Lifelong Variational Autoencoder via Online Adversarial Expansion Strategy

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
The Variational Autoencoder (VAE) suffers from a significant loss of information when trained on a non-stationary data distribution. This loss in VAE models, called catastrophic forgetting, has not been studied theoretically before. We analyse the forgetting behaviour of a VAE in continual generative modelling by developing a new lower bound on the data likelihood, which interprets the forgetting process as an increase in the probability distance between the generator’s distribution and the evolved data distribution. The proposed bound shows that a VAE-based dynamic expansion model can achieve better performance if its capacity increases appropriately considering the shift in the data distribution. Based on this analysis, we propose a novel expansion criterion that aims to preserve the information diversity among the VAE components, while ensuring that it acquires more knowledge with fewer parameters. Specifically, we implement this expansion criterion from the perspective of a multi-player game and propose the Online Adversarial Expansion Strategy (OAES), which considers all previously learned components as well as the currently updated component as multiple players in a game, while an adversary model evaluates their performance. The proposed OAES can dynamically estimate the discrepancy between each player and the adversary without accessing task information. This leads to the gradual addition of new components while ensuring the knowledge diversity among all components. At each training step, the generator, discriminator, and fake images, which are then fed into the discriminator while all other components are frozen. At the evaluation phase, we treat the generation of all previously learnt components and the current component as real and fake images, which are then fed into the discriminator for deciding the model’s expansion.

Bound (ELBO), used as its objective function:

\[
\log p_{\theta}(x) \geq \mathbb{E}_{q_{\omega}(z|x)} \left[ \log p_{\theta}(x|z) \right] - D_{KL} \left[ q_{\omega}(z|x) \| p(z) \right] = \mathcal{ELBO}(x; \theta, \omega),
\]

where \( p(z) = \mathcal{N}(0, I) \) and \( p_{\theta}(x|z) \) are the prior and decoding distribution, respectively. \( D_{KL}[] \) is the Kullback–Leibler divergence. Existing works aiming for the improvement of VAE are mainly deriving a tighter ELBO to the data log-likelihood, which is implemented by using importance sampling (Burda, Grosse, and Salakhutdinov 2015; Domke and Sheldon 2018), a more expressive posterior (Kim and Pavlovic 2020; Maaløe et al. 2016; Kim and Pavlovic 2020), or hierarchical variational models (Molchanov et al. 2019; Vahdat and Kautz 2020).

However, these methods can only guarantee a tight ELBO for a static data domain and do not consider the circumstances of lifelong learning. Recently, (Ye and Bors 2022f)

Introduction
The Variational Autoencoder (VAE) (Kingma and Welling 2013) is one of the most popular deep generative models, which defines an encoding-decoding process for images. A VAE consists of two modules: an inference model mapping an image \( x \) to a low-dimensional latent variable \( z \) and a decoder recovering \( x \) from \( z \). The VAE is a likelihood-based model which is optimized by maximizing the sample log-likelihood \( \log p_{\theta}(x) = \log \int p_{\theta}(x|z)p(z)dz \). However, this objective function is intractable for optimization since it requires integrating over all \( z \). A VAE introduces a lower bound to the sample log-likelihood, called Evidence Lower
provided for the first time a theoretical analysis for the forgetting behaviour of VAEs. However, this theoretical analysis requires two strong assumptions: a Gaussian decoder and knowing the task information. These two assumptions are not guaranteed in a more realistic continual learning scenario called Task-Free Continual Learning (TFCL) (Aljundi, Kelchtermans, and Tuytelaars 2019), where task identity is unavailable. In this paper, we focus on the realistic CL scenario and develop a novel theoretical framework for the VAE, which overcomes the limitations of the previous work (Ye and Bors 2022f). The proposed theoretical framework interprets the forgetting process of VAEs as an increase in the Jensen-Shannon divergence (JS) between the generator and evolved data distribution, which provides new insights into the forgetting behaviour of VAEs under TFCL. Furthermore, the proposed theoretical analysis shows that a VAE-based Dynamic Expansion Model (DEM), which appropriately increases its capacity when facing the data distribution shift, can significantly improve its performance. This takes place while also maintaining the knowledge diversity among components while inducing a compact model structure without sacrificing the performance (Theorem 3).

