Quantum Algorithms of the Subset-sum Problem on a Quantum Computer

Weng-Long Chang[1*], Ting-Ting Ren[2], Mang Feng[3*], Lai Chin Lu[4], Kawuu Weicheng Lin[5] and Minyi Guo[6]

Abstract—**In this paper, quantum algorithms for solving an instance of the subset-sum problem is proposed and a NMR experiment for the simplest subset-sum problem to test our theory is also performed.**

I. Introduction

In this paper, an instance of the subset-sum problem can be implemented by our proposed quantum algorithm. By using nuclear magnetic resonance (**NMR**) technique, we perform an **NMR** experiment for the simplest subset-sum problem to test our theory.

II. Quantum Algorithms OF the Subset-sum Problem

A. Definition of the Subset-sum Problem

Assume that a finite set A is $\{a_1, \ldots, a_m\}$, where a_k is the k^{th} element for $1 \le k \le m$. **Definition 4−1** is applied to denote the subset-sum problem for any a finite set, A.

Definition 4−1: The subset-sum problem for an m-element finite set, A, is to find a subset $A^1 \subseteq A$ such that the sum of every element in A^1 is exactly b, where b is any given positive integer.

B. Computational State Space of Quantum Solutions for the Subset-sum Problem

An arbitrary state $\left|\varphi\right\rangle$ of a quantum bit is nothing else than a linearly weighted combination of the following computational basis vectors (4.1): $\left|\varphi\right\rangle = l_1 \cdot \left|0\right\rangle + l_2 \cdot \left|1\right\rangle = l_1 \cdot \begin{bmatrix}1\\0\end{bmatrix}_{2\times1} + l_2 \begin{bmatrix}0\\1\end{bmatrix}_{2\times1}$, where the weighted factors l_1 and $l_2 \in \mathbf{C}^2$ are the so-called probability amplitudes, thus they must satisfy $|\, l_1\,|^2 + |\, l_2\,|^2 = 1$.

C. Introduction of Quantum Gates for Solving the Subset-sum Problem

The **NOT** gate is a one-qubit gate and sets the only (target) bit to its negation. The **CNOT** (*controlled* **NOT**) gate is a two-qubit gate and flips the second qubit (the target qubit) if and only if the first qubit (the control qubit) is one. The **CCNOT** (*controlled-controlled*-**NOT**) gate is a three-qubit gate and flips the third qubit (the target qubit) if and only if the first qubit and second qubit (the two control qubits) are both one.

D. Constructing Quantum Networks for Solving the Subset-sum Problem

The full addition network is illustrated in Figure 4-1, and can be understood as follows:

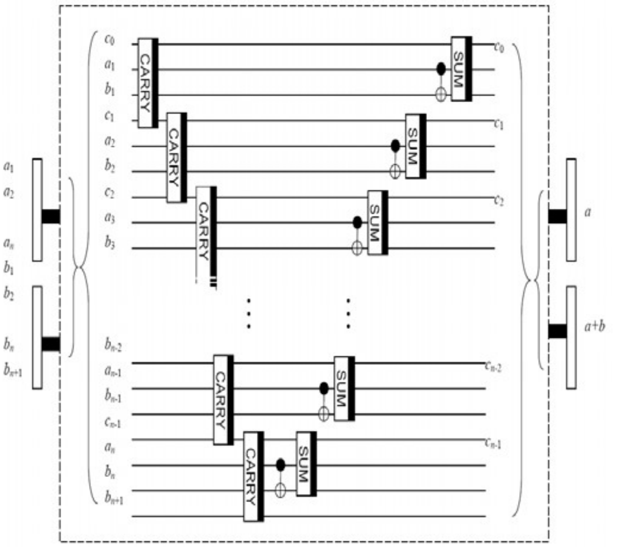


Figure 4-1: Adder network of n quantum bits.

We only reverse all these operations in Figure 4-1 in order to restore every quantum bit of the three registers to its initial state. This enables us to reuse the same registers repeatedly.

E. Quantum Algorithms of Solving the Subset-sum Problem

The following quantum algorithm is proposed as quantum implementation on a physical quantum. The notations used in **Algorithm 4-1** below have been denoted in previous subsections.

