

基于超立方体的多目标量子行走搜索算法

朱皖宁

(金陵科技学院软件工程学院, 江苏 南京 211169)

摘要:提出了可以解决多目标搜索的量子行走算法。量子行走是一种通用的量子计算工具,理论上可以实现任意量子算法。当前提出的基于量子行走的无结构数据库搜索算法只能进行单目标搜索。多目标搜索是一种更常见的问题。为了求解多目标搜索算法,基于超立方体上量子行走框架提出了新的硬币算子,通过对目标节点入边的幅度扩大,增加测量到目标节点的概率,最终解决了多目标搜索问题。最后证明了算法的查询复杂度为 $O\left(\sqrt{\frac{N}{M}}\right)$ 。

关键词:量子行走;超立方体;无结构数据库搜索算法

中图分类号:O413;TP301

文献标识码:A

文章编号:1672-755X(2018)02-0005-05

Multi-objective Searching Algorithm Based on the Quantum Walk on the Hypercube

ZHU Wan-ning

(Jinling Institute of Technology, Nanjing 211169, China)

Abstract: This paper presents a multi-objective searching algorithm based on the quantum walk. Quantum walk is a universal instrument in quantum computing. In theory, quantum walk can realize arbitrary quantum algorithm. At present, quantum walk searching algorithm on the unstructured database can only search single object. Multi-objective searching is able to solve more common problems. In order to solve the multi-objective searching problem by the quantum walk way, this paper presents a novel quantum algorithm by constructing a new quantum coin operator. This new coin operator can amplify the amplitude of the incoming edges of the target vertex, and then the amplitude of the target vertex will increase by performing the migration operator S . At last, this paper proves the query complexity of the algorithm is $O\left(\sqrt{\frac{N}{M}}\right)$.

Key words: quantum walk; hypercube; searching algorithm on the unstructured database

量子信息科学是结合了量子物理和计算机科学的一门交叉学科^[1-3]。利用量子的特殊物理性质,计算机科学研究领域中的很多瓶颈都被打破,如无条件安全通信、算法加速等。量子计算是量子信息科学中的重要分支之一。1994年,Shor基于量子傅里叶变换,提出了大数质因子分解算法,在最好的经典算法复杂度基础上有指数级的加速^[4]。1996年,Grover提出了一个全新的量子算法——在无结构数据库上进行搜索的算法^[5]。Grover搜索算法在最好的经典算法复杂度基础上有二次加速。由于大量的NP问题都

收稿日期:2018-04-11

基金项目:金陵科技学院高层次人才科研启动基金(jit-b-201624)

作者简介:朱皖宁(1983—),男,安徽淮南人,讲师,博士,主要从事量子计算、量子可逆逻辑综合、量子机器等方面的研究。

可以转换为一个多项式复杂度的判定问题和一个指数级复杂度的无结构数据库上搜索的问题,因此 Grover 算法的应用面广,意义重大。经过十几年的研究发展,在无结构数据库上的搜索问题有了很多不同的量子算法解决方案,基于量子行走的搜索算法就是其中一种。

量子行走是经典的随机行走在量子计算中对应的理论。不同于经典随机行走的是,量子行走有其特有的物理现象——量子干涉效应。由于量子干涉效应,量子行走的粒子扩散速度比经典随机行走有着二次加速。因此从理论上说,基于量子行走设计的算法将比经典随机行走有着二次加速。2003 年,Neil Shenvi 提出了一种基于量子行走的无结构数据库上搜索算法(Skw 算法)^[6]。在此后许多学者都基于 Skw 算法提出了新的量子算法。但是 Skw 算法在硬币算子中规定只能做单一目标搜索。当目标多于一个时,论文中定理 1 就无法成立。文献[7]在最后一节提出了一种在原算法基础上的改进方案,但是没有证明其正确性。

在无结构数据库搜索问题中多目标搜索更加常见,因此也更加重要。为了对 Skw 算法在多目标搜索的情况下进行推广,本文基于超立方体量子行走框架,提出了在多目标搜索情况下的搜索算法,假设搜索的目标有 M 个,那么查询复杂度为 $O\left(\sqrt{\frac{N}{M}}\right)$ 。

