

RingTMP: Locally Distributed Machine Learning on Low Power Devices



Prifysgol Abertawe
Swansea University

Christopher Hopkins

Department of Computer Science
Swansea University

This dissertation is submitted for the degree of
Bachelor

April 17, 2021

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 40,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 100 figures.

Christopher Hopkins

October 2020

Abstract

More data than ever is being produced by low power devices such as smart phones and Internet of Things (IoT) devices at the network edge. The data being produced is so enormous it would be infeasible to send it to a centralised location. Instead models can be trained from data distributed across multiple edge nodes, with machine learning algorithms being performed locally. In this paper I explore training multiple low power devices using a new distributed machine learning paradigm *RingTMP*. This paradigm focuses on low power usage and power efficiency while having the capacity for larger models than comparative systems.

Contents

1	Introduction	1
1.1	Motivation and Context	1
2	Background Research	2
2.1	Brief Introduction to Machine Learning, Neural Networks and Stochastic Gradient Descent	2
2.2	The Communication Issue	3
2.3	Limited History of Distributed Machine Learning	4
2.4	Model and Data Parallelism	4
2.5	Low Power Hardware, IoT and Mobile Computation	6
3	Project Plan and Time Management	8
3.1	Software Life Cycle	9
3.2	Research Methodology	9
3.3	Risk Assessment	10
4	Conclusion	13
	References	14

1 Introduction

1.1 Motivation and Context

Machine Learning has become an invisible but ubiquitous part of modern life, and is being used in a plethora of fields and industries. The uses of this technology range from dystopian facial recognition [1] to lifesaving diagnoses [2] and many more purposes besides. Machine Learning leverages existing data to train Machine Learning models in order to perform a task or find patterns, that previously only a human could. The key difference between Machine Learning and conventional programs is that the data itself is used to develop the model. Therefore the quality and quantity of the data can affect the effectiveness of a machine learning model.

As the amount and complexity of the data we are collecting increases so does the size and complexity of the machine learning models we use to make sense of our data. For example the internet archive as of 2020 contains over 70 petabytes of data, while labeled datasets such as AViD have video data in the order of terabytes. [3] We are now reaching a point where the limiting factor of creating a machine learning model is not the data, but the machine learning algorithm itself.

This problem is two pronged. First machine learning models are getting very, very large. For instance GPT-3 the largest Natural Language Model ever trained contains 175 billion parameters. [4] And efforts are being made to create models with trillions of parameters. [5] We have reached the point where its no longer possible to store some machine learning models on a single machine.

The second problem is that training a machine learning model is increasingly taking longer and longer. This is because we have more data and larger models, but the algorithms used to train models have fundamentally stayed the same and are inherently sequential and difficult to parallelise.

2 Background Research

2.1 Brief Introduction to Machine Learning, Neural Networks and Stochastic Gradient Descent

To first understand Distributed Machine Learning you must first understand the fundamentals of Machine Learning and Neural networks.

There are many machine learning methods some requiring training data which we call supervised and some being able to find patterns in data without being given solutions called unsupervised. [?] An example of a supervised system may be predicting house prices, using multiple factors about each house (market data, geographic area, square footage etc.) to come to a conclusion about what the house could sell for. This would be trained using data of previously sold houses to predict current ones. An example of an unsupervised system could be identification of new plant species. This could be done by taking as many features of a plant as possible, then apply a clustering algorithm to see if there are two distinct clusters in the data. If there were then that would suggest two different plant species. Neural networks tend to focus on supervised learning and use a form gradient descent called Stochastic Gradient Descent.

Many machine learning algorithms use a cost function to measure how well or badly they are solving a problem, these algorithms use parameters which are internal variables of a machine learning model and define how they solve the problem. If you map $costFunction(x)$, where x is the model parameter, for every x value. Then a graph will be produced $y = costFunction(x)$, the lowest point on the graph will be the global minimum. There may be other troughs higher than the global minimum these are called local minimums. A global minimum represents the lowest value of the cost function which indicates the parameter values produce the best solution for your problem. Initial model parameters are often randomised, meaning they may start at a high point on the cost function graph, the goal is to get to the lowest point possible. To do this you must *descend* down the *gradient* to a local minima, the algorithm that does this is called gradient descent for that very reason. This often happens in little steps after the observation of each piece of data. However it is computationally expensive to step down the gradient after each example. It is more efficient to calculate the average step of a randomised selection of data. This is know as Stochastic

Gradient Descent.

