

On Learning and Learned Representation with Dynamic Routing in Capsule Networks

Ancheng Lin¹, Jun Li², Zhenyuan Ma^{3,*}

¹ School of Computer Sciences, Guangdong Polytechnic Normal University, Guangzhou, China
cenbylin@163.com

² School of Software and Centre for Artificial Intelligence, Faculty of Engineering and Information Technology, University of Technology Sydney, POBox 123, Broadway, NSW 2007, Australia
Jun.Li@uts.edu.au

³ School of Mathematics and System Sciences, Guangdong Polytechnic Normal University, Guangzhou, China mazy@gpnu.edu.cn

Abstract. Capsule Networks (CapsNet) are recently proposed multi-stage computational models specialized for entity representation and discovery in image data. CapsNet employs iterative routing that shapes how the information cascades through different levels of interpretations. In this work, we investigate i) how the routing affects the CapsNet model fitting, ii) how the representation by capsules helps discover global structures in data distribution and iii) how learned data representation adapts and generalizes to new tasks. Our investigation shows: i) routing operation determines the certainty with which one layer of capsules pass information to the layer above, and the appropriate level of certainty is related to the model fitness, ii) in a designed experiment using data with a known 2D structure, capsule representations allow more meaningful 2D manifold embedding than neurons in a standard CNN do and iii) compared to neurons of standard CNN, capsules of successive layers are less coupled and more adaptive to new data distribution.

1 Introduction

Deep neural networks have achieved great success in image and video processing tasks. Capsule Net (CapsNet) [21] is a recently proposed architecture that represents an alternative arrangement of multiple stage processing of image data. Essentially, CapsNet differs from the traditional deep neural networks in i) in each stage, the atomic units of information are vectors rather than scalar values⁴, and ii) the output of a processing stage no longer contributes equally to the computation of its successive stage. One can intuitively understand the changes as introducing structures in the information and the information no longer flows homogeneously through the processing pipeline.

We present in this work our investigation on three aspects of CapsNet, answering three fundamental questions about the effectiveness of the new architecture in terms of visual analytics, namely model fitting, representation learning and generalization:

- Model fitting: how the routing process affects the training of the network. Routing introduces additional dynamics in the information flow through a network. Different from conventional

* Corresponding author, email: mazy@gpnu.edu.cn

⁴ To be more specific, the “atomic units” refer to the basic random variables that we are concerned with. In practical image/video analytic tasks, this concept of lower “convolutional” layers correspond to an element of a channel at a particular image location.

neural networks, where cross-layer connections are determined completely by network parameters. The connections between two successive layers of capsules in a CapsNet are computed at run-time and vary with individual data samples. Our investigation shows routing determines the (un-)certainty in the information pathway through layers of capsules. The appropriate level of certainty is closely interwoven with the model fitness to data.

- Representation learning: one motivation of CapsNet is that capsule representation can correspond to interpretable attributes of images, such as the style of writing in the case of hand-written digits. In this work, we test trained models on image data on a known 2D manifold spanned by geometric transformations. The ground-truth data manifold allows us to quantitatively assess the data representations in terms of meaningful structure discovery. We found that compared to standard neural networks, CapsNet captured more faithfully the global manifold structure in the image data.
- Representation generalization: if CapsNet could recover parse tree-like structures for images [21], the capsules would correspond to entities at different levels of interpretation. One can then expect the intermediate-level capsules to correspond to cognition ingredients that could be re-adapted to new tasks or contexts. In our comparative study, CapsNet generated mid-level data representations more adaptable to new tasks than conventional neural networks did, which supported the claim above.

In the remaining parts of this paper, we review necessary background in Section 2. Section 3 presents the main findings of the research in three aspects. Section 4 concludes the paper.

2 Background Review

Research in deep neural networks (DNN) have enjoyed rapid growth in recent years [16]. DNN-powered learning models have represented the state-of-the-art in a wide range of application areas [5,15,20,1,3]. On the other hand, fundamental challenges remain in artificial neural network-based vision systems. The training process is complex and expensive in terms of both computation and training data [16,9]. The learning is task-oriented and end-to-end, where the understanding of intermediate data representation is incomplete and the decision making is obscure [14]. The insufficiently understood model may be prone to peculiar failures or attacks [22,19]. Generalization and reliability of an existing DNN beyond the training domain can also be problematic [27].

