Chapter 3

Neural Architecture Search

Thomas Elsken and Jan Hendrik Metzen and Frank Hutter

Abstract

Deep Learning has enabled remarkable progress over the last years on a variety of tasks, such as image recognition, speech recognition, and machine translation. One crucial aspect for this progress are novel neural architectures. Currently employed architectures have mostly been developed manually by human experts, which is a time-consuming and error-prone process. Because of this, there is growing interest in automated neural architecture search methods. We provide an overview of existing work in this field of research and categorize them according to three dimensions: search space, search strategy, and performance estimation strategy.

This chapter is based on a very recent survey article [23].

3.1 Introduction

The success of deep learning in perceptual tasks is largely due to its automation of the feature engineering process: hierarchical feature extractors are learned in an end-to-end fashion from data rather than manually designed. This success has been accompanied, however, by a rising demand for architecture engineering, where increasingly more complex neural architectures are designed manually. Neural Architecture Search (NAS), the process of automating architecture engineering, is thus a logical next step in automating machine learning. NAS can be seen as subfield of AutoML and has significant overlap with hyperparameter optimization and meta-learning (which are described in Chapters 1 and 2 of this book, respectively). We categorize methods for NAS according to three dimensions: search space, search strategy, and performance estimation strategy:

- **Search Space.** The search space defines which architectures can be represented in principle. Incorporating prior knowledge about properties well-suited for a task can reduce the size of the search space and simplify the
search. However, this also introduces a human bias, which may prevent finding novel architectural building blocks that go beyond the current human knowledge.

- **Search Strategy.** The search strategy details how to explore the search space. It encompasses the classical exploration-exploitation trade-off since, on the one hand, it is desirable to find well-performing architectures quickly, while on the other hand, premature convergence to a region of suboptimal architectures should be avoided.

- **Performance Estimation Strategy.** The objective of NAS is typically to find architectures that achieve high predictive performance on unseen data. Performance Estimation refers to the process of estimating this performance: the simplest option is to perform a standard training and validation of the architecture on data, but this is unfortunately computationally expensive and limits the number of architectures that can be explored. Much recent research therefore focuses on developing methods that reduce the cost of these performance estimations.

We refer to Figure 3.1 for an illustration. The chapter is also structured according to these three dimensions: we start with discussing search spaces in Section 3.2, cover search strategies in Section 3.3, and outline approaches to performance estimation in Section 3.4. We conclude with an outlook on future directions in Section 3.5.

### 3.2 Search Space

The search space defines which neural architectures a NAS approach might discover in principle. We now discuss common search spaces from recent works.

A relatively simple search space is the space of **chain-structured neural networks**, as illustrated in Figure 3.2 (left). A chain-structured neural network architecture $A$ can be written as a sequence of $n$ layers, where the $i$th layer $L_i$ receives its input from layer $i - 1$ and its output serves as the input for layer $i + 1$, i.e., $A = L_n \circ \ldots \circ L_1 \circ L_0$. The search space is then parametrized by:
Figure 3.2: An illustration of different architecture spaces. Each node in the graphs corresponds to a layer in a neural network, e.g., a convolutional or pooling layer. Different layer types are visualized by different colors. An edge from layer \( L_i \) to layer \( L_j \) denotes that \( L_i \) receives the output of \( L_j \) as input. Left: an element of a chain-structured space. Right: an element of a more complex search space with additional layer types and multiple branches and skip connections.

(i) the (maximum) number of layers \( n \) (possibly unbounded); (ii) the type of operation every layer can execute, e.g., pooling, convolution, or more advanced layer types like depthwise separable convolutions [13] or dilated convolutions [68]; and (iii) hyperparameters associated with the operation, e.g., number of filters, kernel size and strides for a convolutional layer [4, 59, 10], or simply number of units for fully-connected networks [41]. Note that the parameters from (iii) are conditioned on (ii), hence the parametrization of the search space is not fixed-length but rather a conditional space.

