Perceptron Theory for Predicting the Accuracy of Neural Networks

Denis Kleyko, Antonello Rosato, E. Paxon Frady, Massimo Panella, and Friedrich T. Sommer

Abstract—Many neural network models have been successful at classification problems, but their operation is still treated as a black box. Here, we developed a theory for one-layer perceptrons that can predict performance on classification tasks. This theory is a generalization of an existing theory for predicting the performance of Echo State Networks and connectionist models for symbolic reasoning known as Vector Symbolic Architectures.

In this paper, we first show that the proposed perceptron theory can predict the performance of types of Echo State Networks, which could not be described by the previous theory. Second, we apply our perceptron theory to the last layers of shallow randomly connected and deep multi-layer networks. The full theory is based on Gaussian statistics, but it is analytically intractable. We explore numerical methods to predict network performance for problems with a small number of classes. For problems with a large number of classes, we investigate stochastic sampling methods and a tractable approximation to the full theory. The quality of predictions is assessed in three experimental settings, using reservoir computing networks on a memorization task, shallow randomly connected networks on a collection of classification datasets, and deep convolutional networks with the ImageNet dataset.

This study offers a surprisingly simple, bipartite approach to understand deep neural networks: the input is encoded by the last-but-one layers into a high-dimensional representation. This representation task, shallow randomly connected networks on a collection of classification datasets, and deep convolutional networks with the ImageNet dataset.

Index Terms—deep neural networks, reservoir computing, vector symbolic architectures, accuracy prediction, perceptron theory

I. INTRODUCTION

Due to its ability to provide data-driven solutions to many previously unsolved problems, machine learning is rapidly changing many areas of our life. At the same pace, there is also growing demand from society [1, 2] to improve transparency and interpretability of machine learning solutions, in particular Artificial Neural Networks (ANNs). One avenue to understand ANNs is to build models that can predict the performance of these networks [3, 4, 5]. The most recent works [4, 5] trained another estimator ANN to perform the prediction.

Here, we propose an alternative approach for predicting the expected accuracy on classification problems for different trained networks including deep ANNs, as well as Echo State Networks (ESNs) [6]. Our approach does not require training another ANN, rather it is based on a theory of the simple one-layer perceptron, which can describe the last layer of the ANN. The perceptron theory generalizes an earlier theory [7], proposed for Vector Symbolic Architectures and ESNs with unitary recurrent connections.

In addition to the original formulation in [7], we present formulae for two different levels of approximation for the accuracy prediction. In general terms, the perceptron theory leverages the first two moments of the statistics of the postsynaptic sums at the output neurons. By this means, one formula uses a coarser approximation of the distribution with a diagonal covariance matrix, which is easier to calculate numerically. However, this approximation introduces a bias to the predictions, which can be removed empirically. The second formula is more accurate, but much harder to evaluate numerically.

To assess the quality of the predicted accuracies and to demonstrate their effectiveness in interpreting ANNs, the theory was applied in three experimental settings. First, in Section II-B we applied it to a type of ESN that was not described by the earlier theory [7]. Second, in Section II-C we used a collection of classification datasets with shallow randomly connected ANNs exploring two strategies of training the perceptron. Third, in Section II-D we evaluated the accuracies of 15 deep convolutional ANNs (CNNs) trained on the ImageNet dataset. The results show high correlation between the actual accuracies and the predictions. Thus, the proposed theory identifies critical features for predicting and comparing performances of networks with different architectures. This not only helps to gain a deeper understanding of the principles at work, but also has practical implications. For example, for a particular task, the theory can be used to select the best suited network from a set of pretrained networks.

II. RESULTS

A. Perceptron theory

The perceptron network is the ancestor of all modern ANNs. A perceptron is a simple unit for integrating inputs with
threshold nonlinearity introduced by Rosenblatt [8]. Curiously, but understandably given the lack of universality [9], one cannot find the theory of the perceptron in textbooks. However, the theory of the perceptron has been developed piece by piece in the context of understanding more complicated networks, such as the formation of sensory representations [10], symbolic reasoning in Vector Symbolic Architectures (VSAs) [11] and some types of ESNs [7]. These studies demonstrated that complicated neural computations, involving recurrent circuitry and nonlinear stages, can be successfully dissected into two stages: an encoding stage that maps input patterns to a new \(N\)-dimensional space, and a one-layer perceptron that reads out the mapped representations to classes or network outputs.

In the perceptron network, each output neuron detects the membership of the input pattern to one particular class. The synaptic weights of these neurons are a linear transformation of the inputs to the postsynaptic sums of the neurons. The classification is correct if the postsynaptic sum is the largest in the neuron that corresponds to the actual class of the input pattern. Up to date, the most complete version of a Gaussian theory of the perceptron was presented in [7]. By generalizing signal detection theory [12] and building on earlier work on how Gaussian distributions can be transformed [13], the work [7] shows that if the input pattern belongs to one of \(D\) classes, then the predicted accuracy, i.e. the probability that the perceptron output is the correct class, is given by

\[
\begin{align*}
\text{a} : &= p(\text{class}_{\text{out}} = \text{class}_{\text{inp}}) = \\
&= \int_{-\infty}^{\infty} \frac{dx}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \left[ \Phi \left( \frac{\sigma_x x + \mu_h - \mu_r}{\sigma_h} \right) \right]^{D-1}.
\end{align*}
\]

Here, \(\Phi(x)\) is the cumulative Gaussian; \(\mu_h\) and \(\sigma_h\) denote mean and standard deviation of the postsynaptic sum of the output neuron that corresponds to the correct class; \(\mu_r\) and \(\sigma_r\) denote the mean and standard deviation of the postsynaptic sum for all other neurons. The formula describes the performance of all flavors of VSA frameworks [11], [14], [15], [16], [17], [18], and it also describes some types of ESNs [20], [21].

