Design and regularization of neural networks: the optimal use of a validation set

Larsen, Jan; Hansen, Lars Kai; Svarer, Claus; Ohlsson, Børje Ola Mattias

Published in:

Link to article, DOI:
10.1109/NNSP.1996.548336

Publication date:
1996

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
DESIGN AND REGULARIZATION OF NEURAL NETWORKS: THE OPTIMAL USE OF A VALIDATION SET

J. Larsena, L.K. Hansena, C. Svarerb and M. Ohlsson*

*CONNECT, Department of Mathematical Modelling, Building 349
Technical University of Denmark
DK-2800 Lyngby, Denmark
emails: jl@imm.dtu.dk, lkhansen@ei.dtu.dk, mo@imm.dtu.dk

bDepartment of Neurology
National University Hospital
DK-2100 Copenhagen Ø, Denmark
email: csvarer@pet.rh.dk

Abstract - In this paper we derive novel algorithms for estimation of regularization parameters and for optimization of neural net architectures based on a validation set. Regularization parameters are estimated using an iterative gradient descent scheme. Architecture optimization is performed by approximative combinatorial search among the relevant subsets of an initial neural network architecture by employing a validation set based Optimal Brain Damage/Surgeon (OBD/OBS) or a mean field combinatorial optimization approach. Numerical results with linear models and feed-forward neural networks demonstrate the viability of the methods.

INTRODUCTION

Neural networks are flexible tools for function approximation and by expanding the network any relevant target function can be approximated [6]. The associated risk of overfitting on noisy data is of major concern in neural network design [2]. The objective of architecture optimization is to minimize the generalization error. The literature suggest a variety of algebraic generalization error estimators e.g., FPE [1], FPER [9], GEN [7], GPE [13] and NIC [14]. These estimates, however, depend on a number of statistical assumptions which can be quite hard to justify. Hence, many neural net practitioners resort to empirical methods for design and validation, the simplest being to base the design on a single separate validation set. For further discussion on empirical generalization assessment see e.g., [10]. In this contribution we derive schemes for proper selection of neural net architecture and for estimation of regularization parameters using a simple validation set approach. In fact, one may view estimation of the optimal regularization as an alternative
methodology for architecture selection.

TRAINING AND VALIDATION

In order to train and validate, the available dataset, $D$, of $N$ examples is split into two disjoint sets: a validation set, $V$, with $N_v = \lceil \gamma N \rceil$ examples for architecture selection and estimation of regularization, and a training set, $T$, with $N_t = N - N_v$ examples for estimation of network parameters. $\gamma$ is referred to as the split-ratio.

The neural network is described by the vector function $f(x; w)$ where $x$ is the input vector and $w$ is the vector of network weights and thresholds with dimensionality $m$. The cost function for network training is supposed to be the sum of a loss function (or training error), $S_T(w)$, and a regularization term $R(w)$, i.e.,

$$ C(w) = S_T(w) + R(w) = \frac{1}{N_t} \sum_{k=1}^{N_t} \ell(y(k), \hat{y}(k); w) + R(w) $$

where $\ell(\cdot)$ measures the distance between the output $y(k)$ and the network prediction $\hat{y}(k) = f(x(k); w)$. Often the mean square error loss $\ell = |y - \hat{y}|^2$ is chosen. $N_t \equiv |T|$ defines the number of training examples, i.e., input-output pairs of the training set: $T = \{(x(k), y(k))\}_{k=1}^{N_t}$. Training provides the estimated weight vector $\hat{w} = \arg \min_w C(w)$. The validation set consist of another $N_v \equiv |V|$ examples and the validation error$^2$ of the trained network reads:

$$ S_V(\hat{w}) = \frac{1}{N_v} \sum_{k=1}^{N_v} \ell(y(k), \hat{y}(k); \hat{w}) $$

where the sum runs over the $N_v$ validation examples. $S_V(\hat{w})$ is thus an estimate of the generalization error defined as the expected loss: $G(\hat{w}) = E_{x,y}(\ell(y, \hat{y}; \hat{w}))$, where $E_{x,y}(\cdot)$ denotes the expectation w.r.t. to the joint input-output distribution.

