



ΓΛΩΣΣΙΚΗ ΤΕΧΝΟΛΟΓΙΑ

Κάτια Κερμανίδου kerman@ionio.gr

Αποσπάσματα κάποιων διαφανειών είναι δανεισμένα από τα
slides του Speech and Language Processing

ΜΕΓΑΛΑ ΜΟΝΤΕΛΑ
ΓΛΩΣΣΑΣ

LARGE LANGUAGE
MODELS

Τι είναι τα Μεγάλα Μοντέλα Γλώσσας (Large Language Models – LLMs)

Υπολογιστικοί Πράκτορες που μπορούν να πραγματοποιήσουν επικοινωνιακή διάδραση με χρήση φυσικής γλώσσας

Τα κλασσικά Μοντέλα Γλώσσας Βασισμένα σε N-γραμμα

Υπολογίζουν πιθανότητες μικρών ακολουθιών λέξεων

Παράγουν κείμενο προβλέποντας την πιο πιθανή επόμενη λέξη σε μια ακολουθία

Εκπαιδεύονται από τις εμφανίσεις N-γράμμων σε μεγάλα σώματα κειμένων

Τα Μεγάλα Μοντέλα Γλώσσας

Υπολογίζουν πιθανότητες λέξεων δεδομένων χιλιάδων ή δεκάδων χιλιάδων λέξεων στα συμφραζόμενα

Παράγουν κείμενο πραγματοποιώντας δειγματοληψία ανάμεσα στις πιθανές λέξεις που μπορεί να πάρουν την θέση της επόμενης σε μια ακολουθία

Εκπαιδεύονται μαθαίνοντας να προβλέπουν την επόμενη λέξη

Το κείμενο περιέχει τεράστια ποσότητα γνώσης

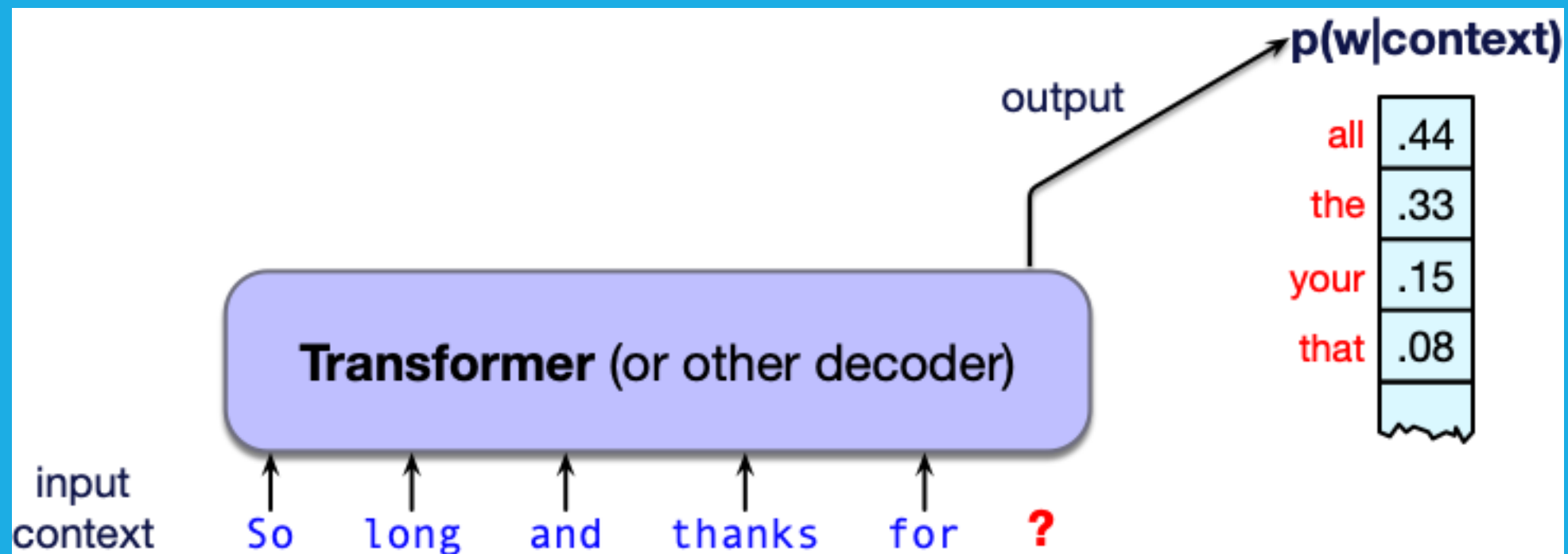
Η Προ-εκπαίδευση σε τεράστιο όγκο κειμένου δίνει την ικανότητα στα ΜΜΓ να έχουν τέτοια απόδοση

