

# CIKM 2023 | 基于提示微调的优惠券滥用检测图神经网络

Zhihao Wen 深度学习与图网络 2023-09-01 19:25 Posted on 新加坡

## CIKM 2023 | 基于提示微调的优惠券滥用检测图神经网络

作者 | Zhihao Wen

单位 | 新加坡管理大学

研究方向 | 图神经网络

### 摘要

本文由来自新加坡管理大学的作者提出了一种基于提示微调的优惠券滥用检测图神经网络 VPGNN。

## Voucher Abuse Detection with Prompt-based Fine-tuning on Graph Neural Networks

Zhihao Wen\*  
zhwen.2019@smu.edu.sg  
Singapore Management University  
Singapore

Yuan Fang<sup>†</sup>  
yfang@smu.edu.sg  
Singapore Management University  
Singapore

Yihan Liu  
yihan.liu@lazada.com  
Lazada Inc.  
Singapore

Yang Guo  
yg.357086@lazada.com  
Lazada Inc.  
Singapore

Shuji Hao<sup>†</sup>  
hao.shuji@gmail.com  
Lazada Inc.  
Singapore

论文标题: Voucher Abuse Detection with Prompt-based Fine-tuning on Graph Neural Networks

论文地址: <https://arxiv.org/abs/2308.10028>

优惠券滥用检测是电子商务中一个重要的异常检测问题。虽然出现了许多基于 GNN 的解决方案,但监督范式依赖于大量标签数据。一种流行的替代方法是使用无标签数据进行自监督预训练,然后在标签有限的下游任务中进一步微调。然而,"预训练、微调"模式往往受到预训练和下游任务之间目标差距的困扰。因此,我们提出了 VPGNN--一种基于提示的微调框架,用于优惠

券滥用检测的 GNN。我们设计了一种新颖的图提示函数，将下游任务重新表述为与预训练中的借口任务类似的模板，从而缩小了目标差距。

## 简介

在激烈的市场竞争中，用户获取一直是电子商务平台的重要指标。主要策略之一是推出电子优惠券，这有助于吸引更多新用户或鼓励现有用户购买更多商品。然而，电子优惠券在电子商务中的广泛使用也为滥用者提供了机会。他们通常先注册大量账户，然后下订单，目的就是利用为新用户提供的优惠券。他们要么以更高的市场价格转售商品（通常在使用优惠券后以大幅折扣购买），要么与卖家串通，在卖家自己的商店中使用优惠券下订单。这种行为不仅会给电子商务平台造成损失，还会破坏合法用户的生态系统。因此，检测这些滥用用户的订单并防止他们收集优惠券具有重要意义。

本文研究的问题称为“优惠券滥用检测”，旨在检测电子商务行业中滥用用户的订单。检测优惠券滥用的关键是订单之间的网络结构。例如，即使订单是通过不同的账户下达的，但如果它们使用相同的设备或相同的送货地址，它们仍然可能是相关的。如图 1(a)所示，订单图编码了订单之间丰富的关系和模式，有助于区分合法用户和滥用用户的行为。如图 1(b)所示，合法用户通常只在一台或两台设备上登录一个账户，并在第一笔订单上使用一张优惠券，以利用新买家激励机制。相反，如图 1(c)所示，滥用用户通常使用大量设备，并在每台设备上创建多个账户，其中包含多组信息（如电子邮件和手机号码）。在每个账户中，他们都会收集新买家奖励的优惠券，并只用该优惠券下一个订单。通过区分与合法订单和滥用订单相关的图结构，我们将优惠券滥用检测问题归结为图上的binary节点分类。