An minimal necessary requirement for a procedure which estimates the network parameters on the training set and optimizes the architecture on the validation set is that the generalization error of an non-optimized network architecture trained on the full data set $D$ is higher. This is not always the case as discussed in [17, Chap. 6]: performing indirect regularization by stopping training when minimum validation error is reached is equivalent to training an non-regularized network on the full data set. There is consequently a risk of overusing the validation set. In order to avoid this situation prior constraints should be imposed, as will be demonstrated in various examples below.

There exist obviously an optimal choice of the split-ratio, $\gamma$, between training and validation set sizes. This choice is an interesting open and difficult

$^1\lceil \cdot \rceil$ denotes rounding upwards to the nearest integer.

$^2$The loss function on the validation set.
problem. The choice depends on the objective, 2. which scheme one for applies for minimizing the validation error, and 3. on the learning curve\textsuperscript{3} \textsuperscript{5} for the problem under consideration. The case of an optimal generalization estimate (in mean square sense) was discussed in \textsuperscript{10}. Without further ado, one would suggest to use the balanced split $\gamma = 0.5$

**ESTIMATION OF REGULARIZATION PARAMETERS**

The standard approach for estimation of regularization parameters, such as e.g., weight decays, is by more and less systematic search and evaluation of the validation set error; however, as will be shown, it is possible to derive an optimization algorithm based on gradient descent.

Consider a regularization term $R(w, \kappa)$ which depends on $q$ regularization parameters contained in the vector $\kappa$. Since the estimated weights $\hat{w} = \text{arg min}_w C(w)$ depend in a definite way on the regularization term, we may in fact consider the validation error as an implicit function of the regularization parameters,

$$S_V(\hat{w}(\kappa)) = \frac{1}{N_v} \sum_{k=1}^{N_v} \ell(y(k), \hat{y}(k); \hat{w}(\kappa))$$ \hspace{1cm} (3)

where $\hat{w}(\kappa)$ is the $\kappa$-dependent vector of weights estimated from the training set. The optimal regularization can be found by e.g., gradient descent\textsuperscript{4},

$$\kappa(j + 1) = \kappa(j) - \eta \frac{\partial S_V}{\partial \kappa}(\hat{w}(\kappa(j)))$$ \hspace{1cm} (4)

where $\eta > 0$ is a gradient step-size and $\kappa(j)$ is the estimate of the regularization parameters in iteration $j$. Using the chain rule the gradient vector can be rewritten as

$$\frac{\partial S_V}{\partial \kappa}(\hat{w}(\kappa(j))) = \frac{\partial w^\top}{\partial \kappa}(\hat{w}(\kappa(j))) \cdot \frac{\partial S_V}{\partial w}(\hat{w}(\kappa(j)))$$ \hspace{1cm} (5)

where $\partial w^\top / \partial \kappa$ is the $q \times m$ derivative matrix of the estimated weights w.r.t. the regularization parameters. In order to find this derivative matrix we use the following fact: if $\hat{w}(\kappa(j))$ and $\hat{w}(\kappa(j + 1))$ are optimal weight vectors then

$$\frac{\partial C}{\partial w}(\hat{w}(\kappa(l))) = 0, \hspace{0.2cm} l = \{j, j + 1\}.$$ \hspace{1cm} (6)

This implies:

$$\frac{\partial^2 C}{\partial \kappa \partial w}(\hat{w}(\kappa(j))) = 0.$$ \hspace{1cm} (7)

\textsuperscript{3}The learning curve is a plot of the generalization error vs. the number of training examples.

