

Quantum Symbolic Execution

Jiang Nan^{1,2}, Wang Zichen¹ and Wang Jian^{3,4*}

¹The Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China.

²Beijing Key Laboratory of Trusted Computing, Beijing 100124, China.

³School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China.

⁴Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China.

*Corresponding author(s). E-mail(s): wangjian@bjtu.edu.cn;

Abstract

With advances in quantum computing, researchers can now write and run many quantum programs. However, there is still a lack of effective methods for debugging quantum programs. In this paper, quantum symbolic execution (QSE) is proposed to generate test cases, which helps to finding bugs in quantum programs. The main idea of quantum symbolic execution is to find the suitable test cases from all possible ones (i.e. test case space). It is different from the way of classical symbol execution, which gets test cases by calculating instead of searching. QSE utilizes quantum superposition and parallelism to store the test case space with only a few qubits. According to the conditional statements in the debugged program, the test case space is continuously divided into subsets, subsubsets and so on. Elements in the same subset are suitable test cases that can test the corresponding branch in the code to be tested. QSE not only provides a possible way to debug quantum programs, but also avoids the difficult problem of solving constraints in classical symbolic execution.

Keywords: quantum symbolic execution, test cases, quantum program testing, quantum program, quantum computing

1 Introduction

Quantum computing has attracted much attention, because quantum superposition, entanglement and other properties can greatly improve the efficiency of computing [1, 2]. In recent years, with the development of quantum computer hardware [3, 4], quantum software and quantum programming [5–8] has also been greatly developed. Researchers can write and run many quantum algorithms that have been proposed before but cannot be implemented due to limitations, such as Grover’s algorithm [9], quantum principal component analysis algorithm [10], quantum phase estimation [11], and *etc.* In the process of writing quantum programs, some errors will inevitably occur [12–14]. For example, Zhao [15] defined a few bugs that focus on misuses of features of the quantum programming language — Qiskit [6]. Huang [16] also recorded some bugs in the Scaffold compiler [17]. For quantum programs we still need to take corresponding measures to find these errors and fix them. Due to the characteristics of quantum computing, we cannot debug programs as in the classical environment. This difficulty in debugging quantum programs hinders the development of quantum computing. An effective quantum program debugging scheme is needed.

Researchers have proposed some methods for debugging quantum programs, including quantum unit tests [18], quantum assertions [16, 19–21], and *etc.* Unit tests are used to determine whether a specific function is correct under a specific condition. The role of the assertion is that when the program executes to the assertion, the corresponding assertion should be true, and if the assertion is not true, the program should terminate execution. These methods have corresponding quantum versions. However, these methods are not very good to meet the needs. Currently, assertions in the quantum environment include statistical assertions [16] based on classical observations, dynamic runtime assertions [19] that use auxiliary qubits to obtain information indirectly, a projection-based runtime assertion [20], and dynamic assertion [21] that extend dynamic runtime assertions [19]. These assertions have two main shortcomings. Firstly, they are mostly used when an error has occurred during the running of the program or when the programmer suspects that there is an error somewhere in the program. Just like people do not directly set breakpoints on the entire program, but often set breakpoints only when the output is not as expected. Secondly, the use of assertions relies on the prediction of results. They need to compare the actual output with the expected result to judge whether the program is error. This is not simple for quantum programs. Microsoft’s *Q#* [18] provides a method for unit testing of quantum programs, which tests a unit of a quantum program individually to verify whether it meets expectations, and internally still uses assertions to achieve this goal. There is another method Quito (quantum input output coverage) [22]. The biggest contribution of this paper is to define three coverage criteria for the input and output of quantum program debugging. But the biggest flaw of this method is that it still uses statistical analysis to determine test pass and fail, which certainly does not reduce the complexity of quantum program

debugging. Therefore, they cannot meet the programmer's needs for quantum program debugging very well.

Only unit tests and assertion cannot meet the needs of program debugging. In classical program debugging field, symbolic execution is another important debug method and it has appeared much earlier [23]. With the development of constraint solving technology, symbolic execution has become an effective technology for generating high-coverage test cases [24] and been widely used in different areas such as software testing, analysis and verification [25–27].

This paper proposes a quantum symbolic execution (QSE) method, which focuses on generating high-coverage test cases for quantum programs. QSE uses quantum superposition and parallel characteristics to store the test case space with only a few qubits. According to the conditional statements in the debugged program, the test case space is continuously divided into subsets. Elements in the same subset are suitable test cases that can test the corresponding branch in the code to be tested. QSE not only provides a possible way to debug quantum programs, but also avoids the difficult problem of solving constraints in classical symbolic execution.

2 Related Works

In this section, we briefly introduce the classical symbolic execution and some existing quantum modules that will be used in QSE.

2.1 classical symbolic execution (CSE)

Programs often have conditional statements, and each branch represents an execution path to the program. In software testing, symbolic execution is a way to generate test cases that cover each execution path. Symbolic execution works by two steps:

- (1) creating execution paths, and
- (2) using a constraint solver to calculate the answers to the execution paths, i.e., generating test cases.

To formally accomplish this task, symbolic execution maintains two states globally: a symbolic state σ , which maps variables to symbolic expressions, and symbolic path constraints PC s, which are quantifier-free first-order logical formulas over symbolic expressions. At the beginning of a symbolic execution, σ is initialized to an empty map and PC is initialized to *true*. Both σ and PC are populated during the course of symbolic execution. The update rule of σ is:

- At every read statement $var = sym_input()$ that receives program input, symbolic execution adds the mapping $var \mapsto s$ to σ , where s is a fresh symbolic value.
- At every assignment $v = e$, symbolic execution updates σ by mapping v to $\sigma(e)$, where $\sigma(e)$ is the mapping of the symbolic state σ to the expression e .

The update rule of PC is:

4 Quantum Symbolic Execution

- At every conditional statement *if* (*e*) *S1* *else* *S2*, *PC* is updated to $PC_1 = PC \wedge \sigma(e)$ (“then” branch) and $PC_2 = PC \wedge \neg\sigma(e)$ (“else” branch).

For example, the symbolic execution of the code in Fig. 1 starts with an empty symbolic state σ and a symbolic path constraint *true*. After Line 03, $\sigma = \{x \mapsto x_0, y \mapsto y_0\}$; after Line 05, a path constraint $(x_0 + y_0 < 4) \wedge (x_0 > y_0)$ is created; and after Line 09, a path constraint $(x_0 + y_0 \geq 4) \wedge (y_0 > 1)$ is created. Finally, there are 4 path constraints: PC_{11} , PC_{12} , PC_{21} , and PC_{22} . Each path constraint is solved with a constraint solver to obtain test cases. $\{x = 2, y = 1\}$, $\{x = 1, y = 2\}$, $\{x = 3, y = 2\}$, and $\{x = 4, y = 1\}$ are the possible outputs of the constraint solver for PC_{11} , PC_{12} , PC_{21} , and PC_{22} respectively, i.e., they are suitable test cases.

All the execution paths of a program can be represented using a tree, called the execution tree. For example, Fig. 2 gives the execution tree of the code in Fig. 1. The 4 branches correspond to the 4 path constraints.

01.	<code>int main(){</code>	$\sigma = \emptyset, PC : true$
02.	<code> x=sym_input();</code>	$\sigma = \{x \mapsto x_0\}, PC : true$
03.	<code> y=sym_input();</code>	$\sigma = \{x \mapsto x_0, y \mapsto y_0\}, PC : true$
04.	<code> if(x+y<4){</code>	
05.	<code> if(x>y){</code>	$\sigma = \{x \mapsto x_0, y \mapsto y_0\}, PC_1 : (x_0 + y_0 < 4)$
06.	<code> return 0;</code>	$\sigma = \{x \mapsto x_0, y \mapsto y_0\}, PC_{11} : (x_0 + y_0 < 4) \wedge (x_0 > y_0)$
07.	<code> }</code>	$\sigma = \{x \mapsto x_0, y \mapsto y_0\}, PC_{12} : (x_0 + y_0 < 4) \wedge (x_0 \leq y_0)$
08.	<code> }else{</code>	$\sigma = \{x \mapsto x_0, y \mapsto y_0\}, PC_2 : (x_0 + y_0 \geq 4)$
09.	<code> if(y>1){</code>	
10.	<code> ERROR;</code>	$\sigma = \{x \mapsto x_0, y \mapsto y_0\}, PC_{21} : (x_0 + y_0 \geq 4) \wedge (y_0 > 1)$
11.	<code> }</code>	$\sigma = \{x \mapsto x_0, y \mapsto y_0\}, PC_{22} : (x_0 + y_0 \geq 4) \wedge (y_0 \leq 1)$
12.	<code> }</code>	
13.	<code> return 0;</code>	
14.	<code>}</code>	

Fig. 1 An example to illustrate symbolic execution

2.2 related quantum modules

Suppose a and b are two n -qubit binary numbers, quantum adder [28] “ A ” implements addition of two qubits:

$$A(|ab\rangle|0\rangle^{\otimes n+1}) = |ab\rangle|a + b\rangle.$$

The quantum module is shown in Fig. 3(a).

