CONTENTS

I. INTRODUCTION

Today classical machine learning is affecting the understanding and better regulation of classical network systems which can be of use in the modern internet. These include pattern recognition for individual computing devices, security and fault management, routing and traffic management, resource management and distributed computation. In these applications, it is not only the speed of processing that is important, but reliability and security can be paramount.

The large intersection between machine learning and network systems (the internet included) is perhaps not surprising. Firstly, machine learning relies on access to data and in many real-life applications, data naturally arise from distributed sources. Secondly, especially for complex systems like large networks, the information to process is complex and contains many uncertainties and errors. Exactly solvable models in these regimes are few and far between, and machine learning may be helpful in making predictions in these messy environments.

In the coming quantum age we can envision three possible ways where quantum resources can come into our internet: quantum communication, quantum processing at individual nodes and data that is naturally quantum in origin. To begin, we first make a classification of the four different types of networks we can have: see Table (I). We can classify them into (i) CC (classical data and processing over classical network), or the current internet; (ii) CQ (classical data and processing over quantum network); (iii) QC (quantum data and processing over classical network) and (iv) QQ (quantum data and processing over quantum network), or a fully-quantum internet.

So now we can pose the inevitable question: how can these different quantum resources in a network influence the relationship between the internet and machine learning?

This is not yet an active research area in its own right. However, there are some preliminary toolkits we can consider that are starting to be developed in the new field of quantum machine learning. By first summarising the intersection between the classical internet and classical machine learning, it gives us an idea of the kinds of tools we need to begin examining their quantum counterparts. For instance, we will see how aspects of quantum processing of quantum data might be aided by machine learning, how machine learning may be enhanced by quantum resources and also in turn how machine learning may be implemented in these distributed quantum settings. See Table (II) for a brief overview.

II. CLASSICAL MACHINE LEARNING IN CLASSICAL NETWORKS

To create and maintain an efficient classical network, one requires efficient and reliable processing on individual nodes, secure processing, efficient routing and data transmission, efficient uses of resources and a means for distributed information processing. For overview of methods see for example (Boutaba *et al.*, 2018), (Wang *et al.*, 2018). We give a brief overview on how machine learning can be used in each of these areas.

A. Machine learning basics for individual processors

Machine learning algorithms enable one to make predictions about one's current or future dataset without requiring explicit instructions. Since its aims are directed more towards *prediction* rather than purely *estimation*, it differs from the field of statistical estimation even though it shares many common tools.

There are 3 mains paradigms for machine learning: supervised, unsupervised and reinforcement learning. Supervised learning relies on having training data from which to form inferences and to make predictions about new incoming 'test' data. On the other hand, unsupervised learning algorithms make inferences using the data at hand without access to a training stage, much like a student learning without an instructor. Reinforcement learning operates using a different framework and aims to find the best action steps in a particular environment to maximize a given reward.

Machine learning is used regularly for data collection, feature engineering and model learning. There are many excellent references on this broad subject, for instance see the introductory texts (Bishop, 2006; Flach, 2012; Marsland, 2011; Shalev-Shwartz and Ben-David, 2014; Trevor *et al.*, 2009).

B. Machine learning for security and fault management

There are two main ways in which machine learning enters into managing security and faults in networks. The first is *using* machine learning techniques to predict and detect security breeches and faults in a network. These include machine learning algorithms for anomaly detection. The second is studying the security vulnerabilities of machine learning algorithms themselves, as the presence of adversaries becomes natural in a network setting, where real-life machine learning algorithms will be deployed. The latter is known as adversarial machine learning.

1. Anomaly detection and fault management

When there are security breeches in classical data on a network, one desires the ability to predict and detect these disturbances, as well as a method for making one's protocols more robust against these adversaries. Machine learning is often used in anomaly detection and intrusion detection. These algorithms look for unusual data or unusual changes in data. Broadly, there are three classes of anomalies: point, contextual and collective, which refer respectively to single datum anomalies, unusual data with respect to a specified context and clusters of data which together point to an unusual pattern. Both supervised and unsupervised algorithms are used for these settings (Ahmed *et al.*, 2007; Thottan and Ji, 2003). One of the prime challenges here include determining the presence of an anomaly when little data is available and determining the relevant rate of false positives and false negatives for a particular application.

Fault management in a network is also extremely relevant, especially for complex networks where there is more room for errors. One requires the prediction, detection and localisation of the fault, and most relevant machine learning methods use supervised algorithms. However, the paucity of real training data (as opposed to synthetic data generated from simulations) means that the algorithms might be poorly trained, especially in new networks (Hood and Ji, 1997; Kogeda and Agbinya, 2006; Snow *et al.*, 2005). This is expected to be true, for instance, when a quantum internet is first set up. To accommodate for this, new methods have arisen where unsupervised machine learning techniques are used instead to detect changes in the network rather relying on labelled fault data (Hajji, 2005).

