AGI Safety From First Principles

Richard Ngo

September 2020

This report explores the core case for why the development of artificial general intelligence (AGI) might pose an existential threat to humanity. It stems from my dissatisfaction with existing arguments on this topic: early work is less relevant in the context of modern machine learning, while more recent work is scattered and brief. This report aims to fill that gap by providing a detailed investigation into the potential risk from AGI misbehaviour, grounded by our current knowledge of machine learning, and highlighting important uncertainties. It identifies four key premises, evaluates existing arguments about them, and outlines some novel considerations for each.

Contents

1 Introduction

The key concern motivating technical AGI safety research is that we might build autonomous artificially intelligent agents which are much more intelligent than humans, and which pursue goals that conflict with our own. Human intelligence allows us to coordinate complex societies and deploy advanced technology, and thereby control the world to a greater extent than any other species. But AIs will eventually become more capable than us at the types of tasks by which we maintain and exert that control. If they don't want to obey us, then humanity might become only Earth's second most powerful "species", and lose the ability to create a valuable and worthwhile future.

I'll call this the "second species" argument; I think it's a plausible argument which we should take very seriously.[1] However, the version stated above relies on several vague concepts and intuitions. In this report I'll give the most detailed presentation of the second species argument that I can, highlighting the aspects that I'm still confused about. In particular, I'll defend a version of the second species argument which claims that, without a concerted effort to prevent it, there's a significant chance that:

1. We'll build AIs which are much more intelligent than humans (i.e. superintelligent).
2. Those AIs will be autonomous agents which pursue large-scale goals.
3. Those goals will be misaligned with ours; that is, they will aim towards outcomes that aren't desirable by our standards, and trade off against our goals.
4. The development of such AIs would lead to them gaining control of humanity's future.

While I use many examples from modern deep learning, this report is also intended to apply to AIs developed using very different models, training algorithms, optimisers, or training regimes than the ones we use today. However, many of my arguments would no longer be relevant if the field of AI moves away from focusing on machine learning. I also frequently compare AI development to the evolution of human intelligence; while the two aren't fully analogous, humans are the best example we currently have to ground our thinking about generally intelligent AIs.

2 Superintelligence

In order to understand superintelligence, we should first characterise what we mean by intelligence. We can start with Legg and Hutter [2007]'s well-known definition, which identifies intelligence as the ability to achieve goals in a wide

[1] Stuart Russell also refers to this as the "gorilla problem" in his recent book, *Human Compatible* [Russell, 2019].

range of environments.[2] However, there are multiple ways to score highly on this metric. The key distinction I'll draw in this section is between agents that understand how to do well at many tasks because they have been specifically optimised for each task (which I'll call the task-based approach to AI), versus agents which can understand new tasks with little or no task-specific training, by generalising from previous experience (the generalisation-based approach).

2.1 Narrow and general intelligence

The task-based approach is analogous to how humans harnessed electricity: while electricity is a powerful and general technology, we still need to design specific ways to apply it to each task. Similarly, computers are powerful and flexible tools - but even though they can process arbitrarily many different inputs, detailed instructions for how to do that processing needs to be individually written to build each piece of software. Meanwhile our current reinforcement learning algorithms, although powerful, produce agents that are only able to perform well on specific tasks at which they have a lot of experience - Starcraft, DOTA, Go, and so on. Drexler [2019] argues that our current task-based approach will scale up to allow superhuman performance on a range of complex tasks (although I'm skeptical of this claim).[3]

An example of the generalisation-based approach can be found in large language models like GPT-2 and GPT-3. GPT-2 was first trained on the task of predicting the next word in a corpus, and then achieved state of the art results on many other language tasks, without any task-specific fine-tuning! [Radford et al., 2019] This was a clear change from previous approaches to natural language processing, which only scored well when trained to do specific tasks on specific datasets. Its successor, GPT-3, has displayed a range of even more impressive behaviour [Sotala, 2020]. I think this provides a good example of how an AI could develop cognitive skills (in this case, an understanding of the syntax and semantics of language) which generalise to a range of novel tasks. The field of meta-learning aims towards a similar goal.

We can also see the potential of the generalisation-based approach by looking at how humans developed. As a species, we were "trained" by evolution to have cognitive skills including rapid learning capabilities; sensory and motor processing; and social skills. As individuals, we were also "trained" during our childhoods to fine-tune those skills; to understand spoken and written language; and to possess detailed knowledge about modern society. However, the key point is that almost all of this evolutionary and childhood learning occurred on different tasks from the economically useful ones we perform as adults. We can perform well on the latter category only by reusing the cognitive skills and knowledge that we gained previously. In our case, we were fortunate that those

[2] Unlike the standard usage, in this technical sense an "environment" also includes a specification of the input-output channels the agent has access to (such as motor outputs), so that solving the task only requires an agent to process input information and communicate output information.

[3] For reasons outlined in Ngo [2019a].

cognitive skills were not too specific to tasks in the ancestral environment, but were rather very *general* skills. In particular, the skill of abstraction allows us to extract common structure from different situations, which allows us to understand them much more efficiently than by learning about them one by one. Then our communication skills and theories of mind allow us to share our ideas. This is why humans can make great progress on the scale of years or decades, not just via evolutionary adaptation over many lifetimes.

I should note that I think of task-based and generalisation-based as parts of a spectrum rather than a binary classification, particularly because the way we choose how to divide up tasks can be quite arbitrary. For example, AlphaZero trained by playing against itself, but was tested by playing against humans, who use different strategies and playing styles. We could think of playing against these two types of opponents as two instances of a single task, or as two separate tasks where AlphaZero was able to generalise from the former task to the latter. But either way, the two cases are clearly very similar. By contrast, there are many economically important tasks which I expect AI systems to do well at primarily by generalising from their experience with very different tasks - meaning that those AIs will need to generalise much, much better than our current reinforcement learning systems can.

Let me be more precise about the tasks which I expect will require this new regime of generalisation. To the extent that we can separate the two approaches, it seems plausible to me that the task-based approach will get a long way in areas where we can gather a lot of data. For example, I'm confident that it will produce superhuman self-driving cars well before the generalisation-based approach does so. It may also allow us to automate most of the tasks involved even in very cognitively demanding professions like medicine, law, and mathematics, if we can gather the right training data. However, some jobs crucially depend on the ability to analyse and act on such a wide range of information that it'll be very difficult to train directly for high performance on them. Consider the tasks involved in a role like CEO: setting your company's strategic direction, choosing who to hire, writing speeches, and so on. Each of these tasks sensitively depends on the broader context of the company and the rest of the world. What industry is their company in? How big is it; where is it; what's its culture like? What's its relationship with competitors and governments? How will all of these factors change over the next few decades? These variables are so broad in scope, and rely on so many aspects of the world, that it seems virtually impossible to generate large amounts of training data via simulating them (like we do to train game-playing AIs). And the number of CEOs from whom we could gather empirical data is very small by the standards of reinforcement learning (which often requires billions of training steps even for much simpler tasks). I'm not saying that we'll never be able to exceed human performance on these tasks by training on them directly - maybe a herculean research and engineering effort, assisted by other task-based AIs, could do so. But I expect that well before such an effort becomes possible, we'll have built AIs using the generalisation-based approach which know how to perform well even on these broad tasks.

In the generalisation-based approach, the way to create superhuman CEOs is to use other data-rich tasks (which may be very different from the tasks we actually want an AI CEO to do) to train AIs to develop a range of useful cognitive skills. For example, we could train a reinforcement learning agent to follow instructions in a simulated world. Even if that simulation is very different from the real world, that agent may acquire the planning and learning capabilities required to quickly adapt to real-world tasks. Analogously, the human ancestral environment was also very different to the modern world, but we are still able to become good CEOs with little further training. And roughly the same argument applies to people doing other highly impactful jobs, like paradigm-shaping scientists, entrepreneurs, or policymakers.

One potential obstacle to the generalisation-based approach succeeding is the possibility that specific features of the ancestral environment, or of human brains, were necessary for general intelligence to arise [Ngo, 2020b]. For example, Dunbar [1998] hypothesised that a social "arms race" was required to give us enough social intelligence to develop large-scale cultural transmission. However, most possibilities for such crucial features, including this one, could be recreated in artificial training environments and in artificial neural networks. Some features (such as quantum properties of neurons) would be very hard to simulate precisely, but the human brain operates under conditions that are too messy to make it plausible that our intelligence depends on effects at this scale. So it seems very likely to me that eventually we will be able to create AIs that can generalise well enough to produce human-level performance on a wide range of tasks, including abstract low-data tasks like running a company. Let's call these systems artificial general intelligences, or AGIs. Many AI researchers expect that we'll build AGI within this century [Grace et al., 2018]; however, I won't explore arguments around the timing of AGI development, and the rest of this document doesn't depend on this question.

2.2 Paths to superintelligence

Bostrom [2014] defines a superintelligence as "any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interest". For the purposes of this report, I'll operationalise "greatly exceeding human performance" as doing better than all of humanity could if we coordinated globally (unaided by other advanced AI). I think it's difficult to deny that in principle it's possible to build individual generalisation-based AGIs which are superintelligent, since human brains are constrained by many factors[4] which will be much less limiting for AIs. Perhaps the most striking is the vast difference between the speeds of neurons and transistors: the latter pass signals about four million times more quickly. Even if AGIs never exceed humans in any other way, a speedup this large would allow one to do as much thinking in minutes or hours as a human can in years or decades. Meanwhile our brain size is important in making humans more capable than most animals - but I don't see any reason

Mind blowing

[4] Muehlhauser [2013]

why a neural network couldn't be several orders of magnitude larger than a human brain. And while evolution is a very capable designer in many ways, it hasn't had much time to select specifically for the skills that are most useful in our modern environment, such as linguistic competence and mathematical reasoning. So we should expect that there are low-hanging fruit for improving on human performance on the many tasks which rely on such skills.[5]

There are significant disagreements about how long it will take to transition from human-level AGI to superintelligence, which won't be a focus of this report, but which I'll explore briefly in the section on Control. In the remainder of this section I'll describe in qualitative terms how this transition might occur. By default, we should expect that it will be driven by the standard factors which influence progress in AI: more compute, better algorithms, and better training data. But I'll also discuss three factors whose contributions to increasing AI intelligence will become much greater as AIs become more intelligent: replication, cultural learning, and recursive improvement.