Quantum multiplier [29] “ M ” implements multiplication of two qubits:

$$M(|ab\rangle|0\rangle^{\otimes 2n}) = |ab\rangle|a \times b\rangle.$$

The quantum module is shown in Fig. 3(b).

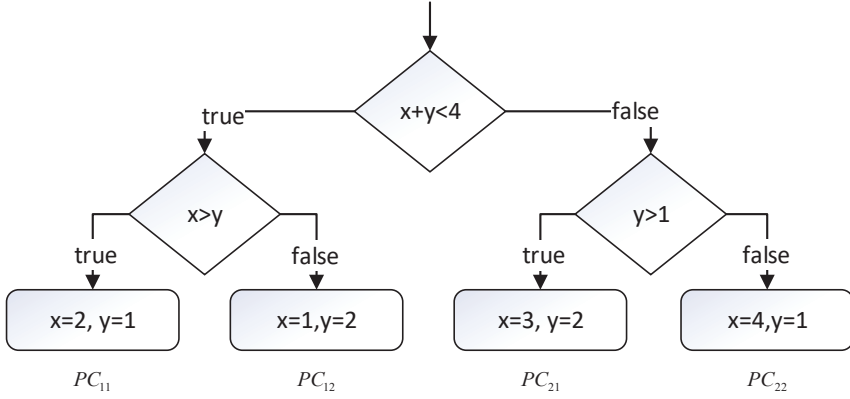


Fig. 2 The execution tree for the example in Fig. 1

The quantum comparator [30] “ C ” is used to compare two binary numbers. c_1 and c_2 are two 1-qubit outputs to record the comparison:

$$C(|ab\rangle|00\rangle) = |ab\rangle|c_1c_2\rangle.$$

When $a > b$, $|c_1c_2\rangle = |10\rangle$; when $a < b$, $|c_1c_2\rangle = |01\rangle$; and when $a = b$, $|c_1c_2\rangle = |00\rangle$. The module is shown in Fig. 3(c).

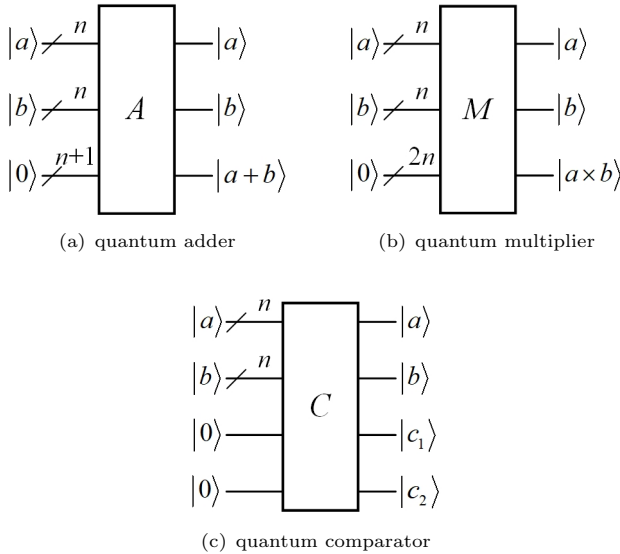


Fig. 3 Three quantum modules

3 Quantum symbolic execution

In this section, we first give the workflow of quantum symbolic execution. Then we explain how to prepare the initial test case space and use relational operators, logical operators to delineate subspaces. Then we give the overall framework of QSE. Finally give an example to illustrate.

3.1 main idea

In Section 2.1, we briefly describe the process of symbolic execution in the classical environment. Generally speaking, it first traverses the program to collect the path constraints, and then uses the constraint solver to calculate a set of inputs that meet the path constraints.

Quantum symbolic execution is completely different, which works by two steps:

- (1) generating a test case space that includes all possible test cases, and
- (2) according to the conditional statements in the code to be tested, partitioning the test case space into subspaces, and each subspace contains all the test cases that fit into a path constraint.

Fig. 4 contrasts classical symbolic execution and quantum symbolic execution.

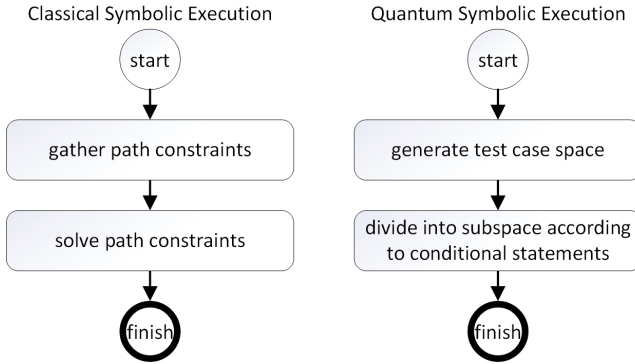


Fig. 4 The contrast between classical symbolic execution and quantum symbolic execution.

QSE uses two quantum registers: $|s\rangle$ and $|c\rangle$, where

$$|q\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |s_i\rangle \otimes |c_i\rangle \quad (1)$$

$|s\rangle = |s^{n-1}s^{n-2}\dots s^0\rangle$ consists of n qubits and s_i is a value used to represent a test case. $|c\rangle = |c^{m-1}c^{m-2}\dots c^0\rangle$ consists of m qubits and is the flag to subspace. $|s\rangle$ and $|c\rangle$ entangle together to realize the partition of $|s\rangle$: s_i with

Table 1 relational operation

relational operators	meaning
<	less than
<=	less than or equal to
>	greater than
>=	greater than or equal to
==	equal to
!=	not equal to

Table 2 logical operation

logical operators	meaning
&&	AND
	OR
!	NOT

the same c_i belongs to the same subset, i.e. test cases for the same branch. $|s\rangle$ and $|c\rangle$ are collectively referred to as $|q\rangle$.

The flag $|c\rangle$ plays an important role in QSE, and it is gradually modified as the conditional statements in the code to be tested. Different conditions correspond to different ways to modify $|c\rangle$. Therefore, it is necessary to know how many types of conditions there are when programming. According to [31–33], the conditions mainly include relational operation in Table 1 and logical operation in Table 2.

The effects of relational and logical operations on $|c\rangle$ will be described in detail in Sections 3.3 and 3.4, respectively.

3.2 Preparation of the test case space

Prepare $m + n$ qubits and set all of them to $|0\rangle$. The initial state of $|q\rangle$ is

$$|q\rangle_0 = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes m} \quad (2)$$

i.e., $|s\rangle_0 = |0\rangle^{\otimes n}$ and $|c\rangle_0 = |0\rangle^{\otimes m}$.

n H quantum gates and m I quantum gates are used to transform the initial state $|q\rangle_0$ to state $|q\rangle_1$, where

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The quantum preparation of the test case space can be expressed as U_1 :

$$U_1 = H^{\otimes n} \otimes I^{\otimes m} \quad (3)$$

8 *Quantum Symbolic Execution*

U_1 changes the initial state $|q\rangle_0$ to the test case space:

$$\begin{aligned}
|q\rangle_1 &= U_1(|q\rangle_0) \\
&= H^{\otimes n}(|s\rangle_0) \otimes I^{\otimes m}(|c\rangle_0) \\
&= (H|0\rangle)^{\otimes n} \otimes (I|0\rangle)^{\otimes m} \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle^m \\
&= \frac{1}{\sqrt{2}^n}(|0 \cdots 00\rangle + |0 \cdots 01\rangle + \cdots + |1 \cdots 11\rangle) \otimes |0\rangle^m \\
&= \frac{1}{\sqrt{2}^n}(|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle) \otimes |0\rangle^m \\
&= \frac{1}{\sqrt{2}^n} \sum_{i=0}^{2^n-1} |i\rangle \otimes |0\rangle^m \\
&= |s\rangle \otimes |0\rangle^m
\end{aligned} \tag{4}$$

where $|s\rangle = \frac{1}{\sqrt{2}^n} \sum_{i=0}^{2^n-1} |i\rangle$. The quantum circuit is shown in Fig. 5.