In particular, to identify and localise unusual behaviour in a network which can be due to natural faults or an adversarial party, network anomaly detection methods can be employed (Ahmed *et al.*, 2007), (Fraley and Cannady, 2017), (Joseph *et al.*, 2013). Since the results can be sensitive to the training datasets used, it is important to examine which datasets are most appropriate for one's particular applications (see a review of datasets for anomaly detection (Yavanoglu and Aydos, 2017)). In particular, there have been many proposals on using anomaly detection in the network intrusion domain. However, this approach has been criticized for its uses in real-life applications since it's often difficult to distinguish anomalies related to intrusions from those related to other factors and the complexity of real-life networks may make it too difficult to define what is a normal signal (Sommer and Paxson, 2010).

2. Adversarial machine learning

Machine learning algorithms themselves are vulnerable to security attacks. This comes under the field of adversarial machine learning (Huang *et al.*, 2011). There are two main types of attacks: attacks of the test data (evasion) and attacks of the training data and the machine learning models (poisoning). In real-life deployments of machine learning, data often comes from different sources which makes adversarial attacks more probable. It has been discovered that many machine learning algorithms are in fact vulnerable to adversarial attacks, the first discovered in (Szegedy *et al.*, 2013). A large proportion of the literature then focuses on the details of specific algorithms: the detection of adversaries, their different methods of attack and the particular defenses to those attacks (Kurakin *et al.*, 2018). However, recently, more foundational work has emerged to try to explain the origins of this vulnerability as arising from the high dimensionality of the data involved (Gilmer *et al.*, 2018; Goodfellow *et al.*, 2014; Mahloujifar *et al.*, 2018).

C. Machine learning for traffic and routing management

The effective operation of a network like an internet also requires automated management. This includes efficient means of traffic prediction, traffic classification, routing and congestion control. Machine learning algorithms have been developed for all these areas.

1. Traffic

Predicting network traffic is becoming increasingly important especially in diverse and complex networks. It is commonly addressed using time-series forecasting (TSF) methods. This can make use of either statistical analysis models or supervised machine learning methods (Bermolen and Rossi, 2009; Chabaa *et al.*, 2010; Cortez *et al.*, 2006)]. Non-TSF methods also exist (Chen *et al.*, 2016; Li *et al.*, 2016).

The most commonly-used technique for traffic classification is the so-called flow feature-based technique. This takes into account information on unidirectional packets sent in the network. Supervised machine learning is found to be accurate in traffic classification in this domain. However, unsupervised techniques are found to be more robust. So the joint application of both supervised and unsupervised machine learning techniques have been found to be more powerful (Erman *et al.*, 2007; Zhang *et al.*, 2015).

2. Routing

Machine learning is most applicable to routing problems where the network is dynamical and thus requires fast updating of new optimal routes. otherwise, already-made routing tables can be sufficient for networks. Since these settings depend on frequent updating on new data, reinforcement learning algorithms are the most appropriate. In particular, Q-learning has performed well in various different networks (Arroyo-Valles *et al.*, 2007; Forster and Murphy, 2007; Wang and Wang, 2006).

3. Congestion

Congestion control in a network is also important to ensure the stability of a network and the minimisation of packet loss. Well-known congestion control methods like queue management already exist. However machine learning can be used to enhance the effectiveness of congestion control in various different networks, although mostly for TCP/IP networks (Barman and Matta, 2004; El Khayat *et al.*, 2005; Liu *et al.*, 2002).

D. Distributed machine learning

Distributed machine learning is the scenario where communication between computing devices are necessary to execute the machine learning algorithm of interest.

These distributed algorithms can be executed over an internet and become highly relevant in the following scenarios: (i) When data used in the training and/or testing of the machine learning algorithm originates from different sources. This is the naturally-distributed setting. In these cases, it is also possible for the loading of all data onto one machine and transferring data may be too costly and interrupts the workflow. It can even be the case that this loading time is greater than computational time, so distributed computation is more resource-efficient; (ii) When data is too large to be stored on the RAM of a single machine; (iii) When fault tolerance becomes important. For instance, for sensitive data, if data is stored in multiple places, there is less likelihood of data corruption from any single source and the data would still be available if one source fails.

The toolbox and infrastructure for distributed machine learning is currently in rapid development. There are many algorithms available. For instance, see (Peteiro-Barral and Guijarro-Berdiñas, 2013) for a survey. Also for distributed clustering see (Florina Balcan and Liang, 2013). There are also systems available to cater to distributed machine learning, like MLbase (et al, 2013), Hadoop (White, 2012) and Spark (Shanahan and Dai, 2015).

However, cautious usage is required. For example, here are some cases when one *shouldn't* use distributed machine learning: (i) When communication and synchronisation between the distributed parties provides a bottleneck for the computation; (ii) When writing and running a distributed program is too complicated; (iii) When one can run the same algorithm on a multi-core machine. This is possible with smart data sampling, offline schemes and efficient parallel codes.

III. CLASSICAL DATA AND MACHINE LEARNING WITH QUANTUM RESOURCES

There are at least three broad ways in which we can employ quantum resources for classical data over a network: (i) using quantum resources to enhance data processing at individual nodes (ii) using quantum resources to assist in security and/or (iii) using quantum resources to assist in communication.

