Εθνικο Μετσοβειο Πολυτεχνειο

Δ.Π.Μ.Σ.:
ΕΦΑΡΜΟΣΜΕΝΕΣ ΜΑΘΗΜΑΤΙΚΕΣ
ΕΠΙΣΤΗΜΕΣ

Διπλωματική Εργασία:

Πολυπλοκότητα Kolmogorov και Αλγοριθμική Τυχαιότητα.

Τηνιακουδάκης Αντώνης

Επιβλέπων Καθηγητής: Αρβανιτάκης Αλέξανδρος.

Ιούνιος 2019

Περιεχόμενα

Περίληψη

Στην συγκεκριμένη εργασία παρουσιάζουμε τις κεντρικές ιδέες της πολυπλοκότητας Kolmogorov ή αλγοριθμικής πολυπλοκότητας, όπως είναι επίσης γνωστή, και πως αυτή σχετίζεται με την έννοια του τυχαίου. Αρχικά, μετά από κάποιες απαραίτητες έννοιες της θεωρίας υπολογισιμότητας, ορίζουμε την απλή πολυπλοκότητα Kolmogorov $C(x)$, μιας πεπερασμένης δυαδικής ακολουθίας (λέξης) $x \in \{0,1\}^{<\mathbb{N}}$ και αποδεικνύουμε ιδιότητες της συνάρτησης πολυπλοκότητας C, τόσο παρέχοντας κάποια φράγματά της όσο και ιδιότητες σχετικά με την υπολογισιμότητα της C. Έπειτα ορίζουμε την προθεματική πολυπλοκότητα $K(x)$ μιας λέξης x, με βάση τις prefix free συναρτήσεις, και κύριοι στόχοι μας είναι οι εξής δύο: πρώτον να μελετήσουμε το πως συνδέεται η K με τα (διακριτά) ημιυπολογίσιμα (ημι)μέτρα αλλά και δεύτερον πως συνδέεται με την έννοια της Martin Löf τυχαίοτητας για τα στοιχεία του $\{0,1\}^{\mathbb{N}}$. Για να πετύχουμε τον πρώτο, βασίζομαστε στην ύπαρξη ενός ημιυπολογίσιμου μέτρου m στο $\mathbb{N}$, το οποίο έχει την εξής ιδιότητα, αν p είναι ένα οποιοδήποτε ημιυπολογίσιμο μέτρο στο $\mathbb{N}$, τότε υπάρχει σταθερά c_p, τέτοια ώστε $c_p m(i) \geq p(i)$, για κάθε $i \in \mathbb{N}$. Ενώ για τον δεύτερο στόχος μας, καταλήγουμε ουσιαστικά σε μια ικανή και αναγκαία συνθήκη τυχαιότητας για ένα $\omega = \omega_0\omega_1 \cdots \in \{0,1\}^{\mathbb{N}}$ ως προς κάποιο υπολογίσιμο μέτρο μ στον $\{0,1\}^{\mathbb{N}}$, η οποία εμπεριέχει την συμπεριφορά της $K(\omega_0\omega_1 \ldots \omega_{n-1})$ σε σχέση με το μέτρο μ.

Abstract

In this thesis we present the basic ideas behind Kolmogorov complexity or algorithmic complexity, as it is also known, and the way that it is connected with the notion of randomness. Initially, after some necessary concepts from computability theory, we define the Kolmogorov complexity $C(x)$, of a finite binary sequence (string) $x \in \{0,1\}^{<\mathbb{N}}$ and we proove some properties of the complexity function C, providing some boundaries and some properties

concerning the computability of C. Next we define the prefix complexity $K(x)$ of a string x based on prefix free functions, and we set our two main goals: first, to study the way that K connects with (discrete) semicomputable (semi)measures and second how it connects with the notion of Martin-Löf randomness for the elements of $\{0,1\}^{\mathbb{N}}$. In order to achieve our first goal, we rest upon the existence of a semicomputable measure m on $\mathbb{N}$ with the following property, for every other semicomputable measure p on $\mathbb{N}$, there exists a constant c_p such that $c_p m(i) \geq p(i)$, for all $i \in \mathbb{N}$. Regarding our second goal, we end up in a necessary and sufficient condition of randomness of an $\omega = \omega_0\omega_1 \cdots \in \{0,1\}^{\mathbb{N}}$ with respect to a given computable measure μ on $\{0,1\}^{\mathbb{N}}$, involving the behaviour of $K(\omega_0\omega_1 \ldots \omega_{n-1})$ compared with the measure μ.

Πρόλογος-Εισαγωγή

Η έννοια της αλγοριθμικής πολυπλοκότητας ενός αντικειμένου εμφανίζεται για πρώτη φορά γύρω στο 1965, από τον A.N. Kolmogorov. Διαισθητικά θα μπορούσαμε να εξηγήσουμε σύντομα την κεντρική της ιδέα ως εξής. Κάθε αντικείμενο φέρει μια ποσότητα πληροφορίας, η οποία είναι άμεσα συνδεδεμένη με το πόσο εύκολο είναι να περιγράψουμε το συγκεκριμένο αντικείμενο, υπό την έννοια ότι ένα αντικείμενο το οποίο φέρει μικρή πόσοτητα πληροφορίας είναι εύκολο να περιγράφει, ενώ για αντικείμενα τα οποία εμπεριέχουν μεγάλη ποσότητα πληροφορίας ισχύει συνήθως το αντίθετο.

Ένα καλό μέτρο πολυπλοκότητας θα ήταν λοιπόν, το μέγεθος της συντομότερης περιγραφής ενός αντικειμένου. Για να είναι όμως η συγκεκριμένη θεωρία συνεπής και να μην καταλήγει σε αντιφατικά συμπεράσματα θα πρέπει να ορίσουμε ακριβώς τι εννοούμε περιγραφή ενός αντικειμένου. Ενα παράδειγμα για να πειστεί κανείς οτι κάτι τέτοιο είναι αναγκαίο είναι το παράδοξο του Berry, " ο μικρότερος φυσικός αριθμός ο οποίος δεν περιγράφεται με λιγότερες από δεκαπέντε λέξεις ". Παρατηρήστε ότι ενώ ο συγκεκριμένος αριθμός δεν περιγάφεται με λιγότερες από δεκαπέντε λέξεις, με βάση την παραπάνω φράση, μόλις τον περιγράψαμε με δεκατρείς. Για να αποφύγει τέτοιου είδους ζητήματα, ο Kolmogorov όρισε ως πολυπλοκότητα ενός αντικείμενου, το μήκος του μικρότερου προγράμματος το οποίο επιστρέφει το εν λόγω αντικείμενο και τερματίζει.

Για τον λόγο αυτό, απαραίτητο συστατικό της αλγοριθμικής πολυπλοκότητας αποτελεί η έννοια της υπολογισιμότητας, η οποία είχε θεμελιωθεί ήδη, με διάφορα θεωρητικά υπολογιστικά μοντέλα από τους A. Church, S. Kleene και A. Turing την δεκαετία του 1930.

Για να γίνουν πιο κατανοητά τα παραπάνω παραθέτουμε το εξής παράδειγμα. Θεωρήστε μια ακολουθία, η οποία αποτελείται από 1000 μηδενικά, τότε το πρόγραμμα {for $i = 1$ to 1000, print 0.} επιστρέφει την ακολουθία μας και χρησιμοποιεί περίπου $\log_2 1000 \simeq 10$ bits. Ο λόγος που χρησιμοποιήσαμε σαν αντικείμενο μια δυαδική ακολουθία είναι προφανής, στην εποχή μας οποιαδήποτε μορφή πληροφορίας μπορεί να κωδικοποιηθεί με μια ακολουθία από 0 και 1, ώστε να επεξεργαστεί από έναν ηλεκτρονικό υπολογιστή. Ένα πιο ενδιαφέρον παράδειγμα είναι ο αριθμός, $\pi = 3.141519....$ Επειδή δεν υπάρχει κάποιο μο-

τίβο στον τρόπο με τον οποίο εμφανίζονται και κατανέμονται τα ψηφία του, θα φαντάζοταν κανείς ότι θα πρέπει να έχει μεγάλη πολυπλοκότητα, παρ᾽ όλα αυτά υπάρχουν σύντομα προγράμματα τα οποία μας επιστρέφουν οποιοδήποτε αρχικό τμήμα της άπειρης ακολουθίας των ψηφίων του.

Όσον αφόρα την παρούσα εργασία, σκοπός μας είναι να παρουσιάσουμε τις παραπάνω ιδεές, και να μελετήσουμε τις ιδίοτητες της συνάρτησης πολυπλοκότητας αλλά και το πως αυτή συνδέεται με άλλες έννοιες όπως για παράδειγμα της τυχαιότητας, ή μη προβλεψιμότητας ενός αντικειμένου. Πιο συγκεκριμένα, στο πρώτο κεφάλαιο κάνουμε μια πολύ σύντομη αναφορά στη θεωρία αναδρομής, παρουσιάζοντας έννοιες οι οποίες θα μας είναι απαραίτητες για την ανάπτυξη των προηγούμενων ιδεών, όπως τι είναι οι αναδρομικές συνάρτησεις και τι αντιπροσωπεύουν ουσιαστικά. Εξαιρετικά χρήσιμη θα μας είναι η Θέση Church-Turing, την οποία και θα υιοθετήσουμε για να αποδεικνύουμε τους ισχυρισμούς μας.

Στο δέυτερο κεφάλαιο, ορίζουμε την πολυπλοκότητα Kolmogorov δυαδικών ακολουθιών και φυσικών αριθμων με βάση τις υπολογίσιμες συνάρτησεις. Αποδεικνύουμε βασικές ιδιότητες της, όπως είναι η μη υπολογισιμότητα της αλλά και την ύπαρξη υπολογίσιμης μη αύξουσας συνάρτησης η οποία προσεγγίζει τη συνάρτηση πολυπλοκότητας C. Επίσης ορίζουμε την πολυπλοκότητα ζεύγους, αλλά και τη δεσμευμένη πολυπλοκότητα του x δεδομένου του y, η οποία περιγράφει το κατα πόσο η γνώση του y, διευκολύνει την περιγραφή του x και αποδεικνύουμε θεωρήματα σχετικά με το πώς σχετίζονται οι παραπάνω ποσότητες μεταξύ τους, όπως το θεώρημα Kolmogorov-Levin για παράδειγμα, το οποίο λέει χονδρικά ότι για να περιγράψουμε από κοινού δύο λέξεις αρκεί να γνωρίζουμε την πολυπλοκότητα της πρώτης και την πολυπλοκότητα της δέυτερης, δεδομένης της πρώτης. Τέλος, παρουσιάζουμε δύο εφαρμογές σε δύο κλασικά προβλήματα της θεωρίας υπολογισιμότητας, την ύπαρξη απλών κατά Post συνόλων και μια ενδιαφέρουσα προσέγγιση μιας " ασθενέστερης " μορφής του προβλήματος τερματισμού.

Στο επόμενο κεφάλαιο παρουσιάζουμε μία ελαφρώς διαφορετική μορφή της πολυπλοκότητας Kolmogorov, την οποία καλούμε προθεματική πολυπλοκότητα, βασιζόμενοι σε υπολογίσιμες συναρτήσεις οι οποίες σέβονται, κατά κάποιον τρόπο τα αρχικά τμήματα των λέξεων-εισόδων τους. Σκόπος μας είναι να απόδειξουμε στο κεφάλαιο αυτό, το πως συνδέεται η προθεματική πολυπλοκότητα K με τον κλάδο της αλγοριθμικής (ή Solomonoff) πιθανότητας, στην οποία κάνουμε μια εισαγωγή στην ενότητα 3.1. Ορίζουμε αρχικά τα ημιυπολογίσιμα μέτρα στο $\mathbb{N}$ και αποδεικνύουμε την ύπαρξη ενός, υπο μία έννοια, μεγιστικού τέτοιου μέτρου m, το οποίο καλείται a priori πιθανότητα, και γίνεται μια προσπάθεια ερμηνείας του με τη βοήθεια μη ντετερμινιστικών αλγορίθμων. Έπειτα παιρνάμε στον ορισμό της προθεματικής πολυπλοκότητας, και αποδεικνύουμε το θεώρημα Levin, δηλαδή ότι, $K(x) = -\log m(x) + O(1)$, καθώς και κάποιες

ενδιαφέρουσες ιδιότητές της.

Στο τελευταίο μέρος, παρουσιάζουμε έναν τρόπο χαρακτηρισμού μιας άπειρης δυαδικής ακολουθίας ως τυχαία ή μη, ο οποίος οφείλεται στον P. Martin-Löf. Η κεντρική ιδέα είναι να διαφοροποιήσουμε ελαφρώς το πότε θα χαρακτηρίζουμε ένα $A \subset \{0,1\}^{\mathbb{N}}$ ως σύνολο μηδενικού μέτρου (ως προς κάποιο μέτρο μ) ως εξής: τα σύνολα V_i για το οποία $A \subset \bigcup_{i\in\mathbb{N}} V_i$ με το $\sum_{i\in\mathbb{N}} \mu(V_i)$ να γίνεται οσοδήποτε μικρό επιθυμούμε , θα πρέπει να επιλέγονται με έναν υπολογίσιμο τρόπο. Ένα τέτοιο υποσύνολο $A \subset \{0,1\}^{\mathbb{N}}$ συναντάται στη βιβλιογραφία ως effectively null set, ενώ εμείς εδώ χρησιμοποιούμε τον όρο Ε-μηδενικό. Αποδεικνύουμε επίσης το θεώρημα Martin Löf, δείχνοντας ότι η ένωση όλων των Ε-μηδενικών υποσυνόλων του $\{0,1\}^{\mathbb{N}}$ είναι επίσης Ε-μηδενικό, με βάση το οποίο ορίζουμε τις τυχαίες ακολουθίες κατά Martin Löf. Τέλος αποδεικνύουμε το θεώρημα Levin-Schnorr, το οποίο παρέχει μια ικάνη και αναγκαία συνθήκη τυχαιότητας, με τη βοήθεια της προθεματικής πολυπλοκότητας, που μελετήσαμε στο τρίτο κεφάλαιο.

Ολοκληρώνοντας αυτή τη σύντομη εισαγωγή-πρόλογο, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγήτη της εργασίας, Αρβανιτάκη Αλέξανδρο, για την καθοδήγηση του, την κατανόηση που έδειξε στα όποια προβλήματα προέκυψαν αλλά και για τις πολύ εποικοδομητικές συζητήσεις μας.

Κεφάλαιο 1

Στοιχεία Θεωρίας Αναδρομής

Σκοπός του πρώτου αυτού κεφαλαίου είναι να παρουσιάσουμε όσο το δυνατόν συντομότερα τις κυριότερες έννοιες της Θεωρίας Αναδρόμης, οι οποίες θα είναι απαραίτητες για τη συνέχεια. Η Θεωρία Αναδρομής ή Θεωρία Υπολογισιμότητας άρχισε να αναπτύσσεται κατα την δεκαετία του 1930, κύριως μέσω των εργασιών των Alonzo Church, Kurt Gödel, Stephen Kleene, Emil Post, Alan Turing αλλά και άλλων. Κύριο αντικείμενό της είναι η μελέτη και η ταξινόμηση συναρτήσεων οι οποίες προκύπτουν με έναν "κατασκευαστικό" τρόπο, ως μια προσπάθεια να διατυπώθει με μαθηματική σαφήνεια αυτό που διαισθητικά αποκαλούμε υπολογίσιμο ή κατασκευάσιμο. Μπορούμε έτσι να φανταζόμαστε τις αναδρομικές ή υπολογίσιμες συνάρτησεις, όπως θα δούμε παρακάτω ως συνάρτησεις, για τις οποίες μπορούμε να γράψουμε ένα πρόγραμμα σε μια γλώσσα προγραμματισμού, το οποίο να δέχεται κάποια είσοδο x και μας επιστρέφει την τιμή της συγκεκριμένης συνάρτησης για το όρισμα x.

Κέντρικό ρόλο παίζουν οι φυσικοί αριθμοί, ως το πιο θεμελιώδες αριθμητικό σύστημα, είναι επόμενό οι εν λόγω συνάρτησεις να ορίζονται αρχικά στο $\mathbb{N}$, και έπειτα με απλό τρόπο να επεκτείνονται σε παράγωγα σύνολα των φυσικών, όπως το $\mathbb{Z}$ και $\mathbb{Q}$. Έτσι λαμβάνεται υπόψιν το αξιώμα της επαγωγής στο $\mathbb{N}$, με τη μορφή των αναδρομικών ορισμών, το οποίο μας επιτρέπει, να παράγουμε, με έναν ξεκάθαρα αλγοριθμικό τρόπο νέες συνάρτησεις από ήδη ορισμένες συνάρτησεις. Φυσικά αυτο δεν είναι αρκετό να παράξει όλα τα δυνατά "προγράμματα", όπως θα δούμε, για αυτό και είναι απαραίτητη η εισαγωγή του τελεστή ελαχιστοποίησης, ένα εργαλείο το οποίο μας επιτρέπει να κάνουμε ακριβώς αυτό που προδίδει το όνομα του, να αναζητούμε τον μικρότερο φυσικό αριθμό που ικανοποιεί μια συγκεκριμένη συνθήκη. Αξίζει να σημείωθει ότι το μοντέλο υπολογισημότητας μέσω της αναδρομής δεν είναι το μοναδικό που έχει αναπτυχθεί, αλλά όπως θα δούμε προς το τελός του κεφαλαίου με την Θέση Church-Turing, είναι ισοδύναμα μεταξύ τους.

Το πρώτο αυτό μέρος είναι υπό μια έννοια ανεξάρτητο των επόμενων και

έχει συμπεριληφθεί στην παρούσα εργάσια με σκοπό αφ'ενός την μαθηματική πληρότητα, αφ'ετέρου την παρουσιάση εννόιων τις οποίες θα χρησιμοποιούμε συνεχώς στα επόμενα κεφάλαια, επομένως οι λιγοστές προτάσεις και θεωρήματα παρουσιάζονται χώρις αποδειξείς.

