Verification of Continuous Time Recurrent Neural Networks (Benchmark Proposal)

Patrick Musau and Taylor T. Johnson

Vanderbilt University, Nashville, Tennessee, USA

patrick.musau@vanderbilt.edu, taylor.johnson@vanderbilt.edu

Abstract

This manuscript presents a description and implementation of two benchmark problems for continuous-time recurrent neural network (RNN) verification. The first problem deals with the approximation of a vector field for a fixed point attractor located at the origin, whereas the second problem deals with the system identification of a forced damped pendulum. While the verification of neural networks is complicated and often impenetrable to the majority of verification techniques, continuous-time RNNs represent a class of networks that may be accessible to reachability methods for nonlinear ordinary differential equations (ODEs) derived originally in biology and neuroscience. Thus, an understanding of the behavior of a RNN may be gained by simulating the nonlinear equations from a diverse set of initial conditions and inputs, or considering reachability analysis from a set of initial conditions. The verification of continuous-time RNNs is a research area that has received little attention and if the research community can achieve meaningful results in this domain, then this class of neural networks may prove to be a superior approach in solving complex problems compared to other network architectures.

Category: Academic Difficulty: High

1 Context and Origins

Artificial Neural Networks have demonstrated an effective and powerful ability to achieve success in numerous contexts, such as adaptive control [43], autonomous vehicles, evolutionary robotics, pattern recognition, image classification, and nonlinear system identification and control [38] [18]. Despite this success, there have been reservations about incorporating them into safety critical systems [23] due to their susceptibility to unexpected and errant behavior from a slight perturbation in their inputs and initial conditions [42] [37]. Typically, neural networks are viewed as "black boxes" since the underlying operation of the neuron activations is often indiscernible to the creators of the network [10]. In light of these challenges, there has been significant work towards obtaining formal guarantees about the behavior of neural networks [25]. However, the majority of verification schemes have only been able to deal with neural networks that make use of piecewise-linear activation functions [7]. This is due to the great difficulty exhibited in obtaining formal guarantees for even simple properties of neural networks. In fact, neural network verification has been demonstrated to be an NP-complete problem, and while
techniques that make use of satisfiability modulo theories [35], mixed integer programming [41], robustness testing [4], and linear programming [13] [37] have been able to deal with small networks, they are incapable of dealing with the complexity and scale of the majority of networks present in real-life applications [23]. Moreover, the majority of verification approaches have dealt only with feed-forward and convolutional neural network architectures.

One class of neural networks that has received particularly little attention in the verification literature is the class of recurrent neural networks. Whereas both feed-forward networks and recurrent networks have demonstrated an ability to approximate continuous functions to any accuracy [16], recurrent neural networks have exhibited several advantages over their feed-forward counterparts [26]. By allowing for the presence of feedback connections in their architecture, recurrent neural networks are able to retain information about the past and capture a higher degree of sophisticated dynamics using fewer neurons than their feed-forward counterparts [5]. In fact, recurrent neural networks have demonstrated a higher level of success in solving problems in which there is a temporal relation between events [32] such as capturing the behavior of biological neurons [28], dynamical system identification [22], real time gesture recognition [3], robotics [6, 8, 27, 30] and speech recognition [1]. Therefore, they represent a more attractive framework than feed-forward networks in these domains [47]. However, due to the complexity exhibited by their architecture as well as the non-linear nature of their activation functions the verification approaches currently available in the research literature are incapable of being applied to these networks. Thus, there is an immediate need for methods and advanced software tools that can provide formal guarantees about their operation [23], particularly in the context of the system identification and the control of safety critical systems.