CapsNet [21] represents an alternative visual information processing mechanism that addressing some abovementioned issues. The neurons are divided into small groups in each network layer, known as *capsules*. The capsules correspond to concepts in different levels of abstraction during the process of parsing visual information. The cross-layer association and the activation status of the capsules represent semantic analysis of the image data. Recently, CapsNet has undergone some developments such as Matrix Capsules [6] and has been employed in new application domains such as text classification [29].

The investigation into CapsNet in this work is mostly related to three topics of research in DNN and broadly machine learning: model training, data representation and knowledge transfer. Arguably, efficient training methodology plays the midwife for real-world success of DNN [7]. Rich techniques have been proposed to address different challenges in various DNN structures, including randomly disturbing cross-layer connections [23], introducing special gate units to keep long-term memory [8,11] and exploiting computationally affordable structures in the gradients during optimization [13]. The iterative routing in CapsNet is a newly introduced technique, where its role in model training demands full investigation.

Data representation is one of the key elements of successful analysis [4]. It is well-known that the learned convolutional neurons in the lower layers of deep networks resemble the primary biological vision processing in discovering low-level features in images [12]. On the other hand, the roles of intermediate or high-layer neurons in DNNs are not well understood [10,14]. To address this issue, CapsNet was proposed and has shown the promise of unveiling the meaningful data structures in image populations. In this work, we perform a comprehensive study on CapsNet and propose a systematic quantitative evaluation protocol.

One advantage of general AI is its supreme adaptability. Tremendous research focus has been placed in transfer learning [18]. In particular, pioneering investigation has revealed characteristics of DNN layers under transfer tasks [27]. The abovementioned meaningful capsule data representation indicates capsules are conducive to knowledge transfer, which is supported by experiments in Section 3.

In following discussion, we will frequently consider the routing between adjacent layers of capsules. Below we provide a brief review of routing; readers can refer to [21] for more details. The pre-activation (total-input) of a capsule j is a vector $\mathbf{s}_j = \sum_i c_{ij} \hat{\mathbf{u}}_{j|i}$, where $\hat{\mathbf{u}}_{j|i}$ is the prediction of j by a low-layer capsule i and c_{ij} is the association coefficient between i and j . Routing determines the association coefficients by iterations of,

- accumulating alignment between activated capsule j , $\mathbf{v}_j = a(\mathbf{s}_j)$, and $\hat{\mathbf{u}}_{j|i}$, where $a(\cdot)$ is a non-linear activation and $\hat{\mathbf{u}}_{j|i}$ is a “prediction vector” from a lower capsule i ,

$$b_{ij} \leftarrow b_{ij} + \langle \mathbf{v}_j, \hat{\mathbf{u}}_{j|i} \rangle \quad (1)$$

- updating c_{ij} using accumulated alignments,

$$c_{ij} \leftarrow \text{Softmax}(b_{ij}) = \frac{e^{b_{ij}}}{\sum_j e^{b_{ij}}} \quad (2)$$

Note \mathbf{v}_j in (1) relies on coefficients $\{c_{ij}\}$ obtained in (2).

3 Experiments

3.1 Model fitting

This section presents our experiment results and analysis of structural and operational factors that affects the model training process of CapsNet. Multi-layer neural networks are powerful generic function approximation models, while the new family of CapsNet[21] introduce extra versatility via routing in data representation which are particularly effective in extracting the semantic hierarchy embedded in sensory data. Nevertheless, a data model can only realize its potential if there is an effective way of fitting the model to data. So it is natural to ask what CapsNet has provided considering the trade-off between model capability and training complexity. In particular, data representation routing is realized as Expectation-Maximization (EM) inference on the association between two layers of capsule units. We test and analyze how the EM operations affect the model training and performance.

Data: The task for the models is to recognize two handwritten digits in one image [21]. Each data sample is a 36×36 grey-scale image by superposition of two hand-written digit images from the MNIST dataset [26], with a duplex label of the two digits. The dataset contains 30,889 training samples and 4,738 test samples. Fig. 1 shows a few example images.

