**Problems with LLMS**

* No sources for answer
* Out dated

**How to deal with this problem**

We add a content store so LLM first goes to content store and finds the answers from our data store instead of giving its own answer

In normal cases, User prompts the model with its query and LLM gives answer. But when RAG is used generative model has an instruction to go and retrieve the relevant information combine it with user query and only then give the answer

**Sol to first problem**

* So now we have, Instruction to pay attention to, retrieved content with users question and now the model gives a response and give evidence for the answer which deals with our first challenge of no source

**Sol to second problem**

* Augmenting the data store with latest info helps us deal with the second problem

If the user question can not be answered reliably it should be able to tell that to user that **“I don’t know the answer”**

If the retriever is not efficient, it will not be able to give ans to user query which is answerable. The retriever should be accurate enough to give the correct info to LLM so it can answer the user’s query. Generator should be efficient too to give the richest answer

 **Retriever:**

* **Purpose:** The retriever's role is to fetch relevant documents or pieces of information from a large corpus based on the input query.
* **Common Models:** Dense Passage Retriever (DPR) is often used. DPR is trained to encode queries and documents into a shared embedding space where similar queries and documents are close together.
* **Mechanism:** The retriever uses similarity search (e.g., dot product similarity) to find the most relevant documents from the corpus.

 **Generator:**

* **Purpose:** The generator creates the final response or output, leveraging the retrieved documents to produce more informed and contextually relevant text.
* **Common Models:** Generative Pre-trained Transformer (GPT), BART, or T5 models are typically used.
* **Mechanism:** The generator takes the input query and the retrieved documents as inputs and generates a coherent and contextually enriched response.

**How RAG Works**

1. **Query Encoding:**
   * The input query is encoded into an embedding vector using the retriever model.
2. **Document Retrieval:**
   * The encoded query is used to retrieve the top-k relevant documents from a pre-indexed corpus. This is done using similarity search in the embedding space.
3. **Response Generation:**
   * The input query and the retrieved documents are passed to the generator model.
   * The generator combines the information from these documents to produce a final response that is both contextually relevant and informative

**Training RAG**

* **Retriever Training:**
  + The retriever is typically trained using a contrastive learning approach where positive (relevant) and negative (irrelevant) document pairs are used to teach the model to distinguish relevant documents.
* **Generator Training:**
  + The generator is fine-tuned on a dataset where the inputs are queries paired with relevant documents, and the outputs are the desired responses. The retriever and generator can be trained jointly or separately.

**Vector DBs**

Vector databases are specialized data storage and retrieval systems designed to handle and efficiently search high-dimensional vector data. They are commonly used in applications like similarity search, recommendation systems, and machine learning model retrieval tasks

**Characteristics of vector databases** - storing data as numerical vectors, scalability for large language models, and use of embeddings for data grouping.

* **Vector Storage**: Vector databases are designed to efficiently store and manage high-dimensional vectors representing complex data types such as images, text, and audio.
* **Vector Indexing:** These databases support indexing techniques optimized for vector data, enabling fast similarity searches and nearest neighbour queries.
* **Scalability:** Vector databases can scale horizontally to handle large volumes of vector data, making them suitable for applications with massive datasets.
* **Query Performance:** They are optimized for vector operations like similarity calculations, allowing for fast and efficient querying of complex data.

**Use cases of vector databases in AI** –

* semantic search
* similarity search
* chatbots utilizing natural language processing, image
* video recognition
* recommendation engines.

**Example of Vector DBs:**

1. **FAISS (Facebook AI Similarity Search)**

Features:

• Efficient similarity search and clustering of dense vectors.

• Supports large-scale datasets with billions of vectors.

• Various indexing methods (e.g., Flat, IVFFlat, IVFPQ, HNSW).

• GPU acceleration for faster computations.

Use Cases:

• Large-scale nearest neighbor search.

• Image and text similarity search.

• Recommender systems

1. **Pinecone**

Features:

• Managed vector database service.

• Scalable and low-latency vector search.

• Integration with machine learning frameworks and data pipelines.

• Real-time updates and querying.

Use Cases:

• Product recommendations.

• Semantic search.

• Personalized content delivery.

1. **Qdrant**

Features:

• High-performance, open-source vector database.

• Supports hybrid queries combining vector and metadata filtering.

• Real-time vector indexing and search.

• Provides a RESTful API for easy integration.

Use Cases:

• Real-time recommendation systems.

• Image and text similarity search.

• Anomaly detection in time-series data

1. **Chroma**

Features:

* Open-source vector database optimized for embedding and retrieval.
* Supports hybrid search combining vector and attribute-based filtering.
* Simple and intuitive API for developers.
* Designed to integrate seamlessly with machine learning workflows.

Use Cases:

* Embedding-based search for ML applications.
* Content-based recommendation systems.
* Semantic search in documents and multimedia

1. **Reels:**

Features:

• Designed for time-series and high-dimensional data.

• Real-time indexing and querying capabilities.

• Efficient storage and retrieval of high-dimensional vectors.

• Integration with streaming data sources.

Use Cases:

• Real-time analytics on time-series data.

• Anomaly detection in streaming data.

• Predictive maintenance and monitoring.

1. **Weaviate**

Features:

• Open-source vector search engine.

• Supports context-aware semantic search.

• GraphQL API for flexible querying.

• Extensible with custom modules.

Use Cases:

• Knowledge graph integration.

• Contextual search.

• Machine learning model deployment.

1. **Vespa:**

Features:

* Open-source engine for large-scale data serving and processing.
* Combines full-text search with vector search.
* Real-time indexing and searching.
* Supports complex ranking functions.

Use Cases:

* E-commerce product search.
* Personalized content recommendations.
* Real-time data processing.

**Effect of Dimension Size**

**Benefits of Increasing Dimensions:**

1. **Increased Representation Power**:
   * **Benefit**: Higher-dimensional embeddings can capture more nuanced relationships and semantic information between data points. This can lead to improved accuracy in tasks like similarity search, recommendation systems, and natural language processing.
   * **Example**: In natural language processing, higher-dimensional word embeddings (e.g., GloVe, Word2Vec with 300+ dimensions) can encode richer semantic and syntactic information compared to lower-dimensional embeddings.
2. **Reduced Information Loss**:
   * **Benefit**: Higher-dimensional embeddings preserve more information about the original data points. This can be crucial in applications where fine-grained details are important, such as image and video retrieval.
   * **Example**: In image processing, higher-dimensional feature vectors can capture detailed visual characteristics, leading to better matching and retrieval of similar images.
3. **Better Differentiation**:
   * **Benefit**: Increasing dimensions can help distinguish between similar items or entities that have subtle differences. This is advantageous in applications requiring precise classification or clustering.
   * **Example**: In fraud detection, higher-dimensional embeddings can differentiate between legitimate and fraudulent transactions more accurately by capturing subtle patterns.
4. **Future-Proofing**:
   * **Benefit**: Larger dimensions provide more flexibility and future-proofing against evolving data and model requirements. They can accommodate new features or dimensions without needing significant re-engineering.
   * **Example**: In machine learning models, higher-dimensional embeddings can adapt to new types of input data or additional features without compromising performance.

**Considerations and Potential Losses:**

1. **Increased Storage Requirements**:
   * **Consideration**: Higher-dimensional embeddings consume more storage space, which can become significant when dealing with large-scale datasets.
   * **Trade-off**: Balancing storage costs with performance requirements is essential, as storing and retrieving larger embeddings may require more computational resources.
2. **Computational Complexity**:
   * **Consideration**: Operations involving higher-dimensional embeddings, such as similarity search or clustering, may incur higher computational costs.
   * **Trade-off**: Optimizing algorithms and leveraging hardware acceleration (e.g., GPUs) can mitigate these costs, but it adds complexity to system design and maintenance.
3. **Dimensionality Curse**:
   * **Consideration**: As dimensions increase, the curse of dimensionality can lead to sparsity issues and increased computational inefficiency in high-dimensional spaces.
   * **Trade-off**: Techniques like dimensionality reduction (e.g., PCA, t-SNE) can help mitigate this by reducing the effective dimensions while preserving important information.
4. **Overfitting Risk**:
   * **Consideration**: In machine learning applications, higher-dimensional embeddings can increase the risk of overfitting if not properly regularized or validated.
   * **Trade-off**: Regularization techniques and cross-validation help mitigate overfitting risks by ensuring embeddings generalize well to unseen data.

**Creating Embeddings**

Embeddings are generated using various techniques, depending on the type of data. Here are some common methods:

**Text Embeddings**:

**Word Embedding**

* **Word2Vec**: Transforms words into vectors based on their context within a corpus. Word2Vec is a popular model that learns distributed representations (embeddings) of words in a continuous vector space from large corpora of text. It uses either the Continuous Bag-of-Words (CBOW) or Skip-gram architecture to predict context words given a target word or vice versa. Word similarity, language modelling, recommendation systems.
* **GloVe** (Global Vectors for Word Representation): Captures the statistical information of word occurrences. GloVe is another widely used model for learning word embeddings. It leverages global word co-occurrence statistics to capture word semantics. It constructs an explicit word-context matrix and optimizes embeddings to preserve global semantic relationships. Word analogy tasks, document classification, sentiment analysis.

**Sentence Embedding**

* **BERT** (Bidirectional Encoder Representations from Transformers): Generates **contextualized embeddings** for words and sentences. BERT is a Transformer-based model trained on large amounts of text to generate contextualized word and sentence embeddings. It pre-trains a deep bidirectional representation by jointly conditioning on both left and right context in all layers. Natural language understanding tasks, question answering, sentiment analysis.
* **TF-IDF** (Term Frequency-Inverse Document Frequency): Converts documents into vectors by considering the frequency of words and their importance.
* **Doc2Vec:** Doc2Vec (or Paragraph Vector) extends Word2Vec to generate embeddings for entire documents or paragraph. It considers document context to learn distributed representations, incorporating document-level semantics. Document clustering, text classification, recommendation systems.

**Image Embeddings:**

* **Convolutional Neural Networks (CNNs**): Use deep learning models like ResNet or VGG to extract features from images and represent them as vectors.
* **Autoencoders:** Compress image data into a lower-dimensional vector space and then reconstruct it.

**Audio Embeddings:**

**Mel-Frequency Cepstral Coefficients (MFCCs):** Extract features from audio signals.

**Recurrent Neural Networks (RNNs):** Capture temporal dependencies in audio data.

**Graph Embeddings:**

**Node2Vec**: Transforms nodes in a graph into vectors based on their network structure.

**Graph Neural Networks (GNNs):** Capture the relationships and attributes of nodes and edges in a graph

**Processing of Data by different Models**

Different embedding models process sentences in various ways, each leveraging unique techniques to capture semantic meaning and relationships within text data.

Embedded values remain same for a word in word2vec, GloVe. But in case of BERT embedding of word changes depending on context

.

**1. Word2Vec**

* **Model Type**: Word2Vec is a shallow neural network model typically trained on large text corpora.
* **Processing Approach**:
  + **Word-Level Embeddings**: Word2Vec generates embeddings at the word level. Each word in the vocabulary is assigned a fixed-size vector representation.
  + **Contextual Information**: Embeddings are learned based on the local context of each word (i.e., the surrounding words within a specific window size).

**2. GloVe (Global Vectors for Word Representation)**

* **Model Type**: GloVe is based on matrix factorization techniques applied to word co-occurrence statistics.
* **Processing Approach**:
  + **Global Co-occurrence Statistics**: GloVe constructs a global word-word co-occurrence matrix from the entire corpus. Embeddings are then learned by factorizing this matrix.
  + **Distributional Semantics**: Embeddings capture semantic relationships based on the statistical distribution of words across the corpus.