Intuitively, (1) computes the probability that for any given value \(x\) of the postsynaptic sum in the output neuron that represents the correct class, the postsynaptic sums in all other neurons are smaller than \(x\). Note that (1) makes three strong assumptions about the distributions of the postsynaptic sums:

i) The distributions are normal.

ii) The distributions for “distractor” classes are all the same.

iii) The distributions for different classes are independent.

For analyzing VSA frameworks, these assumptions are justified because information is represented by normalized pseudo-random vectors and the symbolic operations in VSAs conserve pseudo-randomness and norm. Furthermore, these networks do not have weights that are learned from data. To predict the accuracy with weights learned from input distributions, for example, in ESNs or ANNs, some of these assumptions will be violated.

We generalize (1) in two steps and demonstrate that the generalization can predict a broader variety of ANN architectures. Our first step of generalization of (1) is to drop assumption ii) and compute individual predicted accuracies for each class \(i \in \{1, 2, ..., D\}:

\[
\begin{align*}
a_i &:= p(\text{class}_{\text{out}} = i | \text{class}_{\text{inp}} = i) = \\
&= \int_{-\infty}^{\infty} \frac{dx}{\sqrt{2\pi}\sigma_i} e^{-\frac{(x-\mu_i)^2}{2\sigma_i^2}} \prod_{j=1, j \neq i}^{D-1} \Phi(x, \mu_j, \sigma_j)
\end{align*}
\]

Here \(\mu\) and \(\sigma\) denote vectors representing the first two moments (mean and standard deviation) of the statistics of the postsynaptic sums. The assumptions for (2) to hold are reduced to i) and iii).

Our second generalization is to drop assumption iii), that is, we allow the postsynaptic sums for different neurons to be correlated according to a multivariate normal distribution. We define

\[
\begin{align*}
a_i &:= p(\text{class}_{\text{out}} = i | \text{class}_{\text{inp}} = i) = \\
&= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} ... \int_{-\infty}^{\infty} d\mathbf{x}_D \mathcal{N}(\mathbf{x}, \mu, \Sigma),
\end{align*}
\]

where \(\mathcal{N}(\mathbf{x}, \mu, \Sigma)\) is the multivariate normal distribution with the full covariance matrix \(\Sigma\) replacing the variance vector \(\sigma\) for independent Gaussians in (2), see Appendix A for connection between (3) and (2). The assumptions for (3) to hold are reduced to i).

To aggregate the individual class accuracies \(a\) into the overall prediction, we form the expectation over all classes: \(\sum_{i=1}^{D} f_i a_i\), where \(f_i\) is the prior probability of \(i\)th class in the data. The predicted accuracy can be compared to the actual accuracy of the network.

B. Prediction of Echo State Networks

We test our generalized perceptron theory on predicting an ESN performance in the trajectory association task [22]. In Fig. 1, we compare two ESNs with different readout perceptrons. The synapses of one perceptron (blue line) are set to the centroids of inputs of the different classes (codebook-based). The synapses in the other perceptron (red line) have been optimized with linear regression (regression-based). The average predicted accuracy for the both versions is plotted in Fig. 1 as a function of the delay of the input occurred in the sequence of input vectors.

The solid lines depict empirical accuracies. The dotted lines are the predictions by theory (1), using the statistics reported in Fig. 5 in the Appendix. The original theory (1) correctly describes the experimental performance of the perceptron with centroid filters but overestimates the performance of the perceptron with regression filters (i.e., it has some bias). The bias occurs because (1) neglects the correlation between the linear filters of the regression-based readout, visible in the right panel of Fig. 5. The dashed lines in Fig. 1 depict the predictions by theory (2). The accuracies of both networks are predicted correctly.

The predictions of theory (2) are omitted because they did not differ from the predictions of (1) when \(D = 2\). To
see differences between these two theories, we run another experiment with $D = 3$ and a perceptron with centroid filters where the inputs had different amplitudes (black solid line). For this experiment, theory (1) (black dotted line) overestimated the accuracy, while (2) (black dashed line) provided accurate predictions.\footnote{We also studied the theory predictions for a synthetic binary classification problem in the case of non-independent distributions of postsynaptic sums (Appendix B).}

**C. Prediction of expected accuracies for shallow networks**

We also applied theory (2) to shallow feedforward randomly connected ANNs\cite{23}, which are similar to ESNs without the recurrent connections. The evaluation was done on a collection of the classification tasks\cite{24} where the data are provided in the form of the extracted features. In particular, the reported results are based on 121 real-world classification datasets obtained from the UCI Machine Learning Repository\cite{24}. The considered collection of datasets has been initially analyzed in a large-scale comparison study of different classifiers and the interested readers are kindly referred to the original work\cite{24} for more details. The only preprocessing step was to normalize features in the range $[0,1]$.