In terms of replication, AIs are much less constrained than humans: it's very easy to create a duplicate of an AI which has all the same skills and knowledge as the original. The cost of compute for doing so is likely to be many times smaller than the original cost of training an AGI (since training usually involves running many copies of an AI much faster than they'd need to be run for real-world tasks). Duplication currently allows us to apply a single AI to many tasks, but not to expand the range of tasks which that AI can achieve. However, we should expect AGIs to be able to decompose difficult tasks into subtasks which can be tackled more easily, just as humans can. So duplicating such an AGI could give rise to a superintelligence composed not of a single AGI, but rather a large group of them (which, following Bostrom [2014], I'll call a collective AGI), which can carry out significantly more complex tasks than the original can.[6] Because of the ease and usefulness of duplicating an AGI, I think that collective AGIs should be our default expectation for how superintelligence will be deployed.

The efficacy of a collective AGI might be limited by coordination problems between its members. However, most of the arguments given in the previous paragraphs are also reasons why individual AGIs will be able to surpass us at the skills required for coordination (such as language processing and theories of mind). One particularly useful skill is cultural learning: we should expect AGIs to be able to acquire knowledge from each other and then share their own discoveries in turn, allowing a collective AGI to solve harder problems than any individual AGI within it could. The development of this ability in humans is

[5] This observation is closely related to Moravec's paradox, which I discuss in more detail in the section on Goals and Agency. Perhaps the most salient example is how easy it was for AIs to beat humans at chess.

[6] It's not quite clear whether the distinction between "single AGIs" and collective AGIs makes sense in all cases, considering that a single AGI can be composed of many modules which might be very intelligent in their own right. But since it seems unlikely that there will be hundreds or thousands of modules which are each generally intelligent, I think that the distinction will in practice be useful. See also Ngo [2020a] and the discussion of "collective superintelligence" in Bostrom [2014].

what allowed the dramatic rise of civilisation over the last ten thousand years. Yet there is little reason to believe that we have reached the peak of this ability, or that AGIs couldn't have a much larger advantage over a human than that human has over a chimp, in acquiring knowledge from other agents.

Thirdly, AGIs will be able to improve the training processes used to develop their successors, which then improve the training processes used to develop their successors, and so on, in a process of *recursive improvement*.[7] Previous discussion has mostly focused on recursive *self*-improvement, involving a single AGI "rewriting its own source code" [Yudkowsky, 2007]. However, I think it's more appropriate to focus on the broader phenomenon of AIs advancing AI research, for several reasons. Firstly, due to the ease of duplicating AIs, there's no meaningful distinction between an AI improving "itself" versus creating a successor that shares many of its properties. Secondly, modern AIs are more accurately characterised as models which could be retrained, rather than software which could be rewritten: almost all of the work of making a neural network intelligent is done by an optimiser via extensive training. Even a superintelligent AGI would have a hard time significantly improving its cognition by modifying its neural weights directly; it seems analogous to making a human more intelligent via brain surgery (albeit with much more precise tools than we have today). So it's probably more accurate to think about self-modification as the process of an AGI modifying its high-level architecture or training regime, then putting itself through significantly more training. This is very similar to how we create new AIs today, except with humans playing a much smaller role. Thirdly, if the intellectual contribution of humans does shrink significantly, then I don't think it's useful to require that humans are *entirely* out of the loop for AI behaviour to qualify as recursive improvement (although we can still distinguish between cases with more or less human involvement).

These considerations reframe the classic view of recursive self-improvement[8] in a number of ways. For example, the retraining step may be bottlenecked by compute even if an AGI is able to design algorithmic improvements very fast. And for an AGI to trust that its goals will remain the same under retraining will likely require it to solve many of the same problems that the field of AGI safety is currently tackling - which should make us more optimistic that the rest of the world could solve those problems before a misaligned AGI undergoes recursive self-improvement. However, to be clear, this reframing doesn't imply that recursive improvement will be unimportant. Indeed, since AIs will eventually be the primary contributors to AI research, recursive improvement as defined here will eventually become the key driver of progress. I'll discuss the implications of this claim in the section on Control.

So far I've focused on how superintelligences might come about, and what they will be able to do. But how will they decide what to actually do? For example, will the individuals within a collective AGI even *want* to cooperate

[7] Whether it's more likely that the successor agent will be an augmented version of the researcher AGI itself or a different, newly-trained AGI is an important question, but one which doesn't affect the argument as made here.

[8] Yudkowsky [2013]

with each other to pursue larger goals? Will an AGI capable of recursive improvement have any reason to do so? I'm wary of phrasing these questions in terms of the goals and motivations of AGIs, without exploring more thoroughly what those terms actually mean. That's the focus of the next section.

3 Goals and Agency

The fundamental concern motivating the second species argument is that AIs will gain too much power over humans, and then use that power in ways we don't endorse. Why might they end up with that power? I'll distinguish three possibilities:

1. AIs pursue power for the sake of achieving other goals; i.e. power is an instrumental goal for them.
2. AIs pursue power for its own sake; i.e. power is a final goal for them.
3. AIs gain power without aiming towards it; e.g. because humans gave it to them.

The first possibility has been the focus of most debate so far, and I'll spend most of this section discussing it. The second hasn't been explored in much depth, but in my opinion is still important; I'll cover it briefly in this section and the next. Following Christiano [2019], I'll call agents which fall into either of these first two categories *influence-seeking*. The third possibility is largely outside the scope of this document, which focuses on dangers from the intentional behaviour of advanced AIs, although I'll briefly touch on it here and in the last section.

The key idea behind the first possibility is Bostrom [2012]'s instrumental convergence thesis, which states that there are some instrumental goals whose attainment would increase the chances of an agent's final goals being realised for a wide range of final goals and a wide range of situations. Examples of such instrumentally convergent goals include self-preservation, resource acquisition, technological development, and self-improvement, which are all useful for executing further large-scale plans. I think these examples provide a good characterisation of the type of power I'm talking about, which will serve in place of a more explicit definition.

However, the link from instrumentally convergent goals to dangerous influence-seeking is only applicable to agents which have final goals large-scale enough to benefit from these instrumental goals, and which identify and pursue those instrumental goals even when it leads to extreme outcomes (a set of traits which I'll call *goal-directed agency*). It's not yet clear that AGIs will be this type of agent, or have this type of goals. It seems very intuitive that they will because we all have experience of pursuing instrumentally convergent goals, for example by earning and saving money, and can imagine how much better we'd be at them if we were more intelligent. Yet since evolution has ingrained in us many useful short-term drives (in particular the drive towards power itself), it's difficult to determine the extent to which human influence-seeking behaviour is caused by us reasoning about its instrumental usefulness towards larger-scale goals. Our conquest of the world didn't require any humans to strategise over the timeframe of centuries, but merely for many individuals to expand their personal influence in a relatively limited way - by inventing a slightly better tool, or exploring slightly further afield.

Furthermore, we should take seriously the possibility that superintelligent AGIs might be even less focused than humans are on achieving large-scale goals. We can imagine them possessing final goals which don't incentivise the pursuit of power, such as deontological goals, or small-scale goals. Or perhaps we'll build "tool AIs" which obey our instructions very well without possessing goals of their own - in a similar way to how a calculator doesn't "want" to answer arithmetic questions, but just does the calculations it's given. In order to figure out which of these options is possible or likely, we need to better understand the nature of goals and goal-directed agency. That's the focus of this section.

3.1 Frameworks for thinking about agency

To begin, it's crucial to distinguish between the goals which an agent has been *selected* or *designed* to do well at (which I'll call its *design objectives*[9]), and the goals which an agent itself wants to achieve (which I'll just call "the agent's goals").[10] For example, insects can contribute to complex hierarchical societies only because evolution gave them the instincts required to do so: to have "competence without comprehension", in Dennett's terminology. This term also describes current image classifiers and (probably) RL agents like AlphaStar and OpenAI Five: they can be competent at achieving their design objectives without understanding what those objectives are, or how their actions will help achieve them. If we create agents whose design objective is to accumulate power, but without the agent itself having the goal of doing so (e.g. an agent which plays the stock market very well without understanding how that impacts society) that would qualify as the third possibility outlined above.

By contrast, in this section I'm interested in what it means for an agent to have a goal of its own. Three existing frameworks which attempt to answer this question are Morgenstern and Von Neumann [1953]'s *expected utility maximisation*, Dennett [1989]'s *intentional stance*, and Hubinger et al. [2019]'s *mesa-optimisation*. I don't think any of them adequately characterises the type of goal-directed behaviour we want to understand, though. While we can prove elegant theoretical results about utility functions, they are such a broad formalism that practically any behaviour can be described as maximising some utility function [Ngo, 2019b]. So this framework doesn't constrain our expectations about powerful AGIs.[11] Meanwhile, Dennett argues that taking the intentional

[9] Following Ortega et al. [2018].

[10] AI systems which learn to pursue goals are also known as *mesa-optimisers*, as coined in Hubinger et al. [2019].

[11] Related arguments exist which attempt to do so. For example, Yudkowsky [2018] argues

stance towards systems can be useful for making predictions about them - but this only works given prior knowledge about what goals they're most likely to have. Predicting the behaviour of a trillion-parameter neural network is very different from applying the intentional stance to existing artifacts. And while we do have an intuitive understanding of complex human goals and how they translate to behaviour, the extent to which it's reasonable to extend those beliefs about goal-directed cognition to artificial intelligences is the very question we need a theory of agency to answer. So while Dennett's framework provides some valuable insights - in particular, that assigning agency to a system is a modelling choice which only applies at certain levels of abstraction - I think it fails to reduce agency to simpler and more tractable concepts.