In light of this shortcoming, the following paper presents two benchmark problems for the verification of a specific class of recurrent neural networks known as continuous-time recurrent neural networks (CTRNNs). Since the dynamics of CTRNNs can be expressed solely by a set non-linear ordinary differential equations (ODEs), the verification of such systems relies on an ability to reason about the reachable set from a set of initial conditions and inputs [39]. The two CTRNN benchmark problems we present are described as follows: the first is a network without inputs employed for the approximation of a fixed point attractor described in [46], and the second deals with a CTRNN used for the identification of a damped forced pendulum as described in [12]. The problems elucidated in the paper are modeled using Simulink/Stateflow (SLSF), Matlab scripts, and are available in the SpaceEx format. We aim to provide a thorough problem description to which the numerous tools and approaches for non-linear systems present in the research community can be evaluated and compared [39]. This paper serves as a first step towards recurrent neural network verification.

2 General Mathematical Model for Continuous Time Recurrent Neural Networks

The dynamics of a continuous-time recurrent neural network with \( n \) neurons is given by the following system of ordinary differential equations:

\[
\frac{d u_i}{dt} = -\frac{u_i}{\tau_i} + \sum_{j=1}^{n} w_{ij} f(u_j(t) + \theta_i) + I_i(t) \tag{2.1}
\]

---

\(^1\)The benchmark models are available at https://github.com/verivital/CTRRN
where: $u_i(t)$ denotes the internal state of the $i$-th neuron ($i = 1 \ldots n$), $\theta_i$ denotes a bias term for the $i$-th neuron, $\tau_i$ denotes the time constant, $w_{ij}$ denotes the connection strength between the $i$-th and $j$-th neurons, $I_i(t)$ denotes the input to the $i$-th neuron, and $f(u_j(t))$ is the output of the $j$-th neuron [19]. The function $f$ is typically referred to as the activation function of a neuron, and in most cases it is typically either the logistic sigmoid function or the hyperbolic tangent function given by equations (2.2) and (2.3) respectively.

$$f(x) = \frac{1}{1 + e^{-x}}$$

(2.2)

$$f(x) = \tanh(x)$$

(2.3)

Equation (2.1) can be recast into matrix form as:

$$\dot{\mathbf{u}}(t) = -\frac{1}{\tau} \mathbf{u}(t) + \mathbf{W} f(\mathbf{u}(t) + \mathbf{\theta}) + \mathbf{I}(t)$$

(2.4)

where: $\mathbf{u}(t) = (u_1 \ldots u_n)^T$ and $\mathbf{I}(t)$ are $n$ dimensional column vectors representing the neuron states and inputs respectively, $\mathbf{W} = (w_{ij})$ is a $n \times n$ weight matrix, and $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ is an activation function mapping given by $f(\mathbf{u}(t)) = (f(u_1) \ldots f(u_n))$ [19]. Additionally while numerous feed-forward neural networks make use of the ReLU activation function, which exhibits piecewise linear behavior, it is not typically employed in recurrent neural architectures since the sigmoid and hyperbolic tangent functions often perform better [34]. A simple recurrent architecture is displayed in Figure 2.1.

![Figure 2.1: Simple Recurrent Neural Network Architecture](image)

In order to train a CTRNN to approximate the finite time trajectories of a dynamical system, the number of neurons $n$ must be greater than the dimensionality of the function that we wish to approximate [20]. Typically the weights, biases, and time constants in equation (2.4) are modified using Genetic Algorithms [33] such as back-propagation through time, real-time recurrent learning, the extended Kalman filter, phase space learning, and reservoir computing [46]. In these schemes, the network is trained by minimizing the prediction error between the network output and dynamical system output on a set of time series data collected from the dynamical system. A common learning architecture is displayed in Figure 2.2. The algorithms used in training CTRNNs are quite complex and difficult to implement, however they have largely been successful in training networks to perform various tasks. An in-depth discussion of these techniques is beyond the scope of this paper and we refer readers to the following paper for further detail [33].
3 Description of Benchmarks

