



Εισαγωγή στους Αλγόριθμους

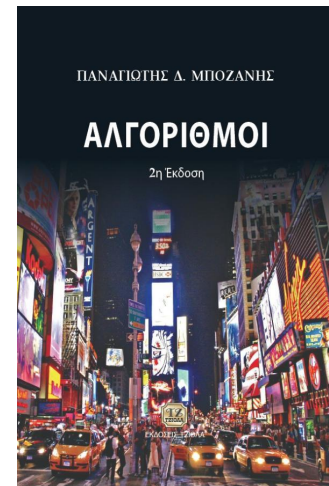
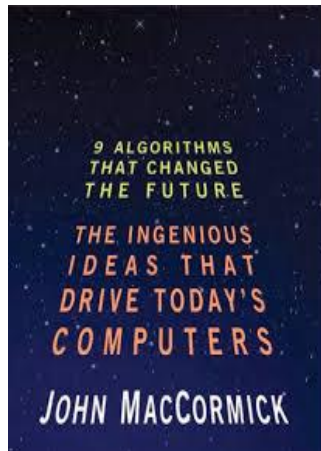
Εύη Παπαϊωάννου
papaiouan@ceid.upatras.gr
papaiouan@upatras.gr

Πότε και πού;

- Ωρολόγιο πρόγραμμα

Βιβλιογραφία (I)

- 9 ΑΛΓΟΡΙΘΜΟΙ ΠΟΥ ΑΛΛΑΞΑΝ ΤΟ ΜΕΛΛΟΝ
– John MacCormick
- ΑΛΓΟΡΙΘΜΟΙ
– Παναγιώτης Μποζάνης



Βιβλιογραφία (II)

- Διαφάνειες διαλέξεων
- Σύντομες σημειώσεις
- Δημοσιευμένες εργασίες
- Διαδίκτυο
- [Δικτυακός τόπος μαθημάτων μου](#)

Περί τίνος πρόκειται;

- Εισαγωγή
 - Βασικά χαρακτηριστικά, όχι εξαιρετικά δύσκολα ή πολύπλοκα με στόχο την εξοικείωση και την κατανόηση θεμελιωδών και πρακτικά χρήσιμων εννοιών
- Αλγόριθμος
 - Ακολουθία βημάτων για να κάνω μια δουλειά
 - Ακριβής συνταγή που καθορίζει την ακριβή ακολουθία βημάτων που απαιτούνται για να λυθεί ένα πρόβλημα

Muḥammad ibn Mūsā al-Khwārizmī (780–850)



Με απλά λόγια...

Φανταστείτε ότι ξυπνάτε το πρωί, φτιάχνετε καφέ, παίρνετε το κινητό και κάθεστε μπροστά στο laptop...

- Ανοίγετε το google και ψάχνετε τα εφημερεύοντα φαρμακεία γιατί θέλετε να πάρετε μια κρέμα σώματος σε προσφορά,
 - στέλνετε (με ενεργοποιημένο το T9) ένα sms σε φίλο/φίλη για την προσφορά,
 - στη συνέχεια πληρώνετε με internet banking ένα λογαριασμό ΔΕΗ που είχατε ξεχάσει
 - και τυπώνετε σε pdf τη σχετική απόδειξη
 - (χτες εγκαταστήσατε τον Acrobat professional: καλή ευκαιρία να το δοκιμάσετε)
 - την οποία αποθηκεύετε στο δίσκο σας και για κάθε ενδεχόμενο,
 - συμπιέζετε και
 - στέλνετε το αρχείο με ένα email στον προσωπικό σας λογαριασμό στο gmail που έχει αρκετό χώρο...
 - Ανοίγετε το Facebook να δείτε τι posts έκαναν οι «φίλοι» σας χτες...
 - Μετά ρίχνετε και μια ματιά στο site του Τμήματος για να δείτε το πρόγραμμα της εξεταστικής και σας πιάνουν τα νεύρα γιατί δε σας βολεύει και αναφωνείτε: μα καλά τόσο χαζοί είναι; ούτε ένα πρόγραμμα της προκοπής δε μπορούν να φτιάξουν?? Ας το έδιναν σε υπολογιστή να το φτιάξει καλά που θα το έκανε σίγουρα... (θα το έκανε, αλήθεια;;;;)
- Για να είστε σε θέση να θεωρείτε όλα τα παραπάνω δεδομένα και, πλέον, απλή καθημερινότητα, χρειάστηκαν πολλά χρόνια και πολλή μελέτη και κυρίως πολύ έξυπνες ιδέες (δηλ., αλγόριθμοι)... ικανές να αξιοποιήσουν την τεχνολογική πρόοδο...
 - Με τους αλγόριθμους αυτούς θα ασχοληθούμε στο συγκεκριμένο μάθημα...

