

基于改进 HAT 网络的多任务连续学习模型

郭正兵^{1,2}, 王 蒙¹

- (1. 昆明理工大学信息工程与自动化学院, 昆明 650500;
2. 云南省人工智能重点实验室, 昆明 650500)

摘要: 神经网络在连续学习多个任务时,随着学习任务数的增多,学习能力降低,之前学会的知识被覆盖产生灾难性遗忘。针对这一问题,提出了一种结合 HAT 与生成对抗学习(GAL)的 HAT-GAL 模型。将 GAL 嵌入 HAT 网络全连接层中,解决网络随任务数增多学习能力降低以及对多姿态数据鲁棒性差的问题。同时,结合进化策略进行网络参数寻优,有效缓解参数冗余,易陷入局部最优导致的遗忘问题。实验结果表明,改进的 HAT-GAL 模型对多姿态数据具有很好的普适性,并且连续学习多个任务后学习能力不下降,遗忘率较小。

关键词: 多任务连续学习;灾难性遗忘;生成对抗学习(GAL);进化策略

中图分类号: TP183 **文献标识码:** A **文章编号:** 1009-2552(2022)05-0001-06

DOI: 10.13274/j.cnki.hdztj.2022.05.001

Multi-task continuous learning model based on improved HAT Network

GUO Zheng-bing^{1,2}, WANG Meng¹

(1. Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, China; 2. Yunnan Key Laboratory of Artificial Intelligence, Kunming 650500, China)

Abstract: When the neural network continuously learns multiple tasks, as the number of learning tasks increases, the learning ability would decrease, and the previously learned knowledge would be overwritten, resulting in catastrophic forgetting. To solve this problem, this paper proposes a HAT-GAL model which combines HAT with generative adversarial learning (GAL). The gal is embedded in the full connection layer of hat network to solve the problem that the learning ability of the network decreases with the increase of the number of tasks and the poor robustness to multi attitude data. At the same time, the evolutionary strategy is used to optimize the network parameters, which can effectively alleviate the parameter redundancy problem and forgetting problem caused by easiness to fall into local optimization. The experiment results show that the improved HAT-GAL model has good universality for multi-pose data, and the learning ability does not decline after learning multiple tasks continuously, and the forgetting rate is the smallest as well.

Key words: multi-task continuous learning; catastrophic forgetting; generative adversarial learning (GAL); evolutionary strategy

基金项目: 国家自然科学基金(61563025);云南省科学技术厅科研项目(KKS0201603019)

作者简介: 郭正兵(1994-),男,硕士研究生,研究方向为计算机视觉、模式识别。

0 引言

人类具有持续学习的能力,能够记住学过的知识,但这对计算机是困难的。神经网络学习新任务时,无法保留先前任务知识的这类现象称为

灾难性遗忘^[1] (CF), 这成为实现多任务连续在线学习必须解决的困难之一。

近年来, 缓解灾难性遗忘的研究取得了一系列进展。一类方法利用混合训练的自我刷新记忆方案, 不断用与历史数据相关的信息刺激神经元, 这类方法通常有一个复杂性限制, 网络的数量随着需要学习的新任务的数量增加而增加。

另一类方法在具有随机梯度下降 (SGD) 的典型学习中使用隐式分布式信息存储可以增大存储容量来解决^[2]。这类方法大多采用 Dropout 或 Maxout 的思想, 利用深度神经网络的大容量来分布式存储每个任务的信息。PathNet^[3] 在 SGD 基础上扩展了在单个网络中进行参数重用的集成方法的思想。Rajasegaran 提出了一种随机路径选择算法 RPS-Net^[4], 该算法在鼓励参数共享的同时, 逐步为新任务选择最优路径。这类模型有效解决内存问题, 但当任务难度较大, 或者任务之间关联性较小, 特别是包含旋转图片的数据集时遗忘现象同样严重。