In this section, we present a description of the two benchmark problems proposed for verification. The first of these problems is a CTRNN with no inputs that captures the vector field dynamics of a fixed point attractor. The approximation of attractors represents a class of problems in recurrent neural network research known as fixed point learning [46] and networks trained in this domain are typically associated with constraint satisfaction and associative memory [33]. Moreover, attractor networks have been extensively studied in neuroscience in an effort to construct artificial neuron models of human memory and perception in an intuitive sense capturing the way that humans remember names, objects, and ideas [31]. The second problem describes the use of a CTRNN in the system identification of a forced damped pendulum. An accurate identification of the plant model is a crucial part in designing robust controllers [21] and in this problem [12], once the network has successfully been trained it is used calculate a linearized state feedback for PID control.

3.1 Approximation of Fixed Point Attractor

In dynamic systems, a fixed point attractor is a point in the phase space where the trajectories of a system converge to as time evolves from a given set of initial states [44]. For our problem we consider a two-dimensional system with a fixed point located at the origin [46]. The vector field for the attractor is given by the following function

\[ F(x, y) = (a(x - p_1), b(x - p_2)) \]  \hspace{1cm} (3.1)

where \( p_1 = p_2 = 0 \), \( a = -0.2 \), and \( b = -0.3 \). To approximate the behavior of this vector field during a 40 second time period, Adam Trischler et al. used two layer CTRNN that consisted of a single hidden layer with \( m = 3 \) hidden neurons and an output layer with \( n = 2 \) output neurons [46]. The recurrent connections are contained within the hidden layer as shown by Figure 3.1. The CTRNN was trained using an algorithm proposed in [46] in which a feed-forward representation of the recurrent neural network is trained using back-propagation and then transformed back into a recurrent neural network. Thus, the differential equations specifying the dynamics of the CTRNN are the same as 2.1 with the exception of the absence of an input signal. They are given by:

\[ \dot{\vec{u}} = -\frac{1}{\tau} \vec{u} + Wf(\vec{u}) \]  \hspace{1cm} (3.2)

\[ \vec{u}(0) = (\vec{q}(0), B\vec{q}(0) + \vec{d})^T \]  \hspace{1cm} (3.3)
where: \( \vec{q}(0) \) is the initial condition for the fixed point attractor, \( B \) is a \( m \times n \) matrix representing the connections among the hidden neurons, \( \tau = 10^6 \) is the time constant for each neuron, \( \vec{\theta} \) represents the bias term for the neurons in the hidden layer, and \( f(\vec{u}) = \tanh(\vec{u}) \) is the activation function used for each neuron [46].

The weight matrix \( W_{(n+m) \times (n+m)} \) used in equation (6) is constructed using two matrices \( A \) and \( B \), where \( A \) is an \( n \times m \) matrix representing the connections from the hidden neurons to the output neurons and \( B \) is the matrix described as above. The matrices \( W, A, B, \) and bias vector \( \vec{\theta} \) trained on the vector field in equation 3.1 are given by,

\[
W = \begin{bmatrix} 0 & A \\ 0 & BA \end{bmatrix}, \quad A = \begin{bmatrix} -1.20327 & -0.07202 & -0.93635 \\ 1.18810 & -1.50015 & 0.93519 \end{bmatrix}, \quad B = \begin{bmatrix} 1.21464 & -0.07202 \\ 1.18810 & -1.50015 \\ 1.18810 & -1.50015 \end{bmatrix},
\]

\[
\vec{\theta} = (-7.56499 \times 10^{-5}, 1.34708 \times 10^{-4}, -6.24925 \times 10^{-6})^T.
\]

Since the network does not receive any inputs, its trajectory is entirely dependent on the choice of initial conditions \( \vec{q}(0) \). Simulating the network is computationally inexpensive and largely depends on the choice of numerical method used to discretize equation (3.2).

