中国科学: 物理学 力学 天文学 2021 年 第 51 卷 第 8 期: 080301
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS

评 述

量子退火理论及其应用综述

王宝楠[1*], 水恒华[2], 王苏敏[3,4], 胡凤[3,4], 王潮[3,4,5]

1. 上海电力大学计算机科学与技术学院, 上海 200090;
2. 南京工程学院计算机工程学院, 南京 211167;
3. 上海大学, 特种光纤与光接入网重点实验室, 特种光纤与先进通信国际合作联合实验室, 上海 200444;
4. 密码科学技术国家重点实验室, 北京 100878;
5. 鹏城实验室量子计算中心, 深圳 518000
*联系人, E-mail: wbn_shu0099@163.com

收稿日期: 2020-10-14; 接受日期: 2021-01-06; 网络出版日期: 2021-05-21
上海市"科技创新行动计划"扬帆计划 (编号: 21YF1415100)、国家自然科学基金(编号: 61572304, 61272096, 61332019)和密码科学技术国家重点实验室开放课题基金项目资助

摘要 量子退火算法是在经典模拟退火算法基础上演进出来的一种新的量子优化算法. 与经典模拟退火算法利用热波动来搜索问题的最优解不同, 量子退火算法利用量子隧穿效应使得量子具有穿透比其自身能量高的势垒的能力, 从而使算法摆脱局部极值, 以更高概率逼近全局最优. 目前, 量子退火算法在组合优化类问题中已展现出良好的优化性能. 本文系统地综述了D-Wave量子计算机核心原理——量子退火算法的基本概念及其应用领域, 较为详细地分析了量子退火算法在密码学、旅行商问题、图着色问题、交通路径等领域的应用, 并对未来量子退火算法的更多待深化与探索的方向进行展望.

关键词 量子退火, D-Wave量子计算机, 量子计算

PACS: 03.67.Dd, 03.67.Lx, 85.35.Be, 66.35.+a

1 引言

优化问题表示为在满足一定的约束条件下, 在众多参数值或方案中寻找最优解或最优方案[1], 最终使得问题的某些性能指标实现最优解. 优化问题广泛地存在于信号处理、图像处理、生产调度、任务分配、模式识别、自动控制和机械设计等众多领域[2].

在信息科学、经济学和管理学等众多学科中, 不断涌现许多复杂的组合优化类问题. 传统的优化方法(如牛顿法等)无法在短时间内完成搜索, 在面对这些大型的优化问题时, 容易产生搜索的"组合爆炸"[1]. 由于实际问题应用中面临诸多难题, 如复杂性、问题的约束性等, 使得寻求高效的优化算法成为众多交叉学科的研究热点[1].

受自然现象或生物群体社会性、人类智能的规律启发, 研究者们提出众多智能优化算法解决实际应用领域的复杂难题, 如模仿鸟群和鱼群群体行为的粒子群算法、模仿自然界生物进化机制的遗传算法及模仿

引用格式: 王宝楠, 水恒华, 王苏敏, 等. 量子退火理论及其应用综述. 中国科学: 物理学 力学 天文学, 2021, 51: 080301
Wang B N, Shui H H, Wang S M, et al. Theories and applications of quantum annealing: A literature survey (in Chinese). Sci Sin-Phys Mech Astron, 2021, 51: 080301, doi: 10.1360/SSPMA-2020-0409

固体物质退火的模拟退火算法等. 这些智能算法通过模拟(演化)自然界的过程和模拟物种群体的智能行为得到发展和扩展.

模拟退火算法(Simulated Annealing, SA)的思想最早由Metropolis等人[3]于1953年提出; Kirkpatrick等人[4]于1983年第一次实现将SA引入组合优化问题中. 模拟退火过程描述为在给定初温下, 通过一定的进度表缓慢降低温度参数值, 使得SA在搜索空间里能够找到最优解.

与SA利用热波动搜索问题最优解不同, 量子退火算法(Quantum Annealing, QA)利用量子波动产生的量子隧穿效应来使算法摆脱局部最优, 从而以更大概率实现全局最优. 量子波动的优势在于它使得量子具有穿透比其自身能量更高的势垒的能力, 这一性能称为量子隧穿效应(Quantum Tunneling Effect). 1988年, Apolloni等人[5]提出将量子物理机制用于求解全局最优解的问题中, 成为一种改进的模拟退火算法. 由于加入了量子机制——量子隧穿效应, 这种改进算法更易找到全局最优解, 克服了传统模拟退火算法的降温速度慢、耗时久、计算量大等缺点. 量子退火算法是一类新的量子优化算法, 它其实是模拟退火算法的一种延伸和改进[6].

2 量子退火算法

最初量子波动用于寻找经典物理系统的能量最低态(基态). 通过在经典物理系统中引入穿透场(Tunneling Field), 也称为外界磁场, 来搜索系统空间的能量最小值, 其搜索过程描述为: 初始穿透场能量保持一个较大值, 使得粒子具有足够大的波动, 能够探索整个系统的能量空间; 然后根据一定策略缓慢减小穿透场的能量, 直至穿透场能量为零. 穿透场可以看作一个动能项, 与经典物理系统的势能场互不影响; 在缓慢减小穿透场强度的条件下使得量子系统恢复稳定, 最终粒子停留在基态, 也是能量最低态, 即待优化问题目标函数的最终解. 量子退火算法通过模拟上述过程来实现对目标函数的优化.

量子退火算法模型一般由两个部分构成: 第一部分为量子势能, 其目的是将量子优化问题与量子系统形成映射, 将优化的目标函数映射为施加在该量子系统的一个势场; 第二部分为量子动能, 通过引入动能项(幅度可控)作为控制量子波动的穿透场. 在势能和动能两个场的作用下, 量子系统的演化就可通过以下式(1)的薛定谔方程来描述:

$$\mathrm{i}\hbar\frac{\mathrm{d}}{\mathrm{d}t}\left|\psi(t)\right\rangle = H(t)\left|\psi(t)\right\rangle. \tag{1}$$

实际中, 直接求解薛定谔方程难度很大, 其计算复杂度随着问题复杂度的增加呈指数增长, 所以研究中通常采取随机过程进行模拟量子退火的过程(薛定谔方程直接求解的代价较大), 其中路径积分蒙特卡罗(Path Integral Monte Carlo, PIMC)是模拟量子退火过程的有效随机过程方法.

$$H(t) = H_{\mathrm{pot}}(t) + H_{\mathrm{kin}}(t), \tag{2}$$

式中, 量子哈密顿函数$H(t)$表示量子退火算法中的评价函数(Cost Function), $H_{\mathrm{pot}}(t)$表示势能, 对应模拟退火算法的评价函数, $H_{\mathrm{kin}}(t)$表示动能, 在动能中加入量子波动(初始值较大, 然后按照一定的进度表慢慢减小到零).

如图1所示, 在经典的热退火情况下, 系统要达到全局最小值, 必须克服$O(N)$的较大势垒ΔE, 其中N为系统的大小(温度为T时, 逃逸概率为$\exp(-\Delta E/T)$), 而在量子退火的情况下, 系统可以隧穿势垒. 如果势垒较窄, 隧穿概率为$\exp(-\omega\sqrt{\Delta E}/\Gamma)$, 其中$\Gamma$为隧穿波动场, ω为势垒宽度.

Kadowaki和Nishimori[7]于1998年提出通过引入横向磁场构造量子波动, 使得粒子具有量子隧穿效应, 从而具有穿越高且窄势垒的能力, 克服模拟退火仅能翻越势垒的缺陷.