近期, 多数研究通过抑制和修剪深层网络的连接可以有效地缓解 CF 问题^[5-8]。这些方法性能取决于修剪参数的阈值, 在简单任务 (如简单 MNIST 拆分) 上表现比较好, 然而在包含图片旋转的多任务上找到合适的约束参数非常困难, 并且随着任务数量增加, 参数变得冗余, 容易陷入局部最优。

为解决这些困难, 本文提出了一种 HAT-GAL 模型, 通过在 HAT 中嵌入 GAL 增加负样本, 解决模型对多姿态任务识别精度低、鲁棒性差的问题; 在对当前任务的梯度优化迭代中采用进化学习策略, 对参数及网络的优化, 缓解复杂网络超参数易陷入局部最优的问题, 减少先前知识的覆盖。

1 HAT-GAL 模型

1.1 问题描述

假设在一个连续学习中任务数据集为 $X_s = \{D_s^i \mid i = 1, \dots, n_s\}$, 其中, S 代表数据集的种类, n_s 代表数据大小。如图 1 所示, 在 0 ~ 50 周期内学习, D_{MNIST} 分类准确度达到 99.89%, 在 50 ~ 100 周期学习数据 $D_{CIFAR10}$ 达到最大精度 76.43%, 而

在连续学习第二个任务时, 第一个任务的分类精度下降到 23.39%, 下降的精度被称之为“网络记忆”的损失。

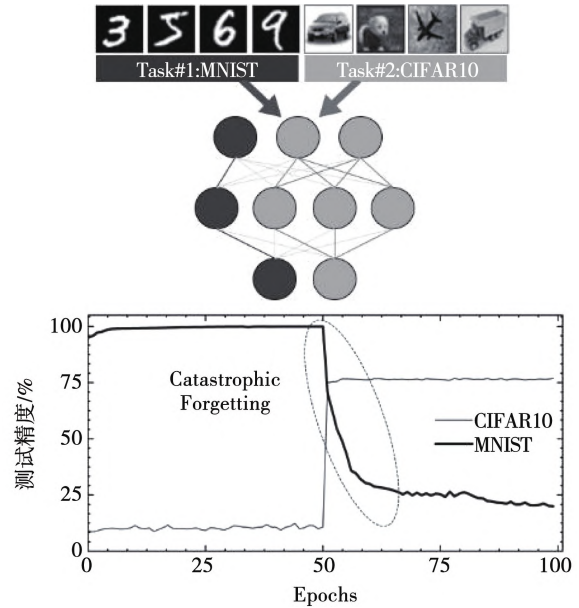


图 1 神经网络中“记忆力”下降的表现

针对“网络记忆”下降问题, 利用提升网络初始分类精度, 以及对网络模型参数的优化减少网络及参数的冗余和陷入局部最优的问题, 来保留更多的“网络记忆”。

1.2 HAT 记忆力保持网络模型

该方法在 HAT^[9] 模型的基础上借鉴了分层注意机制思想, 采用门控对每一层全连接层进行调节, 并在以后利用这种学习到的调节来防止忘记先前的任务。使用反向传播和小批量随机梯度下降 (SGD) 通过门控任务嵌入来学习二进制的注意力向量。算法基本流程如图 2 所示。

为了适应当前任务 t , 首先采用了一种分层注意机制。给定层单元的输出单元 L 层, 按元素进行乘积 $h' = \alpha'_l h_l$ 。和普通的注意力机制不同的是, α'_l 是一个嵌入了 e'_l 矢量的门函数:

$$\alpha'_l = (\sigma s e'_l) \quad (1)$$

其中, $\sigma(x)$ 是门控函数; s 是一个正标度参数, 在实验中使用了一个 sigmoid 函数来激活门函数。所有层 $l = 1, \dots, L-1$ 的工作方式相同, 最后一层 L , α'_l 是二进制硬编码。 L 层的操作相当于多头输出,