虽然优惠券滥用检测是异常检测的一个子类，但现有的解决方案并不是检测优惠券滥用这一特定问题的理想选择。一方面，虽然传统的机器学习方法在业界得到广泛应用，但它们无法利用重要的图结构信息。因此，最近的许多异常检测尝试都转向图神经网络（GNN）来利用结构信息。另一方面，优惠券滥用者通常会不时地采用不同的策略来减少平台的检测。因此，及时和高质量的滥用订单标记实例对检测至关重要，但在实际业务场景的生产环境中却非常有限。因此，大多数基于 GNN 的方法无法很好地受益于监督信息。与此同时，自监督 GNN 目标是捕捉内在图形模式，而不需要任何注释标签，因此前景广阔。然而，大多数自监督方法都遵循“预训练、微调”范式，这存在一个重大缺陷：预训练和下游任务之间存在目标差距，影响了预训练模型的泛化。在我们的场景中，不同地区和/或时间段的优惠券滥用检测可视为不同的下游任务，因为它们的策略不断变化，而且在每个地区或时间段，以时间敏感的方式获取滥用订单的标签只有在很小的范围内才可行。

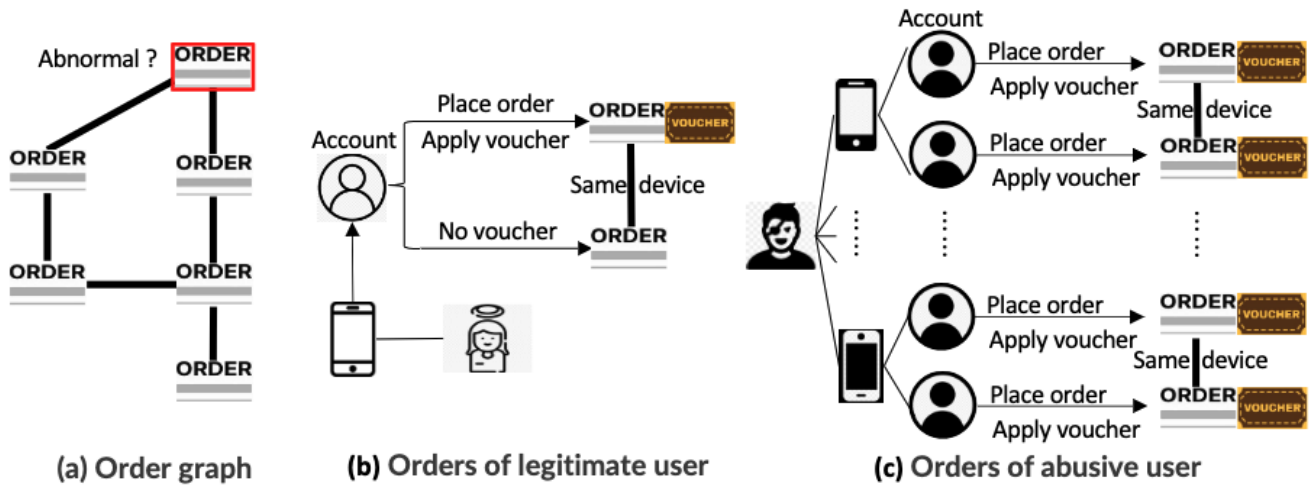


图 1：优惠券滥用检测示意图。

## 面临的挑战和提出的工作

为了弥补 GNN 预训练和下游任务之间的差距，我们提出了一种基于提示的图神经网络微调 (VPGNN) 优惠券滥用检测框架。我们在基于图的任务中引入了提示，将下游节点分类重新表述为与预训练中的借口任务类似的形式。虽然基于提示的 GNN 学习在 NLP 领域越来越流行，但它仍然面临两大挑战。首先，我们无法直接应用文本提示功能来衔接各种基于图的任务，因为文本提示与基本图元素（如节点和边）不兼容。因此，我们在本文中提出了一种图提示函数，它将下游节点分类问题重新表述为 context token 和节点 token 之间的配对匹配任务。具体来说，每个节点 token 代表一个节点类别，通过选择最有可能与节点 token 相匹配的类别（即 context token）来实现节点分类。这种成对模板与图预训练中许多流行的借口任务的成对表述一致。

其次，目前还不清楚如何在调整之前初始化 context token。context token 应该：1) 信息量大，以充分利用预训练过程中学到的先验知识，这也是提示的初衷；2) 稳健，尤其是在资源匮乏、任务标签有限的情况下。为了保证信息量，我们重新使用了预训练中的图读出函数来初始化下游的 context token；为了保证稳健性，我们使用本地子图来增强有限的标记节点。最后，对 context token 和预训练的 GNN 模型进行微调，以进行下游分类。