### 3.2 System Identification for Forced Damped Pendulum

The second problem we present is the approximation of a forced damped pendulum described by the second-order differential equation:

\[
ml^2 \ddot{\phi}(t) + v \dot{\phi}(t) + mgl \sin \phi(t) = I(t)
\]

where \( m = 2.0 \text{ kg} \) is the mass of the object suspended by the pendulum, \( v = 1.0 \text{ kg m}^2/\text{s} \) is the damping coefficient, \( l = 1 \text{ m} \) is the length of pendulum and \( I(t) \) is the driving signal at time \( t \) [12]. To approximate the trajectories of this system, A. Delgado et al. designed a CTRNN with a single hidden layer that consisted of five neurons whose dynamics are described by a set of equations that are an adaptation of equation (2.1). Since the pendulum is driven by a driving signal \( I(t) \), the CTRNN ODE model must include the influence inputs. However, the activation

---

\[2\]The time constant \( \tau \) determines the activation speed of a particular neuron. A description of the influence of time constants can be found in [48].
of the neurons in the network may be influenced differently by the driving input signal \[11, 29\], and to capture this reality, the authors in \[12\] incorporated a vector representing the connection weights from the scalar input to each neuron denoted by $\Gamma$. Additionally, the authors did not incorporate any biases in their CTRNN model. The dynamics of their model are described by:

$$\dot{\mathbf{u}}(t) = -\frac{1}{\tau} \mathbf{u}(t) + \mathbf{W} f(\mathbf{u}(t)) + \Gamma I(t)$$

where $\Gamma$ is an $n \times 1$ column vector denoting the input connection weights and $I(t)$ is the scalar input signal. The authors trained the network using time series data that was collected by supplying the pendulum model with random noise input data over a time period of 20 seconds. The performance of the network was optimized using a chemotaxis learning algorithm \[12\], and after training, the network parameters are given by:

$$\mathbf{W} = \begin{bmatrix} 0.4684 & -2.4994 & 0.4211 & -0.2848 & 0.1995 \\ 1.3615 & 0.0642 & 0.0413 & -1.8925 & -1.6608 \\ -0.8185 & -0.9241 & -0.0743 & -0.1264 & 0.1484 \\ -0.3257 & 1.2319 & -1.0997 & 0.2192 & -0.8547 \\ -1.2444 & 0.4396 & -0.5466 & 1.7342 & -0.5953 \end{bmatrix}$$

$$\Gamma = (-0.005, -0.2111, 0.1689, 0.0645, -0.0413)^T$$

$$\mathbf{u}(0) = (-0.0097, -0.0065, 0.0171, -0.0097, 0.0025)^T$$

4 Simulation of Models

We begin this section by discussing the results of simulating the CTRNN models presented in section 3 in order to assess their fidelity in capturing the dynamical systems that they represent. Figure 4.1 displays a 20 second simulation of the fixed point attractor system and its CTRNN representation from a set of 100 initial points bounded by $(x,y) \in [-1,1]^2$. The results of the simulation demonstrated that the CTRNN was able to faithfully capture the dynamics of equation (3.1). In fact, the maximum separation between the trajectories of the neural network $\mathbf{y}_{nn}(t) \in \mathbb{R}^2$, and the fixed point attractor $\mathbf{y}_{fpa}(t) \in \mathbb{R}^2$, on any of the 100 paths that we considered was $||\mathbf{y}_{nn}(t) - \mathbf{y}_{fpa}(t)||_2 = 9.57 \times 10^{-3}$, as shown by Figure 4.3. Moreover, as the trajectories of the CTRNN model approached the fixed point, the output of all the neurons converged to zero causing the evolution of the network to halt. This indicates stability within the region that we considered.

