1.Explain the term machine learning, and how does it work? Explain two machine learning applications in the business world. What are some of the ethical concerns that machine learning applications could raise?

Machine learning is a modern innovation that has enhanced many industrial and professional processes as well as our daily lives. It's a subset of artificial intelligence (AI), which focuses on using statistical techniques to build intelligent computer systems to learn from available databases.

By incorporating machine learning models into their data analytics, businesses gain far more accurate and powerful capabilities for forecasting demand, which translates into more effective inventory management and big cost savings.

Improvement in the quality and quantity of products, as a machine, ensure high and large production rate. There is a cut in production costs and labour salary. Workers improve their technical skills through training. Higher salaries resulting in better living standards for skilled operators.

3. General ethical issues in Machine Learning

As well as potential benefits, there is increasing awareness that the application of machine learning poses risks and can lead to harms, raising a range ethical questions. This section presents a brief overview of some key concerns.

For a general background on ethics and its relevance to ML, see Appendix 1. Background: Ethics & Machine Learning.

3.1. Accuracy

The accuracy of an ML model is the proportion of examples for which it generates a correct output [Leslie]. In general high accuracy is a good thing, and low accuracy can lead to harms, for example where facial recognition systems are used in law enforcement. But highly accurate facial recognition systems can also pose risks to privacy and autonomy (e.g. mass surveillance).

In some areas such as credit-scoring or loan approval, increasing the accuracy of predictions might come at the cost of requiring access to too much personal data.

There is also concern about the over-hyping of the ability of AI to accurately predict certain things at all, particularly social outcomes such as job performance or criminal recidivism. Accuracy may be a useful measure where an area has a clear, objective ground truth (e.g. vehicle license-plate recognition) but many areas of human judgment are nuanced, messy and contextual, and simple accuracy risks being too reductive a measure.

An incorrect output produced by an ML model can have varying context-dependent impact [Leslie]. For example, when identifying cancerous skin growth, false positives may increase the cost of cancer detection (by requiring additional lab work to rule them out), while false negatives may delay treatment to the point where it is no longer effective. What matters here is lowering the risk of false negatives. In a judicial context, false positives may send innocents behind bars, while false negatives might make it more difficult to convict a criminal. What matters here is lowering the risk of false positives.

3.2. Bias

Bias has a number of meanings, including a systematic deviation from a true value. This can be positive or negative. Bias is a prominent concern in ML ethics, where the concern more specifically is ‘a systematic skew in decision-making that results in unfair outcomes’ [CDEI].

Concerns about bias are particularly prominent where negative outcomes (such as inaccurate predictions and their consequences) disproportionately affect individuals or groups who are vulnerable or historically marginalised. Where the unfair treatment relates to protected characteristics such as race, gender, disability or sexuality, bias can constitute illegal discrimination, depending on relevant laws.

There are a number of causes of bias [Mehrabi], ranging from issues with data to algorithmic design and human perception and decision-making. Perhaps the most prominent cause is that algorithms trained to make decisions based on past data will often replicate the historic biases in that data ([Suresh] also has a useful survey of causes of bias).

3.3. Fairness

There is no single definition of fairness ([Mehrabi] also has a good survey of definitions) - like ethics it is contextual and varies according to different values, perspectives and societies. But one core idea is that people should be treated equally unless there is a justified, relevant reason not to.

Fairness is often a lens through which to make sense of other ethical concerns. As noted above, bias can be positive or negative - it’s when it leads to ‘unfair’ outcomes that it is problematic. Where ethical principles or concerns need to be balanced against each other, considering fairness often provides a guide to how to do that.

Fairness is about both outcomes and process. Outcomes should involve the fair distribution of benefits and costs, and the avoidance of unfair bias or arbitrary decisions. Procedural elements of fairness include involving communities that will be affected by ML outputs in decisions about how the systems are designed and used, and ensuring there is the ability to contest and seek redress for decisions made by ML.

Fairness could also arguably justify bias - for example biasing a system to favour people who have been historically marginalised, in order to achieve an outcome which is in some sense equal or fair (this is known as equity - treating people differently on the basis of need to achieve outcomes which are fair).

Another important aspect of fairness is the distribution of access to computationally complex ML approaches, and the benefits that come from access. People living in countries with less powerful or functioning infrastructure, or who cannot access sufficient computing power, may be unfairly disadvantaged.

3.4. Safety & Security

Safety includes that an ML system should be accurate, but also that it should be reliable (perform as intended, and continue to do so over time), secure (against adversarial attacks), and robust enough to do these things in real-world, unpredictable and sometimes challenging conditions ([Leslie])

Safety is a broad concern, but is particularly relevant where the failure of ML systems could result in real-world harm - for example with medical diagnosis or self-driving cars.

There are a number of security risks to machine learning, including training data poisoning, adversarial inputs, or model inversion and adversarial inference attacks which can expose model parameters or training data ([Xue]).

Machine learning can also increase the effectiveness of other types of security attacks, for example by enabling more effective impersonation for social engineering and phishing attacks.

3.5. Privacy

There are a number of ways in which ML systems can pose risks to privacy.

One is where systems that undermine privacy operate without a user’s knowledge or explicit, informed consent. This is true of systems that undermine privacy explicitly (surveillance systems), but also where undermining privacy is a potential byproduct of intended, legitimate use (e.g. if an ML system which has access to a user’s video camera).

There are also privacy concerns about the data used to train models. Data may be collected in a way which violates privacy, such as without consent from users (e.g. scraping personal information). Models may ‘leak’ personal data (e.g. large language models [Weidinger]). Legitimately collected data may also be compromised, for example through reverse engineering or inference style attacks which can de-anonymise model training data.

The accuracy of the predictions of ML systems may also present risks. Just as the outputs of sensor APIs could be used to identify, fingerprint or correlate user activity (e.g. if the output is too precise), it is possible that the outputs of ML systems could pose similar risks.

And use of ML systems to infer sensitive, personal data about users based on non-sensitive data (e.g. inferring sexuality from content preferences) may also violate privacy.