Το Μεγάλο Μοντέλο Γλώσσας

Είναι ένα Νευρωνικό Δίκτυο με

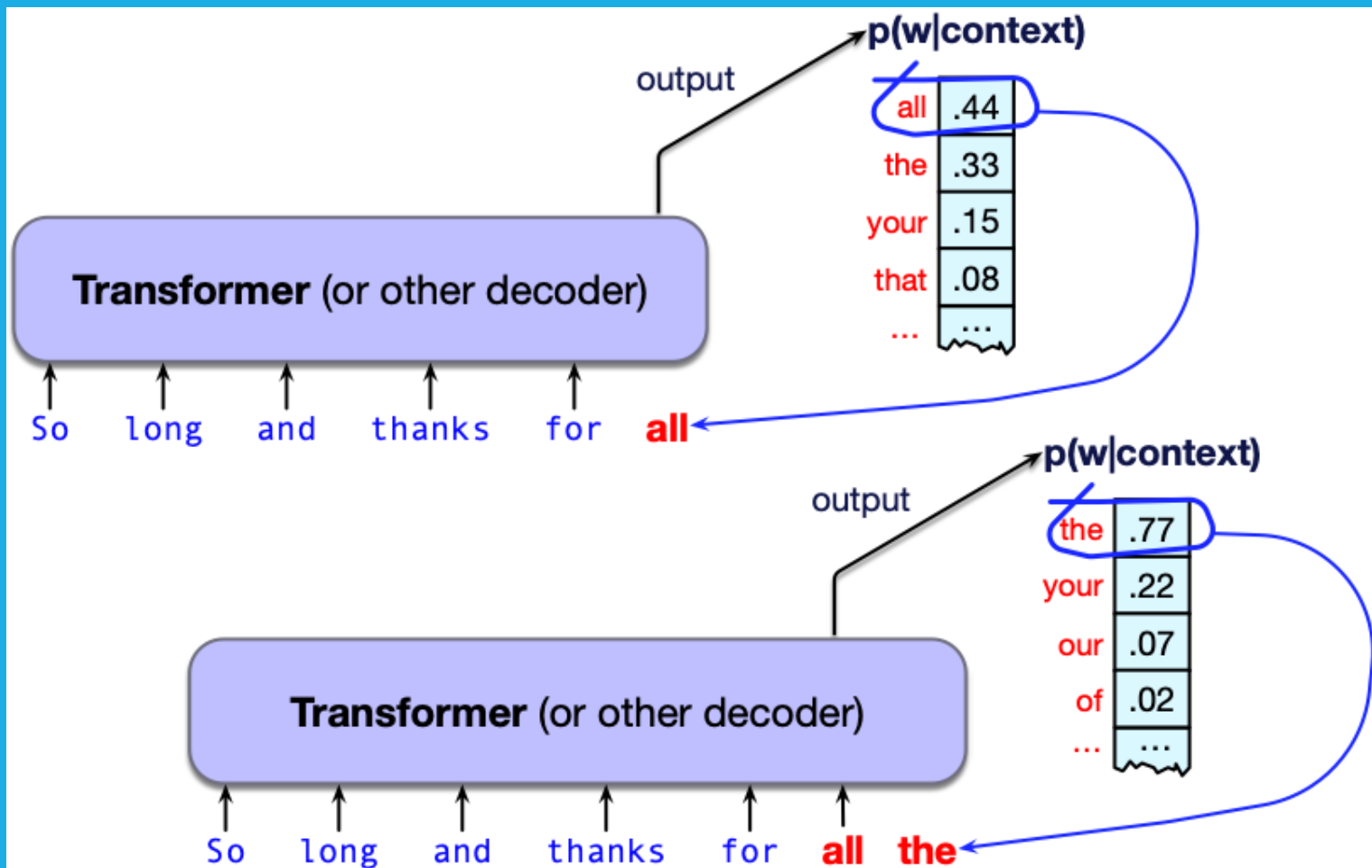
Είσοδο: το περιεχόμενο (συμφραζόμενα) της λέξης που πάω να προβλέψω

Έξοδο: μια κατανομή πιθανοτήτων πάνω σε επόμενες πιθανές λέξεις



Ένα ΜΜΓ παράγει/συνθέτει κείμενο

Με δειγματοληψία από την κατανομή επαναληπτικά



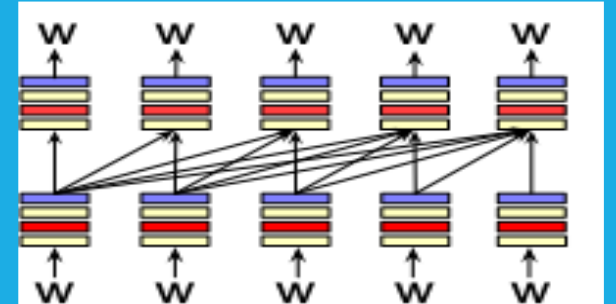
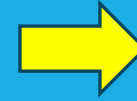
Καθώς παράγεται μια λέξη, προστίθεται στα συμφραζόμενα προκειμένου να παραχθεί η επόμενη

Left-to-right language model
Autoregressive/causal language model

Διαφορετικές Αρχιτεκτονικές LLMs

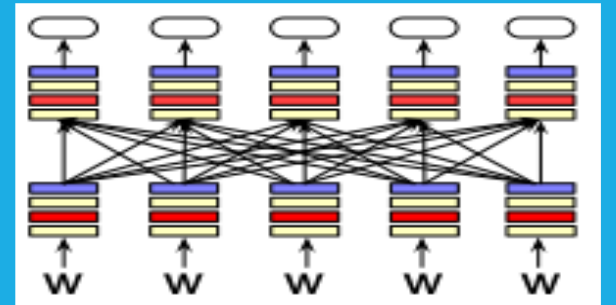
❑ Decoders (GPT, Claude, Llama)

- ❑ Μοντέλα παραγωγής – Generative models
- ❑ Παίρνει σαν είσοδο μια ακολουθία από tokens, και επαναληπτικά παράγει ένα token στην έξοδο τη φορά
- ❑ Εκπαιδεύεται να προβλέπει λέξεις από τις συμφραζόμενες λέξεις που προηγούνται



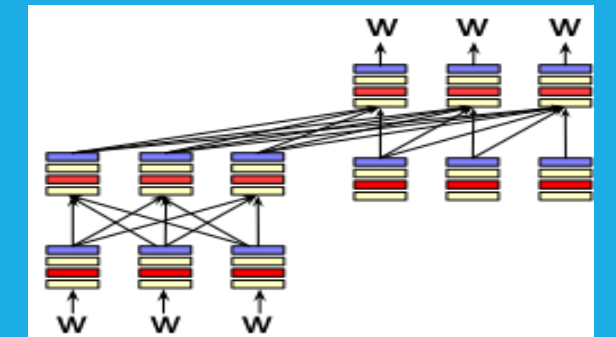
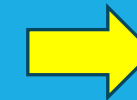
❑ Encoders (BERT)