Inspired by the proposed theoretical analysis, we aim to learn a diverse VAE-based Dynamic Expansion Model (VAE-DEM) for TFCL. Unlike other dynamic expansion criteria (Rao et al. 2019), which recognise input shifts as expansion signals, we implement a dynamic criterion derived from a novel perspective, that of a multi-player game. More specifically, we can consider all the previously learned VAE components and the currently updated VAE component as multiple players while an adversary discriminator estimates the discrepancy between each player and the adversary, as an evaluator. In contrast to traditional adversarial learning (Goodfellow et al. 2014), which learns a static data domain with only two players, we propose the Online Adversarial Expansion Strategy (OAES), which can learn a non-stationary data distribution and dynamically add new players during training. OAES consists of two stages, as shown in Fig. 1. In the first stage (training), we use an episode memory to store some past samples that are used to train a generator and a discriminator using adversarial learning (Eq. (14)) while training the current VAE component (‘VAE t’) using VAE loss (Eq. (1)) as well. In the second phase (evaluation), we treat the data generations by all players (‘VAE 1’, . . . , ‘VAE t−1’) and by the adversary (‘VAE t’) as the real and fake images, which are fed into the discriminator to produce t − 1 pairs of probability measures. We evaluate the difference between each pair of measures as the discrepancy value for each player and the adversary, which guides us to dynamically add a new adversary (‘VAE t+1’) and transfer (‘VAE t’) to the player if (‘VAE t’) learns sufficient novel knowledge. Such a strategy promotes information diversity among components during expansion leading to learning a compact and diverse VAE-DEM for TFCL. Extensive experiments show that OAES can significantly improve the performance of VAE-DEM for TFCL with a minimum number of components.

We summarize our contributions as follows: (1) We propose a novel theoretical framework that provides new insights into the forgetting behaviour of the VAE model under TFCL; (2) The theoretical analysis can be used in realistic continual learning scenarios without the need to know task boundaries; (3) We extend the proposed theoretical framework to analyze the forgetting behaviour of existing VAE models (Appendix-F from Supplemental Material (SM)); (4) Inspired by the theoretical analysis, we propose a plug-and-play dynamic expansion strategy which can be used in any VAE model; (5) To the best of our knowledge, this is the first work to propose a novel solution for model expansion in TFCL from the perspective of an adversarial criterion; (6) The proposed approach achieves state of the art performance in both classification and generative tasks. Supplementary materials (SM) and source code are available.

## Related Work

### Continual learning

A natural approach to relieve forgetting in CL is to build a memory-based replay system, which stores some past training samples from each task and replays them during the subsequent task learning (Bang et al. 2021, 2022). Memory-based approaches can further improve the performance by combining with regularization methods (Kirkpatrick et al. 2017; Kemker et al. 2018; Martens and Grosse 2015; Aljundi et al. 2019b; Chaudhry et al. 2019, 2018; Lopez-Paz and Ranzato 2017; Derakhshani et al. 2021; Shi et al. 2021; Wang et al. 2021; Nguyen et al. 2017; Ahn et al. 2019). In addition, training a generator such as a Generative Adversarial Network (GAN) (Goodfellow et al. 2014) or a Variational Autoencoder (VAE) (Kingma and Welling 2013), used to produce generative samples corresponding to past tasks, was shown to effectively relieve forgetting in CL (Ramapuram, Gregororova, and Kalousis 2020; Rao et al. 2019; Ye and Bors 2021a, 2020a, 2022f, 2023, 2022a, 2021b, 2022d, 2020b). The other approach in CL is to dynamically build new hidden layers, which would preserve the best performance for past tasks (Ye and Bors 2022c; Hung et al. 2019; Li and Hoiem 2017; Polikar et al. 2001; Rao et al. 2019; Rusu et al. 2016; Wen, Tran, and Ba 2020; Xiao et al. 2014; Ye and Bors 2020c, 2021a, 2023; Zhou, Sohn, and Lee 2012).

### Task-Free Continual Learning

TFCL defines a realistic situation in CL, which has attracted recently significant attention. The first work in TFCL (Aljundi, Kelchtermans, and Tuytelaars 2019) trains a classifier with a memory buffer. This approach was extended to train both VAEs and classifiers through a retrieval mechanism that selectively stores the most perturbed samples, called the Maximal Interfered Retrieval (MIR) (Aljundi et al. 2019a). The approach from (Aljundi et al. 2019b) further treats the sample selection of the memory buffer as a constrained optimization problem, called the Gradient Sample Selection (GSS). More recently, (De Lange and Tuytelaars 2021) propose a new learner-evaluator framework which manages a balanced memory buffer, called the Continual Prototype Evolution (CoPE). The Gradient-based Memory Editing (GMED) (Jin et al. 2021) modifies the memorized samples such that it increases the loss in the upcoming model updates. However, these

---

1https://github.com/dtuzi123/OAES
memory-based methods are not scalable for learning infinite data streams due to their fixed memory capacity. The Dynamic Expansion Model (DEM) can solve these limitations by dynamically expanding the model’s capacity to deal with incoming samples (Rao et al. 2019; Lee et al. 2020; Ye and Bors 2022e). However, the expansion mechanism in these approaches relies on the sample log-likelihood evaluation (Rao et al. 2019) or the Dirichlet process (Lee et al. 2020), which do not have theoretical guarantees.