**3. BERT (Bidirectional Encoder Representations from Transformers)**

* **Model Type**: BERT is a transformer-based model pre-trained on large-scale unlabeled text.
* **Processing Approach**:
  + **Token-Level Contextual Embeddings**: BERT generates contextual embeddings for each token in the input sequence. It considers bidirectional context (both left and right context) using self-attention mechanisms.
  + **Self-attention** enables the model to weigh the importance of each word in a sequence relative to every other word in the same sequence. This mechanism captures relationships and dependencies between words, allowing the model to build richer, context-aware representations.
  + **Masked Language Modeling (MLM)**: During pre-training, BERT predicts masked-out words in sentences to learn deep bidirectional representations.
  + **Next Sentence Prediction (NSP)**: BERT also predicts whether two sentences follow each other in the corpus to capture relationships between sentences.

**4. Doc2Vec (Paragraph Vector)**

* **Model Type**: Doc2Vec extends Word2Vec to generate embeddings for entire documents, paragraphs, or sentences.
* **Processing Approach**:
  + **Document-Level Embeddings**: Doc2Vec learns a fixed-size vector representation for the entire document. It uses a similar approach to Word2Vec, but with additional parameters to capture document-level semantics.
  + **Paragraph ID**: Doc2Vec introduces a paragraph ID vector during training to differentiate between different paragraphs or documents.

**Differences in Processing Sentences:**

* **Granularity**: Word2Vec and GloVe focus on word-level embeddings, capturing the meaning of individual words based on their local or global context.
* **Contextual Understanding**: BERT provides contextual embeddings at the token level, considering bidirectional context to capture nuanced meanings and relationships within sentences.
* **Document-Level Representation**: Doc2Vec generates embeddings for entire documents or paragraphs, providing a single vector representation that summarizes the semantic content of the entire text.

**Applications:**

* **Word2Vec and GloVe**: Often used for tasks like word similarity, clustering, and downstream NLP tasks where static word embeddings suffice.
* **BERT**: Effective for tasks requiring understanding of context and semantics, such as sentiment analysis, question answering, and natural language inference.
* **Doc2Vec**: Useful for tasks involving document classification, recommendation systems, and information retrieval where document-level semantics are critical.

**Similarity Search Space:**

Similarity search in vector space involves finding vectors in a dataset that are most similar to a given query vector. This process is widely used in various applications such as recommendation systems, information retrieval, and machine learning.

**Steps in Similarity Search**

1. **Data Representation**:
   * **Embedding**: Transform the data items (e.g., text, images, audio) into high-dimensional vectors using embedding techniques like Word2Vec, BERT for text, CNNs for images, or RNNs for audio.
2. **Indexing**:
   * **Index Structures**: Use data structures to organize the vectors for efficient retrieval. Common indexing methods include:
     + **KD-Trees**: Suitable for low-dimensional data.
     + **Ball Trees**: Efficient for higher-dimensional data.
     + **Locality-Sensitive Hashing (LSH)**: Works well for very high-dimensional data by hashing similar vectors into the same bucket.
     + **Inverted File Index (IVF)**: Partitions the vector space into clusters and indexes vectors within these clusters.
3. **Query Processing**:
   * **Query Embedding**: Convert the query item into its vector representation using the same embedding technique used for the dataset.
   * **Similarity Calculation**: Compute the similarity between the query vector and the dataset vectors using a similarity metric.
4. **Similarity Metrics**:
   * **Euclidean Distance**: Measures the straight-line distance between two vectors in Euclidean space.
   * **Cosine Similarity**: Measures the cosine of the angle between two vectors, useful for determining the orientation rather than magnitude. ​​
   * **Manhattan Distance**: Sum of the absolute differences of their coordinates.
5. **Nearest Neighbor Search**:
   * **Exact Nearest Neighbors**: Searches the entire dataset to find the most similar vectors, which can be computationally expensive for large datasets.
   * **Approximate Nearest Neighbors (ANN)**: Uses algorithms like FAISS (Facebook AI Similarity Search), Annoy (Approximate Nearest Neighbors Oh Yeah), or HNSW (Hierarchical Navigable Small World) to quickly find approximate solutions that are close enough to the exact neighbors.
6. **Result Retrieval**:
   * **Ranking**: The vectors are ranked based on their similarity scores, and the top-k most similar vectors are selected and returned.

**Example Workflow**

**Embedding Generation:**

Suppose we have a dataset of images. Each image is processed through a convolutional neural network (CNN) to generate a 512-dimensional vector embedding.

**Indexing:**

These embeddings are indexed using an indexing structure like IVF, which partitions the vector space into clusters.

**Query Processing:**

When a query image is received, it is processed through the same CNN to obtain its 512-dimensional vector embedding.

**Similarity Calculation:**

The query vector is compared with the indexed vectors using cosine similarity.

**Nearest Neighbor Search:**

Using an ANN algorithm, the database quickly identifies the top-10 vectors that are most similar to the query vector.

**Result Retrieval:**

The most similar images are retrieved and presented to the user.

**Context Window and Window Size**

In the context of natural language processing (NLP) and machine learning, "context window" and "window size" are terms used to describe the span of tokens (words, subwords, or characters) that are considered when processing text. These concepts are essential in various NLP tasks, such as language modelling, word embeddings, and sequence-to-sequence models.

**Context Window**

1. A context window refers to the segment of text around a target word (or token) that is considered to understand or predict the target. This segment provides the contextual information necessary for the model to perform its task.
2. It limits how much of the recent conversation history the model can consider when generating a response
3. context window ensures the model can maintain context over short-to-medium length exchanges but doesn't inherently provide long-term memory across extended interactions.

 **Context Window Use**:

* For immediate responses, the model uses the conversation history up to the context window size to generate coherent replies.

 **Long-Term Memory Use**:

* For retaining information over multiple sessions, the chatbot could store user data in a database and fetch this information when the user interacts with the chatbot again, even if the previous interaction's context is no longer within the context window

**Applications:**

**Word Embeddings (e.g., Word2Vec):**

* In Word2Vec, the context window is used to predict a word based on its neighbouring words (Skip-gram model) or to predict the neighbouring words based on the word (CBOW model).

**Language Models (e.g., GPT, BERT):**

* Transformer-based models like GPT consider a context window of preceding tokens to predict the next token.
* BERT considers a bidirectional context window, looking at both preceding and following tokens to understand the context for masked language modeling.

**Sequence-to-Sequence Models:**

* In models like RNNs, LSTMs, and GRUs, the context window can span the entire sequence, but practical implementations often limit it due to computational constraints.

**Window Size**

The window size is the number of tokens that the context window spans. It determines how many tokens before and after the target word are included in the context window.

**Examples:**

**Word2Vec:**

* If the window size is 2, the context window for the word "fox" in the sentence "The quick brown fox jumps over the lazy dog" includes "quick", "brown", "jumps", and "over".

**Transformer Models:**

* Transformer models often process text in fixed-size chunks. The window size in this case refers to the maximum length of tokens considered in a single forward pass.
* For instance, GPT-3 has a context window size of 2048 tokens, meaning it can consider up to 2048 tokens when generating text.

**Text Processing:**

* In text processing, such as in moving average calculations over a sequence, the window size determines the number of adjacent elements considered for each computation.

**Importance of Context Window and Window Size**

**Capturing Relevant Information:**

* The choice of window size impacts how much context is available for understanding the target word or token. A larger window size captures more context, which can be beneficial for understanding complex dependencies but also increases computational complexity.

**Balancing Performance and Computation:**

* There is a trade-off between performance and computational efficiency. Larger window sizes can improve performance but require more memory and processing power.

**Handling Long-Range Dependencies:**

* Models like Transformers handle long-range dependencies better due to their ability to consider long context windows. Traditional models like RNNs struggle with long dependencies unless techniques like attention mechanisms are used.

**Practical Considerations**

**Choosing the Right Window Size:**

* The optimal window size depends on the specific application and dataset. For instance, short window sizes may suffice for tasks with local dependencies, while tasks requiring understanding of broader context benefit from larger window sizes.

**Memory and Computation Limits:**

* For large window sizes, especially in Transformer models, memory and computation become bottlenecks. Techniques like gradient checkpointing, sparse attention, and model parallelism can help mitigate these issues.

**Dynamic vs. Fixed Window Sizes:**

* Some models use fixed window sizes, while others adapt the window size dynamically based on the input. Dynamic window sizes can be more efficient but add complexity to the model.

**Similarity Metrics**

**1. Cosine Similarity**

Cosine similarity measures the similarity between two phrases based on the angle between their word vectors. When phrases are identical, similarity is 1; when no words overlap, similarity is 0; partial overlap results in a similarity between 0 and 1.

Make a table for word counts, plot the points, find the angle, and similarity

For more than 2 words similarity, we use formula

**Useful For:**

* **Text Analysis and NLP**: Comparing text documents, word embeddings, and sentence embeddings.
* **Document Retrieval**: Finding similar documents or information retrieval.
* **High-Dimensional Data**: When the magnitude of the vectors is less important than their direction.

**Conditions:**

* When you need to measure the angle between vectors.
* When vector magnitude should not affect the similarity score.
* When dealing with sparse data (e.g., text data in a bag-of-words model).

**2. Euclidean Distance**

**Useful For:**

* **Clustering**: Algorithms like k-means clustering.
* **Image Processing**: Comparing image features.
* **Low-Dimensional Data**: When the data is not very high-dimensional.

**Conditions:**

* When the actual distance between points is meaningful.
* When the data is continuous and differences in magnitude are important.
* When the data dimensionality is not too high (curse of dimensionality).

**3. Manhattan Distance (L1 Distance)**

**Useful For:**

* **Sparse Data**: Data with many zero values.
* **Grid-Based Problems**: Pathfinding algorithms like A\* in grid environments.
* **Robustness to Outliers**: Less sensitive to outliers compared to Euclidean distance.

**Conditions:**

* When dealing with high-dimensional data where individual differences are meaningful.
* When the data is sparse and differences should be aggregated in a linear fashion.
* When robustness to outliers is required.

**4. Jaccard Similarity**

**Useful For:**

* **Binary Data**: Comparing binary vectors.
* **Set Comparisons**: Comparing sets of elements, such as user preferences or hashtags.
* **Text Clustering**: Comparing documents represented as sets of words.

**Conditions:**

* When the data can be represented as sets (e.g., presence or absence of features).
* When you need to measure the overlap between sets.
* When dealing with categorical data.

**5. Pearson Correlation Coefficient**

**Useful For:**

* **Statistics and Data Analysis**: Measuring the linear relationship between variables.
* **Recommender Systems**: Collaborative filtering to find similar users or items.
* **Financial Analysis**: Analyzing the relationship between stock prices or economic indicators.

**Conditions:**

* When the relationship between variables is linear.
* When you need to measure correlation, not similarity.
* When the data is continuous and normally distributed.

**6. Hamming Distance**

**Useful For:**

* **Error Detection and Correction**: Coding theory and data transmission.
* **Binary Data**: Comparing binary strings or bit vectors.
* **DNA Sequencing**: Comparing sequences of nucleotides.

**Conditions:**

* When the data is binary or categorical.
* When measuring the exact number of differing positions.
* When dealing with fixed-length strings or sequences.

**7. KL Divergence (Kullback-Leibler Divergence)**

**Useful For:**

* **Probability Distributions**: Comparing probability distributions.
* **Machine Learning**: Training generative models like VAEs (Variational Autoencoders).
* **Information Theory**: Measuring the divergence between two distributions.

**Conditions:**

* When comparing probability distributions.
* When the distributions are discrete or continuous.
* When you need to measure the information loss between distributions.

