

## 生成式对抗网络在金融数据中的应用

崔毅浩, 刘森, 叶广楠

(复旦大学金融科技研究院, 上海 200433)

**摘要:** 数据作为国家基础性战略资源和关键生产要素, 是经济社会发展的基础资源和创新引擎。金融行业作为数据的密集型和科技驱动型行业, 实现数据资产的优化配置, 是促进产业升级的关键因素。但金融数据普遍存在数据分布不均衡、数据信息不对称以及“数据孤岛”等问题, 导致数据无法充分发挥其价值。为了克服这些挑战, 金融机构积极采用各种生成模型合成高度逼真的数据, 以打破数据壁垒和垄断, 成为未来金融业发展的趋势和方向。生成式对抗网络 (generative adversarial network, GAN) 是最流行的模型之一, 在各个领域都有不俗的表现。其在金融表格数据生成、金融时间序列生成以及金融欺诈检测等方面也展现出广泛的应用潜力。文章介绍了 GAN 模型相较于其他生成模型在金融领域的优势; 对自 2014 年生成式对抗网络被提出以来的可被应用于金融领域的 GAN 模型进行整理, 并对各模型的原理进行介绍; 探讨 GAN 模型在生成金融表格数据、生成金融时间序列、金融欺诈检测等金融数据领域中的应用实践; 最后结合中国的实际情况, 分析了 GAN 在未来面临的挑战及发展方向。

**关键词:** 生成式对抗网络; 金融科技; 数据安全

**中图分类号:** TP309; F832

**文献标志码:** A

**DOI:** 10.11959/j.issn.2096-109x.2024047

## Application of generative adversarial networks for financial data

CUI Yihao, LIU Sen, YE Guangnan

Institute of FinTech, Fudan University, Shanghai 200433, China

**Abstract:** Data, recognized as a fundamental strategic resource and key production factor for a nation, has served as the foundational resource and innovation engine for economic and social development. The financial industry, characterized by its data-intensive and technology-driven nature, necessitates the optimal allocation of data assets to facilitate industrial upgrading. However, financial data commonly exhibits issues such as uneven distribution, in-

收稿日期: 2023-02-16; 修回日期: 2024-05-26

通信作者: 刘森, senliu@fudan.edu.cn;

基金项目: 中国工程院战略研究与咨询项目 (2023-33-14); 上海市自然科学基金 (23ZR1404900); 国家重点研发计划项目 (2023YFC3305200); 云南省重大科技专项计划 (202402AD080005)

**Foundation Items:** Chinese Academy of Engineering Strategic Research and Consulting Project (2023-33-14), The Natural Science Foundation of Shanghai (23ZR1404900), National Key Research and Development Program of China (2023YFC3305200), Research on Key Technologies, Innovation and Application of Smart Port (202402AD080005)

引用格式: 崔毅浩, 刘森, 叶广楠. 生成式对抗网络在金融数据中的应用[J]. 网络与信息安全学报, 2024, 10(3): 156-174.

**Citation Format:** CUI Y H, LIU S, YE G N. Application of generative adversarial networks for financial data[J]. Chinese Journal of Network and Information Security, 2024, 10(3): 156-174.

formation asymmetry, and data silos, which have prevented data from fully realizing its value. To address these challenges, various generative models have been actively adopted by financial institutions to synthesize highly realistic data, thereby breaking down data barriers and monopolies, and shaping the future trend of the financial industry. Among these models, Generative Adversarial Networks (GANs) have emerged as particularly popular, demonstrating impressive performance across various fields and showing great potential in generating financial tabular data, financial time series, and detecting financial fraud. The advantages of the GAN model compared with other generative models in the financial field were analyzed. The GAN models that have been applied to the financial field since Generative Adversarial Networks were proposed in 2014 were presented, and the principles of each model were introduced. The application practice of the GAN model in generating financial tabular data, generating financial time series, and financial fraud detection, as well as other financial data fields, was explored. Finally, the challenges and development direction of GANs for the future were discussed, taking into account the actual situation in China.

**Keywords:** generative adversarial networks, fintech, data security

## 0 引言

金融数据区别于交通、教育等行业的常规数据，其存储大量重要敏感数据。这些敏感数据可能在银行、保险、证券等金融机构的众多业务场景中被使用，而一旦敏感数据以真实状态泄露，或遭到恶意破坏，则会为其用户带来潜在安全威胁。

为保护数据隐私，我国颁布了多个法案，构建了网络空间安全与数据保护法律体系的基本框架。其中，《中华人民共和国网络安全法》提出了国家网络空间战略法律规定，《中华人民共和国数据安全法》为数字经济合规发展保驾护航，《中华人民共和国个人信息保护法》从国家层面建立健全个人信息保护制度<sup>[1]</sup>。金融业作为数据密集型行业，由于相关数据的高敏感性和高价值性，全面保障数据安全和个人信息权益成为金融行业数据安全治理的新内核<sup>[2]</sup>。随着相关法律法规相继进入实施阶段，金融行业需要根据要求提升数据安全合规能力<sup>[3]</sup>。

随着数据隐私监管力度的很大，数据的获取和共享变得极为困难<sup>[4]</sup>，引发了数据信息不对称问题和“数据孤岛”问题。而人工智能技术的快速发展，使运用深度学习模型生成高度逼真的金融数据技术解决上述问题成为可能。由于数据是合成的，没有映射到任何原始数据，因此可以被自由使用、共享和存储。相比传统数据合成方法，深度学习方法可以保留更多的统计特征，以应对更高精准度的金融科技产品和模型训练。合

成数据在金融业的应用前景是广泛的，它可以为金融业数据的治理提供基础保障，尤其是可以在客户获取和高级分析、抵押贷款分析、信用决策和限额评估、风险管理和定价、欺诈和异常检测、监控和收集等多个场景中得到广泛应用<sup>[3]</sup>。

金融数据合成的基本步骤有：数据预处理、对生成模型进行建模、数据生成、合成数据评估<sup>[5]</sup>，如图1所示。

## 1 相关背景

### 1.1 金融时间序列

动态金融市场是非常复杂的过程，因为这些过程的基本机制往往是未知的<sup>[6]</sup>。然而，多年来对金融时间序列的研究表明，尽管它们看似完全随机，但资产价格的变化始终符合几个重要的统计特性，这些特性被称为特征事实<sup>[7]</sup>。

特征事实是从大量市场研究所涉及的统计特征中提取的。虽然在进行金融市场分析时，不同的经济环境势必会挖掘出不同的统计特征，但是对金融市场的实证结果表明，一些关键特征会在具有不同假设特征的市场中反复出现。而这些特征（即特征事实）在资产价格动态建模中是至关重要的。

5个重要的市场特征事实<sup>[7]</sup>如下。①线性不可预测性或缺乏自相关：除短期内时间尺度之外，资产收益预期呈现最小线性自相关。②厚尾分布：收益分布似乎呈现出幂律或帕累托式尾部特征，这意味着极端值出现的概率远远高于正态分布数据集出现的概率。③波动性聚类现象：在

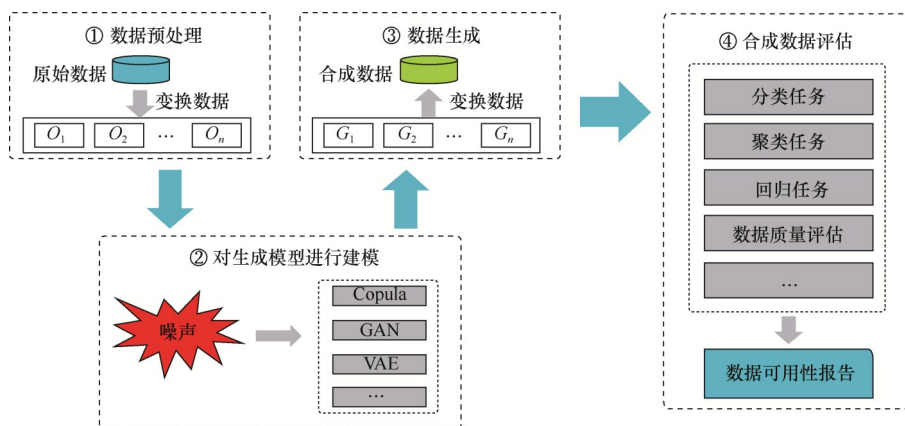


图1 金融数据合成的基本步骤

Figure 1 Basic steps in financial data synthesis

短期内, 各类波动性指标呈现正自相关性。这表明高波动性事件具有一定的聚集倾向。换言之, 较大的价格波动往往与显著的波动相关, 而较小的价格波动则与较为微弱的波动变化相关。④收益/损失不对称: 如股价和指数价值的大幅下跌不会伴随着同样大幅度的上涨。⑤聚合高斯性: 在更大的时间尺度上, 回报的分布是正态分布的。

## 1.2 金融领域的模型

金融时间序列建模有以下两种常见方法。

①ARCH/GARCH (autoregressive conditional heteroskedasticity/generalized autoregressive conditional heteroskedasticity) 模型<sup>[8]</sup>。这类模型基于经典的统计方法来实现, 通过将当前误差项的方差描述为过去误差的函数, 对时间序列中随时间变化的方差进行建模。通常来说, 方差与先前的“新息”, 即 innovation 的平方相关。该模型能准确地模拟时间序列变量的波动性变化, 但其预测严重依赖于过去的信息。因此, 这类模型几乎没有随机成分, 完全取决于以前的值。②基于个体模型 (agent-based model, ABM) <sup>[9]</sup>。该类模型是用来模拟具有自主意识的智能体 (独立个体或共同体, 如组织、团队) 的行动和相互作用的计算模型。用 ABM 模拟多个代理交互作用, 以重新创建和预测复杂现象的行为, 从而达到从较低级别代理的交互中生成较高级别的属性的目标。

金融时间序列的建模是一个巨大的挑战, 因为金融市场的动态本质上非常复杂, 生成数据的机制以及数据的原始分布也是未知的。使用纯数

据驱动的建模方法, 可以消除建模中的偏差来源, 如深度学习方法和生成式对抗网络 (generative adversarial network, GAN)。GAN 可以提供良好的结果, 因为它们仅从真实数据中采样来生成数据, 不需要额外的假设或输入。避免假设是这类建模一个非常重要的方面, 因为在金融数据方面, 避免可能的人为偏见渗透到建模过程中是这一研究领域的要点。

## 1.3 其他生成模型

其他生成模型都是基于似然的方法 (likelihood-based method), 即对于给定的一个数据集  $\{x_1, x_2, \dots, x_N\}$  服从某分布  $p(x)$ , 目标是训练一个生成器去近似该分布。最后通过从该近似分布中采样, 以获取生成数据  $x'$ 。以下 3 种生成模型都是遵循该方法的模型。

### 1.3.1 变分自动编码器

变分自动编码器 (variational auto encoder, VAE) 是生成模型的一种, VAE 的基本架构如图 2 所示。这类模型的主要目标是从对象的学习分布中生成新的采样数据。VAE 由 Kingma 等<sup>[10]</sup>提出, 可以从隐变量空间的概率分布中学习潜在属性并构造新的元素。VAE 的思想用于变分贝叶斯和图模型方法。

