计算机科学
COMPUTER SCIENCE

早期量子算法在量子通信、量子纠错等领域的应用

Renata WONG

引用本文

Renata WONG. 早期量子算法在量子通信、量子纠错等领域的应用[J]. 计算机科学, 2022, 49(6A): 645-648.

Renata WONG. Application of Early Quantum Algorithms in Quantum Communication,Error Correction and Other Fields[J]. Computer Science, 2022, 49(6A): 645-648.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210400214

早期量子算法在量子通信、量子纠错等领域的应用

Renata WONG
南京大学计算机科学与技术系　南京 210023

摘　要　当今量子算法的一个发展方向是对早期量子算法的再思考。在量子计算领域,每一种早期量子算法都提出了突破性概念。一般认为它们在很大程度上仅属理论范畴,原因它们所求解的问题几乎都没有实用价值。但这些早期量子算法依然重要,因为它们在解决问题的速度上相比经典算法呈指数级别的增长。文中做了两件工作:一方面详细阐述对早期量子算法再思考的最新进展,另一方面则对早期量子算法进行所谓的重新目的化,即重新用于量子密钥分发、纠错等领域。Deutsch-Jozsa 算法、Bernstein-Vazirani 算法和 Simon 算法是关注的重点。Deutsch-Jozsa 算法用于判定多引数函数(Multi-argument Function)是平衡的还是常数的。最近的研究表明,其应用可以扩展到量子通信和形式语言(Formal Languages)领域。Bernstein-Vazirani 算法能够搜索出在函数中编码的字符串,其应用可以扩展至量子密钥分发领域和通信中对信息的纠错处理。Simon 算法则用于求解具有特定属性字符串的识别问题,它的现代应用包括量子通信和纠错。

关键词:量子算法;量子计算;Deutsch-Jozsa 算法;Bernstein-Vazirani 算法;Simon 算法;量子密钥分发;量子纠错
中图法分类号　TP3-0,TP39

Application of Early Quantum Algorithms in Quantum Communication, Error Correction and Other Fields

Renata WONG
Department of Computer Science and Technology, Nanjing University, Nanjing 210023, China

Abstract　At present, a development direction of quantum algorithm is to rethink the early quantum algorithms. Each of them involves an important, groundbreaking concept in quantum computing. They are generally considered to only belong to the theoretical category due to the fact that the problems they solve are of little practical value. However, they are still important as they can solve a problem exponentially faster than a classical algorithm. Here, this paper elaborates on some recent developments in repurposing the early quantum algorithms for quantum key distribution and other fields. It especially focuses on Deutsch-Jozsa algorithm, Bernstein-Vazirani algorithm and Simon's algorithm. The Deutsch-Jozsa algorithm is used to determine whether a multi-argument function is balanced or constant. As recent research shows, it can be extended to application in the field of quantum communication and formal languages. The Bernstein-Vazirani algorithm finds a string encoded in a function. Its application can be extended to quantum key distribution and error correction. Simon's algorithm tackles the problem of identifying a string with a particular property. Its modern applications include quantum communication and error correction.

Keywords　Quantum algorithms, Quantum computing, Deutsch-Jozsa algorithm, Bernstein-Vazirani algorithm, Simon's algorithm, Quantum key distribution, Quantum error correction

1　引言

在计算机科学和物理学中,量子计算均是一门新兴学科。第一批量子算法在上世纪 80 年代和 90 年代才被发现。其中一些最值得注意的算法有 Deutsch-Jozsa 算法[1]、Bernstein-Vazirani 算法[2]、Simon 算法[3]、Grover 搜索算法[4]和 Shor 的整数分解算法[5]。Shor 的整数分解算法有具体的用途,通常被用于加密系统。Grover 算法亦有具体用途,即在数据库里寻找一个或多个具有所需特征的元素。它与 Shor 算法的不同之处在于它有较多其他的用途,譬如,确定所需特征元素的数量[6]、求解分团问题[7]、求解最大独立集问题[8]和求解蛋白质折叠问题[9]。

