计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200300015

基于申威26010处理器的大规模量子傅里叶变换模拟

刘晓楠[1] 荆丽娜[2] 王立新[1] 王美玲[1]
1 信息工程大学网络空间安全学院 郑州 450000
2 郑州大学中原网络安全研究院 郑州 450000
(prof.liu.xn@foxmail.com)

摘 要 量子计算由于其纠缠性和叠加性具有天然的并行优势,然而目前的量子计算设备受限于物理实现的工艺水平,距离可发挥巨大计算能力并解决有现实意义的实际问题还需要一定时间的技术积累和突破。因此,采用经典计算机对量子计算进行模拟成为验证量子算法的有效途径。量子傅里叶变换(Quantum Fourier Transform,QFT)是许多量子算法的关键组成部分,它涉及相位估计、求阶、因子等问题。对量子傅里叶变换的研究和大规模模拟实现,可以有效促进相关量子算法的研究、验证以及优化。文中使用我国自主研发的超级计算机——"神威·太湖之光"对大规模量子傅里叶变换进行模拟,并根据申威26010处理器异构并行的特点,采用MPI、加速线程库以及通信与计算隐藏技术进行优化。通过Shor算法中求解周期部分的运算来验证量子傅里叶变换模拟的正确性,实现了46位量子比特QFT算法的模拟和优化,为其他量子算法在超算平台上的验证优化以及新量子算法的提出提供了参考。

关键词:量子傅里叶变换;申威26010;MPI;加速线程库;Shor算法
中图法分类号 TP385

Large-scale Quantum Fourier Transform Simulation Based on SW26010

LIU Xiao-nan[1],JING Li-na[2],WANG Li-xin[1] and WANG Mei-ling[1]
1 Department of Cyberspace Security Academy,Information Engineering University,Zhengzhou 450000,China
2 School of Zhongyuan Cyber Security Institute,Zhengzhou University,Zhengzhou 450000,China

Abstract Quantum computing has a natural parallel advantage due to its entanglement and superposition. However,current quantum computing equipment is limited to the technological level of physical realization. It takes a certain amount of time to accumulate and break through to achieve huge computing power and solve practical problems with practical significance. Therefore,using classical computers to simulate quantum computing has become an effective way to verify quantum algorithms. Quantum Fourier Transform is a key part of many quantum algorithms. It involves phase estimation,order finding,factors,etc. Research on Quantum Fourier Transform and large-scale simulation implementation can effectively promote the research,verification and optimization of related quantum algorithms. In this paper,a large-scale Quantum Fourier Transform is simulated using the supercomputer,"Sunway TaihuLight",independently developed by our country. According to the heterogeneous parallel characteristics of SW26010 processor,MPI,accelerated thread library,and communication and computing hiding technology are adopted to optimize the system. The correctness of the Quantum Fourier Transform simulation is verified by seeking the period in the Shor algorithm,and the simulation and optimization of the Quantum Fourier Transform of 46-Qubits are realized,which provides reference for the verification and optimization of other quantum algorithms on the supercomputing platform and the proposal of new quantum algorithms.

Keywords Quantum fourier transform,SW26010,MPI,Accelerated thread library,Shor algorithm

1 引言

量子傅里叶变换能够实现时域到频域的线性变换,是许多量子计算的关键部分,它涉及相位估计问题、求阶问题、因子问题等。尤其在大数分解中,其能够将周期性的数据变换成概率幅度的正态分布。因此,对傅里叶变换模拟进行研究尤为重要,通过对大规模量子傅里叶变换模拟进行研究以及有效实现,可以更清楚地对其他量子算法进行研究、验证以及优化,还可以为新量子算法的提出给予保障。

然而,目前量子计算的研究面临很多的困难,最困难的地方之一就是硬件方面,即量子计算机的物理实现。虽然研究者在量子逻辑门的物理实现方面已进行了大量的研究工作,并有很多实验结果,但这些实验都是小规模的,距离真正可发挥巨大计算能力的有实用价值的量子计算机还相当遥远[1]。