- ❑ Εκπαιδεύεται να προβλέπει λέξεις από τις συμφραζόμενες λέξεις και που προηγούνται και που έπονται
- ❑ Δεν παράγει κείμενο, παράγει μια διανυσματική αναπαράσταση της εισόδου. Με προσαρμογή (fine-tuning) αυτή η αναπαράσταση μπορεί να χρησιμοποιηθεί για ταξινόμηση κειμένου



❑ Encoder-Decoders

- ❑ Εκπαιδεύονται να ταιριάζουν μια ακολουθία σε μια άλλη
- ❑ Μηχανική Μετάφραση (ταιριάζουν μια γλώσσα σε μια άλλη)
- ❑ Αναγνώριση Ομιλίας (ταιριάζουν την ακουστική σε λέξεις)



Υπο συνθήκη Παραγωγή – Conditional Generation

Παραγωγή κειμένου δεδομένου προηγούμενου κειμένου

Στο ΜΜΓ δίνεται είσοδος ένα κείμενο, ονομάζεται **prompt**.

Το ΜΜΓ παράγει λέξη-λέξη καινούριο κείμενο δεδομένου του prompt και των λέξεων που έχει παράξει μέχρι στιγμής.

1. Υπολογίζεται τι πιθανότητα έχει μια λέξη να ακολουθήσει βάσει των προηγούμενων λέξεων $P(w_i | w_{<i})$
2. Πραγματοποιείται δειγματοληψία από αυτή την κατανομή προκειμένου να επιλεγεί η επόμενη λέξη

Παράδειγμα: Τα MMΓ στην Ανάλυση Συναισθήματος

Έστω ότι θέλω να βρω το συναίσθημα της φράσης «*I like Jackie Chan*».

Δίνω στο MMΓ το εξής κείμενο (**prompt**):

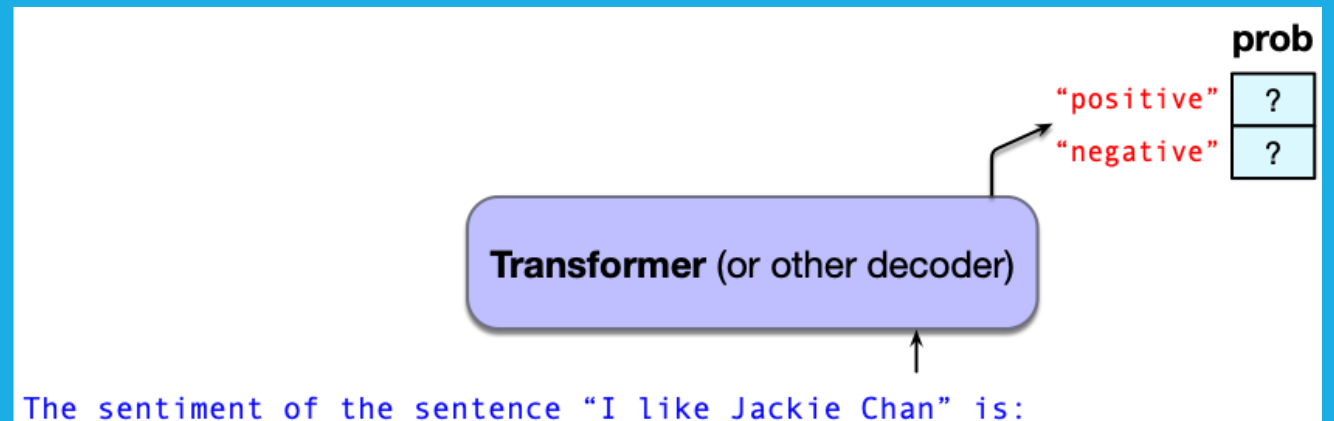
The sentiment of the sentence "I like Jackie Chan" is:

Και βλέπουμε ποια λέξη επιλέγει το MMΓ να ακολουθήσει.

$P(\text{positive} | \text{The sentiment of the sentence ``I like Jackie Chan'' is:})$

$P(\text{negative} | \text{The sentiment of the sentence ``I like Jackie Chan'' is:})$

Ποια από τις δυο λέξεις
έχει μεγαλύτερη
πιθανότητα να ακολουθεί;



Παράδειγμα: Question-Answering

QA: "Who wrote The Origin of Species"

1. Δίνω στο μοντέλο την είσοδο:

2. Q: Who wrote the book ``The Origin of Species"? A:
Υπολογίζεται η πιθανότητα εμφάνισης της επόμενης λέξης w:

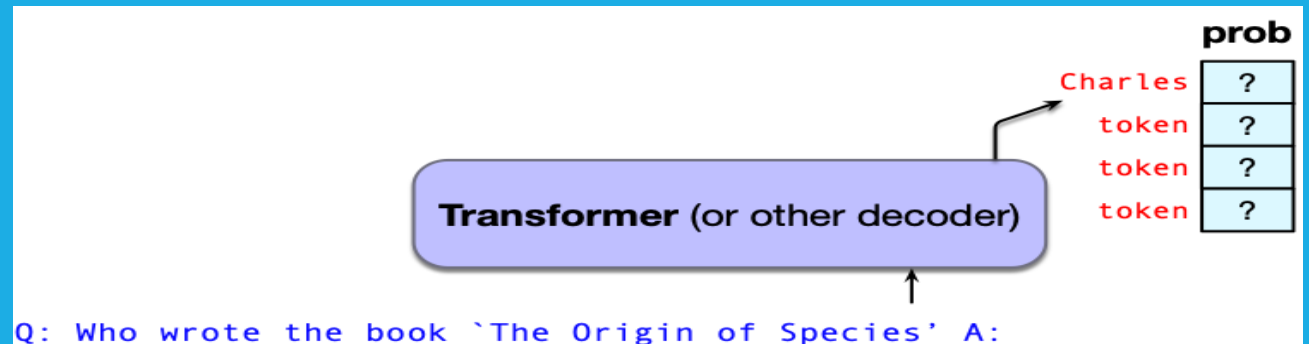
$P(w|Q: \text{Who wrote the book ``The Origin of Species"? A:})$

