Generative AI : From Theory to Practice

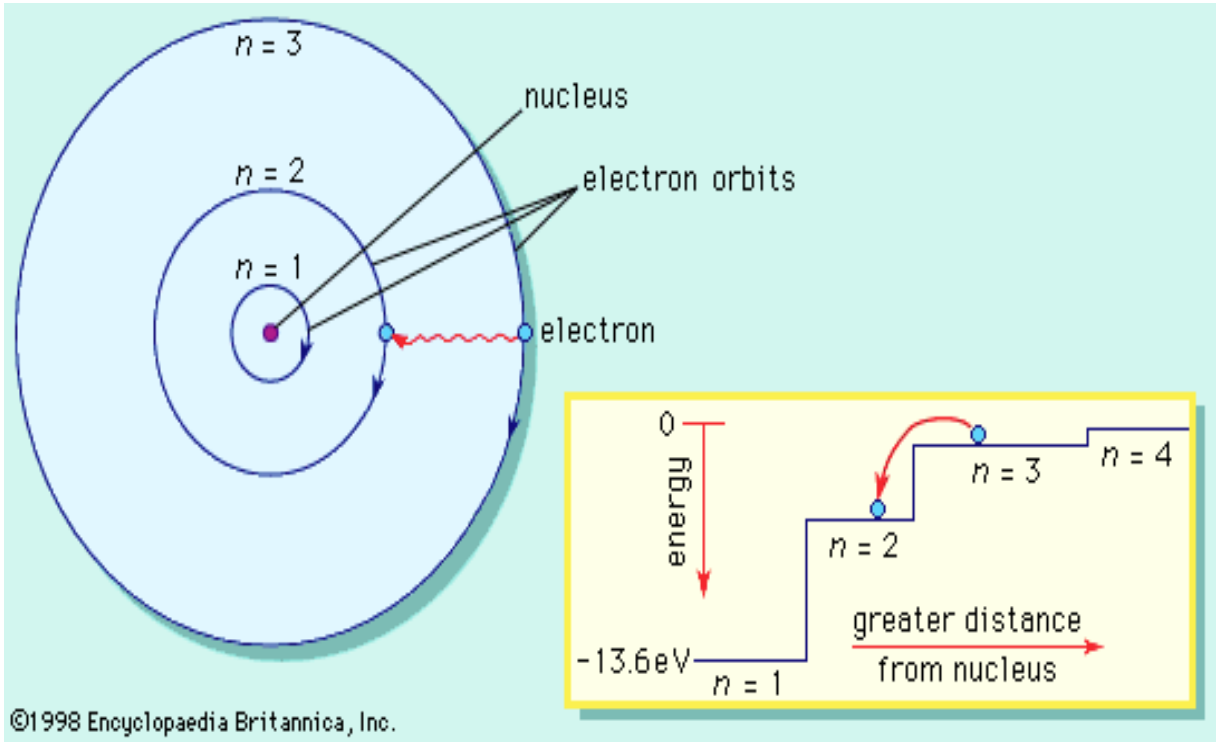
Dr. Nimrita Koul

Associate Professor, Machine Learning

www.linkedin.com/in/nimritakoul

Scientific Modelling

- Scientific modeling is the process of creation of a physical, conceptual, or mathematical representation of a real phenomenon or system (that is difficult to observe directly) to understand, predict or control its behavior.



Bohr's Model of an Atom, Source: Encyclopaedia Brittanica Inc.

Malthusian Models for Population Growth Modelling

$$P(t) = P_0 e^{rt}$$

$P_0 = P(0)$ is the initial size of the population
r is the population growth rate
t = time

The model can also be written in the form of a differential equation:

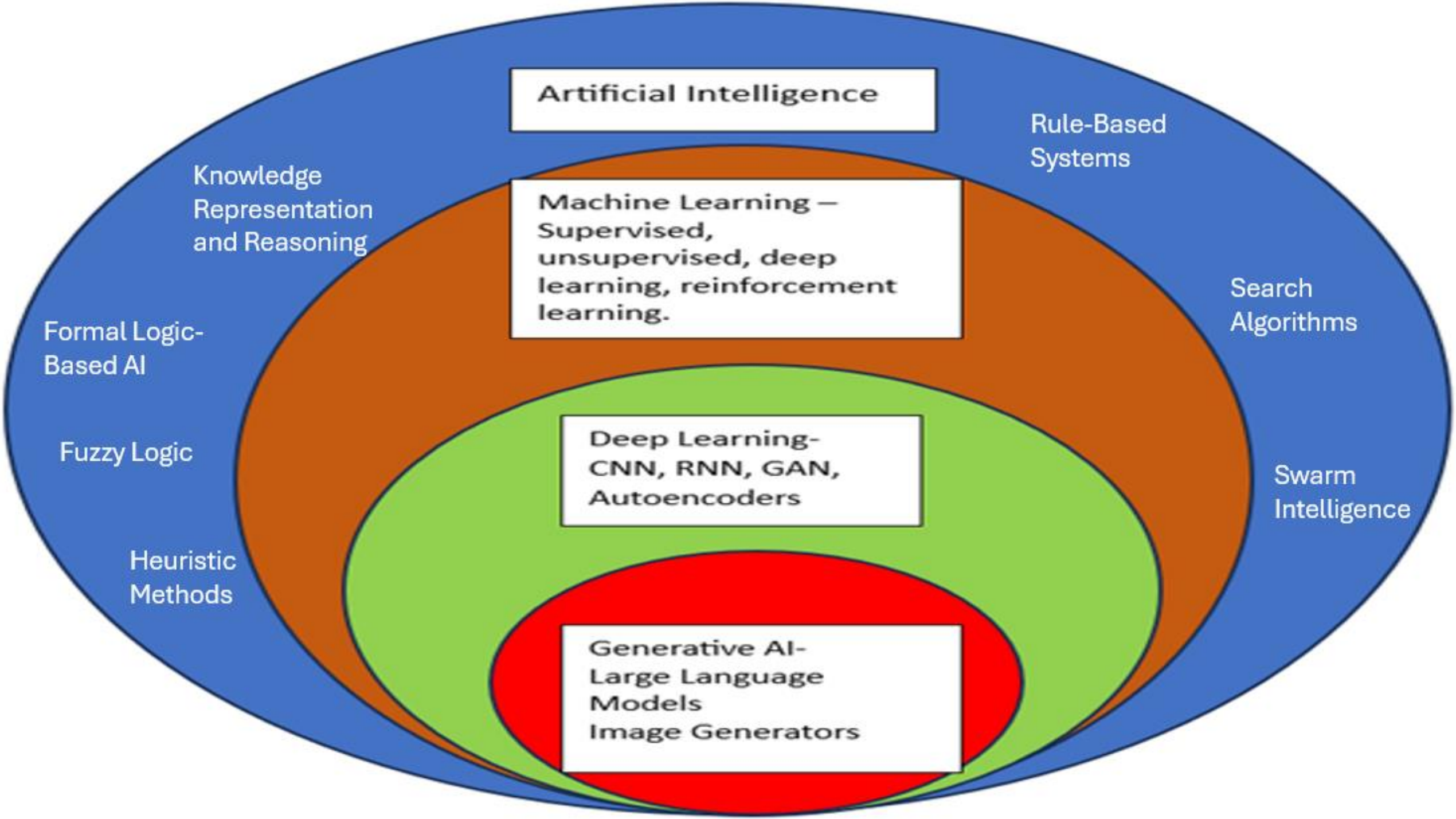
$$\frac{dP}{dt} = rP$$

with initial condition: $P(0) = P_0$

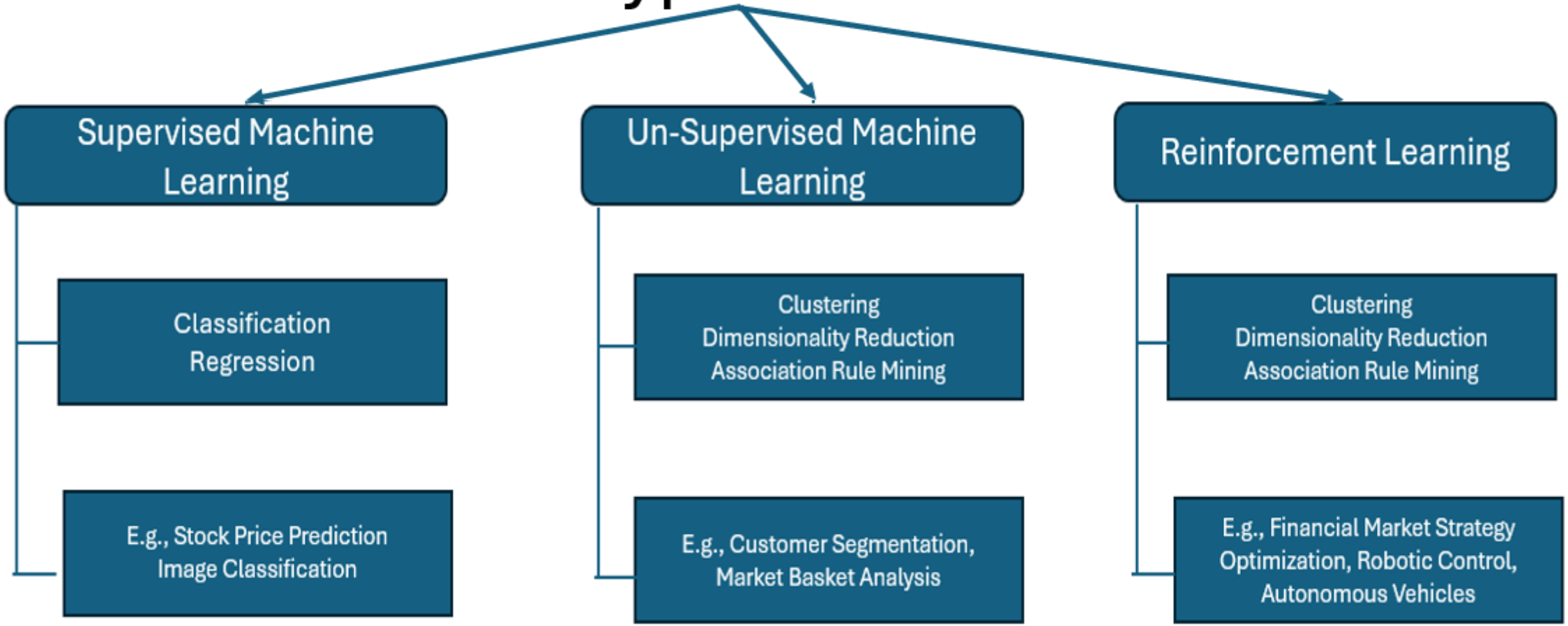
Image Source Credit: https://en.wikipedia.org/wiki/Malthusian_growth_model

Artificial Intelligence

Simulating human intelligence in machines.