Algorithm 4-1: The quantum algorithm is to solve an instance of the subset-sum problem for any given positive integer b with a finite set A involving m elements of n bits.

(1) For an initial input $\left|\varphi_0\right\rangle = (\otimes_{p=n}^{1}\left|r_p{}^{0}\right\rangle) \otimes (\left|r_0{}^{1}\right\rangle) \otimes (\otimes_{q=n+1}^{1}\left|b_{1,q}\right\rangle) \otimes (\left|b_{n+1}{}^{0}\right\rangle) \otimes (\otimes_{j=n}^{1}\left|b_j{}^{0}\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1}{}^{1}\left|a_{k,j}{}^{0}\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1}{}^{1}\left|c_{k,j-1}{}^{0}\right\rangle) \otimes$

Weng-Long Chang is with Department of Computer Science and Information Engineering, National Kaohsiung University of Applied Sciences Kaohsiung City, Taiwan 807-78, Republic of China (e-mail: changwl@cc.kuas.edu.tw).

Mang Feng was with State Key Laboratory of Magnetic Resonance and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan, 430071, People's Republic of China (e-mail: mangfeng@wipm.ac.cn).

978-0-7695-3679-8/09 $25.00 © 2009 IEEE
DOI 10.1109/ICIE.2009.15

$(\otimes_{k=m}^{1}|e_k{}^0\rangle) \otimes (|r_{n+1}{}^0\rangle) \otimes (|1\rangle)$, 2^m possible choices of m bits (including all of the possible subsets) are $|\varphi_1\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes H^{\otimes m} \otimes I_{2\times2} \otimes H$ $|\varphi_0\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{1}|r_p{}^0\rangle) \otimes (|r_0{}^1\rangle) \otimes (\otimes_{q=n+1}^{1}|b_{1,q}\rangle) \otimes (|b_{n+1}{}^0\rangle) \otimes (\otimes_{j=n}^{1}|b_j{}^0\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|a_{k,j}{}^0\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|c_{k,j-1}{}^0\rangle) \otimes (\otimes_{k=m}^{1}(|e_k{}^0\rangle + |e_k{}^1\rangle)) \otimes (|r_{n+1}{}^0\rangle) \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$.

(2) $|\varphi_2\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} U_{k,j}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes (\otimes_{k=m}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes I_{2\times2}$ $|\varphi_1\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{1}|r_p{}^0\rangle) \otimes (|r_0{}^1\rangle) \otimes (\otimes_{q=n+1}^{1}|b_{1,q}\rangle) \otimes (|b_{n+1}{}^0\rangle) \otimes (\otimes_{j=n}^{1}|b_j{}^0\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|y_{k,j}\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|c_{k,j-1}{}^0\rangle) \otimes (\otimes_{k=m}^{1}(|e_k{}^0\rangle + |e_k{}^1\rangle)) \otimes (|r_{n+1}{}^0\rangle) \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$, where

$$U_{k,j} = \begin{cases} I_{2\times2} & \text{if } a_{k,j} = 0 \\ |a_{k,j}{}^0 \oplus (e_k^0 + e_k^1)\rangle & \text{if } a_{k,j} = 1 \end{cases}$$

and

$$y_{k,j} = \begin{cases} a_{k,j}{}^0 \\ a_{k,j}{}^0 \oplus (e_k^0 + e_k^1) \end{cases}.$$