到稿日期:2020-03-02 返修日期:2020-06-04 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金项目(61972413,61701539)
This work was supported by the National Natural Science Foundation of China(61972413,61701539).
通信作者:荆丽娜(1667500346@qq.com)

因此，我们可以使用经典计算机对量子计算进行模拟，实现对现有量子算法的测试和验证。本文选择对量子计算中常用的量子傅里叶变换进行模拟。

用经典计算机对大规模量子傅里叶变换进行数值模拟这一过程是高度计算密集型的，因此大规模量子傅里叶变换模拟过程只能使用超级计算机来进行。作为世界首台峰值运算速度超过 10 亿亿次、并行规模超千万核的新型超级计算机，“神威·太湖之光”是中国自主研发的一台超级计算机。其采用的申威 26010 异构众核处理器具有主从核并行模式，通过一个高性能的加速线程库来进行主从核任务分配，同时提供了寄存器通信等核内部访存优化方式[2]。

利用经典计算机实现量子计算，首先必须使用现有的高级编程语言如 C 和 Python 对量子逻辑操作进行量子线路抽象定义。多量子算符代数理论表明，任何量子逻辑操作都可以分解成一系列单量子位的逻辑操作和双量子位受控非门的组合序列[3]。本文的目的就是应用多量子算符代数理论来分解量子傅里叶变换相应的逻辑操作，进而在“神威·太湖之光”上使用 C 语言来模拟实现，并采用 MPI、加速线程库以及通信与计算隐藏技术进行优化，实现了对 46 量子比特的量子傅里叶变换进行模拟、优化和验证分析。

本文第 2 节介绍申威 26010 处理器架构以及通信模式；第 3 节介绍量子傅里叶变换的理论基础；第 4 节和第 5 节分别介绍大规模量子傅里叶变换模拟实现、优化和验证分析；最后总结全文并展望未来。

2 申威 26010 异构众核处理器

“神威·太湖之光”超级计算机采用的是国产自主研发的申威 26010 异构众核处理器、片上计算阵列集群和分布式共享存储相结合的异构众核体系，使用 64 位自主申威指令系统。

2.1 申威 26010 处理器架构

每个处理器包含 4 个核组，每个核组又包含 1 个主核、64 个从核组成的 8×8 计算处理元件阵列，以及 1 个内存控制器。一个申威 26010 处理器和单个核组的结构如图 1 所示。

“神威·太湖之光”高速计算机系统的每个计算节点包含 1 个众核处理器，内存为 32GB。众核处理器中每个核组的本地内存为 8GB，从核可以通过 gld/gst 方式直接离散访问主存，也可以通过 DMA 方式批量访问主存，从核阵列之间可以采用寄存器通信方式进行通信。每个从核局部存储空间的大小为 64kB。

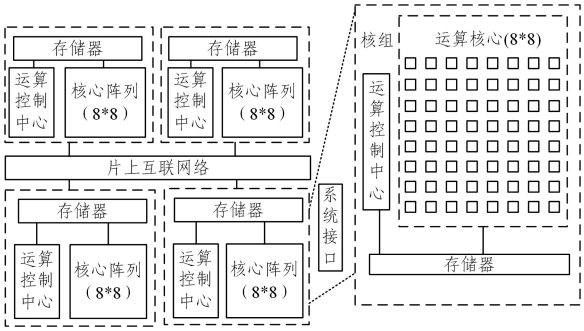

图 1 申威 26010 异构众核处理器架构图

Fig. 1 Architecture of SW26010 heterogeneous multicore processor

2.2 通信模式

神威平台支持主从加速并行等多种异构并行编程，在主从加速并行算法中，程序的计算核心被加载到从核上进行加速运算，而主核只完成应用程序的通信、I/O 和部分串行代码的计算[4]。基于此，对于量子傅里叶变换模拟的优化策略主要是充分利用申威 26010 处理器的架构特性来获得高性能。本文将采用 MPI 与加速线程库的两级并行对量子傅里叶变换进行优化，第一级并行运行在主核上，第二级并行运行在从核组上，主核和从核组一一对应，利用加速线程库在从核阵列上进行众核高效率计算及从核间通信，MPI 在不同核组的主核间进行数据传递[5]。

