Partially-Connected Differentiable Architecture Search for Deepfake and Spoofing Detection

Wanying Ge, Michele Panariello, Jose Patino, Massimiliano Todisco and Nicholas Evans

EURECOM, Sophia Antipolis, France
firstname.lastname@eurecom.fr

Abstract

This paper reports the first successful application of a differentiable architecture search (DARTS) approach to the deepfake and spoofing detection problems. An example of neural architecture search, DARTS operates upon a continuous, differentiable search space which enables both the architecture and parameters to be optimised via gradient descent. Solutions based on partially-connected DARTS use random channel masking in the search space to reduce GPU time and automatically learn and optimise complex neural architectures composed of convolutional and residual blocks. Despite being learned quickly with little human effort, the resulting networks are competitive with the best performing systems reported in the literature. Some are also far less complex, containing 85% fewer parameters than a ResNet2Net competitor.

Index Terms: neural architecture search, differentiable architecture search, deepfakes, anti-spoofing, automatic speaker verification

1. Introduction

Compared to automatic speaker verification for which the research history is decades long, research in deepfake or spoofing detection is relatively embryonic. While recent years have seen rapid progress, front-end feature extraction as well as back-end classification approaches are still evolving [1]. Early work is characterised by a focus on front-end feature engineering, namely the design of parameters or representations which capture the tell-tale signs of manipulated or synthesized speech signals and which help to distinguish these from bona fide speech [2,3]. More recently, greater attention has been paid to the back-end classifier design. Like all fields of speech processing, deep neural network architectures are the classifier of choice [4,5].

The use of end-to-end (E2E) processing, whereby hand-crafted and manually optimised components are replaced with automatically designed and optimised substitutes, has attracted growing attention. Thus far, E2E developments extend mostly to the front-end components [6,7]. While back-end components can be similarly optimised, this usually extends only to the network parameters; the network architecture itself is almost always still hand-crafted. Inspired by original work in [8,9], our first attempt to harness the potential of fully E2E processing [10] explored the use of neuro-evolution for augmenting topologies (NEAT). While NEAT is successful in learning network architectures automatically, performance was found to be far from the state of the art, while computational complexity was found to be prohibitive. Whereas more efficient NEAT implementations are reported in the literature [11,12], we have instead turned to powerful and efficient alternatives with proven potential in speech-related tasks.

We have explored the use of neural architecture search (NAS), originally proposed in [13]. NAS solutions are based upon an architecture search space, a search strategy and an evaluation strategy [13]. A search space contains a set of candidate operations. Using some performance criteria, an architecture is selected from this space and further optimised. The particular variant of NAS known as differentiable architecture search (DARTS) [15], enables the selection of candidate operations, and hence the architecture, from a search space with continuous and learnable weights. DARTS models can be optimised with backpropagation in the usual manner with hardware acceleration. The network is designed automatically by optimising the operations contained within architecture building blocks referred to as cells. Candidate operations, including convolutional operations, pooling layers, and residual connections among others, are selected during an initial search phase, before the resulting cells are stacked together to build a deeper architecture which is then further optimised. The resulting networks resemble the current state of the art in anti-spoofing, hence our adoption of DARTS in this work.

This paper reports our use of a particular variant of DARTS known as partial channel connections (PC-DARTS) [16] for anti-spoofing. We show how partial channel connections, which deliver substantial savings in both computational complexity and memory, enable the automatic learning of a neural network based solution to anti-spoofing. Both the network architecture and parameters are learned automatically with only minimal human input. To the best of our knowledge, our work is both the first reported application of DARTS to anti-spoofing and the first reported application of PC-DARTS in any field of speech processing. The remainder of the paper is organised as follows. Section 2 introduces the related work and objectives. The proposed system is reported in Section 3. Experiments and results are reported in Sections 4 and 5. Our findings and conclusions are reported in Section 6.

2. Related work and objectives

DARTS has already been applied successfully to speech and language tasks [17,19]. Its use for architecture search in a keyword spotting task is reported in [17]. Competitive results were obtained with a search space containing the regular operations used in ResNet. A successful application to automatic speech recognition reported in [18] showed promising results even when architecture search and training stages are performed using different language datasets. The first application of DARTS to speaker verification is reported in [17] which shows that smaller, automatically learned solutions compare favourably to hand-crafted architectures. While results comparable to the state of the art are reported in both [17] and [19], both also report the necessary use of small batch sizes so that architecture search can be performed upon a single GPU.
The first objective of our work is hence to determine whether neural architectures learned automatically with PC-DARTS can compete with hand-crafted networks. Second, we seek to determine the longer term scope for such networks to even outperform the current state of the art. Third, we are interested to learn whether automatically learned and optimised solutions are more efficient. While not an objective of the current work, our hypothesis is also that PC-DARTS may yield less complex networks whose behaviour may be more easily explained.