\textsuperscript{4}Moreover, one might consider suggesting second order schemes. However, these schemes work best for problems where the solution is an interior point somewhat away from the boundary of the domain over which the minimum is searched for. We tried a second order scheme for optimizing multiple weight decay parameters in a linear model without obtaining a convincing result.
This equation can be used for determining $\partial \mathbf{w}^T / \partial \kappa$. To be specific, assume that the regularization term is linear in the regularization parameters, i.e.,

$$ R(\mathbf{w}, \kappa) = \kappa^T \mathbf{r}(\mathbf{w}) = \sum_{i=1}^{q} \kappa_i r_i(\mathbf{w}) \quad (8) $$

where $\kappa_i$ are the regularization parameters and $r_i(\mathbf{w})$ associated regularization functions. Using Eq. (8) in (7) gives after some algebra:

$$ \frac{\partial \mathbf{w}^T}{\partial \kappa} (\mathbf{w}) = - \frac{\partial \mathbf{r}}{\partial \mathbf{w}^T} (\mathbf{w}) \cdot \mathbf{J}^{-1}(\mathbf{w}) \quad (9) $$

where $\mathbf{J} = \partial^2 C / \partial \mathbf{w} \partial \mathbf{w}^T$ is the Hessian of the cost function which e.g., might be evaluated using the Gauss-Newton approximation [12]. Finally, substituting Eq. (9) into (5) gives:

$$ \frac{\partial S_V}{\partial \kappa} (\mathbf{w}) = - \frac{\partial \mathbf{r}}{\partial \mathbf{w}^T} (\mathbf{w}) \cdot \mathbf{J}^{-1}(\mathbf{w}) \cdot \frac{\partial S_V}{\partial \mathbf{w}} (\mathbf{w}) \quad (10) $$

$\partial S_V / \partial \mathbf{w}$ is found by ordinary back-propagation on the validation set while $\partial \mathbf{r} / \partial \mathbf{w}^T$ is calculated from the specific assumptions on the regularizer. If the regularizer is assumed to be a weight decay regularizer with one regularization parameter per weight, i.e., $R(\mathbf{w}, \kappa) = \sum_{i=1}^{m} \kappa_i \mathbf{w}_i^2$, Eq. (10) reads:

$$ \frac{\partial S_V}{\partial \kappa} (\mathbf{w}) = - 2 \left( \mathbf{J}^{-1}(\mathbf{w}) \cdot \frac{\partial S_V}{\partial \mathbf{w}} (\mathbf{w}) \right) \odot \mathbf{w} \quad (11) $$

where $\odot$ denotes the element-by-element vector product. In the case of one regularization parameter per weight there is a potential risk of overusing the validation set: it is frequently possible to choose $\kappa$ such that $\partial S_V / \partial \mathbf{w}|_{\mathbf{w}} = \mathbf{0}^T$. This corresponds to training on the validation set without regularization, which mostly is worse than training a non-regularized network on all data. Consequently, there is a need for constraining the search space. A natural choice is to impose $\kappa_i \geq 0$. Thus the regularization may be interpreted as a pruning regularizer since the weight is pruned by $\kappa_i \to \infty$ and kept in the model by having $\kappa_i = 0$. In practical implementations, the restriction $\kappa_i \geq 0$ is easily incorporated by enforcing $\kappa_i$ the update in Eq. (4) to be positive even though the gradient step suggests it to be negative.

In the case of a simple weight decay, $R(\mathbf{w}, \kappa) = \kappa |\mathbf{w}|^2$, Eq. (10) obeys:

$$ \frac{\partial S_V}{\partial \kappa} (\mathbf{w}) = - 2 \mathbf{w}^T \cdot \mathbf{J}^{-1}(\mathbf{w}) \cdot \frac{\partial S_V}{\partial \mathbf{w}} (\mathbf{w}) \cdot \mathbf{w} \quad (12) $$

---

5Although this regularization term is very general is does not include e.g., weight-elimination by Weigend et al. or Soft Weight Sharing by Nowlan et al.

6For convenience, here $\mathbf{w}$'s explicit $\kappa$-dependence is omitted.

7This possibility is always present for a single output linear model, $\hat{y} = \mathbf{w}^T \mathbf{x}$, using the mean square loss function.

8An alternative solution is to reparameterize; e.g., $\beta_i = |\kappa_i|$ which gives $\partial S_V / \partial \beta_i = \text{sign}(\kappa_i) \cdot \partial S_V / \partial \kappa_i$. 