Artificial Intelligence
Rule-Based Systems
Knowledge Representation and Reasoning
Machine Learning – Supervised, unsupervised, deep learning, reinforcement learning.
Search Algorithms
Formal Logic-Based AI
Fuzzy Logic
Deep Learning- CNN, RNN, GAN, Autoencoders
Swarm Intelligence
Heuristic Methods
Generative AI- Large Language Models Image Generators

Types of ML


Supervised Machine Learning
Classification
Regression
E.g., Stock Price Prediction
Image Classification
Un-Supervised Machine Learning
Clustering
Dimensionality Reduction
Association Rule Mining
E.g., Customer Segmentation,
Market Basket Analysis
Reinforcement Learning
Clustering
Dimensionality Reduction
Association Rule Mining
E.g., Financial Market Strategy
Optimization, Robotic Control,
Autonomous Vehicles

Types of ML

Semi-Supervised Learning

- Self-training models
- Semi-supervised SVMs

Self-Supervised Learning

- Contrastive Learning
- Masked Autoencoders

Generative Models

- Gaussian Mixture Models
- Hidden Markov Models
- GANS
- Variational Autoencoders

Ensemble Learning

- Bagging
- Boosting

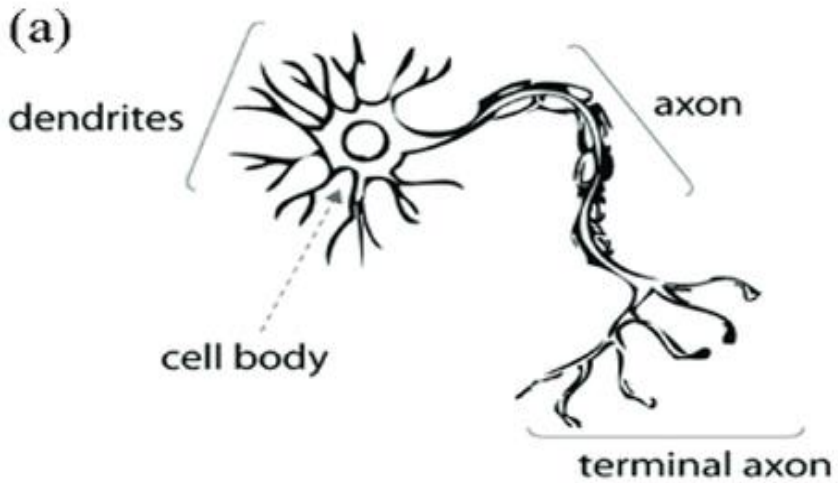
Transfer Learning

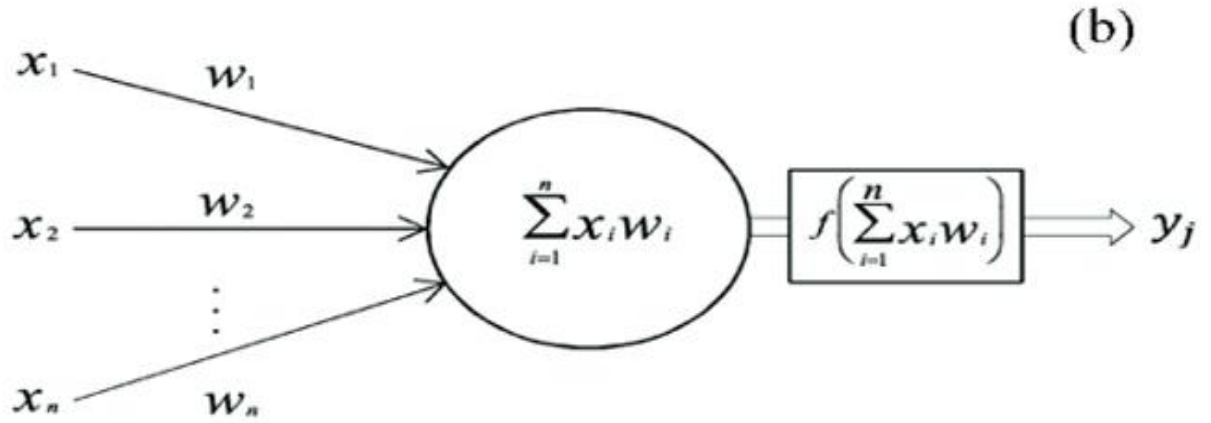
- Fine tuning pre-trained models

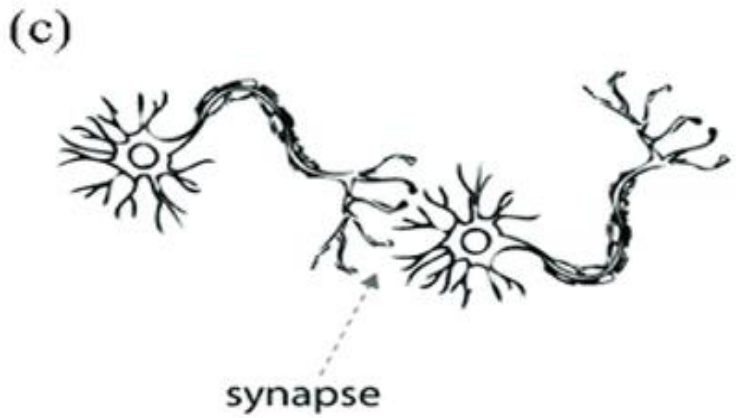
Anomaly Detection Models

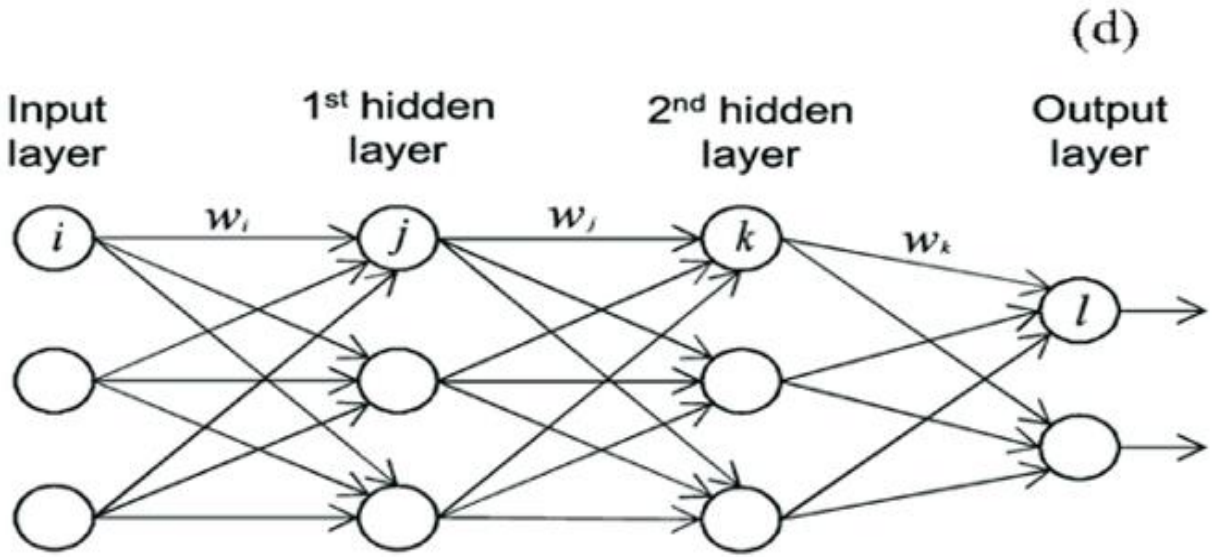
- Isolation Forest
- One Class SVM
- Autoencoders

Artificial Neural Networks



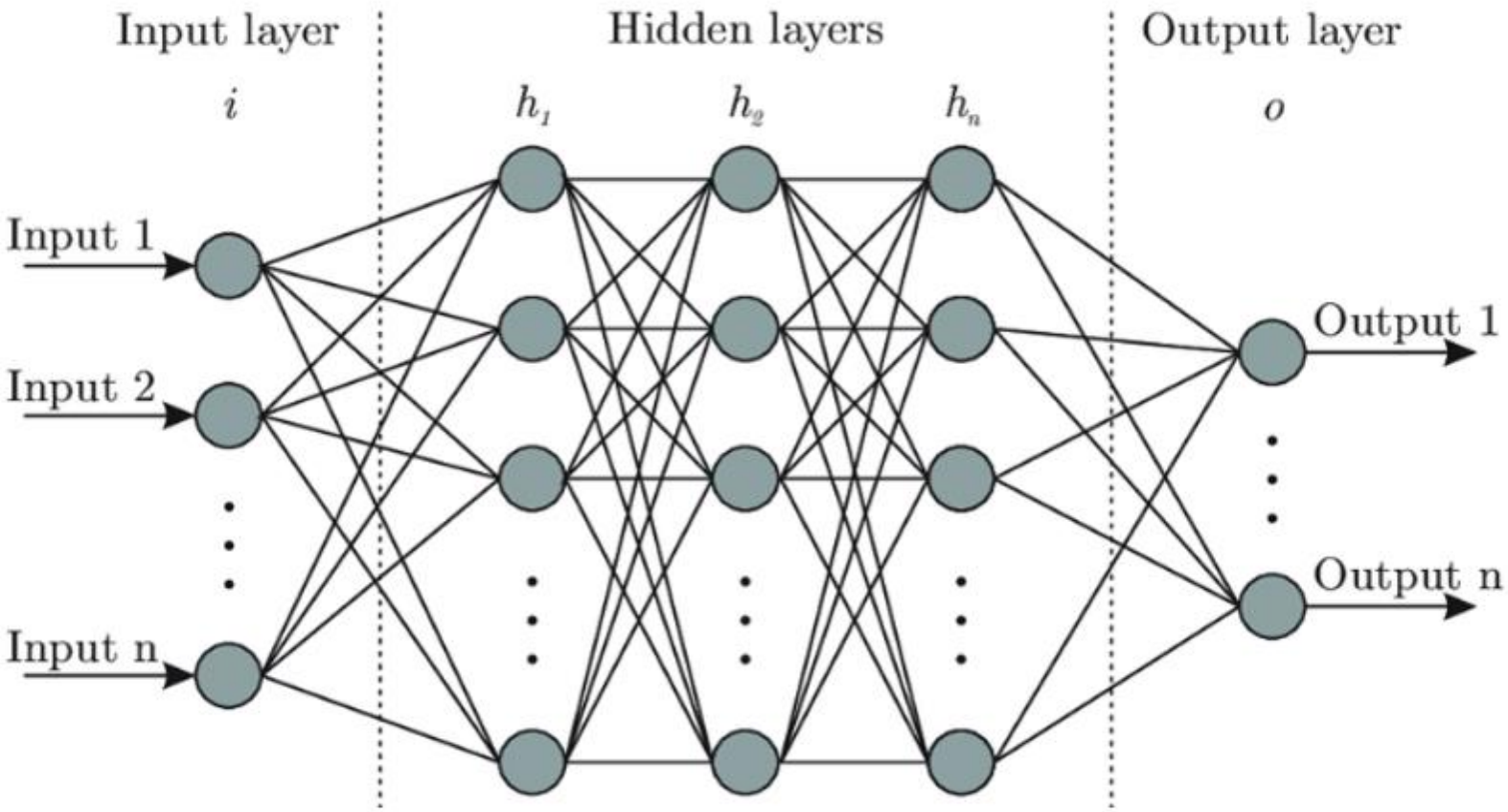






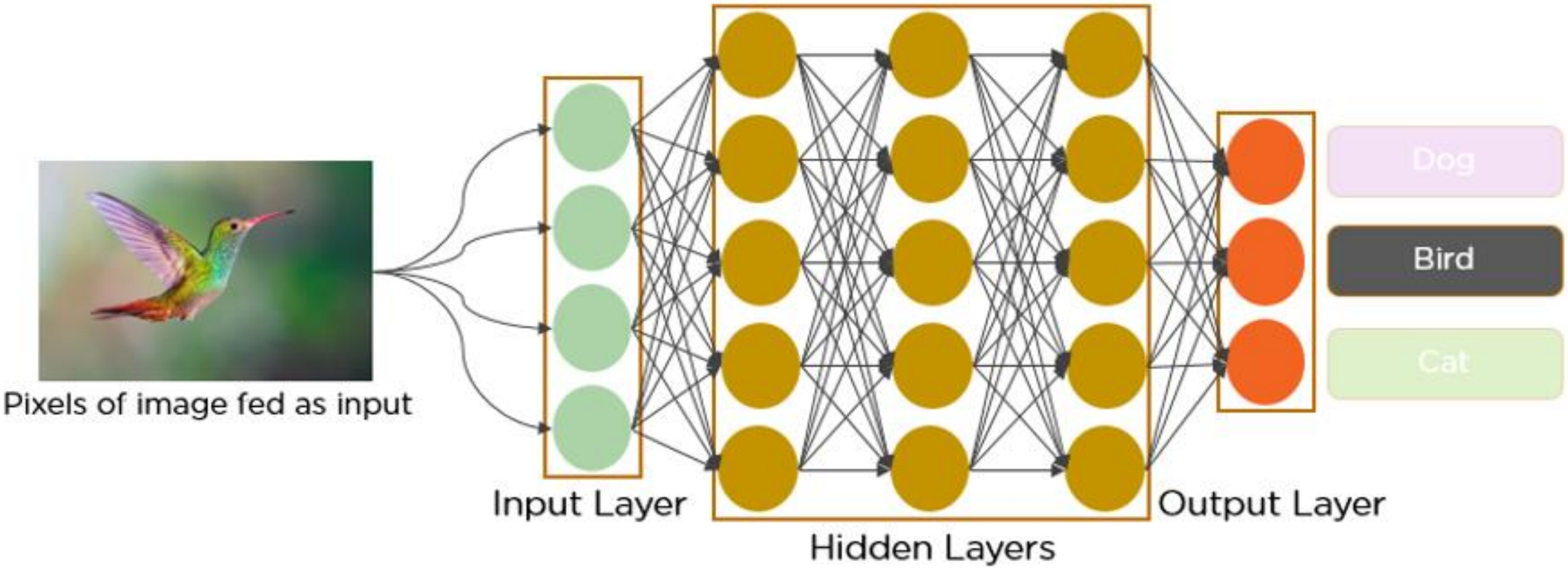
https://www.researchgate.net/publication/339446790/figure/fig2/AS:862019817320450@1582532948784/A-biological-neuron-in-comparison-to-an-artificial-neural-network-a-human-neuron-b.png