Some jurisdictions (e.g. EU/GDPR) also provide a ‘right to be forgotten’, which arguably could include being removed from ML training data. So a privacy-protecting approach would need to ensure that appropriate processes and technical capabilities are in place for this to happen (see e.g. [Bourtoule]).

3.6. Transparency

Very broadly, transparency is about users and stakeholders having access to the information they need to make informed decisions about ML. It’s a holistic concept, covering both ML models themselves and the process or pipeline by which they go from inception to use. [Vaughan] (following the [EGTAI]) propose 3 key components:

* Traceability: Those who develop or deploy machine learning systems should clearly document their goals, definitions, design choices, and assumptions.
* Communication: Those who develop or deploy machine learning systems should be open about the ways they use machine learning technology and about its limitations.
* Intelligibility: Stakeholders of machine learning systems should be able to understand and monitor the behavior of those systems to the extent necessary to achieve their goals.
* Understanding ML systems involves two key related concepts [Gall]:
* Interpretability: is about the extent to which a cause and effect can be observed within a system.
* Explainability: the extent to which the internal mechanics of a machine or deep learning system can be explained in human terms.

Lack of interpretability and explainability is known as the black-box problem, which is particularly prevalent with more complex ML approaches such as neural networks.

3.7. Accountability

Given that ML systems are increasingly being used in high impact areas (healthcare, welfare, criminal justice) and that harms can be large when they go wrong, and that actors in the ML pipeline take responsibility for considering the impact of ML systems, and accountability for when things go wrong.

“Algorithms and the data that drive them are designed and created by people – there is always a human ultimately responsible for decisions made or informed by an algorithm. "The algorithm did it" is not an acceptable excuse if algorithmic systems make mistakes or have undesired consequences, including from machine-learning processes.” [FATML]

Transparency is an enabler for accountability (we need to be able to see what is going wrong and where to be able to determine responsibility). It also requires proper processes for the consideration of risks to be in place, documentation of policies and processes, and the means for those who are harmed to seek redress. The developers of ML systems should also take responsibility for any 3rd party ML they use in their system.

Increasingly in some jurisdictions, there are formal legal mechanisms for accountability and seeking redress.

3.8. Human Control and Decision-making

The need for accountability, as well as other concerns above such as accuracy and fairness, have led to the assertion of the importance of humans making in the final decision in high stakes applications. More broadly, ML applications should always be under ultimate human control.

But there are pitfalls too where ML approaches support human decision-making - problems with explainability can inhibit the full exercise of human capabilities, or humans may exhibit “automation bias” where they place too much trust in information or recommendations provided by an ML system.

3.9. Environmental Impact & Sustainability

There is increasing awareness that computationally complex ML approaches trained on very large data sets can have a large environmental impact, given the amount of energy required to power the training phase.

The broader concern with sustainability suggests that ML applications and systems should not undermine the sustainability of the physical, social and political ecosystems in which they’re deployed. This might include the impact on jobs, employment and the economy, or on the quality of and access to information necessary for a functioning democratic system.

3.10. Types of harm

The above list contains some potential sources or causes of harm from machine learning. It is also important to be aware that harm can take a number of different forms, all of which should be considered.

As noted above, harms can impact individuals, groups and society. To take the example of a biased facial recognition system [Smuha]:

* this may lead to wrongful discrimination against an individual (e.g. wrongful arrest).
* where a number of individuals who belong to a group or collective suffer this discimination (e.g. because of shared ethnicity), there is a group harm. This could be the sum of the individual harms, as well as harms such as an increase in prejudice towards that group caused by the perpetuation of historic bias.
* here could be a harm to the interests of society, such as being able to ‘live in a society that does not discriminate against people based on their skin colour and that treats its citizens equally.’ [Smuha]

Harms can also take a number of forms. These can include:

* physical, either directly (e.g. the failure of driver-less cars), or indirectly (e.g. flaws in a system leading to incorrect medical diagnosis).
* allocative, when a system unfairly allocates or withholds from certain individuals or groups an opportunity or a resource (e.g. benefits or loans) [Crawford].
* representational, when systems “reinforce the subordination of some groups along the lines of identity.” [Crawford] e.g. when a Google search for ‘CEO’ returns mostly pictures of white men, or image recognition systems generate offensive labels for people of colour.

2. Describe the process of human learning:

i. Under the supervision of experts

Teachers are very good at creating exercises that will help us build our communication skills, our ability to make important decisions, and our ability to build rapport with others. We learn that through working together, we can achieve something great.

ii. With the assistance of experts in an indirect manner

Indirect guidance is provided through learners actively observing, listening, and engaging with social practices and norms, which serve to furnish models and goals for performance and individuals' learning. The exercise of learner agency is a defining quality of guided learning.

Indirect instruction is a student-centered approach to learning where students observe, investigate and draw inferences from data. In this instructional model, professors take on the role of a facilitator or supporter as opposed to offering direct instruction.

iii. Self-education

Autodidacticism (also autodidactism) or self-education (also self-learning and self-teaching) is education without the guidance of masters (such as teachers and professors) or institutions (such as schools).

Self-learning is the method of gathering, processing, and retaining knowledge without the help of another person. Any knowledge you get outside of a formal educational setting, such as through self-study or experience, is self-driven learning.

Self-studying is flexible and molds to the interests of the learner. It allows students to go at their own pace, allowing them to spend more time on topics they want to understand a bit better or focus on subjects they are the most interested in.

3. Provide a few examples of various types of machine learning.

Types of Machine Learning :

Supervised Machine Learning : Housing price prediction, medical imaging

Unsupervised Machine Learning : customer segmentation, market basket analysis

Semi-Supervised Machine Learning : text classification, lane-finding on GPS data

Reinforcement Learning: optimized marketing, driverless cars

4. Examine the various forms of machine learning.

**1. Supervised Machine Learning**

As its name suggests, Supervised machine learning is based on supervision. It means in the supervised learning technique, we train the machines using the "labelled" dataset, and based on the training, the machine predicts the output. Here, the labelled data specifies that some of the inputs are already mapped to the output. More preciously, we can say; first, we train the machine with the input and corresponding output, and then we ask the machine to predict the output using the test dataset.

