# 第8章　图神经网络的对抗鲁棒性

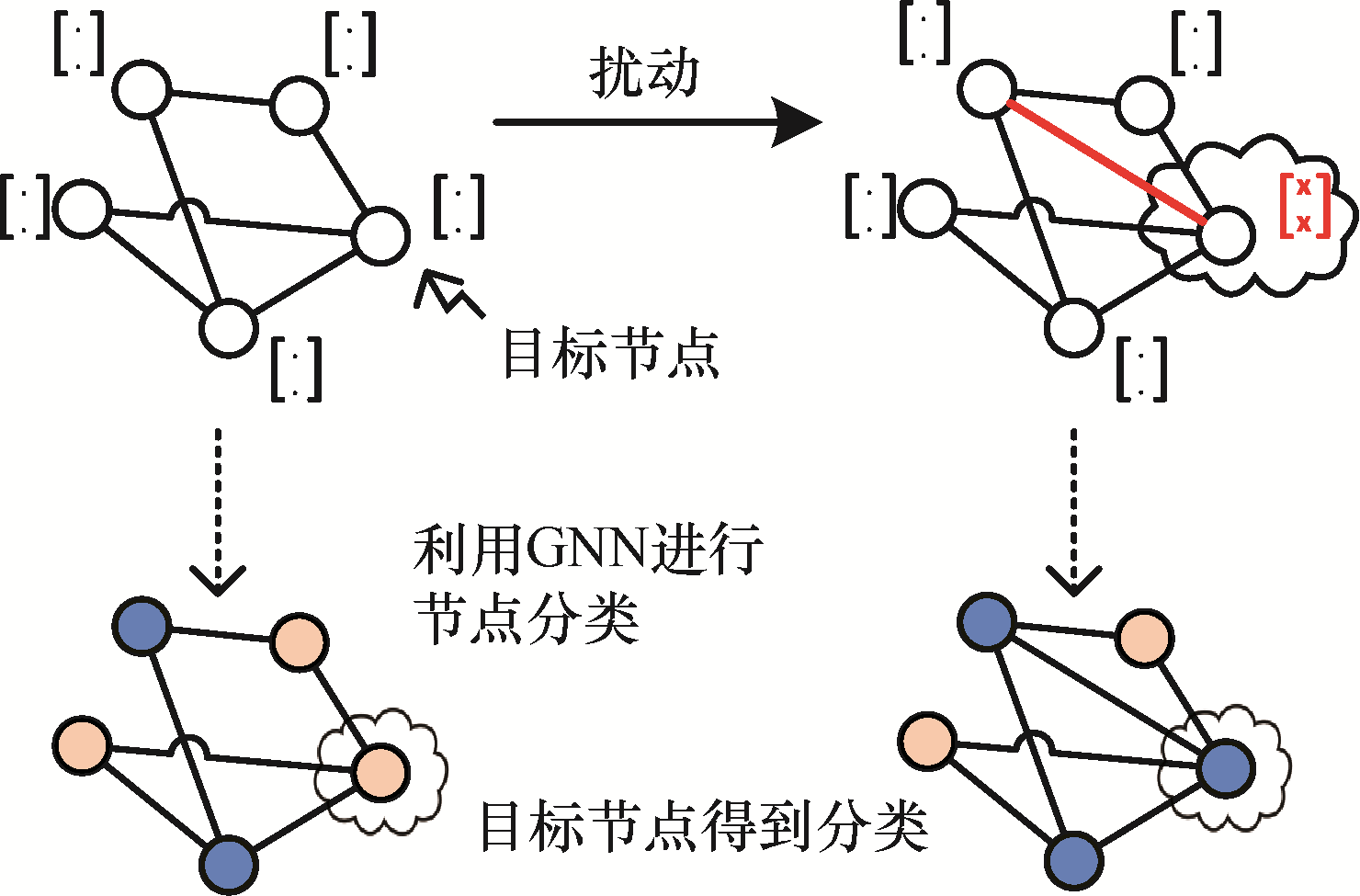


图8.1 左上图是原始输入，右上图是做了一处细小改动后的结果（如增加一条边或改变一些节点属性），下半部分的两个图说明了从GNN得到的每个节点的预测类别。我们有可能改变预测结果吗？GNN是鲁棒的吗

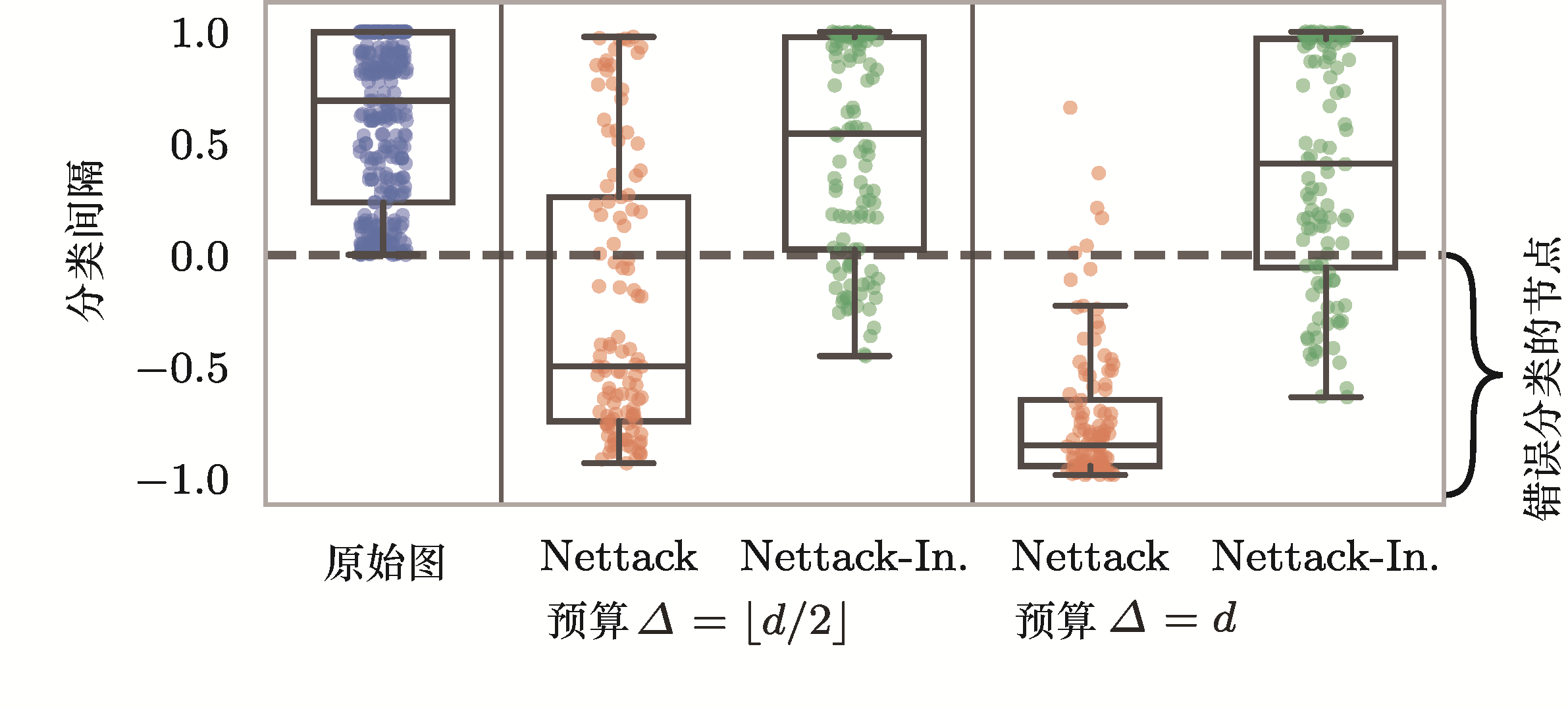


图8.2 使用Nettack（Zügner et al，2018）方法对GCN模型和Cora ML数据进行局部结构攻击。  
如果一个节点在虚线之下，那么相对于标注标签，它将被错误地分类。可以看出，  
几乎任何节点的预测可以被改变