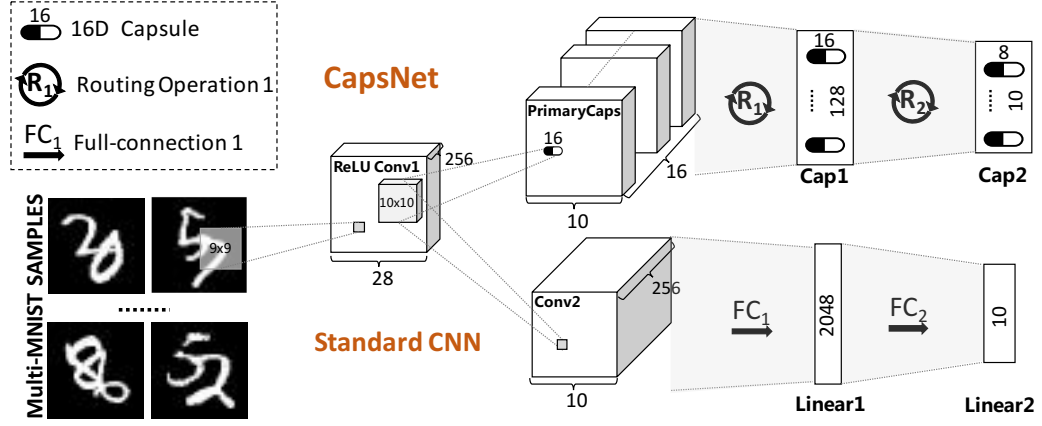


Fig. 1. CapsNet and Standard CNN models. The upper and lower diagrams show a 4-layer CapsNet as in [21] and a similarly structured standard convolutional neural network, respectively. Legends in the figure indicate capsule units of certain dimensions, the routing operation or the fully connection between layers.

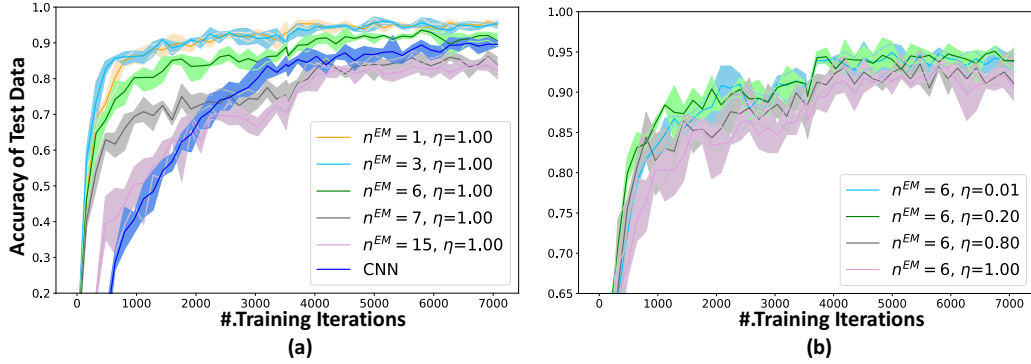


Fig. 2. Effects of EM Iteration Number n^{EM} and Update Rate η on CapsNet Training. This figure shows the training progress in terms of prediction accuracy on the test dataset against the training steps in mini-batches. Solid curve represents the mean accuracy in 5 trails using the same n^{EM} and η . Shaded areas represent one standard variance of the model performance in the trails. (The figures in this paper are best viewed in colors.)

Models: Fig. 1 illustrates the structure of the CapsNet and standard CNN in the experiment. The CapsNet is similar to that in [21]. A convolutional layer receives the input and is followed by 3 layers capsules. The last capsule layer represents the prediction of classes. As a baseline to assess the training, we have also constructed a conventional neural network with standard convolutional and linear layers (*i.e.* standard CNN, as shown in Fig. 1). Standard CNN has the same structure as the CapsNet. In each intermediate layer, we keep the number of total neurons in standard CNN and CapsNet the same.

Experiment: We have tested different *EM iteration numbers* and *EM update rates*, then check the influence on CapsNet training. Both settings refer to the implementation of (2). Iteration number n^{EM} indicates the EM loops which compute the coefficients. The update rate is a parameter we introduce to stabilize the training - instead of using the original computation in (2), we use a soft update rule letting

$$c_{ij}^{New} \leftarrow \eta \hat{c}_{ij} + (1 - \eta) c_{ij}^{Old} \quad (3)$$

where \hat{c}_{ij} is the coefficient computed using the original EM update rule (2), and η is the EM update rate. Testing on various n^{EM} and η , we evaluate the models being trained periodically to gauge the progress as well as quality of training. The evaluation protocol follows that in [21], *i.e.* a correct prediction requires the model to output the identities of both digits correctly. All training processes share the same optimization settings.