Additionally, neither framework accounts for bounded rationality: the idea that systems can be "trying to" achieve a goal without taking the best actions to do so. In order to figure out the goals of boundedly rational systems, we'll need to scrutinise the structure of their cognition, rather than treating them as black-box functions from inputs to outputs - in other words, using a "cognitive" definition of agency rather than "behavioural" definitions like the two I've discussed so far. In *Risks from Learned Optimisation in Advanced ML systems*, Hubinger et al. [2019] use a cognitive definition: "a system is an optimizer if it is internally searching through a search space (consisting of possible outputs, policies, plans, strategies, or similar) looking for those elements that score high according to some objective function that is explicitly represented within the system". I think this is a promising start, but it has some significant problems. In particular, the concept of "explicit representation" seems like a tricky one - what is explicitly represented within a human brain, if anything? And their definition doesn't draw the important distinction between "local" optimisers such as gradient descent and goal-directed planners such as humans.

My own approach to thinking about agency tries to improve on the approaches above by being more specific about the cognition we expect goal-directed systems to do. Just as "being intelligent" involves applying a range of abilities (as discussed in the previous section), "being goal-directed" involves a system applying some specific additional abilities:

1. *Self-awareness*: it understands that it's a part of the world, and that its behaviour impacts the world;

2. *Planning*: it considers a wide range of possible sequences of behaviours (let's call them "plans"), including long plans;

3. *Consequentialism*: it decides which of those plans is best by considering the value of the outcomes that they produce;

that, "while corrigibility probably has a core which is of lower algorithmic complexity than all of human value, this core is liable to be very hard to find or reproduce by supervised learning of human-labeled data, because deference is an unusually anti-natural shape for cognition, in a way that a simple utility function would not be an anti-natural shape for cognition." Note, however, that this argument relies on the intuitive distinction between natural and anti-natural shapes for cognition. This is precisely what I think we need to understand to build safe AGI - but there has been little explicit investigation of it so far.

4. *Scale*: its choice is sensitive to the effects of plans over large distances and long time horizons;

5. *Coherence*: it is internally unified towards implementing the single plan it judges to be best;

6. *Flexibility*: it is able to adapt its plans flexibly as circumstances change, rather than just continuing the same patterns of behaviour.

Note that none of these traits should be interpreted as binary; rather, each one defines a different spectrum of possibilities. I'm also not claiming that the combination of these six dimensions is a precise or complete characterisation of agency; merely that it's a good starting point, and the right *type* of way to analyse agency. For instance, it highlights that agency requires a combination of different abilities - and as a corollary, that there are many different ways to be less than maximally agentic. AIs which score very highly on some of these dimensions might score very low on others. Considering each trait in turn, and what lacking it might look like:

1. *Self-awareness*: for humans, intelligence seems intrinsically linked to a first-person perspective. But an AGI trained on abstract third-person data might develop a highly sophisticated world-model that just doesn't include itself or its outputs. A sufficiently advanced language or physics model might fit into this category.

2. *Planning*: highly intelligent agents will by default be able to make extensive and sophisticated plans. But in practice, like humans, they may not always apply this ability. Perhaps, for instance, an agent is only trained to consider restricted types of plans. Myopic training attempts to implement such agents; more generally, an agent could have limits on the actions it considers. For example, a question-answering system might only consider plans of the form "first figure out subproblem 1, then figure out subproblem 2, then...".

3. *Consequentialism*: the usual use of this term in philosophy describes agents which believe that the moral value of their actions depends only on those actions' consequences; here I'm using it in a more general way, to describe agents whose subjective preferences about actions depend mainly on those actions' consequences. It seems natural to expect that agents trained on a reward function determined by the state of the world would be consequentialists. But note that humans are far from fully consequentialist, since we often obey deontological constraints or constraints on the types of reasoning we endorse.

4. *Scale*: agents which only care about small-scale events may ignore the long-term effects of their actions. Since agents are always trained in small-scale environments, developing large-scale goals requires generalisation (in ways that I discuss below).

5. *Coherence*: humans lack this trait when we're internally conflicted - for example, when our system 1 and system 2 goals differ - or when our goals change a lot over time. While our internal conflicts might just be an artefact of our evolutionary history, we can't rule out individual AGIs developing modularity which might lead to comparable problems. However, it's most natural to think of this trait in the context of a collective, where the individual members could have more or less similar goals, and could be coordinated to a greater or lesser extent.

6. *Flexibility*: an inflexible agent might arise in an environment in which coming up with one initial plan is usually sufficient, or else where there are tradeoffs between making plans and executing them. Such an agent might display sphexish behaviour. Another interesting example might be a multi-agent system in which many AIs contribute to developing plans - such that a single agent is able to execute a given plan, but not able to rethink it very well.

A question-answering system (aka an oracle) could be implemented by an agent lacking either planning or consequentialism. For AIs which act in the real world I think the scale of their goals is a crucial trait to explore, and I'll do so later in this section. We can also evaluate other systems on these criteria. A calculator probably doesn't have any of them. Software that's a little more complicated, like a GPS navigator, should probably be considered consequentialist to a limited extent (because it reroutes people based on how congested traffic is), and perhaps has some of the other traits too, but only slightly. Most animals are self-aware, consequentialist and coherent to various degrees. The traditional conception of AGI has all of the traits above, which would make it capable of pursuing influence-seeking strategies for instrumental reasons. However, note that goal-directedness is not the only factor which determines whether an AI is influence-seeking: the content of its goals also matter. A highly agentic AI which has the goal of remaining subordinate to humans might never take influence-seeking actions. And as previously mentioned, an AI might be influence-seeking because it has the final goal of gaining power, even without possessing many of the traits above. I'll discuss ways to influence the content of an agent's goals in the next section, on Alignment.

3.2 The likelihood of developing highly agentic AGI

How likely is it that, in developing an AGI, we produce a system with all of the six traits I identified above? One approach to answering this question involves predicting which types of model architecture and learning algorithms will be used - for example, will they be model-free or model-based? To my mind, this line of thinking is not abstract enough, because we simply don't know enough about how cognition and learning work to map them onto high-level design choices. If we train AGI in a model-free way, I predict it will end up planning using an implicit model[12] anyway. If we train a model-based AGI, I predict its model will be so abstract and hierarchical that looking at its architecture will tell us very little about the actual cognition going on.

At a higher level of abstraction, I think that it'll be easier for AIs to acquire the components of agency listed above if they're also very intelligent. However, the extent to which our most advanced AIs are agentic will depend on what type of training regime is used to produce them. For example, our best language models already generalise well enough from their training data that they can answer a wide range of questions. I can imagine them becoming more and more competent via unsupervised and supervised training, until they are able to answer questions which no human knows the answer to, but still without possessing any of the properties listed above. A relevant analogy might be to the human visual system, which does very useful cognition, but which is not very "goal-directed" in its own right.

My underlying argument is that agency is not just an emergent property of highly intelligent systems, but rather a set of capabilities which need to be developed during training, and which won't arise without selection for it. One piece of supporting evidence is Moravec's paradox: the observation that the cognitive skills which seem most complex to humans are often the easiest for AIs, and vice versa [Moravec, 1988]. In particular, Moravec's paradox predicts that building AIs which do complex intellectual work like scientific research might actually be easier than building AIs which share more deeply ingrained features of human cognition like goals and desires. To us, understanding the world and changing the world seem very closely linked, because our ancestors were selected for their ability to act in the world to improve their situations. But if this intuition is flawed, then even reinforcement learners may not develop all the aspects of goal-directedness described above if they're primarily trained to answer questions.

However, there are also arguments that it will be difficult to train AIs to do intellectual work without them also developing goal-directed agency. In the case of humans, it was the need to interact with an open-ended environment[13] to achieve our goals that pushed us to develop our sophisticated general intelligence. The central example of an analogous approach to AGI is training a reinforcement learning agent in a complex simulated 3D environment (or perhaps via extended conversations in a language-only setting). In such environments, agents which strategise about the effects of their actions over long time horizons will generally be able to do better. This implies that our AIs will be subject to optimisation pressure towards becoming more agentic (by my criteria above) will do better. We might expect an AGI to be even more agentic if it's trained, not just in a complex environment, but in a complex competitive multi-agent environment. Agents trained in this way will need to be very good at flexibly adapting plans in the face of adversarial behaviour; and they'll benefit from considering a wider range of plans over a longer timescale than any competitor.

[12] As in Guez et al. [2019].

[13] A concept explored further in Ecoffet et al. [2020].

On the other hand, it seems very difficult to predict the overall effect of interactions between many agents - in humans, for example, it led to the development of (sometimes non-consequentialist) altruism.

It's currently very uncertain which training regimes will work best to produce AGIs. But if there are several viable ones, we should expect economic pressures to push researchers towards prioritising those which produce the most agentic AIs, because they will be the most useful (assuming that alignment problems don't become serious until we're close to AGI). In general, the broader the task an AI is used for, the more valuable it is for that AI to reason about how to achieve its assigned goal in ways that we may not have specifically trained it to do. For example, a question-answering system with the goal of helping its users understand the world might be much more useful than one that's competent at its design objective of answering questions accurately, but isn't goal-directed in its own right. Overall, however, I think most safety researchers would argue that we should prioritise research directions which produce less agentic AGIs, and then use the resulting AGIs to help us align later more agentic AGIs. There's also been some work on directly making AGIs less agentic (such as Taylor [2016]'s quantilization), although this has in general been held back by a lack of clarity around these concepts.

I've already discussed recursive improvement in the previous section, but one further point which is useful to highlight here: since being more agentic makes an agent more capable of achieving its goals, agents which are capable of modifying themselves will have incentives to make themselves more agentic too (as humans already try to do, albeit in limited ways). So we should consider this to be one type of recursive improvement, to which many of the considerations discussed in the previous section also apply.