**Variational Autoencoder.** The tightness of the VAE objective function (ELBO) is crucial for improving the performance of the VAE. One possible approach is to use the Importance Weighted Autoencoder (IWELBO) (Burda, Grosse, and Salakhutdinov 2015), which generates a set of weighted samples for the given input resulting in a tighter ELBO. Another approach aims to use a more informative approximate posterior distribution, such as the Normalizing Flows (Kingma et al. 2016; Rezende and Mohamed 2015), Implicit Distributions (Mescheder, Nowozin, and Geiger 2017) or the Hierarchical Variational Inference (Huang et al. 2019). Moreover, these approaches can further improve performance by integrating the IWELBO loss into their primary objective function. In addition, online variation inference (Nguyen et al. 2017) was used in the VAE framework, but it requires to store a subset of training samples for computing the approximate posterior which is impractical for learning an unlimited number of tasks. Moreover, the study of the ELBO’s tightness under TFCL has not been explored before.

**Preliminary**

We first introduce the learning setting of TFCL and then the probabilistic representation of each data domain.

**Definition 1 (The stream of data samples.)** Let us define $D_{n}^{S} = \{x_{j}^{S}|_{j=1}^{n(S,k)}\}$ and $D_{n}^{T} = \{x_{j}^{T}|_{j=1}^{n(T,k)}\}$ be the unlabelled training and testing sets of the k-th domain/dataset, where $x_{j}^{S}$ is the unlabelled data sample. $n(S,k)$ and $n(T,k)$ represent the total number of samples for $D_{n}^{S}$ and $D_{n}^{T}$, respectively. $D_{n}^{S}$ can be divided into $C(S,k)$ parts according to the category or the task information, expressed as $\{D_{1}^{S}(k), \ldots, D_{C(S,k)}^{S}(k)\}$. In TFCL, where there are no task labels, each $D_{n}^{S}(j,k)$ is represented by its probabilistic representation $P_{n}^{S}(i,k)$. Let us define a data stream in a class-incremental manner:

$$W = \bigcup_{j=1}^{C(S,k)} D_{n}^{S}(j,k), \tag{2}$$

At the i-th training step ($T_{i}$), the model only accesses a data batch $B_{i} \in D_{n}^{S}$ with the batch size of 10. Once the model finishes all training steps, its performance is evaluated on the testing set $D_{n}^{T}$.

In the following we define a VAE model and a fixed-length memory buffer which continually stores training samples from W during training.

**Definition 2 (VAE model.)** Let $\mathcal{V}^{i}$ be a single model updated at $T_{i}$, where i represents the index of the training step. $\mathcal{V}^{i}$ consists of an inference model $q_{\theta^{i}}(z|x)$ and the generator $p_{\psi^{i}}(x|z)$. Let $P_{\psi^{i}}$ represent the generator’s distribution.

**Definition 3 (Memory buffer.)** Let $\mathcal{M}_{i}$ denote a memory buffer updated at $T_{i}$. Let $|\mathcal{M}_{i}|$ and $|\mathcal{M}_{i}|^{\max}$ represent the number of memorized samples and the maximum memory size, respectively. Let $P_{\mathcal{M}_{i}}$ denote the distribution of the memory buffer $\mathcal{M}_{i}$ updated at $T_{i}$.

**Theoretical Framework**

**Forgetting Analysis of a Single VAE Model**

The VAE is a likelihood model and a higher log-likelihood estimation indicates a good performance of the VAE (Chen et al. 2018), which, however, is only evaluated on a static distribution. In this section, we develop a novel lower bound to the sample log-likelihood, which can be used to analyze the VAE’s performance on a non-stationary data distribution.

**Theorem 1** Let $p_{\psi^{i}}(x)$ be a probability density function for a single model $\mathcal{V}^{i}$ updated at $T_{i}$. Let $P_{\mathcal{M}_{i}}$ denote a distribution of all visited data batches $\{B_{i}, \ldots, B_{n}\}$ drawn from $W$ at $T_{i}$. Let $p_{\mathcal{M}_{i}}(x)$ and $p_{\psi^{i}}(x)$ denote the density functions for $P_{\mathcal{M}_{i}}$ and $P_{\psi^{i}}$, respectively. We then derive a lower bound for a single VAE model trained on $\mathcal{M}_{i}$ at $T_{i}$ as:

$$E_{P_{\psi^{i}}} [\log p_{\psi^{i}}(x)] \geq E_{P_{\mathcal{M}_{i}}} [\log p_{\psi^{i}}(x)] - D_{JS}(P_{\psi^{i}}||P_{\mathcal{M}_{i}}) - F_{DL}(P_{\mathcal{M}_{i}}, P_{\psi^{i}}, P_{\psi^{i}}) + F_{dis}(P_{\psi^{i}}, P_{\mathcal{M}_{i}}), \tag{3}$$

where we have:

$$F_{DL}(P_{\mathcal{M}_{i}}, P_{\psi^{i}}, P_{\psi^{i}}) \triangleq |D_{KL}(P_{\mathcal{M}_{i}}||P_{\psi^{i}})|, \tag{4}$$

$$F_{dis}(P_{\psi^{i}}, P_{\mathcal{M}_{i}}) \triangleq E_{P_{\psi^{i}}} [p_{\psi^{i}}(x) \log p_{\psi^{i}}(x)] - E_{P_{\mathcal{M}_{i}}} [p_{\mathcal{M}_{i}}(x) \log p_{\psi^{i}}(x)]. \tag{5}$$