For the sake of brevity, here we do not go into the details of the encoding stage. The interested readers are kindly referred to\cite{26}. In essence, the encoding resembles Random Vector Functional Link (RVFL) networks\cite{23}, which are shallow feedforward randomly connected ANNs. Moreover, it is very similar to the known approaches of using VSAs for classification\cite{27,28,29,30}.

The search of the hyperparameters for each dataset has been done according to\cite{25} using the grid search over $\lambda$ (regularization parameter), $N$, and $\kappa$ (activation function parameter). $N$ varied in the range $[50,1500]$ with step 50; $\lambda$ varied in the range $2^{-10-5}$ with step 1; and $\kappa$ varied in the set of $\{1,3,5,7\}$. The obtained optimal hyperparameters were used to estimate the cross-validation accuracy on all datasets.

Similar to the previous section, we considered two ways of training the perceptron. The first way is common in VSAs. It forms a linear filter as a centroid of a class by simply superimposing all mapped representations for this class. The second way is common in Random Vector Functional Link (RVFL) networks\cite{23}. The perceptron is the result of the ridge regression, which uses training data’s mapped representations and their class labels. The average cross-validation accuracy for the perceptron with centroid filters was 0.70 while that for the perceptron with regression filters was 0.80. The correlation coefficient between the obtained result was 0.80. It is clear that the perceptron obtained from the ridge regression usually outperformed the ones with the centroids.

The upper panels in Fig. 2 present the cross-validation accuracies against their corresponding predicted accuracies for the perceptron with centroid filters. The upper-left panel in the figure corresponds to the case when the statistics for (2) was obtained from the training data. The upper-right panel in the figure corresponds to the case when the statistics for (2) was obtained from the test data. The correlation coefficient between the accuracy and predicted accuracy calculated from the statistics for the training data was 0.790 while that of the test data was 0.903. The usage of the statistics for the test data improved the quality of the predictions.

The lower panels in Fig. 2 present the cross-validation accuracies against their corresponding predicted accuracies for the perceptron with regression filters. The correlation coefficient between the actual accuracy and predicted accuracy for the statistics from the training data was 0.466 while that for the test data was 0.966. Similar to the results for the perceptron with centroid filters, the usage of the statistics for the test data improved the quality of the predictions. The difference, however, was that the predicted accuracies from the training data statistics did not correlate well with the accuracies. The most likely explanation is that in the case of the ridge regression the perceptron is calculated to maximize the accuracy on the training data. As a side effect, the statistics of the postsynaptic sums is too promising and so many models are predicted to achieve high accuracy on the test data. Other notable differences were that compared to the perceptron with centroid filters the errors and bias are smaller for the ridge regression with test data statistics. For instance, after removing the bias the mean value of the absolute error was 0.03 for the perceptron with...
Fig. 3. The accuracy of 15 deep CNNs on the ILSVRC 2012 validation dataset against the predicted accuracy. Left panel: the individual predicted accuracies were calculated according to (2). Right panel: the individual predicted accuracies were calculated similar to (2) but using the kernel distributions (correlation coefficient was 0.940).

Fig. 4. Dissecting the functionality of an ANN into multi-layer encoding stage and perceptron parts. The figure indicates components of the network by the terms used in the text.

regression filters while for the perceptron with centroid filters it was 0.12.

Thus, the main finding here is the sequent: for both perceptrons with centroid and regression filters, the theory in [2] introduced some bias but the correlation coefficients between the predictions and the actual accuracies were high: 0.90 and 0.97, respectively. These differences should be attributed to the effect of the assumptions used in [2]. The next section will elaborate more on this topic.

D. Prediction of expected accuracies for deep CNNs

1) Deep ANNs in terms of encoding and perceptron parts:
In the remainder, we will apply the perceptron theory described in Section II-A on deep ANNs. To apply the theory, we dissect the holistic functionality of a deep network into two parts: a multi-layer encoding stage and a single-layer classification by perceptrons as depicted in Fig. 4. It is not very common to look at ANNs this way but, for example, a recent work [31] has used the same dissection to study the terminal phase of the training. Note that this dissection is conceptual, it affects neither training nor inference processes. This bipartite view suggests that most of the network is doing an encoding, i.e. producing a useful representation of an input pattern. As we will see below, a similar conceptual dissection can be applied if the encoding stage includes convolutional layers (i.e., CNNs) or recurrent connections (i.e., RNNs), as long as the last hidden layer and the output later are densely connected.

2) Setup: Here, we describe the results of experiments with a set of well-known deep CNNs, which were pretrained on the ImageNet dataset [32]. The ImageNet dataset arose from ImageNet Large Scale Visual Recognition Challenge (ILSVRC). Currently, it is one of a well-established benchmarks in the object category classification and detection. The ImageNet includes \( D = 1,000 \) classes corresponding to different object categories, which makes it hard to preform well on this task. The training data of the ImageNet includes over 14 million images. The validation set from ILSVRC 2012 challenge has 50,000 images in total; exactly 50 images per each class.

In the experiments below, 15 pretrained deep CNNs were used: AlexNet [33], GoogLeNet [34], ResNet-18, ResNet-50, ResNet-101 [35], VGG-16, VGG-19 [36], ShuffleNet [37], MobileNet-v2 [38], DenseNet-201 [39], Inception-v3 [40], Inception-ResNet-v2 [41], Xception [42], NASNet-Mobile, and NASNet-Large [43]. The accuracy of the deep CNNs was assessed using the validation set from ILSVRC 2012 challenge. Blue solid lines in the figures below are the lines fitted to the results.

