

搜索神经网络集成模型的方法、装置和电子设备

- 5 本申请要求于 2021 年 11 月 22 日提交中国专利局、申请号为 202111387843.8、申请名称为“搜索神经网络集成模型的方法、装置和电子设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

- 10 本申请实施例涉及机器学习领域，尤其涉及一种搜索神经网络集成模型的方法、装置和电子设备。

背景技术

- 15 基于深度神经网络的模型在图像识别、语音识别和机器翻译等各种任务上取得了显著的进展。然而，单个深度模型的预测概率(softmax 概率)一般校准误差较大，置信度较低。尤其是在面对测试数据分布和训练数据分布不一致时(OOD 数据)，单个深度神经网络的拒识能力较弱，不能反映出准确的不确定性(uncertainty)，容易对错误的预测表现过度自信。这些问题大大限制了深度神经网络在高风险，高不确定性或涉及 OOD 数据的现实应用中的可靠性和鲁棒性。

- 20 其中，针对多分类问题，OOD 数据指来自与训练样本数据分布不同的测试样本。该不同可能是由于数据生成环境不同，或者是样本受到损坏或者扰动。以自动驾驶为例，如果训练数据采集来自于晴天而测试数据来自于雨雪天，或者训练数据来自于郊区而测试数据来自于城市，那么测试数据相比于训练数据就是 OOD (out-of-distribution)。针对该类数据，机器学习模型要具有拒识的能力。

- 25 基础学习器(base learner)是指集成模型组合中的单个模型。

集成模型(ensemble model)是通过将多个基础学习器的预测组合起来进行最终预测，形成一个更好的模型/预测。集成模型不但能达到更高的测试精度，而且还能拥有更好校准的预测概率，尤其是针对 OOD 数据能表现出更准确量化的不确定性和更高的鲁棒性。在深度神经网络模型上，集成模型也同样具有这些优势。

- 30 例如，深度集成模型(deep ensembles)通过将多个拥有相同网络架构但是不同的权重训练初始值(initialisation)的神经网络进行组合，将最终的预测输出(output logits)进行平均，能有效地提高测试精度和模型校准(model calibration)精度。

- 模型校准指让模型对事件结果的预测概率和事件的真实经验概率保持一致。例如在一个二分类的任务里，如果我们取出 100 张模型预测概率为 0.7 的图片，其中确实有 70 张图的真实标签为 1，则说明模型的预测概率和真实经验概率是一致的。换言之，模型的预测很准确可靠。在实际应用，尤其是高风险的应用中，机器学习模型的预测概率往往会被用于用户的判断或者决策制定，所以其预测的置信度非常重要。
- 35

集成模型的表现/性能往往取决于其组合中基础学习器的多样性：基础模型间的差异越大，集成效果往往更好，因此很多集成方法试图促进基础学习器间的多样性。如图 1 所示，深度集成模型通过改变基础学习器的训练初始权重来增加多样性；超参集成模型(hyper-deep ensemble)在改变初始权值的基础上又改变了训练的超参数，以此来进一步提高多样性。然而这些深度集成模型的基础学习器都共享同样的神经网络架构，所以一个非常自然的提高多样性的拓展就是使用不同架构的神经网络来组成集成模型(architecture ensemble)。

集成模型是由多个网络架构不同的深度神经网络的基础学习器组成的集成模型。

然而搜索由不同的网络架构组成的集成模型，复杂度远高于单个神经网络架构搜索(neural architecture search, NAS)，因为搜索集成模型不仅要搜索性能较好的基础学习器的网络架构，还要探索不同的基础学习器之间的可能组合的性能。所以现有的方法需要完整评估大量的神经网络架构来生成一个基础学习器候选池，并通过贪心算法来评估不同组合生成的集成模型的测试性能。导致了搜索集成模型需要耗费大量的计算成本和时间。

15

发明内容

为了解决上述的问题，本申请实施例提供了一种搜索神经网络集成模型的方法、装置和终端设备。

第一方面，本申请实施例提供了一种搜索神经网络架构集成模型的方法，所述方法包括：获取数据集，所述数据集包括分类任务中的样本和标注；使用神经网络架构分布搜索算法进行搜索，包括：确定神经网络架构分布的超参；在所述超参定义的架构分布中采样一个神经网络架构；根据所述分类任务中的样本和标注对所述神经网络架构训练和评估，得到性能指标；根据所述性能指标确定共享所述超参的神经网络架构分布，获得基础学习器的候选池；所述基础学习器为符合所述架构分布要求的神经网络架构；所述神经网络架构由神经网络架构单元重复堆叠而成；确定代理模型；所述代理模型用于预测未评估的神经网络架构的测试性能；通过代理模型预测所述候选池中基础学习器的测试性能，确定符合所述分类任务要求的 k 个基础学习器组成集成模型，所述集成模型的大小为 k 。以此，大大减少了对单个神经网络架构和单个集成模型的评估次数，从而在不降低搜索质量的同时显著降低了结构集成模型的难度和成本；针对的集成模型相较于单个深度神经网络模型更擅长拒识 OOD 数据，因此对于数据分布扰动(distributional shift) 更鲁棒。

作为一个可行的实施方式，所述使用神经网络架构分布搜索算法进行搜索，包括：使用基于学习算子概率分布的近似神经网络架构搜索(approximate neural architecture search via operation distribution, ANASOD)算法进行神经网络架构分布搜索。以此，可以对搜索空间中更大的部分进行遍历，极大地提升搜索效率。

作为一个可行的实施方式，所述确定神经网络架构分布的超参，包括：确定神经网络架构分布的超参为 ANASOD 编码；所述 ANASOD 编码为指示神经网络架构单元中各种算子的概率分布的向量，所述 ANASOD 编码和神经网络架构单元的映射是一对多。以此，可以通过算子概率分布对 NAS 问题进行的近似，极大地压缩搜索空间。

作为一个可行的实施方式，，所述确定神经网络架构分布的超参，包括：采用搜索策略优化神经网络架构分布的超参，所述搜索策略为贝叶斯优化，所述搜索策略用于在下一次迭代中采样到比当前的所述神经网络架构单元的性能指标更符合要求的神经网络单元。以此，每一次挑选和评估的都是超参定义覆盖下的架构分布，因此可以对搜索空间中更大的部分进行遍历，极大地提升搜索效率。

作为一个可行的实施方式，在所述超参定义的架构分布中采样一个神经网络架构，包括：根据所述 ANASOD 编码定义的算子概率分布，确定所述神经网络架构的组成单元中各个算子的具体数量；根据设定的搜索空间连接不同的算子来获得所述神经网络架构。以此可以获得一个符合超参定义的有效的架构，作为所有共享此 ANASOD 编码 θ 的神经网络架构分布的性能代理。

作为一个可行的实施方式，所述对所述神经网络架构单元在所述数据集上训练和评估，得到性能指标，包括：在训练数据集上训练所述神经网络架构；在验证数据集上评估所述神经网络架构，获得性能指标；所述训练集数据和验证集数据同属于所述数据集。以此，可以从每个架构分布中只采样和评估一个神经网络架构，并将其性能指标 y 作为所有共享此 ANASOD 编码 θ 的神经网络架构单元的性能指标，可以有效地避免重复评估相似架构单元性能带来的高额成本。

作为一个可行的实施方式，所述将所述使用神经网络架构分布搜索 (distributional NAS) 算法进行搜索，还包括：根据所述性能指标和所述超参确定所述神经网络架构分布的搜索策略。以此，调整搜索策略，确定下一次迭代中神经网络架构分布搜索的搜索策略，在下一次迭代中采样到比当前的所述神经网络架构单元的性能指标更符合要求的神经网络单元。

作为一个可行的实施方式，所述使用神经网络架构分布搜索 (distributional NAS) 算法进行搜索，还包括：根据每次搜索出来的神经网络架构分布的超参和性能指标确定其他未知分布的超参的性能预测值，包括均值和方差；根据所述均值和方差确定神经网络架构分布的性能预测策略，所述性能预测策略用于预测神经网络架构分布的性能指标。以此，可以根据性能预测值来更新性能预测策略 (θ_t , y_t)，从而确定下一次搜索策略。

作为一个可行的实施方式，所述根据所述性能指标确定共享所述超参的神经网络架构分布，获得基础学习器的候选池，包括：根据所述性能指标和所述超参确定所述神经网络架构分布的搜索策略；根据所述性能指标和所述神经网络架构单元确定所述神经网络架构分布的性能预测策略；根据所述搜索策略和性能预测策略，在共享所述超参的所述神经网络架构分布中搜索，确定基础学习器的候选池。以此，可以得到最优的神经网络架构分布，优质的架构分布能生成性能相近的优质神经网络架构，提供一个好的基础学习器候选池。