在 Shor 和 Grover 的量子算法被认为具有实际用途的同时,Deutsch-Jozsa,Bernstein-Vazirani 和 Simon 的算法多半被视为仅具有理论价值。与经典算法相比,这些量子方法提供了指数级加速。这几种算法分别对此演示出一个既简单亦重要的证明。尽管曾经被认为没有什么实际用途,这些算法在近期都成功地扩展到新的应用领域,尤其在量子通信、量子密码学和纠错方面。

本文讨论了对这些算法进行的一些最新修改,修改的目的是使其适用于其他领域。尽管看起来简单,这些修改却都要求对量子计算和量子信息原则有充分的理解。有关量子计算的基本概念以及量子力学的假设,可参考文献[10]。

2　Deutsch-Jozsa 量子算法及其在量子密钥分发领域的应用

2.1　Deutsch-Jozsa 量子算法

Deutsch-Jozsa 算法[1]用于判定具任意引数量的一个布尔函数 $f(x):\{0,1\}^n\rightarrow\{0,1\}$ 为常数或平衡。如 $f(x)=c\in\{0,1\}$,则该函数为常数。如该函数的输入域一半的输出为

通信作者:Renata WONG (renata.wong@protonmail.com)

0，而另一半的输出为1，则该函数为平衡。

在这个算法中，函数 f 以量子 oracle(黑盒)$U_f:|x\rangle|y\rangle\rightarrow|x\rangle|f(x)\oplus y\rangle$ 执行，其中 $\oplus$ 是模2加法。该算法从 $|\psi_0\rangle=|0\rangle^{\otimes n}|1\rangle$ 态开始。前 n 个量子位构成第一个寄存器(Register)，包含了 U_f oracle，而最后一个量子位则是第二个寄存器，包含用于相位反冲(Phase Kickback)的量子位。接下来，将 $n+1$ 量子位的 Hadamard 变换应用于两个寄存器，从而得出 $|\psi_1\rangle=\sum_{x\in\{0,1\}^n}\frac{|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$。然后，应用 oracle U_f 后得出 $|\psi_2\rangle=\pm\sum_{x\in\{0,1\}^n}\frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$。这时，最后一个量子位可以忽略，因为相位反冲已发挥了作用。此后，该量子位再也不会有变化。下一步将 Hadamard 变换应用于第一个寄存器并得出 $|\psi_3\rangle=\pm\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\frac{(-1)^{f(x)+x\cdot y}|y\rangle}{2^n}$，其中，$x\cdot y$ 是模2的按位内积。这时，可以测量第一个寄存器。如 f 是常数，则能够观察到 $|y\rangle=|0\rangle^{\otimes n}$ 的概率是1(相长干涉)。如 f 是平衡，则观察到 $|y\rangle=|0\rangle^{\otimes n}$ 的概率是0，并且可以观察到不同于 $|0\rangle^{\otimes n}$ 的态(相消干涉)。