65
In this case there is no obvious risk of overusing the validation set. That is, it might be advantageous to have a negative weight decay even though the asymptotic \((N_t \to \infty)\) optimal weight decay is positive [9].

**VALIDATION ERROR BASED OBD/OBS**

A natural extension of the Optimal Brain Damage (OBD) [11] and Optimal Brain Surgeon (OBS) [4] pruning schemes is to base saliencies on generalization error rather than training error, as suggested in [15]. This enables deleting weights according to their influence on generalization error. The validation set based saliencies are based on the second order Taylor series expansion:

\[
S_V(w) \approx S_V(\bar{w}) + \frac{\partial S_V}{\partial \bar{w}^T}(\bar{w}) \cdot \Delta w + \frac{1}{2} \Delta w^T \cdot \frac{\partial^2 S_V}{\partial \bar{w} \partial \bar{w}^T}(\bar{w}) \cdot \Delta w
\]  

(13)

where \(\Delta w = w - \bar{w}\). For the OBD approximation: delete one weight and keep the remaining unchanged results in the weight change \(\Delta w = [0 \cdots 0, -\bar{w}_i, 0 \cdots 0]^T\). Hence, the OBD validation saliencies\(^9\) are:

\[
\varrho_i = -\bar{w}_i \frac{\partial S_V}{\partial w_i}(\bar{w}) + \frac{1}{2} \bar{w}_i^2 \frac{\partial^2 S_V}{\partial w_i^2}(\bar{w}).
\]  

(14)

The validation set based OBD procedure, vOBD, is as follows: 1. choose a sufficiently large network, 2. train the network on \(T\), 3. rank weights according to Eq. (14) and delete a small fraction of low saliency weights\(^10\), 4. if \(S_V\) is minimal stop; otherwise go to step 2.

Similarly, vOBS saliencies can be obtained from Eq. (13) using the fact that the remaining weights are retrained within a second order approximation of the cost function, see e.g., [3], [8].

**COMBINATORIAL OPTIMIZATION OF NETWORK ARCHITECTURE**

Architecture selection schemes are based on either network pruning or network growth. Preferably one wish for a hybrid method where deleted weights can reenter the model and vice versa. Exhaustive search would require evaluation of \(2^m - 1\) subnetworks \(-m\) being the number of weights in the fully connected network. An alternative method is to use the computationally cost effective mean field annealing approach (see e.g., [5]) which have shown efficient for hard combinatorial optimization problems [16]. This approach is invoked by using a state vector of binary variables \(s \in \{0, 1\}^m\) indicating if the companion weights are pruned or not. That is, the network function

\(^9\)This corresponds to assuming the Hessian, \(J\), to be diagonal.

\(^10\)The saliencies \(\varrho_i \approx S_V(\bar{w} + \Delta w) - S_V(\bar{w})\).

\(^11\)The saliencies will often be negative, indicating that the generalization actually is improved by removing the particular weight.
becomes \( f(x; w \odot s) \). The weights are estimated on the training set and the state variables on the validation set by using a mean field approach. Initial experiments showed fair results; however, a crucial problem is that retraining is not invoked in the pruning scheme. We are currently pursuing this topic further.

**EXPERIMENTS**

**Linear Model**

Consider the following data generating linear system: \( y(k) = x^T(k)w^o + \epsilon(k) \). \( x(k) \) follows a \( m = 10 \) variate Gaussian distribution \( \mathcal{N}(0, H) \) where \( H \) is the covariance matrix. \( x(k) \) is an i.i.d. sequence, i.e., a time-independent series. The noise \( \epsilon(k) \sim \mathcal{N}(0, \sigma^2_\epsilon) \) is i.i.d. and independent of \( x(k) \). \( \sigma^2_\epsilon = \text{NSR} \cdot V\{y\} \) where \( \text{NSR} = 0.2 \). The “true” weights are \( w^o = [000000011] \).