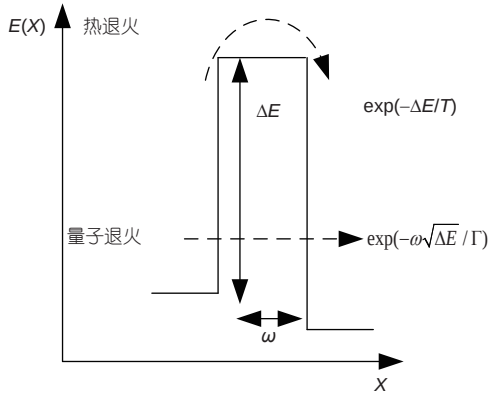

图 1 热退火与量子退火穿越势垒的比较[8]

Figure 1 Comparison of thermal annealing and quantum annealing crossing barrier [8].

如图2所示, 模拟退火算法只能通过翻越势垒的方式从局部最小值P到达全局最小值P'; 而量子退火算法凭借其量子隧穿效应, 可以直接从局部最小点P到达P'. 量子退火算法凭借其量子隧穿效应来跳出局部最优, 这也是与模拟退火相比一个最大的不同. 所以量子退火算法在某些问题上具有比模拟退火算法更好的性能.

量子退火算法的测试模型为横向场随机伊辛模型. 许多组合优化类问题先实现对伊辛模型的映射, 然后再通过量子退火算法进行求解. 横向场随机伊辛模型哈密顿函数为

$$H_{\rm p}=\sum_{i=1}^{N}h_i\sigma_i^z+\sum_{i,\,j=1}^{N}J_{ij}\sigma_i^z\sigma_j^z, \tag{3}$$

其中, h_i为能量偏移度, σ_i^z表示泡利自旋矩阵, J_{ij}表示自旋量i和j之间的耦合度.

根据伊辛模型的哈密顿函数, 可以得到量子退火的哈密顿函数为

$$H(t)=H_{\rm p}+\Gamma(t)\sum_{i=1}^{N}\Delta_i\sigma_i^x, \tag{4}$$

式中, Γ代表场强, 其诱导单个自旋状态向上和向下的转变, 它和模拟退火算法中的温度T作用类似. 任何表示为上述形式的优化问题都可以由量子退火算法处理.

与模拟退火基于热力学的原理不同, 量子退火算法主要利用量子涨落的机制, 即量子隧穿效应, 来完成优化过程. 量子退火算法的步骤表示如下:

步骤1 根据待优化问题, 构造量子系统的评价函数$H_{\rm q}=H_{\rm pot}+H_{\rm kin}$, 即量子哈密顿函数. 其中, $H_{\rm pot}$为势能, 即模拟退火算法中的评价函数, $H_{\rm kin}$为动能;

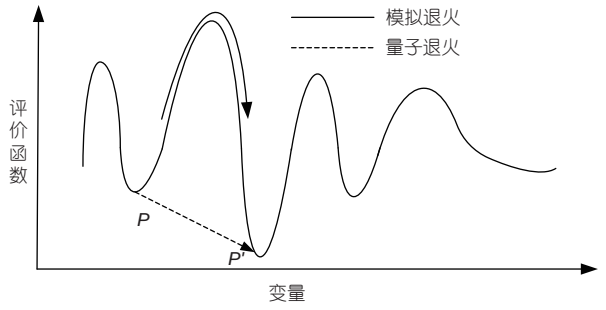

图 2 模拟退火算法与量子退火算法工作原理的比较

Figure 2 Comparison of the working principle of simulated annealing algorithm and quantum annealing algorithm.

步骤2 初始化各个参数, T_0为量子退火的初始温度, Γ为横向场强, 变化的横向场强引起不同量子状态之间的量子跃迁, 最大迭代次数为*MaxSteps*, 初始化状态为x, 对应的状态能量为$H_{\rm pot}(x)$;

步骤3 随机微扰产生新状态x', 对应的状态能量为$H_{\rm pot}(x')$;

步骤4 计算能量差$\Delta H_{\rm pot}=H_{\rm pot}(x')-H_{\rm pot}(x)$以及$\Delta H_{\rm q}=H_{\rm q}(x')-H_{\rm q}(x)$, 如果$\Delta H_{\rm pot}<0$或者$\Delta H_{\rm q}<0$, 则系统接受新解$x=x'$, 反之, 如果$\exp(\Delta H_{\rm q}/T)<rangdom(0,\,1)$, 则$x=x'$, 否则, 重复执行步骤3;

步骤5 进行退温操作, Γ的变化和模拟退火中的温度T作用类似, 横向场强变化形式为$\Gamma=\Gamma-(\Gamma_0/MaxSteps)$;

步骤6 判断是否满足终止条件Γ=0, 如果满足, 量子退火算法终止, 否则, 重复步骤3.

量子退火算法最早是由英国布朗大学的Finnila等人[9]提出, 主要是用来解决多元函数的最小值问题. 近年, 量子退火算法的理论研究和应用研究在国内外掀起了研究热潮, 也取得了很大的进展. 已有研究中, 量子退火算法在解决某些实际问题中展现出较好的优化效果[10–18]. 目前量子退火算法广泛应用于生物学[19]、密码学[20,21]、材料学[22–24]、化学[25,26]等领域. 与经典方法相比, 量子退火算法具有更高的收敛效率且能够以更高的概率更迅速地获得最优值. 量子退火算法可发挥有效的量子隧穿效应, 可克服传统算法易陷入局部极值的缺陷, 在指数级搜索问题中有望逼近甚至达到全局最优解, 是D-Wave量子退火的核心优势(量子退火算法为D-Wave量子计算机的核心原理), 也是D-Wave量子计算机商用化的基础.

3 D-Wave量子计算机的硬件结构分析

根据*Nature*[27], *Science*[28,29], *IEEE Spectrum*[30]的报道, 通用量子计算机的实用化遥遥无期, 亟需探索新的量子计算架构. 2019年谷歌量子芯片(Sycamore)不能在应用层面展示量子优势[31]. 因此, 亟需探索专用D-Wave量子计算机在各领域的应用潜力.

加拿大D-Wave公司于2007年首次推出的以量子退火算法为核心原理的专用量子计算机, 其采用完全不同于通用量子计算机的量子门电路构造思路. D-Wave公司是量子计算系统、软件和服务的开发和交

付的领导者, 并且是全球第一家量子计算机的商业供应商. D-Wave公司的任务是建立有助于解决人类最具挑战性问题的量子计算系统, 并通过结合物理学和计算机科学的知识来设计能够应对世界上最具挑战性问题的新型量子计算机.

D-Wave量子计算机发展迅猛, 目前具有5000多个量子比特. 已与Google, Lockheed Martin, 美国航空航天局, 美国国家实验室等众多机构合作. D-Wave量子计算机利用量子动力学来加速解决复杂的离散优化、约束满足、人工智能、机器学习、材料科学和模拟问题的新方法.

3.1 D-Wave量子硬件互连结构图

用户可以通过多种不同的方式向D-Wave系统提交问题, 如通过使用C, C++, Python或MATLAB中的程序来创建和执行量子机指令(QMI)等. D-Wave量子计算机会根据分布给出一些samples, 作为执行QMI文件的结果. 为了进一步解释这些samples和分布的定义, 引入以下几个核心概念.