Deep Neural Networks (DNN) for Deep Learning



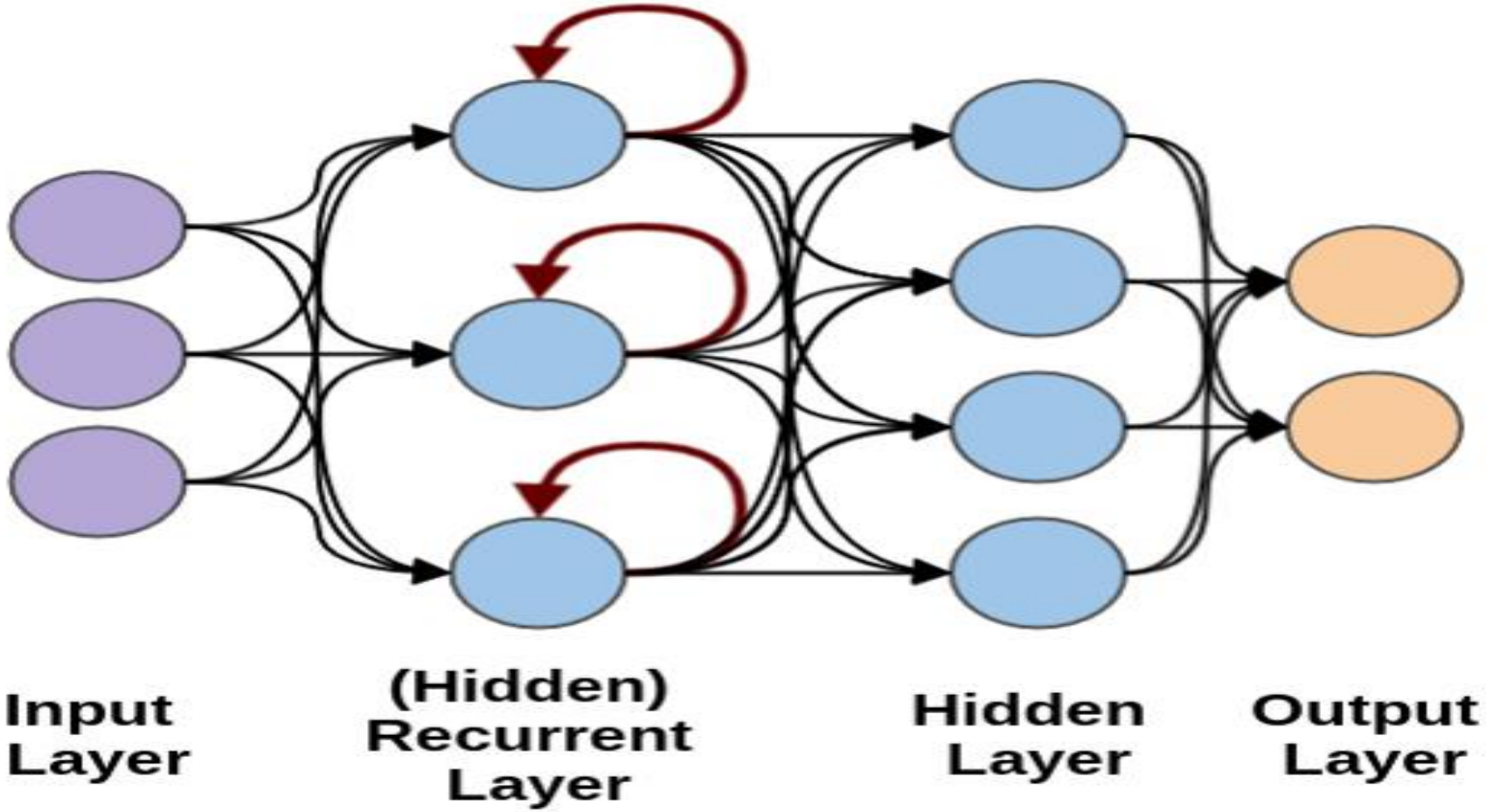
https://www.researchgate.net/figure/Artificial-neural-network-architecture-ANN-i-h-1-h-2-h-n-o_fig1_321259051

Convolutional Neural Networks



https://editor.analyticsvidhya.com/uploads/25366Convolutional_Neural_Network_to_identify_the_image_of_a_bird.png

Recurrent Neural Networks



https://www..medium.com

Transformer Model

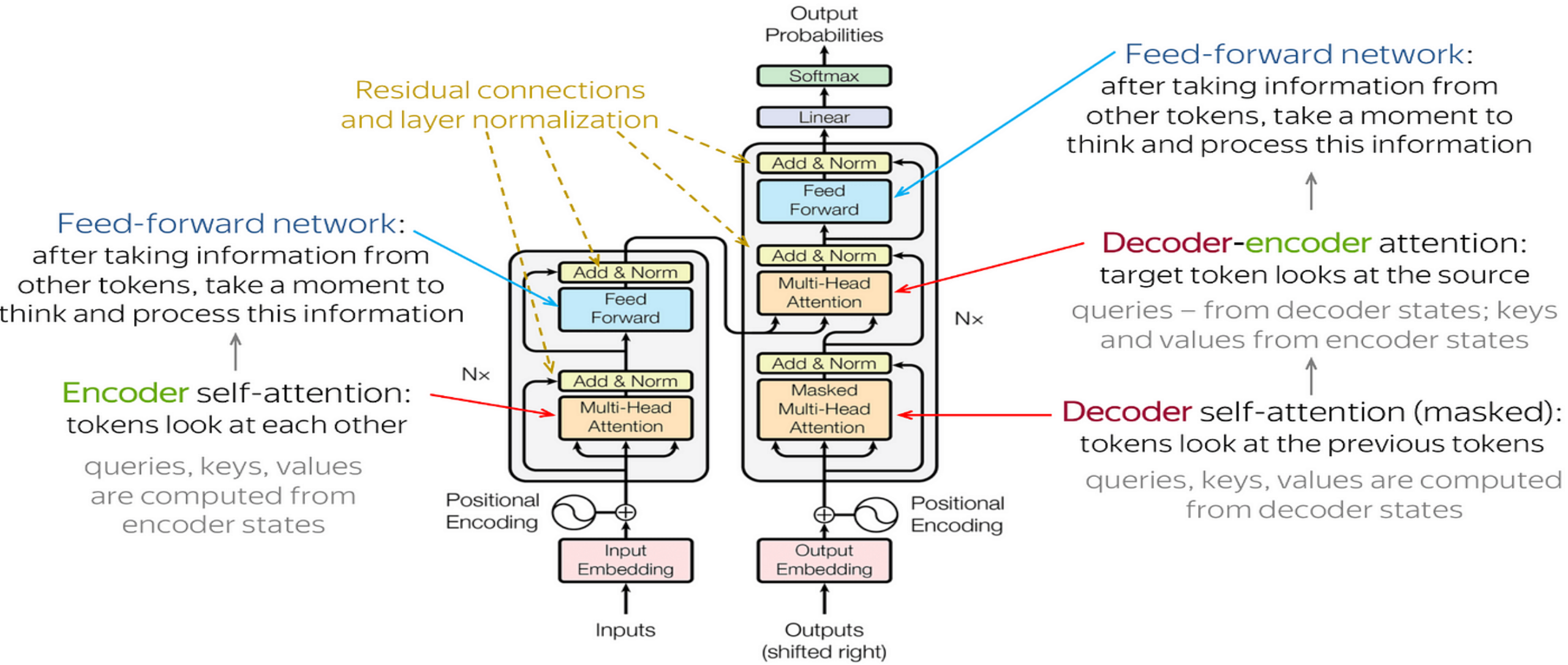
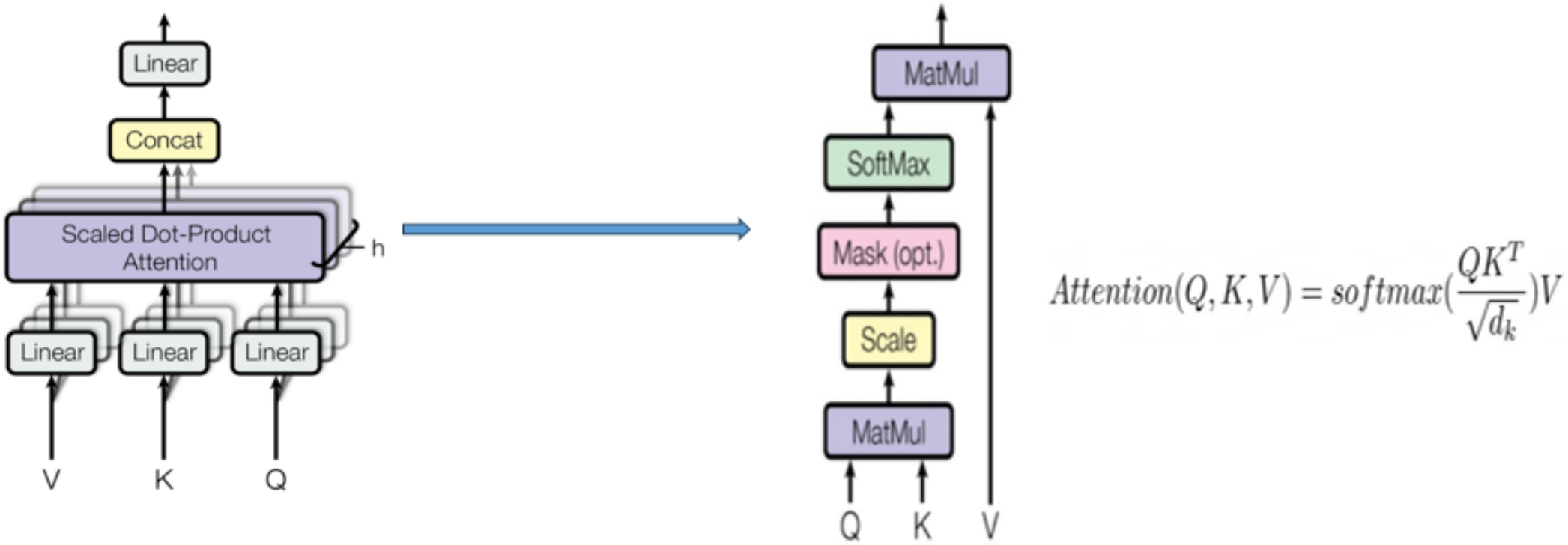