Fig. 2 shows the model performance during training under different n^{EM} settings. Fig. 2(a) shows the process under different η settings. We tested each setting of EM in 5 trails and reported the mean and variance of the model performance during the training processes. It is noteworthy that the training of CapsNet saturates with increasing EM iterations after n^{EM} reaches a small number. In fact, excessive EM iterations (e.g. $n^{EM} \geq 7$ in Fig. 2(a)) impacts the effectiveness of the training and deteriorates the performance. A possible explanation is as follows. At the beginning of the training stage, the network weights have not been conditioned to represent meaningful image elements. The routing produced by EM is mostly random. We can deprive high-layer capsules the chance of being exposed to all data samples by forcing the high-layer capsules to focus only on a small subset of low-layer inputs. In early stage, those subsets tend to be randomly assorted without any semantic significance, and the selective representation scheme (low-high layer association with a sparse matrix $\mathbf{C} : \{c_{ij}\}$) is more likely to impair rather than to improve the capsules' ability to discover meaningful attributes of the entities.

In fact, the observation of the "early over-routing" phenomenon in Fig. 2(a) has motivated our introduction of soft EM update scheme as in (3). Fig. 2(b) shows the model training of $n^{EM} = 6$ under different η -values. The results indicate the advantage of soft EM updates, e.g. by comparing the curve for $\eta = 0.01$ and that for $\eta = 1.0$.

From the viewpoint of a low-layer capsule i , the corresponding association coefficients $\{c_{i1}, c_{i2}, \dots\}$ of the capsules in the layer above can be considered as a probability distribution over the high-layer capsules. Let $P_i^c(j) = c_{ij}$ represent the event that "entity i 's presence is interpreted by the presence of high-level entity j ". In a sense, the entropy of the distribution, $H[P_i^c]$, measures the uncertainty at this step in the simulated cognition process, while forming high-level concepts using low-level information.

Fig. 3 shows the trends of the average association entropy over the training process. In particular, the association coefficients are from the first EM routing operator \mathcal{R}_1 as shown in Fig. 1. Between the two layers, \mathcal{R}_1 produces a coefficient matrix $\mathbf{C}^{(n)}$ for each data sample n , and the i -th row of $\mathbf{C}^{(n)}$ realizes the abovementioned distribution, from which we can compute an entropy value $H_i^{(n)}$.

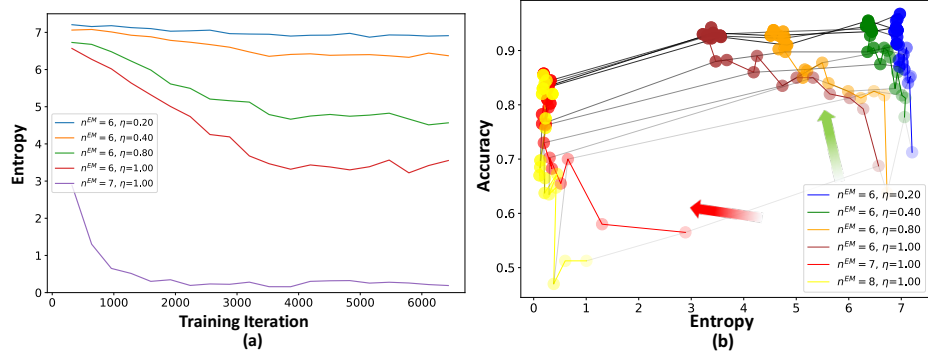


Fig. 3. Trends of entropy of the stochastic association between successive capsule layers during training. **(a)** shows the change of entropy along with training iterations, the top four lines are under different η -values of fixed EM-iteration 6. Last line shows one η -value setting of fixed EM-iteration 7. **(b)** illustrates the trend in the change of entropy and classification accuracy. Curve marker colors represent different EM-settings. Transparency indicates training progress. Markers in one gray line represent models undergone the same number of training iterations. Red and green arrows show appropriate and excessive reduce of associate entropy, respectively. See text for more details.

We take the average for the entropy over every samples n and every low-layer capsules i ,

$$\begin{aligned}\bar{H} &= \frac{1}{N \cdot I} \sum_{n=1}^N \sum_{i=1}^I H[P_i^{c,n}] \\ &= -\frac{1}{N \cdot I \cdot J} \sum_{n=1}^N \sum_{i=1}^I \sum_{j=1}^J c_{ij}^{(n)} \log c_{ij}^{(n)}\end{aligned}$$

where the superscript n indicates the data sample. The trend of the average entropy shown in Fig. 3(a) reveals the mechanism of routing in two aspects:

1. Reading the plot Fig. 3(a) *vertically*, at a certain training iteration (x-axis in Fig. 3(a)), we first compare the average entropy (y-axis in Fig. 3(a)) for different EM settings. As expected, if performing EM with more stringent updating rules (*i.e.* high updating rate), the less uncertainty remains in resultant association distribution, and the entropy reduces.
2. More interestingly, we can also read the plot Fig. 3(a) *horizontally*: we check how the entropy reached *using a certain EM setting* varies along the model training. The plot shows that the entropy reduces when the model gets more completely trained.