3.3 Goals as generalised concepts

I should note that I don't expect our training tasks to replicate the scale or duration of all the tasks we care about in the real world. So AGIs won't be directly selected to have very large-scale or long-term goals. Yet it's likely that the goals they learn in their training environments will generalise to larger scales, just as humans developed large-scale goals from evolving in a relatively limited ancestral environment. In modern society, people often spend their whole lives trying to significantly influence the entire world - via science, business, politics, and many other channels. And some people aspire to have a worldwide impact over the timeframe of centuries, millennia or longer, even though there was never significant evolutionary selection in favour of humans who cared about what happened in several centuries' time, or paid attention to events on the other side of the world. This gives us reason to be concerned that even AGIs which aren't explicitly trained to pursue ambitious large-scale goals might do so anyway. I also expect researchers to actively aim towards achieving this type of generalisation to longer time horizons in AIs, because some important applications rely on it. For long-term tasks like being a CEO, AGIs will need the capability and motivation to choose between possible actions based on their worldwide consequences on the timeframe of years or decades.

Can we be more specific about what it looks like for goals to generalise to much larger scales? Given the problems with the expected utility maximisation framework I identified earlier, it doesn't seem useful to think of goals as utility functions over states of the world. Rather, an agent's goals can be formulated in terms of whatever concepts it possesses - regardless of whether those concepts refer to its own thought processes, deontological rules, or outcomes in the external world.[14] And insofar as an agent's concepts flexibly adjust and generalise to new circumstances, the goals which refer to them will do the same. It's difficult and speculative to try to describe how such generalisation may occur, but broadly speaking, we should expect that intelligent agents are able to abstract away the differences between objects or situations that have high-level similarities. For example, after being trained in a simulation, an agent might transfer its attitudes towards objects and situations in the simulation to their counterparts in the (much larger) real world.[15] Alternatively, the generalisation could be in the framing of the goal: an agent which has always been rewarded for accumulating resources in its training environment might interalise the goal of "amassing as many resources as possible". Similarly, agents which are trained adversarially in a small-scale domain might develop a goal of outcompeting each other which persists even when they're both operating at a very large scale.

From this perspective, to predict an agent's behaviour, we will need to consider what concepts it will possess, how those will generalise, and how the agent will reason about them. I'm aware that this appears to be an intractably difficult task - even human-level reasoning can lead to extreme and unpredictable conclusions (as the history of philosophy shows). However, I hope that we can instill lower-level mindsets or values into AGIs which guide their high-level reasoning in safe directions. I'll discuss some approaches to doing so in the next section, on Alignment.

3.4 Groups and agency

After discussing collective AGIs in the previous section, it seems important to examine whether the framework I've proposed for understanding agency can apply to a group of agents as well. I think it can: there's no reason that the traits I described above need to be instantiated within a single neural network. However, the relationship between the goal-directedness of a collective AGI and the goal-directedness of its individual members may not be straightforward, since it depends on the internal interactions between its members.

[14]For example, when people want to be "cooperative" or "moral", they're often not just thinking about results, but rather the types of actions they should take, or the types of decision procedures they should use to generate those actions. An additional complication is that humans don't have full introspective access to all our concepts - so we need to also consider unconscious concepts.

[15]Consider if this happened to you, and you were pulled "out of the simulation" into a real world which is quite similar to what you'd already experienced. By default you would likely still want to eat good food, have fulfilling relationships, and so on, despite the radical ontological shift you just underwent.

One of the key variables is how much (and what types of) experience those members have of interacting with each other during training. If they have been trained primarily to cooperate, that makes it more likely that the resulting collective AGI is a goal-directed agent, even if none of the individual members is highly agentic. But there are good reasons to expect that the training process will involve some competition between members, which would undermine their coherence as a group [Leibo et al., 2019]. Internal competition might also increase short-term influence-seeking behaviour, since each member will have learned to pursue influence in order to outcompete the others. As a particularly salient example, humanity managed to take over the world over a period of millennia not via a unified plan to do so, but rather as a result of many individuals trying to expand their short-term influence.

It's also possible that the members of a collective AGI have not been trained to interact with each other at all, in which case cooperation between them would depend entirely on their ability to generalise from their existing skills. It's difficult to imagine this case, because human brains are so well-adapted for group interactions. But insofar as humans and aligned AGIs hold a disproportionate share of power over the world, there is a natural incentive for AGIs pursuing misaligned goals to coordinate with each other to increase their influence at our expense.[16] Whether they succeed in doing so will depend on what sort of coordination mechanisms they are able to design.

A second factor is how much specialisation there is within the collective AGI. In the case where it consists only of copies of the same agent, we should expect that the copies understand each other very well, and share goals to a large extent. If so, we might be able to make predictions about the goal-directedness of the entire group merely by examining the original agent. But another case worth considering is a collective consisting of a range of agents with different skills. With this type of specialisation[17], the collective as a whole could be much more agentic than any individual agent within it, which might make it easier to deploy subsets of the collective safely [Ngo, 2020e].

4 Alignment

In the previous section, I discussed the plausibility of ML-based agents developing the capability to seek influence for instrumental reasons. This would not be a problem if they do so only in the ways that are aligned with human values. Indeed, many of the benefits we expect from AGIs will require them to wield power to influence the world. And by default, AI researchers will apply

[16]In addition to the prima facie argument that intelligence increases coordination ability, it is likely that AGIs will have access to commitment devices not available to humans by virtue of being digital. For example, they could send potential allies a copy of themselves for inspection, to increase confidence in their trustworthiness. However, there are also human commitment devices that AGIs will have less access to - for example, putting ourselves in physical danger as an honest signal. And it's possible that the relative difficulty of lying versus detecting lying shifts in favour of the former for more intelligent agents.

[17]Ngo [2020d]

their efforts towards making agents do whatever tasks those researchers desire, rather than learning to be disobedient. However, there are reasons to worry that despite such efforts by AI researchers, AIs will develop undesirable final goals which lead to conflict with humans.

To start with, what does "aligned with human values" even mean? Following Christiano [2015] and Gabriel [2020], I'll distinguish between two types of interpretations. *Minimalist* (aka *narrow*) approaches focus on avoiding catastrophic outcomes. The best example is Christiano [2018a]'s concept of intent alignment: "When I say an AI A is aligned with an operator H, I mean: *A is trying to do what H wants it to do*." While there will always be some edge cases in figuring out a given human's intentions, there is at least a rough commonsense interpretation. By contrast, *maximalist* (aka *ambitious*) approaches attempt to make AIs adopt or defer to a specific overarching set of values - like a particular moral theory, or a global democratic consensus, or a meta-level procedure for deciding between moral theories.

My opinion is that defining alignment in maximalist terms is unhelpful, because it bundles together technical, ethical and political problems. While it may be the case that we need to make progress on all of these, assumptions about the latter two can significantly reduce clarity about technical issues. So from now on, when I refer to alignment, I'll only refer to intent alignment. I'll also define an AI A to be *misaligned* with a human H if H would want A not to do what A is trying to do (if H were aware of A's intentions). This implies that AIs could potentially be neither aligned nor misaligned with an operator - for example, if they only do things which the operator doesn't care about. Whether an AI qualifies as aligned or misaligned obviously depends a lot on who the operator is, but for the purposes of this report I'll focus on AIs which are clearly misaligned with respect to most humans.

One important feature of these definitions: by using the word "trying", they focus on the AI's intentions, not the actual outcomes achieved. I think this makes sense because we should expect AGIs to be very good at understanding the world, and so the key safety problem is setting their intentions correctly. In particular, I want to be clear that when I talk about misaligned AGI, the central example in my mind is not agents that misbehave just because they misunderstand what we want, or interpret our instructions overly literally (which Bostrom [2014] calls "perverse instantiation"). It seems likely that AGIs will understand the intentions of our instructions very well by default. This is because they will probably be trained on tasks involving humans, and human data - and understanding human minds is particularly important for acting competently in those tasks and the rest of the world.[18] Rather, my main concern is that AGIs will understand what we want, but just not care, because the motivations they acquired during training weren't those we intended them to have.

The idea that AIs won't automatically gain the right motivations by virtue of being more intelligent is an implication of Bostrom [2012]'s orthogonality thesis,

[18] Of course, what humans say we want, and what we act as if we want, and what we privately desire often diverge. But again, I'm not particularly worried about a superintelligence being unable to understand how humans distinguish between these categories, if it wanted to.

which states that “more or less any level of intelligence could in principle be combined with more or less any final goal”. For our purposes, a weaker version suffices: simply that highly intelligent agents could have large-scale goals which are misaligned with those of most humans. An existence proof is provided by high-functioning psychopaths, who understand that other people are motivated by morality, and can use that fact to predict their actions and manipulate them, but nevertheless aren't motivated by morality themselves.

We might hope that by carefully choosing the tasks on which agents are trained, we can prevent those agents from developing goals that conflict with ours, without requiring any breakthroughs in technical safety research. Why might this not work, though? Previous arguments have distinguished between two concerns: the *outer misalignment* problem and the *inner misalignment* problem. I'll explain both of these, and give arguments for why they might arise. I'll also discuss some limitations of using this framework, and an alternative perspective on alignment.

4.1 Outer and inner misalignment: the standard picture

We train machine learning systems to perform desired behaviour by optimising them with respect to some objective function - for example, a reward function in reinforcement learning. The outer misalignment concern is that we won't be able to implement an objective function which describes the behaviour we actually want the system to perform, without also rewarding misbehaviour. One key intuition underlying this concern is the difficulty of explicitly programming objective functions which express all our desires about AGI behaviour. There's no simple metric which we'd like our agents to maximise - rather, desirable AGI behaviour is best formulated in terms of concepts like obedience, consent, helpfulness, morality, and cooperation, which we can't define precisely in realistic environments. Although we might be able to specify proxies for those goals, Goodhart's law suggests that some undesirable behaviour will score very well according to these proxies, and therefore be reinforced in AIs trained on them [Manheim and Garrabrant, 2018]. Even comparatively primitive systems today demonstrate a range of specification gaming behaviours, some of which are quite creative and unexpected, when we try to specify much simpler concepts [Krakovna et al., 2020].