3. PC-DARTS

As illustrated in Figure 1, DARTS encompasses a pair of learning stages referred to as architecture search (top half) and train from scratch (bottom half). A key idea is to construct a complex network architecture from a pair of building blocks, referred to as cells (blue and yellow blocks in Figure 1), whose internal architecture and parameters are learned automatically. In contrast to other NAS approaches which search over a discrete set of candidate network operations, DARTS operates upon a relaxed, continuous search space. This makes the architecture representation itself differentiable, meaning that it can be optimised in the usual manner via gradient descent and backpropagation with hardware acceleration. In the architecture search stage, the cell architectures are learned and fixed. The train from scratch stage operates upon a deeper network formed from the stacking of a greater number of cells, thereby forming a deeper residual network. The network parameters are then re-optimised. The initial architecture search stage is computationally demanding. The use of partial connections (PC-DARTS) provides a more efficient solution. Since neither DARTS, much less PC-DARTS are mainstream within the speech community, a brief overview of both is provided in the following.

3.1. Searching for the Optimal Architecture

DARTS networks are constructed from the concatenation of multiple cells. An example is illustrated in Figure 2. Their internal architectures are learned automatically and dictate the sequence of operations performed upon input data in generating their output.

Each cell contains \( N \) nodes, where each node \( x^{(i)} \) represents a feature map in tensor form. The first pair of nodes, \( x^{(1)} \) and \( x^{(2)} \), are the cell inputs and are connected to the outputs of the previous two cells. Nodes \( x^{(3)} \) to \( x^{(N-1)} \), referred to as intermediate nodes, are computed from previous nodes with operation \( o \) selected from the search space \( \mathcal{O} \) according to:

\[
x^{(j)} = \sum_{i<j} o^{(i,j)} \left( x^{(i)} \right)
\]

where \( o^{(i,j)} \) is the operation performed on edge \((i,j)\) that connects \( x^{(i)} \) and \( x^{(j)} \). Node \( x^{(N)} \) is the cell output: its feature map is constructed from the concatenation of the feature maps corresponding to the full set of intermediate nodes.

In the architecture search stage, a linear combination of operations, denoted as \( \tilde{o} \), is performed on edge \((i,j)\) according to some weight \( \alpha^{(i,j)} \). The weights form a continuous search space through a softmax function:

\[
\tilde{o}^{(i,j)} \left( x^{(i)} \right) = \frac{\exp (\alpha^{(i,j)} o)}{\sum_{o' \in \mathcal{O}} \exp (\alpha^{(i,j)} o')}
\]

Architecture search is hence reduced to the learning of a set of continuous variables \( \alpha = \{ \alpha^{(i,j)} \} \), where \( \alpha^{(i,j)} \) is a vector of dimension \( |\mathcal{O}| \). Both the architecture parameters \( \alpha \) and the network parameters \( \omega \) (e.g. the convolutional filter weights) can be jointly optimised through backpropagation. The goal is to determine the \( \alpha \) which minimises the validation loss \( L_{val} \), where the optimal \( \omega \) is determined by minimising the training loss \( L_{train}(\omega, \alpha) \):

\[
\min_{\alpha} L_{val}(\omega^*, \alpha) \quad \text{s.t.} \quad \omega^* = \arg \min_{\omega} L_{train}(\omega, \alpha)
\]

When the search stage is complete, \( \tilde{o}^{(i,j)} \) is replaced with the single operation with the highest \( \alpha^{(i,j)} \). The final cell architecture is obtained by retaining the set of \( K \) edges entering each intermediate node which have the highest weights \( \alpha^{(i,j)} \), where \( K \) is a hyperparameter. The remainder are discarded.

The search space \( \mathcal{O} \) proposed in [19] comprises: a \( 3 \times 3 \) separable convolution; a \( 5 \times 5 \) separable convolution; a \( 3 \times 3 \) dilated convolution; a \( 5 \times 5 \) dilated convolution; a skip connection; a \( 3 \times 3 \) average pooling; a \( 3 \times 3 \) max pooling; none (no connection). The set of operations are used in defining two types of neural cells, namely normal cells and reduction cells. As illustrated to the base of Figure 1, cells are stacked together.
to form the full, deeper residual network, with reduction cells being placed at the $\frac{1}{3}$ and $\frac{2}{3}$ depth positions of the total network depth (number of stacked cells). Feature map dimensions are fixed for the input and output of each normal cell. Reduction cells act to reduce the feature map dimensions by 50% while doubling the number of channels.