As we saw in the previous section, machine learning algorithms come in a variety of ways to assist in classical information processing tasks highly applicable in the network setting. In the presence of a classical network, our first question is then whether or not quantum resources can assist in any of the machine learning algorithms that may be relevant in a network setting . These would include tasks related to security. These belong to the class of quantum-enhanced machine learning algorithms.

In the presence of a quantum network with only classical data, a communication complexity advantage is possible (Brassard, 2003). It is unclear if and how machine learning can be helpful or relevant in this setting. However, there are already some enticing clues (Balcan *et al.*, 2012; Conitzer and Sandholm, 2004; Kane *et al.*, 2017) on the connection between communication complexity and machine learning for classical data over a classical network. We leave questions on the roles that quantum resources can play for future investigation.

A. Quantum-enhanced machine learning overview

Quantum-enhanced machine learning algorithms are quantum algorithms performing machine learning tasks. They have so far mostly concentrated on quantum speed-ups with respect to dimensionality of the data involved.

1. Fully-quantum algorithms

The first set of these algorithms have chiefly relied on assuming completely quantum devices, keeping coherence throughout the computation and could require full fault-tolerance. For those algorithms claiming up to exponential quantum speedups for supervised algorithms (see (Biamonte *et al.*, 2017; Ciliberto *et al.*, 2018)), the HHL algorithm (Harrow *et al.*, 2009) for matrix-inversion is often used. However, HHL has a number of drawbacks that make them impractical for near-term quantum devices: (i) the ability to efficiently encode the classical data into quantum states and into quantum memory (Aaronson, 2015); (ii) effective read-out of the final quantum state (Aaronson, 2015); (iii) generally requiring high circuit-depth and (iv) restrictions on the sparsity and condition numbers of the matrix.

Although later developments have tried to circumvent restrictions on sparsity and focus on low-rank matrices instead (e.g. quantum principal component analysis for low-rank matrices (Lloyd *et al.*, 2014)), recent work on quantum-inspired classical algorithms have demonstrated efficient classical can exist in these cases (Chia *et al.*, 2018; Gilyén *et al.*, 2018; Tang, 2018). In fact, classical sampling methods developed in (Tang, 2018) for quantum-inspired machine learning algorithms suggest that classical methods for linear algebra problems in low-dimensions (used in machine learning for instance) are likely to find efficient classical algorithms. Although these classical sampling methods are not yet more practical than existing classical sampling methods, they are still more realistic than their quantum counterparts in (i) and (ii).

Another set of approaches, which rely on amplitude amplification and Grover's search algorithms, can give up to quadratic speed-ups. These include and quantum algorithms for reinforcement learning (Dunjko *et al.*, 2016) and training of quantum perceptrons (Kapoor *et al.*, 2016). While theoretically very interesting as long-term goals, near-term proposals are missing.

2. Hybrid algorithms

To find algorithms that may be realised in the the near-term, quantum machine learning algorithms are now giving more attention to hybrid classical-quantum algorithms. These algorithms, which include variational methods for optimisation (Moll *et al.*, 2018), have short circuit-depths and where the optimisation process is performed iteratively and classically. They are of roughly two types: one that attempts to enhance classical algorithms with classical input data and another where the quantum advantage lies in efficient quantum state preparation, thus using quantum input data. Prominent examples of the former include quantum approximate optimisation algorithm (QAOA) (Farhi *et al.*, 2014; Farhi and Harrow, 2016) and the latter include variational quantum eigensolvers (VQE) (Kandala *et al.*, 2017; Peruzzo, 2014). We return to VQE in the following section as these solve problems for quantum data.

Both QAOA and VQE can be considered as part of the same framework and their optimisation part (which can be considered only as a component and not the entirety of machine learning) is performed classically. One begins with an ansatz quantum state. An unitary with classically-tunable parameters is then applied to this state and an observable whose expectation value representing the cost function for the problem is subsequently measured. The classical parameters of the unitary are then iteratively tuned until one reaches the lowest value of the cost function (i.e., ground state of a given Hamiltonian), for instance using the classical gradient-descent algorithm.

In QAOA, the ground state reached then encodes the classical solution to a classical optimisation problem, like MaxCut, and it is a polynomial-time algorithm. Thus, it is not a quantum-enhanced algorithm for a classical machine learning problem, but rather takes advantage of classical machine learning algorithm. It remains to be seen if optimisation problems more directly relevant for networks can be solved in this way.

Alternative frameworks have been developed to find quantum-enhanced algorithms that not only take advantage of classical optimisation algorithms like above, but also to enhance classical machine learning algorithms. These new proposals include quantum circuit learning (Mitarai *et al.*, 2018), quantum generalisation of neural networks (Wan *et al.*, 2017) and Born machines (Benedetti *et al.*, 2018; Cheng *et al.*, 2018). Theoretical demonstration of quantum-enhancements in these settings is still an open problem.