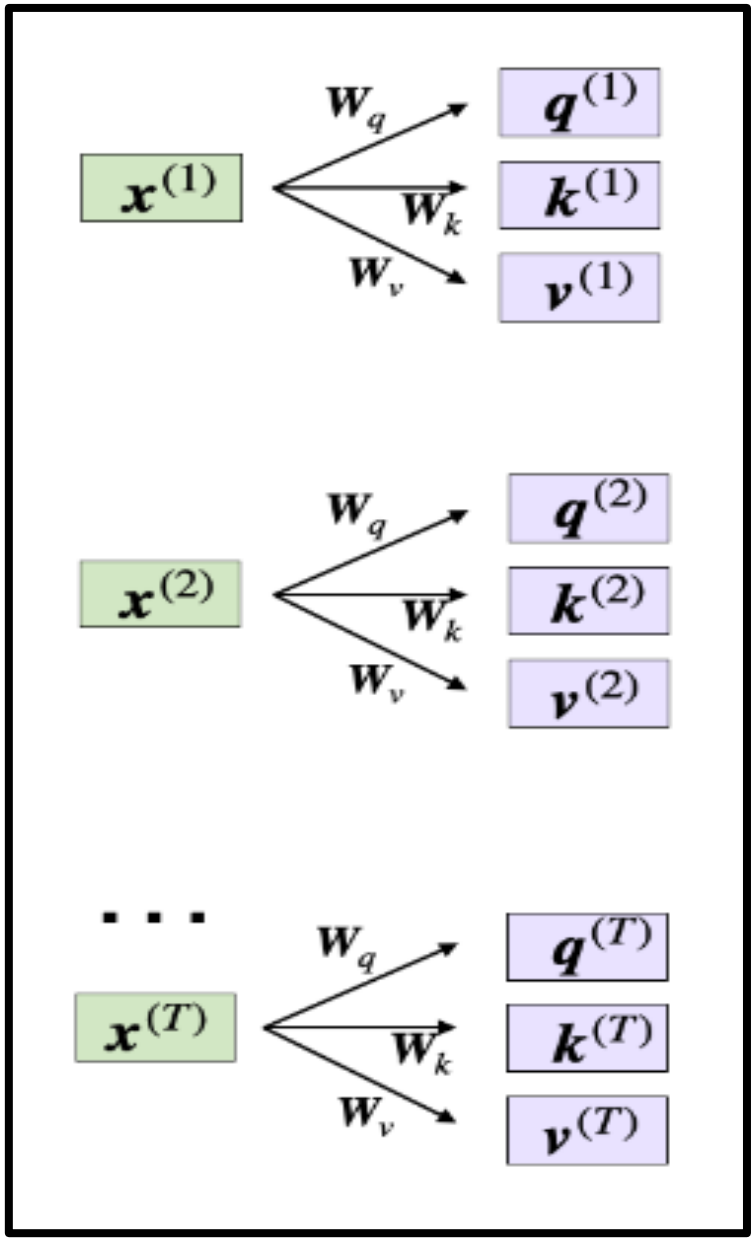
Image Source Credits: Vaswani et al. and https://pub.aimind.so/summary-of-transformer-achitecture-c2cef6dcaca6

Self-Attention

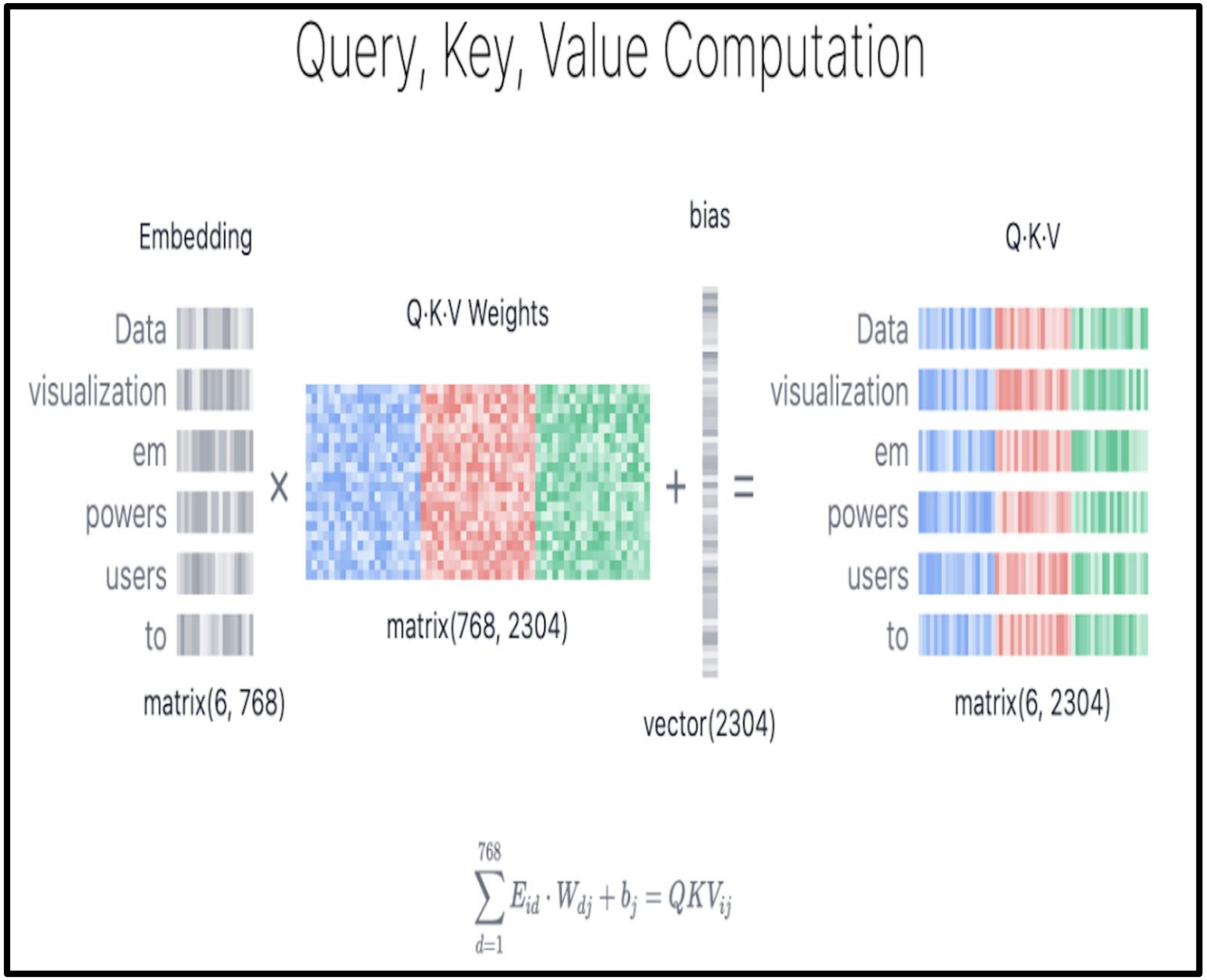


$$Attention(Q, K, V) = softmax(\frac{QK^T}{\sqrt{d_k}})V$$

Image Source Credits: Vaswani et al. Attention is all you need (2017)



Source Credits:
https://sebastianraschka.com/blog/2023/self-attention-from-scratch.html



Source Credits: https://poloclub.github.io/transformer-explainer/

Discriminative Models

Given a set of data samples X and a set of labels Y,

- Discriminative Models learn the conditional probability P(Y|X). i.e., how likely a label Y applies to instance X

- E.g., Logistic Regression and Support Vector Machines (SVMs).

Generative Models

Given a set of data instances X and a set of labels Y:

- Generative Models learn the joint probability distribution P(X,Y) or just P(X) if there are no labels.

- Gaussian Mixture Models (GMMs), Variational Autoencoders (VAEs), Generative Adversarial Networks(GANs).

Generative AI

- AI that generates new data like the existing data used to train these models.

- It learns patterns (probability distribution) of training data and generates new data of similar probability distribution.

Deep Generative Models

- Deep neural network generative models and stochastic optimization methods have enabled scalable modeling of complex, high-dimensional data including images, text, and speech.

- Deep generative models include - variational autoencoders, generative adversarial networks, autoregressive models, normalizing flow models etc.

Generative AI Models

- Autoregressive Models: (e.g., PixelRNN, Generative Pretrained Transformer)
  - Used to generate images pixel-by-pixel and text, respectively.
- Latent Variable Models: (e.g., Variational Autoencoders)
  - VAEs encode data into a latent space and decode to generate new data (image generation and anomaly detection).
- Generative Adversarial Networks (GANs): (e.g., Standard GANs, Conditional GANs)
- Diffusion Models

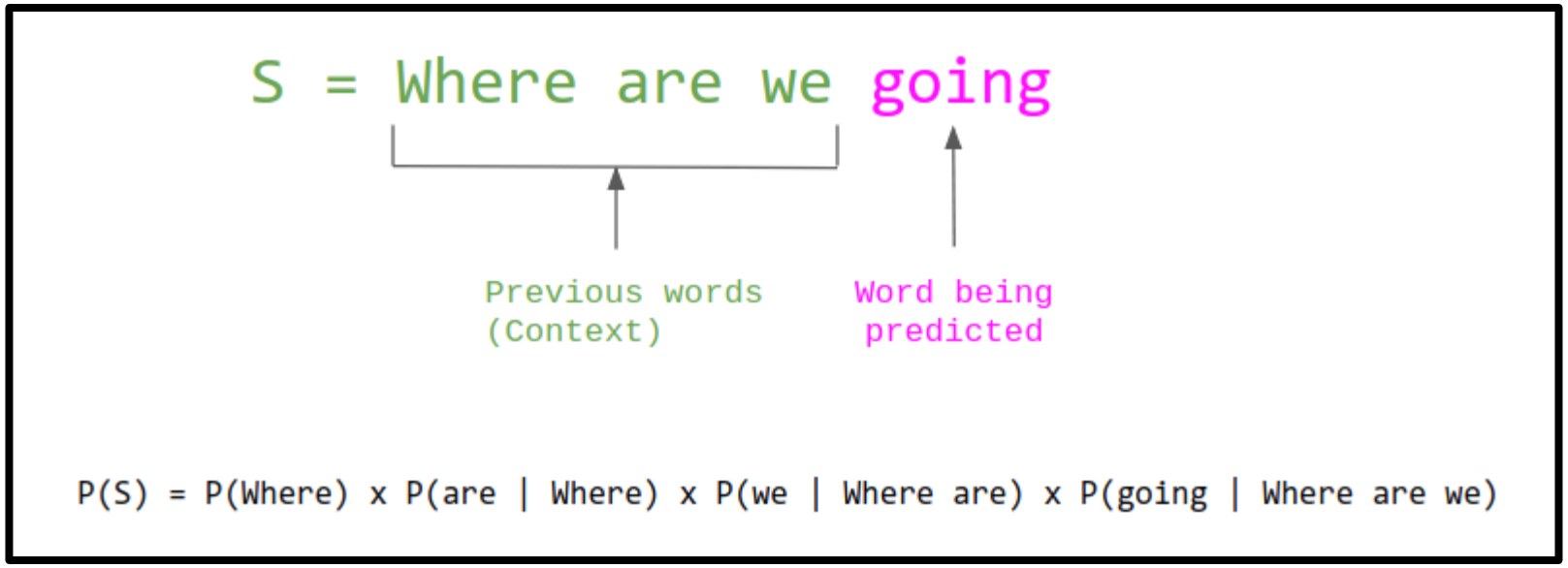
Language Models

Language Modelling

Learning the probability of next word in context

$$P_{(w_1,w_2,\ldots,w_n)} = p(w_1)p(w_2|w_1)p(w_3|w_1,w_2)...p(w_n|w_1,w_2,..,w_{n-1})$$

$$= \prod_{i=1}^{n} p(w_i|w_1,...,w_{i-1})$$



Source Credits: https://thegradient.pub/understanding-evaluation-metrics-for-language-models/

Large Language Models

- Large language models (LLMs) are transformer-based foundational models trained on enormous amounts of text data to understand and generate natural language text.

- LLMs provide foundational capabilities needed to drive multiple use cases, applications, and tasks.

