智能系统学报
CAAI TRANSACTIONS ON INTELLIGENT SYSTEMS

对抗样本三元组约束的度量学习算法

王鑫， 郭鑫垚， 魏巍， 梁吉业

引用本文:
王鑫, 郭鑫垚, 魏巍, 等. 对抗样本三元组约束的度量学习算法[J]. 智能系统学报, 2021, 16(1): 30–37.
WANG Xin, GUO Xinyao, WEI Wei, et al. Metric learning algorithm with adversarial sample triples constraints[J]. *CAAI Transactions on Intelligent Systems*, 2021, 16(1): 30–37.

在线阅读 View online: https://dx.doi.org/10.11992/tis.202009050

DOI: 10.11992/tis.202009050

对抗样本三元组约束的度量学习算法

王鑫[1], 郭鑫垚[1], 魏巍[1,2], 梁吉业[1,2]

(1. 山西大学 计算机与信息技术学院, 山西 太原 030006; 2. 山西大学 计算智能与中文信息处理教育部重点实验室, 山西 太原 030006)

摘 要: 针对已有三元组约束的度量学习算法大多利用先验知识构建约束, 一定程度上制约了度量学习算法性能的问题, 本文借鉴对抗训练中样本扰动的思想, 在原始样本附近学习对抗样本以构造对抗三元组约束, 基于对抗三元组和原始三元组约束构建了度量学习模型, 提出了对抗样本三元组约束的度量学习算法 (metric learning algorithm with adversarial sample triples constraints, ASTCML)。实验结果表明, 提出的算法既克服了已有固定约束方法受先验知识影响大的问题, 也提高了分类精度, 说明区分更加难以区分的三元组约束能够提升算法的性能。

关键词: 机器学习; 度量学习; 三元组约束; 对抗训练; 马氏距离; 样本扰动; 凸优化; 梯度下降

中图分类号: TP181 **文献标志码:** A **文章编号:** 1673−4785(2021)01−0030−08

中文引用格式: 王鑫, 郭鑫垚, 魏巍, 等. 对抗样本三元组约束的度量学习算法 [J]. 智能系统学报, 2021, 16(1): 30–37.

英文引用格式: WANG Xin, GUO Xinyao, WEI Wei, et al. Metric learning algorithm with adversarial sample triples constraints[J]. CAAI transactions on intelligent systems, 2021, 16(1): 30–37.

Metric learning algorithm with adversarial sample triples constraints

WANG Xin[1], GUO Xinyao[1], WEI Wei[1,2], LIANG Jiye[1,2]

(1. School of Computer and Information Technology, Shanxi University, Taiyuan 030006, China; 2. Key Laboratory of Computational Intelligence and Chinese Information Processing of Ministry of Education, Shanxi University, Taiyuan 030006, China)

Abstract: Most of the existing metric learning algorithms with triple constraints use prior knowledge to construct constraints, which restricts the performance of metric learning algorithms to a certain extent. To solve this problem, the metric learning algorithm with adversarial sample triple constraints, named ASTCML, is proposed based on the idea of sample perturbation in adversarial training, in which the adversarial sample is learned near the original sample to construct adversarial triple constraints. The metric learning model is constructed on the basis of adversarial triples and original triples constraints. Experimental results show that the proposed algorithm overcomes the effect of prior knowledge that is problematic for existing fixed constraint methods and improves the classification accuracy. This shows that distinguishing triple constraints that are more difficult to distinguish can improve the performance of the algorithm.

Keywords: machine learning; metric learning; triplet constraints; adversarial training; Mahalanobis distance; sample perturbation; convex optimization; gradient descent

度量学习作为机器学习领域的重要分支, 已广泛应用于多个领域, 如图像检索[1-4]、目标检测[5-7]、亲属关系验证[8]、音乐推荐[9] 等, 目的是学习数据间的相似性关系使相似样本间距离尽可能小, 不相似样本间距离尽可能大[10]。

收稿日期: 2020−09−30.

基金项目: 国家自然科学基金项目 (62006147, 61876103, 61772323); 山西省重点研发计划项目 (201903D121162); 山西省 1331 工程项目.

通信作者: 魏巍. E-mail: weiwei@sxu.edu.cn.

在度量学习中, 样本之间的相似性通常用马氏距离进行度量, 即 $\boldsymbol{d}_{\boldsymbol{M}}(\boldsymbol{x}_i,\boldsymbol{x}_j)=(\boldsymbol{x}_i-\boldsymbol{x}_j)^{\mathrm{T}}\boldsymbol{M}(\boldsymbol{x}_i-\boldsymbol{x}_j)$, 其中 $\boldsymbol{M}$ 要求为半正定矩阵, 以保证距离的有效性。Xing 等[10] 使用所有样本构成二元组约束, 首次提出了关于马氏距离的度量学习算法, 但当样本规模较大时, 约束数量呈爆炸式增长, 导致算法效率降低。为了提高算法效率, Ying 等[11] 将学习度量的过程转化为特征值优化问题, 提出基于特征值优化的距离度量学习算法 (distance met-

