Compositionality is a key strategy for addressing combinatorial complexity and the curse of dimensionality. Recent work has shown that compositional solutions can be learned and offer substantial gains across a variety of domains, including multi-task learning, language modeling, visual question answering, machine comprehension, and others. However, such models present unique challenges during training when both the module parameters and their composition must be learned jointly. In this paper, we identify several of these issues and analyze their underlying causes. Our discussion focuses on routing networks, a general approach to this problem, and examines empirically the interplay of these challenges and a variety of design decisions. In particular, we consider the effect of how the algorithm decides on module composition, how the algorithm updates the modules, and if the algorithm uses regularization.

Keywords Compositionality · Modularity · Meta Learning · Deep Learning · Decision Making

1 Introduction

In machine learning, and in deep learning in particular, modularity is becoming a key approach to reducing complexity and improving generalization by encouraging a decomposition of complex systems into specialized sub-systems. Such observations have similarly motivated studies in human cognition (compare [Bechtel and Richardson, 2010] for an overview). In theory, models without special affordances for modularity can learn to specialize groups of neurons for specific subtasks, but in practice this appears not to be the case. To address this issue, a number of models have been introduced to enforce specialization [Jacobs et al., 1991b, Miikkulainen, 1993, Jordan and Jacobs, 1994, Bengio et al., 2013, Davis and Arel, 2013, Andreas et al., 2015, Bengio et al., 2015, Shazeer et al., 2017, Fernando et al., 2017]. Much of this earlier work has either fixed the composition strategy and learned the modules (neurons or whole networks) or fixed the modules and
learned the composition strategy. But in its most general form, the compositionality problem is to jointly learn both the parameters of the modules and a strategy for their composition with the goal of solving new tasks. Recently we proposed a new paradigm called, routing [Rosenbaum et al., 2017], which is to our knowledge the first approach to jointly optimize both modules and their compositional strategy in the general setting.

A routing network (depicted in Figure 1) consists of a set of modules (parameterized functions) from which a router (the composition strategy) can choose a composition. In a neural network setting, the modules are sub-networks and the router assembles them into a model that processes the input. In making these decisions the routing network can be viewed as selecting a model (path) from the set of combinatorially many such models, one for each possible sequence of modules. This connects routing to a body of related work in conditional computation, meta-learning, architecture search and other areas. Because routing networks jointly train their modules and the module composition strategy, they face a set of challenges which non-routed networks do not. In particular, training a routing network is non-stationary from both the perspective of the router, and from the perspective of the modules, because the optimal composition strategy depends on the module parameters and vice versa.

There is relatively little research on the unique challenges faced when training these networks, which are highly dynamic. In this paper, we conduct an extensive empirical investigation of these challenges with a focus on routing networks. In Sections 2 we review notable related ideas that share a similar motivation to routing networks. In Section 3, we identify five main challenges for routing. One such challenge is to stabilize the interaction of the module and composition strategy training. Another is module collapse [Kirsch et al., 2018], which occurs when the choices made by the composition strategy lack diversity. Overfitting is also a problem which can be severe in a routed network because of the added flexibility of composition order. We also discuss the difficulty extrapolating the learning behavior of heterogeneous modules to better select those with greater potential. Adding to these difficulties is the lack of a compelling mathematical framework for models which perform modular and compositional learning. This paper is the first to consider all of these challenges jointly. One benefit of such a holistic view of the challenges has been that we were able to identify a clear relationship between collapse and overfitting that holds for any form of modular learning. We discuss this in more detail in Section 3. In Section 4, we present a detailed overview of routing, analyzing two strategies for training the router: reinforcement learning and recently introduced reparameterization strategies. There we also identify important design options, such as the choice of optimization algorithm and the router’s architecture. In Section 5, we empirically compare these different choices and how they influence the main challenges we have identified. We conclude with thoughts on promising directions for further investigation.

2 Background and Related Work

Routing networks are clearly related to task-decomposition modular networks [Jacobs et al., 1991a], and to mixtures of experts architectures [Jacobs et al., 1991b, Jordan and Jacobs, 1994] as well as their modern attention based [Riemer et al., 2016] and sparse [Shazeer et al., 2017] variants. The gating network in a typical mixtures of experts model takes in the input and chooses an appropriate weighting for the output of each expert network. This is generally implemented as a soft mixture decision as opposed to a hard routing decision, allowing the choice to be differentiable. Although the sparse and layer-wise variant presented in
Routing networks as a general paradigm of composing trainable transformations were first introduced in [Rosenbaum et al., 2017]. Since then, there have been several approaches extending them. Chang et al. [2019] show that a vanilla routing network can learn to generalize over patterns and thus to classes of unseen samples if it is trained with curriculum learning. Kirsch et al. [2018] identify one of the challenges of compositional computation, collapse, and develop a new policy gradient based routing algorithm that utilizes EM techniques to alternatingly group samples to transformations, and then applies them. Ramachandran and Le [2019] investigate the problem of architectural diversity over transformations, but use a top-k routing approach. Cases et al. [2019] show how routing can be paired with high quality linguistic annotations to learn compositional structures that maximize utilization of task-specific information. Alet et al. [2018] combine a routing-like approach with other meta-learning approaches, to allow for quick adaptation to new tasks. However, this approach relies on pre-trained composable transformations.

2.2 Generalized Architecture based Meta-Learning

Routing networks extend a popular line of recent research focused on automated architecture search, or more generally, architecture-based meta-learning. In this work, the goal is to reduce the burden on the algorithm designers by automatically learning black box algorithms that search for optimal architectures and hyperparameters. These approaches have been learned using reinforcement learning [Zoph and Le, 2017, Baker et al., 2017], evolutionary algorithms [Miikkulainen et al., 2017, Fernando et al., 2017], approximate random simulations [Brock et al., 2017], and adaptive growth [Cortes et al., 2016]. Liang et al. [2018] introduced an evolutionary algorithm approach targeting multi-task learning that comes very close to the original formulation in Rosenbaum et al. [2017]. However, routing networks are a generalization of these approaches [Ramachandran and Le, 2019] and are highly related in particular to the concept of one-shot neural architecture search [Brock et al., 2017, Pham et al., 2018, Bender et al., 2018]. The main distinction we are making here is that the benefit of routing as not solely related to parameter sharing across examples, but also related to architectural biases inherent to specific network structures that may make them helpful for specific problems.

2.3 Biological Plausibility

The high-level idea of task specific “routing” is well founded in biological studies and theories of the human brain [Gurney et al., 2001, Buschman and Miller, 2010, Stocco et al., 2010]. The idea is that regions of the brain collaborate in a complex manner by altering the synchrony in neural activity between different areas and thus changing their effective connectivity so that signals are routed in a task specific coordination. It has been found that coincidence of spikes from multiple neurons converging on a post-synaptic neuron have a super-additive effect [Aertsen et al., 1989, Usrey and Reid, 1999, Engel et al., 2001, Salinas and Sejnowski,
As a result, if neurons tuned to the same stimulus synchronize their firing, that stimulus will be more strongly represented in downstream areas. It is thought that local synchrony may help the brain to improve its signal to noise ratio while, at the same time, reducing the number of spikes needed to represent a stimulus [Aertsen et al., 1989, Tiesinga et al., 2002, Siegel and König, 2003].

The routing of modules can also be loosely linked to two fundamental aspects of the organization of the brain: functional segregation of neural populations and anatomic brain regions as specialized and independent cortical areas, and functional integration, the complementary aspect that accounts for coordinated interaction [Tononi et al., 1994]. Recently, Kell et al. [2018] have been able to replicate human cortical organization in the auditory cortex using a neural model with two distinct, task-dependent pathways corresponding to music and speech processing. When evaluated in real world tasks, their model performs as well as humans and makes human-like errors. This model is also able to predict with good accuracy fMRI voxel responses throughout the auditory cortex, which suggest certain level of convergence with brain-like representational transformations. Kell et al. [2018] use these promising results to suggest that the tripartite hierarchical organization of the auditory cortex commonly found in other species may also become evident in humans once more data is available and more realistic training mechanisms are employed. In particular, their results suggest that the architectural separation of the processing of the streams is compatible with functional segregation observed in the non-primary auditory cortex [Kell et al., 2018, and references therein].

Finally, as we will discuss briefly later, routing networks can be seen as a special case of coagent networks [Thomas and Barto, 2011], which are believed to be more biologically plausible than full end to end backpropogation networks.

### 2.4 Other Similar Forms of Modular Learning

Modular organization is central in research strategies in cognitive sciences, particularly in neuropsychology, where decomposition and localization emerge as crucial scientific research strategies [Bechtel and Richardson, 2010]. In neuropsychology, deficits in high-level cognitive functions are regularly associated with impairments of particular regions of the brain that are regarded as modules, typically under the assumptions that these modules operate independently and, to varying degrees, that their effects are local [Farah, 1994, Shallice, 1988, Bechtel and Abrahamsen, 2002]. These observations have a long tradition in cognitive science, where the nature of cognitive task-specific modules and the implementation details of compositional computation have been highly debated [Fodor, 1975, 1983, Fodor and Pylyshyn, 1988, Touretzky and Hinton, 1988, Smolensky, 1988, i.a.].