For each network, we fist saved the weight matrix corresponding to the connections between the last hidden layer and the output layer. Recall that in our interpretation this weight matrix (readout perceptron) is treated as a set of \( D \) linear filters where for each class the linear filter is the corresponding \( N \)-dimensional vector. Second, for all networks we have also obtained the activations of the last hidden layer for each image in the ILSVRC 2012. Recall that these activations are seen as the results of the multi-layer encoding stage of the network.
Fig. 5. The accuracy of 15 deep CNNs on the ILSVRC 2012 validation dataset against the predicted accuracy. Left: sub-problems of different size randomly sampled from the ImageNet. The predicted accuracies for individual classes were calculated according to (2). Color of point indicates the size of the sub-problems. Title for each panel states network’s name and the correlation coefficient. Right: The predicted accuracies of networks were calculated according to (2) and then compensated using the lines from the left panel.

All linear filters and the last hidden layer activations of a particular class were used to calculate the postsynaptic sums. The resultant matrix was used as a data sample to estimate parameters of probability density functions, which are involved in calculating the predicted accuracy $a_i$ for that class.

3) Predictions according to (2): We compared the actual accuracy of each network against its predicted accuracy, where the predicted accuracies for individual classes were calculated according to (2) and then aggregated into a single prediction (left panel in Fig. 5). The results were mixed. On one hand, the correlation coefficient between the actual accuracies and predicted accuracies was 0.933, indicating a high similarity between the actual and predicted accuracies. Also Kendall’s $\tau$ correlation coefficient measuring the quality of the ranking of the networks performance was 0.86, which is rather high. On the other hand, there are obvious issues with the predicted accuracies. First, there is a clear bias: for networks with predicted accuracies of less than 0.75, the predicted accuracies underestimate the actual accuracies, e.g., for ShuffleNet it was 0.52 and 0.65, respectively. For networks with predicted accuracy of more than 0.75 the situation was the opposite, with the accuracies of NASNet-Mobile and NASNet-Large being overestimated by about 0.07. Second, single points deviate noticeably from the fitted linear trends. For example, even after compensating for bias the largest error was observed for AlexNet, where the predicted accuracy overestimated the accuracy by 0.05; the mean value of the absolute error was 0.02.

One explanation of these prediction errors is that assumption i) in (2) is violated, the assumption that the postsynaptic sums are distributed normally. We quantified the effect of this assumption by using non-parametric kernel density estimation

Practically, it was averaging as in the ILSVRC 2012 each class has the same number of images so $f_i = \frac{1}{D} = 10^{-3}$.

Fig. 6. The difference between the accuracy and the predicted accuracy for 15 deep CNNs against the average correlation coefficient in the covariance matrices. The predicted accuracies were calculated according to (2) for the probability density functions and then calculated the predicted accuracy in the same way as in (2). The accuracies predicted with the kernel estimation (right panel in Fig. 5) indeed differ somewhat from the ones depicted in the left panel. However, dropping the assumption of Gaussianity did not significantly reduce the error in predicted accuracies. The strong bias was still present and the deviations of the points from the fitted line were still non-negligible. The mean value of the absolute error after compensating the bias was at 0.02.

The next natural step was to investigate the effect of assumption iii), that the distributions of individual postsynaptic sums are all independent.

4) On removing bias introduced by (2): Since (2) does not take into account the covariance matrix, it is worth checking
Fig. 7. The accuracy of 6 deep CNNs against the predicted accuracy for the sub-problems of size 4. The predicted accuracies for individual classes were calculated either according to (2) or (3).

whether some information contained in the covariance matrix itself is able to explain the bias introduced by the predicted accuracies. Fig. 6 depicts the difference between the observed accuracy and the predicted accuracy against the average value of correlation coefficients in the covariance matrices of each network. We see that the difference closely follows the average values of correlation coefficients for different networks. In particular, the correlation coefficient between the differences and the average correlation coefficients was −0.95. Thus, at least for the ImageNet dataset we can conclude that it is possible to use the average correlation coefficient to predict whether the predicted accuracy is too optimistic or too pessimistic about the actual accuracy.

Moreover, since it is hard to conclude much from only 15 datapoints, we used ImageNet to create sub-problems with smaller numbers of classes. In our experiments the sub-problem of a given size was generated by randomly (without replacement) choosing the classes to be included in the sub-problem. The following sizes of sub-problems were used \{2, 4, 8, 16, 32, 64, 128, 256, 512, 768\}. For each network and for each sub-problem size, 40 different sub-problems were evaluated.

Each panel in Fig. 5 (left) corresponds to a deep CNN. Each point corresponds to a sub-problem with the size of the sub-problem encoded by color. First of all, we see that each network develops its own bias, which is in line with the bias present in the left panel in Fig. 3. This suggests that assuming independence between distributions of postsynaptic sums of output neurons caused a noticeable bias effect on the predicted accuracies. Moreover, the error between the actual and predicted accuracies caused by the bias was increasing with the size of the sub-problem. However, what is astonishing is that the correlation coefficients between the actual and predicted accuracies were almost exactly one for individual networks (the lowest one was 0.988 for NASNet-Large). This is another implicit indication that the assumption of normal distribution is not critical for predicting accuracy. Moreover, the lines fitted for each network can now be used to compensate the corresponding predicted accuracies in the left panel in Fig. 5. For the compensated predicted accuracies against the actual accuracies the correlation coefficient was 0.998 (right panel in Fig. 5). We also notice that the compensations based on the sub-problems on individual networks have almost removed bias and unsystematic deviations between the accuracies. The compensated predicted accuracies overestimate the actual accuracies to a lesser degree than that depicted in Fig. 3. e.g., the largest error (overestimated) was 0.02 for NASNet-Mobile.