B. Quantum-enhanced machine learning for security and other applications

1. Anomaly detection

The chief machine learning method for detecting and averting faults and security breaches in classical networks belong to anomaly detection. However, for anomalies in classical data, it appears unlikely that currently available quantum machine learning algorithms can enhance the speed and reliability of detection. One of the primary reasons is the necessity of encoding the classical data into quantum states, which can be very costly (Aaronson, 2015). Thus, even if there are quantum-enhanced supervised and unsupervised machine algorithms for anomaly detection in the computational component, the state preparation and read-out demands may be too much. However, the case is different if we begin with quantum data instead and we return to this in section IV.

2. Adversarial quantum machine learning

Just as machine learning algorithms are vulnerable to attacks, so would quantum-enhanced machine learning algorithms. This is very new area, called adversarial quantum machine learning. Like in adversarial machine learning, the aim is to find more robust quantum machine learning algorithms, and some robust algorithms have been indeed been proposed (Wiebe and Kumar, 2018). In addition to finding more robust algorithms, it is also important to understand what the robustness limits of quantum machine learning algorithms actually are, which remains an open problem. A recent result suggests that perhaps just as much quantum resources are necessary for detecting adversaries in higher dimensions as compared to quantum tomography (Liu, 2019). Thus it remains unclear the total resource cost of quantum-enhanced machine learning in the presence of adversaries. However, there is a tantalising yet unexplored possibility that perhaps quantum resources can enhance the security of machine learning algorithms, in a similar way that information-theoretic security is afforded to quantum cryptographic protocols.

3. Other

Whether or not there are helpful applications of quantum-enhanced machine learning algorithms to traffic and routing management is currently very unclear and may even appear unlikely. There may be some quantum-enhancements to supervised and unsupervised machine algorithms that could be used in traffic and routing management. However, a key issue still remains in how classical data can be embedded into the relevant quantum states and then read out, in a way that is easier in the quantum setting. The no-cloning theorem forbids reproducing the state and in general overheads in embedding classical information into the relevant quantum states are very high (Giovannetti *et al.*, 2008a,b). In addition, given the dynamical nature of networks, where machine learning methods appears to be most helpful, the speed of embedding classical data into quantum states must be likewise high. Thus, the necessary quantum resources only to convert classical data to quantum states may overwhelm any computational advantages.

C. Distributed quantum machine learning

The reasons to consider distributed quantum machine learning are similar to those for distributed classical machine learning. Suppose one wishes to perform distributed machine learning, either because the given data is naturally distributed or there is limited processing power on any given device. For this purpose, there are existing protocols for implementing general distributed quantum algorithms that could also be helpful in delegating quantum machine learning algorithms, e.g., (Beals *et al.*, 2013).

Secure delegated quantum computational protocols in (Joseph F. Fitzsimons, 2017) can also be modified to be applied to the quantum machine learning context (Bang *et al.*, 2015; Sheng and Zhou, 2017). However, here the same problem with state preparation could exist, for the server and not for the client. Alternatively, hybrid-classical quantum algorithms for distributed quantum machine learning have been developed in (Yoo *et al.*, 2014). Here the quantum state preparation assumptions can be obviated by using a hybrid gate that takes in classical input data and performs unitary operations controlled by the classical values instead of a quantum control-gate.

IV. QUANTUM DATA AND MACHINE LEARNING

Suppose the data we are give are naturally quantum in the form of quantum states or channels: this is quantum data. This means we are not necessarily given their classical descriptions to begin with. We can also be restricted on the number of copies we have access to due to the no-cloning theorem.

In these cases, it is found that classical machine learning methods may be helpful over traditional methods in dealing with quantum data. Another approach is to use quantum protocols to directly process quantum data. Learning protocols in the latter case belong to the field of quantum learning.

It is possible to process quantum data over either a classical or a quantum network. Techniques from classical machine learning methods for quantum data may assist in the communication of quantum data over a classical network while quantum learning protocols may be more appropriate over a quantum network. We are at the very beginning of this area of investigation. It is yet unclear exactly if and how these methods may be applicable and these serve as tantalizing inspiration for future study.

A. Classical machine learning for quantum data

1. Tomography

Suppose data come naturally in the form of a quantum state or a quantum channel. Then for classical processing of this data over a classical network, the first task is to find its classical description. The canonical methods for this are quantum state tomography and quantum process tomography. However, due to the no-cloning and the cost of quantum measurements, tomography is in general very resource intensive, requiring the number of copies of the quantum states to scale exponentially with the number of qubits per state. However, recent work have revealed methods on efficient state tomography using classical machine learning techniques (Han, 2017; Torlai, 2018) over a larger range of states than previously studied.

2. Separability

While tomography reveals the complete classical description of the quantum data, sometimes it may be sufficient to first classify the data in terms of their quantum properties. For instance, methods for classifying quantum states directly in terms of separability have been devised using classical machine learning (et al, 2017; Gao, 2018; Ma and Yung, 2017). Here there are empirical demonstrations of some advantages compared to the CHSH inequality. However, gathering sufficient training states might still remain a problem for states of higher dimensionality.