1.1 Πρωτογενώς Αναδρομικές Συναρτήσεις

Ξεκινάμε με τις τρεις θεμελιώδεις κατηγορίες συναρτήσεων οι οποίες θα αποτελέσουν την βάση για την κατασκέυη αρχικά της κλάσης των πρωτογενώς αναδρομικών συναρτήσεων και στη συνέχεια των γενικών αναδρομικών. Θα μπορούσαμε να αναφερούμε λοιπόν ως αρχικές συναρτήσεις τις εξής:

(i) Οι σταθερές συναρτήσεις, $C_n^k : \mathbb{N}^k \to \mathbb{N}$, $C_n^k(i_1, i_2, \ldots, i_k) = n$.

(ii) Η συνάρτηση του επομένου $S(n) = n + 1$ στους φυσικούς αριθμούς.

(iii) Οι προβολές $P_j^k : \mathbb{N}^k \to \mathbb{N}$, $1 \leq j \leq k$, $P_j^k(i_1, i_2, \ldots, i_j, \ldots, i_k) = i_j$.

Συνέχιζουμε με το Λήμμα Αναδρομής ώστε να ορισούμε έπειτα την κλάση $\mathcal{R}_P$ των πρωτογενώς αναδρομικών συναρτήσεων.

Λήμμα 1.1.1 (Λήμμα Αναδρομής)**.** *Έστω οποιαδήποτε σύνολα X, Y και συναρτήσεις $g : X \to Y$, $h : Y \times \mathbb{N} \times X \to Y$. Τότε υπάρχει μοναδική συνάρτηση $f : \mathbb{N} \times X \to Y$ τ.ω.*

$$f(0, x) = g(x) \quad \text{και} \quad f(n + 1, x) = h(f(n, x), n, x).$$

Για τη συνάρτηση f του προήγουμενου λήμματος θα λέμε ότι παράγεται με βασική αναδρομή από τις g και h.

Στην απλούστερη περίπτωση όπου η $g(x) = y_0$ για κάθε $x \in X$ και η $h : Y \times \mathbb{N} \to X$ δεν εξαρτάται από κάποια παράμετρο, έχουμε τον κλάσσικο αναδρομίκο ορισμό συνάρτησης με

$$f(0) = y_0 \quad \text{και} \quad f(n + 1) = h(f(n), n).$$

Η απόδειξη του Λήμματος Αναδρομής γίνεται με χρήση της Αρχής της Επαγωγής. Αξίζει να σημειωθεί ότι αν έχουμε κατάλληλες διαδικασίες οι οποίες υπολογίζουν τις συναρτήσεις g, h τότε το Λήμμα Αναδρομής μας παρέχει έναν αλγοριθμίκο τρόπο να παράγουμε τη νέα συνάρτηση f, υπό μια έννοια να κατασκευάσουμε ένα νέο αντικείμενο με τις ιδιότητες που μας ενδιαφέρουν.

Είμαστε έτοιμοι τώρα να ορίσουμε την κλάση $\mathcal{R}_P$ των πρωτογενώς αναδρομικών συναρτήσεων. Πριν συνεχίσουμε, από εδώ και στο εξής θα συμβολίζουμε με,

$$(\mathbb{N}^k \to \mathbb{N}) = \{f \mid f : \text{συνάρτηση}, Dom(f) = \mathbb{N}^k, Rng(f) \subset \mathbb{N}\},$$

και με τον όρο συνάρτηση θα εννοούμε οποιοδήποτε στοιχείο του συνόλου $\bigcup_{k\in\mathbb{N}}(\mathbb{N}^k \to \mathbb{N})$. Τέλος, για λόγους συντομίας, τα στοιχεία $(x_1, \ldots, x_k) \in \mathbb{N}^k$ θα συμβολίζονται συχνα ως $\vec{x}$.

Ορισμός 1.1.1. Έστω σύνολο συναρτήσεων F. Το F θα καλείται πρωτογενώς κλειστό αν:

(i) Το F περιέχει τις αρχικές συναρτήσεις, δηλαδή $S \in F$ και για κάθε $k, n \in \mathbb{N}, 1 \leq j \leq k$, $C_n^k, P_j^k \in F$.

(ii) Το F είναι κλειστό στη σύνθεση, δηλαδή αν $g \in F$ με $Dom(g) = \mathbb{N}^k$, $h_1, h_2, \ldots, h_k \in F$, με $Dom(h_i) = \mathbb{N}^m$, $1 \leq i \leq k$, τότε και $f \in F$, όπου $f = g \circ (h_1, h_2, \ldots, h_k)$.

(iii) Το F είναι κλειστό στην πρωτογενή αναδρομή, δηλαδη αν $g \in F$, με $Dom(g) = \mathbb{N}^k$, $h \in f$, $Dom(h) = \mathbb{N}^{k+2}$, τότε και η $f \in F$ όπου η f ορίζεται αναδρομικά ως

$$f(0, \vec{x}) = g(\vec{x})$$
$$f(n+1, \vec{x}) = h(f(n, \vec{x}), n, \vec{x}).$$

Ορισμός 1.1.2. Μια συνάρτηση f καλείται πρωτογενώς αναδρομική (primitive recursive) αν ανήκει σε κάθε πρωτογενώς κλειστό σύνολο F. Επομένως η κλάση $\mathcal{R}_P$ των πρωτογενώς αναδρομικών συναρτήσεων ορίζεται ως

$$\mathcal{R}_P = \bigcap \big\{ F \subset \bigcup_{k\in\mathbb{N}} (\mathbb{N}^k \to \mathbb{N}) \mid F : \text{πρωτογενώς κλειστό} \big\}.$$

Αρχικά η $\mathcal{R}_P$ είναι μη κένη, αφού εξ'ορισμού κάθε πρωτογενώς κλειστό σύνολο περιέχει τις αρχικές συναρτήσεις. Επίσης κάθε πρωτογενώς αναδρομική συνάρτηση είναι ολική συνάρτηση αφού οι αρχικές συναρτήσεις είναι ολικές και είναι εύκολο να διαπιστώσουμε ότι η σύνθεση καθως και η πρωτογενής αναδρομή διατηρούν αυτή την ιδιότητα.

Για παράδειγμα η συνάρτηση πρόσθεσης $sum(x, y) = x + y$, στους φυσικούς είναι πρωτογενώς αναδρομική, αφού ορίζεται με πρωτογενή αναδρομή μέσω των

$$g(y) = P_1^1(y) = y \quad \text{και} \quad h(z, x, y) = S(P_1^3(z, x, y)) = z + 1,$$

ως εξής,

$$sum(0, y) = P_1^1(y)$$
$$sum(x+1, y) = S(P_1^3(sum(x, y), x, y)).$$

Με αντίστοιχο τρόπο μπορούμε να δείξουμε ότι οι παρακάτω συναρτήσεις είναι πρωτογενώς αναδρομικές, $pred(x) = x - 1$, αν $x \geq 1$, ενώ $pred(x) = 0$ αλλίως. $x \dot{-} y = x - y$, αν $x \geq y$, $x \dot{-} y = 0$, διαφορετικά. $sgn(x) = 0$, αν $x = 0$, $sgn(x) = 1$, διαφορετικά. $abs(x, y) = |x - y|$, $prod(x, y) = xy$, $fact(n) = n!$, $exp(x, y) = x^y$. Παρατηρούμε στο προηγούμενο παράδειγμα, ότι χρησιμοποιήσαμε μια σύνθεση και μια αναδρομή για να ορίσουμε την πρόσθεση. Με αφορμή αυτό μπορούμε να κατασκευάσουμε την κλάση $\mathcal{R}_P$ με έναν λίγο διαφορετικό τρόπο, μέσω μιας επαγωγικής διαδικασίας.

Θέτουμε F_0 ως το σύνολο των αρχίκων συναρτήσεων, και με $R(F_0)$ το σύνολο των συναρτήσεων το οποίο περιέχει όλες τις συναρτήσεις που προκύπτουν είτε από συνθέση είτε από πρωτογενή αναδρομή των στοιχείων του F_0. Αν έχουμε κατασκευάσει τα πρωτα n, F_n, θέτουμε $F_{n+1} = F_n \cup R(F_n)$, για παράδειγμα $sum(\cdot, \cdot) \in F_2$. Είναι εύκολο να διαπιστώσει κάνεις ότι $\mathcal{R}_P = \bigcup_n F_n$. Τέλος, έφοσον το F_0 είναι αριθμήσιμο μπορει κανείς να αποδείξει επαγωγικά, ότι το σύνολο των πρωτογενώς αναδρομικών συναρτήσεων $\mathcal{R}_P$ είναι αριθμήσιμο. Μια χρήσιμη παρατήρηση είναι επίσης το γεγονός ότι αν $f, g \in \mathcal{R}_P$ με $D(f) = D(g) = \mathbb{N}^k$ τότε και $f + g, fg \in \mathcal{R}_P$.

1.2 Ελαχιστοποίηση & Αναδρομικές Συναρτήσεις

Όπως αναφέραμε ήδη, η κλάση $\mathcal{R}_P$ των πρωτογενώς αναδρομικών συναρτήσεων αποτελείται αποκλειστικά από ολικές συναρτήσεις. Έχοντας στο μυαλό μας ότι ενδιαφερόμαστε για συναρτήσεις που ουσιαστικά υπολογίζονται από κάποιο πρόγραμμα, καταλαβαίνουμε ότι η μελέτη μόνο ολικών συναρτήσεων είναι κατί μη ρεαλιστικό, εφόσον ενά πρόγραμμα ενδέχεται για συγκεκριμένες εισόδους να μην τερματίζει πότε. Θα θέλαμε λοίπον έναν νέο " επιτρεπτό " τρόπο να παράγουμε νέες συναρτήσεις από τις βασικές, ώστε να επεκταθούμε και σε μερικές συναρτήσεις.

Πριν συνεχίσουμε, αν $g : Dom(g) \subset \mathbb{N}^k \to \mathbb{N}$ είναι μερική συνάρτηση, θα συμβολίζουμε με $g(x) \downarrow$ και θα λέμε ότι η g συγλίνει για είσοδο x αν $x \in Dom(g)$, ενώ αν $x \notin Dom(g)$ θα γράφουμε $g(x) \uparrow$ και θα λέμε ότι η $g(x)$ αποκλίνει για είσοδο x. Κατά τετριμμένο τρόπο κάθε ολική συνάρτηση είναι μερική, με την ιδιότητα ότι οι τιμές της συγκλίνουν για κάθε είσοδο. Επίσης, αρκετές φορές θα χρησιμοποίουμε και το συμβολισμό $g : \mathbb{N}^k \rightharpoonup \mathbb{N}$, για μερικές συναρτήσεις.

Είμαστε έτοιμοι τώρα να εισάγουμε τον νέο τρόπο παραγωγής συναρτήσεων, τον τελεστή ελαχιστοποίησης μ. Έστω $g : \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$ και ας υποθέσουμε ότι αναζητάμε το μικρότερο $y \in \mathbb{N}$ τ.ω. $g(y, x_1, \ldots, x_k) = 0$, για δεδομένα

$\vec{x} = (x_1, \ldots, x_k)$. Ένας τρόπος για να βρούμε ένα τέτοιο y είναι ο εξής, ξεκινάμε υπολογίζοντας τις τιμές $g(0, \vec{x}), g(1, \vec{x}) \ldots, g(i, \vec{x})$, έως ότου εντοπίσουμε το πρώτο y τ.ω. $g(y, \vec{x}) = 0$. Ο συγκεκριμένος τρόπος μπόρει να αποτύχει μόνο σε δύο περιπτώσεις, είτε αν όλες οι τιμές $g(i, \vec{x}) \downarrow$ και $g(i, \vec{x}) > 0$ για κάθε $i \in \mathbb{N}$, είτε $g(0, \vec{x}) \downarrow, \ldots, g(i-1, \vec{x}) \downarrow$ και είναι όλα θετικά ενώ $g(i, \vec{x}) \uparrow$ για κάποιο i. Επομένως, μπορεί ο τρόπος αυτός να είναι ο λιγότερο αποδοτικός από άποψη υπολογισμών, παρ'όλα αυτά, αν για τη συνάρτηση g έχουμε μια διαδικασία υπολογισμού των τιμών της, π.χ. να είναι πρωτογενώς αναδρομική, τότε είναι προφανές ότι με τον τρόπο αυτό έχουμε επίσης μια διαδικάσια για τον υπολογισμό μιας νέας συνάρτησης. Συνοψίζουμε τα προηγούμενα με τον επόμενο ορισμό.

Ορισμός 1.2.1. Έστω $g : \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$. Ορίζουμε συνάρτηση $\mu g : \mathbb{N}^k \rightharpoonup \mathbb{N}$, την ελαχιστοποίηση (minimization) της g ως εξής:

$$\mu g(\vec{x}) = \begin{cases} y, & \text{αν } g(y, \vec{x}) = 0 \ \& \ g(i, \vec{x}) \downarrow, g(i, \vec{x}) > 0, \\ & \quad \text{για κάθε } 0 \leq i < y. \\ \text{δεν ορίζεται}, & \text{διαφορετικά.} \end{cases}$$

Ο τελεστής μ καλείται τελεστής ελαχιστοποίησης.

Από τον παραπάνω ορισμό και τα σχόλια που προηγήθηκαν είναι φανερό ότι ακόμα κι αν η g είναι ολική δεν είναι απαραίτητο ότι η μg θα είναι και αυτή ολική. Για παράδειγμα, η συνάρτηση $g(x, y) = sum(x, y) = x + y$ είναι ολίκη, όμως για την $\mu g(x)$ ισχύει ότι $\mu g(x) \downarrow$ αν και μόνο αν $x = 0$. Επίσης, αν είχαμε μια συνάρτηση $g : \mathbb{N} \times X \rightharpoonup \mathbb{N}$, για τυχόν σύνολο X, τότε ορίζεται και πάλι η $\mu g : X \rightharpoonup \mathbb{N}$.

Ορισμός 1.2.2. Μια μερική συνάρτηση f καλείται αναδρομική (recursive) ή μ-αναδρομική (μ-recursive) αν ανήκει σε κάθε πρωτογενώς κλείστο σύνολο συναρτήσεων F το οποίο είναι επιπλέον κλειστό και ως προς τον τελεστή ελαχιστοποίησης μ. Δηλαδή αν $g \in F$ τότε και η $f = \mu g \in F$ ή συμβολικά $\mu F \subset F$. Θα συμβολίζουμε το σύνολο των αναδρομικών συναρτήσεων με $\mathcal{R}_\mu$ και σύμφωνα με τα παραπάνω,

$$\mathcal{R}_\mu = \bigcap \big\{ F \subset \bigcup_{k \in \mathbb{N}} (\mathbb{N}^k \rightharpoonup \mathbb{N}) \mid F : \text{πρωτογενώς κλειστό και } \mu F \subset F \big\}.$$

Παρατηρούμε ότι, εφόσον το $\mathcal{R}_\mu$ είναι κλειστό στη σύνθεση και την πρωτογενή αναδρομή, $\mathcal{R}_P \subset \mathcal{R}_\mu$, ενώ ο αντίστροφος εγκλεισμός δεν ίσχυει, δηλαδή υπάρχει ολική αναδρομική συνάρτηση που δεν είναι πρωτογενώς αναδρομική.

Επίσης, θα μας είναι χρήσιμό να ορίσουμε τις αναδρομικές συναρτήσεις και στην περίπτωση όπου λαμβάνουν τιμές σε κάποιο $\mathbb{N}^k$. Αυτό γίνεται πολύ απλά ώς εξής.

Ορισμός 1.2.3. Έστω συνάρτηση $f : \mathbb{N}^n \rightharpoonup \mathbb{N}^k$. Θα λέμε ότι η f είναι ανδρομική αν και μόνο αν για κάθε, $1 \leq j \leq k$, η $P_j^k \circ f$ είναι αναδρομική.

Οι έννοιες πρωτογενώς αναδρομικές και αναδρομικές μπορούν να επεκταθούν και σε n-μελείς σχέσεις αλλά και σε υποσύνολα των φυσικών αριθμών. Συγκεκριμένα δίνουμε τον παρακάτω ορισμό.

Ορισμός 1.2.4. (i) Έστω $A \subset \mathbb{N}^k$. Το A καλείται αναδρομικά αποφασήσιμο (recursively decidable) ή αναδρομικό (recursive) αν η χαρακτηριστική του συνάρτηση χ_A είναι αναδρομική.

(ii) Έστω σχέση $P(x_1, \ldots, x_k)$. Η P καλείται αναδρομική (recursive) αν η χαρακτηριστική της συνάρτηση χ_P είναι αναδρομική, δηλαδή η

$$\chi_P(x_1, \ldots, x_k) = \begin{cases} 1, & \text{αν } P(x_1, \ldots, x_k) \\ 0, & \text{διαφορετικά.} \end{cases}$$

είναι αναδρομική.

Για παράδειγμα κάθε πεπερασμένο σύνολο είναι αναδρομικό, για το οποίο θα επιχειρηματολογήσουμε στην επόμενη ενότητα, κάθως και κάθε συμπερασμένο είναι επίσης αναδρομικο, αφού αν το $A \subset \mathbb{N}^k$ είναι συμπεπερασμένο τότε από το προηγούμενο το $\mathbb{N}^k \backslash A$ είναι αναδρομικό και $\chi_A = 1 \dot{-} \chi_{\mathbb{N}^k \backslash A}$.