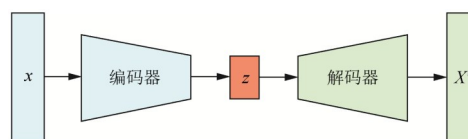


图2 VAE 的基本架构

Figure 1 The basic architecture of VAE

标准的自动编码器 (auto encoder, AE) 包括 2 个相似的神经网络, 即一个编码器和一个解码器。编码器接收输入并将其转换为维度更小的表示形式, 解码器可以使用该表示形式将其转换为原始输入。它们将输入转换到的潜在空间以及它们的编码向量所在的空间, 可能不是连续的。为解决这个问题, 变分自动编码器具备连续的潜在空间特性, 从而使随机采样和插值操作变得更加便捷。

VAE 可以处理各种类型的数据 (序列的和非序列的, 连续的或离散的, 甚至有标签的或无标签的), 这使其成为强大的生成工具。然而, 最原始的 VAE 模型的生成数据质量比较糟糕, 经过后续的改进, 目前最先进的 VAE 有不错的效果。IntroVAE (introspective variational autoencoder) [11] 将 VAE 与 GAN 相结合, 提升了效果; IAF-VAE (improving variational inference with inverse autoregressive flow) [12] 将 VAE 与基于流的模型相结合; VQ-VAE (vector quantised-variational autoencoder) [13] 引入了离散的因变量, 再使用 PixelRNN (pixel recurrent neural network) [14] 来建模对应的先验分布; NVAE (nouveau variational autoencoder) [15] 则包含了多尺度架构、可分离卷积、Swish 激活函数、Flow 模型等多个 CV (computer vision) 领域的成果。

### 1.3.2 基于流的生成模型

基于流的模型 (flow-based model) [16] 与其他生成模型不同, 该模型不使用近似的方法去逼近真实分布, 而是直接计算概率分布。

流模型  $f$  是由一系列的可逆函数  $f(x) = f_1 \cdots f_L(x)$ , 以及每个  $f_i$  的逆和雅可比矩阵行列式组成的, 如图 3 所示。

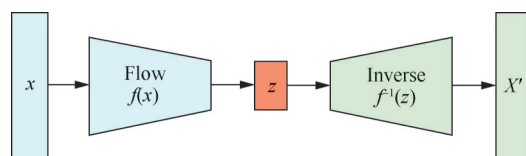


图3 基于流的模型的基本架构  
Figure 3 The basic architecture of flow-based model

基于流的模型有两大类: 标准化流模型和试图增强基本模型性能的自回归流的模型。前者有诸如 RealNVP [17] 以及 Glow [18] 模型, 提供了鲁棒的分布近似。它们通过应用一系列可逆变换函数

将简单的分布转化为复杂的分布, 根据变量变换定理, 可以反复地用新变量替换原变量, 得到最终目标变量的概率分布。后者有用于图像生成的 PixelCNN [14] 和用于音频信号生成的 WaveNet [19]。它们皆由大量因果卷积组成, 即在特定时间戳的预测只使用过去观察到的数据, 因为卷积运算要考虑顺序。具体而言, PixelCNN 中的因果卷积由一个带掩码的积核执行, WaveNet 则将输出通过几个时间戳转移到未来时间。

### 1.3.3 扩散模型

扩散模型 (diffusion model) [20] 是受非平衡热力学启发的模型, 也是目前讨论度最高的生成模型。该模型定义马尔可夫链, 逐渐向数据添加随机噪声, 然后学习逆扩散过程, 从噪声中构建所需的数据样本, 如图 4 所示。与 VAE 或基于流的模型不同, 扩散模型是用固定的程序学习的, 而且隐变量具有高维度 (与原始数据相同)。

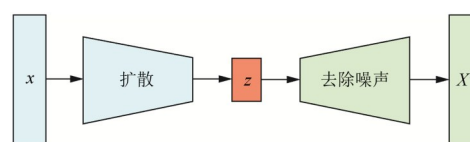


图4 扩散模型的基本架构  
Figure 4 The basic architecture of diffusion model

扩散模型主要用于生成图像, 其生成过程大致分为 3 步。①前向。该阶段在原始图像上逐步增加噪声, 第  $t$  步获得的图像只与第  $t-1$  步获得的图像相关, 直到第  $T$  步时图像变成纯高斯噪声。②逆向。逆向阶段是不断去除噪声的过程, 直至最终还原原始图像。③从噪声中生成随机图像。该模型训练完成后, 只要给定高斯随机噪声, 就可以生成一张从未见过的图像。

以上 3 种生成模型最初都是应用于 CV 领域的模型, 后续迁移至 NLP (natural language processing) 领域。然而, 无论图像数据和文本数据的结构有多复杂, 终究可以归类为简单的矩阵或者序列, 以上 3 种模型都非常适合处理这些“均质” (数据类型一致) 的数据, 因此有良好的生成效果。而金融领域中常见的表格数据的列与列之间的数据类型可以是不同的 (离散或连续), 故将以上模型迁移至该领域的研究较少。

生成式对抗网络虽然起源于图像生成领域,

但结构的灵活性使其可以在各个领域都发挥作用,接下来将具体介绍其架构以及它在金融领域的应用。

## 2 生成式对抗网络

生成性对抗网络最初是由 Goodfellow 等<sup>[21]</sup>提出的。由于其简单和有效性,该模型获得了很多关注。GAN 在初始的应用领域(图像生成)取得了相当大的进展,随后各领域的研究人员创建了数百种不同类型的 GAN,以优化各种任务,从计算机视觉到银行欺诈检测。从生成手写数字图像开始,截至 2021 年,GAN 已经可以使用 StyleGAN<sup>[22]</sup>生成近乎完美的人脸,并且具有不断扩展的应用。

### 2.1 生成式对抗网络的架构

#### 2.1.1 GAN 的基本架构

原始 GAN 框架是以随机噪声为输入并生成输出的无监督模型,通过对抗来形成生成的两个模型(通常是神经网络),并且并行地训练。第一个模型是生成模型,即生成器(G),它捕获数据分布并生成新数据。第二个模型是分类器,即鉴别器(D),它估计样本来自训练数据而不是来自生成器的概率。生成器的训练过程是最大化其输出被鉴别器错误分类的概率;鉴别器的训练过程是尽可能正确分类,即最小化错误分类的概率。GAN 的基本架构如图 5 所示。

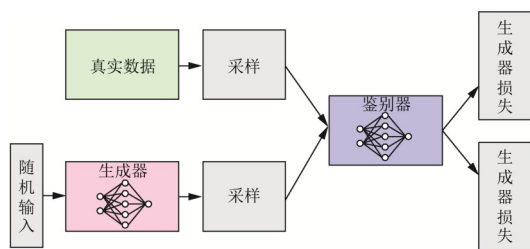


图5 GAN 的基本架构

Figure 5 Basic architecture of GAN

#### 2.1.2 损失函数

GAN 训练过程使用损失函数来测量生成数据和真实数据的分布之间的距离,以评估它们的相似性。在最初的 GAN 中,引入了最小最大损失:

$$\min_G \max_D V(D, G) = \mathbb{E}_{x \sim P_{\text{data}}(x)} [\log D(x)] + \mathbb{E}_{z \sim p(z)} [\log (1 - D(G(z)))] \quad (1)$$

其中,  $D(x)$  是鉴别器对真实数据实例  $x$  为真实的

概率的估计;  $\mathbb{E}_{x \sim P_{\text{data}}(x)}$  是所有真实数据实例的预期值,  $x$  表示真实的数据;  $G(z)$  是给定噪声  $z$  时生成器的输出;  $D(G(z))$  是鉴别器对假实例为真的概率的估计;  $\mathbb{E}_{z \sim p(z)}$  是生成器所有随机输入的预期值(即所有生成的伪实例  $G(z)$  的预期值)。

当鉴别器是最优时,通过 JS (jensen shannon) 散度从真实分布和生成分布之间的交叉熵导出最小最大损失的公式。对于生成器,最小化损失等于最小化  $\log(1 - D(G(z)))$ , 因为它不会直接影响函数中  $\log(D(x))$  的项。用 JS 散度量两个概率分布之间的相似性。

#### 2.1.3 训练过程

生成器和鉴别器网络分别通过不同的交替过程进行训练。

1) 生成器: 来自随机噪声  $z$  的样本  $\rightarrow$  在  $G$  中产生新样本  $\rightarrow D$  将样本分类为“真实”或“伪”  $\rightarrow$  根据  $D$  分类计算损失  $\rightarrow$  通过鉴别器和生成器反向传播以获得梯度  $\rightarrow$  用于更改  $G$  权重的梯度。

2) 鉴别器:  $D$  对真实数据和  $G$  生成的数据进行分类  $\rightarrow$  鉴别器损失惩罚  $G$  对真实和伪实例进行错误分类  $\rightarrow D$  从鉴别器损失中反向传播来更新其权重。

3) 理想收敛情况: 在最佳情况下,当鉴别器和生成器以相同的速度提升性能时,生成器将最终生成与从真实数据中抽取的样本无法区分的数据,即鉴别器对所有的输入都只能输出 50% 的真实概率。GAN 的理论训练过程<sup>[21]</sup>如图 6 所示,随着生成分布(绿线)接近真实数据分布,鉴别分布(蓝色虚线)将无法区分它们,并稳定在  $D(x)=0.5$ 。

#### 2.1.4 挑战

##### (1) GAN 模型训练困难

GAN 虽然能够生成非常精确的合成样本,但 GAN 模型很难训练<sup>[23]</sup>。模式崩溃是由于训练不足而发生的 GAN 故障模式,当生成器将多个噪声输入值映射到同一输出区域时,或者当生成器忽略目标数据分布的某个区域时,可能会发生这种情况。这意味着,如果生成器陷入样本的局部最小值,鉴别器将最终学会区分生成器生成的“假货”,从而结束学习过程,并导致不可逆的输

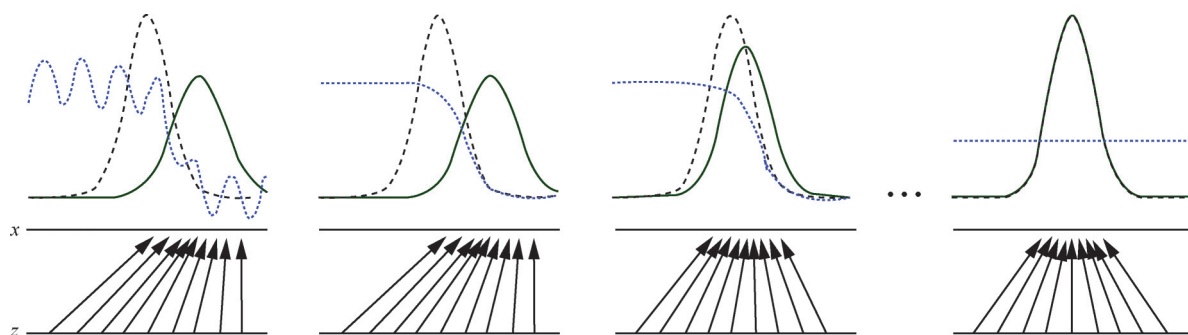


图6 GAN的理论训练过程

Figure 6 Theoretical training process of GAN

出。这是一个很难解决的问题，因为在生成建模中，目标不仅是创建看起来逼真的样本，而且是能够生成更广泛的样本。后续的研究对原始模型进行修改来缓解这类问题。

### (2) 缺乏适当的评估指标

GAN面临的另一个挑战是如何评估其训练精度，目前常用的评估指标有如下几种。

1) 可视化评估指标。生成数据的可视化表示（如数据分布图、相关矩阵）是评估生成器性能的有效方法。可以用分布、累积和和列相关性来进行可视化评估。基于此，尽管它没有揭示任何隐藏的关系，但人类可以很直观地验证结果，并识别真实数据和合成数据之间的相似度。此外，结果的可视化分析提供了定量指标无法涵盖的信息。