Among others, there are two notable early attempts to build modular systems with a cognitive focus: Miikkulainen [1993] developed a modular system for Natural Language Understanding with task-specific components, some of them with correlates to cognitive functions; and Jacobs et al. [1991a]’s modular networks, a modular and conditional computation model that performed task decomposition based on the input and is, to some extent, a direct ancestor of routing networks.

Another important framework for compositional learning that is also influenced by the challenges of routing discussed in this paper is the options framework [Sutton et al., 1999] for hierarchical reinforcement learning. In particular, challenges of routing are related to those experienced by end to end architectures for learning sequencing between policies over time with neural networks [Bacon et al., 2017] and extensions to hierarchical policies [Riemer et al., 2018]. Option models, similar to routing networks, are known to experience "option collapse" where either only one option is actually used or all options take on the same meaning. This common difficulty has motivated recent research showing improvement in learned options by imposing information theoretic objectives on learning that incentivize increased option diversity and increased entropy in option selection [Gregor et al., 2016, Florensa et al., 2017, Hausman et al., 2018, Eysenbach et al., 2018, 1].

1A review of this long and at times acrimonious debate is outside of the scope of this paper. For particularly interesting accounts we refer to Bechtel and Abrahamsen [2002] and Marcus [2001].
In contrast to routing networks, option models are also concerned with deciding the duration over which its decisions will last. In this paper we focus just on empirical analysis of the simpler case of routing at every time step so that we can directly address diversity of the chosen modules without introducing the additional complicating factor of sequencing selections over time.

3 Challenges to Compositional Computation

We have experienced several challenges particular to training compositional architectures, including training stability, module collapse, and overfitting as well as difficulties with performance extrapolation and formalizing the setting. Instability in training may occur because of a complex dynamic interplay between the router and module training. Module collapse may occur if module selection collapses to a policy which makes the same decision for all inputs. Overfitting may be severely exacerbated in modular architectures because of their added flexibility to learn specialized modules for a very narrow subset of samples. Successfully extrapolating the performance of specific modules out over the course of training would potentially allow a more successful selection strategy, but achieving this is a difficult problem itself. Finally, we lack a good formalization of popular training methodologies, unifying reinforcement learning for the module selection training with supervised training for the modules. There has been some progress on each of these problems (for example, module collapse was discussed in [Kirsch et al., 2018]). However, we believe this is the first time they have been collected and given a systematic treatment jointly.

One may argue that core problems of a more general nature underlie these issues. In fact, we can see that learning to compose is difficult because we must simultaneously balance two challenges of learning: the transfer-interference trade-off [Riemer et al., 2019], and the exploration-exploitation dilemma [Sutton and Barto, 1998].

The “transfer-interference trade-off” refers to the problem of choosing which parameters in the model are shared across different input samples or distributions. When there is a large amount of sharing of model parameters during training we may see better performance as a consequence of transfer, since each parameter is trained on more data. But it may also lead to worse performance if the training on different samples produces updates that ‘cancel’ each other out, or cause interference. Compositional architectures can offer an interesting balance between the two, as different modules may be active for different samples.

The “exploration-exploitation dilemma”, while mostly associated with reinforcement learning, exists for any kind of hard stochastic update. For modular learning, this means that the composer has to strike a balance between ‘exploiting’, i.e. selecting and training already known modules which may perform well at some point in time during training, and ‘exploring’ or selecting and training different modules that may not perform well yet, but which may become the globally optimal choice, given sufficient additional training. Unfortunately, high exploration increases the likelihood of both beneficial transfer and unwanted interference. But low exploration may bias the model towards selections which limit its ability to achieve an optimal balance between transfer and interference. Striking the right balance between exploration and exploitation can therefore help with interference but is not sufficient to mitigate it entirely. This entanglement complicates the learning and means we cannot treat these tradeoffs in isolation.
3.1 Training Stability

One of the most challenging problems for routing networks is overcoming the early learning phase when both modules and the router have just been initialized. In this phase, the router needs to learn the value of the modules, while these are effectively randomly trained and have not yet taken on any real meaning, since pathways and gradient-flows are not yet stable.

In our experience, this “chicken-and-egg” problem of stabilizing the early training of a routing network, before paths have had the opportunity to specialize, can result in the routing dynamics never stabilizing, leaving the network at effectively random performance. This problem roughly correlates with the complexity of the decision making problem. If the router only needs to make decisions on a very local distribution of inputs, then stability is less of a problem. If, however, the router has to consider very complex distributions, it consistently struggles.

A mitigating strategy can be to slow down the learning behavior of either the modules or the router, by either fixing their parameters for a short initial period, or by reducing their learning rate. In practice, we have found that simply reducing the learning rate of the router is an effective strategy to stabilize early training. Another strategy that can be applied is curriculum learning [Bengio et al., 2009] as is done by Chang et al. [2019]. This can be very effective, but can only be applied if the training data can naturally ordered by complexity, which is not the case in many important domains. Neither of these strategies offer a general solution to the problem. They may work in some settings and fail in others.

3.2 Module Collapse

Another common training difficulty is module collapse [Kirsch et al., 2018]. This occurs when the router falls into a local optimum, choosing one or two modules exclusively. Module collapse occurs when the router overestimates the expected reward of a selection. This may happen due to random initialization or because one module has a higher expected return during early training. Either way, the module will be chosen more often by the router, and therefore receive more training. This in turn improves the module so that it will be selected yet more often and receive yet more training until the module is dominant and no others seem promising.

As an example, consider Figure 4, which depicts a routing problem of one-dimensional linear regression (since it is easily illustrated). In plot (a), we depict a dataset with two noisy linear modes. Plot (b) shows the perfect, and desired, routing solution, where the routing model correctly assigns a routing path to each mode. Plot (c) depicts the regression curves produced by the available modules at initialization. Since the red and yellow approximations have been initialized producing too great an initial loss, the router will only update these during exploration phases, and will instead choose the green approximation. This may result in a...
suboptimal approximation (depicted in plot (d)), which can form a local optimum that will trap the router without prolonged additional, poorly rewarded exploration.

This illustrates the view of collapse as a local optimum achieved by maximizing for early transfer. When every selection is “bad”, training a transformation even on generally less compatible samples, such as shown in Figure 4, will improve its representative power. Similarly, it can be seen as a local optimum in the exploration-exploitation dilemma, since the router correctly believes at a given time that one module is better than others, and may thus not explore the other options sufficiently.

Existing solutions to this problem include: adding regularization rewards that incentivize diversity [Cases et al., 2019]; separating the training of the router from the training of the modules with an EM-like approach that learns over mini-batches, explicitly grouping samples first [Kirsch et al., 2018]; and conditioning the router entirely on discrete meta-data associated with the sample, e.g., task labels [Rosenbaum et al., 2017, Cases et al., 2019]. This has the additional benefit of reducing the dimensionality of the information on which the decisions are made, which, in turn, makes the routing problem easier.

### 3.3 Overfitting

Previous work [Kirsch et al., 2018, Shazeer et al., 2017] observes that models of conditional computation can overfit more than their “base”-models, but do examine this issue in depth. We have also encountered this problem multiple times, and believe that it stems from the flexibility of routing models to compose highly local approximations. Consider the example in Figure 5, where we again route a linear scalar approximator.

Suppose we have a training dataset consisting of observations of a noisy linear process, such as the one in Figure 5(a). It can be clearly seen that a linear model gives good (and desired) approximations, as in Figure 5(b), and that it does not overfit to the noise present in the data. However, imagine that we wanted to learn such an approximation with a routing model that consists of three parameterized functions, \( f_1 = a \cdot x, f_2 = b \cdot x, f_3 = c \cdot x \), which the router can combine to a maximum depth of three. If the router now routes purely based on input information, i.e., if the router can route each sample through a different route, then it may choose a different path for different subsets of the training data, resulting in different (local) approximations as illustrated in Figure 5(c). For neural architectures in particular, this implies that routing breaks an implicit smoothness assumption which, arguably, allows them to generalize well in spite of high dimensionality (see Zhang et al. [2016] for a further discussion). Since the space of routes or paths grows exponentially with routing depth, deep routing networks can potentially learn highly local approximations with only few samples covered per approximation.

This perspective also explains why Rosenbaum et al. [2017] and Cases et al. [2019] do not experience overfitting: if the path of a sample is independent of its input value or its intermediate activations, the resulting
paths and approximations cannot learn to match individual areas in activation-space only, but are constrained by the meta-information instead.

Within the transfer-interference trade-off, overfitting is a natural consequence of avoiding training interference. In models of uniform, i.e., non-compositional, computation, the training algorithm always enforces some amount of interference over the model’s parameters. While often harmful, it can also steer training away from local suboptimal solutions that cause the model to overfit.

