On recurrent neural networks

Giulio Galvan

19th August 2015

Contents

Chapter 1

Artificial neural networks

1.1 A family of models

An artificial neural network is a network of connected units called neurons or perceptrons, as can be seen in figure 1.1; the link which connects neurons i and j, is associated with a weight w_{ji}. Perceptrons share the same structure for all models, what really distinguish a particular model in the family of artificial neural networks is how the perceptron units are arranged and connected together, for example whether there are cycles or not, and how data inputs are *fed* to the network.

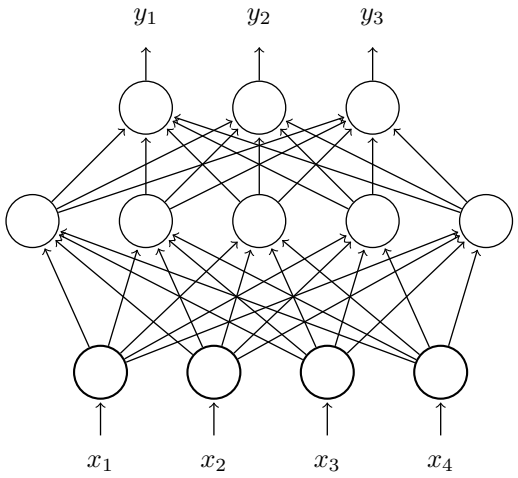

Figure 1.1: Artificial neural network example

As you can see in figure 1.2 each neuron is *fed* with a set of inputs which are the weighted outputs of other neurons and/or other external inputs. Formally

the output of a perceptron ϕ_j is defined as:

$$\phi_j \triangleq \sigma(a_j) \tag{1.1}$$

$$a_j \triangleq \sum_l w_{jl}\phi_l + b_j \tag{1.2}$$

where w_{jl} is the weight of the connection between neuron l and neuron j, $\sigma(\cdot)$ is a non linear function and $b_j \in \mathbb{R}$ is a bias term. It's worth noticing that in this formulation the input ϕ_l can be the outputs of other neurons or provided external inputs.

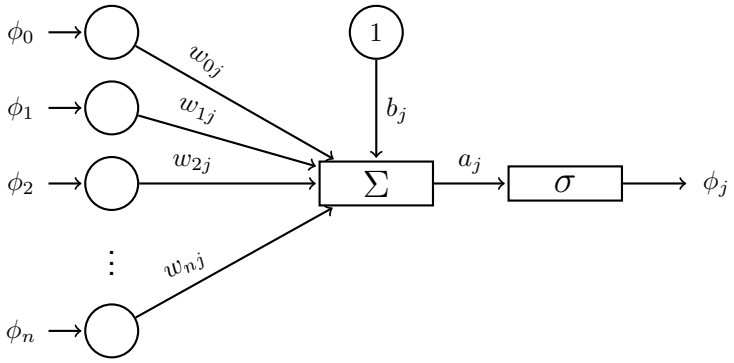

Figure 1.2: Neuron model

So, given a set of inputs $\{x\}_i$ which are *fed* to some of the units of the net which we call *input units* the output of the network $\{y\}_i$ is given by the some of units of the network, the 'upper' ones which we call *output units*. All remaining units, i.e the ones which are neither input nor output units are called *hidden units* because their value is not *observed* from the outside. The mapping from input to output is captured by equations 1.1 and 1.2.

The activation function The σ function is called *activation* function and should determine whether a perceptron unit is *active* or not. When artificial neural networks where first conceived, trying to mimic the brain structure, such function was a simple threshold function, trying to reproduce the behaviour of brain neurons: a neuron is *active*, i.e it's output ϕ_j is 1, if the sum of input stimuli $\sum_l w_{jl}\phi_l + b_j$ is greater than a given threshold τ.

$$\sigma_\tau(x) = \begin{cases} 1 & \text{if } x > \tau. \\ 0 & \text{otherwise.} \end{cases} \tag{1.3}$$

Such function, however, is problematic when we are to compute gradients because it's not continuous, so one of the following function is usually chosen:

$$sigmoid(x) = \frac{1}{1 + e^{-x}} \tag{1.4}$$

$$tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{1.5}$$

These functions behave similarly to the threshold function, but, because of their *smoothness*, present no problems in computing gradients. Another function which is becoming a very popular choice is the *rectified linear unit*:

$$ReLU(x) = \begin{cases} x & \text{if } x > 0. \\ 0 & \text{otherwise.} \end{cases} \tag{1.6}$$

ReLU activation function is rather different from previous activation functions, some of these difference, in particular with respect to gradients will be analysed in later sections.

It's worth noticing that the activation function it's the only component which make artificial neuron networks a non linear model. Were we to choose a *linear* function as activation function we will end up with a simple linear model since the outputs of the network would be ultimately composed only of sums of products.

The bias term Let's consider the old threshold function σ_τ, and ask ourselves what the bias term is for, what does changing this term bring about. Suppose neuron j has no bias term, the neuron value would be $a_j = \sum_l w_{jl}\phi_l$; if $a_j > \tau$ that neuron is active otherwise it is not. Now, let's add the bias term to a_j; we obtain that neuron j is active if $a_j > \tau - b_j$. So the effect of the bias term is to change the activation threshold of a given neuron. Using bias terms in a neural network architecture gives us the ability to change the activation threshold for each neuron; that's particularly important considering that we can learn such bias terms. We can do these same considerations in an analogous way for all the other activation functions.

Layered view of the net It's often useful to think of a neural network as series of layers, one on top of each other, as depicted in figure 1.3. The first layer is called the input layer and its units are *fed* with external inputs, the upper layers are called *hidden layers* because theirs outputs are not observed from outside except the last one which is called *output layer* because it's output is the output of the net.

When we describe a network in this way is also useful to adopt a different notation: we describe the weights of the net with a set of matrices W^k one for each layer, and neurons are no more globally indexed, instead with refer to a neuron with a relative index with respect to the layer; this allows to write easier equations in matrix notation [1]. In this notation W^k_{ij} is the weight of the link connecting neuron j of layer $k-1$ to neuron i of level k

[1] In the rest of the book we will refer to the latter notation as *layer notation* and to the previous one as *global notation*

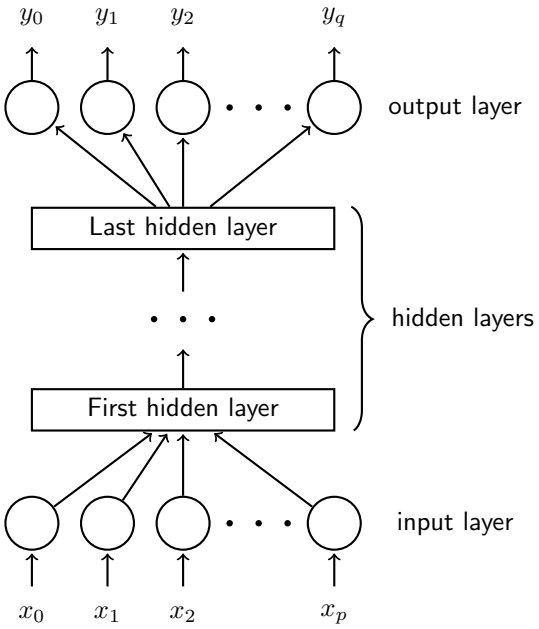

Figure 1.3: Layered structure of an artificial neural network

1.2 Feed forward neural networks

A feed forward neural network is an artificial neural network in which there are no cycles, that is to say each layer output is *fed* to the next one and connections to earlier layers are not possible.

Definition 1 (Feed forward neural network)**.** A feed forward neural network is tuple:

$$\text{FFNN} \triangleq < \boldsymbol{p}, \mathcal{W}, \mathcal{B}, \sigma(\cdot), F(\cdot) >$$

- $\boldsymbol{p} \in \mathbb{N}^U$ is the vector whose elements $p(k)$ are the number of neurons of layer k; U is the number of layers
- $\mathcal{W} \triangleq \{W^k_{p(k+1)\times p(k)}, k = 1, ..., U-1\}$ is the set of weight matrices of each layer
- $\mathcal{B} \triangleq \{\boldsymbol{b}^k \in \mathbb{R}^{p(k)}, k = 1, ..., U\}$ is the set of bias vectors
- $\sigma(\cdot) : \mathbb{R} \to \mathbb{R}$ is the activation function
- $F(\cdot) : \mathbb{R}^{p(U)} \to \mathbb{R}^{p(U)}$ is the output function

Remark 1. Given a FFNN:

- The number of output units is $p(U)$

- The number of input units is $p(1)$
- The total number of weights is $\mathcal{N}(\mathcal{W}) \triangleq \sum_{k=1}^{U} p(k+1)p(k)$
- The total number of biases is $\mathcal{N}(\mathcal{B}) \triangleq \sum_{k=1}^{U} p(k)$

Definition 2 (Output of a FFNN)**.** Given a FFNN and an input vector $\boldsymbol{x} \in \mathbb{R}^{p(1)}$ the output of the net $\boldsymbol{y} \in \mathbb{R}^{p(U)}$ is defined by the following:

$$\boldsymbol{y} = F(\boldsymbol{a}^U) \tag{1.7}$$
$$\boldsymbol{\phi}^i \triangleq \sigma(\boldsymbol{a}_i), \qquad i = 2, ..., U \tag{1.8}$$
$$\boldsymbol{a}^i \triangleq W^{i-1} \cdot \boldsymbol{\phi}^{i-1} + \boldsymbol{b}^i \qquad i = 2, ..., U \tag{1.9}$$
$$\boldsymbol{\phi}^1 \triangleq \boldsymbol{x} \tag{1.10}$$

1.2.1 Learning with FFNNs

A widespread application of neural networks is that of machine learning. In the following we will model an optimisation problem which rely on FFNNs. To model an optimisation problem we first need to define a data-set D as

$$D \triangleq \{\overline{\boldsymbol{x}}^{(i)} \in \mathbb{R}^p, \overline{\boldsymbol{y}}^{(i)} \in \mathbb{R}^q, i = 1, ..., N\} \tag{1.11}$$

Then we need a loss function $L_D : \mathbb{R}^{\mathcal{N}(\mathcal{W})+\mathcal{N}(\mathcal{B})} \to \mathbb{R}_{\geq 0}$ over D defined as

$$L_D(\mathcal{W}, \mathcal{B}) \triangleq \frac{1}{N} \sum_{i=1}^{N} L(\overline{\boldsymbol{x}}^{(i)}, \boldsymbol{y}^{(i)}) \tag{1.12}$$

$L(\boldsymbol{x}, \boldsymbol{y}) : \mathbb{R}^{p(U)} \to \mathbb{R}$ is an arbitrary loss function computed on the i^{th} example. Note that $\boldsymbol{y}$ is the output of the networks, so it depends on $(\mathcal{W}, \mathcal{B})$

The problem is then to find a FFNN which minimise L_D. As we have seen feed forward neural networks allow for large customisation: the only variables in the optimisation problem are the weights and the biases, the other parameters are said *hyper-parameters* and are determined *a priori*. Usually the output function is chosen depending on the output, for instance for multi-way classification is generally used the *softmax* function, for regression a simple identity function. For what concerns the number of layers and the number of units per layers they are chosen relying on experience or performing some kind of hyper-parameter tuning, which usually consists on training nets with some different configurations of such parameters and choosing the 'best one'.

