Lifelong Infinite Mixture Model Based on Knowledge-Driven Dirichlet Process

Fei Ye and Adrian G. Bors
Department of Computer Science, University of York, York YO10 5GH, UK
fy689@york.ac.uk, adrian.bors@york.ac.uk

Abstract

Recent research efforts in lifelong learning propose to grow a mixture of models to adapt to an increasing number of tasks. The proposed methodology shows promising results in overcoming catastrophic forgetting. However, the theory behind these successful models is still not well understood. In this paper, we perform the theoretical analysis for lifelong learning models by deriving the risk bounds based on the discrepancy distance between the probabilistic representation of data generated by the model and that corresponding to the target dataset. Inspired by the theoretical analysis, we introduce a new lifelong learning approach, namely the Lifelong Infinite Mixture (LIMix) model, which can automatically expand its network architectures or choose an appropriate component to adapt its parameters for learning a new task, while preserving its previously learnt information. We propose to incorporate the knowledge by means of Dirichlet processes by using a gating mechanism which computes the dependence between the knowledge learnt previously and stored in each component, and a new set of data. Besides, we train a compact Student model which can accumulate cross-domain representations over time and make quick inferences. The code is available at https://github.com/dtuzi123/Lifelong-infinite-mixture-model.

1. Introduction

Lifelong learning (LLL) aims to learn successively a series of tasks from their corresponding probabilistic representations of specific databases. The objective of the lifelong learning model is to implement all learnt tasks at any given time. Modern deep learning approaches have been successful in a variety of applications including image translation [24], image synthesis [29] and object detection [37], but all these models face a major challenge in the performance, when applied on prior tasks, while learning multiple tasks, one after the other. This challenge is caused by catastrophic forgetting which happens when a model adapts its parameters in order to learn a new task [31].

The Generative Replay Mechanism (GRM) [41] is a popular lifelong learning approach showing promising results overcoming catastrophic forgetting [1, 33, 39, 48, 56]. A generative replay model $G_\theta : Z \rightarrow X$, aims to transform a low dimensional random variable $Z$ into a high dimensional variable $X$. $G_\theta$ can be an implicit generative model such as a Generative Adversarial Network (GAN) [11] or an explicit latent model such as a Variational Autoencoder (VAE) [16]. Once a task is learnt, $G_\theta$ generates data which then can be combined with data sampled from a given database, corresponding to a new task, to form a joint dataset used for training. Some methods [1, 41] reduce the memory size by only generating a batch of samples for each training step, by using only a copy $G'_\theta$ of the GRM. However, a major challenge for GRM based methods is that of gradually losing knowledge across tasks since a GRM model is trained on its own generations repeatedly. Another drawback, when GANs are used as GRMs, is that of facing mode collapse [44]. Two solutions have been proposed to address this problem. Rao et al. [34] enable GRMs with a network expansion mechanism in which the model’s capacity is increased when shifting data distributions. The other solution is to use the expansion mechanism [20] or an ensemble
In this paper, we provide the theoretical analysis for lifelong learning models, inspired by the idea illustrated in Fig. 1. The forgetting behaviour of the model, when learning a certain task, is affected by an ever increasing upper bound (solid line in Fig. 1) to the target-risk, during the lifelong learning. This is mainly caused by the increased accumulated errors when learning additional tasks while the discrepancy between the target and source distribution is also gradually increased. However, the optimal source-risk can not guarantee a low target-risk since the source distribution of the trained model is gradually degenerated. Inspired by these results, the main idea of the proposed Lifelong Infinite Mixture (LIMix) model is to automatically grow its network architecture if the given task is sufficiently novel when compared to the previously learned knowledge or update an appropriate component that has a small discrepancy to the given task. The Dirichlet process, which is usually computationally expensive when using the expectation-maximization algorithm to estimate component parameters [8], can be used for these mechanisms. In order to reduce the computational costs and make an accurate inference for the selection and expansion of the model architecture, we infer an indicator variable for each data sample by using a gating mechanism based on the Dirichlet process that computes the corrections between the knowledge stored in each component and the new data. Furthermore, by accumulating knowledge, while enabling fast inference across data domains, using a lightweight model is an attractive feature in LLL, which does not appear in existing lifelong mixtures or ensemble models [20, 47]. Our main contributions are:

- We analyse the forgetting behaviour during LLL by evaluating the accumulated risk and find that the discrepancy distance between the source and target distribution is key to overcome forgetting.
- This is the first study to provide theory insights when using mixture models for LLL. We also extend the theoretical analysis to explain the performance change for a model when shifting the order of tasks.
- We propose a new lifelong mixture model with theoretical guarantees for LLL. We also explore training a compact Student model from the mixture under LLL.

2. Related works

Artificial lifelong learning models are trained three different approaches: regularization, dynamic architectures and memory replay. Regularization methods introduce an auxiliary term in the loss function in order to penalize changes in the network’s weights when learning a new task [12, 15, 17, 23, 28, 38]. This can alleviate catastrophic forgetting but cannot guarantee the effective performance on the previously learnt tasks. Dynamic architectures methods would grow the size of the network by adding processing layers or increase the number of parameters in order to adapt to a growing number of tasks [6, 20, 32, 40, 50, 59]. Lee et al. [20] used Dirichlet processes for expanding their network architecture. However, their approach does not provide any theoretical guarantees for the performance, and mainly focuses on the generation and classification tasks and still requires to store past samples.