第一个就是比特(Qubit), 如q这个单变量, 取值为0或1. D-Wave系统拥有多个qubits, 所以一般以下标方式区别不同的量子比特, 如q_i. 然而, 量子系统里的程序设计模型并不允许直接通过编译器对qubit进行赋值. D-Wave系统会根据qubits间的影响做出相应的响应. 一般有两种方式影响qubits: 第一种是通过权重(Weight)对比特进行控制, 如定义单量子比特q_i的系数为a_i; 第二种方式依赖于耦合强度(Coupler), coupler允许控制一个qubit施加到另一个qubit的影响. Coupler一般位于两个qubits之间, 也就是说coupler连接了qubits. Weight表征单量子比特qubit的系数值, 变量strength表征双量子比特之间的coupler值. 比如coupler连接q_i和q_j, 那么它们之间的strength表示为b_{ij}[32].

以下的目标函数通过定义4个变量来描述samples所符合的分布. 对于某个特定的输入, 会返回一个目标值[33]:

$$O(a,b;q)=\sum_{i=1}^{N}a_iq_i+\sum_{<i,j>}b_{ij}q_iq_j, \tag{5}$$

式中, 第一部分的N代表系统中的qubits的数量; 第二部分表示所有的coupler部分. 每个QMI都精确定义了目标函数中所有的系数a_i和b_{ij}, 最终会给出这个目标函数的最小值.

这里的关键点是将所需解决的实际问题转化为优化问题, 也就是将限制条件转换成weight和strength, 这样一旦目标函数得到最小值, 且满足限制条件的情况下, 目标函数的最小值对应实际问题的解决方案.

D-Wave的量子处理单元(Quantum Computing Unit, QCU)是互连的qubits组成的晶格, 比特间相互连接的结构称为奇美拉(Chimera)图. Chimera结构是由单元(Unit Cells)相互连接而成, 每个单元有8个qubits. 图3为9个单元组成的Chimera图, D-Wave 2000Q的Chimera结构由16×16的单元组成.

如图4所示, 每个顶点代表一个qubit, 每条边代表qubits之间的coupler. 为了解决没有多顶点结构的问题, 在逻辑qubits和couplers和实际物理qubits和couplers之间引入链(chain). 每个逻辑qubit对应与一个或多个相连的物理qubits, 多个相连的物理qubit称为chain. 图中每个点代表一个物理qubit, 标有相同字母的绿色区域的三个物理qubit即为一条链, 表示一个逻辑qubit. 为了实现逻辑qubits之间的coupler, 可以将第一个逻辑qubit链中的一些物理qubit和第二个逻辑qubit链中的其他qubit相连.

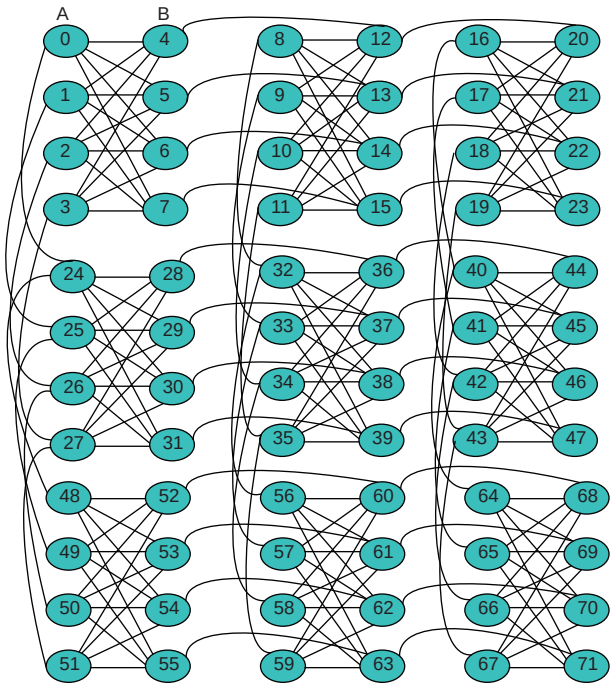

图 3 (网络版彩图) 9单元Chimera图

Figure 3 (Color online) Nine-unit Chimera figure.

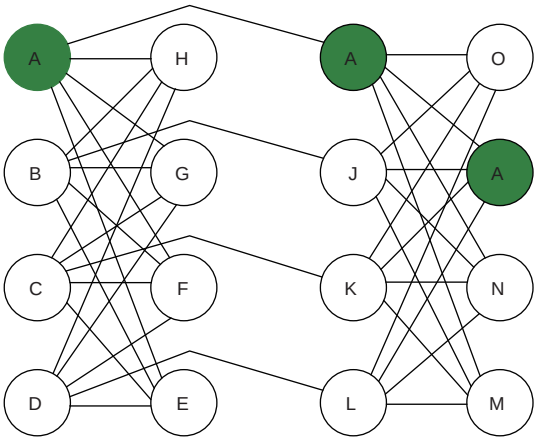

图 4 (网络版彩图)物理qubit间的“链”结构图

Figure 4 (Color online) Diagram of the “chain” between physical qubits.

3.2 D-Wave量子硬件互连结构缺陷分析

一个量子单元有两种形式: 十字行(Cross)或列行(Column). D-Wave One (128-Qubit), D-Wave Two (512-Qubit), D-Wave 2X (1024-Qubit)的量子芯片均采用量子簇column单元设计, 每一个小圆圈为一个物理量子比特, 每8个物理量子比特构成一个量子簇. 图5描述了物理qubits和couplers在D-Wave系统中对应于一个unit cell的局部图.

D-Wave在2020年9月29日宣布推出Advantage™量子系统. 该系统具有超过5000个量子位, 其采用Pegasus拓扑结构, 每个量子比特可与其他15个量子比特互连. 与Chimera拓扑结构相比, Pegasus拓扑结构的连通性提高了2.5倍, 使系统能以更少的物理量子比特处理更复杂的问题. 业内专家认为, D-Wave的2000量子比特系统的性能将与45个量子比特的超导系统(如谷歌、Rigetti或英特尔的设备)相近(45与2000的平方根相近)[34]. 也就是说, D-Wave的Pegasus拓扑结构新系统的性能将与拥有70–80个量子比特的超导系统相当.

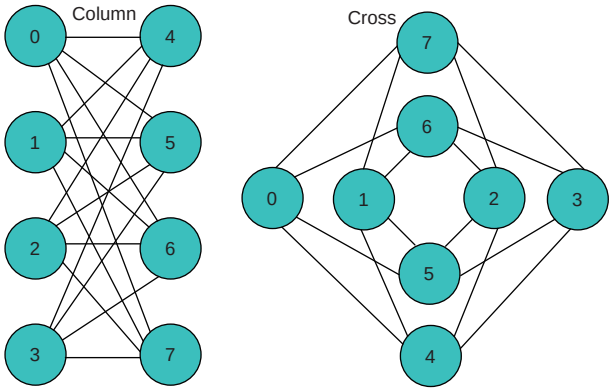

图 5 (网络版彩图)量子单元排列图

Figure 5 (Color online) Quantum element arrangement diagram.

D-Wave量子计算机研制进程中, 所需物理器件的硬件要求随着设备的构建技术与精度的不断提升而不断降低, 然而技术的提升与硬件要求的降低并不能解决D-Wave量子计算机硬件互连结构的缺陷.

(1) D-Wave硬件互连结构无法直接实现高于2个量子比特的耦合, 且Chimera拓扑结构中的每个物理量子比特能且仅能与之相邻的至多6个量子比特互连.

以上述Chimera拓扑结构图(图3)中的一个量子单元为例, 在一个量子单元内, 左侧垂直列的比特数字标号为“0”的量子比特可以与其他5个量子比特互连, 水平方向第一行第二列的量子单元中的比特数字标号为“12”的量子比特可以与其他6个量子比特互连.