3.2. Partial Channel Connections and Edge Normalisation

DARTS remains computationally demanding, especially in the architecture search stage. To improve efficiency, we used partial channel connections and edge normalisation [19]. Partially-connected DARTS (PC-DARTS) delivers substantial savings in computation and memory. For a given edge $(i, j)$, partial channel connections are formed from the element-wise multiplication of $x^{(i)}$ by a masking operator $S^{(i,j)}$ of the same dimension. The masking operator either selects (multiplication by 1) or masks (multiplication by 0) each channel in $x^{(i)}$:

$$g^{(i,j)}(x^{(i)}) = \sum_{o \in \mathcal{O}} \frac{\exp(\alpha^{o}_{i,j})}{\sum_{o' \in \mathcal{O}} \exp(\alpha^{o'}_{i,j})} \circ (S^{(i,j)} \odot x^{(i)})$$

$$+ (1 - S^{(i,j)}) \odot x^{(i)}$$ (4)

where $\odot$ indicates element wise multiplication. A hyperparameter $K$ is set to conserve a random fraction $1/K$ of the available channels. Partial connections hence reduce the computational load by a factor $K$ while acting to regularise the choice of weight-free candidate operations (e.g., max pooling) in $\mathcal{O}$ for a given edge [19]. There is hence a trade off between performance (smaller $K$) and efficiency (larger $K$). As a result of random channel sampling, the linear combination of operations $g^{(i,j)}$ for each node can become unstable under training. This issue is addressed by introducing a set of edge normalisation parameters $\beta$ which smooth node inputs according to:

$$x^{(j)} = \sum_{i < j} \frac{\exp(\beta^{(i,j)})}{\sum_{i' < j} \exp(\beta^{(i',j)})} g^{(i,j)}(x^{(i)})$$ (5)

where $\beta^{(i,j)}$ is a learnable smoothing factor. The set of architecture parameters optimised by minimizing $L_{\text{real}}$ now comprises both $\alpha$ and $\beta$.

4. Experiments

In this section we describe the experimental setup, the choice of front-end and our specific PC-DARTS configuration.

4.1. Database, protocols and metrics

All work reported in this paper was performed using the ASVspoof 2019 Logical Access (LaA) database [20] which comprises the usual train, development and evaluation partitions. In the architecture search stage, a random selection of half the number of utterances for each class in the training partition, including bona fide and spoofed (A01-A16), is used to learn network parameters. The other half is used to learn architectures, namely one normal cell and one reduction cell. The cell architectures which produce the highest classification accuracy are then used in the train from scratch stage.

After the train from scratch stage, the performance of the resulting model is assessed using the full evaluation partition. Performance is reported in terms of the pooled minimum normalised tandem detection cost function (min-DCF) [21] in addition to the pooled equal error rate (EER).

4.2. Front-end

Initial experiments showed that the application of neural architecture search to raw audio waveforms places excessive demands upon GPU memory, implying lower batch sizes and greater training time [22]. We hence used linear frequency cepstral coefficients (LFCCs) of 60 dimensions encompassing static, delta and delta-delta coefficients. Features are extracted using 64 ms Hamming windows with a 16 ms shift and a 1024-point FFT. In order to improve generalisation, frequency masking is applied according to the procedure described in [23] with a maximum of 12 masked frequency channels per mini-batch.

4.3. PC-DARTS

As is customary [16], we applied three convolutional layers of stride 2 to the input features in order to reduce resolution. Architecture search is performed using 4 neural cells (2 normal cells and 2 reduction cells) with 16 initial channels. Each cell has $N = 7$ nodes, and each intermediate node retains $K = 2$ inputs after search.

Training for the architecture search stage is performed for 50 epochs with a batch size of 64 using an Adam optimiser to learn both architecture and network parameters. Both are optimised by minimising the weighted cross-entropy loss between spoofed and bona fide data with a ratio 1:9. According to [19][23], architecture parameters are not updated in the first 10 epochs. For the learning of architecture parameters we used a learning rate of 6e-4 and a weight decay of 0.001. For network parameters, we used an initial learning rate of 0.01 which is annealed down to 0.001 according to a cosine schedule. Partial channel connections use a value of $K = 2$. When the architecture search stage is complete, network parameters $\omega$ are forgotten. Only the normal and reduction cell architectures are then retained.