Με απλά λόγια...

Φανταστείτε ότι ξυπνάτε το πρωί, φτιάχνετε καφέ, παίρνετε το κινητό και κάθεστε μπροστά στο laptop...

- Ανοίγετε το google και ψάχνετε τα εφημερεύοντα φαρμακεία γιατί θέλετε να πάρετε μια κρέμα σώματος σε προσφορά, [**ΑΛΓΟΡΙΘΜΟΣ PAGERANK**]
 - στέλνετε (με ενεργοποιημένο το T9) ένα sms σε φίλο/φίλη για την προσφορά, [**ΑΛΓΟΡΙΘΜΟΙ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΤΥΠΩΝ**]
 - στη συνέχεια πληρώνετε με internet banking ένα λογαριασμό ΔΕΗ που είχατε ξεχάσει [**ΑΛΓΟΡΙΘΜΟΣ ΡΚΚ**]
 - και τυπώνετε σε pdf τη σχετική απόδειξη
 - (χτες εγκαταστήσατε τον Acrobat professional: καλή ευκαιρία να το δοκιμάσετε) [**ΑΛΓΟΡΙΘΜΟΙ ΓΙΑ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ**]
 - την οποία αποθηκεύετε στο δίσκο σας και για κάθε ενδεχόμενο, [**ΚΩΔΙΚΕΣ ΔΙΟΡΘΩΣΗΣ ΣΦΑΛΜΑΤΩΝ**]
 - συμπιέζετε και [**ΚΩΔΙΚΕΣ ΔΙΟΡΘΩΣΗΣ ΣΦΑΛΜΑΤΩΝ**]
 - στέλνετε το αρχείο με ένα email στον προσωπικό σας λογαριασμό στο gmail που έχει αρκετό χώρο... [**ΚΩΔΙΚΕΣ ΔΙΟΡΘΩΣΗΣ ΣΦΑΛΜΑΤΩΝ, ΑΛΓΟΡΙΘΜΟΙ ΣΥΜΠΙΕΣΗΣ, ΑΛΓΟΡΙΘΜΟΙ ΔΙΑΧΕΙΡΙΣΗΣ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ**]
 - Ανοίγετε το Facebook να δείτε τι posts έκαναν οι «φίλοι» σας χτες... [**ΑΛΓΟΡΙΘΜΟΙ ΔΙΑΧΕΙΡΙΣΗΣ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ**]
 - Μετά ρίχνετε και μια ματιά στο site του Τμήματος για να δείτε το πρόγραμμα της εξεταστικής και σας πιάνουν τα νεύρα γιατί δε σας βολεύει και αναφωνείτε: μα καλά τόσο χαζοί είναι; ούτε ένα πρόγραμμα της προκοπής δε μπορούν να φτιάξουν?? Ας το έδιναν σε υπολογιστή να το φτιάξει καλά που θα το έκανε σίγουρα... (θα το έκανε, αλήθεια;;;;) [**ΘΕΣΗ ΤΩΝ CHURCH-TURING**]
- Για να είστε σε θέση να θεωρείτε όλα τα παραπάνω δεδομένα και, πλέον, απλή καθημερινότητα, χρειάστηκαν πολλά χρόνια και πολλή μελέτη και κυρίως πολύ έξυπνες ιδέες (δηλ., αλγόριθμοι)... ικανές να αξιοποιήσουν την τεχνολογική πρόοδο...
 - Με τους αλγόριθμους αυτούς θα ασχοληθούμε στο συγκεκριμένο μάθημα...