3. Automated experiment design

In a future quantum internet with entangled quantum networks, it is desirable to find the optimal methods of creating the types and extent of entanglement required with respect to resource constraints. It is also desirable this process may be automated. Recently, such automated methods based on classical reinforcement learning (Alexey A Melnikov, 2018) have been proposed, to experimentally create a variety of entangled states with more efficiency. This provides an exciting beginning for automated design of future quantum internet protocols.

4. VQE

We saw that variational quantum eigensolvers rely on classical optimisation. When used with input quantum data, they have found success mostly in quantum chemistry (Moll *et al.*, 2018; Peruzzo, 2014). In the context of quantum networks on the other hand, the most relevant work so far may be its use in quantum data compression (**?**) which may aid the communication of quantum data over a network.

B. Quantum learning protocols

1. Template matching

The first quantum algorithms for quantum data most relevant for machine learning are quantum template matching algorithms (Masahide Sasaki, 2002; **?**). These are classification algorithms, where each class is represented by a quantum state: a ‘template’. The task is to find the class to which a given test quantum state belongs, where this state is not identical to any of the template states. It is not clear on its own whether quantum template matching is directly useful in a quantum network setting. However, the ideas introduced here provide the key foundation for supervised learning of quantum data, which can be used in the quantum counterparts to supervised algorithms in traffic prediction, classification and anomaly detection.

2. Learning quantum processes

Suppose one wants to send just enough information about a quantum process over a quantum network in order for the other parties to replicate the use of this process onto any desired quantum state. In the quantum data scenario, one is not a priori given the classical description of this quantum process. Instead, one is provided only a finite number of queries of this quantum process. For a unitary operation, this problem is tackled in (**?**), in a problem called the quantum learning of unitary operations. A very interesting observation made here is that the optimal strategy is semi-classical instead of fully-quantum: meaning that it is sufficient for the classical data encoding the estimation of the unknown unitary to be stored. It remains an open question on how these results may change if one extends to more general quantum processes.

3. Quantum learning and security

In a future quantum network with quantum data being exchanged between different parties, it becomes important to detect unusual behaviour in the incoming quantum data. These may be the first signs of a security breach or a fault in the network. For dynamical data in a time-series, for instance, change point detection addresses precisely this problem. This has been extended to the quantum domain (Gael Sentís, 2016; Shang Yu, 2018) where the optimal methods for detecting a change in quantum data are found using methods from state discrimination. For static data, anomaly detection methods based on machine learning become more appropriate as the definition of of unusual behaviour is based on priori training data. Classical anomaly detection algorithms have been applied to quantum data in (Satoshi Hara, 2014) for the purpose of error detection, in the case where the classical description for the quantum data is known. However, for cases where the classical description for the quantum data is unknown (as expected over a quantum internet), it is instead much more efficient to directly apply quantum algorithms onto the quantum data directly. Examples of this include several quantum algorithms for anomaly detection was proposed in (Liu and Rebentrost, 2018).

Data/Network	Classical	Quantum
Classical	Current internet (CC)	Classical data in quantum network (CQ)
Quantum	Quantum data in classical network (QC)	Fully quantum internet (QQ)

Table I Classical and quantum data in a network

Network concerns	Classical data	Quantum resources and classical data	Quantum data
Individual computing	Classical machine learning	Quantum-enhanced machine learning	Quantum learning
Security and faults	Machine learning for anomalies and faults: detection and prediction; Adversarial machine learning	Adversarial quantum machine learning	Anomaly detection and change point detection for quantum data
Routing and traffic	Machine learning for traffic prediction, classification, congestion control and routing	Open problems	Open problems
Distributed computing	Distributed machine learning	Distributed quantum machine learning	Distributed quantum learning
Communication	Data compression and machine learning	Open problems	Data compression and quantum machine learning

Table II Classical and quantum machine learning applications in classical and quantum networks. Almost all of the categories here are very new and open to exploration in the quantum domain.

REFERENCES

Aaronson, Scott (2015), "Read the fine print," Nature Physics **11**, 291.

Ahmed, Tarem, Boris Oreshkin, and Mark Coates (2007), "Machine learning approaches to network anomaly detection," in *Proceedings of the 2nd USENIX workshop on Tackling computer systems problems with machine learning techniques*, p. 1.

et al, Kraska T (2013), "Mlbase: A distributed machine-learning system," Cidr **1**.

et al, S Lu (2017), "A separability-entanglement classifier via machine learning," 10.1103/physreva.98.012315, arXiv:1705.01523.

Alexey A Melnikov, Hendrik Poulsen Nautrup, Mario Krenn Vedran Dunjko Markus Tiersch-Anton Zeilinger Hans J Briegel (2018), "Active learning machine learns to create new quantum experiments," Proceedings of the National Academy of Sciences **115**, 1221, arXiv:1706.00868v3.

Arroyo-Valles, Rocio, Rocio Alaiz-Rodriguez, Alicia Guerrero-Curieses, and Jesús Cid-Sueiro (2007), "Q-probabilistic routing in wireless sensor networks," in *IEEE 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP)*, p. 1.

Balcan, Maria Florina, Avrim Blum, Shai Fine, and Yishay Mansour (2012), "Distributed learning, communication complexity and privacy," in *Conference on Learning Theory*, p. 26, arXiv:1204.3514v3.