Since this problem is not well investigated for machine learning models, we can only speculate on possible solutions. The most obvious is to apply regularization of some kind that prevents the router from fitting samples to highly expressive local approximators. A very successful solution with a different set of problems is the ‘routing-by-meta-information’ architecture of [Rosenbaum et al., 2017, Cases et al., 2019]. Another possible solution might be module diversity: if only different kinds of approximators can be fit the “locality” of routing does not have the same effect. This would explain why Ramachandran and Le [2019] were able to achieve very high performance with a modular architecture even when learning with few examples, although we need to take their particular top-k architecture into account. Another uninvestigated area which seems promising for exploration is the tradeoff in capacity between the router and the modules. Is it better to have a ‘smart’ router and ‘dumb’ modules or vice versa? Either will probably have an effect on overfitting.

The Flexibility Dilemma for Modular Learning

Comparing the two challenges discussed this far, it becomes clear that they are not unrelated, but are an effect of too little – or too much – flexibility on the router’s part, where flexibility is a routing network’s ability to localize its routing decisions. If the router is not flexible enough to realize how truly different modes in a distribution should be treated differently, it will cause underfitting, oftentimes through collapse. If, on the other hand, the router is too flexible in mapping different inputs to different routing paths, it creates hyperlocal approximations that can overfit badly.

This goes to the core of what routing does, and why it can be such a powerful machine learning model. Routing always has an enormous degree of expressivity, as we have a combinatorial number of implicitly defined models, in the form of paths. If the model finds a good ‘locality’ of approximations, routing can allow a model to achieve truly impressive levels of generalization (compare [Chang et al., 2019], and in particular the section on nested implicatives in [Cases et al., 2019]), as it can adapt to unseen samples by mapping these to known solutions in a highly variable way. However, on both sides of this ‘locality’ of approximation lie the above mentioned pitfalls of collapse and overfitting.

While we illustrated and explained this problem on routing (neural models), it is by no means limited to it. Any modular approach that can treat different samples differently will be exposed to this dilemma between under- and overfitting, as it comes with any form of local approximation approach.

3.4 Module Diversity

While much of the prior work has focused on the case where each module is of the same kind but with different parameters, routing modules that have different architectures has the potential to be even more
powerful and sample efficient. This allows for a larger coverage of functional capabilities, thereby increasing the expressive power of a routing network. Interestingly, this is a specific instance of the “Algorithm Selection Problem” [Rice, 1976]. For learning problems, however, the problem is complicated by the different learning dynamics that different architectures might exhibit.

Consider Figure 7. For any learning algorithm selection problem, deciding that Module 2 will yield superior performance requires the meta-learning algorithm to sufficiently explore – and thus train – both selections. However, for routing networks, exploration correlates with interference. This means that even if the router were to explore Module 1 sufficiently, the sampling noise of exploration could potentially interfere with the training procedure of selections taken before or after. While some progress on this problem has been made [Ramachandran and Le, 2019], it focuses on selections with similar learning characteristics. The full problem, for selections with arbitrary learning characteristics, was only explored in an offline setting, where selections are trained until completion and not varied while training [Zoph and Le, 2017, Liu et al., 2018]. Finding optimal selections online remains an open problem due to the difficulty of anticipating future rewards.

3.5 A uniform formal framework

All of the previous challenges are complicated by the lack of a principled mathematical formalization for compositional learning. In particular, it is not clear how the training of the router relates to and interacts with the training of the modules. Although existing approaches have found very successful solutions, even without such a formalization, a principled framework may provide additional insight, convergence guarantees and directions for the development of better algorithms.

Specifically, it is not clear how training of the modules is impacted by the training of the routers, and vice versa. For how compositionality may interfere with the training of the modules, compare section 5.3. For the other direction, consider the case of a reinforcement learning strategy for training the routers (arguably the most relevant update strategy). Reinforcement learning relies fundamentally on the assumption that the environment is governed by an underlying Markov Decision Process (MDP) [Sutton and Barto, 1998]. A naive though intuitive characterization of routing in this context might interpret individual modules as actions. But an MDP requires a static, non-changing set of actions and here the modules are themselves trained and change over time. Although in practice this strategy has been shown to work in any case [Rosenbaum et al., 2017, Chang et al., 2019, Cases et al., 2019], it lacks theoretical justification, and more principled approaches may yield superior performance.

This critique extends to the two special cases of MDPs introduced in the literature: Meta-MDPs and stochastic games. Meta-MDPs were introduced by Hay et al. [2014] and applied to routing by Chang et al. [2019], and specifically model the computational steps required to make a decision in another underlying MDP. That is, their states are partial results, and their actions are computations. Once they terminate, the resulting computation produces an action in the underlying decision problem. This approach emphasizes that the routing problem consists of computation steps, and not steps taken in an environment. A stochastic game, related to routing by Rosenbaum et al. [2017] is the multi-agent extension to MDPs and allows for an arbitrary number of agents to exist, which collaborate or compete in the same environment. As other agents interact with the environment, the environment becomes non-stationary from the perspective of any single agent. While this approach consequently models the non-stationarity of a routing problem better than a Meta-MDP, it still does not solve the more fundamental problem of possible interference between update strategies.
There are two scenarios which have more principled solutions to this criticism, although they, too, may benefit from a more targeted solution as they suffer from many of the same problems in practice. In the first, for neural networks, we use some form of reparameterized sampling function to update the composition (compare section 4.2). This addresses the core of the problem since the reparameterized decision making algorithms explicitly use the same update strategy as the (neural) models. In the second scenario, the problem solved with a routing network is optimizing a policy for a given MDP. In this case, the routing network is the policy, and can consequently be modeled as a coagent network [Thomas and Barto, 2011]. A coagent network is a theoretical framework that, like Meta-MDPs, models the decision making in an underlying MDP but explicitly allows for non-stationary interactions between parts of the policy. These parts, called coagents, can update locally on stochastic information. For routing, we can model the policy solving the underlying MDP as a routing network with routing coagents and transformation coagents (i.e., the module parameters are part of the policy). Then the policy gradient theorems in [Thomas, 2011] for the acyclic and [Kostas et al., 2019] for the cyclic case hold, as the modules will also be updated with REINFORCE. Extending this work on coagent networks to also cover non-reinforcement learning problems such as supervised learning as well might offer a principled way of modeling routing and similar RL-integrated approaches for conditional computation.

4 Routing

Routing describes a general framework of repeatedly selecting trainable function modules with a trainable router. As such, arbitrary components of a machine learning model can be routed, as long as the model is composed by a sequential application of functions in a set of (compatible) functions. We will focus on routing networks, where the learnable function modules are neural networks and parts thereof. The router receives the state of the computation, the current activation – the input \( x \) at step 0 – and evaluates it to select the best function, which will produce a new activation, which then triggers a new computational loop. If the router decides that the result has been processed sufficiently, the last activation will be handed to other computations or interpreted as the output of the model. This result will then be used to jointly train the function modules and the router.

As routing relies on hard decisions to select the modules (as opposed to ‘soft’ decisions, where several modules are activated and combined in different ways), training algorithms for the router are limited. While other approaches are conceivable (in particular genetic algorithms and other stochastic training techniques), we focus on Reinforcement Learning (RL) and Stochastic Reparameterization in this work.
4.1 Reinforcement Learning

Reinforcement learning describes a general machine learning paradigm in which an agent that makes a series of hard decisions is trained by providing simple scalar feedback, the reward. Applied to routing, the general outline is that the output of the model $\hat{y}$ has to be translated to a reward $r$ which is then used to improve the router’s policy $\pi$.

4.1.1 Routing MDPs

Markov Decision Processes (MDPs) are a common model for formally describing sequential decision making problems. While we have argued in section 3.5 that existing attempts to model compositional computation are problematic, we will still adopt a common formalism for now so that we can discuss some relevant concepts.

Given a routing MDP $M = \langle S, A, R, P, \gamma \rangle$, a set of applicable transformations $F$, the space of samples $X$, the space of transformations $H$ (i.e., the space of applications of members of $F$ to $X$), and the space of possibly available meta-information $M$, we can define:

- the states $S = (X \cup H) \times M$
- the actions $A = F \cup \{\bot\}$, where $\bot$ is a termination action
- the transition probability $P(s, a, s') = \begin{cases} 1, & \text{if } s = h, a = f, s' = f(h), h \in S, f \in F \\ 0, & \text{otherwise} \end{cases}$
- the discount factor $\gamma = 1$

The reward function $R$ can freely be designed by the model designer and is not defined any further for now. Solving an MDP generally consists of finding a policy $\pi^*(\theta)$ (parameterized by parameters $\theta$) that maximizes the objective, or score function, $J(\pi(\theta)) := E(\sum_t r_t | \pi(\theta))$.

4.1.2 Reward Design

One of the most important questions when modeling a problem as an MDP is the question of how to design the reward function $R$. For a routing network there are two types of rewards to be considered. The first is the final reward that reflects the model’s performance of solving the main problem, i.e., of predicting a sample-label. The second are different forms of regularization rewards that can either be computed for entire trajectories or as immediate responses to individual actions.