Let's understand supervised learning with an example. Suppose we have an input dataset of cats and dog images. So, first, we will provide the training to the machine to understand the images, such as the shape & size of the tail of cat and dog, Shape of eyes, colour, height (dogs are taller, cats are smaller), etc. After completion of training, we input the picture of a cat and ask the machine to identify the object and predict the output. Now, the machine is well trained, so it will check all the features of the object, such as height, shape, colour, eyes, ears, tail, etc., and find that it's a cat. So, it will put it in the Cat category. This is the process of how the machine identifies the objects in Supervised Learning.

The main goal of the supervised learning technique is to map the input variable(x) with the output variable(y). Some real-world applications of supervised learning are Risk Assessment, Fraud Detection, Spam filtering, etc.

Categories of Supervised Machine Learning:

Supervised machine learning can be classified into two types of problems, which are given below:

* Classification
* Regression

a) Classification

Classification algorithms are used to solve the classification problems in which the output variable is categorical, such as "Yes" or No, Male or Female, Red or Blue, etc. The classification algorithms predict the categories present in the dataset. Some real-world examples of classification algorithms are Spam Detection, Email filtering, etc.

Some popular classification algorithms are given below:

* Random Forest Algorithm
* Decision Tree Algorithm
* Logistic Regression Algorithm
* Support Vector Machine Algorithm

b) Regression

Regression algorithms are used to solve regression problems in which there is a linear relationship between input and output variables. These are used to predict continuous output variables, such as market trends, weather prediction, etc.

Some popular Regression algorithms are given below:

* Simple Linear Regression Algorithm
* Multivariate Regression Algorithm
* Decision Tree Algorithm
* Lasso Regression

Advantages and Disadvantages of Supervised Learning

Advantages:

* Since supervised learning work with the labelled dataset so we can have an exact idea about the classes of objects.
* These algorithms are helpful in predicting the output on the basis of prior experience.

Disadvantages:

* These algorithms are not able to solve complex tasks.
* It may predict the wrong output if the test data is different from the training data.
* It requires lots of computational time to train the algorithm.

Applications of Supervised Learning

Some common applications of Supervised Learning are given below:

Image Segmentation:

Supervised Learning algorithms are used in image segmentation. In this process, image classification is performed on different image data with pre-defined labels.

Medical Diagnosis:

Supervised algorithms are also used in the medical field for diagnosis purposes. It is done by using medical images and past labelled data with labels for disease conditions. With such a process, the machine can identify a disease for the new patients.

Fraud Detection - Supervised Learning classification algorithms are used for identifying fraud transactions, fraud customers, etc. It is done by using historic data to identify the patterns that can lead to possible fraud.

Spam detection - In spam detection & filtering, classification algorithms are used. These algorithms classify an email as spam or not spam. The spam emails are sent to the spam folder.

Speech Recognition - Supervised learning algorithms are also used in speech recognition. The algorithm is trained with voice data, and various identifications can be done using the same, such as voice-activated passwords, voice commands, etc.

**2. Unsupervised Machine Learning**

Unsupervised learning is different from the Supervised learning technique; as its name suggests, there is no need for supervision. It means, in unsupervised machine learning, the machine is trained using the unlabeled dataset, and the machine predicts the output without any supervision.

In unsupervised learning, the models are trained with the data that is neither classified nor labelled, and the model acts on that data without any supervision.

The main aim of the unsupervised learning algorithm is to group or categories the unsorted dataset according to the similarities, patterns, and differences. Machines are instructed to find the hidden patterns from the input dataset.

Let's take an example to understand it more preciously; suppose there is a basket of fruit images, and we input it into the machine learning model. The images are totally unknown to the model, and the task of the machine is to find the patterns and categories of the objects.

So, now the machine will discover its patterns and differences, such as colour difference, shape difference, and predict the output when it is tested with the test dataset.

Categories of Unsupervised Machine Learning

Unsupervised Learning can be further classified into two types, which are given below:

* Clustering
* Association

1) Clustering

The clustering technique is used when we want to find the inherent groups from the data. It is a way to group the objects into a cluster such that the objects with the most similarities remain in one group and have fewer or no similarities with the objects of other groups. An example of the clustering algorithm is grouping the customers by their purchasing behaviour.

Some of the popular clustering algorithms are given below:

* K-Means Clustering algorithm
* Mean-shift algorithm
* DBSCAN Algorithm
* Principal Component Analysis
* Independent Component Analysis

2) Association

Association rule learning is an unsupervised learning technique, which finds interesting relations among variables within a large dataset. The main aim of this learning algorithm is to find the dependency of one data item on another data item and map those variables accordingly so that it can generate maximum profit. This algorithm is mainly applied in Market Basket analysis, Web usage mining, continuous production, etc.

Some popular algorithms of Association rule learning are Apriori Algorithm, Eclat, FP-growth algorithm.

Advantages and Disadvantages of Unsupervised Learning Algorithm

Advantages:

* These algorithms can be used for complicated tasks compared to the supervised ones because these algorithms work on the unlabeled dataset.
* Unsupervised algorithms are preferable for various tasks as getting the unlabeled dataset is easier as compared to the labelled dataset.

Disadvantages:

* The output of an unsupervised algorithm can be less accurate as the dataset is not labelled, and algorithms are not trained with the exact output in prior.
* Working with Unsupervised learning is more difficult as it works with the unlabelled dataset that does not map with the output.

Applications of Unsupervised Learning:

Network Analysis: Unsupervised learning is used for identifying plagiarism and copyright in document network analysis of text data for scholarly articles.

Recommendation Systems: Recommendation systems widely use unsupervised learning techniques for building recommendation applications for different web applications and e-commerce websites.

Anomaly Detection: Anomaly detection is a popular application of unsupervised learning, which can identify unusual data points within the dataset. It is used to discover fraudulent transactions.

Singular Value Decomposition: Singular Value Decomposition or SVD is used to extract particular information from the database. For example, extracting information of each user located at a particular location.