One way to address this problem is by incorporating human feedback into the objective function used to evaluate AI behaviour during training. However, there are at least three challenges to doing so. The first is that it would be prohibitively expensive for humans to provide feedback on all data required to train AIs on complex tasks. This is known as the *scalable oversight* problem; reward modelling[19] is the primary approach to addressing it. A second challenge is that, for long-term tasks, we might need to give feedback before we've had the chance to see all the consequences of an agent's actions. Yet even in domains as simple as Go, it's often very difficult to determine how good a given

[19] As in Christiano et al. [2017].

move is without seeing the game play out. And in larger domains, there may be too many complex consequences for any single individual to evaluate. The main approach to addressing this issue is by using multiple AIs to recursively decompose the problem of evaluation, as in Irving et al. [2018]'s Debate, Leike et al. [2018]'s Recursive Reward Modelling, and Christiano et al. [2018]'s Iterated Amplification. By constructing superhuman evaluators, these techniques also aim to address the third issue with human feedback: that humans can be manipulated into interpreting behaviour more positively than they otherwise would, for example by giving them misleading data (as in the robot hand example from Christiano et al. [2017]).

Even if we solve outer alignment by specifying a "safe" objective function, though, we may still encounter a failure of *inner alignment*: our agents might develop goals which differ from the ones specified by that objective function. This is likely to occur when the training environment contains subgoals which are consistently useful for scoring highly on the given objective function, such as gathering resources and information, or gaining power.[20] If agents reliably gain higher reward after achieving such subgoals, then the optimiser might select for agents which care about those subgoals for their own sake. (This is one way agents might develop a final goal of acquiring power, as mentioned at the beginning of the section on Goals and Agency.)

This is analogous to what happened during the evolution of humans, when we were "trained" by evolution to increase our genetic fitness. In our ancestral environment, subgoals like love, happiness and social status were useful for achieving higher inclusive genetic fitness, and so we evolved to care about them. But now that we are powerful enough to reshape the natural world according to our desires, there are significant differences between the behaviour which would maximise genetic fitness (e.g. frequent sperm or egg donation), and the behaviour which we display in pursuit of the motivations we actually evolved. Another example: suppose we reward an agent every time it correctly follows a human instruction, so that the cognition which leads to this behaviour is reinforced by its optimiser. Intuitively, we'd hope that the agent comes to have the goal of obedience to humans. But it's also conceivable that the agent's obedient behaviour is driven by the goal "don't get shut down", if the agent understands that disobedience will get it shut down - in which case the optimiser might actually reinforce the goal of survival every time it leads to a completed instruction. So two agents, each motivated by one of these goals, might behave very similarly until they are in a position to be disobedient without being shut

[20]Note the subtle distinction between the existence of useful subgoals, and my earlier discussion of the instrumental convergence thesis. The former is the claim that, for the specific tasks on which we train AGIs, there are some subgoals which will be rewarded *during training*. The latter is the claim that, for most goals which an AGI might develop, there are some specific subgoals which will be useful when the AGI tries to pursue those goals *while deployed*. The latter implies the former only insofar as the convergent instrumental subgoals are both possible and rewarded during training. Self-improvement is a convergent instrumental subgoal, but I don't expect most training environments to support it, and those that do may have penalties to discourage it.

down.[21]

What will determine whether agents like the former or agents like the latter are more likely to actually arise? As I mentioned above, one important factor is whether there are subgoals which reliably lead to higher reward during training. Another is how easy and beneficial it is for the optimiser to make the agent motivated by those subgoals, versus motivated by the objective function it's being trained on. In the case of humans, for example, the concept of inclusive genetic fitness was a very difficult one for evolution to build into the human motivational system. And even if our ancestors had somehow developed that concept, they would have had difficulty coming up with better ways to achieve it than the ones evolution had already instilled in them. So in our ancestral environment there was relatively little selection pressure for us to be inner-aligned with evolution. In the context of training an AI, this means that the complexity of the goals we try to instil in it incurs a double penalty: not only does that complexity make it harder to specify an acceptable objective function, it also makes that AI less likely to become motivated by our intended goals even if the objective function is correct. Of course, late in training we expect our AIs to have become intelligent enough that they'll understand exactly what goals we intended to give them. But by that time their existing motivations may be difficult to remove, and they'll likely also be intelligent enough to attempt deceptive behaviour (as in the hypothetical example in the previous paragraph).

So how can we ensure inner alignment of AGIs with human intentions? This research area has received less attention than outer alignment so far, because it's a trickier problem to get a grip on. One potential approach involves adding training examples where the behaviour of agents motivated by misaligned goals diverges from that of aligned agents. Yet designing and creating this sort of adversarial training data is currently much more difficult than mass-producing data (e.g. via procedurally-generated simulations, or web scraping). This is partly just because specific training data is harder to create in general, but also for three additional reasons. Firstly, by default we simply won't know which undesirable motivations our agents are developing, and therefore which ones to focus on penalising. Interpretability techniques could help with this, but seem very difficult to create (as I'll discuss further in the next section). Secondly, the misaligned motivations which agents are most likely to acquire are those which are most robustly useful. For example, it's particularly hard to design a training environment where access to more information leads to lower reward. Thirdly, we are most concerned about agents which have large-scale misaligned goals. Yet large-scale scenarios are again the most difficult to set up during training,

[21] In fact these two examples showcase two different types of inner alignment failure: *upstream mesa-optimisers* and *downstream mesa-optimisers* [Christiano, 2018b]. When trained on a reward function R, upstream mesa-optimisers learn goals which lead to scoring highly on R, or in other words are *causally upstream* of R. For example, humans learning to value finding food since it leads to greater reproductive success. Whereas downstream mesa-optimisers learn goals that are causally downstream of scoring highly on R: for example, they learn the goal of survival, and realise that if they score badly on R, they'll be discarded by the optimisation procedure. This incentivises them to score highly on R, and hide their true goals - an outcome called deceptive alignment [Hubinger et al., 2019].

either in simulation or in the real-world. So there's a lot of scope for more work addressing these problems, or identifying new inner alignment techniques.

4.2 A more holistic view of alignment

Outer alignment is the problem of correctly evaluating AI behaviour; inner alignment is the problem of making the AI's goals match those evaluations. To some extent we can treat these as two separate problems; however, I think it's also important to be aware of the ways in which the narrative of "alignment = outer alignment + inner alignment" is incomplete or misleading. In particular, what would it even mean to implement a "safe" objective function? Is it a function that we want the agent to actually maximise? Yet while maximising expected reward makes sense in formalisms like MDPs and POMDPs, it's much less well-defined when the objective function is implemented in the real world. If there's some sequence of actions which allows the agent to tamper with the channel by which it's sent rewards, then "wireheading" by maxing out that channel will practically always be the strategy which allows the agent to receive the highest reward signal in the long term (even if the reward function heavily penalises actions leading up to wireheading).[22] And if we use human feedback, as previously discussed, then the optimal policy will be to manipulate or coerce the supervisors into giving maximally positive feedback. (There's been some suggestion that "myopic" training could solve problems of tampering and manipulation, but as I argued in Ngo [2020c], I expect that it merely hides them.)

A second reason why reward functions are a "leaky abstraction" is that any real-world agents we train in the foreseeable future will be very, very far away from the limit of optimal behaviour on non-trivial reward functions. In particular, they will only see rewards for a tiny fraction of possible states. Furthermore, if they're generalisation-based agents, they'll often perform new tasks after very

[22] One useful distinction here is between the *message*, the *code*, and the *channel* (following Shannon). In the context of reinforcement learning, we can interpret the message to be whatever goal is intended by the designers of the system (e.g. win at Starcraft); the code is real numbers attached to states, with higher numbers indicating better states; and the channel is the circuitry by which these numbers are passed to the agent. We have so far assumed that the goal the agent learns is based on the message its optimiser infers from its reward function (albeit perhaps in a way that generalises incorrectly, because it can be hard to decode the intended message from a finite number of sampled rewards). But it's also possible that the agent learns to care about the state of the channel itself. I consider pain in animals to be one example of this: the message is that damage is being caused; the code is that more pain implies more damage (as well as other subtleties of type and intensity); and the channel is the neurons that carry those signals to our brains. In some cases, the code changes - for example, when we receive an electric shock but know that it has no harmful effects. If we were only concerned with the message, then we would ignore those cases, because they provide no new content about damage to our body. Yet what actually happens is that we try to prevent those signals being sent anyway, because we don't want to feel pain! Similarly, an agent which was trained via a reward signal may desire to continue receiving those signals even when they no longer carry the same message. Another way of describing this distinction is by contrasting internalisation of a base objective versus modeling of that base objective, as discussed in section 4 of Hubinger et al. [2019].

little training directly on those tasks. So the agent's behaviour in almost all states will be primarily influenced not by the true value of the reward function on those states, but rather by how it generalises from previously-collected data about other states.[23] This point is perhaps an obvious one, but it's worth emphasising because there are so many theorems about the convergence of reinforcement learning algorithms which rely on visiting every state in the infinite limit, and therefore tell us very little about behaviour after a finite time period.

A third reason is that researchers already modify reward functions in ways which change the optimal policy when it seems useful. For example, we add shaping terms to provide an implicit curriculum, or exploration bonuses to push the agent out of local optima. As a particularly safety-relevant example, neural networks can be modified so that their loss on a task depends not just on their outputs, but also on their internal representations [Ganin et al., 2016]. This is particularly useful for influencing how those networks generalise - for example, making them ignore spurious correlations in the training data. But again, it makes it harder to interpret reward functions as specifications of desired outcomes of a decision process.

How should we think about them instead? Well, in trying to ensure that AGI will be aligned, we have a range of tools available to us - we can choose the neural architectures, RL algorithms, environments, optimisers, etc, that are used in the training procedure. We should think about our ability to specify an objective function as the most powerful such tool. Yet it's not powerful because the objective function defines an agent's motivations, but rather because samples drawn from it shape that agent's motivations and cognition.