Εξέλιξη μαθήματος

- Περιγραφή και ανάλυση θεμελιωδών τεχνικών (δηλ., αλγορίθμων) που τις συναντάμε – σχεδόν χωρίς να το αντιλαμβανόμαστε – καθημερινά στη ζωή και τις δραστηριότητες μας...
- Μελέτη πιο τυπικών ζητημάτων, όπως:
 - ορθότητα και απόδοση αλγορίθμων (αν λειτουργούν σωστά και με τι κόστος σε χρόνο, χώρο κτλ)
 - κατηγορίες αλγορίθμων
 - παρουσίαση τεχνικών σχεδιασμού αλγορίθμων: αναδρομή, εξαντλητική αναζήτηση, αναγωγή
- Παρουσίαση και ανάλυση θεμελιωδών αλγορίθμων

Ημερολόγιο μαθήματος

- Εισαγωγή
- Ο αλγόριθμος PageRank
 - Ασυμπτωτική ανάλυση, Πρόσθεση
- Ο αλγόριθμος Diffie-Hellman
- **1η ενδιάμεση εξέταση**
- Κώδικες διόρθωσης σφαλμάτων
 - Πολλαπλασιασμός
- Αλγόριθμοι συμπίεσης δεδομένων
 - Διάσχιση Γραφημάτων
- Αλγόριθμοι αναγνώρισης προτύπων
- **2η ενδιάμεση εξέταση**
- Αλγόριθμοι διαχείρισης βάσεων δεδομένων
 - Εύρεση ελάχιστων μονοπατιών, Κατηγορίες αλγορίθμων
- Ψηφιακές υπογραφές
 - Εύρεση Μέγιστου Κοινού Διαιρέτη
- Όρια υπολογισμού
 - Δυαδική αναζήτηση, Ταξινόμηση με συγχώνευση
- **Τελική εξέταση**



40%



60%

Έχει τύχει ...

- ψάχνοντας π.χ., στο Google, να επιλέξετε από εκατομμύρια έγγραφα **2 ή 3 που είναι σχετικότερα** με αυτό που ψάχνετε;
- να έχετε αποθηκεύσει ή μεταδώσει πολλά εκατομμύρια τμημάτων πληροφορίας **χωρίς να γίνει ούτε ένα λαθάκι** – παρά τις ηλεκτρομαγνητικές παρεμβολές που επηρεάζουν όλες τις ηλεκτρονικές συσκευές;
- να **ολοκληρώσατε επιτυχώς μια ηλεκτρονική συναλλαγή**, ακόμα κι αν πολλές χιλιάδες άλλων πελατών χρησιμοποιούσαν συνεχώς τον ίδιο εξυπηρετητή (server);
- να **στείλετε κάποια απόρρητη πληροφορία** (για παράδειγμα, τον αριθμό της πιστωτικής σας κάρτας) ασφαλώς πάνω από καλώδια που επιτρέπουν υποκλοπές από δεκάδες άλλους υπολογιστές;
- να **χρησιμοποιήσατε συμπίεση** για να μειώσετε τα πολλά MB μιας εικόνας σε κάποιο περισσότερο διαχειρίσιμο μέγεθος για την επισυνάψετε και να την στείλετε με e-mail;
- ή – χωρίς ίσως καν να το σκεφτείτε – να **χρησιμοποιήσατε τεχνητή νοημοσύνη σε κάποια φορητή συσκευή** (π.χ., κινητό τηλέφωνο) που διορθώνει από μόνη της το κείμενο που πληκτρολογείτε στο μικροσκοπικό της πληκτρολόγιο;

Τι θα μελετήσουμε;

- Τον αλγόριθμο που χρησιμοποιεί η Google για να εξασφαλίσει ότι τα πιο σχετικά έγγραφα βρίσκονται στην κορυφή των αποτελεσμάτων αναζήτησης

Τι θα μελετήσουμε;

- Τον αλγόριθμο Κρυπτογράφησης με χρήση Δημοσίου Κλειδιού (Public Key Cryptography - PKC)
 - Κάθε φορά που επισκέπτεσθε έναν ιστότοπο του οποίου η διεύθυνση ξεκινάει με https αντί για http, πρέπει να χρησιμοποιήσετε τη διαδικασία της Κρυπτογράφησης με χρήση Δημοσίου Κλειδιού μέσω της οποίας με ανταλλαγή ενός κλειδιού εγγυάται την εγκαθίδρυση ασφαλούς σύνδεσης

Τι θα μελετήσουμε;

- Αλγόριθμους/Κώδικες διόρθωσης σφαλμάτων
 - Οι κώδικες αυτοί υπάρχουν παντού:
χρησιμοποιούνται σε όλους τους σκληρούς δίσκους, στις μεταδόσεις μέσω δικτύων, σε CDs και DVDs, ακόμα και στις μνήμες των υπολογιστών χωρίς συνήθως να αντιλαμβανόμαστε καν την ύπαρξή τους...