作为一个可行的实施方式，所述根据所述性能指标确定共享所述超参的神经网络架构分布，获得基础学习器的候选池，包括：根据历史搜索中的多个神经网络架构和对应性能指标输出多个共享所述超参的神经网络架构；根据所述多个共享所述超参的神经网络架构确定符合要求的神经网络架构分布；根据所述符合要求的神经网络架构分布，生成多个神经网络架构单元，获得基础学习器的生成分布/候选池。以此，用神

神经网络架构分布搜索的方法来学习候选池/架构分布，更高效，且大大减少了评估单个神经网络架构的次数和成本。

作为一个可行的实施方式，所述确定代理模型，包括：根据所述神经网络架构单元和所述性能指标通过在所述数据集上训练，获得所述代理模型。以此，可以通过代理模型来直接预测其他未评估的架构的性能，以避免巨大的评估成本。

作为一个可行的实施方式，所述通过代理模型预测所述候选池中基础学习器的测试性能，确定符合任务场景要求的 k 个基础学习器组成集成模型，包括：通过代理模型预测所述候选池中多个基础学习器的测试性能；根据预测结果进行区域搜索（local search），确定 q 个预估的顶点架构，所述预估的顶点架构为所述代理模型在验证集上预测的性能指标高于相邻架构的神经网络架构；将所述 q 个预估的顶点架构中性能指标符合要求的 k 个架构进行组合，得到集成模型。以此，可以从候选池中挑选出最优组合，将复杂度极高的排列组合问题难度降低，只需评估极少次基础学习器的组合就可以搜索出优质集成模型。

作为一个可行的实施方式，将所述 q 个预估的顶点架构中性能指标符合要求的 k 个架构进行组合，包括：将 q 个预估的顶点架构的性能指标由优到劣排序，取性能指标位于前面的 k 个架构进行组合。以此，可以从候选池中挑选出最优组合，将复杂度极高的排列组合问题难度降低，只需评估极少次基础学习器的组合就可以搜索出优质集成模型。

作为一个可行的实施方式，将所述 q 个预估的顶点架构中性能指标符合要求的 k 个架构进行组合，包括：使用贪心算法（greedy selection algorithm），遍历 q 个预估的顶点架构，依此选取添加 k 个架构进入集成模型。以此，可以从候选池中挑选出最优组合，将排列组合的可能性和复杂度大大降低（从候选池的所有基础学习器中挑选 k 个减少到从 q 个基础学习器中挑选 k 个），只需评估极少次基础学习器的组合就可以搜索出优质集成模型。

第二方面，本申请实施例提供一种搜索神经网络架构集成模型的装置，所述装置包括：数据获取模块，用于获取数据集，所述数据集包括分类任务中的样本和标注；架构分布搜索模块，用于使用神经网络架构分布搜索算法进行搜索，包括：用于确定神经网络架构分布的超参；在所述超参定义的架构分布中采样一个神经网络架构；根据所述分类任务中的样本和标注对所述神经网络架构训练和评估，得到性能指标；根据所述性能指标确定共享所述超参的神经网络架构分布，获得基础学习器的候选池；所述基础学习器为符合所述架构分布要求的神经网络架构；所述神经网络架构由神经网络架构单元重复堆叠而成；确定代理模型；所述代理模型用于预测未评估的神经网络架构的测试性能；架构集成模型组合模块，用于通过代理模型预测所述候选池中基础学习器的测试性能，确定符合所述分类任务要求的 k 个基础学习器组成集成模型，所述集成模型的大小为 k 。

第三方面，本申请实施例提供一种电子装置，包括处理器和存储器；所述处理器用于执行所述存储器所存储的计算机执行指令，所述处理器运行所述计算机执行指令执行第一方面任意实施例所述的基于演化学习的神经网络结构搜索的方法。

第四方面，本申请实施例提供一种存储介质，包括可读存储介质和存储在所述可

读存储介质中的计算机程序，所述计算机程序用于实现第一方面任意一实施例所述的基于演化学习的神经网络结构搜索的方法。

附图说明

5 为了更清楚地说明本说明书披露的多个实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书披露的多个实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

下面对实施例或现有技术描述中所需使用的附图作简单地介绍。

10 图 1 为第一方案的集成模型搜索方法流程图；

图 2 为本申请实施例提供的系统架构图；

图 3 为本申请实施例提供的搜索神经网络集成模型的方法应用于图片分类场景的示意图；

15 图 4 为本申请实施例提供的搜索神经网络集成模型的方法应用于目标检测识别场景的示意图；

图 5 为本申请实施例提供的搜索神经网络集成模型的流程框图；

图 6 为包括本申请提供的 DistriNAS-PM 在内的各个基准在 CIFAR10 上取得的测试误差对比曲线图；

20 图 7 为随机选择添加到 CIFAR10 和 CIFAR100 验证集图片上的 15 种干扰/噪音方式示意图；

图 8 为随机选择添加到 CIFAR10 和 CIFAR100 验证集图片上的干扰/噪音后的效果图；

图 9 为在 NAS-Bench-201 空间上本申请提供的 DistriNAS-PM 与其他搜索方法的 OOD 验证比较示意图；

25 图 10 为一种电子设备示意图。

具体实施方式

30 在以下的描述中，涉及到“一些实施例”，其描述了所有可能实施例的子集，但是可以理解，“一些实施例”可以是所有可能实施例的相同子集或不同子集，并且可以在不冲突的情况下相互结合。

在以下的描述中，所涉及的术语“第一\第二\第三等”或模块 A、模块 B、模块 C 等，仅用于区别类似的对象，不代表针对对象的特定排序，可以理解地，在允许的情况下可以互换特定的顺序或先后次序，以使这里描述的本申请实施例能够以除了在这里图示或描述的以外的顺序实施。

35 在以下的描述中，所涉及的表示步骤的标号，如 S110、S120……等，并不表示一定会按此步骤执行，在允许的情况下可以互换前后步骤的顺序，或同时执行。

除非另有定义，本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同。本文中所使用的术语只是为了描述本申请实施例的目的，不是旨在限制本申请。

下面将结合附图，对与本申请实施例相关的技术方案进行描述。

第一方案如图 1 所示，采用随机搜索（random search, NES-RS）或者进化算法（evolutionary algorithm, NES-RE）来搜索适合作为基础学习器的架构，从而搭建一个足够大的基础学习器的候选池，然后采用贪心算法（greedy selection algorithm, GSA）来遍历候选池中的基础学习器，逐个挑选组成最终集合的成员。

其中，随机搜索算法是以目标函数和基础学习器候选池大小 n_{pool} 为输入，在 NAS 搜索空间中随机采样 n_{pool} 个架构单元，并对每个架构单元进行完整训练和性能评估获得其指标，输出为基础学习器候选池。

进化算法是以目标函数和基础学习器候选池大小 n_{pool} 为输入，在 NAS 搜索空间中随机采样 n_{init} 个架构单元，并对每个架构单元进行完整训练和性能评估获得其指标。将性能指标最好的 n_{parent} 个架构单元作为父代单元。在达到终止标准前迭代执行：从父代单元中随机采样 B 个架构单元，将其进行随机变异获得 B 个子代架构单元；对这个 B 个子代架构单元进行完全训练和性能评估；遍历这 B 个子代架构单元，从中挑选出能组成最大优化目标函数的集成模型的架构单元，将其加入父代架构单元池，并将最旧的父代架构单元去除以保证父代架构单元池大小不变仍然为 n_{parent} 。输出为基础学习器候选池。

贪心算法是以基础学习器候选池和架构集成大小 k 为输入；初始化架构集成，将其设为候选池中测试误差最低的神经网络架构，并将此架构从候选池中去除，在架构集成大小小于 k 前迭代执行：遍历候选池中剩余的基础学习器，逐个将其添加到现有的架构集成中，评估新的架构集成的性能；选择能导致最大性能提升的架构加入现有的架构集成中，并将此架构从候选池中去除。输出为最终集成模型。

此方法采用了传统 NAS 的思维，将架构搜索空间中的每一个神经网络架构都看做是一个单一的个体，所以被选入候选池的每一个神经网络架构/基础学习器都需要经过完整训练和评估。而此类方法的架构搜索一般需要一个含有几百个神经网络架构的候选池，导致搭建候选池这一环节就需要极高的评估成本。