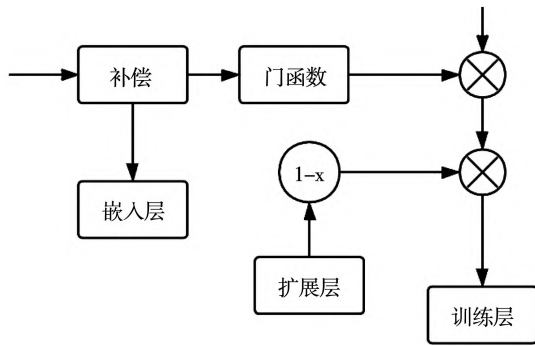


图2 HAT 算法基本流程

通常在灾难性遗忘的情况下使用。

为了保存在学习新任务时从以前的任务中学到的信息,根据以前所有任务的累积注意力来确定渐变的条件。为了获得一个累积的注意力向量,在学习完任务 t , 而且获得 α_t^i 之后, 进行递归计算:

$$\alpha_i^{\leq t} = \max(\alpha_t^i, \alpha_i^{\leq t-1}) \quad (2)$$

这里使用所有元素方向的最大值和全零向量。这保留了对以前的任务很重要的单位的注意力值,允许它们为未来任务的训练设定条件。为了保持记忆到任务 $t + 1$, 在当前层和以前层的累积

注意力最小值的反方向上修改了层的梯度 $g_{l,i}$, 使之成为当前层和先前层中最小累积注意力的倒数:

$$g_{l,i} = [1 - \min(\alpha_{l,i}^{\leq t}, \alpha_{l-1,j}^{\leq t})] g_{l,i} \quad (3)$$

式中, i 和 j 分别对应于输出 l 和输入 $l - 1$ 层, 扩展向量 $\alpha_l^{\leq t}$ 和 $\alpha_{l-1}^{\leq t}$ 以匹配层 l 的梯度张量的维数, 然后按元素执行最小值, 减法和乘法运算。

在 HAT 中, 反向传播阶段的权重更新直接将 $g_{l,i}$ 经过退火然后通过门函数来进行, 直接保存的是当前训练批次内最好的模型来进行模型的测试。经过大量的试验发现这样的方法存在缺点, 主要表现在保存的模型鲁棒性差, 当验证数据稍微变化精度将变低, 特别是在具有旋转样本的多任务数据集下。其次, 当任务数量增多存在超参数冗余与陷入局部最优的问题, 保存的任务“记忆力”下降较大。

1.3 GAL 模块增加负样本

在原 HAT 的前项传播过程门函数之前, 通过增加了 GAL 模块来增加负样本, 增加的 GAL 模块包括生成器 (Generator, G) 和判别器 (Discriminator, D), 如图 3 所示, 负样本主要用生成器生成, 具体实现过程如下。