**Final Rewards** The final reward $r_f$ models the overall performance of the model for a sequence of routing decisions. For classification problems, the outcome is binary – correct or false – and an obvious choice is a simple binary reward of $\pm 1$ corresponding to the prediction agreement with the target label. As the objective for the training of the modules is a loss function $L_m(y, \hat{y})$, a different reward design for the same objective can be derived as the negative of the module loss: $r_f = -L_m(y, \hat{y})$. The reward has to be the negative of the module loss as – by convention – we minimize model losses but maximize RL rewards. In addition, this allows for a natural application of routing networks to regression problems, as these cannot be translated into a simple binary $\pm 1$ reward. While the second reward design seems like the better choice, as it both richer in information and a more principled meta-learning objective that coincides with the main model’s objective, we found that it does not necessarily perform better in practice depending on the problem of focus.

**Regularization Rewards** As the reward signal is sparse for complex compositions, it can also be quite helpful to incorporate additional rewards that can act as an intrinsic reward or regularizer of the choices made by the router. One option is to model problem-specific information in this reward – e.g. to reflect the cost of computation of choosing a specific function, or to incorporate domain-knowledge, such as intuitions as to
which model should be preferable. The second option, as employed in Rosenbaum et al. [2017], is to use this regularizer to incentivize transfer between different kinds of samples. There, the reward can be defined to correlate with how often a particular function $a$ is chosen within some window $w$, $C(a) = \frac{\#a}{\sum_w \text{samples}}$, thereby motivating the router to choose, and thereby share, that function for a wider set of samples. This reward is defined as $R(a) = \frac{\alpha}{t} C(a)$, with a ratio $\alpha$, normalized by the trajectory length $t$ – such that even for long trajectories this reward may be limited to be smaller than the final reward $r_f$. Rosenbaum et al. [2017] only investigate values of $\alpha \in [0, 1]$. However, this can lead to a lack of variety in decision making, as the selection collapses – as discussed in section 3.4 in detail. To compensate, Cases et al. [2019] investigate a different set of values for $\alpha$, $\alpha \in [-1, 0]$, with the goal of incentivizing diversity of decision making.

4.1.3 Algorithms

Several RL algorithms have been successfully used to train routing policies. Rosenbaum et al. [2017] compare a variety of algorithms, but settle for a multi-agent algorithm, fitting their multi-agent approach to multi-task learning. Cases et al. [2019] find that plain Q-Learning performs the best for their domain. Kirsch et al. [2018] extend a REINFORCE based algorithm with an alternating, EM-like training for modules and router that also optimizes for module diversity and does lookaheads. Meanwhile, Chang et al. [2019] use Proximal Policy Optimization.

While this might seem to suggest that there is not necessarily a “best” reinforcement learning algorithm, there are some constraints to be considered. The first is that the nonstationarity of the parameters of $\hat{F}$ prevents the use of replay buffers, as these would be invalidated after each transformation training step. Additionally, we argue that RL algorithms that can accommodate the change in the modules’ respective values over training will perform the best.

Consider the following example: Given a set of module choices $M$, and a value estimator for a set of states $S$, $\hat{v}(s, m), m \in M, s \in S$. Given some training, the module parameters change, and thereby the expected value for each of the modules given a specific state $s_k$; using some value-based RL algorithm, we also update $\hat{v}$. As, for routing, we generally want to exploit more than explore, the module estimates for state $s_k$ are of different quality, as some modules have been sampled less from state $s_k$ than others. However, these modules may have been trained a lot from a different state $s_l$. Given that there can be transfer from state $s_k$ to state $s_l$, this implies that the value of the less sampled modules from state $s_k$ will probably be underestimated, as the estimator for $\hat{v}$ does not consider the additional training from state $s_l$. Consequently, this may “lock” the router in its selection (see also section 3.2 for a discussion of this problem) early on.

A possible solution to this problem – at least for RL algorithms with a value-based component – might be to use the Advantage instead of (Q)-values: $A_{\pi}(s, a) = Q_{\pi}(s, a) - V_{\pi}(s)$, as the value component compensates for the inductive bias built up by training all transformations. Put differently, the increase in return for the on-policy average return, even when effectively only training one transformation, is not captured by the Q-component, but instead by the value component of the router. This may keep the difference in Q-value between different transformations low enough to lock the router permanently into a particular transformation, thereby helping to overcome selection collapse.

4.2 Stochastic Reparameterization

When it comes to hard decision making in differentiable architectures, stochastic reparameterization was recently introduced as an important alternative to Reinforcement Learning. While earlier work on stochastic reparameterization focused on low-dimensional stochastic distributions, Maddison et al. [2016] and Jang et al. [2016] discovered that the concrete – or Gumbel Softmax – distribution allows to reparameterize $k$
dimensional distributions (we will refer to the corresponding decision making algorithm as “Gumbel”). Considering that these can be implemented as differentiable ‘layers’ in deep architectures, they appear to be the better choice for a routing networks. Maddison et al. [2016] already note that the concrete distribution and its reparameterization do not yield an unbiased estimate of the gradient. The REINFORCE estimator [Williams, 1992] for the gradients of the score function, on the other hand, is known to be unbiased (but has very high variance). Therefore two more techniques were introduced to estimate the gradient of discrete random variables. The first, REBAR [Tucker et al., 2017] compensates for REINFORCE’s variance by introducing a control variate based on the concrete distribution. The second, RELAX [Grathwohl et al., 2018], generalizes this for non-discrete and non-differentiable stochastic functions, and allows a neural network to model the control variate.

To better understand the relative performance of reparameterized approaches when compared to a reinforcement learning algorithm, we performed the following analysis: Given a known distribution as a policy \( \pi \) parameterized by \( \theta \) over a known reward function \( r \), we do not sample, but instead analytically compute the value of the score-function \( J(\theta) = E(r|\pi(\theta)) = r \cdot \pi(\theta) \), where \( \cdot \) denotes the inner product. We can continue by analytically computing the gradient for all parameters \( \theta \). We know that these gradients are the ground truth that policy gradient and reparameterization approaches approximate only. Relying on this ground-truth information, we can then approximate the same gradients \( \frac{\delta J}{\delta \theta} \) using REINFORCE, Gumbel and RELAX, and finally compute the average difference between the ground truth values and the approximations.

For Figure 9, we use this approach to compute both the average gradient differences and the average variances over all parameters. More specifically, we initialize a random reward function (where each reward is uniformly sampled from \([0, 1]\), of dimensionality \( k \). We also randomly initialize a policy of dimensionality \( k \), parameterized by \( \theta \). After computing the ground truth gradient for a given pair of reward function and policy, we use the same reward function and policy to sample the gradients for \( \theta \) \( 22 \times k \) times (so that on average each action will be sampled equally often, even with increasing dimensionality). For each \( k \), we compute and approximate the gradients for 22 reward and 22 policy values, totalling over \( 10000 \times k \) datapoints for each point in Figure 9.

Figure 9 shows the mean squared error between the ground-truth gradient values and the sampled values using reparameterization and different RL policy gradient algorithms on top, and the corresponding variances on the bottom. While the gradients estimated by the Gumbel softmax trick are of much lower variance, they are also biased, with an average MSE larger than the MSE of the Policy Gradient algorithms. This is consistent with the analysis in [Maddison et al., 2016]. As for RELAX, we found very low variance for high dimensionalities, but – interestingly enough – a much higher MSE than REINFORCE and even than Gumbel, suggesting a higher bias. However, this may stem from the problem that RELAX relies on a trained surrogate network, which is difficult to train for these single-sample experiments. While we try to accommodate for this requirement by updating this network over multiple samples first, this might not suffice to fully initialize RELAX. However, as we will show in Section 5, where RELAX and its surrogate network are trained over millions of iterations, it is still very difficult to draw clear conclusions about how reparameterization techniques relate to REINFORCE based approaches in practice.
4.3 Simultaneously Selecting Multiple Function Blocks

While in principle a routing network that only chooses a single function block at each step is capable of learning any function, it could be useful for sample efficiency to combine the output of multiple parallel routing paths. One popular approach for implementing this idea is to use a sparse version of the mixtures of experts architecture as in [Shazeer et al., 2017, Ramachandran and Le, 2019]. This approach leverages a typical mixtures of experts gating network that combines the output of multiple experts using a weighted averaging procedure. However, in general we would like to have an even more expressive mechanism of combining the output from multiple parallel routing paths that can represent more complex relationships between the output of each path. As sparse mixtures of experts architectures only use the top K experts at each step, there is also an inherent exploitation and exploration dilemma that impacts the system despite the fact that is not modeled explicitly. As a result, sparse mixtures of experts architectures must include special procedures for adding noise to the system and load balancing to achieve strong performance [Shazeer et al., 2017]. In order to arrive at a general purpose solution, it makes more sense to model the selection of a subset of experts as an explicit reinforcement learning problem. For example, in [Bengio et al., 2015] each "expert" is gated by a Boolean routing decision that is modeled as a reinforcement learning problem.

4.4 Training

Training a routing network is illustrated in Figure 10 and the corresponding algorithm is Algorithm 2. The core idea is that the training of the router and of the modules happens simultaneously, after completing an episode, i.e., the forward pass. After the network has been assembled in the forward pass, the output of the network is translated into a loss for the module parameters and a final reward for a reinforcement learner. That reward, in combination with any accumulated per-action rewards, can be used to define a training loss for the router, either a Bellman Error, a negative log probability loss or some other loss function used to train a decision maker. The resulting losses can be added, and then backpropagated along the decision making parameters to define a gradient for each parameter in the model. Backpropagating along the sum of the losses allows for higher mini-batch parallelization in the update process of the network.