From this perspective, we should be less concerned about what the extreme optima of our objective functions look like, because they won't ever come up during training (and because they'd likely involve tampering). Instead, we should focus on how objective functions, in conjunction with other parts of the training setup, create selection pressures towards agents which think in the ways we want, and therefore have desirable motivations in a wide range of circumstances.[24] (See Arora [2019] for a more mathematical framing of a similar point.)

This perspective provides another lens on the previous section's arguments about AIs which are highly agentic. It's not the case that AIs will inevitably end up thinking in terms of large-scale consequentialist goals, and our choice of reward function just determines which goals they choose to maximise. Rather, all the cognitive abilities of our AIs, including their motivational systems, will

[23] The mistake of thinking of RL agents solely as reward-maximisers (rather than having other learned instincts and goals) has an interesting parallel in the history of the study of animal cognition, where behaviorists focused on the ways that animals learned new behaviours to increase reward, while ignoring innate aspects of their cognition.

[24] One useful example is the evolution of altruism in humans. While there's not yet any consensus on the precise evolutionary mechanisms involved, it's notable that our altruistic instincts extend well beyond the most straightforward cases of kin altruism and directly reciprocal altruism. In other words, some interaction between our direct evolutionary payoffs, and our broader environment, led to the emergence of quite general altruistic instincts, making humans "safer" (from the perspective of other species).

develop during training. The objective function (and the rest of the training setup) will determine the extent of their agency and their attitude towards the objective function itself! This might allow us to design training setups which create pressures towards agents which are still very intelligent and capable of carrying out complex tasks, but not very agentic - thereby preventing misalignment without solving either outer alignment or inner alignment.

Failing that, though, we will need to align agentic AGIs. To do so, in addition to the techniques I've discussed above, we'll need to be able to talk more precisely about what concepts and goals our agents possess. However, I am pessimistic about the usefulness of mathematics in making such high-level claims. Mathematical frameworks often abstract away the aspects of a problem that we actually care about, in order to make proofs easier - making those proofs much less relevant than they seem. I think this criticism applies to the expected utility maximisation framework, as discussed previously; other examples include most RL convergence proofs, and most proofs of robustness to adversarial examples. Instead, I think we will need principles and frameworks similar to those found in cognitive science and evolutionary biology. I think the categorisation of upstream vs downstream inner misalignment is an important example of such progress;[21] I'd also like to see a framework in which we can talk sensibly about gradient hacking,[25] and the distinction between being motivated by a reward signal versus a reward function.[22] We should then judge reward functions as "right" or "wrong" only to the extent that they succeed or fail in pushing the agent towards developing desirable motivations and avoiding these sorts of pathologies.

In the final section, I will address the question of whether, if we fail, AGIs with the goal of increasing their influence at the expense of humans will actually succeed in doing so.

5 Control

It's important to note that my previous arguments by themselves do not imply that AGIs will end up in control of the world instead of us. As an analogy, scientific knowledge allows us to be much more capable than stone-age humans. Yet if dropped back in that time with just our current knowledge, I very much doubt that one modern human could take over the stone-age world. Rather, this last step of the argument relies on additional predictions about the dynamics of the transition from humans being the smartest agents on Earth to AGIs taking over that role. These will depend on technological, economic and political factors, as I'll discuss in this section. One recurring theme will be the importance of our expectation that AGIs will be deployed as software that can be run on many different computers, rather than being tied to a specific piece of hardware

[25] See Hubinger [2019a]: "Gradient hacking is a term I've been using recently to describe the phenomenon wherein a deceptively aligned mesa-optimizer might be able to purposefully act in ways which cause gradient descent to update it in a particular way."

as humans are.[26]

I'll start off by discussing two very high-level arguments. The first is that being more generally intelligent allows you to acquire more power, via large-scale coordination and development of novel technological capabilities. Both of these contributed to the human species taking control of the world; and they both contributed to other big shifts in the distribution of power (such as the industrial revolution). If the set of all humans and aligned AGIs is much less capable in these two ways than the set of all misaligned AGIs, then we should expect the latter to develop more novel technologies, and use them to amass more resources, unless strong constraints are placed on them, or they're unable to coordinate well (I'll discuss both possibilities shortly.)

On the other hand, though, it's also very hard to take over the world. In particular, if people in power see their positions being eroded, it's generally a safe bet that they'll take action to prevent that. Further, it's always much easier to understand and reason about a problem when it's more concrete and tangible; our track record at predicting large-scale future developments is pretty bad. And so even if the high-level arguments laid out above seem difficult to rebut, there may well be some solutions we missed which people will spot when their incentives to do so, and the range of approaches available to them, are laid out more clearly.

How can we move beyond these high-level arguments? In the rest of this section I'll lay out two types of disaster scenarios, and then four factors which will affect our ability to remain in control if we develop AGIs that are not fully aligned:

1. Speed of AI development
2. Transparency of AI systems
3. Constrained deployment strategies
4. Human political and economic coordination

5.1 Disaster scenarios

There have been a number of attempts to describe the catastrophic outcomes that might arise from misaligned superintelligences, although it has proven difficult to characterise them in detail. Broadly speaking, the most compelling scenarios fall into two categories. Christiano [2019] describes AGIs gaining influence within our current economic and political systems by taking or being given control of companies and institutions. Eventually "we reach the point where we could not recover from a correlated automation failure" - after which those AGIs are no longer incentivised to follow human laws. Hanson [2016] also lays out a scenario in which virtual minds come to dominate the economy (although he is less worried about misalignment, partly because he focuses on

[26]For an exploration of the possible consequences of software-based intelligence (as distinct from the consequences of increased intelligence) see Hanson [2016].

emulated human minds). In both scenarios, biological humans lose influence because they are less competitive at strategically important tasks, but no single AGI is able to seize control of the world. To some extent these scenarios are analogous to our current situation, in which large corporations and institutions are able to amass power even when most humans disapprove of their goals. However, since these organisations are staffed by humans, there are still pressures on them to be aligned with human values which won't apply to groups of AGIs.

By contrast, Yudkowsky et al. [2008] and Bostrom [2014] describe scenarios where a single AGI gains power primarily through technological breakthroughs, in a way that's largely separate from the wider economy. The key assumption which distinguishes this category of scenarios from the previous category is that a single AGI will be able to gain enough power via such breakthroughs that they can seize control of the world. Descriptions of these scenarios have featured superhuman nanotechnology, biotechnology, and hacking; however, detailed characterisations are difficult because the relevant technologies don't yet exist. Yet it seems very likely that there exist some future technologies which would provide a decisive strategic advantage if possessed only by a single actor, and so the key factor influencing the plausibility of these scenarios is whether AI development will be rapid enough to allow such concentration of power, as I discuss below.

In either case, humans and aligned AIs end up with much less power than misaligned AIs, which could then appropriate our resources towards their own goals. An even worse scenario is if misaligned AGIs act in ways which are deliberately hostile to human values - for example, by making threats to force concessions from us [Clifton, 2020]. How can we avoid these scenarios? It's tempting to aim directly towards the final goal of being able to align arbitrarily intelligent AIs, but I think that the most realistic time horizon to plan towards is the point when AIs are much better than humans at doing safety research. So our goal should be to ensure that those AIs are aligned, and that their safety research will be used to build their successors. Which category of disaster is most likely to prevent that depends not only on the intelligence, agency and goals of the AIs we end up developing, but also on the four factors listed above, which I'll explore in more detail now.

5.2 Speed of AI development

If AI development proceeds very quickly, then our ability to react appropriately will be much lower. In particular, we should be interested in how long it will take for AGIs to proceed from human-level intelligence to superintelligence, which we'll call the *takeoff period*. The history of systems like AlphaStar, AlphaGo and OpenAI Five provides some evidence that this takeoff period will be short: after a long development period, each of them was able to improve rapidly from top amateur level to superhuman performance. A similar phenomenon occurred during human evolution, where it only took us a few million years to become much more intelligent than chimpanzees. In our case one of the key factors was scaling up our brain hardware - which, as I have already discussed, will be much easier for AGIs than it was for humans.

While the question of what returns we will get from scaling up hardware and training time is an important one, in the long term the most important question is what returns we should expect from scaling up the intelligence of scientific researchers - because eventually AGIs themselves will be doing the vast majority of research in AI and related fields (in a process I've been calling *recursive improvement*). In particular, within the range of intelligence we're interested in, will a given increase δ in the intelligence of an AGI increase the intelligence of the best successor that AGI can develop by more than or less than δ? If more, then recursive improvement will eventually speed up the rate of progress in AI research dramatically. In favour of this hypothesis, Yudkowsky [2013] argues:

> The history of hominid evolution to date shows that it has not required exponentially greater amounts of evolutionary optimization to produce substantial real-world gains in cognitive performance - it did not require ten times the evolutionary interval to go from Homo erectus to Homo sapiens as from Australopithecus to Homo erectus. All compound interest returned on discoveries such as the invention of agriculture, or the invention of science, or the invention of computers, has occurred without any ability of humans to reinvest technological dividends to increase their brain sizes, speed up their neurons, or improve the low-level algorithms used by their neural circuitry. Since an AI can reinvest the fruits of its intelligence in larger brains, faster processing speeds, and improved low-level algorithms, we should expect an AI's growth curves to be sharply above human growth curves.

I consider this a strong argument that the pace of progress will eventually become much faster than it currently is. I'm much less confident about when the speedup will occur - for example, the positive feedback loop outlined above might not make a big difference until AGIs are already superintelligent, so that the takeoff period (as defined above) is still quite slow. There has been particular pushback against the more extreme fast takeoff scenarios, which postulate a discontinuous jump in AI capabilities before AI has had transformative impacts [Christiano, 2018c, Grace, 2018c]. Some of the key arguments:

1. The development of AGI will be a competitive endeavour in which many researchers will aim to build general cognitive capabilities into their AIs, and will gradually improve at doing so. This makes it unlikely that there will be low-hanging fruit which, when picked, allow large jumps in capabilities. (Arguably, cultural evolution was this sort of low-hanging fruit during human evolution, which would explain why it facilitated such rapid progress.)