GPT-2 Architecture based on Transformer Model

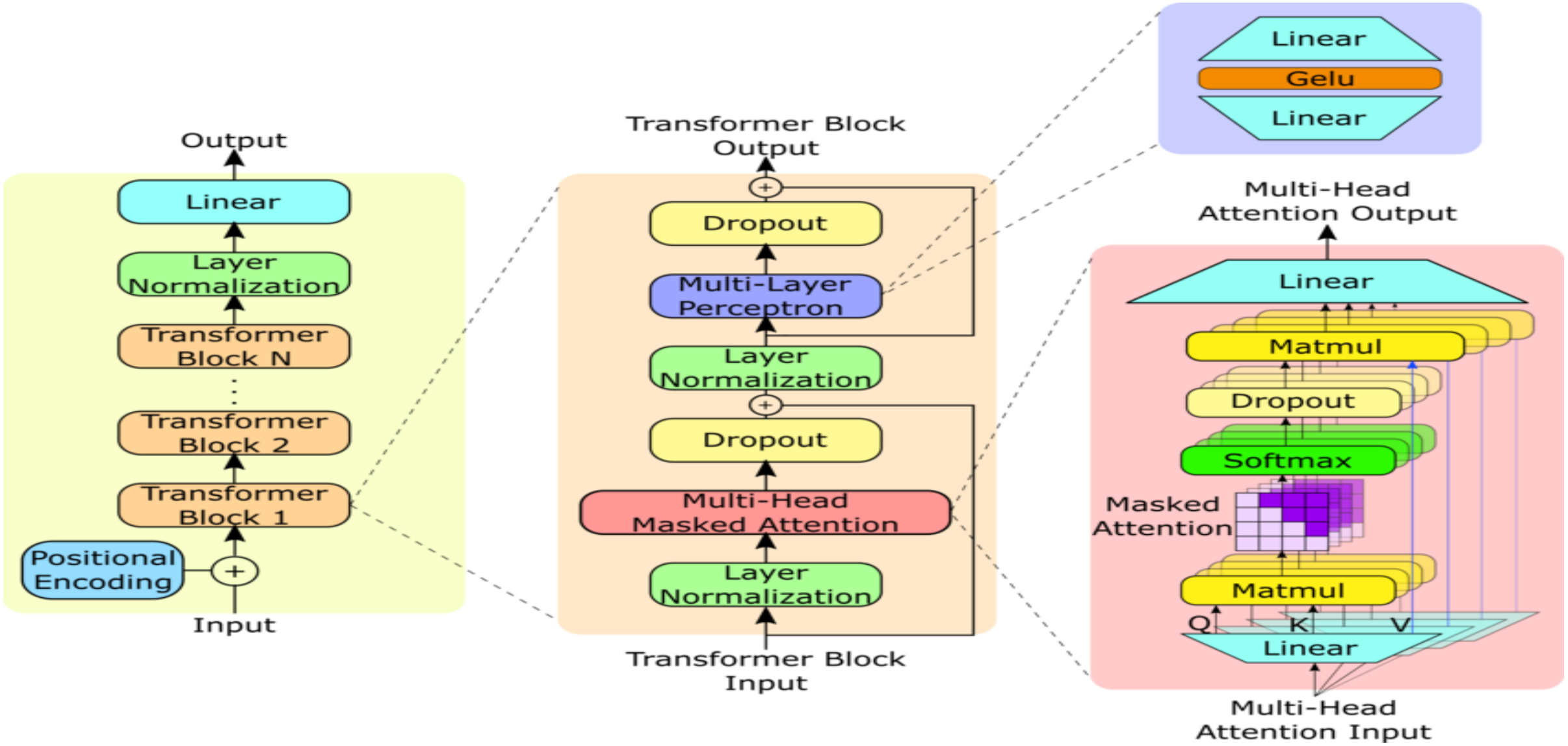


Image Source Credits: https://www.researchgate.net/figure/GPT-2-model-architecture-The-GPT-2-model-contains-N-Transformer-decoder-blocks-as-shown_fig1_373352176

GeLU: Gaussian Error Linear Unit Activation

- GELU(x) = x * P(X <= x), where P(X) ~ N(0, 1).

- Also written as, GELU(x) = x * 0.5 * (1 + erf(x / sqrt(2))),
  where erf is the error function.

LLM Use Cases

- Text generation.
- Content summarization.
- AI assistants.
- Code generation.
- Sentiment analysis.
- Language translation.

Generative Adversarial Networks

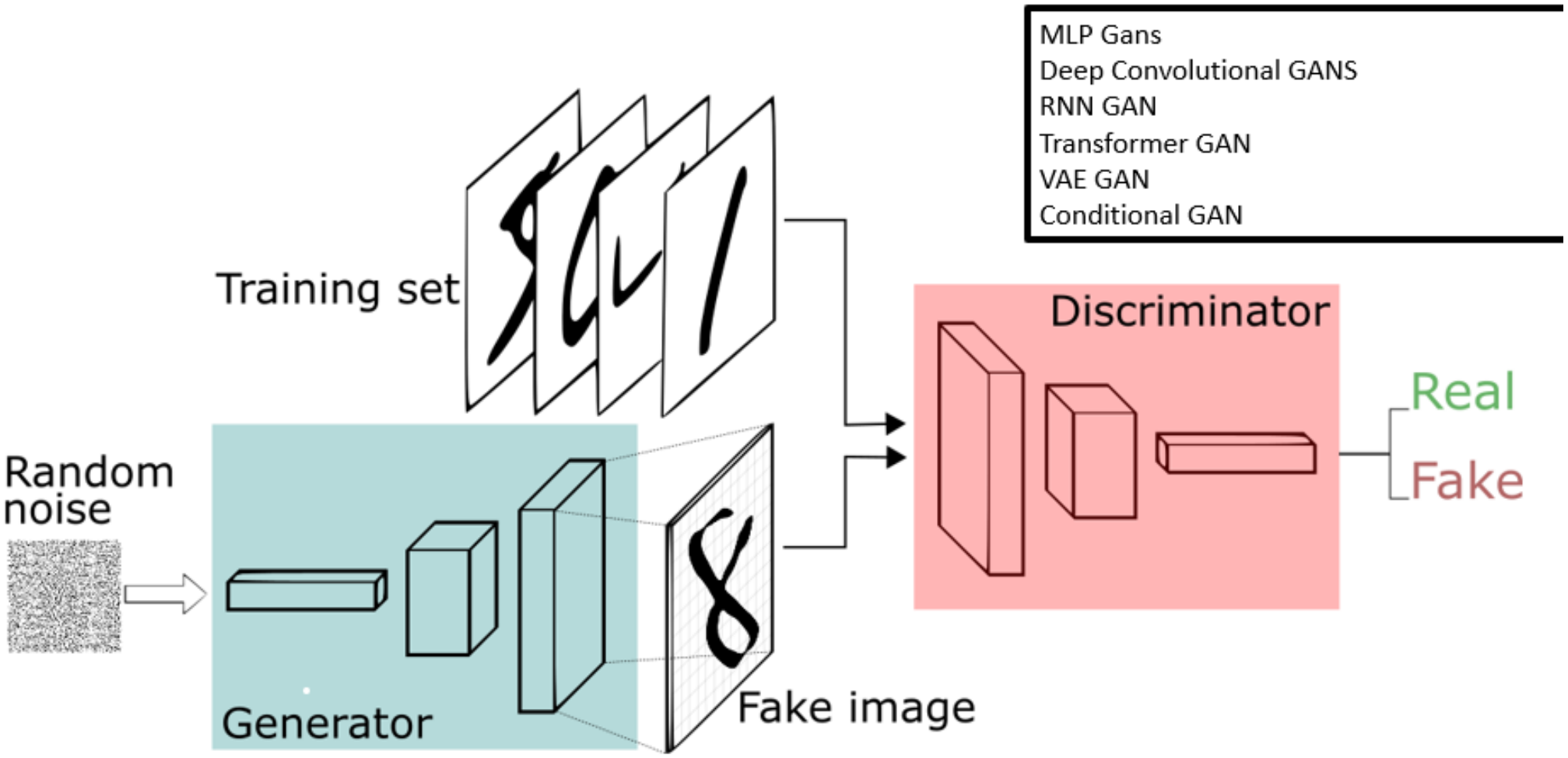


Image Source Credits: https://sthalles.github.io/intro-to-gans/

GAN Types

- Standard GAN
- Conditional GAN
  - Generate data with specific attributes
- Cycle GAN
  - Translate images from one domain to another without paired examples.

Variational Autoencoders (VAEs)