2) 统计测试评估指标。由于GAN最初是围绕图像生成开发的，最常用的统计量是Fréchet起始距离（fréchet inception distance, FID）。FID基于Fréchet距离，是一种比较两个多变量正态分布（均值和协方差矩阵）统计数据的度量，以量化分布之间的距离。

3) 基于机器学习的评估指标。使用机器学习

模型来区分生成数据与真实数据。基本方法为，首先给每个数据记录打标签，分为真实的还是生成的；然后对带有标签的数据进行洗牌，并对机器学习模型进行交叉验证，试图预测标签。机器学习效能度量可以同时应对分类问题和回归问题，以评估生成数据是否可以替代真实数据。在分类问题的情况下，可以使用决策树<sup>[24]</sup>、AdaBoost<sup>[25]</sup>或MLP分类器，同时根据准确度和F1分数评估这些模型的性能。对于回归任务，线性回归或MLP回归可以用作机器学习模型，用 $R^2$ 的值进行评估。不同模型的平均性能可以用作评估的度量，从而评估生成数据是否可以替代真实数据。

然而，上述的大多数方法是由图像领域迁移而来的，对于金融表格数据或者时间序列数据仍缺少普式的、权威的评判指标。

## 3 生成式对抗网络在金融方面的应用

生成式对抗网络在诸多领域中取得显著的效果，GAN的应用领域及相关模型如表1所示。

GAN在金融领域中的应用主要集中于金融表格数据的合成以及金融时间序列，GAN在金融领域的应用如表2所示。

表1 GAN在不同领域的应用

Table 1 Applications of GAN in different fields

| 领域       | 方法                                                                                                                                                                                                         |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 图像       | BicycleGAN <sup>[26]</sup> 、Coupled GAN <sup>[27]</sup> 、CycleGAN <sup>[28]</sup> 、InfoGAN <sup>[29]</sup> 、Pix2Pix <sup>[30]</sup> 、Super-Resolution GAN <sup>[31]</sup> ...                              |
| 表格数据     | TableGAN <sup>[32]</sup> 、TGAN <sup>[33]</sup> 、CTGAN <sup>[34]</sup> 、CopulaGAN <sup>[35]</sup> 、TabFairGAN <sup>[36]</sup> 、CTAB-GAN <sup>[37]</sup> 、CTAB-GAN+ <sup>[38]</sup> ...                      |
| 图(graph) | NetGAN <sup>[39]</sup> 、Misc-GAN <sup>[40]</sup> 、MolGAN <sup>[41]</sup> ...                                                                                                                               |
| 时间序列     | TimeGAN <sup>[42]</sup> 、WGAN-GP <sup>[43]</sup> 、FIN-GAN <sup>[6]</sup> 、Quant GAN <sup>[44]</sup> 、RA-GAN <sup>[45]</sup> 、CDRAGAN <sup>[46]</sup> 、SigCWGAN <sup>[47]</sup> 、ST-GAN <sup>[48]</sup> ... |
| 轨迹       | Social GAN <sup>[49]</sup> ...                                                                                                                                                                             |

表 2 GAN 在金融领域的应用

Table 2 Applications of GAN in the financial sector

| 领域     | 应用            | 方法                                                                                                                                                                                                     |
|--------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 表格数据生成 | 合成金融表格数据      | TableGAN <sup>[32]</sup> 、TGAN <sup>[33]</sup> 、CTGAN <sup>[34]</sup> 、CopulaGAN <sup>[35]</sup> 、TabFairGAN <sup>[36]</sup> 、CTAB-GAN <sup>[37]</sup> 、CTAB-GAN+ <sup>[38]</sup>                      |
| 时间序列预测 | 市场预测          | GAN-FD <sup>[50]</sup> 、ST-GAN <sup>[48]</sup> 、MTSGAN <sup>[51]</sup>                                                                                                                                 |
|        | 交易模型调整        | C-GAN <sup>[52]</sup> 、MAS-GAN <sup>[53]</sup>                                                                                                                                                         |
| 投资组合管理 | 投资组合优化        | PAGAN <sup>[54]</sup> 、GAN-MP <sup>[55]</sup> 、DAT-CGAN <sup>[56]</sup> 、CorrGAN <sup>[57]</sup>                                                                                                       |
| 时间序列生成 | 时间序列生成和财务数据扩充 | TimeGAN <sup>[42]</sup> 、WGAN-GP <sup>[43]</sup> 、FIN-GAN <sup>[6]</sup> 、Quant GAN <sup>[44]</sup> 、RA-GAN <sup>[45]</sup> 、CDRAGAN <sup>[46]</sup> 、SigCWGAN <sup>[47]</sup> 、ST-GAN <sup>[48]</sup> |
| 欺诈检测   | 市场操纵检测        | LSTM-GAN <sup>[58]</sup>                                                                                                                                                                               |
|        | 信用卡欺诈检测       | RWGAN <sup>[59]</sup> 、LSTM-GAN-2 <sup>[60]</sup>                                                                                                                                                      |

### 3.1 生成式对抗网络用于合成金融表格数据

GAN 经常被用来生成表格数据<sup>[61]</sup>。常用于生成表格数据的方法有 MedGAN<sup>[62]</sup>、TableGAN<sup>[32]</sup>、TGAN<sup>[33]</sup>、CTGAN<sup>[34]</sup>、CopulaGAN<sup>[35]</sup>、TabFairGAN<sup>[36]</sup>、CTAB-GAN<sup>[37]</sup>、CTAB-GAN+<sup>[38]</sup>等。其中，MedGAN 是专门针对医疗数据设计的模型，不在本文中过多讨论。其余模型皆为普式模型，在生成金融表格数据都有不错的表现，并且引用了 CTAB-GAN+ 文献中的实验结果阐述了这些模型的优劣。

#### 3.1.1 TableGAN

TableGAN<sup>[32]</sup>是最早一批用于合成表格数据的生成式对抗网络模型。TableGAN 的鉴别器和生成器均为卷积神经网络。如图 7 所示，TableGAN 的架构基于深度卷积生成式对抗网络 (deep convolution generative adversarial network, DCGAN)<sup>[63]</sup>，这是用于图像合成的模型之一，该模型的主要创新点在于除了尽可能提高合成数据与真实数据在统计特征上的相似性，重点考虑

了隐私保护问题，防止信息泄露。

TableGAN 特殊的架构组件是分类器 (C) 参与训练过程，旨在提高生成记录的语义完整性。分类器的架构与鉴别器相同，但是根据真实表格的基本标签进行训练。分类器学习真实标签与表格特征之间的相关性，并预测合成数据的标签。因此，分类器用于指导生成器判断生成的记录是否在语义上正确。

#### 3.1.2 CTGAN

CTGAN (conditional generative adversarial network)<sup>[34]</sup>是 Xu 等提出的针对表格数据而设计的生成式对抗网络模型，是该作者团队先前提出的 TGAN (generative adversarial network)<sup>[33]</sup>模型的升级版，专注于生成具有混合变量类型 (离散和连续) 的表格数据。

表格数据的不同列中通常包含离散数据和连续数据，该模型先将这两种数据进行归一化，离散数据可以直接被转换成独热向量；而运用变分高斯混合模型 (variational gaussian mixture

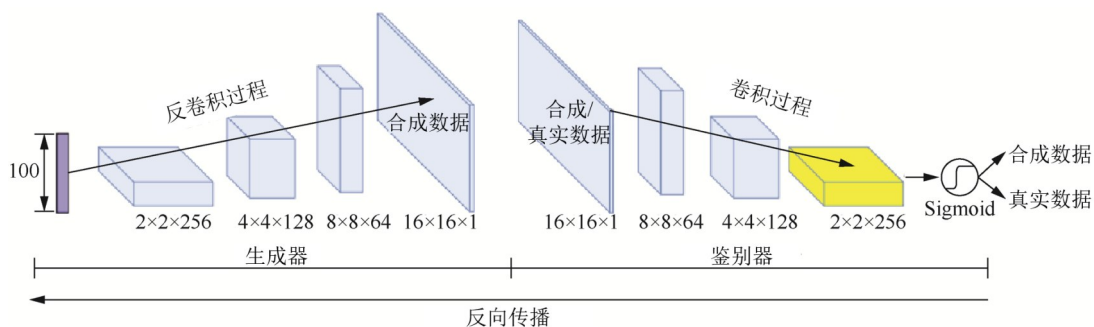


图 7 TableGAN 的架构

Figure 7 The architecture of TableGAN

model, VGM) 将分布复杂的连续数据归一化为由独热向量和标量组合而成的向量, 使用变分高斯混合模型进行归一化<sup>[34]</sup>如图8所示。经过如上处理后, 一行数据中无论离散还是连续都可以用向量表示, 将组合起来的“大向量”作为生成式对抗网络中的真实数据, 从而进行训练。