2. Compute availability, which on some views[27] is the key driver of progress

[27] See Sutton [2019].

in AI, increases fairly continuously.

3. Historically, continuous technological progress has been much more common than discontinuous progress [Grace, 2018b]. For example, progress on chess-playing AIs was steady and predictable over many decades [Grace, 2018a].

Note that these three arguments are all consistent with AI development progressing continuously but at an increasing pace, as AI systems contribute to it an increasing amount.

5.3 Transparency of AI systems

A transparent AI system is one whose thoughts and behaviour we can understand and predict; we could be more confident that we can maintain control over an AGI if it were transparent. If we could tell when a system is planning treacherous behaviour, then we could shut it down before it gets the opportunity to carry out that plan. Note that such information would also be valuable for increasing human coordination towards dealing with AGIs; and of course for training, as I discussed briefly in the previous section.

Hubinger [2019b] lists three broad approaches to making AIs more transparent. One is by creating interpretability tools which allow us to analyse the internal functioning of an existing system. While our ability to interpret human and animal brains is not currently very robust, this is partly because research has been held back by the difficulty of making high-resolution measurements. By contrast, in neural networks we can read each weight and each activation directly, as well as individually changing them to see what happens. On the other hand, if our most advanced systems change rapidly, then previous transparency research may quickly become obsolete. In this respect, neuroscientists - who can study one brain architecture for decades - have it easier.

A second approach is to create training incentives towards transparency. For example, we might reward an agent for explaining its thought processes, or for behaving in predictable ways. Interestingly, ideas such as the cooperative eye hypothesis imply that this occurred during human evolution, which suggests that multi-agent interactions might be a useful way to create such incentives (if we can find a way to prevent incentives towards deception from also arising).

A third approach is to design algorithms and architectures that are inherently more interpretable. For example, a model-based planner like AlphaGo explores many possible branches of the game tree to decide which move to take. By examining which moves it explores, we can understand what it's planning before it chooses a move. However, in doing so we rely on the fact that AlphaGo uses an exact model of Go. More general agents in larger environments will need to plan using compressed representations of those environments, which will by default be much less interpretable. It also remains to be seen whether transparency-friendly architectures and algorithms can be competitive with the performance of more opaque alternatives, but I strongly suspect not.

Despite the difficulties inherent in each of these approaches, one advantage we do have in transparency analysis is access to different versions of an AI over time. This mechanism of cross-examination in Debate takes advantage of this [Barnes and Christiano, 2020]. Or as a more pragmatic example, if AI systems which are slightly less intelligent than humans keep trying to deceive their supervisors, that's pretty clear evidence that the more intelligent ones will do so as well. However, this approach is limited because it doesn't allow us to identify unsafe plans until they affect behaviour. If the realisation that treachery is an option is always accompanied by the realisation that treachery won't work yet, we might not observe behavioural warning signs until an AI arises which expects its treachery to succeed.

5.4 Constrained deployment strategies

If we consider my earlier analogy of a modern human dropped in the stone age, one key factor that would prevent them from taking over the world is that they would be "deployed" in a very constrained way. They could only be in one place at a time; they couldn't travel or even send messages very rapidly; they would not be very robust to accidents; and there would be little existing infrastructure for them to leverage. By contrast, it takes much more compute to train deep learning systems than to run them - once an AGI has been trained, it will likely be relatively cheap to deploy many copies of it. A misaligned superintelligence with internet access will be able to create thousands of duplicates of itself, which we will have no control over, by buying (or hacking) the necessary hardware. At this point, our intuitions about the capabilities of a "single AGI" become outdated, and the "second species" terminology becomes more appropriate.

We can imagine trying to avoid this scenario by deploying AGIs in more constrained ways - for example by running them on secure hardware and only allowing them to take certain pre-approved actions (such as providing answers to questions) [Ngo, 2020e]. This seems significantly safer. However, it also seems less likely in a competitive marketplace - judging by today's trends, a more plausible outcome is for almost everyone to have access to an AGI personal assistant via their phone. This brings us to the fourth factor:

5.5 Human political and economic coordination

By default, we shouldn't rely on a high level of coordination to prevent AGI safety problems. We haven't yet been able to coordinate adequately to prevent global warming, which is a well-documented, gradually-worsening problem. In the case of AGI deployment, the extrapolation from current behaviour to future danger is much harder to model clearly. Meanwhile, in the absence of technical solutions to safety problems, there will be strong short-term economic incentives to ignore the lack of safety guarantees about speculative future events.

However, this is very dependent on the three previous points. It will be much easier to build a consensus on how to deal with superintelligence if AI systems approach then surpass human-level performance over a timeframe of decades, rather than weeks or months. This is particularly true if less-capable systems display misbehaviour which would clearly be catastrophic if performed by more capable agents. Meanwhile, different actors who might be at the forefront of AGI development - governments, companies, nonprofits - will vary in their responsiveness to safety concerns, cooperativeness, and ability to implement constrained deployment strategies. And the more of them are involved, the harder coordination between them will be.

6 Conclusion

Let's recap the second species argument as originally laid out, along with the additional conclusions and clarifications from the rest of the report.

1. We'll build AIs which are much more intelligent than humans; *that is, much better than humans at using generalisable cognitive skills to understand the world.*

2. Those AGIs will be autonomous agents which pursue long-term, large-scale goals, *because goal-directedness is reinforced in many training environments, and because those goals will sometimes generalise to be larger in scope.*

3. Those goals will by default be misaligned with what we want, *because our desires are complex and nuanced, and our existing tools for shaping the goals of AIs are inadequate.*

4. The development of autonomous misaligned AGIs would lead to them gaining control of humanity's future, *via their superhuman intelligence, technology and coordination - depending on the speed of AI development, the transparency of AI systems, how constrained they are during deployment, and how well humans can cooperate politically and economically.*

Personally, I am most confident in 1, then 4, then 3, then 2 (in each case conditional on all the previous claims) - although I think there's room for reasonable disagreement on all of them. In particular, the arguments I've made about AGI goals might have been too reliant on anthropomorphism. Even if this is a fair criticism, though, it's also very unclear how to reason about the behaviour of generally intelligent systems without being anthropomorphic. The main reason we expect the development of AGI to be a major event is because the history of humanity tells us how important intelligence is. But it wasn't just our intelligence that led to human success - it was also our relentless drive to survive and thrive. Without that, we wouldn't have gotten anywhere. So when trying to predict the impacts of AGIs, we can't avoid thinking about what will lead them to choose some types of intelligent behaviour over others - in other words, thinking about their motivations.

Note, however, that the second species argument, and the scenarios I've outlined above, aren't meant to be comprehensive descriptions of all sources of existential risk from AI. Even if the second species argument doesn't turn out to be correct, AI will likely still be a transformative technology, and we should try to minimise other potential harms. In addition to the standard misuse concerns laid out in Brundage et al. [2018] (e.g. about AI being used to develop weapons), we might also worry about increases in AI capabilities leading to undesirable structural changes [Zwetsloot and Dafoe, 2019]. For example, they might shift the offense-defence balance in cybersecurity [Garfinkel and Dafoe, 2019], or lead to more centralisation of human economic power. I consider Christiano [2019]'s "going out with a whimper" scenario to also fall into this category. Yet there's been little in-depth investigation of how structural changes might lead to long-term harms, so I am inclined to not place much credence in such arguments until they have been explored much more thoroughly.

By contrast, I think the AI takeover scenarios that this report focuses on have received much more scrutiny - but still, as discussed previously, have big question marks surrounding some of the key premises. However, it's important to distinguish the question of how likely it is that the second species argument is correct, from the question of how seriously we should take it. Often people with very different perspectives on the latter actually don't disagree very much on the former. I find the following analogy from Stuart Russell illustrative: suppose we got a message from space telling us that aliens would be landing on Earth sometime in the next century. Even if there's doubt about the veracity of the message, and there's doubt about whether the aliens will be hostile, we (as a species) should clearly expect this event to be a huge deal if it happens, and dedicate a lot of effort towards making it go well. In the case of AGI, while there's reasonable doubt about what it will look like, its development may nevertheless be the biggest thing that's ever happened. At the very least we should put serious effort into understanding the arguments I've discussed above, how strong they are, and what we might be able to do about them.[28]

7 Acknowledgements

This report benefited greatly from the contributions of a number of people. In particular I'm grateful to Joe Carlsmith, Will MacAskill, Daniel Kokotajlo, Rohin Shah, Vladimir Mikulik, Beth Barnes, and Ben Garfinkel, for discussions which shaped the ideas presented here. Thanks also to many others who gave feedback (much of which can be found on the Alignment Forum).

[28] I want to explicitly warn against taking this argument too far, though - for example, by claiming that AI safety work should still be a major priority even if the probability of AI catastrophe is much less than 1%. This claim is misleading because most researchers in the field of safety think it's much higher than that; and also because, if it really is that low, there are probably some fundamental confusions in our concepts and arguments that need to be cleared up before we can actually start object-level work towards making AI safer.

References

Sanjeev Arora. Is optimization a sufficient language for understanding deep learning?, 2019. URL http://www.offconvex.org/2019/06/03/trajectories/.

Beth Barnes and Paul Christiano. Writeup: Progress on AI safety via debate, 2020. URL https://www.alignmentforum.org/posts/Br4xDbYu4Frwrb64a/writeup-progress-on-ai-safety-via-debate-1.

Nick Bostrom. The superintelligent will: Motivation and instrumental rationality in advanced artificial agents. *Minds and Machines*, 22(2):71–85, 2012. URL https://www.nickbostrom.com/superintelligentwill.pdf.

Nick Bostrom. *Superintelligence: Paths, dangers, strategies*. 2014.

Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, and Dario Amodei. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation, 2018. URL https://arxiv.org/abs/1802.07228.

Paul Christiano. Ambitious vs. narrow value learning, 2015. URL https://ai-alignment.com/ambitious-vs-narrow-value-learning-99bd0c59847e.