(3) **For** $s = 1$ **to** m

(3a) $|\varphi_{s+2}\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{1} I_{2\times2}) \otimes QA \otimes (\otimes_{k=m}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes I_{2\times2}$ $|\varphi_{s+1}\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{1}|r_p{}^0\rangle) \otimes (|r_0{}^1\rangle) \otimes (\otimes_{q=n+1}^{1}|b_{1,q}\rangle) \otimes (|b_{n+1}\rangle) \otimes (\otimes_{j=n}^{1}|b_j + y_{s,j}\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|y_{k,j}\rangle) \otimes (\otimes_{k=m,\, j=n}^{s+1\;\;\;1}|c_{k,j-1}{}^0\rangle) \otimes (\otimes_{k=s,\, j=n}^{s\;\;\;1}|c_{k,j-1}\rangle) \otimes (\otimes_{k=s-1,\, j=n}^{1\;\;\;1}|c_{k,j-1}\rangle) \otimes (\otimes_{k=m}^{1}(|e_k{}^0\rangle + |e_k{}^1\rangle)) \otimes (|r_{n+1}{}^0\rangle) \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$, where QA is the quantum adder of n bits denoted in Figure 4-1, $b_{n+1} = y_{s,n}$ AND b_n AND $c_{s,n-1}$, $c_{s,j-1} = y_{s,j-1}$ AND b_{j-1} AND $c_{s,j-2}$ for $1 \le j \le n$ and $c_{k,j-1} = y_{k,j-1}$ AND b_{j-1} AND $c_{k,j-2}$ for $1 \le k \le s-1$ and $1 \le j \le n$.

EndFor

(4) $|\varphi_{m+3}\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{1} CNOT) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes (\otimes_{k=m}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes I_{2\times2}$ $|\varphi_{m+2}\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{1}|r_p{}^0\rangle) \otimes (|r_0{}^1\rangle) \otimes (\otimes_{q=n+1}^{1}|b_{1,q} \oplus b_q\rangle) \otimes (|b_{n+1}\rangle) \otimes (\otimes_{j=n}^{1}|b_j\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|y_{k,j}\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|c_{k,j-1}\rangle) \otimes (\otimes_{k=m}^{1}(|e_k{}^0\rangle + |e_k{}^1\rangle)) \otimes (|r_{n+1}{}^0\rangle) \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$, where $b_j = b_j + y_{k,j}$ and $c_{k,j-1} = y_{k,j-1}$ AND b_{j-1} AND $c_{k,j-2}$ for $1 \le k \le m$ and $1 \le j \le n$, and $|b_{n+1}\rangle$ is that the last carry is the most significant bit of the result from the last execution of Step (3a).

(5) **For** $t = 1$ **to** n

(5a) $|\varphi_{m+3+t,-1}\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{t+1} I_{2\times2}) \otimes (\otimes_{q=t}^{t} NOT) \otimes (\otimes_{q=t\text{-}1}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes (\otimes_{k=m}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes I_{2\times2}$ $|\varphi_{m+3+t-1}\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{t}|r_p{}^0\rangle) \otimes (\otimes_{p=t-1}^{1}|r_p^0 \oplus (r_{p-1} \bullet \overline{b}_{1,p})\rangle) \otimes (|r_0{}^1\rangle) \otimes (\otimes_{q=n+1}^{t+1}|b_{1,q}\rangle) \otimes (|\overline{b}_{1,t}\rangle) \otimes (\otimes_{q=t-1}^{1}|\overline{b}_{1,q}\rangle) \otimes (|b_{n+1}\rangle) \otimes (\otimes_{j=n}^{1}|b_j\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|y_{k,j}\rangle) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1}|c_{k,j-1}\rangle) \otimes (\otimes_{k=m}^{1}(|e_k{}^0\rangle + |e_k{}^1\rangle)) \otimes (|r_{n+1}{}^0\rangle) \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}})$, where for $1 \le q \le t-1$ $\overline{b}_{1,q}$ is obtained from the execution of the previous iterations for Step (5a) and for $1 \le p \le t - 1$ $|r_p^0 \oplus (r_{p-1} \bullet \overline{b}_{1,p})\rangle$ is obtained from the execution of the previous iterations for Step (5b).

(5b) $|\varphi_{m+3+t}\rangle = (\otimes_{p=n}^{t+1} I_{2\times2}) \otimes (\otimes_{p=t}^{t} CCNOT) \otimes (\otimes_{p=t-1}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes (\otimes_{k=m,\, j=n}^{1\;\;\;1} I_{2\times2}) \otimes$