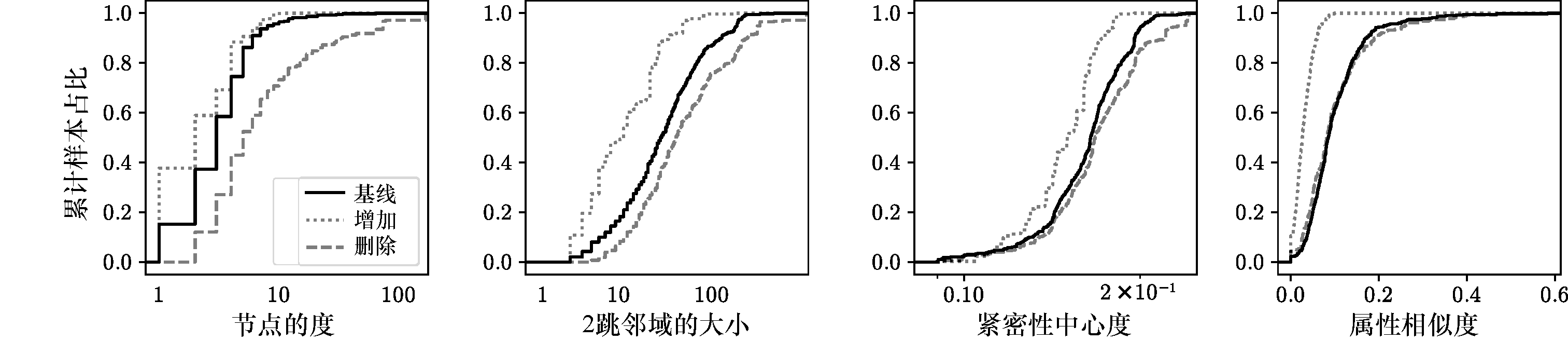


图8.3 使用Nettack方法与目标节点连接（增加）或断开连接（删除）的  
节点的属性累积分布（以整个图中的分布为基线）

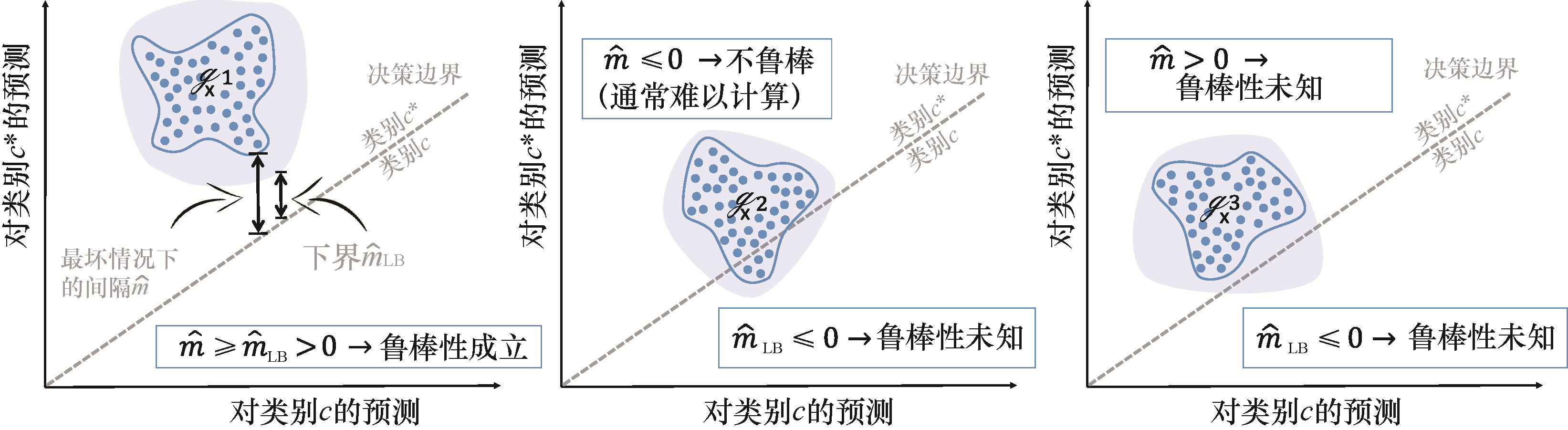


图8.4 通过最坏情况下的间隔获得鲁棒性认证。从未受扰动图G*i*中得到的预测值用一个交叉点显示，而从受扰动图*Φ*( G*i*)中得到的预测值则显示在这个交叉点的周围。最坏情况下的间隔衡量的是到决策边界的最短距离，如果结果是正的（见G1），则所有的预测都在边界的同一侧，鲁棒性成立；如果结果是负的（见G2），那么一些预测就会越过决策边界，在扰动下，类别预测就会发生变化，这意味着模型不是鲁棒的。当使用下界（图中的阴影区域）时，正值的鲁棒性得到保证（见G1），因为最坏情况下的精确间隔只能更大。如果下界变成负值，则不能做出任何说明（见G2和G3，鲁棒性未知）。G2和G3都有一个负的下界，而最坏情况下精确间隔（难以计算）的符号是不同的

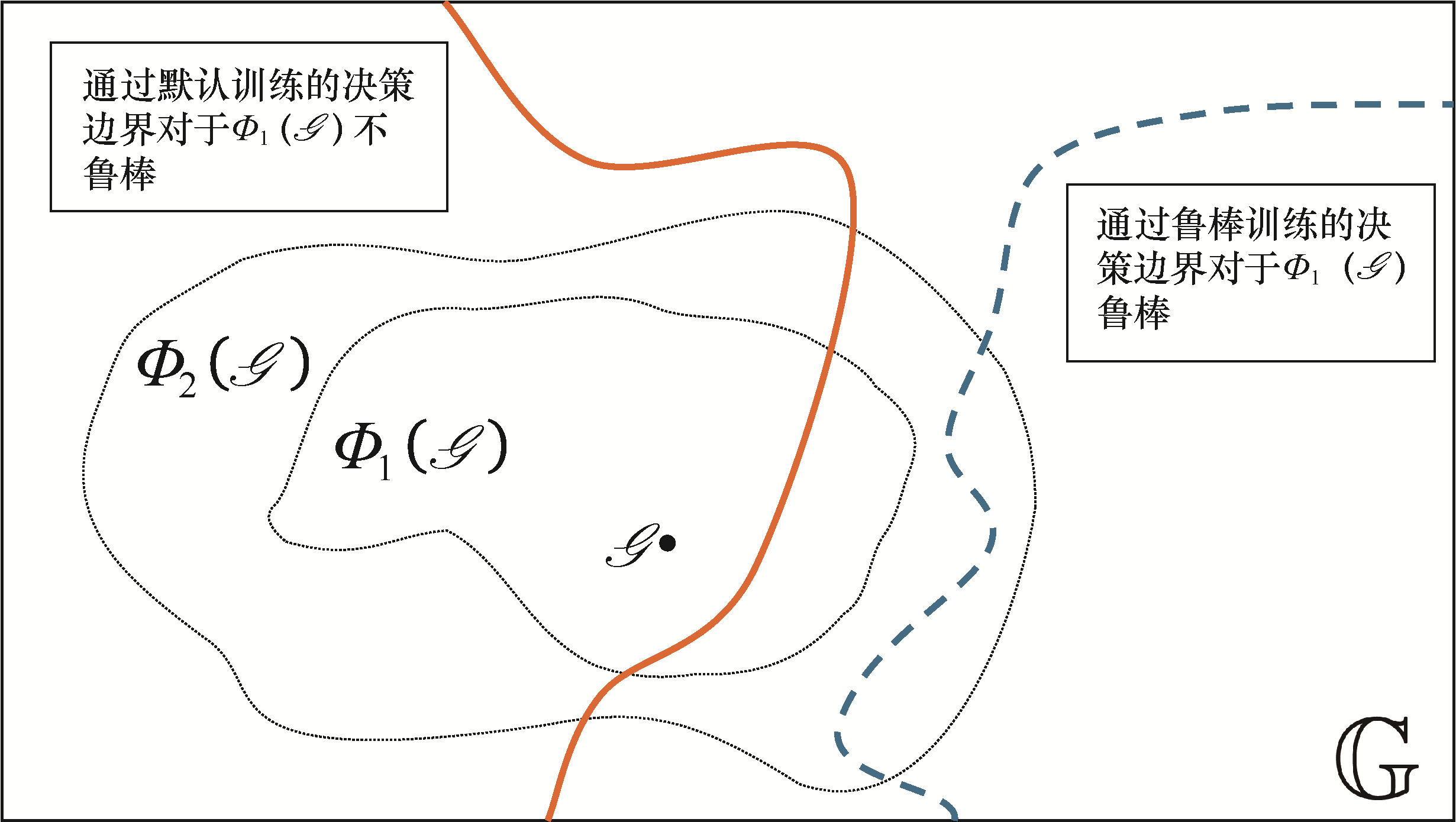


图8.5 关于鲁棒训练的说明。与橙色/实线决策边界对应的分类器对的扰动并不鲁棒：  
一些图越过了边界，因此被分配到不同的类别。通过鲁棒训练得到的分类器（蓝色/虚线决策边界）  
为中的所有图分配了相同的类别：对鲁棒，但对不鲁棒

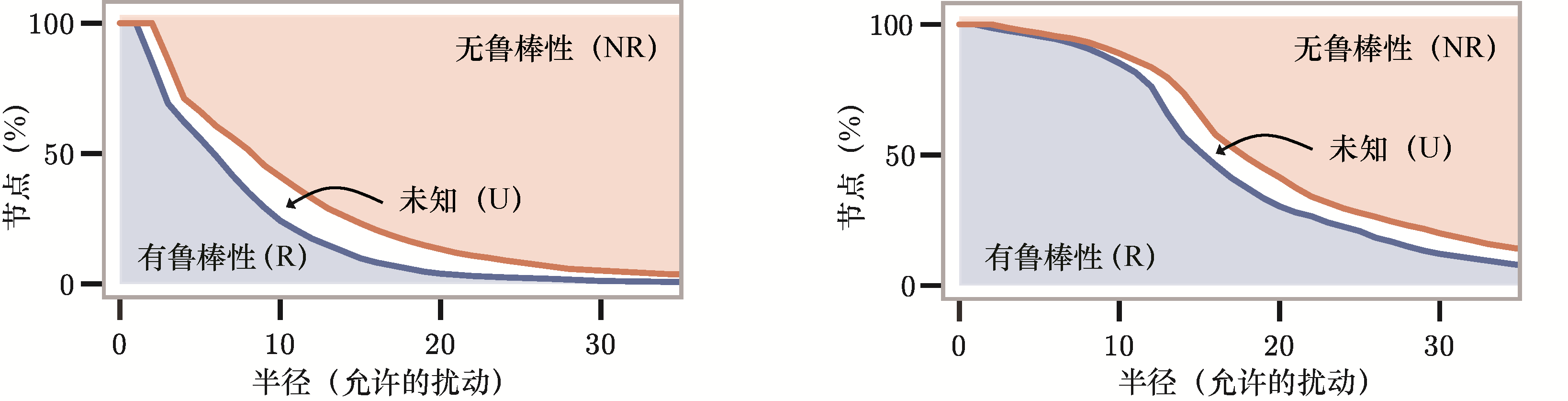


图8.6 在扰动半径增加的情况下，被证明有鲁棒性的节点（蓝色；R）、通过对抗性样本构建的无鲁棒性的节点（橙色；NR）或鲁棒性未知的节点（“缝隙”；U）所占的份额。对于一个给定的半径，（R）+（NR）+（U）的份额为100%。左图：标准训练。右图：Zügner and Günnemann（2019）提出的鲁棒训练。  
数据来自Citeseer数据和节点属性的扰动