## 前言

**预训练。**有许多借口任务被提出来对 GNN 进行预训练。在优惠券滥用检测中，滥用订单占少数，合法订单占多数。因此，我们利用 DGI 来最大化局部-全局互信息，其中图层的全球信息捕捉了大多数人表现出的“正常”模式，这有助于表明节点偏离正常的程度。具体来说，设  $H$  为节点表示矩阵，其中每一行  $h_i$  都是由 GNN 编码器生成的节点  $i$  的表示，参数为  $\theta$ 。此外，让  $h_G$  成为  $G$  的全局表示，其公式为  $h_G = \Omega(H; \omega) = \text{POOL}(\{h_i \mid i \in V\})$  其中， $\Omega$  是参数攸关的读出函数。在预训练中，DGI 的目标是最小化以下损失：

$$\arg \min_{\theta, \omega, \phi} \sum_{(i, G)} \mathcal{L}^{\text{pre}} (\Phi^{\text{pre}} (\mathbf{h}_i, \mathbf{h}_G; \phi), \text{match}(i, G))$$

其中，由  $\phi$  参数化的  $\Phi^{\text{pre}}$  是一个投影头，用于评估节点图对  $(i, G)$  的匹配得分，衡量局部与全局的一致性。请注意，监督来自  $\text{match}(i, G)$ ，它是一个 indicator 函数：如果节点  $i$  来自原始图  $G$ ，则为 1；如果节点  $i$  来自损坏版本的  $G$ ，则为 0。因此，预训练过程不需要任何人工标注，而是以自监督的方式更新模型参数，包括  $\theta$  (GNN)、 $\omega$  (readout) 和  $\phi$  (投影头)。

**微调。** 经公式 (1) 优化的预训练 GNN 参数  $\theta^{\text{pre}}$  可作为下游分类任务的良好初始化。按照 "预训练，微调" 的模式，初始化与一组新的分类权重  $\psi$  一起通过优化以下公式进一步微调：

$$\arg \min_{\theta', \psi} \sum_{i \in V} \mathcal{L}^{\text{down}} (\Phi^{\text{down}} (\mathbf{h}_i; \psi), y_i)$$

其中， $\Phi^{\text{down}}$  是一个新的投影头，其参数  $\psi$  是随机初始化的，取代了之前的投影头  $\Phi^{\text{pre}}$ 。 $\mathcal{L}^{\text{down}}$  是下游分类损失（如交叉熵）， $y_i$  是节点  $i$  的特定任务标签。