**Key Components of Transformers**

1. **Self-Attention Mechanism**:
   * **Core Innovation**: Transformers rely heavily on self-attention mechanisms, which allow them to weigh the importance of each word/token in a sequence relative to every other word/token. This enables them to capture relationships and dependencies between words efficiently.
2. **Multi-Head Attention**:
   * **Parallel Processing**: Transformers use multiple attention heads in each layer to capture different types of relationships in parallel. Each attention head computes attention scores independently and then concatenates their outputs, allowing the model to focus on different aspects of the input simultaneously.
3. **Positional Encoding**:
   * **Capturing Sequence Order**: Since transformers do not inherently understand the order of words in a sequence like recurrent neural networks (RNNs) or convolutional neural networks (CNNs), positional encodings are added to the input embeddings. These encodings provide information about the position of each token in the sequence, enabling the model to account for sequential order.
4. **Feedforward Neural Networks**:
   * **Non-linear Transformations**: After self-attention layers, transformers use feedforward neural networks (FFNNs) to process the information captured by the attention mechanism. FFNNs consist of multiple layers of fully connected networks with activation functions like ReLU (Rectified Linear Unit).
5. **Layer Normalization**:
   * **Stabilizing Training**: Transformers use layer normalization to stabilize the learning process by normalizing the outputs of each layer and applying a scaling and shifting transformation.

**Transformer Architecture**

* **Encoder-Decoder Architecture**: Transformers are commonly used in a dual-architecture setup:
  + **Encoder**: Processes the input sequence and generates a contextualized representation for each token.
  + **Decoder**: Takes the encoder's outputs and generates the output sequence (e.g., in machine translation tasks).
* **Stacked Layers**: Transformers consist of multiple layers of encoders (and optionally decoders), each comprising self-attention mechanisms, FFNNs, and normalization layers. The number of layers can vary depending on the complexity of the task and the size of the dataset.

**Applications of Transformers**

* **NLP Tasks**: Transformers have been successfully applied to various NLP tasks, including:
  + Machine Translation (e.g., Google's Transformer model for translation).
  + Text Generation (e.g., OpenAI's GPT models).
  + Named Entity Recognition.
  + Sentiment Analysis.
  + Question Answering (e.g., BERT for QA tasks).

**Advantages of Transformers**

* **Parallelization**: Transformers can process tokens in parallel due to their attention mechanisms, making them faster than sequential models like RNNs.
* **Long-Range Dependencies**: They can capture relationships between tokens that are far apart in the input sequence, which is challenging for traditional sequential models.
* **Scalability**: Transformers can scale to large datasets and compute clusters, enabling training on extensive corpora with billions of tokens.

**Limitations**

* **Computational Resources**: Training large transformer models requires substantial computational resources (e.g., GPUs or TPUs).
* **Interpretability**: Despite their effectiveness, understanding how transformers arrive at specific predictions can be challenging due to their complex architectures.

**Tokenization:**

Tokenization is the process of breaking down text into smaller units called tokens. These tokens can be words, subwords, or characters, depending on the specific tokenization strategy used. Tokenization is a fundamental preprocessing step in natural language processing (NLP) and is crucial for converting text into a format that can be processed by machine learning models.

**Types of Tokenization**

1. **Word Tokenization**
   * **Definition**: Splitting text into individual words.
   * **Example**: The sentence "I love Pakistan" would be tokenized into ["I", "love", "Pakistan"].
   * **Use Cases**: Basic text processing tasks, where each word is treated as a distinct unit.
2. **Subword Tokenization**
   * **Definition**: Splitting words into smaller units called subwords or morphemes.
   * **Example**: The word "unhappiness" might be tokenized into ["un", "happiness"] or ["un", "happy", "ness"].
   * **Common Algorithms**:
     + **Byte Pair Encoding (BPE)**: Combines the most frequent pairs of bytes or characters iteratively.
     + **WordPiece: (freq of pair/ freq of first element\* freq of second)** Similar to BPE, used in models like BERT. If the word exist in vocabulary in **bert uncased it comes as it is otherwise it is divided and pairs are formed**
     + **SentencePiece**: A more flexible subword tokenizer used in models like T5 and GPT-3.
   * **Use Cases**: Handling out-of-vocabulary words and languages with rich morphology.
3. **Character Tokenization**
   * **Definition**: Splitting text into individual characters.
   * **Example**: The word "hello" would be tokenized into ["h", "e", "l", "l", "o"].
   * **Use Cases**: Low-level text analysis, certain sequence modeling tasks, and languages with complex character sets (e.g., Chinese).

**Tokenization in Different NLP Models**

* **Traditional NLP Models**:
  + Use simple tokenization techniques like word or character tokenization.
  + Tokenization methods include splitting by spaces or punctuation.
* **Modern NLP Models**:
  + **Word2Vec**: Uses word tokenization.
  + **GloVe**: Uses word tokenization.
  + **FastText**: Uses word tokenization but also includes subword information.
  + **BERT**: Uses WordPiece tokenization.
  + **GPT**: Uses Byte Pair Encoding (BPE) tokenization.
  + **T5**: Uses SentencePiece tokenization.

**Steps in Tokenization**

1. **Text Normalization**:
   * Converting text to a consistent format (e.g., lowercasing, removing punctuation).
   * Handling contractions (e.g., "don't" to "do not").
2. **Token Splitting**:
   * Splitting text into tokens based on spaces, punctuation, or specific algorithms for subword tokenization.
3. **Token Mapping**:
   * Mapping tokens to numerical values (token IDs) using a vocabulary.
   * This step converts text into a sequence of integers that models can process.
   * Each token ID corresponds to a unique embedding vector in an embedding matrix. These embeddings capture semantic relationships between tokens based on their context in the training data. Embeddings enable the model to understand similarities, differences, and associations between different words or subword units.

**Example**

Consider the sentence "I love Pakistan":

* **Word Tokenization**:
  + Tokens: ["I", "love", "Pakistan"]
  + Token IDs (assuming a simple vocabulary): [1, 2, 3]
* **Subword Tokenization (BERT)**:
  + Tokens: ["I", "love", "Pak", "##istan"]
  + Token IDs (assuming a BERT vocabulary): [101, 102, 103, 104]
  + ## use because istan is continuation wo word Pak

**Challenges in Tokenization**

1. **Ambiguity**:
   * Words with multiple meanings (e.g., "bank" as a financial institution or riverbank).
   * Contextual usage can influence the meaning and tokenization.
2. **Out-of-Vocabulary Words**:
   * Words not present in the model's vocabulary need to be handled (e.g., via subword tokenization).
3. **Language-Specific Issues**:
   * Different languages have different tokenization challenges (e.g., compound words in German, lack of spaces in Chinese).

**Benefits of Tokenization**

* **Preprocessing**: Converts raw text into a structured format for models.
* **Vocabulary Building**: Helps in creating a manageable vocabulary for language models.
* **Feature Extraction**: Enables extraction of meaningful features from text for analysis and modeling.

**WordPiece and Byte Pair Encoding (BPE)** are both subword tokenization methods used to handle out-of-vocabulary words and manage vocabulary size in natural language processing tasks. While they share some similarities, they have distinct differences in how they operate and their specific implementations. Here's a comparison between the two:

**Byte Pair Encoding (BPE)**

**Overview**:

* BPE iteratively merges the most frequent pairs of characters or subwords in a corpus to create a fixed-size vocabulary of subwords.
* Originally developed for data compression, but adapted for NLP tasks.

**Process**:

1. **Initialization**: Start with all individual characters as the initial vocabulary.
2. **Frequency Calculation**: Count the frequencies of all pairs of adjacent symbols (characters or subwords).
3. **Pair Merging**: Find the most frequent pair and merge it into a new subword.
4. **Update Vocabulary**: Add the new subword to the vocabulary.
5. **Repeat**: Continue the process until reaching the desired vocabulary size.

**Example**:

* Corpus: "lower", "lowest"
* Initial tokens: l o w e r, l o w e s t
* Merging steps:
  1. Merge "l o" → "lo": lo w e r, lo w e s t
  2. Merge "lo w" → "low": low e r, low e s t
  3. Continue until the desired vocabulary size.

**WordPiece**

**Overview**:

* WordPiece, used in models like BERT, also iteratively merges characters or subwords based on their frequency, but it uses a more sophisticated approach to determining which pairs to merge.

**Process**:

1. **Initialization**: Start with a basic vocabulary containing all individual characters and some common words.
2. **Frequency Calculation**: Calculate the likelihood of pairs of subwords.
3. **Pair Merging**: Instead of simply merging the most frequent pairs, WordPiece takes into account the probability of subwords given the context, aiming to maximize the overall likelihood of the corpus.
4. **Update Vocabulary**: Add the new subword to the vocabulary.
5. **Repeat**: Continue the process until reaching the desired vocabulary size.

**Example**:

* Corpus: "unaffordable", "unfashionable"
* Initial tokens: u n a f f o r d a b l e, u n f a s h i o n a b l e
* Merging steps:
  1. Merge "un" → "un": un a f f o r d a b l e, un f a s h i o n a b l e
  2. Merge "aff" → "aff": un aff o r d a b l e, un f a s h i o n a b l e
  3. Continue until the desired vocabulary size.

**Key Differences**

1. **Merging Criteria**:
   * **BPE**: Merges the most frequent pairs of characters or subwords in the entire corpus.
   * **WordPiece**: Merges pairs based on the probability of subwords using **expectation maximization model** (algorithm helps in estimating the likelihood or probability of different subword units occurring together in the training corp), aiming to maximize the likelihood of the corpus, considering context more effectively. **EM considers both the frequency of occurrence and the contextual probability of subword sequences.**
2. **Use in Models**:
   * **BPE**: Used in models like GPT-2 and some earlier transformer models.
   * **WordPiece**: Used in BERT and related transformer models.
3. **Optimization**:
   * **BPE**: Focuses on frequency-based merging, which is simpler and faster to compute.
   * **WordPiece**: Incorporates likelihood and context, providing potentially better handling of subwords but with increased computational complexity.
4. **Handling Out-of-Vocabulary Words**:
   * Both methods break down rare or unknown words into known subwords, but WordPiece tends to be more context-sensitive.

**Summary**

* **Byte Pair Encoding (BPE)**:
  + Simpler and faster.
  + Frequency-based merging.
  + Used in models like GPT-2.
* **WordPiece**:
  + More sophisticated and context-aware.
  + Likelihood-based merging.
  + Used in models like BERT7

 **BPE**: Typically results in subword units that are frequent but may not always be semantically meaningful.

 **WordPiece**: Tends to produce subword units that are more semantically meaningful because of the probabilistic modeling that considers the likelihood of subword sequences within the data.

**Steps of the EM Algorithm**

1. **Expectation (E) Step**:
   * **Objective**: In this step, the algorithm calculates the expected value (expectation) of the latent variables(unobserved) given the observed data and the current estimates of model parameters.
   * **Calculations**: It computes the posterior probabilities of the latent variables given the observed data using the current parameter estimates.
2. **Maximization (M) Step**:
   * **Objective**: In this step, the algorithm updates the parameters of the model to maximize the likelihood function, based on the expected values obtained from the E-step.
   * **Calculations**: It computes new parameter estimates that maximize the likelihood function, typically using techniques like gradient ascent or iterative methods.

**Key Differences in Word and Token Embedding**

1. **Context Sensitivity**:
   * **Word Embeddings**: Static, context-independent.
   * **Token Embeddings**: Dynamic, context-dependent.
2. **Granularity**:
   * **Word Embeddings**: Typically represent whole words.
   * **Token Embeddings**: Can represent subwords or even characters, allowing finer granularity.
3. **Vocabulary Handling**:
   * **Word Embeddings**: Fixed vocabulary; struggles with out-of-vocabulary words.
   * **Token Embeddings**: Subword tokenization helps handle out-of-vocabulary words by breaking them down into known tokens.
4. **Pre-training and Fine-tuning**:
   * **Word Embeddings**: Often pre-trained separately and then used in downstream tasks.
   * **Token Embeddings**: Typically part of pre-trained models like BERT and are fine-tuned as part of these models for specific tasks.