2.2 Deutsch-Jozsa 量子算法在密钥分发上的应用

与现有的任何确定性经典算法相比，Deutsch-Jozsa 算法提供了指数加速，因而有可能在其他领域中提供类似的加速。Nagata 等[11]考虑了一个有趣的情节，即使用 Deutsch-Jozsa 算法，让 Alice 和 Bob 通过一个密钥分发机制来安全地进行通信(Alice，Bob 和 Eve 属于量子通讯领域中的常规称呼，即 Alice 通常指通讯发起者，Bob 指通讯接收者，Eve 则指通讯的潜在窃听者)。Alice 和 Bob 的这个情节利用了形式为 $|GHZ\rangle=\frac{|0\rangle^{\otimes m}+|1\rangle^{\otimes m}}{\sqrt{2}}$ 的 GHZ(Greenberger-Horne-Zeilinger)态，以及 Ekert'91 协议[12]。文献[11]中提出的算法以量子态 $|\psi_0\rangle=\frac{|1\rangle^n|0\rangle+|0\rangle^n|1\rangle}{\sqrt{2^{n+1}}}$ 为起点。根据此态的结构/形式，我们可以轻易确认如何制备此态：将 Pauli X 闸应用于前 n 个量子位，将 Hadamard 闸应用于最后一个量子位，再应用 n 个 CNOT 闸(每个 CNOT 闸都将最后一个量子位用作其控制量子位，而将第一个寄存器中的 n 个量子位中的一个用作其目标量子位)。然后应用 $n+1$ Hadamard 量子闸，从而得出 $|\psi_1\rangle=\frac{1}{\sqrt{2}}\left(\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]^n\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]+\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]^n\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\right)$。再然后，应用 oracle U_f，随后再应用一次 $n+1$ Hadamard 量子闸。若该函数为常数，则结果为纠缠态 $|\psi_2\rangle=\pm\frac{|1\rangle^n|0\rangle\pm|0\rangle^n|1\rangle}{\sqrt{2}}$；若该函数为平衡，则结果为非纠缠态 $|\psi_2\rangle=\pm\frac{|1\rangle^n|0\rangle\pm|1\rangle^n|1\rangle}{\sqrt{2}}$。最后一步是执行 GHZ 测量，而其4个基态为 $|\Psi_+\rangle=\frac{|1\rangle^n|0\rangle+|0\rangle^n|1\rangle}{\sqrt{2}}$，$|\Psi_-\rangle=\frac{|1\rangle^n|0\rangle-|0\rangle^n|1\rangle}{\sqrt{2}}$，$|\Phi_+\rangle=\frac{|1\rangle^n|1\rangle+|0\rangle^n|0\rangle}{\sqrt{2}}$ 和 $|\Phi_-\rangle=\frac{|1\rangle^n|1\rangle-|0\rangle^n|0\rangle}{\sqrt{2}}$。对 $|\psi_2\rangle$ 进行 GHZ 测量时，我们将看到 GHZ 4个基态中的一个。若该函数为常数，则看到此态的概率为1；若该函数为平衡，则看到此态的概率为 $\frac{1}{2}$[11]。

为了安全地分发量子密钥，Alice 和 Bob 按照文献[11]中给出的 Ekert'91 协议[12]所指示的步骤进行操作：1)Alice 制备 $|\psi_1\rangle$，然后将其发送给 Bob；2)Bob 选定一个函数，然后先将 oracle、再将 Hadamard 闸应用于 $|\psi_1\rangle$；3)Bob 将 $|\psi_2\rangle$ 态的前 n 个量子位发送回 Alice；4)Alice 进行一次 GHZ 测量，以了解该函数是平衡还是常数。因此，Alice 和 Bob 共享一个密钥，即该函数的类型。此外，若该函数属常数而测量结果不为1，则 Eve(第三方)必然进行了窃听，因此必须放弃原来的密钥。若 Bob 选择一个平衡函数，此协议则无法检测 Eve 的监听。这是因为的窃听破坏了 GHZ 纠缠态，而平衡函数的 $|\psi_2\rangle$ 态本来就是纠缠态。

2.3 Deutsch-Jozsa 量子算法的其他应用领域

综上，修改后的 Deutsch-Jozsa 算法可用于基于 Ekert 91 协议的安全量子密钥分发。Ekert 协议是第一个使用纠缠态的量子密钥分发协议。使用经过修改的 Deutsch-Jozsa 算法的量子密钥分发以 $O(2^n)$ 倍优于经典算法。关于 Deutsch-Jozsa 算法的新应用，比较受关注的有文献[13]，用于另一种量子密钥分发协议；另一方面，文献[14]对原来的算法进行了修改，然后在形式语言的脉络中用于区分平凡和非平凡的单词。