Neural networks are structures that can perform multi-variable gradient descent when provided with training data. Neural networks are comprised of layers of interconnected neurons in a lattice like structure. Each neuron holds parameter information the adjusting of which through stochastic gradient descent leads to the solving of a problem through reaching the local minimum of the cost function.

2.2 The Communication Issue

Distributed neural networks must communicate with each other in some way in order to work together. This needs to be formalised to be able to measure the efficiency of our machine learning system. Parts of this reasoning already appears in these papers too. [?, ?]

If we consider how a neural network operates if we were to run it on a single node, we could characterise its computation as such:

$$TIME = I_A(\epsilon) \times T_A \quad (1)$$

Where $I_A(\epsilon)$ is the number of iterations of the algorithm A it takes to reach accuracy ϵ and T_A is the time of each iteration of the algorithm. Here maximising the convergence per iteration or decreasing the time an iteration takes will decrease the runtime of the algorithm. In a distributed setting this equation changes to this:

$$TIME = I_A(\epsilon) \times (c + T_A) \quad (2)$$

In this equation we have the added variable c , this represents time taken for communication per iteration. In a distributed setting this will always remain above a non trivial amount of data. Unfortunately The majority of machine learning algorithms use a stochastic method which means a very large number of iterations ($I_A(\epsilon)$) that take a short amount of time (small T_A). You can see that no matter how small c is there will be a significant impact of the time taken. In fact with a naive approach of communication each iteration almost certainly $c > T_A$.

However this view doesn't take into account the possibility that communication could happen at the same time as an iteration. For example imagine a pipeline of nodes where

each nodes performs an iteration but can communicate its previous iteration to the next node at the same time. Then the time taken could be described like so:

$$TIME = I_A(\epsilon) \times \max(c, T_A) \quad (3)$$

Here you can see that if you can find a way of making the communication time equal to the time per iteration. Then c would have a negligible effect on the equation.

2.3 Limited History of Distributed Machine Learning

One of the first pieces of research into distributed machine learning was 'Distributed Inference for Latent Dirichlet Allocation' in 2008 [?]. One of the first instances of distributed machine learning was used to categorise New York Times articles using Latent Dirichlet Allocation (LDA), which identifies the affiliations words have to certain topics. While the paper focused on parallelising the algorithm and running them over multiple artificially isolated cores the results showed that distributed machine learning could have scalability and didn't impact the rate of convergence of the model significantly. This was followed by a paper by Jia et al. [?] which produced much faster results than its predecessors by using memcache layer in every machine, every machine would message every other machine with updates of its local parameters to create an approximate global state, it was mentioned in passing that arranging the nodes in a star topology and caching the values that passed through it could make the system more scalable. After this followed a cambrian explosion of work in this area [?, ?, ?, ?] culminating in 2014 when the parameter server as it is known today [?] was produced. This parameter server is highly sophisticated and flexible accommodating the difference in hardware components while spending more on computation and less time waiting.

2.4 Model and Data Parallelism

When creating distributed machine learning models there two different methods for distributing training, model parallelism and data parallelism. These two methods are not mutually exclusive and can be used in conjunction with one another, such as in DistBelief. [?]. model parallelism is when model parameters are split between the nodes. As data parallelism is when the data is split between the nodes. [?] Often with model parallelism the whole set of

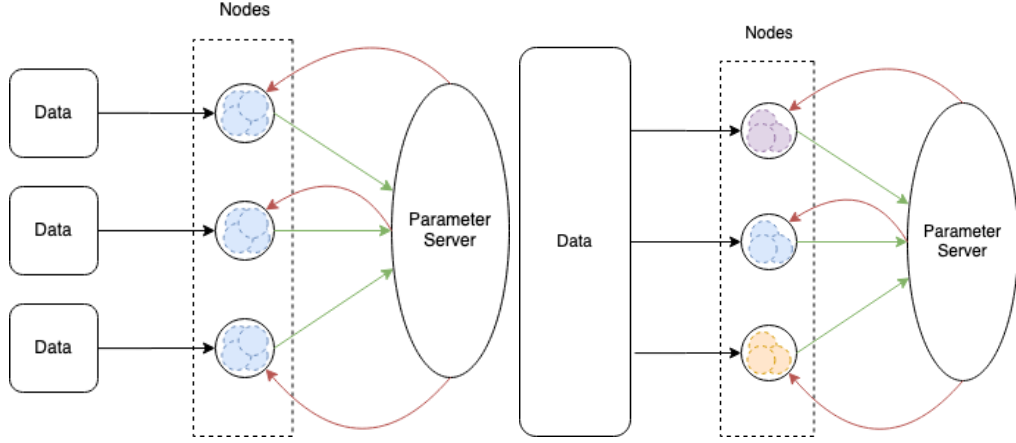


Figure 1: Left: Data Parallelism. Right: Model Parallelism. In both diagrams the green lines indicate local parameters being sent to the parameter server and red lines indicate parameters being sent to the worker nodes.

training data is passed through each node. While in data parallelism its common for each node to hold the whole machine learning model.