Έχει μεγαλύτερη πιθανότητα η απάντηση
Charles

Και επαναληπτικά:

$P(w|Q: \text{Who wrote the book ``The Origin of Species"? A: Charles})$

Έχει μεγαλύτερη πιθανότητα πχ η απάντηση Darwin.



Prompting

Είναι κείμενο που δίνει ο χρήστης στο ΜΜΓ για να αναγκάσει το μοντέλο να κάνει κάτι χρήσιμο.

Το ΜΜΓ επαναληπτικά παράγει λέξεις δεδομένου του prompt.

Prompts που εκφράζουν ρητά τον τρόπο με τον οποίο θέλει ο χρήστης να απαντηθεί το ερώτημά του, δίνοντας ενδεχομένως το σετ των πιθανών απαντήσεων, οδηγούν σε πολύ βελτιωμένη απόδοση.

Ένα prompt που αποτελείται από δομή, από σετ απαντήσεων, καθώς και μια ατελή πρόταση

Human: Do you think that "input" has negative or positive sentiment?

Choices:

(P) Positive

(N) Negative

Assistant: I believe the best answer is: (

Zero-shot και few-shot Prompting

Η χρήση παραδειγμάτων με απαντήσεις (labeled examples) στο prompt επίσης βελτιώνει πολύ την απόδοση.

Η χρήση επισημειωμένων παραδειγμάτων ονομάζεται **few-shot prompting** σε αντίθεση με το **zero-shot prompting** που δεν περιλαμβάνει επισημειωμένα παραδείγματα.

Example of demonstrations in a computer science question from the MMLU dataset described in Section 7.6

The following are multiple choice questions about high school computer science.

Let $x = 1$. What is $x \ll 3$ in Python 3?

(A) 1 (B) 3 (C) 8 (D) 16

Answer: C

Which is the largest asymptotically?

(A) $O(1)$ (B) $O(n)$ (C) $O(n^2)$ (D) $O(\log(n))$

Answer: C

What is the output of the statement "a" + "ab" in Python 3?

(A) Error (B) aab (C) ab (D) a ab

Answer:

Figure 7.6 Sample 2-shot prompt from MMLU testing high-school computer science. (The correct answer is (B)).

Prompting

Δεν χρειάζεται τα παραδείγματα να είναι πάρα πολλά.

Τα παραδείγματα αυτά δεν είναι εκπαίδευση, δεν προσπαθώ να εκπαιδεύσω με αυτά να απαντά πιο σωστά το ΜΜΓ.

Τα πάρα πολλά παραδείγματα προκαλούν υπερπροσαρμογή του μοντέλου σε αυτά.

Η χρήση τους είναι για να παρουσιάσουν την εργασία που θέλει ο χρήστης και το φορματ της εξόδου.

Ακόμα και παραδείγματα με λανθασμένη επισημείωση μπορεί να οδηγήσουν σε βελτιωμένη απόδοση

Example of demonstrations in a computer science question from the MMLU dataset described in Section 7.6

The following are multiple choice questions about high school computer science.

Let $x = 1$. What is $x \ll 3$ in Python 3?

(A) 1 (B) 3 (C) 8 (D) 16

Answer: C

Which is the largest asymptotically?

(A) $O(1)$ (B) $O(n)$ (C) $O(n^2)$ (D) $O(\log(n))$

Answer: C

What is the output of the statement "a" + "ab" in Python 3?

(A) Error (B) aab (C) ab (D) a ab

Answer:

Figure 7.6 Sample 2-shot prompt from MMLU testing high-school computer science. (The correct answer is (B)).

Prompting

Το prompting δεν μεταβάλλει τις παραμέτρους του ΜΜΓ (τα βάρη του δικτύου).
Αλλάζουν μόνο τα συμφραζόμενα.
Αυτό λέγεται **in-context learning**.



System Prompt

- ❑ Prompt που διαθέτουν συστημικά τα ΜΜΓ, και μπαίνει σαν σιωπηλό πρόθεμα (σαν πρώτη αφανή οδηγία) πριν από κάθε κείμενο χρήστη.
- ❑ Καθορίζει τον ρόλο, τον τόνο του ΜΜΓ
- ❑ Πχ για το CLAUDE το system prompt είναι 1700 λέξεις και ενδεικτικά περιλαμβάνει προτάσεις όπως

Claude should give concise responses to very simple questions, but provide thorough responses to complex and open-ended questions.

Claude is able to explain difficult concepts or ideas clearly. It can also illustrate its explanations with examples, thought experiments, or metaphors.