ric learning witheigenvalue optimization, DML-eig), 该算法每次迭代只关注最近的不相似样本。为减少约束的规模, Davis 等[12] 随机选择二元组, 提出关于度量参数正则化的信息理论度量学习算法 (information-theoretic metric learning, ITML), 由于随机选择约束, 该算法的结果不稳定; Zadeh 等[13] 随机选择约束, 在相似样本与不相似样本中使用不同的度量方法提出几何平均度量学习算法 (geometric mean metric learning, GMML), 该算法存在闭式解, 当样本规模较大时, 随着迭代次数的增加, 部分样本对在训练中不产生作用。针对该问题, Omara 等[14] 提出了动态生成二元组的算法。然而, 当二元组样本间的相似性或相异性存在较大差异时, 也将相同阈值应用于所有约束。因此, Weinberger 等[15-16] 基于样本与其最近的同类样本间的距离和不同类样本之间尽可能以一个间隔分开的原则, 提出了大间隔近邻分类算法 (distancemetric learning for large margin nearest neighbor classification, LMNN)。Yang 等[17] 将自适应地选择近邻个数引入到目标函数中, 提出了自适应大间隔近邻分类算法 (adaptive large margin nearest neighborclassification algorithm, ALMNN), 但该算法受参数影响较大。Song 等[18] 利用特征空间中样本的几何信息对 LMNN 算法进行改进, 提出了只关注距离最近的不同类样本对的无参大间隔最近邻度量学习算法 (parameter free large margin nearest neighbor for distance metric learning, PFLMNN), 该算法不需要调参, 且考虑的约束相对较少。Liu 等[19] 提出一种新的约束构建方法, 依据样本的先验信息, 针对所有目标样本, 只选与其同类距离远的样本及不同类距离近的样本生成固定的三元组, 该算法受先验知识影响较大。Capitaine[20] 利用损失的加权选择约束, 关注较难区分的区域或类重叠区域, 适用于小样本度量学习。为了减少约束数量, Perrot 等[21] 提出回归虚拟度量学习算法 (regressive virtual metric learning, RVML), 该算法中每个样本逼近先验定义的虚拟点, 可以在线性时间内学习度量, 但算法受数据分布的影响。由于三元约束与支持向量机出发点一致, 都是采用大间隔思想, 鉴于支持向量机 (support vector machine, SVM) 成熟的求解方式, Wang 等[22] 提出了距离度量学习的一种核分类框架, 所提出的框架可以使用标准支持向量机 (SVM) 求解器有效地实现, 但不能得到全局最优解。Zuo 等[23] 将三元组约束形式用 SVM 表示, 提出了新的度量学习算法, 该算法可以得到全局最优解。基于三元组约束的度量学习大都通过设置不同的损失函数来学习度量。

基于三元组约束的度量学习通常依据先验知识, 采用不同策略构建固定约束。随着迭代次数的增加, 部分三元组在训练中不产生作用, 于是, 一些动态选择三元组的算法被提出。Mei 等[24] 提出了使用三元组的基于 Logdet 散度的度量学习算法 (logdet divergence based metric learning with triplet constraints, LDMLT), 该算法在每次迭代中选择有效的约束进行度量学习, 降低了先验知识对度量学习的影响, 但是构成三元组约束的样本都是在原始样本中选择, 不能充分利用数据蕴含的三元约束。针对这一问题, 研究人员将对抗训练与度量学习进行结合, 在度量学习中通过产生对抗样本增强算法性能。Chen 等[25] 提出对抗度量学习算法 (adversarial metric learning, AML), 通过产生对抗样本对用于混淆学得的度量, 提高度量学习算法鲁棒性。

基于二元组约束的对抗度量学习受参数和样本对间相似性差异的影响, 使得对所有二元组约束产生对抗样本对是很难实现的, 而三元约束解决了样本对间差异性的问题, 同时考虑类间样本和类内样本的关系, 可以将三元约束与对抗训练进行结合。基于三元组约束的度量学习与对抗训练进行结合的关键问题是如何生成对抗样本。本文借鉴对抗训练中样本扰动的思想, 在原始样本附近产生对抗样本以构建对抗三元组约束, 提出一种新的三元组约束的构造方法, 并构建对抗样本三元组约束的度量学习模型。本文的贡献主要有:

1) 通过在三元组中的入侵样本附近学习对抗样本, 构造了间隔更小的对抗样本三元组约束;

2) 构造的对抗样本学习优化模型具有闭式解;

3) 实验结果表明提出算法的性能优于代表性的三元组度量学习算法。

1　约束构建的相关算法

1.1　三元组约束构建

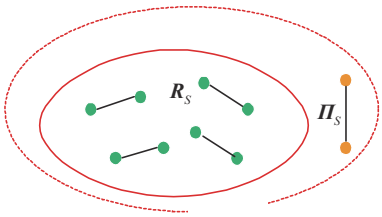
三元组的构建是基于三元组约束的度量学习关键问题之一。Liu 等[19] 通过选择位于类边界的样本构建三元组约束, 提出了一种有效的三元组约束构建方法。该论文利用任意样本、与其欧氏距离最大的同类样本和与其欧氏距离最小的异类样本构造三元组约束, 并随机选择其中的一部分约束用于度量学习, 这些约束一旦构造和选择将在整个度量学习的过程中固定不变。然而, 这些基于欧氏距离构造并随机选择的三元组约束并不