Once we have selected the values for all hyper-parameters the optimisation problem becomes:

$$\min_{\mathcal{W}, \mathcal{B}} L_D(\mathcal{W}, \mathcal{B}) \tag{1.13}$$

1.2.2 Gradient

Consider a FFNN $=< \boldsymbol{p}, \mathcal{W}, \mathcal{B}, \sigma(\cdot), F(\cdot) >$, let $L : \mathbb{R}^{p(U)} \to \mathbb{R}$ a loss function and $g(\cdot) : \mathbb{R}^{\mathcal{N}(\mathcal{W})+\mathcal{N}(\mathcal{B})} \to \mathbb{R}$ be the function defined by

$$g(\mathcal{W}, \mathcal{B}) \triangleq L(F(a^U(\overline{\boldsymbol{x}}^{(i)}(\mathcal{W}, \mathcal{B}))), \overline{\boldsymbol{y}}^{(i)}) \tag{1.14}$$

Equation 1.14, tough it seems rather scary, express a very simple thing: we consider a single input example $\overline{\boldsymbol{x}}^{(i)}$, we run it through the network and we confront it's output $F(a^U(\overline{\boldsymbol{x}}^{(i)})$ with it's label $\overline{\boldsymbol{y}}^{(i)}$ using the loss function L; the function $g(\mathcal{W}, \mathcal{B})$ it's simply the loss function computed on the i^{th} example which of course depends only on the weights and biases of network since the examples are constant.

$$\frac{\partial g}{\partial W^i} = \nabla L \cdot J(F) \cdot \frac{\partial \boldsymbol{a}^U}{\partial W^i} \tag{1.15}$$

$$= \frac{\partial g}{\partial \boldsymbol{a}^U} \cdot \frac{\partial \boldsymbol{a}^U}{\partial W^i} \tag{1.16}$$

We can easily compute $\frac{\partial g}{\partial \boldsymbol{a}^U}$ once we define $F(\cdot)$ and $L(\cdot)$, note that the weights are not involved in such computation. Let's derive an expression for $\frac{\partial \boldsymbol{a}^U}{\partial W^i}$. We will start deriving such derivative using global notation. Let's consider a single output unit u and a weight w_{lj} linking neuron j to neuron l.

$$\frac{\partial a_u}{\partial w_{lj}} = \frac{\partial a_u}{\partial a_l} \cdot \frac{\partial a_l}{\partial w_{lj}} \tag{1.17}$$

$$= \delta_{ul} \cdot \phi_j \tag{1.18}$$

where we put

$$\delta_{ul} \triangleq \frac{\partial a_u}{\partial a_l}$$

.

Let $P(l)$ be the set of parents of neuron l, formally:

$$P(l) = \{k : \exists \text{ a link between } l \text{ and } k \text{ with weight } w_{lk}\} \tag{1.19}$$

We can compute δ_{ul} simply applying the chain rule, if we write it down in bottom-up style, as can be seen in figure 1.4, we obtain:

$$\delta_{ul} = \sum_{k \in P(l)} \delta_{uk} \cdot \sigma'(a_k) \cdot w_k l \tag{1.20}$$

The derivatives with respect to biases are compute in the same way:

$$\frac{\partial a_u}{\partial b_l} = \frac{\partial a_u}{\partial a_l} \cdot \frac{\partial a_l}{\partial b_l} \tag{1.21}$$

$$= \delta_{ul} \cdot 1 \tag{1.22}$$

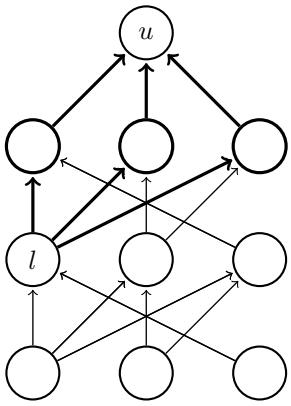

Figure 1.4: Nodes and edges involved in $\frac{\partial a_u}{\partial a_l}$

In layered notation we can rewrite the previous equations as:

$$\frac{\partial a^U}{\partial W^i} = \frac{\partial a^U}{\partial a^{i+1}} \cdot \frac{\partial^+ a^{i+1}}{\partial W^i} \tag{1.23}$$

$$\frac{\partial^+ a^{i+1}}{\partial W^i_j} = \begin{bmatrix} \phi^i_j & 0 & \cdots & \cdots & 0 \\ 0 & \phi^i_j & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & \phi^i_j \end{bmatrix} \tag{1.24}$$

$$\frac{\partial a^U}{\partial a^i} \triangleq \Delta^i = \begin{cases} \Delta^{i+1} \cdot diag(\sigma'(\boldsymbol{a}^{i+1})) \cdot W^i & \text{if } i < U \\ Id & \text{if } i == U \\ 0 & \text{otherwise.} \end{cases} \tag{1.25}$$

where

$$diag(\sigma'(\boldsymbol{a}^i)) = \begin{bmatrix} \sigma'(a^i_1) & 0 & \cdots & \cdots & 0 \\ 0 & \sigma'(a^i_2) & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & \sigma'(a^i_{p(i)}) \end{bmatrix} \tag{1.26}$$

$$\frac{\partial a^U}{\partial b^i} = \frac{\partial a^U}{\partial a^i} \cdot \frac{\partial a^i}{\partial b^i} \tag{1.27}$$

$$= \Delta^i \cdot Id \tag{1.28}$$

Backpropagation Previous equations are the core of the famous *backpropagation* algorithm which was first introduced by Rumelhart et al. [12]. The algorithm consists in two *passes*, a *forward pass* and a *backward pass* which give

the name to the algorithm. The *forward pass* start from the first layer, compute the hidden units values and the proceed to upper layers using the value of the hidden units $\boldsymbol{a^i}$ of previous layers which have already been computed. The *backward pass* instead, start from the upmost layer and computes Δ^i which can be computed, as we can see from equation 1.25 , once it's known Δ^{i+1}, which has been computed in the previous step, and $\boldsymbol{a^i}$ which has been computed in the *forward pass*.

Backpropagation algorithm has time complexity $\mathcal{O}(\mathcal{N}(\mathcal{W}))$.

1.3 Recurrent neural networks

Recurrent neural networks differ from feed forward neural networks because of the presence of recurrent connections: at least one perceptron output at a given layer i is *fed* to another perceptron at a level $j < i$, as can be seen in figure 1.5. This is a key difference, as we will see in later sections, because it introduces *memory* in the network changing, somehow, the expressiveness of the model.

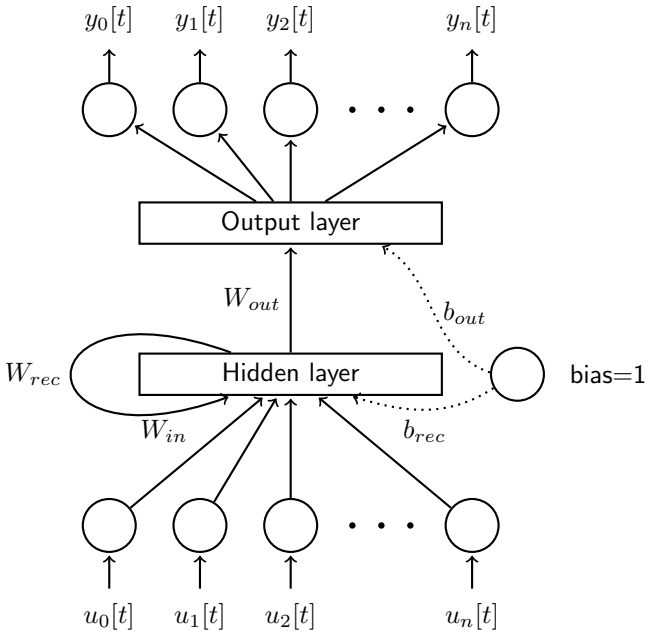

Figure 1.5: RNN model

This difference in topology reflects also on the network's input and output domain, where, in feed froward neural networks, inputs and outputs were real valued vectors, recursive neural networks deal with sequences of vectors; in other words, now, time is also considered. One may argue that, taking time (and sequences) into consideration, is some sort of limitation, because it restricts our

model to deal only with temporal inputs; that's not true, in fact we can apply RNNs to non temporal data by considering space as the temporal dimension, or we can feed the network with the same input for all time steps, or just providing no input at all after the first time step.

Definition 3 (Recurrent neural network)**.** A recurrent neural network is tuple

$$\text{RNN} \triangleq < \mathcal{W}, \mathcal{B}, \sigma(\cdot), F(\cdot) >$$

- $\mathcal{W} \triangleq \{W^{in}, W^{rec}, W^{out}\}$ where
  - W^{in} is the $r \times p$ input weight matrix
  - W^{rec} is the $r \times r$ recurrent weight matrix
  - W^{out} is the $o \times r$ output weight matrix
- $\mathcal{B} \triangleq \{\boldsymbol{b^{rec}}, \boldsymbol{b^{out}}\}$ where
  - $\boldsymbol{b}^{rec} \in \mathbb{R}^r$ is the bias vector for the recurrent layer
  - $\boldsymbol{b}^{out} \in \mathbb{R}^o$ is the bias vector for the output layer
- $\sigma(\cdot) : \mathbb{R} \to \mathbb{R}$ is the activation function
- $F(\cdot) : \mathbb{R}^o \to \mathbb{R}^o$ is the output function

Remark 2. Given a RNN

- The total number of weights si given by $\mathcal{N}(W) \triangleq rp + r^2 + ro$
- The number of biases by $\mathcal{N}(b) \triangleq r + o$
- p is the size of input vectors,
- r is the number of hidden units
- o is the size of output vectors.