Memory replay approaches would either use a generator [1, 34, 33, 41, 56, 51, 52, 55, 57] or a memory buffer [2, 4, 46] as a replay mechanism generating data, which is statistically consistent to the previously learnt knowledge. Continual Unsupervised Representation Learning (CURL) [34] is a memory replay method which trains a latent generative model in order to replay data consistent with the previously learnt information. CURL expands its architecture for the inference component but not for the decoder. This can lead to catastrophic forgetting when learning certain tasks.

Besides these three directions of research, there are other methods such as [10, 53, 54] which create network architectures consisting of a shared module and other multiple task-specific modules. The shared module would not change its parameters too much, while the task-specific modules would only update their parameters when learning certain tasks. These approaches may guarantee the full performance on the previously learnt tasks but would still require knowing the number of tasks and the task labels during both training and testing phases. In this paper, we assume that our lifelong learning model does not know the exact number of tasks to be learnt while the task boundaries are only provided during the training phase. Although some methods can be used in a task-free manner [34], they are still limited to learning a sequence of tasks from a single domain.

3. Methodology

3.1. Problem setting

The lifelong artificial learning systems aim to learn a sequence of tasks, where each time we have a training set $D_S = \{(x_i, y_i)\}_{i=1}^N$ of $N$ paired instances of data $x_i$, considered as images, and their corresponding labels $y_i$. Let us consider the training of a model (classifier or generator) $\mathcal{M}_t$, sequentially, with $t$ tasks, each defined by the training set and the testing set $D_T$. The learning goal of $\mathcal{M}_t$ is to make precise predictions for classification tasks on all testing data sets $\{D_T, \ldots, D_T^t\}$ after the training with a sequence of sets $\{D_S^1, \ldots, D_S^t\}$. When considering the unsupervised learning setting, the learning goal of $\mathcal{M}_t$ is to learn meaningful data representations without having any labels.
3.2. The lifelong infinite mixture (LIMix) model

In this section, we first introduce a mixture of deep learning networks for unsupervised learning, and then extend this framework for a supervised setting. Let us define a deep learning mixture of $K$ components at the $t$-th task learning:

$$ p \left( x \mid \Theta, \pi_1, \ldots, \pi_K \right) = \sum_{j=1}^{K} \pi_j p_{\theta_j} \left( x \mid z \right) p \left( z \right), \quad (1) $$

where $\Theta = \{ \theta_1, \ldots, \theta_K \}$ are the parameters of components. $x \in \mathcal{X}$ and $z \in \mathcal{Z}$ are the observed and latent variables where $\mathcal{X}$ and $\mathcal{Z}$ are the input and latent space. Each $p_{\theta_j} \left( x \mid z \right)$ is implemented as a Gaussian distribution $\mathcal{N} \left( g_{\theta_j} \left( z \right), \Sigma \right)$ with $\Sigma$ considered as a diagonal matrix, and $g_{\theta_j}$ represents the deterministic mapping that maps $z$ into the mean of $p_{\theta_j} \left( x \mid z \right)$, implemented as a deep learning network [53, 54]. $\pi_j$ is the mixing parameter for the $j$-th component. $p \left( z \right)$ is the prior, implemented by the normal distribution.

One approach for training this model would be to maximize the marginal likelihood of $p \left( x, z \mid \Theta, \Omega, \pi_1, \ldots, \pi_K \right)$ as:

$$ p \left( x_1, \ldots, x_M, \Theta, \pi_1, \ldots, \pi_K \right) = \prod_{t=1}^{M} \prod_{n=1}^{N_t} \int_{j=1}^{K} \pi_j p_{\theta_j} \left( x_n^t \mid z \right) p \left( z \right) dz, \quad (2) $$

where $M$ and $N_t$ are the total number of tasks and the number of data samples considered for each $i$-th task, $i = 1, \ldots, M$. This optimization problem is intractable in practice since we cannot access data samples from previous tasks with associated training sets $\{ D_s^i \mid i = 1, \ldots, t - 1 \}$ after learning the $t$-th task. Furthermore, by maximizing Eq. (2) when learning only a single task would cause the mixture model to forget the information learnt previously, as the network parameters are updated to new values during the training with the data $x_1^t \sim D_s^t$. To address this problem, we propose to adapt the number of components in the mixture according to the complexity of the tasks being learnt. The Dirichlet process is suitable for the selection and expansion mechanisms for the mixture [35]. In this paper we adapt a Dirichlet process by defining a probabilistic measure of similarity in order to be able to train the same mixing component with several tasks. We introduce an indicator variable $c_i^t$ for each $x_i^t$ which indicates which component is assigned to $x_i^t$. Estimating the mixing weights $\{ \pi_1, \ldots, \pi_K \}$ can be indirectly realized by the inference of the indicator variable, [5]:

$$ p \left( c_1^1, \ldots, c_K^{N_k} \mid \pi_1, \ldots, \pi_K \right) = \prod_{j=1}^{K} \pi_j^{N_j}, \quad (3) $$

where $\{ \pi_1, \pi_2, \ldots, \pi_K \} \sim Dirv \left( a \right), a = \{ a / 1, \ldots, a / K \}$ and $Dirv \left( a \right)$ is a symmetric Dirichlet distribution with $a$ its parameter vector. Inferring a single indicator $c_i^t$ can be implemented by integrating over $\pi_j$ and allowing $K$ to increase to infinity, [36]:

$$ p \left( c_i^t = j \mid c_{-i}^t, a \right) = \frac{n_{-i,j}}{n - 1 + a}, \quad (4) $$