Τι θα μελετήσουμε;

- Αλγόριθμους αναγνώρισης προτύπων (nearest-neighbor classifiers, decision trees, and neural networks)
 - Η αναγνώριση προτύπων συνίσταται σε μια πολύ πρόσφατη (21^{ος} αιώνας) κλάση τεχνικών μέσω των οποίων οι υπολογιστές αναγνωρίζουν πληροφορία όπως γραφικό χαρακτήρα, λόγο και πρόσωπα
 - Κινητές συσκευές με μικροσκοπικά πληκτρολόγια πάνω σε οθόνες χρησιμοποιούν αυτόματη διόρθωση
 - Γράφουμε με το χέρι σε συσκευές τύπου tablet και αυτές αναγνωρίζουν τα χειρόγραφα
 - Τέτοιες συσκευές, ειδικά τα smartphones ενεργοποιούνται πλέον και φωνητικά
 - websites χρησιμοποιούν αναγνώριση προτύπων για να καθορίσουν το είδος διαφημίσεις να εμφανίσουν σε κάθε χρήστη

Τι θα μελετήσουμε;

- Αλγόριθμους συμπίεσης
 - Χρησιμοποιούμε συμπίεση πολύ συχνά π.χ., για να κερδίσουμε αποθηκευτικό χώρο ή να μειώσουμε το μέγεθος μιας εικόνας πριν τη στείλουμε με e-mail...
 - Χωρίς να το αντιλαμβανόμαστε, συμπίεση χρησιμοποιείται:
 - όταν κατεβάζουμε (download) ή ανεβάζουμε (upload) πληροφορία στο διαδίκτυο για να «σωθεί» εύρος ζώνης
 - από κέντρα παροχής δεδομένων σε πελάτες για μείωση κόστους
 - Παρατηρήστε ότι τα π.χ., 5 GB χώρου που μας δίνουν πάροχοι λογαριασμών email (gmail, hotmail, yahoo, κτλ) αντιστοιχούν στην πραγματικότητα στα δικά τους συστήματα σε χώρο πολύ μικρότερο από 5 GB!!!

Τι θα μελετήσουμε;

- Αλγόριθμους για ψηφιακές υπογραφές
 - Είναι τεχνικές που διασφαλίζουν ότι είναι δυνατόν να υπογράψουμε έγγραφα με ηλεκτρονικό τρόπο χωρίς να κινδυνεύουμε να παραποιηθεί (πλαστογραφηθεί) η ψηφιακή μας υπογραφή

Τι θα μελετήσουμε;

- Αλγόριθμους για διαχείριση βάσεων δεδομένων
 - Είναι τεχνικές που χρησιμοποιούνται για να διασφαλίσουν τη συνέπεια σε βάσεις δεδομένων
 - Χωρίς αυτές δε θα ήταν δυνατές online αγορές ούτε αλληλεπίδραση στα πλαίσια κοινωνικών δικτύων όπως το Facebook

Τι θα μελετήσουμε;

- Δε θα περιγράψουμε κάποιον άλλο υπαρκτό αλγόριθμο αλλά θα μάθουμε για έναν αλγόριθμο που θα ήταν εξαιρετικό ΑΝ ΥΠΗΡΧΕ
- Θα δούμε ότι ο αλγόριθμος αυτός ΔΕΝ ΜΠΟΡΕΙ ΝΑ ΥΠΑΡΞΕΙ...
- Επομένως, υπάρχουν ΟΡΙΑ στα προβλήματα που μπορούν να «λύνουν» οι υπολογιστές και θα συζητήσουμε τι αυτό συνεπάγεται από φιλοσοφική και βιολογική πλευρά...