能很好地指导不断更新的度量学习，制约了算法的性能。为了解决这一问题，Mei 等[24] 提出了一种面向度量学习的三元组动态选择策略，使每次迭代都能有效地利用约束进行度量学习。该方法基于当前 (第 t 次迭代) 的马氏矩阵 $\boldsymbol{M}_t$ 计算样本的距离矩阵和相似矩阵，根据当前度量下的近邻与先验目标近邻的偏离程度定义了样本的混乱度，并依据样本混乱度选择三元组约束，用于学习下一次 (t+1 次) 迭代时度量矩阵 $\boldsymbol{M}_{t+1}$。

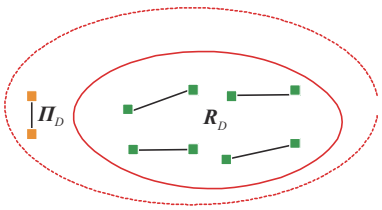
尽管 LDMLT 算法在每次迭代时动态选择混乱度高的约束，可以提升度量学习算法的性能，但并不能充分挖掘数据蕴含的相似性关系。

1.2　对抗度量学习

对抗度量学习 (AML) 算法[25] 基于对抗样本构造二元组约束，用于提高度量学习算法的鲁棒性。AML 算法包括 2 个阶段：混淆阶段和区分阶段。在混淆阶段，通过对每个约束的 2 个端点产生样本扰动，即学习对抗样本对，不断放大或者缩小当前对抗样本的距离，使得在当前度量下该样本对难以区分，如图 1 所示。同类样本生成的对抗样本对 (即 $\boldsymbol{\Pi}_S$) 的 2 个样本彼此相距甚远，其描述对抗样本对为同类的极端情况。类似地，生成的异类样本的 2 个对抗样本对 (即 $\boldsymbol{\Pi}_D$) 变得非常相似，其描述了对抗样本对仍为异类的极端情况。在区分阶段，实现学得的度量尽可能地区分对抗样本对。



(a) 相似样本的对抗对生成



(b) 不相似样本的对抗对生成

图 1　对抗样本示意

Fig. 1　Schematic illustration of adversarial samples

图 1 中 S 为相似样本，D 为不相似样本，$\boldsymbol{R}_S$ 表示相似样本对，$\boldsymbol{\Pi}_S$ 表示相似样本对产生的对抗样本对，$\boldsymbol{R}_D$ 表示不相似样本对，$\boldsymbol{\Pi}_D$ 表示不相似样本对产生的对抗样本对。

AML 算法通过对同类样本生成同类彼此相距甚远的对抗样本对，而异类样本生成异类彼此相对较近的对抗样本对来增强算法的鲁棒性。然而，由于需要为每一个二元约束构建对抗样本对，仅用单个参数来控制对抗样本的学习，使其参数难以调整，且构建的对抗样本对绝大多数是无效的。

2　对抗样本三元组约束的度量学习

现有的方法基于欧氏距离构建三元组约束，并随机选择部分三元组约束用于度量学习。虽然有一些方法提出了动态构造三元组约束的方法，但大多都是从数据中选择或强调部分约束，并没有构造新的约束，受对抗度量学习 (AML) 的启发，本文提出一种三元对抗约束的构造方法。

2.1　模型构建

通过调整参数动态构建三元组，提出了对抗样三元组约束的度量学习算法 (metric learning algorithm with adversarial sample triples constraints, ASTCML)。算法分为 2 个阶段：对抗阶段和区分阶段。

对抗阶段，生成对抗样本。初始三元组构建参考文献 [15]，针对每个样本 $\boldsymbol{x}_i$，选择与其距离最近的 K 个样本 $\boldsymbol{x}_j$ 及不同类的所有样本 $\boldsymbol{x}_l$ 构成三元组。当 $(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{x}_l)$ 三元组约束间的距离不满足约束关系 $\boldsymbol{d}_M(\boldsymbol{x}_i,\boldsymbol{x}_l)-\boldsymbol{d}_M(\boldsymbol{x}_i,\boldsymbol{x}_j)\geqslant 1$ 时，样本 $\boldsymbol{x}_l$ 为入侵样本，三元组 $(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{x}_l)$ 为违反约束关系的三元组。对初始三元组中违反约束关系的三元组构建对抗三元组，在入侵样本 $\boldsymbol{x}_l$ 的附近生成对抗样本 $\boldsymbol{\pi}_{il}$，使 $(\boldsymbol{x}_i,\boldsymbol{\pi}_{il})$ 间的距离尽可能小，$(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{\pi}_{il})$ 之间更加难以区分，如图 2 所示。通过式 (1) 中的损失函数计算对抗样本。

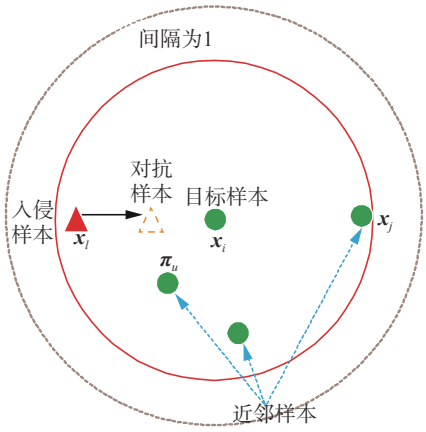


图 2　对抗过程示意

Fig. 2　Schematic illustration of adversarial processes

$$\min \sum_{(i,j,l)\in N} \boldsymbol{d}_M(\boldsymbol{x}_i,\boldsymbol{\pi}_{il})+\alpha \sum_{(i,j,l)\in N} \boldsymbol{d}_M(\boldsymbol{\pi}_{il},\boldsymbol{x}_l) \tag{1}$$