在从候选池中寻找最优的基础学习器组合/架构集成时，使用的贪心算法虽然能将原本高复杂度的排列组合问题大大简化，却依然需要评估大量可能的架构组合/架构集成，导致集成挑选这一环节又增加了很多评估成本。

因此此类搜索方法需要花费高昂的图形处理单元（graphics processing unit, GPU）时间和算力成本，才能找到高质量的集成模型。对于 GPU 时间和硬件资源的巨大要求往往限制了其在实际场景中的应用。

GPU 时间（GPU time）是一个常见的衡量算法计算量的单位，为完成某任务单个 GPU 需运行的时间，具体表达为 GPU-天数（GPU-days），GPU-秒数（GPU-seconds）等。

现有的自动搜索集成模型的方法搜索成本巨大，搜索效率低下。其根本原因是它们需要先构建一个足够大的基础学习器候选池，然后尝试候选池中基础学习器的多种组合来找到最优的集成模型。而构建一个足够大的基础学习器候选池需要完整训练及评估大量的神经网络架构，因为采用传统 NAS 的方法以单个神经网络架构作为搜索目标，很多极为相似的神经网络架构也需要被单独训练和评估。从候选池中基础学习器

的多种组合找到最优的集成模型则需要评估众多可能的架构组合，虽然使用贪心算法可以将 NP-难度的排列组合问题大大简化，但是需要评估的组合数量依然和候选池中基础学习器的数量以及集成模型的规模成正比。

下面将结合本申请实施例中的附图，对与本申请实施例的技术方案进行描述。

5 在现有的神经网络架构搜索空间中，集成模型具有以下特性：集成模型的性能取决于集成中基础学习器的平均性能；在保证平均性能优异的前提下，基础学习器之间的差异即集成的多样性越大，集成模型的性能越好；神经网络架构搜索空间中的顶点架构的预测输出差异相对较大，由顶点架构组成的集成模型具有较高的多样性。其中，顶点架构是指测试精度高于其直接相邻的其它架构的测试精度的架构。

10 基于以上集成模型的特性，本申请实施例提供一种搜索神经网络集成模型的方法使用神经网络架构分布搜索（distributional NAS）确定生成基础学习器的架构分布或候选池。根据生成基础学习器的架构分布或候选池，通过代理模型(surrogate model)来预测候选池中最优的神经网络顶点架构，将这些顶点架构进行组合，获得集成模型。

15 需要理解的是，神经网络架构分布搜索将架构相似或属于同一分布的神经网络整合起来进行评估，从而避免反复多次评估单个神经网络架构，大大提高搜索效率。同时，从最终找到的架构分布中生成的基础学习器都具有比较接近且优异的平均性能，从而满足了集成模型的性能取决于集成模型中基础学习器的平均性能的要求。

本申请实施例提供一种搜索神经网络集成模型的方法采用更高效的基础学习器候选池生成方案和基础学习器组合方案，能够降低集成模型搜索成本，在保证性能的前提下，大大提高集成模型的搜索成本，使得在更大的搜索空间中搜索集成模型的成本可控可接受，适用于更多的实际生产场景下。

25 代理模型通常是一种简单模型，用于模拟过于复杂或者黑盒的实际问题，也可用于快速预测黑盒或者过于复杂的问题的输出。代理模型能快速且相对准确地预测神经网络架构的测试性能，从而避免了大量的训练和评估来获取它们的真实性能。基于神经网络架构搜索空间中的顶点架构的预测输出差异相对较大，而由顶点架构组成的集成模型具有较高的多样性，将这些顶点架构进行组合，能保证集成模型的多样性，避免多次尝试不同架构组合来生成的集成模型的评估成本。

30 因为集成模型的性能主要取决于其基础学习器的平均性能和多样性，本申请实施例提供一种搜索神经网络集成模型的方法在减少评估次数的同时，针对性地保证了集成模型的上述特性，从而使得用户能高效地搜索到高性能的集成模型。

图 2 为本申请实施例提供的系统架构图。本申请实施例提供一种搜索神经网络集成模型的方法可广泛应用于各种需要使用卷积神经网络的系统架构和场景。如图 3 所示，数据收集设备 10 通过各种途径获得所需要的数据或样本，并向计算设备 11 提供数据。本申请实施例提供的搜索神经网络集成模型的方法将在计算设备 11 上运行，进行神经网络架构的搜索和对最终搜索出的架构进行训练，并将训练后的集成模型部署到各种应用场景的设备上，如个人计算机 12，服务器 13 和移动设备 14 等。

图 3 为本申请实施例提供的搜索神经网络集成模型的方法应用于图片分类场景的示意图。如图 3 所示，用户经常在智能手机或者其他多媒体储存设备的用户相册中存储大量图片，而根据图片内的信息对它们进行分类可以帮助用户管理与查找。本申请

实施例提供的搜索神经网络集成模型的方法可以快速地在相似的图片分类任务上预先搜索并训练出最适合的卷积神经网络的集成模型部署在智能手机上，以替代常见的人类专家手动设计的网络模型，从而达到更高的分类准确率，提升用户的使用体验。

图 4 为本申请实施例提供的搜索神经网络集成模型的方法应用于目标检测识别场景的示意图。如图 4 所示，应用本申请实施例提供的搜索神经网络集成模型的方法搜索到的集成模型，可以识别原有图片上的物体目标，输出带标记的目标检测后的图片。对图像或视频中物体目标的检测识别广泛应用于智慧城市、自动驾驶等任务中。与图 3 的应用场景相似，本申请实施例提供的搜索神经网络集成模型的方法可以针对于各种目标和限制，如移动设备的硬件限制，找到针对于各种场景中物体检测识别任务中最合适的神经网络骨架（neural network backbone），部署在相关设备上以提升识别精度。

本申请实施例提供的搜索神经网络集成模型的方法还适用于医学影像的图片分类情景。机器学习系统现已应用于医学影像方面帮助医护人员通过影像学资料进行诊断。经过已有数据的训练，通过本申请实施例提供的搜索神经网络集成模型的方法搜索到的卷积神经网络集成模型，不仅可以根据影像的特征高效且高精度地进行分类诊断，同时由于集成模型对预测的不确定性拥有较好的校准，也可以输出对其诊断的置信度，帮助医生筛选需要人工确认的案例。

本申请实施例提供的搜索神经网络集成模型的方法，可以部署在相关设备的计算节点上。其数据与代码可以储存在各种计算机中各种常见的储存器上。对于指令和功能模块的执行，除性能评估以外的步骤一般可以由中央处理器（central processing unit, CPU）执行。而性能评估涉及到对神经网络架构的训练，一般由图形处理单元（graphics processing unit, GPU）执行。本申请实施例提供的搜索神经网络集成模型的方法获得的集成模型在训练之后可以部署在各种计算机和移动计算设备上，应用于图片分类、目标检测识别和医学影像的图片分类等各种需要卷积神经网络预测的任务中。

本申请实施例提供的搜索神经网络集成模型的方法，该方法包括：获取数据集，数据集包括分类任务中的样本和标注；使用神经网络架构分布搜索（distributional NAS）算法进行搜索，包括：确定神经网络架构分布的超参；在超参定义的架构分布中采样一个神经网络架构；根据分类任务中的样本和标注对神经网络架构训练和评估，得到性能指标；根据性能指标确定共享超参的神经网络架构分布，获得基础学习器的候选池；基础学习器为符合架构分布要求的神经网络架构；神经网络架构由神经网络架构单元重复堆叠而成；确定代理模型（surrogate model）；代理模型用于预测未评估的神经网络架构的测试性能；通过代理模型预测候选池中基础学习器的测试性能，确定符合分类任务场景要求的 k 个基础学习器组成集成模型，集成模型的大小为 k 。

本申请实施例中会涉及两方面的评估：1）对于单个神经网络架构即基础学习器的评估包括了在训练数据集上从头开始训练该神经网络架构，并在训练结束后，在验证数据集上测评其测试精度等表现。2）对于单个集成模型的评估，在验证数据集上测评整个集成模型的表现。其中，评估次数（number of evaluations）是一个常见的衡量算法计算成本的指标。

图 5 为本申请实施例提供的搜索神经网络集成模型的方法的流程框图。下文将结

合图 5 详细解释本申请实施例提供一种搜索神经网络集成模型的方法中的每一步骤。如图 5 所示, 本申请实施例提供一种搜索神经网络集成模型的方法, 执行以下步骤 1-5 进行神经网络架构分布搜索获得基础学习器的候选池。