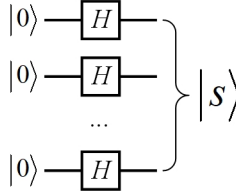


Fig. 5 The preparation of the test case space

Eq. (4) shows that the test case space $|s\rangle$ stores all integers from 0 to $2^n - 1$, which are all the possible test cases. If the code to be tested contains l ($l > 1$) variables x_1, x_2, \dots, x_l , $|s\rangle$ is still able to store all possible test cases. Divide the n qubits of $|s\rangle$ into l parts and each part stores all the possible value of a variable. The i th part contains n_i qubits $|s_{x_i}\rangle = |s_{x_i}^{n_i-1} s_{x_i}^{n_i-2} \cdots s_{x_i}^0\rangle$, where $n = \sum_{i=1}^l n_i$. For example, the code in Fig. 1 has two variables: x and y . They contain 3 and 2 qubits respectively. Hence,

$$|s\rangle = |s_x s_y\rangle = \frac{1}{\sqrt{2}^3} \sum_{i=0}^7 |i\rangle \otimes \frac{1}{\sqrt{2}^2} \sum_{j=0}^3 |j\rangle = \frac{1}{\sqrt{2}^5} \sum_{i=0}^{31} |i\rangle$$

3.3 Relational operator

Relational operators compare two numbers. Therefore, QSE uses the quantum comparator to divide the test case space. Section 2.2 shows that the quantum comparator has two output qubits: $|c_1 c_2\rangle$. Suppose they correspond to some

Table 3 The output of rational operation

relational operator	$ c^i c^{i-1}\rangle$
$<$	$ 01\rangle$
$<=$	$ 0*\rangle$
$>$	$ 10\rangle$
$>=$	$ *0\rangle$
$=$	$ 00\rangle$
\neq	$ 01\rangle$ or $ 10\rangle$

two adjacent qubits in $|c\rangle = |c^{m-1}c^{m-2}\dots c^0\rangle$, and mark them as $|c^i c^{i-1}\rangle$. Combining Table 1, we can get the relationship between the relational operators and the state of the output qubits as shown in Table 3. In this table, “*” indicates that there is no requirement for the state of that qubit.

Sometimes, instead of directly comparing two variables, the code to be tested compares the values of two expressions. Suppose the two expressions are e_1 and e_2 , and their outputs are $|\varphi_1\rangle$ and $|\varphi_2\rangle$ respectively. A quantum comparator is used to compare $|\varphi_1\rangle$ and $|\varphi_2\rangle$. $|c^i\rangle$ and $|c^{i-1}\rangle$ record the results of the comparison, i.e., they are the flags to segment the test case space. The segmentation of the test case space by a relational operator is expressed as U_r :

$$U_r = C \otimes e_1 \otimes e_2 \quad (5)$$

U_r can segment the test case space by modifying the state of $|c^i c^{i-1}\rangle$.

$$\begin{aligned}
& U_r(|s\rangle|0\rangle^{\otimes k}|0\rangle^{\otimes t}|00\rangle) \\
&= C(e_1(|s\rangle|0\rangle^{\otimes k})e_2(|s\rangle|0\rangle^{\otimes t})|00\rangle) \\
&= C(|s\rangle|\varphi_1\rangle|\varphi_2\rangle|00\rangle) \\
&= |s\rangle \otimes C(|\varphi_1\rangle|\varphi_2\rangle|00\rangle) \\
&= |s\rangle|\varphi_1\rangle|\varphi_2\rangle|c^i c^{i-1}\rangle
\end{aligned} \quad (6)$$

In $|s\rangle \otimes |c^i c^{i-1}\rangle$, due to the entanglement between $|s\rangle$ and $|c^i c^{i-1}\rangle$, different states of $|c^i c^{i-1}\rangle$ correspond to different subspaces of $|s\rangle$. The circuit is shown in Fig. 6.

In the following, we use $|c^i c^{i-1}\rangle_e$ to indicate that $|c^i c^{i-1}\rangle$ is in the output state of e , and $|c^i c^{i-1}\rangle_{\bar{e}}$ to indicate that $|c^i c^{i-1}\rangle$ is not in the output state of e , where $e = (e_1 \circ e_2)$ and $\circ \in \{<, \leq, >, \geq, =, \neq\}$. For example, if $e = (e_1 < e_2)$, $|c^i c^{i-1}\rangle_e = |01\rangle$, and $|c^i c^{i-1}\rangle_{\bar{e}} = |10\rangle$ or $|11\rangle$ or other non- $|01\rangle$ states.

3.4 Logical operators

3.4.1 T module

Usually, the inputs to a logical operator are the outputs of rational operator(s). A rational operator has two outputs $|c^i c^{i-1}\rangle$. Hence, Module T is defined firstly to facilitate later descriptions.

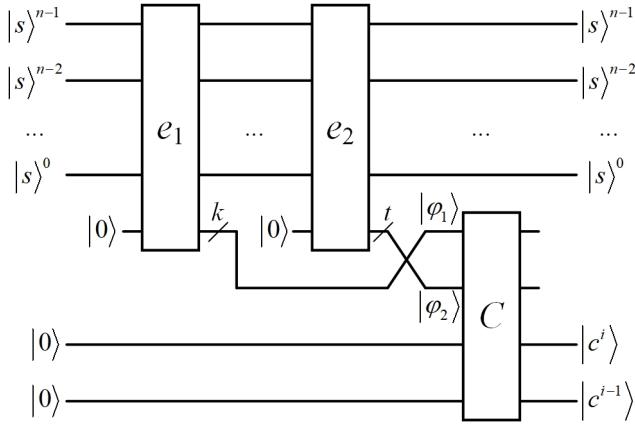


Fig. 6 The segmentation of the test case space by relational operations.

T is a control module that acts on two qubits $|c^i c^{i-1}\rangle$. According to Table 3, $|c^i c^{i-1}\rangle$ have 6 states. Therefore, there are also 6 cases of $T = \{T_<, T_\leq, T_>, T_\geq, T_=: T_\neq\}$. Their circuits are shown in Fig. 7.

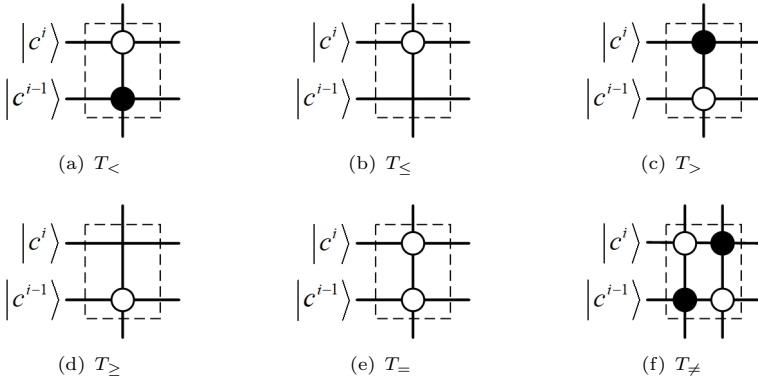


Fig. 7 Six cases of Module T

For example, in Fig. 7(a), because it is $T_<$, the state of $|c^i c^{i-1}\rangle$ is $|01\rangle$. Hence, we place a 0-control on qubit $|c^i\rangle$ and a 1-control on $|c^{i-1}\rangle$. Thus, these two control qubits represent that the result of the previous relational operation is “less than”.

3.4.2 Logical operators

There are 3 logical operators. We will give their quantum circuits one by one.

(1) AND

Suppose there is an expression $e_1 \& e_2$, where e_1 and e_2 are two rational operations. The logical AND in QSE is shown in Fig. 8(a), where $T_{e_1}, T_{e_2} \in T$,

$|c_1^i c_1^{i-1}\rangle$ are the flags of e_1 , and $|c_2^i c_2^{i-1}\rangle$ are the flags of e_2 . The output of logical AND is $|c_A\rangle$: if and only if both e_1 and e_2 are satisfied, $|c_A\rangle$ becomes $|1\rangle$; otherwise, it remains unchanged in $|0\rangle$ state. That is to say, $|c_A\rangle$ becomes a flag of logical AND.

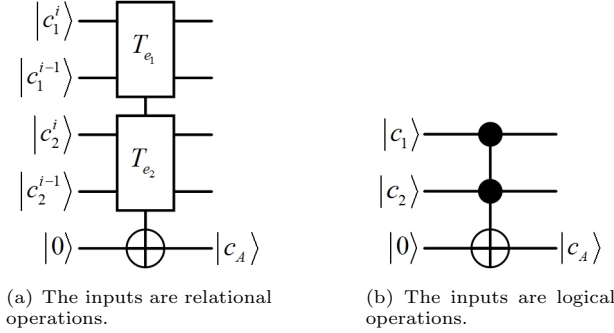


Fig. 8 logical AND for QSE

Define

$$U_{Ar} = T_{e_1} - T_{e_2} - \text{NOT} \quad (7)$$

Then,

$$\begin{aligned} & U_{Ar}(|c_1^i c_1^{i-1}\rangle \otimes |c_2^i c_2^{i-1}\rangle \otimes |0\rangle) \\ &= T_{e_1} - T_{e_2} - \text{NOT}(|c_1^i c_1^{i-1}\rangle \otimes |c_2^i c_2^{i-1}\rangle \otimes |0\rangle) \\ &= |c_1^i c_1^{i-1}\rangle_{e_1} \otimes |c_2^i c_2^{i-1}\rangle_{e_2} \otimes |1\rangle + |c_1^i c_1^{i-1}\rangle_{\bar{e}_1} \otimes |c_2^i c_2^{i-1}\rangle_{e_2} \otimes |0\rangle \\ &\quad + |c_1^i c_1^{i-1}\rangle_{e_1} \otimes |c_2^i c_2^{i-1}\rangle_{\bar{e}_2} \otimes |0\rangle + |c_1^i c_1^{i-1}\rangle_{\bar{e}_1} \otimes |c_2^i c_2^{i-1}\rangle_{\bar{e}_2} \otimes |0\rangle \end{aligned} \quad (8)$$