式中：N 表示初始三元组中违反约束关系的三元组；α 为调控因子，控制 $\boldsymbol{\pi}_{il}$ 是否为对抗样本。

区分阶段, 学到的度量尽可能区分对抗三元组。将生成的对抗样本代入初始违反约束关系的三元组中, 通过调整参数动态生成新的三元组。在新的三元组 $(\boldsymbol{x}_i,\boldsymbol{x}_j,\boldsymbol{\pi}_{il})$ 中, 使相似样本 $(\boldsymbol{x}_i,\boldsymbol{x}_j)$ 间距离尽可能小, 相似样本与不相似样本之间以一定的间隔分离开。引入非负的松弛变量 ξ_{ijl}, 构建如式 (2) 所示的损失函数进行度量学习:

$$\begin{aligned}&\min(1-\mu)\sum_{i,j\sim i}\boldsymbol{d}_{\boldsymbol{M}}(\boldsymbol{x}_i,\boldsymbol{x}_j)+\mu\sum_{i,j\sim i}\sum_{l}(1-y_{il})\xi_{ijl}\\&\text{s.t.}\quad \boldsymbol{d}_{\boldsymbol{M}}(\boldsymbol{x}_i,\boldsymbol{\pi}_{il})-\boldsymbol{d}_{\boldsymbol{M}}(\boldsymbol{x}_i,\boldsymbol{x}_j)\geqslant 1-\xi_{ijl}\geqslant 0\\&\qquad\boldsymbol{M}\geqslant 0\end{aligned}\tag{2}$$

式中: 最小化损失函数中的前者表示近邻损失, 后者表示三元组损失; μ 为权衡因子, 调节近邻损失与三元组损失在损失函数中的比重; 当 $y_i=y_l$ 时, $y_{il}=1$, 否则, $y_{il}=0$; 第 1 约束条件为三元组约束条件, 使相似样本与不相似样本之间以一定的间隔分离开; 第 2 约束条件 $\xi_{ijl}\geqslant 0$ 表示违反了三元组约束条件的间隔; 第 3 约束条件 $\boldsymbol{M}\geqslant 0$ 以保证距离的有效性。

2.2　优化问题求解

该模型的目标函数是一个凸优化问题, 可以利用梯度下降方式进行求解。根据式 (1) 可以得到对抗样本的闭式解:

$$\boldsymbol{\pi}_{il}=\frac{1}{\alpha+1}\boldsymbol{x}_i+\frac{\alpha}{\alpha+1}\boldsymbol{x}_l,(i,j,l)\in\mathcal{N}\tag{3}$$

将对抗样本代入违反约束的初始三元组中。区分阶段的损失函数也可以表示为

$$\begin{aligned}\boldsymbol{L}=&(1-\mu)\sum_{i,j\sim i}\boldsymbol{d}_{\boldsymbol{M}}(\boldsymbol{x}_i,\boldsymbol{x}_j)+\\&\mu\sum_{i,j\sim i}\sum_{l}(1-y_{il})[1+\boldsymbol{d}_{\boldsymbol{M}}(\boldsymbol{x}_i,\boldsymbol{x}_j)-\boldsymbol{d}_{\boldsymbol{M}}(\boldsymbol{x}_i,\boldsymbol{\pi}_{il})]_+\end{aligned}\tag{4}$$

利用式 (4) 得到 $\boldsymbol{M}$ 的梯度:

$$\begin{aligned}\frac{\partial\boldsymbol{L}}{\partial\boldsymbol{M}}=&(1-\mu)\sum_{i,j\sim i}\boldsymbol{X}_{ij}+\\&\mu\sum_{(i,j,l)\in\mathcal{J}}\boldsymbol{X}_{ij}-\left(\left(\left(\frac{\alpha}{\alpha+1}\right)^2-1\right)[\xi_{ijl}^{\text{ori}}]_+ +1\right)\boldsymbol{X}_{il}\end{aligned}\tag{5}$$

式中: $\mathcal{J}$ 表示以对抗样本构成的三元组中违反约束条件间隔的三元组; $\boldsymbol{x}_{ij}=(\boldsymbol{x}_i-\boldsymbol{x}_j)(\boldsymbol{x}_i-\boldsymbol{x}_j)^{\mathrm{T}}$, $\boldsymbol{x}_{il}=(\boldsymbol{x}_i-\boldsymbol{x}_l)(\boldsymbol{x}_i-\boldsymbol{x}_l)^{\mathrm{T}}$, 初始三元组中不相似样本间距离小于相似样本间距离 $[\xi_{ijl}^{\text{ori}}]_+=1$, 反之 $[\xi_{ijl}^{\text{ori}}]_+=0$。为了便于调整参数, 令 $\beta=\dfrac{\alpha}{\alpha+1}$, 详细过程如算法 1 所示。