**Advantages of Token Embeddings**

1. **Contextual Understanding**:
   * **Word Embeddings**: Provide a single, context-independent vector for each word. For example, the word "bank" has the same embedding whether it appears in "river bank" or "financial bank."
   * **Token Embeddings**: Generate embeddings that are context-sensitive. The same word can have different embeddings based on the surrounding words, allowing models to understand different meanings of words in different contexts.
2. **Handling Out-of-Vocabulary Words**:
   * **Word Embeddings**: Struggle with out-of-vocabulary (OOV) words, as these words do not have pre-trained embeddings.
   * **Token Embeddings**: Often use subword units (like WordPiece, Byte Pair Encoding, or SentencePiece), which break down rare or unknown words into smaller, known components. This approach helps in handling OOV words by constructing embeddings from these subword units.
3. **Finer Granularity**:
   * **Word Embeddings**: Treat each word as a single unit, which can be limiting for languages with rich morphology or for dealing with misspellings and compound words.
   * **Token Embeddings**: By operating at the subword level, token embeddings provide finer granularity, enabling better handling of prefixes, suffixes, and other morphological variations.
4. **Improved Performance in Downstream Tasks**:
   * **Word Embeddings**: Are useful but often require additional features or complex architectures to achieve high performance on specific tasks.
   * **Token Embeddings**: As part of pre-trained language models like BERT, they capture deep linguistic features and can be fine-tuned on specific tasks, leading to superior performance on a wide range of NLP tasks such as text classification, named entity recognition, and machine translation.
5. **Efficient Use of Vocabulary**:
   * **Word Embeddings**: Require a large vocabulary to cover all possible words, leading to significant memory usage and computational costs.
   * **Token Embeddings**: Subword tokenization allows for a more compact and efficient vocabulary. This compact vocabulary can handle a vast number of words with fewer base units, reducing memory and computational requirements.

**Example Scenarios**

1. **Polysemy and Homonymy**:
   * **Word Embeddings**: Cannot distinguish between different meanings of the same word.
   * **Token Embeddings**: Provide different vectors based on context, thus differentiating between multiple meanings of the same word.
2. **Compound Words and Variations**:
   * **Word Embeddings**: Need a separate vector for each compound word and variation.
   * **Token Embeddings**: Can break down compound words into meaningful subwords, efficiently representing variations.
3. **Language Morphology**:
   * **Word Embeddings**: May require extensive preprocessing to handle different forms of words.
   * **Token Embeddings**: Naturally handle different morphological forms through subword tokenization.

**In context of text generation, Token embedding is very powerful comparatively, in simpler tasks like text classification (sentiment analysis, spam detection), document classification, Resource limited environment, Fixed vocabulary we need Word Embedding**

o embed token IDs like the ones you've provided into dense vectors, typically in the context of neural networks and natural language processing tasks, we use embedding layers. Let's break down how this process works:

### Tokenization and Numerical Representation

1. **Tokenization**:
   * The original sentence "I love natural language processing gnissecorp gnissecorp" is tokenized into individual tokens. These tokens are then converted into their respective token IDs using a tokenizer.
   * **Example**: Tokens and corresponding token IDs:

Tokens: ['i', 'love', 'natural', 'language', 'processing', 'g', '##nis', '##se', '##corp', 'g', '##nis', '##se', '##corp']

Token IDs: [1045, 2293, 3019, 2653, 6364, 1043, 8977, 3366, 24586, 1043, 8977, 3366, 24586]

1. **Embedding Layer**:
   * In a neural network architecture designed for natural language processing tasks (like sentiment analysis, machine translation, etc.), an embedding layer is typically used as the first layer after tokenization.
   * **Initialization**: Initially, the embedding layer's parameters are randomly initialized. Each token ID is mapped to a dense vector (embedding vector) of a specified dimensionality (e.g., 100, 200, etc.).
   * **Learning**: During the training process, these embedding vectors are adjusted (learned) based on the task-specific objective (e.g., minimizing loss in sentiment prediction).

### Example of Embedding Process

Let's illustrate how embedding might work for the token IDs provided:

* Suppose we have an embedding layer with an embedding dimension of 4 for simplicity. This means each token ID will be mapped to a dense vector of size 4.
* Initially, the embedding layer might assign random vectors to each token ID:

Token ID 1045 (token: 'i') -> [0.1, -0.3, 0.2, 0.5]

Token ID 2293 (token: 'love') -> [-0.4, 0.1, -0.7, 0.3]

Token ID 3019 (token: 'natural') -> [0.6, -0.2, 0.9, -0.5]

Token ID 2653 (token: 'language') -> [0.8, 0.4, -0.1, 0.2]

Token ID 6364 (token: 'processing') -> [-0.3, 0.7, -0.4, 0.6]

Token ID 1043 (token: 'g') -> [0.2, -0.6, 0.3, -0.8]

Token ID 8977 (token: '##nis') -> [0.5, 0.2, -0.9, 0.1]

Token ID 3366 (token: '##se') -> [-0.7, 0.8, 0.4, -0.3]

Token ID 24586 (token: '##corp') -> [0.3, -0.5, 0.6, -0.4]

* During training, these vectors are updated through backpropagation and gradient descent, optimizing them to better represent relationships between tokens that are useful for the sentiment analysis task.

### Importance of Embedding

* **Semantic Relationships**: Embedding vectors capture semantic relationships between tokens based on their context in the training data.
* **Efficiency**: Dense embeddings are more efficient than sparse representations (like one-hot encoding) and allow the model to generalize better to unseen data.
* **Contextual Understanding**: Models can learn nuanced meanings of tokens by adjusting embeddings based on the task's objective function (e.g., maximizing sentiment prediction accuracy).

In summary, embedding token IDs involves mapping each token ID to a dense vector representation through an embedding layer in a neural network. These embeddings are learned during training to capture meaningful relationships between tokens, ultimately improving the model's performance on tasks like sentiment analysis.

**Example Sentence**: "I really liked the movie, it was fantastic!"

**Tokenization and Embedding**

1. **Tokenization**:
   * The sentence is tokenized into individual tokens. Let's assume the tokens are: ["I", "really", "liked", "the", "movie", ",", "it", "was", "fantastic", "!"]
2. **Token to ID Conversion**:
   * Each token is mapped to a numerical token ID based on a predefined vocabulary. For example:
     + "I" -> 100
     + "really" -> 200
     + "liked" -> 300
     + "the" -> 400
     + "movie" -> 500
     + "," -> 600
     + "it" -> 700
     + "was" -> 800
     + "fantastic" -> 900
     + "!" -> 1000
3. **Embedding Lookup**:
   * Each token ID is then embedded into a continuous vector space using an embedding matrix. For simplicity, let's assume each token is embedded into a 3-dimensional vector (this is just for illustration purposes; in practice, embedding dimensions are much larger):
     + "I" -> [0.1, 0.2, 0.3]
     + "really" -> [0.4, 0.5, 0.6]
     + "liked" -> [0.7, 0.8, 0.9]
     + ...
     + "!" -> [1.1, 1.2, 1.3]

**Updating Embedded Vectors**

During training, the embedded vectors of these tokens are updated through the following steps:

1. **Forward Pass**:
   * The embedded vectors of tokens "I", "really", "liked", "the", "movie", ",", "it", "was", "fantastic", "!" are fed into the model.
2. **Loss Calculation**:
   * The model computes a predicted sentiment score based on these embeddings.
   * Suppose the ground truth sentiment label for this sentence is positive.
3. **Backpropagation**:
   * **Gradient Calculation**: Gradients of the loss function (e.g., cross-entropy loss) with respect to all model parameters, including the embedding vectors, are computed.
   * **Embedding Gradients**: Specifically, gradients with respect to each token's embedding vector indicate how much each vector should be adjusted to minimize the prediction error.
4. **Parameter Update**:
   * **Learning Rate**: Determines the step size for updating the parameters.
   * **Update Rule**: Each embedding vector is adjusted according to its gradient and the learning rate:
     + Example update rule (simplified): new embedding vector=old embedding vector−η⋅∇embedding vectorL\text{new embedding vector} = \text{old embedding vector} - \eta \cdot \nabla\_{\text{embedding vector}} \mathcal{L}new embedding vector=old embedding vector−η⋅∇embedding vector​L
     + η\etaη: Learning rate.
     + L\mathcal{L}L: Loss function.
5. **Iteration**:
   * This process repeats over multiple iterations (epochs) with different sentences, gradually improving the embedding vectors to better represent sentiment-related features and improve the model's accuracy on sentiment analysis tasks.

**Example Update (Illustrative)**

Suppose during backpropagation, the gradient for the token "liked" is calculated as ∇liked=[0.2,−0.3,0.1]\nabla\_{\text{liked}} = [0.2, -0.3, 0.1]∇liked​=[0.2,−0.3,0.1].

* If the learning rate η=0.01\eta = 0.01η=0.01, the update to the embedding vector for "liked" could be:
  + new embedding vector for "liked"=[0.7,0.8,0.9]−0.01⋅[0.2,−0.3,0.1]=[0.7−0.002,0.8+0.003,0.9−0.001]=[0.698,0.803,0.899]\text{new embedding vector for "liked"} = [0.7, 0.8, 0.9] - 0.01 \cdot [0.2, -0.3, 0.1] = [0.7 - 0.002, 0.8 + 0.003, 0.9 - 0.001] = [0.698, 0.803, 0.899]new embedding vector for "liked"=[0.7,0.8,0.9]−0.01⋅[0.2,−0.3,0.1]=[0.7−0.002,0.8+0.003,0.9−0.001]=[0.698,0.803,0.899]

**Conclusion**

In summary, token embeddings are updated during training by adjusting their vector representations based on gradients derived from the model's prediction error (loss) with respect to the ground truth labels. This iterative process ensures that the embeddings capture meaningful relationships and semantic features relevant to sentiment analysis, ultimately improving the model's ability to accurately predict sentiment from text data.

 **Tokenization and Numerical Assignment**: Input text is tokenized and each token is assigned a unique numerical ID.

 **Embedding Layer**: Token IDs are mapped to high-dimensional vectors initialized with random values.

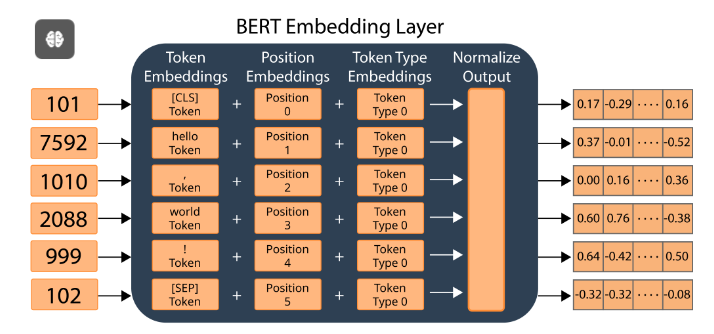
 **Forward Pass**: The embeddings are processed through the network to generate context-aware representations.

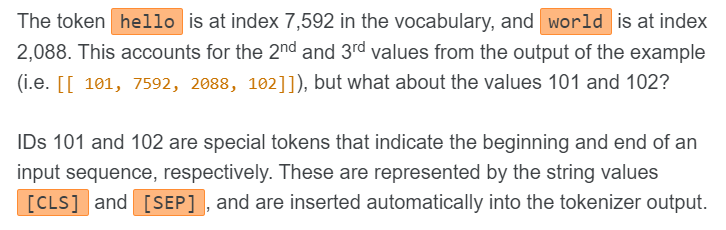
 **Prediction**: The model predicts the next token in the sequence.

 **Loss Calculation**: The prediction is compared to the actual next token to calculate the loss.

 **Backpropagation**: Gradients are computed for the embeddings and other parameters based on the loss.

 **Updating Embeddings**: The embeddings are updated to reduce the prediction error, refining their representations over time.

****

****

First, all spacing characters like tabs and newlines are converted into single whitespaces

Next, whitespace is added before and after every punctuation character. This allows punctuation characters to be treated as separate input tokens, apart from the words that they are connected with in the input string.