Bang, Jeongho, Seung-Woo Lee, and Hyunseok Jeong (2015), "Protocol for secure quantum machine learning at a distant place," Quantum Information Processing **14**, 3933, arXiv:1504.04929v2.

Barman, Dhiman, and Ibrahim Matta (2004), "Model-based loss inference by tcp over heterogeneous networks," in *Proceedings of WiOpt*, Vol. 4.

Beals, Robert, Stephen Brierley, Oliver Gray, Aram W Harrow, Samuel Kutin, Noah Linden, Dan Shepherd, and Mark Stather (2013), "Efficient distributed quantum computing," Proceedings of the Royal Society A **469**, 20120686, arXiv:1207.2307v2.

Benedetti, Marcello, Delfina Garcia-Pintos, Oscar Perdomo, Vicente Leyton-Ortega, Yunseong Nam, and Alejandro Perdomo-Ortiz (2018), "A generative modeling approach for benchmarking and training shallow quantum circuits," arXiv:1801.07686.

Bermolen, Paola, and Dario Rossi (2009), "Support vector regression for link load prediction," Computer Networks **53** (2), 191.

Biamonte, Jacob, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd (2017), "Quantum machine learning," Nature **549**, 195, arXiv:1611.09347v2.

Bishop, Christopher M (2006), *Pattern recognition and machine learning* (Springer).

Boutaba, Raouf, Mohammad A Salahuddin, Noura Limam, Sara Ayoubi, Nashid Shahriar, Felipe Estrada-Solano, and Oscar M Caicedo (2018), "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," Journal of Internet Services and Applications **9**, 16.

Brassard, Gilles (2003), "Quantum communication complexity," Foundations of Physics **33**, 1593.

Chabaa, Samira, Abdelouhab Zeroual, and Jilali Antari (2010), "Identification and prediction of internet traffic using artificial neural networks," Journal of Intelligent Learning Systems and Applications **2**, 147.

Chen, Zhitang, Jiayao Wen, Yanhui Geng, *et al.* (2016), "Predicting future traffic using hidden markov models," in *IEEE 24th International Conference on Network Protocols (ICNP)*, p. 1.

Cheng, Song, Jing Chen, and Lei Wang (2018), "Information perspective to probabilistic modeling: Boltzmann machines versus born machines," Entropy **20**, 583, arXiv:1712.04144v1.

Chia, Nai-Hui, Han-Hsuan Lin, and Chunhao Wang (2018), "Quantum-inspired sublinear classical algorithms for solving low-rank linear systems," arXiv:1811.04852.

Ciliberto, Carlo, Mark Herbster, Alessandro Davide Ialongo, Massimiliano Pontil, Andrea Rocchetto, Simone Severini, and Leonard Wossnig (2018), "Quantum machine learning: a classical perspective," Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **474**, 20170551, arXiv:1707.08561v3.

Conitzer, Vincent, and Tuomas Sandholm (2004), "Communication complexity as a lower bound for learning in games," in *ACM Proceedings of the twenty-first international conference on Machine learning*, p. 24.

Cortez, Paulo, Miguel Rio, Miguel Rocha, and Pedro Sousa (2006), "Internet traffic forecasting using neural networks," in *IEEE International Joint Conference on Neural Networks (IJCNN'06)*, p. 2635.

Dunjko, Vedran, Jacob M Taylor, and Hans J Briegel (2016), "Quantum-enhanced machine learning," Physical Review Letters **117**, 130501, arXiv:1610.08251v1.

El Khayat, Ibtissam, Pierre Geurts, and Guy Leduc (2005), "Improving tcp in wireless networks with an adaptive machine-learnt classifier of packet loss causes," in *International Conference on Research in Networking*, p. 549.

Erman, Jeffrey, Anirban Mahanti, Martin Arlitt, Ira Cohen, and Carey Williamson (2007), "Offline/realtime traffic classification using semi-supervised learning," Performance

Evaluation **64**, 1194.

Farhi, Edward, Jeffrey Goldstone, and Sam Gutmann (2014), "A quantum approximate optimization algorithm," arXiv:1411.4028.

Farhi, Edward, and Aram W Harrow (2016), "Quantum supremacy through the quantum approximate optimization algorithm," arXiv:1602.07674.

Flach, Peter (2012), *Machine learning: the art and science of algorithms that make sense of data* (Cambridge University Press).

Florina Balcan, Maria, Steven Ehrlich, and Yingyu Liang (2013), "Distributed k-means and k-median clustering on general topologies," Advances in Neural Information Processing Systems , 1995arXiv:1306.0604v3.

Forster, Anna, and Amy L Murphy (2007), "Froms: Feedback routing for optimizing multiple sinks in wsn with reinforcement learning," in *IEEE 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP)*, p. 371.

Fraley, James B, and James Cannady (2017), "The promise of machine learning in cybersecurity," in *IEEE SoutheastCon*, p. 1.

