arXiv:2304.03616v1 [cs.CR] 7 Apr 2023

2023年4月10日

最近向量问题的 QUBO 模型

EDUARDOCANALE、CLAUDIO QURESHI 和 ALFREDO VIOLA

Abstract. 本文考虑由生成矩阵 $A \in \mathcal{M}_{n\times n}(\mathbb{Z})$ $\Lambda \subseteq \mathbb{Z}^n$ 给出的格 $\Lambda \subseteq \mathbb{Z}^n$ 上的最近向量问题（CVP）。令 $b > 0$ 为矩阵 A各项绝对值中的最大值。我们证明，CVP 可以在多项式时间内归约为一个二次无约束二元优化（QUBO）问题，该问题包含 $O(n^2(\log(n) + \log(b)))$ 个二元变量，其中相应二次型的系数长度为 $O(n(\log(n) + \log(b)))$。

K关键词 CVP、格、条件数、QUBO、量子桥接分析

M数学学科分类52C17, 52C22, 94B05, 94B27, 11H31

1. Introduction and notation

量子退火是一种基于绝热量子计算的方法，用于求解能够表示为 QUBO模型（或伊辛模型）的一些优化问题。尽管 QUBO问题属于NP 困难问题类别，但对于某些（较小的）特殊实例，量子退火技术已被证明相当高效。从这个意义上说，一些作者已经展示了如何将若干重要的优化问题转换为 QUBO框架。这些问题包括数划分问题、最大割问题、集合打包问题和最大 2-SAT 问题 [2, 3, 5]。鉴于格问题在一些后量子密码算法中的重要性，我们研究了如何将最近向量问题（CVP）归约为 QUBO 问题，使得该归约以及 QUBO 问题的维数和规模均关于 CVP 的参数呈多项式增长。

QUBO模型由一个最小化二次型的优化问题表示 x^tQx 其中 $Q \in \mathcal{M}_N(\mathbb{Z})$ 是给定的整数方阵，而 x 是一个二元变量向量（即，对于 $1 \leq i \leq N$，每个坐标 $x_i \in \{0, 1\}$）。这里我们考虑 QUBO 的两个参数：维数 N（即待确定的二元变量数量）和规模 s，即矩阵 Q 各项绝对值的最大值。在 CVP 中，输入是一个整数非奇异矩阵 $A \in \mathcal{M}_n(\mathbb{Z})$ 和一个（列）向量 $x \in \mathbb{Z}^n$，我们要找到一个向量 $z \in \mathbb{Z}^n$，使 $||x - Az||$ 的值最小。请注意，所有相关信息 $\widetilde{}$ 都包含在增广矩阵 $A = (A|x)$ 中。对于矩阵 $\widetilde{A}$，我们定义一个新的方阵 $Q^{\widetilde{A}}$；我们的主要结果（定理 2.6）$\frown$ 将 QUBO 问题 $\widetilde{x} = \operatorname{argmin} x^tQ^Ax$ 的每个解对应到 CVP 问题 $\widetilde{z} = \operatorname{argmin}_{z\in\mathbb{Z}^n} ||x - Az||$ 的一个解。我们还估计了 Q^A 的维数和规模 $\frown$（注 2.7）。最后一节列出了更多有趣的研究问题，涉及使用量子退火有效实现 QUBO 问题，以及我们主要定理给出的对应关系。

记号 1.1. $\mathcal{M}_{n\times m}(\mathbb{Z})$ 表示 $n\times m$ 整数矩阵的集合， $\mathcal{M}_n(\mathbb{Z}):=\mathcal{M}_{n\times n}(\mathbb{Z})$，而 $\mathbb{Z}^n$ 是整数 n 元组构成的空间，这些元组与 $\mathcal{M}_{n\times 1}(\mathbb{Z})$ 等同（为简便起见，我们将向量 $x\in\mathbb{Z}^n$ 记作行向量）。本文中的对数均以 2 为底。向量 $x\in\mathbb{Z}^n$ 与集合 $\Lambda\subseteq\mathbb{Z}^n$ 之间的距离为 $d(x,\Lambda):=\min_{\lambda\in\Lambda} d(x,\lambda)$。