A possible interpretation of observation 2 is as follows. When the model fits well to the images, the parts to which individual capsule units response become clearer and the connections between layers (coefficients W , not to be confused with association \mathbf{C}) become more relevant. Generally speaking, we can be more certain about whether a low-layer capsule should contribute to the activation of a high-layer one. As an intuitive example, one can usually determine with more confidence whether a body part belongs to some creature, and one can with amorphous blob of pixels to some blurry assortment.

The above understanding leads to a heuristic training strategy: the EM operation should be modulated such that the certainty of the resultant association matches the model fitness to the data. In Fig. 3(b), we plot the average association entropy against the model performance for models at different training stages and EM settings. Each colored curve represents one EM operation setting. Each grey line links models tested after the same number of training steps. The general tendency in the plot is consistent with our observation in both Fig. 3(a) and Fig. 2: during training, model accuracy increases with the association certainty. The green arrow in Fig. 3(b) intuitively illustrates the phenomenon. On the other hand, the red arrow in Fig. 3(b), corresponding to deeply reduced entropy in early training stage, does not bode well for the training. It indicates that the CapsNet overestimates the confidence without appropriable fitting, thereby may encounter the “early over routing” issue as discussed above.

3.2 Representation learning



Fig. 4. Example images of 2 shifted and overlapping hand-written digit images. The left panels shows images of fixed “7” and moving “8”; the right panels are of fixed “3” and moving “5”. The label below each image indicates the offset (\pm rows, \pm cols) of the moving part with respect to the fixed part. Take the (7,8)-images for example, (0,0) means that the image “8” is located with the center overlapping that of “7” and (-1,-4) means that the “8” has been shifted 1 units up and 4 units to the left.

This section presents experiment results on how the CapsNet learned data representation corresponds to the intrinsic structures in the population distribution of the data. Beyond assessing the representation by intuition and visual plausibility, we have especially constructed a dataset with internal structures induced by geometric transformations. We perform both quantitative and qualitative assessment of the learned data representations by CapsNet and standard CNN.

Data: It is common to render data samples encoded by a model in a 2D plane to examine how well the model has learned to represent the data [17,25,28]. In this experiment, we directly construct test image datasets with known underlying 2D manifold spanned by geometric translations. The data resemble the multiple overlapping hand-written digit images. We generate images of two digits by moving one digit while keeping the other one fixed. The population of such a dataset is naturally distributed on a 2D manifold. Fig. 4 shows two example test datasets of digits (fixed-7, moving-8) and (fixed-3, moving-5), respectively. We shifted the moving digit horizontally and vertically by $[-4, +4]$ units, resulting in $9 \times 9 = 81$ sample images per test dataset. Note that we discussed above the *test* datasets. The models are trained on the multi-MNIST data as in the last experiment. Notably, we evaluate the intermediate data representations in networks trained for classification, rather than optimizing the network deliberately for discovering the intrinsic manifold in the test data.

Models: In this experiment, we use the same CapsNet and standard CNN models as described in Subsection 3.1.

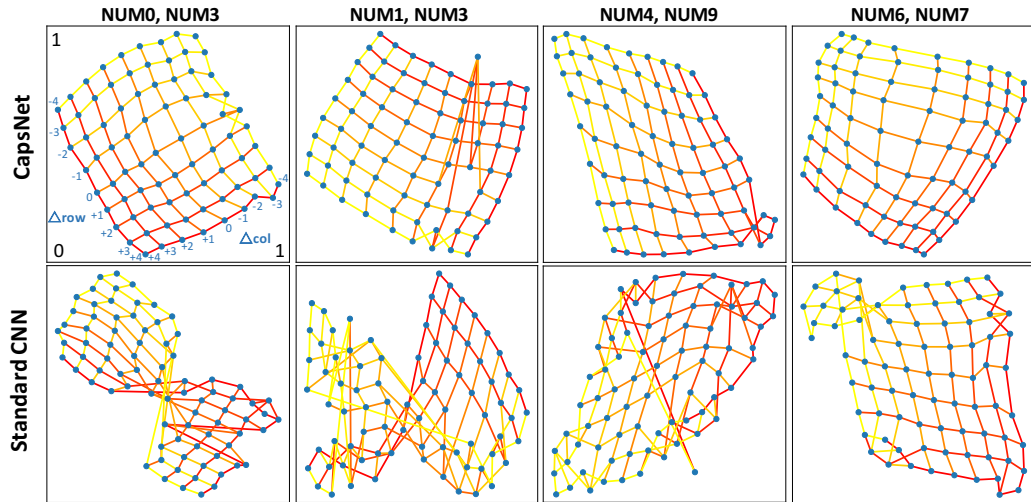


Fig. 5. Embedding of learned representations. This figure shows the 2D embedding result of CapsNet and Standard CNN on 4 different test dataset. Points in subplot corresponding to samples in a dataset. Digits being shifted for the same amount of units and direction have been connected by a line with certain color.