步骤 1, 获取数据集。

- 5 在一个可以实现的实施方式中, 获取已有的数据和目标任务对应的数据。

示例性地, 可以从现有的数据集或其他人工标注的数据中获得图片分类任务中一定数量的图片和其正确的标注作为样本 (ground truth)。可以将这些数据作为训练数据集和/或测试集数据。

步骤 2, 确定架构搜索空间。

- 10 在一个可以实现的实施方式中, 通过定义搜索空间和目标函数, 确定备选神经网络架构的形态和神经网络架构搜索的目标。

其中, 一种常见的搜索空间是基于神经网络架构单元 (neural architecture cell) 定义的, 包括定义搜索神经网络架构单元中算子的数量、可供选择算子的类型、各个算子之间最大连接数量以及最终神经网络架构中神经网络架构单元堆叠的次数。

- 15 示例性地, 可以定义一个 NAS 搜索空间为: 一个神经网络架构单元 a 中算子的数量为 10, 可供选择算子的类型有 3 种: A、B、C; 各个算子之间最大连接数量为 i 个, 神经网络架构单元堆叠的次数为 j 次。

- 目标函数视目标任务而定义。常见的目标函数为最大化任务精度, 示例性地, 可以定义图片分类问题中验证集上的准确率为目标函数。目标函数也可以包括其他的限制和目标, 示例性地, 定义在最大化图片分类准确率的前提下最小化神经网络的每秒浮点运算量 (floating-point operations per second, FLOPs) 为目标函数, 以应用于算力受限的移动设备。

- 本申请实施例提供的搜索神经网络集成模型的方法使用神经网络架构分布搜索 (distributional NAS) 算法进行搜索, 确定架构搜索空间为神经网络架构分布搜索 (distributional NAS) 的搜索空间。该神经网络架构分布分布的搜索空间在定义 NAS 搜索空间的同时定义架构分布的超参, 以确定各个算子在神经网络架构单元中出现的分布概率。

- 30 在一个可以实现的实施方式中, 神经网络架构分布搜索 (distributional NAS) 算法可以采用基于学习算子概率分布的近似神经网络架构搜索 (approximate neural architecture search via operation distribution, ANASOD) 算法进行神经网络架构分布搜索, 在定义 NAS 搜索空间的同时, 定义对应的 ANASOD 的编码 θ 为架构分布的超参。

- 35 在一个可以实现的实施方式中, 可以定义 ANASOD 的搜索空间为: 每一个神经网络架构单元 a 对应的编码 θ 是一个位于 k 维单纯形空间 (simplex space) 的向量, 向量中的每个值为每种算子在神经网络架构单元 a 中出现的概率。

示例性地, 一个常规的神经网络架构单元有 10 个算子, 可供选择算子的类型有 3 种: A、B 和 C, 其中 A 在神经网络架构单元中出现 5 次, B 在神经网络架构单元中出现 2 次, C 在神经网络架构单元中出现 3 次, 则神经网络架构单元对应的编码 θ 为: [0.5, 0.3, 0.2]。

编码 θ 和神经网络架构单元的映射是一对多的，多个相似的神经网络架构单元共享同一个编码 θ ，从而极大地压缩搜索空间。例如以下神经网络架构单元共享同一个编码 θ 。

神经网络架构单元 1: A-A-A-A-A-B-B-B-C-C

5 神经网络架构单元 2: A-A-A-A-B-A-B-B-C-C

神经网络架构单元 3: A-A-A-B-B-A-A-B-C-C

以上 3 个神经网络架构单元仅仅是共享编码 $\theta=[0.5, 0.3, 0.2]$ 的多个相似的神经网络架构单元中的一部分，其他的通过排列组合得到的相似的神经网络架构单元不在一一枚举。

10 与此同时，在 NAS 搜索空间中，拥有相同 ANASOD 编码 θ 的不同神经网络架构单元的在测试集上的测试精度表现往往极为相似，说明仅通过算子分布概率对 NAS 问题进行的近似是较为精确的。

可以理解的是，通过对现有的 NAS 搜索空间进行分析可知：搜索一个算子类型、数量和拓扑结构都已完全确定的精确解是不必要的。与之相反，一组具有相同算子类型和数量、相同的算子概率分布但拓扑结构不同的神经网络架构单元具有非常相似的性能表现。据此，将 ANASOD 编码 θ 定义为神经网络架构单元中各种算子的分布概率的向量，神经网络架构单元中各种算子的概率分布之和为 1。

20 与 NAS 中庞大的排列组合原有搜索空间不同，ANASOD 编码 θ 位于更易优化且更小的向量空间。基于此，可以在编码 θ 对应的搜索空间中使用一系列近似 NAS 算法的 ANASOD 算法，在基本保持搜索精度不受影响的情况下大大减少了搜索难度并提升了搜索效率。因为一个低维编码 θ 可对应一组多个近似的神经网络架构单元，ANASOD 算法可以直接搜索多个近似的神经网络架构单元应用于集成模型。

本申请实施例提供的神经网络架构集成模型搜索方法也可以采用其他的神经网络架构分布搜索方法。

25 步骤 3，采用搜索策略推荐新的神经网络架构分布的超参，以确定神经网络架构分布的超参。

在一个可以实现的实施方式中，搜索策略可以为贝叶斯优化，采用贝叶斯优化来推荐新的架构分布的超参。示例性地，可以采用贝叶斯优化推荐新的 ANASOD 的编码 θ ；还可以采用进化算法推荐新的神经网络架构分布的超参。

30 示例性地，搜索策略可以表示为：搜索策略 (θ, y) ；其中 θ 为贝叶斯优化模型推荐的 ANASOD 的编码/超参， y 为预测的神经网络架构分布的性能指标。其意义可以这样解读：搜索 ANASOD 的编码 θ 覆盖下的，预测的性能指标为 y 的神经网络架构分布。

35 用于预测神经网络架构分布的性能指标的性能预测模型可以是高斯过程 (gaussian process)、贝叶斯神经网络 (Bayesian neural network)、随机森林(random forest)等。

本申请实施例提供的采用搜索策略推荐新的神经网络架构分布的超参与第一方案的集成模型搜索方法完全不同；第一方案使用 NAS 的方法搜索适合成为集成模型基础学习器的候选架构，每次搜索策略直接推荐一个新的神经网络架构单元。而在本申请实施例提供的步骤 3 中每一次挑选和评估的都是超参定义覆盖下的架构分布，因此可

以对搜索空间中更大的部分进行遍历，极大地提升搜索效率。

步骤 4，在超参定义的架构分布中随机采样一个神经网络架构，进行性能评估，得到性能指标。

- 5 在一个可以实现的实施方式中，在采用 ANASOD 优化/搜索架构分布 (θ, a, y) 时，从 θ 定义的架构分布中搜索和训练一个神经网络架构 a ，对其进行性能评估，并将其性能指标 y 作为拥有相同 ANASOD 编码 θ 的神经网络架构分布共同的性能指标。

在一个可以实现的实施方式中，步骤 4 包括：

步骤 41，在超参定义分布中随机采样一个神经网络架构。

- 10 在一个可以实现的实施方式中，在 ANASOD 的编码空间中，根据 ANASOD 编码 θ 定义的神经网络架构单元中的算子分布概率，确定神经网络架构单元中各个算子的具体数量；根据搜索空间的限制，随机连接不同的算子来获得神经网络架构单元；在确定神经网络架构单元后，根据搜索空间的定义堆叠该神经网络架构单元数次，得到神经网络架构 a 。在确定神经网络架构 a 中算子的分布概率符合 ANASOD 编码 θ 后，使用神经网络架构 a 作为所有共享此 ANASOD 编码 θ 的神经网络架构分布的性能代理。

- 15 步骤 42，对神经网络架构 a 在数据集上训练和评估，得到性能指标。

在一个可以实现的实施方式中，可以在步骤 1 获得的训练数据集上，根据分类任务中的样本和标注按照常规的神经网络优化方法训练该神经网络架构 a ，并根据步骤 2 中定义的目标函数在验证集上评估并获得其性能指标 y 。该过程可以表示为性能评估 (y, a) 。训练集数据和验证集数据属于同一分布，同属于一个数据集。

- 20 在一个可以实现的实施方式中，可以根据性能评估 (y, a) 进行神经网络架构分布的性能评估，将其性能指标 y 作为所有共享此超参 θ 的架构分布的性能指标。