**3. Semi-Supervised Learning**

Semi-Supervised learning is a type of Machine Learning algorithm that lies between Supervised and Unsupervised machine learning. It represents the intermediate ground between Supervised (With Labelled training data) and Unsupervised learning (with no labelled training data) algorithms and uses the combination of labelled and unlabeled datasets during the training period.

Although Semi-supervised learning is the middle ground between supervised and unsupervised learning and operates on the data that consists of a few labels, it mostly consists of unlabeled data. As labels are costly, but for corporate purposes, they may have few labels. It is completely different from supervised and unsupervised learning as they are based on the presence & absence of labels.

To overcome the drawbacks of supervised learning and unsupervised learning algorithms, the concept of Semi-supervised learning is introduced. The main aim of semi-supervised learning is to effectively use all the available data, rather than only labelled data like in supervised learning. Initially, similar data is clustered along with an unsupervised learning algorithm, and further, it helps to label the unlabeled data into labelled data. It is because labelled data is a comparatively more expensive acquisition than unlabeled data.

We can imagine these algorithms with an example. Supervised learning is where a student is under the supervision of an instructor at home and college. Further, if that student is self-analysing the same concept without any help from the instructor, it comes under unsupervised learning. Under semi-supervised learning, the student has to revise himself after analyzing the same concept under the guidance of an instructor at college.

Advantages and disadvantages of Semi-supervised Learning

Advantages:

* It is simple and easy to understand the algorithm.
* It is highly efficient.
* It is used to solve drawbacks of Supervised and Unsupervised Learning algorithms.

Disadvantages:

* Iterations results may not be stable.
* We cannot apply these algorithms to network-level data.
* Accuracy is low.

**4. Reinforcement Learning**

Reinforcement learning works on a feedback-based process, in which an AI agent (A software component) automatically explore its surrounding by hitting & trail, taking action, learning from experiences, and improving its performance. Agent gets rewarded for each good action and get punished for each bad action; hence the goal of reinforcement learning agent is to maximize the rewards.

In reinforcement learning, there is no labelled data like supervised learning, and agents learn from their experiences only.

The reinforcement learning process is similar to a human being; for example, a child learns various things by experiences in his day-to-day life. An example of reinforcement learning is to play a game, where the Game is the environment, moves of an agent at each step define states, and the goal of the agent is to get a high score. Agent receives feedback in terms of punishment and rewards.

Due to its way of working, reinforcement learning is employed in different fields such as Game theory, Operation Research, Information theory, multi-agent systems.

A reinforcement learning problem can be formalized using Markov Decision Process(MDP). In MDP, the agent constantly interacts with the environment and performs actions; at each action, the environment responds and generates a new state.

Categories of Reinforcement Learning

Reinforcement learning is categorized mainly into two types of methods/algorithms:

* Positive Reinforcement Learning: Positive reinforcement learning specifies increasing the tendency that the required behaviour would occur again by adding something. It enhances the strength of the behaviour of the agent and positively impacts it.
* Negative Reinforcement Learning: Negative reinforcement learning works exactly opposite to the positive RL. It increases the tendency that the specific behaviour would occur again by avoiding the negative condition.

Real-world Use cases of Reinforcement Learning

Video Games:

RL algorithms are much popular in gaming applications. It is used to gain super-human performance. Some popular games that use RL algorithms are AlphaGO and AlphaGO Zero.

Resource Management:

The "Resource Management with Deep Reinforcement Learning" paper showed that how to use RL in computer to automatically learn and schedule resources to wait for different jobs in order to minimize average job slowdown.

Robotics:

RL is widely being used in Robotics applications. Robots are used in the industrial and manufacturing area, and these robots are made more powerful with reinforcement learning. There are different industries that have their vision of building intelligent robots using AI and Machine learning technology.

Text Mining

Text-mining, one of the great applications of NLP, is now being implemented with the help of Reinforcement Learning by Salesforce company.

Advantages and Disadvantages of Reinforcement Learning

Advantages

* It helps in solving complex real-world problems which are difficult to be solved by general techniques.
* The learning model of RL is similar to the learning of human beings; hence most accurate results can be found.
* Helps in achieving long term results.

Disadvantage

* RL algorithms are not preferred for simple problems.
* RL algorithms require huge data and computations.
* Too much reinforcement learning can lead to an overload of states which can weaken the results.

The curse of dimensionality limits reinforcement learning for real physical systems.

5. Can you explain what a well-posed learning problem is? Explain the main characteristics that must be present to identify a learning problem properly.

A (machine learning) problem is well-posed if a solution to it exists, if that solution is unique, and if that solution depends on the data / experience but it is not sensitive to (reasonably small) changes in the data / experience.

The formal definition of Well posed learning problem is, “A computer program is said to learn from Experience E when given a task T, and some performance measure P. If it performs on T with a performance measure P, then it upgrades with experience E.

Any problem can be segregated as well-posed learning problem if it has three traits –

* Task
* Performance Measure
* Experience

6. Is machine learning capable of solving all problems? Give a detailed explanation of your answer.

machine learning is not the answer to all problems. Given the usefulness of machine learning, it can be hard to accept that sometimes it is not the best solution to a problem.

Some problems that cannot be solved by ML are:

1. Reasoning Power

One area where ML has not mastered successfully is reasoning power, a distinctly human trait. Algorithms available today are mainly oriented towards specific use-cases and are narrowed down when it comes to applicability. They cannot think as to why a particular method is happening that way or ‘introspect’ their own outcomes.

For instance, if an image recognition algorithm identifies apples and oranges in a given scenario, it cannot say if the apple (or orange) has gone bad or not, or why is that fruit an apple or orange. Mathematically, all of this learning process can be explained by us, but from an algorithmic perspective, the innate property cannot be told by the algorithms or even us.

In other words, ML algorithms lack the ability to reason beyond their intended application.

2. Contextual Limitation

If we consider the area of natural language processing (NLP), text and speech information are the means to understand languages by NLP algorithms. They may learn letters, words, sentences or even the syntax, but where they fall back is the context of the language. Algorithms do not understand the context of the language used. A classic example for this would be the “Chinese room” argument given by philosopher John Searle, which says that computer programs or algorithms grasp the idea merely by ‘symbols’ rather than the context given.