Definition 4 (Output of a RNN)**.** Given a RNN and an input sequences $\{\boldsymbol{x}\}_{t=1,\dots,T}, \boldsymbol{x}_t \in \mathbb{R}^p$ the output sequence $\{\boldsymbol{y}\}_{t=1,\dots,T}, \boldsymbol{y}_t \in \mathbb{R}^o$ of the net is defined by the following:

$$\boldsymbol{y}_t \triangleq F(W^{out} \cdot \boldsymbol{a}_t + \boldsymbol{b}^{out}) \tag{1.29}$$

$$\boldsymbol{a}_t \triangleq W^{rec} \cdot \boldsymbol{\phi}_{t-1} + W^{in} \cdot \boldsymbol{x}_t + \boldsymbol{b}^{rec} \tag{1.30}$$

$$\boldsymbol{\phi}_t \triangleq \sigma(\boldsymbol{a}^t) \tag{1.31}$$

$$\boldsymbol{\phi}_0 \triangleq \overrightarrow{0} \tag{1.32}$$

As we can understand from definition 4, there is only one recurrent layer, whose weights are the same for each time step, so one could asks where does the deepness of the network come from. The answer lies in the temporal unfolding of the network, in fact if we unfold the network step by step we obtain a structure

similar to that of a feed forward neural network. As we can observe in figure 1.6, the unfolding of the network through time consist of putting identical version of the same recurrent layer one on top of each other and linking the inputs of one layer to the next one. The key difference from feed forward neural networks is, as we have already observed, that the weights in each layer are identical; another important unlikeness is of course the presence of additional timed inputs for each unfolded layer.

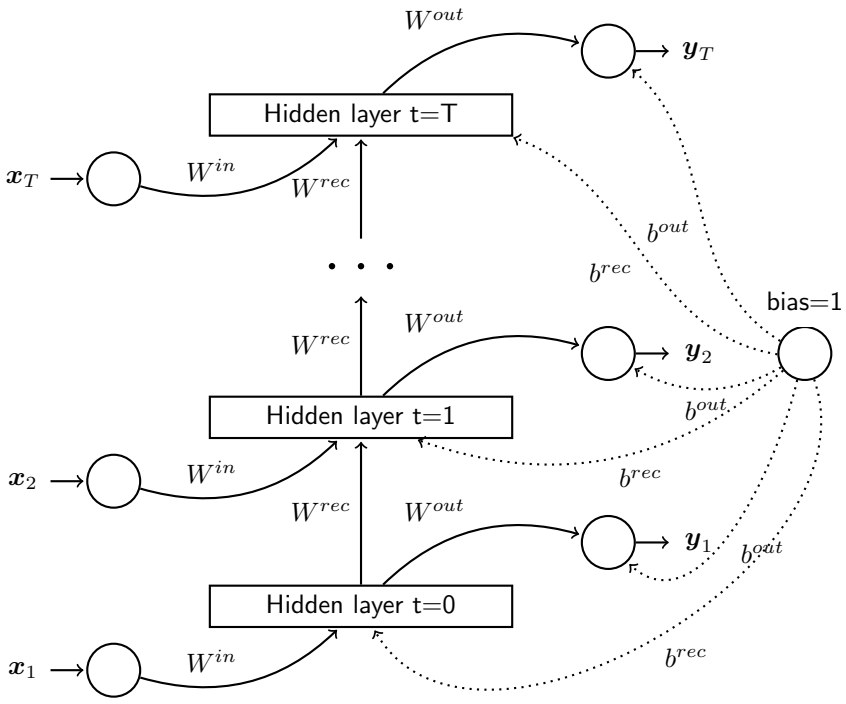

Figure 1.6: Unfolding of a RNN

1.3.1 Learning with RNNs

We can model an optimisation problem in the same way we did for feed forward neural networks, the main difference is, again, that we now deal with temporal sequences so we need a slightly different loss function. Given a data-set D:

$$D \triangleq \{\{\overline{\boldsymbol{x}}\}_{t=1,...,T}, \overline{\boldsymbol{x}}_t \in \mathbb{R}^p, \{\overline{\boldsymbol{y}}\}_{t=1,...,T}, \overline{\boldsymbol{y}}_t \in \mathbb{R}^o; i = 1, ..., N\} \tag{1.33}$$

we define a loss function $L_D : \mathbb{R}^{\mathcal{N}(W)+\mathcal{N}(b)} \to \mathbb{R}_{\geq 0}$ over D as

$$L_D(\mathcal{W}, \mathcal{B}) \triangleq \frac{1}{N} \sum_{i=1}^{N} \sum_{t=1}^{T} L_t(\overline{\boldsymbol{x}}_t^{(i)}, \boldsymbol{y}_t^{(i)}) \tag{1.34}$$

L_t is an arbitrary loss function at time step t.

The definition takes into account the output for each temporal step, depending on the task at hand, it could be relevant or not to consider intermediate outputs; that's not a limitation, in fact we could define a loss which is computed only on the last output vector, at time T, and adds 0 for each other time step.

1.3.2 Gradient

Consider a RNN $=< \mathcal{W}, \mathcal{B}, \sigma(\cdot), F(\cdot) >$. Let $L : \mathbb{R}^o \to \mathbb{R}$ a loss function:

$$L(\mathcal{W}, \mathcal{B}) \triangleq \frac{1}{N} \sum_{i=1}^{N} \sum_{t=1}^{T} L_t(\overline{\boldsymbol{x}}_t^{(i)}, \boldsymbol{y}_t^{(i)})$$

Let $g_t(\cdot) : \mathbb{R}^{\mathcal{N}(\mathcal{W})+\mathcal{N}(\mathcal{B})} \to \mathbb{R}$ be the function defined by

$$g_t(\mathcal{W}, \mathcal{B}) \triangleq L(F(\boldsymbol{y}^t(\mathcal{W}, \mathcal{B})))$$

and

$$g(\mathcal{W}, \mathcal{B}) \triangleq \sum_{t=1}^{T} g_t(\mathcal{W}, \mathcal{B})$$

$$\frac{\partial g}{\partial W^{rec}} = \sum_{t=1}^{T} \nabla L_t \cdot J(F) \cdot \frac{\partial \boldsymbol{y}^t}{\partial \boldsymbol{a}^t} \cdot \frac{\partial \boldsymbol{a}^t}{\partial W^{rec}} \tag{1.35}$$

$$= \sum_{t=1}^{T} \frac{\partial g_t}{\partial \boldsymbol{a}^t} \cdot \frac{\partial \boldsymbol{a}^t}{\partial W^{rec}} \tag{1.36}$$

As we noticed for FNNs it's easy to compute $\frac{\partial g_t}{\partial \boldsymbol{a}^t}$ once we define $F(\cdot)$ and $L(\cdot)$, note that the weights are not involved in such computation. Let's see how to compute $\frac{\partial \boldsymbol{a}^t}{\partial W^{rec}}$.

Let's consider a single output unit u, and a weight w_{lj}, we have

$$\frac{\partial a_u^t}{\partial w_{lj}} = \sum_{k=1}^{t} \frac{\partial a_u^t}{\partial a_l^k} \cdot \frac{\partial a_l^k}{\partial w_{lj}} \tag{1.37}$$

$$= \sum_{k=1}^{t} \delta_{lu}^{tk} \cdot \phi_j^{t-1} \tag{1.38}$$

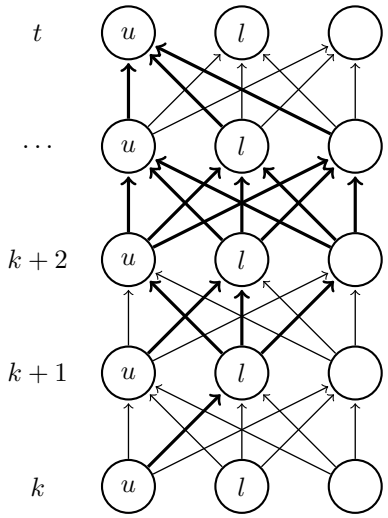

Figure 1.7: Nodes involved in $\frac{\partial a_u^t}{\partial a_l^k}$

where

$$\delta_{lu}^{tk} \triangleq \frac{\partial a_u^t}{\partial a_l^k} \tag{1.39}$$

Let's observe a first difference from ffnn case: since the weights are shared in each unfolded layer, in equation 1.37 we have to sum over time.

Let $P(l)$ be the set of parents of neuron l, defined as the set of parents in the unfolded network.

$$\delta_{lu}^{tk} = \sum_{h \in P(l)} \delta_{hu}^{tk} \cdot \sigma'(a_h^{t-1}) \cdot w_{hl} \tag{1.40}$$

In figure 1.7 we can see the arcs wich are involved in the derivatives in the unfolded network.

In matrix notation we have:

$$\frac{\partial \boldsymbol{a}^t}{\partial W^{rec}} = \sum_{k=1}^{t} \frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k} \cdot \frac{\partial^+ \boldsymbol{a}^k}{\partial W^{rec}} \tag{1.41}$$

$$\frac{\partial^+ a^k}{\partial W_j^{rec}} = \begin{bmatrix} \phi_j^k & 0 & \cdots & \cdots & 0 \\ 0 & \phi_j^k & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & \phi_j^k \end{bmatrix} \tag{1.42}$$

$$\triangleq \Delta^{tk} \tag{1.43}$$

$$\Delta^{tk} = \Delta^{t(k+1)} \cdot diag(\sigma'(\boldsymbol{a}^k)) \cdot W^{rec} \tag{1.44}$$

$$= \prod_{i=t-1}^{k} diag(\sigma'(\boldsymbol{a}^i)) \cdot W^{rec} \tag{1.45}$$

The derivatives with respect to W^{in} and $\boldsymbol{b}^{rec}$ have the same structure. The derivatives with respect to W^{out}, b^{out} are straightfoward:

$$\frac{\partial \boldsymbol{g}}{\partial W^{out}} = \sum_{t=1}^{T} \frac{\partial g_t}{\partial \boldsymbol{y}^t} \cdot J(F) \cdot \frac{\partial \boldsymbol{y}^t}{\partial W^{out}} \tag{1.46}$$

$$\frac{\partial \boldsymbol{g}}{\partial \boldsymbol{b}^{out}} = \sum_{t=1}^{T} \frac{\partial g_t}{\partial \boldsymbol{y}^t} \cdot J(F) \cdot \frac{\partial \boldsymbol{y}^t}{\partial \boldsymbol{b}^{out}} \tag{1.47}$$

Backpropagation through time (BPTT) *Backpropagation through time* is an extension of the *backpropagation* algorithm we described for FNNs, we can think of BPTT simply as a standard BP in the unfolded network. The same considerations done for BP also apply for BPTT, the difference is of course in how derivatives are computed, equation 1.45. Time complexity is easily derived noticing that in the unfolded network there are $n \cdot T$ units, where n is the number of units of the RNN .This yields time complexity $\mathcal{O}(\mathcal{N}(\mathcal{W}) \cdot T)$. Please see [16] for more details.