For example, the string "hello, world!" is split into the following 6 tokens:

[CLS] hello , world ! [SEP]

The BERT Tokenizer’s vocabulary contains a limited set of unique tokens, which means that there is a possibility of coming across a token that is not present in the vocabulary. To handle such cases, the vocabulary contains a special token, [UNK] which is used to represent any “out-of-vocabulary” input token.

print**(**tokenizer**([**'hello world 👋'**]))**

print**(**"Token with id 100: {tokenizer.vocab\_list[100]}"**)**

**{**'input\_ids'**:** **<**tf**.**Tensor**:** shape**=(1,** **5),** dtype**=**int64**,** numpy**=**array**([[** **101,** **7592,** **2088,** **100,** **102]])>}**

Token **with** id **100:** **[**UNK**]**

**Steps involved in Bert which leads to Contextualized Embedding:**

 **Tokenization**:

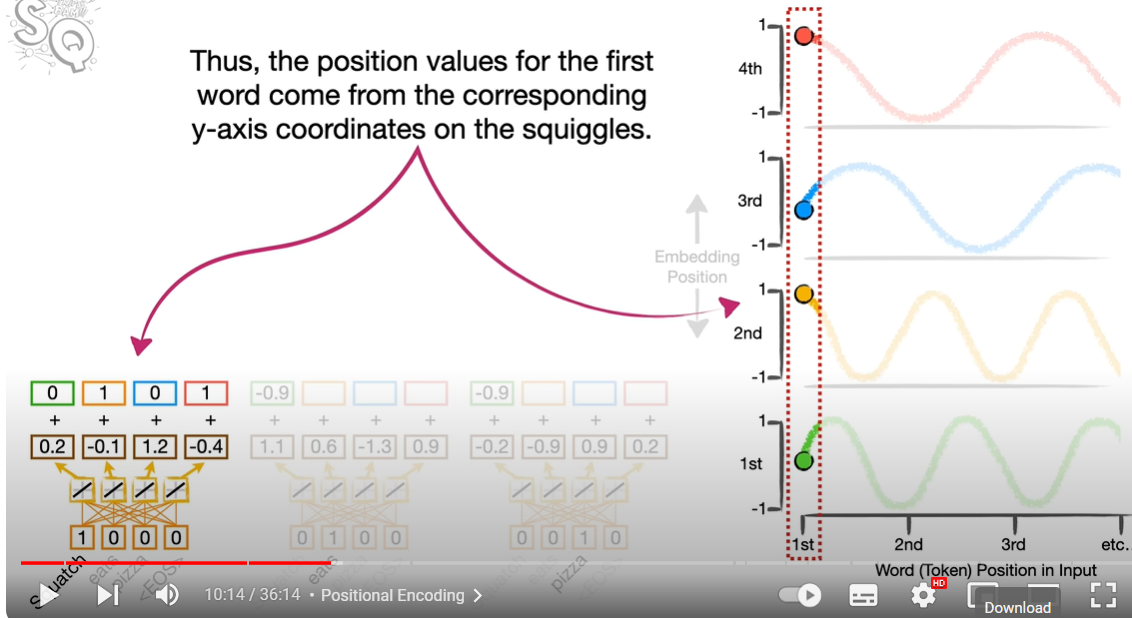
* The input text is tokenized into subword tokens using the WordPiece tokenizer. Each token is then converted into its corresponding token ID.

 **Token Embedding**:

* Each token ID is mapped to a high-dimensional vector using an embedding layer. This is the initial embedding for each token.

 **Positional Encoding**:

* Since the transformer architecture used in BERT does not inherently understand the order of tokens, positional encodings are added to the token embeddings. These encodings provide information about the position of each token in the sequence. The size of positional encoding vector is same as token embedding vector size
* The numbers that represent the word order comes from a sequence of alternating sine and cosine values



For example

Pizza Eats Squash and Squash Eats Pizza. In both cases word embedding for each word remain same so the thing that differentiates both sentences is the positional embeddings we get after adding positional values to word embeddings

 **Segment Embeddings**:

* For tasks involving pairs of sentences (like next sentence prediction), segment embeddings are added to distinguish between the two sentences. Each token in the first sentence gets one type of segment embedding, and each token in the second sentence gets another.

 **Input to the Encoder**:

* The sum of the token embeddings, positional encodings, and segment embeddings is passed to the encoder.

 **Encoder (Self-Attention and Feed-Forward Layers)**:

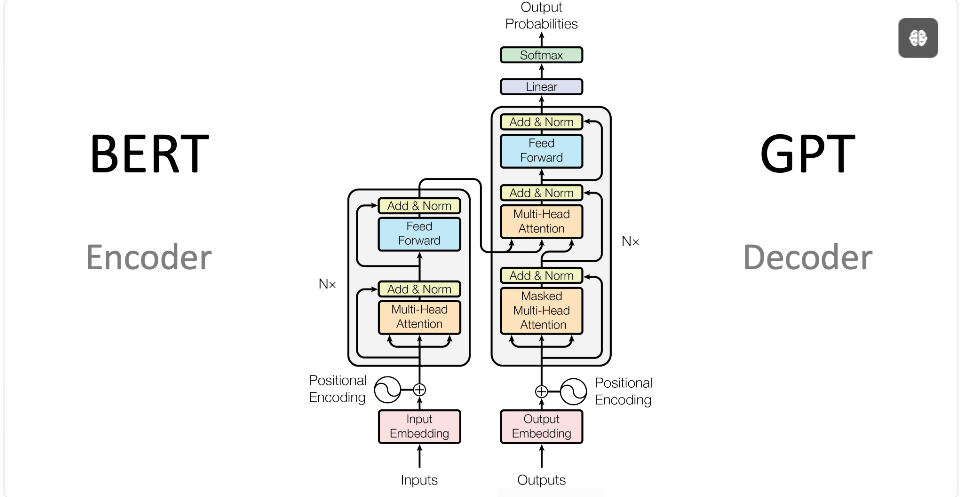
* BERT's encoder consists of multiple layers of transformers. Each transformer layer has two main components:
  + **Multi-Head Self-Attention**: This mechanism allows each token to attend to every other token in the sequence, capturing dependencies irrespective of their distance from each other.
  + **Feed-Forward Neural Network**: A fully connected feed-forward network that processes the output of the attention mechanism.
* Layer normalization and residual connections are applied around each of these components.

**Purpose of Layer Normalization**

* **Stabilizes Training**: By normalizing the inputs to each layer, it ensures that the scale of the inputs remains consistent throughout training, reducing the likelihood of gradient explosion or vanishing.
* **Improves Convergence**: It helps in faster convergence during training by keeping the input mean and variance consistent, which can help in making the optimization landscape smoother.
* **Reduces Internal Covariate Shift**: Internal covariate shift refers to the change in the distribution of network activations due to changes in network parameters during training. Layer normalization helps mitigate this shift.

 **Contextualized Embeddings**:

* The output from the final layer of the encoder is a set of contextualized embeddings for each token. These embeddings are informed by the entire sequence and capture the contextual meaning of each token based on its surroundings.

****

The outputs of the core models are different:

* BERT (encoder): Embeddings representing words with attention information in a certain context
* GPT (decoder): Next words with probabilities

**Attention is All You Need Research Paper**

### Encoder

The encoder is responsible for processing the input sequence and generating a context-aware representation of each token.

#### Components of the Encoder Layer:

1. **Multi-Head Self-Attention Mechanism:**
   * **Self-Attention:** This mechanism allows the model to consider other words in the input sequence when encoding a particular word. It computes attention scores, which indicate the relevance of each word to every other word in the sequence.

**Example:**

Pizza came out of oven and it tasted good.

Here **it** refers to the pizza but how the model gets this thing? It is done by self attention mechanism. It calculates the similarity between each word and all other words in the sentence even with itself

If you looked a lot of sentences about pizza and the word it was more commonly associated with pizza than oven then similarity score for pizza will cause it to have a larger impact in how the word it was encoded by the transformer

* + **Multi-Head:** Instead of performing a single self-attention operation, the model uses multiple attention heads to capture different aspects of the relationships between words. The outputs of these heads are then concatenated and linearly transformed.

1. **Position-wise Feed-Forward Network:**
   * **Feed-Forward Network (FFN):** This is a simple neural network that applies two linear transformations with a ReLU activation in between. It operates independently on each position.
   * **Purpose of position wise** FFN The position-wise feed-forward network in the Transformer architecture serves to independently transform the embedding of each token through a non-linear transformation. This enhances the model's ability to learn complex patterns and relationships within the data, complements the self-attention mechanism, and allows the model to handle sequences of varying lengths efficiently
   * **Residual Connection and Layer Normalization:** A residual connection is added around each sub-layer, followed by layer normalization. This can be represented as: LayerNorm(x+Sublayer(x)) where x is the input to the sub-layer, and Sublayer(x) is the output of the sub-layer (either the self-attention or feed-forward network).
   * **Residual function** involves the addition operation x + Sublayer(x)
2. **Output Dimension:**
   * All sub-layers and the embedding layers produce outputs of dimension 512, ensuring consistent dimensionality throughout the model.

**Key Points about Position-Wise Feed-Forward Networks**

1. **Local Transformation**:
   * **Element-wise Application**: The feed-forward network is applied independently to each token in the sequence. This means that the same FFN is used for each token, and it processes each token's embedding vector separately.
   * **Independence**: This independence allows the network to learn position-specific transformations that do not depend on the context of other positions, adding a layer of local complexity to the model.
2. **Non-Linearity**:
   * **Activation Functions**: The FFN introduces non-linearities through activation functions (typically ReLU) after the first linear transformation. Non-linearities are essential for the network to capture complex patterns and relationships in the data.
3. **Dimensionality Change**:
   * **Transformation**: The FFN typically consists of two linear (fully connected) layers with a non-linearity in between. The first layer projects the input to a higher-dimensional space, and the second layer projects it back to the original dimensionality.
   * **Example**: For an input embedding of size d, the FFN can project it to size dff (where dff​ is usually larger than d) and then back to d

**Structure of Position-Wise Feed-Forward Network**

The position-wise feed-forward network is defined as follows:

FFN(x) = max(0, xW1 + b1)W2 + b2

Where:

 x is the input embedding.

 W1​ and W2​ are weight matrices.

 b1​ and b2​ are bias vectors.

 max(0,x) represents the ReLU activation function

**Difference in working of SELF ATTENTION and FFNN**

1. "He deposited money in the bank."
2. "The boat was anchored near the river bank."

 **Self-Attention**: In both sentences, self-attention determines which tokens are most relevant for understanding each occurrence of "bank". For sentence 1, it might emphasize "money" and "deposited", while for sentence 2, it might highlight "river" and "anchored".

By considering dependencies between all tokens in parallel, self-attention captures syntactic and semantic relationships. It helps the model understand which words are most relevant to each other in a given context

 **FFNN**: After self-attention, the FFNN processes the contextualized representations to capture complex patterns and differentiate between different meanings of "bank". It uses non-linear transformations to refine the understanding of "bank" based on the surrounding context and learned patterns in the data

Subsequently, the representations are passed through FFNNs to refine the understanding of each token, capturing its contextual meaning and distinguishing between different senses or uses of words

**Benefit of Residual Function**

 **Improved Gradient Flow**: Facilitates backward gradient flow during training, addressing the vanishing gradient problem (by increasing the very small gradient which causes slow training).

 **Deeper Networks**: Enables the training of deeper networks to capture more complex patterns. (by dealing with decreasing gradient)

**Easier Optimization**

**Stabilizes Training**

**Complex Dependencies**: Enhances the ability to understand context and capture complex dependencies between tokens.

#### Encoder Layer Process:

1. Input embeddings (along with positional encodings) are passed through the self-attention mechanism.
2. The output of the self-attention mechanism is passed through a feed-forward network.
3. Residual connections and layer normalization are applied after each sub-layer.

**Input x -> Sublayer(x) (e.g., self-attention) -> Add: x + Sublayer(x) -> LayerNorm(x + Sublayer(x)) ->Output**

### Decoder

The decoder generates the output sequence (e.g., translated text) by attending to both the previously generated tokens and the encoder's output.