算法 1 对抗样本三元组约束的度量学习算法。

输入 $\boldsymbol{X}$: 样本集; $\boldsymbol{Y}$: 样本标签集; β: 调控参数; μ: 权衡因子。

输出 $\boldsymbol{M}$。

初始化 $\boldsymbol{M}_0=\boldsymbol{I}$。

根据式 (3) 计算对抗样本, 代入初始三元组中。

迭代计算:

1) 根据式 (5) 计算梯度 $\nabla\boldsymbol{G}_t$。

2) 更新梯度 $\boldsymbol{M}_{t+1}=\boldsymbol{M}_t-\lambda\nabla\boldsymbol{G}_t$。

3) 将 $\boldsymbol{M}_{t+1}$ 进行分解, 得到 $\boldsymbol{U},\boldsymbol{V}_+$。

4) $\boldsymbol{M}_{t+1}=\boldsymbol{U}^{\mathrm{T}}\boldsymbol{V}_+\boldsymbol{U}$。

5) 直到收敛。

假定样本个数为 N, 共有 C 类且每个类的样本数相同, β 和 μ 的取值个数分别为 p 和 q, t 为迭代次数。由式 (2) 构建的三元组约束个数大致为 $KN^2(1-1/C)$, 并计算每个三元组约束间的距离, 对违反约束的三元组进行梯度下降。为取得较高的分类精度, 选取合适的 β 和 μ 值进行分类, 算法所需次数为 $2pqtKN^2(1-1/C)$。所以算法 1 的时间复杂度为 $O(N^2)$。

3　实验分析

本节在 12 个数据集上 (如表 1 所示), 对提出的 ASTCML 算法与目前几个代表性算法进行比较, 并分析了实验中参数的灵敏度与提出算法的收敛性。

3.1　实验数据与设计

本文提出的 ASTCML 算法与与 K 近邻算法 (K-nearest neighbor, KNN)、ITML 算法[12]、GMML 算法[13]、LMNN 算法[16]、PFLMNN 算法[18]、RVML 算法[21]、LDMLT 算法[24]和 AML 算法[25] 进行了对比。

表 1　数据描述

Table 1　Data sets description

数据集	Balance	Dermatology	Diabetes	German	Ionosphere	Wine	Zoo	Segment	Waveform-21	Corel_5k	Satellite	Wilt
样本数	625	366	768	1 000	351	178	101	2 310	2 746	5 000	6 435	4 839
特征	4	34	8	20	34	13	16	19	21	423	36	5
类别	3	6	2	2	2	3	7	7	3	50	6	2

实验中, 对表 1 数据中的 Corel_5k 数据集, 先用主成分分析 (principal component analysis, PCA) 进行降维, 保留的数据信息大于 95%, 除 Satellite 和 Wilt 数据集外, 对其他数据集进行预处

理操作，对处理后的数据集进行划分，其中 80% 的数据为训练集，20% 的数据为测试集。采用 5 折交叉验证的方法进行实验，将训练集随机分为 5 部分，轮流作为验证集，并对 5 次实验结果求平均，选择在验证集上达到最高分类精度的参数，在测试集上进行测试。Satellite 数据集由 4 435 个训练样本和 2 000 个测试样本组成，Wilt 数据集是由 4 339 个训练样本和 500 个测试样本组成，针对这 2 个数据集，首先对训练集进行预处理操作，记录下训练集的归一化方法，将该方法应用于测试集进行预处理，在所有参数实验结果中选择分类精度最高的精度，即为当前数据集的分类精度。初始化度量矩阵 $\boldsymbol{M}=\boldsymbol{I}$，参数 β 的取值范围为 $\{0.1, 0.2, \cdots, 0.9\}$，$\mu$ 的取值范围为 $\{0.1, 0.2, \cdots, 1\}$。此外，由式 (8) 可以得到，当 β 取值为 1 时，算法精度与 LMNN 算法的结果相同或相近。使用 KNN 分类器的分类正确率评价度量学习算法的性能。当样本数大于或等于 4 500 时，μ 的取值范围为 $\{0.1, 0.3, 0.5, 0.7, 0.9\}$，且当数据集为 Corel_5k 时，$\beta$ 的取值范围为 $\{0.2, 0.4, 0.6, 0.8\}$，同时采用 3 折进行交叉验证。

3.2　实验结果与分析

实验结果在表 2 中列出，表 2 中粗体表示最高的分类正确率，在次高的分类正确率下划横线。当数据集为 Corel_5k 时，AML 算法运行时间相对较长，不参与算法比较。实验结果显示本文算法普遍优于代表性的度量学习方法，相比于动态构建三元组的 LDMLT 算法，除在 German 数据集上取得次高的分类精度，在其他数据集上的分类精度明显提高；与 LMNN 算法相比，提出算法的分类精度最低与其保持一致；相比基于对抗训练的 AML 算法，分类精度普遍较高。可以得出，本文算法在一定程度上说明区分更加难以区分的三元组约束能够提升算法的性能。