So, ML does not have an overall idea of the situation. It is limited by mnemonic interpretations rather than thinking to see what is actually going on.

3. Scalability

Although we see ML implementations being deployed on a significant basis, it all depends on data as well as its scalability. Data is growing at an enormous rate and has many forms which largely affects the scalability of an ML project. Algorithms cannot do much about this unless they are updated constantly for new changes to handle data. This is where ML regularly requires human intervention in terms of scalability and remains unsolved mostly.

In addition, growing data has to be dealt the right way if shared on an ML platform which again needs examination through knowledge and intuition apparently lacked by current ML.

4. Regulatory Restriction For Data In ML

ML usually need considerable amounts (in fact, massive) of data in stages such as training, cross-validation etc. Sometimes, data includes private as well as general information. This is where it gets complicated. Most tech companies have privatised data and these data are the ones which are actually useful for ML applications. But, there comes the risk of the wrong usage of data, especially in critical areas such as medical research, health insurance etc.,

Even though data are anonymised at times, it has the possibility of being vulnerable. Hence this is the reason regulatory rules are imposed heavily when it comes to using private data.

5. Internal Working Of Deep Learning

This sub-field of ML is actually responsible for today’s AI growth. What was once just a theory has appeared to be the most powerful aspect of ML. Deep Learning (DL) now powers applications such as voice recognition, image recognition and so on through artificial neural networks.

But, the internal working of DL is still unknown and yet to be solved. Advanced DL algorithms still baffle researchers in terms of its working and efficiency. Millions of neurons that form the neural networks in DL increase abstraction at every level, which cannot be comprehended at all. This is why deep learning is dubbed a ‘black box’ since its internal agenda is unknown.

7. What are the various methods and technologies for solving machine learning problems? Any two of them should be defined in detail.

Some most popular methods for solving machine learning problems are:

* Regression
* Classification
* Clustering
* Dimensionality Reduction
* Ensemble Methods
* Neural Nets and Deep Learning
* Transfer Learning
* Reinforcement Learning
* Natural Language Processing
* Word Embeddings

**Different technologies: Machine learning**

1. Deep Neural Networks (DNN)

Deep neural networks are a subset of machine learning algorithms that have been around since the 1950s. DNNs can perform tasks like image recognition, speech recognition, and natural language processing. They consist of multiple hidden layers of neurons where each layer learns a representation of its input data. These representations are then used to make predictions about the output data.

2. Generative Adversarial Networks

Generative adversarial networks (GANs) are a type of generative model that trains two competing neural networks against each other. One network tries to generate samples that look realistic, while the other evaluates whether those samples come from real data or generated data. GANs have shown great success in generating images and videos.GANs are used to generate new data that resembles the existing data but is in fact totally new we can use GANs to produce new images from existing masterpieces made by renowned artists also known as contemporary AI art they are artists working with the generative models produced masterpieces already you can find out a few of the artists who are using AI and ML for their contemporary art. We are using the existing data and we are generating new images.

3. Deep Learning

Deep learning is a subset of machine learning that uses multiple processing layers (usually hundreds) to learn data representations. This allows computers to perform tasks that are difficult for humans. Deep learning has been used in many fields, including computer vision, speech recognition, natural language processing, robotics, and reinforcement learning.

5. Conversational AI or conversational BOTS

It is a technology where we speak to a chatbot and it processes the voice after recognizing the voice input or text input as well and then a certain task or a response is enabled like

Real-life examples

Google Assistant, Alexa, and Siri. You see a lot of chatbots on many websites on product landing pages where they will simply give you a response based on the input. But what’s new now? Now conversational bots in the form of virtual assistants are enabling a new ground for customer engagement at the next level where organizations will be going for cognitive conversational AI where a part is efficient enough to understand the context and dialogue as human behavior so this will shape the future of conversational AI which will enable more ground of studies related to human

6. Machine learning in cybersecurity

Cybersecurity is a domain where it is made sure that an organization or anyone for that matter is safe from all security-related threats on the Internet or where there is a network involved. An organization deals with a lot of sophisticated data that needs to be saved from malicious threats like anyone trying to break into your server or trying to get access to your data or unauthorized access so that is the cyber security. With machine learning, it becomes quite easier to study the previous data to make alerts for the upcoming threats. So let’s say we have a company or we have cybersecurity having a lot of previous year’s data where so many malicious attacks or malicious threats happened. We can use that data to train a model which will eventually prevent our help in maintaining the system and make it more secure so more and more companies will look for machine learning-related solutions to tackle the security threats.

8. Can you explain the various forms of supervised learning? Explain each one with an example application.

Various types of algorithms and computation methods are used in the supervised learning process. Below are some of the common types of supervised learning algorithms:

**1. Regression**

Regression is used to understand the relationship between dependable and independent variables. Moreover, it is a type of supervised learning that learns from labelled data sets to predict continuous output for different data in an algorithm. It is believed to be widely used in scenarios where the output needs to be a finite value, for instance, height or weight, etc.

There two types of regression; they are as follows:

Linear regression

It is used to identify the relationship between two variables, typically used for making future predictions. Moreover, linear regression is sub-divided based on the number of independent and dependent variables.

For instance, if there is one independent and one dependent variable, it is known as simple linear regression. Meanwhile, if there are two or more independent and dependent variables, it is called multiple linear regression.

Logistic regression

Logistic regression is used when the dependent variable is categorical or has binary outputs like ‘yes’ or ‘no’. Moreover, logistic regression is used to solve binary classification problems; that’s why it predicts discreet values for variables.

**2. Naive Bayes**

A Naive Bayes algorithm is used for large datasets. The approach works on the fundamental that every programme in the algorithm works independently. This means that the presence of one feature will not impact the other. Generally, it is used in text classification, recommendation systems, and others.

There are different types of Naive Bayes models, and the decision tree remains the most popular among business organizations. A decision tree is a unique supervised learning algorithm structurally resembling a flowchart. However, they fundamentally perform different roles and responsibilities.