Ανάλογα ορίζονται οι αντίστοιχες έννοιες για πρωτογενώς αναδρομικά αποφασήσιμα σύνολα και σχέσεις. Επίσης αν P είναι αναδρομική σχέση τότε αναδρομική είναι και η άρνηση της $\neg P$, αφού $\chi_{\neg P} = 1 \dot{-} \chi_P$. Δεν είναι δύσκολο να δείξουμε ότι πολύ βασικές σχέσεις όπως οι $=$ και $\leq$ είναι ανδρομικές. Για παράδειγμα, η $\chi_=$ δίνεται από τον τύπο

$$\chi_=(x, y) = 1 \dot{-} (sgn(abs(x, y))).$$

Επίσης οι αναδρομικές σχέσεις είναι κλειστές ως προς τους τελέστες ένωσης $\vee$ και τομής $\wedge$, δηλάδη:

Πρόταση 1.2.1. *Έστω $P_1(x_1, x_2, \ldots, x_k), P_2(x_1, x_2, \ldots, x_k)$ αναδρομικές σχέσεις. Τότε οι παρακάτω σχέσεις είναι επίσης αναδρομικές.*

(i) $R(x_1, x_2, \ldots, x_k) \iff P_1(x_1, x_2, \ldots, x_k) \vee P_2(x_1, x_2, \ldots, x_k)$

(ii) $S(x_1, x_2, \ldots, x_k) \iff P_1(x_1, x_2, \ldots, x_k) \wedge P_2(x_1, x_2, \ldots, x_k)$

Είναι σχετικά άμμεσο τώρα να δούμε ότι αν έχουμε συναρτήσεις που ορίζονται κατα περιπτώσεις, μέσω των σχέσεων $P_1, P_2, \ldots, P_n$, οποίες έχουν έχουν

κενή τομή θα έχουμε μια νέα αναδρομική συνάρτηση, δηλαδή αν για παράδειγμα $f_1, f_2, \ldots, f_n : \mathbb{N}^2 \rightharpoonup \mathbb{N}$ είναι αναδρομικές και $P_1, P_2, \ldots, P_n$ είναι διμελείς αναδρομικές σχέσεις, αμοιβαία αποκλειόμενες τότε η συνάρτηση:

$$g(x,y) = \begin{cases} f_1(x,y), & \text{αν } P_1(x,y) \\ f_2(x,y), & \text{αν } P_2(x,y) \\ \vdots & \\ f_n(x,y), & \text{αν } P_n(x,y) \end{cases}$$

είναι επίσης αναδρομική, αφού

$$g(x,y) = \sum_{i=1}^{n} \chi_{P_i}(x,y) f_i(x,y),$$

και για οποιοδήποτε ζέυγος (x,y) ακριβώς μια P_i αληθεύει, επομένως μπορούμε να υπολογίσουμε την τιμή $g(x,y)$ μέσω της αντίστοιχης f_i. Με βάση τα παραπάνω οι συναρτήσεις $max(x,y)$ και $min(x,y)$, που επιστρέφουν τον μέγιστο και έλαχιστο των x, y αντίστοιχα, είναι αναδρομικές.

Μια άλλη κατηγορία συνόλων που θα μας είναι χρήσιμη είναι αυτή των αναδρομικά απαριθμήτων συνόλων τα οποία αποτελούν μια ευρύτερη κατηγορία από τα αναδρομικά.

Ορισμός 1.2.5. (i) Έστω $A \subset \mathbb{N}^k$. Το A καλείται αναδρομικά απαριθμήτο (recursively enumerable) αν η συνάρτηση

$$\phi_A(x_1, \ldots, x_k) = \begin{cases} 1, & \text{αν } (x_1, \ldots, x_k) \in A \\ \text{δεν ορίζεται}, & \text{διαφορετικά.} \end{cases}$$

είναι αναδρομική.

(ii) Έστω σχέση $P(x_1, \ldots, x_k)$. Η P καλείται αναδρομικά απαριθμητή (recursively enumerable) ή ημιαποφασίσιμη (semidecidable) αν η συνάρτηση,

$$\phi_P(x_1, \ldots, x_k) = \begin{cases} 1, & \text{αν } P(x_1, \ldots, x_k) \\ \text{δεν ορίζεται}, & \text{διαφορετικά.} \end{cases}$$

είναι αναδρομική.

Ένα χαρακτηριστικό παράδειγμα αναδρομικά απαριθμητού σύνολου είναι το εξής: έστω αναδρομική $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$, τότε το $Dom(f)$ είναι αναδρομικά απαριθμητό. Πράγματι, αν θέλουμε να απαφανθούμε αν $(n_0, n_1, \ldots, n_{k-1}) \in Dom(f)$, τότε υπολογίζουμε την τιμή $f(n_0, n_1, \ldots, n_{k-1})$, και αν $f(n_0, n_1, \ldots, n_{k-1}) \downarrow$ τότε " απαντάμε " 1, ενώ διαφορετικά δεν απαντάμε τίποτα. Αποδεικνύεται ότι όλα τα παρακάτω είναι ισοδύναμα για $A \subset \mathbb{N}^k$,

(i) Το A είναι αναδρομικά απαριθμητό.

(ii) Για κάποια αναδρομική συνάρτηση f ισχύει ότι $Dom(f) = A$.

(iii) Για κάποια αναδρομική συνάρτηση f ισχύει ότι $Rng(f) = A$.

Είναι προφανές ότι αν ένα σύνολο A είναι αναδρομικό τότε είναι και αναδρομικά απαριθμήτο, ενώ το αντίστροφο δεν ισχύει απαραίτητα, δηλαδή υπάρχουν αναδρομικά απαριθμητά σύνολα τα οποία δεν είναι αναδρομικά. Ισχύει όμως το παρακάτω.

Πρόταση 1.2.2. *Έστω $A \subset \mathbb{N}^k$ αναδρομικά απαριθμητό, τέτοιο ώστε το $\mathbb{N}^k \backslash A$ να είναι επίσης αναδρομικά απαριθμητό. Τότε το A είναι αναδρομικό.*

Επίσης οι ημιαπαφασίσιμες σχέσεις συμπεριφέρονται κάλως ως προς τους ποσοδείκτες $\exists$ και $\forall$. Πιο συγκεκριμένα ισχύει η παρακάτω πρόταση.

Πρόταση 1.2.3. *Έστω $P(x_1, x_2, \ldots, x_k)$ ημιαποφασίσιμη σχέση. Τότε οι παρακάτω σχέσεις είναι επίσης ημιαποφασίσιμες.*

(i) $R(x_1, x_2, \ldots, x_{k-1}, y) \iff \exists y(P(x_1, x_2, \ldots, x_{k-1}, y))$

(ii) $S(x_1, x_2, \ldots, x_{k-1}, y) \iff \forall z < y(P(x_1, x_2, \ldots, x_{k-1}, z))$

Επιστρέφοντας στις αναδρομικές συνάρτησεις είναι εύκολο να διαπιστώσει κανείς ότι είναι αριθμήσιμες το πλήθος. Επόμενως αναρωτιέται κανείς αν θα μπορούσαμε να κατασκευάσουμε μια κωδικοποίηση τους, υπό την έννοια ότι σε κάθε αναδρομική συνάρτηση f να αντιστοιχίσουμε έναν κωδικό αριθμό $[f]$, και δύο διαφορέτικες συνάρτησεις να έχουν διαφορετικό κωδικό.

Για τον σκοπό αυτό, υπενθυμίζουμε ότι με βάση τον ορισμό 1.2.2, προκύπτει ότι σε κάθε αναδρομική συνάρτηση f αντιστοιχεί μια πεπερασμένη ακολουθία από $f_1, f_2, \ldots, f_n$ από τις οποίες προκύπτει η f μέσω συνδιασμών τους και συνδιασμο των τελεστών σύνθεσης, αναδρομής και ελαχιστοποίησης πάνω σε αυτές, δηλάδη μια ακολουθία από υπολογισμούς για τις τιμές της f. Φυσικά αυτη η ακολουθία δεν είναι μοναδική, αφού για μια συνάρτηση μπορούμε να έχουμε παραπάνω από έναν τύπο υπολογισμού για τις τιμές της ($x^{y+z} = x^y x^z$). Επειδή η αριθμητικοποίηση που θα παρουσιάσουμε βασίζεται πάνω σε τέτοιου είδους ακολουθίες είναι φανερό ότι μια συνάρτηση μπορεί να αντιστοιχίζεται σε περισσότερους από έναν αριθμούς.

Αρχικά, αν $x_0, x_2, \ldots, x_k$, είναι πεπερασμένη ακολουθία φυσικών αριθμών, αντιστοιχούμε σε αυτή τον φυσικό,

$$\langle x_1, x_2, \ldots, x_k \rangle = \prod_{i=1}^{k} p_i^{x_i+1},$$

όπου p_i είναι ο i-οστός πρώτος. Από το Θεμελιώδες Θεώρημα της Αριθμητικής, έχουμε ότι αν κάποιος μας δώσει τον αριθμό e μιας πεπερασμένης ακολουθίας, τότε βρίσκοντας την παραγοντοποίηση του e σε πρώτους, έστω $e = \prod_{i=1}^{l} p_i^{r_i}$, έχουμε ότι ο e είναι κωδικός της ακολουθίας $r_i - 1, \ldots, r_l - 1$.

Αριθμητικοποίηση Αναδρομικών Συναρτήσεων: Σε κάθε αναδρομική f αντιστοιχούμε τον αριθμό $[f]$ με τον εξής τρόπο:

(1) Στη σταθερή συνάρτηση C_0^1, $[C_0^1] = 0$.

(2) Στη συνάρτηση επομένου S, $[S] = 1$.

(3) Στην προπολή P_j^k, $[P_j^k] = \langle 2, j, k \rangle$.

(4) Στην $f = g \circ (h_1, h_2, \ldots, h_k)$, $[f] = \langle 3, [g], [h_1], \ldots, [h_k] \rangle$.

(5) Στην f που παράγεται με βασική αναδρομή από τις g και h, $[f] = \langle 4, [g], [h] \rangle$.

(6) Στην $f = \mu g$, $[f] = \langle 5, [g] \rangle$.

Με βάση όσα προηγήθηκαν, έχοντας έναν κωδικό e, μπορούμε να αναγνωρίσουμε σε ποια αναδρομική συνάρτηση αντιστοιχεί. Πάρ᾽ όλα αυτά όμως, δεν ισχύει ότι κάθε φυσικός αριθμός είναι κωδικός για κάποια αναδρομική συνάρτηση. Επίσης αποδεικύνεται ότι η διαδικάσια που περιγράψαμε παραπάνω είναι αναδρομική.

Η αριθμητικοποίηση των αναδρομικών συναρτήσεων παίζει ουσιώδη ρόλο στην απόδειξη του Θεωρήματος Κανονικής Μορφής του Kleene, το οποίο θα είναι και το τελευταίο απότελεσμα που θα συζητήσουμε σε αυτή την ενότητα, χωρίς όμως να το αποδείξουμε.

Πριν διατυπώσουμε το εν λόγω θεώρημα, θα χρειαστούμε την έννοια του υπολογισμού για μια αναδρομική συνάρτηση, την οποόια θα προσπαθήσουμε να παρουσιάσουμε πολύ συνοπτικά παρακάτω. Είπαμε ότι σε κάθε αναδρομική συνάρτηση f αντιστοιχίζεται μια ακολουθία απο άλλες αναδρομικές συναρτήσεις, έστω $f_1, f_2, \ldots, f_n$. Για δεδομένη είσοδο x στην αναδρομική συνάρτηση f, δημιουργείται μια αλληλουχία υπολογισμών μέσω των f_i, για παράδειγμα αν $f = f_1 \circ (f_2, \ldots, f_n)$, τότε πρώτα υπολογίζουμε τις $z_i = f_i(x)$ για $2 \leq i \leq n$ και έπειτα την $f_1(z_2, \ldots, z_n)$. Πολύ συνοπτικά, μπορουμέ να αντιστοιχίσουμε και σε αυτή την αλληλουχία υπολογσμών έναν κωδικό με ανάλογο τρόπο, όπως κάναμε και στην περίπτωση των αναδρομικών συναρτήσεων. Έχοντας τα παραπάνω, μπορούμε να ορίσουμε μια σχέση $T_n \subset \mathbb{N}^{n+2}$ ώς εξής,

$$T_n(e, x_1, \ldots, x_n, y) \iff \text{ο } y \text{ είναι κωδικός υπολογισμού για την } f_e \text{ με είσοδο } x_1, x_2, \ldots, x_n,$$

όπου με f_e συμβολίζουμε την αναδρομική συνάρτηση με κωδικό e. Επίσης αν f, g είναι μερικές συνάρτησεις θα συμβολίζουμε με $f(x) \simeq g(x)$ αν είτε και οι δύο ποσότητες δεν ορίζονται ή όριζόνται και είναι $f(x) = g(x)$. Είματε έτοιμοι να διατυπώσουμε το θέωρημα κανονικής μορφής,

Θεώρημα 1.2.1 (Kleene). *Υπάρχουν πρωτογενώς αναδρομική συνάρτηση $U : \mathbb{N} \to \mathbb{N}$ και για κάθε $n \geq 1$ πρωτογενώς αναδρομική σχέση $T_n \subset \mathbb{N}^{n+2}$ τέτοιες ώστε για κάθε αναδρομική $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ να ισχύει ότι, υπάρχει αριθμός e έτσι ώστε,*

$$f(x_1, x_2, \ldots, x_n) \simeq U(\mu y T_n(e, x_1, x_2, \ldots, x_n, y)). \tag{1.1}$$

Ο αριθμός e που εμφανίζεται είναι ο κωδικός της συνάρτησης f, και το θεώρημα μας λέει ότι κάθε αναδρομική συνάρτηση παράγεται από πρωτογένως αναδρομικές μέσω μόνο μια ελαχιστοποίησης. Το σημάντικο είναι ότι η συνάρτηση U είναι ανεξάρτητη της f επομένως αν θέσουμε,

$$\phi^n(e, x_1, , \ldots, x_n) = \phi^n_e(x_1, \ldots, x_n) = U(\mu y T_n(e, x_1, x_2, \ldots, x_n, y),$$

τότε η $\phi^n(e, x_1, \ldots, x_n)$ είναι αναδρομική και προκύπτει μέσω αυτής μια απαρίθμηση όλων των n-μελών αναδρομικών συνάρτησεων.

Μια ενδιαφέρουσα ερμηνεία του θεωρήματος κανονικής μορφής είναι η εξής, η συνάρτηση U παίζει τον ρόλο του υπολογιστή που έχουμε στο σπίτι μας, ο οποίος δοθέντος του κωδικού ένος προγράμματος (δηλαδή μιας αναδρομικής συνάρτησης) και μιας εισόδου από εμάς, τρέχει το πρόγραμμα, όπως θα λέγαμε, και μας επιστρέφει την έξοδο, η οποία δεν είναι άλλη από τον τελευταίο υπολόγισμο πού έκανε με το πρόγραμμα πριν βρεθεί σε κατάσταση τερματισμού.

1.3 Υπολογισιμότητα και η Θέση Church-Turing

Όπως έχουμε ήδη αναφέρει οι αναδρομικές συνάρτησεις δεν είναι ο μοναδικός τρόπος να έχουμε ένα μοντέλο υπολογισμού. Υπάρχει επίσης το μοντέλο το οποίο βασίζεται στις μηχανές Turing, αλλά στην παρούσα εργασία δεν θα ασχοληθούμε με αυτό. Ο αναγνώστης μπορεί να αναζητήσει περισσότερα σε ένα από τα [1],[7]. Το πιο διαισθητικό, αλλά δυστύχως όχι το πιο αυστηρό από μαθηματικής σκοπίας, είναι το να περιγράφουμε τους υπολογισμούς που πρέπει να γίνουν για να έχουμε τις τιμές μιας συνάρτησης μέσω διαδικάσιων με σαφώς καθορισμένα βήματα και υπολογισμούς, ή με μία λέξη μέσω ενός αλγορίθμου. Το κάλο με το συγκεκριμμένο μοντέλο είναι, αφ᾽ ενός ότι είναι πολύ κοντά στη διαίσθηση μας, αφ᾽ ετέρου αποφεύγονται οι μακροσκελείς ισχυρισμοί που θα

χρειαζόμασταν για να παρουσιάσουμε τον κύριο κορμό της παρούσας εργασίας, κάνοντας πόλλες από τις ιδέες και τα επιχειρήματα που θα χρησιμοποιούμε στη συνέχεια πολύ πιο έυκολα διαχειρίσιμα από τον αναγνώστη.

Σκόπος μας λοιπόν σε αυτή την σύντομη ενότητα είναι να παρούσιάσουμε την πιο διαισθητική έννοια της υπολογίσιμης συνάρτησης και να πειστούμε για την ισοδυναμία της με την έννοια της αναδρομικής συνάρτησης, μέσω της Θέσης Church-Turing. Ξεκινάμε λοίπον με τον επομένο ορισμό.

Ορισμός 1.3.1. Μια συνάρτηση $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ θα λέγεται υπολογίσιμη (computable) αν υπάρχει αλγόριθμος που την υπολογίζει, δηλαδή ένας αλγόριθμος A ο οποίος,

(i) Αν η τιμή $f(x_1, \ldots, x_k)$ ορίζεται, τότε ο αλγόριθμος A με είσοδο $(x_1, \ldots, x_k)$ τερματίζει και μας επιστρέφει το $f(x_1, \ldots, x_k)$.

(ii) Αν η τιμή $f(x_1, \ldots, x_k)$ δεν ορίζεται τότε ο αλγόριθμος A με είσοδο $(x_1, \ldots, x_k)$ δεν τερματίζει.

Δηλαδή υπολογίσιμη συνάρτηση θεωρούμε οποιαδήποτε συνάρτηση μπορεί να υπολογίστει μεσώ ενός εντελώς μηχανικού τρόπου. Την έννοια μηχανικό μπορούμε να την εκλάβουμε εδώ κυριολέκτικα, εφόσον σκοπός μας είναι να μπορούμε να υπολογίζουμε συνάρτησεις, ακόμα και αν δεν “ σκέφτομαστε ” τι κάνουμε, αρκεί να μπορούμε πρώτον να αναγνωρίζουμε τι πρέπει να κάνουμε και δέυτερον πότε πρέπει να το κάνουμε. Ακολουθώντας δηλάδη τυφλά κάποια βήματα να είμαστε σε θέση να καταλήξουμε στο ζητούμενο.