1.4 Activation functions and gradient

Activation functions play a central role in the artificial neural networks model, they are responsible for the non linearity of the model. In the history of neural networks several activation functions have been proposed and used, in the following some of them are taken into consideration underling the difference between them, with a special focus on their derivative expression. A special class of activation function, is that of *squashing* functions.

Definition 5. A function $f(\cdot) : \mathbb{R} \to [a, b]$ with $a, b \in \mathbb{R}$ is said to be a *squashing* function if it is not decreasing and

$$\lim_{x \to +\infty} f(x) = b \tag{1.48}$$

$$\lim_{x \to -\infty} f(x) = a \tag{1.49}$$

Step function, ramp function and all sigmoidal functions are all examples of squashing functions.

Remark 3. An important property of a *squashing* function $\sigma(\cdot)$ is that

$$\lim_{\alpha \to +\infty} \sigma(\alpha \cdot (x - \tau)) = \begin{cases} b \cdot \sigma_\tau(x) & \text{if } x > \tau \\ a + \sigma_\tau(x) & \text{otherwise} \end{cases} \tag{1.50}$$

being σ_τ the usual step function. This property is extensively used in several proofs of the universal approximator property of neural networks. Roughly speaking we can say that *squashing* functions act as step functions at the limit; please note that this property has a practical use since inputs of activation functions are the weighted sum of some neurons output, so activation function inputs can be arbitrarily big or small.

Sigmoid

$$sigmoid(x) = \frac{1}{1 + e^{-x}} \tag{1.51}$$

$$sigmoid'(x) = sigmoid(x) \cdot (1 - sigmoid(x)) \tag{1.52}$$

As we can see from figure 1.8, the sigmoid derivative has only one maximum in 0 where it assume value 0.25. Receding from 0, in both direction leads to regions where the the derivative take zero value, such regions are called *saturation* regions. If we happen to be in such regions, for a given neuron, we cannot learn anything since that neuron doesn't contribute to the gradient.

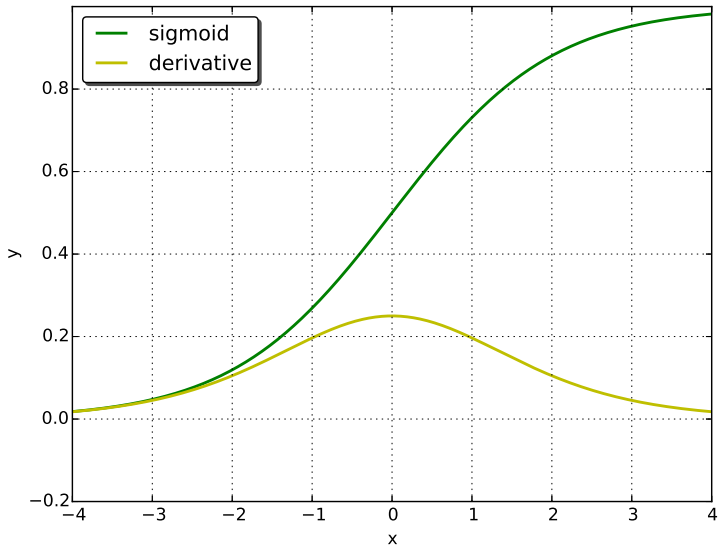

Figure 1.8: sigmoid and its derivative

Tanh

$$tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{1.53}$$

$$tanh'(x) = 1 - tanh^2(x) \tag{1.54}$$

As we can see from figure 1.9 tanh (and it's derivative) have a behavior similar to the sigmoid one; Again we have two saturation region towards infinity: that's typical of all squashing functions.

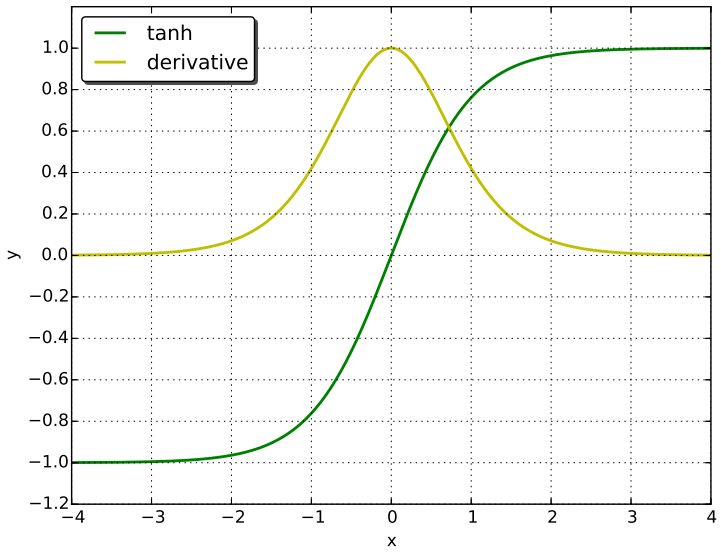

Figure 1.9: tanh and its derivative

ReLU

$$ReLU(x) = \begin{cases} x & \text{if } x > 0. \\ 0 & \text{otherwise.} \end{cases} \tag{1.55}$$

$$ReLU'(x) = \begin{cases} 1 & \text{if } x > 0. \\ 0 & \text{otherwise.} \end{cases} \tag{1.56}$$

ReLU is a bit different from other activation function seen so far: the main difference is that's it's not a squashing function. As we can see from figure 1.10, ReLU's derivative is the step function; it has only one *saturation* region $(-\infty, 0]$ and a region in which is always takes value 1, $(0, +\infty]$ This leads to the fact that we cannot learn to *turn on* a switched off neuron ($x < 0$), but we have no

saturation region toward infinity. The constancy of the derivative in the *active* region is a distinctive property of ReLU which plays an important role in the *vanishing gradient* problem too, as it's explained in the relative section.

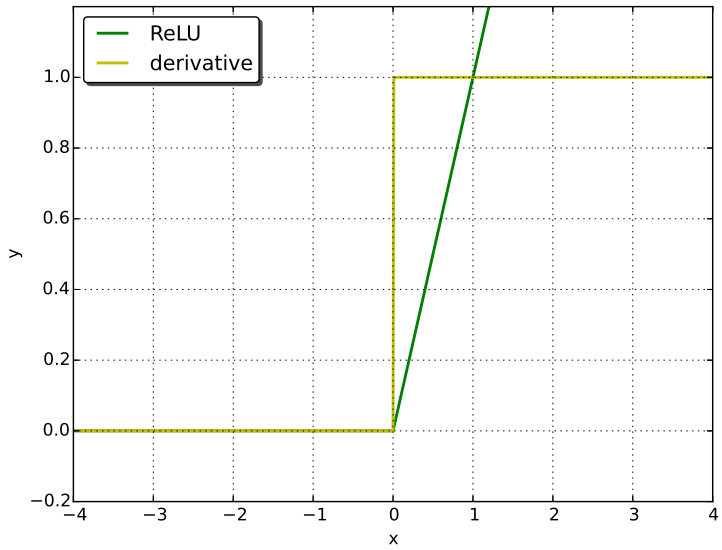

Figure 1.10: ReLU and its derivative

1.5 Stochastic gradient descent: a common framework

In this section we will describe a framework based on gradient descent optimization method which can be used to train neural network of any kind. Such framework constitutes the core of many learning methods used in today's applications. Suppose we have a training set of pairs $D = \{\langle \boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)} \rangle\}$ and a loss function $L(\theta)$ where θ represents all the parameters of the network.

A standard gradient descend would update θ at each iteration using the gradient computed on the whole training set, as shown below.

$$\theta = \theta - \alpha \nabla_\theta L(\theta) \tag{1.57}$$

This can be very slow or even impractical if the training set is too huge to fit in memory. Stochastic gradient descent (SGD) overcome this problem taking into account only a part of the training set for each iteration, i.e the gradient is computed only on a subset I of training examples.

$$\theta = \theta - \alpha \nabla_\theta L(\theta; \langle \boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)} \rangle, i \in I) \tag{1.58}$$

The subset of training examples used for the update is called *minibatch*. The number of examples for each minibatch is an important hyper-parameter because it affects both the speed of convergence in terms of number of iteration and the time needed for each iteration. At each iteration new exampled are chosen among the training set examples, so it could, and it always does in real applications, happen that all training set exampled have been used. This is not a problem, since we can use the same examples over and over again. Each time we go over the entire training set we say we completed and *epoch*. It's not unusual to iterate the learning algorithm for several epochs before converging.

The method is summarized in algorithm 1.

Algorithm 1: Stochastic gradient descent

Data:
$D = \{\langle \boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)} \rangle\}$: training set
θ_0: initial solution
m: size of each minibatch

Result:
θ: solution

```
θ ← θ_0
while stop criterion do
    I ← select m training example ∈ D
    α ← compute learning rate
    θ ← θ − α∇_θ L(θ; ⟨x^(i), y^(i)⟩, i ∈ I)
end
```

In the following paragraphs we will analyze in more detail each step of the method, surveying the different alternatives that can be used.

The stop criterion Usually a gradient based method adopts a stop criterion which allows the procedure to stop when close enough to a (local) minimum, i.e $\nabla_\theta L(\theta) = 0$. This could easily lead to over-fitting, so is common practice to use a cross-validation technique. The most simple approach to cross-validation is to split the training set in two parts, one actually used as a pool of training examples, which will be called training set, and the other, called *validation* set, used to decide when to stop.

Being $D = \{\langle \boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)} \rangle, i \in (1, M)\}$ a generic subset of the dataset, we can define the *error* on such set in a straightforward manner as

$$E_D = \frac{1}{M} \sum_{i=1}^{M} L(\boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)}) \tag{1.59}$$

Since training examples are sampled from the training set, the error on the training set will always[2] be decreasing across iterations. The idea behind cross-

[2]This is not actually true; it would in a standard gradient descent, but since we are using

validation is to compute, and *monitor* the error on the validation set, since it's not guaranteed at all that the error would be decreasing. On the contrary, tough error will generally decrease during the first part of training, it will reach a point when it will become to increase. This is the point when we need to stop training since we are starting to over-fitting. Of course this is an ideal situation, in real applications the validation error could have a more irregular trend, but the idea holds.