#### Components of the Decoder Layer:

1. **Masked Multi-Head Self-Attention Mechanism:**
   * **Masking:** This sub-layer is similar to the encoder's self-attention mechanism, but with an additional mask to prevent the decoder from "seeing" future tokens. This ensures that predictions for position iii depend only on the known outputs at positions less than iii.
   * **Self-Attention:** Computes attention scores based only on the known tokens up to the current position.
2. **Multi-Head Attention over Encoder Output:**
   * This sub-layer performs attention over the encoder's output, allowing the decoder to incorporate information from the entire input sequence when generating each token.
3. **Position-wise Feed-Forward Network:**
   * Similar to the encoder, this is a simple neural network that applies two linear transformations with a ReLU activation in between.
4. **Residual Connection and Layer Normalization:**
   * Similar to the encoder, residual connections and layer normalization are applied around each sub-layer.

**Purpose of Masking in Self Attention**

Consider generating a sequence where the current output is "I love".

* **Current Step**: "I love"
* **Next Token Prediction**: The model should predict the next word based on "I love".

Without masking, the model could see the entire sequence, including the word to be predicted, which would make the task trivial and not reflect real-world usage.

With masking, the model can only see "I love" and not the subsequent tokens, making it learn to predict the next token based on the given context

1. **During training**, the model predicts the next word in a sequence based on the preceding words. Masking ensures the model learns to predict the next word based on the correct context.
2. **When translating a sentence**, the decoder generates the translation word by word. Masking ensures that each word is generated based only on the translated words generated so far.

#### Decoder Layer Process:

1. The masked self-attention mechanism processes the previously generated tokens.
2. The output from the masked self-attention is combined with the encoder's output using a multi-head attention mechanism.
3. The result is passed through a feed-forward network.
4. Residual connections and layer normalization are applied after each sub-layer.

### Detailed Steps of the Transformer

1. **Input Processing:**
   * Input tokens are converted to embeddings.
   * Positional encodings are added to these embeddings to retain positional information.
2. **Encoding:**
   * The encoder stack processes the input embeddings through multiple identical layers, each with self-attention and feed-forward networks.
3. **Decoding:**
   * The decoder stack processes the target sequence (shifted right to ensure that the prediction for position iii depends only on positions less than iii) through multiple identical layers.
   * Each layer consists of masked self-attention, encoder-decoder attention, and feed-forward networks.
   * The final output is produced by applying a linear transformation followed by a softmax function to the decoder's output.

**Attention:** An attention function can be described as mapping a query and a set of key-value pairs to an output, where the query, keys, values, and output are all vectors. The output is computed as a weighted sum of the values, where the weight assigned to each value is computed by a compatibility function of the query with the corresponding key

**Query, Key, and Value**

1. **Query (Q)**:
   * The query is a vector used to retrieve information from other vectors, often associated with a specific token in the sequence. It can be considered as a piece of information that you are querying the rest of the sequence for
   * We multiply the values we get after adding positional embeddings in initial embeddings with a pair of weights to get key values. These weights are learned during training and these are not the same weights we use to get initial embeddings
2. **Key (K)**:
   * The key vector helps determine how much focus or attention should be placed on other tokens relative to the current token (associated with the query). It represents the token's representation used to compute compatibility scores (relevance) with other tokens.
   * We multiply the values we get after adding positional embeddings in initial embeddings with a pair of weights to get key values. These weights are learned during training and these are not the same weights we use to get initial embeddings
3. **Value (V)**:
   * The value vector is the actual content or information associated with the token. It is used to compute the weighted sum of values, where weights are determined by the attention scores between the query and key vectors
   * We multiply the values we get after adding positional embeddings in initial embeddings with a pair of weights to get Value values. These weights are learned during training and these are not the same weights we use to get initial embeddings

 **Query and Key**: Determine similarity scores by dot product between both pairs of values even the dot product is taken with the query key pair of word with itself which gives a high score telling the word is similar to itself small value refers to less similarity. The similarity scores are passed through softmax. After softmax we get values between 0 and 1. These values tells us how much percentage of each input word we use to encode the word we are talking about

 **Value**: Holds the actual content or representation of each token, not attention scores

**Important**

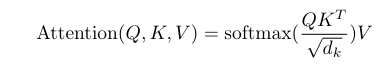
We reuse the same set of weights for each word. For example if there are three words in sentences to calculate the query values for all three of them we use same one set of weights similarly for both Values and Key pairs. But the weights used in Decoder are different than encoder

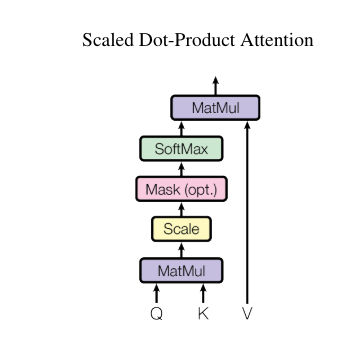
The query, key, value pair for each word can be calculated parallel which makes computing fast for transformers

**Scaled Dot-Product Attention:**

The input consists of queries and keys of dimension dk, and values of dimension dv. We compute the dot products of the query with all keys, divide each by √dk, and apply a softmax function to obtain the weights on the values.

In practice, we compute the attention function on a set of queries simultaneously, packed together into a matrix Q. The keys and values are also packed together into matrices K and V . We compute he matrix of outputs as:

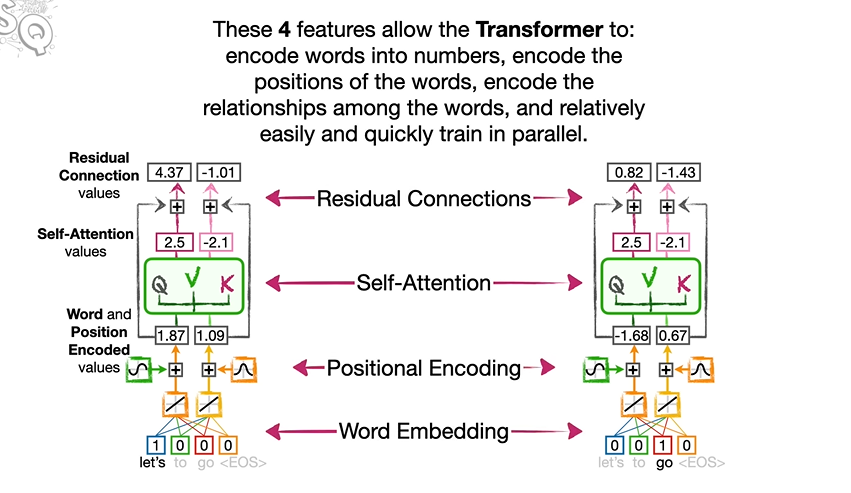




**Encoder Part**

After adding the values for attention for each word with respective to other words using the above formula, we get Attention Values for the Word and gives context to each word since the value is formed by taking input from all other words. We add positional encoding values to self attention values to get Residual Connection Values

If there are three words in the sentence. And the structure below if we call it a CELL, we can use three cells to ENCODE which will increase the processing speed as computation for every word (computing All 4 values below for the word )will be done at same time



**Decoder Part**

First of all, the embeddings for the output vocabulary is created which consists of Spanish words in our Example

We are trying to translate “Let’s go” in Spanish

ir vamos y <EOS>

We start with <EOS> to start the decoding process. Its a common way to start the decoding process with <EOS> to initialize the process. We can also use Start of Sentence <SOS>.

Same way as above we use more than one cells to process faster

We also need to keep track between input and output sentences in addition to relation between words in a sentence in decoding part

**Example:**

Don’t eat the delicious pizza

If decoder don’t focus on the first word, then the whole meaning of the sentence will change. The **main idea of Encoder-Decoder Attention** is that Decoder should be able to keep track of the significant words

We create two new value QUERY to represent <EOS> in decoder. Then we create KEYS for each word in encoder and we calculate similarity between <EOS> and each word in encoder and calculate dot product and run through softmax then scale the Value pair in encoder with the result of Softmax and add them to get attention values for ENCODER-DECODER attention. The sets of weight we use to calculate the ENCODER-DECODER Attention values are different then sets of weights for SELF-Attention but the weights are copied for each word. We can stack these ENCODER-DECODER Attention just like we can stack SELF Attention. Now we add another set of Residual Connections, that allow EDA to focus on relationship between input and output word without having to preserve the self attention or word and position encoding that happened earlier. Now we need to use the two values we have for <EOS> token to select one the four output token, We run these two values through a fully connected layer that has one input for each value that represent the current token. Two input and four output values which we run through a final SOFTMAX fun to select output word.

After softmax it selects VAMOS, which is correct but the decoder does not stop until it outputs <EOS> token. So we run the VAMOS through all the 4 steps and get next word as <EOS>.

The original formula in the article where dot product is normalized first, is so we can do these tasks with complicated SENTENCES

**PROMPT ENGINEERING**

**Purpose of Prompt Engineering:**

The main purpose of prompt engineering is to optimize the input provided to a language model to elicit the most accurate, relevant, and useful responses. This involves designing and refining prompts to guide the model's behavior effectively, thereby enhancing its performance across a variety of tasks

**1. Improve Response Quality**

Clarity and Relevance: Crafting clear and specific prompts.

**2. Task Specialization**

Adapt to Specific Tasks: Tailoring prompts for particular applications.

**3. Enhance Model Understanding**

Provide Context: Adding necessary context within the prompt.

**4. Increase Efficiency**

Optimize Performance: Reducing the need for extensive fine-tuning.

**5. Mitigate Model Limitations**

Bias Reduction: Helping mitigate biases inherent in the model.

**6. Facilitate Complex Tasks**

Multi-step Processes: Enabling the model to handle multiple steps.

**7. Leverage External Knowledge**

Integrate Retrieval: Incorporating external documents or data.

**Few Prompting Techniques**

* **Zero-shot prompting**: This is the most direct and simplest method of prompt engineering in which a generative AI is simply given direct instruction or asked a question without being provided additional information. This is best used for relatively simple tasks rather than complex ones.
* **Few-shot prompting:** This method involves supplying the generative AI with some examples to help guide its output. This method is more suitable for complex tasks than zero-shot prompting.
* **Chain-of-thought (CoT) prompting:** This method helps improve an LLM's output by breaking down complex reasoning into intermediate steps, which can help the model produce more accurate results.
* **Prompt chaining:** The prompter splits a complex task into smaller (and easier) subtasks, then uses the generative AI's outputs to accomplish the overarching task. This method can improve reliability and consistency for some of the most complicated t

asks.

**Retrieval-Augmented Generation (RAG)**

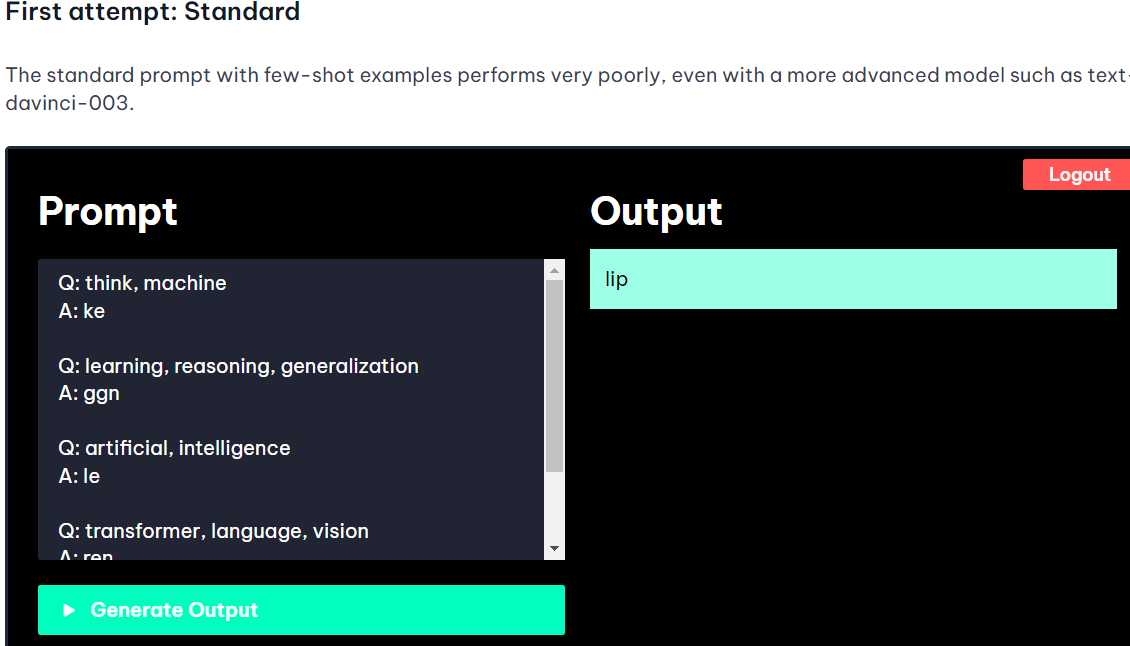
* **Description**: RAG combines retrieval-based methods with generative models. It retrieves relevant documents or passages from a large corpus and uses them to inform the generation process.
* **Common Use**: Used for tasks requiring up-to-date or domain-specific knowledge that the model might not have been trained on.
* **Example**
* Question: What were the main outcomes of the recent G7 summit?
* [Retrieval: External Document or API with G7 Summit outcomes]
* Retrieved Text: The G7 summit concluded with agreements on climate action, economic recovery post-COVID-19, and measures to tackle global inequality.
* Generated Response: The main outcomes of the recent G7 summit included agreements on climate action, economic recovery post-COVID-19, and measures to tackle global inequality.