Recent work on NAS [9, 21, 75, 22, 49, 11] incorporate modern design elements known from hand-crafted architectures such as skip connections, which allow to build complex, multi-branch networks, as illustrated in Figure 3.2 (right). In this case the input of layer \( i \) can be formally described as a function \( g_i(L_{out}^{i-1}, \ldots, L_{out}^{0}) \) combining previous layer outputs. Employing such a function results in significantly more degrees of freedom. Special cases of these multi-branch architectures are (i) the chain-structured networks (by setting \( g_i(L_{out}^{i-1}, \ldots, L_{out}^{0}) = L_{out}^{i-1} \)), (ii) Residual Networks [28], where previous layer outputs are summed \( (g_i(L_{out}^{i-1}, \ldots, L_{out}^{0}) = L_{out}^{i-1} + L_{out}^{j}, j < i) \) and (iii) DenseNets [29], where previous layer outputs are concatenated \( (g_i(L_{out}^{i-1}, \ldots, L_{out}^{0}) = concat(L_{out}^{i-1}, \ldots, L_{out}^{0})) \).

Motivated by hand-crafted architectures consisting of repeated motifs [62, 28, 29], Zoph et al. [75] and Zhong et al. [71] propose to search for such motifs, dubbed cells or blocks, respectively, rather than for whole architectures. Zoph et al. [75] optimize two different kind of cells: a normal cell that preserves the dimensionality of the input and a reduction cell which reduces the spatial
Figure 3.3: Illustration of the cell search space. Left: Two different cells, e.g., a normal cell (top) and a reduction cell (bottom) [75]. Right: an architecture built by stacking the cells sequentially. Note that cells can also be combined in a more complex manner, such as in multi-branch spaces, by simply replacing layers with cells.

dimension. The final architecture is then built by stacking these cells in a predefined manner, as illustrated in Figure 3.3. This search space has two major advantages compared to the ones discussed above:

1. The size of the search space is drastically reduced since cells can be comparably small. For example, Zoph et al. [75] estimate a seven-times speed-up compared to their previous work [74] while achieving better performance.

2. Cells can more easily be transferred to other datasets by adapting the number of cells used within a model. Indeed, Zoph et al. [75] transfer cells optimized on CIFAR-10 to ImageNet and achieve state-of-the-art performance.

Consequently, this cell-based search space was also successfully employed by many later works [49, 37, 46, 22, 11, 39, 72]. However, a new design-choice arises when using a cell-based search space, namely how to choose the meta-architecture: how many cells shall be used and how should they be connected to build the actual model? For example, Zoph et al. [75] build a sequential model from cells, in which each cell receives the outputs of the two preceding cells as input, while Cai et al. [11] employ the high-level structure of well-known manually designed architectures, such as DenseNet [29], and use their cells within these models. In principle, cells can be combined arbitrarily, e.g.,
within the multi-branch space described above by simply replacing layers with cells. Ideally, the meta-architecture should be optimized automatically as part of NAS; otherwise one easily ends up doing meta-architecture engineering and the search for the cell becomes overly simple if most of the complexity is already accounted for by the meta-architecture.

One step in the direction of optimizing meta-architectures is the hierarchical search space introduced by Liu et al. [38], which consists of several levels of motifs. The first level consists of the set of primitive operations, the second level of different motifs that connect primitive operations via a direct acyclic graphs, the third level of motifs that encode how to connect second-level motifs, and so on. The cell-based search space can be seen as a special case of this hierarchical search space where the number of levels is three, the second level motifs corresponds to the cells, and the third level is the hard-coded meta-architecture.

The choice of the search space largely determines the difficulty of the optimization problem: even for the case of the search space based on a single cell with fixed meta-architecture, the optimization problem remains (i) non-continuous and (ii) relatively high-dimensional (since more complex models tend to perform better, resulting in more design choices). We note that the architectures in many search spaces can be written as fixed-length vectors; e.g., the search space for each of the two cells by Zoph et al. [75] can be written as a 40-dimensional search space with categorical dimensions, each of which chooses between a small number of different building blocks and inputs. Similarly, unbounded search spaces can be constrained to have a maximal depth, giving rise to fixed-size search spaces with (potentially many) conditional dimensions.

In the next section, we discuss Search Strategies that are well-suited for these kinds of search spaces.