(2) 任一量子单元自身的物理量子比特之间不存在互连关系, 即量子单元内部的量子比特间互相独立. 如图3所示, 将Column形式的量子单元分为A和B两组比特. A组比特数字标号分别为0, 1, 2, 3; B组比特数字标号分别为4, 5, 6, 7. 各组的4个qubits中的每个qubit都会和另外组的所有qubits相连接, 但是不会和同组内的其他qubit相连接.

(3) 量子单元与量子单元之间的可连接方式也是一一对应.

综上所述, 这些量子比特互连特性对将实际问题映射为量子自旋模型来说是一大难题[32].

4 量子退火算法的应用

量子人工智能提供了一种新的、不同于经典算法的量子计算模式. 典型的量子人工智能算法——D-Wave量子计算机核心原理的量子退火算法, 其特有的量子隧穿效应可避免传统算法易陷入局部极值的缺陷, 在飞控软件测试、图像识别、蛋白质折叠、金融分析、量子生物化学、交通、地球反演问题等领域取得了很好的效果[35].

本节主要介绍量子退火算法在密码学、旅行商问题、图着色问题、交通路径等领域的应用, 给出了它

们的理论基础和应用及在组合优化问题中的优缺点分析.

4.1 量子退火算法在密码学的应用

由于通用量子器件精度、量子操控可行性、硬件可扩展性等要求较高, 通用量子计算机进展缓慢. Google量子计算研究组负责人John Martinis (原加州圣巴巴拉分校教授)及Microsoft量子研究组首席研究员Matthias Troyer (原苏黎世联邦理工学院(ETH Zurich)教授)均指出通用量子计算机在短期内无法实现Shor算法破译实际RSA等典型应用. 因此, 在不具备突破性的量子纠错码等技术之前, 通用量子计算的小规模专用领域应用的实用性仍处于探索阶段, 寻找通用量子计算机的杀手级应用仍是一大挑战.

很少有学者关注和探索D-Wave专用量子计算机在密码学领域的研究与应用. 因此, 需探索专用D-Wave量子计算机在密码破译及密码设计领域的新计算架构. 本节主要介绍量子退火算法在密码破译与密码设计领域的应用与分析.

4.1.1 基于量子退火的整数分解

量子计算的发展对现有的公钥密码体制提出了严峻的挑战, 利用Shor算法就可攻击公钥密码RSA. 众所周知, RSA密码体制的安全性在于整数分解问题的困难性, 其所依赖的数论问题不能在有效的多项式时间内解决. 破译RSA的核心问题即整数分解问题[36]. 在传统方法中, 最快的整数分解算法为数域筛法(Number Field Sieve)[37,38], 但其复杂性是亚指数的, 即$O(\exp(c(\log_2 n)^{1/3}(\log_2\log_2 n)^{2/3}))$, 其中$c\approx1.92$.

1994年, Shor[39]提出一种整数分解的量子多项式复杂性算法, 它可以在多项式时间内解决整数分解问题. 业内长期以来认为Shor算法是唯一有效的攻击RSA的量子计算算法, 所以业内在抗量子密码的研究方面几乎仅考虑到Shor算法的潜在威胁.

尽管当前已有许多关于在量子计算硬件上实施Shor算法的尝试[40–45], 但通用物理器件的构建发展缓慢, *Science*, *Nature*和美国科学院的报道均认为实现Shor算法破译仍旧遥遥无期[27–29]. 因此, 纠错和量子操纵技术的精确性、短时间的退相干、易受噪音干扰等因素导致通用量子设备的进展缓慢, 限制了Shor算法的发展和实际应用. 当前, Shor算法最大分解的整数规模不超过整数100[45].

另一种量子绝热计算(QAC)[46], 也可用于解决整数分解问题. 基于量子绝热理论的核磁共振(Nuclear Magnetic Resonance, NMR)量子处理器最大可分解291311[47], 但不具通用性和扩展性. D-Wave原理量子退火实际也源自绝热量子计算, 它已被广泛用于采样、优化、机器学习等[18,22,48,49]. 很少有人提出将D-Wave应用于密码破译与设计领域. 王潮和张焕国[50]于2012年提出D-Wave的专用量子计算可用于破译RSA的猜想. 1QB信息技术公司研究者Dridi和Alghassi[49]通过引入计算代数几何, 将整数分解问题转化为二次无约束二进制优化(Quadratic Unconstrained Binary Optimization, QUBO)模型, 分别由细胞算法和分栏算法求解. 通过D-Wave 2X的实验表明, 用分栏算法实现897个比特分解200099. 美国普渡大学Jiang等人[51]根据整数二进制乘法表, 将目标函数转化为可由D-Wave退火处理器处理的伊辛模型, 该模型具有通用性和可扩展性, 实现以94个量子比特分解整数376289.

上海大学王潮研究组[52]在Jiang等人[51]的工作基础上通过根据乘法表中目标值及进位的约束条件减少量子比特数, 成功实现以89个量子比特分解整数1005973 (20-bit整数), 验证了D-Wave破译RSA公钥密码的理论可行性. Shor算法至少需要40多个量子比特才可达到同样20-bit整数的攻击效果, Shor算法所需精度及规模都远超当前通用量子计算机硬件水平[35].

2019年, 洛克希德·马丁公司Warren[53]提出能够分解1000以内所有正整数的通用模型, 且该方法不需使用任何先验的质因子信息, 实现D-Wave 2000量子位处理器分解最大整数7781.

尽管基于量子退火的整数分解可以分解百万整数, 但仍受D-Wave硬件连接限制[54], 且D-Wave量子退火精度受环境影响. 当前受限的D-Wave量子计算机难以分解20-bit以上的大数[52], 存在理论构建无法对应实际映射的限制. 因此, 单纯依靠量子计算机实现大数分解难以克服量子硬件自身所带来的限制, 即当前已有的量子计算模型, 包括通用量子计算机和专用D-Wave量子计算机, 均由于器件、算法等制约, 离实际分解大数遥远, 需考虑新的计算架构以实现可扩展的大规模整数分解.

2019年, 王宝楠等人[55]提出一种新的基于D-Wave原理量子退火的量子经典混合计算架构, 有望突破D-

Wave硬件设备受限的瓶颈.

在通用量子计算机发展受限的今天, Shor算法仅可实现理论验证性实验(分解规模不超过100), 专用量子计算方面虽然实现了20-bit整数的分解, 但仍存在D-Wave硬件受限问题. 在当前硬件连接受限的D-Wave量子计算机背景下, 从节约量子比特资源和提升量子退火精度两个方面, 可以有效地保证模型通用性的同时, 减少所需量子比特数, 提升量子比特的循环利用率, 将有望在真实D-Wave量子计算平台中展现更大优势.

因此, 这不仅从理论层面降低了密码破译实用化的量子硬件精度需求, 而且有望增强实际量子退火过程中对大数分解问题的描述精度, 在当前设备有限条件下拓展至更大规模问题, 具备实际意义. 将来设计抗量子密码需考虑来自D-Wave量子退火的攻击可行性.

4.1.2 量子人工智能密码设计

在信息科学领域, 主要包含三类量子计算环境下的密码理论研究: (1) 通用量子算法对公钥密码的计算攻击; (2) 抗量子密码研究, 如基于NP问题的格密码研究; (3) 量子密码研究, 目前更侧重量子密钥分发, 且都是国外学者提出的.