Το ερώτημα που εύλογα μπορεί να θέσει κανείς είναι το εξής: είναι κάθε αναδρομική συνάρτηση υπολογίσιμη; Η απάντηση σε αυτό είναι μάλλον εύκολη, εφόσον από τον τρόπο που όριζονται οι αναδρομικές συνάρτησεις, μας παρέχουν από μόνες τους την διαδικασία υπολογισμού τους. Για παράδειγμα, ή συνάρτηση $prod(x, y) = xy$ είναι αναδρομική και ορίζεται μέσω της

$$prod(x, 0) = 0 \quad \text{και} \quad prod(x, y + 1) = sum(prod(x, y), P_1^2(x, y)),$$

άρα για να υπολογίσω το γινόμενο δυο φυσικών η παραπάνω αναδρομή μας λέει, αν ένας εκ των δύο είναι μηδέν, τότε επίστρεψε μηδέν, διαφορετικά υπολόγισε για $i = 0, 1, \ldots, y - 1$ τα $prod(x, i + 1) = sum(prod(x, i), P_1^2(x, i))$ και επίστρεψε τον τελευταίο αριθμό που θα υπολογίσεις.

Τι γίνεται όμως με το αντίστροφο ερώτημα; Είναι κάθε υπολογίσιμη συνάρτηση αναδρομική; Η απάντηση εδώ δεν είναι άπλη, ή πιο σωστά δεν έχει απάντηθει ακόμη, αλλά υπόθετούμε πως ισχύει, καθώς το ερώτημα έχει περισσότερο φιλοσοφικό χαρακτήρα παρά μαθηματικό. Δηλαδη το ερώτημα είναι ισοδύναμο με το εξής: χρειάζομαστε περισσότερα από απλές συνθέσεις συναρτήσεων, βρόγχους (αναδρομή) και έναν τρόπο αναζήτησης ώστε να κατασκευάζουμε αλγοριθμούς οι οποίοι να υπολογίζουν συνάρτησεις; Είναι πολύ πιθανό

η διαίσθηση μας να μας οδηγήσει άμεσα στο συμπέρασμα ότι, πράγματι αυτά αρκούν, παρ' όλα αυτα, απάντηση δεν μπορεί να δωθεί με έναν αυστηρά μαθηματικά τρόπο. Γι' αύτο το λόγο έχουμε την Θέση των Church-Turing.

Θέση Church-Turing. Μια συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}$ είναι υπολογίσιμη (σύμφωνα με τον ορισμό 1.3.1) αν και μόνο αν είναι αναδρομική.

Η παραπάνω πρόταση δεν γίνεται να αποδειχθεί γιατί η μία αναφέρεται σε ένα συγκεκριμένο μοντέλο ενώ η άλλη στο γενικότερο πλαίσιο της διαίσθησης μας για την έννοια του υπολογίσιμου. Αυτό που έχει αποδειχθεί είναι ότι μια συνάρτηση είναι αναδρομική αν και μόνο αν υπολογίζεται από μία μηχανή Turing, και αντίστοιχα αποτελέσματα για όλα μοντέλα για την θεωρία υπολογισιμότητας όπως ο λ-λογισμός του Alonzo Church, τα οποία οδήγησαν τους μαθηματικούς προς την απόδοχη της παραπάνω θεσης.

Με βάση λοιπόν τα παραπάνω ο ορισμός 1.3.1 είναι ισοδυνάμος του ότι μια συνάρτηση f είναι αναδρομική. Φυσικά όλες οι έννοιες που είδαμε στην ενότητα 1.2 ορίζονται ανάλογα όπως τα υπολογίσιμα σύνολα, υπολογίσιμα απαριθμήτα σύνολα και τα λοιπά, καθώς επίσης και οι λιγοστές προτάσεις που αναφέραμε.

Θα μπορούσαμε εναλλακτικά να πούμε ότι όλες οι συναρτήσεις που θα συναντήσουμε είναι ακριβώς εκείνες για τις οποίες μπορούμε να γράψουμε ένα πρόγραμμα που να τις υπολογίζει, σε μια από τις γλώσσες Java ή C++, το οποίο θα ήταν επίσης ισοδύναμο με τα όσα έχουμε αναφέρει. Εμείς από εδώ και στο εξής θα επιχειρηματολογούμε για την αναδρομικότητα-υπολογισιμοτητα μιας συνάρτησης κυρίως με βάση τον ορισμό 1.3.1, ενώ σε κάποιες άλλες περιπτώσεις με βάση τα όσα είδαμε στις ενότητες 1.1 και 1.2. Για το λόγο αύτο κλείνουμε αυτή την ενότητα με ένα εργαλείο από τη θεωρία αλγορίθμών τα οποία θα χρησιμοποιούμε αρκετά.

Έστω αλγόριθμος A με $Dom(A) \subset \mathbb{N}^k$. Επεδή αρκετές φορές στα επόμενα κεφάλαια θα τροφοδοτούμε αλγορίθμους με μια σειρά από εισόδος $\vec{x}_1, \vec{x}_2, \ldots$, θέλουμε να αποφύγουμε περιπτώσεις όπου για κάποια απ' αυτές ο αλγόριθμος δεν τερματίζει, π.χ. $A(\vec{x}_i) \uparrow$ γιατί ποτέ δεν θα περάσουμε στον υπολόγισμο του $A(\vec{x}_{i+1})$. Γι αυτό το λόγο σε κάθε αλγόριθμο αντιστοιχίζουμε τον εξής ολικό αλγόριθμο T_A, $Dom(T_A) = \mathbb{N}^{k+1}$ με

$$T_A(\vec{x}, n) = \begin{cases} y, & \text{αν } A(\vec{x}) = y \text{ σε } \leq n \text{ βήματα.} \\ \text{δεν ορίζεται}, & \text{διαφορετικά.} \end{cases}$$

Έχοντας τώρα εισόδους $\vec{x}_1, \vec{x}_2, \ldots$ για τον A, θα λέμε ότι υπολογίζουμε παράλληλα τα $A(\vec{x}_i)$, όταν τρέχουμε τον αλγόριθμο T_A, με εισόσους $T_A(\vec{x}_i, i)$ για κάθε $i \leq l$ και για κάθε $l \in \mathbb{N}$. Δηλαδη για το $\vec{x}_1$ εκτελούμε ένα βήμα από τον A, έπειτα δύο βήματα του A για τα $\vec{x}_1, \vec{x}_2$ και τα λοιπά.

Κεφάλαιο 2

Πολυπλοκότητα Kolmogorov

Το 1968 στο άρθρο Three Approaches to the Quantitative Definition of Information [3], ο Andrey Kolmogorov, ορίζει για πρώτη φορά την έννοια της πολυπλοκότητας ένος πεπερασμένου αντικειμένου, ως το μήκος της μικρότερης δυνάτης περιγραφής του, σε μια προσπάθεια να περιγράψει την πληροφορία που φέρει ένα αντικείμενο δίχως να λαμβάνεται υπόψιν το πόσο πιθανό είναι να συναντήσουμε το συγκεκριμένο αντικείμενο. Παράλληλα τις ίδιες ιδέες παρουσίαζε σε άρθρα του και ο Ray Solomonoff χώρις όμως μεγάλη μαθηματική αυστηρότητα, και γι αυτό το λόγο ίσως να έχει επικρατήσει ο όρος πολυπλοκότητα Kolmogorov. Ο συγκεκριμένος τρόπος, είναι αρκετά κοντά με την διαίσθηση μας, αφού θα χαρακτηρίζαμε ένα αντικείμενο ως απλό, αν ήμασταν σε θέση να το περιγράψουμε με μεγάλη ακρίβεια πολύ σύντομα, ενώ από την άλλη, θα το χαρακτηρίζαμε ως πολύπλοκο αν για να το περιγράψουμε θα χρειαζόταν να είμαστε όλο και πιο συγκεκριμένοι σχετικά με τις ιδιότητες του.

Για παράδειγμα, θεωρήστε τις παρακάτω πεπερασμένες ακολουθίες από 0 και 1,

1. 01010101010101010101
2. 01101010000010011110
3. 10100101100000101110.

Είναι βέβαιο ότι όλοι μας θα χαρακτηρίζαμε ως απλή την ακολουθία 1, αφού πρόκειται για δέκα επαναλήψεις του 01, ενώ για τις 2 και 3 δεν είναι εύκολο να αναγνωρίσει κανείς κάποιο "μοτίβο" ώστε να τις περιγράψει με κάποιον πιο σύντομο τρόπο. Παρ' όλα αυτά, η ακολουθία 2 είναι η δυαδική αναπαράσταση του $\sqrt{2}-1$, ενώ η ακολουθία 3, είναι παράγματι μια τυχαία ακολουθία από 0 και 1. Επομένως γνωρίζοντας κανείς ότι η 2 δεν είναι τίποτα άλλο παρά μια διαφορετική κωδικοποίηση του συγκεκριμένου αριθμού, έχει μια αρκετα σύντομη περιγραφή και γι' αυτήν.

Είναι σημαντικό λοιπόν, για να μελετήσουμε αυτή την έννοια πολυπλοκότητας, να έχουμε καθορίσει τι εννοούμε λέγοντας περιγραφές για τα αντικείμενα μας. Ο λόγος είναι προφανής, χώρις ένα πλαίσιο, ή μια " γλώσσα " ώστε να περιγράφουμε τα αντικείμενα μας, ακόμη και η πιο γενική αναφορά σε κάτι θα μπορουσε να θεωρηθεί ως μια περιγραφή του. Για εμάς εδώ, τα αντικείμενά μας θα περιγράφονται μέσω υπολογίσιμων συναρτήσεων, όπως αυτές αναφέρθηκαν στο πρώτο κεφάλαιο, τις οποίες μπορούμε να τις θεωρήσουμε σαν προγράμματα σε μια γλώσσα προγραμματισμού, στην οποία βέβαια, δεν έχουμε περιορισμούς χρόνου και μνήμης.

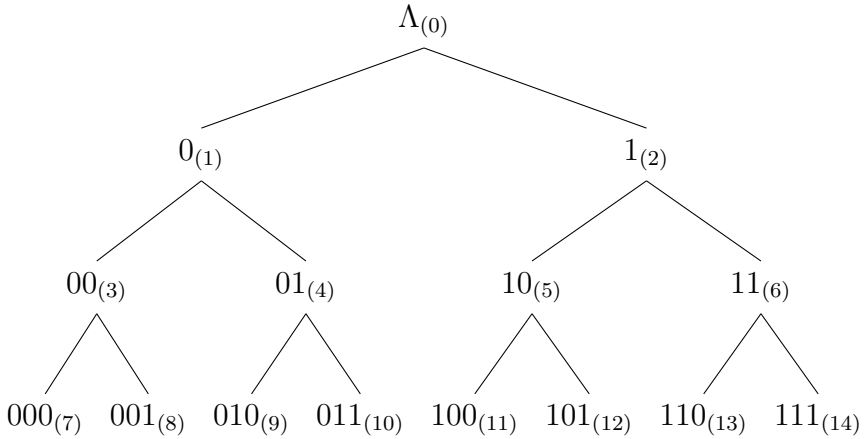
Τα αντικείμενα από την άλλη θα είναι οι φυσικοί αριθμοί και οι πεπερασμένες ακολουθίες από 0 και 1, το σύνολο των οποίων θα συμβολίζουμε με $\{0,1\}^{<\mathbb{N}}$, δηλαδή,

$$\{0,1\}^{<\mathbb{N}} = \bigcup_{n\in\mathbb{N}} \{0,1\}^n,$$

και θα αναφερόμαστε στα στοιχεία του ως λέξεις, ενώ την κενή συνάρτηση, δηλαδή την κενή λέξη θα συμβολίζουμε με Λ. Ουσιαστικά, μπορούμε να ταυτίζουμε φυσικούς και λέξεις με βάση την εξής διάταξη στο $\{0,1\}^{<\mathbb{N}}$,

$$\begin{aligned} x \leq y \iff\ & x = y \text{ ή } l(x) < l(y) \\ & \text{ή } l(x) = l(y) \ \&\ \exists n(x(i) = y(i)\ \forall i < n \ \&\ x(n) < y(n)), \end{aligned}$$

την οποία θα αναφέρουμε ως λεξικογραφική διάταξη των λέξεων. Στο παρακάτω σχήμα φαίνεται πώς διατάσσονται η πρώτες 14 λέξεις.



Σχήμα 2.1: Η λεξικογραφική διάταξη στο $\{0,1\}^{<\mathbb{N}}$.

Με βάση αυτή την αντιστοιχία, δε θα γίνεται ουσιαστική δίακριση ανάμεσα στα δύο αυτά σύνολα, και έτσι όσα είδαμε στο πρώτο κεφάλαιο μεταφέρονται

εύκολα σε συνάρτησείς με πεδίο ορισμού και πεδίο τιμων το $\{0,1\}^{<\mathbb{N}}$. Στο πλαίσιο αυτό λοιπόν θα παρουσιάσουμε αρχικά τις βασικές ιδέες, και έπειτα θα προσπαθήσουμε να μελετήσουμε κυριώς, κάποιες ιδιότητες της συνάρτησης πολυπλοκότητας, με βασικό άξονα την θεωρία υπολογισιμότητας,

Επειδή σχεδόν όλα τα αποτελέσματα που θα συναντήσουμε στο υπόλοιπο της εργασίας, συνδέουν πόσοτητες με ένα " σφάλμα " μιας σταθεράς, και για να αποφύγουμε την επανειλημμένη χρήση της φράσης "... υπάρχει σταθερά c, τέτοια ώστε...", θα χρησιμοποιούμε το σύμβολο Landau O. Θα γράφουμε για δύο συναρτήσεις f, g, $f(x) \leq g(x) + O(1)$, εννοώντας ότι υπάρχει σταθερά c, με $f(x) \leq g(x) + c$ για κάθε x σε κάποιο συγκεκριμένο σύνολο, το οποίο θα αναφέρεται. Το σημαντικό είναι οτι σταθερά μπορεί να εξαρτάται από τις f, g, αλλά όχι από το x. Αντίστοιχα, για περιπτώσεις ισότητας, θα γράφουμε $f(x) = g(x) + O(1)$. Με $l(x)$ θα συμβολίζουμε το μήκος της λέξης x, δηλαδή,

$$l(x) = \max\{i \in \mathbb{N} \mid i = 0 \text{ ή } i - 1 \in Dom(x)\},$$

με $x^\frown y$, θα εννοούμε τη λέξη που προκύπτει με παράθεση των ψηφίων των x, y, δηλαδή

$$x^\frown y = x(0) \dots x(l(x) - 1)y(l(x)) \dots y(l(x) + l(y) - 1),$$

ενώ αν $n \leq l(x)$, με $x_{|n}$ θα συμβολίζουμε τα πρώτα n ψηφία της λέξης x, δηλαδή, $x_{|n} = x(0)x(1) \dots x(n-1)$. Τέλος, με $bin(n)$ θα συμβολίζουμε τη δυαδική αναπαράσταση του φυσικού αριθμού n, ενώ με log θα συμβολίζουμε τον λογάριθμο με βάση το 2.

2.1 Απλή Πολυπλοκότητα

Ξεκινάμε αυτή την ενότητα δίνοντας το ανάλογο της φράσης, που χρησιμοποιήσαμε και νωρίτερα, " η μικρότερη δυνάτη περιγραφή για το αντικείμενο x " στο πλάισιο στο οποίο θα εργαστούμε. Ο παρακάτω ορισμός μάζι με το θεώρημα 2.1.1 που θα αποδείξουμε παρακάτω θα μας οδηγήσουν στον ορισμό της πολυπλοκότητας Kolmogorov.

Ορισμός 2.1.1. Έστω $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ υπολογίσιμη συνάρτηση και $x \in \{0,1\}^{<\mathbb{N}}$. Ορίζούμε την πολυπλοκότητα Kolmogorov (Kolmogorov Complexity) της λέξης x ως προς την f, την ποσότητα,

$$C_f(x) = \begin{cases} \min\{l(y) \mid f(y) = x\}, & \text{αν } x \in Rng(f). \\ +\infty, & \text{αν } x \notin Rng(f). \end{cases}$$

Αν $f, g : f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ είναι υπολογίσιμες ώστε να ισχύει ότι,

$$C_f(x) \leq C_g(x) + O(1),$$

για κάθε $x \in \{0,1\}^{<\mathbb{N}}$, με τη σταθερά να είναι ανεξάρτητη της λέξης x, θα λέμε ότι η f είναι ασυμπτωτικά καλύτερη της g.

Ο ορισμός 2.1.1. όσο διαισθητικά φυσιολογικός μπορεί να φαίνεται, έχει ένα σημαντικό μειονέκτημα. Η ποσότητα $C_f(x)$ μεταβάλεται ανάλογα ποιο "πρόγραμμα" f χρησιμοποιούμε, ενώ θα θέλαμε ένα καθολικό μέτρο για την πολυπλοκότητα μιας λέξης x. Η λύση σε αυτό το πρόβλημα μας δίνεται μέσω του επόμενου θεωρήματος, πληρώνοντας όμως κάποιο τίμημα.

Θεώρημα 2.1.1 (Kolmogorov-Solomonoff)**.** *Υπάρχει υπολογίσιμη συνάρτηση $D : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ η οποία είναι ασυμπτωτικά βέλτιστη, δηλαδή για κάθε υπολογίσιμη $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$,*

$$C_D(x) \leq C_f(x) + O(1), \quad \forall\, x \in \{0,1\}^{<\mathbb{N}}.$$

Απόδειξη. Υπενθυμίζουμε αρχικά ότι κάθε υπολογίσιμη συνάρτηση έχει ένα κωδικό, και αν έχουμε τον κωδικό $e \in \mathbb{N}$ και την λέξη x μπορούμε να κωδικοποιήσουμε την πληρφορία " η υπολογίσιμη συνάρτηση με κωδικό e έχει ως είσοδο τη λέξη x" ως εξής $\langle e, x\rangle = \overline{bin(e)}01x$, με $\overline{z}$ την λέξη που παράγεται από το διπλασιασμό όλων των ψηφίων της z, δηλαδή αν π.χ. $z = 010$ τότε $\overline{z} = 001100$. Με αυτό τον τρόπο είναι εύκολο να " αποσυνθέσουμε " τον κωδικό e από τη λέξη x.