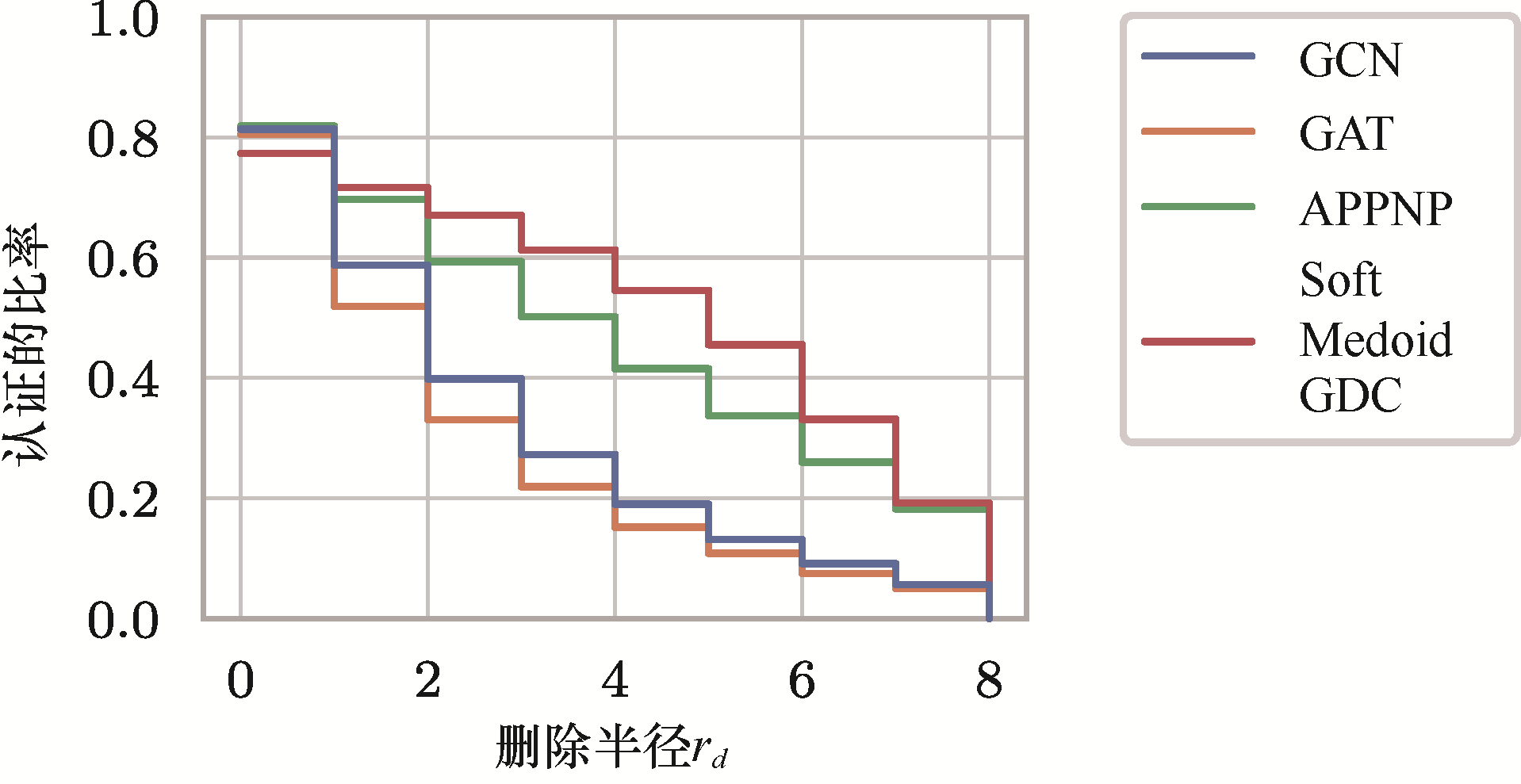


图8.7 使用（Bojchevski et al，2020a）中的认证从不同的GNN模型得到的平滑分类器的认证的比率。  
其中，由边删除扰动组成。认证的模型无关性允许我们比较不同模型的鲁棒性

# 第10章　链接预测

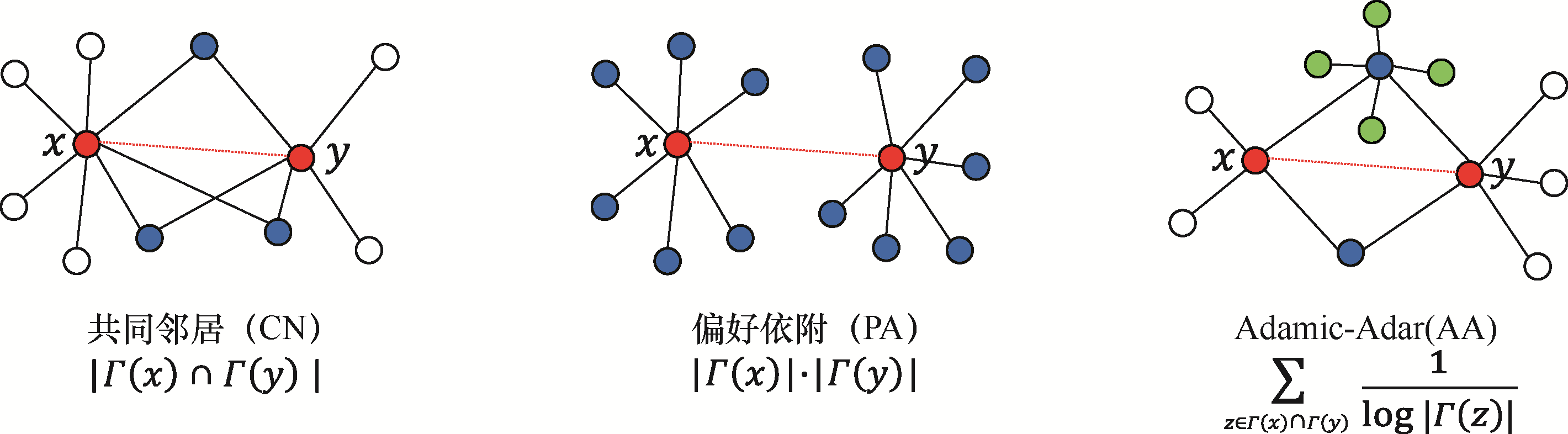


图10.1 传统链接预测的三种局部启发式方法—CN、PA和AA

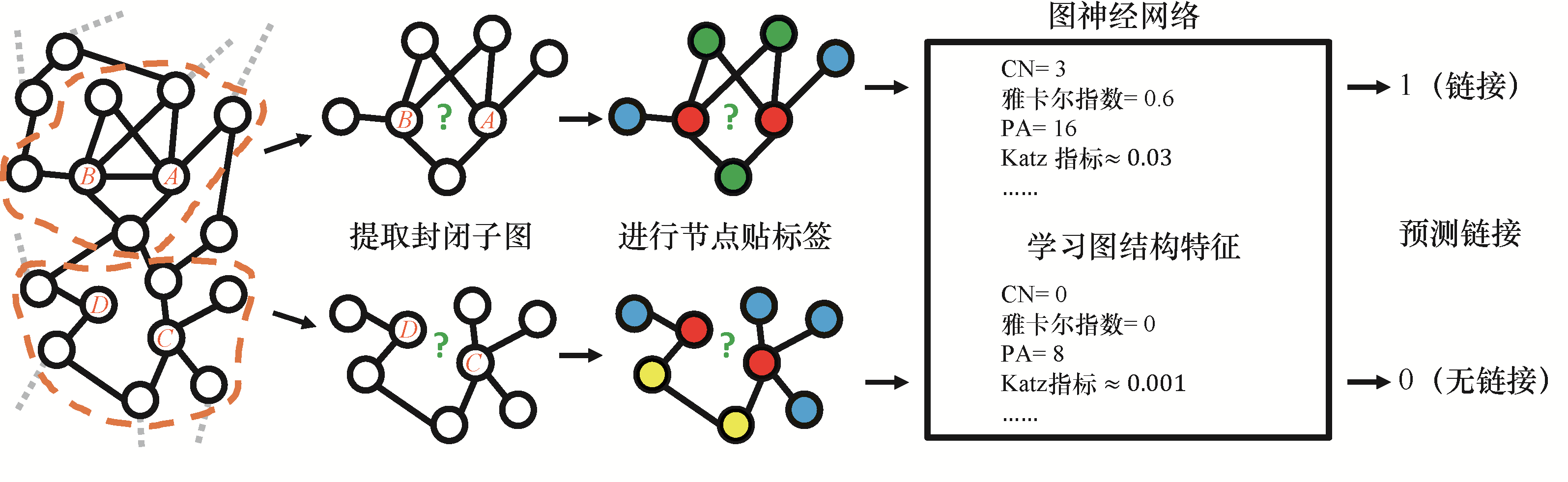


图10.2 关于SEAL框架的说明。SEAL首先提取目标链接周围的封闭子图来进行预测；然后对封闭子图进行节点标记，以区分子图中不同角色的节点；最后将有标签子图送入GNN，以学习用于链接预测的图结构特征（监督启发式方法）