表 2　分类精度的对比

Table 2　Comparisons of classification accuracy

数据集	KNN	ITML	GMML	RVML	LDMLT	LMNN	PFLMNN	AML	ASTCML
Balance	0.8080	0.9280	0.8000	0.8080	0.7840	0.8240	0.8000	0.8080	**0.9760**
Dermatology	0.9324	0.9595	0.9324	0.9324	0.9459	**0.9730**	0.9324	0.9459	**0.9730**
Diabetes	0.6883	0.6818	0.6883	0.6883	0.6688	0.6948	**0.7273**	0.7078	**0.7273**
German	0.6850	0.7100	0.6850	0.6850	**0.7200**	0.6900	0.7100	0.7050	0.7150
Ionosphere	0.8592	0.8873	0.8592	0.8592	0.7887	0.9296	0.9014	0.8592	**0.9437**
Wine	0.9722	**1.0000**	0.9722	0.9722	0.9722	0.9722	0.9722	0.9722	**1.0000**
Zoo	0.8571	0.9048	0.8571	0.8571	0.8571	0.9048	0.8571	0.8571	**0.9524**
Segment	0.9416	**0.9675**	0.9416	0.9416	0.9610	0.9589	0.9567	0.9545	0.9654
Waveform-21	0.7709	0.7564	0.7709	0.7709	0.6873	0.7909	0.7891	0.7764	**0.8400**
Corel_5k	0.2680	0.2630	0.2680	0.2680	0.2560	0.2930	0.2660	—	**0.2980**
Satellite	0.9065	0.8880	0.9065	0.9065	0.8270	0.9085	**0.9155**	0.9065	0.9105
Wilt	0.6780	0.7640	0.6780	0.6780	0.8020	0.8220	0.8040	0.7140	**0.8260**
Mean	0.7806	0.8092	0.7799	0.7806	0.7725	0.8135	0.8026	—	**0.8439**

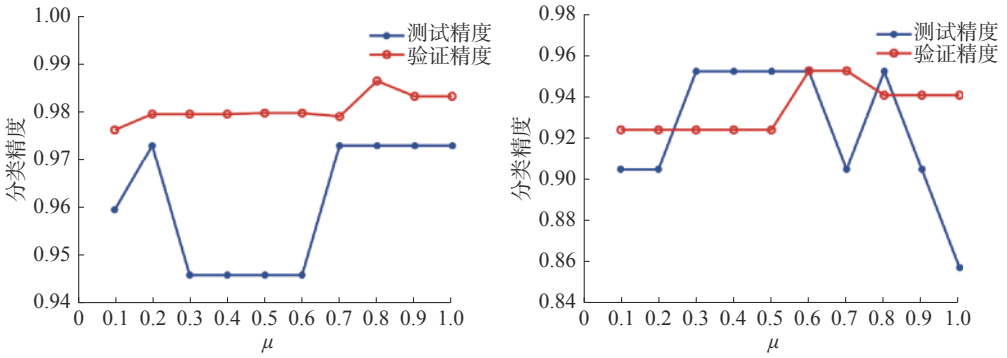
3.3　参数的灵敏度分析

在本文提出的算法中，超参数 β 和 μ 的设置对实验结果会产生一定的影响，其中参数 β 控制在入侵样本附近产生对抗样本，参数 μ 为权衡因子，调节三元组损失在整个损失中的比重。在不同数据集下，只以最高的验证集分类正确率设置超参数 β 和 μ，通过固定其中的一个超参数，调整另一个超参数，观察在验证集与测试集上分类正确率的变化情况。从图 3、4 可以看出，当测试集上取得最高分类正确率时，验证集上的分类正确率也最高；在不同的参数设置下，验证集上分类准确率的变化幅度相对较小，而测试集上变化幅度相对较大。

3.4　收敛性分析

在对抗样本三元组约束的度量学习算法迭代优化的过程中，若相邻 2 次损失值的差小于设定

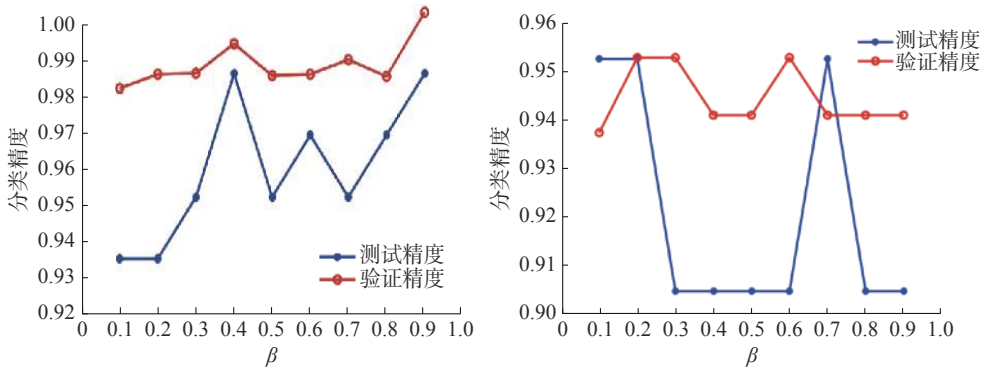
的阈值或迭代次数大于最大迭代次数, 则算法结束。本文通过不同数据集分别在测试集上迭代 100 次的损失值变化情况分析提出算法的收敛性。从图 5 可以看出, 在迭代过程中, 随着迭代次数的增加, 损失函数的值呈现下降趋势, 表明提出算法是可以收敛的。



(a) Dermatology 数据集 (β=0.9)　　(b) Zoo 数据集 (β=0.2)