Ορίζούμε τώρα την D ως εξής,

$$D(\langle e, x\rangle) = f_e(x),$$

δηλαδή η D δεχόμενη μια είσοδο, τη σαρώνει από αριστερά από τα δεξία έως ότου συναντήσει κάπου 01, ελέγχει να ότι προηγείται του 01 αποτέλει κωδικό κάποιας υπολογίσιμης συνάρτησης, αν ναι υπολογίζει την τιμή της συγκεκριμένης συνάρτησης με είσοδο ότι βρίσκεται δεξία του 01. Ουσιαστικά η συνάρτηση D δεν είναι άλλη από την U που είχαμε συναντήσει στο Θεώρημα Κανονικής Μορφής του πρώτου Κεφαλαίου, η οποία είναι υπολογίσιμη. Τέλος για να δείξουμε ότι η D είναι ασυμπτωτικά βέλτιστη, θεωρούμε $x \in \{0,1\}^{<\mathbb{N}}$, f υπολογίσιμη με κωδικό e και έστω ότι για κάποιο $y \in \{0,1\}^{<\mathbb{N}}$ ισχύει ότι $C_f(x) = l(y)$, δηλαδή η y είναι μια f-περιγραφή της x. Από τον ορισμό της D είναι άμμεσο ότι η $z = \overline{bin(e)}01y$ είναι μια D-περιγραφή της x, όχι απαραίτητα όμως βέλτιστη. Με χρήση της ανισότητας $l(bin(e)) \leq \log(e) + 1$, έχουμε ότι,

$$C_D(x) \leq l(z) \leq l(y) + 2\log(e) + O(1) = C_{f_e}(x) + O(1),$$

το οποίο είναι το ζητούμενο αφού η σταθερά εξαρτάται μόνο από τη συνάρτηση f_e και όχι από τη λέξη x. ◇

Έχοντας αποδείξει την υπάρξη μιας ασυμπτώτικα βέλτιστης συνάρτησης, μπορούμε να " απαλαγούμε " από την εξάρτηση της ποσότητας $C(x)$ από τη συνάρτηση που χρησιμοποιούμε κάθε φορά. Δίνουμε λοιπόν τον επόμενο ορισμό.

Ορισμός 2.1.2. Θεωρούμε D μια ασυμπτωτικά βέλτιστη (συγκεκριμένη και σταθερή από εδώ και στο εξής) υπολογίσιμη συνάρτηση και $x \in \{0,1\}^{<\mathbb{N}}$, η ποσότητα,

$$C(x) = \min\{l(y) \mid D(y) = x\}, \tag{2.1}$$

ονομάζεται πολυπλοκότητα Kolmogorov της λέξης x.

Το τίμημα το οποίο πληρώνουμε για την απαλάγη του ορισμού της πολυπλοκότητας από την εκάστοτε συνάρτηση f, είναι ότι η μπορούμε να την προσδιορίσουμε μεσα στα όρια κάποιου σταθερού σφάλματος. Επίσης από το θεώρημα 2.1.1 δεν προκύπτει ότι η ασυμπτωτικά βέλτιστη συνάρτηση είναι μοναδική. Επομένως για το μόνο που είμαστε σίγουροι είναι ότι αν D_1, D_2 είναι ασυμπτωτικα βέλτιστες τότε,

$$|C_{D_1}(x) - C_{D_2}(x)| \leq O(1),$$

επομένως δεν έχει μεγάλη σημασία ποια επιλέξαμε στον ορισμό 2.1.2. Συνεχίζουμε με δύο πολύ βασικές ιδιότητες.

Πρόταση 2.1.1. *Ισχύει ότι:*

(i) Για κάθε $x \in \{0,1\}^{<\mathbb{N}}$,

$$C(x) \leq l(x) + O(1). \tag{2.2}$$

(ii) Για κάθε $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ υπολογίσιμη συνάρτηση, για κάθε $x \in Dom(f)$,

$$C(f(x)) \leq C(x) + O(1). \tag{2.3}$$

Απόδειξη. (i) Η ταυτοτική συνάρτηση $id : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ είναι υπολογίσιμη και για κάθε $x \in \{0,1\}^{<\mathbb{N}}$ είναι άμμεσο ότι $C_{id}(x) = l(x)$. Επομένως από το Θεώρημα 2.1.1. έχουμε ότι υπάρχει σταθερά c τ.ω. $C(x) \leq C_{id}(x) + c$ ή ισοδύναμα $C(x) \leq l(x) + O(1)$ για κάθε $x \in \{0,1\}^{<\mathbb{N}}$.
(ii) Έστω f υπολογίσιμη συνάρτηση και $x \in \{0,1\}^{<\mathbb{N}}$ με πολυπλοκότητα $C(x)$, δηλάδη για κάποιο $y \in \{0,1\}^{<\mathbb{N}}$ έχουμε ότι $D(y) = x$ και $C(x) = l(y)$. Η συνάρτηση $f \circ D$ είναι υπολογίσιμη και εφόσον το y είναι βέλτιστη περιγραφή για το x τότε, το y είναι μια $f \circ D$-περιγραφή του $f(x)$ (αν φυσικά $f(x) \downarrow$) όχι απαραίτητα βέλτιστη, επομένως

$$C_{f\circ D}(f(x)) \leq l(y) = C(x).$$

Άρα από το Θεώρημα 2.1.1. έχουμε ότι,

$$C(f(x)) \leq C_{f \circ D}(f(x)) + O(1) \leq C(x) + O(1),$$

το οποίο ολοκληρώνει την απόδειξη. ◇

Η ιδιότητα (ii) της προηγούμενης πρότασης θα μας είναι εξαιρέτικα χρήσιμη στη συνέχεια και θα τη σχρησιμοποιήσουμε σε αρκετές αποδείξεις. Με βάση το (ii) για παράδειγμα συμπεραίνουμε ότι άλλαζοντας το πρώτο ή το τελευταίο ψηφίο μιας λέξης, προσθέτοντας ή αφαιρώντας κάποιο ψηφίο στην αρχή ή στο τέλος μιας λέξης θα μεταβάλουμε την πολυπλοκότητα της το πολύ κατα μιά σταθερά.

Στην επόμενη πρόταση θα απόδείξουμε ότι η σταθέρα που εμφανίζεται στην σχέση 2.2 δεν γίνεται να παραληφθεί, το οποίο θα έχει σημαντικές συνέπειες όπως θα δούμε παρακάτω.

Πρόταση 2.1.2. *Για κάθε $n \in \mathbb{N}$ υπάρχει $x \in \{0,1\}^{<\mathbb{N}}$ με $l(x) = n$ και $C(x) \geq n$.*

Απόδειξη. Έστω $n \in \mathbb{N}$. Υπάρχουν $2^n - 1$ λέξεις μήκους μικρότερου από n και ακριβώς 2^n λέξεις μήκους n. Επομένως αν y_x είναι η $D-$βέλτιστη περιγραφή του x, διαφορετικά x θα έχουν προφανώς διαφορετικά y_x, έχουμε ότι θα πρέπει να υπάρχει τουλάχιστον μια λέξη x μήκους n η οποία θα περιγράφεται μέσω της D από λέξη y_x μήκους μεγαλύτερου ή ίσου από n. ◇

Λέξεις για τις οποίες ισχύει ότι $C(x) \geq l(x)$ θα λέγονται Kolmogorov random. Με βάση την πρόταση 2.1.2. θα αποδείξουμε ότι η C δεν γίνεται να είναι υπολογίσιμη.

Θεώρημα 2.1.2. *Η συνάρτηση $C : \{0,1\}^{<\mathbb{N}} \to \mathbb{N}$ δεν είναι υπολογίσιμη.*

Απόδειξη. Προς απαγωγή σε άτοπο υποθέτουμε ότι η C είναι υπολογίσιμη. Μπορουμε τότε να ορίσουμε την συνάρτηση $F : \mathbb{N} \to \{0,1\}^{<\mathbb{N}}$ ως εξής,

$$F(n) = \text{η πρώτη λέξη } x \text{ τ.ω. } C(x) \geq n,$$

όπου με πρώτη εννόουμε την μικρότερη στην λεξικογραφική διάταξη. Από τον ορισμό της F και την υποθέση μας ότι η C είναι υπολογίσιμη έπεται ότι και η F είναι υπολογίσιμη αφού για κάθε n υπολογίζουμε την τιμή της F ως εξής, υπολογίζουμε παράλληλα την πολυπλοκότητα κάθε λέξής με την σειρά που αυτές εμφανίζονται λεξικογραφικά, με το που συναντήσουμε την πρώτη λέξη x με $C(x) \geq n$, σταματάμε και θέτουμε $F(n) = x$. Είναι άμμεσο τώρα ότι η F ικανοποιεί την εξής σχέση

$$C(F(n)) \geq n, \quad \forall\, n \in \mathbb{N}.$$

Θεωρώντας το n στη δυαδική του αναπαράσταση από την σχέση 2.3 έχουμε ότι για κάθε $n \in \mathbb{N}$,

$$n \leq C(F(n)) \leq C(n) + O(1) \leq l(bin(n)) + O(1) \leq \log n + O(1),$$

το οποίο είναι άτοπο αφού η διαφορά $n - \log n$ δεν είναι άνω φραγμένη κάθως $n \to \infty$. $\diamond$

Όπως μόλις είδαμε η C δεν είναι υπολογίσιμη, μάλιστα είναι εύκολο να συμπεράνουμε από την απόδειξη του θεωρήματος 2.1.2 ότι κάθε υπολογίσιμη συνάρτηση η οποίο αποτελεί κάτω φράγμα για την C θα πρέπει αναγκαστικά να είναι φραγμένη. Παρ'όλα αυτά θα αποδείξουμε στο επόμενο θεώρημα ότι μπορουμε να προσεγγίσουμε τις τιμές της από πάνω με υπολογίσμες συναστήσεις. Πιο συγκεκριμένα θα δείξουμε ότι η συνάρτηση C είναι άνω ημιυπολογίσιμη.

Μια συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \mathbb{N}$ καλείται άνω ημιυπολιγίσιμη (upper semicomputable) αν υπάρχει $F : \{0,1\}^{<\mathbb{N}} \times \mathbb{N} \to \mathbb{N}$ υπολογίσιμη τ.ω. για κάθε $x \in \{0,1\}^{<\mathbb{N}}$ να ισχύει,

$$F(x,0) \geq F(x,1) \geq \cdots \geq F(x,n) \geq \ldots$$

καθώς και

$$f(x) = \lim_{n\to\infty} F(x,n).$$

Είναι εύκολο να δούμε ότι μια f ικανοποιεί τα παραπάνω αν και μόνο αν το άνω γράφημα της, δηλαδή το σύνολο $Gr_<(f) = \{(x,n) \mid f(x) < n\}$, είναι αναδρομικά απαριθμητό. Πράγματι, έστω f άνω ημιυπολογίσιμη, για να απαριθμήσουμε το $Gr_<(f)$ χρησιμοποιούμε την F ως εξής, υπολογίζουμε παράλληλα τις τιμές $F(x,k)$ για όλα $x \in \{0,1\}^{<\mathbb{N}}$ και $k \in \mathbb{N}$, και κάθε φορά που βρίσκουμε κάποιο k τ.ω. $F(x,k) < n$ εμφανίζουμε το $\langle x,k\rangle$ στην απαρίθμηση του $Gr_<(f)$, αφού

$$f(x) < n \iff \exists k(F(x,k) < n).$$

Αντίστροφα αν το $Gr_<(f)$ είναι αναδρομικά απαριθμητό τότε υπάρχει αλγόριθμός ο οποίος απαριθμεί τα στοιχεία του. Θέτουμε $F(x,k)$ να είναι το μικρότερο $n \in \mathbb{N}$ τ.ω. το ζευγάρι $(x,n+1)$ έχει επιστραφεί από τον αλγόριθμο μετά από k βήματα του αλγορίθμου. Αν δεν υπάρχει τέτοιο n θέτουμε $F(x,k) = +\infty$ και συνεχίζουμε. Η F είναι φθίνουσα ως προς k αφού στο $k+1$ βήμα θα παίρνουμε το έλαχιστο ένος υπερσυνόλου από αυτό που είχαμε στο k βήμα, και προφανώς φράσσονται από το $f(x)$.

Θα χρησιμοποιήσουμε την παραπάνω ισοδυναμία για αν αποδείξουμε το επόμενο θεώρημα, το οποίο επιπλεον μας λέει χονδρίκα, ότι η συνάρτηση C είναι υπό μία έννοια η μικρότερη άνω υπολογίσιμη συνάρτηση για την οποία το πλήθος των λέξεων x, για τις οποίες ισχύει $C(x) < n$ είναι το πολύ 2^n.

Θεώρημα 2.1.3. *(i) Η συνάρτηση $C : \{0,1\}^{<\mathbb{N}} \to \mathbb{N}$ είναι άνω ημιυπολογίσιμη και για κάθε $n \in \mathbb{N}$ ισχύει ότι*

$$|\{x \in \{0,1\}^{<\mathbb{N}} \mid C(x) < n\}| < 2^n. \tag{2.4}$$

(ii) Αν κάποια $C' : \{0,1\}^{<\mathbb{N}} \rightharpoonup \mathbb{N}$ είναι άνω ημιυπολογίσιμη και για κάθε $n \in \mathbb{N}$ ισχύει ότι $|\{x \in \{0,1\}^{<\mathbb{N}} \mid C'(x) < n\}| < 2^n$, τότε για κάθε λέξη $x \in \{0,1\}^{<\mathbb{N}}$ ισχύει,

$$C(x) \leq C'(x) + O(1).$$

Απόδειξη. (i) Με βάση τα σχόλια που προηγήθηκαν του Θεωρήματος 2.1.2. αρκεί να δείξουμε ότι το σύνολο $\{(x,n) \mid C(x) < n\}$ είναι αναδρομικά απαριθμητό. Για να κατασκευάσουμε έναν αλγόριθμο που απαριθμεί το συκεριμένο σύνολο θεωρούμε την ασυμπτωτικά βέλτιστη υπολογίσιμη συνάρτηση D, που χρησιποποιήσαμε στον ορισμό της C. Για κάθε k υπολογίζουμε παράλληλα τις τιμές της D πάνω στις k πρώτες λέξεις του $\{0,1\}^{<\mathbb{N}}$. Αν για κάποια λέξη z βρούμε ότι $D(z)\downarrow$ και $D(z) = x$, τότε ο αλγόριθμος επιστρέφει το ζευγάρι $(x, l(z)+1)$, έτσι εξασφαλίζεται ότι, εφόσον η λέξη z αποτελεί μια D-περιγραφή για την x θα έχουμε ότι $C(x) \leq l(z) < l(z)+1$, άρα $(x, l(z)+1) \in \{(x,n) \mid C(x) < n\}$. Επίσης απαιτούμε ο αλγόριθμος να εμφανίζει και όλα τα $(x, l(z)+2)$, $(x, l(z)+3)$..., εξαντλώντας όλα τα στοιχεία του $\{(x,n) \mid C(x) < n\}$. Τέλος, έφοσον υπάρχουν 2^k λέξεις μήκους k έχουμε ότι

$$\{x \in \{0,1\}^{<\mathbb{N}} \mid l(x) < n\} = \bigcup_{i=0}^{n-1} \{x \in \{0,1\}^{<\mathbb{N}} \mid l(x) = i\},$$

από το οποίο προκύπτει ότι,

$$|\{x \in \{0,1\}^{<\mathbb{N}} \mid l(x) < n\}| = \sum_{i=0}^{n-1} 2^i = 2^n - 1,$$

άρα, επειδή αν $C(x) < n$ τότε υπάρχει $y \in \{0,1\}^{<\mathbb{N}}$ με $l(y) < n$ και $D(y) = x$, αντιστοιχίζεται στο x δηλαδή ένα $y \in \{x \in \{0,1\}^{<\mathbb{N}} \mid l(x) < n\}$, έχουμε ότι $|\{x \in \{0,1\}^{<\mathbb{N}} \mid C(x) < n\}| < 2^n$.
(ii) Θα δείξουμε ότι υπάρχει c, ώστε για κάθε n αν $\langle x, n\rangle \in Gr_<(C')$ τότε $C(x) \leq n + c$. Εφόσον η C' είναι άνω ημιυπολογίσιμη έχουμε ότι το σύνολο $Gr_<(C')$ είναι αναδρομικά απαριθμητό, επομένως υπάρχει αλγόριθμος ο οποίος απαριθμεί τα στοιχεία του. Κατασκευάζουμε υπολογίσιμη συνάρτηση D' ως εξής, αν x_k είναι η k-οστή λέξη που εμφανίζεται στην απαρίθμηση του $Gr_<(C')$ με δεύτερη συντεταγμένη n (π.χ. για $n = 3$ και $k = 1$, x_1 θα είναι η πρώτη συντεταγμένη του πρώτου ζευγαριού που θα εμφανιστεί από τον αλγόριθμο

που απαριθμεί το $Gr_<(c')$ με $C'(x) < 3$), και y_k είναι η k-όστη λέξη μήκους n όπως αυτές εμφανίζονται σε λεξικογραφική διάταξη, θέτουμε τότε $D'(y_k) = x_k$. Εφόσον από υπόθεση έχουμε ότι για κάθε n υπάρχουν λιγότερες από 2^n λέξεις με $C'(x) < n$ έχουμε ότι σίγουρα για κάθε x με $C'(x) < n$ θα βρούμε με την παραπάνω διαδικάσια μια D'-περιγραφή. Η D' είναι υπολογίσιμη, αφού για τον υπολογίσμο του $D'(y)$, αρχικα υπολογίζουμε το $l(y)$ και βρίσκουμε τη θέση του y, έστω k_y, στη λεξικογραφική διάταξη των λέξεων με μήκος $l(y)$. Έπειτα απαριθμούμε το $Gr_<(C')$ και περιμένουμε έως ότου εμφανιστούν k_y το πλήθος ζεύγη με δεύτερη συνεταγμένη $l(y)$, τότε η πρώτη συντεταγμένη του τελευταίου ζεύγους είναι το $D'(y)$.