### 3.3 Search Strategy

Many different search strategies can be used to explore the space of neural architectures, including random search, Bayesian optimization, evolutionary methods, reinforcement learning (RL), and gradient-based methods. Historically, evolutionary algorithms were already used by many researchers to evolve neural architectures (and often also their weights) decades ago [see, e.g., 2, 56, 23, 65]. Yao [67] provides a literature review of work earlier than 2000.

Bayesian optimization celebrated several early successes in NAS since 2013, leading to state-of-the-art vision architectures [7], state-of-the-art performance for CIFAR-10 without data augmentation [19], and the first automatically-tuned neural networks to win competition datasets against human experts [41]. NAS became a mainstream research topic in the machine learning community after Zoph and Le [74] obtained competitive performance on the CIFAR-10 and Penn Treebank benchmarks with a search strategy based on reinforcement learning. While Zoph and Le [74] use vast computational resources to achieve this result (800 GPUs for three to four weeks), after their work, a wide variety of methods
have been published in quick succession to reduce the computational costs and achieve further improvements in performance.

To frame NAS as a reinforcement learning (RL) problem, the generation of a neural architecture can be considered to be the agent’s action, with the action space identical to the search space. The agent’s reward is based on an estimate of the performance of the trained architecture on unseen data (see Section 3.4). Different RL approaches differ in how they represent the agent’s policy and how they optimize it: Zoph and Le use a recurrent neural network (RNN) policy to sequentially sample a string that in turn encodes the neural architecture. They initially trained this network with the REINFORCE policy gradient algorithm, but in follow-up work use Proximal Policy Optimization (PPO) instead. Baker et al. use Q-learning to train a policy which sequentially chooses a layer’s type and corresponding hyperparameters. An alternative view of these approaches is as sequential decision processes in which the policy samples actions to generate the architecture sequentially, the environment’s “state” contains a summary of the actions sampled so far, and the (undiscounted) reward is obtained only after the final action. However, since no interaction with an environment occurs during this sequential process (no external state is observed, and there are no intermediate rewards), we find it more intuitive to interpret the architecture sampling process as the sequential generation of a single action; this simplifies the RL problem to a stateless multi-armed bandit problem.

A related approach was proposed by Cai et al., who frame NAS as a sequential decision process: in their approach the state is the current (partially trained) architecture, the reward is an estimate of the architecture’s performance, and the action corresponds to an application of function-preserving mutations, dubbed network morphisms, see also Section 3.4, followed by a phase of training the network. In order to deal with variable-length network architectures, they use a bi-directional LSTM to encode architectures into a fixed-length representation. Based on this encoded representation, actor networks decide on the sampled action. The combination of these two components constitute the policy, which is trained end-to-end with the REINFORCE policy gradient algorithm. We note that this approach will not visit the same state (architecture) twice so that strong generalization over the architecture space is required from the policy.

An alternative to using RL are neuro-evolutionary approaches that use evolutionary algorithms for optimizing the neural architecture. The first such approach for designing neural networks we are aware of dates back almost three decades: Miller et al. use genetic algorithms to propose architectures and use backpropagation to optimize their weights. Many neuro-evolutionary approaches since then use genetic algorithms to optimize both the neural architecture and its weights; however, when scaling to contemporary neural architectures with millions of weights for supervised learning tasks, SGD-based weight optimization methods currently outperform evolutionary ones. More recent work shows that evolving even millions of weights is competitive to gradient-
recent neuro-evolutionary approaches \cite{50, 59, 38, 49, 43, 66, 22} therefore again use gradient-based methods for optimizing weights and solely use evolutionary algorithms for optimizing the neural architecture itself. Evolutionary algorithms evolve a population of models, i.e., a set of (possibly trained) networks; in every evolution step, at least one model from the population is sampled and serves as a parent to generate offsprings by applying mutations to it. In the context of NAS, mutations are local operations, such as adding or removing a layer, altering the hyperparameters of a layer, adding skip connections, as well as altering training hyperparameters. After training the offsprings, their fitness (e.g., performance on a validation set) is evaluated and they are added to the population.