图 3　不同 μ 下的分类精度

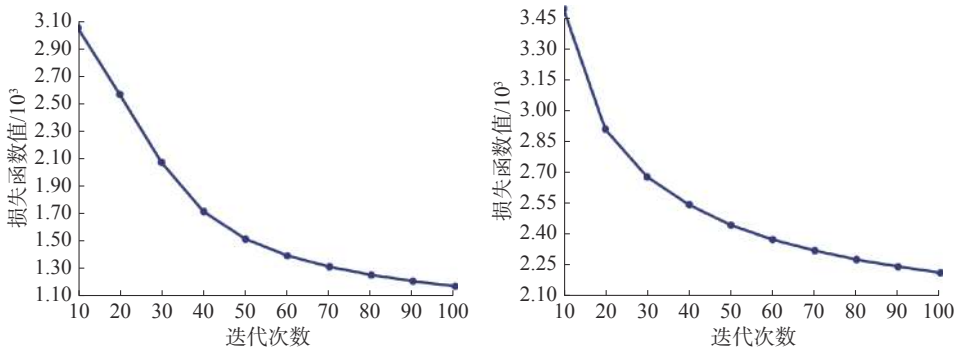
Fig. 3　Classification accuracy under different μ values



(a) Dermatology 数据集 (μ=0.8)　　(b) Zoo 数据集 (μ=0.6)

图 4　不同 β 下的分类精度

Fig. 4　Classification accuracy under different β values



(a) Wine 数据集 (β=0.5 μ=0.2)　　(b) Ionosphere 数据集 (β=0.9 μ=0.3)

图 5　损失值变化情况

Fig. 5　Change of loss value on different data sets

4　结束语

本文借鉴对抗训练的思想, 建立了学习对抗样本的优化模型, 构建了对抗样本三元组约束度量学习模型, 并提出相应的度量学习算法。理论上, 基于对抗训练思想得到的三元组约束更加符合数据的情况, 学习对抗样本的模型求解简单, 且可以提高分类精度。实验结果验证了提出算法的性能。虽然, 与已有代表性算法相比提出算法的性能有所提升, 但其对参数较为敏感。如何降低模型对参数的敏感性将是值得进一步研究的问题。

参考文献:

[1] QIAN Qi, JIN Rong, ZHU Shenghuo, et al. Fine-grained visual categorization via multi-stage metric learning[C]// 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Boston, USA, 2015: 3716–3724.

[2] GAO Yue, WANG Meng, JI Rongrong, et al. 3-D object retrieval with hausdorff distance learning[J]. IEEE transactions on industrial electronics, 2014, 61(4): 2088–2098.

[3] HOI S C H, LIU W, CHANG S F. Semi-supervised distance metric learning for collaborative image retrieval[C]// 2008 IEEE Conference on Computer Vision and Pattern Recognition. Anchorage, AK, USA, 2008: 1–7.

[4] HOI S C H, LIU W, LYU M R, et al. Learning distance metrics with contextual constraints for image retrieval[C]// 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06). New York, NY, USA, 2006: 2072–2078.

[5] DONG Yanni, DU Bo, ZHANG Liangpei, et al. Hyperspectral target detection via adaptive information-theoretic metric learning with local constraints[J]. Remote sensing, 2018, 10(9): 1415.

[6] DONG Yanni, DU Bo, ZHANG Liangpei. Target detection based on random forest metric learning[J]. IEEE journal of selected topics in applied earth observations and remote sensing, 2015, 8(4): 1830–1838.

[7] DONG Yanni, DU Bo, ZHANG Lefei, et al. Local decision maximum margin metric learning for hyperspectral target detection[C]//2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS). Milan, Italy, 2015: 397–400.

[8] HU Junlin, LU Jiwen, YUAN Junsong, et al. Large margin multi-metric learning for face and kinship verification in the wild[C]//12th Asian Conference on Computer Vision. Singapore, Singapore, 2015: 252–267.

[9] LU Rui, WU Kailun, DUAN Zhiyao, et al. Deep ranking: triplet MatchNet for music metric learning[C]//2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). New Orleans, USA, 2017: 121–125.

[10] XING E P, NG A Y, JORDAN M I, et al. Distance metric learning, with application to clustering with side-information[C]//Proceedings of the 15th International Conference on Neural Information Processing Systems. Cambridge, MA, USA, 2002: 521–528.

[11] YING Yiming, LI Peng. Distance metric learning with eigenvalue optimization[J]. The journal of machine learning research, 2012, 13(1): 1–26.

[12] DAVIS J V, KULIS B, JAIN P, et al. Information-theoretic metric learning[C]//Proceedings of the 24th International Conference on Machine Learning. Corvallis, Oregon, USA, 2007: 209–216.

[13] ZADEH P H, HOSSEINI R, SRA S. Geometric mean metric learning[C]//Proceedings of the 33rd International Conference on Machine Learning. New York, NY, USA, 2016: 2464–2471.

[14] OMARA I, ZHANG Hongzhi, WANG Faqiang, et al. Metric learning with dynamically generated pairwise constraints for ear recognition[J]. Information, 2018, 9(9): 215.

[15] WEINBERGER K Q, BLITZER J, SAUL L. K. Distance metric learning for large margin nearest neighbor classification[M]. WEISS Y, SCHÖLKOPF B, PLATT J. Advances in Neural Information Processing Systems. Cambridge, MA: MIT Press, 2006: 1473–1480.