上海大学王潮团队[35]提出第四类研究: 量子人工智能密码, 旨在利用D-Wave量子计算机核心原理量子退火算法, 将密码设计问题映射为D-Wave量子退火能够处理的组合优化类问题, 其密码设计的思路和方案完全不同于传统密码理论设计和搜索分析. 2017年, 在国际上首次完成基于真实D-Wave 2000Q系统的抗多种密码攻击的布尔函数设计实验[54].

4.2 量子退火算法在旅行商问题领域应用

旅行商问题(Travelling Salesman Problem, TSP)描述为: 假设一个商人要拜访N个城市, 问题的约束条件为每个城市只能拜访一次, 而且最后要回到原地, 且路程为所有可能路径中的最小值[56].

TSP是组合优化中的一个NP难问题, 为量子退火算法实现的进一步基准测试提供了一个理想的平台, 在运筹学和理论计算机科学中非常重要. 许多实际中出现的问题都可以转化为旅行商问题的模型而得以解决. 最初, TSP是为解决交通运输问题的(如海空航线安排、邮件派送、车辆调度问题等). 此后, TSP问题渐渐在许多交叉学科等领域实现了进一步的拓展, 如结晶学中的结构分析问题、计算机布线问题、机器人路径规划、单个机器上的工序调度问题等.

下文具体介绍量子退火算法在求解TSP中的应用.

对于N个城市的TSP问题, 有值为0,1的$(N-1)\times(N-1)$维上三角矩阵$\mathbf{U}$, 若旅行者通过城市i, j间路线则$U_{ij}=1$, 否则为0. d_{ij}表示城市i,j的距离, 则整个旅行线路可表示为$H_{\text{tour}}(\mathbf{U})=\sum_{<i,j>} d_{ij}U_{ij}$. 由于$U_{ij}\in\{0,1\}$, 为构成哈密顿函数, 加入$\sum U_{ij}(U_{ij}-1)$,

$$H_{\text{TSP}}=\sum_{i=1}^{N-1}\sum_{j=i+1}^{N} d_{ij}U_{ij}+\sum_{ij}U_{ij}(U_{ij}-1). \tag{6}$$

TSP问题中, 每个城市仅与其他两个城市相连, 故有$\sum_{j(j\neq i)} U_{ij}=2$, 上述条件将$U_{ij}$的$N(N-1)/2$个变量分为两类: $K=N(N-3)/2$个变量属于类I, 其他的N变量可用类I表示. 由此, 可以重新定义$U_{ij}\in I$为U_k (k=1, K), 其他变量可用U_k表示.

在量子系统中, TSP问题的哈密顿可描述为K自旋的伊辛模型, $U_k\to(1+\sigma_z^k)/2$, σ_z^k为k qubit的泡利矩阵. 于是$H_{\text{TSP}}=\sum_{i=1}^{K}\sum_{j=i+1}^{K}J_{ij}\sigma_z^i\sigma_z^j+\sum_{i=1}^{K}v_i\sigma_z^i$, 量子退火系统中要加入与$H_{\text{TSP}}$不相关的动能项, 横向场中选择$H_{\text{kin}}=\Gamma(t)\sum_{i=1}^{K}\sigma_x^i$, 最终可得量子退火哈密顿函数为

$$H(t)=\sum_{i=1}^{K}\sum_{j=i+1}^{K}J_{ij}\sigma_z^i\sigma_z^j+\sum_{i=1}^{K}v_i\sigma_z^i+\Gamma(t)\sum_{i=1}^{K}\sigma_x^i. \tag{7}$$

初始时, $\Gamma(0)$足够大, 系统由H_{kin}决定. 然后Γ随时间按一定的退火规则下降, 直至为0. 若退火过程足够慢, 根据量子系统的绝热定理, 系统总是保持在哈密顿函数的瞬时基态. 最终, $H(t)$变为H_{TSP}, 系统获得基态.

2004年, Martonák等人[11]将量子退火算法应用到解决旅行商问题, 指出应用量子退火算法最重要的两点: (1) 怎么描述希尔伯特空间; (2) 怎么设计量子哈密顿函数. 通过一个量子耦合函数把TSP问题转化为一个高度受限伊辛自旋问题, 在标准的横向伊辛模型下, 借助PIMC用量子退火算法实现一个N=1002的TSP问题, 并与模拟退火算法进行比较, 实验结果表明量子退火算法的搜索效率比模拟退火算法要好(量子退火算法需要10^4MC步数, 而模拟退火算法需要10^5MC

步数).

2011年, 国内学者陈宏伟等人[57]提出将量子退火算法应用于旅行商问题中, 并成功实现用核磁共振(NMR)量子模拟器模拟相应的薛定谔方程的演化, 从而在实验上证明了量子退火算法方法在旅行商问题简化版本中的应用. 实验结果明确地得出了最佳的行驶路线, 与理论预测吻合良好. 与门模型相比, 该方法的主要优点是对来自外部控制和环境的错误具有鲁棒性.

2015年, Microsoft量子研究组首席研究员Troyer(原苏黎世联邦理工学院教授)等人[58]考虑将量子绝热算法应用于TSP, 提出一种将TSP问题映射到伊辛自旋哈密顿量的新型映射方式, 并将其与以前的已知映射进行比较. 通过直接微扰分析、幺正演化和模拟量子退火方式, 证明了这种新型映射具有明显的优越性, 并讨论这一优势如何转化为TSP在量子退火炉上的实际物理实现.

2017年, 苏黎世联邦理工学院Heim等人[59]以TSP为例, 说明了在量子退火硬件上实施优化问题时要考虑的方面和面临的挑战. 并且证明, 如果量子动力学不能很好地适应TSP, 局部极小值之间的隧穿可以指数级地被抑制. 此外表明, 不等式约束是在模拟量子退火器上实现的主要障碍. 可编程数字量子退火器可以克服这些障碍, 并且一旦有足够大的量子计算机存在, 便可以为在大量问题上使用量子退火提供一条有趣的途径.

2019年, 洛克希德·马丁公司Warren[60]分析了在D-Wave量子退火机上求解对称旅行商问题的4个软件程序. 其中3个是用来寻找近似解的, 另一个被设计用来寻找最佳旅行解. 这些程序证明了一个应用程序可以同时运行在经典和量子计算平台上, 并可充分发挥各自的最大优势.

上述量子退火算法在旅行商问题的应用清楚地表明了该算法选择最优出行路线的优势, 与理论预测吻合较好. 通过对量子退火问题的量子绝热演化的研究, 发现了量子退火算法是解决TSP的极具前景的工具.

4.3 量子退火在图着色问题的应用

图着色问题(Graph Coloring Problem, GCP)又称着色问题, 是最著名的NP完全问题之一. 数学定义: 给定一个无向图$G=(V, E)$, 其中V为顶点集合, E为边集合, 每条边含有一对顶点. 图着色问题即为将V分为K个颜色组, 每个组形成一个独立集, 即其中没有相邻的顶点. 其约束条件为两个: (1) 着的颜色数目为K; (2) 每条边(相邻的顶点)必须着不同的颜色.

设图G需要最少的颜色数目为$X(G)$, V_j为颜色j的顶点集合, 此时顶点集合V分为独立集$V_1,\ldots,V_k$, $X(G)\leq k\leq|V|$, 优化问题即令k尽可能接近$X(G)$.

近年来一些启发式算法成功应用于求解GCP, 包括模拟退火、禁忌搜索以及混合演化算法. 这些算法求解GCP大致过程可概括为: 先将对$X(G)$的高度估值作为k值, 然后逐渐缩小k, 直到不存在为止.