1 量子行走基础知识

由于直接将经典随机行走量子化会引起行走的塌缩,即朝一个方向行走的概率为 1,所以需要使用一些其他的方法来表示量子行走。当前最常用的方法有两种:基于“抛掷硬币”的量子行走和边上的量子行走^[8-9]。本文使用前一种方法。

基于硬币的量子行走将算法的运行空间 H 分成两个希尔伯特空间的张量: $H = H_l \otimes H_c$ 。其中 H_l 为位置空间,由节点向量张成; H_c 为硬币空间,由行走的方向向量张成。属于 H 的一个向量(带方向的行走者)可以表示为 $|\vec{x} \otimes |d\rangle$ 。算法的一步可以表示为:

1) 令行走者经过抛掷硬币算子 $(I \otimes C_0)$:

$$|\vec{x}\rangle \otimes |d\rangle \xrightarrow{I \otimes C_0} |\vec{x}\rangle \otimes |d'\rangle$$

2) 令行走者根据新的方向经过偏移算子 S 行走一步:

$$|\vec{x}\rangle \otimes |d'\rangle \xrightarrow{S} |\vec{x}'\rangle \otimes |d'\rangle$$

将算法迭代 t 次以后测量位置空间得到最终行走的结果。在超立方体上行走有更多的特殊性质。

2 基于超立方体的量子行走多目标搜索算法

2.1 量子行走多目标搜索算法

Skw 算法在自然推广到多目标搜索情况时,继续使用原文证明的推广形式是错误的。在单目标情况下证明其正确性时,使用了商图的概念。将超立方体上行走变为线上行走的前提条件是行走的 U 算子必须和比特置换算子 P_{ij} 对易。在原文定理 1 中进行了证明:

$$P_{ij}^\dagger U' P_{ij} = P_{ij}^\dagger U P_{ij} - 2P_{ij}^\dagger S \cdot (|s_c\rangle\langle s_c| \otimes |\vec{0}\rangle\langle\vec{0}|) P_{ij} = U - \frac{2}{\sqrt{n}} \sum_{d=0}^{n-1} P_{ij}^\dagger |d, \vec{e}_d\rangle\langle d, \vec{0}| P_{ij} = U'$$

这个等式的最后一步能够成立就要求搜索的目标态必须是 $|\vec{0}\rangle$ 或者是 $|\vec{N}\rangle$ 。将 Skw 算法自然推广到多目标情况时需要考虑定理 1 并不适用于多目标。本文基于超立方体在多目标搜索下的情况提出新的硬币算子,并证明经过 $O\left(\sqrt{\frac{N}{M}}\right)$ 次迭代后可以以接近 1/2 的概率直接测量得到目标态,并且再最多进行 n 次检查后将得到目标态的概率提高到接近于 1。

将节点全集划分为 3 个集合:目标节点集合 $\alpha = \{|x\rangle | x \text{ is marked}\}$,目标邻居节点集合 $\beta = \{|y\rangle | S|y\rangle \in \alpha\}$,其他节点集合 $\gamma = \{|z\rangle | z \in \overline{\alpha \cup \beta}\}$ 。量子行走算子迭代的目标就是要增加目标节点集合

α 的幅度。

设判定目标节点的算子为: $\text{Oracle} = -\sum_{|x\rangle} |x\rangle\langle x|$ 。构造新的硬币算子 C 如下:

$$C = (I + \text{Oracle}) \otimes G + \text{Oracle} \otimes I$$

当初态首次经过硬币算子 C 后,会翻转目标节点出边的相位。经过了 S 算子一步行走后,目标节点出边相位值将会转变为入边相位值,即 β 中指向 α 的子集(下文中称为目标态),也正是需要进行幅度放大的部分。在第二次经过 C 算子时, G 算子将会放大相位为负的边的幅度。令多目标搜索算子 $U = SC$ 。反复迭代 U 算子即可增加目标态的幅度,从而使得目标节点的幅度变大。可以证明迭代次数为 $O(\sqrt{\frac{N}{M}})$,可使直接测量到目标态的概率接近 $1/2$,再通过检查测量结果的所有邻居可以将最终得到目标态的概率接近 1。