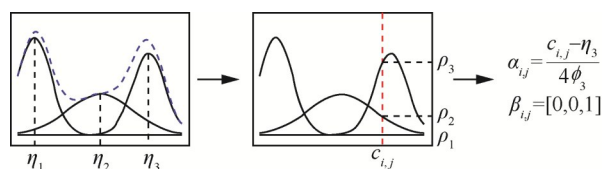


图8 使用变分高斯混合模型进行归一化

Figure 8 Normalisation using a variational Gaussian mixture model

CTGAN使用条件向量辅助鉴别器, 以防止模型出现模式崩溃的问题, CTGAN中的条件向量如图9所示<sup>[34]</sup>。

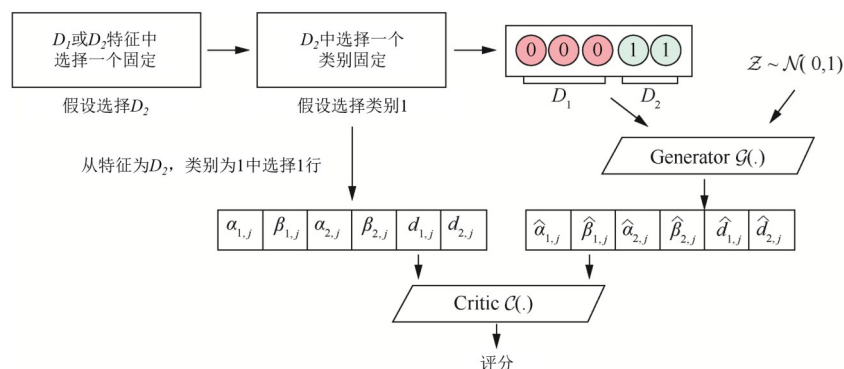


图9 CTGAN中的条件向量

Figure 9 Conditional vectors in CTGAN

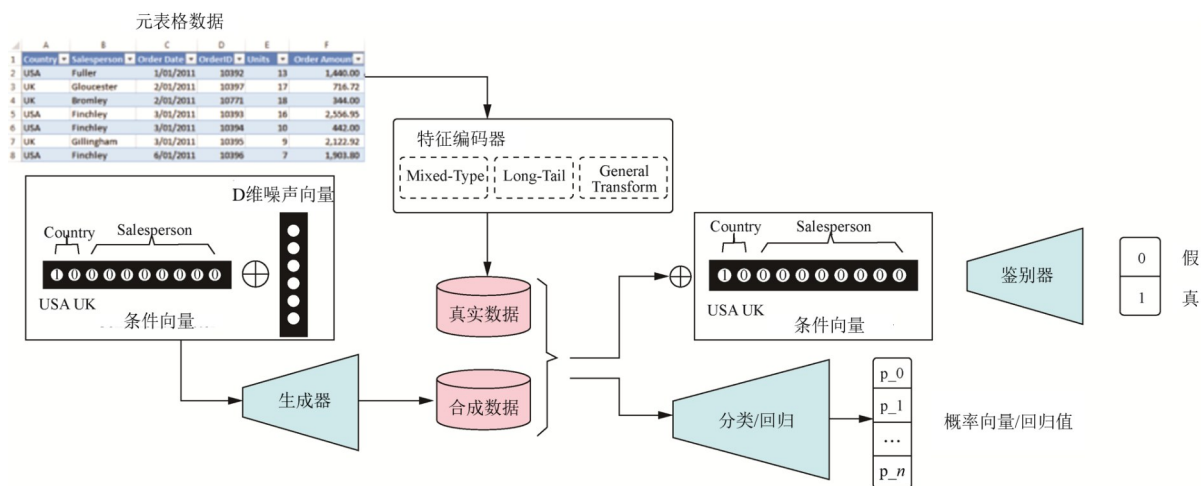


图10 CTAB-GAN+模型

Figure 10 CTAB-GAN+ model

在金融领域中, CTGAN可以很好地应用于合成企业的表格数据, 这类数据集往往存在大量的缺失值, 并且由于数据量的不足很难进行进一步的研究。借助CTGAN可以先对数据集进行扩充, 生成大量没有隐私问题且符合真实数据分布的合成数据, 以推进下一步的研究。

### 3.1.3 CTAB-GAN+

为解决数据共享问题, 用生成式对抗网络生成合成数据的技术越发成熟, 合成数据越发接近真实数据, 反而增加了泄露隐私的风险。差分隐私(differential privacy, DP)为隐私损失提供理论保证, 但降低了数据效用。找到最佳权衡仍然是充满挑战的研究问题。Zhao等<sup>[38]</sup>提出的CTAB-GAN+模型是基于CTAB-GAN<sup>[37]</sup>模型的改进版, 也是目前在表格数据合成方面性能较好的模型之一, 具体模型如图10所示。

CTAB-GAN+在 CTAB-GAN 基础上进行了改进, 具体如下。①在条件 GAN 中添加下游损失, 以便在分类和回归领域获得更高效用的合成数据。②使用带梯度惩罚的 Wasserstein 损失以实现更好的训练收敛。③引入针对连续-分类混合变量以及不平衡或偏斜数据的变量的新颖编码器。④使用 DP 随机梯度下降进行训练, 以施加严格的隐私保证。⑤对厚尾分布的数据进行特殊处理 (在金融数据中很常见), 使变分高斯混合模型可以更好地对数据进行编码。

如图 11 所示, CTAB-GAN+对厚尾分布数据合成效果超越先前模型<sup>[38]</sup>。文献[38]对 CTAB-GAN+在数据相似性和分析效用方面进行广泛评估, 与用于生成表格数据的 GAN 进行了比较, 结果表明, CTAB-GAN+能够在多个应用场景中合成更真实的数据。

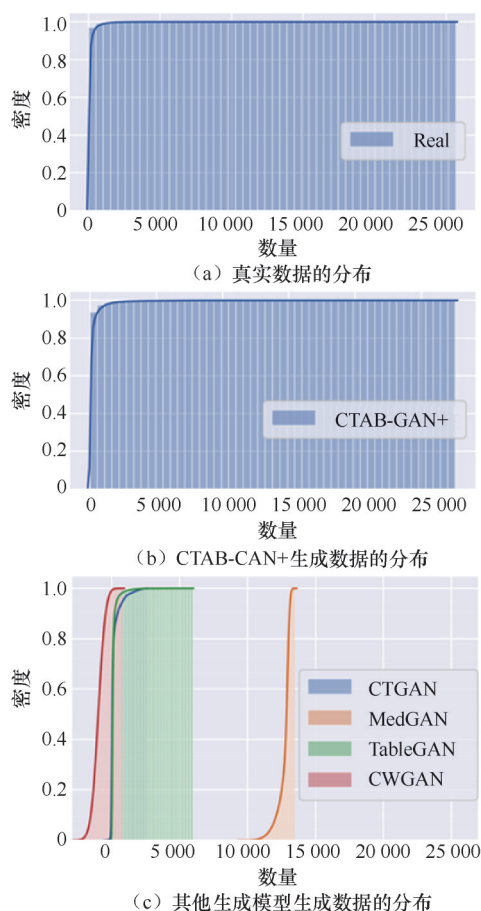


图 11 CTAB-GAN+与先前模型对厚尾分布数据的合成效果  
Figure 11 Effectiveness of CTAB-GAN+ versus previous models for synthesizing thick-tailed distribution data

### 3.1.4 用于生成表格数据的生成式对抗网络性能评估

本节从机器学习效用和统计相似性两个维度进行性能评估。这些度量标准用于衡量合成数据是否可以作为原始数据的良好替代。

#### (1) 机器学习效用

分类任务和回归任务的机器学习效用量化方法不同。对于分类任务, 本文通过 5 种广泛使用的机器学习算法 (决策树分类器、线性支持向量机 SVM、随机森林分类器、多项式逻辑回归和 MLP) 在真实数据与合成数据上的性能, 即准确性 (accuracy),  $F1$ -分数 ( $F1$ -score) 和 AUC (area under curve) 来量化机器学习效用; 对于回归任务, 使用 4 种常见的回归算法 (线性回归、岭回归、Lasso 回归和贝叶斯岭回归) 和 3 个回归度量, 即平均绝对百分比误差 (mean absolute percentage error, MAPE)、解释方差得分 (explained variance score, EVS) 和  $R^2$  得分来量化机器学习效用。

#### (2) 统计相似性

使用 3 个度量标准, 即 Jensen-Shannon 散度、Wasserstein 距离和差异化相关性来量化真实数据和合成数据之间的统计相似性。

图 12 显示了分类任务的机器学习效用评估过程。表 3 和表 4 为 4 种主要的用于合成表格数据的 GAN 模型在 7 个数据集上的表现<sup>[37-38]</sup>。其中, 原始数据和合成数据分类的机器学习效用之差和统计相似度之差如表 3 所示, 原始数据和合成数据回归的机器学习效用之差和统计相似度之差如表 4 所示, 其中所有性能指标皆为数值越接近 0, 则模型性能越优。

在合成表格数据方面, 性能最好的生成对抗网络模型是 CTAB-GAN+模型, 无论在分类任务还是回归任务上, 其机器学习效用和统计相似性都是最好的, 并且该模型对金融数据中的特征事实 (如厚尾分布) 的合成效果相比其他模型有很大的提升, 如图 12、表 3<sup>[38]</sup>和表 4 所示。

## 3.2 生成式对抗网络用于时间序列预测

### 3.2.1 GAN-FD

股票价格预测是金融界的重要问题, 因为它有助于制定有效的股票交易策略。在 GAN-FD<sup>[50]</sup>

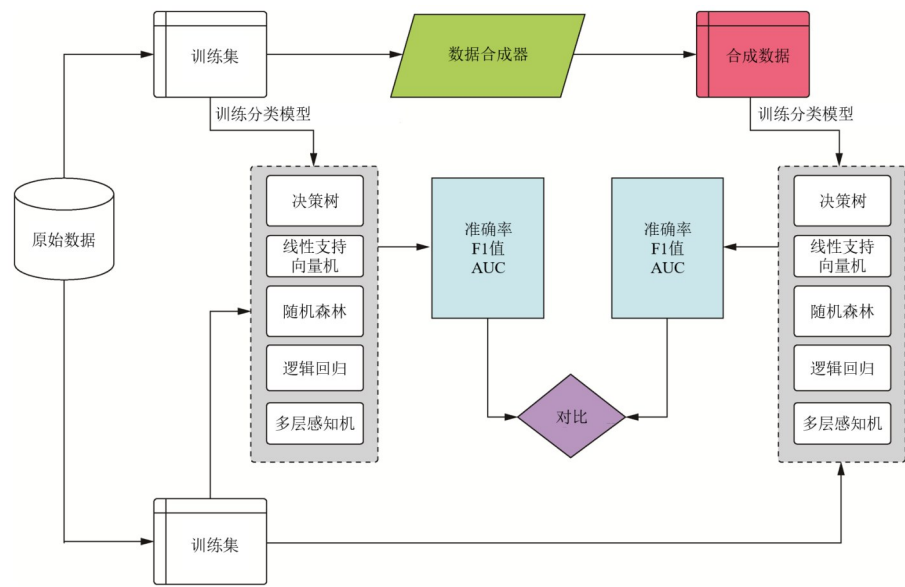


图 12 分类的机器学习效用评估流程

Figure 12 Evaluation flows for ML utility of classification task

表 3 原始数据和合成数据分类的机器学习效用和统计相似度之差（在 5 个数据集上取平均值）

Table 3 Difference of ML utility and statistical similarity for classification between original and synthetic data (averaged on five datasets)

| 模型        | 机器学习效用之差 |       |       | 统计相似度之差 |        |            |
|-----------|----------|-------|-------|---------|--------|------------|
|           | Accuracy | F1-分数 | AUC   | Avg JSD | Avg WD | Diff. Corr |
| CTAB-GAN+ | 5.23%    | 0.090 | 0.041 | 0.039   | 484    | 2.03       |
| CTAB-GAN  | 8.90%    | 0.107 | 0.094 | 0.062   | 1197   | 2.09       |
| CTGAN     | 21.51%   | 0.274 | 0.253 | 0.070   | 1769   | 2.73       |
| TableGAN  | 11.40%   | 0.130 | 0.169 | 0.080   | 2117   | 2.30       |

表 4 原始数据和合成数据回归的机器学习效用和统计相似度之差（在 2 个数据集上取平均值）

Table 4 Difference of ML utility and statistical similarity for regression between original and synthetic data (averaged on two datasets)

| 模型        | 机器学习效用之差 |      |                | 统计相似度之差 |        |             |
|-----------|----------|------|----------------|---------|--------|-------------|
|           | MAPE     | EVS  | R <sup>2</sup> | Avg JSD | Avg WD | Diff. Corr. |
| CTAB-GAN+ | 0.04     | 0.03 | 0.04           | 0.040   | 856    | 0.65        |
| CTAB-GAN  | 0.06     | 0.05 | 0.06           | 0.119   | 3396   | 1.23        |
| CTGAN     | 0.87     | 0.59 | 0.71           | 0.139   | 3030   | 2.60        |
| TableGAN  | 0.34     | 0.43 | 0.48           | 0.317   | 2366   | 2.26        |