DISEGNO CON LE DUE CURVE

Learning rate The parameter α in equation 1.58, know as *step* in the optimization field, is called in AI *learning rate*. Of course the strategy employed to compute such learning rate is an important ingredient in the learning method. The most easy, and often preferred, strategy is that of **constant learning rate**; Learning rate α becomes another hyper-parameter of the network that can be tuned, but it remains equal, usually a very small value, across all iterations.

Another popular strategy is that of **momentum** which, in the optimization field is know as the *Heavy Ball* method. The main idea behind momentum is to accelerate progress along dimensions in which gradient consistently point in the same direction and to slow progress along dimensions where the sign of the gradient continues to change. This is done by keeping track of past parameter updates with an exponential decay as shown in equation 1.61

$$v = \gamma v + \alpha \nabla_\theta L(\theta; \langle \boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)} \rangle, i \in I) \tag{1.60}$$

$$\theta = \theta - v \tag{1.61}$$

Another way of choosing the learning rate is to fix an initial value and **annealing** it, at each iteration (or epoch), according to a policy, for instance *exponential* or *linear* decay; the idea behind it being that, initially, when far from a minimum having a larger learning rate causes greater speed and after some iterations when approaching a minimum a smaller learning rate allows a finer refinement.

Adaptive methods instead choose the learning rate monitoring the objective function, hence learning rate can be reduced or increased depending on the need, being a little more versatile than annealing methods. Of course different strategies for detection when to reduce or increase the learning rate have been devised.

Finally **line search** can be used; usually line search is used when working with (non stochastic) gradient descend or when dealing with large batches; for stochastic gradient with small batches other strategies are usually preferred.

Regularization TODO

stochastic gradient the error could be non monotonic decreasing; however the matter here is that error mainly follow a decreasing path

How to choose batches Empirical evidence has been provided that choosing a "meaningful" order in which examples are presented to the network can both speed the convergence and yield better solutions. Generally speaking, the network can learn faster if trained first with easier examples and then with examples with gradually increasing difficulty, as humans or animals would do. The idea was introduced by Bengio et al. [1] in 2009, as *curriculum* learning. Experiments on different curriculum strategies can be found in [17].

1.6 The vanishing and exploding gradient problem

The training of recurrent neural networks is afflicted by the so called *exploding* and *vanishing* gradient problem. Such problem is directly linked to the notion of memory. When we talk about memory what are we really talking about is the dependency of neurons output at a given time t from previous time steps, that is how ϕ^t depends on ϕ^k with $t > k$. This dependency is captured by the expression $\frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k}$. Obviously when such expression equals zero it means neuron output at time t is not affected by output at time k. The terms $\frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k}$ are usually referred as *long term* contribution when $k << t$ or *short term* contributions otherwise. We talk of *exploding* gradient problem when *long term* components grow exponentially, on the contrary of *short term* ones, causing the overall norm of the gradient to explode. We refer to *vanishing* gradient problem when, vice versa, *long term* components diminish exponentially.

Vanishing gradient means long term components approach zero value, this in turn leads to the fact that the output of the net won't depend on inputs of distant temporal steps, i.e the output sequence is determined only by recent temporal input: we say that the network doesn't have memory. Evidently this can have catastrophic effects on the classification error. Imagine we would like to classify an input sequence as positive whether or not it contains a given character. It would seem a rather easy task, however, if the neural network we are training suffers from the *vanishing* gradient issue, it could perform the classification using only the most recent temporal inputs. What if the character was at the beginning of the sequence? Of course the prediction would be wrong.

Exploding gradient seems to be a different kind of a problem, it does not affect the ability of the network to use information from distant temporal step, on the contrary we have very strong information about where to go using the gradient direction. One could argue that some components, namely, the long term ones, have gradient norm exponentially bigger than short term ones. I fail to see why this could be a problem: the output of the first time steps influences all successive steps, so changing the output of a long term neuron do imply big changes in the output of more distant in time neurons. The only situation in which *exploding* gradient can be a problem is when using learning algorithms like gradient

descent with constant step: if we are to compute a step in the gradient direction with a fixed step and gradient has too big norm we may make a too big step.

Let's now return to the nature of the problem and try to explaining the mechanics of it. We have seen in the previous section that

$$\frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k} = \prod_{i=t-1}^{k} diag(\sigma'(\boldsymbol{a}^i)) \cdot W^{rec} \tag{1.62}$$

Intuitively we can understand why such problems arises, more evidently in *long term* components, just by looking at equation 1.69. We can notice each temporal contribution is the product of $l = t - k - 1$ jacobian matrix, so in *long term* components l is large and depending on the values of the matrices in the product we can go exponentially fast towards 0 or infinity.

Hochreiter Analysis: Weak upper bound In this paragraph we report some useful consideration made by Hochreiter, please see [7] for more details.

Let's put:

$$\|A\|_{max} \triangleq \max_{i,j} |a_{ij}|$$

$$\sigma'_{max} \triangleq \max_{i=k,\dots,t-1} \{\left\|diag(\sigma'(a^i))\right\|_{max}\}$$

Since

$$\|A \cdot B\|_{max} <= r \cdot \|A\| \cdot \|B\|_{max} \qquad \forall A, B \in \mathbb{R}_{r \times r} \tag{1.63}$$

it holds:

$$\left\| \frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k} \right\|_{max} = \left\| \prod_{i=t-1}^{k} diag(\sigma'(\boldsymbol{a}^i)) \cdot W^{rec} \right\|_{max} \tag{1.64}$$

$$\leq \prod_{i=t-1}^{k} r \cdot \left\|diag(\sigma'(\boldsymbol{a}^i))\right\|_{max} \cdot \|W^{rec}\|_{max} \tag{1.65}$$

$$\leq \left(r \cdot \sigma'_{max} \cdot \|W^{rec}\|_{max}\right)^{t-k-1} \tag{1.66}$$

$$= \tau^{t-k-1} \tag{1.67}$$

where

$$\tau \triangleq r \cdot \sigma'_{max} \cdot \|W^{rec}\|_{max}$$

So we have exponential decay if $\tau < 1$. We can match this condition if $\|W^{rec}\|_{max} \leq \frac{1}{r \cdot \sigma'_{max}}$. As pointed out by Hochreiter in his work we can match this condition, in the case of sigmoid activation function by choosing $\|W^{rec}\|_{max} < \frac{1}{0.25 \cdot r}$.

Let's note that we would actually reach this upper bound for some i, j only if all the path cost have the same sign and the activation function takes always maximal value.

An upper bound with singular values Lets decompose W^{rec} using the singular value decomposition. We can write

$$W^{rec} = S \cdot D \cdot V^T \tag{1.68}$$

where S, V^T are squared orthogonal matrices and $D \triangleq diag(\mu_1, \mu_2, ..., \mu_r)$ is the diagonal matrix containing the singular values of W^{rec}. Rewriting equation 1.69 using this decomposition leads to

$$\frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k} = \prod_{i=t-1}^{k} diag(\sigma'(\boldsymbol{a}^i)) \cdot S \cdot D \cdot V^T \tag{1.69}$$

Recalling that for any orthogonal matrix U it holds

$$\|U\boldsymbol{x}\|_2 = \|\boldsymbol{x}\|_2$$

and using

$$\|diag(\lambda_1, \lambda_2, ..., \lambda_r) \cdot \boldsymbol{x}\|_2 \leq \lambda_{max} \|\boldsymbol{x}\|_2$$

we get

$$\left\| \frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k} \cdot \boldsymbol{e}_i \right\|_2 = \left\| \left(\prod_{i=t-1}^{k} diag(\sigma'(\boldsymbol{a}^i)) \cdot S \cdot D \cdot V^T \right) \cdot \boldsymbol{e}_i \right\|_2 \tag{1.70}$$

$$\leq (\sigma'_{max} \cdot \mu_{max})^{t-k-1} \tag{1.71}$$

The previous equation provide us a sufficient condition, $\sigma'_{max} \cdot \mu_{max} < 1$, as in Hochreiter's analysis, for exponential decay of long term components. In this case however the bound depends on the singular value of the recurrent weights rather than on the maximal weight of the matrix itself.

Explaining the problem using the network's graph Let's now dig a bit deeper and rewrite equation 1.69 with respect to a couple of neurons i and j.

$$\frac{\partial \boldsymbol{a}_i^t}{\partial \boldsymbol{a}_j^k} = \sum_{q \in P(j)} \sum_{l \in P(q)} \cdots \sum_{h:i \in P(h)} w_{qj} \dots w_{jh} \cdot \sigma'(a_j^k)\sigma'(a_q^{k+1}) \dots \sigma'(a_i^{t-1}) \tag{1.72}$$

Observing the previous equation we can argue that each derivatives it's the sum of p^{t-k-1} terms; each term represents the path cost from neuron i to neuron j in the unfolded network, obviously there are p^{t-k-1} such paths. If we bind the cost $\sigma'(a_l^t)$ to neuron l in the t^{th} layer in the unfolded network we can read the path cost simply surfing the unfolded network multiply the weight of each arc we walk through and the cost of each neuron we cross, as we can see from figure 1.11.

We can further characterize each path cost noticing that we can separate two components, one that depends only on the weights $w_{qj} \dots w_{jh}$ and the other that depends both on the weights and the inputs $\sigma'(a_j^k)\sigma'(a_q^k) \dots \sigma'(a_i^{t-1})$.