where $n_{-i,j}$ is the number of samples that are associated with the $j$-th component, excluding $x_i^t$ where the subscript $-i$ denotes all indices except $i$. Eq. (4) represents the probability for the $i$-th data sample to be associated with the $j$-th component of the mixture. The hyperparameter vector $a$ can influence the prior probability of assigning a sample to a new component and the total number of components after training [36]. However, this probability does not infer properly $c_i^t$ given that it does not evaluate the consistency of the new sample $x_i^t$ with the information learnt by each component. Comparing the previously learned knowledge with the incoming data is useful for selecting the most suitable mixture component in order to be updated, or for adding a new component to the mixture. In this paper, instead of comparing the new sample with those already stored [20, 36], we propose to incorporate the knowledge learned by each component for estimating $n_{-i,j}$ in order to consider the similarity between the prior knowledge and the new sample:

$$ n_{-i,j} = \left( n - 1 \right) \times e^{(1/K_{i,j})} \sum_{q=1}^{K} e^{(1/K_{i,q})} + e^{(1/V)}, \quad (5) $$

where $V$ is a constant controlling the expansion of the mixture model and

$$ K_{i,j} = \left| F \left( x_i^t \mid c_i^t, \theta_j, \omega_j \right) - F \left( x_i' \mid c_i^t, \theta_j, \omega_j \right) \right| $$

and $F(\cdot \mid c_i^t, \theta_j, \omega_j)$ is the log-likelihood function. $n$ is the total number of samples, and $x_i' \sim D_s^t$ is the $i$-th sample generated by the component $j$. We evaluate $K_{i,j}$ between the log-likelihood of the new sample $x_i^t$ and the log-likelihood of the generated sample $x_i', j'$, estimated by the $j$-th component. If $K_{i,j}$ is very small, then $x_i^t$ has a high likelihood to be assigned to the $j$-th component. The probability of generating a new component and of assigning the indicator variable $c_i^t$ to $x_i^t$ is then defined as:

$$ p \left( c_i^t = K + 1 \mid c_{-i}^t, a \right) = \frac{a + \left( n - 1 \right) \left( \exp \left( 1 / V \right) \right)}{n - 1 + a}, \quad (7) $$

where $Z = \sum_{q=1}^{K} e^{(1/K_{i,q})} + e^{(1/V)}$ is denominator of (5). Determining the indicator for a new task. By using the inferring indicator variable for all samples when learning the last given t-th task, is computationally intensive. We also know that data samples from a database, characterizing a certain task, share similar features. We consider only the calculation of a single indicator variable for a task, after each task switch, while the indicator variables for all data samples within a task are identical. Suppose that we have finished the $(t-1)$-th task learning, we would like to infer the indicator for the $t$-th task. Firstly, we randomly select a
group of samples \( \{ \mathbf{x}_1^t, \ldots, \mathbf{x}_{n_G}^t \} \) from the \( t \)-th training set and then calculate the probability of each \( \mathbf{x}_i^t \) belonging to each \( j \)-th component \( p(c_i^t = j | c_{-i}^t, a) \), \( \forall i = 1, \ldots, n_G \), where \( n_G \) is the group size. Then we define the indicator \( c^t \) for the \( t \)-th task by:

\[
c^t = \arg \max_{j=1,\ldots,K+1} \frac{1}{n_G} \sum_{i=1}^{n_G} p \left( c_i^t = j \mid c_{-i}^t, a \right) ,
\]

(8)

Once \( c^t \) is determined, at the \( t \)-th task learning we only update the parameters of the chosen component instead of updating the whole model \( \Theta \), by maximizing the sample log-likelihood \( \log \int p_{\theta,S} (\mathbf{x} \mid z) p(z) \, dz \) which is intractable in optimization since we need integrating over \( z \). Similar to [16], we introduce to maximize a lower bound to the sample log-likelihood by using a variational distribution \( q_{\omega,c} (z \mid x) \) at \( t \)-th task learning:

\[
\log p_{\theta,c} (\mathbf{x}) \geq \mathbb{E}_{q_{\omega,c}} [ \log p_{\theta,c} (\mathbf{x} \mid z) ] - D_{KL} \left[ q_{\omega,c} (\mathbf{z} \mid \mathbf{x}) \parallel p(z) \right] ,
\]

(9)

where the right-hand side is our log-likelihood function \( F( \cdot | c^t, \theta_{\omega,c}, \omega_c ) \), called the Evidence Lower Bound (ELBO), used for training the model and the evaluation of Eq. (6). \( p_{\theta,c} (\mathbf{x} \mid z) \) and \( q_{\omega,c} (z \mid x) \) are decoding and encoding distributions, implemented by the network \( g_{\theta,c} : \mathcal{Z} \rightarrow \mathcal{X} \) and \( f_{\omega,c} : \mathcal{X} \rightarrow \mathcal{Z} \), respectively, where the subscript denotes the component index. In Lemma 4 from Appendix-F of the Supplementary Material (SM), we show how LIMix can infer across domains by the selection process.