[16] WEINBERGER K Q, SAUL L K. Distance metric learning for large margin nearest neighbor classification[J]. The journal of machine learning research, 2009, 10: 207–244.

[17] 杨柳, 于剑, 景丽萍. 一种自适应的大间隔近邻分类算法 [J]. 计算机研究与发展, 2013, 50(11): 2269–2277.
YANG Liu, YU Jian, JING Liping. An adaptive large interval nearest neighbor classification algorithm[J]. Journal of computer research and development, 2013, 50(11): 2269–2277.

[18] SONG Kun, NIE Feiping, HAN Junwei, et al. Parameter free large margin nearest neighbor for distance metric learning[C]//The 31st AAAI Conference on Artificial Intelligence. San Francisco, USA, 2017: 2555–2561.

[19] LIU Meizhu, VEMURI B C. A robust and efficient doubly regularized metric learning approach[C]//12th European Conference on Computer Vision. Florence, Italy, 2012: 646–659.

[20] LE CAPITAINE H. Constraint selection in metric learning[J]. Knowledge-based systems, 2018, 146(15): 91–103.

[21] PERROT M, HABRARD A. Regressive virtual metric learning[C]//Advances in Neural Information Processing Systems. Montréal, Canada, 2015: 1810–1818.

[22] WANG Faqiang, ZUO Wangmeng, ZHANG Lei, et al. A kernel classification framework for metric learning[J]. IEEE transactions on neural networks and learning systems, 2015, 26(9): 1950–1962.

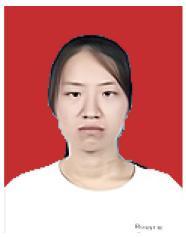
[23] ZUO Wangmeng, WANG Faqiang, ZHANG D, et al. Distance metric learning via iterated support vector machines[J]. IEEE transactions on image processing, 2017, 26(10): 4937–4950.

[24] MEI Jiangyuan, LIU Meizhu, KARIMI H R, et al. LogDet divergence-based metric learning with triplet constraints and its applications[J]. IEEE transactions on im-

age processing, 2014, 23(11): 4920–4931.

[25] CHEN Shuo, GONG Chen, YANG Jian, et al. Adversarial metric learning[C]//Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence. Stockholm, Sweden, 2018: 2021–2027.

作者简介：



王鑫，硕士研究生，主要研究方向为度量学习。

郭鑫垚，博士研究生，主要研究方向为度量学习。

魏巍，教授，博士生导师，中国人工智能学会知识工程与分布智能专委会常委，主要研究方向为数据挖掘、机器学习、粒计算。主持和参与国家自然科学基金项目、山西省自然科学基金项目 10 余项。发表学术论文 20 余篇。

CAAI 第六届全国大数据与社会计算学术会议

China National Conference on Dig Data and Social Computing

2021 年 8 月 21−22 日，由中国人工智能学会主办，CAAI 社会计算与社会智能专委会、重庆工商大学承办的“CAAI 第六届全国大数据与社会计算学术会议”（以下简称 BDSC 2021）将在重庆召开。

BDSC 创建于 2012 年，旨在搭建全国大数据与社会计算学术交流平台，培育社会计算与社会智能学科发展，助力社会计算与社会智能领域人才成长，建设“有仁、有信、有情”的学术共同体，已成为全国大数据与社会计算领域的知名学术交流品牌。

本次会议的主题为“数字社会的重构与转型”，面向国家经济社会发展战略，立足数字社会构建，通过跨学科交叉视野剖析数字社会的机遇与挑战。会议面向全国开展大数据与社会计算领域的学术征文，重点探讨数字社会的基础性、前瞻性和战略性理论及其应用，讨论数字社会领域前沿进展，交流新的学术思想和新方法，探索数字社会对人类发展的意义，展望数字社会未来的发展趋势。

本次大会将组织专家对所有投稿论文进行双盲评审，优秀论文将有机会被推荐到 11 本高水平期刊进入期刊快速评审通道，所有录用论文在大会上进行墙报（poster）交流。

大会将邀请人工智能、IoT+5G 网络、地理信息以及社会科学、系统科学等交叉领域的重量级学者做大会报告，举办系统科学的前沿讲习班。大会致力于跨越传统学科分界，呈现大数据智能时代社会研究新境界，将重磅发布极具创新性的大规模社会计算试验场和社会计算开放数据集，并举办全国社会计算大赛。

征文主题：

1）社会系统建模与仿真；2）人工智能与认知科学；3）社会网络与群体行为；4）社会地理与城市计算；5）计算人口新范式、新方法；6）数字基础建设与智能社会；7）数据价值评估与流通服务；8）数字社会与公共安全；9）数字政府与公共大数据；10）数字技术与社会韧性；11）数据与社会治理；12）数字平台建设与管理；13）计算社会与系统工程；14）数据伦理与隐私保护。

重要时间：

投稿截止日期：2021 年 6 月 15 日

审稿通知日期：2021 年 7 月 15 日

审稿修改日期：2021 年 8 月 1 日

录用通知日期：2021 年 8 月 7 日

会议召开日期：2021 年 8 月 21−22 日

投稿链接：https://easychair.org/conferences/?conf=bdsc2021

大会网站：http://idke.ruc.edu.cn/BDSC2021/