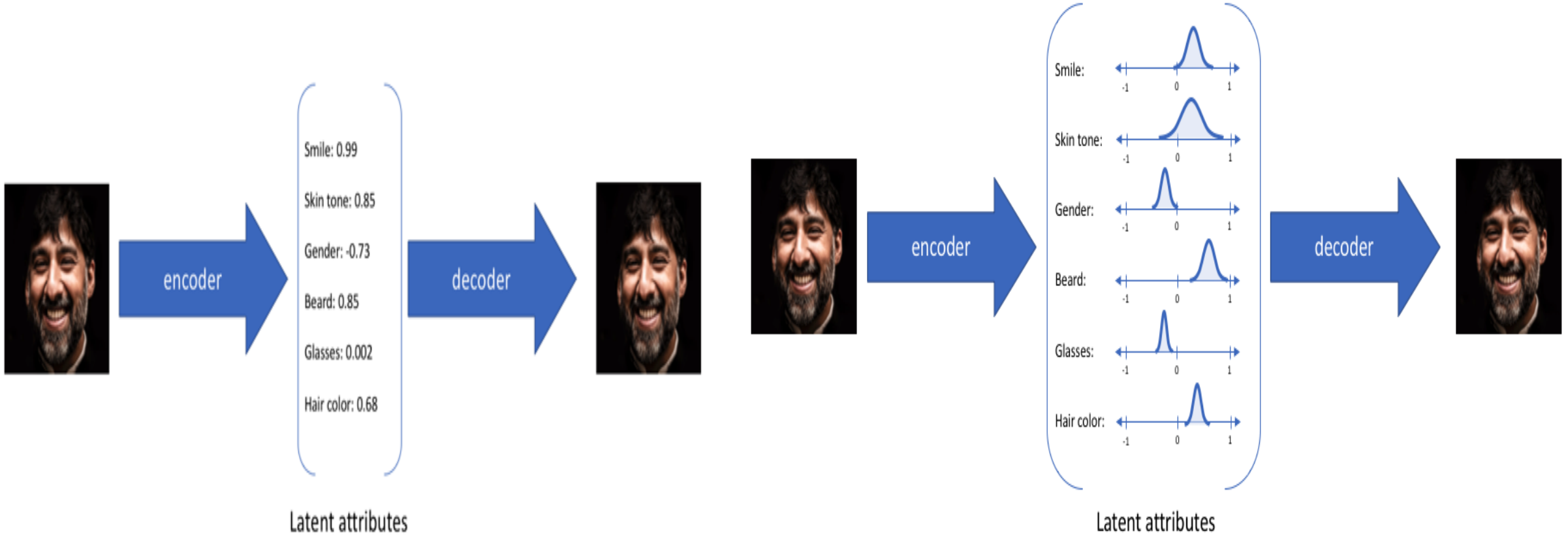


Image Source Credits: https://www.jeremyjordan.me/variational-autoencoders/

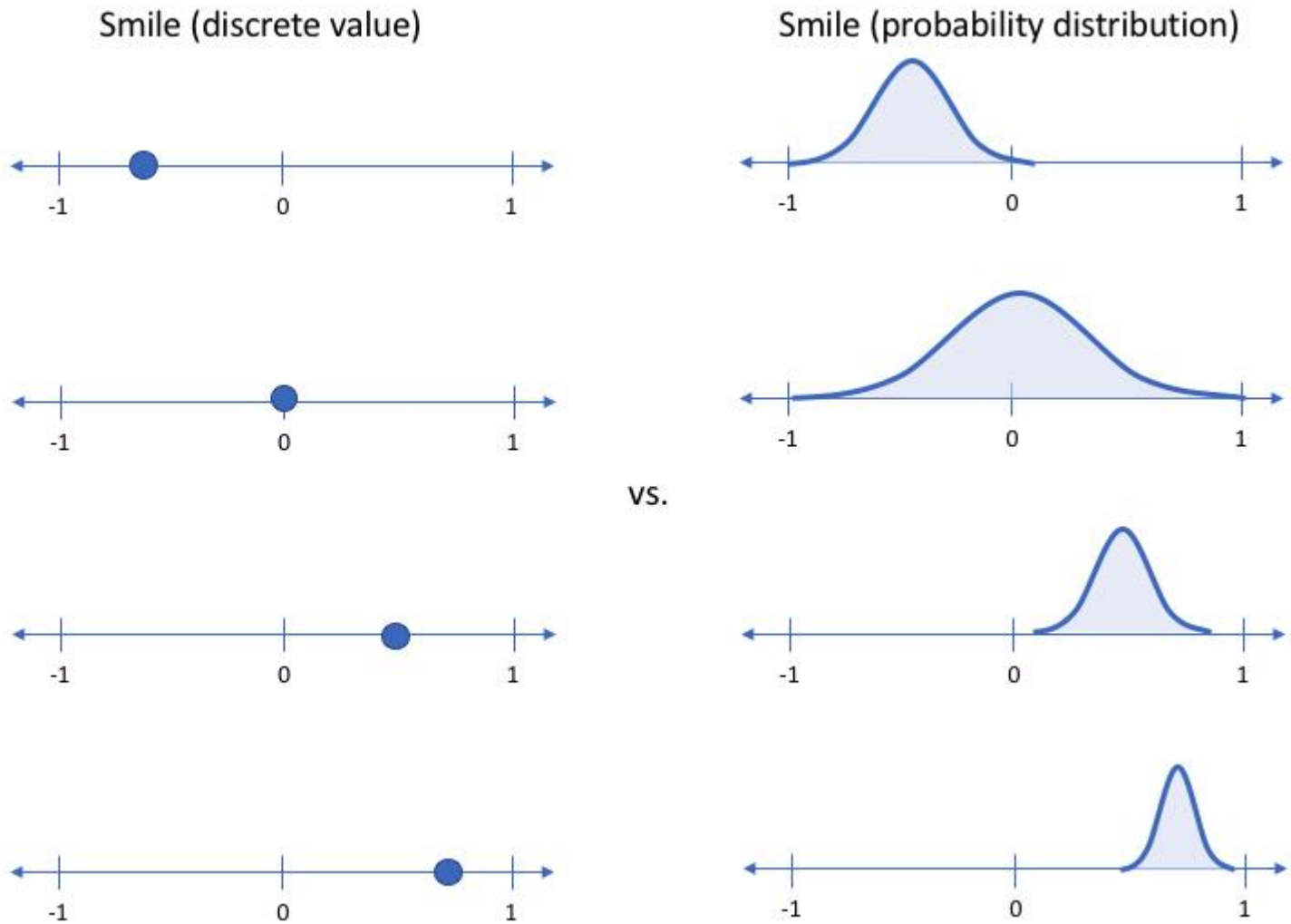


Image Source Credits: https://www.jeremyjordan.me/variational-autoencoders/

Applications of VAEs

- Image generation
- Image in-painting
- Super resolution
- Synthetic data generation
- Anomaly detection
- Data compression
- Language Modelling
- Sentence Embedding
- Speech synthesis
- Music generation

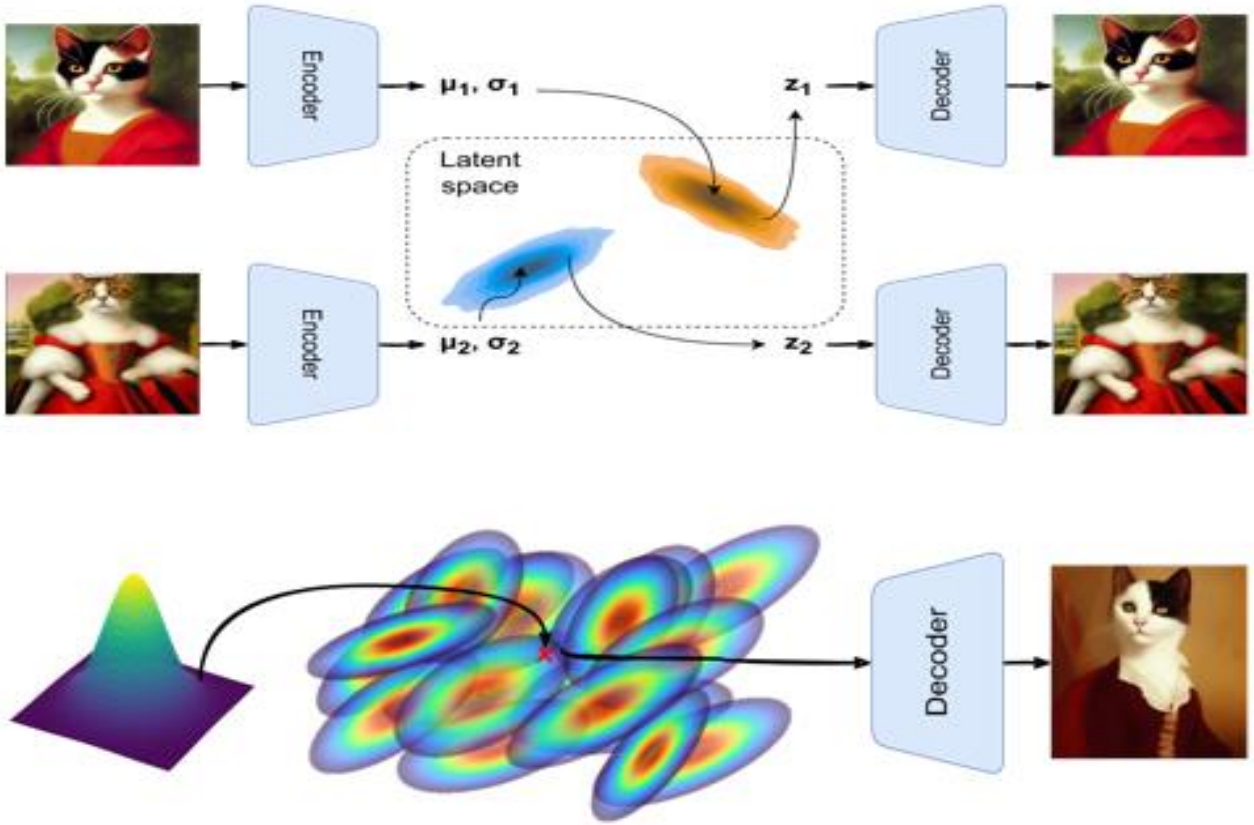
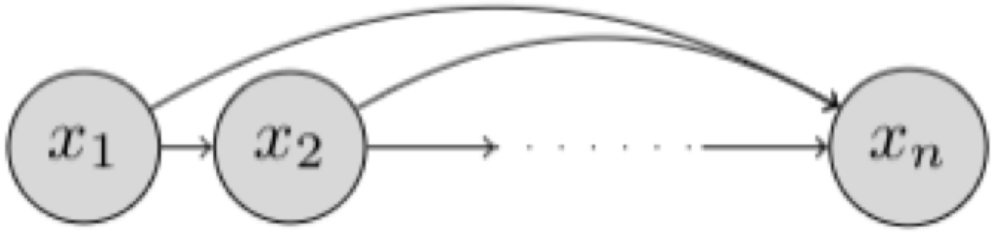


Image Source Credits: https://synthesis.ai/2023/02/07/generative-ai-i-variational-autoencoders/

Autoregressive Models

- In an autoregressive model, future values of a variable are assumed to be a linear function of past values.
- Time series modelling, language modelling, image generation (PixelRNN, PixelCNN, WaveNet), sequence-to-sequence modelling.

$$X_t = c + \sum_{i=1}^{p} \phi_i X_{t-i} + \epsilon_t$$



X_t is the value at time t.

c is a constant.

ϕ_i are the coefficients of the model.

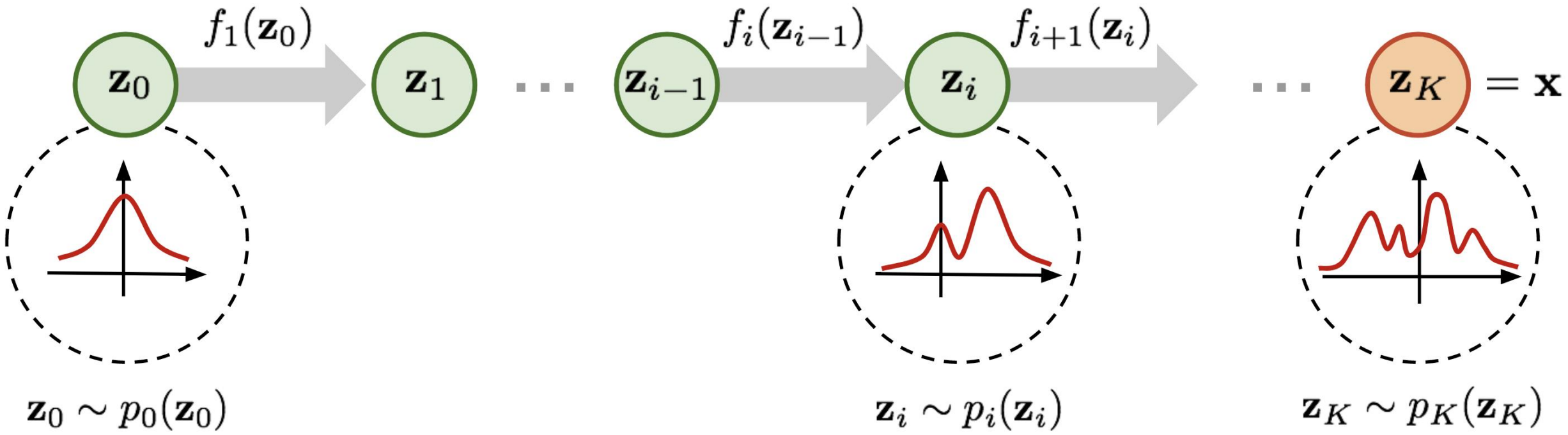
p is the order of the model (number of lagged terms).

ϵ_t is the error term (white noise).

Flow-based models

- Flow-based models use a series of bijective transformations (Normalizing Flow) to model complex data distributions.
- This means that for every input, there is a unique output and vice versa, allowing the model to easily switch between data space and latent space.
- Example flow-based models –
  - RealNVP (Real-valued Non-volume Preserving model) uses coupling layers to achieve invertibility. In each coupling layer, part of the input is transformed while the other part remains unchanged.
  - Glow (Generative Flow) uses a series of 1 x 1 convolutions to model data distributions.
  - MAF (Masked Autoregressive Flow) uses autoregressive models built using masked neural networks to do invertible transformations autoregressively.
- Applications: Image and speech generation, density estimation of HD data, anomaly detection

Normalizing Flow



Flowing through a chain of transformations, the variable is repeatedly substituted for the new one according to the change of variables theorem and eventually a probability distribution of the final target variable is obtained.

Source Credits: https://lilianweng.github.io/posts/2018-10-13-flow-models/

Diffusion Models

- Probabilistic generative models that model complex data distributions by using a diffusion process. These models progressively transform a simple distribution (like Gaussian noise) into the complex data distribution (data generation) through a series of steps.

- There is a forward and a reverse diffusion process both modeled as Markov chains.
  - **Forward diffusion process**
  - **Reverse diffusion process**

- Applications: Image generation, inpainting, super-resolution, text-to-image generation.