The key advantage of model parallelism is that machine learning models can be far larger as they no longer have to sit on one machine. However this one great advantage comes with some disadvantages. Some parameters may take more time to converge than others, this means that at times some nodes may be idle while others are still converging, so the spread of computation is not equal or efficient. [?] Because some parameters converge at different rates a scheduler can be used, which does improve model convergence. However this requires more computational overhead and communication and reduces iteration throughput. [?]

data parallelism has the benefit that data throughput can be very large, making processing using this method very fast. However with more nodes the communication overhead increases as the nodes must communicate the changes in their model parameters to each other. [?] The nodes can communicate with each other synchronously, but this means the computation is only as fast as the slowest node. If the nodes communicate with each other asynchronously then some of the calculations will be made on out of date model parameters so training examples may be needlessly wasted.

2.5 Low Power Hardware, IoT and Mobile Computation

Historically machine learning algorithms have been focused on high model accuracy through large models and vast amounts of training data, energy consumption and efficiency has rarely been taken into consideration. However with the rise of Internet of Things (IoT) devices and the established ubiquity of smart phones more data than ever is being produced. Soon this data generation will exceed the capacity of the internet, and experts estimate that over 90% of data will be stored and processed locally. [?] By extension this means machine learning algorithms will have to be performed locally too. This introduces some challenging issues. Modern machine learning algorithms require vast computational power and large amounts of data. Local devices don't have the capacity to hold large data sets or the power to compute large machine learning models in a viable amount of time, while many of them are also battery powered so power consumption becomes another issue.

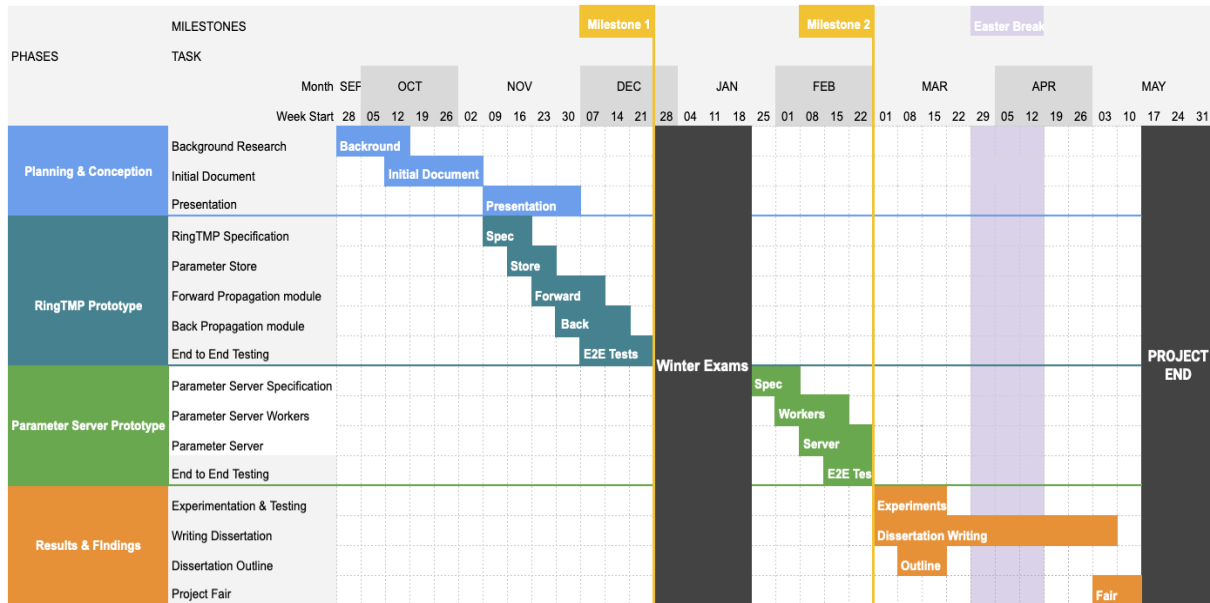
A solution to this is to massively distribute the model over multiple decentralised nodes. The level of distribution is even greater than that of centralised compute clusters. In this solution each device computes a model using its own local data, infrequently (due to network constraints) the model is shared with a coordination server, which will then distribute the changes across all nodes in the network. [?] While this method is inefficient as the infrequent communications mean that many nodes may do much of the same work, and the merging of local models into a global one infrequently may cause loss of information. It still produces a model which converges in a relatively few rounds of communication. [?]