$$(\otimes_{k=m}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes I_{2\times2} \left|\varphi_{m+3+t,\,-1}\right\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{t+1}\left|r_p{}^0\right\rangle) \otimes (\left|r_t{}^0 \oplus (r_{t-1} \bullet \overline{b}_{1,t}\right\rangle) \otimes (\otimes_{p=t-1}^{1}\left|r_p^0 \oplus (r_{p-1} \bullet \overline{b}_{1,p})\right\rangle) \otimes (\left|r_0{}^1\right\rangle) \otimes (\otimes_{q=n+1}^{t+1}\left|b_{1,q}\right\rangle) \otimes (\left|\overline{b}_{1,t}\right\rangle) \otimes (\otimes_{q=t-1}^{1}\left|\overline{b}_{1,q}\right\rangle) \otimes (\left|b_{n+1}\right\rangle) \otimes (\otimes_{j=n}^{1}\left|b_j\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|y_{k,j}\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|c_{k,j-1}\right\rangle) \otimes (\otimes_{k=m}^{1}(\left|e_k{}^0\right\rangle + \left|e_k{}^1\right\rangle)) \otimes (\left|r_{n+1}{}^0\right\rangle) \otimes (\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}),$$

where for $1 \leq p \leq t - 1$ $\left|r_p^0 \oplus (r_{p-1} \bullet \overline{b}_{1,p})\right\rangle$ is obtained from the execution of the previous iterations for Step (5b).

EndFor

(6) $$\left|\varphi_{m+3+n+1}\right\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{n+1} NOT) \otimes (\otimes_{q=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1} I_{2\times2}) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1} I_{2\times2}) \otimes (\otimes_{k=m}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes I_{2\times2} \left|\varphi_{m+3+n}\right\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{1}\left|r_p^0 \oplus (r_{p-1} \bullet \overline{b}_{1,p})\right\rangle) \otimes (\left|r_0{}^1\right\rangle) \otimes (\left|\overline{b}_{1,\,n+1}\right\rangle) \otimes (\otimes_{q=n}^{1}\left|\overline{b}_{1,q}\right\rangle) \otimes (\left|b_{n+1}\right\rangle) \otimes (\otimes_{j=n}^{1}\left|b_j\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|y_{k,j}\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|c_{k,j-1}\right\rangle) \otimes (\otimes_{k=m}^{1}(\left|e_k{}^0\right\rangle + \left|e_k{}^1\right\rangle)) \otimes (\left|r_{n+1}{}^0\right\rangle) \otimes (\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}).$$

(7) $$\left|\varphi_{m+3+n+2}\right\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1} I_{2\times2}) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1} I_{2\times2}) \otimes (\otimes_{k=m}^{1} I_{2\times2}) \otimes CCNOT \otimes I_{2\times2} \left|\varphi_{m+3+n+1}\right\rangle = \frac{1}{\sqrt{2^m}} (\otimes_{p=n}^{1}\left|r_p^0 \oplus (r_{p-1} \bullet \overline{b}_{1,p})\right\rangle) \otimes (\left|r_0{}^1\right\rangle) \otimes (\left|\overline{b}_{1,\,n+1}\right\rangle) \otimes (\otimes_{q=n}^{1}\left|\overline{b}_{1,q}\right\rangle) \otimes (\left|b_{n+1}\right\rangle) \otimes (\otimes_{j=n}^{1}\left|b_j\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|y_{k,j}\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|c_{k,j-1}\right\rangle) \otimes (\otimes_{k=m}^{1}(\left|e_k{}^0\right\rangle + \left|e_k{}^1\right\rangle)) \otimes (\left|r_{n+1}^0 \oplus (r_n \bullet \overline{b}_{1,n+1})\right\rangle) \otimes (\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}).$$

(8) $$\left|\varphi_{m+3+n+3}\right\rangle = (\otimes_{p=n}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{q=n+1}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\otimes_{j=n}^{1} I_{2\times2}) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1} I_{2\times2}) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1} I_{2\times2}) \otimes (\otimes_{k=m}^{1} I_{2\times2}) \otimes I_{2\times2} \otimes (\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} \oplus r_{n+1}) \left|\varphi_{m+3+n+2}\right\rangle = ((-1)^{r_{n+1}} \times \frac{1}{\sqrt{2^m}}) (\otimes_{p=n}^{1}\left|r_p^0 \oplus (r_{p-1} \bullet \overline{b}_{1,p})\right\rangle) \otimes (\left|r_0{}^1\right\rangle) \otimes (\left|\overline{b}_{1,\,n+1}\right\rangle) \otimes (\otimes_{q=n}^{1}\left|\overline{b}_{1,q}\right\rangle) \otimes (\left|b_{n+1}\right\rangle) \otimes (\otimes_{j=n}^{1}\left|b_j\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|y_{k,j}\right\rangle) \otimes (\otimes_{k=m,\,j=n}^{1\quad\quad 1}\left|c_{k,j-1}\right\rangle) \otimes (\otimes_{k=m}^{1}(\left|e_k{}^0\right\rangle + \left|e_k{}^1\right\rangle)) \otimes (\left|r_{n+1}\right\rangle) \otimes (\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}).$$