3 量子傅里叶变换

标准的离散傅里叶变换是以一个长度为 N 的复向量 $\boldsymbol{x}_0,\cdots,\boldsymbol{x}_{N-1}$ 为输入，以复向量 $\boldsymbol{y}_0,\cdots,\boldsymbol{y}_{N-1}$ 为输出，符合如下定义：

$$y_k \equiv \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j \mathrm{e}^{2\pi ijk/N}$$

量子傅里叶变换与离散傅里叶变换尽管在符号表示上有些差异，但有严格相同的变换。量子傅里叶变换是作用在 Hilbert 空间上任意矢量上的变换，其定义为在一组标准正交基 $|0\rangle,\cdots,|N-1\rangle$ 上的一个线性算子，在基态上的作用为：

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\mathrm{e}^{2\pi ijk/N}|k\rangle$$

其中，$|j\rangle$ 表示一个量子态源，它被转换成所有 n^2 个可能的量子态的线性组合。利用代数变换可进行如下变换：

$$\begin{aligned}
|j\rangle &\rightarrow \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1}\mathrm{e}^{2\pi ijk/2^n}|k\rangle \\
&= \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\mathrm{e}^{2\pi ij\left(\sum_{l=1}^{n}k_l 2^{-l}\right)}|k_1\cdots k_n\rangle \\
&= \frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n}\mathrm{e}^{2\pi ijk_l 2^{-l}}|k_1\rangle \\
&= \frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[\sum_{k_l=0}^{1}\mathrm{e}^{2\pi ijk_l 2^{-l}}|k_1\rangle\right] \\
&= \frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[|0\rangle+\mathrm{e}^{2\pi ij2^{-l}}|1\rangle\right] \\
&= \frac{(|0\rangle+\mathrm{e}^{2\pi i0.j_n}|1\rangle)(|0\rangle+\mathrm{e}^{2\pi i0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle+\mathrm{e}^{2\pi i0.j_1j_2\cdots j_n}|1\rangle)}{2^{n/2}}
\end{aligned}$$

特别地，整数 j 的二进制表示为 $j=j_1j_2\cdots j_n$，展开可以写成 $j=j_1 2^{n-1}+j_2 2^{n-2}+\cdots+j_n 2^0$。小数 j 的二进制表示为：$j=0.j_lj_{l+1}\cdots j_m$，展开可以写成 $j=j_l/2+j_{l+1}/2^2+\cdots+j_m/2^{m-l+1}$。量子傅里叶变换的线路图如图 2 所示，其中省略了 $1/\sqrt{2}$ 归一化因子。

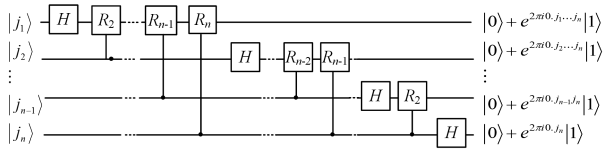

图 2 量子傅里叶变换线路图

Fig. 2 Quantum Fourier transform circuit diagram

通过进一步的代数变换可以发现，在由 n 个量子位构成的 $N=2^n$ 维 Hilbert 空间中，量子傅里叶变换可由一系列基本逻辑门组成。在量子傅里叶变换的有效线路图中[6]，只需

要两种量子逻辑门，一种是作用于单量子位的 Hadamard(H)变换，另一种是作用在两个量子位的受控相移(R)变换。

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},R_k=\begin{bmatrix}1 & 0\\ 0 & e^{2\pi i/2^k}\end{bmatrix}$$

4 模拟实现

本文的目标是利用神威平台的异构特点实现对量子傅里叶变换的大规模模拟，因此使用高级编程语言(C 语言)对量子逻辑操作进行量子线路抽象定义，并采用“多进程 MPI 并行＋进程内主从核并行”的两级并行技术来缩短量子计算的模拟时间，提高模拟效率。