Efforts have been made in techniques to reduce the power memory and storage needed for machine learning algorithms to operate. One of these is Data Stream Mining. The idea is that a device can stream the analytics data directly into the model rather than storing the data in storage for later use. [?] This means after the data has been read by the model it is lost. But that also means that no data needs to be stored, meaning resources are not spent reading and writing to storage. This has an application in mobile devices, as they produce data at a low rate through user interaction. Therefore the model can be built in real time as actions occur. The data produced on the mobile itself may not be enough to effectively train the model, but via communication with other users distributed over the network the model can converge. [?]

From the research available there seems to be research into distributed computing on local

devices, investigation in to power measurements of machine learning algorithms [?, ?] and power reduction of machine learning algorithms on local devices. [?] But there is a distinct lack of research into efficiency of *distributed algorithms* from the perspective of efficiency and power consumption on local devices. Having a more power efficient distributed machine learning algorithm, even if the optimisation was marginal on each device, would have an enormous effect on the output of the system, as many devices are connected.

3 Project Plan and Time Management



The Gantt chart above outlines the order and time frame each task should take in order to complete this dissertation on time and to a high quality. Building a RingTMP prototype of my system is the most important task to embark on. It is better to do this first as it will take the longest time to produce and has the most 'unknown unknowns', moreover this is the centrepiece of my project, if I have not finished this there will be no dissertation to write. I then take a month break to revise for my exams. I acknowledge that this is a long time, however the semester 1 modules contribute more to my final grade than my dissertation does, therefore it's important this project isn't detrimental to my grades in other modules. After Christmas I'll start work on a basic prototype of a parameter server. This will use the same tools and languages as my framework. In this way it will be easy to compare and contrast the benefits and shortcomings of each system on a level playing field. Once both pieces of software have been complete I will run various tests to see how well my aims have been achieved. While I'm conducting these tests I shall also be writing up my results. Once my experiments have finished I shall start working on my dissertation document in earnest. I'll hand in my outline a week before Easter break and shall keep working till it is complete.

3.1 Software Life Cycle

The methodology I will use to produce my software will be a variation of Agile methodology. Generally speaking Agile software development models tend to take the form of doing a small amount of specification upfront and thereafter working in small cycles to design, develop, validate and deploy a new version of software. Agile development places particular focus on showing customers working versions of the software as early as possible and being able to adapt to changing customer requirements easily. [?] However the pure Agile methodology does not completely suit my needs, as Agile programming is customer focused and my project is not. Agile programming also focuses on changing customer requirements. However there will be no changing requirements from a customer as there is none. On the other hand optimising for working software over small iterations is a good philosophy for my work. Therefore my methodology will specify work upfront and then follow an agile workflow with week long iterations. I can do this as I won't be beholden to a customer. This will mean that I have more of an architectural design roadmap than if I were following a pure Agile methodology.

I also intend to take this iterative methodology to a smaller scale using Test Driven Development. [?] This is a philosophy where you write your tests before you write your code for each logical block. This means you specify the code's function before you have written it and you have solid acceptance criteria for when that piece of code is working. If a piece of code is too complex to test then that is an indication that your logical block needs to be broken down into small pieces. This way you end up with highly cohesive but loosely coupled components, and a high degree of confidence that they work. When introducing new features that effect existing code you can instantly see where it is breaking as the tests will fail, saving you valuable debugging time.

3.2 Research Methodology

My project lends itself to using an experimental research methodology to collect my findings, with this in mind it is paramount to ensure that my results are taken in as controlled conditions as possible. I will achieve this by creating two software prototypes, one is my new novel machine learning framework, the other is the established parameter server design. I will make these using the same languages and tools as each other. Only the architecture will differ, meaning comparisons of the two systems will only reflect the performance of the

respective architectures. On these systems I will conduct a series of tests. Each of these tests will compare each system to one another and will correspond to the aims I outlined in the introduction:

- To compare the efficiency of the systems we can measure the idle time of each worker in each of the systems and divide that by the time each system took to train a model on some basic task. This will give us a percentage of how much time the machine spend processing and how much time was spent on communication between nodes. This same experiment can be repeated with a different amount of nodes to see how the results change.
- To compare the progress made per iteration, the loss function can be measured for each iteration in both of the systems, then it is straightforward to see which ones makes the most progress.
- To measure scalability both systems can be run with a varying number of different nodes. In all experiments they are given the same dataset to be trained on. We can measure how long it takes for them to complete the task, and how well both systems scale when more nodes are added.
- To measure resilience a node can be permanently or temporarily removed from each system while a model is being trained. Then the success of its mitigation and recovery strategies can be assessed.
- To discover the limits of how large a neural network each system can hold. Tests which incrementally increase the amount of layers and number of layers until the system crashes can be run.