Gael Sentís, Emilio Bagan, John Calsamiglia Giulio Chiribella Ramon Munoz-Tapia (2016), "Quantum change point," Physical Review Letters **117**, 150502, arXiv:1605.01916v3.

Gao, Jun, et al (2018), "Experimental machine learning of quantum states," Physical Review Letters **120**, 10.1103/physrevlett.120.240501.

Gilmer, Justin, Luke Metz, Fartash Faghri, Samuel S Schoenholz, Maithra Raghu, Martin Wattenberg, and Ian Goodfellow (2018), "Adversarial spheres," arXiv:1801.02774.

Gilyén, András, Seth Lloyd, and Ewin Tang (2018), "Quantum-inspired low-rank stochastic regression with logarithmic dependence on the dimension," arXiv:1811.04909.

Giovannetti, Vittorio, Seth Lloyd, and Lorenzo Maccone (2008a), "Architectures for a quantum random access memory," Physical Review A **78**, 052310.

Giovannetti, Vittorio, Seth Lloyd, and Lorenzo Maccone (2008b), "Quantum random access memory," Physical Review Letters **100**, 160501, arXiv:0708.1879v2.

Goodfellow, Ian J, Jonathon Shlens, and Christian Szegedy (2014), "Explaining and harnessing adversarial examples," arXiv:1412.6572.

Hajji, Hassan (2005), "Statistical analysis of network traffic for adaptive faults detection," IEEE Transactions on Neural Networks **16**, 1053.

Han, Z Y et al (2017), "Efficient quantum tomography with fidelity estimation," arXiv:1712.03213.

Harrow, Aram W, Avinatan Hassidim, and Seth Lloyd (2009), "Quantum algorithm for linear systems of equations," Physical Review Letters **103**, 150502.

Hood, Cynthia S, and Chuanyi Ji (1997), "Proactive network-fault detection [telecommunications]," IEEE Transactions on reliability **46**, 333.

Huang, Ling, Anthony D Joseph, Blaine Nelson, Benjamin IP Rubinstein, and JD Tygar (2011), "Adversarial machine learning," in *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, p. 43.

Joseph, Anthony D, Pavel Laskov, Fabio Roli, J Doug Tygar, and Blaine Nelson (2013), "Machine learning methods for computer security (dagstuhl perspectives workshop 12371)," in *Dagstuhl Manifestos*, Vol. 3.

Joseph F. Fitzsimons, Elham Kashefi (2017), "Unconditionally verifiable blind quantum computation," Physical Review A **96**, 012303.

Kandala, Abhinav, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M Chow, and Jay M Gambetta (2017), "Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets," Nature **549**, 242, arXiv:1704.05018v2.

Kane, Daniel M, Roi Livni, Shay Moran, and Amir Yehudayoff (2017), "On communication complexity of classification problems," arXiv:1711.05893.

Kapoor, Ashish, Nathan Wiebe, and Krysta Svore (2016), "Quantum perceptron models," in *Advances in Neural Information Processing Systems*, p. 3999, arXiv:1602.04799v1.

Kogeda, P, and Johnson I Agbinya (2006), "Prediction of faults in cellular networks using bayesian network model," in *International conference on Wireless Broadband and Ultra Wideband Communication* (UTS ePress).

Kurakin, Alexey, Ian Goodfellow, Samy Bengio, Yinpeng Dong, Fangzhou Liao, Ming Liang, Tianyu Pang, Jun Zhu, Xiaolin Hu, Cihang Xie, *et al.* (2018), "Adversarial attacks and defences competition," in *The NIPS'17 Competition: Building Intelligent Systems* (Springer) p. 195, arXiv:1804.00097v1.

Li, Yi, Hong Liu, Wenjun Yang, Dianming Hu, and Wei Xu (2016), "Inter-data-center network traffic prediction with elephant flows," in *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, p. 206.

Liu, Jun, Ibrahim Matta, and Mark Crovella (2002), *End-to-end inference of loss nature in a hybrid wired/wireless environment*, Tech. Rep. (Boston University Computer Science Department).

Liu, Nana, and Patrick Rebentrost (2018), "Quantum machine learning for quantum anomaly detection," Physical Review A **97**, 042315, arXiv:1710.07405v1.

Liu, Nana, Wittek Peter (2019), "Adversarial quantum learning," Upcoming.

Lloyd, Seth, Masoud Mohseni, and Patrick Rebentrost (2014), "Quantum principal component analysis," Nature Physics **10**, 631, arXiv:1307.0401v2.

Ma, Y-C, and M.-H. Yung (2017), "Transforming bell's inequalities into state classifiers with machine learning," 10.1038/s41534-018-0081-3, arXiv:1705.00813.

Mahloujifar, Saeed, Dimitrios I Diochnos, and Mohammad Mahmoody (2018), "The curse of concentration in robust learning: Evasion and poisoning attacks from concentration of measure," arXiv:1809.03063.

Marsland, Stephen (2011), *Machine learning: an algorithmic perspective* (Chapman and Hall/CRC).

Masahide Sasaki, Alberto Carlini (2002), "Quantum learning and universal quantum matching machine," Physical Review A **66**, 022303, arXiv:quant-ph/0202173v1.