## 方法

在本节中，我们将概述我们的方法，并详细介绍基于提示的微调。

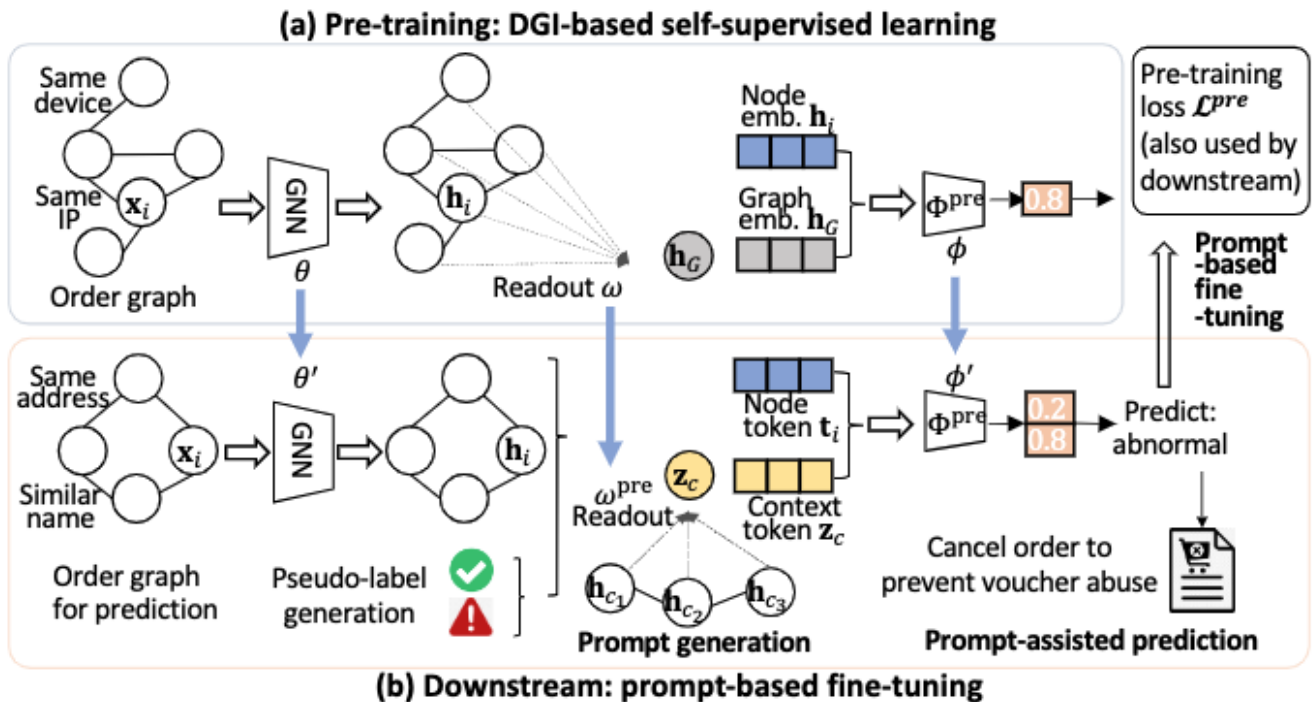


图 2: VPGNN的总体框架

## VPGNN 概述

与 NLP 中的文本提示不同，在图数据上，由于传统文本提示与图元素不兼容，设计提示并不容易。为了在图上实现基于提示的微调，我们的 VPGNN 分为两个主要阶段，如图 2 所示。首先，在图 2(a)中，我们基于 DGI 进行预训练。然后，在 (b) 中，我们对下游的优惠券滥用检测进行基于提示的微调。

其中，基于提示的微调包括三个关键模块：(1) 提示生成：我们的图提示功能为每个输入节点生成一组 token 对；(2) 提示辅助预测：对于每个输入节点，其 token 对的匹配概率可通过预训练中的同一投影头进行评分。匹配概率将用于预测合法/违规订单。(3) 基于提示的微调：提示中的 context token 将与预训练的 GNN 一起进行微调，与传统微调的主要区别在于，预训练中使用的相同借口投影头  $\Phi^{\text{pre}}$  和借口损失函数  $\mathcal{L}^{\text{pre}}$  将在下游任务中重复使用，而不需要新的投影头或任务损失。

下面，我们将首先简要介绍数据准备过程，然后重点介绍图 2(b) 中的下游阶段，因为预训练阶段已在前言中介绍过。

## 数据准备

我们的 VPGNN 模型需要两个关键输入元素，包括订单图和少量标签，具体如下。

**图表构建。**我们使用两类专有原始数据：(1) 包含电子邮件、IP 和送货地址等详细信息的用户配置文件；(2) 登录、订单、付款等买家旅程日志。我们根据各种共享属性（如相同的设备或地址、相似的用户名等）构建订单图，如图 1(a)所示，以捕捉订单之间的串通模式。

**有限的伪标签生成**由于优惠券滥用的不稳定性，及时和高置信度的标签更受欢迎。因此，我们通过使用一组预定义的业务规则来生成伪标签，这些规则是由 Lazada 公司的内部专家精心制定的。特别是，这些规则设计得比较保守，以避免触怒合法用户，这样只有最明显的滥用订单才会被标记出来。因此，这些伪标签的可信度很高，但可用性有限。在下游预测中，我们将利用这些为数不多的标签示例进行基于提示的微调。