If e_1 and e_2 are two logical operations, it is only necessary to replace $|c_1^i c_1^{i-1}\rangle$ with $|c_1\rangle$, $|c_2^i c_2^{i-1}\rangle$ with $|c_2\rangle$, and T_{e_1} and T_{e_2} with 1-control, as shown in Fig. 8(b), where $|c_1\rangle$ and $|c_2\rangle$ are the outputs of e_1 and e_2 respectively. Now

$$U_{Al} = \text{CC-NOT} \quad (9)$$

and

$$\begin{aligned} & U_{Al}(|c_1\rangle \otimes |c_2\rangle \otimes |0\rangle) \\ &= \text{CC-NOT}(|c_1\rangle \otimes |c_2\rangle \otimes |0\rangle) \\ &= |1\rangle \otimes |1\rangle \otimes |1\rangle + |0\rangle \otimes |1\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |0\rangle \otimes |0\rangle \end{aligned} \quad (10)$$

(2) OR

For logical OR, there is an expression $e_1 || e_2$. Fig. 9(a) shows the logical OR in QSE if e_1 and e_2 are two rational operations. The output of logical OR is $|c_O\rangle$: as long as one of e_1 and e_2 is satisfied, $|c_O\rangle$ becomes $|1\rangle$; otherwise, it

remains unchanged in $|0\rangle$ state. That is to say, $|c_O\rangle$ becomes a flag of logical OR.

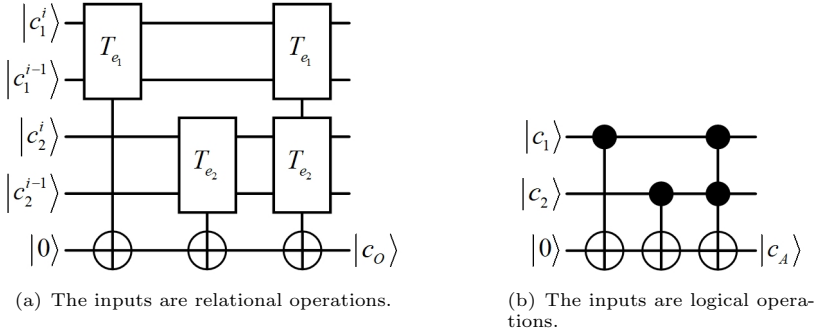


Fig. 9 logical OR for QSE

Define

$$U_{Or} = T_{e_1}\text{-}T_{e_2}\text{-NOT} \otimes T_{e_2}\text{-NOT} \otimes T_{e_1}\text{-NOT} \quad (11)$$

Then,

$$\begin{aligned} & U_{Or}(|c_1^i c_1^{i-1}\rangle \otimes |c_2^i c_2^{i-1}\rangle \otimes |0\rangle) \\ &= T_{e_1}\text{-}T_{e_2}\text{-NOT} \otimes T_{e_2}\text{-NOT}(T_{e_1}\text{-NOT}(|c_1^i c_1^{i-1}\rangle \otimes |c_2^i c_2^{i-1}\rangle \otimes |0\rangle)) \\ &= T_{e_1}\text{-}T_{e_2}\text{-NOT} \otimes T_{e_2}\text{-NOT}(|c_1^i c_1^{i-1}\rangle_{e_1} \otimes |c_2^i c_2^{i-1}\rangle \otimes |1\rangle + |c_1^i c_1^{i-1}\rangle_{\bar{e}_1} \otimes |c_2^i c_2^{i-1}\rangle \otimes |0\rangle) \\ &= T_{e_1}\text{-}T_{e_2}\text{-NOT}(|c_1^i c_1^{i-1}\rangle_{e_1} \otimes |c_2^i c_2^{i-1}\rangle_{e_2} \otimes |0\rangle + |c_1^i c_1^{i-1}\rangle_{e_1} \otimes |c_2^i c_2^{i-1}\rangle_{\bar{e}_1} \otimes |1\rangle \\ &\quad + |c_1^i c_1^{i-1}\rangle_{\bar{e}_1} \otimes |c_2^i c_2^{i-1}\rangle_{e_2} \otimes |1\rangle + |c_1^i c_1^{i-1}\rangle_{\bar{e}_1} \otimes |c_2^i c_2^{i-1}\rangle_{\bar{e}_1} \otimes |0\rangle) \\ &= |c_1^i c_1^{i-1}\rangle_{e_1} \otimes |c_2^i c_2^{i-1}\rangle_{e_2} \otimes |1\rangle + |c_1^i c_1^{i-1}\rangle_{e_1} \otimes |c_2^i c_2^{i-1}\rangle_{\bar{e}_1} \otimes |1\rangle \\ &\quad + |c_1^i c_1^{i-1}\rangle_{\bar{e}_1} \otimes |c_2^i c_2^{i-1}\rangle_{e_2} \otimes |1\rangle + |c_1^i c_1^{i-1}\rangle_{\bar{e}_1} \otimes |c_2^i c_2^{i-1}\rangle_{\bar{e}_1} \otimes |0\rangle \end{aligned} \quad (12)$$

If e_1 and e_2 are two logical operations, the quantum circuit is shown in Fig. 9(b) and represented as U_{Ol} . The migration principle is the same as in Fig. 8 and will not be repeated.

(3) NOT

NOT does not need to be implemented with any quantum circuits. For $!e$, not matter e is a rational operation or a logical operation, e divides $|s\rangle$ into two subsets: one satisfies e and the other does not. $!e$ just reverses the satisfiability and does not affect the division of the two subsets. Therefore, there is no need for quantum circuits to change the division of the subsets or to divide the subsets further.

3.5 Divide the test case space

Programs often have complex e or the branch statements are nested. Therefore, multiple quantum operations are needed to be connected to continuously divide the test case space.

Define

$$U_2 = U^{\otimes k} \quad (13)$$

where $U \in \{U_r, U_{Ar}, U_{Al}, U_{Or}, U_{Ol}\}$ and k is a positive integer. Act U_2 on $|q\rangle_1$:

$$\begin{aligned} |q\rangle_2 &= U_2(|q\rangle_1) \\ &= U^{\otimes k}(|s\rangle \otimes |0\rangle^m) \\ &= \frac{1}{\sqrt{2}^n} \sum_{i=0}^{2^n-1} |s_i\rangle \otimes |c_i\rangle \end{aligned} \quad (14)$$

According to the definitions of $U_r, U_{Ar}, U_{Al}, U_{Or}, U_{Ol}$ in Section 3.3 and Section 3.4, the qubits $|0\rangle^m$ in $|q\rangle_1$ is gradually modified based on the relational and the logical operators in the program to be tested. Eventually, through the entanglement of $|s\rangle$ and $|c\rangle$, the test case space is divided into multiple subsets. The values belonging to the same subset are test cases that can cover the same branch.

4 Experiments

4.1 An example

4.1.1 The division of the test space

The program shown in Fig. 1 is used as an example to further illustrate how QSE works. There are 3 branch statements in the program. Coupled with the process of preparing the test case space, the quantum circuit consists of 4 parts as shown in Fig. 10.

(1) Prepare the test case space

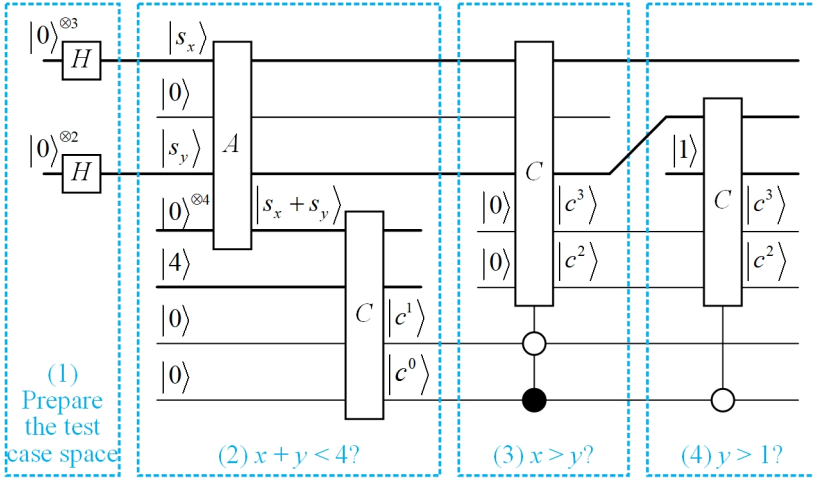
3 and 2 qubits are used to represent variables x and y respectively. Hence, 5 H quantum gates transform the initial state $|0\rangle^{\otimes 5}$ to state $|s_x\rangle \otimes |s_y\rangle$, i.e.,

$$\begin{aligned} H^{\otimes 5}(|0\rangle^{\otimes 5}) &= (H|0\rangle)^{\otimes 3} \otimes (H|0\rangle)^{\otimes 2} \\ &= \frac{1}{\sqrt{2}^3} \sum_{i=0}^7 |i\rangle \otimes \frac{1}{\sqrt{2}^2} \sum_{i=0}^3 |i\rangle = |s_x\rangle \otimes |s_y\rangle \end{aligned}$$

That is to say, $|s_x\rangle$ stores $0 \sim 7$ and $|s_y\rangle$ stores $0 \sim 3$. This is the test case space.