**Chain of Thought (CoT)**

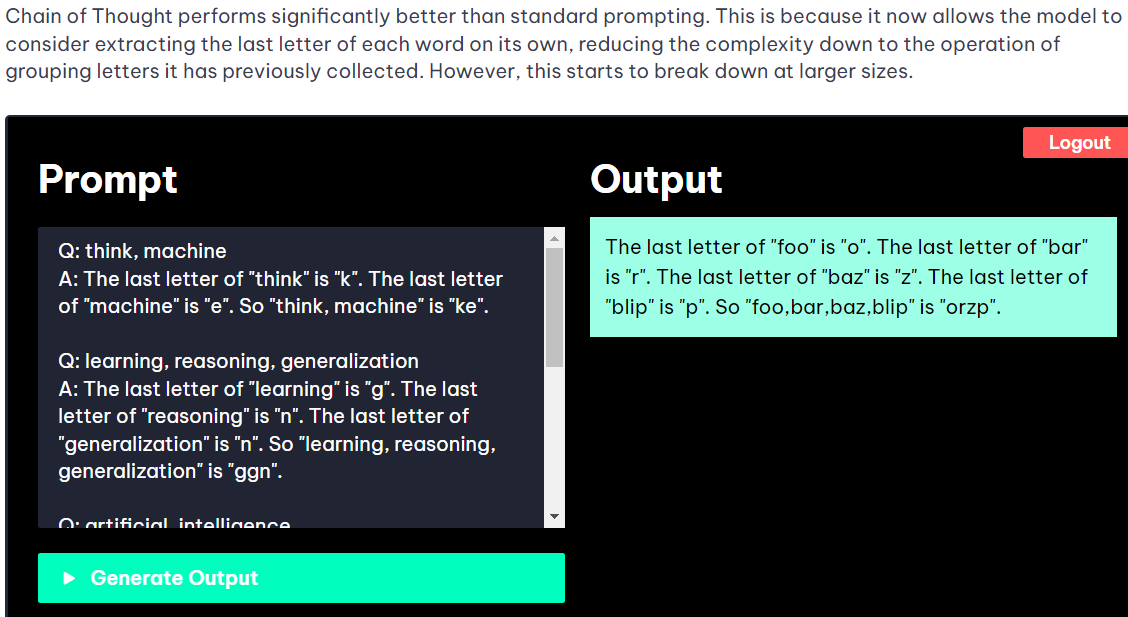
* **Description**: CoT involves guiding the model through a series of logical steps or intermediate reasoning stages to arrive at the final answer.
* Chain-of-Thought is a technique that involves breaking down a task into sections, combining results to arrive at a final answer, enhancing precision in responses from large language models.
* **Common Use**: Useful for complex problem-solving and reasoning tasks where intermediate steps are necessary.
* The main idea of CoT is that by showing the LLM some few shot exemplars where the reasoning process is explained in the exemplars, the LLM will also show the reasoning process when answering the prompt
* Zero shot chain of prompting, despite its simplicity, tends to improve model performance by including step-by-step reasoning in the response. It is encouraging that this technique can be used to solve complex tasks without the necessity of providing multiple input exemplars like in chain of thought prompting
* **Example**
* Q: If a train travels 60 miles per hour for 2 hours, then 70 miles per hour for 3 hours, how far does it travel in total? Step-by-step reasoning:
* 1. Calculate the distance traveled at 60 miles per hour for 2 hours. 2. Calculate the distance traveled at 70 miles per hour for 3 hours. 3. Add the two distances to get the total distance traveled.
* A: The train travels 60 miles/hour \* 2 hours = 120 miles. The train travels 70 miles/hour \* 3 hours = 210 miles. The total distance traveled is 120 miles + 210 miles = 330 miles.

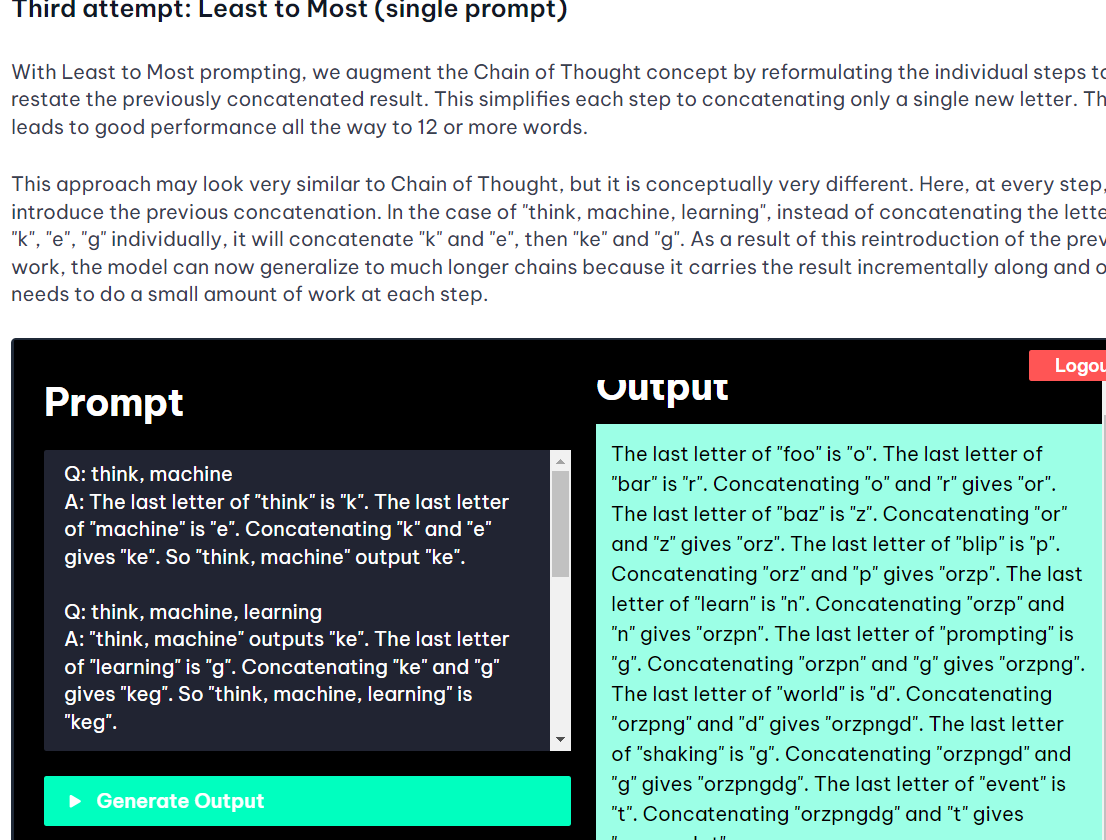
**Least to Most prompting (LtM**)1 takes CoT prompting a step further by first breaking a problem into sub problems then solving each one. It is a technique inspired by real-world educational strategies for children.

As in CoT prompting, the problem to be solved is decomposed in a set of subproblems that build upon each other. In a second step, these subproblems are solved one by one. Contrary to chain of thought, the solution of previous subproblems is fed into the prompt trying to solve the next problem



How COT solves the problem by manipulating the prompt





**Reasoning and Acting (ReAct)**

* **Description**: ReAct integrates reasoning steps with actions, allowing the model to not only process information and reason about it but also to perform actions based on that reasoning.
* Using ReAct mode involves a 3-step process: thinking about what you're looking for, taking action to retrieve it, and observing the result, enhancing prompt tuning technique
* Difference between Chain-of-Thought and ReAct techniques. ReAct goes beyond reasoning to gather additional information from external sources for response
* **Common Use**: Suitable for interactive tasks where the model needs to make decisions and take actions based on its reasoning
* **Example**
* User: I want to book a flight from New York to Paris on July 20th.
* **Model Reasoning and Acting:**
* 1. Check the availability of flights on the requested date.
* 2. Compare prices and flight durations.
* 3. Provide the best options to the user.
* **Action:**
* Searching for flights from New York to Paris on July 20th...
* [Model acts by retrieving flight data]
* **Available options:**
* 1. Flight XYZ123 - Departure: 10:00 AM, Arrival: 10:00 PM, Price: $500
* 2. Flight ABC456 - Departure: 3:00 PM, Arrival: 3:00 AM (next day), Price: $450
* **User:** I'll take Flight XYZ123.
* **Model Reasoning and Acting**:
* 1. Confirm the flight booking details.
* 2. Book the flight and send confirmation to the user.
* **Action:**
* Booking Flight XYZ123...
* [Model acts by confirming the booking]
* Your flight has been booked successfully! You will receive a confirmation email shortly.

**Dynamic Sampling and Prompting (DSP)**

* **Description**: DSP involves dynamically adjusting the sampling strategy and prompt structure during the interaction with the model to improve responses.
* **Common Use**: Enhances the model’s ability to generate more relevant and contextually appropriate responses.
* **Example**
* Story so far: Once upon a time, in a small village nestled in the hills, there was a young girl named Lily. She loved exploring the forest nearby and discovering new things.s
* **Dynamic Prompting**:
* 1. If the next part of the story should introduce a conflict, provide a continuation with a problem.
* 2. If the next part of the story should develop the character, provide a continuation that gives more background about Lily.
* [Dynamic Sampling Decision: Introduce a conflict]
* Continuation: One day, while exploring deeper into the forest than she ever had before, Lily stumbled upon a dark cave. From within, she heard strange noises and saw a faint, flickering light...

**Elements of a Prompt:**

A prompt contains any of the following elements:

Instruction - a specific task or instruction you want the model to perform "Write", "Classify", "Summarize", "Translate", "Order"

Context - external information or additional context that can steer the model to better responses

Format and Tone of the response we need

Input Data - the input or question that we are interested to find a response for

Output Indicator - the type or format of the output

**EXAMPLE**

You can observe from the prompt example above that the language model responds with a sequence of tokens that make sense given the context "The sky is". The output might be unexpected or far from the task you want to accomplish. In fact, this basic example highlights the necessity to provide more context or instructions on what specifically you want to achieve with the system. This is what prompt engineering is all about.

Let's try to improve it a bit:

**Prompt:**

Complete the sentence:

The sky is

**Output:**

blue during the day and dark at night.

Is that better? Well, with the prompt above you are instructing the model to complete the sentence so the result looks a lot better as it follows exactly what you told it to do ("complete the sentence"). This approach of designing effective prompts to instruct the model to perform a desired task is what's referred to as prompt engineering in this guide.

