文章编号：2095-2163(2021)07-0177-03 中图分类号：TP399 文献标志码：A

基于聚类分析的人工智能产品发展风险评估方法

袁炳夏
（惠州学院，广东 惠州 516007）

摘 要：人工智能产品已经多元化地应用于社会生活中，推动技术发展进步的同时也带来了一定的安全风险，准确地评估人工智能产品发展风险可以为其可持续发展提供良好的参考与借鉴。为此，提出基于聚类分析的人工智能产品发展风险评估方法。首先，以主题词的形式设计人工智能产品目前应用范围的关联图谱，提取人工智能产品发展的关键特征；其次，依据产品发展特征深度提取产品发展中应用的高频主题词，结合发展过程中可能存在的风险因素，对其进行聚类处理，实现人工智能产品发展的风险评估。实验发现，人工智能产品发展确实存在一定的风险，所设计的聚类分析方法可以准确评估其发展风险。

关键词：聚类分析；人工智能；聚类结果；风险评估

The risk assessment method of artificial intelligence product development based on cluster analysis

YUAN Bingxia
（Huizhou University, Huizhou Guangdong 516007, China）

【Abstract】 Artificial intelligence products have been widely used in social life, promoting the development and progress of technology, but also brings a certain security risk. Accurate assessment of the development risk of artificial intelligence products can provide a good reference for its sustainable development. Therefore, a risk assessment method of AI product development based on cluster analysis is proposed. Firstly, the association map of the current application range of artificial intelligence products is designed in the form of subject words, and the key features of the development of artificial intelligence products are extracted. Secondly, the high-frequency subject words applied in the development of products are deeply extracted according to the characteristics of product development, and combined with the possible risk factors in the development process, they are clustered to realize the risk assessment of the development of artificial intelligence products. Experiments show that there are some risks in the development of AI products, and the cluster analysis method can accurately evaluate the development risk.

【Key words】 clustering analysis; artificial intelligence; clustering results; risk assessment

0 引 言

人工智能是当代工业革命中的核心驱动力，随着该技术在基础理论和技术实践方面科研成果的陆续涌现，人工智能在时下的产业环境中获得了快速发展。人工智能不仅在智能家居、人脸识别等方面改变了人们的生活方式，而且可能引起巨大的社会变革[1]。国内各省市地方层面上有关人工智能的发展规划也相继出台。但随着人工智能产品的快速发展与进步，也带来了一定的经济、隐私、伦理及安全风险，如身份信息泄露、隐私数据公开等。由此，预估人工智能产品发展风险是目前亟待解决的重要问题。发展至今，研究中常用的主要是关联规则和聚类分析方法，因此本文结合上述 2 种方法，将各个省市地方近年来出台的人工智能产业规划产业发展作为研究样本，运用聚类分析等文本挖掘与数据可视化方法，从高频关键词和内容关联度着手，评估人工智能产品发展风险，以期进一步理清国内不同区域人工智能产业布局，为提高未来人工智能产业高质量发展提供相关参考。

1 提取人工智能产品发展的关键特征

1.1 设计人工智能产品应用范围关联图谱

以主题词的形式设计人工智能产品目前应用范围的关联图谱，提取人工智能产品发展的关键特征；完成聚类中心在样本点中的选择，其特征离散属性与连续属性的定义式如下所示：

$$\rho_i = \chi \sum_{j \neq 1} (d_{ij} + d_c) \tag{1}$$

$$\rho_j = \sum_{j \neq 1} \exp[d_{ij} d_c] \tag{2}$$

其中，i 表示关键特征离散的样本点；j 表示关键特征连续的样本点；χ 表示样本点离散分布的分布

作者简介：袁炳夏（1979-），男，硕士，计算机高级工程师，主要研究方向：计算机网络、电子信息、信息安全等。

收稿日期：2021-04-22

规律；d_{ij} 表示样本点 i 到 j 之间的距离；d_c 表示 2 个样本点之间的截断距离[2]。在此基础上生成伪代码如下：

```
def calcluate_distance(core: tuple, dot: tuple):
"""
计算 2 个点之间的欧氏距离
:param core: 质心坐标 (x,y) 类型为 tuple
:param dot:  要计算距离的点(m,n) 类型为 tuple
:return: 距离 dist 类型为 float
```