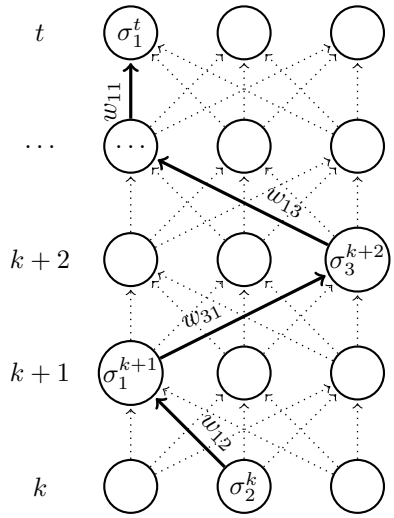

Figure 1.11: The cost for a path from neuron 2 at time k to neuron 1 at time t is $w_{12}w_{31}w_{13}\dots w_{11}\cdot\sigma_2^k\sigma_1^{k+1}\sigma_3^{k+2}\dots\sigma_1^{t-1}$

The ReLU case ReLU case is a bit special, because of it's derivative. ReLU's derivative is a step function, it can assume only two values: 1 when the neuron is active, 0 otherwise. Returning to the path graph we introduced earlier we can say that a path is *enabled* if each neuron in that path is active. In fact if we encounter a path which cross a non active neuron it's path cost will be 0; on the contrary for an *enabled* path the cost will be simply the product of weight of the arcs we went through, as we can see in figure 1.12

So $|(\frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k})_{ij}|$ ranges from 0, when no path is enabled to, $|((W^{rec})^{t-k-1})_{ij}|$ when all paths are enabled and all path cost have the same sign, which is consistent with what we found in Hochreiter analysis. We can argue then that ReLU has an advantage over sigmoidal activation functions, for instance, because gradient depends only on the W^rec matrix: ReLU function *only* enables or disables the paths but doesn't change their costs as sigmoids do

Poor solutions Let's pretend we have found, with some learning technique, an assignment for all the weights which causes the gradient to have zero norm. We could be happy with it and claim to have 'solved' the problem. However, by chance, we discover that $\frac{\partial \boldsymbol{a}^T}{\partial \boldsymbol{a}^k}$ has zero norm for all time steps $k < \tau$. So, the output of the network doesn't depend on the inputs of the sequence for those time steps. In other words we have found a possibly optimal solution for the truncated sequence $x_{[\tau:T]}$. The solution we have found is an optimal candidate to be a bad local minimum.

As a final observation on this matter it's worth noticing how a bad initialization of W^{rec} can lead to poor solutions or extremely large convergence time just because such initialization imply $\frac{\partial \boldsymbol{a}^t}{\partial \boldsymbol{a}^k}$ approaching zero norm for $t >> k$.

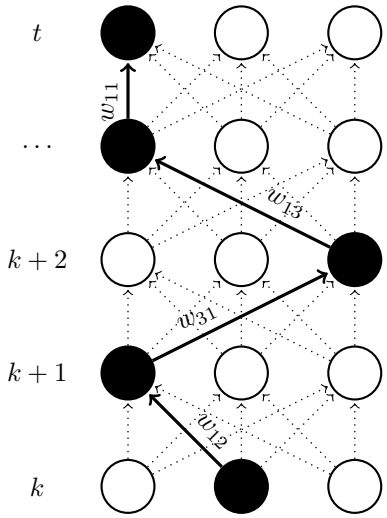

Figure 1.12: The cost for an enabled path from neuron 2 at time k to neuron 1 at time t is $w_{12}w_{31}w_{13}\dots w_{11}$

Moreover, even if we somehow provide an initialization matrix which is unaffected by this curse, it's certainly possible that we reach such a bad matrix during learning phase. Several techniques have been proposed to overcome this problem, they will be the topic of later chapters.

1.7 On expressiveness

In this section we will investigate the expressive power of neural networks, presenting some results that motivate the use of neural networks as learning models and underline the differences between the two paradigm of FNNs and RNNs.

One of the first import results regarding the expressive power of neural networks it's due to Hornik et al. [8] which basically states *"Multilayered feed foward networks with at least one hidden layer, using an arbitrary squashing function, can approximate virtually any function of interest to any desired degree of accuracy provided sufficiently many hidden units are available"*.

To give a more formal result we need first to define what *approximate to any degree of accuracy means*, this concept is captured in definition 6

Definition 6. A subset S of $\mathbb{C}^n$ (continuoos functions in $\mathbb{R}^n$) is said to be *uniformly dense on compacta in* $\mathbb{C}^n$ if $\forall$ compact set $K \subset \mathbb{R}^n$ holds: $\forall \epsilon > 0$, $\forall g(\cdot) \in \mathbb{C}^n \ \exists f(\cdot) \in S$ such that $\sup_{x \in K} \|f(x) - g(x)\| < \epsilon$

Hornik result is contained in theorem 1.

Theorem 1. For every squashing function σ, $\forall n \in \mathbb{N}$, feed forward neural networks with one hidden layer are a class of functions which is *uniformly dense on compacta in* $\mathbb{C}^n$.

Theorem 1 extends also to Borel measurable functions, please see [8] for more details.

A survey of other approaches, some of which constructive, which achieve similar results can be found in [13] At the moment I don't know of any results concerning ReLU activation function.

This results implies that FNN are *universal approximators*, this is a strong argument for using such models in machine learning. It's important to notice, however, that the theorem holds if we have *sufficiently many* units. In practice the number of units will bounded by the machine capabilities and by computational time, of course greater the number of units greater will be the learning time. This will limit the expressiveness of the network to a subset of all measurable functions.

Let's now turn our attention to RNNs and see how the architectural changes, namely the addition of backward links, affect the expressive power of the model. It suffice to say that RNNs are as powerfull as turing machine. Siegelman and Sontag [15] proved the existence of a finite neural network, with sigmoid activation function, which simulates a universal Turing machine. Hyötyniemi [9] proved, equivalently, that turing machine are recurrent neural network showing how to build a network, using instead ReLU activation function, that performs step by step all the instruction of a computer program. Hyötyniemi work is particularly interesting because it shows how to construct a network that simulate an algorithm written a simple language equivalent to a turing machine. For each instruction type (increment,decrement,conditional branch,...) a particular setting of weights and neuron is devised allowing the net so simulate step by step the behaviour of the program. In the program equivalent network there are a unit for each program variable and one or two, depending on the instruction type, units for each program instruction. This is very interesting from an expressiveness point of view since it bounds the number of units we ought to use with the length of the algorithm we are trying to reproduce.

For better understanding the implications of this fact, imagine how many complex function you can express with short algorithms, for example fractals (approximations). It's worth underling the difference with feed forward neural networks where a large number of units seems to be required. This seems to suggest that FFNNs and RNNs differ mainly in a manner of representation, where FNNs use space to define a somehow explicit mapping from input to output, RNNs use time to implicitly define an algorithm responsible for such mapping.

This seems extremely good news, since we could simulate turing machines, hence all algorithms we can think of, using a recurrent neural network with a relatively small number of units; recall that for FFNN we had to suppose infinitely many units to obtain the universal approximator property. Of course

there is a pitfall: we can simulate any turing machine but we have to allow sufficiently many time steps and choose a termination criterion. This is of course impractical, and we don't use RNNs in this way. Usually the number of time steps is choose to be equal to the input sequence length. This of course restrict the class of algorithm we can learn with RNNs. A particular class of algorithms suited to be learned by such models is that of algorithms consisting in one loop, inside which some invariants are enforced. The output, step by step, depends on the loop invariants.

Chapter 2

Literature review

Hochreiter [7] in 1991, Bengio et al. [2] in 1994, and others, observed that gradient in deep neural networks tends to either vanish or explode. From then onward several methods have been proposed to overcome what is now know as the *exploding/vanishing gradient* problem. We can roughly partition such methods in two broad categories. The approaches of the first kind, the ones we will call *architectural driven*, usually use a simple stochastic gradient descend (SGD) as learning algorithm, and act on the network topology, modifying the way the neural units operates, the connections between them or the relationship between layers; the idea of such methods is to build networks architectures in which gradient are less likely to vanish, or in other words whose units are able to store information for several time steps.

The second approach, which we'll call *learning driven*, instead, focus on the learning algorithm, leaving the network architecture untouched. Methods belonging to these categories, either employ learning algorithms different from SGD, or they propose modification to the SGD framework.

In the rest of the chapter we will review the most relevant approaches for both the categories.

2.1 Architectural driven methods

2.1.1 Long short-term memory

Long short-term memory (LSTM) were proposed (1997) by Hochreiter and Schmidhuber [7] as a novel network structure to address the vanishing gradient problem, which was first studied by Hochreiter (1991) in his diploma thesis, a milestone of deep learning.

The idea behind this structure is to enforce a constant error flow, that is to say, to have constant gradient norm, thus preventing the gradient to vanish. This is done by introducing special types of neurons called *memory cells* and *gate units*. As we can see by looking at figure 2.1, a memory cell is essentially a

neuron with a self connection with unitary weight, whose input and output are managed by two multiplicative neurons: the gate units.

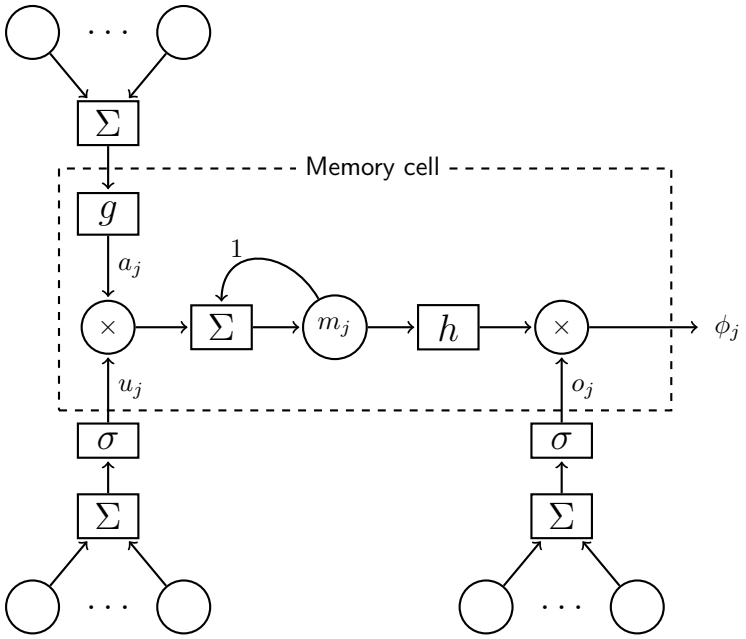

Figure 2.1: Memory cell and gate units of LSTM network

The memory cell and the gate units behave accordingly to the following:

$$u_j^t = \sigma[W_u \cdot \boldsymbol{x_t} + U_u \cdot \boldsymbol{\phi}_{t-1}]_j \tag{2.1}$$

$$o_j^t = \sigma[W_o \cdot \boldsymbol{x_t} + U_o \cdot \boldsymbol{\phi}_{t-1}]_j \tag{2.2}$$

$$a_j^t \triangleq g[W \cdot \boldsymbol{x_t} + U \cdot \phi_i^t]_j \tag{2.3}$$

$$m_j^t \triangleq a_j \cdot u_j^t + (1 \cdot m_j^{t-1}) \tag{2.4}$$

$$\phi_j \triangleq h(m_j^t) \cdot o_j^t \tag{2.5}$$

As we can see from equation 2.4, the value of the memory cell $m(t)$ remains constant as long as the input gate u doesn't "open" causing a "write" operation. Similarly the output o of the memory cell, which is connected with the other neurons of the network, is controlled by an output gate: the memory will have a non zero output only if the output gate opens, which we could call a a "read" operation. As for constant error flow it is ensured because the memory cell has only a self-loop with unitary weight.