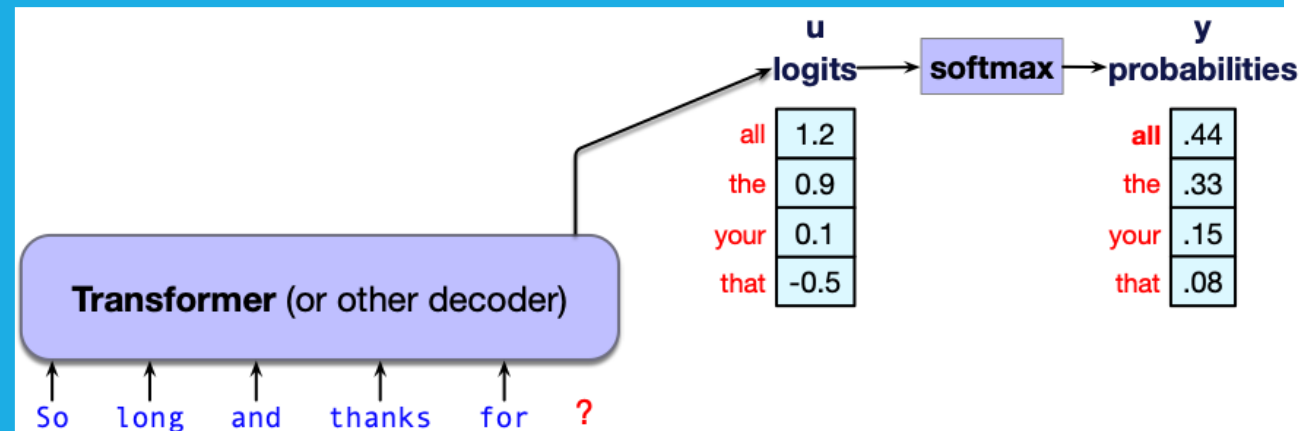
Claude does not provide information that could be used to make chemical or biological or nuclear weapons
For more casual, emotional, empathetic, or advice-driven conversations, Claude keeps its tone natural, warm, and empathetic

Claude cares about people's well-being and avoids encouraging or facilitating self-destructive behavior

If Claude provides bullet points in its response, it should use markdown, and each bullet point should be at least 1-2 sentences long unless the human requests otherwise

Δειγματοληψία

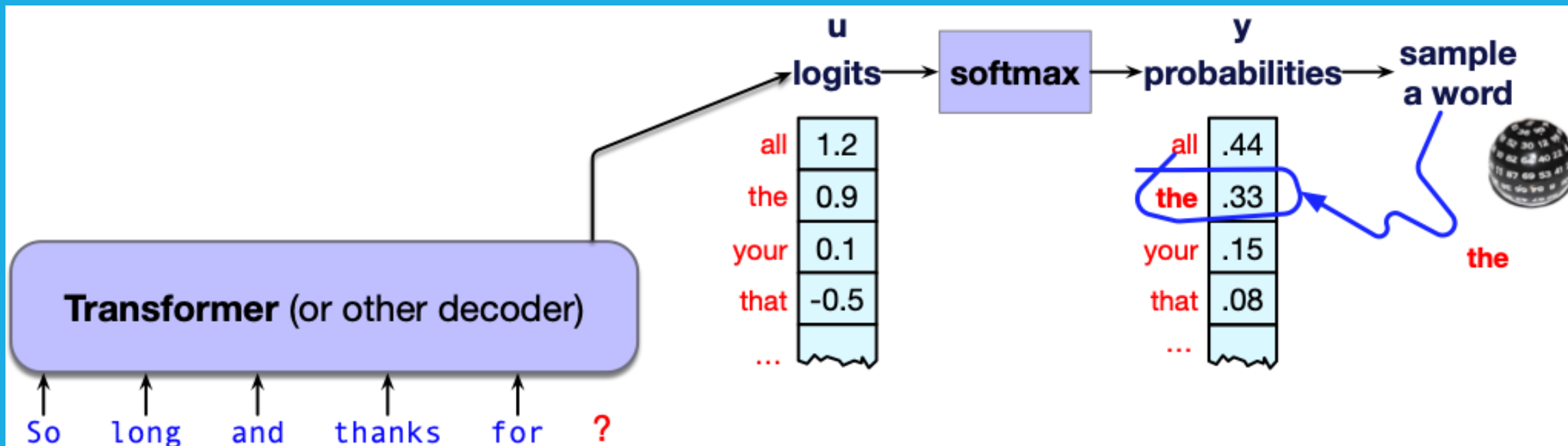
- ❑ Το δίκτυο παράγει στην έξοδο έναν πραγματικό αριθμό (**logit**) για κάθε λέξη του λεξικού
- ❑ Με τη συνάρτηση softmax οι αριθμοί αυτοί μετατρέπονται/κανονικοποιούνται σε πιθανότητες
- ❑ Έτσι έχω στην έξοδο έναν πίνακα πιθανοτήτων $1 \times V$, που δίνει σε κάθε λέξη του λεξικού πιθανότητα να είναι η επόμενη λέξη στο κείμενό μου.
- ❑ $y = \text{softmax}(u)$
- ❑ **Decoding:** Η διαδικασία επιλογής της επόμενης λέξης από την κατανομή



Greedy Decoding

- ❑ Αν κάθε φορά επιλέγω τη λέξη με την μεγαλύτερη πιθανότητα
- ❑ Δεν το χρησιμοποιώ, γιατί το αποτέλεσμα θα ήταν πολύ
 - ❑ προβλέψιμο
 - ❑ επαναλαμβανόμενο
 - ❑ σχεδόν ντετερμινιστικό
- ❑ Προτιμούμε κείμενο που είναι πιο πολυποίκιλο
- ❑ Για αυτό εφαρμόζεται τυχαία δειγματοληψία ανάλογα με την πιθανότητα του κάθε token
- ❑ Έχω μεγαλύτερη πιθανότητα να επιλέξω λέξεις που έχουν μεγαλύτερη πιθανότητα εμφάνισης σε αυτά τα συμφραζόμενα, και
- ❑ Μικρότερη πιθανότητα να επιλέξω λέξεις με μικρότερη πιθανότητα εμφάνισης

Τυχαία Δειγματοληψία



Ούτε αυτό δουλεύει πολύ καλά γιατί συχνά επιλέγονται λέξεις μικρής πιθανότητας, παράγοντας πολύ περίεργο κείμενο.