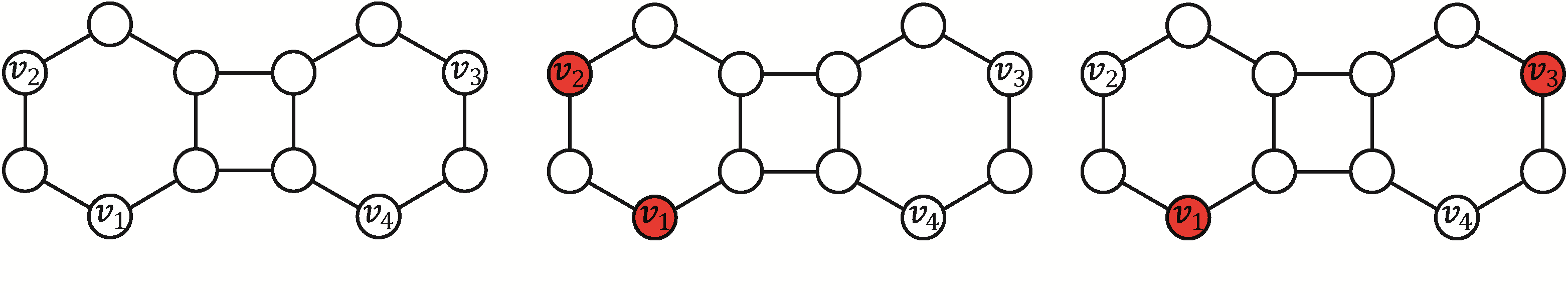


图10.3 基于节点的方法和基于子图的方法之间不同的链接表征能力。在左图中，节点*v*2和*v*3是同构的，链接（*v*1, *v*2）和链接（*v*4, *v*3）是同构的，但链接（*v*1, *v*2）和链接（*v*1, *v*3）不是同构的，基于节点的方法无法区分链接（*v*1, *v*2）和链接（*v*1, *v*3）。在中间图中，当预测链接（*v*1, *v*2）时，我们将给这两个节点贴上与其他节点不同的标签，这样GNN在学习节点*v*1和*v*2的表征时就能意识到目标链接了。同样，当预测链接（*v*1, *v*3）时，节点*v*1和*v*3将被贴上不同的标签（如右图所示）。如此一来，左图中节点*v*2的表征将与右图中节点*v*3的表征不同，从而使得GNN能够区分链接（*v*1, *v*2）和链接（*v*1, *v*3）

# 第11章　图生成

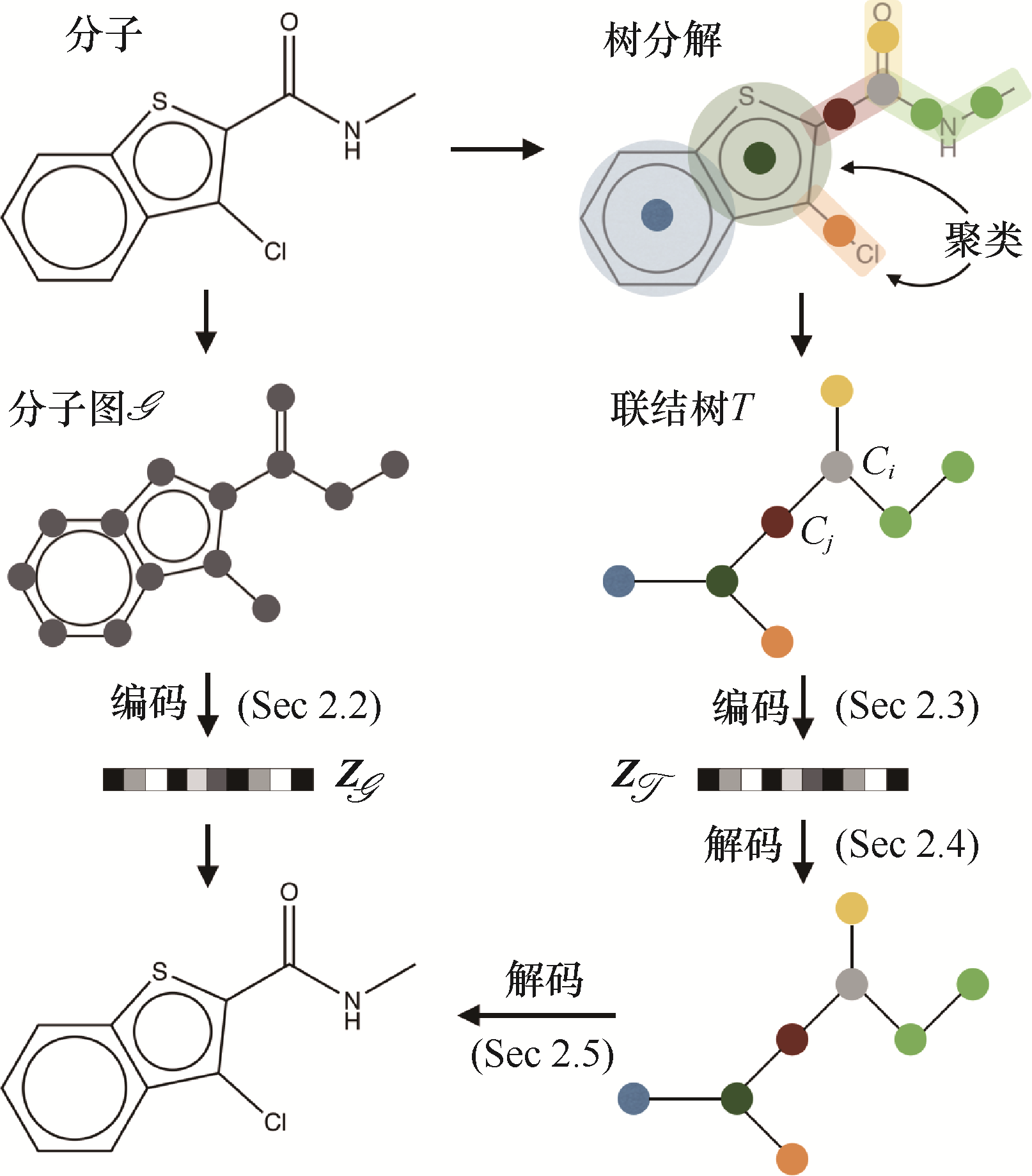


图11.1 联结树VAE。对应于分子图的联结树是通过树分解得到的，如右上图所示。联结树中的一个节点/聚类（彩色阴影）可能对应于原始分子图中的一个子图。两个基于GNN的编码器被分别应用于分子图和联结树，以构建潜向量***Z***G和***Z***T的变分后验分布。在生成过程中，首先使用自回归解码器生成联结树，然后通过近似解决最大后验分布问题以获得最终的分子图。改编自（Jin et al，2018a）中的图3

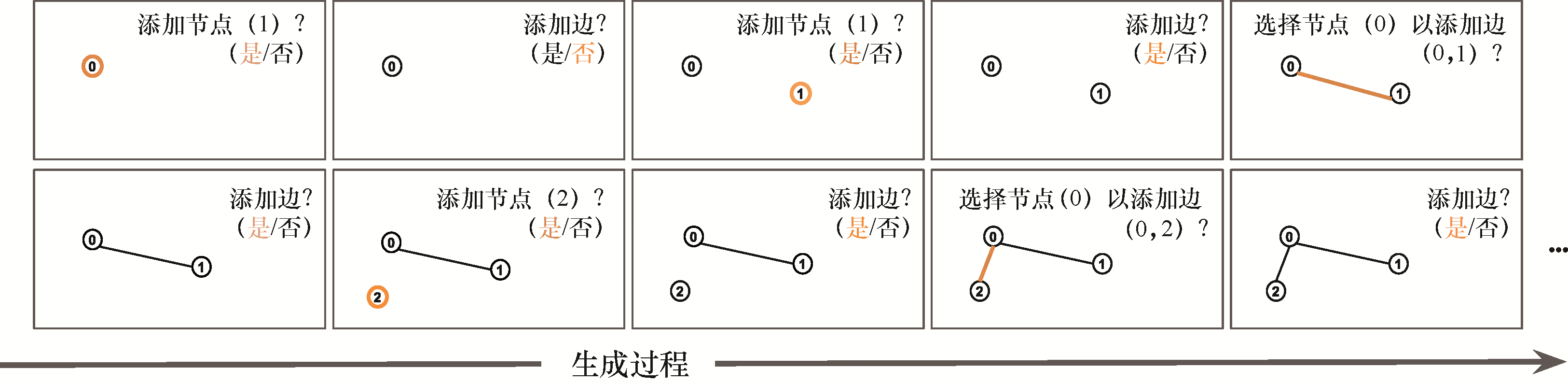


图11.2 Li et al（2018d）对深度图生成模型做了概述。图生成被表述为一个连续决策过程。在生成的每一步，该模型需要决定：（1）是否添加一个新的节点或停止整个生成过程；（2）是否添加一条新的边（其中一端连接到新的节点）；（3）新的边要连接哪个现有的节点。改编自（Li et al，2018d）中的图1