2.2 算法分析

假设目标节点共有 M 个,即 $|\alpha| = M$ 。可以设 $M \ll N$ 。设 H 中一个一般的状态为:

$$|\psi\rangle = \sum_{i=0}^{2^n} \sum_{d=0}^n \alpha_{id} |i\rangle \otimes |d\rangle$$

节点 $|i\rangle$ 在经过 t 步以后概率的计算可以定义为:

$$p^t(i) = \sum_d |\alpha_{id}|^2$$

因此可以通过分析所有的出边幅度变化来获得节点幅度的变化。下面将会给出 U 算子只作用在方向空间的变换形式。一般积状态可以变换为:

$$|\psi\rangle = \sum_i \sum_{d=0}^n \alpha_{id} |\vec{i}\rangle \otimes |d\rangle = \frac{1}{\sqrt{2^n}} \sum_i |\vec{i}\rangle \otimes |\varphi_i\rangle$$

其中 $|\varphi_i\rangle = \sum_{d=0}^n \sqrt{2^n} \alpha_{id} |d\rangle$, $U|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_i |\vec{i}\rangle \otimes R_i |\varphi_i\rangle$ 。令 $R_i = R_{is} \cdot R_{ic}$ 。

用 R_{ic} 重新定义算子 $C = (I + \text{Oracle}) \otimes G + \text{Oracle} \otimes I$:

$$R_{ic} = \begin{cases} -I & \text{if } i \text{ is marked} \\ 2|s\rangle\langle s| - I & \text{if } i \text{ is not marked} \end{cases}$$

其中 $|s\rangle = \frac{1}{\sqrt{n}} \sum_{d=0}^n |d\rangle$ 。

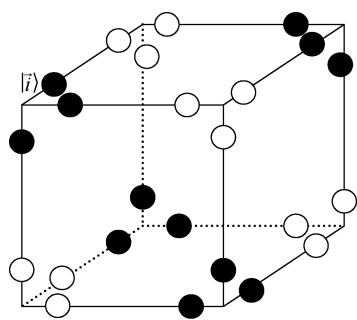
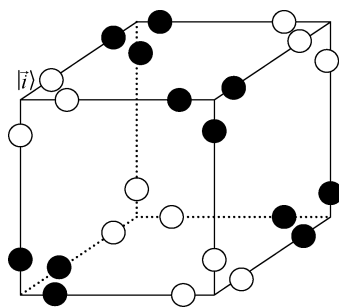
用 R_{ic} 重新定义算子 $S = \sum_d \sum_{\vec{x}} |\vec{x} \otimes \vec{e}_d, d\rangle \langle \vec{x}, d|$:

$$R_{is} |\varphi_i\rangle = \sum_{d=0}^n \sqrt{2^n} \alpha_{i \otimes \vec{e}_d} |d\rangle$$

根据上面的公式,可以将位置向量空间的分析转化为对出边向量空间的分析。出边的搜索空间是位置搜索空间的 n 倍,因此需要扩大原有的搜索空间,方法为原搜索空间中所有的元素都复制到原来的 n 倍。

如图 1 所示,所有的出边分成了空心组和实心组。注意到迭代算子 $R_i = R_{is} \cdot R_{ic}$ 。第一次执行 R_{ic} 算子时, R_{ic} 会对 $|\vec{i}\rangle$ 节点中的 3 个边元素(n -cube 是 n 个边元素)做均值反演或者是 Oracle。然后执行 S 算子时, R_{is} 将所有邻居节点朝向 $|\vec{i}\rangle$ 的边元素都变为节点 $|\vec{i}\rangle$ 的边元素,变换到图 2 的状态。如图 2 所示,第二次迭代时将 R_{ic} 会继续对第 $|\vec{i}\rangle$ 节点中所有边元素做均值反演或者是 Oracle,注意此时空心组和实心组并没有发生交叉,也就是说无论是均值反演还是 Oracle 都会在本组内进行,不会影响到其他组。再次迭代就会回到第一次的情况。