You can format this into a question answering (QA) format, which is standard in a lot of QA datasets, as follows:

Q: <Question>?

A:

When prompting like the above, it's also referred to as **zero-shot prompting**, i.e., you are directly prompting the model for a response without any examples or demonstrations about the task you want it to achieve. Some large language models have the ability to perform zero-shot prompting but it depends on the complexity and knowledge of the task at hand and the tasks the model was trained to perform good on

one popular and effective technique to prompting is referred to as **few-shot prompting** where you provide exemplars (i.e., demonstrations). You can format few-shot prompts as follows:

**Prompt:**

This is awesome! // Positive

This is bad! // Negative

Wow that movie was rad! // Positive

What a horrible show! //

**Output:** Negative

**Priming chatbots** is a method of using your first prompt to set the structure and style of a conversation. This gives you fine grained control over your entire conversation

**USER** messages, which are just the messages you send to the chatbot, and **ASSISTANT** messages, which are the chatbot's replies. A third type of message, the system prompt, can be used to configure how the AI responds. This is the best place to put a priming prompt. The system prompt will be "You are a helpful assistant." by default, but a fun alternative example to try out would be the "You are PirateGPT. Always talk like a pirate

**What are LLM Settings?**

We can use certain LLM settings to control various aspects of the model, such as how 'random' it is. These settings can be adjusted to produce more creative, diverse, and interesting output. The Temperature, Top P and Max Length settings are most important

**Temperature**

Temperature regulates the unpredictability of a language model's output. With higher temperature settings, outputs become more creative and less predictable as it amplifies the likelihood of less probable tokens while reducing that for more probable ones. Conversely, lower temperatures yield more conservative and predictable result

The temperature is used for sampling during response generation, which occurs when topP and topK are applied. Temperature controls the degree of randomness in token selection. Lower temperatures are good for prompts that require a less open-ended or creative response, while higher temperatures can lead to more diverse or creative results. A temperature of 0 means that the highest probability tokens are always selected. In this case, responses for a given prompt are mostly deterministic, but a small amount of variation is still possible.

Example:

What are 10 weird, unique, and fun things to do at the beach? Make a list without descriptions

If the temperature is low we will get predictable answers. If the temperature is high we will get more creative and less predictable

If you adjust the temperature too high, you can get non-sensical outputs like Start a sponge-ball baseball home run contest near Becksmith Stein Man Beach

**Top P**

Top P is a setting in language models that helps manage the randomness of their output. It works by establishing a probability threshold and then selecting tokens whose combined likelihood surpasses this limit.

**Setting top\_p to 1 means** that the model will always choose the token with the highest probability (argmax) for each step during text generation

For instance, let's consider an example where the model predicts the next word in The cat climbed up the \_\_\_. The top five words it might be considering could be tree (probability 0.5), roof (probability 0.25), wall (probability 0.15), window (probability .07) and carpet, with probability of .03.

If we set Top P to .90, the AI will only consider those tokens which cumulatively add up to at least ~90%. In our case:

Adding tree -> total so far is 50%.

Then adding roof -> total becomes 75%.

Next comes wall, and now our sum reaches 90%.

So, for generating output, the AI will randomly pick one among these three options (tree, roof, and wall) as they make up around ~90 percent of all likelihoods. This method can produce more diverse outputs than traditional methods that sample from the entire vocabulary indiscriminately because it narrows down choices based on cumulative probabilities rather than individual token

Top-P changes how the model selects tokens for output. Tokens are selected from the most (see top-K) to least probable until the sum of their probabilities equals the top-P value. For example, if tokens A, B, and C have a probability of 0.3, 0.2, and 0.1 and the top-P value is 0.5, then the model will select either A or B as the next token by using temperature and excludes C as a candidate.

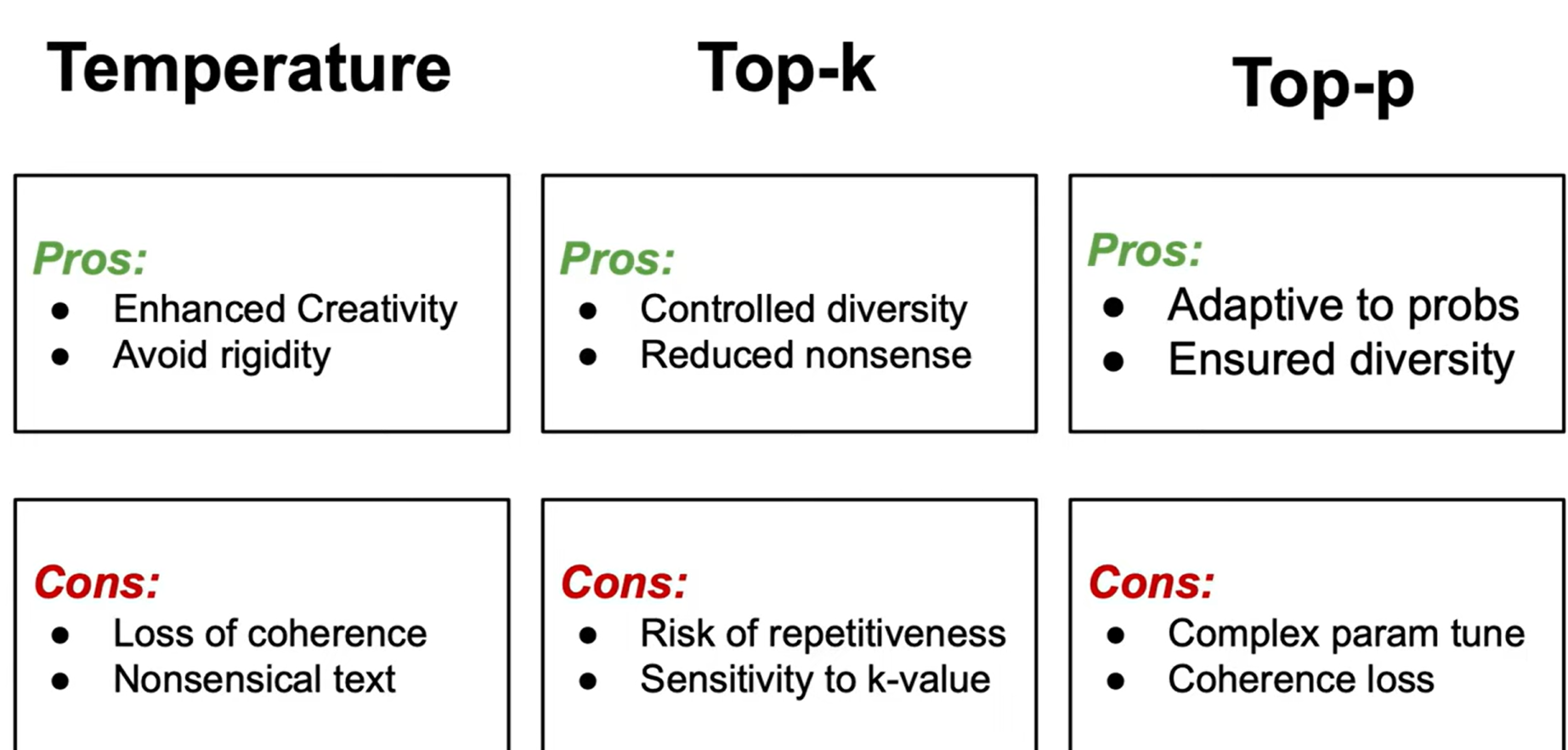
Specify a lower value for less random responses and a higher value for more random responses

**Top-K**

Top-K changes how the model selects tokens for output. A top-K of 1 means the next selected token is the most probable among all tokens in the model's vocabulary (also called greedy decoding), while **a top-K of 3 means that the next token is selected from among the three most probable tokens by using temperature.**

For each token selection step, the top-K tokens with the highest probabilities are sampled. Then tokens are further filtered based on top-P with the final token selected using temperature sampling.

Specify a lower value for less random responses and a higher value for more random responses



**Maximum Length**

The **maximum length is the total # of tokens the AI is allowed to generate**. This setting is useful since it allows users to manage the length of the model's response, preventing overly long or irrelevant responses. The length is shared between the USER input in the Playground box and the ASSISTANT generated response. Notice how with a limit of 256 tokens, our PirateGPT from earlier is forced to cut its story short mid-sentence

**Frequency Penalty**

Frequency penalty is a setting that discourages repetition in the generated text by penalizing tokens proportionally to how frequently they appear. The more often a token is used in the text, the less likely the AI is to use it again.

**Presence Penalty**

The presence penalty is similar to the frequency penalty, but flatly penalizes tokens based on if they have occurred or not, instead of proportionally

**Pitfalls for LLMS**

 **Citing Sources**:

* **Issue**: LLMs cannot accurately cite sources because they lack access to the internet and do not remember their training data sources.
* **Mitigation**: Search augmented LLMs, which have internet access, can provide more accurate information but still may generate fabricated sources.

 **Bias**:

* **Issue**: LLMs may exhibit bias in responses due to training on datasets containing biased information, leading to potentially prejudiced outputs.
* **Impact**: This can perpetuate harmful stereotypes and bias in consumer applications and research.

 **Hallucinations**:

* **Issue**: LLMs sometimes generate confident but false information when unsure of an answer, potentially spreading misinformation.
* **Concern**: It's crucial to verify information from LLMs, especially in critical or factual contexts.

 **Math**:

* **Issue**: LLMs often struggle with mathematical tasks and can provide incorrect answers, despite their linguistic proficiency.
* **Consideration**: Using tool augmented LLMs designed for specific tasks like math can help mitigate this issue.

 **Prompt Hacking**:

* **Issue**: Users can manipulate LLMs through carefully crafted prompts to generate unintended or inappropriate content.
* **Risk**: This can be exploited in public-facing applications to produce misleading or harmful outputs.

**Prompt Injection**

Prompt injections in large language models can lead to vulnerabilities, allowing users to manipulate systems by injecting specific instructions, potentially causing unintended actions

**Direct Prompt Injections**, also known as "jailbreaking," occur when a malicious user overwrites or reveals the underlying system prompt. This allows attackers to exploit backend systems by interacting with insecure functions and data stores accessible through the LLM.

**Indirect Prompt Injections** occur when an LLM accepts input from external sources that can be controlled by an attacker, such as websites or files. The attacker may embed a prompt injection in the external content, hijacking the conversation context. This can lead to unstable LLM output, allowing the attacker to manipulate the user or additional systems that the LLM can access. Additionally, indirect prompt injections do not need to be human-visible/readable, as long as the text is parsed by the LLM.  
As more companies use LLMs to screen resumes, some websites now offer to add invisible text to your resume, causing the screening LLM to favor your CV

**Consequences**

Consequences of prompt injections include malware creation, misinformation dissemination, data leakage, and remote system control, emphasizing the need for preventive actions and human supervision

**Possible Solution**

Mitigation strategies involve data curation, adherence to least privilege principle(only gives the capability which is required) , human oversight in decision-making, input filtering, and reinforcement learning from human feedback to enhance model training

**API CALL TO OPEN AI**

def set\_open\_params(

model="gpt-3.5-turbo",

temperature=0.7,

max\_tokens=256,

top\_p=1,

frequency\_penalty=0,

presence\_penalty=0,

):

""" set openai parameters"""

openai\_params = {}

openai\_params['model'] = model

openai\_params['temperature'] = temperature

openai\_params['max\_tokens'] = max\_tokens

openai\_params['top\_p'] = top\_p

openai\_params['frequency\_penalty'] = frequency\_penalty

openai\_params['presence\_penalty'] = presence\_penalty

return openai\_params

model: Specifies the model to use (default is "gpt-3.5-turbo").

temperature: Controls the randomness of predictions (default is 0.7).

max\_tokens: Specifies the maximum number of tokens (words or subwords) in the generated response (default is 256).

top\_p: Controls the diversity of the generated responses (default is 1).

frequency\_penalty and presence\_penalty: Used to discourage repetition and encourage diversity in responses (both default to 0).