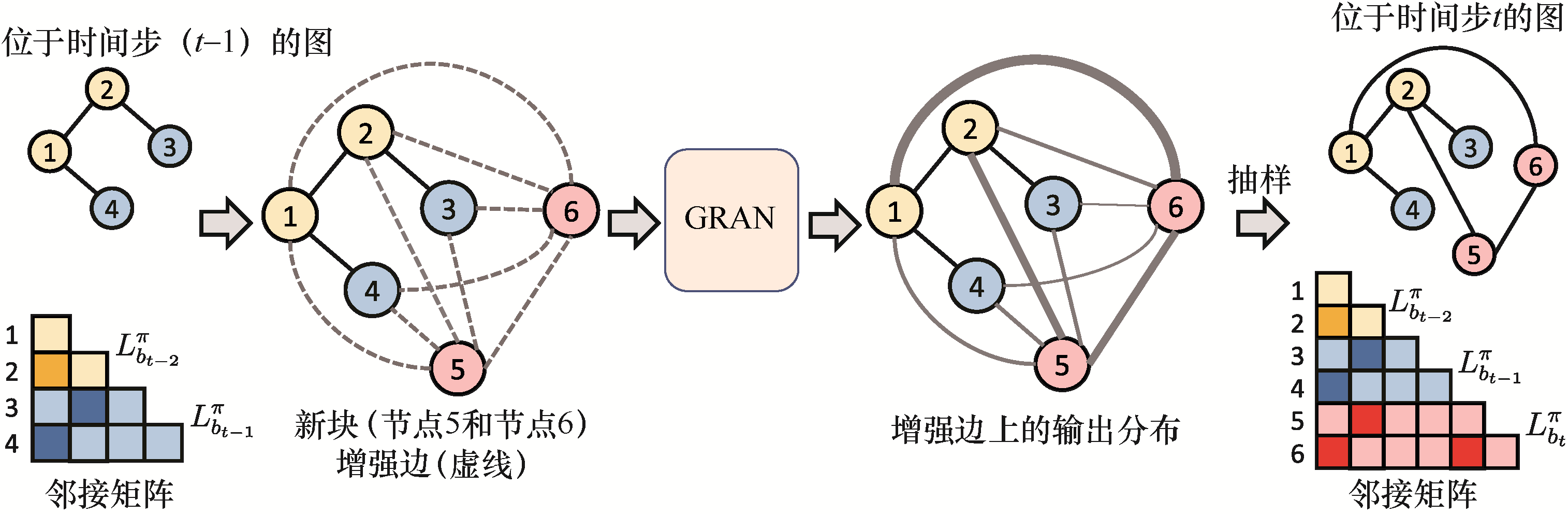


图11.3 Liao et al（2019a）对图循环注意力网络（GRAN）做了概述。在每一步，给定一个已经生成的图，添加一个新的节点块（大小为2，颜色表示可视化中个别组的成员）和一些增强边（虚线）。然后将GRAN应用于这个图，以获得增强边的输出分布（这里显示了一个独立于边的伯努利分布，其中，线宽表示产生单个增强边的概率）。最后从输出分布中取样，得到一个新的图。改编自（Liao et al，2019a）中的图1

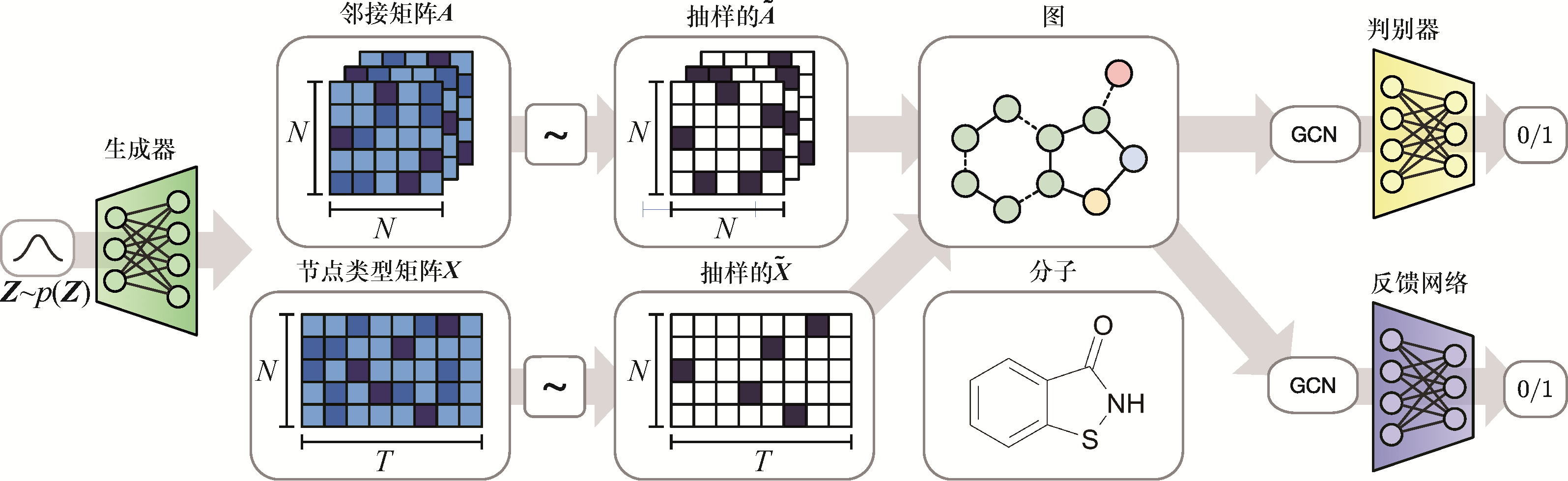


图11.4 De Cao and Kipf（2018）对MolGAN做了概述。首先绘制一个潜向量，并将其送入一个生成器，生成一个概率（连续）邻接矩阵***A***和一个概率（连续）节点类型矩阵***X***。然后绘制一个离散的邻接矩阵和一个离散的节点类型矩阵，它们共同构成了一个分子图。在训练过程中，将生成的图分别送入判别器和反馈网络，以获得对抗性损失（评估生成的图和观察到的图的相似程度）和负反馈  
（衡量生成的图满足特定化学约束的可能性）。改编自（De Cao and Kipf，2018）中的图2

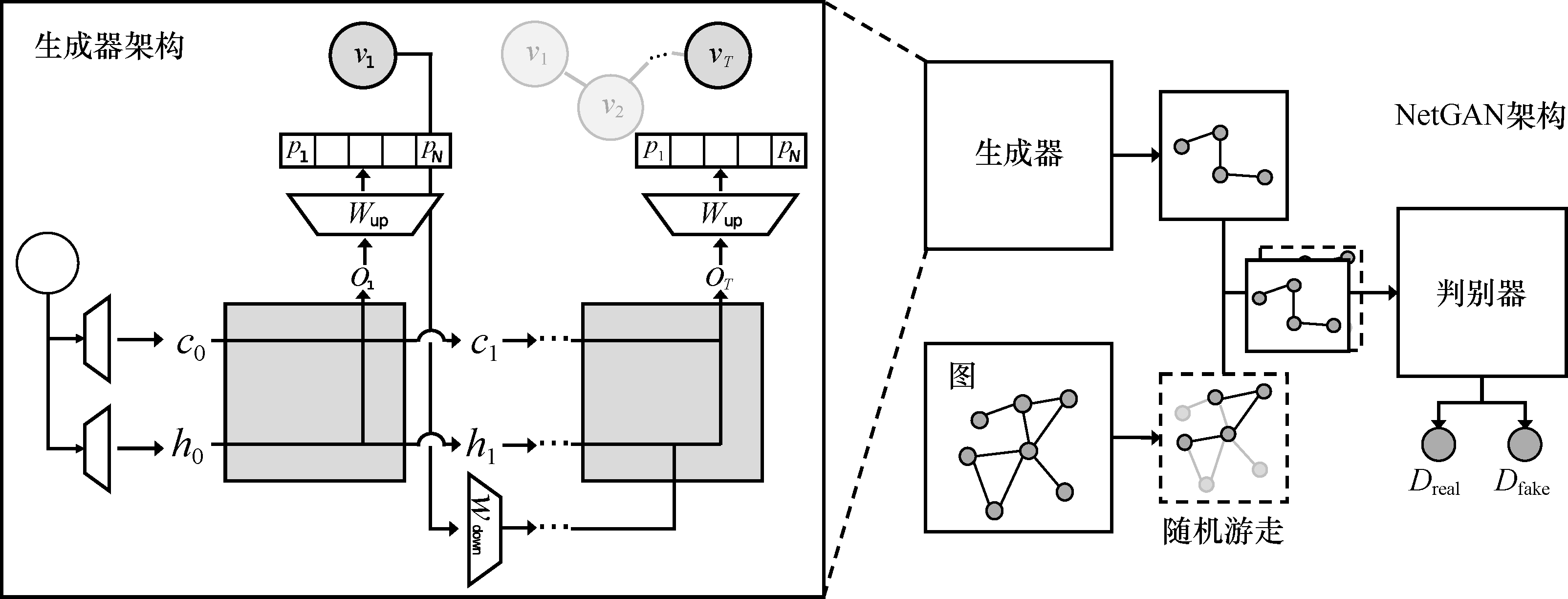


图11.5 Bojchevski et al （2018）对NetGAN做了概述。首先从一个固定的先验N (0,***I***)中抽取一个随机向量，并初始化LSTM的记忆*c*0和隐藏状态***h***0。然后，LSTM生成器生成每一步要访问的节点，并对固定的步数*T*进行展开。最后，节点索引的独热编码被送入LSTM并作为下一步的输入。判别器是另一个LSTM，用于执行二分类，以预测给定的随机游走从数据分布中抽样的概率。改编自（Bojchevski et al，2018）中的图2