Memory cells, guarded by gate units can be employed in networks with different topology alongside traditionally input, output and hidden units. Another way to look at this kind of architecture is to think of memory cells as units able to store one bit of information, even for long periods of time, hence able to learn distant time correlations between inputs.

As we have seen these network units are specifically designed to store information, through the use of gates; these gates however are no different from other units, apart from the fact they are multiplicative units, hence without further precautions, the networks would incur in the same vanishing problem it aimed to resolve. In fact LSTM comes with a proper learning algorithm: essentially errors arriving at memory cells inputs are not propagated back in time, only the error within the memory cell gets propagated; in other words gradients are truncated taking into account only the self-connection of the memory cells and not it's other input connections, hence providing constant error flow.

LSTM units have proven to be very successful in various tasks and even at present times (2015), they continue to be employed. In recent implementations however, alongside small modifications, as the introduction of other gates, LSTM architecture is often used without the original learning algorithm which is often replaced by a standard stochastic gradient descend as done in [6].

2.1.2 Gated recurrent units

Gated recurrent units (GRU) were introduced by Cho et al. in 2014 [3] as units similar to LTSM with same purpose but claimed to simpler to compute and implement. A GRU unit j make use of two gate units, z, the *update* gate, and r, the *reset* gate, which are standard neurons.

$$z_j^t = [\sigma(W_z \boldsymbol{x_t} + U_z \boldsymbol{\phi}_{t-1})]_j \tag{2.6}$$

$$r_j^t = [\sigma(W_r \boldsymbol{x_t} + U_r \boldsymbol{\phi}_{t-1})]_j \tag{2.7}$$

As in LSTM units, the gates are used to managed the access to memory cell, but in GRU they are used a little bit differently. The update gate is used to decide how to update the memory cell: the activation value of the cell ϕ_j^t is a linear interpolation between the previous activation ϕ_j^{t-1} and the candidate activation $\tilde{\phi}_j^t$.

$$\phi_j^t \triangleq (1 - z_j^t)\phi_j^{t-1} + z_j^t \tilde{\phi_j^t} \tag{2.8}$$

$$\tilde{\phi}_j^t = [\sigma(W \boldsymbol{x_t} + U(\boldsymbol{r}_t \odot \boldsymbol{\phi}_{t-1})]_j \tag{2.9}$$

As we can see from equation 2.9, when the reset gate r_j^t is close to zero, the units acts as if reading the first symbol of the input sequence *forgetting* the previous state.

LSTM and GRU present very similarities, the most relevant one being the additive mechanism of update which helps the networks to store information

during several time step. One difference between the two architectures is, instead, the lacking of an output gate in GRU, which hence expose the content of the memory cell without any supervision. In [4] Cho et al. compare the two architectures showing how a gated architecture improves the performance of a network composed of traditional units; The comparison results obtained were however mixed, and in the end they could not demonstrate the superiority of one of the two approaches.

IMMAGINE???

2.1.3 Gated feedback recurrent neural networks

Gated feedback recurrent neural networks were proposed in 2015 by Chung et al. [5] as a novel recurrent network architecture. Unlike LSTM or GRU were the novelty of the proposal was a new kind of unit, designed to better capture long-term dependencies between inputs, the novelty of this approach is the way the units are arranged. For starters multiple recurrent layer are used, like in a *Stacked RNN*, i.e the network is composed of several layers, each one of which is connected to all the others; in other words the layers are fully connected. Moreover unlike traditional stacked RNNs, the feedback connection between different layers is gated by a *global reset gate* which is essentially a logistic unit computed on the current inputs and the previous states of hidden layers. This global reset gates is reminiscent of the gates of LSTM and GRU but it controls the connection between layers not between units: the hidden state values of layer i at time $t-1$ are fed to a lower layer j multiplied by $g^{i\to j}$. The gate between layers i and j is computed as:

$$g^{i\to j} \triangleq \sigma(\boldsymbol{w}_g^{i\to j} \cdot \boldsymbol{h_t}^{j-1} + \boldsymbol{u}_g^{i\to j} \cdot \boldsymbol{h}_{t-1}^{*}) \tag{2.10}$$

where $\boldsymbol{w}_g^{i\to j}$ and $\boldsymbol{u}_g^{i\to j}$ are the weights of the links between the gate and the input and the hidden states of all layers at time-step $t-1$ respectively; for $j=1$, $\boldsymbol{h}_t^{j-1} = \boldsymbol{x}_t$ and $\boldsymbol{h}_{\boldsymbol{t-1}}^{\boldsymbol{*}}$ represents all the hidden states at time $t-1$.

The idea behind this architecture is to encourage each recurrent layer to work at different timescales, hence capturing both long-term and short-term dependencies. In addition, the units composing the layers, can be traditional sigmoidal units but also LSTM or GRU, hence benefiting from both the strength of these kind of units and the global gated mechanism. In [5], the architecture is evaluated against traditional and stacked RNNs with both LSTM and GRU units; gated feedback networks are shown to offer better performance and accuracy in several challenging tasks.

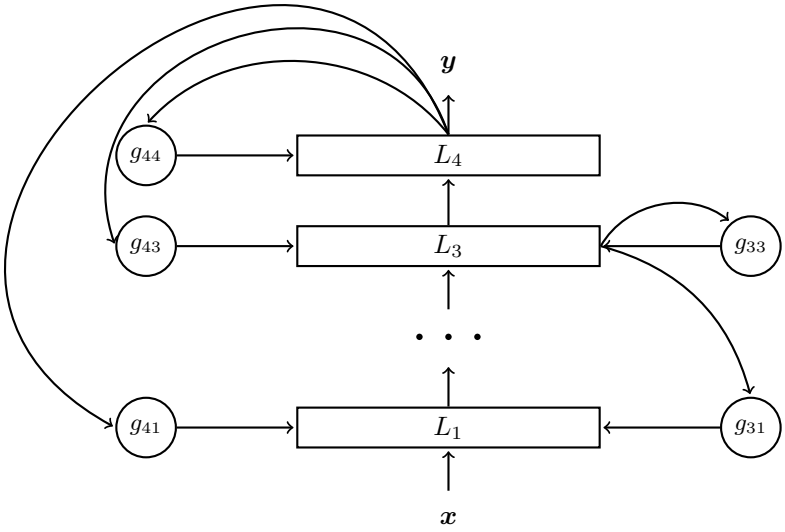

Figure 2.2: Gated feedback architecture; only connections between layers trough gates are shown

2.2 Learning driven methods

2.2.1 Preserve norm by regularization and gradient clipping

In 2013 Pascanu [11] proposed a regularization term Ω for the loss function $L(\theta)$ which should address the vanishing gradient problem. The objective function hence become:

$$\tilde{L}(\theta) \triangleq L(\theta) + \lambda\Omega(\theta) \tag{2.11}$$

Such term represents a preference for solutions such that back-propagated gradients preserves norm in time.

$$\Omega = \sum_t \left(\frac{\left\| \frac{\partial L}{\partial \boldsymbol{h}_{t+1}} \cdot \frac{\partial \boldsymbol{h}_{t+1}}{\partial \boldsymbol{h}_t} \right\|}{\left\| \frac{\partial L}{\partial \boldsymbol{h}_{t+1}} \right\|} - 1 \right)^2 \tag{2.12}$$

As we can see from equation 2.12 the regularization term forces $\frac{\partial \boldsymbol{h}_{t+1}}{\partial \boldsymbol{h}_t}$ to preserve norm in the relevant direction of the error $\frac{\partial L}{\partial \boldsymbol{h}_{t+1}}$.

The intuition behind this technique is that $\frac{\partial \boldsymbol{h}_t}{\partial \boldsymbol{h}_k}$ measure the dependence of outputs at time t on the previous time steps $t-1, ...k$. In [11] is argued that even though some precedent inputs $k < t$ will be irrelevant for the prediction of time time t, the network cannot learn to ignore them unless there is an error signal; hence it's a good idea to force the network to increase $\frac{\partial \boldsymbol{h}_t}{\partial \boldsymbol{h}_k}$, even at the expense of greater error of the loss function $L(\theta)$, and then wait for it to learn to ignore these inputs.

As for the exploding vanishing gradient, in [11] is argued that a simple method called *gradient clipping* can be effective against exploding gradient. The method, shown in algorithm 2, simply consists in rescale the gradient norm when it goes over a threshold.

Algorithm 2: Gradient clipping

$\boldsymbol{g} \leftarrow \nabla_\theta L$
if $\|\boldsymbol{g}\| \geq threshold$ **then**
    $\boldsymbol{g} \leftarrow \frac{threshold}{\|\boldsymbol{g}\|}\boldsymbol{g}$
end

A drawback of such an approach is the introduction of another hyper-parameter, the threshold, however in [11] is said that a good heuristic is to choose a value from half to ten time the average gradient norm over a sufficiently large number of updates.

2.2.2 Hessian-free optimization

During 2010-2011 Martens and Sutskever [10] proposed an developed an hessian-free method for recurrent neural network training. The proposal consists in

using hessian-free optimization with some crucial modifications which make the approach suitable for recurrent neural networks.

As in the classical Newton's method the idea is to iteratively compute the updates to parameter θ by minimizing a local quadratic approximation $M_k(\delta)$ of the objective function $f(\theta_k+\delta)$, which in the case of RNNs is the loss function $L(\theta)$, as shown in equation 2.13.

$$M_k(\delta) = f(\delta_k) + \nabla f(\delta_k)^T \delta + \frac{1}{2}\delta^T B_k \delta \tag{2.13}$$

where B_k is the curvature matrix, which in the standard Newton matrix would the hessian $\nabla^2 f(x_k)$. The update of the parameter δ is given by:

$$\theta_{k+1} = \alpha_k \delta_k^* \tag{2.14}$$

where δ_k^* is the minimum $M_k(\delta)$ and $\alpha_k \in [0,1]$ is chosen typically via line-search.

The use of the hessian is however impractical for several reason: first of all if not positive definite $M(\delta_k)$ will not be bounded below; moreover even if positive definite, computing $\delta_k^* = \delta_k - B_{k-1}^{-1}\nabla f(\delta_{k-1})$, as in standard Newton, can be too much computationally expensive.