Έστω τώρα $n \in \mathbb{N}$ και $x \in \{0,1\}^{<\mathbb{N}}$ με $C'(x) < n$, τότε από την κατασκευή της D' έχουμε ότι $C_{D'}(x) \leq n$, και από το Θεώρημα 2.1.1. έχουμε ότι υπάρχει σταθερά c ώστε,

$$C(x) \leq C_{D'}(x) + c \leq n + c, \quad \forall\, x \in \{0,1\}^{<\mathbb{N}}.$$

Άρα για κάθε $n \in \mathbb{N}$, αν $C'(x) < n$ τότε $C(x) \leq n + c$, και αφαιρώντας τώρα την πρώτη ανισότητα από τη δεύτερη καταλήγουμε ότι $C(x) \leq C'(x) + c$, που είναι και το ζητούμενο. ◇

Με βάση το (i) του θεωρήματος 2.1.3 μπορουμε να διαπιστώσουμε ότι το μεγαλύτερο ποσοστό λέξεων δεν μπορουν να έχουν και πολύ μικρότερη περιγραφή από ότι το μήκος τους. Πιο συγκεκριμένα, έστω ότι θέλουμε να βρούμε το ποσοστό των λέξεων μήκους n που έχουν πολυπλοκότητα μικρότερη από $n - k$ για $k < n$, τότε

$$\frac{|\{x \in \{0,1\}^{<\mathbb{N}} \mid l(x) = n, C(x) \leq n - k\}|}{|\{x \in \{0,1\}^{<\mathbb{N}} \mid l(x) = n\}|} \leq \frac{2^{n-k+1}}{2^n} = 2^{-k+1}.$$

Για παράδειγμα αν $n = 1000$ και $k = 10$, τότε το ποσοστό των λέξεων μήκους 1000, τις οποίες μπορούμε να περιγράψουμε με λιγότερα από 990 ψηφία είναι μικρότερο του 0.2%!

Η επόμενη πρόταση μας δίνει ένα και ένα κάτω φράγμα για το πλήθος των λέξεων με πολυπλοκότητα μικρότερη του n.

Πρόταση 2.1.3. *Υπάρχουν σταθερές c_1, c_2 τέτοιες ώστε,*

$$2^{n-c_1} \leq |\{x \in \{0,1\}^{<\mathbb{N}} \mid C(x) < n\}| \leq 2^{n+c_2} \quad \forall\, n \in \mathbb{N}.$$

Απόδειξη. Για την δεξία ανισότητα είδαμε ότι σε κάθε λέξη x με $C(x) < n$ αντιστοιχίζεται μια λέξη y με $l(y) < n$ επομένως

$$|\{x \in \{0,1\}^{<\mathbb{N}} \mid C(x) < n\}| \leq |\{y \in \{0,1\}^{<\mathbb{N}} \mid l(y) < n\}| < 2^n,$$

άρα μπορούμε να επιλέξουμε $c_2 = 0$. Για την αριστερή ανισότητα, γνωρίζουμε από την Πρόταση 2.1.1. ότι υπάρχει σταθερά c έτσι ώστε $C(x) \leq l(x) + c$ για κάθε x. Άρα αν $n \in \mathbb{N}$, τότε κάθε λέξη μήκους $l(x) < n-c$ έχει πολυπλοκότητα $C(x) < n$, επομένως για $c_1 = c$ έχουμε ότι

$$2^{n-c_1} = |\{y \in \{0,1\}^{<\mathbb{N}} \mid l(y) < n - c_1\}| \leq |\{x \in \{0,1\}^{<\mathbb{N}} \mid C(x) < n\}|,$$

το οποίο ολοκληρώνει την απόδειξη. ◇

Παρατηρώντας κυρίως το (ii) του θεωρήματος 2.1.3, συμπεράινουμε ότι η C θα μπορούσε να όριστει και ώς, η έλαχιστη (modulo μια σταθερά) άνω ημιυπολογίσιμη συνάρτηση η οποία η ικανοποιεί την 2.4. Έχοντας αποδείξει μερικές ιδιότητες για τη συνάρτηση C, ολοκληρώνουμε την ενότητα αυτή με ένα θέωρημα παρόμοιο με το 2.1.3 υπο την έννοια ότι μας παρέχει έναν αξιώματικο τρόπο ορισμού της C, αυτή τη φορά με διαφορέτικα κριτήρια.

Θεώρημα 2.1.4. *Έστω συνάρτηση $\kappa : \{0,1\}^{<\mathbb{N}} \rightharpoonup \mathbb{N}$ για την οποία υποθέτουμε πως ισχύουν τα παρακάτω:*

(i) Η κ είναι άνω ημιυπολογίσιμη.

(ii) Για κάθε υπολογίσιμη $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ ισχύει ότι

$$\kappa(f(x)) \leq \kappa(x) + O(1) \quad \forall\, x \in Dom(f).$$

(iii) Υπάρχουν σταθερές c_1, c_2 τέτοιες ώστε

$$2^{n-c_1} \leq |\{x \in \{0,1\}^{<\mathbb{N}} \mid \kappa(x) < n\}| \leq 2^{n+c_2} \quad \forall\, n \in \mathbb{N}.$$

Τότε για κάθε λέξη x, $\kappa(x) = C(x) + O(1)$.

Απόδειξη. Παρατηρούμε αρχικά ότι η κ ικανοποιεί τις υποθέσεις του Θεωρήματος 2.1.2.(ii) επομένως ισχύει ότι $C(x) \leq \kappa(x) + O(1)$, άρα μένει να δείξουμε ότι $\kappa(x) \leq C(x) + O(1)$.

Δείχνουμε αρχικά ότι υπάρχει σταθερά c και υπολογίσιμη ακολουθία από πεπερασμένα σύνολα λέξεων $M_0, M_1, \ldots$ (δηλαδή υπάρχει αλγόριθμος ο οποίος με είσοδο n επιστρέφει τα στοιχεία του M_n) με

$$M_0 \subset M_1 \subset \cdots \subset M_i \subset \ldots,$$

τέτοια ώστε για κάθε i ισχύει ότι $|M_i| = 2^i$ και $\kappa(x) \leq i + c$ για κάθε $x \in M_i$.

Από την υπόθεση (iii), για $n = i + c_1$ έχουμε ότι το σύνολο

$$A_i = \{x \in \{0,1\}^{<\mathbb{N}} \mid \kappa(x) < i + c_1\},$$

έχει τουλάχιστον 2^i στοιχεία, επίσης πάλι από την (iii) κάθε A_i είναι πεπερασμένο και συνεπώς αναδρομικό. Από τα A_i παράγουμε σύνολα B_i ως εξής, δοθέντος i, απαριθμούμε τα στοιχεία του A_i και περιμένουμε έως ότου εμφανιστούν τα πρώτα 2^i στοιχεία του. Όσα στοιχεία έχουν εμφανιστεί μέχρι εκείνη τη στιγμή είναι οι λέξεις που ανήκουν στο B_i. Από τον ορισμό των B_i έχουμε ότι, αν $x \in B_i$ τότε $\kappa(x) < i + c_1 < i + 1 + c_1$, επομένως $x \in A_{i+1}$ αλλά όχι απαραίτητα στο B_{i+1}. Για να αποφύγουμε αυτό το λάθος, ορίζουμε επαγωγικά τα M_i, με

(1) $M_0 = B_0$

(2) $M_{i+1} = M_i \cup B_{i+1}$,

δηλαδή το M_{i+1} προκύπτει από το M_i και όλα τα 2^i στοιχεία του B_{i+1} που δεν ανηκουν στο M_i, από το οποίο προκύπτει και ότι $|M_i| = 2^i$. Από την παραπάνω κατασκευή είναι άμμεσο ότι δοθέντος i και αφού τα A_i είναι αναδρομικά μπορούμε να έχουμε έναν αλγόριθμο ο οποίος μας εμφανίζει τα στοιχέια του M_i και άρα $\{M_i\}_{i\in\mathbb{N}}$ είναι υπολογίσιμη.

Δείχνουμε τώρα ότι $\kappa(x) \leq l(x)+O(1)$. Θεωρούμε $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ με $dom(f) = \bigcup_i M_i$, η οποία είναι υπολογίσιμη και απεικονίζει 1-1 για κάθε i το $M_{i+1}\backslash M_i$ στο σύνολο των λέξεων μήκους i (το $M_{i+1}\backslash M_i$ έχει ακριβώς 2^i στοιχεία), η f θα μπορουσε να οριστεί για παραδειγμά με χρήση της λεξικογραφικής διάταξης των συνόλων που αντιστοιχίζει. Από την υπόθεση (ii) έχουμε ότι $\kappa(f(x)) \leq \kappa(x) + O(1)$, για κάθε $x \in Dom(f)$. Έστω τώρα λέξη x, τότε υπάρχει $y \in M_{l(x)+1}\backslash M_{l(x)}$ τέτοια ώστε $f(y) = x$, άρα έχουμε ότι

$$\begin{aligned}\kappa(x) = \kappa(f(y)) &\leq \kappa(y) + O(1)\\ &\leq l(x) + 1 + c_1 + O(1)\\ &\leq l(x) + O(1),\end{aligned}$$

οπού η δεύτερη ανισότητα προκύπτει από το γεγονός ότι $y \in M_{l(x)+1}$ και τον ορισμό των M_i.

Είμαστε έτοιμοι τώρα να δείξουμε ότι $C(x) \leq \kappa(x) + O(1)$. Έστω $x, y \in \{0,1\}^{<\mathbb{N}}$ όπου y είναι μια D-βέλτιστη περιγραφή του x, όπου D η ασυμπτωτικά βέλτιστη υπολογίσιμη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της C. Έχουμε τότε με χρήση της υπόθεσης (ii) ότι,

$$\kappa(x) = \kappa(D(y)) \leq \kappa(y) + O(1) \leq l(y) + O(1) = C(x) + O(1),$$

το οποίο ολοκληρώνει την απόδειξη. ◇

2.2 Πολυπλοκότητα Kolmogorov Ζεύγους

Σε αυτό το μέρος θα δώσουμε νόημα αρχικά στην "από κοινού" πολυπλοκότητα $C(x, y)$ δύο λέξεων x, y, και έπειτα θα αποδείξουμε κάποιες βασικές ιδότητες της κάθως και το πώς σχετίζεται με τις επιμέρους πολυπλοκότητες $C(x)$ και $C(y)$.

Για να ορίσουμε την πολυπλοκότητα του ζεύγους (x, y) χρειαζόμαστε ένα (υπολογίσιμο) τρόπο να κωδικοποιούμε τις δύο λέξεις σε μία. Μια πρώτη ιδεά θα ήταν να χρησιμοποιήσουμε την απλή παράθεση λέξεων, δηλαδη τη λέξη $z = x^\frown y$. Ο συγκεκριμένος τροπός έχει το έξης μειονέκτημα, ότι δεν είναι 1-1 και συνεπώς δεν μπορούμε να αντιστρέψουμε την όλη διαδικασία. Χρειαζόμαστε λοιπόν μια απεικόνιση $[\cdot, \cdot] : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \to \{0,1\}^{<\mathbb{N}}$ υπολογίσιμη, 1-1 και με υπολογίσιμη αντίστροφη. Ένα παράδειγμα μιας τέτοιας απεικόνισης είναι η $[x, y] = \bar{x}01y$, η οποία είναι εύκολο να διαπιστώσουμε ότι ικανοποιεί και τις τρείς απαιτήσεις μας. Είμαστε έτοιμοι τώρα να δώσουμε τον ορισμό της πολυπλοκότητας ζεύγους σταθεροποιώντας μια κωδικοποίηση $[\cdot, \cdot]$.

Ορισμός 2.2.1. Έστω $x, y \in \{0,1\}^{<\mathbb{N}}$. Ορίζουμε την πολυπλοκότητα του ζεύγους (pair complexity) x, y ως,

$$C(x, y) = C([x, y]), \tag{2.5}$$

όπου $[\cdot, \cdot] : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \to \{0,1\}^{<\mathbb{N}}$ υπολογίσιμη απεικόνιση, 1-1 και έχει υπολογίσιμη αντίστροφη.

Αξίζει να σημειώθει ότι αν έχουμε $P, F : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \to \{0,1\}^{<\mathbb{N}}$, υπολογίσιμες, ολικές, 1-1, και οι P^{-1}, F^{-1} επίσης υπολογίσιμες, τότε οι $P \circ F^{-1}$ και $F \circ P^{-1}$ είναι υπολογίσιμες, άρα από την σχέση 2.3 έχουμε ότι,

$$\begin{aligned} C(P \circ F^{-1}(y)) &\leq C(y) + O(1), \quad \forall\, y \in Rng(F) \\ C(F \circ P^{-1}(y)) &\leq C(y) + O(1), \quad \forall\, y \in Rng(P) \end{aligned}$$

από το οποίο προκύπτει ότι,

$$\begin{aligned} C(P(x)) &\leq C(F(x)) + O(1), \quad x \in \{0,1\}^{<\mathbb{N}} \\ C(F(x)) &\leq C(P(x)) + O(1), \quad x \in \{0,1\}^{<\mathbb{N}}. \end{aligned}$$

Δηλαδή, αλλάζοντας την κωδικοποίηση, η πολυπλοκότητα του ζεύγους $\langle x, y\rangle$ διαφέρει μόνο κατα μία σταθερά. Συνεχίζουμε με κάποιες ιδιότητες.

Πρόταση 2.2.1. *Για κάθε $x, y \in \{0,1\}^{<\mathbb{N}}$ ισχύουν τα εξής:*

(i) $C(x) \leq C(x, y) + O(1)$ *και* $C(y) \leq C(x, y) + O(1)$.

(ii) $C(x,x) = C(x) + O(1)$.

(iii) $C(x,y) = C(y,x) + O(1)$.

Απόδειξη. (i) Θέτουμε $A([x,y]) = P_1^2([x,y]^{-1}) = x$ η οποία είναι προφανώς υπολογίσιμη, άρα από τη σχέση 2.3 έχουμε ότι

$$C(x) = C(A([x,y])) \leq C([x,y]) + O(1) = C(x,y) + O(1).$$

Ανάλογα αποδεικνύεται και η δεύτερη ανισότητα.
(ii) Λόγω της (i) αρκεί να δείξουμε ότι $C(x,x) \leq C(x) + O(1)$. Αυτό είναι άμμεσο αφού η απεικόνιση $x \mapsto [x,x]$ είναι υπολογίσιμη επομένως πάλι από τη σχέση 2.3 καταλήγουμε στο ζητούμενο.
(iii) Για την $C(x,y) \leq C(y,x) + O(1)$, θέτουμε

$$A([y,x]) = [P_1^2([y,x]^{-1}), P_2^2([y,x]^{-1})] = [x,y],$$

άρα από τη σχέση 2.3. έπεται ότι,

$$C(x,y) = C([x,y]) = C(A([y,x])) \leq C([y,x]) + O(1) = C(y,x) + O(1).$$

Αντίστοιχα αποδεικνύεται και η αντίστροφη ανισότητα, επομένως καταλήγουμε ότι $C(x,y) = C(y,x) + O(1)$. ◇

Πρόταση 2.2.2. *Για κάθε $x, y \in \{0,1\}^{<\mathbb{N}}$, ισχύει ότι,*

$$C(x,y) \leq C(x) + C(y) + 2\log(C(x)) + O(1). \tag{2.6}$$

Απόδειξη. Θεωρούμε την απεικόνιση $x \mapsto \hat{x} = \overline{bin(l(x))}01x$ και θεωρούμε την εξής συνάρτηση,

$$D'(\hat{p}q) = [D(p), D(q)],$$

όπου D η ασυμπτωτικά βέλτιστη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της C και $[\cdot,\cdot]$ η κωδικοποίηση που χρησιμοποιήσαμε στον ορισμό της πολυπλοκότητας του ζεύγους λέξεων.

Από τον τρόπο που ορίσαμε την απεικόνιση $x \mapsto \hat{x}$ είναι άμεσο ότι αν έχουμε δύο λέξεις x, y με $x \neq y$ τότε το $\hat{x}$ δεν είναι πρόθεμα του $\hat{y}$ (και αντίστροφα). Επομένως, αν υποθέσουμε ότι για κάποια p_1, p_2, q_1, q_2, με $p_1 \neq p_2$ ίσχυε ότι $\hat{p_1}q_1 = \hat{p_2}q_2$ τότε το $\hat{p_1}$ είναι πρόθεμα της λέξης $\hat{p_2}q_2$ το οποίο είναι άτοπο. Επομένως η D' είναι καλά ορισμένη. Επίσης είναι υπολογίσιμη αφού προκύπτει από συνθέσεις υπολογίσιμων συναρτήσεων.

Έστω τώρα $x, y \in \{0,1\}^{<\mathbb{N}}$ με p, q D-βέλτιστες περιγραφές αντίστοιχα. Από τον όρισμό του D' έχουμε ότι η λέξη $\hat{p}q$ είναι περιγραφή της $[x,y]$, όχι

απαραίτητα βέλτιστη επομένως,

$$\begin{aligned} C(x,y) = C([x,y]) &\leq C_{D'}([x,y]) + O(1) \\ &\leq l(\hat{p}q) + O(1) \\ &\leq 2\log(l(p)) + l(p) + l(q) + O(1) \\ &= C(x) + C(y) + 2\log(C(x)) + O(1), \end{aligned}$$

το οποίο ολοκληρώνει την απόδειξη. ◇

Αν περιοριστούμε σε λέξεις x με $l(x) \leq n$ τοτε η σχέση 2.6 γίνεται

$$C(x,y) \leq C(x) + C(y) + O(\log n), \tag{2.7}$$

δηλαδή, η από κοινού πολυπλοκότητα των x, y δεν ξεπερνά το άθροισμα των επιμέρους πολυπλοκότητων με λογαριθμικό σφάλμα.