(2) $x + y < 4$?

The outermost branch statement is to determine whether $x + y$ is less than 4. The quantum adder “A” is used to get the sum of x and y . We add a $|0\rangle$

**Fig. 10** QSE circuit for example in Fig. 1

qubit as the highest bit of $|s_y\rangle$ to make $|s_y\rangle$ and $|s_x\rangle$ both have 3 qubits. The quantum comparator “ C ” is used to compare $|s_x + s_y\rangle$ and $|4\rangle$, and the output is $|c^1c^0\rangle$. If $x + y < 4$, $|c^1c^0\rangle = |01\rangle$; otherwise, $|c^1c^0\rangle = |*0\rangle$. The whole

process can be described with the following equation.

$$\begin{aligned}
& (C \otimes A)(|s_x\rangle|s_y\rangle \otimes |0\rangle|4\rangle|0\rangle|0\rangle) = C(A(|s_x\rangle|s_y\rangle|0\rangle) \otimes |4\rangle|0\rangle|0\rangle) \\
& = C((|0\rangle|0\rangle|0\rangle + |0\rangle|1\rangle|1\rangle + |0\rangle|2\rangle|2\rangle + |0\rangle|3\rangle|3\rangle \\
& \quad + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|2\rangle + |1\rangle|2\rangle|3\rangle + |1\rangle|3\rangle|4\rangle \\
& \quad + |2\rangle|0\rangle|2\rangle + |2\rangle|1\rangle|3\rangle + |2\rangle|2\rangle|4\rangle + |2\rangle|3\rangle|5\rangle \\
& \quad + |3\rangle|0\rangle|3\rangle + |3\rangle|1\rangle|4\rangle + |3\rangle|2\rangle|5\rangle + |3\rangle|3\rangle|6\rangle \\
& \quad + |4\rangle|0\rangle|4\rangle + |4\rangle|1\rangle|5\rangle + |4\rangle|2\rangle|6\rangle + |4\rangle|3\rangle|7\rangle \\
& \quad + |5\rangle|0\rangle|5\rangle + |5\rangle|1\rangle|6\rangle + |5\rangle|2\rangle|7\rangle + |5\rangle|3\rangle|8\rangle \\
& \quad + |6\rangle|0\rangle|6\rangle + |6\rangle|1\rangle|7\rangle + |6\rangle|2\rangle|8\rangle + |6\rangle|3\rangle|9\rangle \\
& \quad + |7\rangle|0\rangle|7\rangle + |7\rangle|1\rangle|8\rangle + |7\rangle|2\rangle|9\rangle + |7\rangle|3\rangle|10\rangle) \otimes |4\rangle|0\rangle|0\rangle) \\
& = |0\rangle|0\rangle C(|0\rangle|4\rangle|0\rangle|0\rangle) + |0\rangle|1\rangle C(|1\rangle|4\rangle|0\rangle|0\rangle) + |0\rangle|2\rangle C(|2\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |0\rangle|3\rangle C(|3\rangle|4\rangle|0\rangle|0\rangle) + |1\rangle|0\rangle C(|1\rangle|4\rangle|0\rangle|0\rangle) + |1\rangle|1\rangle C(|2\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |1\rangle|2\rangle C(|3\rangle|4\rangle|0\rangle|0\rangle) + |1\rangle|3\rangle C(|4\rangle|4\rangle|0\rangle|0\rangle) + |2\rangle|0\rangle C(|2\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |2\rangle|1\rangle C(|3\rangle|4\rangle|0\rangle|0\rangle) + |2\rangle|2\rangle C(|4\rangle|4\rangle|0\rangle|0\rangle) + |2\rangle|3\rangle C(|5\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |3\rangle|0\rangle C(|3\rangle|4\rangle|0\rangle|0\rangle) + |3\rangle|1\rangle C(|4\rangle|4\rangle|0\rangle|0\rangle) + |3\rangle|2\rangle C(|5\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |3\rangle|3\rangle C(|6\rangle|4\rangle|0\rangle|0\rangle) + |4\rangle|0\rangle C(|4\rangle|4\rangle|0\rangle|0\rangle) + |4\rangle|1\rangle C(|5\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |4\rangle|2\rangle C(|6\rangle|4\rangle|0\rangle|0\rangle) + |4\rangle|3\rangle C(|7\rangle|4\rangle|0\rangle|0\rangle) + |5\rangle|0\rangle C(|5\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |5\rangle|1\rangle C(|6\rangle|4\rangle|0\rangle|0\rangle) + |5\rangle|2\rangle C(|7\rangle|4\rangle|0\rangle|0\rangle) + |5\rangle|3\rangle C(|8\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |6\rangle|0\rangle C(|6\rangle|4\rangle|0\rangle|0\rangle) + |6\rangle|1\rangle C(|7\rangle|4\rangle|0\rangle|0\rangle) + |6\rangle|2\rangle C(|8\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |6\rangle|3\rangle C(|9\rangle|4\rangle|0\rangle|0\rangle) + |7\rangle|0\rangle C(|7\rangle|4\rangle|0\rangle|0\rangle) + |7\rangle|1\rangle C(|8\rangle|4\rangle|0\rangle|0\rangle) \\
& \quad + |7\rangle|2\rangle C(|9\rangle|4\rangle|0\rangle|0\rangle) + |7\rangle|3\rangle C(|10\rangle|4\rangle|0\rangle|0\rangle) \\
& = |0\rangle|0\rangle|0\rangle|4\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|1\rangle|4\rangle|0\rangle|1\rangle + |0\rangle|2\rangle|2\rangle|4\rangle|0\rangle|1\rangle + |0\rangle|3\rangle|3\rangle|4\rangle|0\rangle|1\rangle \\
& \quad + |1\rangle|0\rangle|1\rangle|4\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|2\rangle|4\rangle|0\rangle|1\rangle + |1\rangle|2\rangle|3\rangle|4\rangle|0\rangle|1\rangle + |1\rangle|3\rangle|4\rangle|4\rangle|0\rangle|0\rangle \\
& \quad + |2\rangle|0\rangle|2\rangle|4\rangle|0\rangle|1\rangle + |2\rangle|1\rangle|3\rangle|4\rangle|0\rangle|1\rangle + |2\rangle|2\rangle|4\rangle|4\rangle|0\rangle|0\rangle + |2\rangle|3\rangle|5\rangle|4\rangle|1\rangle|0\rangle \\
& \quad + |3\rangle|0\rangle|3\rangle|4\rangle|0\rangle|1\rangle + |3\rangle|1\rangle|4\rangle|4\rangle|0\rangle|0\rangle + |3\rangle|2\rangle|5\rangle|4\rangle|1\rangle|0\rangle + |3\rangle|3\rangle|6\rangle|4\rangle|1\rangle|0\rangle \\
& \quad + |4\rangle|0\rangle|4\rangle|4\rangle|0\rangle|0\rangle + |4\rangle|1\rangle|5\rangle|4\rangle|1\rangle|0\rangle + |4\rangle|2\rangle|6\rangle|4\rangle|1\rangle|0\rangle + |4\rangle|3\rangle|7\rangle|4\rangle|1\rangle|0\rangle \\
& \quad + |5\rangle|0\rangle|5\rangle|4\rangle|1\rangle|0\rangle + |5\rangle|1\rangle|6\rangle|4\rangle|1\rangle|0\rangle + |5\rangle|2\rangle|7\rangle|4\rangle|1\rangle|0\rangle + |5\rangle|3\rangle|8\rangle|4\rangle|1\rangle|0\rangle \\
& \quad + |6\rangle|0\rangle|6\rangle|4\rangle|1\rangle|0\rangle + |6\rangle|1\rangle|7\rangle|4\rangle|1\rangle|0\rangle + |6\rangle|2\rangle|8\rangle|4\rangle|1\rangle|0\rangle + |6\rangle|3\rangle|9\rangle|4\rangle|1\rangle|0\rangle \\
& \quad + |7\rangle|0\rangle|7\rangle|4\rangle|1\rangle|0\rangle + |7\rangle|1\rangle|8\rangle|4\rangle|1\rangle|0\rangle + |7\rangle|2\rangle|9\rangle|4\rangle|1\rangle|0\rangle + |7\rangle|3\rangle|10\rangle|4\rangle|1\rangle|0\rangle
\end{aligned}$$

(3) $x > y$?