Gauss-Newton curvature matrix The proposal of [10] for indefiniteness is to use the generalized Gauss-Newton matrix (GGN) proposed by Schraudolph [14] as an approximation of the hessian. As for the computational cost of the matrix inversion it is addressed, as in Truncated-Newton methods, by partially minimizing the quadratic function $M_k(\delta)$ using the conjugate gradient algorithm.

Let decompose the objective function $f(\theta)$ in $L(F(\theta))$ using the usual loss function $L(\cdot)$ and the output vectorial valued function of the network $F(\theta)$. Is required that $L(\cdot)$ is convex. The GNN can be derived as follows:

$$\nabla f(\theta) = J^T \nabla L \tag{2.15}$$

$$\nabla^2 f(\theta) = J^T \nabla^2 L + \sum_{i=1}^{m} [\nabla L]_i \cdot [\nabla^2 F_i] \tag{2.16}$$

The GNN is defined as:

$$GNN \triangleq J^T \nabla^2 L \tag{2.17}$$

GNN is convex, provided $L(\cdot)$ is, and it easy to see that GNN is the hessian of $f(\theta)$ if $F(\theta)$ is replaced by it's first order approximation.

Damping As observed in [10], Newton's method is guaranteed to converge to a local minimum only if initialized sufficiently close to it. In fact, the minimum of the quadratic approximation $M_k(\delta)$, can be far beyond the region where $M_k(\delta)$ is a "reliable" approximation of $f(\theta_k + \delta)$. For this reason applying the previously described method to highly non linear objective function, as in the

case of RNNs, can lead to very poor results. A solution to overcome this problem can be using a first order method as stochastic gradient descend, to reach a point close enough to a minimum and the switch to hessian-free optimization for finer convergence. In [10] however is argued that making use of the curvature can be beneficial in constructing the updates from the beginning.

Damping is a strategy to make use of curvature information as in Newton's like methods, in a more conservative way, so that updates lie in a region where $M_k(\delta)$ remains a reasonable approximation of $f(\theta_k + \delta)$. A classic damping strategy is Tikhonov damping; it consists in adding a regularization term to the quadratic approximation:

$$\tilde{M}_k(\delta) \triangleq M_k(\delta) + \frac{\lambda}{2} \|\delta\|^2 \tag{2.18}$$

Of course λ is a very critical parameter, too small values of λ lead to regions where the quadratic doesn't not closely approximate the objective function, conversely, too big values lead to updates similar to that we would have obtained with a first order method. Another important observation is that λ cannot be set once and for all at the beginning of the optimization, but has to be tuned for each iteration. One classic way to compute λ adaptively is to use the Levenberg-Marquardt like heuristic. Let the reduction ration ρ be:

$$\rho \triangleq \frac{f(\theta_k + \delta_{k-1}) - f(\theta_k)}{M_k(\delta_{k-1})} \tag{2.19}$$

The Levenberg-Marquardt heuristic is given by

$$\lambda = \begin{cases} \frac{2}{3}\lambda & \text{if } \rho > \frac{3}{4} \\ \frac{3}{2}\lambda & \text{if } \rho < \frac{1}{4} \end{cases} \tag{2.20}$$

The idea behind this strategy is that when ρ is smaller than 1 the quadratic model overestimate the amount of reduction and so λ should be increased, conversely when ρ is close to 1 the quadratic approximation is accurate and hence we can afford a smaller value of λ.

However in [10] is argued that Tikhonov damping can perform very poorly when applied to RNNs, the reason being that $\|\cdot\|$ is not a reasonable way to measure change in θ; as pointed out in [10] $\|\cdot\|$ works well when the parameters θ "operate"[1] at roughly the same scale and that's not certainly the case of RNNs, which by the way, is also the motives that urged Martens to try second order methods and it's linked to the vanishing gradient problem.

To overcame this problem, in [10], a novel damping scheme, called *structural damping*, is proposed. Structural damping consists, as in Tikhonov, in a regularization term which penalizes the directions of change in the parameter space which lead to large changes in the hidden state sequence, which corresponds to highly inaccurate quadratic approximations.

$$\tilde{M}_k(\delta) \triangleq M_k(\delta) + \frac{\lambda}{2} \|\delta\|^2 + \mu D(h(\theta_{k+1}, \theta_k)) \tag{2.21}$$

[1] changing two different weights by the same amount in an RNN can produce very little to none changes in the output function or, conversely, the changes can be substantial

where $D(\cdot, \cdot)$ is a distance (or loss) function which measure the variation in the hidden states due to the update of θ.

Since minimization of $\tilde{M}_k(\delta)$ is done by conjugate gradient and such function is not not quadratic, in practice, a Taylor series approximation, along with the use of the Gauss-Newton matrix, is used in place of $D(h(\theta_{k+1}, \theta_k))$.

Minibatching As last note regarding the proposed method it's important to notice that the method can work in a stochastic fashion, i.e using a small subset (minibatch) of the training examples, like stochatsic gradient descend (SGD), for istance. This is a very important feature since dataset are getting bigger and bigger, hence computing gradients on the whole training set is becoming computationally impractical. However, unlike SGD, where minibatch can be arbitrary small, the proposed method, and all second order method in general, deteriorate it's performance with too small batches, but that's seems to but not much of a problem.

RIMANE FUORI: stopping criterion of CG, line searching

Appendix A

Notation

Let $F : \mathbb{R}^N \to \mathbb{R}^{\mathbb{M}}$ be defined by

$$F(\boldsymbol{x}) = (f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \cdots, f_M(\boldsymbol{x}))) \text{ for some } f_i : \mathbb{R}^N \to \mathbb{R} \tag{A.1}$$

Definition 7 (Derivative with respect to a vector)**.** We define the derivative of $F(x(\boldsymbol{w}))$ with respect to a vector $\boldsymbol{w}$ of p elements as the $M \times p$ matrix

$$\frac{\partial F}{\partial \boldsymbol{w}} \triangleq \begin{bmatrix} \frac{\partial f_1}{\partial \boldsymbol{w}_1} & \frac{\partial f_1}{\partial \boldsymbol{w}_2} & \cdots & \cdots & \frac{\partial f_1}{\partial \boldsymbol{w}_p} \\ \frac{\partial f_2}{\partial \boldsymbol{w}_1} & \frac{\partial f_2}{\partial \boldsymbol{w}_2} & \cdots & \cdots & \frac{\partial f_2}{\partial \boldsymbol{w}_p} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\partial f_M}{\partial \boldsymbol{w}_1} & \frac{\partial f_M}{\partial \boldsymbol{w}_2} & \cdots & \cdots & \frac{\partial f_M}{\partial \boldsymbol{w}_p} \end{bmatrix} \tag{A.2}$$

Definition 8 (Derivative with respect to a matrix)**.** We define the derivative of $F(x(W))$ with respect to a matrix W, being W_j the j^{th} column of a $p \times m$ matrix W as the $M \times (p \cdot m)$ matrix:

$$\frac{\partial F}{\partial W} \triangleq \left[\begin{array}{c|c|c|c} \frac{\partial F}{W_1} & \frac{\partial F}{W_2} & \cdots & \frac{\partial F}{W_m} \end{array} \right] \tag{A.3}$$

Bibliography

[1] Yoshua Bengio, Jérôme Louradour, Ronan Collobert, and Jason Weston. Curriculum learning. In *Proceedings of the 26th Annual International Conference on Machine Learning*, ICML '09, pages 41–48, New York, NY, USA, 2009. ACM.

[2] Yoshua Bengio, Patrice Simard, and Paolo Frasconi. Learning long-term dependencies with gradient descent is difficult.

[3] Kyunghyun Cho, Bart van Merrienboer, Çaglar Gülçehre, Dzmitry Bahdanau, Fethi Bougares, Holger Schwenk, and Yoshua Bengio. Learning phrase representations using RNN encoder-decoder for statistical machine translation. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing, EMNLP 2014, October 25-29, 2014, Doha, Qatar, A meeting of SIGDAT, a Special Interest Group of the ACL*, pages 1724–1734, 2014.

[4] Junyoung Chung, Çaglar Gülçehre, KyungHyun Cho, and Yoshua Bengio. Empirical evaluation of gated recurrent neural networks on sequence modeling. *CoRR*, abs/1412.3555, 2014.

[5] Junyoung Chung, Çaglar Gülçehre, KyungHyun Cho, and Yoshua Bengio. Gated feedback recurrent neural networks. *CoRR*, abs/1502.02367, 2015.

[6] Alex Graves. Generating sequences with recurrent neural networks. *CoRR*, abs/1308.0850, 2013.

[7] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural Comput.*, 9(8):1735–1780, November 1997.

[8] K. Hornik, M. Stinchcombe, and H. White. Multilayer feedforward networks are universal approximators. *Neural Netw.*, 2(5):359–366, July 1989.

[9] Heikki Hyotyniemi. Turing machines are recurrent neural networks, 1996.

[10] James Martens and Ilya Sutskever. Training deep and recurrent networks with hessian-free optimization. In Grégoire Montavon, Genevieve B. Orr, and Klaus-Robert Müller, editors, *Neural Networks: Tricks of the Trade - Second Edition*, volume 7700 of *Lecture Notes in Computer Science*, pages 479–535. Springer, 2012.

[11] Razvan Pascanu, Tomas Mikolov, and Yoshua Bengio. On the difficulty of training recurrent neural networks. In *Proceedings of the 30th International Conference on Machine Learning, ICML 2013, Atlanta, GA, USA, 16-21 June 2013*, pages 1310–1318, 2013.

[12] D. E. Rumelhart, G. E. Hinton, and R. J. Williams. Parallel distributed processing: Explorations in the microstructure of cognition, vol. 1. chapter Learning Internal Representations by Error Propagation, pages 318–362. MIT Press, Cambridge, MA, USA, 1986.

[13] Franco Scarselli and Ah Chung Tsoi. Universal approximation using feedforward neural networks: A survey of some existing methods, and some new results. *Neural Netw.*, 11(1):15–37, January 1998.

[14] Nicol N. Schraudolph. Fast curvature matrix-vector products for second-order gradient descent. *Neural Computation*, 14(7):1723–1738, 2002.

[15] Hava T. Siegelmann and Eduardo D. Sontag. Turing computability with neural nets. *Applied Mathematics Letters*, 4:77–80, 1991.

[16] Ronald J. Williams and Jing Peng. An efficient gradient-based algorithm for on-line training of recurrent network trajectories. *Neural Computation*, 2:490–501, 1990.

[17] Wojciech Zaremba and Ilya Sutskever. Learning to execute. *CoRR*, abs/1410.4615, 2014.