(9) Since quantum operations are naturally reversible, the auxiliary quantum bits can be restored to their initial states by reversing the operations from Steps (7) to (2).

(10) Apply Grover's operator in **Grover's algorithm** to the quantum state vector generated in Step (9).

(11) At most repeat to execute from Step (2) to Step (10) of $2^{\frac{m}{2}}$ times.

(12) The answer is obtained with a successful probability of at least $\frac{1}{2}$ after a measurement is finished.

End Algorithm

Lemma 4-1: For a finite set with *m* elements, *n* bits of each element in the finite set, and a given positive integer *b*, the quantum implementation of the DNA-based algorithm of solving an instance of the subset-sum problem **in Algorithm 4-1** is equivalent to the oracle work in **Grover's Algorithm**, i.e., the target state labeling, preceding Grover's searching step.

Proof: It is omitted due to space. ■

III. Complexity Assessment

The following lemmas are used to demonstrate time complexity and space complexity of **Algorithm 4-1** for solving an instance of the subset-sum problem for any given positive integer *b* and a finite set including *m* elements of *n* bits.

Lemma 5-1: For any given positive integer *b* and a finite set involving *m* elements of *n* bits, the time complexity of solving an instance of the subset-sum problem is O(m + 1) Hadamard gates, O($(2 \times m \times n + 2 \times n + 2 \times 1) \times \sqrt{2^m}$) **NOT** gates, O($(8 \times m \times n + 2 \times n + 3 \times 1) \times \sqrt{2^m}$) **CNOT** gates, O($(4 \times m \times n + 2 \times n + 2 \times 1) \times \sqrt{2^m}$) **CCNOT** gates, O($\sqrt{2^m}$) Grover's operators, and O(1) measurement.

Proof: Refer to **Algorithm 4-1**. ■

Lemma 5-2: For any given positive integer *b* and a finite set involving *m* elements of *n* bits, the space complexity of solving an instance of the subset-sum problem is O($2 \times m \times n + m + 3 \times n + 5$) quantum bits.