Algorithm 2: Backward step

Training a routing network is illustrated in Figure 10 and the corresponding algorithm is Algorithm 2. The core idea is that the training of the router and of the modules happens simultaneously, after completing an episode, i.e., the forward pass. After the network has been assembled in the forward pass, the output of the network is translated into a loss for the module parameters and a final reward for a reinforcement learner. That reward, in combination with any accumulated per-action rewards, can be used to define a training loss for the router, either a Bellman Error, a negative log probability loss or some other loss function used to train a decision maker. The resulting losses can be added, and then backpropagated along the decision making parameters to define a gradient for each parameter in the model. Backpropagating along the sum of the losses allows for higher mini-batch parallelization in the update process of the network.

SGD Finally, a gradient descent style algorithm can use these gradients to derive a new set of parameter values. However, it is worth noticing that routing networks can be highly sensitive to the choice of optimization algorithm. We will discuss this further in Section 5.

Exploratory Actions Another useful change to the training procedure is to limit the updates of the transformations if they were chosen by an exploratory action. The intuition is that we do not want the network to add interference to the training of modules if they were just evaluated and found not fitting to a particular
sample. As, however, any exploratory action has an effect on any return from the entire trajectory, we simply squash the optimization step size of the modules for the particular trajectory using the following formula:

$$\alpha = \left(1 - \frac{\#\text{exploratory actions}}{\text{trajectory length}}\right)^\kappa$$

where \(\alpha\) is factor to the learning rate, and \(\kappa\) is a hyperparameter. For \(\kappa = 0\), exploratory actions will be treated no differently, while for a very large \(\kappa\), the transformations are effectively not trained on the entire trajectory if even only one action was taken non-greedily.

**Splitting training data** One of the challenges of training a routing network is overfitting (see Section 3.3 for a thorough explanation). To prevent this, we investigate splitting the training data into a part for training the transformations, and a part to train the router.

### 4.5 Architectures

**Model Architectures** In general, any machine learning model can be routed. However, for non-layered architectures, routing collapses to the better investigated model selection problem. For layered architectures, any single layer can be routed by creating parallel copies of the respective layer, each with different (hyper)parameters. Existing routing architectures have included routing several fully connected layers with identical hyperparameters but different parameters [Rosenbaum et al., 2017, Kirsch et al., 2018, Chang et al., 2019, Cases et al., 2019], routing entire convolutional networks [Kirsch et al., 2018], routing the hidden to hidden transformation of recurrent neural architectures [Kirsch et al., 2018, Cases et al., 2019], routing the input to hidden transformation [Cases et al., 2019]; and routing word representations [Cases et al., 2019]. However, only Ramachandran and Le [2019] have studied the effect of routing among modules that have different architectures.

**Router Architectures** In the conceptually simplest version used by Chang et al. [2019], Kirsch et al. [2018], Ramachandran and Le [2019] and unsuccessfully tried by Rosenbaum et al. [2017], there is only one router, that learns to make all required decisions (compare Figure 11(a)). This router’s statespace contains the possible space of all activations, including the input activation. However, it requires additional work to stabilize – curriculum learning for Chang et al. [2019], separate grouping for Kirsch et al. [2018] and soft-routing for Ramachandran and Le [2019]. Rosenbaum et al. [2017] introduce two other interesting router architectures that consist of multiple subrouters. The first is assigning one subrouter to each decision problem (see Figure 11(b)). Consequently, each subrouter has a statespace constrained to the activations possible at the respective depth. In general, this approach has the disadvantage that it only allows a recursion depth not deeper than the number of subrouters defined. However, it is an effective way to implement routing
architectures where the modules available at different timesteps have to be different\textsuperscript{2}. The second option discussed in [Rosenbaum et al., 2017] is what they call a “dispatched” routing network (compare Figure 11(c)). This hierarchical configuration has an extra preceding subrouter with the interesting task to assign – or cluster – samples in input space first, before assigning the sample to be routed to one of a set of parallel subrouters, each of which exclusively works in activation space.

Another routing architecture design choice is the available action space. One already discussed option – particularly relevant for fully recursive routing models – is to include a “termination” action to stop routing and forward the last activation. This termination action, is not required for per-decision router designs (Figure 11(b)), but could be implemented if model constraints permit. Another one, introduced by Rosenbaum et al. [2017] for per-decision routing networks, is to include a “skip” action that does not terminate routing, but instead simply skips one sub-router. These two actions can result in identical behavior for limited-depth routing networks. In practice, dividing the decision problem over multiple subrouters, each with only a subset of actions and states to learn, can make training the router considerably easier. In particular in early stages of training, the problem of training a policy on modules that are similarly untrained can make fully recursive, single subrouter routing models hard to train. We will discuss this – and related problems – in more detail in the following section.

5 Evaluation

For evaluation, we consider two different domains: image classification and natural language inference. For image classification, we follow the architecture of Rosenbaum et al. [2017], i.e., we route the fully connected layers of a simple convolutional network with three $3 \times 3$ convolutional layers. For natural language inference, we follow the successful architecture by Cases et al. [2019], i.e., we route the word projections of a standard sentence to sentence comparison architecture.

Following the general architectures choices described in Section 4.5, we try to do each experiment twice. One experiment relies on meta-information, i.e., task-labels, using a task-wise dispatched architecture, where each task is assigned to a separate subrouter which only routes based on meta-information and stores its policy in a table. The other experiment covers architectures without a dispatching subagent that route without any meta-information based on input sample information and consecutive activations.

For image classification experiments, we use CIFAR 100, as it has predefined ‘tasks’ in form of its ‘coarse’ label structure, allowing us to naturally implement routing networks relying on meta-information. All experiments try to predict the ‘fine’ label in the context of the coarse label, i.e., the problem is five-way classification. All language inference experiments are on the Stanford Corpus of Implicatives [Cases et al., 2019], which is a three-way classification task. For experiments relying on meta-information, we use the provided ‘signatures’ as task-labels.

All results shown in this section are results on test datasets. The entropy plots show the entropy of the selection distribution over the entire dataset, also at test time. As most of the results are meant to be qualitative in nature, we did not do extensive hyperparameter searches, and we do expect better results to be found. As we will show in the following section, Q-Learning is consistently among the best performing decision making algorithms. Thus, unless otherwise noted, all plots utilize Q-Learning.

\textsuperscript{2}This can result as a consequence of e.g., dimensionality constraints; other approaches to solve this problem may include solutions where the agent, if it chooses an incompatible action, is heavily penalized and the episode ends immediately. We assume that several existing approaches also use separate approximations to deal with these dimensionality problems, though they do not mention this.
5.1 Decision Making Strategies

In this section, we evaluate different decision making strategies. Evaluated strategies include reparameterization strategies and several reinforcement learning algorithms.

5.1.1 Learning with meta-information

Figure 12: Multi-task results for different decision making strategies

Figure 12 shows results for different decision making algorithms when relying on meta-information. The starkest result is that the policy gradient based approaches, including the related reparameterization algorithms – Gumbel and RELAX, are consistently outperformed by value-based reinforcement learning based approaches. As can be seen when comparing Figures 12(a) with (b), this difference grows with routing depth – i.e., number of routed layers. We stipulate that this difference results from the effect exploration has on interference, as discussed in section 3.2. In contrast to policy gradient strategies, \( \epsilon \)-greedy strategies are guaranteed to interfere with another transformation, even of near-identical value, only a fraction of the time purely determined by \( \epsilon \). This also explains the best performing policy gradient based approach, the weighted policy learner (WPL) [Abdallah and Lesser, 2006], which was already successfully tested in the routing multi-agent setting of Rosenbaum et al. [2017]. WPL is a non-standard policy gradient algorithm (in that it does not use the REINFORCE log-probability trick) that was explicitly designed for stochastic games, and that has specific properties to emphasize exploitation even for similar-value actions. This effectively lowers its exploration and thereby its interference.

In Figure 12(c), the language inference experiments, it is apparent how different algorithms stabilize (or not) over time. As for CIFAR, the value-based approaches Q-Learning and Advantage learning have a clear edge over the policy gradient based approaches. It is particularly interesting to see how both algorithms have nearly the same learning behavior for the first 20 epochs, until Advantage learning, and 20 epochs later, Q-Learning, apparently stabilize to then quickly leave the other algorithms behind. We speculate that the benefit of Advantage learning stems from the argument in Section 4.1.3, as it is able to offset the general increase in value of the different transformations.