By doing all this I can measure the performance between these two systems and accurately assess my architecture's performance relative to the parameter server.

3.3 Risk Assessment

A dissertation is a long arduous process in which many things could go wrong. Hence it is best to identify possible hazards and decide how to mitigate them before they happen, whilst also having a contingency plan should anything occur.

Risk: The RingTMP prototype is not finished due to time constraints.

Likelihood: Low

Potential Impact: Severe Impact on the grade for my dissertation.

Mitigation: I have thoroughly researched the tools and algorithms I need to complete this prototype and am familiar with them. This is the first task I will start work on. Meaning that I have the most time to complete it.

Contingency Plan: If I need more time I can reduce the scope of tasks further down the project timeline.

Risk: Winter exams interfere with my project timeline.

Likelihood: Low

Potential Impact: The project becomes behind schedule

Mitigation: The Winter exams have been factored into the project timeline, ensuring that I have enough time to revise and keep the project on schedule.

Risk: Parameter Server more complex than initially believed.

Likelihood: Medium

Potential Impact: The Project becomes behind schedule

Mitigation: I have read many papers on the operations of the parameter server and by being aware with its inner workings. Open source versions of the parameter server can be found that I can use as a template for my own.

Contingency Plan: If the task of creating the parameter server was greatly underestimated, then an open source version could be used though this would have repercussions for the meaningfulness of my findings.

Risk: I contract Coronavirus

Likelihood: Medium

Potential Impact: I have to rest for a number of days, and possibly have lasting symptoms for months after. [?]

Mitigation: By not returning physically to university, I reduce the probability of catching Coronavirus, as the cases are much lower in my current location. My physical social contact will also be kept to a minimum and good hygiene will be observed

Contingency Plan: I will have to isolate for 10 days after displaying symptoms. For the majority of tasks can be completed in isolation. If I am still exhibiting symptoms such as fatigue, cognitive impairment and breathlessness I may have to reassess the scope of the

project and apply for extenuating circumstances.

4 Conclusion

In conclusion machine learning algorithms already power large parts of our digital lives. This is driven by data hungry learning models with potentially billions of parameters. However now so much data is being produced that it is no longer viable to centralise the data, leading to the need for efficient machine learning on-device and communication between devices to improve the model. I have introduced a new machine learning paradigm that should be more power efficient than existing frameworks on low power devices over a local network. I have displayed and explained the relevant research in distributed machine learning and related fields, as well as core machine learning and neural networking concepts. I have also shown the project timeline of building the new framework, my testing methodology and how I will control risk within my project.

References

- [1] W. U. Matt Burgess, “Some uk stores are using facial recognition to track shoppers.”
- [2] S. M. McKinney, M. Sieniek, V. Godbole, J. Godwin, N. Antropova, H. Ashrafian, T. Back, M. Chesus, G. S. Corrado, A. Darzi, M. Etemadi, F. Garcia-Vicente, F. J. Gilbert, M. Halling-Brown, D. Hassabis, S. Jansen, A. Karthikesalingam, C. J. Kelly, D. King, J. R. Ledsam, D. Melnick, H. Mostofi, L. Peng, J. J. Reicher, B. Romera-Paredes, R. Sidebottom, M. Suleyman, D. Tse, K. C. Young, J. De Fauw, and S. Shetty, “International evaluation of an ai system for breast cancer screening,” *Nature*, vol. 577, pp. 89–94, Jan 2020.
- [3] A. Piergiovanni and M. S. Ryoo, “Avid dataset: Anonymized videos from diverse countries,” 2020.
- [4] T. B. Brown, B. Mann, N. Ryder, M. Subbiah, J. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, S. Agarwal, A. Herbert-Voss, G. Krueger, T. Henighan, R. Child, A. Ramesh, D. M. Ziegler, J. Wu, C. Winter, C. Hesse, M. Chen, E. Sigler, M. Litwin, S. Gray, B. Chess, J. Clark, C. Berner, S. McCandlish, A. Radford, I. Sutskever, and D. Amodei, “Language models are few-shot learners,” 2020.
- [5] S. Rajbhandari, J. Rasley, O. Ruwase, and Y. He, “Zero: Memory optimizations toward training trillion parameter models,” 2020.