Neuro-evolutionary methods differ in how they sample parents, update populations, and generate offsprings. For example, Real et al. \cite{50}, Real et al. \cite{49}, and Liu et al. \cite{38} use tournament selection \cite{27} to sample parents, whereas Elsken et al. \cite{22} sample parents from a multi-objective Pareto front using an inverse density. Real et al. \cite{50} remove the worst individual from a population, while Real et al. \cite{49} found it beneficial to remove the oldest individual (which decreases greediness), and Liu et al. \cite{38} do not remove individuals at all. To generate offspring, most approaches initialize child networks randomly, while Elsken et al. \cite{22} employ Lamarckian inheritance, i.e, knowledge (in the form of learned weights) is passed on from a parent network to its children by using network morphisms. Real et al. \cite{50} also let an offspring inherit all parameters of its parent that are not affected by the applied mutation; while this inheritance is not strictly function-preserving it might also speed up learning compared to a random initialization. Moreover, they also allow mutating the learning rate which can be seen as a way for optimizing the learning rate schedule during NAS.

Real et al. \cite{49} conduct a case study comparing RL, evolution, and random search (RS), concluding that RL and evolution perform equally well in terms of final test accuracy, with evolution having better anytime performance and finding smaller models. Both approaches consistently perform better than RS in their experiments, but with a rather small margin: RS achieved test errors of approximately 4% on CIFAR-10, while RL and evolution reached approximately 3.5% (after “model augmentation” where depth and number of filters was increased; the difference on the actual, non-augmented search space was approx. 2%). The difference was even smaller for Liu et al. \cite{38}, who reported a test error of 3.9% on CIFAR-10 and a top-1 validation error of 21.0% on ImageNet for RS, compared to 3.75% and 20.3% for their evolution-based method, respectively.

*Bayesian Optimization* (BO, see, e.g., \cite{53}) is one of the most popular methods for hyperparameter optimization (see also Chapter \ref{chapter1} of this book), but it has not been applied to NAS by many groups since typical BO toolboxes are based on Gaussian processes and focus on low-dimensional continuous optimization based optimization when only high-variance estimates of the gradient are available, e.g., for reinforcement learning tasks \cite{51, 67, 15}. Nonetheless, for supervised learning tasks gradient-based optimization is by far the most common approach.
problems. Swersky et al. [60] and Kandasamy et al. [31] derive kernel functions for architecture search spaces in order to use classic GP-based BO methods, but so far without achieving new state-of-the-art performance. In contrast, several works use tree-based models (in particular, treed Parzen estimators [8], or random forests [30]) to effectively search very high-dimensional conditional spaces and achieve state-of-the-art performance on a wide range of problems, optimizing both neural architectures and their hyperparameters jointly [7, 19, 41, 69]. While a full comparison is lacking, there is preliminary evidence that these approaches can also outperform evolutionary algorithms [83].

Architectural search spaces have also been explored in a hierarchical manner, e.g., in combination with evolution [38] or by sequential model-based optimization [37]. Negrinho and Gordon [45] and Wistuba [65] exploit the tree-structure of their search space and use Monte Carlo Tree Search. Elsken et al. [21] propose a simple yet well performing hill climbing algorithm that discovers high-quality architectures by greedily moving in the direction of better performing architectures without requiring more sophisticated exploration mechanisms.

In contrast to the gradient-free optimization methods above, Liu et al. [39] propose a continuous relaxation of the search space to enable gradient-based optimization: instead of fixing a single operation \( o_i \) (e.g., convolution or pooling) to be executed at a specific layer, the authors compute a convex combination from a set of operations \( \{o_1, \ldots, o_m\} \). More specifically, given a layer input \( x \), the layer output \( y \) is computed as \( y = \sum_{i=1}^{m} \lambda_i o_i(x), \lambda_i \geq 0, \sum_{i=1}^{m} \lambda_i = 1 \), where the convex coefficients \( \lambda_i \) effectively parameterize the network architecture. Liu et al. [39] then optimize both the network weights and the network architecture by alternating gradient descent steps on training data for weights and on validation data for architectural parameters such as \( \lambda \). Eventually, a discrete architecture is obtained by choosing the operation \( i \) with \( i = \text{arg max}_i \lambda_i \) for every layer. Shin et al. [54] and Ahmed and Torresani [1] also employ gradient-based optimization of neural architectures, however they only consider optimizing layer hyperparameters or connectivity patterns, respectively.