Forward Diffusion

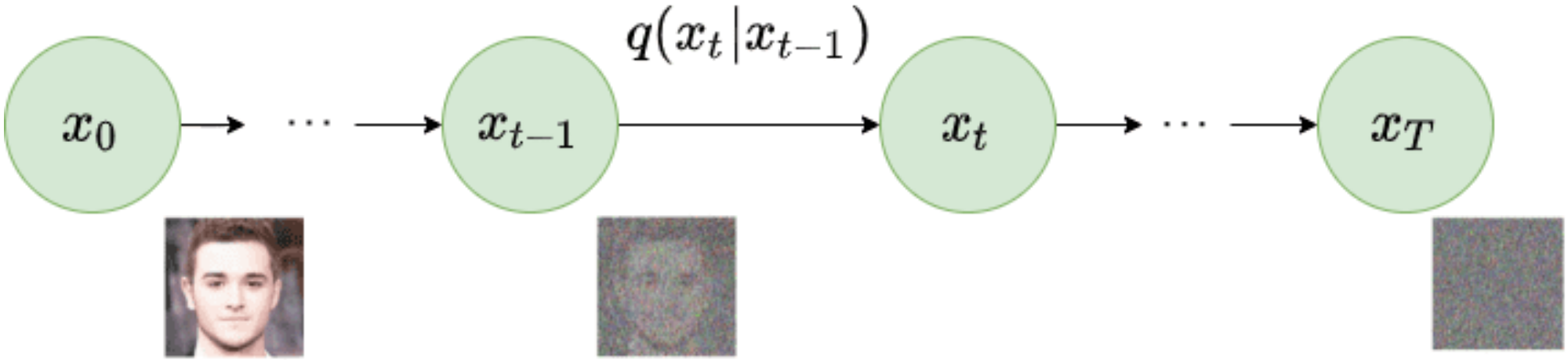


Image Source Credits: https://lilianweng.github.io/posts/2021-07-11-diffusion-models

Reverse Diffusion

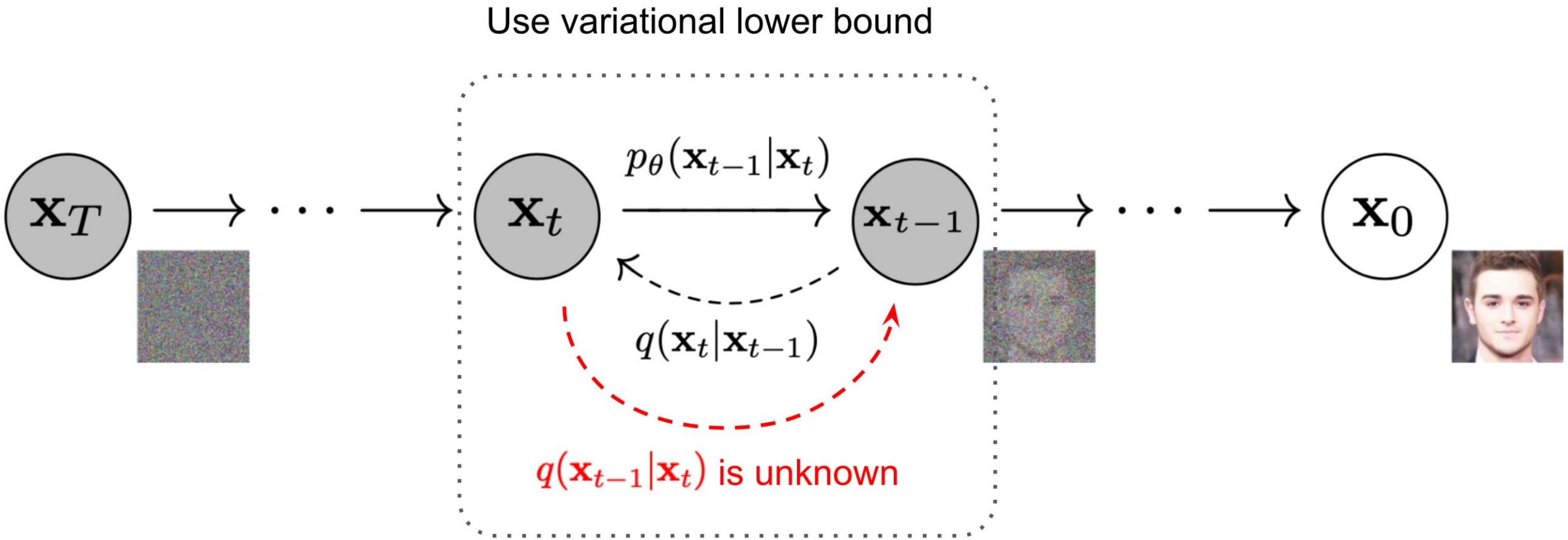


Image Source Credits: https://lilianweng.github.io/posts/2021-07-11-diffusion-models

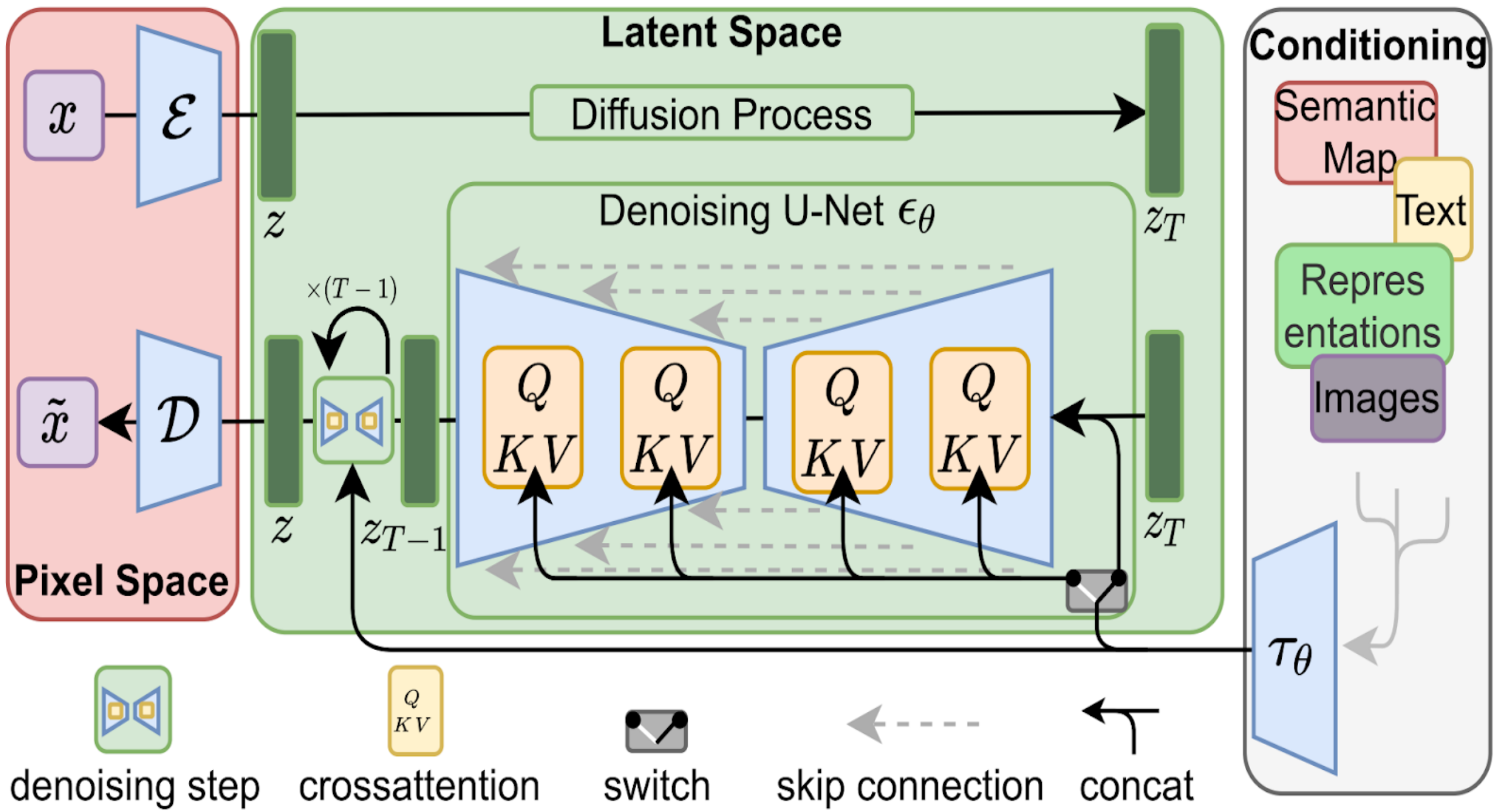


Image Source Credits: https://ommer-lab.com/research/latent-diffusion-models/

Large Multimodal Models

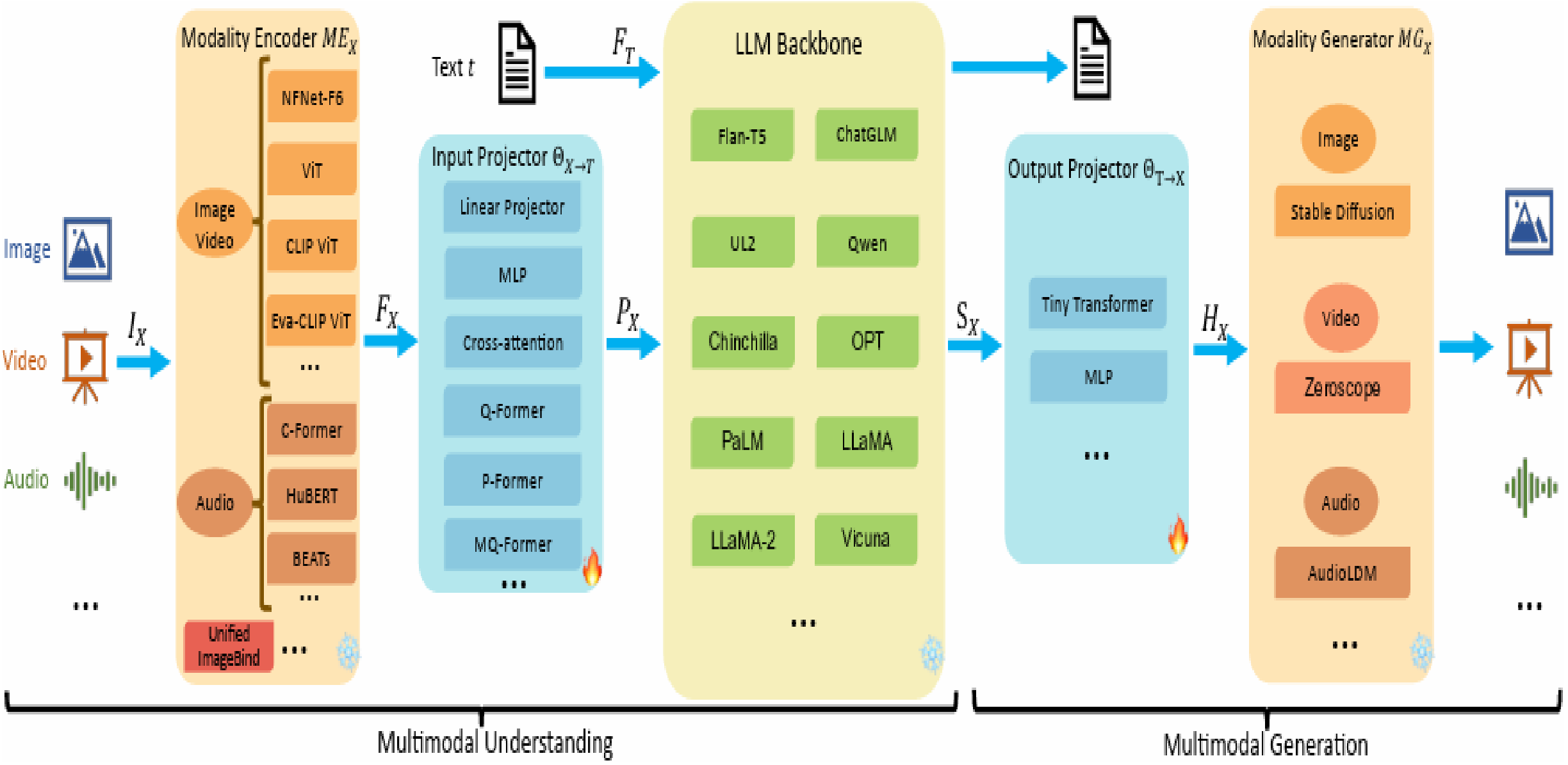
- Large multimodal models are AI models that can learn representations from different types of data “modalities”.

- When an LLM appears to work with multiple modalities, it uses an additional AI model to convert the other input into text.

- For example, before the launch of GPT-4o (a multimodal model), ChatGPT used GPT-3.5 and GPT-4 to power its text features, but it relied on Whisper to parse audio inputs and DALL·E 3 to generate images

- Multimodal models – GPT-4, Gemini.