If $x + y < 4$, it needs to be further judged whether x is greater than y . Hence, a $T_{<-C}$ module acts on the subspace $|s_x\rangle|s_y\rangle \otimes |c^3c^2c^1c^0\rangle$.

$$\begin{aligned}
& T_{<-C}(|0\rangle|0\rangle|0001\rangle + |0\rangle|1\rangle|0001\rangle + |0\rangle|2\rangle|0001\rangle + |0\rangle|3\rangle|0001\rangle \\
& + |1\rangle|0\rangle|0001\rangle + |1\rangle|1\rangle|0001\rangle + |1\rangle|2\rangle|0001\rangle + |1\rangle|3\rangle|0000\rangle \\
& + |2\rangle|0\rangle|0001\rangle + |2\rangle|1\rangle|0001\rangle + |2\rangle|2\rangle|0000\rangle + |2\rangle|3\rangle|0010\rangle \\
& + |3\rangle|0\rangle|0001\rangle + |3\rangle|1\rangle|0000\rangle + |3\rangle|2\rangle|0010\rangle + |3\rangle|3\rangle|0010\rangle \\
& + |4\rangle|0\rangle|0000\rangle + |4\rangle|1\rangle|0010\rangle + |4\rangle|2\rangle|0010\rangle + |4\rangle|3\rangle|0010\rangle \\
& + |5\rangle|0\rangle|0010\rangle + |5\rangle|1\rangle|0010\rangle + |5\rangle|2\rangle|0010\rangle + |5\rangle|3\rangle|0010\rangle \\
& + |6\rangle|0\rangle|0010\rangle + |6\rangle|1\rangle|0010\rangle + |6\rangle|2\rangle|0010\rangle + |6\rangle|3\rangle|0010\rangle \\
& + |7\rangle|0\rangle|0010\rangle + |7\rangle|1\rangle|0010\rangle + |7\rangle|2\rangle|0010\rangle + |7\rangle|3\rangle|0010\rangle) \\
& = |0\rangle|0\rangle|0001\rangle + |0\rangle|1\rangle|0101\rangle + |0\rangle|2\rangle|0101\rangle + |0\rangle|3\rangle|0101\rangle \\
& + |1\rangle|0\rangle|1001\rangle + |1\rangle|1\rangle|0001\rangle + |1\rangle|2\rangle|0101\rangle + |1\rangle|3\rangle|0000\rangle \\
& + |2\rangle|0\rangle|1001\rangle + |2\rangle|1\rangle|1001\rangle + |2\rangle|2\rangle|0000\rangle + |2\rangle|3\rangle|0010\rangle \\
& + |3\rangle|0\rangle|1001\rangle + |3\rangle|1\rangle|0000\rangle + |3\rangle|2\rangle|0010\rangle + |3\rangle|3\rangle|0010\rangle \\
& + |4\rangle|0\rangle|0000\rangle + |4\rangle|1\rangle|0010\rangle + |4\rangle|2\rangle|0010\rangle + |4\rangle|3\rangle|0010\rangle \\
& + |5\rangle|0\rangle|0010\rangle + |5\rangle|1\rangle|0010\rangle + |5\rangle|2\rangle|0010\rangle + |5\rangle|3\rangle|0010\rangle \\
& + |6\rangle|0\rangle|0010\rangle + |6\rangle|1\rangle|0010\rangle + |6\rangle|2\rangle|0010\rangle + |6\rangle|3\rangle|0010\rangle \\
& + |7\rangle|0\rangle|0010\rangle + |7\rangle|1\rangle|0010\rangle + |7\rangle|2\rangle|0010\rangle + |7\rangle|3\rangle|0010\rangle
\end{aligned}$$

If and only if $|c^1c^0\rangle = |01\rangle$, $|s_x\rangle$ and $|s_y\rangle$ need to be compared, i.e., $|c^3c^2\rangle$ is changed according to $|s_x\rangle$ and $|s_y\rangle$: if $|s_x\rangle > |s_y\rangle$, $|c^3c^2\rangle = |10\rangle$; otherwise, $|c^3c^2\rangle = |0*\rangle$. As long as $|c^1c^0\rangle \neq |01\rangle$, $|c^3c^2\rangle$ remains unchanged at state $|00\rangle$.
(4) $y > 1$?

If $x + y \geq 4$, it needs to be further judged whether y is greater than 1. Hence, a $T_{\geq -C}$ module acts on the subspace $|s_y\rangle|1\rangle \otimes |c^3c^2c^1c^0\rangle$.

$$\begin{aligned}
& T_{\geq -C}(|0\rangle|1\rangle|0001\rangle + |1\rangle|1\rangle|0101\rangle + |2\rangle|1\rangle|0101\rangle + |3\rangle|1\rangle|0101\rangle \\
& + |0\rangle|1\rangle|1001\rangle + |1\rangle|1\rangle|0001\rangle + |2\rangle|1\rangle|0101\rangle + |3\rangle|1\rangle|0000\rangle \\
& + |0\rangle|1\rangle|1001\rangle + |1\rangle|1\rangle|1001\rangle + |2\rangle|1\rangle|0000\rangle + |3\rangle|1\rangle|0010\rangle \\
& + |0\rangle|1\rangle|1001\rangle + |1\rangle|1\rangle|0000\rangle + |2\rangle|1\rangle|0010\rangle + |3\rangle|1\rangle|0010\rangle \\
& + |0\rangle|1\rangle|0000\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|0010\rangle + |3\rangle|1\rangle|0010\rangle \\
& + |0\rangle|1\rangle|0010\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|0010\rangle + |3\rangle|1\rangle|0010\rangle \\
& + |0\rangle|1\rangle|0010\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|0010\rangle + |3\rangle|1\rangle|0010\rangle \\
& + |0\rangle|1\rangle|0010\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|0010\rangle + |3\rangle|1\rangle|0010\rangle) \\
& = |0\rangle|1\rangle|0001\rangle + |1\rangle|1\rangle|0101\rangle + |2\rangle|1\rangle|0101\rangle + |3\rangle|1\rangle|0101\rangle \\
& + |0\rangle|1\rangle|1001\rangle + |1\rangle|1\rangle|0001\rangle + |2\rangle|1\rangle|0101\rangle + |3\rangle|1\rangle|1000\rangle \\
& + |0\rangle|1\rangle|1001\rangle + |1\rangle|1\rangle|1001\rangle + |2\rangle|1\rangle|1000\rangle + |3\rangle|1\rangle|1010\rangle \\
& + |0\rangle|1\rangle|1001\rangle + |1\rangle|1\rangle|0000\rangle + |2\rangle|1\rangle|1010\rangle + |3\rangle|1\rangle|1010\rangle \\
& + |0\rangle|1\rangle|0100\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|1010\rangle + |3\rangle|1\rangle|1010\rangle \\
& + |0\rangle|1\rangle|0110\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|1010\rangle + |3\rangle|1\rangle|1010\rangle \\
& + |0\rangle|1\rangle|0110\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|1010\rangle + |3\rangle|1\rangle|1010\rangle \\
& + |0\rangle|1\rangle|0110\rangle + |1\rangle|1\rangle|0010\rangle + |2\rangle|1\rangle|1010\rangle + |3\rangle|1\rangle|1010\rangle
\end{aligned}$$

If and only if $|c^0\rangle = |0\rangle$, $|s_y\rangle$ and $|1\rangle$ need to be compared, i.e., $|c^3c^2\rangle$ is changed according to $|s_y\rangle$ and $|1\rangle$: if $|s_y\rangle > |1\rangle$, $|c^3c^2\rangle = |10\rangle$; otherwise, $|c^3c^2\rangle = |0*\rangle$. As long as $|c^0\rangle \neq |0\rangle$, $|c^3c^2\rangle$ remains unchanged.

Finally, the state of the subspace $|s_x\rangle|s_y\rangle \otimes |c^3c^2c^1c^0\rangle$ is

$$\begin{aligned}
& |0\rangle|0\rangle|0001\rangle + |0\rangle|1\rangle|0101\rangle + |0\rangle|2\rangle|0101\rangle + |0\rangle|3\rangle|0101\rangle \\
& + |1\rangle|0\rangle|1001\rangle + |1\rangle|1\rangle|0001\rangle + |1\rangle|2\rangle|0101\rangle + |1\rangle|3\rangle|1000\rangle \\
& + |2\rangle|0\rangle|1001\rangle + |2\rangle|1\rangle|1001\rangle + |2\rangle|2\rangle|1000\rangle + |2\rangle|3\rangle|1010\rangle \\
& + |3\rangle|0\rangle|1001\rangle + |3\rangle|1\rangle|0000\rangle + |3\rangle|2\rangle|1010\rangle + |3\rangle|3\rangle|1010\rangle \\
& + |4\rangle|0\rangle|0100\rangle + |4\rangle|1\rangle|0010\rangle + |4\rangle|2\rangle|1010\rangle + |4\rangle|3\rangle|1010\rangle \\
& + |5\rangle|0\rangle|0110\rangle + |5\rangle|1\rangle|0010\rangle + |5\rangle|2\rangle|1010\rangle + |5\rangle|3\rangle|1010\rangle \\
& + |6\rangle|0\rangle|0110\rangle + |6\rangle|1\rangle|0010\rangle + |6\rangle|2\rangle|1010\rangle + |6\rangle|3\rangle|1010\rangle \\
& + |7\rangle|0\rangle|0110\rangle + |7\rangle|1\rangle|0010\rangle + |7\rangle|2\rangle|1010\rangle + |7\rangle|3\rangle|1010\rangle
\end{aligned} \tag{15}$$

There are 4 cases of the state $|c^3c^2c^1c^0\rangle$:

- $|1001\rangle$: $|c^1c^0\rangle = |01\rangle$ indicates $x + y < 4$ and $|c^3c^2\rangle = |10\rangle$ indicates $x > y$. Hence, $|1001\rangle$ indicates $x + y < 4$ & $x > y$, which corresponds to PC_{11} in classical symbolic execution.