2010年, Titiloye和Crispin[12,13]将量子退火算法应用到GCP上, 分别给出了模拟退火和量子退火在GCP上的具体实现算法, 并在MinGW C++软件环境下进行了仿真实验, 实验数据表明在搜索效率和成功率上量子退火算法都比模拟退火算法高(模拟退火算法成功率在70%–80%, 但是量子退火算法成功率接近100%; 5 h内量子退火算法完成了19幅图的着色问题, 模拟退火算法只完成了8幅图).

2013年, D-Wave白皮书[33]通过简单的地图着色问题描述如何通过执行一个量子机器执行文件(QMI)控制模型进行参数配置找到最优值. 用户需要将地图着色问题映射成一种在大规模空间中寻找最低点的搜索模式, 其中最低点就对应着问题的输出解. 这个处理器可以同时考虑所有可能性最终得到最低能量.

2016年, 美国航天局艾姆斯研究中心量子人工智能实验室的Tran等人[61]提出量子经典混合处理器解决复杂问题, 并比较了3个调度领域的问题: 图着色型调度、简化火星着陆器任务调度和机场跑道调度. 受目前量子退火硬件的限制, 仅能测试小尺寸的问题. 实验表明, 与标准的经典方法相比, 从量子退火器获得的信息可以用于更有效的剪枝搜索和改进启发式搜索.

2018年, 东京学者Kudo[62]研究了一种基于实时量子动力学的图着色量子退火算法. 该方法选择了一个驱动哈密顿量, 使约束条件自然满足而不受惩罚项的限制, 并大大降低了希尔伯特空间的维数. 总的哈密顿量由驱动哈密顿量和问题哈密顿量组成, 就像一个无序的量子自旋链. 小型系统中的实时量子仿真显示出有趣的结果, 并为量子退火提供了新的见解.

量子退火算法是一个新的启发式算法, 已有研究证明了该算法在解决图着色、TSP、伊辛自旋等问题

时比模拟退火算法更加有效. 模拟退火算法通过在Metropolis蒙特卡罗模拟过程中, 逐步将温度降低至0获得评价函数的全局最小值. 这一过程利用温度跨越势垒, 防止搜索陷入局部最小. 量子退火算法引入量子波动扩展了模拟退火算法, 通过量子隧穿效应来搜索全局最小.

4.4 量子退火在交通领域的应用

量子退火算法属于元启发式工具类问题, 适用于求解二进制优化问题. D-Wave Systems制造的量子退火的硬件QPU被设计来解决复杂的组合优化问题. 文献[63,64]已显示如何使用这些QPU来执行复杂的采样和优化任务, 以及qubits的性质如何在解决方案的计算中发挥作用. QPU设计用于解决QUBO问题, 其中每个量子位代表一个变量, 量子位之间的耦合器代表与量子位对qubit pairs相关联的耗散成本. QPU是具有量子位作为顶点以及耦合器作为量子位间边的无向图的一个物理实现. QPU旨在最小化的QUBO的功能形式为

$$\mathrm{Obj}(\mathbf{x},\mathbf{Q}) = \mathbf{x}^{\mathrm{T}}\cdot\mathbf{Q}\cdot\mathbf{x}, \tag{8}$$

其中, $\mathbf{x}$是大小为N的二进制变量的向量, $\mathbf{Q}$是描述变量之间关系的$N\times N$实值矩阵. 给定矩阵$\mathbf{Q}$, 找到二进制变量分配以最小化在式(8)中的目标函数形式等效于最小化伊辛模型, 这是已知的NP难题.

2013年Alan等人[65]在IEEE会议上提出将量子退火应用于限量的车辆路径问题, 通过设计一个结合量子退火算法和经验参数调整的旋转编码方案, 对26个汽车路径标准实例进行了测试. 实验结果表明, 量子退火算法能以极高的成功率获得路径的优化, 且优化后性能得到大幅提升.

在2017年, CeBIT, 大众集团作为第一家制造商与D-Wave合作借助量子计算机提出第一个交通拥堵优化项目[48]. 交通流量优化问题的目的是通过最大限度地减少所有道路段的总拥挤量, 最小化给定的一组汽车在其各个初始点和目的地之间行驶的时间. 单个路段的拥塞由在特定时间间隔内车辆行驶在这个路段上的数量的一个二次方程决定.

但是目前呈现的问题是交通流量优化的简化版本, 因为它只包含一个有限的汽车, 没有通信基础设施, 没有其他交通参与者, 没有其他优化目标, 除了最小化道路拥堵. 未来, 考虑以上参数及将这些参数创造性地作为QUBO问题的一部分是一大挑战与难题.

2017年, 德国航空航天中心Stollenwerk等人[66]提出了一类简化的空中交通管理(Air Traffic Management, ATM)问题(战略冲突解决)映射为QUBO问题. 根据冲突图对冲突解决问题的原始表示来执行映射, 其中图的节点表示飞行, 而边表示飞行之间的潜在冲突. 该研究混合使用经典求解器和D-Wave 2X和D-Wave 2000Q量子芯片对实例的硬度进行了基准测试. 初步结果表明, 对于合理的建模选择, 当前器件中可编程的最具挑战性的子问题在退火时间1 s内以99%的概率得到最优解.

2020年, Hussain等人[67]提出一种在人工网格结构的道路网络上优化控制随时间变化的交通信号以缓解交通流问题的QUBO格式, 并使用了D-Wave Systems的量子退火炉解决这个问题. 由于当前的D-Wave退火炉具有有限的量子位数量和有限的量子位间连通性, 采用混合(经典/量子)的方法来解决这个问题. 由于交通流是一个连续的、不断发展的现象, 研究者通过采用工作流来定期生成和解决多个问题实例的方式来解决这个时间依赖性问题.

D-Wave QPU从一代到另一代的量子位数量一直在增长, 鉴于这种趋势, 预计在未来几代QPU中, 能够通过量子机器学习, 量子模拟和量子优化直接嵌入更多现实世界的实时优化问题.

这些应用无一例外地都反映了量子退火算法在减少计算工作量、搜索精度和加快收敛速度等方面的优势. 尽管D-Wave量子退火仅可处理组合优化类问题, 但是通过将实际问题映射为D-Wave量子计算机可以处理的伊辛模型, 可以使得量子退火算法应用于更多领域.

5 总结与展望

量子退火算法凭借大自然对低能态的倾向性本质, 发挥量子隧穿效应具备穿越比其自身能量更高的势垒的能力, 以更大概率逼近局部最优甚至全局最优解, 可用于表征问题的最优解分布区域和最优演化方向. 与传统计算易陷入局部极值相比, 量子退火算法具有很大优势.

D-Wave量子计算机原理的量子退火算法在组合优化、机器学习、人工智能、生物化学模拟及通用量

子计算难以实用化的密码设计与密码破译等领域得以广泛应用, 已在中小型规模量子实验中完成理论探索与验证、应用拓展、性能优化等基础工作, 实现跨领域多学科应用.

量子算法理论和量子计算的基本框架已形成, 各方面的研究也取得了初步阶段的理论探索与验证. 随着量子技术的进步, 越来越复杂的量子退火设备变得可用. 虽然它们为解决优化问题提供了新的可能性, 但它们的真正潜力仍然是一个悬而未决的问题. 本文通过对量子退火算法在各个领域应用的介绍与分析, 为未来解决复杂现实世界问题的研究提供一些启示.