3 Bernstein-Vazirani 量子算法及其在量子密钥分发和量子纠错中的应用

3.1 Bernstein-Vazirani 量子算法

Bernstein 和 Vazirani 要求解如下问题。对于 $\xi\in\{0,1\}^n$ 来说，函数 $f:\{0,1\}^n\rightarrow\{0,1\}$ 被定义为 $f(x)=\xi\cdot x=\sum_{i=0}^{n}\xi_i x_i\pmod 2=\xi_i x_i\oplus\cdots\oplus\xi_n x_n$，然后任务是要找出 ξ。

与 Deutsch-Jozsa 算法的情况一样，初始态为 $|\psi_0\rangle=|0\rangle^n|1\rangle$。通过 Hadamard 变换($|\psi_1\rangle$)和 oracle $U_f:|x\rangle|y\rangle\rightarrow|x\rangle|y\oplus f(x)\rangle$ 的应用，我们取得 $|\psi_2\rangle$ 态。再执行一次 Hadamard 变换后取得 $|\psi_3\rangle=\pm\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\frac{(-1)^{f(x)+x\cdot y}|y\rangle}{2^n}$。根据该函数的定义，我们有 $(-1)^{f(x)+x\cdot y}=(-1)^{\xi\cdot x+x\cdot y}=(-1)^{x\cdot(\xi\oplus y)}$。这时我们观察到，对于 y 的任一特定值来说，$\sum_{x\in\{0,1\}^n}(-1)^{x\cdot(\xi\oplus y)}=2^n\delta_{\xi,y}$，其中 $\delta_{\xi,y}=1$ 仅当 $\xi=y$。按此即有 $|\psi_3\rangle=\pm\sum_{y\in\{0,1\}^n}\frac{2^n\delta_{\xi,y}|y\rangle}{2^n}=\pm|\xi\rangle=\pm|\xi_1\xi_2\cdots\xi_n\rangle$。

经典算法需要 $2^{n/2}+1$ 个查询。量子算法则只需要一个查询即可建立字符串。因此，Bernstein-Vazirani 算法以指数级别优于经典算法。

3.2 Bernstein-Vazirani 量子算法在密钥分发上的应用

上述算法可用于文献[15]中提出的量子密钥分发。假设 Alice 和 Bob 同意使用函数 $f(x)=\xi\cdot x$。Bob 知悉值 $|\xi\rangle$，但值 $|\xi\rangle$ 却不为 Alice 所知悉。因此，Alice 首先要确立 Bob 所选择的字符串。在经典情节中，Alice 需要向 Bob 提问 n 个问题。在量子情节中，Alice 则只需要问一个问题即能获知该字符串。为了问这个问题，Alice 先要准备好 $n+1$ 个量子位的 $|\psi_0\rangle$ 态。她会对该态进行 Hadamard 变换，然后将所得态 $|\psi_1\rangle$ 发送给 Bob。Bob 使用他选定的 $|\xi\rangle$ 将 Bernstein-Vazirani 算法用于该态。然后，他将 $|\psi_2\rangle$ 的前 n 个量子位发送回 Alice。Alice 应用 Hadamard 变换，并取得 $|\psi_3\rangle$，从而获悉 Bob 所选定的字符串 $|\xi\rangle$。从而 Alice 亦获悉函数 $f(x)$。

经过此程序,此时 Alice 和 Bob 共享 n 位信息。

在经典的情节中,Alice 至少需要与 Bob 进行 n 次通信才能共享 n 位信息。因此,使用上面给出的 Bernstein-Vazirani 算法的量子密钥分发协议比经典协议快 n 倍。