根据上述公式计算，本文选取了出现频率最高的前 15 位的相关主题词，为了找出粗糙集中产业主题词之间的聚类情况，进一步理清产业发展内容的关系架构[3]。基于度数中心性和中间中心性的数据，利用 SPSS20，对主题词进行了系统聚类分析，得到聚类结果，并使用 Gephi 软件进行可视化，对文献和相关数据源的要求较低，对关键词矩阵进行聚类分析，得到产业发展相关因素的关联度图谱如图 1 所示。

图 1 关联度图谱

Fig. 1 Correlation map

以上 15 个主题词大致可以分成 4 类。这 4 类主题词所忘掉的重点是有所不同的，可以依次概括为：人工智能的研发创新与管理，注重人才和平台建设、人工智能发展的相关支撑、人工智能的产业化应用与服务体系以及培育工业与制造基础，形成人工智能的示范效应。

1.2 获取人工智能产品发展的关键特征

聚类分析的应用第一步，就是利用该聚类分析中的论域，建立一个最大近邻粗糙集，获取常规因素、异常因素的特征参量[2]。粗糙数据集利用已知影响条件，描述不确定的影响因素，发现数据的潜在特点。假设论域是影响因素等相关数据的非空集合，用字母 W 来表示，根据该集合将研究的影响数据进行分类，将特征性相似的数据归结为对象相同或者不同的类簇子集，子集可用 $w_1, w_2, \cdots, w_i$ 予以表示。

粗糙数据集在此论域空间上，对集合中的因素按照等价关系划分，其中类目相同且差距较小的数据关系，称之为不可辨关系。

假设给定一个论域为 U，用 γ_i 表示该论域 U 中的等价关系；设置 x_i 为 U 中的对象，$u_1, u_2, \cdots, u_i$ 为论域 U 的子集，判断属于 u_i 的数据 x_i 组成的最大集合 $u_{\max}$，该集合为集合 u_i 关于等价关系 γ_i 的下逼近；而与 u_i 相交的非空等效并集为最小集合 $u_{\min}$，此时称之为集合 u_i 关于等价关系 γ_i 的下逼近。该过程可利用图 2 进行表示。

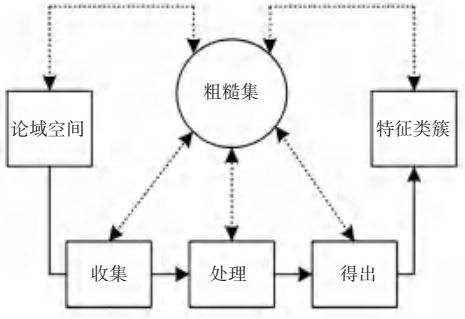

图 2 粗糙集特征提取过程

Fig. 2 Feature extraction process of Rough Set

通过上述提取过程，得出量化影响因素特征参量，该参量可以利用如下公式来描述：

$$q_i(x_i) = [x_i \mid \Delta({x_i}^a, {x_i}^b) < d(x_i), x_i \in u_i] \tag{3}$$

其中，$q_i(x_i)$ 表示第 i 个论域子集上的粗糙集，在等价关系约束下的特征参量；x_i 表示影响人工智能产业发展的变量因子；a 表示该因素的表层影响关系；b 表示该因素的深层影响关系；$\Delta({x_i}^a, {x_i}^b)$ 表示不同关联深度下的挖掘系数[4]。通过上述公式得到具有相似特征的影响参量，为定义相似度提供精确的数据。

2 人工智能产品发展风险聚类分析

每项产业发展都有明确的目标和相应的产业发展工具类型。因此，在“目标工具”框架下分析人工智能产业发展时，有必要细化产业发展目标，对产业发展工具进行分类。通过对不同地区的人工智能产业环境进行分析，构建了基于产业发展目标的人工智能产业环境视角，具体包括基本理论、关键技术、支撑平台、产业发展、集成与应用等几个方面，旨在

优化人工智能产业环境。考虑到每项产业发展过程中风险存在海量特征，且标签信息较多，风险类型较复杂。将人工智能产品发展风险建立多维特征并实施分类，能够细分风险类型，以此判断不同属性下的风险特征。基于此，构建人工智能产品发展风险评估指标见表 1。

表 1　人工智能产品发展风险评估指标

Tab. 1　Risk assessment indicators for artificial intelligence product development