# 第13章　图匹配

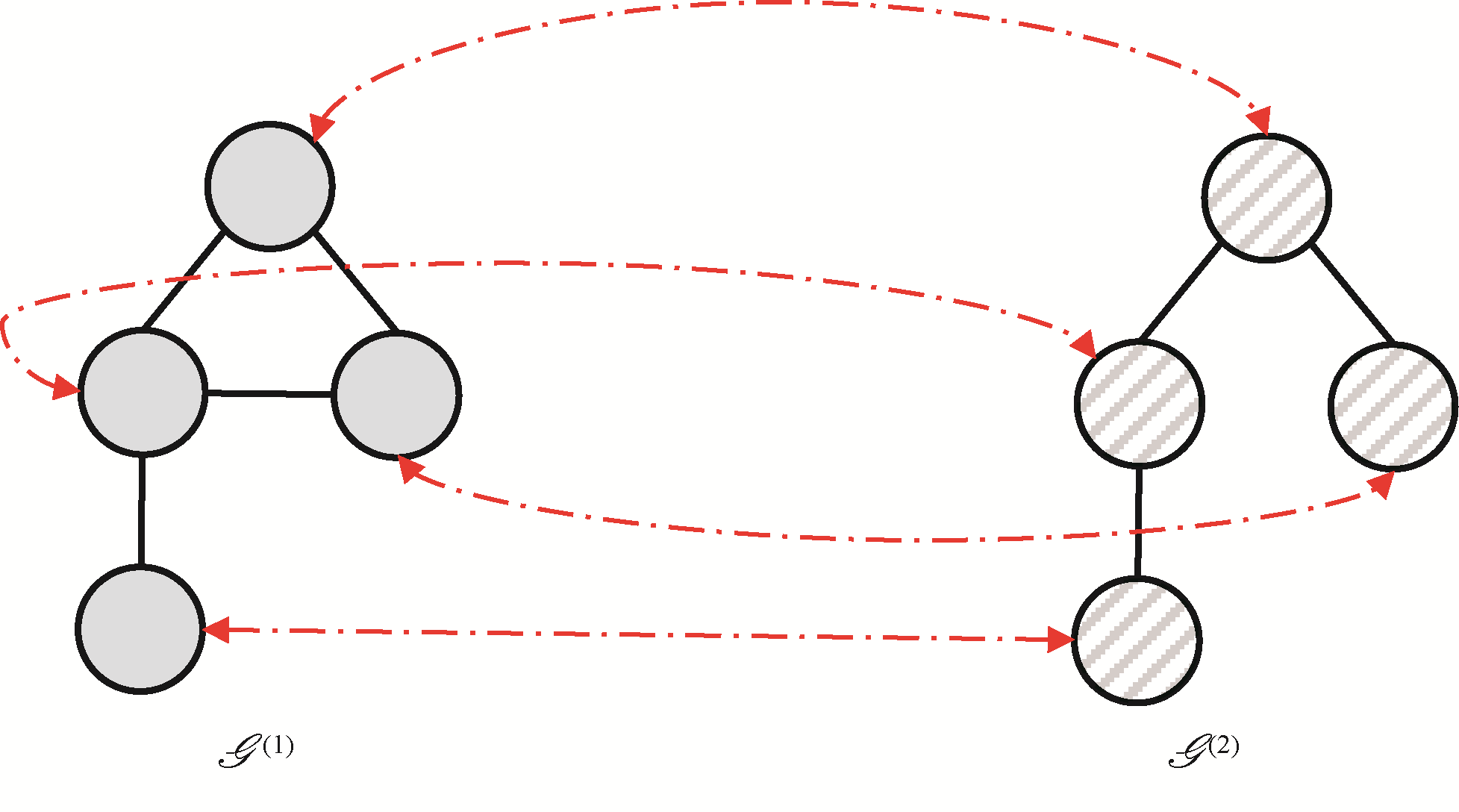


图13.1 图匹配问题的示例说明。两个输入图（左边的图和右边的图）需要匹配，  
红色虚线代表这两个图之间的节点与节点的对应关系

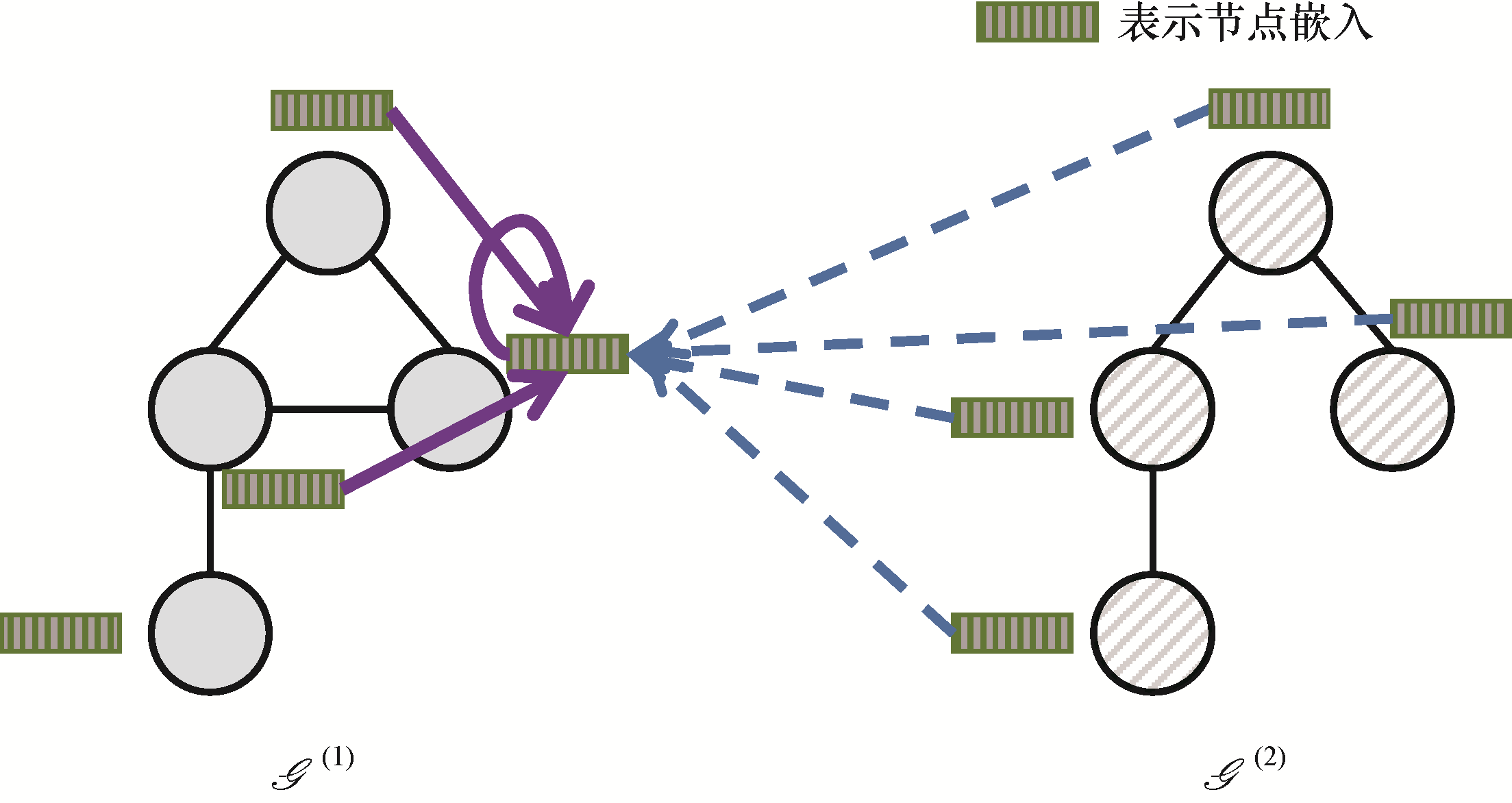


图13.2 对于左图中的一个节点，图内卷积网络只对自己的图（即中的紫色实线）进行操作。  
然而，跨图卷积网络既对自己的图（即中的紫色实线）进行操作，也对另一个图（即从中的  
所有节点到中的这个节点的蓝色虚线）进行操作