5.1.2 Learning without meta-information

Routing decisions that do not rely on meta-information rely on the activation at the input to the routed layer instead. That is, they only consider the activation produced by the previous layer, which may or may not be routed, and which may even be the input. This allows the most fine-grained control over the routing path, as – possibly – each sample may be routed through a different path. The most straightforward implementation is a ‘single router’ architecture depicted in Figure 11(a), where the router consists of only one subrouter – one parameterization that gets passed in activations from any layer. This also allows arbitrary depth routing networks, as the router may decide to apply an arbitrary number of transformations before...
stopping. Unfortunately, this complicates the routing process in at least two ways. The first is that the subrouter does not only need to learn where to route based on an activation alone, but even needs to do so for activations that may have been produced at completely different steps in the routing network. This makes the distribution of activations the router will have to decide on dramatically more difficult for the router to interpret, as it is likely that each ‘depth’ of activations adds another mode to the distribution. The second, related, reason is that the activations are highly volatile, as any change to the subrouter’s policy may dramatically transform the distribution of activations, making the modes non-stationary and even more difficult to disentangle. For illustration, consider a simple single router model where the router can select from \{t_1, t_2, t_3\}. At a given training time, the router only selects \(t_1\) or \(t_2\). When an update changes the router to use \(t_3\) instead of \(t_2\), the space of activations will now have been created by \(\{t_1, t_3\}\), instead of by \(\{t_1, t_2\}\). It is obvious how this can ‘confuse’ a router, in particular when this non-stationarity is combined with the already existing non-stationarity produced by updating the transformations.

Consequently, performance on both CIFAR and SCI, as depicted in Figure 13 is basically the same as random. For the results on language inference in Figure 13(b), the routing problem becomes so complex that the router even picks a fourth class for language inference (which generally only has three) that only exists for implementation reasons, thereby consistently achieving 0% accuracy instead of the 33% of the random baseline.

To investigate the problem posed by these results, we additionally experiment with two more architectures not relying on meta-information. In the first, we fix the depth for the single router architecture, and in the second, we design a per-layer subrouter architecture depicted in Figure 11(b). Other than the single router architecture used for the experiments in Figures 13, this architecture does not have one approximation network over all routing layers, of which there may be an arbitrary number, but instead only makes (at most) \(k\) decisions, with a separate subrouter for each layer. As shown in Figure 14(a), fixing the routing depth does help to stabilize the training for some algorithms. As with other experiments, the (Q-)value based approaches start learning, but, more surprisingly, RELAX is able to stabilize, although at the cost of complete collapse. We assume that in this highly volatile environment the rich gradient information provided by RELAX can help the most. In Figure 14, we show results for a separate subrouter for each layer, thereby limiting the maximum number of applied transformations to 3 (each subrouter is able to terminate earlier). This makes the decision making problem easier so that some algorithms are able to stabilize. However, most policy gradient approaches, including RELAX, collapse to achieve this stability, while the remaining policy gradient
algorithms, WPL and Gumbel, do not achieve noteworthy performance. Only Q-Learning and Advantage learning learn while maintaining selection entropy. Interestingly, the router apparently does not learn to completely minimize interference, as it does not achieve non-routed performance, not even when it collapses. It should be noted, though, that even for algorithms that successfully stabilize, the solutions found are local optima of very bad performance. For both the results in Figure 14, the final performance stays about 30% below the performance achieved by models relying on meta-information.

These results strongly suggest that routing networks – and quite probably any other kind of approach to compositional computation – have difficulty overcoming the initial instability of the training process, if they are not provided with a strong external signal. One such signal, as discussed in the previous section, are task-labels or other pieces of meta-information that allow the routing network to find paths at the dimensionality of the meta-information, which tends to be much smaller than the full space of activations. Another approach, as introduced by Chang et al. [2019], is to carefully curate the order in which samples are provided to the network. This, also, drastically limits the complexity of the decision problem, as only ‘similar’ samples are shown at any given time during training, but relies on such an order to exist for a given dataset.

5.1.3 Reparameterization Techniques and Exploration Strategies

In general, the results for reparameterized routing, i.e., using Gumbel and RELAX, are very similar to the results for policy gradient approaches. We even found that for deeper architectures, the reparameterization techniques suffer from the same decrease in performance as other PG algorithms, as shown in Figure 12(b). As mentioned above, we assume that this stems from inferior exploration behavior for on-policy stochastic sampling. To verify, we designed a version of REINFORCE that samples actions using an \( \epsilon \)-greedy policy, i.e., that takes the best action \( \epsilon \) of the time, and that samples from the actual policy \( 1 - \epsilon \) of the time. When training, we compensate for the difference in sampling and training policies using importance sampling [Precup et al., 2000]. As shown in Figure 15, this indeed changes the behavior of REINFORCE to act more like a value-based approach. These results suggest that routing may greatly benefit from a targeted decision making algorithm. In particular exploration, with its added complexity of causing interference, seems to be a promising direction for future research. For example, it may be useful to consider algorithms that have separate exploitation and exploration policies, along the lines of Garcia and Thomas [2019], or algorithms that can incorporate more complex exploration mechanics into reparameterization techniques.

5.2 Reward Design

Figure 16 shows results for different final reward functions. In general, the correct/incorrect final reward strategy, \( \pm 1 \) for correct and incorrect classification, appears clearly superior to the negative classification (cross-entropy) loss reward \( r_f = -\mathcal{L}(\hat{y}, y) \). While this seems initially surprising, as the negative loss reward contains more information, we believe that this is exactly what makes learning more difficult, for two reasons. First, a negative classification loss may overemphasize outliers, as, relatively to other samples, it may add a much larger part to the total loss. While this may be useful for supervised learning, a reinforcement learning router may update to accommodate these samples at the cost of other, non-outlyer samples.

\[ \text{We should also note that exploration for the Q-Learning experiments is very high, with over 0.4 for the first 5 epochs, which suggests that the amount of exploration may play a role, but that the exploitation strategy dominates the results.} \]
Second, as suggested by the high fluctuation in the learning on SCI, the finer granularity of the negative classification loss reward may reduce the difference between the value of different transformations, resulting in even small updates changing the greedy strategy. As this reduces stability, it will also decrease overall performance.

Figure 17 shows plots for different intermediate reward values. These rewards are computed as a fraction of the overall probability of choosing a particular transformation. Positive values are expected to increase transfer and lower entropy, while negative values are expected to decrease interference and increase entropy. Comparing the results for CIFAR in Figure 17(a) with the results for SCI in Figure 17(b) it becomes apparent that the domain – or the architecture – plays a major role in the effect of this regularization reward. While the reward has no discernable effect on CIFAR, it dramatically changes the convergence behavior – if not the final performance – on SCI. Interestingly, negative reward values, meant to increase diversity, appear to stabilize learning as the model learns much faster, but have no effect on the routing entropy. While a complete interpretation of this result is very difficult, we speculate that this results from the higher potential for interference on SCI, and maybe even on language domains in general. The potential for interference is higher when training on SCI because the effective input dimensionality is nearly an order of magnitude lower than it is for CIFAR, which leads to a larger average overlap between examples in the input space. Additionally, as is also the case for us here, models used for NLP tend to use smaller hidden representations than computer vision models, resulting in a larger average overlap between examples in the activation space as well. This would not only explain why ‘pushing’ the router to diversify stabilizes learning, but also why the results with the negative loss reward function have such a high variance, as any change in routing decision may end up with a much higher amount of interference.

These results suggest that future research should consider different new reward functions. In particular, it could be worthwhile to find a final reward function that can rely on the information contained in the negative loss, but that is less susceptible to its problems. Additionally, it would be interesting to investigate an adaptive intermediate reward that incentivizes diversity as long as it is needed for stability, but that eventually anneals to zero, so that the router only optimizes for the overall model performance.

5.3 Other Design Choices

Figure 18 shows the effect that lowering the training of transformations chosen non-greedily has. As one can see, $\kappa$ has very little effect on the overall performance and only mild effect on the entropy.
Splitting the training set into samples to train the transformations and samples to train the router, on the other hand, has a clear effect on the performance, as shown in Figure 19. Here, the curves show the percentage of the data used to train the transformations. As one can see, using the full data benefits both performance and entropy.

More interesting is Figure 20. As already reported by Rosenbaum et al. [2017], Cases et al. [2019], routing becomes unstable for many optimizers, and consistently yields the best performance for ‘plain’ SGD. We stipulate that similar problems can be observed for any architecture with an adaptive computation graph. Consider a simple example, where we route a sample \(x\) through a two-layer routing network. The first routing decision can choose from transformations \(\{t_1, t_2\}\) and the second from \(\{t_2, t_1\}\). Now consider the gradients for \(t_1, t_2\) over two different routing paths, \(t_1(t_2(x))\) and \(t_2(t_1(x))\). It is obvious that for those two paths, \(t_2, t_1\) and \(t_1, t_2\) may yield vastly different activations, and thereby vastly different inputs to \(t_1, t_2\). If an optimizer relies on parameter-specific approximations, such as, e.g., momentum, an approximation for \(t_2, t_1\) may be completely incompatible with \(t_1, t_2\), thereby making training difficult, or even impossible. This explains why plain optimization strategies that do not compute parameter-specific information generally do better in the context of dynamic computation graphs.