Ποιότητα vs. Ποικιλομορφία

Αν δώσω έμφαση σε λέξεις με μεγάλη πιθανότητα

- έχω ποιότητα, σωστό κείμενο, με συνοχή
- Είναι όμως βαρετό και επαναλαμβανόμενο

Αν δώσω έμφαση σε λέξεις με μεσαία πιθανότητα

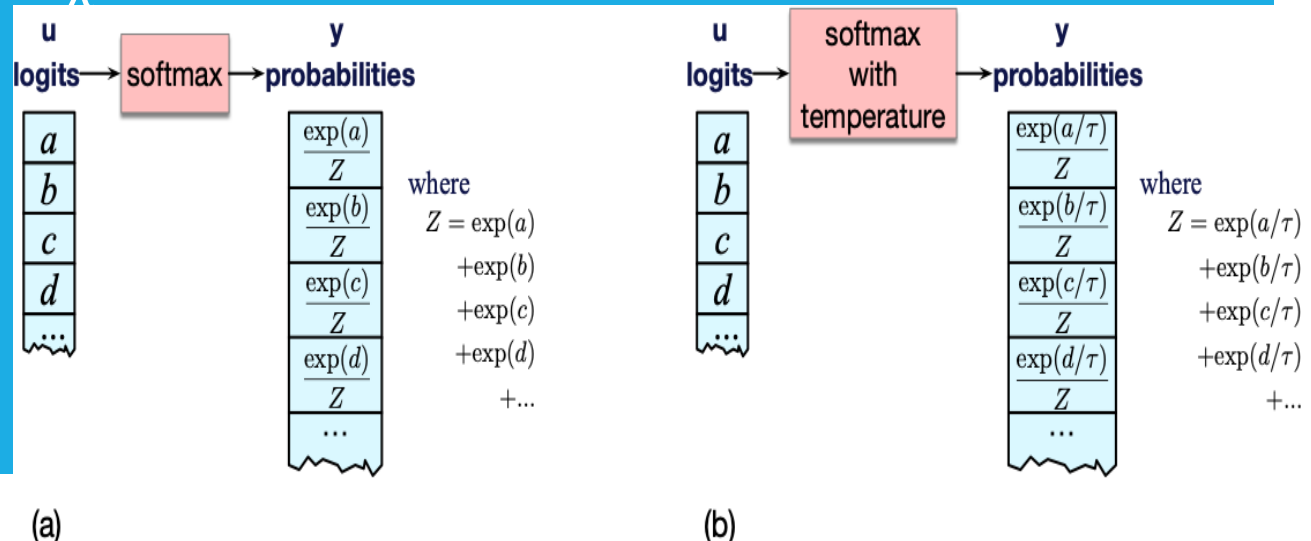
- Έχω περισσότερη ποικιλομορφία, δημιουργικότητα
- Έχω πιο περίεργο κείμενο, που δεν παρουσιάζει πολλές φορές συνοχή, δε βγάζει νόημα