General Architecture of Large Multimodal Models



General Architecture of MM LLMs Image Source Credits: https://blog.csdn.net/yalecaltech/article/details/136471559

Transformer Explainer

- https://poloclub.github.io/transformer-explainer/

Diffusion Explainer

https://poloclub.github.io/diffusion-explainer/

Autonomous AI Agents

Autonomous AI Agents

- AI systems that can operate independently without direct human intervention.

- Can perceive their environment (through sensors or data feeds), make decisions, reason about their goals, perform tasks (physical or digital actions) using tools, adapt to objectives.

LLM acts as the brain of the agent

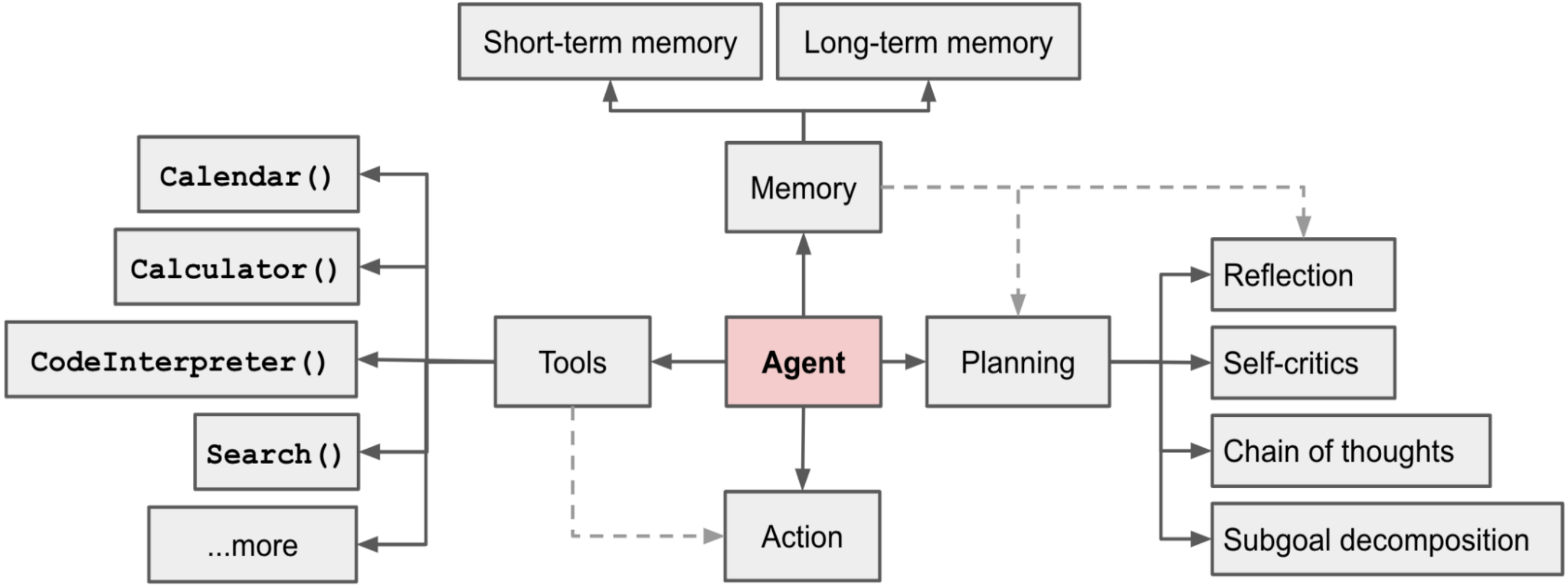


Image Source Credits: https://lilianweng.github.io/posts/2023-06-23-agent/

Use Cases

In Software Development

Applications in Software Development

- As coding assistants or copilots to help you generate complete boiler plate code or code snippets in multiple programming languages.
- Automating code refactoring.
- Creating design prototypes based on user requirements and preferences.

Applications in Software Quality Assurance

- Generating test cases, including both expected and edge cases to improve test coverage.

- Identifying complex software issues, unexpected bugs and vulnerabilities by analysis of code, logs, and execution traces.

Use Cases

In Cyber Security

Gen AI for Cyber Security

- In security operations centers (SOCs) and security event and incident management (SEIM) for **threat mitigation or prevention**.
- **Anomaly detection** in SIEM systems.
- **Simulation of advanced attack scenarios** for testing and enhancing security systems.
- **Automation of routine tasks** to streamline the implementation of security protocols.
- **Generating training content** for IT security professionals.

https://www.paloaltonetworks.com/cyberpedia/generative-ai-in-cybersecurity#:~:text=Generative%20AI%20can%20analyze%20individuals,to%20launch%20more%20targeted%20attacks.&text=Generative%20AI%20can%20automate%20certain,difficult%20to%20detect%20and%20counter.

- **Data Masking and Privacy Preservation –** With synthetic data generated using Gen AI models, need for collecting real, often sensitive and personal information, is reduced.

- **Automated security policy generation** based on specific needs of an organization.

- **Incident Response –** Gen AI can generate incident response actions based on severity and recommending mitigation strategies.

- **Reporting –** Generation of comprehensive reports.

Use Cases

In Graphic Design

Gen AI models help improve graphic design

- Generation of multiple **design options for inspiration.**

- Automation of mundane tasks like layout generation, suggesting color schemes.

Use Cases

In Creative Writing

Gen AI in Creative Writing

- AI writing assistants.
- Getting grammar and style corrections.
- Plain-English explanations and text summaries.
- Multilanguage content with translations for better accessibility.
- Generating writing prompts
- Producing unique story ideas and plotlines
- Structuring your story and fleshing out your characters.
- Building the world in which your story takes place.
- Generating catchy titles or names
- Drafting whole narratives.

https://www.forbes.com/sites/bernardmarr/2024/01/24/13-ways-writers-should-embrace-generative-ai/

Use Cases

In Media and Entertainment

Gen AI in Media and Entertainment

- Gen AI has impacted the **complete value chain** from the **content creation, to content management and engagement.**
- Has enabled a whole new paradigm of monetization opportunities.
- The EY survey** points to the top three applications of Gen AI :
  - Content Development (92%)
  - Product Development/Design (69%)
  - Customer Engagement (65%).

**https://www.ey.com/en_in/services/ai/generative-ai-india-report/industries-in-transformation/media-entertainment

EY survey forecasts extensive use of Gen AI for

- **Content Processing:** EY research forecasts Gen AI to drive over 10% revenue growth and a 15% efficiency increase, adding INR450 billion in value soon.

- Key opportunities for India include becoming a **content processing hub** and offering services for content compliance, addressing the challenges of global OTT platforms potentially generating a US$15-20 billion impact

- **Content compliance:** Building a services layer on top of all content produced globally, in content creation and moderation, scheduling and distribution, and monetization.
- Dubbing, subtitling, multi-language search and content discovery, multilinguistic recommendation engines etc.

Benefits of Gen AI to Media and Entertainment Companies

- Improve content monetization by making it **multilingual**.
- Enabling a deeper audience engagement with **personalized media experiences.**
- Personalized advertisements and real time incremental inventory
- Content production efficiency with **first cut of content coming from generative AI models**, the costs can come down by 20 to 25%.
- **Moderated user generated content** to make it comply with the platform or country guidelines.

**https://www.ey.com/en_in/services/ai/generative-ai-india-report/industries-in-transformation/media-entertainment

Use Cases

In Legal and Judicial Systems

Legal Document Review

- Document review: Examining and analyzing large volumes of documents as part of legal proceedings or investigations.

Legal Research

- Finding pertinent information and precedents for a specific legal issue or case.

- Researching statutes, regulations, case law, legal opinions, and scholarly articles.

- Contract Analysis: Comprehensive examination and evaluation to extract critical information, identify **crucial clauses**, assess **potential risks**, and **ensure compliance** with legal standards.

Prediction of legal outcomes

- Legal proceedings determine outcomes by applying laws to specific cases.

- Predicting legal outcomes manually is challenging due to the complexity of legal cases, the volume of legal data, subjectivity, limited historical data analysis, time constraints, risk of bias, and inability to consider all factors.

Use Cases

In Scientific Research

2024-8-16

The AI Scientist: Towards Fully Automated Open-Ended Scientific Discovery

Chris Lu[1,2,*], **Cong Lu**[3,4,*], **Robert Tjarko Lange**[1,*], **Jakob Foerster**[2,†], **Jeff Clune**[3,4,5,†] **and David Ha**[1,†]
[*]Equal Contribution, [1]Sakana AI, [2]FLAIR, University of Oxford, [3]University of British Columbia, [4]Vector Institute, [5]Canada CIFAR AI Chair, [†]Equal Advising

One of the grand challenges of artificial general intelligence is developing agents capable of conducting scientific research and discovering new knowledge. While frontier models have already been used as aides to human scientists, e.g. for brainstorming ideas, writing code, or prediction tasks, they still conduct only a small part of the scientific process. This paper presents the first comprehensive framework for fully *automatic scientific discovery*, enabling frontier large language models (LLMs) to perform research independently and communicate their findings. We introduce THE AI SCIENTIST, which generates novel research ideas, writes code, executes experiments, visualizes results, describes its findings by writing a full scientific paper, and then runs a simulated review process for evaluation. In principle, this process can be repeated to iteratively develop ideas in an open-ended fashion and add them to a growing archive of knowledge, acting like the human scientific community. We demonstrate the versatility of this approach by applying it to three distinct subfields of machine learning: diffusion modeling, transformer-based language modeling, and learning dynamics. Each idea is implemented and developed into a full paper at a meager cost of less than $15 per paper, illustrating the potential for our framework to democratize research and significantly accelerate scientific progress. To evaluate the generated papers, we design and validate an automated reviewer, which we show achieves near-human performance in evaluating paper scores. THE AI SCIENTIST can produce papers that exceed the acceptance threshold at a top machine learning conference as judged by our automated reviewer. This approach signifies the beginning of a new era in scientific discovery in machine learning: bringing the transformative benefits of AI agents to the *entire* research process of AI itself, and taking us closer to a world where *endless affordable creativity and innovation* can be unleashed on the world's most challenging problems. Our code is open-sourced at https://github.com/SakanaAI/AI-Scientist.

1. Introduction

The modern scientific method (Chalmers, 2013; Dewey, 1910; Jevons, 1877) is arguably one of the greatest achievements of the Enlightenment. Traditionally, a human researcher collects background knowledge, drafts a set of plausible hypotheses to test, constructs an evaluation procedure, collects evidence for the different hypotheses, and finally assesses and communicates their findings. Afterward, the resulting manuscript undergoes peer review and subsequent iterations of refinement. This procedure has led to countless breakthroughs in science and technology, improving human quality of life. However, this iterative process is inherently limited by human researchers' ingenuity, background knowledge, and finite time. In the field of AI, researchers have envisioned the possibility of

Automatic scientific discovery and research by Foundational Models.

- The paper proposes a fully AI-driven end-to-end pipeline for automated machine learning research including following steps:

  - Generation of novel research ideas
  - Writing code to experiment or implement the ideas.
  - Summarizing experimental results
  - Visualization of experimental results
  - Generating scientific manuscript using LaTeX to report the entire process.
  - Peer review generated manuscript with near human accuracy
  - Generate peer review feedback reports
  - Repeat above steps to improve the results, develop better ideas in an open-ended fashion.
  - Add the generated and evaluated ideas with good results to growing archive of knowledge, thus imitating the human scientific community.

Source: https://www.arxiv.org/pdf/2408.06292

Ethical Considerations

Ethical Consideration

- Deepfakes and Misinformation:
  - The potential for misuse in spreading false information.
- Bias in Generative Models:
  - Risks of amplifying biases in training data.
- Regulatory Challenges:
  - The need for policies to manage AI-generated content.
- Data Privacy and Security

Future Trends

- Improving model robustness, interpretability.
- Explainable, more controllable generation aligned with human values
- Multimodal generative models.
- Applications for Good (in healthcare, education, and art).

Thank You

www.linkedin.com/in/nimritakoul