5) Predictions according to (3): The results in the right panel of Fig. 5 are encouraging from the point that the compensated predicted accuracies nearly perfectly corresponded to the accuracies. Obviously, Kendall’s τ correlation coefficient was 1.00. On the other hand, in order to make the compensation it is necessary to observe accuracies of smaller sub-problems, which is highly undesirable. The solution to this problem is to get rid of the independence assumption by calculating the predicted accuracies according to (3). This approach, however, has its own complications as the numerical integration of (3) is challenging, even for the moderate number of classes. Thus, to demonstrate that (3) addresses the bias issue, we have performed another experiment. We selected the sub-problems from ImageNet where the size of the sub-problem was fixed to 4 classes. Different from the previous experiment, we first randomly chose 10,000 sub-problems and calculated both the actual and predicted accuracies using (2). Then we handpicked 25 most challenging sub-problems choosing the ones whose predicted accuracies calculated using (2) resulted in large errors. For these sub-problems, we used both formulae, (2) and (3), to predict the accuracies (Fig. 7). For the considered networks
there was no bias in the predictions calculated according to (3), which is an empirical demonstration that (3) can predict a wider range of network architectures.

As Fig. 7 suggests, calculating the predicted accuracies with (3) should address the problem of bias introduced by (2). However, the numerical integration for problems with many classes such as the ImageNet is not tractable. We partially circumvented this problem by using a Monte Carlo approach for sampling from the estimated distributions. The results obtained with the Monte Carlo approach (Fig. 8) are quite obviously better than the ones obtained with (2). The correlation coefficient was 0.98, the Kendall’s $\tau$ correlation coefficient was 0.92. Another nice outcome is that the points are arranged on a line (dashed line) parallel to the line of perfect correspondence (solid line), i.e., all the predictions slightly overestimated the actual accuracies by a constant offset. This offset just comes from the fact that one should use the normalization constant in our estimations, which Monte Carlo sampling does not provide.

Fig. 9 presents the results of applying the same sampling approach to different sizes of sub-problems randomly formed from the ImageNet. Overall, we still see the same trend as in Fig. 8 i.e., that the predicted accuracies were approximately offset from the line of perfect correspondence by a constant (dashed lines). The difference is more noticeable with the decreased size of a sub-problem, which indicates the increased importance of normalization constants.

6) Predicted accuracy from the readout only: One interesting question with the proposed theory is: how well could it work given only the readout perceptron but no activations of the last hidden layer? Quite surprisingly, as we will see below, it was possible to achieve a $\tau$ correlation coefficient of 0.71 by computing the predicted accuracy only from the readout perceptrons, without any access to the mapped representations of input patterns.

Intuitively, a possible way to calculate the required statistics (i.e., $\mu$ and $\sigma$) would be to use linear filters themselves in place of the hidden layer activations. The issue with this approach, however, is that the postsynaptic sums to linear filters themselves are much higher than that of the hidden layer activations from real data, therefore, the predicted accuracies calculated in this way are nearly 1. A possible way to mitigate this issue is to disturb the linear filters by adding some white noise to them. The white noise acts as a way to obtain surrogates of actual statistical distribution of data. We have made the experiments for different level of noise. In a single experiment, each linear filter was disturbed 50 times. The disturbed versions were used as the hidden layer activations for linear filter’s class. Fig. 10 (solid line) reports the mean correlation coefficients between the actual accuracy and the predicted accuracies obtained from surrogate statistics from ten experiments for each level on noise. The results suggest that either high or low noise levels did not result in high correlation but there was a window between 8 and 17 dB where the correlation peaked getting as high as 0.66.

A natural question to ask would be: how to know which level of noise to use to obtain the highest correlation? We think that it could be identified in a straightforward manner; we use two observations to do so. First, we expect that different networks have somewhat different accuracy. Second, we know that the best value of noise is somewhere in between the extremes. That is because when the noise is too high the predicted accuracies of all the networks would vanish to zero while when the noise is too low the predicted accuracies would saturate at one. Using these observations we expect that the best level of noise should result in the largest dispersion of the predicted accuracies, which can be simply measured by the standard deviation of the predicted accuracies. The dashed line in Fig. 10 depicts mean (across ten experiments) standard deviations for each level of noise. As we can see from comparing this curve with the curve for the correlation coefficients, both curves peaked approximately in the same window between 8 and 17 dB. Thus, choosing the level on noise corresponding to the largest standard deviation we also expect to get close to the peak in the correlation coefficient. The absence of a clear peak might be interpreted as the indication that the accuracy of all the networks is so close to each other that we cannot discriminate between them using only information about their perceptrons.