### 3.4 Performance Estimation Strategy

The search strategies discussed in Section 3.3 aim at finding a neural architecture \( A \) that maximizes some performance measure, such as accuracy on unseen data. To guide their search process, these strategies need to estimate the performance of a given architecture \( A \) they consider. The simplest way of doing this is to train \( A \) on training data and evaluate its performance on validation data. However, training each architecture to be evaluated from scratch frequently yields computational demands in the order of thousands of GPU days for NAS [74, 50, 75, 49].

To reduce this computational burden, performance can be estimated based on lower fidelities of the actual performance after full training (also denoted as proxy metrics). Such lower fidelities include shorter training times [75, 69], training on a subset of the data [34], on lower-resolution images [14], or with
less filters per layer \cite{75, 49}. While these low-fidelity approximations reduce the computational cost, they also introduce bias in the estimate as performance will typically be underestimated. This may not be problematic as long as the search strategy only relies on ranking different architectures and the relative ranking remains stable. However, recent results indicate that this relative ranking can change dramatically when the difference between the cheap approximations and the “full” evaluation is too big \cite{69}, arguing for a gradual increase in fidelities \cite{35, 24}.

Another possible way of estimating an architecture’s performance builds upon learning curve extrapolation \cite{61, 19, 32, 5, 48}. Domhan et al. \cite{19} propose to extrapolate initial learning curves and terminate those predicted to perform poorly to speed up the architecture search process. Swersky et al. \cite{61}, Klein et al. \cite{32}, Baker et al. \cite{5}, Rawal and Miikkulainen \cite{48} also consider architectural hyperparameters for predicting which partial learning curves are most promising. Training a surrogate model for predicting the performance of novel architectures is also proposed by Liu et al. \cite{37}, who do not employ learning curve extrapolation but support predicting performance based on architectural/cell properties and extrapolate to architectures/cells with larger size than seen during training. The main challenge for predicting the performances of neural architectures is that, in order to speed up the search process, good predictions in a relatively large search space need to be made based on relatively few evaluations.

Another approach to speed up performance estimation is to initialize the weights of novel architectures based on weights of other architectures that have been trained before. One way of achieving this, dubbed network morphisms \cite{64}, allows modifying an architecture while leaving the function represented by the network unchanged \cite{10, 11, 21, 22}. This allows increasing capacity of networks successively and retaining high performance without requiring training from scratch. Continuing training for a few epochs can also make use of the additional capacity introduced by network morphisms. An advantage of these approaches is that they allow search spaces without an inherent upper bound on the architecture’s size \cite{21}; on the other hand, strict network morphisms can only make architectures larger and may thus lead to overly complex architectures. This can be attenuated by employing approximate network morphisms that allow shrinking architectures \cite{22}.

One-Shot Architecture Search is another promising approach for speeding up performance estimation, which treats all architectures as different subgraphs of a supergraph (the one-shot model) and shares weights between architectures that have edges of this supergraph in common \cite{52, 9, 40, 39, 6}. Only the weights of a single one-shot model need to be trained (in one of various ways), and architectures (which are just subgraphs of the one-shot model) can then be evaluated without any separate training by inheriting trained weights from the one-shot model. This greatly speeds up performance estimation of architectures, since no training is required (only evaluating performance on validation data). This approach typically incurs a large bias as it underestimates the actual performance of architectures severely; nevertheless, it allows ranking ar-
CHAPTER 3. NEURAL ARCHITECTURE SEARCH

Chapter 3


A GENERAL LIMITATION OF ONE-SHOT NAS IS THAT THE SUPERGRAPH DEFINED A-PRIORI restricts the search space to its subgraphs. Moreover, approaches which require that the entire supergraph resides in GPU memory during architecture search will be restricted to relatively small supergraphs and search spaces accordingly and are thus typically used in combination with cell-based search spaces. While approaches based on weight-sharing have substantially reduced the computational resources required for NAS (from thousands to a few GPU days), it is currently not well understood which biases they introduce into the search if the sampling distribution of architectures is optimized along with the one-shot model. For instance, an initial bias in exploring certain parts of the search space more than others might lead to the weights of the one-shot model being better adapted for these architectures, which in turn would reinforce the bias of the search to these parts of the search space. This might result in premature convergence of NAS and might be one advantage of a fixed sampling distribution as used by Bender et al. [6]. In general, a more systematic analysis of biases introduced by different performance estimators would be a desirable direction for future work.