### 5.4 Stability

As we argued before, stability is a consequence of the routing ‘chicken-and-egg’ problem: Upon initialization of a routing network, both the modules and the router do not yet have any information on the problem, and act randomly. The router cannot stabilize, as it cannot discern which selected module caused any increase in performance, and the modules cannot stabilize as they are trained with samples and activations so different that interference can destroy any learning that may happen. This, in turn, may destroy any progress the router may have made with the credit assignment. This problem is never worse than for the ‘single router’ architecture (compare Figure 11), for the reasons described in Section 5.1.2. Consequently, a routing network may fail to learn anything, as depicted in Figure 13.

### 5.5 Module Collapse

Figure 14 already showed how different router training algorithms can lead to collapse in different domains. Additionally, consider Figure 21, where the experiment is on CIFAR with a dispatched architecture\(^4\). For this architecture, collapse is not a consequence of the routing algorithm, but of the general architecture, as all algorithms lead to collapse. However, in difference to the results in Figure 14, the results achieved are good, reaching standard non-routed performance.

\(^4\)The same fc layers are routed as in the other experiments. However, the dispatching action is based on the activation after the convolutional layers. The dispatched subrouters are tabular, and do not consider the intermediate activations.
This is a not surprising result, as collapse will stabilize the router, and as there are no later activations to consider. This is reflected by the test-time selection entropy of nearly all algorithms going to zero within ten epochs. Surprisingly, this extends to the stochastic reparameterization algorithms Gumbel and RELAX which do not rely purely on rewards, further establishing that in the context of routing, Gumbel and RELAX behave ‘just as’ any other PG algorithm.

The only algorithms that do not collapse completely are WPL and Advantage learning. We assume that WPL does not collapse as much as it was specifically designed for non-stationary returns, and that Advantage learning performs well as a consequence of the argument put forth in 4.1.3.

5.6 Overfitting

As the main reference architectures for this section – routing the classifier of a convolutional network, and routing the word representations of a natural language inference model – were chosen because of their performance, they overfit only little.

However, if we consider an sequence-to-sequence architecture for language inference with a dispatched routed classifier, we can show how routing can lead a model to overfit. Consider Figure 22, which shows from top to bottom the test accuracy, train accuracy and test entropy on SCI. While both a basic, non-routed network and the routed network easily reach perfect train accuracy (> 99.5%), the routing architecture starts flattening out even earlier than the basic architecture, reaching accuracy around 10% lower than the basic model, and over 20% lower than the routed model.

As discussed in section 3.3, overfitting is less of a problem in the presence of metainformation, as the router can ignore spurious activations in these cases. However, as the goal of modular architectures is to adaptively modularize without any kind of external information guiding the composition, future work should investigate how routing architectures can be regularized to achieve good generalization properties.

6 Conclusion

Summary of Results: Considering the results presented in this paper, it becomes clear how much of the performance of a routing network still depends on design- and hyperparameter decisions. However, many other results are also clear:

- In the context of routing, reparameterization techniques behave similar to RL policy gradient approaches, and have oftentimes even identical performance and selection behavior.
- All policy gradient approaches, including reparameterization techniques, fall short compared to value-based learning. We established that the problem of PG approaches is their exploitation strategy.
• Routing networks often need externally provided structure to properly stabilize and to achieve maximal performance given typical dataset sizes today. This structure may come in form of meta-information, or as a guided curricula of training samples.
• We evaluated the role that the reward design has on training reinforcement learning routers, observing that simple rewards tend to perform better than high information rewards that may be more difficult to interpret.
• The choice of optimization algorithm has a huge impact on the overall stability of routing networks, and presumably on any kind of compositional model of learning. Here, modern, more sophisticated algorithms can fail completely, with a simple SGD update performing the best.
• We investigated each of the challenges introduced and discussed in Section 3, and illustrated how different design decisions can lead to instability, to collapse, and how the high expressivity of a routing network can lead to overfitting.
• We additionally identified a dilemma of flexibility for modular learning. This arises out of a need to balance the flexibility (or locality) of modular approaches to avoid both collapse and overfitting.

Open Questions: Research into compositional architectures has accelerated in recent years. In this area, routing, as a general formulation of functional composition relying on trainable modules, can provide good insights into the challenges ahead. Stability, selection collapse, overfitting, mathematical justifications and learning over different architectures may only be some of the challenges that need to be solved before a fully compositional and modular architecture that is able to quickly adapt to any new problem, task, or context can be designed. With this paper we hope to contribute an overview that is useful for establishing these problems within the research community and lay out some future steps. Moreover, our analysis in this paper reveals that decision making strategies for routing, different routing architectures, and new reward design strategies seem to be very promising directions for future research that have the potential to lead to significant improvements in general purpose models with compositional architectures.
References

Abdallah, S. and V. Lesser
2006. Learning the task allocation game. In *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems*, Pp. 850–857. ACM.

Aertsen, A., G. Gerstein, M. Habib, and G. Palm
1989. Dynamics of neuronal firing correlation: modulation of" effective connectivity". *Journal of neurophysiology*, 61(5):900–917.

Alet, F., T. Lozano-Pérez, and L. P. Kaelbling
2018. Modular meta-learning. *CoRR*, abs/1806.10166.

Aljundi, R., J. Chakravarty, and T. Tuytelaars
2017. Expert gate: Lifelong learning with a network of experts. In *Proceedings CVPR 2017*, Pp. 3366–3375.

Andreas, J., M. Rohrbach, T. Darrell, and D. Klein
2015. Deep compositional question answering with neural module networks. *CoRR*, abs/1511.02799.

Bacon, P.-L., J. Harb, and D. Precup
2017. The option-critic architecture. *AAAI*.

Baker, B., O. Gupta, N. Naik, and R. Raskar
2017. Designing neural network architectures using reinforcement learning. *ICLR*.

Bechtel, W. and A. Abrahamsen
2002. *Connectionism and the mind: Parallel processing, dynamics, and evolution in networks*. Blackwell Publishing.

Bechtel, W. and R. C. Richardson
2010. *Discovering Complexity: Decomposition and Localization as Strategies in Scientific Research*. Mit Press.

Bender, G., P.-J. Kindermans, B. Zoph, V. Vasudevan, and Q. Le
2018. Understanding and simplifying one-shot architecture search. In *International Conference on Machine Learning*, Pp. 549–558.

Bengio, Y., N. Léonard, and A. C. Courville
2013. Estimating or propagating gradients through stochastic neurons for conditional computation. *CoRR*, abs/1308.3432.

Bengio, Y., J. Louradour, R. Collobert, and J. Weston
2009. Curriculum learning. In *Proceedings of the 26th annual international conference on machine learning*, Pp. 41–48. ACM.

Brock, A., T. Lim, J. M. Ritchie, and N. Weston
2017. SMASH: one-shot model architecture search through hypernetworks. *CoRR*, abs/1708.05344.

Buschman, T. J. and E. K. Miller
2010. Shifting the spotlight of attention: evidence for discrete computations in cognition. *Frontiers in human neuroscience*, 4.

Cases, I., C. Rosenbaum, M. Riemer, A. Geiger, T. Klinger, A. Tamkin, O. Li, S. Agarwal, J. D. Greene, D. Jurafsky, C. Potts, and L. Karttunen
2019. Recursive routing networks: Learning to compose modules for language understanding. In
Routing Networks and the Challenges of Modular and Compositional Computation

Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers).

Chang, M., A. Gupta, S. Levine, and T. L. Griffiths
2019. Automatically composing representation transformations as a means for generalization. In International Conference on Learning Representations.

Cortes, C., X. Gonzalvo, V. Kuznetsov, M. Mohri, and S. Yang
2016. Adanet: Adaptive structural learning of artificial neural networks. arXiv preprint arXiv:1607.01097.

Davis, A. and I. Arel
2013. Low-rank approximations for conditional feedforward computation in deep neural networks. arXiv preprint arXiv:1312.4461.

Engel, A. K., P. Fries, and W. Singer
2001. Dynamic predictions: oscillations and synchrony in top–down processing. Nature Reviews Neuroscience, 2(10):704.

Eysenbach, B., A. Gupta, J. Ibarz, and S. Levine
2018. Diversity is all you need: Learning skills without a reward function. arXiv preprint arXiv:1802.06070.

Farah, M. J.
1994. Neuropsychological inference with an interactive brain: A critique of the "locality" assumption. Behavioral and Brain Sciences, 17(1), 43-104.

Fernando, C., D. Banarse, C. Blundell, Y. Zwols, D. Ha, A. A. Rusu, A. Pritzel, and D. Wierstra
2017. Pathnet: Evolution channels gradient descent in super neural networks. arXiv preprint arXiv:1701.08734.

Florensa, C., Y. Duan, and P. Abbeel
2017. Stochastic neural networks for hierarchical reinforcement learning. arXiv preprint arXiv:1704.03012.

Fodor, J. A.
1975. The Language of Thought. Harvard University Press.

Fodor, J. A.
1983. The Modularity of Mind. MIT Press.

Fodor, J. A. and Z. W. Pylyshyn
1988. Connectionism and cognitive architecture: A critical analysis. Cognition, 28(1-2):3–71.

Fries, P.
2005. A mechanism for cognitive dynamics: neuronal communication through neuronal coherence. Trends in cognitive sciences, 9(10):474–480.