Finally, we can use the obtained predicted accuracies in order to rank networks using, for example, Kendall’s $\tau$ correlation coefficient to measure the quality of the ranking. The largest mean $\tau$ was 0.71, which is not a perfect ranking ($\tau = 1$),
III. Discussion

A. Summary of results

We present a theory for classification with perceptron networks, which describes the network performance for any learning rule. The perceptron being one of the earliest ANN models [8], one would expect such a theory in standard textbooks. Maybe the lacking universality of one-layer perceptrons [9] explains the late and gradual development of a general perceptron theory, which occurred in the context of neuroscience and more complex ANNs [10], [7]. The presented perceptron theory generalizes the earlier versions, and thus is applicable to a wider variety of ANNs that contain a perceptron-like output layer.

We first verified that our perceptron theory [3] can accurately predict the performance of Echo State Networks, even with the readout optimized by linear regression. In this scenario, the previous theory [2] was insufficient. Next, we investigated the application of the perceptron theory to shallow and deep networks. The empirical evaluation of the predicted accuracy was performed on numerous classification datasets with shallow networks and with the ImageNet dataset on several deep networks. In both cases, we observed high correlation between the predicted accuracies and actual accuracies even when assumptions in the theory definition were violated, namely independence of postsynaptic sum distributions for different classes. This formulation, however, introduced a bias to the predicted accuracies. The bias can be mitigated either empirically, or by using formula [3], which does not assume independence.

B. Relations to previous ANN work

Investigations on how to analyze and predict the classification performance of ANNs go back to many decades [3], [44], [45]. Recent interest in this research topic has been in the context of Network Architecture Search (NAS) [46], [47], [48], Knowledge Distillation (KD) [49], and in studies on how to enhance the performance of simpler models by leveraging more complex ones [50], [51].

The previous works most similar to ours have proposed to predict accuracy based on the weights of various layers within the ANN [4], or based on activations in the different layers [5]. In [4], the authors train estimators, which were able to reasonably rank the classification performance of a plethora of CNNs. In [5], the authors trained a “meta network” to predict the correctness of an ANN on an individual input pattern, by using the activations in the hidden layers. The results of these studies, as well as [52], support our approach to bisect ANNs into a encoding and readout perceptron stages: In [4] it was observed that parameters of the last fully connected weight layer (i.e., readout perceptron) were among the most informative and frequently used ones. In [5], the authors reported that for predicting network accuracy the activations of the last hidden and output layer were the most useful.

Most of the described previous work on performance estimation relies on training an estimator model (e.g., an elementary regressor or another ANN). In contrast, our theory is based solely on the computation of a statistical formula and does not require an estimator model. One might argue that a theory that predicts accuracies based on the activations in the last hidden layer does not add anything new, because the accuracies could be computed directly by going through the last layer. Note, however, that the theory does not use the activations explicitly. Rather, it estimates the accuracies from the low-order statistical moments of the postsynaptic sums in the output neurons. Thus, the theory gives insight into statistical properties of the postsynaptic sums (which depend on synaptic weights and input statistics) determine the accuracy of the network.

C. Future directions

The presented work raises some interesting new questions for further investigation. One question is whether the theory could be used to design more efficient or faster training algorithms, perhaps by using the theory predictions to identify classes that need more training. Another obvious research direction concerns the numerical evaluation of the theory formulae. It would be interesting to compare existing methods for numerical multidimensional integration in their ability to evaluate the more precise formula [3] for larger number of classes.

With respect to the possible applications of this work, we foresee the following:

- The proposed perceptron theory is applicable to any network architecture with perceptron-like output layer. Thus, the potential application range goes far beyond the network architectures we have investigated in the paper.
- The proposed theory enables ranking of different network models for a particular task without direct access to the data, which is important as in many cases data privacy is a huge issue.
- An even more innovative potential use of our theory is for comparing networks without any access to the data nor to the encoding stage of the network. As we have shown in the experiments, the results are less accurate but can be considered as a the first filtering step in a multi-stage evaluation process for granting access to the data only to the most promising networks.
- Last, our approach can not only predict classification accuracies but also be extended to estimate probabilities of observing a certain vector of postsynaptic sums in the output layer. This estimation can potentially be used to detect adversarial examples and other outliers.

APPENDIX A

ORIGINAL PROBLEM FORMULATION

The original problem formulation in [7] was devoted to studying the short-term memory of distributed representations in such frameworks as Vector Symbolic Architectures (VSAs)
and recurrent randomly connected ANNs (e.g., Echo State Networks, ESNs [20]). In particular, here we consider the trajectory association task [22] as one of the ways of studying the short-term memory of a simplified version of the ESN [53]. The ability of being able to form and use short-term memory is a key enabler for many VSAs use-cases such as representation of data structures [54], [55], [56] and processing of strings [57], [58], [59].

The trajectory association task has two stages: memorization and recall. At the memorization stage, at every time step \( m \) the ESN stores a symbol \( s(m) \) from the sequence of symbols \( s \) to be memorized. The number of unique symbols (i.e., alphabet size) is denoted as \( D \). The symbols are represented using \( N \)-dimensional random bipolar dense vectors stored in the codebook \( \Phi \in \{−1, 1\}^{N \times D} \). Thus, at every time step \( m \) the ESN is presented with the corresponding \( N \)-dimensional vector \( \Phi s(m) \), which is added to the hidden layer of the ESN \( x \in \mathbb{Z}^{N \times 1} \). The state of the hidden layer at time step \( m \) (denoted as \( x(m) \)) is updated as follows:

\[
x(m) = f(x(m-1)) + \Phi s(m),
\]

where \( x(m-1) \) is the previous state of the hidden layer at time step \( m-1 \); \( \rho \) denotes the permutation operation (e.g., circular shift to the right), which acts as a simple variant of a recurrent connection matrix; \( f(x) \) is a clipping function – nonlinear activation function, which keeps the values of the hidden layer in the limited range using a threshold value \( \kappa \) as:

\[
f(x) = \begin{cases} 
-\kappa & x \leq -\kappa \\
\kappa & x \geq \kappa
\end{cases}
\]

In practice, the value of \( \kappa \) regulates the recurrence effect of the ESN.