## 提示生成、预测和调整

我们的基于提示的微调框架不是为下游任务引入新的投影头和损耗，而是生成和调整提示，并根据提示进行预测。首先，我们提出了一个图提示函数  $\mathcal{P}$ ，它将输入节点  $i$  转换为提示  $p_i$ 。提示  $p_i$  是一个连续的嵌入向量，其形状与预训练中借口投影头的输入相同。鉴于我们在 DGI 中的借口任务是最大化节点图对的互信息，我们的提示  $p_i$  也假定了一个成对模板，由一对节点 token 和 context token 组成。对于节点  $i \in V$ ，我们有



$$\mathbf{p}_i = \mathcal{P}(i) = [\mathbf{t}_i, \mathbf{z}_c]$$

其中，节点token  $t_i$  是节点  $i$  的向量表示，可由 GNN 编码；context token  $z_c$  是下游任务中类  $y_c$  的可学习嵌入，具体解释如下

**节点token。**节点token捕捉节点信息。与 NLP 中的输入文本嵌入相对应，我们的节点token  $t_i$  是输入节点  $i$  的嵌入。它可以是由 GNN 编码的节点  $i$  的表示形式  $h_i$ ，也可以是相邻节点  $i$  的嵌入向量的聚合。在我们的工作中，我们只需实现  $t_i = h_i$  即 GNN 的直接输出。

**Context token。**Context token旨在捕捉类的上下文信息。受提示调整的启发，我们为下游任务中的每个类别  $y_c$  建立了一个可学习的向量  $z_c$  作为context token。假设有一组  $C$  类  $\{1, 2, \dots, C\}$ 。因此，对于每个输入节点  $i$ ，我们可以将其节点token与  $C$  个不同的context token配对，形成  $C$  个token对，即  $(t_i, z_1), (t_i, z_2), \dots, (t_i, z_C)$ 。context token可用可学习的提示矩阵  $Z = [z_1, z_2, \dots, z_C]^\top \in \mathbb{R}^{C \times d}$  表示，其中  $d$  也是节点表示的嵌入维度。

**提示初始化。**既然context token是可学习的向量，我们就需要解决它们的初始化问题。传统的方法是随机初始化，即从头开始训练，这种方法信息量不大，而且无法利用我们预先训练好的模型。

为了提高初始化的鲁棒性，我们用邻近节点来增强已标注节点，这可以提供已标注节点周围的额外局部信息。为了提高信息量，我们重新使用了预训练中的图读出函数。由于 Readout 的设计目的是汇集图中的节点以得出图级摘要表示，因此它同样可以应用于下游，汇集与类相关的节点以得出类级摘要表示。类级摘要可以为context token提供更多的初始化信息，而context token则旨在捕捉有关类的信息。具体来说，对于每个类  $c$ ，我们收集标注节点集及其邻近节点

$V_c = \{c_1, c_2, \dots, c_N\}$ ，其中  $N = |V_c|$ 。然后，我们为  $V_c$  中的节点构建一个输入嵌入矩阵  $H_c = [h_{c_1}, h_{c_2}, \dots, h_{c_N}]^\top \in \mathbb{R}^{N \times d}$ ，其中  $h_{c_i}$  是节点  $c_i \in V_c$  的表示，由预训练的 GNN 编码。随后，context token  $z_c$  可以通过  $\Omega(H_c; \omega^{\text{pre}})$  进行初始化，其中  $\omega^{\text{pre}}$  是读出函数的预训练参数。为了提高效率，我们只对每个标注节点的  $\eta$  个邻居进行采样。

基于我们的提示设计，我们概述了基于提示学习的优惠券滥用检测，其中包括提示辅助预测和基于提示的微调

**提示辅助预测。**对于每个输入节点  $i$ ，提示函数会生成两个标记对  $(t_i, z_0)$  和  $(t_i, z_1)$ ，给定类别  $\{0 = \text{legitimate}, 1 = \text{abusive}\}$ ，用于二元优惠券滥用检测。我们可以利用相同的借口投影头  $\Phi^{\text{pre}}$  对每个token对的匹配概率进行评分，类似于在预训练中对节点图对进行评分。因此，我们预测节点  $i$  所代表的顺序为 "滥用"，当且仅当

$$\Phi^{\text{pre}}(\mathbf{t}_i, \mathbf{z}_1; \phi') > \Phi^{\text{pre}}(\mathbf{t}_i, \mathbf{z}_0; \phi')$$