Garcia, F. M. and P. S. Thomas
2019. A meta-mdp approach to exploration for lifelong reinforcement learning. CoRR, abs/1902.00843.

Grathwohl, W., D. Choi, Y. Wu, G. Roeder, and D. Duvenaud
2018. Backpropagation through the void: Optimizing control variates for black-box gradient estimation. In International Conference on Learning Representations.

Gregor, K., D. J. Rezende, and D. Wierstra
2016. Variational intrinsic control. arXiv preprint arXiv:1611.07507.

Gurney, K., T. J. Prescott, and P. Redgrave
2001. A computational model of action selection in the basal ganglia. i. a new functional anatomy. Biological cybernetics, 84(6):401–410.
Routing Networks and the Challenges of Modular and Compositional Computation

Harutyunyan, A., W. Dabney, D. Borsa, N. Heess, R. Munos, and D. Precup
2019. The termination critic. *arXiv preprint arXiv:1902.09996*.

Hausman, K., J. T. Springenberg, Z. Wang, N. Heess, and M. Riedmiller
2018. Learning an embedding space for transferable robot skills. In *International Conference on Learning Representations*.

Hay, N., S. Russell, D. Tolpin, and S. E. Shimony
2014. Selecting computations: Theory and applications. *arXiv preprint arXiv:1408.2048*.

Jacobs, R. A., M. I. Jordan, and A. G. Barto
1991a. Task decomposition through competition in a modular connectionist architecture: The what and where vision tasks. *Cognitive Science*, 15(2):219 – 250.

Jacobs, R. A., M. I. Jordan, S. J. Nowlan, and G. E. Hinton
1991b. Adaptive mixtures of local experts. *Neural computation*, 3(1):79–87.

Jang, E., S. Gu, and B. Poole
2016. Categorical reparameterization with gumbel-softmax. *arXiv preprint arXiv:1611.01144*.

Jordan, M. I. and R. A. Jacobs
1994. Hierarchical mixtures of experts and the em algorithm. *Neural computation*, 6(2):181–214.

Kell, A. J., D. L. Yamins, E. N. Shook, S. V. Norman-Haignere, and J. H. McDermott
2018. A task-optimized neural network replicates human auditory behavior, predicts brain responses, and reveals a cortical processing hierarchy. *Neuron*, 98(3):630 – 644.e16.

Kirsch, L., J. Kunze, and D. Barber
2018. Modular networks: Learning to decompose neural computation. In *Advances in Neural Information Processing Systems*, pp. 2414–2423.

Kostas, J., C. Nota, and P. S. Thomas
2019. Reinforcement learning without backpropagation or a clock. *arXiv preprint arXiv:1902.05650*.

Liang, J. Z., E. Meyerson, and R. Miikkulainen
2018. Evolutionary architecture search for deep multitask networks. *CoRR*, abs/1803.03745.

Liu, C., B. Zoph, M. Neumann, J. Shlens, W. Hua, L.-J. Li, L. Fei-Fei, A. Yuille, J. Huang, and K. Murphy
2018. Progressive neural architecture search. In *The European Conference on Computer Vision (ECCV)*.

Maddison, C. J., A. Mnih, and Y. W. Teh
2016. The concrete distribution: A continuous relaxation of discrete random variables. *arXiv preprint arXiv:1611.00712*.

Marcus, G. F.
2001. *The Algebraic Mind*. MIT Press.

Miikkulainen, R.
1993. *Subsymbolic natural language processing - an integrated model of scripts, lexicon, and memory*, Neural network modeling and connectionism. MIT Press.

Miikkulainen, R., J. Liang, E. Meyerson, A. Rawal, D. Fink, O. Francon, B. Raju, A. Navruzyan, N. Duffy, and B. Hodjat
2017. Evolving deep neural networks. *arXiv preprint arXiv:1703.00548*.

Misra, I., A. Shrivastava, A. Gupta, and M. Hebert
2016. Cross-stitch networks for multi-task learning. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 3994–4003.
Pham, H., M. Y. Guan, B. Zoph, Q. V. Le, and J. Dean  
2018. Efficient neural architecture search via parameter sharing. *arXiv preprint arXiv:1802.03268.*

Precup, D., R. S. Sutton, and S. P. Singh  
2000. Eligibility traces for off-policy policy evaluation. In *Proceedings of the Seventeenth International Conference on Machine Learning*, Pp. 759–766. Morgan Kaufmann Publishers Inc.

Rajendran, J., P. Prasanna, B. Ravindran, and M. M. Khapra  
2017. ADAAPT: attend, adapt, and transfer: Attentative deep architecture for adaptive policy transfer from multiple sources in the same domain. *ICLR*, abs/1510.02879.

Ramachandran, P. and Q. V. Le  
2019. Diversity and depth in per-example routing models. In *International Conference on Learning Representations*.

Rice, J. R.  
1976. The algorithm selection problem. In *Advances in computers*, volume 15, Pp. 65–118. Elsevier.

Riemer, M., I. Cases, R. Ajemian, M. Liu, I. Rish, Y. Tu, and G. Tesauro  
2019. Learning to learn without forgetting by maximizing transfer and minimizing interference. In *International Conference on Learning Representations (ICLR)*.

Riemer, M., M. Liu, and G. Tesauro  
2018. Learning abstract options. In *Advances in Neural Information Processing Systems*, Pp. 10424–10434.

Riemer, M., A. Vempaty, F. Calmon, F. Heath, R. Hull, and E. Khabiri  
2016. Correcting forecasts with multifactor neural attention. In *International Conference on Machine Learning*, Pp. 3010–3019.

Rosenbaum, C., T. Klinger, and M. Riemer  
2017. Routing networks: Adaptive selection of non-linear functions for multi-task learning. *CoRR*, abs/1711.01239.

Ruder, S., J. Bingel, I. Augenstein, and A. Søgaard  
2017. Sluice networks: Learning what to share between loosely related tasks. *arXiv preprint arXiv:1705.08142*.

Salinas, E. and T. J. Sejnowski  
2001. Correlated neuronal activity and the flow of neural information. *Nature reviews neuroscience*, 2(8):539.

Shallice, T.  
1988. *From neuropsychology to mental structure*. Cambridge University Press.

Shazeer, N., A. Mirhoseini, K. Maziarz, A. Davis, Q. V. Le, G. E. Hinton, and J. Dean  
2017. Outrageously large neural networks: The sparsely-gated mixture-of-experts layer. *CoRR*, abs/1701.06538.

Siegel, M. and P. König  
2003. A functional gamma-band defined by stimulus-dependent synchronization in area 18 of awake behaving cats. *Journal of Neuroscience*, 23(10):4251–4260.

Smolensky, P.  
1988. On the proper treatment of connectionism. *Behavioral and Brain Sciences*, 11(1):1–23.

Stocco, A., C. Lebiere, and J. R. Anderson  
2010. Conditional routing of information to the cortex: A model of the basal ganglia’s role in cognitive coordination. *Psychological review*, 117(2):541.
Stollenga, M. F., J. Masri, F. Gomez, and J. Schmidhuber
2014. Deep networks with internal selective attention through feedback connections. In Advances in Neural Information Processing Systems 27, Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, eds., Pp. 3545–3553. Curran Associates, Inc.

Sutton, R. S. and A. G. Barto
1998. Introduction to Reinforcement Learning, 1st edition. Cambridge, MA, USA: MIT Press.

Sutton, R. S., D. Precup, and S. Singh
1999. Between mdps and semi-mdps: A framework for temporal abstraction in reinforcement learning. Artificial intelligence, 112(1-2):181–211.

Thomas, P. S.
2011. Policy gradient coagent networks. In Advances in Neural Information Processing Systems, Pp. 1944–1952.

Thomas, P. S. and A. G. Barto
2011. Conjugate markov decision processes. In Proceedings of the 28th International Conference on Machine Learning (ICML-11), Pp. 137–144.

Tiesinga, P., J.-M. Fellous, J. Jos, and T. Sejnowski
2002. Information transfer in entrained cortical neurons. Network: Computation in Neural Systems, 13(1):41–66.

Tononi, G., O. Sporns, and G. M. Edelman
1994. A measure for brain complexity: relating functional segregation and integration in the nervous system. Proceedings of the National Academy of Sciences, 91(11):5033–5037.

Touretzky, D. S. and G. E. Hinton
1988. A distributed connectionist production system. Cognitive Science, 12(3):423–466.

Tucker, G., A. Mnih, C. J. Maddison, and J. Sohl-Dickstein
2017. REBAR: low-variance, unbiased gradient estimates for discrete latent variable models. CoRR, abs/1703.07370.

Usrey, W. M. and R. C. Reid
1999. Synchronous activity in the visual system. Annual review of physiology, 61(1):435–456.

Williams, R. J.
1992. Simple statistical gradient-following algorithms for connectionist reinforcement learning. Machine learning, 8(3-4):229–256.

Zhang, C., S. Bengio, M. Hardt, B. Recht, and O. Vinyals
2016. Understanding deep learning requires rethinking generalization. CoRR, abs/1611.03530.

Zoph, B. and Q. V. Le
2017. Neural architecture search with reinforcement learning. ICLR.