2. A Qubo model for the CVP

我们考虑一个矩阵 $A\in\mathcal{M}_n(\mathbb{Z})$，其$\det(A)\neq 0$ 且令 Λ 为由 A生成的格（即 $\Lambda=\mathbb{Z}a_1+\ldots+\mathbb{Z}a_n$，其中 $a_i\in\mathbb{Z}^n$ 是A的第 i 列）。我们用 $d(x,y)=||x-y||$表示 x与 $y\in\mathbb{R}^n$ 之间的欧氏距离。令 $\mathcal{P}_A=\{Ax:\ x\in[0,1)^n\}$ 为关于矩阵 A 的 Λ 的基本平行多面体。注意，从向量 $x=\sum_{i=1}^n x_i a_i\in\mathbb{R}^n$ 中寻找最近格向量的问题，等价于从$\widehat{x}$ 中寻找最近格向量：$=\sum_{i=1}^n(x_i-\lfloor x_i\rfloor)a_i\in\mathcal{P}_A$。事实上，如果 $\widehat{\lambda}\in\Lambda$ 满足 $d(\widehat{x},\widehat{\lambda})=d(\widehat{x},\Lambda)$ 且$\lambda_0=\sum_{i=1}^n\lfloor x_i\rfloor a_i$，那么 $d(x,\widehat{\lambda}+\lambda_0)=d(\widehat{x},\widehat{\lambda})=d(\widehat{x},\Lambda)=d(\widehat{x}+\lambda_0,\Lambda+\lambda_0)=d(x,\Lambda)$。因此，我们可以假设希望从中寻找最近格向量的向量 x位于基本平行多面体 $\mathcal{P}_A$ 中。

在矩阵空间 $\mathcal{M}_n(\mathbb{R})$ 中，我们考虑由 $||A||=\max_{x:||x||=1}||Ax||$ 给出的谱范数，而可逆矩阵的条件数定义为 $\kappa(A)=||A||\cdot||A^{-1}||$。文献 [1] 证明了 $\kappa(A)$ 的以下上界。

引理 2.1. 设 $A=(a_{ij})\in\mathcal{M}_n(\mathbb{R})$，且 $||A||_F=\left(\sum_{i,j}a_{ij}^2\right)^{\frac{1}{2}}$ 为 A 的 Frobenius 范数，则

$$\kappa(A)\leq\frac{2}{|\det(A)|}\cdot\left(\frac{||A||_F}{\sqrt{n}}\right)^n.$$

为了从基本平行多面体中的一个向量得到最近格向量，我们可以将范围限制在某些特殊的格向量上。

定义 2.2. 使用与上文相同的记号，若格向量 $\lambda\in\Lambda$ 满足：对于某个 $x\in\mathcal{P}_A$，有 $d(\lambda,x)=d(\Lambda,x)$，则称其为 A- 可行格向量。A- 可行格向量的集合记为 $\mathcal{F}_A$。

下一个引理给出了可行格向量坐标的上界。

引理 2.3. 若 $\lambda=Az\in\mathcal{F}_A$ with $z\in\mathbb{Z}^n$，则 $||z||\leq\left(\frac{\kappa(A)}{2}+1\right)\cdot\sqrt{n}$。

证明。令 $\epsilon=(\epsilon_1,\ldots,\epsilon_n)\in[0,1)^n$，使得 $d(\Lambda,A\epsilon)=||\lambda-A\epsilon||$。考虑由 $z_i'=\lfloor\epsilon_i+\frac{1}{2}\rfloor$, $1\leq i\leq n$ 给出的 $z'=(z_1',\ldots,z_n')$。我们有 $||z||=||A^{-1}(\lambda-A\epsilon)+\epsilon||\leq||A^{-1}||\cdot||Az'-A\epsilon||+||\epsilon||\leq\kappa(A)\cdot||z'-\epsilon||+||\epsilon||\leq\kappa(A)\cdot\frac{\sqrt{n}}{2}+\sqrt{n}$。□