2.3 Δεσμευμένη Πολυπλοκότητα Kolmogorov

Μερικές φορές στην καθημερινότητά μας, μας ενδιαφέρει το κατά ποσό μια συγκεκριμένη πληροφορία που έχουμε στη διάθεσή μας ή μια πληροφορία από το παρελθόν για ένα γεγονός, θα επιρεάσει το ίδιο γεγονός σήμερα ή μπορεί να μας φανεί χρήσιμη σε ένα συγκεκριμένο πρόβλημα.

Η έννοια της Δεσμευμένης ή Υπο συνθήκη Πολυπλοκότητας μοιάζει πολύ με τέτοιου είδους συλλογισμούς όπως παραπάνω. Πιο συγκεκριμένα αν x, y είναι δύο λέξεις, τότε η πολυπλοκότητα του x δεδομένου του y, την οποία θα συμβολίζουμε με $C(x|y)$, μετρά υπό μία έννοια το κατά πόσο η γνώση του y κάνει ευκολότερη την περιγραφή του x. Για τον ορισμό της $C(x|y)$ την ίδια ιδέα με την απλή πολυπλοκότητα αλλά αυτή τη φορά θα χρησιμοποιήσουμε υπολογίσιμες συναρτήσεις δύο μεταβλητών, όπου το δεύτερο όρισμα θα είναι η λέξη ως προς την οποία δεσμεύουμε. Ξεκινάμε με τον επόμενο ορισμό.

Ορισμός 2.3.1. Έστω $f : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, υπολογίσιμη συνάρτηση και $x, y \in \{0,1\}^{<\mathbb{N}}$. Ορίζουμε τη δεσμευμένη πολυπλοκότητα Kolmogorov (Conditional Kolmogorov Complexity) του x δεδομένου του y ως προς τη συνάρτηση f την ποσότητα,

$$C_f(x|y) = \begin{cases} \min\{l(z) \mid f(z,y) = x\}, & \text{αν } x \in Rng(f). \\ +\infty, & \text{αν } x \notin Rng(f). \end{cases}$$

Ακριβώς ανάλογα με την ενότητα 2.1 αν για κάποιες συνάσρτησεις f, g όπως στον ορισμό 2.3.1 ισχύει ότι

$$C_f(x|y) \leq C_g(x|y) + c,$$

για κάποια σταθερά c και για κάθε λέξη x, y, θα λέμε ότι η f είναι ασυμπτωτικά καλύτερη της g. Για να δώσουμε το ορισμό της δεσμευμένης πολυπλοκότητας θα χρειάστουμε και πάλι μια ασυμπτωτικά βέλτιστη συνάρτηση D, την οποία μας παρέχει το παρακάτω θεώρημα, αντίστοιχο του 2.1.1.

Θεώρημα 2.3.1. *Υπάρχει $D : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, υπολογίσιμη συνάρτηση, η οποία είναι ασυμπτωτικά βέλτιστη, δηλαδή για κάθε υπολογίσιμη $f : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$,*

$$C_D(x|y) \leq C_f(x|y) + O(1), \quad \forall\, x, y \in \{0,1\}^{<\mathbb{N}}.$$

Απόδειξη. Η απόδειξη είναι άναλογή του θεωρήματος 2.1.1, θέτουμε

$$D(\overline{bin(n)}01z, y) = f_n(z, y),$$

όπου n είναι ο κωδικός της υπολογίσιμης συνάρτησεις f_n. Προκύπτει ότι η D είναι υπολογίσιμη (όπως στο θεώρημα 2.1.1) και μένει να δείξουμε ότι είναι ασυμπτωτικά βέλτιστη. Πράγματι έστω f υπολογίσιμη με κώδικο e, και λέξεις x, y, z έτσι ώστε $f(z, y) = x$ και $C_f(x|y) = l(z)$, τότε το ζεύγαρι $(\overline{bin(e)}01z, , y)$ είναι μια D περιγραφή για το x, όχι όμως απαραίτητα η καλύτερη, άρα,

$$\begin{aligned} C_D(x|y) &= \min\{l(p) \mid D(p, y) = x\} \\ &\leq l(\overline{bin(e)}01z) \\ &\leq l(z) + 2\log e + 4 \\ &= C_f(x|y) + O(1), \end{aligned}$$

και η απόδειξη ολοκληρώθηκε. ◇

Ορισμός 2.3.2. Θεωρούμε D μια ασυμπτωτικά βέλτιστη (συγκεκριμένη και σταθερή από εδώ και στο εξής) υπολογίσιμη συνάρτηση δύο ορισμάτων. Τότε για $x, y \in \{0,1\}^{<\mathbb{N}}$, η ποσότητα,

$$C(x|y) = \min\{l(z) \mid D(z, y) = x\},$$

ονομάζεται δεσμευμένη πολύπλοκότητα Kolmogorov του x δεδομένου του y.

Συνεχίζουμε αποδεικνύοντας κάποιες βασικές ιδιότητες.

Πρόταση 2.3.1. *Για κάθε $x, y \in \{0,1\}^{<\mathbb{N}}$ ισχύουν τα εξής:*

(i) $C(x|y) \leq C(x) + O(1)$.

(ii) $C(x|x) = O(1)$.

(iii) $C(f(x,y)|y) \leq C(x|y) + O(1)$, *για* $f : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ *υπολογίσιμη και* $(x,y) \in dom(f)$.

(iv) $C(x|y) \leq C(x|g(y)) + O(1)$, *για* $g : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ *υπολογίσιμη και* $y \in dom(g)$.

Απόδειξη. (i) Κάθε υπολογίσιμη συνάρτηση f ενός ορίσματος μπορεί να θεωρηθεί ως συνάρτηση δύο ορισμάτων πολύ απλά ως $\tilde{f}(x,y) = f(x)$ για κάθε $(x,y) \in dom(f) \times \{0,1\}^{<\mathbb{N}}$, επομένως αν D είναι η ασυμπτωτικά βέλτιστη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της απλής πολυπλοκότητας, από το θεώρημα 2.3.1 έχουμε ότι,

$$C(x|y) \leq C_{\tilde{D}}(x|y) + O(1) = C(x) + O(1).$$

(ii) Θεωρούμε ως $f(x,y) = y$ για κάθε $x, y \in \{0,1\}^{<\mathbb{N}}$, η οποία είναι προφανώς υπολογίσιμη. Από τον ορισμό της f είναι άμμεσο ότι $f(0,y) = y$ για κάθε λέξη y, άρα για κάθε x έχουμε,

$$C_f(x|x) = min\{l(z) \mid f(z,x) = x\} = 1.$$

Επομένως από το θεώρημα 2.3.1. έχουμε ότι $C(x|x) = O(1)$.
(iii) Έστω f υπολογίσιμη συνάρτηση 2 ορισμάτων και D όπως στον ορισμό 2.3.2. Θεωρούμε μια νέα συνάρτηση D' ως εξής,

$$D'(z,y) = f(D(z,y),y),$$

η οποία είναι υπολογίσιμη ως $D' = f \circ (D, P_2^2)$. Έστω τώρα $(x,y) \in dom(f)$ και $z \in \{0,1\}^{<\mathbb{N}}$, ώστε $C(x|y) = l(z)$. Εφόσον, $D(z,y) = x$ έχουμε ότι $D'(z,y) = f(x,y)$, δηλαδή το z είναι μια D' περιγραφή για το $f(x,y)$ δεδομένου του y, άρα με βάση τον όρισμό 2.3.1. και το θεώρημα 2.3.1. έχουμε ότι,

$$C(f(x,y)|y) \leq C_{D'}(f(x,y)|y) + O(1) \leq l(z) + O(1) = C(x|y) + O(1).$$

(iv) Έστω g υπολογίσιμη, θεωρούμε τώρα D' ως εξής,

$$D'(z,y) = D(z,g(y)),$$

που είναι υπολογίσιμη αφού $D' = D \circ (P_1^2, g \circ P_2^2)$. Έστω πάλι $x, z \in \{0,1\}^{<\mathbb{N}}$ και $y \in dom(g)$, τέτοια ώστε $D(z,g(y)) = x$ και $C(x|g(y)) = l(z)$. Τότε το z είναι μια D' περιγραφή του x δεδομένου του y, άρα

$$C(x|y) \leq C_{D'}(x|y) + O(1) \leq l(z) + O(1) = C(x|g(y)) + O(1),$$

και η απόδειξη ολοκληρώνεται. ◇

Με βάση την προηγούμενη πρόταση έχουμε το εξής: έστω υπολογίσιμη άπειρη ακολουθία ω από 0 και 1, δηλαδή υπάρχει υπολογίσιμη $f : \mathbb{N} \to \{0,1\}^{<\mathbb{N}}$, με $f(n) = \omega_{|n}$. Τότε για κάθε $n \in \mathbb{N}$,

$$\begin{aligned} C(\omega_{|n}|n) &\leq C(\omega_{|n}|f(n)) \\ &= C(\omega_{|n}|\omega_{|n}) \leq d, \end{aligned}$$

όπου η d είναι σταθερά ανεξάρτητη του n. Δηλαδή αν ένα στοιχείο του $\{0,1\}^{\mathbb{N}}$ είναι υπολογίσιμο, τότε η δεσμευμένη πολυπλοκότητα κάθε αρχικού τμήματος του, ως προς το μήκους του, φράσσεται από μια σταθερά. Αποδεικνύεται ότι ισχύει και το αντίστροφο αλλά η απόδειξη του είναι πολύ πιο περίπλοκη από μια απλή παρατήρηση, όπως κάναμε εδώ. Επομένως ένα $\omega \in \{0,1\}^{\mathbb{N}}$ είναι υπολογίσιμο αν και μόνο αν υπάρχει σταθερά d, ώστε για κάθε n, $C(\omega_{|n}|n) \leq d$.

Σχέδον όλα τα αποτελέσματα που είδαμε στην ενότητα 2.1 αποδεικνύονται και στην περίπτωση της δεσμευμένης πολυπλοκότητας με ουσιαστικά τα ίδια επιχειρήματα. Παρουσιάζονται ενδεικτικά παρακάτω κάποια απο αυτά, χώρις όμως αποδείξεις.

Πρόταση 2.3.2. *Για κάθε $y \in \{0,1\}^{<\mathbb{N}}$ και κάθε $n \in \mathbb{N}$ υπάρχει λέξη x με $l(x) = n$ και $C(x|y) \geq n$.*

Θεώρημα 2.3.2. *Η συνάρτηση $C(\cdot|\cdot) : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \to \mathbb{N}$ δεν είναι υπολογίσιμη.*

Η απόδειξη για το θεώρημα 2.3.2 βασίζεται και σε αυτή την περίπτωση στην πρόταση 2.3.2.

Θεώρημα 2.3.3. *Η συνάρτηση $C(\cdot|\cdot) : \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \to \mathbb{N}$ είναι άνω ημιυπολογίσιμη και επίσης για κάθε $y \in \{0,1\}^{<\mathbb{N}}$ και $n \in \mathbb{N}$ έχουμε ότι,*

$$|\{x \in \{0,1\}^{<\mathbb{N}} \mid C(x|y) < n\}| < 2^n.$$

Για την απόδειξη του θεωρήματος αποδεικνύουμε με αντιστοίχο τρόπο όπως στο θεώρημα 2.1.3 ότι το σύνολο,

$$\{(x,y,n) \in \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \times \mathbb{N} \mid C(x|y) < n\},$$

αναδρομικά απαριθμητό, από το οποίο προκύπτει το συμπέρασμα.

Έχοντας στη διάθεση μας πλέον την δεσμευμενη πολυπλοκότητα μπορούμε να την συνδέσουμε με την πολυπλοκότητα για ζεύγη και να βελτιώσουμε αρχικά το φράγμα για την πολυπλοκότητα του ζεύγους (x,y) στη σχέση 2.6. Έχουμε λοιπόν την εξής πρόταση.

Πρόταση 2.3.3. *Ισχύει ότι,*

$$C(x,y) \leq C(x) + 2\log C(x) + C(y|x) + O(1). \tag{2.8}$$

Απόδειξη. Έστω D η ασυμπτωτικά βέλτιστη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της απλής πολυπλοκότητας και D_c η αντίστοιχη για την δεσμευμένη. Για $z, q \in \{0,1\}^{<\mathbb{N}}$ θέτουμε,

$$D'(\hat{z}q) = [D(z), D_c(q, D(z))],$$

όπου $\hat{z} = \overline{bin(l(z))}01z$ και $[\cdot,\cdot]$ όπως στον ορισμό 2.2.1.. Η D' είναι υπολογίσιμη αφού προκύπτει απο σύνθεση υπολογίσιμων συναρτήσεων.

Έστω τώρα $z, p \in \{0,1\}^{<\mathbb{N}}$ τ.ω. $D(z) = x$, $C(x) = l(z)$ και $D_c(p,x) = y$, $C(y|x) = l(p)$. Από τον όρισμό της D' έχουμε ότι η $\hat{z}p$ είναι μια D'-περιγραφή για το $[x,y]$ όχι απαραίτητα βέλτιστη, άρα

$$\begin{aligned} C(x,y) = C([x,y]) &\leq C_{D'}([x,y]) + O(1) \\ &\leq l(\hat{z}p) + O(1) \\ &\leq 2\log(l(z)) + l(z) + l(p) + O(1) \\ &= C(x) + 2\log(C(x)) + C(y|x) + O(1), \end{aligned}$$

και η σχέση 2.7 ισχύει. ◇

Και για την σχέση 2.8 έχουμε ότι αν περιοριστούμε σε λέξεις μήκους το πολύ n έχουμε ότι,

$$C(x,y) \leq C(x) + C(y|x) + O(\log n), \tag{2.9}$$

η οποία χονδρικά λέει ότι για να περιγράψουμε από κοινου τις λέξεις x, y θα χρειαστούμε το πολύ όση πληροφορία εμπεριέχεται στο x καθώς και όση πληροφορία επιπλέον μας δίνει η y (με λογαριθμική ακρίβεια).

Από το τελευταίο αποτέλεσμα αυτής της ενότητας, το οποίο ακολουθεί, προκύπτει μάλιστα ότι η 2.8 είναι στην πραγματικότητα ισότητα. Το συγκεκριμένο θεώρημα αποδείχθηκε ανεξάρτητα από τους Andrei Kolmogorov και Leonid Levin.

Θεώρημα 2.3.4 (Kolmogorov-Levin)**.** *Για κάθε λέξεις $x, y \in \{0,1\}^{<\mathbb{N}}$ με $l(x), l(y) \leq n$, ισχύει ότι,*

$$C(x,y) = C(x) + C(y|x) + O(\log n). \tag{2.10}$$

Απόδειξη. Έστω $x, y \in \{0,1\}^{<\mathbb{N}}$, μήκους το πολύ n. Λόγω της 2.8, αρκεί να δείξουμε ότι,

$$C(x,y) \geq C(x) + C(y|x) + O(\log n).$$

Έστω $c = C(x, y)$ και,

$$A = \{(z, p) \in \{0,1\}^{<\mathbb{N}} \times \{0,1\}^{<\mathbb{N}} \mid C(z, p) \leq c\},$$

για το οποίο από το θεώρημα 2.1.3 έχουμε ότι $|A| \leq 2^{c+1}$ και $(x, y) \in A$.

Για κάθε λέξη $t \in \{0,1\}^{<\mathbb{N}}$ θεωρούμε το σύνολο,

$$A_t = \{u \in \{0,1\}^{<\mathbb{N}} \mid (t, u) \in A\},$$

και θέτουμε $m = \lfloor \log(|A_x|) \rfloor \geq 0$, και άρα $2^m \leq |A_x| \leq 2^{m+1}$.

Για να καταλήξουμε στο ζητούμενο, δείχνουμε πρώτα ότι,

$$C(y|x) \leq m + O(\log n). \tag{2.11}$$

Από το θεώρημα 2.3.1 έχουμε ότι γνωρίζοντας το c, το σύνολο A είναι αναδρομικά απαριθμητό και δεδομένου του x μπορούμε να απαριθμήσουμε και το A_x, αφου απαριθμώντας το A κρατάμε κάθε φορά τα ζεύγη (z, p) για το οποία $z = x$. Επομένως για να προσδιορίσουμε το y χρειαζόμαστε τη σειρά με την οποία θα εμφανιστεί αυτο στην απαρίθμηση του A_x. Δηλαδή, έχοντας στη διάθεσή μας τον αλγόριθμο ο οποίος απαριθμεί το A_x, μπορούμε να κατασκευάσουμε ένα άλλο αλγόριθμο, ο οποίος θα έχει ως εισόδους φυσικούς αριθμούς i στη δυαδική τους αναπαράσταση, και θα μας επιστρέφει την i-οστή λέξη στην απαρίθμηση του A_x. Μέσω της διαδικασίας που περιγράψαμε παραπάνω, για τον προσδιορίσμο του y θα χρειαστούμε μια λέξη με μήκος το πολύ $\lfloor \log(|A_x|) \rfloor + 1$, ή ισοδύναμα $m + O(1)$. Τέλος από την σχέση 2.9 έχουμε ότι το c είναι μικρότερης τάξης από $O(\log n)$, άρα $C(y|x) \leq m + O(\log n)$.