Paul Christiano. Clarifying ”AI alignment”, 2018a. URL https://ai-alignment.com/clarifying-ai-alignment-cec47cd69dd6.

Paul Christiano. Open question: are minimal circuits daemon-free?, 2018b. URL https://www.alignmentforum.org/posts/nyCHnY7T5PHPLjxmN/open-question-are-minimal-circuits-daemon-free.

Paul Christiano. Takeoff speeds, 2018c. URL https://sideways-view.com/2018/02/24/takeoff-speeds/.

Paul Christiano. What failure looks like, 2019. URL https://www.alignmentforum.org/posts/HBxe6wdjxK239zajf/what-failure-looks-like.

Paul Christiano, Jan Leike, Tom B. Brown, Miljan Martic, Shane Legg, and Dario Amodei. Deep reinforcement learning from human preferences. 2017. URL https://openai.com/blog/deep-reinforcement-learning-from-human-preferences.

Paul Christiano, Buck Shlegeris, and Dario Amodei. Supervising strong learners by amplifying weak experts, 2018. URL https://arxiv.org/abs/1810.08575.

Jesse Clifton. Cooperation, conflict, and transformative artificial intelligence: A research agenda. 2020. URL https://longtermrisk.org/files/Cooperation-Conflict-and-Transformative-Artificial-Intelligence-A-Research-Agenda.pdf.

Daniel Clement Dennett. *The intentional stance*. MIT press, 1989.

K. Eric Drexler. Reframing superintelligence: Comprehensive AI services as general intelligence. Technical Report 2019-1, Future of Humanity Institute, University of Oxford, 2019. URL https://www.fhi.ox.ac.uk/wp-content/uploads/Reframing_Superintelligence_FHI-TR-2019-1.1-1.pdf.

Robin IM Dunbar. The social brain hypothesis. *Evolutionary Anthropology: Issues, News, and Reviews: Issues, News, and Reviews*, 6(5):178–190, 1998. URL http://archives.evergreen.edu/webpages/curricular/2006-2007/languageofpolitics/files/languageofpolitics/Evol_Anthrop_6.pdf.

Adrien Ecoffet, Jeff Clune, and Joel Lehman. Open questions in creating safe open-ended AI: Tensions between control and creativity, 2020. URL https://arxiv.org/abs/2006.07495.

Iason Gabriel. Artificial intelligence, values, and alignment. *Minds and Machines*, 30(3):411–437, Sep 2020. ISSN 1572-8641. doi: 10.1007/s11023-020-09539-2. URL http://dx.doi.org/10.1007/s11023-020-09539-2.

Yaroslav Ganin, Evgeniya Ustinova, Hana Ajakan, Pascal Germain, Hugo Larochelle, François Laviolette, Mario Marchand, and Victor Lempitsky. Domain-adversarial training of neural networks, 2016. URL https://arxiv.org/abs/1505.07818.

Ben Garfinkel and Allan Dafoe. How does the offense-defense balance scale? *Journal of Strategic Studies*, 42(6):736–763, 2019. doi: 10.1080/01402390.2019.1631810. URL https://doi.org/10.1080/01402390.2019.1631810.

Katja Grace. Historic trends in chess AI, 2018a. URL https://aiimpacts.org/historic-trends-in-chess-ai/.

Katja Grace. Discontinuous progress investigation, 2018b. URL https://aiimpacts.org/discontinuous-progress-investigation/.

Katja Grace. Likelihood of discontinuous progress around the development of agi, 2018c. URL https://aiimpacts.org/likelihood-of-discontinuous-progress-around-the-development-of-agi/.

Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, and Owain Evans. When will AI exceed human performance? evidence from ai experts, 2018. URL https://arxiv.org/abs/1705.08807.

Arthur Guez, Mehdi Mirza, Karol Gregor, Rishabh Kabra, Sébastien Racanière, Théophane Weber, David Raposo, Adam Santoro, Laurent Orseau, Tom Eccles, Greg Wayne, David Silver, and Timothy Lillicrap. An investigation of model-free planning, 2019. URL https://arxiv.org/abs/1901.03559.

Robin Hanson. *The Age of Em: Work, Love, and Life when Robots Rule the Earth*. Oxford University Press, 2016. URL https://ageofem.com.

Evan Hubinger. Gradient hacking, 2019a. URL https://www.alignmentforum.org/posts/uXH4r6MmKPedk8rMA/gradient-hacking.

Evan Hubinger. Relaxed adversarial training for inner alignment, 2019b. URL https://www.alignmentforum.org/posts/9Dy5YRaoCxH9zuJqa/relaxed-adversarial-training-for-inner-alignment.

Evan Hubinger, Chris van Merwijk, Vladimir Mikulik, Joar Skalse, and Scott Garrabrant. Risks from learned optimization in advanced machine learning systems. *arXiv preprint arXiv:1906.01820*, 2019. URL https://arxiv.org/abs/1906.01820.

Geoffrey Irving, Paul Christiano, and Dario Amodei. AI safety via debate, 2018. URL https://arxiv.org/abs/1810.08575.

Victoria Krakovna, Jonathan Uesato, Vladimir Mikulik, Matthew Rahtz, Tom Everitt, Ramana Kumar, Zac Kenton, Jan Leike, and Shane Legg. Specification gaming: the flip side of AI ingenuity. 2020. URL https://deepmind.com/blog/article/Specification-gamingthe-flip-side-of-AI-ingenuity.

Shane Legg and Marcus Hutter. Universal intelligence: A definition of machine intelligence. 2007. URL https://arxiv.org/abs/0712.3329.

Joel Z. Leibo, Edward Hughes, Marc Lanctot, and Thore Graepel. Autocurricula and the emergence of innovation from social interaction: A manifesto for multi-agent intelligence research, 2019. URL https://arxiv.org/abs/1903.00742.

Jan Leike, David Krueger, Tom Everitt, Miljan Martic, Vishal Maini, and Shane Legg. Scalable agent alignment via reward modeling: a research direction, 2018. URL https://arxiv.org/abs/1811.07871.

David Manheim and Scott Garrabrant. Categorizing variants of Goodhart's law, 2018. URL https://arxiv.org/abs/1803.04585.

Hans Moravec. *Mind children: The future of robot and human intelligence*. Harvard University Press, 1988.

Oskar Morgenstern and John Von Neumann. *Theory of games and economic behavior*. Princeton university press, 1953.

Luke Muehlhauser. *Facing the Intelligence Explosion*. 2013. URL https://intelligenceexplosion.com/2011/plenty-of-room-above-us/.

Richard Ngo. Comments on CAIS, 2019a. URL https://www.alignmentforum.org/posts/HvNAmkXPTSoA4dvzv/comments-on-cais.

Richard Ngo. Coherent behaviour in the real world is an incoherent concept, 2019b. URL https://www.alignmentforum.org/posts/vphFJzK3mWA4PJKAg/coherent-behaviour-in-the-real-world-is-an-incoherent.

Richard Ngo. AGIs as collectives, 2020a. URL https://www.alignmentforum.org/posts/HekjhtWesBWTQW5eF/agis-as-populations.

Richard Ngo. Environments as a bottleneck in AGI development, 2020b. URL https://www.alignmentforum.org/posts/vqpEC3MPioHX7bv4t/environments-as-a-bottleneck-in-agi-development.

Richard Ngo. Arguments against myopic training, 2020c. URL https://www.alignmentforum.org/posts/GqxuDtZvfgL2bEQ5v/arguments-against-myopic-training.

Richard Ngo. Safety via selection for obedience, 2020d. URL https://www.alignmentforum.org/posts/7jNveWML34EsjCD4c/safety-via-selection-for-obedience.

Richard Ngo. Safer sandboxing via collective separation, 2020e. URL https://www.alignmentforum.org/posts/Fji2nHBaB6SjdSscr/safer-sandboxing-via-population-separation.

Pedro A Ortega, Vishal Maini, and DeepMind Safety Team. Building safe artificial intelligence: specification, robustness, and assurance. *DeepMind Safety Research Blog*, 2018. URL https://medium.com/@deepmindsafetyresearch/building-safe-artificial-intelligence-52f5f75058f1.

Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. Language models are unsupervised multitask learners. *OpenAI blog*, 1(8):9, 2019. URL https://d4mucfpksywv.cloudfront.net/better-language-models/language_models_are_unsupervised_multitask_learners.pdf.

Stuart J. Russell. *Human Compatible*. 2019.

Kaj Sotala. Collection of GPT-3 results, 2020. URL https://www.alignmentforum.org/posts/6Hee7w2paEzHsD6mn/collection-of-gpt-3-results.

Richard Sutton. The bitter lesson. *Incomplete Ideas*, 2019. URL http://www.incompleteideas.net/IncIdeas/BitterLesson.html.

Jessica Taylor. Quantilizers: A safer alternative to maximizers for limited optimization. In *AAAI Workshop: AI, Ethics, and Society*, 2016. URL http://intelligence.org/files/QuantilizersSaferAlternative.pdf.

Eliezer Yudkowsky. Levels of organization in general intelligence. In *Artificial general intelligence*, pages 389–501. Springer, 2007. URL https://arxiv.org/abs/1505.07818.

Eliezer Yudkowsky. Intelligence explosion microeconomics. *Machine Intelligence Research Institute, accessed online October*, 23:2015, 2013. URL https://intelligence.org/files/IEM.pdf.

Eliezer Yudkowsky. Comment on Paul Christiano's research agenda, 2018. URL https://www.alignmentforum.org/posts/Djs38EWYZG8o7JMWY/paul-s-research-agenda-faq?commentId=79jM2ecef73zupPR4.

Eliezer Yudkowsky et al. Artificial intelligence as a positive and negative factor in global risk. *Global catastrophic risks*, 1(303):184, 2008. URL https://intelligence.org/files/AIPosNegFactor.pdf.

Remco Zwetsloot and Allan Dafoe. Thinking about risks from AI: accidents, misuse and structure. *LawfareBlog. com, February*, 11, 2019. URL https://www.lawfareblog.com/thinking-about-risks-ai-accidents-misuse-and-structure.