Η Λύση: Temperature Sampling

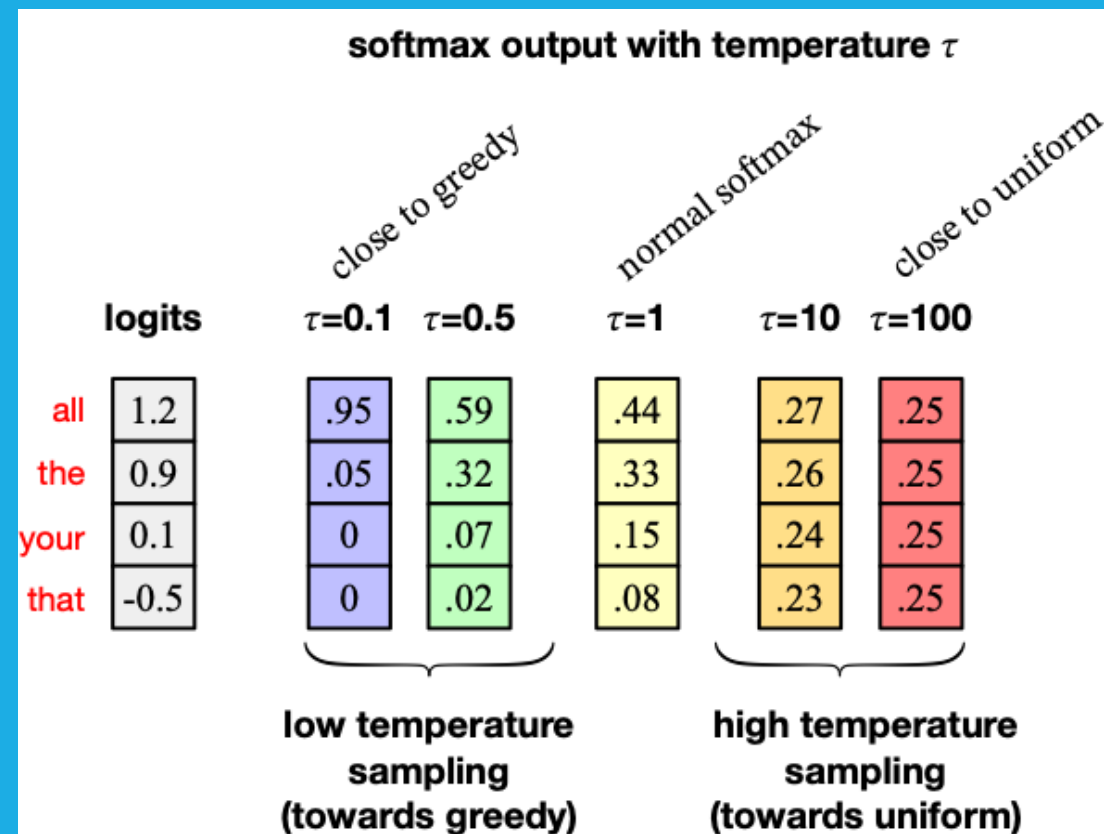
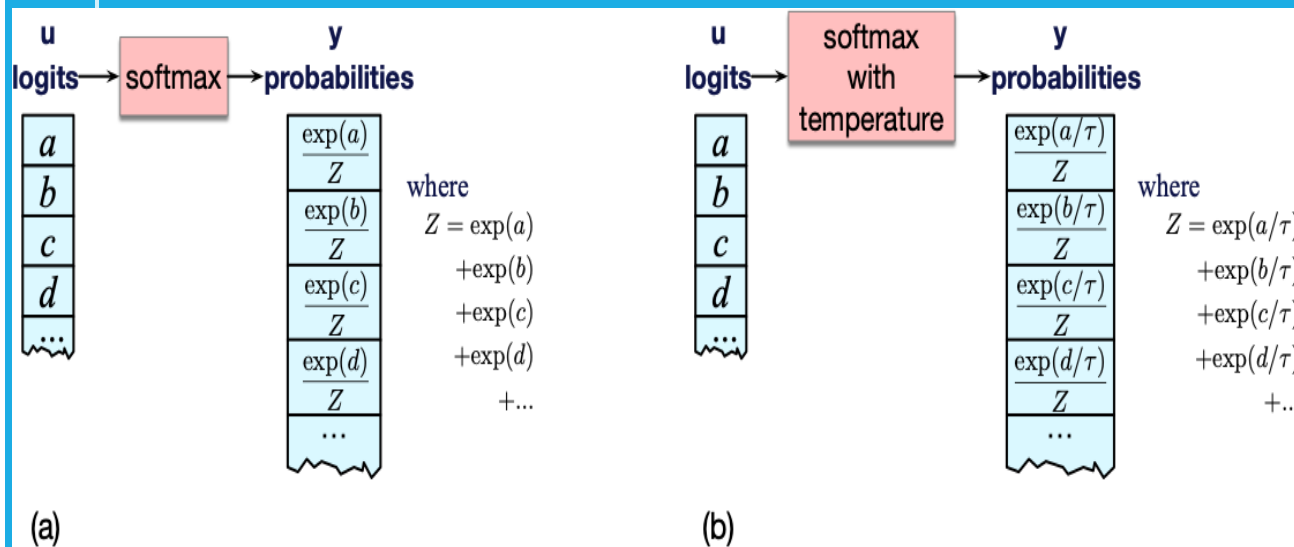
Πειράζω την κατανομή πιθανοτήτων ώστε

- οι λέξεις με μεγάλες πιθανότητες να αυξήσουν ακόμα περισσότερο την πιθανότητά τους
- Οι λέξεις με μικρές πιθανότητες να μειώσουν περισσότερο την πιθανότητά τους
- Διαιρώ κάθε logit ε μια παράμετρο θερμοκρασίας (temperature parameter) τ
- Το τ ανήκει $(0,1]$.
- Αν τ είναι κοντά στο 1, η κατανομή δεν αλλάζει πολύ.
- Όσο πιο μικρό το τ , τόσο πιο μεγάλα τα νούμερα που περνάνε στη softmax.
- Τα μεγάλα ορίσματα η softmax τα στριμώνει στο 1.
- Τα μικρά τα στριμώνει στο 0.
- Όσο πιο κοντά στο 0 είναι το τ , η πιθανότητα επιλογής της πιο πιθανής λέξης πλησιάζει το 1.

$$\mathbf{y} = \text{softmax}(\mathbf{u}/\tau)$$



Η Λύση: Temperature Sampling



Εκπαίδευση ενός MMΓ

1. Προ-εκπαίδευση (Pre-training)

Το μοντέλο εκπαιδεύεται να προβλέπει επόμενη λέξη σε τεράστια σώματα κειμένου. Χρησιμοποιεί το cross-entropy loss, το οποίο οπισθοδιαδίδεται δια μήκους όλου του δικτύου.

Τα δεδομένα εκπαίδευσης συνήθως είναι καθαρισμένα κομμάτια του κειμένου στο διαδίκτυο.

2. Προσαρμογή (fine-tuning)

Εκπαίδευση σε ένα εξειδικευμένο σώμα κειμένων, με οδηγίες και απαντήσεις.

3. Ευθυγράμμιση (Alignment)

Το μοντέλο εκπαιδεύεται σε ένα συμφραστικό περιβάλλον που συνοδεύεται από μια από δυο πιθανές καταστάσεις (continuations): Δεκτό ή Μη Αποδεκτό. Με re-inforcement learning εκπαιδεύεται να παράγει την αποδεκτή continuation και όχι την μη αποδεκτή.

Προ-εκπαίδευση ενός MMΓ

Αυτό-επίβλεψη (Self-supervised learning) : η επόμενη λέξη στο κείμενο είναι η ετικέτα!

1. Πάρε ένα σώμα κειμένου
2. Σε κάθε βήμα
 1. Το μοντέλο προβλέπει την επόμενη λέξη
 2. Το μοντέλο εκπαιδεύεται με χρήση της τεχνικής gradient descent για την ελαχιστοποίηση του σφάλματος που γίνεται .