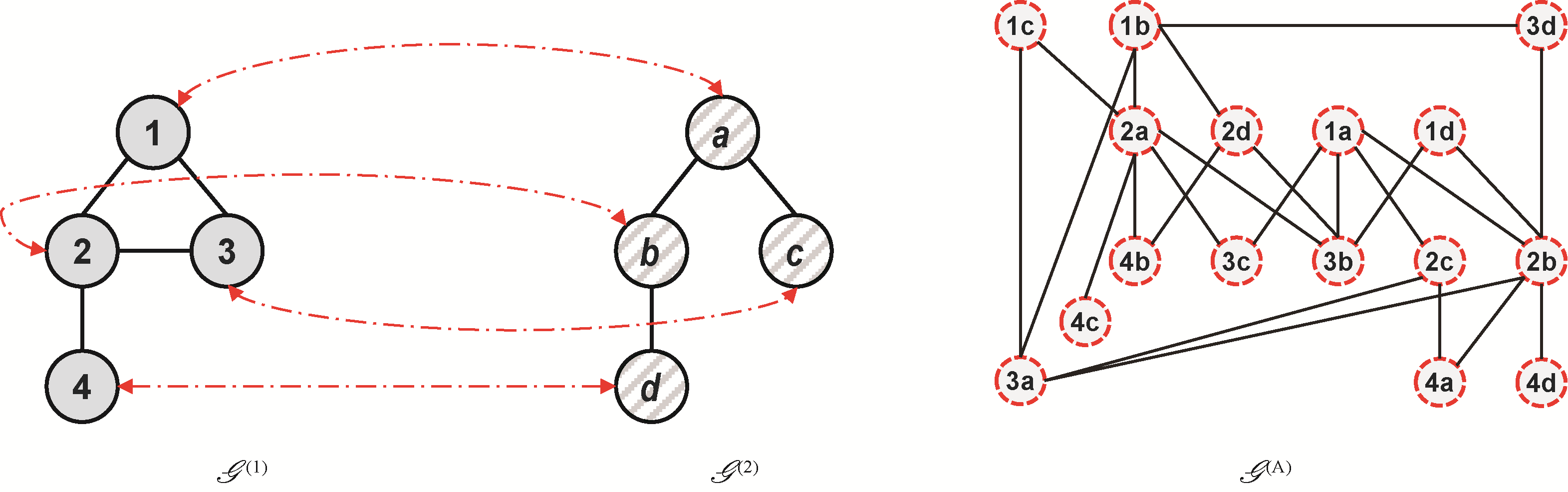


图13.3 通过一对图和建立分配图的示例说明

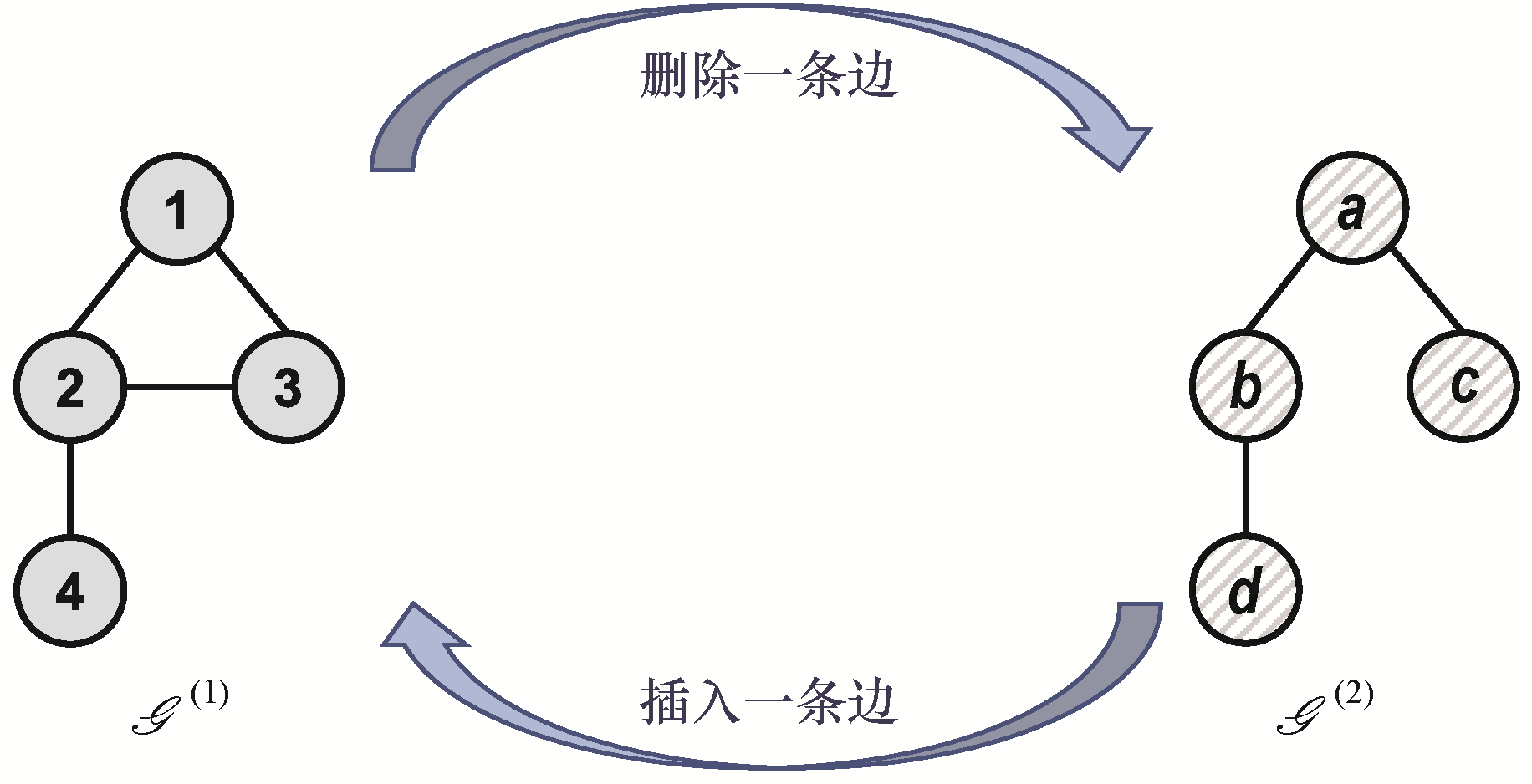


图13.4 计算和之间的GED。由于既可以通过删除边将转换为，  
也可以通过插入边将转换为，因此这两个图之间的GED为1

# 第14章　图结构学习

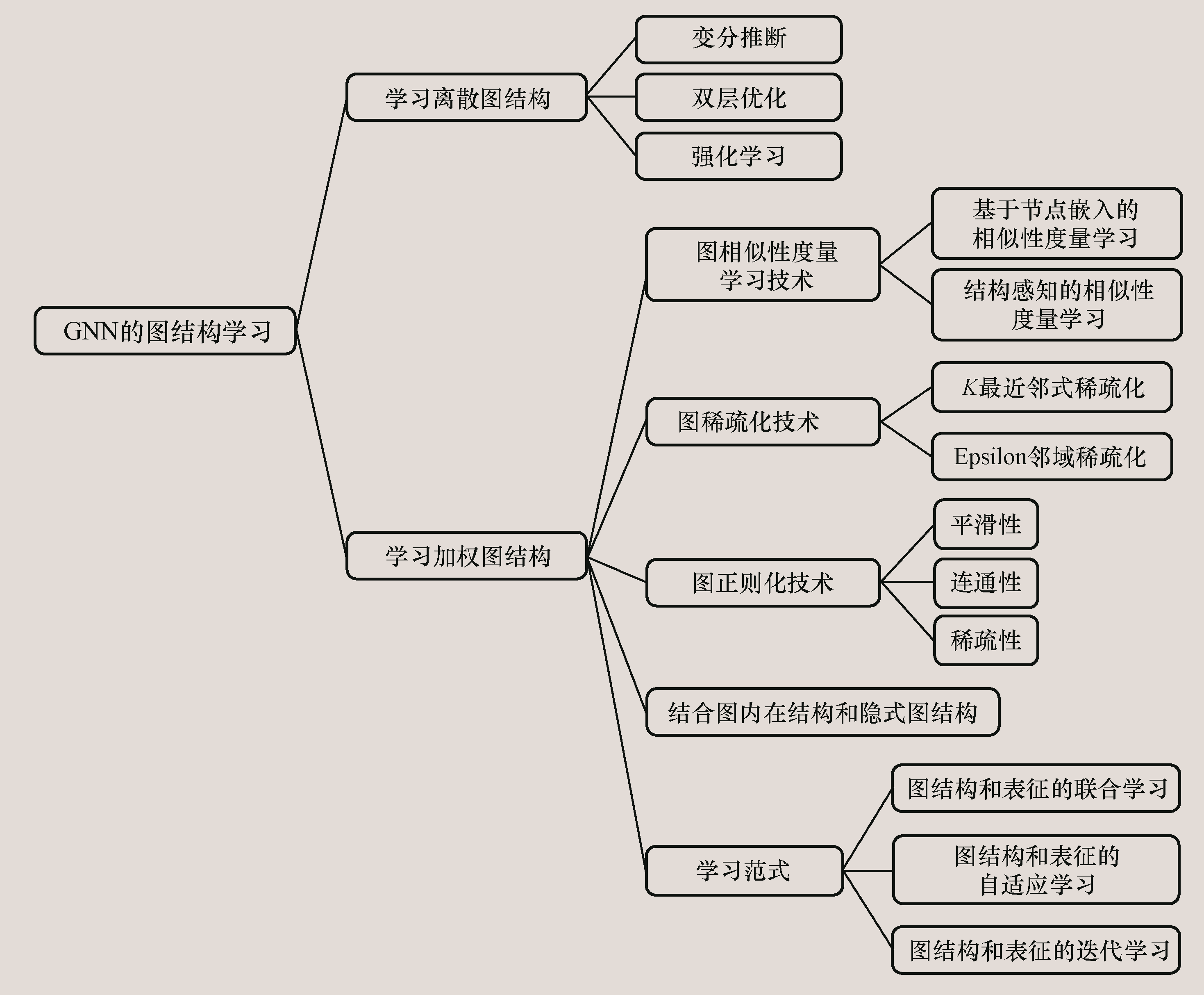


