于或等于89%。未来的研究可以进一步探索本文算法在其他NP难问题中的应用，并对量子线路进行优化设计。

参考文献：

[1] CHEN L, LIAN J Y, MAO Y C, et al. Faster algorithms for bounded knapsack and bounded subset sum via fine-grained proximity results[C]// Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA2024), New York: ACM Press, 2024:4828-4848.

[2] ABUGHANEM M. IBM quantum computers: evolution, performance, and future directions[J]. The Journal of Supercomputing, 2025, 81 (5): 687.

[3] DALEY A J, BLOCH I, KOKAIL C, et al. Practical quantum advantage in quantum simulation[J]. Nature, 2022, 607(7920): 667-676.

[4] ZHANG M, DONG L H, ZENG Y, et al. Improved circuit implementation of the HHL algorithm and its simulations on QISKIT[J]. Scientific Reports, 2022, 12: 13287.

[5] ZHOU Z Q, DU Y X, TIAN X M, et al. QAOA-in-QAOA: solving large-scale MaxCut problems on small quantum machines[J]. Physical Review Applied, 2023, 19(2): 024027.

[6] ZENG Q G, CUI X P, LIU B W, et al. Performance of quantum annealing inspired algorithms for combinatorial optimization problems[J]. Communications Physics, 2024, 7: 249.

[7] WURTZ J, LOVE P J. Classically optimal variational quantum algorithms[J]. IEEE Transactions on Quantum Engineering, 2021, 2: 3104107.

[8] ZHENG Q L, ZHU P Y, XUE S C, et al. Quantum algorithm and experimental demonstration for the subset sum problem[J]. Science China Information Sciences, 2022, 65(8): 182501.

[9] BIESNER D, GERLACH T, BAUCKHAGE C, et al. Solving subset sum problems using quantum inspired optimization algorithms with applications in auditing and financial data analysis[C]//Proceedings of the 2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA). Piscataway: IEEE Press, 2022: 903-908.

[10] ZHENG Q L, YU M M, ZHU P Y, et al. Solving the subset sum problem by the quantum Ising model with variational quantum optimization based on conditional values at risk[J]. Science China Physics, Mechanics & Astronomy, 2024, 67(8): 280311.

[11] LANCELLOTTI G, PERRIELLO S, BARENGHI A, et al. Design of a quantum walk circuit to solve the subset-sum problem[C]//Proceedings of the 61st ACM/IEEE Design Automation Conference. New York: ACM Press, 2024: 1-6.

[12] NÜBLEIN J, SCHUMAN D, BUCHER D, et al. Towards less greedy quantum coalition structure generation in induced subgraph games[C]// Proceedings of the 2024 IEEE International Conference on Quantum Computing and Engineering (QCE). Piscataway: IEEE Press, 2024: 28-33.

[13] BENOIT A, SCHWARTZ S, CYTRON R K. Optimization of a quantum subset sum oracle[J]. arXiv Preprint, arXiv: 2410.01775, 2024.

[14] SATO R, CUI G, SAITO K, et al. Two-step quantum search algorithm for solving traveling salesman problems[J]. arXiv Preprint, arXiv: 2405.07129, 2024.

[15] AMAN B, CIOBANU G. Solving subset sum and SAT problems by reaction systems[J]. Natural Computing, 2024, 23(2): 177-187.

[16] STOUDENMIRE E M, WAINTAL X. Opening the black box inside Grover's algorithm[J]. Physical Review X, 2024, 14(4): 041029.

[17] SRIVASTAVA S, PATI A K, CHAKRABARTY I, et al. Using quantum switches to mitigate noise in Grover's search algorithm[J]. Journal of Physics A: Mathematical and Theoretical, 2025, 58(10): 105304.

[18] QIU D W, LUO L, XIAO L G. Distributed Grover's algorithm[J]. Theoretical Computer Science, 2024, 993: 114461.

[19] LI G S, DING Y F, XIE Y. Tackling the qubit mapping problem for NISQ-era quantum devices[C]//Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems. New York: ACM Press, 2019: 1001-1014.

[20] LIU H, LI F K, FAN Y L. Optimizing the quantum circuit for solving Boolean equations based on Grover search algorithm[J]. Electronics, 2022, 11(15): 2467.

[21] GUO W X, ZHEN H L, LI X J, et al. Machine learning methods in solving the Boolean satisfiability problem[J].Machine Intelligence Research, 2023, 20(5): 640-655.

[22] HERRMAN R, LOTSHAW P C, OSTROWSKI J, et al. Multi-angle quantum approximate optimization algorithm[J]. Scientific Reports, 2022, 12: 6781.

[作者简介]

叶天语（1982– ），男，浙江温州人，博士，浙江工商大学教授，主要研究方向为量子信息、量子计算、量子与半量子密码等。

吴恒（2000– ），女，安徽黄山人，浙江工商大学硕士生，主要研究方向为量子计算。

甘志刚（1979– ），男，江西抚州人，博士，浙江工商大学讲师，主要研究方向为量子信息、量子计算、量子人工智能。