目前, 量子退火在组合优化问题中取得了很大的进步, 已有的研究成果仅仅是一个开端. 未来或许可以通过以下方面去进一步深化、探索量子退火算法在更多领域的应用.

(1) 目前尚不清楚什么样的条件下, 量子退火算法会优于经典模拟退火算法, 即以什么样的算法形式或优化目标函数才可使得量子退火算法优势发挥到极致. 并不是说量子退火算法一定都会有比模拟退火更好的表现, 比如在SAT问题上, 模拟退火有比量子退火算法更好的表现.

(2) 探索量子退火算法的退火进度表的参数选择, 使得最终参数的选择能够达到最优化的平衡点. 理论上量子退火算法的退火速度越慢越好, 但是同时消耗的CPU时间也就越长, 所以需要选择合适的退火进度表.

(3) 探索D-Wave专用量子计算机在其他密码部件设计的潜能.

(4) 探索量子经典混合计算架构在复杂现实世界问题中的应用.

(5) 增强现有的量子人工智能方法的实用性和扩展现有量子退火算法的应用范围.

参考文献

1 Su Y Y. Multi-objective Optimization Model for Diversion of Open Channel in Hydropower Project (in Chinese). Dissertation for Master's Degree. Wuhan: Wuhan University, 2018 [苏杨杨. 水电工程明渠导流多目标优化模型. 硕士学位论文. 武汉: 武汉大学, 2018]

2 Zhou X G. Global Optimization Algorithm for Nonconvex Optimization Problems (in Chinese). Dissertation for Doctoral Degree. Changsha: Central South University, 2010 [周雪刚. 非凸优化问题的全局优化算法. 博士学位论文. 长沙: 中南大学, 2010]

3 Metropolis N, Rosenbluth A W, Rosenbluth M N, et al. Equation of state calculations by fast computing machines. J Chem Phys, 1953, 21: 1087–1092

4 Kirkpatrick S, Gelatt C D, Vecchi M P. Optimization by simulated annealing. Science, 1983, 220: 671–680

5 Apolloni B, Cesa-Bianchi N, De Falco D. Quantum tunneling in stochastic and combinatorial opitimization. Parallel Architect Neural Netw, 1988, 27-29: 1–13

6 Zhang H T, Dai Y T, Tu L Y. Quantum annealing of the random-field Ising model based on transverse ferromagnetic interactions (in Chinese). J Huaqiao Univ (Nat Sci), 2016, 1: 7–11 [张洪涛, 代永涛, 涂玲英. 采用横向铁磁交互作用的随机场伊辛模型的量子退火算法. 华侨大学学报: 自然科学版, 2016, 1: 7–11]

7 Kadowaki T, Nishimori H. Quantum annealing in the transverse Ising model. Phys Rev E, 1998, 58: 5355–5363, arXiv: cond-mat/9804280

8 Rajak A, Chakrabarti B K. Quantum annealing search of Ising spin glass ground state(s) with tunable transverse and longitudinal fields. Ind J Phys, 2014, 88: 951–955, arXiv: 1405.3905

9 Finnila A B, Gomez M A, Sebenik C, et al. Quantum annealing: A new method for minimizing multidimensional functions. Chem Phys Lett, 1994, 219: 343–348

10 Huntsman S. Quantum simulated annealing. arXiv: 0012112

11 Martonák R, Santoro G E, Tosatti E. Quantum annealing of the traveling-salesman problem. Phys Rev E, 2004, 70: 057701, arXiv: cond-mat/0402330

12 Titiloye O, Crispin A. Quantum annealing of the graph coloring problem. Discrete Optimizat, 2011, 8: 376–384

13 Titiloye O, Crispin A. Graph Coloring with a Distributed Hybrid Quantum Annealing Algorithm. In: O'Shea J, Nguyen N T, Crockett K, et al., eds. Agent and Multi-Agent Systems: Technologies and Applications. KES-AMSTA 2011. Lecture Notes in Computer Science, vol 6682. Berlin, Heidelberg: Springer, 2011

14 Brooke J, Bitko D, Rosenbaum T F, et al. Quantum annealing of a disordered magnet. Science, 1999, 284: 779–781

15 Wei C, Zhu P M, Wang J Y. Quantum annealing inversion and its implementation (in Chinese). Chin J Geophys, 2006, 49: 577–583 [魏超, 朱培民, 王家映. 量子退火反演的原理和实现. 地球物理学报, 2006, 49: 577–583]

16 Wei C, Li X F, Zhang M G. Quantum annealing optimization and geophysical inverse method (in Chinese). Prog Geophys, 2007, 22: 785–789 [魏超, 李小凡, 张美根. 量子退火最优化与地球物理反演方法. 地球物理学进展, 2007, 22: 785–789]

17 Morita S, Nishimori H. Mathematical foundation of quantum annealing. J Math Phys, 2008, 49: 125210, arXiv: 0806.1859

18 Du W L, Li B, Tian Y. Quantum annealing algorithms: State of the art (in Chinese). J Comput Res Develop, 2008, 45: 1501–1508 [杜卫林, 李斌, 田宇. 量子退火算法研究进展. 计算机研究与发展, 2008, 45: 1501–1508]

19 Perdomo-Ortiz A, Dickson N, Drew-Brook M, et al. Finding low-energy conformations of lattice protein models by quantum annealing. Sci Rep, 2012, 2: 571, arXiv: 1204.5485

20 Su J, Tu T, He L. A quantum annealing approach for boolean satisfiability problem. In: Proceedings of the 53rd Annual Design Automation Conference. ACM, 2016. 148

21 Zhong M, Jia H H, Jiang L Y, et al. The optimization of DPA defense system based on quantum annealing algorithm (in Chinese). Netinform Secur, 2016, 3: 28–33 [仲明, 贾徽徽, 姜丽莹, 等. 基于量子退火算法的DPA防御系统优化. 信息网络安全, 2016, 3: 28–33]

22 Harris R, Sato Y, Berkley A J, et al. Phase transitions in a programmable quantum spin glass simulator. Science, 2018, 361: 162–165

23 King A D, Carrasquilla J, Raymond J, et al. Observation of topological phenomena in a programmable lattice of 1800 qubits. Nature, 2018, 560: 456–460, arXiv: 1803.02047

24 Kitai K, Guo J, Ju S, et al. Designing metamaterials with quantum annealing and factorization machines. Phys Rev Res, 2020, 2: 013319

25 Streif M, Neukart F, Leib M. Solving quantum chemistry problems with a D-Wave quantum annealer. In: International Workshop on Quantum Technology and Optimization Problems. Cham: Springer, 2019. 111–122

26 Xia R, Bian T, Kais S. Electronic structure calculations and the Ising hamiltonian. J Phys Chem B, 2018, 122: 3384–3395

27 Gibney E. Physics: Quantum computer quest. Nature, 2014, 516: 24–26

28 Brainard J. What's coming up in 2018. Science, 2018, 359: 10–12

29 Cho A. DOE pushes for useful quantum computing. Science, 2018, 359: 141–142

30 Dyakonov M. The case against quantum computing. IEEE Spectrum, 2019-03-24

31 Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574: 505–510, arXiv: 1910.11333

32 Wang B N. Quantum Artificial Intelligence Cryptography with D-Wave's Quantum Computer (in Chinese). Dissertation for Doctoral Degree. Shanghai: Shanghai University, 2020 [王宝楠. D-Wave量子人工智能密码研究. 博士学位论文. 上海: 上海大学, 2020]