- $|0 * 01\rangle: |c^1 c^0\rangle = |01\rangle$ indicates $x + y < 4$ and $|c^3 c^2\rangle = |0*\rangle$ indicates $x \leq y$. Hence, $|0 * 01\rangle$ indicates $x + y < 4 \ \&\& \ x \leq y$, which corresponds to PC_{12} in classical symbolic execution.
- $|10 * 0\rangle: |c^1 c^0\rangle = |* 0\rangle$ indicates $x + y \geq 4$ and $|c^3 c^2\rangle = |10\rangle$ indicates $y > 1$. Hence, $|10 * 0\rangle$ indicates $x + y \geq 4 \ \&\& \ y > 1$, which corresponds to PC_{21} in classical symbolic execution.
- $|0 * * 0\rangle: |c^1 c^0\rangle = |* 0\rangle$ indicates $x + y \geq 4$ and $|c^3 c^2\rangle = |0*\rangle$ indicates $y \leq 1$. Hence, $|0 * * 0\rangle$ indicates $x + y \geq 4 \ \&\& \ y \leq 1$, which corresponds to PC_{22} in classical symbolic execution.

These 4 states of $|c^3 c^2 c^1 c^0\rangle$ divide $|s_x\rangle|s_y\rangle$ into 4 subsets. As shown in Eq. 15,

- Subset $\{|1\rangle|0\rangle, |2\rangle|0\rangle, |3\rangle|0\rangle, |2\rangle|1\rangle\}$ contains all the test cases that can test the branch $x + y < 4 \ \&\& \ x > y$.
- Subset $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |0\rangle|2\rangle, |0\rangle|3\rangle, |1\rangle|1\rangle, |1\rangle|2\rangle\}$ contains all the test cases that can test the branch $x + y < 4 \ \&\& \ x \leq y$.
- Subset $\{|2\rangle|2\rangle, |3\rangle|2\rangle, |4\rangle|2\rangle, |5\rangle|2\rangle, |6\rangle|2\rangle, |7\rangle|2\rangle, |1\rangle|3\rangle, |2\rangle|3\rangle, |3\rangle|3\rangle, |4\rangle|3\rangle, |5\rangle|3\rangle, |6\rangle|3\rangle, |7\rangle|3\rangle\}$ contains all the test cases that can test the branch $x + y \geq 4 \ \&\& \ y > 1$.
- Subset $\{|4\rangle|0\rangle, |5\rangle|0\rangle, |6\rangle|0\rangle, |7\rangle|0\rangle, |3\rangle|1\rangle, |4\rangle|1\rangle, |5\rangle|1\rangle, |6\rangle|1\rangle, |7\rangle|1\rangle\}$ contains all the test cases that can test the branch $x + y \geq 4 \ \&\& \ y \leq 1$.

4.1.2 Running on a quantum computer

We use the *ibmq_qasm_simulator* quantum computer on the *IBM Quantum* platform to perform the example. The circuit is shown in Fig. 11. This experiment uses 28 qubits, with q_0 as the lowest bit and q_{25} as the highest bit:

- $q_2 q_1 q_0$ represent $|s_x\rangle$;
- $q_5 q_4 q_3$ represent $|s_y\rangle$;
- $q_9 q_8 q_7 q_6$ represent $|s_x + s_y\rangle$;
- $q_{12} q_{11} q_{10}$ are the auxiliary qubits of the quantum adder “A”;
- $q_{16} q_{15} q_{14} q_{13}$ are used to represent constant $|4\rangle$ and q_{17} is used to represent constant $|1\rangle$;
- $q_{23} q_{22} q_{21} q_{20} q_{19} q_{18}$ are the auxiliary qubits of the quantum comparator “C”;
- $q_{24} q_{25}$ are the flags $|c^3 c^2\rangle$ and $q_{26} q_{27}$ are the flags $|c^1 c^0\rangle$.

The three purple bars in the figure are three quantum comparators. At the end of the circuit, $q_0 q_1 q_2 q_3 q_4 q_5$ and $q_{24} q_{25} q_{26} q_{27}$ are measured and they have 32 results as shown in Fig. 12. The abscissa displays all the results and the default state of qubits that are not measured is 0. The ordinate represents the probability of each state in a total of 8192 measurements.

The 32 results can be divided into four test case spaces. Fig. 13(a) gives the measurement results whose $|c_3 c_2 c_1 c_0\rangle = |1001\rangle$, i.e., $x + y < 4 \ \&\& \ x > y$. Fig. 13(b) gives the measurement results whose $|c_3 c_2 c_1 c_0\rangle = |0 * 01\rangle$, i.e., $x + y < 4 \ \&\& \ x \leq y$. Fig. 13(c) gives the measurement results whose $|c_3 c_2 c_1 c_0\rangle =$

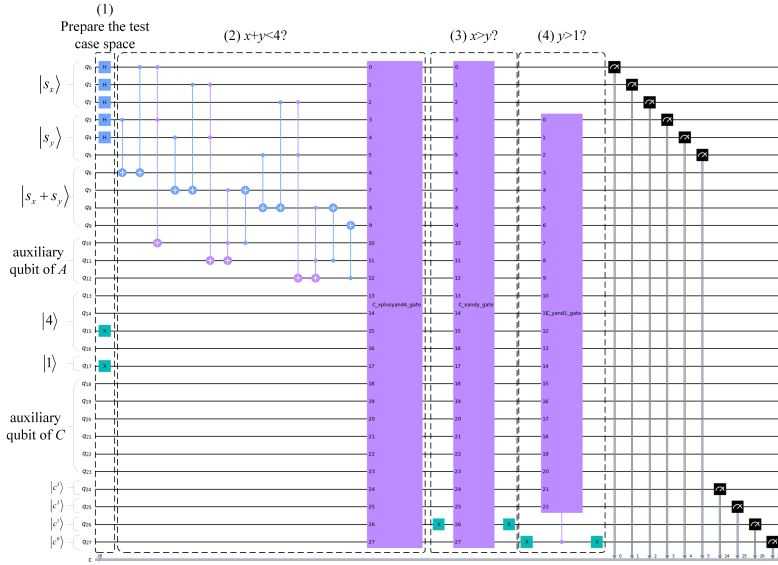


Fig. 11 circuit implementation of QSE

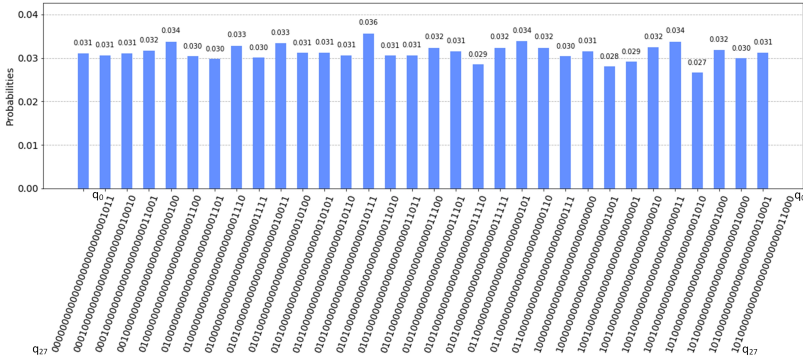


Fig. 12 measurement results for the circuit in Fig. 11

$|10 * 0\rangle$, i.e., $x + y \geq 4 \ \&\& \ y > 1$. Fig. 13(d) gives the measurement results whose $|c_3 c_2 c_1 c_0\rangle = |0 * * 0\rangle$, i.e., $x + y \geq 4 \ \&\& \ y \leq 1$.

4.2 Experiment data

8 real programs are used to evaluate the performance of QSE. They come from 2 references: [34] and [35] as shown in Table 4. The “Operations” column describes the type of operations appearing in the path conditions. The “Line of code” column lists the number of source code lines in the program, excluding comments and empty lines.