模拟开始后，首先获取所需要模拟的量子比特位数以及使用的进程数目，调度各个节点协同模拟量子寄存器，每个节点由 1 个 MPI 进程执行模拟任务，申请所需的存储空间，并进行初态制备，即初始化各个基态的概率幅。然后根据量子线路模拟量子门，进而开始计算，每个进程均等地负责一部分基态概率幅的计算更新。主核上的每个进程又可以通过加速线程库开启从核的 64 个线程，概率幅的计算更新又可以由线程来实现，以充分发挥神威异构众核的能力。主核主要负责量子寄存器的申请、初始化以及进程的调度，从核通过线程对量子门模拟运算后，将更新后的概率幅送回主核。

申威 26010 处理器的每个处理器包含 4 个核组，每个核组由 1 个主核和 64 个从核构成，每个核组的本地内存有 8GB[7]。由于其物理特性，单进程最多可模拟的量子比特数为 30。经测试，对于 30 量子比特的量子傅里叶变换模拟单进程需要 868s，而两进程仅需要 454 s。因此可以得知，使用多进程可以加快模拟速度。然而，到目前为止并没有发挥神威主从加速异构的特点，因此需要采用加速线程库对其进行进一步优化。

量子傅里叶变换主要由 Hadamard 变换(H)和相移变换(R)两部分组成。通过对量子傅里叶变换的程序进行热点分析发现，相移变换的运行时间占总时间的 91%，且该程序的执行过程相对独立，适合在并行结构上进行并行优化。因此，本文将首先令主核发送概率幅到从核，即主核将其进程内的概率幅进行任务划分，并将结果分别发送到从核的局部存储器。然后对当前位相关概率幅状态执行相移操作，并将操作结果发送到主核存储器，直到主核上的概率全部计算完毕为止，从而进一步提高算法在众核结构上的执行效率。

在从核上，我们采用计算与通信隐藏的方式，将要处理的数据分块，用计算将通信隐藏。本文将从核的局部存储器分成 4 块，标记为 pem1，pem2，pem3 和 pem4，其示意图如图 3 所示。

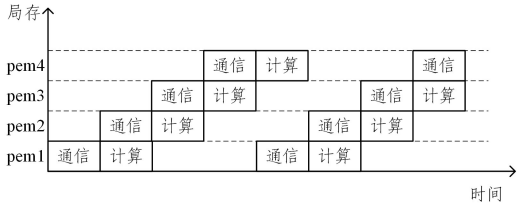

图 3 计算与通信隐藏的示意图

Fig. 3 Diagram of computation and communication hiding

同时，在量子傅里叶变换模拟过程中引入 numprocs 参数和 qubits 参数，分别表示使用的进程数和要模拟的量子比特数。将其编写为 run. sh 脚本，可供用户编译后动态输入运行，达到人机交互的目的。run. sh 脚本如下：

```
1. for((i=1;;i++))
2. do
3.    echo "How many processes do you want to choose?"
4.    echo "Our processes numbers are in 2^0～2^16."
5.    echo "Please choose a number form 0～16:"
6.    read exponent
7.    if[[" $exponent" -lt0 || " $exponent"-gt 16]];
8.      then
9.        echo "ERROR"
10.       continue
11.   else
12.     let numprocs=2 * * " $exponent"
13.     if[[" $exponent"%2-eq0]]
14.       then
15.           let qumin=20+" $exponent"
16.           let qumax=30+" $exponent"
17.     else
18.         let qumin=21+" $exponent"
19.         let qumax=29+" $exponent"
20.     fi
21.     for((j=1;;j++))
22.     do
23.       echo "how many qubits do you want to choose?"
24.       echo "please choose a number from " $qumin" ～ " $qumax""
25.       echo "Notice! qubits must be an even number!"
26.       read qubits
27.        if [[ " $qubitsr"%2-ne 0 ‖ " $qubits"-lt " $qumin" ‖
          " $qubits"-gt " $qumax"]];
28.       then
29.         echo "ERROR!"
30.         continue
31.       else
32.        bsub-I-b-q q_test_yyz-n  $numprocs-cgsp 64-share_size
          14000-host_stack 2048. /a. out  $qubits
33.        break
34.       fi
35.    done
36.  break
37.  fi
38. done
```

run. sh 脚本中 bsub 为作业提交命令。busb 命令常用的参数说明如表 1 所列。

表 1 bsub 命令常用的参数说明

Table 1 Common parameters of busb command

参数	说明
-I	提交交互式作业，使作业在作业提交窗口输出
-b	指定从核栈位于局存
-q	向指定的队列提交作业，必须选
-n	指定需要的所有主核数
-cgsp	指定每个核组内需要的从核个数，该参数必须小于或等于 64
-share_size	指定核组共享空间大小
-host_stack	指定主核栈空间大小，默认为 8M