Mitarai, Kosuke, Makoto Negoro, Masahiro Kitagawa, and Keisuke Fujii (2018), "Quantum circuit learning," Physical Review A **98**, 032309, arXiv:1803.00745v2.

Moll, Nikolaj, Panagiotis Barkoutsos, Lev S Bishop, Jerry M Chow, Andrew Cross, Daniel J Egger, Stefan Filipp, Andreas Fuhrer, Jay M Gambetta, Marc Ganzhorn, *et al.* (2018), "Quantum optimization using variational algorithms on near-term quantum devices," Quantum Science and Technology **3**, 030503, arXiv:1710.01022v2.

Peruzzo, A (2014), "A. peruzzo, j. mcclean, p. shadbolt, m.-h. yung, x.-q. zhou, pj love, a. aspuru-guzik, and jl o'brien, nat. commun. 5, 4213 (2014)." Nature Communications **5**, 4213.

Peteiro-Barral, Diego, and Bertha Guijarro-Berdiñas (2013), "A survey of methods for distributed machine learning," Progress in Artificial Intelligence **2**, 1.

Satoshi Hara, Takafumi Ono, Ryo Okamoto Takashi Washio Shigeki Takeuchi (2014), "Anomaly detection in reconstructed quantum states using a machine-learning technique," Physical Review A **89**, 022104, arXiv:1401.4785v1.

Shalev-Shwartz, Shai, and Shai Ben-David (2014), *Understanding machine learning: From theory to algorithms* (Cambridge University Press).

Shanahan, James G, and Laing Dai (2015), "Large scale distributed data science using apache spark," in *Proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining*, p. 2323.

Shang Yu, Chang-Jiang Huang, Jian-Shun Tang Zhih-Ahn Jia Yi-Tao Wang Zhi-Jin Ke Wei Liu Xiao Liu Zong-Quan Zhou Ze-Di Cheng Jin-Shi Xu Yu-Chun Wu Yuan-Yuan Zhao Guo-Yong Xiang Chuan-Feng Li Guang-Can Guo Gael Sentís Ramon Muñoz-Tapia (2018), "Experimentally detecting a quantum change point via the bayesian inference," Physical Review A **98** (4), 040301, arXiv:1801.07508v1.

Sheng, Yu-Bo, and Lan Zhou (2017), "Distributed secure quantum machine learning," Science Bulletin **62**, 1025.

Snow, A, P Rastogi, and G Weckman (2005), "Assessing dependability of wireless networks using neural networks," in *IEEE Military Communications Conference (MILCOM)*, p. 2809.

Sommer, Robin, and Vern Paxson (2010), "Outside the closed world: On using machine learning for network intrusion detection," in *IEEE Symposium on Security and Privacy (SP)*, p. 305.

Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus (2013), "Intriguing properties of neural networks," arXiv:1312.6199.

Tang, Ewin (2018), "Quantum-inspired classical algorithms for principal component analysis and supervised clustering," arXiv:1811.00414.

Thottan, Marina, and Chuanyi Ji (2003), "Anomaly detection in ip networks," IEEE Transactions on signal processing **51**, 2191.

Torlai, Giacomo et al (2018), "Neural-network quantum state tomography," Nature Physics **14**, 447.

Trevor, Hastie, Tibshirani Robert, and Friedman JH (2009), "The elements of statistical learning: data mining, inference, and prediction,".

Wan, Kwok Ho, Oscar Dahlsten, Hlér Kristjánsson, Robert Gardner, and MS Kim (2017), "Quantum generalisation of feedforward neural networks," NPJ Quantum Information **3**, 36.

Wang, Mowei, Yong Cui, Xin Wang, Shihan Xiao, and Junchen Jiang (2018), "Machine learning for networking: Workflow, advances and opportunities," IEEE Network **32**, 92, arXiv:1709.08339v2.

Wang, Ping, and Ting Wang (2006), "Adaptive routing for sensor networks using reinforcement learning," in *The Sixth IEEE International Conference on Computer and Information Technology (CIT'06)*, p. 219.

White, Tom (2012), *Hadoop: The definitive guide* ("O'Reilly Media, Inc.").

Wiebe, Nathan, and Ram Shankar Siva Kumar (2018), "Hardening quantum machine learning against adversaries," New Journal of Physics 10.1088/1367-2630/aae71a, arXiv:1711.06652v1.

Yavanoglu, Ozlem, and Murat Aydos (2017), "A review on cyber security datasets for machine learning algorithms," in *IEEE International Conference on Big Data*, p. 2186.

Yoo, Seokwon, Jeongho Bang, Changhyoup Lee, and Jinhyoung Lee (2014), "A quantum speedup in machine learning: finding an n-bit boolean function for a classification," New Journal of Physics **16**, 103014, arXiv:1303.6055v4.

Zhang, Jun, Xiao Chen, Yang Xiang, Wanlei Zhou, and Jie Wu (2015), "Robust network traffic classification," IEEE/ACM Transactions on Networking (TON) **23**, 1257.