- 25 由于同一架构分布生成的不同神经架构单元最终性能表现极为相似，因此在优化/搜索架构分布时，从每个架构分布中只采样和评估一个神经网络架构，并将其性能指标 y 作为所有共享此 ANASOD 编码 θ 的神经网络架构单元的性能指标，可以有效地避免重复评估相似架构单元性能带来的高额成本。

步骤 5，根据性能指标 y 更新搜索策略；在更新搜索策略的同时根据搜索历史输出目前最优的神经网络架构分布；更新神经网络架构性能代理模型。目前最优的神经网络架构分布为符合要求的神经网络架构分布。

- 30 在一个可以实现的实施方式中，可以根据性能指标和超参确定神经网络架构分布的搜索策略，使其在下一次迭代中搜索到更高性能指标的神经网络架构单元。包括以下步骤：

步骤 51，根据超参和性能指标更新搜索策略 (θ_t, y_t) ，确定搜索策略。 t 为迭代次数。

- 35 示例性地，根据每次搜索出来的神经网络架构分布的超参 θ_t 和性能指标 y_t 调整搜索策略，确定下一次迭代中神经网络架构分布搜索的搜索策略。

步骤 52，根据性能指标和神经网络架构分布的超参确定神经网络架构分布的性能预测策略。

在一个可以实现的实施方式中，可以根据每次搜索出来的神经网络架构分布的超参 θ_t 和性能指标 y_t 更新性能预测策略 (θ_t, y_t) ，从而确定神经网络架构分布

的性能预测策略。

示例性地，将每次搜索出来的神经网络架构分布的超参 θ_t 和其性能指标 (θ_t, y_t) 输入性能预测模型，可以输出其他未知分布的超参的性能预测值，包括均值(mean) m 值和方差(variance) v 值：

- 5 第 t 次的性能预测值 $(m, v) = \text{性能预测模型}(\theta | \{\theta_i, y_i\}_{i=1, 2, \dots, t})$ 。
其中， θ 是未知的超参数值， $\{\}$ 部分指的是搜索评估过的超参历史。

步骤 53，根据性能预测值来更新性能预测策略，从而确定下一次的评估目标 $(\theta_{(t+1)}, y_{t+1})$ 。

步骤 54，根据搜索历史输出目前最优的神经网络架构分布。

- 10 在一个可以实现的实施方式中，根据历史搜索中的多个神经网络架构分布和对应性能指标确定符合要求的神经网络架构分布。

示例性地，搜索历史有 3 个架构分布的超参及其性能： (θ_1, y_1) 、 (θ_2, y_2) 、 (θ_3, y_3) ，其中 (θ_2, y_2) 的性能指标 y_2 为最优，则共享超参 θ_2 的架构分布为符合要求的神经网络架构分布。

- 15 步骤 55，根据符合要求的神经网络架构分布，生成多个神经网络架构单元，获得基础学习器的生成分布/候选池。

在一个可以实现的实施方式中，可以根据 S54 输出的最优的神经网络架构分布，随机生成众多具体的神经网络架构，获得基础学习器的生成分布/候选池。其中最优的神经网络架构分布为符合要求的神经网络架构分布。

- 20 步骤 56，确定代理模型，代理模型用于预测未评估的神经网络架构的测试性能，以帮助预测和辅助搜索最优的顶点架构，从而快速生成高质量的集成模型。

在一个可以实现的实施方式中，可以根据 t 次搜索过程中评估过的神经网络架构单元和性能指标训练和更新代理模型。

- 25 在一个可以实现的实施方式中，代理模型可以为基于 weisfeiler-lehman 图核的高斯过程 (gaussian process with WL graph kernel, GPWL)，示例性地， $y = \text{GPWL 模型}(a | \{a_i, y_i\}_{i=1, 2, \dots, t})$ ，其中其中， a 是未知的神经网络架构， y 是代理模型预测的架构性能， $\{\}$ 部分指的是搜索评估过的神经网络架构历史。

- 30 根据神经网络架构分布搜索 (distributional NAS) 的工作以及实验验证，优质的架构分布往往能生成性能相近的优质神经网络架构。因此，对于集成模型搜索，一个好的架构分布很自然地提供了一个好的基础学习器候选池。相较于现有技术使用传统 NAS 来迭代评估单个神经网络架构后添加到候选池中，本申请实施例提出的用神经网络架构分布搜索的方法来学习候选池/架构分布，更高效，且大大减少了评估单个网络架构的次数和成本。

- 35 集成模型的效果不仅仅取决于基础学习器的性能，还取决于其组合中基础学习器的多样性。因此直接将性能最优的 k 个基础学习器组合起来，未必能生成最优的集成模型。而从候选池中挑选出大小为 k 的最优组合，是一个复杂度极高的排列组合问题。

第一方案中的集成模型搜索主要通过贪心算法来逐个选择组合中的基础学习器，但是这种方法需要评估的集成模型的数量和候选池大小以最终集成模型的大小成正比。

根据之前集成模型的研究以及进一步的实验分析，可以发现在基础学习器的平均

性能保证的前提下，组成集成模型的学习器之间的预测差异越大，集成模型的性能越好。而搜索空间中的顶点架构之间的预测差异往往较大。因此将 k 个最好的顶点架构组合能自然地保证集成模型的多样性，生成性能优异的架构集成。而要找到真正的顶点架构需要遍历评估搜索空间中所有的神经网络架构。

- 5 本申请实施例的搜索神经网络集成模型的方法执行如下步骤 6 进行架构采样和搜索架构集成，只需评估极少次（甚至 1 次）基础学习器的组合就可以搜索出优质集成模型。下面对步骤 6 详细阐述。

步骤 6，通过代理模型预测候选池中基础学习器的测试性能，确定符合分类任务场景要求的 k 个基础学习器组成集成模型，集成模型的大小为 k 。

- 10 根据基础学习器的生成分布/候选池，需要从中搜索出最合适的 k 个基础学习器来组成集成模型，则集成模型的大小为 k 。

在一个可以实现的实施方式中，步骤 6 通过以下步骤 S61- S63 获得集成模型

步骤 61，使用步骤 5 中确定的代理模型来直接预测其他未评估的架构的性能，以避免巨大的评估成本。

- 15 在一个可以实现的实施方式中，可以先从最优的架构分布中进行随机采样，然后从多个采样的架构开始，根据预测的性能指标进行区域搜索（local search）。

步骤 62，根据代理模型输出的预测性能指标，确定 q 个预估的顶点架构，预估的顶点架构为代理模型在验证集上预测的性能指标高于相邻架构的神经网络架构。

- 20 其中，相邻架构是指算子排布只相差一位的网络架构。示例性地，有如下 3 个神经网络架构，架构 1：A-A-B-C，架构 2：A-B-B-C，架构 3：A-A-C-C，架构 1 与架构 2 互为相邻架构，架构 1 与架构 3 互为相邻架构。

步骤 63，将 q 个预估的顶点架构中性能指标最好的 k 个进行组合得到集成模型。

- 25 在一个可以实现的实施方式中，可将 q 个预估的顶点架构的性能指标由优到劣排序，取性能指标位于前面的 k 个架构进行组合，得到集成模型。在一个可以实现的实施方式中，可将 q 个预估的顶点架构中性能指标符合分类任务要求的 k 个进行组合，得到集成模型。分类任务要求可以是准确度最高，错误率最低或损失函数最小等。

在一个可以实现的实施方式中，可使用贪心算法，在 q 个预估顶点架构中逐个找出能带来现有集成模型性能最大提升的 k 个进行组合，得到最终集成模型。

最后，执行步骤 S7，输出集成模型。

- 30 在一个可以实现的实施方式中，可以定义最大搜索次数或最大搜索时间为终止标准，如果终止标准还未达到，则继续步骤 3 至步骤 6 的迭代。在达到终止标准后，本申请实施例的算法迭代终止。下游可直接将输出的集成模型应用于前述所提到的各种场景。

实施例一

- 35 在图片分类任务中应用本申请实施例提供的搜索神经网络集成模型的方法，目的是在常见的搜索空间如 DARTS 和 NAS-Bench-201 上和数据集如 CIFAR10, CIFAR100 和 ImageNet16-120 上搜索高性能的神经网络集成模型，并设定训练集数据和验证集数据属于同一分布。下面详细地描述本申请提供的搜索神经网络集成模型的方法在实施例一的图片分类任务场景中的具体步骤。

S701, 数据获取。

示例性地, 可以从常见的图片分类数据集中获取数据。示例性地, CIFAR-10 和 CIFAR-100 的训练集/验证集中各有 50,000/10,000 张图片, 而 ImageNet16-120 中则有超过 154,700/3,000 张训练/验证集图片, 可以从这些数据集中获取训练集数据和验证集数据。