因为  $z_0, z_1$  捕获了两个类别的上下文信息。在这里， $\phi'$  可以由投影头的预训练参数  $\phi^{\text{pre}}$  来初始化，并根据特定任务的标签进一步微调，正如我们接下来展示的那样。

**基于提示的微调。** 我们的提示设计不仅可以重复使用借口投影头，而无需引入新的分类头，还可以重复使用借口任务损失，而无需制定新的任务损失。

$$\arg \min_{\theta', \phi', \mathbf{Z}} \sum_{(i,c)} \mathcal{L}^{\text{pre}}(\Phi^{\text{pre}}(\mathbf{t}_i, \mathbf{z}_c; \phi'); \text{match}(i, c)) + \lambda \mathcal{L}^o$$

其中， $\text{match}(i, c)$  是之前提到的indicator函数：如果节点  $i$  被标记为  $c$ ，则为 1；否则为 0。  
 $\mathcal{L}^o = \|\mathbf{Z}\mathbf{Z}^\top - \mathbf{I}\|_2^2$  是对提示矩阵的正交约束，用于促进每个类别的可分离性， $\lambda \geq 0$  是控制约束重要性的系数。

实验

离线实验

**数据集。** 首先，在遵守所有安全和隐私政策的前提下，我们从 Lazada 公司提供的电子商务平台上收集了四个专有的大规模数据集，用于检测代金券滥用情况，分别命名为 VN0909、VN1010、ID0909 和 ID1023。每个数据集都是一个包含数百万个节点的图，其中节点代表具有预定义特征的订单，而边则是它们之间预定义的关系。VN0909 和 VN1010 来自 Lazada 的越南市场，收集时间为 2022 年 9 月 9 日和 10 月 10 日；ID0909 和 ID1023 来自 Lazada 的印度尼西亚市场，收集时间为 9 月 9 日和 10 月 23 日。请注意，VN0909 仅用于预训练，我们在其他三个数据集上进行了测试。其次，我们还使用了一个有关异常检测的公共数据集，即亚马逊数据集，并且我们在这个数据集上进行了预训练。

	SVM	XGBoost	MLP	GCN	SAGE <sub>sup</sub>	GAT	CARE-GNN	GeniePath	AMNet	DCI	SAGE <sub>unsup</sub>	Pre-train	VPGNN
Number of shots = 10													
VN1010	37.1±8.9	65.7±5.5	62.9±2.8	59.1±6.7	61.9±3.6	60.9±4.6	/	58.0±4.5	/	/	61.8±4.6	64.8±3.6	<b>67.1±3.1</b>
ID0909	28.1±11.0	51.3±9.9	61.6±3.8	64.1±3.9	61.2±7.3	65.6±3.7	/	62.1±2.8	/	/	62.2±3.7	66.1±3.0	<b>69.0±3.7</b>
ID1023	38.7±8.3	73.5±6.1	69.3±2.1	69.3±4.8	71.3±5.2	73.7±3.6	73.0±2.9	72.0±5.0	70.0±3.5	73.4±1.6	67.5±5.3	71.8±5.2	<b>75.1±1.9</b>
Amazon	41.4±9.2	62.5±11.5	63.3±5.7	16.5±4.9	59.9±9.1	20.5±6.1	38.6±2.9	30.7±2.8	64.8±6.2	18.5±4.0	36.7±6.0	62.3±8.1	<b>70.0±2.7</b>
Number of shots = 20													
VN1010	59.2±3.8	73.1±3.9	69.2±2.2	71.6±2.8	73.6±3.2	74.5±4.4	/	69.5±5.7	/	/	72.8±2.0	75.7±3.0	<b>75.9±2.8</b>
ID0909	53.1±6.1	64.9±3.8	64.9±1.7	68.7±2.5	70.3±2.8	71.0±3.4	/	61.4±9.1	/	/	67.5±2.2	71.4±2.5	<b>72.7±2.8</b>
ID1023	65.2±3.6	78.9±1.4	74.7±1.6	79.0±1.7	81.5±1.3	81.1±1.1	74.2±0.9	80.7±4.2	75.6±1.9	79.4±1.3	78.1±2.1	81.3±1.4	<b>81.8±1.1</b>
Amazon	60.3±3.6	72.9±8.2	70.4±4.4	16.8±8.0	63.0±8.5	48.8±10.1	42.2±6.7	30.8±4.4	75.1±3.1	21.8±2.6	54.5±2.8	73.1±3.9	<b>76.6±2.5</b>
Semi-supervised													
VN1010	86.7±0.1	87.8±0.1	86.7±0.1	91.8±0.1	94.1±0.1	91.9±0.0	/	91.7±0.4	/	/	89.3±0.0	94.1±0.1	<b>95.2±0.1</b>
ID0909	86.0±0.2	89.2±0.3	86.8±0.3	92.2±0.2	93.4±0.2	92.3±0.2	/	91.1±0.4	/	/	86.3±0.2	93.3±0.2	<b>94.1±0.2</b>
ID1023	89.3±0.1	89.9±0.2	88.8±0.2	94.4±0.1	95.6±0.1	94.5±0.1	87.0±0.3	94.5±0.1	94.1±0.3	93.7±1.0	92.6±0.1	95.6±0.1	<b>96.2±0.1</b>
Amazon	78.8±1.1	75.6±2.7	78.1±1.8	34.4±3.6	81.1±1.5	73.3±2.9	45.2±5.6	30.9±4.5	81.7±1.1	26.1±4.5	76.1±0.9	80.9±0.9	80.6±0.7