During the train from scratch stage, models are trained for 100 epochs with a batch size of 128 and an initial learning rate of 0.001. The drop-path rate [15] is set to 0.2. We experimented with different numbers of stacked layers ($L$) and initial channels ($C$). The models are optimized with the same loss function as in the architecture search stage. The final scores are taken from the output for the bona fide class.

All experiments reported in this paper were performed on a single NVIDIA GeForce RTX 2080 Ti GPU. Using the implementation available online[4] all results are reproducible with the same random seed and GPU environment.

5. Results

5.1. Architecture Search

The architecture search stage is the most computationally expensive. We are hence interested in both the search time and performance, both of which are illustrated in Table 1 for experiments with DARTS and PC-DARTS for models with 4 layers and 16 channels ($L = 4, C = 16$). In DARTS case, the batch size is set to the largest possible given GPU memory constraints. The use of partial connections improves on search time by approximately 50% while regularisation results in improved accuracy. Performance also translates well from the training partition to the development partition. Illustrations of the resulting normal and reduction cell operations are shown in Figure 3.

architecture and parameters are satisfying results and are the first to show that anti-spoofing differences in terms of min-tDCF are modest (even if greater in forms all but two others, both Res2Net models. Even then, the performance than the two ASVspoof baselines and also outperlines [25]. The best (16,64) model achieves substantially better systems reported in the literature and the two ASVspoof baselines.

Table 3 shows a comparison of results to top-performing systems reported in the literature. Results for the ASVspoof LA evaluation partition.

<table>
<thead>
<tr>
<th>Systems</th>
<th>Features</th>
<th>min-tDCF</th>
<th>EER</th>
<th>Params</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResNet [26]</td>
<td>CQT</td>
<td>0.0743</td>
<td>2.50</td>
<td>0.96M</td>
</tr>
<tr>
<td>ResNet [26]</td>
<td>LFCC</td>
<td>0.0786</td>
<td>2.87</td>
<td>0.96M</td>
</tr>
<tr>
<td>PC-DARTS (16,64)</td>
<td>LFCC</td>
<td>0.0914</td>
<td>4.96</td>
<td>7.51M</td>
</tr>
<tr>
<td>PC-DARTS (4,16)</td>
<td>LFCC</td>
<td>0.0992</td>
<td>5.53</td>
<td>0.14M</td>
</tr>
<tr>
<td>LCNN [27]</td>
<td>LFCC</td>
<td>0.1000</td>
<td>5.06</td>
<td>10M</td>
</tr>
<tr>
<td>LCNN [27]</td>
<td>LPS</td>
<td>0.1028</td>
<td>4.53</td>
<td>10M</td>
</tr>
<tr>
<td>LFCC-GMM [25]</td>
<td>LFCC</td>
<td>0.2116</td>
<td>8.09</td>
<td>-</td>
</tr>
<tr>
<td>ResNet [26]</td>
<td>LPS</td>
<td>0.2237</td>
<td>8.78</td>
<td>0.96M</td>
</tr>
<tr>
<td>CQCC-GMM [25]</td>
<td>CQCC</td>
<td>0.2366</td>
<td>9.57</td>
<td>-</td>
</tr>
<tr>
<td>Deep Res-Net</td>
<td>LPS</td>
<td>0.2741</td>
<td>9.68</td>
<td>0.31M</td>
</tr>
</tbody>
</table>

6. Conclusions

This paper reports what is, to the best of our knowledge, the first successful application of neural architecture search (NAS) to the spoofing detection problem. We show that partially connected differentiable architecture search (PC-DARTS) is able to learn complex neural architectures from a fixed set of candidate operations. Architectures learned with PC-DARTS can be optimised using backpropagation and with hardware acceleration, meaning that even complex convolutional and residual networks can be learned automatically.

The performance of the resulting models is competitive with the state of the art. Our best performing model achieves a min-tDCF of 0.09 for the ASVspoof 2019 Logical Access database, a result outdone only by a Res2Net system, and even then only by a modest margin. Given that our result was generated by a network whose architecture and parameters are all learned automatically, instead of from many hours of manual optimisation, this is a satisfying result. Our second-best system which achieves a min-tDCF of 0.1 has 85% fewer parameters than the best performing Res2Net system. With these results, we are encouraged to pursue PC-DARTS further. The obvious next step is to apply PC-DARTS directly to raw signal inputs. Other directions include the use of PC-DARTS as a full end-to-end solution to both spoofing detection and automatic speaker verification.

7. Acknowledgements

This work is supported by the TReSSPA-ETN project funded from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No.860813. It is also supported by the ExTENSoR project funded by the French Agence Nationale de la Recherche (ANR).
8. References