Βαθμολόγηση

- (Α) 2 ενδιάμεσες εξετάσεις σε υπολογιστή με 10 ερωτήσεις πολλαπλής επιλογής – συνεισφέρουν την τελική βαθμολογία σε ποσοστό 40%
- (Β) Τελική εξέταση σε υπολογιστή με 15 ερωτήσεις πολλαπλής επιλογής – συνεισφέρει στην τελική βαθμολογία σε ποσοστό 60%
 - βασίζεται σε σύνολο ερωτήσεων που θα ανακοινωθούν μετά το τέλος των διαλέξεων και καλύπτουν ό,τι έχουμε συζητήσει στην τάξη
- Μη συμμετοχή στις ενδιάμεσες εξετάσεις ΔΕΝ συνεπάγεται αποκλεισμό από την τελική εξέταση
- Η φυσική παρουσία ΔΕΝ είναι υποχρεωτική ... αλλά είναι ιδιαίτερα ευπρόσδεκτη!! 😊

Τι μας χρειάζονται οι αλγόριθμοι;

- Οι αλγόριθμοι χρησιμοποιούνται καθημερινά σε ό,τι κι αν κάνουμε
 - Πάντα μηχανεύομαστε τρόπους για να αντιμετωπίζουμε προβλήματα που λύνονται...

Υπάρχουν προβλήματα που «δε λύνονται»;

- ΝΑΙ!! Υπάρχουν προβλήματα που δεν λύνονται, δηλ. δεν μπορούμε να επινοήσουμε σχετικό αλγόριθμο
 - Π.χ., κανένας αλγόριθμος δεν μπορεί να ελέγξει αν ένα πολυώνυμο έχει ακέραιες ρίζες (10^ο πρόβλημα του Hilbert)



Hilbert;;; 10^ο πρόβλημα;;;

- 1900: ο Γερμανός μαθηματικός David Hilbert σε διάλεξή του στο Διεθνές Συνέδριο Μαθηματικών στο Παρίσι απαρίθμησε 23 μαθηματικά προβλήματα την επίλυση των οποίων πρότεινε σα στόχο για τον επόμενο αιώνα
- Το 10^ο πρόβλημα στον κατάλογο αυτό αφορούσε στους αλγόριθμους: να επινοηθεί αλγόριθμος που να ελέγχει αν κάποιο πολυώνυμο έχει ακέραια ρίζα
 - *«Να επινοηθεί διαδικασία σύμφωνα με την οποία να μπορεί να διαπιστωθεί με πεπερασμένο πλήθος πράξεων αν ένα πολυώνυμο έχει ακέραια ρίζα»*
- 1970: Yuri Matijasevic (Γιούρι Ματίζεβιτς) απέδειξε ότι κανένας αλγόριθμος δεν μπορεί να ελέγξει αν ένα πολυώνυμο έχει ακέραιες ρίζες

Πολυώνυμα...; Ρίζες...;

- Πολυώνυμο: άθροισμα όρων
 - Κάθε όρος είναι γινόμενο μεταβλητών και μιας σταθεράς που λέγεται συντελεστής
 - $6 \cdot x \cdot x \cdot x \cdot y \cdot z \cdot z = 6x^3yz^2$
 - $6x^3yz^2 + 3xy^2 - x^3 - 10$
- “ Ρίζα ενός πολυωνύμου είναι ένας συνδυασμός τιμών στις μεταβλητές του ώστε το πολυώνυμο να έχει τιμή 0
 - Το παραπάνω πολυώνυμο έχει ρίζα: $x=5, y=3, z=0$

Από τα προβλήματα που λύνονται...

- Κάποια είναι εύκολα, δηλ., μπορούμε να επινοήσουμε αλγόριθμο που να βρίσκει λύση τους «γρήγορα»
 - Π.χ., βρες το άθροισμα δύο ακεραίων αριθμών
- Αλλά υπάρχουν προβλήματα που είναι δύσκολα, δηλ., ο μόνος τρόπος να βρω τη λύση τους είναι να ψάξω μία-μία όλες τις πιθανές λύσεις
 - Π.χ., κάλυψη συνόλων (set cover)
 - Δίνεται σύνολο $U = \{1, 2, \dots, m\}$ και σύνολο S από n σύνολα η ένωση των οποίων δίνει το U
 - Το πρόβλημα κάλυψης συνόλων ζητά τον προσδιορισμό του μικρότερου υποσυνόλου του S του οποίου η ένωση δίνει το U
 - $U = \{1, 2, 3, 4, 5\}$
 - $S = \{\{1, 2, 3\}, \{2, 4\}, \{3, 4\}, \{4, 5\}\}$ – Η ένωση των στοιχείων του S δίνει το U
 - Το U καλύπτεται από το υποσύνολο $\{\{1, 2, 3\}, \{4, 5\}\}$ του S