A decision tree consists of control statements containing decisions and their consequences. The output in a decision tree relates to the labelling of unforeseen data. ID3 and CART are some of the popular decision tree algorithms widely used across various industries.

**3. Classification**

It is a type of supervised learning algorithm that accurately assigns data into different categories or classes. It recognizes specific entities and analyses them to conclude where those entities must be categorized. Some of the classification algorithms are as follows:

K-nearest neighbor

Random forest

Support vector machines

Decision tree

Linear classifiers

**4. Neutral networks**

This type of supervised learning algorithm is used to group or categorize raw data. In addition, it is used for finding a pattern or interpreting sensory data. However, the algorithm requires numerous amounts of computation resources. As a result, its uses are constrained.

**5. Random forest**

A random forest algorithm is often called an ensemble method because it combines different supervised learning methods to conclude. Moreover, it uses many decision trees to output the classification of individual trees. As a result, it is widely used across industries.

In our data science and analytics courses, you will learn more about supervised learning and other artificial intelligence systems. In addition, we have partnered with reputed universities and colleges to develop courses that help in building a successful career in data science and analytics. Therefore, enrolling in Emeritus India courses will ensure that you know more than data analytics meaning.

9. What is the difference between supervised and unsupervised learning? With a sample application in each region, explain the differences.

|  |  |  |
| --- | --- | --- |
|  | SUPERVISED LEARNING | UNSUPERVISED LEARNING |
| Input Data | Uses Known and Labeled Data as input | Uses Unknown Data as input |
| Computational Complexity | Less Computational Complexity | More Computational Complex |
| Real Time | Uses off-line analysis | Uses Real Time Analysis of Data |
| Number of Classes | Number of Classes are known | Number of Classes are not known |
| Accuracy of Results | Accurate and Reliable Results | Moderate Accurate and Reliable Results |
| Output data | Desired output is given. | Desired output is not given. |
| Model | In supervised learning it is not possible to learn larger and more complex models than with supervised learning | In unsupervised learning it is possible to learn larger and more complex models than with unsupervised learning |
| Training data | In supervised learning training data is used to infer model | In unsupervised learning training data is not used. |
| Another name | Supervised learning is also called classification. | Unsupervised learning is also called clustering. |
| Test of model | We can test our model. | We can not test our model. |
| Example | Optical Character Recognition | Find a face in an image. |

10. Describe the machine learning process in depth.

Machine Learning – Stages: We can split ML process stages into 5 as below mentioned in the flow diagram.

* Collection of Data
* Data Wrangling
* Model Building
* Model Evaluation
* Model Deployment

Identifying the Business Problems, before we go to the above stages. So, we must be clear about the objective of the purpose of ML implementation. To find the solution for the given/identified problem. we must collect the data and follow up the below stages appropriately.

**Collection of Data**

Data collection from different sources could be internal and/or external to satisfy the business requirements/problems. Data could be in any format. CSV, XML.JSON, etc., here Big Data is playing a vital role to make sure the right data is in the expected format and structure.

**Data Wrangling and Data Processing:**

The main objective of this stage and focus are as below.

Data Processing (EDA):

* Understanding the given dataset and helping clean up the given dataset.
* It gives you a better understanding of the features and the relationships between them
* Extracting essential variables and leaving behind/removing non-essential variables.
* Handling Missing values or human error.
* Identifying outliers.
* The EDA process would be maximizing insights of a dataset.

Feature engineering:

* Handling missing values in the variables
* Convert categorical into numerical since most algorithms need numerical features.
* Need to correct not Gaussian(normal). linear models assume the variables have Gaussian distribution.
* Finding Outliers are present in the data, so we either truncate the data above a threshold or transform the data using log transformation.
* Scale the features. This is required to give equal importance to all the features, and not more to the one whose value is larger.
* Feature engineering is an expensive and time-consuming process.
* Feature engineering can be a manual process, it can be automated

Training and Testing:

* The training data is used to make sure the machine recognizes patterns of the data, cross-validation of data is used to ensure better accuracy and
* the efficiency of the algorithm which is used to train the machine.
* Test data is used to see how well the machine can predict new answers based on its training.
* The train-test split procedure is used to estimate the ML performance of algorithms when they are used to make predictions on data that is not used to train the model.

Training

* Training data is the data set on which you train the model.
* Train data from which the model has learned the experiences.
* Training sets are used to fit and tune your models.

Testing

* Test data is the data which is used to check if the model has learnt good enough from the experiences it got in the train data set.
* Test sets are “unseen” data to evaluate your models.

Train data: It trains our machine learning algorithm

Test data: After the training the model, test data is used to test its efficiency and performance of the model

The purpose of the random state in train test split: Random state ensures that the splits that you generate are reproducible. The random state that you provide is used as a seed to the random number generator. This ensures that the random numbers are generated in the same order.

Data Split into Training/Testing Set

* We used to split a dataset into training data and test data in the machine learning space.
* The split range is usually 20%-80% between testing and training stages from the given data set.
* A major amount of data would be spent on to train your model
* The rest of the amount can be spent to evaluate your test model.
* But you cannot mix/reuse the same data for both Train and Test purposes
* If you evaluate your model on the same data you used to train it, your model could be very overfitted. Then there is a question of whether models can predict new data.
* Therefore, you should have separate training and test subsets of your dataset.

MODEL EVALUATION: Each model has its own model evaluation mythology, some of the best evaluations are here.

* Evaluating the Regression Model.
* Sum of Squared Error (SSE)
* Mean Squared Error (MSE)
* Root Mean Squared Error (RMSE)
* Mean Absolute Error (MAE)
* Coefficient of Determination (R2)
* Adjusted R2
* Evaluating Classification Model.
* Confusion Matrix.
* Accuracy Score.
* AUC and ROC.|

Deployment of an ML-model simply means the integration of the finalized model into a production environment and getting results to make business decisions.

a. Make brief notes on any two of the following:

MATLAB is one of the most widely used programming languages.

MATLAB as a computer language written in a mathematical scripting code is very much similar to C++ and has the following advantages over other programs: It uses efficient vector and matrix computations. It allows for string processing. It allows for easy creation of engineering graphics.