中，提出了一种通用框架，该框架采用长短期记忆（long short-term memory，LSTM）<sup>[64]</sup>和卷积神经网络（convolutional neural networks，CNN）进行对抗性训练来预测高频股市交易。该模型以交易软件提供的公开可用指数为输入，避免了复

杂的金融理论研究和困难的技术分析，为非金融专业的普通交易者提供了便利。该研究模拟了实际交易者的交易模式，并使用滚动分区训练集和测试集的方法来分析模型更新周期对预测性能的影响。大量实验结果表明，GAN-FD可以有效提

高股价方向预测的准确性，减少预测误差。

### 3.2.2 MAS-GAN

MAS-GAN (multi-agent simulations GAN)<sup>[53]</sup>是由摩根大通人工智能研究团队提出的，是一种多智能体市场模拟器校准的模型。它使用GAN的鉴别器来校准使用基于个体模型构建的市场模拟器，首先使用鉴别器学习校准目标，然后使用学习的校准目标来模拟参数优化。这是首个使用GAN训练的鉴别器作为多智能体系统优化的目标函数的模型。

这项工作建立在架构变体SAGAN<sup>[65]</sup>的基础上，为卷积GAN引入了自注意力层。使用卷积神经网络以及自注意力机制旨在通过使用自然语言处理研究领域的注意机制，在效率和长程依赖性之间建立平衡。自注意力机制如图13所示<sup>[65]</sup>，自注意力层中，特征图通过3个 $1 \times 1$ 卷积（query、key和value）来创建概率向量，以决定向下一层暴露Value的个数。该层与常规卷积互补，有助于网络从输入的特征中捕获更细粒度的特征。

### 3.2.3 cGAN

cGAN (conditional GAN)<sup>[52]</sup>由Koshiyama于2019年应用于金融行业。原始的GAN模型不要求假设的数据分布，是完全无监督模型，一方面让其有极高的自由度，理论上完全逼近真实数据；另一方面在处理较复杂的实际任务时有极强的不可控性，由此诞生了cGAN。该模型在结构上被扩展为条件模型，其中生成器和鉴别器以一

些额外的辅助信息 $y$ 为条件。这种辅助信息 $y$ 可以采取类标签或其他数据的形式，作为额外的输入层被送入生成器和鉴别器。增加的独热编码标签的输入层指导生成器产生特定的输出。

cGAN的结构如图14所示<sup>[52]</sup>，与最初的GAN一样，鉴别器和生成器网络是MLP，其中生成器输出层的激活是线性函数，鉴别器输出层的激活是sigmoid函数。损失函数对生成器和鉴别器都有一个附加的条件元素，它们都通过随机梯度下降进行优化。

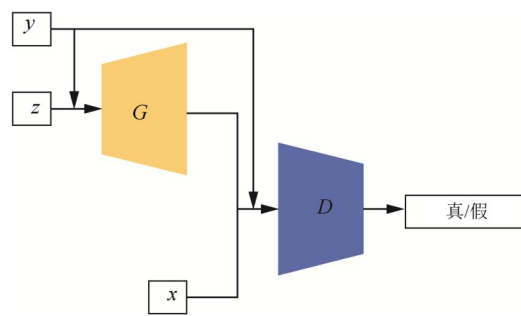


图 14 cGAN 的结构

Figure 14 The structure of cGAN

金融中的条件信息，增加的辅助信息 $y$ 可以代表当前或预期的市场状况，适合于对时间序列等连续数据进行建模。它还可以构建“what-if”情景，通常用于压力测试和其他基于情景的模型。已实施的cGAN显示了一些改进交易策略的新工具，特别是用于寻找交易算法的最佳超参数（微调），以及交易策略的组合，其中交易模型在

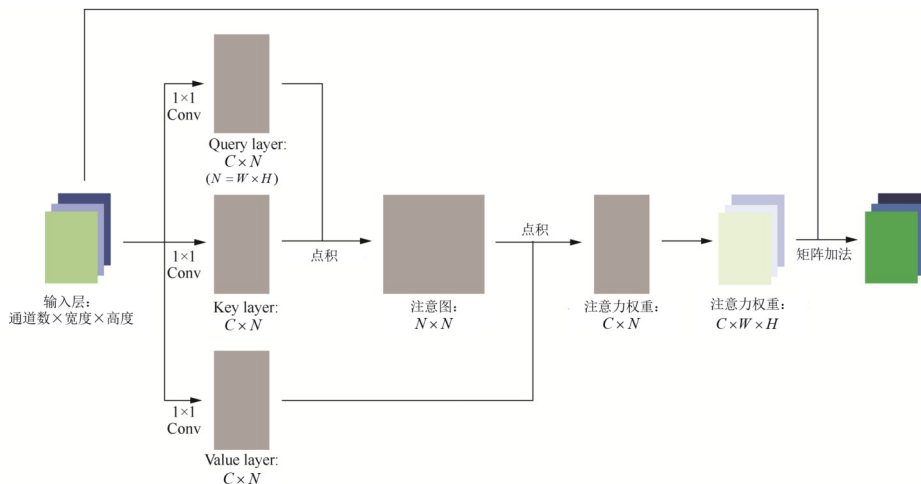


图 13 自注意力机制

Figure 13 Self-attention module

cGAN产生的样本上进行训练，并将其输出合并以获得最终结果。在金融表格数据生成方面，前文提及的CTGAN<sup>[34]</sup>同样借助条件信息辅助鉴别器，以防止模型出现模式崩溃的问题。

与经典的引导法（重采样）相比，cGAN可以产生更多样化的训练和测试集，还有针对压力事件的抽样能力，以及为数据集增加一层匿名性，这在其他重采样技术上是无法实现的。

### 3.3 生成式对抗网络用于投资组合管理

投资组合管理指的是对投资者的风险承受能力、投资目标和时间范围等限制条件下，通过组合多种资产来实现资产配置的最优化，旨在平衡风险和收益之间找到最佳的平衡点。

#### 3.3.1 CorrGAN

CorrGAN<sup>[57]</sup>是用于生成对资产收益进行估计的经验性相关矩阵的模型。该模型是基于DCGAN架构的，DCGAN<sup>[63]</sup>的生成器结构如图15所示。该模型是第一个在生成器中应用卷积神经网络的GAN。与原来的GAN相比，DCGAN的架构有一些关键性的变化，这使更高的分辨率建模和稳定的训练成为可能。它还引入了对自然图像中表征层次的学习。反卷积也被称为转置卷积，它们通过交换卷积的前向和后向通道工作。DCGAN有以下几个重要的架构设计。①DCGAN架构用分层卷积代替了鉴别器的池层，用分层卷积代替了生成器的池层。②鉴别器和生成器中的批量归一化，改善了以零为中心的真实样本的生成位置。③生成器的所有层都使用ReLU激活，只有输出层使用Tanh，而鉴别器的所有层都使用

LeakyReLU激活。LeakyReLU激活可以有效防止网络在生成器从鉴别器接收梯度时不再变化。

在实际金融应用中，CorrGAN框架可以用于优化交易策略、风险评估以及投资组合压力测试。具体地，研究人员在不同宏观经济情境下，利用该模型调整市场制度变量以提升蒙特卡洛回测和投资组合压力测试的效果。与此同时，相关研究人员创建了一个网站，以测试人们能否区分真实数据和合成数据的相关矩阵。结果显示，它们在肉眼下是难以被区分的。

### 3.4 生成式对抗网络用于时间序列生成

#### 3.4.1 WGAN-GP

WGAN<sup>[66-67]</sup>（Wasserstein GAN）提出了一个新的损失函数，使用Wasserstein距离作为原始GAN损失函数的替代，它是基于KL和JS距离的。Wasserstein距离是用来度量两个概率分布之间距离的方法，它表示通过逐步（离散）增量将一个概率分布重塑为另一个概率分布的最小能量损失，即将一个概率分布“搬移”到另一个概率分布所需的最小“代价”，因此，也被称为Earth Mover距离。

这一修改解决了二分类交叉熵损失在GAN中发生的梯度消失和模式崩溃的问题。通常情况下，当鉴别器性能比生成器提高得更快时，就会输出更多的极端值，给生成器的反馈意义不大，从而停止学习过程。而在使用W-Loss函数时，鉴别器被批判器所取代，其中批判器用线性激活函数取代了sigmoid激活函数，输出不会被限制在0和1之间，无论分布相差多远，损失函数都

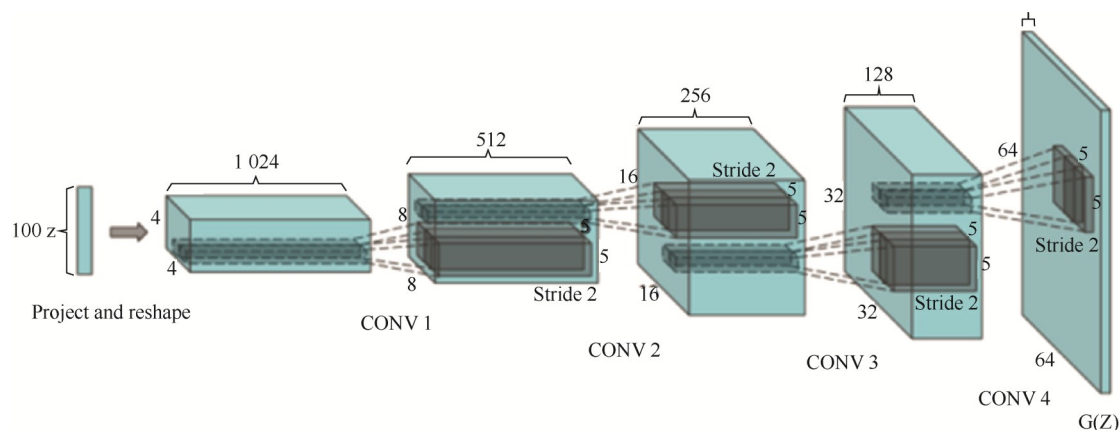


图15 DCGAN的生成器结构  
Figure 15 Generator Structure of DCGAN

会继续增长。这样,梯度不会过于接近零,使 GAN 不容易出现梯度消失问题,从而导致模式崩溃。

然而,当使用 W-Loss 函数时,批判器的神经网络需要 1-Lipschitz 连续。这个条件保证了 W-Loss 函数是连续的(可微分的),并且在训练过程中它的增长是稳定的,这使基础的 Earth Mover 距离有效。为了达成这个条件, WGAN 使用了权重剪裁,即强制批判器的权重在一个固定的区间内取值。在梯度下降过程中更新权重后,任何超出所需区间的权重都会被截断,因此过高或过低的值都被设置为某个固定的最大值。迫使权重在一个有限的值范围内,可能会限制批判器的学习能力,并最终限制 GAN 的表现。因此需要大量的超参数调整来调整训练的模型。WGAN-GP<sup>[67]</sup>对该问题进行了优化,引入了另一种执行 1-Lipschitz 连续性的方法,即在损失函数中加入了一个正则化项,当其梯度规范高于 1 时,对判别器进行惩罚。