在一个可以实现的实施方式中, 可以使用训练集的图片及其人工标注的标签搜索神经网络架构, 并在验证集上进行验证。

S702, 定义搜索空间及目标函数。

在一个可以实现的实施方式中, 可以定义搜索空间为 NAS-Bench-201 的搜索空间: 其中有 6 个算子位置 $N=6$, 和 5 种算子类型选项 $k=5$, 5 种算子类型为: 3x3 卷积、3x3 全局池化、1x1 卷积、残差连接和零连接。该搜索空间中包含的总神经网络架构单元数量有 15,625 个, 去除同构 (isomorphic) 架构单元后, 一共有 6466 个不同 (unique) 的神经网络架构单元。在这个搜索空间里, 本申请的目标函数是输出集成模型在 CIFAR-10 验证集上的分类错误率。

在 NAS-Bench-201 搜索空间里, 希望找到的集成模型是在验证集上分类错误率低的集成模型。

在一个可以实现的实施方式中, 可以定义搜索空间为基于 DARTS 的搜索空间, 其中有 8 个算子位置 $N=8$, 和 7 种类型选项 $k=7$, 其算子的具体类型为: 3x3 或 5x5 大小的可分卷积 (separable convolution)、3x3 或 5x5 大小的空洞卷积 (dilated convolution)、3x3 最大池化 (max pooling)、3x3 平均池化 (average pooling) 和残差连接 (skip connection)。在这个搜索空间里, 本申请的目标函数同样是输出集成模型在 CIFAR-10 验证集上的分类错误率。

下面, 基于 ANASOD 和高斯过程进行神经网络集成模型的搜索, 具体步骤详见以下:

以目标函数和集成模型大小 k 为输入, 初始化架构分布搜索 ANASOD 及初始架构分布的超参, 又称做 ANASOD 编码。在达到终止标准前迭代以下步骤:

S703, 由搜索策略推荐架构分布的超参, 即 ANASOD 编码。

S704, 在 ANASOD 编码定义的算子分布中随机采样一个具体的神经网络架构, 进行性能评估, 并将评估结果作为所有共享此 ANASOD 编码的神经网络架构的性能代理。

S705, 使用 S704 神经架构的评估结果更新分布搜索策略和代理模型, 代理模型为基于 weisfeiler-lehman 图核的高斯过程 (gaussian process with WL graph kernel, GPWL)。

S706, 从搜索策略推荐的当前最优架构分布/ANASOD 编码中进行 q 个采样, 使用代理模型评估每个采样的测试性能, 然后从每个采样开始, 运用局部搜索找到其附近的预估的顶点架构, 从 q 个预估的顶点架构中选择预测性能最优的 k 个架构组成集成模型。

输出集成模型。

在本申请提供的实施例一中, 在架构集成搜索的第一阶段采用了 ANASOD 神经

络架构分布搜索方法，如步骤 S703- S705，在第二阶段采用了基于 weisfeiler-lehman 图核的高斯过程结（gaussian process with WL graph kernel, GPWL）作为代理模型，如步骤 S705 中被更新的代理模型，来辅助顶点模型的预测和最终集成的搜索，如步骤 S706。

5 在 NAS-Bench-201 的搜索空间上将本申请实施例提供的搜索神经网络集成模型的方法与现有的架构集成搜索标杆 NES-RS 和 NES-RE 进行对比。表 1 是在 NAS-Bench-201 搜索空间上，本申请实施例提供的搜索神经网络集成模型的方法（记为 DistriNAS-PM）和其他方法的比较数据。结果是 10 次试验中的平均验证集错误率（%）（ ± 1 个标准误差）。表 1 中本申请实施例提供的搜索神经网络集成模型的方法
10 记为 DistriNAS-PM，其他方法包括 NES-RS、NES-RE 和 Deep Ensemble，分别在数据集 CIFAR10, CIFAR100 和 ImageNet16-120 上比较评估数量、测试误差和置信度。

如表 1 可见，本申请实施例提出的方法 DistriNAS-PM 评估的网络架构的数量 N 为 30，相比于 NES-RS 和 NES-RE，本申请实施例提出的方法 DistriNAS-PM 只需要不到 1/3 的搜索成本就可以找到到测试误差(Error)相当甚至更低的集成模型。而且本申请
15 实施例找到的架构集成不仅仅测试误差低，模型的校准程度、置信度也和 NES-RE 找到的最优集成模型相当。其中置信度由负对数似然（negative log likelihood, NLL）衡量，NLL 越低，模型校准程度越高。

表 1

搜索方法	搜索成本 (网络架构评估数量N)	数据集					
		CIFAR10		CIFAR100		ImageNet16-120	
		Error	NLL	Error	NLL	Error	NLL
NES-RS	100	5.20 ± 0.29	0.210 ± 0.006	25.40 ± 0.48	1.10 ± 0.010	50.93 ± 0.52	2.00 ± 0.025
NES-RE	100	4.80 ± 0.11	0.206 ± 0.004	23.88 ± 0.71	1.05 ± 0.011	49.78 ± 0.63	1.93 ± 0.014
DistriNAS-PM	30	4.90 ± 0.24	0.208 ± 0.012	23.78 ± 1.10	1.05 ± 0.032	49.56 ± 0.60	1.93 ± 0.022
Deep Ensemble	—	5.43 ± 0.11	0.238 ± 0.019	25.21 ± 0.84	1.11 ± 0.042	50.96 ± 0.066	1.98 ± 0.030

此外，表 1 的最后一行，添加了深度集成(deep ensemble)基准：将本申请实施例
20 找到的架构集成中的基础学习器各自使用 k 个不同的训练初始权重进行训练来评估其对应的深度集成效果。表 1 的结果再次证明使用不同架构（architecture）组成的集成模型比使用不同训练初始权重（initialization）组成的集成模型更优。

图 6 为包括本申请提供的 DistriNAS-PM 在内的各个基准在 CIFAR10 上取得的测试误差对比曲线图。如图 6 所示，将各个基准在 CIFAR10 上取得的测试误差随着搜索
25 的进行和架构评估的数量逐渐增加进行了对比。包括 NAS-Bench-201 搜索空间中不同方法搜索到的集成模型如 DistriNAS-PM、NES-RS 和 NES-RE,以及本申请 DistriNAS 找到的架构集成中每个架构对应的深度集成模型（DeepEnsemble），和最优基础学习器，在 CIFAR-10 数据集上的验证集错误率（%）错误率越低越好。图 8 上 x 轴是架构评估的数量。

30 由图 6 可知，本申请实施例提出的架构集成搜索方法（distriNAS-pm）比 NES-RS

和 NES-RE 能更快地找到验证误差更低的架构集成，大大减少了搜索成本；对比架构集成和深度集成，架构集成的验证取得的误差更低；所有的集成模型都明显优于最优的单个神经网络架构/基础学习器。

5 为了验证本申请实施例的搜索方法在更大，更真实的搜索空间上的效果，可以进一步在 DARTS 搜索空间上和使用不同搜索成本的 NES-RS 进行对比。表 2 为在 DARTS 搜索空间上，本申请实施例提出的方法（DistriNAS-PM）和使用不同搜索成本的 NES-RS 在 CIFAR10 任务上的比较数据。结果是 3 次试验中的平均验证集错误率（%）。

表 2

搜索方法	搜索成本 (网络架构评估数量N)	数据集	
		DARTS-CIFAR10	
		Error	NLL
NES-RS	50	0.052	0.178
	200	0.051	0.180
	400	0.050	0.179
DistriNAS-PM	50	0.047	0.165

10 表 2 的结果显示，在 DARTS 搜索空间上，本申请实施例提出的架构集成搜索方法只需要 1/8 的搜索成本，就可以找到比于现有的标杆 NES-RS 所找到的更优的架构集成。

在本实施例的应用场景里，本申请实施例的流程与现有方法比，本申请实施例能用更少的时间和计算量成本搜索到相近表现的神经网络集成模型，既加快了集成模型的搜索效率也提高了架构集成搜索的精度。

15 相对于现有方法，本申请实施例用同样的时间和成本可以搜索到精度更优的神经网络架构集成。应用于实际生产中，使用本申请实施例可以在更短时间和更少的计算量的情况下搜索到精度更高的卷积神经网络架构集成以应用于图片分类任务。这种有益效果主要是因为本申请实施例采用了架构分布搜索来寻找基础学习器候选池（第一阶段）并使用代理模型和顶点架构的组合来寻找高质量集成模型（第二阶段），大大
20 减少了大量训练和评估单个神经网络架构（单个基础学习器）的需求。