假设图 1 的左上角实心边元素聚集的节点 $|\vec{i}\rangle$ 为解。那么在第一次迭代中, R_{ic} 算子会认为这 3 个实心边元素为边解,对这 3 个元素进行 Oracle 运算。在迭代一次后,进入到图 2 状态, R_{ic} 算子同样会认为处于 s 位置的 3 个空心边元素为边解。也就是说虽然将总的边元素分成了两组,但是在每一组内都有同样多的边解。

图 1 第一次执行 R_{ic} 算子时的情况图 2 第二次执行 R_{ic} 算子时的情况

根据以上的分析,可以将超立方体上量子行走的分析转化成对一个特殊的 Grover 算法进行分析。详细的分析方法如下:

首先将所有的节点分割成 $n+1$ 组。随机挑选一个目标节点,设与目标节点汉明距离最大的节点为终结组 V_n (汉明距离为 n),目标节点为 V_0 。凡是 $m \neq 0, m \neq n, V_m$ 中的每一个节点都有 m 个元素在移动中朝向 V_0 方向, $n-m$ 个元素朝向 V_n 的方向。 m 值为 V_m 与 V_0 的汉明距离。也可以说每个边元素都在不同节点组之间移动。假设有一组元素在 V_m 和 V_{m+1} 之间进行移动,将这组边元素称为 G_m 。由于对称性,可以知道处于同一组的边元素相位都是相等的。共有 n 组边元素,设从 G_0 到 G_{n-1} 。

均值反演运算是在两个相邻的边元素组之间进行, G_m 先与 G_{m-1} 的元素进行,再与 G_{m+1} 的元素进行,反复如此。每次均值反演都会增加标号小的边元素,降低标号大的边元素。在运算时,只有两个组是特殊的。 G_0 没有前面的组,所以 $G_{-1}G_0$ 会做 Oracle 运算。 G_{n-1} 没有后面的组,因此 $G_{n-1}G_n$ 不变。

如果只关心目标节点的幅度扩大,那么实际上只需要考察目标节点 G_0G_1 运算即可,因为这次运算才是真正增加了目标节点的幅度值。 G_0G_1 运算中的边元素数量是 G_0 为 1, G_1 为 $n-1$ (这里已经除去了数量上的公约数,因为是算均值)。以此类推, G_mG_{m+1} 中 G_m 数量为 $m+1$, G_{m+1} 数量为 $n-m-1$ 。

每个边元素组中边元素的数量可以不需要考虑。注意到每个组的元素值都相等,并且在进行均值反演运算时只考虑两组之间参与联合运算的元素的值,因此只需要计算每个组中一个元素的值就足够了,不需要了解每个边元素组中共有多少个边元素。

在无 Oracle 的均值反演过程中,会降低原本大的值,增加原本小的值。但是增加和减少的值都为 $O\left(\frac{\omega}{n}\right)$, 设 $\omega = \frac{1}{\sqrt{n}2^n}$, 可以看到 ω 是决定性的值。第 $G_{m-1}G_m$ 组中的均值运算应该是:

$$\frac{m\left(\omega - O\left(\frac{\omega}{n}\right)\right) + (n-m)\omega}{n} = \omega - \frac{m}{n}O\left(\frac{\omega}{n}\right)$$

由于 $\frac{m}{n} \leq 1$, 所以每次计算的均值为 $\omega - O\left(\frac{\omega}{n}\right)$ 。令 G_{m-1} 中元素值为 $\omega + O\left(\frac{\omega}{n}\right)$, G_m 组元素为 $\omega - O\left(\frac{\omega}{n}\right)$ 。可以看出在这种传递性的均值反演计算下, G_1 中元素的值虽然在和 G_0 中元素发生运算时降低了 $O\left(\frac{\omega}{n}\right)$, 但在计算 G_1G_2 时,又提高了 $O\left(\frac{\omega}{n}\right)$, 而且总体看其大小为 $\omega + O\left(\frac{\omega}{n}\right)$ 。由于 G_1 中元素的值始终为 $\omega + O\left(\frac{\omega}{n}\right)$, 可以通过 G_0G_1 运算令 G_0 中元素值每次增加 $2\omega - O\left(\frac{\omega}{n}\right)$ 。