At the recall stage, the ESN uses the content of its hidden layer \( x(m) \) as the query vector to retrieve the symbol stored \( d \) steps ago, where \( d \) denotes delay. In the experiments below, the range of the delays varied between 0 and 25. The recall is done by using the readout perceptron for particular \( d \), which contains one \( N \)-dimensional vector (linear filter) corresponding to each symbol. The readout vector is denoted as \( W^d \in \mathbb{R}^{D \times N} \) and the recall is done as:

\[
s(m-d) = \arg \max(W^d x(m)),
\]

where \( \arg \max(\cdot) \) returns the symbol with the highest postsynaptic sum among the output neurons for the chosen delay \( W^d \) value and the given hidden layer state \( x(m) \).

Let us consider two approaches of forming the readout perceptron. First, it can be constructed as done usually in VSAs from the codebook \( \Phi \) and the reverse permutation by \( d \):

\[
W^d = \rho^{-d}(\Phi^T).
\]

The advantage of this approach is that no training is required to obtain the readout perceptron.

An alternative approach, which is more native for ESNs, is to obtain \( W^d \) via solving a linear regression on a given training sequence and the corresponding states of the hidden layer. The advantage of this approach is that, as we have seen in Fig. 1 in the main text, it has higher accuracy, than the codebook-based approach.

While it is straightforward to simulate the presented network and obtain the accuracies for different values of \( d \) empirically, predicting the accuracy analytically given only the parameters \((N, D, d, \text{and} \kappa)\) is challenging. Nevertheless, [7] has proposed a solution to this problem when the perceptron is based on the codebook as in (4). The solution includes two components. The first one is the equation for calculating the predicted accuracies \( a \) (i.e., the expected accuracy):

\[
a := p(s(m-d) = \hat{s}(m-d)) = \int_{-\infty}^{\infty} dx \frac{e^{-(x-\mu_h)^2/(2\sigma_h^2)}}{\sqrt{2\pi}\sigma_h} (\Phi(x, \mu_r, \sigma_r))^{D-1},
\]

where \( \mu_h \) and \( \sigma_h \) denote the mean and standard deviation of the postsynaptic sum (i.e., dot product) between \( x(m) \) and the row of \( W^d \) (i.e., linear filter) corresponding to the correct symbol \( s(m-d) \) while \( \mu_r \) and \( \sigma_r \) denote the mean and standard deviation of the postsynaptic sum for all other symbols in the codebook. Note that (5) is equivalent to (1) in the main text. Moreover, (5) is a special case of (2) where for all symbols in the codebook other than the correct symbol the same \( \mu_r \) and \( \sigma_r \) are assumed that is because the codebook-based perceptron uses \( \Phi \) where representations for different symbols are random and, therefore, for large \( N \) they are quasi orthogonal to each other. Due to this fact, we know that the expected value of \( \mu_r \) is 0 and that of \( \sigma_r \) is \( \sqrt{N\kappa/(k+1)/3} \). However, the values of \( \mu_h \) and \( \sigma_h \) depend on the given values of \( d \) and \( \kappa \), therefore, the second component of the solution determines them (please refer to (2.44)-(2.47) in [7]).

It is also worth mentioning that (5) is the generalization of (2) because once we assume that \( \Sigma \) is diagonal (i.e., variables in \( x \) are independent) (3) can be simplified to (2) as follows:

\[
a = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{i=1}^{L} p(x, \mu, \Sigma) dx_1 dx_2 \cdots dx_L = \\
\int_{-\infty}^{\infty} p(x_1) dx_1 \int_{-\infty}^{\infty} p(x_2) dx_2 \cdots \int_{-\infty}^{\infty} p(x_L) dx_L = \\
\int_{-\infty}^{\infty} \cdot \cdots \int_{-\infty}^{\infty} p(x_1, \mu_1, \sigma_1) dx_1 \Phi(x_1, \mu_2, \sigma_2) \cdots \Phi(x_1, \mu_L, \sigma_L) = \\
\int_{-\infty}^{\infty} \cdot \cdots \int_{-\infty}^{\infty} p(x_1, \mu_1, \sigma_1) dx_1 \prod_{j=2}^{L} \Phi(x_1, \mu_j, \sigma_j).
\]

Note that in the case of the regression-based perceptron one cannot assume the independence of linear filters in the perceptron. Therefore, currently, there is no way of analytically estimating \( \mu_h, \mu_r, \sigma_h, \text{and} \sigma_r \) for the regression-based perceptron. Nevertheless, these values could be estimated empirically using the simulations. Fig. 5 presents the \( \mu_h, \mu_r, \sigma_h, \text{and} \sigma_r \) for different values of \( d \) for both regression-based (red color) and codebook-based (blue color) perceptrons. Notice, that there are several important differences between the statistics.
we have observed both underestimation and overestimation of the empirical accuracy while in Fig. 1 we have observed for different perceptrons. First, $\mu_h$ for the regression-based perceptron is higher than that of the codebook-based perceptron, however, for both perceptrons $\mu_h$ is decreasing with the increased delay, which is expected. Second, both $\sigma_h$, and $\sigma_r$ are much lower in the case of the regression-based perceptron. Both facts should positively affect the accuracy. Third, there is a strong negative correlation between the linear filters in the regression-based perceptron. As it was shown in Fig. 1 in the main text, the presence of correlation hindered the applicability of (5) but the use of (3) allowed getting the correct accuracy.