3.3 Bernstein-Vazirani 量子算法在纠错上的应用

上述量子通信协议没有指定任何针对 Eve 窃听的保护措施,因此不如使用 Deutsch-Jozsa 算法安全,而且它还可能包含传输错误。误码不一定与窃听相关。低检测效率、传输损耗、不完善的纠缠源以及许多其他因素均会导致误报。纠错是一个重要的后处理过程,可以容忍实现制约,但又可同时确保传输密钥的准确性。通常,量子密钥分发协议通过协调机制来处理错误,例如 Alice 和 Bob 同意使用一个比特子集作为共享密钥,而不用整个字符串。文献[15]中演示了一种使用 Bernstein-Vazirani 算法纠正错误的方法。纠正方法如下。

Nagata 等[15]将函数重新定义为 $f(x)=g(x)\oplus h(x)$,其中 $g(x)=\gamma\cdot x$ 及 $h(x)=\eta\cdot x$,而 γ 是 Bob 拥有的字符串,η 是 Alice 拥有的字符串。由此而得出 $f(x)=\sum_{i=0}^{n}(\gamma_i\oplus\eta_i)\cdot x_i \pmod 2$。前面给出的 Bernstein-Vazirani 算法中的 $|\psi_3\rangle$ 态因而变为 $|\psi_3\rangle=\pm\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\frac{(-1)^{f(x)+x\cdot y}|y\rangle}{2^n}=\pm\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\frac{(-1)^{g(x)\oplus h(x)+x\cdot y}|y\rangle}{2^n}=\pm\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\frac{(-1)^{x\cdot(\gamma+\eta)+x\cdot y}|y\rangle}{2^n}$。此时我们有 $\gamma+\eta=(\gamma_1\oplus\eta_1,\cdots,\gamma_n\oplus\eta_n)$,随之取得 $\sum_{x\in\{0,1\}^n}(-1)^{x\cdot(\gamma+\eta)+x\cdot y}=2^n\delta_{\gamma+\eta,y}$;最后得出 $|\psi_3\rangle=\pm|\gamma+\eta$。换言之,Alice 能观察到 $|\gamma_1\oplus\eta_1,\gamma_2\oplus\eta_2,\cdots,\gamma_n\oplus\eta_n\rangle$ 态。因此,如果 Alice 测量第一个寄存器并获得字符串 $|010\cdots0\rangle$,那么她知道第二个量子位上出错,因为 $\gamma_2\oplus\eta_2=1$ 表示这些字符串元素彼此有异。据此,Alice 可以检测出与 Bob 进行量子通信时发生的错误。

3.4 Bernstein-Vazirani 量子算法的其他应用

如上所述,使用 Bernstein-Vazirani 算法的这种量子密钥分发不如使用 Deutsch-Jozsa 算法的协议,但是它的性能仍然以 n 倍优于经典协议。文献[16]给出了该算法的其他一些延伸应用,主要用于攻击分组密码。

4 Simon 量子算法及其在量子密钥分发中的应用

4.1 Simon 量子算法

Simon 要针对的问题可具体说明如下。假设有函数 $f(x):\{0,1\}^n\to\{0,1\}^n$ 将 n 位字符串映射到 n 位字符串。我们进一步假设该函数满足所有 x 的特性 $f(x)=f(x\oplus\xi)$,其中 $x\oplus\xi=(x_1\oplus\xi_1,x_2\oplus\xi_2,\cdots,x_n\oplus\xi_n)$。任务是找出字符串 ξ。Simon 量子算法求解了这个问题,速度比任何确定性或概率性经典算法更快,而且呈指数级别的加速。窍妙之处在于其设计减少了对 oracle 所需的查询数量,因而能够在确定 ξ 时实现这种加速。