We can observe that $F_{dis}(P_{\psi^{i}}, P_{\mathcal{M}_{i}})$ is constant if and only if $P_{\psi^{i}}$ and $P_{\mathcal{M}_{i}}$ are fixed. $F_{dis}(P_{\psi^{i}}, P_{\mathcal{M}_{i}})$ is bounded by $|D_{KL}(P_{\psi^{i}}||P_{\mathcal{M}_{i}})| - |D_{KL}(P_{\mathcal{M}_{i}}||P_{\psi^{i}})|$. From Eq. (3), we can estimate the sample log-likelihood of $P_{\psi^{i}}$ by ELBO:

$$E_{P_{\psi^{i}}} [\log p_{\psi^{i}}(x)] \geq E_{P_{\mathcal{M}_{i}}} [\mathcal{L}_{ELBO}(x; \theta^{i}, \omega^{i})] - D_{JS}(P_{\psi^{i}}||P_{\mathcal{M}_{i}}) - F_{DL}(P_{\mathcal{M}_{i}}, P_{\psi^{i}}, P_{\psi^{i}}) + F_{dis}(P_{\psi^{i}}, P_{\mathcal{M}_{i}}), \tag{6}$$

where $D_{JS}$ is the Jensen-Shannon divergence. We then find that Eq. (6) can be recovered to a standard ELBO (Eq. (1)) if and only if $P_{\psi^{i}}$ is equal to $P_{\mathcal{M}_{i}}$. We provide the proof in Appendix-B from SM1.

**Remark.** We have several observations from Theorem 1:

(1) The term $D_{JS}(P_{\psi^{i}}||P_{\mathcal{M}_{i}})$ in Eq. (6) plays an important role for the generalization performance. Reducing $D_{JS}(P_{\psi^{i}}||P_{\mathcal{M}_{i}})$ would lead to increasing the right-hand-side (RHS) of Eq. (6) and therefore the model $\mathcal{V}^{i}$ can have a good performance on $P_{\psi^{i}}$. (2) A large $D_{JS}(P_{\psi^{i}}||P_{\mathcal{M}_{i}})$ indicates a significant reduction in the RHS of Eq. (6), resulting in a poor performance on $P_{\psi^{i}}$. This usually happens when the memory buffer does not store sufficient information about $P_{\psi^{i}}$, due to the forgetting process; (3) Unlike the theoretical analysis from (Ye and Bors 2022f, 2021a) which
relies on the task information, Eq. (3) can analyze the forgetting behaviour of a single VAE model without accessing any task information at each training step. In the following, we evaluate the generalization performance achieved by a single model on the target set.

**Lemma 1** Let \{\(D^T(1, k), \cdots, D^T(C(T, k), k)\)\} be several target sets, where each \(D^T(j, k)\) is represented by the probabilistic representation \(P_{(j, k)}\). We derive a lower bound to the sample log-likelihood for a single VAE model \(V^i\) at \(T_i\):

\[
\begin{align*}
    C(T, k) \sum_{j=1}^{C(T, k)} \{E_{p_{\Phi}}[\log p_{\Phi}(\mathbf{x})]\} & \geq \sum_{j=1}^{C(T, k)} \{F_{\text{dis}}(P_{(j, k)}, P_{M_i}) \}
    + \mathbb{E}_{\hat{P}_{M_i}}[\mathcal{L}_{\text{ELBO}}(\mathbf{x}; \theta^i, \omega^i)] - D_{JS}(P_{(j, k)} \parallel P_{M_i}) \\
    & - \mathcal{F}_{\text{DL}}(P_{M_i}, P_{(j, k)}, P_{\Theta^i}) \},
\end{align*}
\]

Eq. (3) indicates that encouraging the sample diversity in the memory would help forgetting by minimizing the JS divergence terms since the diversity can allow \(\mathcal{M}_i\) to store the information corresponding to all target sets, empirically demonstrated in (Bang et al. 2021); (2) In practice, a single model has significant limitations when aiming to learn infinite data streams or a data stream involving more underlying distributions (\(C(T, k)\) is large). In addition, a single model would also suffer from interference between the old and newly seen samples (Lee, Goldt, and Saxe 2021). In the following, we provide the theoretical analysis and show how the Dynamic Expansion Model (DEM) can overcome the limitations of a single model.

**Forgetting Analysis of DEM**

The DEM can dynamically adapt its network architecture according to the complexity of the data stream. In this section, we theoretically demonstrate that the DEM can achieve better generalization performance than a single model.

**Definition 4 Dynamic expansion model (DEM).** Let us define a DEM, \(\mathbf{V} = \{V_1^c, \cdots, V^n_c\}\) with \(t\) components where the superscript \(c_i\) denotes that the \(i\)-th component \(V_i^c\) finished its training and froze at \(T_i\). Each component \(V_i^c\) has already preserved the knowledge of the memory buffer \(M_{c_i}\) with the parameters \(\{\theta^i, \omega^i\}\).