We also show the impact of test case space on program branch coverage. In the example given in Section 4.1.2, three qubits are used for each variable. In fact, more or fewer qubits can affect the performance of QSE. Too few qubits make it impossible for QSE to cover all branches. Consider the more

Table 4 Programs for the experiments

Program	Operations	Line of code	From
dart	Polynomials	11	[34]
power	Exponential function	20	[34]
stat	Mean and std. dev. computation	62	[34]
tcas	Constant equality checks	82	[34]
early	Polynomials	14	[34]
basic00181	Constant equality checks	30	[35]
snp3-ok	Constant equality checks	24	[35]
CWE789	Integer computation	141	[35]

Table 5 The comparison of complexity and time consumption of CSE and QSE.

Program	CSE		QSE	
	number of path constraints	time/s	number of subspace divisions	time/s
dart	4	0.48	3	0.45
power	11	1.32	7	1.05
stat	3	0.36	2	0.3
tcas	5	0.6	4	0.6
early	2	0.24	1	0.15
basic00181	3	0.36	2	0.3
snp3-ok	1	0.12	1	0.15
CWE789	6	0.72	3	0.45

extreme case: there are 4 branches in the program, but only 1 qubit is used to store variables, i.e., there are only 2 test cases in the test case space. Such a test case space is unlikely to cover all branches. Isn't the more qubits used, the better? No. Too many qubits will increase the difficulty of QSE, and lead to the waste of quantum resources. Therefore, the smallest number of qubits that can cover all branches is the best choice. Fig 14 shows the relationship between the number of qubits used by variables in the three programs in Table 5 and the program branch coverage. The best numbers of qubits for the three programs are 2, 4 and 5 respectively.

5 Conclusion

This paper proposes a quantum symbolic execution for the first time to generate high-coverage test cases. It is completely different from not only classical symbolic executions, but also quantum debugging schemes. QSE divides the test case space into subsets according to the conditional statements in the debugged program, and a subset contains all test cases that can test the same program branch. QSE not only provides a possible way to debug quantum programs, but also avoids the difficult problem of solving constraints in classical symbolic execution, which obviously reduces the difficulty and improves the efficiency of the work.

Funding This work is supported by the National Natural Science Foundation of China under Grants No.61502016.



Fig. 14 The relationship between the number of qubits and branch coverage

Data availability All data generated or analysed during this study are included in this article.

References

- [1] Nielsen, M.A., Chuang, I.: Quantum computation and quantum information. American Association of Physics Teachers (2002)
- [2] Jiang, N., Liang, X., Wang, M.: Programmable quantum processor implemented with superconducting circuit. *Communications in Theoretical Physics* **73**(5), 055102 (2021)
- [3] Zhong, H., Wang, H., Deng, Y., Chen, M., Peng, L., Luo, Y., Qin, J., Wu, D., Ding, X., Hu, Y., *et al.*: Quantum computational advantage using photons. *Science* **370**(6523), 1460–1463 (2020)
- [4] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G., Buell, D.A., *et al.*: Quantum supremacy using a programmable superconducting processor. *Nature* **574**(7779), 505–510 (2019)
- [5] Broughton, M., Verdon, G., McCourt, T., Martinez, A.J., Yoo, J.H., Isakov, S.V., Massey, P., Halavati, R., Niu, M.Y., Zlokap, A., *et al.*: Tensorflow quantum: A software framework for quantum machine learning. arXiv preprint arXiv:2003.02989 (2020)
- [6] Cross, A.: The ibm q experience and qiskit open-source quantum computing software. In: APS March Meeting Abstracts, vol. 2018, pp. 58–003 (2018)
- [7] Paolini, L., Piccolo, M., Zorzi, M.: Qpcf: higher-order languages and quantum circuits. *Journal of Automated Reasoning* **63**(4), 941–966 (2019)

- [8] Selinger, P.: Towards a quantum programming language. *Mathematical Structures in Computer Science* **14**(4), 527–586 (2004)
- [9] Adedoyin, A., Ambrosiano, J., Anisimov, P., Bärtschi, A., Casper, W., Chennupati, G., Coffrin, C., Djidjev, H., Gunter, D., Karra, S., et al.: Quantum algorithm implementations for beginners. *arXiv preprint arXiv:1804.03719* (2018)
- [10] He, C., Li, J., Liu, W.: An exact quantum principal component analysis algorithm based on quantum singular value threshold. *arXiv preprint arXiv:2010.00831* (2020)
- [11] O’Brien, T.E., Tarasinski, B., Terhal, B.M.: Quantum phase estimation of multiple eigenvalues for small-scale (noisy) experiments. *New Journal of Physics* **21**(2), 023022 (2019)
- [12] Paltenghi, M., Pradel, M.: Bugs in quantum computing platforms: An empirical study. *arXiv preprint arXiv:2110.14560* (2021)
- [13] Wang, J., Gao, M., Jiang, Y., Lou, J., Gao, Y., Zhang, D., Sun, J.: Qun-fuzz: Fuzz testing of quantum program. *arXiv preprint arXiv:1810.10310* (2018)
- [14] Miransky, A., Zhang, L., Doliskani, J.: Is your quantum program bug-free? *arXiv preprint arXiv:2001.10870* (2020)
- [15] Zhao, P., Zhao, J., Ma, L.: Identifying bug patterns in quantum programs. *arXiv preprint arXiv:2103.09069* (2021)
- [16] Huang, Y., Martonosi, M.: Statistical assertions for validating patterns and finding bugs in quantum programs. In: *Proceedings of the 46th International Symposium on Computer Architecture*, pp. 541–553 (2019)
- [17] JavadiAbhari, A., Patil, S., Kudrow, D., Heckey, J., Lvov, A., Chong, F.T., Martonosi, M.: Scaffcc: Scalable compilation and analysis of quantum programs. *Parallel Computing* **45**, 2–17 (2015)
- [18] Bright, P.: Microsoft’s q# quantum programming language out now in preview. *Ars Technica*, December **11** (2017)
- [19] Liu, J., Byrd, G.T., Zhou, H.: Quantum circuits for dynamic runtime assertions in quantum computation. In: *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*, pp. 1017–1030 (2020)
- [20] Li, G., Zhou, L., Yu, N., Ding, Y., Ying, M., Xie, Y.: Proq: Projection-based runtime assertions for debugging on a quantum computer. *arXiv*

preprint arXiv:1911.12855 (2019)

- [21] Liu, J., Zhou, H.: Systematic approaches for precise and approximate quantum state runtime assertion. In: 2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA), pp. 179–193 (2021). IEEE
- [22] Ali, S., Arcaini, P., Wang, X., Yue, T.: Assessing the effectiveness of input and output coverage criteria for testing quantum programs. In: 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST), pp. 13–23 (2021). IEEE
- [23] King, J.C.: Symbolic execution and program testing. *Communications of the ACM* **19**(7), 385–394 (1976)
- [24] Cadar, C., Sen, K.: Symbolic execution for software testing: three decades later. *Communications of the ACM* **56**(2), 82–90 (2013)
- [25] ZHAO, W., ZHANG, W., WANG, J., WANG, H., WU, C.: Smart contract vulnerability detection scheme based on symbol execution. *Journal of Computer Applications* **40**(4), 947–953
- [26] YANG, C., GUO, Y., HU, H., LIU, W., HUO, S., WANG, Y.: Cache-based side-channel vulnerability detection based on symbolic execution. *ACTA ELECTONICA SINICA* **47**(6), 1194 (2019)
- [27] Wang, S., Wang, P., Liu, X., Zhang, D., Wu, D.: Cached: Identifying cache-based timing channels in production software. In: 26th {USENIX} Security Symposium ({USENIX} Security 17), pp. 235–252 (2017)
- [28] CHANG, L., ZHU, Y., JIANG, H.: Design of quantum full adder. *ACTA ELECTONICA SINICA* **47**(9), 1863 (2019)
- [29] Yuan, S., Wang, Y., Wang, Y., Huang, F.: Quantum multiplier and its implementation method. *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)* (2019)
- [30] Wang, D., Liu, Z., Zhu, W., Li, S.: Design of quantum comparator based on extended general toffoli gates with multiple targets. *Computer Science* **39**(9), 302–306 (2012)
- [31] Prata, S.: *C Primer Plus*, (2014)
- [32] Bruce, E.: *Thinking in Java (Fourth Edition)*, (2006)
- [33] Eric, M.: *Python Crash Course: A Hands-On, Project-Based Introduction to Programming (First Edition)*, (2015)

- [34] Dinges, P., Agha, G.: Solving complex path conditions through heuristic search on induced polytopes (2014)
- [35] Li, Z., Zou, D., Xu, S., Ou, X., Jin, H., Wang, S., Deng, Z., Zhong, Y.: Vuldeepecker: A deep learning-based system for vulnerability detection (2018)
- [36] Luckow, K.S., Dimjaevi, M., Giannakopoulou, D., Howar, F., Isberner, M., Kahsai, T., Rakamaric, Z., Raman, V.: Jdart: A dynamic symbolic analysis framework (2016)
- [37] Jovanovi, D., Moura, L.D.: Solving non-linear arithmetic (2012)