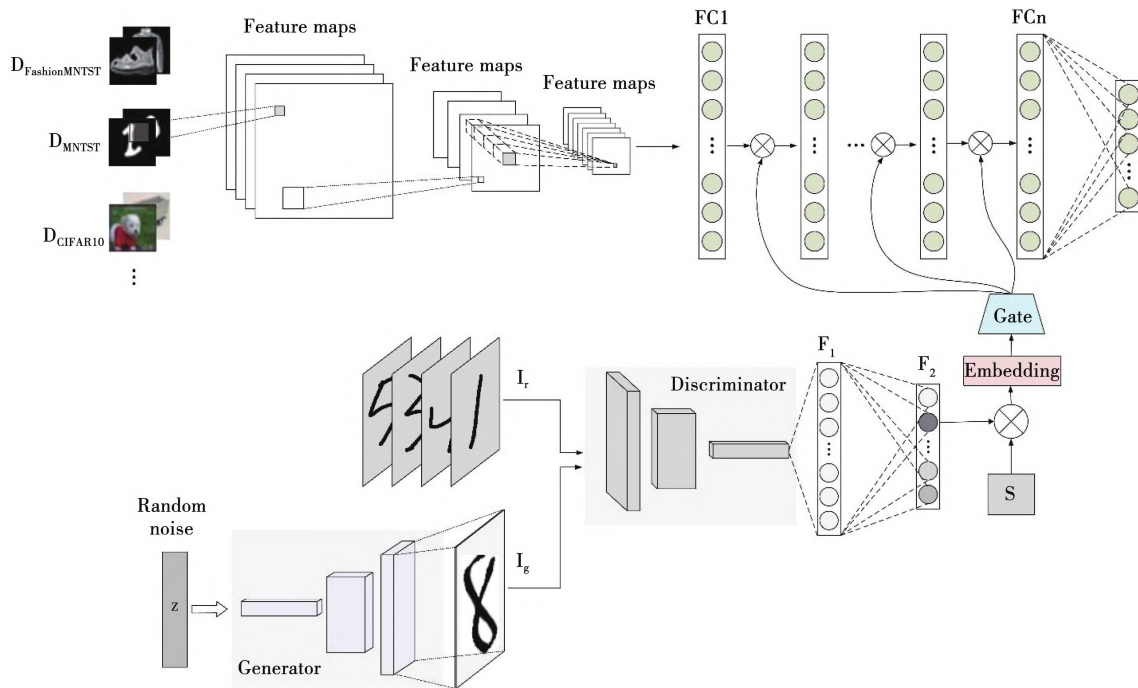


图3 基于 GAL 的多任务连续学习网络模型

将当前网络正在训练的真实图像样本 I_r 以及标签 T_{true} 输入到鉴别器中, 经过鉴别器的前向传播得到输出 t_p , 由鉴别器根据交叉熵损失来计算真实损失:

$$\begin{aligned} T_{loss} &= loss(t_p, t_{true}) = -\log\left(\frac{\exp(T_{class})}{\sum_j \exp(I_r^j)}\right) \\ &= -T_{class} + \log\left(\sum_j \exp(I_r^j)\right) \end{aligned} \quad (4)$$

其中, t_p 是网络的输出向量; t_{true} 是真实标签; I_r 表示输入的真实图片样本; T_{class} 表示 I_r 对应的正确分类输出; j 表示网络为 j 分类网络。

将一个噪声信号 Z 输入到生成器 D 中, 这里的 Z 的张量形状与 I_r 的相同, 将 Z 经过 D 的传播得到输出 t_g , 同样由生成器根据交叉熵损失来计算假损失:

$$\begin{aligned} F_{loss} &= loss(t_g, t_{true}) = -\log\left(\frac{\exp(Z_{class})}{\sum_j \exp(Z^j)}\right) \\ &= -Z_{class} + \log\left(\sum_j \exp(Z^j)\right) \end{aligned} \quad (5)$$

则 GAL 部分的损失 L_{GAL} 表示为:

$$L_{GAL} = T_{loss} - F_{loss} \quad (6)$$

在 D 的反向传播过程中对 L_{GAL} 进行优化, 理想情况下, 生成的虚假样本 I_g 和真实样本 I_r 基本上完全一致。将鉴别器得到的最大值 t_p (max) 与任务 t 加权求和代替原网络的 t 经过门函数进行网络的前向传播运算。

1.4 进化策略缓解局部最优问题

在执行退火算法后, 试验发现在训练中网络常陷入局部最优解, 精度不高。在这里引入了一个进化策略进行局部不连续随机搜索。进化策略在遗传算法的基础上, 可以对于新种群变异加以定向控制, 这就有利于网络在进行最优解的寻找时, 能够快速准确地找到全局最优解。该进化策略还能很好地处理网络权值约束, 有效地在梯度下降迭代中跳出对单个任务集的局部最优解, 从而得到网络冗余度较低的当前最优解。具体而言, 在原始网络交叉算子 E 的网络权值 θ 的基础上加入随机扰动 N_i 产生的新个体, 防止性能太小的个体在下一代中大量增长, 这一改进能够保持种群多样性并且能缓解过早收敛:

$$\rho_i = \theta_E^i + \Delta N_i \quad (7)$$

式中, $i = 1, 2, \dots, m$, 表示每一个权值, ρ_i 表示加入扰动后的新权值。为了防止加入扰动过大, 导致网络性能变差, 将 ρ_i 加进到区间:

$$\rho_i = \begin{cases} \min, & \text{if } \rho_i < \min \\ \rho_i, & \text{if } \min \leq \rho_i \leq \max \\ \max, & \text{if } \rho_i > \max \end{cases} \quad (8)$$