In the following, we derive a new lower bound to analyze the forgetting behaviour of a dynamic expansion model during the training.

**Theorem 2** Let \(P^B_i\) represent the distribution of all visited data batches \(\{B_1, \cdots, B_i\}\) at \(T_i\) where each data batch \(B_j\) is denoted by the probabilistic representation \(P_{\hat{B}}^j\). Let \(\mathbf{V} = \{V_1^c, \cdots, V^n_c\}\) be a dynamic mixture model trained on \(\mathcal{M}_i\) at \(T_i\) where \(c_i = i\). We derive a lower bound as:

\[
\sum_{j=1}^{i} \{E_{p_{\hat{B}^j}}[\log p_{\Theta}(\mathbf{x})]\} \geq \sum_{j=1}^{i} \{F_{s}(P_{\hat{B}^j}, \mathbf{V})\},
\]

where \(\Theta^i\) represent the parameters of \(\mathbf{V}\) and \(F_{s}(\cdot, \cdot)\) is the component selection function defined as:

\[
F_{s}(P_{\hat{B}^j}, \mathbf{V}) \triangleq \arg \max_{c_1, \cdots, c_t} \left\{ \mathbb{E}_{\hat{P}_{M_{c_i}}}[\mathcal{L}_{\text{ELBO}}(\mathbf{x}; \theta^i, \omega^i)] - D_{JS}(P_{\hat{B}^j} \parallel P_{M_{c_i}}) - \mathcal{F}_{\text{DL}}(P_{M_{c_i}}, P_{\hat{B}^j}, P_{\Theta^i}) + \mathcal{F}_{\text{dis}}(P_{\hat{B}^j}, P_{M_{c_i}}) \right\},
\]

Eq. (9) can be seen as an optimal component selection function which always returns the component with the highest selectivity function value.

**Remark.** We have several observations from Theorem 2: (1) Since each component \(V_j^c\) preserved the information of the associated memory buffer \(M_{c_i}\), \(V\) would capture more information about \(W\) when compared with a single VAE model. (2) By increasing the number of components in \(V\) we improve the performance since more components capture more underlying distributions and thus increase RHS of Eq. (8); In the following, we study the generalization performance of \(V\) on target sets by deriving a new lower bound.

**Lemma 2** Let \(\{D^T(1, k), \cdots, D^T(C(T, k), k)\}\) be several target sets where each target set \(D^T(c, k)\) can be divided into several data batches \(\{B^T(c, 1), \cdots, B^T(c, n(T, c, k))\}\) where \(n(T, c, k)\) is the total number of data batches for \(D^T(c, k)\). Let \(P^B_{\hat{B}^j}(c, j)\) represent the probabilistic representation of the data batch \(B^T(c, j)\). We suppose that \(V\) has already learnt \(t\) components trained on \(\mathcal{M}_i\) at \(T_i\). The generalization performance on all target sets, achieved by \(V\) at \(T_i\), is defined as:

\[
\sum_{c=1}^{C(T, k)} \left\{ \sum_{j=1}^{n(T, c, k)} \left\{ \mathbb{E}_{p_{\hat{B}^j}(c, j)}[\log p_{\Theta}(\mathbf{x})] \right\} \right\} \geq \sum_{c=1}^{C(T, k)} \left\{ \sum_{j=1}^{n(T, c, k)} \left\{ F_{s}(P^B_{\hat{B}^j}(c, j), \mathbf{V}) \right\} \right\},
\]

Similar to the conclusion of Theorem 2, increasing the number of components in \(V\) leads to a better generalisation performance on all target sets. In practice, we use the sample log-likelihood comparison for component selection, which would introduce additional errors compared to using the optimal component selection Eq. (9) (see details in Appendix-F from SM1). In addition, we also extend our theoretical analysis to the existing VAE models in Appendix-F as well as to general continual learning with explicit task boundary in Appendix-G from SM1.

**Theoretical Analysis for The Component Diversity**

In this section, we study how component diversity can influence the trade-off between the model’s complexity and generalization performance.

**Assumption 1** Let us consider that \(V\) has already learnt \(t\) components at \(T_i\). Under the optimal component selection (Eq. (8)), we can treat the DEM \(V\) as a single model that has been trained on all memory buffers \(\{M_{c_1}, \cdots, M_{c_t}\}\).

\(P_{\mathcal{M}_{c_1}}\) represent the distribution of all memories data.
where $C$ is the same underlying data distribution and ignore other disadvantages. In practice, using a large number of components may not always ensure good performance for $V$ at $T_t$. According to the theoretical analysis from Theorem 3, we desire to train a diverse and compact VAE-DEM by ensuring the knowledge diversity among its components. In this section, we first introduce a new dynamic expansion criterion and then implement it using the proposed OAES.