表 1：VPGNN 与基线的性能比较（百分比，含 95% 置信区间）。在每一行中，最佳结果用粗体表示，亚军用下划线表示。“/”表示由于内存不足或训练时间过长（超过 72 小时）而没有结果。

鉴于预训练是在 VN0909 上进行的，VPGNN 在 VN1010、ID0909 和 ID1023 上的优异表现显示了其跨时间和/或市场的泛化能力。

线上测试


**在线表现。** VPGNN 于 2022 年 12 月 11 日至 13 日在印度尼西亚市场部署测试，用于双 12 活动。我们将 VPGNN 与现有的两种部署模型进行了比较：BCP 是无监督 K-means 聚类模型的分布式实施，LPA 是高效的无监督社区检测算法。

Model	11 Dec 2022	12 Dec 2022	13 Dec 2022	Overall
BCP	100.0%	100.0%	100.0%	100.0%
LPA	816.9%	1784.1%	330.3%	809.3%
VPGNN (% ↑ over LPA)	<b>1964.1%</b> (140.4%)	<b>1990.3%</b> (11.6%)	<b>469.1%</b> (42.0%)	<b>998.7%</b> (23.4%)

表 2：以 BPWC 衡量的双 12 期间印度尼西亚市场的在线表现

结语

在本文中，我们提出了一种基于提示的 GNN 微调方法，称为 VPGNN，以解决优惠券滥用检测问题。我们试图弥合借口任务和下游任务之间的差距，提出了一种图提示功能，将下游任务重新制定为遵循与借口任务类似的模板。鉴于滥用订单的下游标签有限，预训练的 GNN 模型只需进行相对较少的微调即可应用。在专有数据集和公共数据集上进行的广泛离线实验表明，VPGNN 在少数情况下和半监督情况下的表现优于最先进的基线。此外，在线评估还表明，VPGNN 比现有的两个部署模型有显著提高。



深度学习与图网络

关注图网络、图表示学习，最近顶会顶刊动态以及机器学习基本方法，包括无监督学习...>

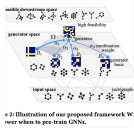
351篇原创内容

公众号



KDD 2023 || 图预训练都是有效的吗？什么时候预训练图神经网络?从数据生成角度回答该问题

深度学习与图网络



密西根州立大学汤继良教授出品：《图深度学习理论与实践》在线中文课程

深度学习与图网络



厉害了!!! 24岁，她将任准聘副教授！

深度学习与图网络