上面的内容为其中一个目标节点的变化,由于每次增加的幅度值为 $O\left(\frac{1}{\sqrt{n}2^n}\right)$, 因此只要最多 $\frac{\sqrt{2^n}}{\sqrt{M}}$ 次迭代就可以令幅度值变化为接近于 $\frac{1}{\sqrt{nM}}$, 此时得到边解的概率为 $\left|\frac{1}{\sqrt{nM}}\right|^2 \times nM = 1$ 。在一个组中得到边解的概率可以接近于 1。但是在进行最终的测量时由于是对节点进行,由于只有某一组的 G_0 存在于 V_0 ,

因此测量到 V_0 的概率接近 $1/2$ 。另外一个组的 G_0 的元素则分散到了当前的 V_1 中,还有 $1/2$ 的概率会测量到 V_1 中的某个节点。如果可以将 V_1 和 V_0 进行联合测量,即可令测量到解的概率接近于 1。共有 $c_n^1 = n$ 组 V_1 ,每次只要多检查 n 个邻居节点即可以接近于 1 的概率测量到解。根据文献[7]中的算法,经过直接测量后检查得到的结果是否为需要的解,如果不是则再将测量得到结果的所有邻居分量都再次检查一遍即可得到最终要搜索的分量。这个过程只增加了 n 次查询,即 $O(\log N)$ 的查询复杂度,因此总体的复杂度不变。

3 结 语

无结构数据库上进行搜索一直是重要的问题之一。因为大量的 NP 问题都可以变换为一个多项式复杂度的判定问题和一个无结构数据库上搜索的问题。因此能够找到高效率的无结构数据库上搜索的算法,对于高效解决 NP 问题有很大的帮助。量子计算通过高度的并行计算带来了非常快的计算速度。量子行走是量子计算中重要的算法框架之一。尽管当前尚且没有通用量子计算机,但是随着 D-Wave2 等特型量子计算机的纷纷面世,通用量子计算机也必将在不久的将来到来。因此讨论如何运用量子行走框架解决无结构数据库上的搜索问题是非常具有价值的。

Skw 算法可以快速求解无结构数据库上搜索的问题。但是 Skw 算法只能搜索一个目标。而搜索多个目标才是一个更一般性的问题。为了能够搜索多目标,本文提出了基于超立方体上量子行走的快速搜索算法。简要地介绍了在超立方体上进行量子行走的偏移算子结构和硬币算子选取。基于放大目标态入边的思路,设计了含有 G 算子的新硬币算子。最终证只需要查询 $O\left(\sqrt{\frac{N}{M}}\right)$ 次,就可以接近 1 的概率得到目标态。

参考文献:

- [1] Childs A M. Universal computation by quantum walk[J]. Phys. Rev. Lett., 2009, 102: 1-8
- [2] Lovett N B, Cooper S, Everitt M, et al. Universal quantum computation using the discrete-time quantum walk[J]. Phys. Rev. A, 2010, 81(4): 33-42
- [3] Benioff P A. The computer as a physical system; a microscopic quantum mechanical hamiltonian model of computers as represented by turing machines[J]. J. Stat. Phys., 1980, 22(5): 563-591
- [4] Shor P W. Algorithms for quantum computation; discrete logarithms and factoring[C]//Foundations of computer science, 1994 proceedings. 35th Annual Symposium on. IEEE, 1994: 124-134
- [5] Grover L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the twenty-eighth annual ACM symposium on theory of computing. ACM, 1996: 212-219
- [6] Shenvi N, Kempe J, Whaley K B. Quantum random-walk search algorithm[J]. Physical Review A, 2003, 67(5): 052307
- [7] Potoček v, Gábris A, Kiss T, et al. Optimized quantum random-walk search algorithms on the hypercube[J]. Physical Review A, 2009, 79(1): 012325
- [8] Feldman E, Hillery M. Scattering theory and discrete-time quantum walks[J]. Physics Letters A, 2004, 324(4): 277-281
- [9] Feldman E, Hillery M. Modifying quantum walks; a scattering theory approach[J]. Journal of Physics A: Mathematical and Theoretical, 2007, 40(37): 11343

(责任编辑:谭彩霞)