### 3.3. Learning prediction tasks

In this section, we extend LIMix model for prediction tasks. Conditional VAEs [43] is one of the most used generative models for predictive tasks, defined by:

\[
\log p_{\nu,c} (y \mid x) \geq \mathbb{E}_{q_{\omega,c} (\mathbf{z} \mid x, y)} [ \log p_{\nu,c} (y \mid x, z) ] - D_{KL} ( q_{\omega,c} (\mathbf{z} \mid x, y) \parallel p_{\nu,c} (\mathbf{z} \mid x) ) .
\]

(10)

For classification, \( y \) belongs to the discrete domain (one-hot vector), and \( p_{\nu,c} (y \mid x, z) \) is implemented as a classifier. We represent \( p_{\nu,c} (z \mid x) \) as \( \mathcal{N}(0, I) \) in Eq. (10) for reducing the model size, and this results in the objective function:

\[
L_P = \mathbb{E}_{q_{\omega,c} (\mathbf{z} \mid x, y)} [ \log p_{\nu,c} (y \mid x, z) ] - D_{KL} ( q_{\omega,c} (\mathbf{z} \mid x, y) \parallel p(z) ) .
\]

(11)

We also require each component to learn a generator in order to overcome forgetting when reusing a selected component to model more than one task. Therefore, we define the ELBO for the generative model, \( p_{\theta,c} (x \mid y) \) as:

\[
L_G = \mathbb{E}_{q_{\omega,c} (\mathbf{z} \mid x, y)} [ \log p_{\nu,c} (x \mid z, y) ] - D_{KL} ( q_{\omega,c} (\mathbf{z} \mid x, y) \parallel p(z) ) .
\]

(12)

Each component in the classification setting has three models \( p_{\nu,c} (y \mid x, z), q_{\omega,c} (z \mid x, y), p_{\nu,c} (x \mid y, z) \). The likelihood function \( F(\cdot | c^t, \theta_{\nu,c}, \omega_{\nu,c} ) \) for the classification is only \( L_G \) and the main objective function for optimizing the \( c^t \)-th component is to maximize \( L_G + L_P \). In practice, we optimize \( L_P \) and \( L_G \) separately, in the same mini-batch. In Appendix-J from SM, we provide the framework for applying LIMix for Image-to-Image Translation tasks and in Appendix-M we provide the experimental results.

### 3.4. Training a compressed Student model

In order to reduce the complexity of LIMix, we propose to share most parameters of the generator and the inference models through a joint network, where the parameters \( \theta_i = \{ \theta_S, \hat{\theta}_i \} \) and \( \omega_i = \{ \omega_S, \hat{\omega}_i \} \) of each component consists of the shared part \( \{ \theta_S, \omega_S \} \) and the individual part \( \{ \hat{\theta}_i, \hat{\omega}_i \} \) for each component. The mixing components are built on top of the shared component. We also train a compressed Student model under the unsupervised learning only, aiming to embed knowledge from LIMix into one latent space which supports interpolation across multiple domains. The Student shares the same network architecture with the component and is trained using the knowledge distillation (KD) loss along with the sample log-likelihood at the \( t \)-th task learning:

\[
L_{stu} = \mathbb{E}_{S_{x,x}} \log p_{\theta_{stu}} (\mathbf{x}) + \sum_{i=1}^{K} \mathbb{E}_{p_{\theta,i}} \log p_{\theta_{stu}} (\mathbf{x})
\]

(13)

where \( \theta_{stu} = \{ \theta_S, \hat{\theta}_{stu} \} \) and \( \hat{\theta}_{stu} \) is the individual set for the Student. \( \log p_{\theta_{stu}} (\mathbf{x}) \) is estimated by ELBO and \( \mathbb{E}_{\theta_i} \) is the distribution modelled by the \( i \)-th component in LIMix. More details together with the LIMix model diagram are provided in Appendix-J from SM. Additionally, this paper does not focus on the improvement of KD and we find that the Student is weaker than LIMix. This is theoretically explained in Appendix-I.2 from SM.

### 4. Theoretical analysis for lifelong learning

In this section, we first provide the theoretical analysis for the proposed infinite mixture model that does not grow its architecture during the lifelong learning. In this case, the model uses GRM to overcome the catastrophic forgetting and is seen as a single model represented by \( \mathcal{M}(\theta, \varsigma, \varphi) \), consisting of a generator \( g_S : \mathcal{Z} \rightarrow \mathcal{X} \) and a classifier \( h_S : \mathcal{X} \rightarrow \mathcal{Y} \), where \( \mathcal{Y} \) is an output space, which is \( \{ -1, 1 \} \) for binary classification and \( \{ 1, 2, \ldots, n' \} \) for multi-class classification. We assume that the model also contains a task-inference network \( U_{c} : \mathcal{X} \rightarrow \mathcal{T} \) where \( \mathcal{T} \) is the task domain. We then provide theoretical guarantees for the convergence of LIMix. Eventually, we analyse the forgetting behaviour of existing methods and the trade-off between the model’s performance and complexity.
4.1. Preliminaries

Definition 1 (Approximation distribution). Let us define a joint distribution \( S^i \) approximated by the generator \( g_\theta \) and the classifier \( h_\phi \) of \( M(\theta^i, \phi^i) \) trained on a sequence of sets \( \{ D^i_1, \ldots, D^i_{M_1} \} \). We assume that we have a perfect task-inference network \( U_\varphi \), which can exactly predict the task label for a given sample \( x \). With the optimal task-inference network \( U_\varphi \), we can form several joint distributions \( \{ \tilde{S}^i_1, \ldots, \tilde{S}^i_{M_1} \} \) where each \( \tilde{S}^i_{(t-i+1)} \) is made up of a set of samples where each paired sample is drawn by using the sampling process \( \{ x, h_\varphi(x) \} \sim \tilde{S}^i \) if \( U_\varphi(x) = i \). We use the superscript \( (t-i+1) \) in \( \tilde{S}^i_{(t-i+1)} \) to denote that \( \tilde{S}^i_{(t-i+1)} \) is refined for \( (t-i+1) \) times through the GRM processes after the \( t \)-th task learning. We further use \( \tilde{S}^i_{(t-i+1)} \) to denote the marginal distribution of \( \tilde{S}^i_{(t-i+1)} \). \( \tilde{S}^i_{(t-i+1)} \) is formed by the samples from \( D^i_1 \) if \( n = 1 \), otherwise, by samples drawn from \( G_\theta \) and \( h_\phi \), with the optimal task-inference network.