在本文中, $\min = -6, \max = 6$, 交叉概率 $pra = 0.9$, 变异概率 $pmu = 0.1$, 迭代数 P 设置为 50 代, 经过 50 代的交叉变异将更新后的 ρ_i 用于网络的训练, 每个迭代训练完以后, 对网络 $loss$ 进行评估, 将最好的网络模型保存下来用于最终的网络测试。

试验发现只使用进化算法, 而不对新权值进行约束, 种群变异方向也无法约束, 在迭代超过 10 代后效果反而变差。当任务变难, 就要增加训练批次来提高网络的学习能力, 批次增多容易使得局部最优解梯度为零, 意味着没有变化, 一直维持着某一种状态, 但是加入扰动则会跳出梯度为零的情况。除此之外, 在经过进化算法对权值的更新后, 这里的权值是在增加负样本后的权值, 在相同训练数据集情况下网络的感受野增大, 并且保存下来的网络模型是在 P 次迭代下表现最好的模型, 在测试的时候样本有微小变化依然会保持精度。

2 实验结果

2.1 实验设置与评价指标

为证明提出检测模型的有效性, 在常见的图像分类数据集 MNIST 上进行实验。

为了公平准确衡量各个模型的性能, 除了测试精度外, 还包括以下三个衡量指标:

单任务平均准确度 (Avg. S): 依次对模型进行训练直至任务 t 的平均验证准确度, 定义为:

$$\Delta_t = \frac{1}{t} \sum_{i=1}^t a_{t,i} \quad (9)$$

其中, a_t 是模型完成学习任务 t 时数据集 i 的验证准确性。

多任务最大平均准确度 (Avg. MT): 模型顺序学习 t 个任务, t 个任务峰值准确性的平均值,

定义为:

$$\Gamma_t = \frac{1}{t} \sum_{i=1}^t \max a_{t,i} \quad (10)$$

遗忘率 (FM): 在所有任务上对模型进行顺序训练后的平均遗忘。遗忘定义为在持续学习结束后, 每个任务的峰值准确性和准确性之间的性能下降。对于具有 T 个顺序任务的持续学习数据集, 其定义为:

$$\Phi = \frac{1}{T-1} \sum_{i=1}^{T-1} \max_{t \in 1, \dots, T-1} (a_{t,i} - a_{T,i}) \quad (11)$$

所有实验均采用与 HAT 相似的设置, 通过反向传播和普通随机梯度下降进行训练。批次大小为 64 时, 学习率为 0.05, 当连续 5 个时期对验证损失没有改善时, 学习率将降低 3 倍, 直到学习率降低到 10^{-4} 以下或 200 个周期为止。在给定 seed 的情况下, 所有方法的数据拆分、任务序列、数据加载、随机播放和网络初始化都是固定的。根据 CL^[10]

(Continual learning) 中的结果, 使用 $\rho = 0.5$ 的丢失率。以上所有实验均在 Ubuntu18.04 操作系统上完成, 使用 pytorch0.4.0、tensorflow1.14.0、python 3.6 和显卡 GeForce RTX 2070 完成模型训练。

2.2 在 MNIST 旋转任务上的性能比较

在实验中, 扩展数据集被分为几个顺序的任务, 以评估提出的模型和其他最新方法, 包括 EWC^[5], HAT^[9], LWF^[6], IMM^[11], iCaRL^[12], RPS-Net^[4], TFM^[8], CLAW^[7], LFL^[13] (less-forgetting learning) 和 PathNet^[3] 以及传统方法 SGD^[2]。将 HAT-GAL 模型与一些目前较先进的方法进行了比较, 参数评价如表 1 所示。从表 1 中, 可以看到 HAT-GAL 在学习结束时优于所有其他方法, Avg. S 为 96.22%, Avg. MT 为 97.45%, 参数 FM 最低, 为 3.16%。每个任务的结果的演变如图 4 所示, LWF 在学习每一个新任务时, 借助于先前任务的