命题 2.4。设 $A=(a_{ij})\in\mathcal{M}_n(\mathbb{Z})$，其中 $n\geq 3$，且 $\det(A)\neq 0$。设 Λ 为由 A 的列生成的格，$\mathcal{F}_A$ 为其 A-可行格向量的子集。设 $b=\max\{|a_{ij}|:\ 1\leq i、\ j\leq n\}$。若 $\lambda=Az\in\mathcal{F}_A$，且 $z=(z_1,\ldots,\ z_n)\in\mathbb{Z}^n$，则对于 $1\leq i\leq n$，$\log(|z_i|)\leq n(\log(n)+\log(b))$。

证明。由引理 2.1 和界 $||A||_F\leq nb$，我们有 $\kappa(A)\leq 2n^{n/2}b^n$。由引理 2.3，我们有 $||z||\leq\frac{3}{2}\cdot\kappa(A)\cdot\sqrt{n}\leq 3n^{\frac{n+1}{2}}b^n$。因此，$\log(|z_i|)\leq\log(||z||)\leq\log(3)+n\log(b)+\left(\frac{n+1}{2}\right)\cdot\log(n)\leq n(\log(n)+\log(b))$。□

设 $A \in \mathcal{M}_{n\times n}(\mathbb{Z})$ 且 $x \in \mathbb{Z}^n$。我们将 A 的增广矩阵记为 $\sim A = (A|x)$。接下来，我们引入 A 的 Q 矩阵，它在将 CVP 归约为 QUBO 问题的过程中发挥重要作用。

定义 2.5。令 $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{Z})$，$x \in \mathbb{Z}^n$ 且 $\sim A = (A|x)$。令 $b = \max\{|a_{ij}| : 1 \le i, j \le n\}$ 且 $m = \lceil n(\log(n) + \log(b))\rceil$。$A$ 的 Q 矩阵是由下式给出的矩阵 $Q^A = (q_{hr}) \in \mathcal{M}_{n(m+1)}(\mathbb{Z})$：

$$q_{hr} := \begin{cases} 2^{j+l}\sum_{t=1}^{n} a_{ti}a_{tk} & \text{若 } h \ne r; \\ 4^l\sum_{t=1}^{n} a_{ti}^2 - 2^{m+j+1}\sum_{t=1}^{n}\sum_{s=1}^{n} a_{st}a_{si} + 2^{j+1}\sum_{t=1}^{n} x_t a_{ti} & \text{若 } h = r, \end{cases}$$

其中 $h = jn + i$，$r = ln + k$ 对 $0 \le j \le m$，$1 \le i \le n$，$0 \le l \le m$ 且 $1 \le k \le n$。

注意，每个正整数 $h \le n(m+1)$ 都可以唯一地写成 $h = jn + i$，其中 $0 \le j \le m$ 且 $1 \le i \le n$，因此矩阵 Q^A 定义良好。

设 A、n 和 b 如命题 2.4 中所述。我们用 $\mathcal{B}_{n\times m}$ 表示由 $n \times m$ 个二进制矩阵（即矩阵的每个元素均为 0 或 1）构成的空间，$m := \lceil n(\log(n) + \log(b))\rceil$，$u := (2^m, 2^m, \ldots, 2^m) \in \mathbb{Z}^n$，以及 $p := (1, 2, \ldots, 2^m) \in \mathbb{Z}^{m+1}$。我们还考虑一个固定向量 $x \in \mathcal{P}_A$。若 $z \in \mathbb{Z}^n$ 满足 $||Az - x|| = d(\Lambda, x)$，根据命题 2.4，我们有 $|z_i| \le 2^m$，其中 $1 \le i \le n$。于是，存在一个二进制矩阵 $B \in \mathcal{B}_{n\times(m+1)}$，使得 $z + u = Bp$。CVP 是寻找使 $||Az - x||^2 = (Az - x)^t(Az - x)$ 最小的向量 $z \in \mathbb{Z}^n$ 的问题。经过直接计算，将 z 替换为 $Bp - u$ 并消去常数项后，可以看出，CVP 也等价于寻找使下列函数最小的二进制矩阵 $B \in \mathcal{B}_{n\times(m+1)}$：