MATLAB language is the first (and often only) programming language for many engineers and scientists because the matrix math and array orientation of the language makes it easy to learn and apply to engineering and scientific problem-solving.

Millions of engineers and scientists worldwide use MATLAB for a range of applications, in industry and academia, including deep learning and machine learning, signal processing and communications, image and video processing, control systems, test and measurement, computational finance, and computational biology.

ii. Deep learning applications in healthcare

Drug Discovery

The role of deep learning in identifying drug combinations is significant. During the pandemic, vaccine and drug development were funded by disruptive technologies like AI, machine learning, and deep learning. Since drug discovery is a complex task, deep learning can make it faster, cost-effective, and easier. Deep learning algorithms can predict the drug properties, drug-target interaction prediction, and in generating a compound with desired properties. Deep learning algorithms can easily process genomic, clinical, and population data and various toolkits can be used to detect patterns between the data. By leveraging machine learning and deep learning, researchers are now able to perform faster molecular modeling and predictive analytics in defining protein structures.

Medical Imaging and Diagnostics

Deep learning models can interpret medical images like X-ray, MRI scan, CT scan, etc., to perform diagnosis. The algorithms can detect any risk and flag anomalies in the medical images. Deep learning is extensively used in detecting cancer. The recent innovation of computer vision was enabled by machine learning and deep learning. With a faster diagnosis through medical imaging, it becomes easier to treat diseases.

Simplifying Clinical Trials

Clinical trials are complicated and expensive. Machine learning and deep learning can be leveraged to perform predictive analytics to identify potential candidates for clinical trials and enable scientists to pool in people from different data points and sources. Deep learning will also enable continuous monitoring of these trials with minimum errors and human intervention.

Personalized Treatment

With deep learning models, it becomes easier to analyze patient’s health data, medical history, vital symptoms, medical test results, and others. Hence, this enables healthcare providers to understand each patient and provide personalized treatment for them. These disruptive technologies enable the detection of suitable and multiple treatment options for different patients. With real-time data collection through connected devices, machine learning models can use deep neural networks to predict upcoming health conditions or risks and provide specific medicines or treatments.

Improved Health Records and Patient Monitoring

Deep learning and machine learning models can process and analyze various medical and healthcare data, both structured and unstructured. Document classification and maintaining up-to-date health records might become manually difficult. Thus, machine learning and its subset deep learning can be used to maintain smart health records. With the advent of telemedicine, wearables, and remote patient monitoring, there is now abundant real-time data on health and deep learning can help in intelligently monitoring the patients and predict risks.

Health Insurance and Fraud Detection

Deep learning can efficiently identify insurance frauds and predict future risks. Health insurance providers are also an advantage if they use deep learning because the models can predict the future trends and behavior to suggest smart insurance policies to their clients.

Deep Learning and NLP

Natural language processing (NLP) leverages deep learning algorithms for classification and identification. These two technologies can be used in identifying and classifying health data and can also be leveraged to develop chatbots and voice bots. In the current scenario of telehealth, chatbots play a pivotal role. It makes the interaction with patients easier and faster. These chatbots were also used to spread the word about Covid-19 and answer primary queries.

iii. Study of the market basket

Market basket analysis is a data mining technique used by retailers to increase sales by better understanding customer purchasing patterns. It involves analyzing large data sets, such as purchase history, to reveal product groupings, as well as products that are likely to be purchased together.

Nowadays Machine Learning is helping the Retail Industry in many different ways. You can imagine that from forecasting the performance of sales to identify the buyers, there are many applications of machine learning(ML) in the retail industry. “Market Basket Analysis” is one of the best applications of machine learning in the retail industry. By analyzing the past buying behavior of customers, we can find out which are the products that are bought frequently together by the customers.

Frequent itemset mining leads to the discovery of associations and correlations between items in huge transactional or relational datasets. With vast amounts of data continuously being collected and stored, many industries are becoming interested in mining such kinds of patterns from their databases. The disclosure of “Correlation Relationships” among huge amounts of transaction records can help in many decision-making processes such as the design of catalogs, cross-marketing, and behavior customer shopping Analysis.

A popular example of frequent itemset mining is Market Basket Analysis. This process identifies customer buying habits by finding associations between the different items that customers place in their “shopping baskets” as you can see in the following fig. The discovery of this kind of association will be helpful for retailers or marketers to develop marketing strategies by gaining insight into which items

are frequently bought together by customers.

For example, if customers are buying milk, how probably are they to also buy bread (and which kind of bread) on the same trip to the supermarket? This information may lead to increase sales by helping retailers to do selective marketing and plan their ledge space.

Suppose just think of the universe as the set of items available at the store, then each item has a Boolean variable that represents the presence or absence of that item. Now each basket can then be represented by a Boolean vector of values that are assigned to these variables. The Boolean vectors can be analyzed of buying patterns that reflect items that are frequently associated or bought together. Such patterns will be represented in the form of association rules.

What is Association Rule for Market basket Analysis?

Let I = {I1, I2,…, Im} be an itemset. Let D, the data, be a set of database transactions where each transaction T is a nonempty itemset such that T ⊆ I. Each transaction is associated with an identifier, called a TID(or Tid). Let A be a set of items(itemset). T is the Transaction which is said to contain A if A ⊆ T. An Association Rule is an implication of the form A ⇒ B, where A ⊂ I, B ⊂ I, and A ∩B = φ.

The rule A ⇒ B holds in the data set(transactions) D with supports, where ‘s’ is the percentage of transactions in D that contain A ∪ B (that is the union of set A and set B, or, both A and B). This is taken as the probability, P(A ∪ B). Rule A ⇒ B has confidence c in the transaction set D, where c is the percentage of transactions in D containing A that also contains B. This is taken to be the conditional probability, like P(B|A). That is,

support(A⇒ B) =P(A ∪ B)

confidence(A⇒ B) =P(B|A)

Rules that satisfy both a minimum support threshold (called min sup) and a minimum confidence threshold (called min conf ) are called “Strong”.