例如，向高速计算系统队列 q_test_yyz 提交交互式作业 a. out，该作业使用 numprocs(用户动态输入)个主核，每个主核调用 64 从核实现并行，作业提交命令为：bsub-I-b-q q_test_

yyz-n $numprocs-cgsp 64-share _ size 14 000-host _ stack 2048./a.out MYMqubits。作业提交成功后，将显示一行包括 jobid 的提示信息，其中包括作业 id 号，如“Job〈8020〉has been submitted to queue〈q_test_yyz〉”，此时 jobid 就是 8020，它是全局唯一的。一旦作业提交成功，用户对作业的终止、查询等操作就可以通过 jobid 来实现。

5 测试验证

5.1 正确性测试

Shor 算法的流程如图 4 所示。

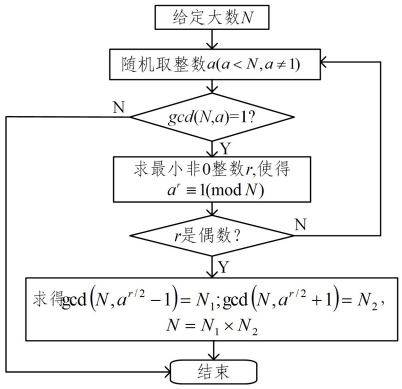

图 4 Shor 算法的流程

Fig. 4 Structure of Shor algorithm

大数因式分解问题的复杂性是目前广泛使用的 RSA 密钥系统的理论基础，Shor 算法不仅证明了量子算法的优越性，更动摇了现行的 RSA 密码系统的安全性基础[8]。量子傅里叶变换在大数分解中，能够将周期性的数据变换成概率幅度的正态分布。该算法分为经典实现和量子实现两部分，其中求最小正整数 r 使得 $a^r \equiv 1 \pmod N$ 成立为量子算法部分。

本文选取 $N=799$ 作为输入，选取 $a=7$，采用 20 位量子比特进行模拟，则可以清楚地得知周期 r 为 368，概率幅度为 2849。输出运行后的结果并使用 Python 的 matplotlib 进行绘图验证，产生的结果如图 5 所示，然后不断选中放大，产生如图 6 所示的一系列变换。由此得知，本文所模拟的量子傅里叶变换有效。