$$q(B) := (ABp)^t ABp - 2u^t A^t ABp + 2x^t ABp \tag{1}$$

由此容易看出，$q(B)$ 是关于矩阵 B 各元素的二次多项式，即 $q(B) = \sum c_{i,j,k,l} \cdot b_{i,j}b_{k,l} - 2\sum d_{i,j} \cdot b_{i,j} + 2\sum e_{i,j} \cdot b_{i,j}$，其中系数 $c_{i,j,k,l}$，$d_{i,j}$ 和 $e_{i,j}$ 均为整数，且 $1 \le i \le n$，$0 \le j \le m$，$1 \le k \le n$ 和 $0 \le l \le m$。为了将其写成标准 QUBO 模型的形式，我们使用关系式 $b_{i,j} = b_{i,j}^2$，并将表达式改写为 $q(B) = \sum' c_{i,j,k,l} \cdot b_{i,j}b_{k,l} + \sum(c_{i,j,i,j} - 2d_{i,j} + 2e_{i,j}) \cdot b_{i,j}^2$，其中 $\sum'$ 表示求和仅限于满足 $(i, j) \ne (k, l)$ 的 i, j, k, l。这样，$q(B) = v_B^t Q v_B$，其中 v_B 是一个长度为 $n(m+1)$ 的二进制（列）向量，其第 $jn + i$ 个分量为 $b_{i,j}$（$1 \le i \le n$ 和 $0 \le j \le m$），而 Q 是一个 $n(m+1) \times n(m+1)$ 矩阵，其主对角线外的元素 $c_{i,j,k,l}$ 以及主对角线上的元素 $c_{i,j,i,j} - 2d_{i,j} + 2e_{i,j}$ 均为整数。

我们可以使用公式（1）来计算这些系数，并将得到与定义 2.5 中相同的数值。上述内容都可以总结为以下结果。

定理 2.6. 设 $A \in \mathcal{M}_n(\mathbb{Z})$ 是一个非奇异矩阵，且 $n \ge 3$ 和 Λ_A 是由 A 的列生成的格。设 $x \in \mathbb{Z}^n$ 和 $\sim A = (A|x)$。假设 x 位于 Λ 的基本平行多面体中。设 $b = \max\{|a_{ij}| : 1 \le i, j \le n\}$，$m = \lceil n(\log(n) + \log(b))\rceil$，$u = (2^m, 2^m, \ldots, 2^m) \in \mathbb{Z}^n$，$p = (1, 2, \ldots, 2^m) \in \mathbb{Z}^{m+1}$ 且 $\widetilde{Q}$ 是 $\widetilde{A}$ 的 Q 矩阵。考虑关于二次型 x^tQx 的 QUBO 问题的一个解 $\widetilde{x} \in \{0,1\}^{n(m+1)}$（即对于所有 $x \in \{0,1\}^{n(m+1)}$，$\widetilde{x}^t\widetilde{Q}\widetilde{x} \le x^t\widetilde{Q}x$）。设 $B \in \mathcal{B}_{n\times(m+1)}$ 为一个二进制矩阵，其元素为 $B_{ij} = \widehat{x}_{jn+i}$，其中 $1 \le i \le n$ 且 $0 \le j \le m$。若 $\sim \lambda = A(Bp - u)$，则 $\lambda \in \Lambda_A$ 且对于所有 $\sim \lambda \in \Lambda_A$，$||x - \lambda|| \le ||x - \lambda||$。