Definition 2 (Data distribution across tasks). Let \( S_i \) represent the joint distribution characterizing the probabilistic representation for the testing set in the \( i \)-th database \( D^i_T \), and \( S_{i,X} \) is its marginal distribution along \( X \).

Assumption 1 We assume \( \tau : \mathcal{X} \times \mathcal{Y} \to [0, 1] \) be a symmetric and bounded loss function \( \forall (y, y') \in \mathcal{Y}^2 \), \( \tau(y, y') \leq M' \) and \( \tau(\cdot, \cdot) \) obeys the triangle inequality, where \( M' \) is a positive number.

Definition 3 (Discrepancy distance). For two given joint distributions \( \tilde{S}^i_{(t-i+1)} \) and \( S_i \) over \( X \times \mathcal{Y} \) and \( \tau : \mathcal{X} \times \mathcal{Y} \to [0, 1] \) is a loss function satisfying Assumption 1. Let \( h, h' \in \mathcal{H} \) be two classifiers, where \( \mathcal{H} \) is the space of all classifiers, and we define the discrepancy distance \( \Psi \) between the two marginals \( \tilde{S}_{i,X} \) and \( S_{i,X} \) as:

\[
\Psi(\tilde{S}_{i,X}, S_{i,X}) = \sup_{(h,h') \in \mathcal{H}^2} \left| E_{\tilde{S}^i_{(t-i+1)}} [\tau(h'(x), h(x))] - E_{S_{i,X}} [\tau(h'(x), h(x))] \right|.
\]

(14)

Definition 4 (Empirical risk). For a given loss function \( \tau : \mathcal{X} \times \mathcal{Y} \to [0, 1] \) and a joint distribution \( S_i \), we form an empirical set where we draw each paired sample as \( \{x_j, y_j\} \sim S_i \), the empirical risk \( R(h, S_i) \) for a given classifier \( h \in \mathcal{H} \) is evaluated by \( n \) number of independent runs.

\[
R(h, S_i) = \frac{1}{n} \sum_{j=1}^{n} \tau(h(x_j), y_j).
\]

(15)

4.2. Risk bounds for lifelong learning

The discrepancy distance, defined through Eq. (14), was used to derive generalization bounds for domain adaptation methods [3, 7, 26] and also for matching generated and real data distributions in the GAN’s discriminator during training [9, 21, 22]. In the following we derive the risk bound for the lifelong learning model based on the discrepancy distance. The main idea for analyzing the degenerated performance of the model is to evaluate the risk between the target and the dynamically degenerated source distribution caused by the retraining process using GRMs. In this case, the errors accumulated when learning each task can be measured in an explicit way.

Theorem 1 Let \( S_i \) and \( \tilde{S}^i_{(t-i+1)} \) be two joint distributions over \( X \times \mathcal{Y} \). Let \( h_i = \arg \min_{h \in \mathcal{H}} R(h, S_i) \) and \( \tilde{h}^i_{(t-i+1)} = \arg \min_{h \in \mathcal{H}} R(h, \tilde{S}^i_{(t-i+1)}) \) represent the ideal classifiers for \( S_i \) and \( \tilde{S}^i_{(t-i+1)} \), respectively, where \( \mathcal{H} \) is the classifier space. By satisfying Assumption 1, we have:

\[
R(h, S_i) \leq R'(h, \tilde{h}^i_{(t-i+1)}, \tilde{S}^i_{(t-i+1)}) + \Psi(S_{i,X}, \tilde{S}_{i,X}) + \sigma(S_i, \tilde{S}^i_{(t-i+1)})
\]

(16)

where the optimal combined error is represented by

\[
\sigma(S, \tilde{S}^i_{(t-i+1)}) = R'(h^*_i, h_i, S_i) + R'(h_i, \tilde{h}^i_{(t-i+1)}, \tilde{S}^i_{(t-i+1)})
\]

(17)

and

\[
R'(h^*_i, h_i, S_i) = E_{x - S_{i,X}} \tau(h^*_i(x), h_i(x)),
\]

(18)

where \( h^*_i \) is the true labeling function for \( S_i \).

We provide the proof in the Appendix-A from SM. This theorem provides a way to measure the gap on the risk bound for the model, after learning the \( t \)-th task, but does not provide any insight on how the previously learnt knowledge is forgotten. The following theorem provides an explicit way to measure the accumulated errors when learning a certain task.