**Dynamic Expansion Criterion**

Let us consider that $V$ has already learnt $t$ components at $T_t$. According to the theoretical analysis from Theorem 3, we aim to promote the knowledge diversity among components, which can be realized as an optimization function:

$$F_{\text{div}}(\mathbb{P}_{(j,k)}, \mathbb{P}_{\mathcal{M}_{t-1}}) + E_{\mathbb{P}_{\mathcal{M}_{t-1}}} [L_{\text{ELBO}}(x; \Theta', \Omega')] - D_{ JS}(\mathbb{P}_{(j,k)} || \mathbb{P}_{\mathcal{M}_{t-1}}) - F_{\text{DL}}(\mathbb{P}_{\mathcal{M}_{t-1}}, \mathbb{P}_{\Theta'}) $$

where $C' = C(T, k)$ and $\mathbb{P}_{\Theta'}$ is the distribution of samples uniformly drawn from generators (decoders) of $V$ at $T_t$.

**Methodology**

Based on the analysis of Theorem 3, we desire to train a diverse and compact VAE-DEM by ensuring the knowledge diversity among its components. In this section, we first introduce a new dynamic expansion criterion and then implement it using the proposed OAES.

**Online Adversarial Expansion Strategy (OAES)**

The proposed criterion (Eq. (13)) employs the Wasserstein distance for assessing the similarity between two probability distributions. However, evaluating Wasserstein distance in the high-dimensional image space still requires enormous computational resources. To address this issue, instead of directly estimating Wasserstein distance, we formulate the expansion strategy as a multi-player game and introduce the proposed OAES to solve this game. OAES consists of two stages, as shown in Fig. 1: training and evaluation stages.

**Training stage:** Let $G_x$ and $D_{\psi}$ represent a generator and a discriminator, trained on the memory buffer $\mathcal{M}_t$ at $T_t$. The
where \( n \) is the absolute value and \( \hat{\cdot} \) runs when testing various models on three datasets. * and † denote the results cited from (De Lange and Tuytelaars 2021) and (Jin et al. 2021), respectively.

### Table 2: Classification accuracy results for five independent runs when testing various models on three datasets.

<table>
<thead>
<tr>
<th>Methods</th>
<th>Split MNIST</th>
<th>Split CIFAR10</th>
<th>Split CIFAR100</th>
</tr>
</thead>
<tbody>
<tr>
<td>finetune*</td>
<td>19.75 ± 0.05</td>
<td>18.55 ± 0.34</td>
<td>3.53 ± 0.04</td>
</tr>
<tr>
<td>GEM*</td>
<td>93.25 ± 0.36</td>
<td>24.13 ± 2.46</td>
<td>11.12 ± 2.48</td>
</tr>
<tr>
<td>iCARL*</td>
<td>83.95 ± 0.21</td>
<td>37.32 ± 2.66</td>
<td>10.80 ± 0.37</td>
</tr>
<tr>
<td>reservoir*</td>
<td>92.16 ± 0.75</td>
<td>42.48 ± 3.04</td>
<td>19.57 ± 1.79</td>
</tr>
<tr>
<td>MIR*</td>
<td>93.20 ± 0.36</td>
<td>42.80 ± 2.22</td>
<td>20.00 ± 0.57</td>
</tr>
<tr>
<td>GSS*</td>
<td>92.47 ± 0.92</td>
<td>38.45 ± 1.41</td>
<td>13.10 ± 0.94</td>
</tr>
<tr>
<td>CoPE-CE*</td>
<td>91.77 ± 0.87</td>
<td>39.73 ± 2.26</td>
<td>18.33 ± 1.52</td>
</tr>
<tr>
<td>CoPE*</td>
<td>93.94 ± 0.20</td>
<td>48.92 ± 1.32</td>
<td>21.62 ± 0.69</td>
</tr>
<tr>
<td>ER + GMED†</td>
<td>82.67 ± 1.90</td>
<td>34.84 ± 2.20</td>
<td>20.93 ± 1.60</td>
</tr>
<tr>
<td>ERo + GMED‡</td>
<td>82.21 ± 2.90</td>
<td>47.47 ± 3.20</td>
<td>19.60 ± 1.50</td>
</tr>
<tr>
<td>CURL*</td>
<td>92.59 ± 0.66</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CNDPM*</td>
<td>93.23 ± 0.09</td>
<td>45.21 ± 0.18</td>
<td>20.10 ± 0.12</td>
</tr>
<tr>
<td>Dynamic-OCM*</td>
<td>94.02 ± 0.23</td>
<td>49.16 ± 1.52</td>
<td>21.79 ± 0.68</td>
</tr>
<tr>
<td>OAES</td>
<td>94.69 ± 0.18</td>
<td>52.16 ± 0.25</td>
<td>26.01 ± 1.02</td>
</tr>
</tbody>
</table>

Table 2: Classification accuracy results for five independent runs when testing various models on three datasets.