注 2.7. 上述定理表明，CVP 可以归约为一个 QUBO~问题，即最小化一个二次型 x^tQx，其中 x 是一个二元变量向量。二元变量的数量为 $n(m+1) = O(n^2(\log(n) + \log(b)))$。$Q$ 中系数的长度~（以比特为单位）可以利用定义 2.5 中的表达式以及事实 $|x_i| \leq nb$（因为 $x \in \mathcal{P}_A$）来界定。具体而言，$|q_{hr}| \leq 4^m nb^2 + 2^{2m+1}n^2b^2 + 2^{m+1}nb^2 \leq 3 \cdot 2^{2m+1}n^2b^2$。那么 $\log|q_{hr}| \leq \log(3) + 2m + 1 + 2(\log(n) + \log(b)) = O(n(\log(n) + \log(b)))$。

3. Further remarks

本文明确展示了如何将 CVP 化为一个 QUBO 问题，并给出了所涉及二元变量数量的上界，以及二次型 Q 系数长度（以比特为单位）的上界。尽管 QUBO 问题通常难以求解（它们是 NP-hard 优化问题 [2]），但某些特定实例可以通过绝热量子优化 [4] 在合理时间内求解。在量子退火设备上求解 QUBO 问题的效率，很大程度上取决于矩阵 Q 数据的处理方式~。例如，在 D-Wave 计算机中，网络拓扑由宿主图建模（D-Wave 2000 量子比特设备使用 Chimera 图，D-Wave 5000 量子比特设备使用 Pegasus 图），而矩阵 Q 的数据由其对应的连接图给出。一个关键之处在于设计高效的嵌入算法，使其能够将一大类连接图（与 QUBO 问题相关联）嵌入量子退火设备的宿主图中，例如参见 [6]。一般而言，寻找次嵌入是 NP 完全问题，但对于某些图类，已有高效算法。本研究的后续工作将包括找出 CVP 的某些特定实例类别，使对应的 QUBO 问题适合由 D-Wave 计算机求解（这最终取决于与 Q 矩阵相关联的连接图的性质）。值得注意的是，通过量子退火求解 QUBO 问题时，通常得到的是问题的近似解。定理 2.6 将 QUBO 问题的每个精确解 $\widehat{x}$ 与对应 CVP 的一个精确解 λ 联系起来~。若从近似解 $\widehat{x}$ 而非精确解出发，那么我们距离 CVP 的最优解有多远？对此作出估计将很有意义。

Acknowledgement

作者的研究部分得到了 CyTeD（“伊比利亚美洲科学与技术促进发展计划”）项目 522RT0131 的支持。

References

[1] Guggenheimer, H. W.、Edelman, A. S. 和Johnson,C. R.（1995）。线性系统条件数的简单估计。《大学数学杂志》，26(1)，2-5。[2] Glover, F.、Kochenberger, G.、Hennig, R. 和 Du, Y.（2022）。Quantum BridgeAnalyticsI：QUBO模型的构建与使用教程。《运筹学年鉴》，1-43。[3] Glover,F.、Kochenberger, G.、Ma, M. 和 Du, Y.（2022）。Quantum Bridge AnalyticsII：QUBO-Plus、网络优化与资产交换的组合链式连接。《运筹学年鉴》，1-28。[4] Lucas, A.（2014）。许多NP问题的伊辛表述。《物理学前沿》，5。[5] Kadowaki, T.和Nishimori, H.（1998）。横场伊辛模型中的量子退火。《物理评论E辑》，58(5)，5355。

[6] Zbinden, S., B¨artschi,A.,Djidjev, H. & Eidenbenz, S.（2020年6月）。面向采用 Chimera 和 Pegasus 连接拓扑的量子退火器的嵌入算法。载于《高性能计算：第35届国际会议，ISC高性能计算 2020》，德国法兰克福/美因河畔，2020年6月22日至25日，论文集（第187—206页）。沙姆：Springer International Publishing。

Instituto de Matemática y Estadística, Universidad de la República, Uruguay
Email address: canale@fing.edu.uy

Instituto de Matemática y Estadística, Universidad de la República, Uruguay
Email address: cqureshi@fing.edu.uy

Instituto de Computación, Universidad de la República, Uruguay
Email address: viola@fing.edu.uy