In order to evaluate the typical algorithm performance, generate, say \( Q \), independent data sets of size \( N = 60 \) and train initially \( m = 10 \) dimensional linear models using the standard mean square error cost to obtain the estimates \( \tilde{w}^{(i)} \), \( i \in [1; Q] \). The true generalization error of each model is then given by \( G(\tilde{w}^{(i)}) = \sigma^2_\epsilon + (\tilde{w}^{(i)} - w^o)^T H (\tilde{w}^{(i)} - w^o) \).

**One Weight Decay.** Dealing with the linear model and a single weight decay, i.e., \( R(w, \kappa) = \kappa \| w \|^2 \), it is possible to show that Eq. (12), for the optimal \( \kappa \), becomes a 3rd order equation in \( \kappa \). However, the coefficients of the equation depends in a very complicated way on the actual training and validation data; hence, we resort to numerical optimization\(^{12}\). Define \( G(w_D) \), the generalization error of the model trained on all data \( D \) without any architecture optimization. Further define \( G(\tilde{w}) \), the generalization error of the model using architecture optimization — in the present case; weight decay optimization. We consider basically two measures of algorithm performance: First, the probability of improvement, defined as

\[
P_{\text{imp}} = Q^{-1} \sum_{i=1}^{Q} \mu(G(w_D^{(i)}) - G(\tilde{w}^{(i)}))
\]

where \( \mu(x) = 1 \) for \( x > 0 \) and zero otherwise. Secondly, the relative improvement in generalization error, defined as

\[
\text{RGI}^{(i)} = 100\% \cdot \frac{G(w_D^{(i)}) - G(\tilde{w}^{(i)})}{G(w_D^{(i)})}. \quad (16)
\]

The results are summarized in Table 1.

**Multiple Weight Decays and vOBD.** In order to evaluate the performance of the gradient descent method for optimizing regularization parameters, we choose the individual weight decay regularizer \( R(w, \kappa) = \sum_{i=1}^{m} \kappa_i w_i^2 \).

\(^{12}\)Here the MATLAB function \texttt{fmin.m} is used.
Table 1: Performance when optimizing a single weight decay on a linear model. $\gamma$ is the split-ratio, $P_{imp}$ the probability of improvement with associated 95% confidence error bars, and $avr(RGI)$ is the average RGI over cases in which improvement was present. Experiment parameters: $Q = 10000$, $H = AA^T$ where $A$ is a randomly chosen Vandermonde matrix (large eigenvalue spread). Note that the results do only have a week dependency on the split-ratio.

<table>
<thead>
<tr>
<th>$\gamma$</th>
<th>$P_{imp}$</th>
<th>$avr(RGI)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.4</td>
<td>0.846 ± 0.007</td>
<td>9.49</td>
</tr>
<tr>
<td>0.5</td>
<td>0.892 ± 0.006</td>
<td>9.61</td>
</tr>
<tr>
<td>0.6</td>
<td>0.911 ± 0.006</td>
<td>9.87</td>
</tr>
<tr>
<td>0.7</td>
<td>0.939 ± 0.005</td>
<td>9.88</td>
</tr>
</tbody>
</table>

The $\kappa_i$'s are forced to be positive in order to eliminate overuse of the validation data. First the model is trained with initial values of $\kappa_i$, then $\kappa_i$ are updated by Eq. (11) and (4) using a gradient parameter $\eta$, finally retrain the weights, and repeat the scheme until the relative change in $S_V$ is less than a prescribed small number. Subsequently, the weights are retrained on all data using the optimized regularization. We tried many different parameter settings and found that the algorithm is sufficiently robust. Fig. 1 summaries a few results of running the algorithm. For comparison we ran a standard

Figure 1: Performance when optimizing multiple weight decays on a linear model. $\gamma$ is the split-ratio, $P_{imp}$ the probability of improvement with associated 95% confidence error bars, and $avr(RGI)$ is the average RGI over cases in which improvement was present. Experiment parameters: $Q = 5000$, $H = AA^T$ where $A$ is a randomly chosen Vandermonde matrix (different from that used in Table 1), gradient parameter $\eta = 10^{-5}$, initial value of $\kappa_i$ was $10^{-10}$, algorithm stops when relative change in $S_V$ is less than $2 \cdot 10^{-4}$. With this stopping, the average number of iterations was around 20. Note – as in Table 1 – a relatively week dependency on the split-ratio. The plot in the right panel shows a typical run of the algorithm. Note that non-monotonic weights which start out to be regularized later on become non-regularized.