实施例二

实例二通过图片分类应用，检验本申请实施例对 OOD 数据的鲁棒性。OOD 数据在很多现实应用中非常常见，例如自动驾驶，医疗图像诊断等等。本申请实施例在常见的搜索空间和数据集上搜索高性能的神经网络集成模型，其中常见的搜索空间包括
25 DARTS 和 NAS-Bench-201，数据集包括 CIFAR10 和 CIFAR100；采用被多种噪音进行不同程度扰动的验证样本来评估不同方法所搜索到的架构集成在 OOD 数据上的测试误差，校准程度以及拒识能力。被多种噪音扰动的验证样本包括 CIFAR10-C、CIFAR100-C。

30 CIFAR10-C 和 CIFAR100-C 是分别是通过向 CIFAR10 和 CIFAR100 的验证集图片添加 15 种扰动/噪音中的随机一种而生成。扰动/噪音的强度(shift severity)由低到高有 5 级，强度等级越高，表示对图像生成分布的移动越大，即被干扰的图像和原图的分布差异越大。

图 7 为随机选择添加到 CIFAR10 和 CIFAR100 验证集图片上的 15 种干扰/噪音方式。

图 8 为随机选择添加到 CIFAR10 和 CIFAR100 验证集图片上的干扰/噪音后的效果图；图 8 显示干扰/噪音的等级越高，生成的被干扰后的图片和原图的（分布）差异越大。

先在 NAS-Bench-201 的搜索空间上将本申请实施例提出的方法 DistriNAS-PM 与现有的架构集成搜索方法 NES-RS 和 NES-RE 在 CIFAR100-C 的 OOD 任务上进行对比。与实施例一场景的比较结果相同，NES-RS 和 NES-RE 的架构集成是经过评估 100 个神经网络架构后找到的，而本申请实施例提出的 DistriNAS-PM 只需要评估 30 个神经网络架构。

图 9 为在 NAS-Bench-201 空间上本申请提供的 DistriNAS-PM 与其他搜索方法的 OOD 验证比较示意图；图 9 显示在 NAS-Bench-201 空间上，相比于 NES-RS 及 NES-RE，本申请实施例 DistriNAS-PM 用低于 1/3 的成本就能找到在 OOD 验证集上误差更低、模型校准更好（NLL 更低）的架构集成。

如图 9 所示，DistriNAS-PM 找到的架构集成不仅在原图像(severity = 0)上测试误差优于 NES-RS 并和 NES-RE 相当。在数据受不同程度(severity = 2, 4)的干扰的 OOD 情况下，DistriNAS-PM 找到的架构集成甚至在测试误差和模型校准程度上（NLL）都略微优于 NES-RS 和 NES-RE 找到的架构集成，证明本申请实施例提出的搜索方法不但能更快地找到好的集成，而且能找到对 OOD 数据鲁棒性更高的集成。

值得一提的是在图 9 也展示了不同方法找的各自架构集成中最优基础学习器的性能（亮色模块），可以发现所有的集成模型在 OOD 数据上所达到的测试误差和 NLL 都明显低于最优单个神经网络架构/基础学习器，证明了本申请提及的集成模型在数据受干扰时或测试数据分布与训练数据分布不一致时，有更好的拒识能力和鲁棒性。

同样进一步在更大的 DARTS 搜索空间上进行搜索，在 CIFAR10-C 数据集上进行验证。表 3 是在 DARTS 搜索空间上，本申请实施例提出的方法（DistriNAS-PM）和使用不同搜索成本的 NES-RS 在 CIFAR10-C 任务上的比较数据。结果是 3 次试验中的平均验证集错误率（%），如表 3 所示。

表 3 的结果表明在 DARTS 空间上，本申请实施例提出的方法也能高效地搜索到对 OOD 数据测试误差更小，模型不确定性校准更好（NLL 更低）及鲁棒性更好的架构集成。

表 3

搜索方法	搜索成本 (网络架构 评估数量 N)	干扰等级		干扰等级		干扰等级	
		1		3		5	
		Error	NLL	Error	NLL	Error	NLL
NES-RS	50	0.090	0.288	0.123	0.382	0.179	0.549
	200	0.089	0.291	0.124	0.390	0.179	0.553
	400	0.088	0.289	0.122	0.386	0.176	0.550
DistriNAS-PM	50	0.085	0.278	0.117	0.380	0.158	0.495

在本实施例 2 的应用场景中,与现有方法比,本申请实施例提供的搜索神经网络集成模型的方法能用更少的时间和计算量成本搜索到相近表现的神经网络集成模型,既加快了集成模型的搜索效率,也提高了架构集成搜索对 OOD 数据的鲁棒性,获得更低的验证误差,更高的模型校准和更准确的不确定值。应用于实际生产中,使用本申请实施例可以在更短时间和更少的计算量的情况下搜索到适用于高风险或高不确定性的使用场景的优质架构集成。

本申请实施例提供一种高效搜索多神经网络集成模型的方法,基于高效并更加适用于集成模型搜索的两阶段搜索框架,使用神经架构分布搜索而非传统 NAS 来快速找到一个基础学习器的候选池,以避免重复评估类似网络架构获得搜索效率的提升;使用代理模型在候选池中通过预测(而非实际)性能快速选择最优且多样化的顶点模型来组成目标集合模型。

本申请实施例方法与现有方法相比能更高效地进行集成模型的搜索,从而大大降低搜索成本,使得集成模型的搜索在更多的应用场景下的可行性大大增强。原有方法依靠传统 NAS,需要对基础学习器逐个搜索和评估来搭建足够大的候选池,而本方法利用架构分布搜索可以快速搭建基础学习器的候选池,简化搜索空间、降低搜索难度。

在从基础学习器候选池搜索搭建最优集成模型时,本申请实施例使用代理模型在候选池中搜索顶点模型,在高效的同时确保顶点模型的多样化、确保集合模型相对于单个基础学习器可以获得较大的性能提升。

本申请实施例可以和各种类型的架构分布搜索相结合,且适用于不同地搜索空间,泛用性强、可应用于不同场景与任务。

本申请实施例除了可以应用在卷积神经网络的架构搜索上,也可潜在应用在其他类型的、有类似架构搜索单元结构的神经架构搜索的任务中,及其他使用集成模型可以带来进一步收益的任务中,如常用于自然语言处理的循环神经网络(recurrent neural network, RNN)架构和常用于自然语言处理和视觉任务的以 transformer 为代表的深度自注意力变化网络(deep transformer self-attention networks)中,以获得对不确定性良好的度量。

本申请实施例提供一种搜索神经网络架构集成模型的装置,所述装置包括:数据获取模块,用于获取数据集,所述数据集包括分类任务中的样本和标注;架构分布搜索模块,用于使用神经网络架构分布搜索算法进行搜索,包括:用于确定神经网络架构分布的超参;在所述超参定义的架构分布中采样一个神经网络架构;根据所述分类任务中的样本和标注对所述神经网络架构训练和评估,得到性能指标;根据所述性能指标确定共享所述超参的神经网络架构分布,获得基础学习器的候选池;所述基础学习器为符合所述架构分布要求的神经网络架构;所述神经网络架构由神经网络架构单元重复堆叠而成;确定代理模型;所述代理模型用于预测未评估的神经网络架构的测试性能;架构集成模型组合,通过代理模型预测所述候选池中基础学习器的测试性能,确定符合所述分类任务要求的 k 个基础学习器组成集成模型,所述集成模型的大小为 k 。

本申请实施例提供一种电子装置 1000,如图 10 所示,包括处理器 1001 和存储器 1002;所述处理器 1001 用于执行所述存储器 1002 所存储的计算机执行指令,所述处理器 1001 运行所述计算机执行指令执行上述任意实施例所述的基于演化学习的神经

网络结构搜索的方法。

本申请实施例提供一种存储介质，包括可读存储介质和存储在所述可读存储介质中的计算机程序，所述计算机程序用于实现上述任一实施例所述的基于演化学习的神经网络结构搜索的方法。