33 Dahl E D. Programming with D-Wave: Map coloring problem. Technical Report. Burnaby: Corporate Headquarters, 2013

34 Calude C S, Calude E. The road to quantum computational supremacy. arXiv: 1712.01356

35 Wang B N, Hu F, Zhang H G, et al. From evolutionary cryptography to quantum artificial intelligent cryptography (in Chinese). J Comput Res Develop, 2019, 56: 2112–2134 [王宝楠, 胡风, 张焕国, 等. 从演化密码到量子人工智能密码综述. 计算机研究与发展, 2019, 56: 2112–2134]

36 Yan S Y. Quantum Computational Number Theory. Berlin: Springer, 2015

37 Lenstra A K, Lenstra Jr. H W. The Development of the Number Field Sieve. Berlin: Springer-Verlag, 1993

38 Kleinjung T, Aoki K, Franke J, et al. Factorization of a 768-bit RSA modulus. In: Conference on Advances in Cryptology. 2010

39 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the Annual Symposium on the Foundations of Computer Science. Los Alamitos: IEEE Computer Society Press, 1994. 124–134

40 Vandersypen L M K, Steffen M, Breyta G, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 2001, 414: 883–887, arXiv: quant-ph/0112176

41 Lu C Y, Browne D E, Yang T, et al. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. Phys Rev Lett, 2007, 99: 250504, arXiv: 0705.1684

42 Lucero E, Barends R, Chen Y, et al. Computing prime factors with a Josephson phase qubit quantum processor. Nat Phys, 2012, 8: 719–723, arXiv: 1202.5707

43 Politi A, Matthews J C F, O'Brien J L. Shor's quantum factoring algorithm on a photonic chip. Science, 2009, 325: 1221, arXiv: 0911.1242

44 Monz T, Nigg D, Martinez E A, et al. Realization of a scalable shor algorithm. Science, 2016, 351: 1068–1070, arXiv: 1507.08852

45 Geller M R, Zhou Z. Factoring 51 and 85 with 8 qubits. Sci Rep, 2013, 3: 3023, arXiv: 1304.0128

46 Farhi E, Goldstone J, Gutmann S, et al. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. Science, 2001, 292: 472–475, arXiv: quant-ph/0104129

47 Li Z K, Dattani N S, Chen X, et al. High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311. arXiv: 1706.08061

48 Neukart F, Compostella G, Seidel C, et al. Traffic flow optimization using a quantum annealer. Front ICT, 2017, 4: 29

49 Dridi R, Alghassi H. Prime factorization using quantum annealing and computational algebraic geometry. Sci Rep, 2017, 7: 43048, arXiv: 1604.05796

50 Wang C, Zhang H G. The impact of Canada's commercial quantum computer on cryptography (in Chinese). Inf Secur Commun Priv, 2012, 2: 31–32 [王潮, 张焕国. 加拿大商用量子计算机对密码学的影响. 信息安全与通信保密, 2012, 2: 31–32]

51 Jiang S, Britt K A, McCaskey A J, et al. Quantum annealing for prime factorization. Sci Rep, 2018, 8: 17667, arXiv: 1804.02733

52 Peng W C, Wang B N, Hu F, et al. Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. Sci China-Phys Mech Astron, 2019, 62: 060311

53 Warren R H. Factoring on a quantum annealing computer. Quantum Inf Comput, 2019, 19: 0252–0261

54 Hu F, Lamata L, Sanz M, et al. Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-wave quantum computer. Phys Lett A, 2020, 384: 126214

55 Wang B N, Yao H N, Hu F, et al. Quantum annealing distributed integer decomposition study of local field coefficient h and coupling coefficient J with stability Ising model (in Chinese). Sci Sin-Phys Mech Astron, 2020, 50: 030301 [王宝楠, 姚皓南, 胡凤, 等. 具有稳定性Ising模型局部场系数h和耦合项系数J的量子退火分布式整数分解研究. 中国科学: 物理学 力学 天文学, 2020, 50: 030301]

56 Li L. Research on Within-network Classification and Key Technology Based on Behavior Feature (in Chinese). Dissertation for Doctoral Degree. Changsha: National University of Defense Technology, 2017 [李乐. 基于行为特征的网络数据分类方法及关键技术研究. 博士学位论文. 长沙: 国防科学技术大学, 2017]

57 Chen H, Kong X, Chong B, et al. Experimental demonstration of a quantum annealing algorithm for the traveling salesman problem in a nuclear-magnetic-resonance quantum simulator. Phys Rev A, 2011, 83: 032314

58 Troyer M, Heim B, Brown E, et al. Improved mapping of the travelling salesman problem for quantum annealing. In: APS Meeting Abstracts. 2015

59 Heim B, Brown E W, Wecker D, et al. Designing adiabatic quantum optimization: A case study for the traveling salesman problem. arXiv: 1702.06248

60 Warren R H. Solving the traveling salesman problem on a quantum annealer. SN Appl Sci, 2020, 2: 75

61 Tran T T, Do M, Rieffel E G, et al. A hybrid quantum-classical approach to solving scheduling problems. In: Proceedings of the Ninth Annual Symposium on Combinatorial Search. 2016

62 Kudo K. Constrained quantum annealing of graph coloring. Phys Rev A, 2018, 98: 022301, arXiv: 1806.05782

63 O'Gorman B, Babbush R, Perdomo-Ortiz A, et al. Bayesian network structure learning using quantum annealing. Eur Phys J Spec Top, 2015, 224: 163–188, arXiv: 1407.3897

64 Raymond J, Yarkoni S, Andriyash E. Global warming: Temperature estimation in annealers. Front ICT, 2016, 3: 23

65 Alan C, Alex S. Quantum annealing algorithm for vehicle scheduling. In: Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. 2013

66 Stollenwerk T, O'Gorman B, Venturelli D, et al. Quantum annealing applied to de-conflicting optimal trajectories for air traffic management. IEEE Trans Intell Transp Syst, 2020, 21: 285–297

67 Hussain H, Javaid M B, Khan F S, et al. Optimal control of traffic signals using quantum annealing. Quantum Inf Process, 2020, 19: 312, arXiv: 1912.07134

Theories and applications of quantum annealing: A literature survey

WANG BaoNan[1*], SHUI HengHua[2], WANG SuMin[3,4], HU Feng[3,4] & WANG Chao[3,4,5]

[1] *College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 200090, China;*
[2] *School of Computer Engineering, Nanjing Institute of Technology, Nanjing 211167, China;*
[3] *China Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai 200444,China;*
[4] *State Key Laboratory of Cryptology, Beijing 100878, China;*
[5] *Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518000, China*

Quantum annealing (QA) algorithm is a new quantum optimization algorithm based on the classical simulated annealing (SA) algorithm. Unlike classical SA algorithm, which uses the thermal waves to search for the optimal solution, the QA algorithm uses the quantum tunneling effect to allow a quantum to penetrate a potential barrier with a higher energy than itself. Therefore, the algorithm can get rid of the local extreme values and is more likely to approach the global optimal with higher probability. In the literature, the QA algorithm has shown perfect optimization effects on combinatorial optimization problems. In this paper, the basic concepts and application fields of QA algorithm, which is the core principle of D-Wave quantum computer, are systematically reviewed. The applications of QA algorithm in cryptography, traveling salesman problem, graph coloring problem, and traffic path are discussed in detail. In addition, the direction of future research for QA algorithm is explored.

quantum annealing, D-Wave quantum computer, quantum computing

PACS: 03.67.Dd, 03.67.Lx, 85.35.Be, 66.35.+a

doi: 10.1360/SSPMA-2020-0409