Theorem 2 Let \( \tilde{S}^i_{(t-i+1)} \) be the joint distribution over \( X \times \mathcal{Y} \), and \( \tau \) be a loss function which satisfies Assumption 1. The accumulated errors in the knowledge associated with a previously learnt, \( i \)-th task, after learning a given \( t \)-th task, can be defined as:

\[
R(h, S_i) \leq R'(h, \tilde{h}^i_{(t-i+1)}, \tilde{S}^i_{(t-i+1)}) + \sum_{k=0}^{t-1} \left( \Psi(\tilde{S}^k_{i,X}, \tilde{S}^k_{i,X}) + \sigma(\tilde{S}^k_{i}, \tilde{S}^k_{i}) \right),
\]

(19)

where the last term of the right hand side (RHS) is expressed as:

\[
\sigma(\tilde{S}^k_{i}, \tilde{S}^k_{i}) = R'(\tilde{h}^k_i, h_i, \tilde{S}^k_{i}) + R'(\tilde{h}^k_i, \tilde{h}^k_{(t-k-1)}, \tilde{S}^k_{i})
\]

(20)
In practice, the number of components is smaller than the number of tasks being learnt. This explains that $M(\theta^t, \psi^t, \varphi^t)$ would tend to forget the tasks learnt earlier during its lifelong learning process. We visualize this forgetfulness process in Figure 1.

**Lemma 1** Let us consider that we have Assumption 1, then the accumulated error after learning the probabilistic representations of all databases after $t$-th task learning is:

$$
\sum_{i=1}^{t} R(h, S_i) \leq \sum_{i=1}^{t-1} \left( R'(h, \tilde{n}_{i+1}^t, \tilde{S}_i^t) + \sum_{k=0}^{t-i} \left( \Psi(\tilde{S}_{i+k}^t, \tilde{S}_{i+k}^t) + \sigma(\tilde{S}_i^t, \tilde{S}_{i+k}^t) \right) \right).
$$

We consider Theorem 2 and sum up the accumulated errors from Eq. (19) for learning $t$ tasks and this results in Eq. (21) (Appendix-C from SM). Lemma 1 shows that minimizing the discrepancy distance $\Psi(\tilde{S}_{i+k}^t, \tilde{S}_{i+k}^t)$ between the generated distribution approximated by the model and the target distributions, when learning each task, plays an important role in the improvement of the performance. However, the accumulated errors of the model will increase significantly when increasing the number of new tasks to be learnt. The following lemma shows how a mixture or ensemble model can address this problem and improve the performance.

**Lemma 2** Let us consider Assumption 1 and assume that we are training the LIMix model with $K$ components onto the $t$-th task learning. If $K = t$, then the accumulated errors of the infinite mixture model for all tasks is defined as:

$$
\sum_{i=1}^{t} R(h, S_i) \leq \sum_{i=1}^{t-1} \left( R'(h, \tilde{n}_i, \tilde{S}_i^1) + \Psi(\tilde{S}_{i,X}, \tilde{S}_{i,X}) + \sigma(\tilde{S}_i, \tilde{S}_i^1) \right).
$$

We provide the proof in Appendix-D from SM. Lemma 2 provides the framework for an optimal solution for LIMix in which the lifelong learning problem is transformed into a generalization problem under multiple target-source domains where there is no forgetting error during the training. $h$ is implemented by the mixture of $\{h_{s_i}, \ldots, h_{s_{K}}\}$, $h_{s_i} \in \mathcal{H}$, $i = 1, \ldots, K$ in LIMix and therefore the performance on each target domain is relying on the generalization ability of the associated component. In practice, the number of components is smaller than the number of tasks being learnt. We investigate a specific case in Appendix-D from SM. The following lemma provides an analysis of the relationship between the model’s performance and complexity.

**Lemma 3** Let $B = \{b_1, \ldots, b_n\}$ represent the labels for the tasks that the corresponding distributions $\{S_{b_1}, \ldots, S_{b_n}\}$ are accessed only once after lifelong learning. Let $B' = \{b'_1, \ldots, b'_m\}$ indicate which task was used for re-training more than once. We also define a set $B = \{b_1, \ldots, b_n\}$ that records how many times each task was used for re-training, where $b_i > 1$ represents that the $b_i$-th task has been retrained for $(b_i - 1)$ times $S_{b_i}^{(1)} \rightarrow S_{b_i}^{(b_i)}$.

$$
\hat{\psi}(\tilde{S}_{b_i}^{b_i}) \text{ represents that the } b_i \text{ component is implemented by the mixture of } \{h_{s_i}, \ldots, h_{s_{K}}\}, h_{s_i} \in \mathcal{H}, i = 1, \ldots, K \text{ in LIMix.}
$$

where $\hat{\psi}(\tilde{S}_{b_i}^{b_i})$ represents the corresponding probabilistic representation. For a given mixture model, we have:

$$
\sum_{i=1}^{t} R(h, S_i) \leq \sum_{i=1}^{\text{card}(B)} \left( R'(h, \tilde{n}_i, \tilde{S}_{b_i}^{1}) + \Psi(\tilde{S}_{b_i}^{1}, \tilde{S}_{b_i}^{1}) + \sum_{k=0}^{\text{card}(B')} \left( \Psi(\tilde{S}_{b_i}^{k}, \tilde{S}_{b_i}^{k+1}) + \sigma(\tilde{S}_{b_i}^{k}, \tilde{S}_{b_i}^{k+1}) \right) \right) = R_{\text{mixture}}
$$

where $t > 1$ represents the number of tasks being learnt, $\text{card}()$ denotes the cardinal number in the set which satisfies $\text{card}(B) + \text{card}(B') > K$ and $0 \leq \text{card}(B) \leq K$, $0 \leq \text{card}(B') \leq K$, $\text{card}(B') = \text{card}(B)$, where $K$ is the number of components used for training. The risk for a single learnt model $M(\theta^t, \psi^t, \varphi^t)$ is defined as $R_{\text{single}}$, as in Eq. (21), while the risk for the mixture model, $R_{\text{mixture}}$, is the RHS of Eq. (23). From all these expressions we have $R_{\text{single}} \geq R_{\text{mixture}}$.