The objective function (Wasserstein GAN loss) for training \( G_{\epsilon t} \) and \( D_{\psi t} \) at \( T_i \) is defined as (Gulrajani et al. 2017):

\[
\min_{\bar{\psi}} \max_{D_{\psi t} \in \Theta} \mathbb{E}_{x \sim M_i} \left[ D_{\psi t}\left( x \right) \right] - \mathbb{E}_{\bar{x} \sim \bar{\mathbb{P}}_t} \left[ D_{\psi t}\left( \bar{x} \right) \right] + \gamma \mathbb{E}_{\bar{x} \sim \bar{\mathbb{P}}_t} \left[ \left( \| \nabla_{\bar{x}} D_{\psi t}\left( \bar{x} \right) \|_2 - 1 \right)^2 \right], \tag{14}
\]

where \( \bar{x} \) is an interpolated image produced by \( \bar{x} = \alpha x + (1 - \alpha) x' \) where \( \alpha \) is drawn from a uniform distribution \( U(0, 1) \) and \( \bar{\mathbb{P}}_t \) is the distribution of the interpolated images. Different from WGAN (Gulrajani et al. 2017) which is trained on a static dataset, we train \( G_{\epsilon t} \) and \( D_{\psi t} \) on the evolved memory buffer \( M_i \) in an online fashion.

**Evaluation stage**: At this stage, we evaluate the discrepancy between each previously learnt component and the current component by comparing the discriminator’s outputs and therefore Eq. (13) is reformulated as:

\[
\min \left\{ C_{\psi t}(\bar{\mathbb{P}}_{\psi_{t-1}}, \mathbb{P}_{\psi t}), \ldots, C_{\psi t}(\bar{\mathbb{P}}_{\psi_{t-1}}, \mathbb{P}_{\psi t}) \right\} \geq \beta, \tag{15}
\]

where \( C_{\psi t}(\mathbb{P}_{\psi_{t-1}}, \mathbb{P}_{\psi t}) \) is defined as:

\[
C_{\psi t}(\mathbb{P}_{\psi_{t-1}}, \mathbb{P}_{\psi t}) = \frac{1}{n'} \sum_{j=1}^{n'} \left| D_{\psi t}\left( x'_j \right) - D_{\psi t}\left( x_j \right) \right| \tag{16}
\]

where \( x'_j \sim \mathbb{P}_{\psi_{t-1}} \) and \( x_j \sim \mathbb{P}_{\psi t} \) are treated as the real and fake images in the context of the adversarial criterion. \( \cdot \) is the absolute value and \( n' = 128 \) is the number of samples. A small \( \left| D_{\psi_{t-1}}\left( x'_j \right) - D_{\psi t}\left( x_j \right) \right| \) indicates that \( \mathbb{P}_{\psi_{t-1}} \) is similar to \( \mathbb{P}_{\psi t} \) since \( \mathbb{P}_{\psi_{t-1}} \) is trained to approximate \( \mathbb{P}_{M_i} \). The implementation for the OAES is explained in the following.

### Algorithm Implementation

In this section, we provide the algorithm implementation of OAES (See the pseudocode in Appendix-A from SM1), which is summarized into three stages:

**Stage 1. Memory updating**: Let \( |M| \) be the number of samples in the memory buffer and \( |M|^{max} \) be the maximum memory buffer size. The memory buffer \( M_i \) when reaching \( |M|^{max} \) at the \( i \)-th training step, is updated by removing the earliest stored samples, while adding newly given samples.

**Stage 2. Training the component**: Let us suppose that we have already learnt \( t \) components \( V = \{ V_1, \ldots, V_t \} \) at \( T_i \). We only train \( V_{t+1} \) on \( M_i \) at \( T_i \) by using Eq. (1) to avoid forgetting previously learnt knowledge. In addition, we train the generator \( G_{\zeta t} \) and the discriminator \( D_{\psi t} \) on \( M_i \) using adversarial loss (Eq. (14)).

**Stage 3. Check the expansion**: When reaching \( |M|^{max} \) we check the expansion criterion using Eq. (15) (OAES evaluation stage). If Eq. (15) is satisfied, we add a new component \( V_{t+1} \in V \) and clear up the memory \( M_i \), in order to learn statistically non-overlapping data in the following training step. We return to Stage 1 for next training step (\( T_{i+1} \)).

### Experiments

### Experiment Setting and Datasets

**Datasets**. For the generative modelling task, we have the following datasets: (1) Split MNIST/Fashion. We split MNIST/Fashion (LeCun et al. 1998) into ten parts according to the class. (2) Split MNIST-Fashion. We combine Split MNIST and Split Fashion in a class-incremental manner; (3) Cross-Domain. We consider to combine Split MNIST-Fashion and OMNIGLOT (Lake, Salakhutdinov, and Tenenbaum 2015). See more details in Appendix-H2 from SM1.

**Criteria**. The task classification task is employed for testing the accuracy. For testing the generative modelling task, we estimate the sample log-likelihood (Log) by using IWVAE bound (Burda, Grosse, and Salakhutdinov 2015), considering 1000 importance samples, as in (Ye and Bors 2022b).