3.5 Future Directions

In this section, we discuss several current and future directions for research on NAS. Most existing work has focused on NAS for image classification. On the one hand, this provides a challenging benchmark since a lot of manual engineering has been devoted to finding architectures that perform well in this domain and are not easily outperformed by NAS. On the other hand, it is relatively easy to define a well-suited search space by utilizing knowledge from manual en-
3.5. FUTURE DIRECTIONS

gineering. This in turn makes it unlikely that NAS will find architectures that substantially outperform existing ones considerably since the found architectures cannot differ fundamentally. We thus consider it important to go beyond image classification problems by applying NAS to less explored domains. Notable first steps in this direction are applying NAS to language modeling [74], music modeling [48], image restoration [58] and network compression [3]; applications to reinforcement learning, generative adversarial networks, semantic segmentation, or sensor fusion could be further promising future directions.

An alternative direction is developing NAS methods for multi-task problems [36, 12] and for multi-objective problems [22, 20, 73], in which measures of resource efficiency are used as objectives along with the predictive performance on unseen data. Likewise, it would be interesting to extend RL/bandit approaches, such as those discussed in Section 3.3 to learn policies that are conditioned on a state that encodes task properties/resource requirements (i.e., turning the setting into a contextual bandit). A similar direction was followed by Ramachandran and Le [47] in extending one-shot NAS to generate different architectures depending on the task or instance on-the-fly. Moreover, applying NAS to searching for architectures that are more robust to adversarial examples [17] is an intriguing recent direction.

Related to this is research on defining more general and flexible search spaces. For instance, while the cell-based search space provides high transferability between different image classification tasks, it is largely based on human experience on image classification and does not generalize easily to other domains where the hard-coded hierarchical structure (repeating the same cells several times in a chain-like structure) does not apply (e.g., semantic segmentation or object detection). A search space which allows representing and identifying more general hierarchical structure would thus make NAS more broadly applicable, see Liu et al. [38] for first work in this direction. Moreover, common search spaces are also based on predefined building blocks, such as different kinds of convolutions and pooling, but do not allow identifying novel building blocks on this level; going beyond this limitation might substantially increase the power of NAS.

The comparison of different methods for NAS is complicated by the fact that measurements of an architecture’s performance depend on many factors other than the architecture itself. While most authors report results on the CIFAR-10 dataset, experiments often differ with regard to search space, computational budget, data augmentation, training procedures, regularization, and other factors. For example, for CIFAR-10, performance substantially improves when using a cosine annealing learning rate schedule [40], data augmentation by CutOut [15], by MixUp [70] or by a combination of factors [16], and regularization by Shake-Shake regularization [26] or scheduled drop-path [75]. It is therefore conceivable that improvements in these ingredients have a larger impact on reported performance numbers than the better architectures found by NAS. We thus consider the definition of common benchmarks to be crucial for a fair comparison of different NAS methods. A first step in this direction is the definition of a benchmark for joint architecture and hyperparameter search for a fully connected neural network with two hidden layers [33]. In this bench-
mark, nine discrete hyperparameters need to be optimized that control both architecture and optimization/regularization. All 62,208 possible hyperparameter combinations have been pre-evaluated such that different methods can be compared with low computational resources. However, the search space is still very simple compared to the spaces employed by most NAS methods. It would also be interesting to evaluate NAS methods not in isolation but as part of a full open-source AutoML system, where also hyperparameters [41, 50, 69], and data augmentation pipeline [16] are optimized along with NAS.

While NAS has achieved impressive performance, so far it provides little insights into why specific architectures work well and how similar the architectures derived in independent runs would be. Identifying common motifs, providing an understanding why those motifs are important for high performance, and investigating if these motifs generalize over different problems would be desirable.

Acknowledgements

We would like to thank Esteban Real, Arber Zela, Gabriel Bender, Kenneth Stanley and Thomas Pfeil for feedback on earlier versions of this survey. This work has partly been supported by the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme under grant no. 716721.

Bibliography


CHAPTER 3. NEURAL ARCHITECTURE SEARCH