In a similar fashion, the CTRNN model of the forced damped pendulum displayed a high level of model fidelity in representing a chaotic system \[17\]. The results of several simulations using a series of sinusoidal input functions given by:

$$u(t) = c_1(\frac{\pi}{2}) \sin(\frac{2\pi t}{5}) + c_2(\frac{\pi}{2}) \sin(\frac{2\pi t}{5})$$

is displayed in Figure 4.2. The maximum separation at any moment between the trajectories of the network model and the pendulum system was $|y_{nn}(t) - y_{fp}(t)| = 2.16 \times 10^{-3}$, as shown in Figure 4.3. Thus, although both models are low dimensional neural networks, they are good representations of the dynamical systems that they seek to identify.
5 Observations

This is a novel research direction. To the best of the authors’ knowledge there are currently no verification approaches that deal with recurrent neural networks despite their success in numerous contexts. The development of successful verification approaches will have a monumental impact in the field of artificial intelligence, and in particular, in the design of neural network control systems. Thus, the deliberate consideration of this problem by the research community is considerably important.

Choice of CTRNN Architecture. There have been numerous proposed architectures for recurrent neural networks, with varying levels of depth in terms of hidden layers, trained to perform a myriad of tasks. While these networks have largely been successful, they are significantly more difficult to train and gradient-descent based optimization methods suffer from the
vanishing and exploding gradient problem [36]. In response to this problem, researchers have proposed the Long-Short Term Network (LSTM), the Gated Recurrent Unit (GRU), Memory Networks, and other similar variants that have been broadly successful in mitigating the optimization challenges faced by other architectures. Unfortunately, these architectures suffer from high model complexity. In fact, LSTM architectures possess four times the number of trainable parameters than classic recurrent neural network architectures with the same number of hidden layers [36]. Thus in order to keep the size of the network models small, we chose to focus only on CTRNNs.

**Scalability**: The number of variables in equation (2.1) increases linearly with the number of neurons present in the network. However, the number of connections among the neurons increases quadratically and may lead to very large weight matrices. A typical real-world neural network can contain hundreds to millions of neurons [24], thus an effective verification approach will need to scale well with the dimensionality of large networks. Additionally, it should be noted that changing the size of any neural network necessitates retraining the network parameters. However in this work we do not focus on the learning process. **Challenges**: Verifying continuous non-linear systems is a particularly difficult problem. In particular, the performance of verification tools is dependent on the stiffness of the ODEs [40]. In our experiments we attempted to generate reachtubes for the CTRNN models using Flow$^*$ [9] and C2e2 [14], however both tools were not able to deal with the complexity exhibited by our models. This further serves to demonstrate the need for novel reachability tools for CTRNNs.
6 Outlook and Model Extensions

In this manuscript, we have presented a description and implementation of two challenging continuous-time recurrent neural network benchmark problems. The interest in these problems is that they serve as a first step in considering the verification of recurrent neural networks. The verification of CTRNNs has not been studied extensively and in this domain, the verification problem is reduced to an ability to reason about the reachable set of the non-linear differential equations that specify their behavior. However, understanding the nature of these dynamics is not an easy problem [45]. Still, if the research community can demonstrate an ability to formally verify this class of neural networks, they can be used in numerous application domains beyond system identification and fixed-point learning as discussed in this paper. Furthermore, CTRNNs have an impressive ability to capture temporal information [1] and can be used to achieve remarkable results in problem domains currently dominated by other network architectures. The problems posed in this paper are easily scalable to a given level of complexity by increasing the number of neurons used in implementing the CTRNNs.

There are several interesting possibilities for the extension of the proposed benchmarks and future work, including:

- Analyzing the dynamics of a system in which a CTRNN is used in conjunction with a controller as described in [21] and [2]
- Studying the effects of using various neuron activation functions on the dynamics of CTRNNs,
- Considering the effects of different neural network training regimes on the reachable set
- Investigating the possibility of linearizing a specific subset of CTRNN models
- Considering multilayer CTRNNs as well as other recurrent neural network architectures.
- and evaluating the possible transformation of other neural network architectures into CTRNNs

References

Verification of Continuous Time Recurrent Neural Networks (Benchmark Proposal) Musau and Johnson


Verification of Continuous Time Recurrent Neural Networks (Benchmark Proposal) Musau and Johnson