该算法如下。初始态是 $|\psi_0\rangle=|0\rangle^{\oplus n}|0\rangle^{\oplus n}$。将 Hadamard 变换应用于前 n 个量子位取得 $|\psi_1\rangle=\sum_{x\in\{0,1\}^n}\frac{|x\rangle}{\sqrt{2^n}}|0\rangle^n$ 态。然后,应用 oracle $U_f:|x\rangle|y\rangle\to|x\rangle|f(x)\oplus y\rangle$,从而取得 $|\psi_2\rangle=\sum_{x\in\{0,1\}^n}\frac{|x\rangle}{\sqrt{2^n}}|f(x)\rangle$ 态。使用恒等式 $f(x)=f(x\oplus\xi)$ 后亦可取得 $|\psi_3\rangle=\sum_{x\in\{0,1\}^n}\frac{|x\oplus\xi\rangle}{\sqrt{2^n}}|f(x)\rangle$ 态。接下来,我们观察第二个寄存器。如果对其进行测量,那么第一个寄存器所呈现的态将与第二个寄存器上观察到的态相应(由量子叠加现象所造成),即第一个寄存器仅包含致使 $f(x)=y$ 的 x。因此,通过所假设的恒等式 $f(x)=f(x\oplus\xi)$,我们可以将该态记为 $|\psi_4\rangle=\frac{1}{2}(|\psi_2+\psi_3\rangle)=\sum_{x\in\{0,1\}^n}\frac{|x\rangle+|x\oplus\xi\rangle}{\sqrt{2^{n+2}}}|f(x)\rangle$。最后,我们在第一个寄存器上应用 Hadamard 变换而获得 $|\psi_5\rangle=H^{\oplus n}|\psi_4\rangle=\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y+(x\oplus\xi)\cdot y}|y\rangle|f(x)\rangle$。这与 $\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}(1+(-1)^{y\cdot\xi})|y\rangle|f(x)\rangle$ 相对应。若 $y\cdot\xi=1$,则概率幅度变作 0。因此,该态可以简化为 $|\psi_5\rangle=\frac{1}{\sqrt{2^n}}\sum_{y\cdot\xi=0}(-1)^{x\cdot y}|y\rangle|f(x)\rangle$。现在我们可以通过多次重复上述程序及测量寄存器 $|y\rangle$ 来确定字符串 ξ。该算法只需要对 oracle 进行 $O(n)$ 个查询,经典算法则至少需要 $\Omega(2^{n/2})$ 个查询。

与最佳确定性经典算法相比,Deutsch-Jozsa 算法展示出指数级别的量子改进;与最佳随机经典算法相比,Bernstein-Vazirani 算法展示出多项式的改进,其误差概率小于 1/3。Simon 算法结合了这两个特色,即在指数级别上优于有界误差随机经典算法的速度。Simon 算法只需要对 oracle 进行 $O(n)$ 个查询。经典算法则至少需要 $\Omega(2^{n/2})$ 个查询,这使得该问题成为一个经典的困难问题,即使使用经典概率算法亦是一个困难问题。

4.2 Simon 量子算法在密钥分发上的应用

文献[17]给出了 Simon 算法的一个可能应用:Alice 和 Bob 希望能安全地进行通信,于是就多周期函数 f 达成共识,即同意:对所有的 x 来说,$f(x)=f(x\oplus\xi)$。Bob 知悉周期 ξ,Alice 不知道。Alice 要获知 ξ,因此她制备了一个 $2n$ 量子位的 $|\psi_0\rangle$ 态,执行 Hadamard 变换后将 $|\psi_1\rangle$ 态发送给 Bob。Bob 选定一个 n 位的字符串 ξ,然后将 oracle 应用于 $|\psi_1\rangle$ 态而获得 $|\psi_2\rangle$。他将 $|\psi_2\rangle$ 发送给 Alice。Alice 将 Hadamard 变换应用于前 n 个量子位并对其进行测量。经过这个程序,Alice 获悉字符串 ξ。这时 Alice 和 Bob 共享 n 位信息,而这 n 位信息就是他们两人的密钥。

与 Bernstein-Vazirani 算法的情况一样,这个密钥分发协议的安全性不及基于 Deutsch-Jozsa 算法的密钥分发协议的安全性。Bernstein-Vazirani 协议和 Simon 算法协议均未使用纠缠现象,而纠缠是安全量子密钥分发中经常使用的特性。Simon 算法通常被应用于量子通信和密码学领域,文献[18]对此作出了一些引介。