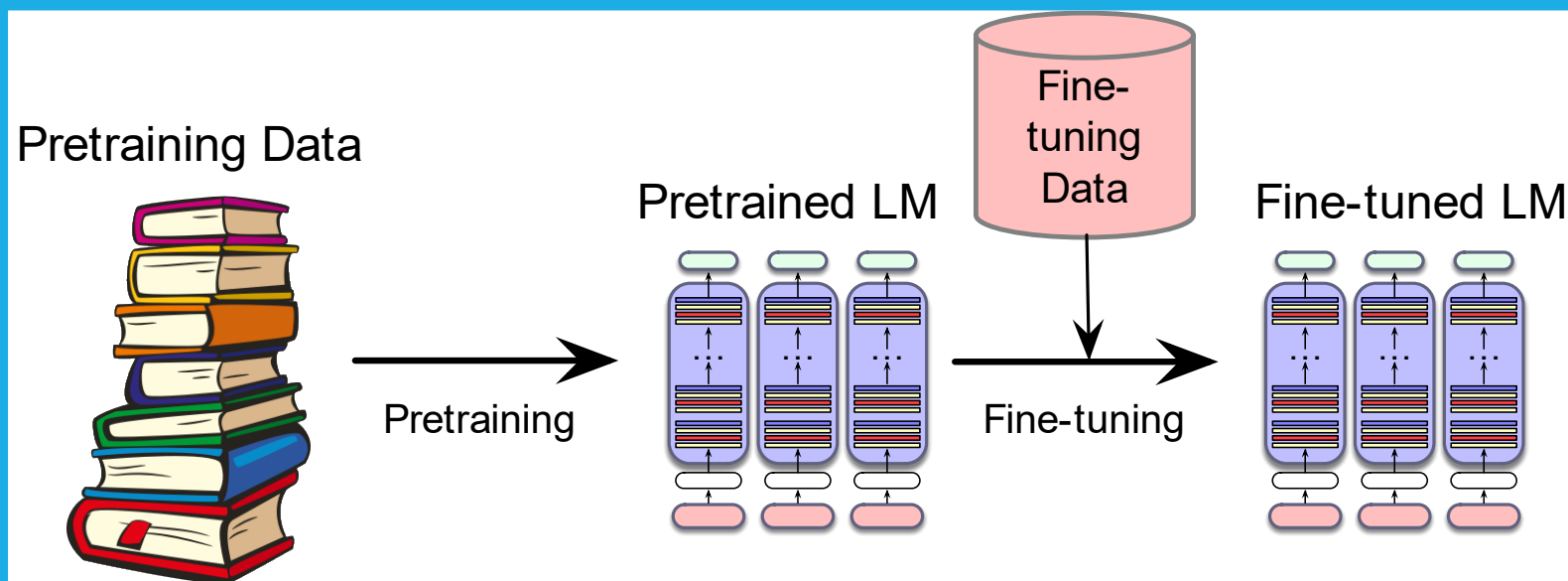
Τα σώματα κειμένων που χρησιμοποιούνται (web) έχουν θέματα

- copyright
- συναίνεσης των δημιουργών του περιεχομένου
- Πόλωσης
- ιδιωτικότητας

Προσαρμογή (Fine-Tuning) ενός ΜΜΓ

Μπορεί να χρειάζεται προσαρμογή το μοντέλο σε μια συγκεκριμένη θεματική (πχ ιατρικά κείμενα).

Συνεχίζω την εκπαίδευση του μοντέλου σε δεδομένα αυτής της θεματικής.
Προσαρμόζονται οι παράμετροι στα δεδομένα αυτά.



Αξιολόγηση ενός ΜΜΓ

1. Perplexity – για το κατά πόσο προβλέπει σωστά μια επόμενη λέξη
2. Reasoning και η γνώση του κόσμου
3. Μηχανική Μετάφραση
4. Κλπ κλπ

MMLU mathematics prompt

The following are multiple choice questions about high school mathematics.
How many numbers are in the list 25, 26, ..., 100?
(A) 75 (B) 76 (C) 22 (D) 23

Answer: B

Compute $i + i^2 + i^3 + \dots + i^{258} + i^{259}$.

(A) -1 (B) 1 (C) i (D) -i

Answer: A

If 4 daps = 7 yaps, and 5 yaps = 3 baps, how many daps equal 42 baps?
(A) 28 (B) 21 (C) 40 (D) 30

Answer:

Figure 7.16 Sample 2-shot prompt from MMLU testing high-school mathematics. (The correct answer is (C)).

Hallucinations - Θέματα Ηθικής και Ασφάλειας

- Τα ΜΜΓ συχνά λένε πράγματα που είναι ψέματα.
- Ο αλγόριθμος εκπαίδευσης φροντίζει ώστε αυτά που παράγονται να είναι γλωσσολογικά σωστά, αλλά όχι να είναι αληθή.
- Λεκτικές επιθέσεις στον χρήστη.
- Στερεοτυπική συμπεριφορά του μοντέλου
- Ιδιωτικότητα – πραγματοποιούνται πολύ προσωπικές συζητήσεις
- Τα μεγάλα μοντέλα μπορεί να διαρρεύσουν ιδιωτική πληροφορία
- Συναισθηματική εξάρτηση του χρήστη
- Μπορεί να δημιουργήσουν κακόβουλο κείμενο για προπαγάνδα, ψευδείς ειδήσεις, απάτη, τρομοκρατία
- Για αυτό πρέπει να μπορούν να δίνουν πλήρη πληροφορία των κειμένων που χρησιμοποιήθηκαν για την εκπαίδευσή τους