The proof is in the Appendix-E from SM. Lemma 3 does not explicitly indicate which task is associated with the information recorded by a specific component of the LIMix model. Nevertheless, we provide an explicit way to analyse the risk bound for the mixture model in a more practical way, where we vary the number of components and the number of times the model was trained for each task, according to different learning settings such as by considering the learning order of tasks or their complexity. If $B' = \emptyset$, then Eq. (23) is reduced to Eq. (22), meaning a smaller gap in the risk bound, while requiring additional memory. On the other hand, if $\text{card}(B) = 1 \Rightarrow B = \{\}$, the RHS of Eq. (23) becomes equal to that from Eq. (21), meaning a large gap on the risk bound. We define the ratio $v = (K - \text{card}(B))/ (K - \text{card}(B'))$ as an index which explains the trade-off between the model complexity and its performance. When $v$ increases, the model improves its performance while also increasing its complexity. In contrast, when $v$ is small, the model’s complexity is reduced.
while it accumulates more error terms when learning new tasks. In the Appendix-G from SM, we use the proposed theoretical framework to analyse the forgetting behaviour for various models such as the classical GRM model [41], a mixture model enabled with expansion mechanisms [34], an ensemble model from [47] and an episodic memory model [25, 30]. We also extend Lemmas 2 and 3 for analyzing the risk bounds for a model when changing the order of tasks in the Appendix-H from SM.

5. Experiments

5.1. Datasets and evaluation criteria

We consider the following experimental settings:

- For the unsupervised learning setting we create a sequence of learning tasks corresponding to the databases: MNIST [19], SVHN [27], Fashion [49], InverseFashion (IFashion) and Rated MNIST (RMNIST), and this learning setting is named MSFIR.
- We add CIFAR10 [18] after MSFIR, as the last training task, resulting in MSFIRC sequence for supervised classification. All images are resized to $32 \times 32 \times 3$.

Evaluation criteria: In the classification tasks, we use the average accuracy over all tasks as the performance criterion. Although the proposed theoretical analysis is only used in prediction tasks, LIMix can also achieve good performance in the unsupervised setting where we use the Mean Squared Error (MSE), the structural similarity index measure (SSIM) [13] and the Peak-Signal-to-Noise Ratio (PSNR) [13] for the reconstruction quality evaluation.

5.2. Unsupervised learning tasks

We firstly evaluate various methods on MSFIR lifelong learning tasks and the results are provided in Table 1. We compare our proposed LIMix model with three state of the art methods: LGM [33], CURL [34] and BatchEnsemble (BE) [47]. BE is designed to be used for classification tasks and we implement BE as an ensemble made up of VAE components, where each VAE has a tuple of trainable vectors built on the top layer of a neural network which does not update its parameters in the $k$-th task learning, $k = \{2, 3, \ldots, K\}$. We use large neural networks, containing more parameters, for LGM and BE, respectively, in order to ensure fair comparisons. The model size is provided in Appendix-L from SM. “Stud” denotes the performance of the Student model which is worse than LIMix because the Student learns its knowledge from the generation results of LIMIX. Fig. 2a shows the absolute difference on the log-likelihood between the incoming task and each component $K_{i,j}$, as in Eq. (6), and the number of components derived during MSFIR lifelong learning. We can observe that the first component is reused when learning the fifth task (RMNIST) and LIMix expands to 4 components after LLL. We also evaluate the LIMix model when considering more complicated tasks in the Appendix-K.2 from SM.

5.3. Classification tasks

In this section we present the results when considering the lifelong learning of classification tasks. In order to use LGM [33] for classification, we continually train an auxiliary classifier on the real data samples from successive tasks and by also using paired data samples $\{x_i, y_i\}_{i=1}^n$, where $x_i$ is generated by either the Teacher or Student in LGM and each $y_i$ is inferred by the classifier during the last task learning. Table 2 provides the LLL classification accuracy, where it can be observed that LIMix achieves the best results. Unlike in the image reconstruction results, CURL [34] also provides good results on the LLL of classification tasks. CURL uses a single decoder which is continually updated across multiple tasks and therefore leads to poor image reconstructions, which explains the difference between the reconstruction and the classification results for CURL.

Although the proposed LIMix is mainly designed for cross-domain lifelong learning, we also apply LIMix to the continuous learning benchmarks, Permuted MNIST and Split MNIST [58] (see Appendix-K.4 from SM). Similar to [30], we use a smaller network for the implementation of each component and perform five independent runs for cal-

<table>
<thead>
<tr>
<th>Datasets</th>
<th>MSE</th>
<th>SSMI</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LGM</td>
<td>CURL</td>
<td>BE</td>
</tr>
<tr>
<td>MNIST</td>
<td>129.93</td>
<td>211.21</td>
<td>19.24</td>
</tr>
<tr>
<td>Fashion</td>
<td>89.28</td>
<td>110.60</td>
<td>36.52</td>
</tr>
<tr>
<td>SVHN</td>
<td>169.55</td>
<td>102.06</td>
<td>39.57</td>
</tr>
<tr>
<td>IFashion</td>
<td>432.90</td>
<td>115.29</td>
<td>36.52</td>
</tr>
<tr>
<td>RMNIST</td>
<td>130.28</td>
<td>279.47</td>
<td>25.44</td>
</tr>
<tr>
<td>Average</td>
<td>190.38</td>
<td>163.72</td>
<td>31.91</td>
</tr>
</tbody>
</table>