Last, let us make an important note on how the considered scenario is related to predicting the accuracy of an ANN. First, in the case of classification we do not assume delay so we can safely say that $d = 0$. Second, the activation of the last hidden layer of an ANN corresponds to the hidden layer activity in the considered ESN. Note, however, that there is no guarantee that these activations are noisy versions of the entries of some fixed random matrix as the activations come from (usually continuous) real data. Last, the weights of the output layer of an ANN are more similar to the regression-based perceptron than to the codebook-based perceptron because they are obtained through an optimization procedure (e.g., error backpropagation). This implicitly explains the bias observed in Fig. 5 when using (2) to calculate the predicted accuracy. Recall, that in Fig. 5 we have observed both underestimation and overestimation of the empirical accuracy while in Fig. 1 we have observed only the overestimation. Therefore, in Section B we will study the effect of the correlation on the results produced by (2) or (1)/(5).

APPENDIX B
THE EFFECT OF CORRELATION ON (2) AND (1)/(5)

In Fig. 1 in the main text, we have seen that even in the case of two symbols (or two classes) the presence of correlation might result in inaccuracies between the predicted accuracy and the actual accuracy. Nevertheless, using (1)/(5) or (2) to calculate the predicted accuracy is tempting because numerically it is a simple task compared to (5). Therefore, one interesting question is whether it is possible to compensate bias introduced by (1)/(5) or (2) without the need of, e.g., calculating the accuracies on sub-problems as in Fig. S.1.

In order to study this, we created a synthetic binary classification problem ($D = 2$) assuming that the mean value of postsynaptic sums of the incorrect class is 0 while that of the correct class is a parameter. It was also assumed that postsynaptic sums distributions of both classes have the same standard deviation, which is also a parameter. Finally, the postsynaptic sum distributions can correlate with each other positively or negatively and their correlation coefficient is a parameter. Note that when there is no correlation between the classes we can perfectly use (1)/(5) or (2) for the given mean and standard deviation values. We can also use (1)/(5) or (2) even when there is a correlation but in this case the predicted accuracy would differ from the actual accuracy. In order to see the effect of the correlation between classes on the accuracy we simulated many cases for different values of correlation, mean, and standard deviation. Fig. S.2 depicts the results. As we can see, there is a highly non-linear relation between the predicted accuracy, correlation coefficient, and the empirical accuracy. Qualitatively, we expect that in the case of a negative correlation the accuracy will be lower than the predicted accuracies (cf. red lines in Fig. 1) and vice versa in the case of the positive correlation. However, it seems hard to make more quantitative correction without making a look-up table like structure, which would interpolate the expected accuracy value for the given correlation and predicted accuracy. While this is possible to do for the binary classification problems, this solution becomes inadequate for larger values of $D$ because we would have to deal with many interactions in the covariance matrix, which cannot be simply stored as a compact look-up table.

REFERENCES
[1] High-Level Expert Group on Artificial Intelligence. *Ethics Guidelines for Trustworthy AI*. 2019.
[2] Executive Office of the President National Science and Technology Council Committee on Technology. *Preparing for the Future of Artificial Intelligence*. 2016.
[3] M. Egmont-Petersen, J. L. Talmon, J. Brender, and P. McNair. On the Quality of Neural Net Classifiers. *Artificial Intelligence in Medicine*, 6(5):359–381, 1994.
[4] T. Unterthiner, D. Keysers, S. Gelly, O. Bousquet, and I. Tolstikhin. Predicting Neural Network Accuracy from Weights. *arXiv:2002.11448*, pages 1–17, 2020.
[55] D. Kleyko, A. Rahimi, R. W. Gayler, and E. Osipov. Autoscaling Bloom Filter: Controlling Trade-off Between True and False Positives. *Neural Computing and Applications*, 32:3675–3684, 2020.

[56] T. Yerxa, A. Anderson, and E. Weiss. The Hyperdimensional Stack Machine. In *Cognitive Computing*, pages 1–2, 2018.

[57] D. V. Pashchenko, D. A. Trokoz, A. I. Martyshkin, M. P. Sinev, and B. L. Svistunov. Search for a Substring of Characters using the Theory of Non-deterministic Finite Automata and Vector-Character Architecture. *Bulletin of Electrical Engineering and Informatics*, 9(3):1238–1250, 2020.

[58] D. Kleyko, E. Osipov, and R. W. Gayler. Recognizing Permuted Words with Vector Symbolic Architectures: A Cambridge Test for Machines. *Procedia Computer Science*, 88:169–175, 2016.

[59] A. Joshi, J. T. Halseth, and P. Kanerva. Language Geometry Using Random Indexing. In *Quantum Interaction (QI)*, pages 265–274, 2016.