5 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请实施例的范围。

10 此外，本申请实施例的各个方面或特征可以实现成方法、装置或使用标准编程和/或工程技术的制品。本申请中使用的术语“制品”涵盖可从任何计算机可读器件、载体或介质访问的计算机程序。例如，计算机可读介质可以包括，但不限于：磁存储器件（例如，硬盘、软盘或磁带等），光盘（例如，压缩盘（compact disc，CD）、数字通用盘（digital versatile disc，DVD）等），智能卡和闪存器件（例如，可擦写可编程只读存储器（erasable programmable read-only memory，EPROM）、卡、棒或钥匙驱动器等）。
15 另外，本文描述的各种存储介质可代表用于存储信息的一个或多个设备和/或其它机器可读介质。术语“机器可读介质”可包括但不限于，无线信道和能够存储、包含和/或承载指令和/或数据的各种其它介质。

应当理解的是，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本申请实施例的实施过程构成任何限定。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

25 在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

30 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

35 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请实施例的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者接入网设备等）执行本申请实施例各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读

存储器(ROM, Read-Only Memory)、随机存取存储器(RAM, Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

- 5 以上所述, 仅为本发明的具体实施方式, 但本发明的保护范围并不局限于此, 任何熟悉本技术领域的技术人员在本发明揭露的技术范围内, 可轻易想到变化或替换, 都应涵盖在本发明的保护范围之内。因此, 本发明的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1. 一种搜索神经网络架构集成模型的方法，其特征在于，所述方法包括：
获取数据集，所述数据集包括分类任务中的样本和标注；
使用神经网络架构分布搜索算法进行搜索，包括：确定神经网络架构分布的超参；
5 在所述超参定义的架构分布中采样一个神经网络架构；根据所述分类任务中的样本和标注对所述神经网络架构训练和评估，得到性能指标；根据所述性能指标确定共享所述超参的预测的神经网络架构分布，获得基础学习器的候选池；所述基础学习器为符合所述架构分布要求的神经网络架构；所述神经网络架构由神经网络架构单元重复堆叠而成；确定代理模型；所述代理模型用于预测未评估的神经网络架构的测试性能；
10 通过代理模型预测所述候选池中基础学习器的测试性能，确定符合所述分类任务要求的 k 个基础学习器组成集成模型，所述集成模型的大小为 k 。
2. 根据权利要求1所述的搜索神经网络架构集成模型的方法，其特征在于，所述使用神经网络架构分布搜索算法进行搜索，包括：
使用基于学习算子概率分布的近似神经网络架构搜索（approximate neural
15 architecture search via operation distribution，ANASOD）算法进行神经网络架构分布搜索。
3. 根据权利要求1或2所述的搜索神经网络架构集成模型的方法，其特征在于，所述确定神经网络架构分布的超参，包括：
确定神经网络架构分布的超参为ANASOD编码；所述ANASOD编码为指示神经网络架构单元中各种算子的概率分布的向量，所述ANASOD编码和神经网络架构单元的映射是一对多。
20 4. 根据权利要求1或2所述的搜索神经网络架构集成模型的方法，其特征在于，所述确定神经网络架构分布的超参，包括：
采用搜索策略优化神经网络架构分布的超参，所述搜索策略为贝叶斯优化，所述搜索策略用于在下一迭代中采样到比当前的所述神经网络架构单元的性能指标更符合要求的神经网络单元。
25 5. 根据权利要求3所述的搜索神经网络架构集成模型的方法，其特征在于，在所述超参定义的架构分布中采样一个神经网络架构，包括：
根据所述ANASOD编码定义的算子概率分布，确定所述神经网络架构的组成单元
30 中各个算子的具体数量；
根据设定的搜索空间连接不同的算子来获得所述有效神经网络架构。
6. 根据权利要求1或2所述的搜索神经网络架构集成模型的方法，其特征在于，所述对所述神经网络架构单元在所述数据集上训练和评估，得到性能指标，包括：
在训练数据集上训练所述神经网络架构；
35 在验证数据集上评估所述神经网络架构，获得性能指标；所述训练集数据和验证集数据同属于所述数据集。
7. 根据权利要求1或2所述的搜索神经网络架构集成模型的方法，其特征在于，所述将所述使用神经网络架构分布搜索（distributional NAS）算法进行搜索，还包括：
根据所述预测的神经网络架构分布的性能指标和超参确定所述神经网络架构分布

的搜索策略。

8. 根据权利要求 1 或 2 所述的搜索神经网络架构集成模型的方法, 其特征在于, 所述使用神经网络架构分布搜索 (distributional NAS) 算法进行搜索, 还包括:

5 根据每次搜索出来的神经网络架构分布的超参和性能指标确定其他未知分布的超参的性能预测值, 包括均值和方差;

根据所述均值和方差确定神经网络架构分布的性能预测策略, 所述性能预测策略用于预测神经网络架构分布的性能指标。

9. 根据权利要求 1 或 2 所述的搜索神经网络架构集成模型的方法, 其特征在于, 所述根据所述性能指标确定共享所述超参的神经网络架构分布, 获得基础学习器的候选池, 包括:

根据所述性能指标和所述超参确定所述神经网络架构分布的搜索策略;

根据所述性能指标和所述神经网络架构单元确定所述神经网络架构分布的性能预测策略;

15 根据所述搜索策略和性能预测策略, 在共享所述超参的所述神经网络架构分布中搜索, 确定基础学习器的候选池。

10. 根据权利要求 1 或 2 所述的搜索神经网络架构集成模型的方法, 其特征在于, 所述根据所述性能指标确定共享所述超参的神经网络架构分布, 获得基础学习器的候选池, 包括:

20 根据历史搜索中的多个神经网络架构和对应性能指标输出多个共享所述超参的神经网络架构;

根据所述多个共享所述超参的神经网络架构确定符合要求的神经网络架构分布;

根据所述符合要求的神经网络架构分布, 生成多个神经网络架构单元, 获得基础学习器的生成分布/候选池。

25 11. 根据权利要求 1 或 2 所述的搜索神经网络架构集成模型的方法, 其特征在于, 所述确定代理模型, 包括:

根据所述神经网络架构单元和所述性能指标通过在所述数据集上训练, 获得所述代理模型。

30 12. 根据权利要求 1 或 2 所述的搜索神经网络架构集成模型的方法, 其特征在于, 所述通过代理模型预测所述候选池中基础学习器的测试性能, 确定符合任务场景要求的 k 个基础学习器组成集成模型, 包括:

通过代理模型预测所述候选池中多个基础学习器的测试性能;

根据预测结果进行区域搜索 (local search), 确定 q 个预估的顶点架构, 所述预估的顶点架构为所述代理模型在验证集上预测的性能指标高于相邻架构的神经网络架构;

35 将所述 q 个预估的顶点架构中性能指标符合要求的 k 个架构进行组合, 得到集成模型。

13. 根据权利要求 12 所述的搜索神经网络架构集成模型的方法, 其特征在于, 将所述 q 个预估的顶点架构中性能指标符合要求的 k 个架构进行组合, 包括:

将 q 个预估的顶点架构的性能指标由优到劣排序, 取性能指标位于前面的 k 个架

构进行组合。

14. 根据权利要求 12 所述的搜索神经网络架构集成模型的方法，其特征在于，将所述 q 个预估的顶点架构中性能指标符合要求的 k 个架构进行组合，包括：

5 使用贪心算法（greedy selection algorithm），遍历 q 个预估的顶点架构，逐个添加 k 个架构组成集成模型。

15. 一种搜索神经网络架构集成模型的装置，其特征在于，所述装置包括：

数据获取模块，用于获取数据集，所述数据集包括分类任务中的样本和标注；

10 架构分布搜索模块，用于使用神经网络架构分布搜索算法进行搜索，包括：用于确定神经网络架构分布的超参；在所述超参定义的架构分布中采样一个神经网络架构；根据所述分类任务中的样本和标注对所述神经网络架构训练和评估，得到性能指标；根据所述性能指标确定共享所述超参的神经网络架构分布，获得基础学习器的候选池；所述基础学习器为符合所述架构分布要求的神经网络架构；所述神经网络架构由神经网络架构单元重复堆叠而成；确定代理模型；所述代理模型用于预测未评估的神经网络架构的测试性能；

15 架构集成模型组合模块，用于通过代理模型预测所述候选池中基础学习器的测试性能，确定符合所述分类任务要求的 k 个基础学习器组成集成模型，所述集成模型的大小为 k 。

20 16. 一种电子装置，其特征在于，包括：处理器和存储器；所述处理器用于执行所述存储器所存储的计算机执行指令，所述处理器运行所述计算机执行指令，执行权利要求 1-14 所述的基于演化学习的神经网络结构搜索的方法。

17. 一种存储介质，其特征在于，包括可读存储介质和存储在所述可读存储介质中的计算机程序，所述计算机程序用于实现权利要求 1-14 所述的基于演化学习的神经网络结构搜索的方法。