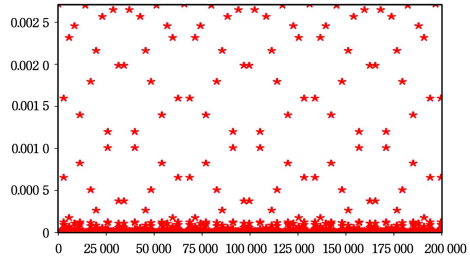

图 5 输出结果

Fig. 5 Output result

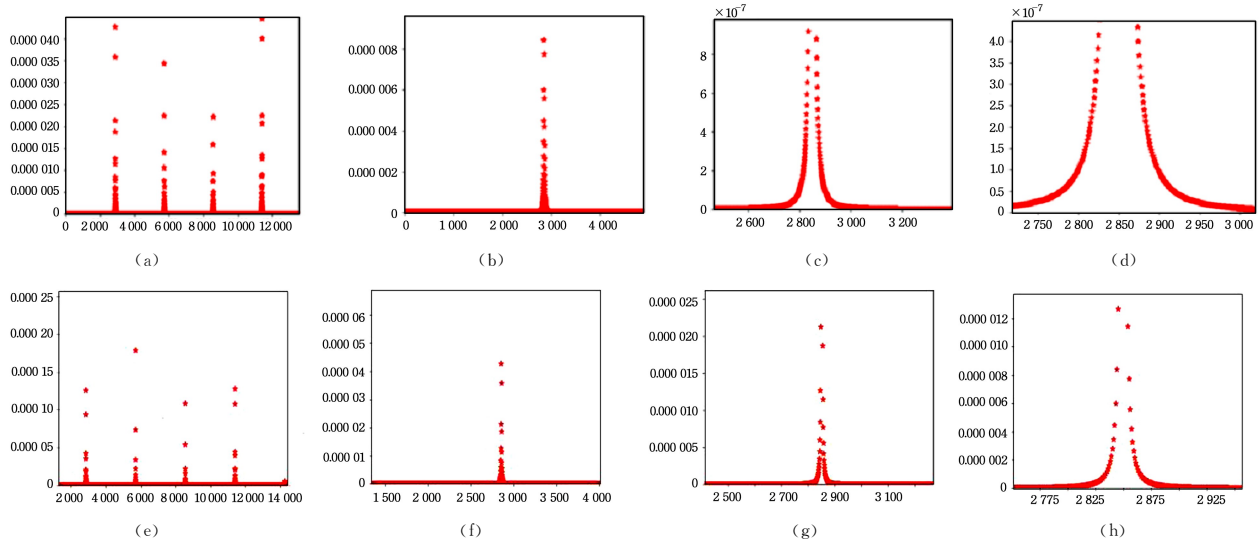

图 6 变换示意图

Fig. 6 Variation diagram

5.2 功能性测试

对于 20 量子比特的傅里叶变换模拟，首先将程序在单个主核上编译成功并运行，这相当于纯 CPU 版本，仅使用进程；然后运行主从核优化策略改进过的主从并行版本，其运行时间如表 2 所列。可以看出，相比于主核，使用从核并行计算在理论上产生了 64 倍的加速。但从实际模拟效果看，加速比远远小于理论值，但仍然取得了 6.45 倍的加速，主从核优化策略取得了不错的结果。其主要原因如下：1）量子傅里叶变换仅仅将 R 变换进行从核加速，没有考虑 H 变换；2）任务的切分需要时间；3）从核所需要的计算数据由主核获取，需要通信时间；4）由于从核局部存储空间的限制，从核无法从局部存储空间获取计算所需要的全部数据，导致有些数据需要通过直接访问主核内存来获取，这大大增长了计算时间，以至于无法获得理论加速比。

表 2 单主核版本与单主从核版本的运行时间对比

Table 2 Run time comparison between single master core version and single master slave version

版本	时间/s	加速比
单主核	3.61	6.45
单主从核	0.56	

上文仅仅对单核进行测试分析，并没有充分利用超算平台多核的特性，因此我们将对多核多进程进行测试分析。对

于 30 量子比特的傅里叶变换，单进程模拟需要 868s，两进程模拟需要 454s，加速比达到近 50%。为了更直观地比较 MPI 程序的加速效果，不断地增加进程进行测试，表 3 列出了当进程数由 1 扩展到 32(计算节点由 1 扩展到 16)时的加速比和并行效率。由表 3 可知，当进程数小于 8 时，程序有很好的 MPI 并行效率。随着进程数目的不断增加，并行效率逐渐降低，这是由于通信延迟所引起的。当进程数增加到一定程度时，MPI 集合通信相对计算部分的比例逐步增大，MPI 的通信瓶颈效应凸显了出来[9]。总体来看，优化后的并行效率较高，在 MPI 进程数达到 32 时并行效率仍可达到 66.16%，效果良好。

表 3 30-Qubit 的 MPI 扩展性测试结果

Table 3 30-Qubit MPI scalability test results

进程数	运行时间/s	加速比	MPI 并行效率/%
1	868	1	100
2	454	1.91	95.60
4	232	3.74	93.53
8	117	7.42	92.74
16	76	11.42	71.38
32	41	21.17	66.16

至此，本文不仅以 20 量子比特的量子傅里叶变换为例对单主核和单主从核进行了测试，还选取了 30 量子比特在不同进程数目下测试加速比以及并行效率，两者都取得了不错的效果，较为理想地展示和发挥了神威异构并行的特点。