Table 1. The performance of various models after the MSFIR lifelong learning.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>MSE</th>
<th>SSMI</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>90.54</td>
<td>91.30</td>
<td>99.40</td>
</tr>
<tr>
<td>SVHN</td>
<td>22.56</td>
<td>62.05</td>
<td>74.46</td>
</tr>
<tr>
<td>Fashion</td>
<td>68.29</td>
<td>79.18</td>
<td>88.95</td>
</tr>
<tr>
<td>IFashion</td>
<td>73.70</td>
<td>82.51</td>
<td>86.45</td>
</tr>
<tr>
<td>RMNIST</td>
<td>90.52</td>
<td>98.56</td>
<td>99.10</td>
</tr>
<tr>
<td>CIFAR10</td>
<td>57.43</td>
<td>67.34</td>
<td>52.48</td>
</tr>
<tr>
<td>Average</td>
<td>67.17</td>
<td>80.16</td>
<td>83.47</td>
</tr>
</tbody>
</table>

Table 2. Classification accuracy of various models after the MSFRC lifelong learning.
Figure 2. (a) Absolute difference on the log-likelihood and the number of components under the MSFIR lifelong learning. (b) The change of the model’s performance and complexity when using different thresholds during MSFIR lifelong learning. (c) The risk and discrepancy for the first task (MNIST) by using LIMix without expansion. (d) The risk and discrepancy for MNIST by using LIMix with expansion.

Table 3. Results of continuous learning benchmark.

<table>
<thead>
<tr>
<th>Methods</th>
<th>Permutated MNIST</th>
<th>Split MNIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP* [42]</td>
<td>82%</td>
<td>61.2%</td>
</tr>
<tr>
<td>EWC* [17]</td>
<td>84%</td>
<td>63.1%</td>
</tr>
<tr>
<td>SI* [58]</td>
<td>86%</td>
<td>98.9%</td>
</tr>
<tr>
<td>Improved VCL* [45]</td>
<td>93.1 ± 1%</td>
<td>98.4 ± 0.4%</td>
</tr>
<tr>
<td>FRCL-RND* [46]</td>
<td>94.2 ± 0.3%</td>
<td>97.1 ± 0.7%</td>
</tr>
<tr>
<td>FRCL-TR* [46]</td>
<td>94.3 ± 0.2%</td>
<td>97.8 ± 0.7%</td>
</tr>
<tr>
<td>FROMP* [30]</td>
<td>94.9 ± 0.1%</td>
<td>99.0 ± 0.1%</td>
</tr>
</tbody>
</table>

LIMix | 96.46 ± 0.03% (10 C) | 99.21 ± 0.04% (5 C) |
LIMix | 88.78% (7 C)        | 96.77% (4 C)        |
LIMix | 95.25% (8 C)        | 91.37% (3 C)        |

5.4. Ablation study and theoretical results

We evaluate the performance of the LIMix model when varying various hyperparameters and thresholds and the results are shown in Figures 2a and 2b. The performance is improved by expanding the model’s architecture, but this would increase its complexity, as discussed in Lemma 3. We provide additional results for the hyperparameter parameter setting in the Appendix-K.1 from SM. We investigate the theoretical results for Theorem 2 and train a single model under MNIST, Fashion and SVHN (MFS) learning setting and evaluate the source-risk, target-risk and discrepancy on MNIST and present the results in Fig. 2c. We can observe that the increase of the target-risk largely depends on the discrepancy instead of the source-risk which keeps stable when learning additional tasks. We also investigate the results for LIMix under MFS lifelong learning and the results are provided in Fig. 2d, where “Source + Discrepancy” represents the source-risk plus the discrepancy on MNIST. The discrepancy does not increase for LIMix when learning additional tasks. Besides, “Source + Discrepancy” is very close to the target-risk and the gap to the target-risk is the combined error $\sigma(S_1, S_1^t)$, according to Eq. (19).

We also investigate the target-risk for LIMix, BE, and LGM and the results are shown in Fig 3a, where the target-risk is evaluated on MNIST for each epoch. The target-risk for BE does not change across the LLL of six tasks, given that it does not accumulate any errors. LGM continually increases its target-risk, which is bounded by $R_{Single}$, adding an error term after learning each task. LIMix only increases the target-risk when it reuses a component, which was updated when learning RMNIST after MNIST. These results are explained by Lemma 3 and further explored in Appendix-G from SM. We also estimate the average target-risk for all tasks (20 epochs for each task) when reusing a component trained on MNIST for learning a new task and the results are shown in Fig. 3b. We find that a single component would lead to a large degeneration in the performance when learning an entirely different task (CIFAR10) than a related task (RMNIST). This demonstrates that the proposed selection mechanism can choose an appropriate component minimizing the target-risk. Examples of image reconstruction, generation and Image to Image translation are shown in the Appendix-M from SM.

6. Conclusion

We propose a new theoretical analysis framework for lifelong learning based on the discrepancy distance between the probabilistic measures of the knowledge already learnt by the model and a target distribution. We provide an insight into how the model forgets some of the knowledge acquired during LLL, through the analysis of the model’s risk. Inspired by the analysis, we propose LIMix model which performs better in cross-domain lifelong learning.
References