文献[43]将 WGAN-GP 应用于金融领域。针对一维情况,带有梯度惩罚的 Wasserstein GAN<sup>[66]</sup>和一维卷积网络来处理时间序列数据被提出。通过比较生成的时间序列与原始时间序列的相关统计数据,在将原始序列送入模型之前使用一个滚动窗口,目的是诱发更多的变化情况,从而覆盖更多的模式。在结果中,生成的数据在很大程度上能够复现标准普尔 500 指数的特征事实,同时保留可见的波动集群的视觉相似性。

### 3.4.2 FIN-GAN

FIN-GAN<sup>[6]</sup>目标是生成复制金融时间序列的主要特征事实的合成时间序列。该模型的生成器和鉴别器包含 3 种结构。①多层感知器(MLP)结构,有四层全连接的神经网络以及 Tanh 激活函数。②卷积神经网络结构,有 6 个卷积层和 Leaky ReLU 激活函数。③MLP-CNN,通过对它们的输出进行元素相乘,将 CNN 和 MLP 相结合。

FIN-GAN 模型与原来的 GAN 基本保持不变,采用最小损失和 Adam(自适应学习率)优化器<sup>[68]</sup>来更新  $D$  和  $G$  参数。研究发现,生成器的神经网络结构的变化对输出质量的影响比对鉴别

器的变化影响更大。使用批量归一化(重新缩放隐藏向量以在训练期间保持平均值和方差一致)显示了生成的时间序列的巨大波动和强烈的自相关性。这表明在深度学习中这种常用的图像生成工具对于金融时间序列的建模并不理想。时间序列的长度应足够长,以便可靠地计算统计财产,如概率分布和相关函数,因此将输出设为较大的值。

FIN-GAN 生成的时间序列保留了大部分金融数据的特征事实,因此和现实的金融时间序列有很高的相似度。该模型是金融领域 GAN 的一个重要标志,因为它是不需要明确假设或数学公式就能学习数据属性的模型,这是随机过程和基于个体建模在没有非微观假设的情况下无法做到的。

### 3.4.3 QuantGAN

QuantGAN<sup>[44]</sup>包括一个 GAN 的变体,即利用时间卷积网络(temporal convolutional network, TCN<sup>[69]</sup>),捕捉长距离的依赖关系,如波动性聚类现象,目的是通过使用神经网络、数据驱动的概念实现现实的资产价格模拟器。

TCN<sup>[69]</sup>是卷积框架,提供了统一的方法来捕捉单一模型中的低水平和高水平信息。TCN 包括一个因果的一维全卷积网络结构,其输出只取决于过去的序列元素。该模型的架构包含很多的扩张的卷积,即输入序列的元素之间的距离更大。换言之,该模型不是增加内核或过滤器的大小,而是引入空的空间以获得更多的覆盖,增加接收域并给出更广泛的视图,捕捉更多输入中的上下文信息。

实证结果表明,与其他卷积方法相比,TCN 更善于捕捉时间序列中的长期依赖关系。与递归神经网络相比,TCN 具有更多的可控梯度,简化了优化过程。

QuantGAN 使用 TCN 作为鉴别器和生成器网络。它在标准普尔 500 指数数据上进行了训练,并使用 Wasserstein 距离作为分布评价指标,又使用了 ACF(自相关函数)和杠杆效应分数来评估基于特征事实的准确性。结果显示,QuantGAN 产生的收益与实际收益高度相关。

### 3.5 生成式对抗网络用于金融领域异常检测

异常检测在金融领域中是一个重要的应用，主要用于识别不寻常或可疑的交易行为、市场操作或金融数据。异常检测的目的是预防欺诈、洗钱、市场操纵等非法活动，以及确保金融市场的公平、安全和稳定。在金融领域中，异常检测主要包括以下几个方面。①信用卡欺诈检测：通过分析用户的交易历史、消费习惯和地理位置等信息，识别可能的信用卡欺诈行为。②反洗钱检测：对客户的交易行为进行分析，识别可能涉及洗钱活动的异常交易。银行和金融机构需要严格遵守反洗钱法规，确保资金来源的合法性。③高频交易监测：监测金融市场中的高频交易行为，以防止操纵市场价格、操纵交易量等不公平竞争行为。④内幕交易检测：识别可能涉及内幕交易的行为，如某股票在重大信息发布前的异常交易量、价格波动等。⑤账户异常检测：对客户金融账户进行监控，以防止未经授权的访问、资金盗用等风险。

#### 3.5.1 LSTM-GAN

LSTM-GAN<sup>[58]</sup>是针对股票交易市场的异常检测的生成式对抗网络模型。股票市场中一些不良参与者试图通过欺骗其他投资者的方式，从股票交易中获取个人利益的行为被称为股票操纵<sup>[70]</sup>。在大多数情况下，股票操纵是非法的，但对于市场监管者来说，它很难被发现和预防<sup>[71]</sup>。随着使用计算机程序自动交易的兴起，每个交易日都有数以百万计的订单进入股票市场，仅依靠人工是不可能监控这些交易的。市场监管机构亟须智能计算机程序来调查这些交易，以便及时执行反措施。由于操纵案例的样本数不足，作为无监督学习方法的代表，GAN可以很好地适配这项任务，将其与长短期记忆结合，即提出LSTM-GAN模型，用于股票价格操纵检测。

如图16所示，LSTM-GAN模型使用生成对抗网络来检测由股价操纵引起的异常交易行为。长期短期记忆被用作LSTM-GAN的基础结构，它以无监督的方式学习正常的市场行为。训练后，GAN的鉴别器网络被用作检测器，以区分正常交易和操纵交易。与先前工作的不同之处在于LSTM-GAN没有使用操纵案例来训练神经网络，相反，使用正常数据来训练它们，模拟操纵案例仅用于测试目的。

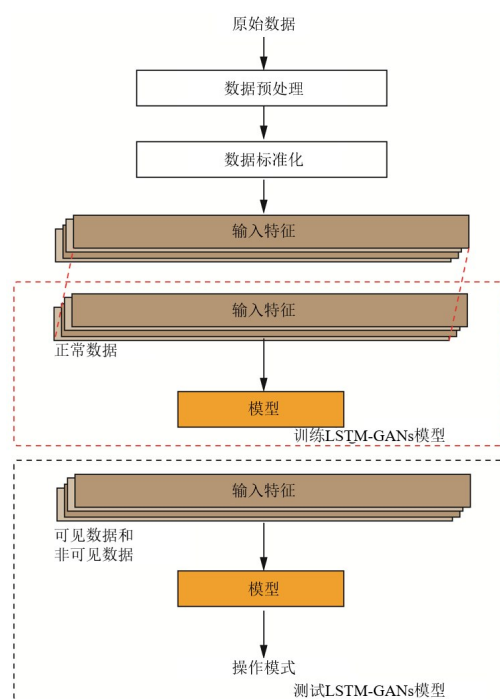


图16 LSTM-GAN模型

Figure 16 LSTM-GAN model

### 3.6 生成式对抗网络在金融领域的应用案例

生成式对抗网络在金融领域有了大量的理论模型，但大多数公司在实践中使用生成式对抗网络的程度有限或未完全披露，本节简要介绍已知的生成式对抗网络的应用。

#### 3.6.1 摩根大通人工智能研究所合成数据的生成

为了推进金融服务领域的人工智能研发，摩根大通的人工智能研究部门有专门用于生成合成数据集的分支机构。这些数据集可提供给其他的研究小组，包括：①反洗钱模型的客户相关数据集；②客户旅程事件、较低级别的客户-银行交互数据集；③市场执行数据：描述公共证券交易所金融工具买入和卖出订单匹配的限价订单簿数据；④欺诈检测的支付数据：具有合法和异常活动的几种交易类型，以提高检测能力。

研究部门为合成数据的理想表示和传输提出了框架<sup>[4]</sup>。该框架建议：①隐私性：即需要强制执行隐私的特定数据和上下文；②可读性：数据及其相关生成模型必须易于监管机构和其他代理

机构理解；③紧凑性：合成数据的表示应该是紧凑和可重构的，它应该需要很少的技术知识来改进在不同环境中的合成。

摩根大通的研究人员于 2021 年提出了 MAS-GAN<sup>[53]</sup>模型，用于多代理模拟的校准。

### 3.6.2 美国运通 AI 实验室的欺诈检测

欺诈损失主要来自电汇和信用卡/借记卡，近年来给银行、商户和客户造成了约 169 亿美元的损失<sup>[72]</sup>。在真实数据集上进行欺诈检测的一个已知问题是类不平衡。通常，数据集可以代表与现实有偏差的样本，并不可避免地导致错误的模型。美国运通公司的人工智能实验室正在通过生成合成数据来改进欺诈检测模型，以寻求解决这一问题的方法。Amex 研究人员<sup>[46]</sup>提出了条件和深度回归分析 GAN 的混合来生成合

成数据集。

使用 3 个包含公司内部数据的表格数据集来重新创建统计上相似的样本。通过比较真实数据分布和生成数据分布的特征，以及内部开发的工具 DataQC<sup>[73]</sup>对生成的数据进行评估。研究团队发现，虽然生成的数据显示了令人满意的结果，但基于合成数据训练的模型仍然比基于真实数据训练的模型差。

### 3.6.3 华泰证券的金融时间序列模拟

华泰证券对 GAN 模型进行研究，并将其应用于金融时间序列模拟。其中，华泰证券使用 cGAN 对多资产协方差矩阵进行预测框架如图 17 所示。cGAN 和其他生成方法生成质量的评估指标对比和各种生成方法在捕捉特征事实能力的对比分别如表 5 和表 6 所示。

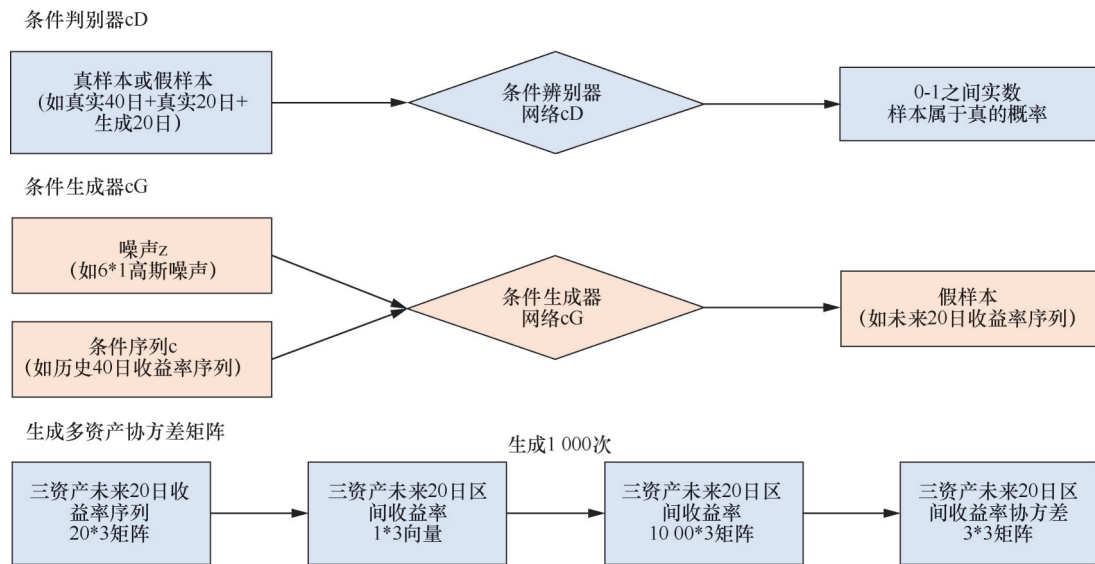


图 17 华泰证券使用 cGAN 对多资产协方差矩阵进行预测的框架

Figure 17 Framework of Huatai Securities uses cGAN to forecast multi-asset covariance matrices