OBD$^{13}$ and a validation set based vOBD deleting one weight per iteration

$^{13}$As in [18], the standard OBD is terminated when the FPE criterion [1] is minimal.
with the same covariance matrix $H$ as used in Fig. 1. In $Q = 10000$ repetitions the vOBD result is: $P_{\text{imp}} = 0.863 \pm 0.007$ and $avr(\text{RG1}) = 4.57$ for $\gamma = 0.7$. OBD delivers: $P_{\text{imp}} = 0.835 \pm 0.007$ and $avr(\text{RG1}) = 3.65$. Thus individual weight decay regularization is superior to vOBD, which again is slightly better than standard OBD.

Feed-Forward Neural Network

We tested the performance of the individual weight decay optimization using the gradient descent algorithm Eq. (4) on the Mackey-Glass chaotic time series prediction problem, see e.g., [8], [18]. The goal is to predict the series 100 steps ahead based on previous observations. The feed-forward net configuration is an input lag-space $x = [x(k), x(k-6), x(k-12), x(k-18)]$ of 4 inputs, 15 hidden hyperbolic tangent neurons, and a single linear output unit $\hat{y}(k)$ which predicts $y(k) = x(k + 100)$. We used a data set, $D$, of $N = 500$ examples and an independent test set of 8500 examples. The network was trained on $T$ using a Gauss-Newton off-line training scheme with initial $\kappa_0 = 4 \cdot 10^{-6}$. The gradient parameter $\eta$ was initialized at $10^{-3}$. If the $S_V$ drops $\eta \leftarrow 1.2 \cdot \eta$; otherwise perform a successive bisection until a drop in $S_V$ is achieved. Initial experiments showed that the algorithm is fairly insensitive to the split-ratio in a region around $\gamma = 0.5$, thus $\gamma = 0.5$ is used in the following experiments. We made an ensemble of 5 networks with different random initial weights and splits of training and validation data and ran the algorithm. Afterwards, we retrained on all data using the optimized weight decays found at minimum validation error. The performance is measured by the test error normalized with the variance of $x(k)$. For comparison we made 11 repetitions of the standard OBD approach as described in [18]. The network employed 25 hidden neurons. Fig. 2 shows the algorithm performance.

CONCLUSIONS

In this paper it was suggested to optimize the network architecture by minimizing the error on a validation set. We derived a gradient descent scheme for optimizing regularization parameters, suggested to use validation set based saliency estimates for OBD/OBS, and finally discussed the possibility of approximative combinatorial architecture search by using the mean field algorithm. Numerical examples with linear models and neural networks demonstrated the potential of the framework.

ACKNOWLEDGMENTS

This research was supported by the Danish Natural Science and Technical Research Councils through the Computational Neural Network Center. JL furthermore acknowledge the Radio Parts Foundation for financial support.

\[14\text{If } \eta \text{ reaches } 10^{-6} \text{ the update of } \kappa \text{ is done irrespective of a an increase in } S_V.\]

69
Figure 2: (a) Evolution of training, validation and test errors. (b) Evolution of input-to-hidden weight decays. (c) Evolution of hidden-to-output weight decays. (d) Test error normalized with the variance of $x(n)$ for the algorithm compared to standard OBD. $\text{avr}$, $\text{min}$, $\text{max}$ are the average, minimum and maximum performance over different runs, respectively. The effective number of parameters [9] was on the average $m_{\text{eff}} \approx 58$ for individual weight decay regularization and $m_{\text{eff}} \approx 83$ for OBD. The best normalized test error reported (see e.g., [8]) was around $2.5 \cdot 10^{-3}$.

REFERENCES