最后，本文分别对 40-Qubit，42-Qubit，44-Qubit，46-Qubit 的量子傅里叶变换模拟进行测试，结果如表 4 所列。观察表 4 发现，对于不同规模的量子比特模拟，时间有所浮动，主要是因为测试时有其他任务也在神威上运行，任务之间可能产生影响。

表 4 不同量子比特模拟的运行时间

Table 4 Run time of different qubit simulations

量子比特数	40-Qubit	42-Qubit	44-Qubit	46-Qubit
时间/s	2168	2056	2397	2301

整体来说，本文通过采用 MPI、加速线程库以及通信与计算隐藏等方法在“神威·太湖之光”上实现了 46 量子比特的量子傅里叶变换模拟，为其他量子算法的验证优化以及新量子算法的提出给予保障。

结束语 量子计算是量子理论与计算科学交叉的新型计算模式，代表了量子力学在当今时代最具潜力的发展方向。量子计算的并行性不仅为研究经典慢算法的解决方案提供了一种革命性的算法设计思路，更重要的是它从可操作的层面为人类理解量子理论指明了方向[10]。但从目前发展水平来看，虽然硬件和模拟平台都在不断进步，但尚未达到需求，不能提供足够多的量子比特对现有的量子算法进行完全模拟。本文利用“神威·太湖之光”对量子傅里叶变换进行大规模模拟，基于现有的编程语言如 C，Python 等进行量子电路的抽象定义，并采用多级并行、众核加速、计算与通信隐藏的优化技术提高模拟效率，加快量子算法的研究、验证、优化。同时也可以验证神威超级计算机的量子模拟性能，促进并提高超算的性能优化与自我升级，拓宽我国自主可控超级计算机的应用领域。但我们没有考虑向量化版本，对其进行向量化优化可进一步提高模拟效率。

参 考 文 献

[1] WECKER D，SVORE K M. LIQUi|>：A software design architecture and domain-specific language for quantum computing [J]. arXiv：1402.4467，2014.

[2] HONG W J，LI K L，QUAN Z，et al. PETSc's Heterogeneous Parallel Algorithm Design andPerformance Optimization on the Sunway TaihuLight System [J]. Chinese Journal of Computers，2017，40(9)：2057-2069.

[3] MIAO X. Universal construction of unitary transformation of quantum computation with one-and two-body interactions[J]. arXiv preprint quant-ph/0003068，2000.

[4] TAHO X H，PANG J M，GAO W，et al. Performance Optimization of FT Program Based on SW26010 Processor[J]. Computer Science，2019，46(4)：321-328.

[5] LI R L，WU B J，YING M S，et al. Quantum Supremacy Circuit Simulation on Sunway TaihuLight[J]. arXiv：1804.04797.

[6] HÄNER T. Steiger D S. 0.5 petabyte simulation of a 45-qubit quantum circuit[C]// International Conference for High Performance Computing. 2017.

[7] LIU X，GUO H，SUN R J，et al. The Characteristic Analysis and Exascale Scalability Research of Large Scale Parallel Applications on Sunway TaihuLight Supercomputer [J]. Journal of Computer，2018，14(10)：2209-2220.

[8] WANG Y H，ZHANG H G，WU W Q，et al. Quantum Algorithms for Breaking RSA Based on Phase Estimation and EquationSolving[J]. Journal of Computer，2017，40(12)：2688-2699.

[9] WANG M Q，LI M，ZHANG Q，et al. Speedup of GMRES Based on MIC Heterogeneous Cluster Platform[J]. Computer Science，2017，44(4)：197-201，240.

[10] WANG K M. Parallelism of Quantum Computing and its Philosophical Significance [D]. Taiyuan：Shanxi University，2008：669-677.

LIU Xiao-nan，born in 1977，Ph.D，associate professor，master's supervisor，is a member of China omputer Federation. His main research interests include quantum algorithm，high-performance parallel computation.

JING Li-na，born in 1996，postgraduate，is a member of China Computer Federation. Her main research interests include quantum algorithm and so on.