图14.1 GNN的图结构学习

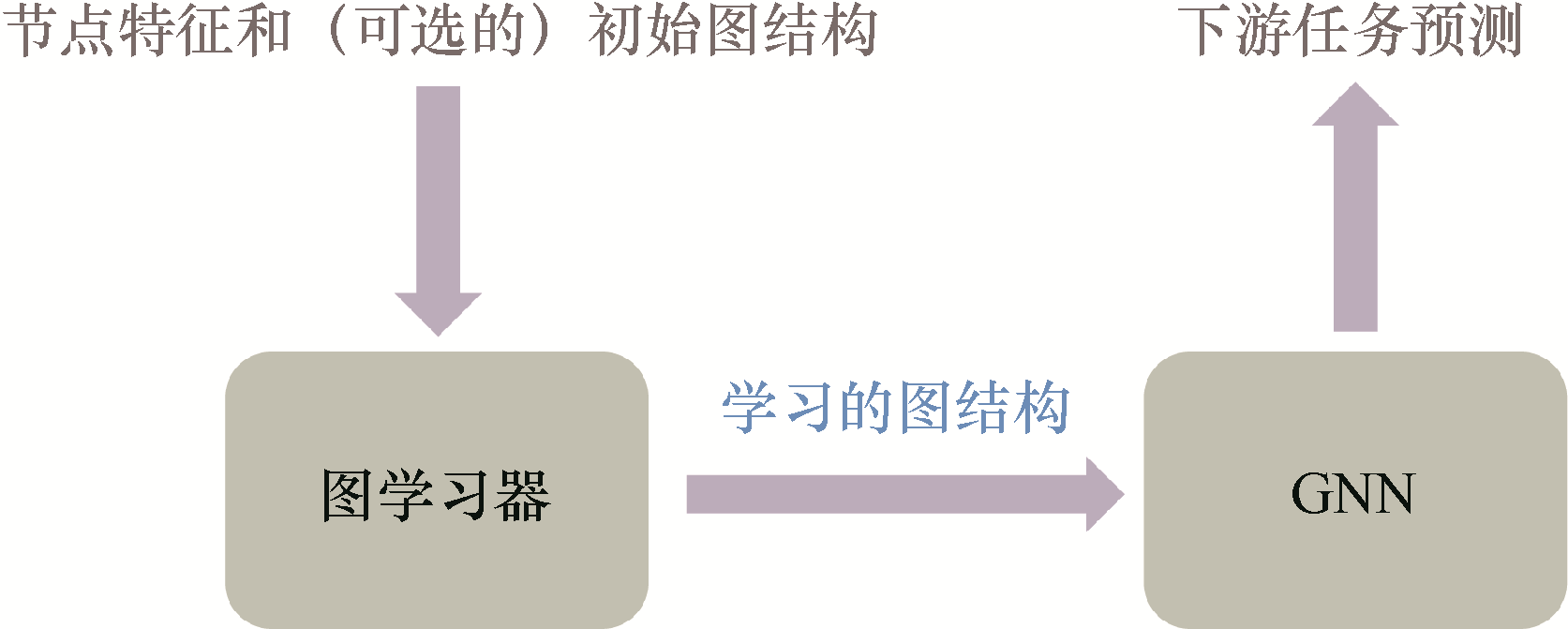


图14.2 联合学习范式

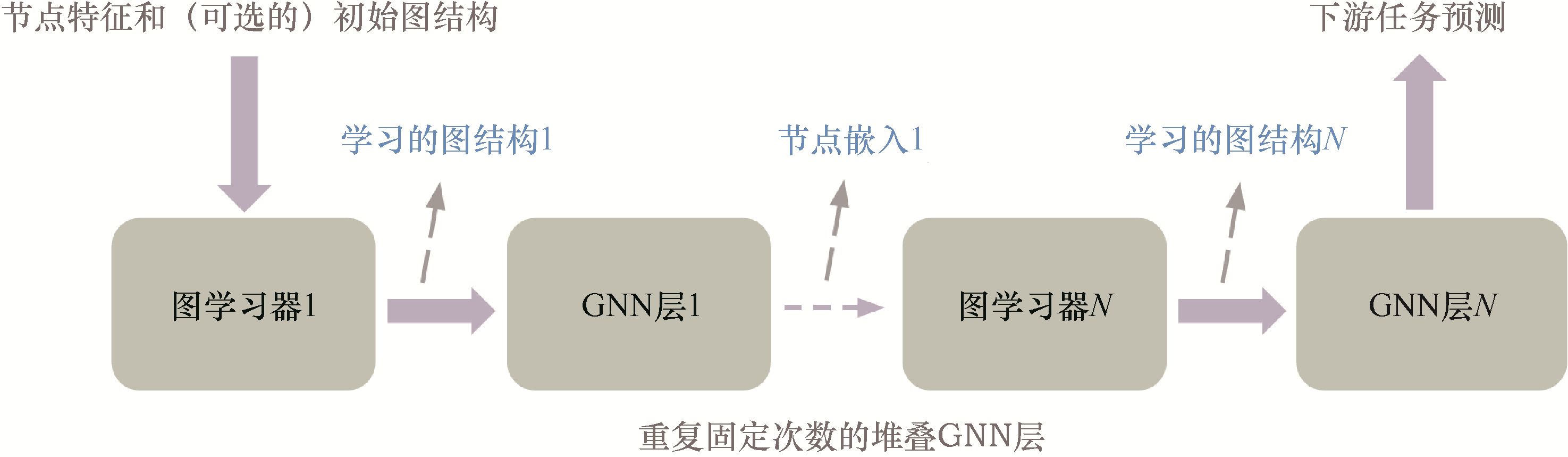


图14.3 自适应学习范式

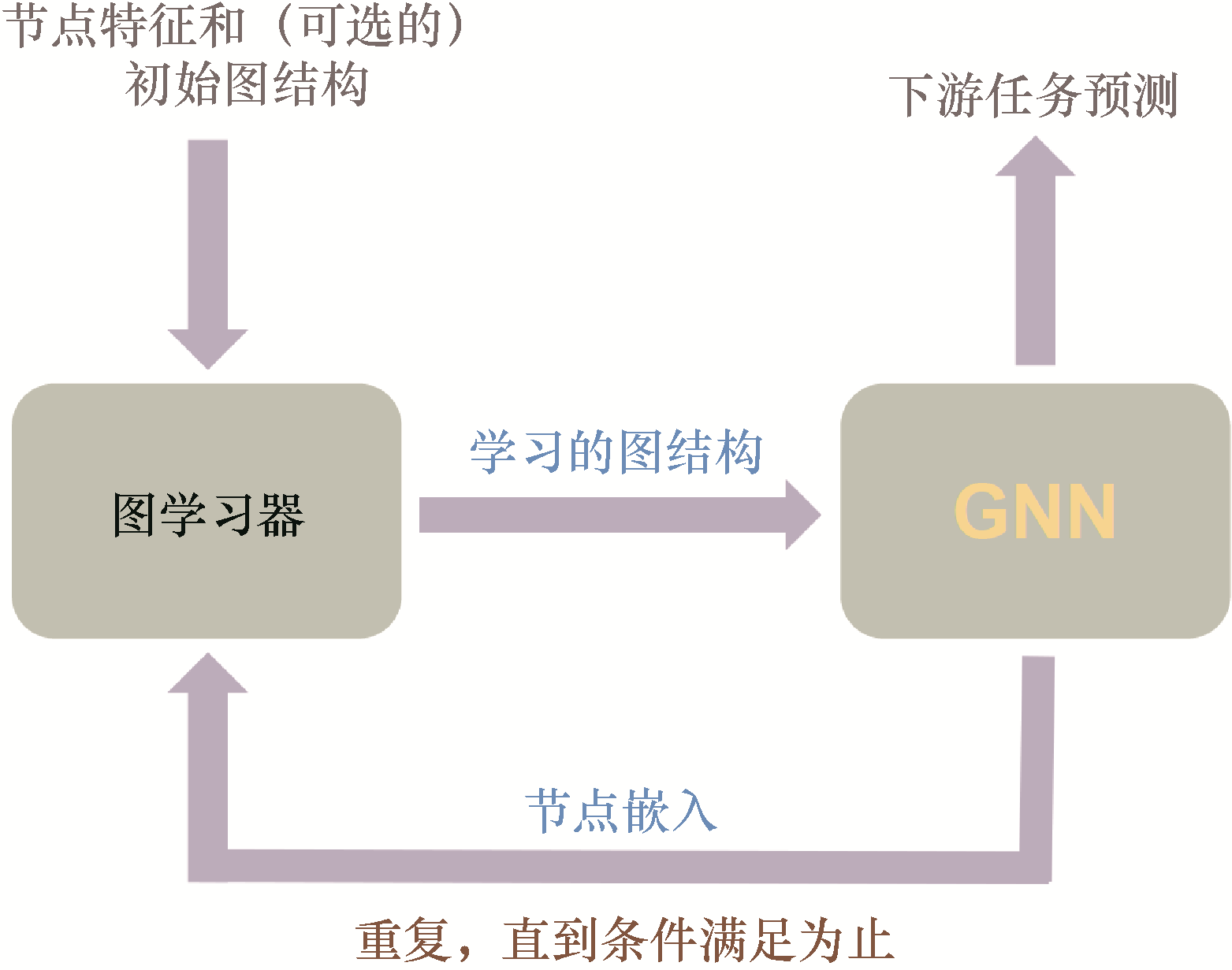


图14.4 迭代学习范式