表 5 上证综指日频序列：各种生成方法评价指标对比

Table 5 Daily frequency series of SSE Composite Index: comparison of evaluation indicators of various generation methods

| 评价指标    | 统计量                        | 真实序列  | GAN   | Bootstrap | GARCH |
|---------|----------------------------|-------|-------|-----------|-------|
| 自相关性    | 前 10 阶自相关系数均值              | 0.11  | 0.11  | 0.10      | 0.10  |
| 厚尾分布    | 拟合幂率衰减系数 $\alpha$          | 4.22  | 4.52  | 4.26      | 4.60  |
| 波动率聚集   | 拟合幂率衰减系数 $\beta$           | 0.16  | 0.32  | 0.58      | 0.17  |
| 杠杆效应    | 前 10 阶相关系数均值               | -7.02 | -4.56 | -0.05     | 0.02  |
| 粗细波动率相关 | 滞后 $\pm 1$ 阶相关系数之差         | -0.02 | -0.03 | 0.00      | 0.00  |
| 盈亏不对称性  | 盈亏 $\pm \theta$ 所需天数分布峰值之差 | 4.00  | 7.45  | 2.26      | 0.89  |

表6 各种生成方法在捕捉特征事实能力的对比  
Table 6 Comparison of evaluation indicators of various generation methods

| 评价指标    | 真实序列 | GAN | Bootstrap | GARCH |
|---------|------|-----|-----------|-------|
| 相关性     | √    | √   | √         | √     |
| 厚尾分布    | √    | √   | √         | √     |
| 波动率聚集   | √    | √   | ×         | √     |
| 杠杆效应    | √    | √   | ×         | ×     |
| 粗细波动率相关 | √    | √   | ×         | ×     |
| 盈亏不对称性  | √    | √   | √         | ×     |

根据资料显示, GAN模型的生成效果显著优于传统的计量经济学生成方法(如GARCH和Bootstrap)。此外, 当GAN应用于预测任务时, 可以将其转换为生成任务。具体而言, 给定过去40个交易日的资产收益率序列, 就可以使用GAN模型基于这40天的序列生成未来20个交易日的资产收益率序列。

#### 4 结束语

本文介绍了GAN模型相较其他生成模型在金融领域的优势; 对自2014年生成式对抗网络被提出以来的GAN模型根据应用方向分类; 着重整理了GAN模型在金融领域(金融表格数据生成、金融时间序列生成以及金融欺诈检测等)的应用与实践, 并对各模型的原理进行简要的介绍。而GAN在金融领域的不同应用中, 生成合成数据集的主题尤其值得关注。因为它可以针对不同金融场景中数据缺乏或不可用的条件进行定制。这种灵活性体现在许多方面: ①隐私和合规规则可能会严重限制数据的可用性和应用<sup>[74]</sup>; ②产品测试环境中通常需要数据, 而测试人员通常无法使用数据<sup>[75]</sup>; ③机器学习需要大量的训练数据, 这些数据可能昂贵且稀缺<sup>[76]</sup>。

数据驱动流程的增长以及这种分析和建模提供的新可能性, 对金融领域数据和数据科学家提出了更高需求。金融数据通常受到严格监管, 这限制了它们在开发新产品和流程中的使用。正如摩根大通的AI研究所描述的, 匿名化是不可靠的, 加密会削弱数据。高质量的合成金融数据可以解决大多数这些限制, 生成大量人工测试数据也大大提高了可扩展性, 增加了使用敏感或有限

数据集的机会。而在GAN得以更大范围地投入使用之前, 仍有若干问题需要注意, 具体如下。

##### (1) 更好的隐私机制

虽然由模型合成的数据不存在隐私问题, 但模型训练过程中会大量使用具有敏感信息的真实数据, 这同样可能存在安全隐患。

目前, 基于差分隐私的PEARL (private embeddings and adversarial reconstruction learning)<sup>[77]</sup>框架对敏感数据加入差分隐私, 进行了严格的隐私保护, 从理论上一定程度地避免了上述问题。一些模型为了解决原始数据在训练机器学习等任务时不同属性的公平性问题, 引入因果关系, 然后基于生成式对抗网络来消除敏感属性对最终结果的影响, 如CFGAN (collaborative filtering GAN)<sup>[78]</sup>和DECAF (dynamic executable code analysis framework)<sup>[79]</sup>。探寻更好的隐私机制, 提高模型的安全系数是后续需要挖掘的方向。

##### (2) 金融表格数据的隐含关系

金融表格数据有别于普通的表格数据, 行与行之间往往具有一定联系(如在企业的表格数据中, 企业之间存在上下游的联系), 而现有的模型很难捕捉到这类隐含关系, 导致最后生成的数据丢失了这一部分信息。未来的研究可以着重针对这一点, 改进GAN的模型结构或者算法, 实现合成数据质量的进一步提升, 从而让GAN模型在金融领域能够有更广泛的实际应用。

##### (3) 数据偏见问题

金融领域数据可能存在偏向性或歧视性, 这可能导致不公平的决策和对特定群体的不利影响。其中, 数据偏见又可以分为两类。①数据本身可能存在偏见。这主要来源于数据来源偏见和数据采样偏见, 选取的样本有时未必能代表整个目标群体。②如果模型就是用带有偏见的历史数据训练的, 那么模型算法在预测和决策时会产生不公平或歧视性结果。因此, 用更先进的GAN模型消除数据偏见也是重要的研究方向。

##### (4) 法规与合规挑战

随着GAN技术在金融领域的应用, 监管机构可能需要修改或制定新的法规来确保合规性。例如, 需要明确关于生成数据的使用、存储和传

输的具体规定,以防止不当行为和滥用。目前,国家互联网信息办公室的《生成式人工智能服务管理办法》征求意见稿已于 2023 年 4 月发布, GAN 作为生成式模型的一种,未来也将受到该管理办法的约束。由此可见,生成式人工智能相关的法律法规已经引起了国家的重视,相信将来进一步的完善,能够为这些技术大规模地落地使用奠定良好的法律基础。

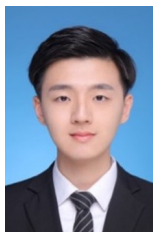
### 参考文献:

- [1] 鲁金彪, 胡国强, 周金赞, 等. 金融数据安全现状与趋势研究[J]. 中国金融电脑, 2022(5): 39-43.  
LU J B, HU G Q, ZHOU J Z, et al. Research on the present situation and trend of financial data security technology[J]. Financial Computer of China, 2022(5): 39-43.
- [2] 朱建明, 杨鸿瑞. 金融科技中数据安全的挑战与对策[J]. 网络与信息安全学报, 2019, 5(4): 71-79.  
ZHU J M, YANG H R. Data security challenges and countermeasures in financial technology[J]. Chinese Journal of Network and Information Security, 2019, 5(4): 71-79.
- [3] 张旭东. 金融数据安全与个人信息保护[J]. 清华金融评论, 2021(12): 93-95.  
ZHANG X D. Financial data security and personal information protection[J]. Tsinghua Financial Review, 2021(12): 93-95.
- [4] ASSEFA S A, DERVOVIC D, MAHFOUZ M, et al. Generating synthetic data in finance: opportunities, challenges and pitfalls[C]//Proceedings of the First ACM International Conference on AI in Finance. New York: ACM, 2020: 1-8.
- [5] FAN J, LIU T Y, LI G L, et al. Relational data synthesis using generative adversarial networks: a design space exploration[EB]. arXiv Preprint arXiv: 2008.12763, 2020.
- [6] TAKAHASHI S, CHEN Y, TANAKA-ISHII K. Modeling financial time-series with generative adversarial networks[J]. Physica A: Statistical Mechanics and Its Applications, 2019, 527: 121261.
- [7] CONT R. Empirical properties of asset returns: stylized facts and statistical issues[J]. Quantitative Finance, 2001, 1(2): 223-236.
- [8] BAUWENS L, LAURENT S, ROMBOUTS J V K. Multivariate GARCH models: a survey[J]. Journal of Applied Econometrics, 2006, 21(1): 79-109.
- [9] BANKES S C. Agent-based modeling: a revolution?[J]. Proceedings of the National Academy of Sciences of the United States of America, 2002, 99(Suppl 3): 7199-7200.
- [10] KINGMA D P, WELING M. Auto-encoding variational bayes [EB]. arXiv Preprint arXiv: 1312.6114, 2013.
- [11] HUANG H B, LI Z H, HE R, et al. IntroVAE: introspective variational autoencoders for photographic image synthesis[EB]. arXiv Preprint arXiv: 1807.06358, 2018.
- [12] KINGMA D P, SALIMANS T, JOZEFOWICZ R, et al. Improved variational inference with inverse autoregressive flow[C]// Proceedings of the 30th International Conference on Neural Information Processing Systems. New York: ACM, 2016: 4743-4751.
- [13] RAZAVI A, VAN DEN OORD A, VINYALS O. Generating diverse high-fidelity images with VQ-VAE-2[EB]. arXiv Preprint arXiv: 1906.00446, 2019.
- [14] VAN DEN OORD A, KALCHBRENNER N, KAVUKCUOGLU K. Pixel recurrent neural networks[J]. 33rd International Conference on Machine Learning, ICML 2016, 2016, 4: 2611-2620.
- [15] VAHDAT A, KAUTZ J. NVAE: A deep hierarchical variational autoencoder[J]. Advances in neural information processing systems, 2020, 33: 19667-19679.
- [16] REZENDE D, MOHAMED S. Variational inference with normalizing flows[EB]. arXiv Preprint arXiv: 1505.05770, 2015.
- [17] DINH L, SOHL-DICKSTEIN J, BENGIO S. Density estimation using Real NVP[EB]. arXiv Preprint arXiv: 1605.08803, 2016.
- [18] KINGMA D P, DHARIWAL P, YANG C L, et al. Glow: generative flow with invertible 1x1 convolutions[EB]. arXiv Preprint arXiv: 1807.03039, 2018.
- [19] OORD A, DIELEMAN S, ZEN H, et al. Wavenet: A generative model for raw audio[EB]. arXiv Preprint arXiv: 1609.03499, 2016.
- [20] YANG L, ZHANG Z L, HONG S D, et al. Diffusion models: a comprehensive survey of methods and applications[J]. ACM Computing Surveys, 2022, 56: 1-39.
- [21] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial nets[J]. Advances in neural information processing systems, 2014, 27.
- [22] KARRAS T, LAINE S, AITTALA M, et al. Analyzing and improving the image quality of StyleGAN[C]//Proceedings of the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2020: 8107-8116.
- [23] WANG Z W, SHE Q, WARD T E. Generative adversarial networks in computer vision: a survey and taxonomy[J]. ACM Computing Surveys, 2021, 54(2): 37.
- [24] SAFAVIAN S R, LANDGREBE D. A survey of decision tree classifier methodology[J]. IEEE Transactions on Systems, Man, and Cybernetics, 1991, 21(3): 660-674.
- [25] 曹莹, 苗启广, 刘家辰, 等. AdaBoost 算法研究进展与展望[J]. 自动化学报, 2013, 39(6): 745-758.  
CAO Y, MIAO Q G, LIU J C, et al. Advance and prospects of AdaBoost algorithm[J]. Acta Automatica Sinica, 2013, 39(6): 745-758.
- [26] ZHU J Y, ZHANG R, PATHAK D, et al. Toward multimodal image-to-image translation[EB]. arXiv Preprint arXiv: 1711.11586v4, 2017.
- [27] LIU M Y, TUZEL O. Coupled generative adversarial networks [EB]. arXiv Preprint arXiv: 1606.07536, 2016.
- [28] ZHU J Y, PARK T, ISOLA P, et al. Unpaired image-to-image translation using cycle-consistent adversarial networks[C]//Proceedings of the 2017 IEEE International Conference on Computer Vision (ICCV). Piscataway: IEEE Press, 2017: 2242-2251.
- [29] CHEN X, DUAN Y, HOUTHOOFT R, et al. InfoGAN: interpretable representation learning by information maximizing generative adversarial nets[C]//Proceedings of the 30th International Conference on Neural Information Processing Systems. New York: ACM, 2016: 2180-2188.