**Baseline**. We introduce several baselines which are used for density estimation (Ye and Bors 2022b): (1) VAE-ELBO/OCM: A single VAE model with ELBO using the Online Cooperative Memorization (OCM) (Ye and Bors 2022b). (2) VAE-IWVAE50-OCM: A single VAE model with IWVAE using the OCM where the number of importance samples is 50. (3) VAE-ELBO-Random: A single VAE model with a memory that randomly removes samples when it reaches the maximum memory size. (4) Dynamic-ELBO/OCM: A mixture model with ELBO using OCM (Ye and Bors 2022b). (5) CNDPM (Lee et al. 2020); (6) LIMix (Ye and Bors 2021a): we assign an episodic memory with a fixed buffer size for the LIMix model used for TFCL. The

<table>
<thead>
<tr>
<th>Methods</th>
<th>M-S Param</th>
<th>M-C Param</th>
<th>Split IM Param</th>
</tr>
</thead>
<tbody>
<tr>
<td>ER</td>
<td>10.89</td>
<td>161M</td>
<td>15.28</td>
</tr>
<tr>
<td>ER + GMED†</td>
<td>16.23</td>
<td>161M</td>
<td>21.26</td>
</tr>
<tr>
<td>CoPE</td>
<td>22.45</td>
<td>161M</td>
<td>26.85</td>
</tr>
<tr>
<td>CNDPM‡</td>
<td>47.64</td>
<td>237M</td>
<td>66.25</td>
</tr>
<tr>
<td>OAES</td>
<td>55.35</td>
<td>157M</td>
<td>72.56</td>
</tr>
</tbody>
</table>

Table 3: Classification accuracy of various models in the cross-domain setting.
maximum number of components for various models is set to 30 to avoid memory overload.

**Density Estimation**

The results of various models on the density estimation task are shown in Table 1, where ‘Memory’ and ‘N’ denotes the memory size and the number of components. The threshold $\beta$ for Split MNIST, Split Fashion, Split MNIST-Fashion and Cross-domain is 4.2, 3, 4 and 4.2, respectively. We observe that dynamic expansion models usually outperform static models while using a small memory buffer, especially in the cross-domain setting involving multiple data domains. These results demonstrate that DEM provides a better generalization performance than a single model when the data stream involves more underlying data distributions, which is theoretically explained in Theorem 2. In addition, the OAES-ELBO outperforms other DEM baselines in all settings. Compared with the Dynamic-ELBO-OCM, which performs the sample selection for the memory buffer, the OAES-ELBO requires less training while achieving better performance since it does not require the sample selection.

**Classification Task**

We replace each component using a conditional VAE or train a classifier along with each VAE component in order to test the classification task performance. We employ the learning setting and network architecture from (De Lange and Tuytelaars 2021). We adopt Split MNIST, Split CIFAR10 and Split CIFAR100 from (De Lange and Tuytelaars 2021) for the classification tasks. The details of all classification baselines and the threshold $\beta$ are provided in Appendix-H3 from SM1. The results for Split MNIST, Split CIFAR10 and Split CIFAR100 are reported in Table 2. We also consider Split MiniImageNet (Split IM) (Vinyals et al. 2016) which divides MiniImageNet into 20 tasks, where each task collects the images of five classes (Aljundi et al. 2019a).

In the following we consider evaluating our model in the more challenging setting where a data stream involves multiple data domains. First, we create a data stream named M-S, combining Split MNIST and SVHN. Then, we create another data stream M-C, which combines Split MNIST and Split CIFAR10. The memory buffer size is 1000 for Split M-S and Split M-C, and the results are reported in Table 3, where ‘Param’ denotes the number of parameters. Together with the results from Tables 2 and 3, we show that DEM methods outperform other baselines on all datasets. In addition, the proposed OAES achieves better performance while using fewer parameters than other baselines, according to the results from Table 3.

**Ablation Study**

The impact of the threshold $\beta$: We consider different values for $\beta$ in Eq. (13) when training OAES on Split MNIST and the results are reported in Fig. 2a where ‘Negative log’ denotes the negative sample log-likelihood. We can observe that a small $\beta$ leads to training more components while improving the performance. In contrast, a large $\beta$ leads to fewer components in OAES.

The impact of the memory buffer size: We train various models under Split MNIST by using different memory buffer sizes and the results are shown in Fig. 2b. These results show that a large-scale memory buffer can improve the performance of all DEM models. The proposed OAES outperforms other baselines, especially when the memory buffer size is small (500 samples). More ablation studies are provided in Appendix-I from SM1.

**Conclusion**

In this paper, we develop a novel theoretical framework for VAEs, which interprets their forgetting process, when used in continual learning, as an increase in the JS divergence between the generator distribution and the evolved data distribution. Based on the theoretical analysis, we propose a novel dynamic expansion strategy that provides appropriate signals for the VAE-based Dynamic Expansion Model (DEM) expansion. The proposed model is shown to outperform other models in continual learning applications while ensuring a minimal architecture.
References