Experiment: Using trained networks to process the test dataset, we collect the data representation at an intermediate layer of neurons / capsules (the capsule layer after the first routing operation and the counterpart layer in the standard CNN, see Fig. 1 for “Cap1” and “Linear1”, respectively). Then we apply manifold embedding algorithm t-SNE [24] to render the learned representations into \mathbb{R}^2 . Fig. 5 illustrates the t-SNE \mathbb{R}^2 embedding of the samples in several test datasets. The observation is that the data representation and the corresponding embedding from CapsNet are better aligned with the internal 2D manifold than those from the standard CNN are. The quantitative validation is as follows. We computed the Chamfer distance (CD) [2] between the regular grid of movements $\{(-4, -4), (-3, -4), \dots, (+4, -4), \dots, (+4, +4)\}$ and the \mathbb{R}^2 embedding. The table below shows the mean and variance of the Chamfer distance.

	CapsNet	Standard CNN
mean	0.313	0.394
variance	0.010	0.025

Compared to the intermediate data representation of the standard CNN, that of CapsNet is more strongly related to the geometrically meaningful structures of the data population. Recall that the models were trained as classifiers, which means that the CapsNet discovered relevant data representation *without* explicit training goal of such structures.

3.3 Representation generalisation

Meaningful data representation can facilitate knowledge transfer or generalization to distinctive cognition tasks. In this experiment, we further investigate how a trained CapsNet generalizes beyond the original task, in particular, how transferrable the CapsNet are.

Data: We have made two subsets of the multi-MNIST image data for the test of transfer-domain fitness. The two subsets, namely S_A and S_B , are constructed so that i) each two-digit class

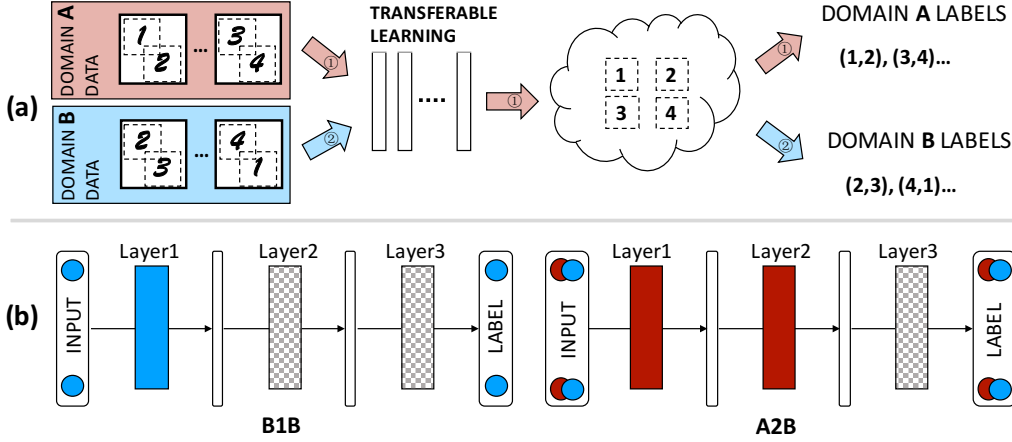


Fig. 6. Example Testing Schemes of Domain Transfer. Colors represent domain, red for A and blue for B. (a) Domain data are superposition of 2 hand-written digits. Domain A and B contain different combinations of digits. (b) The tests are to determine how representations produced by pre-trained layers can help new cross-/same-domain tasks. Chessboard pattern stands for layers to re-adjust. B1B represents keeping 1 pre-trained layer on domain B and re-adjust the top 2 layers also on domain B. A2B represents keeping 2 pre-trained layers on domain A and re-adjust the top 1 layer on domain B. See text and refer to [27] for more detailed discussions of the testing protocol.

of images are exclusively within S_A or S_B , and ii) S_A and S_B both contain a complete set of digits. The motivation of using such S_A and S_B is as follows. Condition i) ensures that during training, the model does not use the images of the same two-digit label on which it will be tested, and Condition ii) ensures that the model has seen all necessary concepts, *i.e.* the individual digits, in order to successfully perform the new task. For example, if the model to be tested on images containing digits (7, 8), then we do not use images of (7, 8) in the training stage. Instead, the training data contain the appearance of both 7 and 8 in images such as (7, 9), (1, 8), etc. as shown in Fig. 6(a).