表 1 各模型在 MNIST 旋转任务上的参数表现

参数	LWF	LFL	HAT	iCaRL	SGD	PathNet	RPS-Net	EWC	IMM	TFW	CLAW	HAT-GAL
Avg. S	54.30	21.99	93.64	64.23	52.73	87.65	51.69	64.66	92.73	76.98	95.83	96.22
Avg. MT	97.33	25.65	96.85	96.88	97.68	73.76	96.38	96.11	73.37	96.38	97.09	97.45
FM	47.62	14.12	6.18	37.39	47.35	14.59	43.96	38.69	13.20	26.97	5.42	3.16

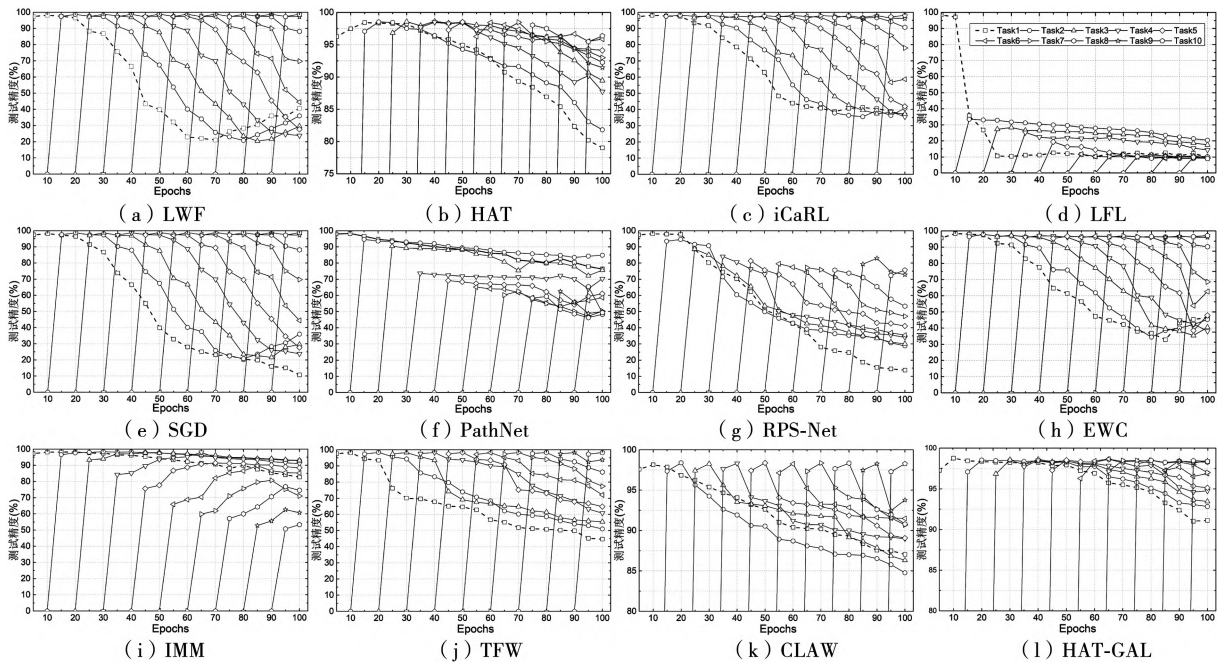


图 4 各种方法在 MNIST 数据集旋转间隔为 18° 实验中精度对比

表示, LWF 前两个任务表现得很好, 但是, 随着任务的增加, 旧任务开始遗忘更多。IMM 的作用正好相反, 它关注的是先前记忆的“顽固”性, 并试图保持对旧任务的了解, 从而耗尽新任务的容量, 这使得该方法不会忘记太多, 甚至有一个小的向后转换, 但代价是在更新的任务中执行得更差。EWC 的性能下降也比较明显, 是因为当每个任务有太多类时, 不能很好地进行可塑性约束。