Confidence(A⇒ B) = P(B|A) =

support(A ∪ B) /support(A) =

support count(A ∪ B) / support count(A)

Generally, Association Rule Mining can be viewed in a two-step process:-

1. Find all Frequent itemsets: By definition, each of these itemsets will occur at least as

frequently as a pre-established minimum support count, min sup.

2. Generate Association Rules from the Frequent itemsets: By definition, these

rules must satisfy minimum support and minimum confidence.

Association Rule Mining is primarily used when you want to identify an association between different items in a set, then find frequent patterns in a transactional database, relational databases(RDBMS).

Algorithms used in Market Basket Analysis

There are Multiple Techniques and Algorithms are used in Market Basket Analysis. One of the important objectives is “to predict the probability of items that are being bought together by customers”.

AIS

SETM Algorithm

Apriori Algorithm

FP Growth

> Apriori Algorithm:

Apriori Algorithm is a widely-used and well-known Association Rule algorithm and is a popular algorithm used in market basket analysis. It is also considered accurate and overtop AIS and SETM algorithms. It helps to find frequent itemsets in transactions and identifies association rules between these items. The limitation of the Apriori Algorithm is frequent itemset generation. It needs to scan the database many times which leads to increased time and reduce performance as it is a computationally costly step because of a huge database. It uses the concept of Confidence, Support.

> AIS Algorithm:

The AIS algorithm creates multiple passes on the entire database or transactional data. During every pass, it scans all

transactions. As you can see, in the first pass, it counts the support of separate items and determines then which of them are frequent in the database. Huge itemsets of every pass are enlarged to generate candidate itemsets. After each scanning of a transaction, the common itemsets between these itemsets of the previous pass and then items of this transaction are

determined. This algorithm was the first published algorithm which is developed to generate all large itemsets in a

transactional database. It was focusing on the enhancement of databases with the necessary performance to process

decision support. This technique is bounded to

only one item in the consequent.

Advantage: The AIS algorithm was used to find whether there was an association between items or not.

Disadvantage: The main disadvantage of the AIS algorithm is that it generates too many candidates set that after turn out to be small. As well as the data structure is to be maintained.

> SETM Algorithm:

This Algorithm is quite similar to the AIS algorithm. The SETM algorithm creates collective passes over the database. As you can see, in the first pass, it counts the support of single items and then determines which of them are frequent in the

database. Then, it also generates the candidate itemsets by enlarging large itemsets of the previous pass. In addition to this, the SETM algorithm recalls the TIDs(transaction ids) of the generating transactions with the candidate itemsets.

Advantage: While generating candidate itemsets, SETM algorithm arranges candidate itemsets together with the TID(transaction Id) in a sequential manner.

Disadvantage: For every item set, there is an association with Tid, hence it requires more space to store a huge number of TIDs.

> FP Growth

FP Growth is known as Frequent Pattern Growth Algorithm. FP growth algorithm is a concept of representing the data in the form of an FP tree or Frequent Pattern. Hence FP Growth is a method of Mining Frequent Itemsets. This algorithm is an advancement to the Apriori Algorithm. There is no need for candidate generation to generate the frequent pattern. This frequent pattern tree structure maintains the association between the itemsets.

A Frequent Pattern Tree is a tree structure that is made with the earlier itemsets of the data. The main purpose of the FP tree is to mine the most frequent patterns. Every node of the FP tree represents an item of that itemset. The root node represents the null value whereas the lower nodes represent the itemsets of the data. The association of these nodes with the lower nodes that is between itemsets is maintained while creating the tree.

iv. Linear regression (simple)

What is Simple Linear Regression in Machine Learning?

By Simplilearn

Last updated on Feb 24, 20233694

What is Simple Linear Regression in Machine Learning?

Table of Contents

What Is Simple Linear Regression?Simple Linear Regression vs. Multiple Linear RegressionImplementation of Simple Linear Regression Algorithm using PythonAssumptions of Simple Linear RegressionOur Learners Also AskedView More

Regression is a tool that allows you to estimate how the dependent variable changes as the independent variable(s) change.

Regression models describe the relationship between variables by fitting a line to the observed data. Linear regression models use a straight line, while logistic and nonlinear regression models use a curved line.

Regression models can be used for many purposes:

Evaluating the effect of an independent variable on a dependent variable.

Forecasting future values of the dependent variable based on prior observations of both variables.

Master The Right AI Tools For The Right Job!

Caltech Post Graduate Program in AI & MLEXPLORE PROGRAMMaster The Right AI Tools For The Right Job!

What Is Simple Linear Regression?

Simple linear regression is a statistical method for establishing the relationship between two variables using a straight line. The line is drawn by finding the slope and intercept, which define the line and minimize regression errors.

The simplest form of simple linear regression has only one x variable and one y variable. The x variable is the independent variable because it is independent of what you try to predict the dependent variable. The y variable is the dependent variable because it depends on what you try to predict.

y = β0 +β1x+ε is the formula used for simple linear regression.

y is the predicted value of the dependent variable (y) for any given value of the independent variable (x).

B0 is the intercept, the predicted value of y when the x is 0.

B1 is the regression coefficient – how much we expect y to change as x increases.

x is the independent variable ( the variable we expect is influencing y).

e is the error of the estimate, or how much variation there is in our regression coefficient estimate.

Simple linear regression establishes a line that fits your data, but it does not guarantee that the line is good enough. For example, if your data points have an upward trend and are very far apart, then simple linear regression will give you a downward-sloping line, which will not match your data.

11. Make a comparison between:-

1. Generalization and abstraction

Abstraction: It involves the translation of data into broader representations. Generalization: It uses abstracted data to form a basis for action.

Abstraction aims at simplifying the description of an entity while generalization looks for common properties among these abstractions. Generalizations are clearly important and prevalent in many disciplines of study.

2. Learning that is guided and unsupervised

Supervised machine learning is generally used to classify data or make predictions, whereas unsupervised learning is generally used to understand relationships within datasets. Supervised machine learning is much more resource-intensive because of the need for labelled data.

3. Regression and classification

The most significant difference between regression vs classification is that while regression helps predict a continuous quantity, classification predicts discrete class labels. There are also some overlaps between the two types of machine learning algorithms.