Models: The CapsNet and standard CNN models are similar to those used in Subsection 3.1 with one more capsule/CNN layer, respectively. The extra layer is for testing the transferability of the neurons at different layers.

Experiment: We follow a similar test protocol as that in [27]: the models are trained in domain S_A and tested in domain S_B . We re-adjust the last 1 or 2 layers using training data of domain S_B , while keeping the remaining net parameters as trained in S_A . Such models are called A1B (1 layer fixed to S_A -training, 2 layers adjusted on S_B) or A2B (2 layers fixed to S_A -training, 1 layer adjusted on S_B). As a control test, the experiment also includes networks prepared following the above protocol with the difference that the first training pass is on the target domain S_B . We call such control set of models B1B (fixing 1 layer and re-adjusting 2) and B2B (fixing 2, re-adjusting 1), respectively. Fig. 6(b) illustrates the test schemes of B1B and A2B.

Keeping lower layers fixed and re-adjusting the higher ones breaks the coupling between the layers formed during training. BnB schemes test if the data representation of the lower layers can be decoupled from the original higher ones. AnB schemes tend to be more challenging, where the learned representation must survive cross-domain readaption. Cross-domain readaption can benefit

from representation contains intermediate-level knowledge that is relevant to both tasks, e.g. the appearance of individual digits in this experiment.

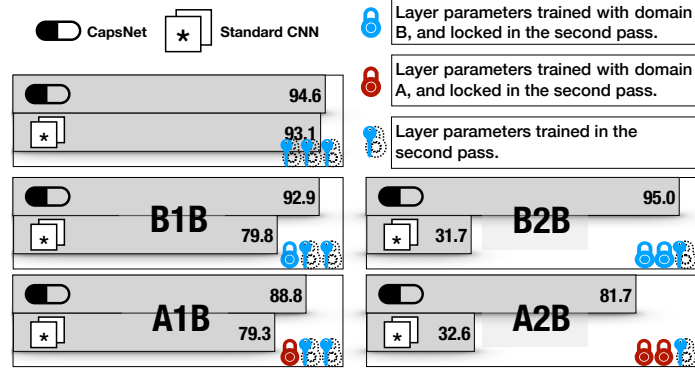


Fig. 7. Transfer Performance of CapsNet and Standard CNN. The figure shows model performance on different testing schemes. The first plot shows the baseline model performance of standard supervised learning on domain B.

Fig. 7 displays the results of CapsNet and standard CNN on different transfer test schemes. We have observed that breaking the coupling between the layers significantly reduced the fitness of standard CNN, regardless of the domain on which the original model was trained. On the other hand, CapsNet representation can be successfully used by newly learned higher layers. When the new task is cross-domain, CapsNet has a minor performance drop. Nevertheless, the CapsNet representations remain satisfactorily relevant on AnB tasks, which supports the claim that the intermediate level capsules can capture knowledge on appearance of meaningful object parts [21].

4 Conclusion

In this paper we investigate several important aspects of CapsNet, including model learning, attributes of learned data representations and generality of the representations. Our tests demonstrate that appropriate routing operation plays a significant role in CapsNet training. In the early stage of training, the routing between capsules should contain a level of *uncertainty*; early over-confidence about the routing tends to impose excessive limits on the training process, which leads to suboptimal models. CapsNet can produce data representation with interesting attributes. To explore such attributes, we especially designed a test using image data on a 2D manifold spanned by geometric transformations. The test shows that compared to standard CNN, CapsNet can capture more faithfully the global manifold structures in data. Moreover, following test protocol in [27], we show the representation by CapsNet is more transferrable than that by standard CNN.

References

1. Hani Altwaijry, Andreas Veit, and Serge J. Belongie. Learning to detect and match keypoints with deep architectures. In *Proceedings of the British Machine Vision Conference, BMVC*, 2016.