PathNet, RPS-Net 和 LFL 对网络容量的依赖程度高于其他方法。如图 4(f) 所示, PathNet 在第一个任务(虚线)上具有较好的性能, 利用了修剪和微调的压缩能力, 然而, 随着网络剩余容量越来越小, 能够以更高的可扩展速度增长, 在剩余的 9 个任务上性能逐渐降低。HAT 和 CLAW 的下降相对较小, 如图 4(b) 与图 4(k) 第一个任务(虚线)精度最终分别为 79.02% 和 87.05%, 因为实施的硬性注意遮罩, 它是根据当前任务通过梯度下降的迭代来学习的, 并且以前的遮罩被用来限制这种学习。因此, 可以保留先前学习的知识而不会影响当前任务。SGD 会通过严格的约束条件保留学习到的知识, 然后按照先前任务的错误梯度学习新任务, 因此随着任务数量的增加, 先前学习的知识可能会被遗忘。

与 HAT 相比, 由于网络中增加了 GAL 产生的负样本, 使得网络鲁棒性增强, 能适应多种姿态的样本, 因此每个任务的初始精度均比 HAT 高, 其次由于进化算法减少了网络中多余参数, 使得保留每个任务更加重要的权重, 所以当学习完第十个任务后, 第一个任务的知识保留最多, 如图 4(1) 所示, 第一个任务(虚线)测试精度最终为 92.75%。

2.3 对进化算法进行消融试验

在对当前任务的梯度优化迭代中嵌入进化学习策略, 可以缓解复杂网络超参数易陷入局部最优的问题, 为了验证, 在 MNIST 旋转 18° 数据集上进行消融试验。

图 5 中, 横坐标包含 10 个任务, 每个任务 10 个批次, 记录的是学习完所有任务第一个任务的测试精度情况, 可以看出, 在当前任务的梯度优化迭代中嵌入进化学习策略, 精度下降平缓, 且下降幅度不大, 最终精度为 90.98%。没有进化策略,

在第二个批次之后, 测试精度下降迅速, 最终为 82.86%, 波动比较明显, 加入进化策略确实可以缓解复杂网络超参数易陷入局部最优问题, 由于收敛加快, 在相同 Epoch 内精度提升 8.12%。

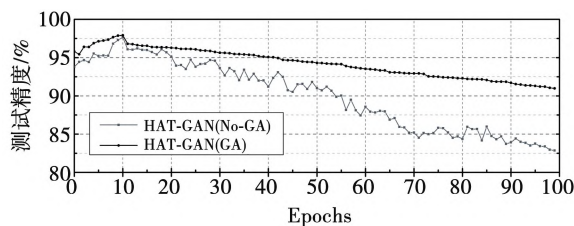


图 5 进化算法消融试验

3 结束语

本文提出了一种 HAT-GAL 的多任务连续学习模型。针对现有多任务连续学习模型中缺乏对多种样本姿态的负样本, 多任务时识别率不高, 网络结构冗余, 易陷入局部最优解等问题。采用 GAL 产生图片不同姿态负样本, 负样本的加入提升网络的自适应能力和识别能力, 对任务特征表现更敏感。最后, 通过进化策略解决了传统方法网络结构冗余, 陷入局部最优解导致遗忘知识增多的问题。试验结果表明, 本文提出的模型不仅能提高网络的学习能力, 同时能减少网络中不重要的、冗余的参数, 提高收敛速度, 在多任务连续学习精度中具有一定优越性。在未来的工作中, 将探索在更多的任务和不同数据上的表现, 提高模型的泛化能力。

参考文献:

- [1] French R M. Catastrophic forgetting in connectionist networks[J]. Trends in Cognitive Sciences, 1999, 3(4): 128 - 135.
- [2] Goodfellow I J, Mirza M, Xiao D, et al. An empirical investigation of catastrophic forgetting in gradient-based neural networks[J]. Computer Science, 2013, 84(12): 1387 - 1391.
- [3] Fernando C, Banarse D, Blundell C, et al. Pathnet: evolution channels gradient descent in super neural networks[J]. ArXiv Preprint, 2017, 5(2): 165 - 173.
- [4] Rajasegaran J, Hayat M, Khan S H, et al. Random path selection for continual learning[C]. Advances in Neural Information Processing Systems, 2019: 12669 - 12679.