5 隐子群问题

有些计算问题可以归约为隐子群问题(Hidden Subgroup Problem),而求解这类问题的量子算法在时间复杂度上相比经典算法有可能提供指数级加速。

定义 1(隐子群问题) G 为一个有限群,$H\leqslant G$ 是 G 的子群,X 为一个集合。如映射 $f:G\to X$ 满足 $\forall g_1,g_2\in G:f(g_1)=f(g_2)\equiv g_1H=g_2H$,则我们说映射 $f:G\to X$ 隐藏了子群 H。f 以 oracle 形式实现。通过查询 oracle 而对 f 求值,我们可以确定 H 的生成集 S。作为一个数学事实,生成集 $h_1,h_2,\cdots h_k\in H$ 具有 $k=O(\log n)$ 个元素。

其中可以归约为隐子群问题的一些最著名的量子算法有Shor的整数分解和离散对数算法[5]。整数分解算法可以归约为周期查找问题，因此用于其中的群 G 为 $\mathbb{Z}_n$，而用于离散对数问题的群 G 为 $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$，其中的 $\mathbb{Z}/n\mathbb{Z}$ 是模 n 整数的加法群。我们知道，当有关群属阿贝尔群时，多项式运行时间是可以实现的；但对于非阿贝尔群来说，通常不可以实现[19]。这一事实使 Shor 算法特别适合用于密码学领域。

如前文所示，这3个早期量子算法均可用于密码学。不出所料，这3个算法同时亦可以轻易地归约为隐子群问题。对于 Deutsch-Jozsa 算法来说，群 $G=\mathbb{Z}_2^n$，其中 $\mathbb{Z}_2$ 是整数模2的循环群。若该函数 f 是常数的，则我们要寻找的隐藏子群是 $H=\mathbb{Z}_2^n$；若 f 是平衡的，则我们要寻找的隐藏子群是 $H=\{0\}$，$0\in\mathbb{Z}_2^n$。对于 Bernstein-Vazirani 算法来说，$G=\mathbb{Z}_2^n$，而其隐藏子群是 $H=\{z\in\mathbb{Z}_2^n:\xi\cdot z=0\}$。对于 Simon 算法来说，$G=\mathbb{Z}_2^n$，但其隐藏子群是 $H=\{0,\xi\}$，其中 $0,\xi\in\mathbb{Z}_2^n$。

结束语 本文论述了有关早期量子算法用于量子密钥分发和其他领域的最新研究(见表1)。这些早期量子算法的一个重要优势是，相比经典算法，它们提供了指数级别的加速。在量子计算领域中寻找以指数级别优于经典算法的新量子算法非常困难。然而，某些算法可以归约为特定问题，譬如隐子群问题。因此，未来可以多个方向寻找新的多项式时间算法，譬如在隐子群问题框架内尝试各种阿贝尔群，看能否引出新的快速算法。另一种做法是为现有的快速量子算法寻找新的应用领域。这两个方向在量子计算研究中都十分活跃。值得注意的是，第一个方向的一个例子就是最近将 Grover 的搜索算法[4]、量子模拟算法[20]和整数分解算法[5]求解的问题归约为奇异值转换问题(Singular Value Transformation)[21]。直至文献[21]发表前，上述3个算法都被认为是不属于同一类型的问题。本文对第二个方向进行了调查。

表1 应用综述

Table 1 Summary of applications

算法	原来的应用	新应用
Deutsch-Jozsa	布尔函数是平衡的/常数的	安全量子密钥分发，形式语言中的单词区分
Bernstein-Vazirani	查找具有 $f(x)=\xi\cdot x$ 属性的字符串 ξ	量子密钥分发，纠错，对付分组密码
Simon	查找具有 $f(x)=f(x\oplus\xi)$ 属性的字符串 ξ	量子密钥分发

参 考 文 献

[1] DEUTSCH D, JOZSA R. Rapid solutions of problems by quantum computation [J]. Proceedings of the Royal Society of London A, 1992, 439: 553-558.