2. Haoqiang Fan, Hao Su, and Leonidas J. Guibas. A point set generation network for 3d object reconstruction from a single image. In *CVPR*, pages 2463–2471, 2017.
3. Martin Garbade and Bjuergen Gall. Thinking outside the box: Spatial anticipation of semantic categories. In *Proceedings of the British Machine Vision Conference, BMVC*, 2017.
4. Trevor Hastie, Robert Tibshirani, and Jerome H. Friedman. *The elements of statistical learning: data mining, inference, and prediction, 2nd Edition*. Springer series in statistics. Springer, 2009.
5. Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *CVPR*, pages 770–778, 2016.
6. Geoffrey Hinton, Sara Sabour, and Nicholas Frosst. Matrix capsules with EM routing. In *ICLR*, 2018.
7. Geoffrey E. Hinton, Simon Osindero, and Yee Whye Teh. A fast learning algorithm for deep belief nets. *Neural Computation*, 18(7):1527–1554, 2006.
8. Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural Computation*, 9(8):1735–1780, 1997.
9. Kui Jia, Dacheng Tao, Shenghua Gao, and Xiangmin Xu. Improving training of deep neural networks via singular value bounding. In *CVPR*, pages 3994–4002, 2017.
10. Andrej Karpathy, Justin Johnson, and Fei-Fei Li. Visualizing and understanding recurrent networks. *CoRR*, abs/1506.02078, 2015.
11. Hirokatsu Kataoka, Yudai Miyashita, Masaki Hayashi, Kenji Iwata, and Yutaka Satoh. Recognition of transitional action for short-term action prediction using discriminative temporal CNN feature. In *Proceedings of the British Machine Vision Conference, BMVC*, 2016.
12. Saeed Reza Kheradpisheh, Masoud Ghodrati, Mohammad Ganjtabesh, and Timothée Masquelier. Deep networks resemble human feed-forward vision in invariant object recognition. *CoRR*, abs/1508.03929, 2015.
13. Diederik P. Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *CoRR*, abs/1412.6980, 2014.
14. Pang Wei Koh and Percy Liang. Understanding black-box predictions via influence functions. pages 1885–1894, 2017.
15. Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton. Imagenet classification with deep convolutional neural networks. In *NIPS*, pages 1106–1114, 2012.
16. Yann LeCun, Yoshua Bengio, and Geoffrey E. Hinton. Deep learning. *Nature*, 521(7553):436–444, 2015.
17. Feiping Nie, Dong Xu, Ivor Wai-Hung Tsang, and Changshui Zhang. Flexible manifold embedding: A framework for semi-supervised and unsupervised dimension reduction. *IEEE Trans. Image Processing*, 19(7):1921–1932, 2010.
18. Sinno Jialin Pan and Qiang Yang. A survey on transfer learning. *IEEE Trans. Knowl. Data Eng.*, 22(10):1345–1359, 2010.
19. Nicolas Papernot, Patrick D. McDaniel, Ian J. Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami. Practical black-box attacks against machine learning. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 506–519, 2017.
20. Umer Rafi, Bastian Leibe, Juergen Gall, and Ilya Kostrikov. An efficient convolutional network for human pose estimation. In *Proceedings of the British Machine Vision Conference, BMVC*, 2016.
21. Sara Sabour, Nicholas Frosst, and Geoffrey E. Hinton. Dynamic routing between capsules. In *NIPS*, pages 3859–3869, 2017.
22. Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1528–1540, 2016.
23. Nitish Srivastava, Geoffrey E. Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: a simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15(1):1929–1958, 2014.
24. Laurens van der Maaten and Geoffrey Hinton. Visualizing data using t-SNE. *Journal of Machine Learning Research*, 9(2605):2579–2605, 2008.

25. Wei Wang, Yan Yan, Feiping Nie, Shuicheng Yan, and Nicu Sebe. Flexible manifold learning with optimal graph for image and video representation. *IEEE Trans. Image Processing*, 27(6):2664–2675, 2018.
26. Corinna Cortes Yann LeCun and Christopher J.C. Burges. The MNIST database of handwritten digits. 1998.
27. Jason Yosinski, Jeff Clune, Yoshua Bengio, and Hod Lipson. How transferable are features in deep neural networks? In *NIPS*, pages 3320–3328, 2014.
28. Baochang Zhang, Alessandro Perina, Vittorio Murino, and Alessio Del Bue. Sparse representation classification with manifold constraints transfer. In *CVPR*, pages 4557–4565, 2015.
29. Wei Zhao, Jianbo Ye, Min Yang, Zeyang Lei, Suofei Zhang, and Zhou Zhao. Investigating capsule networks with dynamic routing for text classification. *CoRR*, abs/1804.00538, 2018.