(下转第 12 页)

用中选用一副天线进行通信,由于飞机飞行姿态的变化,机身会遮挡,选用的天线不会总是最理想的,而传统通信方式在通信时若同时使用两副天线,会造成多信号的干扰,反而影响通信性能。而 OFDM 技术应用于航空通信中,可以很好地消除多天线信号之间的干扰,也就可以同时使用两副机载天线进行通信,这样就可以消除只选用一副天线进行通信的弊端,提高通信质量。

参考文献:

[1] 郭宝华. 空管数据链技术应用及发展[J]. 指挥信息系统与技术,2019,10(6):8-13.
 [2] 彭笠. 利用天线切换技术增强机载超短波后向通信能力[J]. 中国新通信,2018,20(22):11-13.
 [3] 高超. 高速环境下 OFDM 系统的多普勒频偏估计研究[D]. 北京:北京邮电大学,2017.
 [4] 赵悠悠. 航空通信系统基于先验信息的信道估计算法研究[D]. 郑州:郑州大学,2019.
 [5] 胡梅霞. 正交频分复用系统峰均比抑制问题研究[D]. 西安:西安电子科技大学,2014.

[6] 黄敏,李兵兵. 基于整体最小二乘的联合信道估计及 OFDM 信号检测算法[J]. 电子与信息学报,2014,36(6):1448-1453.
 [7] Bessehier M, Djebbar A B, Zoggaret A, et al. Joint channel estimation and data detection for OFDM based cooperative system[J]. Telecommunication Systems: Modeling, Analysis, Design and Management, 2020, 73(2): 545-556.
 [8] 王薇,梁燕. 基于预编码改进的多载波系统 ICI 消除方案[J]. 重庆邮电大学学报:自然科学版,2020,32(2):255-262.
 [9] Vahid Vahidi, Ebrahim Saberinia. MIMO-OFDM communication systems for traffic data transmission in 5G drone small cells[J]. IET Communication, 2019, 13(20): 3565-3574.
 [10] 王群诚. OFDM 系统基于导频的信道估计方法研究[J]. 信息技术,2011(12):33-37,45.
 [11] 解永生,周磊磊,刘建坡. 基于 ICI 干扰消除的 OFDM 线性时变信道估计方法[J]. 信息技术,2018(1):67-70.

(责任编辑:丁晓清)

(上接第 6 页)

[5] Chaudhry A, Ranzato M A, Rohrbach M, et al. Efficient lifelong learning with a-gem[J]. arXiv Preprint,2018,12(6):38-47.
 [6] Li Z, Hoiem D. Learning without forgetting[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 40(12):2935-2947.
 [7] Adel T, Zhao H, Turner R E. Continual learning with adaptive weights (CLAW)[J]. ArXiv Preprint,2019,11(6):168-173.
 [8] Masana M, Tuytelaars T, van de Weijer J. Ternary feature masks: continual learning without any forgetting[J]. arXiv Preprint,2020,8(7):17-23.
 [9] Serrà, D Surís, Miron M, et al. Overcoming catastrophic forgetting with hard attention to the task[J]. arXiv Preprint,2018,8(7):17-23.

[10] De L M, Aljundi R, Masana M, et al. Continual learning: a comparative study on how to defy forgetting in classification tasks[J]. arXiv Preprint,2019,2(6):1909-1928.
 [11] Lee S W, Kim J H, Jun J, et al. Overcoming catastrophic forgetting by incremental moment matching[C]. Advances in Neural Information Processing Systems, 2017: 4652-4662.
 [12] Rebuffi S A, Kolesnikov A, Sperl G, et al. Icarl: incremental classifier and representation learning[C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017:2001-2010.
 [13] Jung H, Ju J, Jung M, et al. Less-forgetting learning in deep neural networks[J]. arXiv Preprint,2016,7(15):1607-1613.

(责任编辑:陈文艳)