Ποια είναι η χρησιμότητα του μαθήματος;

- Πίσω από κάθε μεγάλο τεχνολογικό επίτευγμα, υπάρχει μια (συνήθως) απλή ιδέα:
 - μαθαίνετε και κατανοείτε τις ιδέες πίσω από σημαντικά τεχνολογικά επιτεύγματα τα οποία χρησιμοποιείτε καθημερινά και θα κληθείτε να τα χρησιμοποιήσετε και σαν εργαλεία για τη δουλειά σας
 - κατανοώντας τη λειτουργία ενός τεχνολογικού επιτεύγματος (π.χ. συσκευής/υπηρεσίας/λύσης) μπορείτε να το προσαρμόσετε στις ανάγκες σας ή να το βελτιώσετε
 - αντιλαμβάνεστε ευκολότερα τι είναι εφικτό και τι όχι...
 - αν σας δώσουν μια μακροσκελή λίστα με τα μουσεία της Ελλάδας και τις αποστάσεις μεταξύ τους και σας ζητήσουν να υπολογίσετε **γρήγορα** τη συντομότερη δυνατή διαδρομή ώστε να περάσετε ακριβώς μία φορά από καθένα και να επιστρέψετε στην αφετηρία συμπεραίνετε ότι ή δεν ξέρουν τι τους γίνεται ή σας κοροϊδεύουν...

Ποια είναι η χρησιμότητα του μαθήματος;

- Για να επινοήσω λύση για κάποιο πρόβλημα πρέπει:
 - Να κατανοήσω τα δεδομένα και τα ζητούμενα
 - Να ξεκαθαρίσω ποιοι είναι οι πόροι που έχω στη διάθεσή μου
 - Να επινοήσω μια ιδέα ώστε ξεκινώντας από τα δεδομένα, να χρησιμοποιήσω τους πόρους ώστε να φτάσω στο ζητούμενο ή ίσως σε κάτι κοντά στο ζητούμενο ή να αποφανθώ ότι δεν μπορώ να βρω λύση...
- Η διαδικασία αυτή – του να **μαθαίνουμε να ΣΚΕΦΤΟΜΑΣΤΕ** - ΠΡΟΦΑΝΩΣ έχει γενική χρησιμότητα ανεξάρτητα από την επιμέρους περιοχή στην οποία εφαρμόζεται

Ποια είναι η χρησιμότητα του μαθήματος;

- Μέρος της δουλειά σας είναι να εφαρμόζετε υπάρχουσες λύσεις αποδοτικά ή/και να επινοείτε νέες λύσεις και να δείχνετε ότι δουλεύουν «καλά»... \Leftrightarrow δηλ. να σχεδιάζετε και να αναλύετε αλγόριθμους...
 - Πώς να οργανώσω επισκέψεις σε αρχαιολογικούς χώρους;
 - Πώς να χρονοπρογραμματίσω τη χρήση ενός εκθεσιακού χώρου;
 - Πώς να κατανείμω κονδύλια σε σύνολο πολιτισμικών δραστηριοτήτων;
 - Πώς να «στήσω» ένα ασύρματο δίκτυο σε ένα πολιτιστικό χώρο;
 - Πώς να αναλύσω ένα κείμενο για να εντοπίσω γλωσσικές επιδράσεις;
 - Πώς να αναλύσω μια έκρυθμη κατάσταση μεταξύ κρατών ώστε να αποφευχθεί ένας πόλεμος;
 - Πώς να αντιμετωπίσω τη μετακίνηση πληθυσμών ώστε να μετατραπεί σε αποδοτική συνύπαρξη διαφορετικών πολιτισμών και όχι σε πηγή συγκρούσεων και οπισθοδρόμησης;

...και γενικότερα:

LEARN \Rightarrow EARN