[2] BERNSTEIN E, VAZIRANI U. Quantum Complexity Theory [J]. SIAM Journal on Computing, 1992, 26(5): 1411-1473.

[3] SIMON D. On the Power of Quantum Computation [C]// Proceedings of the 35th Annual IEEE Sympo-sium on Foundations of Computer Science. 1994: 116-123.

[4] GROVER L K. A fast quantum mechanical algorithm for database search[C]// Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. 1996: 212.

[5] SHOR P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[6] BRASSARD G, HOYER P, TAPP A. Automata, Languages and Programming[C]// 25th International Colloquium ICALP'98. Aalborg, Denmark. 1998: 820-831.

[7] CHANG W L, YU Q, LI Z, et al. Quantum Speedup in Solving the Maximal-Clique Problem [J]. Physical Review A, 2018, 97: 032344.

[8] CHANG W L, CHEN J C, CHUNG W Y, et al. Quantum Speedup and Mathematical Solutions from Implementing Biomolecular Solutions for the Independent Set Problem on IBM's Quantum Computers [J]. IEEE Transactions on NanoBioscience, 2021, 20(3): 354-376.

[9] WONG R, CHANG W L. Quantum Speedup for Protein Structure Prediction [J]. IEEE Transactions on NanoBioscience, 2021, 20(3): 323-330.

[10] WONG R. The Uncertainty Principle as related to Quantum Computing [J]. Computer Science, 2020, 47(1): 40-50.

[11] NAGATA K, NAKAMURA T, FAROUK A. Quantum Cryptography Based on the Deutsch-Jozsa Algorithm [J]. International Journal of Theoretical Physics, 2017, 56: 2887-2897.

[12] EKERT A K. Quantum Cryptography Based on Bell's Theorem [J]. PRL, 1991, 67(6): 661-663.

[13] NGUYEN D M, KIM S. Quantum Key Distribution Protocol Based on Modified Generalization of Deutsch-Jozsa Algorithm in d-Level Quantum Systems[J]. International Journal of Theoretical Physics, 2019, 58: 71-82.

[14] BATTY M, CASSACCINO A, DUNCAN A J, et al. An Application of the Deutsch-Jozsa Algorithm to Formal Languages and the Word Problem in Groups[C]// TQC: Theory of Quantum Computation, Communication and Cryptography. 2008: 57-69.

[15] NAGATA K, NAKAMURA T. Quantum Cryptography, Quantum Communication, and Quantum Computer in a Noisy Environment [J]. International Journal of Theoretical Physics, 2017, 56: 2086-2100.

[16] XIE H Q, YANG L. Using Bernstein-Vazirani Algorithm to Attack Block-ciphers [J]. Designs, Codes and Cryptography, 2019, 87: 1161-1182.

[17] NAGATA K, NAKAMURA T, GEURDES H, et al. Quantum Communication Based on Simon's Algorithm [J]. International Journal of Emerging Engineering Research and Technology, 2017, 5(8): 28-31.

[18] CUI J Y, GUO J S, DING S Z. Applications of Simon's Algorithm in Quantum Attacks on Feistel Variants [J]. QIP, 2021, 20: 117.

[19] KITAEV A Y. Quantum measurements and the Abelian stabilizer problem [J]. arXiv: quant-ph/9511026.

[20] FEYNMAN R. Simulating physics with computers [J]. International Journal of Theoretical Physics, 1982, 21(6/7): 467-488.

[21] GILYEN A, SU Y, LOW G H, et al. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetic[C]// STOC 2019. 2019: 193-104.

Renata WONG, Ph. D. Her main research interests include quantum computing, foundations of physics and linguistics.