- [30] ISOLA P, ZHU J Y, ZHOU T H, et al. Image-to-image translation with conditional adversarial networks[C]//Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2017: 5967-5976.
- [31] LEDIG C, THEIS L, HUSZÁR F, et al. Photo-realistic single image super-resolution using a generative adversarial network[C]// Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2017: 105-114.
- [32] PARK N, MOHAMMADI M, GORDE K, et al. Data synthesis based on generative adversarial networks[EB]. arXiv Preprint arXiv: 1806.03384, 2018.
- [33] XU L, VEERAMACHANENI K. Synthesizing tabular data using generative adversarial networks[EB]. arXiv Preprint arXiv: 1811.11264, 2018.
- [34] XU L, SKOULARIDOU M, CUESTA-INFANTE A, et al. Modeling Tabular data using Conditional GAN[EB]. arXiv Preprint arXiv: 1907.00503, 2019.
- [35] ESPINOSA E, FIGUEIRA A. On the quality of synthetic generated tabular data[J]. Mathematics, 2023, 11(15): 3278.
- [36] RAJABI A, GARIBAY O O. TabFairGAN: fair tabular data generation with generative adversarial networks[EB]. arXiv Preprint arXiv: 2109.00666, 2021.
- [37] ZHAO Z L, KUNAR A, VAN DER SCHEER H, et al. CTAB-GAN: effective table data synthesizing[EB]. arXiv Preprint arXiv: 2102.08369, 2021.
- [38] ZHAO Z L, KUNAR A, BIRKE R, et al. CTAB-GAN+: enhancing tabular data synthesis[EB]. arXiv Preprint arXiv: 2204.00401, 2022.
- [39] BOJCHEVSKI A, SHCHUR O, ZÜGNER D, et al. NetGAN: generating graphs via random walks[EB]. arXiv Preprint arXiv: 1803.00816, 2018.
- [40] ZHOU D W, ZHENG L C, XU J J, et al. Misc-GAN: a multi-scale generative model for graphs[J]. Frontiers in Big Data, 2019, 2: 3.
- [41] DE CAO N, KIPF T. MolGAN: an implicit generative model for small molecular graphs[EB]. arXiv Preprint arXiv: 1805.11973, 2018.
- [42] YOON J, JARRETT D, VAN D SCHAAR M. Time-series generative adversarial networks[C]//Proceedings of the 33rd International Conference on Neural Information Processing Systems. 2019: 5508-5518.
- [43] DE M P F. Enriching financial datasets with generative adversarial networks[D]. MS thesis, Delft University of Technology, The Netherlands, 2019.
- [44] MAGNUS W, ROBERT K, RALF K, et al. Quant GANs: deep generation of financial time series[J]. Quantitative Finance, 2020, 20(9): 1419-1440.
- [45] JOLICOEUR-MARTINEAU A. The relativistic discriminator: a key element missing from standard GAN[EB]. arXiv Preprint arXiv: 1807.00734, 2018.
- [46] EFIMOV D, XU D, KONG L Y, et al. Using generative adversarial networks to synthesize artificial financial datasets[EB]. arXiv Preprint arXiv: 2002.02271, 2020.
- [47] LIAO S J, NI H, SZPRUCH L, et al. Conditional sig-Wasserstein GANs for time series generation[EB]. arXiv Preprint arXiv: 2006.05421, 2020.
- [48] MUTHUKUMAR P, ZHONG J. A stochastic time series model for predicting financial trends using nlp[EB]. arXiv Preprint arXiv: 2102.01290, 2021.
- [49] GUPTA A, JOHNSON J, LI F F, et al. Social GAN: socially acceptable trajectories with generative adversarial networks[C]// Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2018: 2255-2264.
- [50] ZHOU X Y, PAN Z S, HU G H Y, et al. Stock market prediction on high-frequency data using generative adversarial nets[J]. Mathematical Problems in Engineering, 2018, 4: 1-11.
- [51] WU W J, HUANG F, KAO Y D, et al. Prediction method of multiple related time series based on generative adversarial networks[J]. Information, 2021, 12(2): 55.
- [52] MIRZA M, OSINDERO S. Conditional generative adversarial nets[EB]. arXiv Preprint arXiv: 1411.1784, 2014.
- [53] ECKERLI F, OSTERRIEDER J. Generative adversarial networks in finance: an overview[EB]. arXiv Preprint arXiv: 2106.06364, 2021.
- [54] MARIANI G, ZHU Y D, LI J B, et al. PAGAN: portfolio analysis with generative adversarial networks[EB]. arXiv Preprint arXiv: 1909.10578, 2019.
- [55] KIM Y, KANG D, JEON M, et al. GAN-MP hybrid heuristic algorithm for non-convex portfolio optimization problem[J]. The Engineering Economist, 2019, 64(3): 1-31.
- [56] SUN H, DENG Z, CHEN H, et al. Decision-aware conditional GANs for time series data[C]//Proceedings of the Fourth ACM International Conference on AI in Finance. New York: ACM, 2023: 36-45.
- [57] MARTI G. CORRGAN: sampling realistic financial correlation matrices using generative adversarial networks[C]//Proceedings of the ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2020: 8459-8463.
- [58] LEANGARUN T, TANGAMCHIT P, THAJCHAYAPONG S. Stock price manipulation detection using generative adversarial networks[C]//Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI). Piscataway: IEEE Press, 2018: 2104-2111.
- [59] SETHIA A, PATEL R, RAUT P. Data Augmentation using Generative models for Credit Card Fraud Detection[C]//Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA). Piscataway: IEEE Press, 2018: 1-6.
- [60] ZHANG Z H, YANG L J, CHEN L G, et al. A generative adversarial network-based method for generating negative financial samples[J]. International Journal of Distributed Sensor Networks, 2020, 16(2): 155014772090705.
- [61] BOUROU S, EL SAER A, VELIVASSAKI T H, et al. A review of tabular data synthesis using GANs on an IDS dataset[J]. Information, 2021, 12(9): 375.
- [62] ARMANIOUS K, JIANG C M, FISCHER M, et al. MedGAN: medical image translation using GANs[J]. Computerized Medical

- Imaging and Graphics, 2020, 79: 101684.
- [63] RADFORD A, METZ L, CHINTALA S, et al. Unsupervised representation learning with deep convolutional generative adversarial networks[EB]. arXiv Preprint arXiv: 1511.06434, 2015.
- [64] HOCHREITER S, SCHMIDHUBER J. Long short-term memory [J]. Neural computation, 1997, 9(8): 1735-1780.
- [65] ZHANG H, GOODFELLOW I, METAXAS D, et al. Self-attention generative adversarial networks[EB]. arXiv Preprint arXiv: 1805.08318, 2018.
- [66] ARJOVSKY M, CHINTALA S, BOTTOU L. Wasserstein generative adversarial networks[C]//Proceedings of the 34th International Conference on Machine Learning-Volume 70. New York: ACM, 2017: 214-223.
- [67] GULRAJANI I, AHMED F, ARJOVSKY M, et al. Improved training of Wasserstein GANs[EB]. arXiv Preprint arXiv: 1704.00028, 2017.
- [68] KINGMA D P, BA J. Adam: a method for stochastic optimization [EB]. arXiv Preprint arXiv: 1412.6980, 2014.
- [69] LEA C, VIDAL R, REITER A, et al. Temporal convolutional networks: A unified approach to action segmentation[C]//Computer Vision - ECCV 2016 Workshops: Amsterdam, The Netherlands, October 8-10 and 15-16, 2016, Proceedings, Part III 14. Springer International Publishing, 2016: 47-54.
- [70] AGGARWAL R K, WU G. Stock market manipulation-theory and evidence[C]//AFA 2004 San Diego Meetings. 2003.
- [71] CAO Y, LI Y H, COLEMAN S, et al. Detecting price manipulation in the financial market[C]//Proceedings of the 2014 IEEE Conference on Computational Intelligence for Financial Engineering & Economics (CIFER). Piscataway: IEEE Press, 2014: 77-84.
- [72] BARKER K J, D'AMATO J, SHERIDON P. Credit card fraud: awareness and prevention[J]. Journal of financial crime, 2008, 15 (4): 398-410.
- [73] LOVE D, AGGARWAL N, STATNIKOV A, et al. An automated system for data attribute anomaly detection[C]//Proceedings of KDD 2017 Workshop on Anomaly Detection in Finance. PMLR: ADF, 2018: 95-101.
- [74] DANKAR F K, IBRAHIM M. FAKE it till you make it: Guidelines for effective synthetic data generation[J]. Applied Sciences, 2021, 11(5): 2158.
- [75] GĄSIORKIEWICZ L, MONKIEWICZ J, MONKIEWICZ M. Technology-driven innovations in financial services: The rise of alternative finance[J]. Foundations of Management, 2020, 12(1): 137-150.
- [76] MONTANTES J. Deep learning in finance: Is this the future of the financial industry[J]. Digital Finance. 2023, 5: 1-2.
- [77] LIEW S P, TAKAHASHI T, UENO M. PEARL: data synthesis via private embeddings and adversarial reconstruction learning[EB]. arXiv Preprint arXiv: 2106.04590, 2021.
- [78] CHAE D K, KANG J S, KIM S W, et al. CFGAN: a generic collaborative filtering framework based on generative adversarial networks[C]//Proceedings of the 27th ACM International Conference on Information and Knowledge Management. New York: ACM, 2018: 137-146.
- [79] DONAHUE J, JIA Y Q, VINYALS O, et al. DeCAF: a deep convolutional activation feature for generic visual recognition[J]. 31st International Conference on Machine Learning, ICML 2014, 2014, 2: 988-996.

## [作者简介]



崔毅浩 (1997-), 男, 上海人, 复旦  
大学硕士生, 主要研究方向为金融科技、  
表格数据仿真。



刘森 (1986-), 男, 湖南怀化人, 复旦  
大学副研究员, 主要研究方向为分布式  
系统互联和应用性能优化。



叶广楠 (1985-), 男, 广东龙州人, 复  
旦大学研究员、博士生导师, 主要研究  
方向为金融科技、图模型算法、多模态  
特征融合、计算机视觉。