Proof: Refer to **Algorithm 4-1**. ■

IV. NMR Experiments of Three-qubit Solution to the Subset-sum Problem

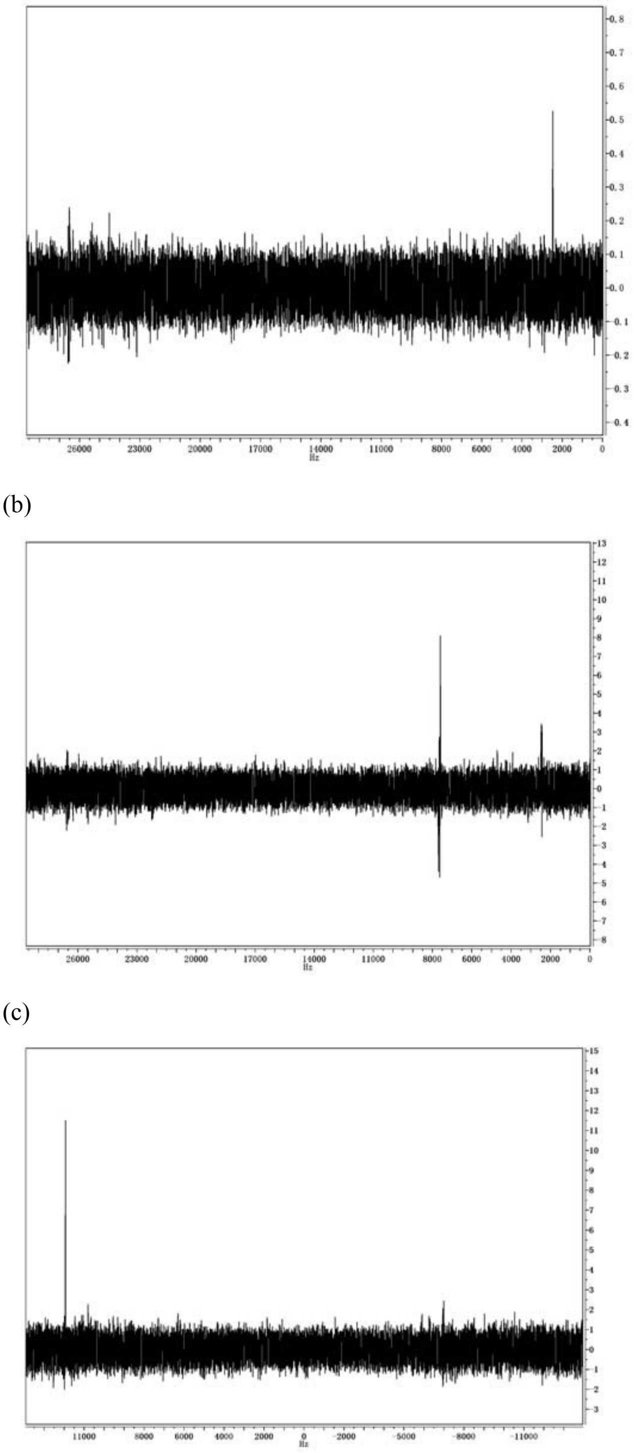
Consider the simplest case of the subset-sum problem with a finite set $A_1 = \{1\}$ and any given value $b = 1$. The size of the first (only) element in the finite set, A_1, is represented as $a_{1,1}^1$. The size of b (its size is one) is represented as $b_{1,1}^1$. The value of m is equal to one and the value of n is also equal to one. NMR approach has been widely employed to quantum information processing over past years due to its mature and well-controllable technology. Although the quantum information processing by NMR is made on ensembles of nuclear spins, instead of individual spins, NMR has remained to be the most convenient experimental tool to demonstrate quantum information processing. We here also adopt this technology to check our theory.

Note that in NMR measurements, the frequencies and phases of NMR signals could clearly indicate the state the system evolves to after the readout pulses had been applied. In our experiment, the phases of the reference of ^{13}C spectra from a thermal equilibrium were adjusted to be in absorption (i.e., to be positive), and then the same phase corrections were used to determine the absolute phases of the experimental spectra of ^{13}C after the algorithm was accomplished. In our case, the final state was $\mathbf{(|000\rangle_{123} + |111\rangle_{123})/\sqrt{2}}$ which means the three qubits are entangled. As the readout by NMR is a weak measurement, we have no state collapse after the measurement. Besides, only single quantum coherence can be detected in NMR. As a result, we have to employ some additional operations to disentangle them for detecting the output state $\mathbf{(|000\rangle_{123} + |111\rangle_{123})/\sqrt{2}}$. For this end, we apply a **CNOT** gate on the second and first qubits to get the state $\mathbf{(|000\rangle_{123} + |011\rangle_{123})/\sqrt{2}}$. The second qubit is control quibte and the first qubit is the target qubit. Then the first qubit can be read out by a s ingle $\boldsymbol{\pi/2}$ pulse along the x-axis, as shown in Figure 6-1 (a). Similar steps applied to the second and third quits, respectively, result in the spectrum in Figure 6-1 (b) and Figure 6-1 (c). It's evident that the experimental results are in good agreement with our theoretical prediction.

V. Conclusions

We have investigated the availability of quantum implementation for an instance of the subset-sum problem with a finite set involving m elements of n bits. We have also estimate the complexity of our solution and carried out an experiment by NMR technology for a simplest example.

(a)



(b)

(c)

Figure 6-1: Experimental spectra (a)-(c) of the three-qubit solution to the subset-sum problem after the readout on the first, second and third qubits, respectively.