一级指标	二级指标	
	指标	举例
技术风险	核心技术是否泄露	技术沉溺风险
	技术人员操作能力	失业风险
安全问题	是否有紧急事故处理预案	隐私泄露风险
伦理风险	是否遵循伦理道德底线	网络犯罪风险

以表 1 的评价指标为基础，本文通过 K 均值聚类算法实现人工智能产品发展风险评估。通过使用最近邻质心决策规则把上文处理后的人工智能产品发展风险关键特征分为 f 个簇，再迭代运算各个簇的质心。K 均值算法的步骤是：

(1)选取 f 个数据点设成初始质心。

(2)实施迭代运算，把各个数据点纳入距离最短的质心，建立 f 个簇，再次运算各个簇的质心，当质心不出现变动时，输出分类结果。

综上所述，本文使用聚类算法实现人工智能产品发展风险的分类评估。

3　实验分析

为进一步验证本文评估方法的准确性，以 4 个人工智能产品发展风险评估二级指标为例，利用本文方法与文献[2]方法、文献[4]方法实施风险评估，通过均方根误差分析 3 种方法的评估准确性，测试结果见表 2。

表 2　3 种方法均方根误差对比结果

Tab. 2　Comparison of root mean square error of three methods

	本文方法	文献[2]方法	文献[4]方法
技术沉溺风险	2.2	4.5	4.5
隐私泄露风险	2.3	4.8	5.0
失业风险	3.0	5.3	5.4
网络犯罪风险	2.4	5.9	4.8

根据表 2 可知，本文方法的均方根误差明显低于其余 2 种方法。实验证明：在不同风险评估一级指标情况下，本文方法的均方根误差最低，表明本文方法的风险评估结果与真实风险评估结果更为接近，即本文方法的风险评估准确性更高。

分别统计风险指标数量为 10~20 个时，本文方法与文献[2]方法、文献[4]方法实施人工智能产品发展风险的效率，测试结果如图 3 所示。

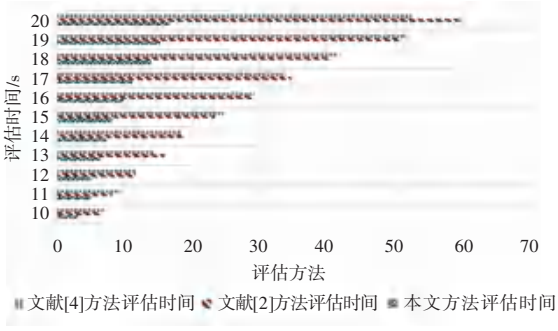

图 3　3 种方法评估时间对比结果

Fig. 3　Comparison of time among three methods

根据图 3 可知，随着风险指标数量的不断增加，3 种方法的风险评估时间均有所提升，本文方法的风险评估时间提升幅度明显低于其他两种方法，且整体风险评估时间也明显低于其他两种方法。实验证明：本文方法的风险评估时间用时较少，即风险评估效率高。

4　结束语

在互联网时代，人工智能产业是具有标志性、引领性及战略性的技术，是社会进步和国际竞争的动力源泉。在产业的发展过程中，应该注重安全与伦理的规范约束，并将其体现在产业发展制定规划中，同时亦不能忽略产业发展目标的差异化。提早完善人工智能的相关法律制度，进一步将人工智能产业进程加速完成，目的是解决人工智能产业在发展过程中产生的个人隐私、数据安全以及知识产权等方面的问题，否则人工智能发展过程中产生的核心矛盾会在一定程度上影响社会、甚至全球的安全和治理，因此在接下来的发展阶段中，国内需要推出一套完备的体系来规范人工智能产业的发展，搭建人工智能与其他领域产业的沟通互联。

参考文献

[1] 袁野，于敏敏，陶于祥，等. 基于文本挖掘的我国人工智能产业政策量化研究[J]. 中国电子科学研究院学报，2018，13(6)：663-668.

[2] 胡红博. 智能家居远距离可视化风险自动监测系统设计[J]. 现代电子技术，2019，42(4)：171-174.

[3] 李艳红. 基于机器学习的企业产品评论数据的情感分析研究[J]. 微型电脑应用，2019，35(11)：33-35，81.

[4] 李新瑜，张永庆. 基于产业链视角的人工智能风险分析及其防范[J]. 人文杂志，2020(4)：47-57.