Δεύτερον, δείχνουμε ότι,

$$C(x) \leq c - m + O(\log n). \tag{2.12}$$

Γι᾽ αυτό το λόγο θεωρούμε το σύνολο B ως εξής,

$$B = \{t \in \{0,1\}^{<\mathbb{N}} \mid |A_t| \geq 2^m\}.$$

Αρχικά έχουμε ότι $x \in B$ και επίσης ότι $|B| \leq 2^{c+1}/2^m$. Πράγματι, εφόσον

$$|A| = \sum_{t \in \{0,1\}^{<\mathbb{N}}} |\{t\} \times A_t| = \sum_{t \in \{0,1\}^{<\mathbb{N}}} |A_t|,$$

αν υποθέσουμε ότι $|B| > 2^{c+1}/2^m$, τότε θα προέκυπτε ότι,

$$|A| \geq \sum_{t \in B} |A_t| \geq |B| \min\{|A_t| \mid t \in B\} > \frac{2^{c+1}}{2^m} 2^m = 2^{c+1},$$

το οποίο είναι άτοπο. Επίσης το B είναι αναδρομικά απαριθμητό αφού γνωρίζοντας τα m, c και απαριθμώντας τα στοιχεία του A, συλλέγουμε τα στοιχεία με κοινή την πρώτη συντεταγμένη, αν για κάποια λέξη t έχουμε συλλέξει 2^m στοιχεία, τότε γνωρίζουμε ότι $t \in B$.

Άρα για να προσδιορίσουμε το x, αντιστοίχα όπως και παραπάνω, θα χρειαστούμε μια λέξη με μήκος το πολύ $\lfloor \log(2^{c+1}/2^m) \rfloor + 1$, δηλαδή $c - m + O(1)$. Τέλος από τον ορισμό του m, έχουμε ότι $m \leq c + 1$ και το c όπως είδαμε είναι μικρότερο από κάποιον όρο $O(\log n)$, άρα θα χρειαστουμε συνολικά $c - m + 1 + O(\log n)$, δηλαδή $C(x) \leq c - m + O(\log n)$.

Προσθέτοντας κατα μέλη τώρα τις 2.11 και 2.12 έχουμε ότι,

$$C(y|x) + C(x) \leq c + O(\log n),$$

από το οποίο προκύπτει το ζητούμενο. ◇

Σημειώνουμε ότι παραπάνω δεν χρησιμοποιήσαμε πουθενά το μήκος των λέξεων αλλά μόνο τις πολυπλοκότητες τους, επομένως η 2.10 γίνεται

$$C(x, y) = C(x) + C(y|x) + O(\log(C(x, y))).$$

2.4 Εφαρμογές

Σε αυτή την ενότητα θα δούμε μερικές εφαρμογές της πολυπλοκότητας Kolmogorov, κυρίως στην θεωρία υπολογισιμότητας.

Η πρώτη εφαρμογή έχει να κάνει με κάτι το οποίο έχουμε ήδη αναφέρει στην ενότητα 1.2, και έχει να κάνει με την ύπαρξη συνόλων τα οποία είναι αναδρομικά απαριθμητά αλλά όχι αναδρομικά. Ας θυμηθούμε ότι αν ένα αναδρομικά απαριθμητό $A \subset \mathbb{N}$ έχει συμπλήρωμα που είναι επίσης αναδρομικά απαριθμητό τότε αποδεικνύεται ότι το A είναι ανδρομικό. Επομένως, αν θέλουμε να έχουμε ένα αναδρομικά απαριθμητό σύνολο το οποίο δεν είναι αναδρομικό, θα πρέπει κάθε απόπειρα μας να απαριθμήσουμε το συμπλήρωμα του να είναι αποτυχημένη. Το συγκεκριμένο πρόβλημα δεν είναι τετριμμένο και μια κατηγορία τέτοιων συνόλων είναι τα απλά σύνολα που ορίστηκαν από τον Emil Post με σκοπό να δώθει απάντηση σε ένα ερώτημα το οποίο σήμερα είναι γνωστό ως Post's Problem. Δίνουμε τον εξής ορισμό.

Ορισμός 2.4.1. Ένα σύνολο $A \subset \{0,1\}^{<\mathbb{N}}$ καλείται απλό (simple) αν είναι αναδρομικά απαριθμητό, με το $\{0,1\}^{<\mathbb{N}} \backslash A$ άπειρο και κάθε άπειρο υποσύνολο του $\{0,1\}^{<\mathbb{N}} \backslash A$ δεν είναι αναδρομικά απαριθμητό.

Σκόπος μας είναι να αποδείξουμε την ύπαρξη απλών συνόλων με τη βοήθεια της πολυπλοκότητας Kolmogorov. Έχουμε λοιπόν το επόμενο θεώρημα.

Θεώρημα 2.4.1. *Υπάρχει $S \subset \{0,1\}^{<\mathbb{N}}$ το οποίο είναι απλό.*

Απόδειξη. Θέτουμε S να είναι το εξής σύνολο,

$$S = \{x \in \{0,1\}^{<\mathbb{N}} \mid C(x) < l(x)/2\}.$$

Κατ' αρχάς το S είναι αναδρομικά απαριθμητό, αφού από το θέωρημα 2.1.3 η C είναι άνω υπολογίσιμη, άρα υπάρχει υπολογίσιμη $F : \{0,1\}^{<\mathbb{N}} \times \mathbb{N} \to \mathbb{N}$, φθίνουσα ως προς n με $C(x) = \lim_n F(x,n)$. Επομένως,

$$x \in S \iff \exists n(F(x,n) < l(x)/2),$$

και η σχέση $F(x,n) < l(x)/2$ είναι αναδρομική, αφού και η F και η l είναι υπολογίσιμες, άρα από πρόταση 1.2.3 έχουμε ότι το S είναι αναδρομικά απαριθμητό.

Για να δούμε ότι το S έχει άπειρο συμπλήρωμα παρατηρούμε αρχικά ότι, για κάθε n το ποσοστό των λέξεων με $C(x) < n/2$ ως προς τις λέξεις μήκους n είναι το πολύ $2^{-\frac{n}{2}}$, άρα για κάθε n υπάρχει λέξη μηκούς n με $C(x) \geq n/2$, άρα το $\{0,1\}^{<\mathbb{N}} \backslash S$ είναι άπειρο.

Τέλος, προς απαγωγή σε άτοπο υποθέτουμε ότι υπάρχει $W \subset S$ άπειρο το οποίο είναι αναδρομικά απαριθμητό. Εφόσον το W είναι αναδρομικά απαριθμητό, θεωρούμε έναν αλγόριθμο ο οποίος απαριθμεί τα στοιχεία του. Για κάθε $i \in \mathbb{N}$ απαριθμήμουμε το U έως ότου ο αλγόριθμος μας εμφανίσει λέξη $u_i \in U$ με $l(u_i) \geq 2i$. Εφόσον το U είναι άπειρο είμαστε σίγουροι ότι για κάθε i υπάρχει τέτοια λέξη και επίσης λόγω αυτού να υποθέσουμε ότι για $i \neq j$, $u_i \neq u_j$ (αν για κάποια $i < j$ έχουμε $u_i = u_j$ τότε περιμένουμε μέχρι ο αλγόριθμος να εμφανισεί λέξη u'_j με $l(u'_j) > l(u_j)$ και θέτουμε $u'_j = u_j$). Έχουμε λοιπόν μια απεικόνιση $i \mapsto g(i) = u_i$, η οποία με βάση τήν διαδικάσια που περιγράψαμε παραπάνω είναι υπολογίσιμη. Από την επιλογή των u_i και το γεγονός ότι είναι στοιχεία του U, έχουμε ότι για κάθε $i \in \mathbb{N}$,

$$C(g(i)) = C(u_i) \geq \frac{l(u_i)}{2} \geq \frac{2i}{2} = i.$$

Όμως, αφού η g είναι υπολογίσιμη, από τη σχέση 2.3 σε συνδιασμό με την παραπάνω ιδιότητα της g, έχουμε ότι,

$$i \leq C(g(i)) \leq C(i) + O(1) \leq \log i + O(1),$$

το οποίο δεν ισχύει για αρκούντως μεγάλα i. Άρα δε γίνεται το U να είναι αναδρομικά απαριθμητό, και συνεπώς το S είναι απλό. ◇

Αξίζει να σημειωθεί, ότι στον ορισμό του S η επιλογή του $l(x)/2$ δεν παιζει ουσιαστικό ρόλο, θα μπορούσαμε να είχαμε $C(x) < \log(l(x))$ και έπειτα να επιλέγαμε λέξεις u_i με $l(u_i) \geq 2^i$.

Πριν συνέχισουμε, θέλουμε να δώσουμε νόημα στην πολυπλοκότητα του φυσικού αριθμού n. Με $C(n)$ λοιπόν θα εννοούμε την πολυπλοκότητα του n με βάση την λεξικογραφική διάταξη που ορίσαμε στην αρχή του κεφαλαίου. Αν με $\lambda(n)$ συμβολίσουμε την n-οστή λέξη στην διάταξη αυτή, τότε μια πρώτη προσέγγιση για την $C(n)$ είναι το μήκος $l(\lambda(n))$ της λέξης $\lambda(n)$. Ισχύριζόμαστε ότι $l(\lambda(n)) = \log n + O(1)$, πράγματι επιλέγουμε το μεγαλύτερο $m \in \mathbb{N}$ τέτοιο ώστε $2^{m+1} - 1 \leq n$, και έχουμε ότι όλες οι λέξεις που προηγούνται της $\lambda(n)$ έχουν μήκος το πολύ m, άρα η $\lambda(n)$ έχει μήκος το πολύ $m+1$ από το οποίο προκύπτει ότι το $l(\lambda(n))$ είναι περίπου όσο το $\log n$. Άρα από την σχέση 2.2 έχουμε, $C(n) \leq \log n + O(1)$.

Ορίζουμε τώρα τη συνάρτηση $B : \mathbb{N} \to \mathbb{N} \cup \{-1\}$ με τύπο,

$$B(n) = \max\{m \in \mathbb{N} \mid C(m) \leq n\}, \tag{2.13}$$

με τη σύμβαση ότι αν για κάποια μικρά n έχουμε όλες τις $C(m) > n$ τότε $B(n) = -1$. Η B εξ᾽ ορισμού έχει την ιδότητα ότι αν $k > B(n)$ τότε $C(k) > n$. Από όσα έχουμε δει στην ενότητα 2.1 έχουμε ότι η $C(m) \to \infty$ καθώς $m \to \infty$, άρα για κάθε N υπάρχει n τέτοιο ώστε $C(m) > N$ για κάθε $m \geq n$, επομένως η συνάρτηση B υπολογίζει ουσιαστικά για κάθε N το αντίστοιχο n. Η επόμενη πρόταση μας δείχνει πόσο γρήγορα αυξάνει η B.

Πρόταση 2.4.1. *Έστω $f : \mathbb{N} \rightharpoonup \mathbb{N}$ υπολογίσιμη συνάρτηση. Τότε το σύνολο $\{n \in \mathbb{N} \mid f(n) > B(n)\}$ είναι πεπερασμένο.*

Απόδειξη. Από τη σχέση 2.3 έχουμε αρχικά ότι υπάρχει σταθερά c έτσι ώστε,

$$C(f(n)) \leq C(n) + O(1) \leq \log n + c.$$

Επίσης από τον ορίσμο της B αν $f(n) > B(n)$ τότε, $C(f(n)) > n$, άρα αν $n \in \mathbb{N}$ με $f(n) > B(n)$, τότε,

$$n < C(f(n)) \leq \log n + c,$$

το οποίο ισχύει για πεπερασμένα το πλήθος n (ανάλογα τη σταθερά c κάθε φορά), άρα το $\{n \in \mathbb{N} \mid f(n) > B(n)\}$ πεπερασμένο. ◇

Η προηγούμενη πρόταση αποδεικνύει ότι οποιαδήποτε υπολογίσιμη συνάρτηση και να μας δώσουν, μπορούμε να βρούμε ένα N έτσι ώστε $f(n) \leq B(n)$, για κάθε $n \geq N$, δηλαδή η B τελικά αυξάνει πιο γρηγόρα από οποιαδήποτε υπολογίσιμη συνάρτηση.

Μπορούμε να δώσουμε και έναν εναλλακτικό ορισμό για την συνάρτηση B, χρησιμοποιώντας την υπολογίσιμη συνάρτηση D, με βάση την οποία ορισάμε την C, ως

$$B(n) = \max\{D(x) \mid l(x) \leq n\}. \tag{2.14}$$

Πράγματι αν θεωρήσουμε τις τιμές της D ως φυσικούς αριθμούς, με βάση την αντιστοιχία που είδαμε παραπάνω, τότε ισχύουν οι εξής ισοδυναμίες,

$$\begin{aligned} k \in \{m \in \mathbb{N} \mid C(m) \leq n\} &\iff \exists x, l(x) \leq n \text{ με } D(x) = k \\ &\iff k \in \{D(x) \mid l(x) \leq n\}. \end{aligned}$$

Άρα τα δύο maximum στις 2.13 και 2.14 θα ταυτίζονται. Γενικεύουμε τώρα την 2.14 σε οποιαδήποτε υπολογίσιμη συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \mathbb{N}$, συμβολίζοντας με B_f, δηλαδή,

$$B_f(n) = \max\{f(x) \mid l(x) \leq n \text{ και } f(x) \downarrow\}.$$

Με μία πολύ εύκολη παρατήρηση μπορούμε να αποδείξουμε το επόμενο.

Πρόταση 2.4.2. *Για κάθε υπολογίσιμη συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \mathbb{N}$, υπάρχει σταθερά d τέτοια ώστε,*

$$B_f(n) \leq B(n+d), \quad \forall n \in \mathbb{N}.$$

Απόδειξη. Έστω $x \in Dom(f)$ με $l(x) \leq n$. Από τις σχέσεις 2.2 και 2.3 έχουμε ότι,

$$C(f(x)) \leq C(x) + O(1) \leq n + O(1),$$

άρα υπάρχει σταθερά d έτσι ώστε $C(f(x)) \leq n + d$. Δηλάδη,

$$f(x) \in \{m \in \mathbb{N} \mid C(m) \leq n + d\},$$

και από την 2.13 έχουμε ότι $f(x) \leq B(n+d)$, άρα και $B_f(n) \leq B(n+d)$. $\diamond$

Ο σκοπός για τον οποίο ορίσαμε τις συναρτήσεις B και B_f, είναι για να προσπαθήσουμε να δώσουμε μια απάντηση στο εξής ερωτήμα:

Έστω αλγόριθμος A και $S \subset \{0,1\}^{<\mathbb{N}}$. Για δεδομένο $x \in S$, μπορούμε να αποφανθούμε αν ο A με είσοδο x τερματίζει ή όχι;

Ένα κλασσικό απότελεσμά της Θεωρίας Αναδρομής, το πρόβλημα τερματισμού, μας διαβεβαιώνει ότι σε αν $S = \{0,1\}^{<\mathbb{N}}$, τότε το παραπάνω ερώτημα δεν μπορει να απαντηθεί. Εμάς μας ενδιαφέρει η περίπτωση όπου γνωρίζουμε ότι το S περιέχει λέξεις φραγμένου μήκους, δηλαδή υπάρχει $n_0 \in \mathbb{N}$ ώστε για κάθε $x \in S$, να ισχύει ότι $l(x) \leq n_0$.

Υποθέτουμε λοιπόν ότι A είναι αλγόριθμος και σύνολο λέξεων S όπως παραπάνω. Θεωρούμε ότι σε κάθε χρονική μονάδα εκτελούμε και ένα βήμα του Α και για $x \in S$ την ποσότητα, $\tau(x)$, η οποία μετρά το πλήθος των βημάτων που κάνει ο A με είσοδο x, ή ισοδύναμα τον χρόνο υπολογίσμου του A με είσοδο

x. Η συνάρτηση $\tau : \{0,1\}^{<\mathbb{N}} \rightharpoonup \mathbb{N}$, είναι υπολογίσιμη, αφού για δεδομένο x τρέχουμε τον A με είσοδο x και μετράμε παράλληλα το πλήθος βημάτων του A που εκτελέσαμε για να υπολογίσουμε την έξοδο $A(x)$. Είναι προφανές ότι αν $A(x) \uparrow$ τότε η ποσότητα $\tau(x)$ δεν ορίζεται, επομένως $Dom(A) = Dom(\tau)$.

Εξ' ορισμού της συνάρτησης B_τ, η ποσότητα $B_\tau(n_0)$ είναι ο μέγιστος χρόνος υπολογισμού του A πάνω στα στοιχεία του S. Γνωρίζοντας τον αριθμό $B_\tau(n_0)$ ή κάποιον αριθμό k μεγαλύτερό του, μπορούμε να απάντησουμε στο αν για $x \in S$ ο A τερματίζει ή όχι: τρέχουμε τον A με είσοδο x, αν δεν τερμάτισει στα πρώτα k βήματα, τότε $A(x) \uparrow$. Τώρα από την πρόταση 2.4.2 αρκεί για τον συγκριμένο αλγόριθμο να γνωρίζουμε τη σταθέρα d, αφού τότε ισχύει ότι $B_\tau(n_0) \leq B(n_0 + d)$. Δηλαδή, μετασχηματίσαμε το αρχικό μας πρόβλημα, στην εύρεση ένος αριθμού $k \geq B(n_0 + d)$.

Ουσιαστικά παραπάνω αποδείξαμε (συνοπτικά) το εξής.

Θεώρημα 2.4.2. *Για κάθε αλγόριθμο A, υπάρχει σταθερά d και αλγόριθμος H με την εξής ιδιότητα. Για κάθε $n \in \mathbb{N}$ και κάθε $k \geq B(n+d)$, ο H με είσοδο τα n, k, επιστρέφει το σύνολο όλων των λέξεων x, με $l(x) \leq n$, για τις οποίες $A(x) \downarrow$.*

Το θεώρημα 2.4.2 μας λέει ότι πέρα από το γεγονός οτι αν γνωρίζουμε το $B(n+d)$ έχουμε με λύση για το πρόβλημα τερματισμού του A για λέξεις μήκους το πολύ n, ότι ουσιαστικά μπορούμε να υποβιβάσουμε το αρχικό μας πρόβλημα στην εύρεση του $B(n + d)$.

Κεφάλαιο 3

Προθεματική Πολυπλοκότητα

Σε αυτό το κεφάλαιο θα παρουσιάσουμε αρχικά την έννοια του ημιυπολογίσιμου μέτρου στο $\mathbb{N}$ και θα δώσουμε μια διαισθητική εξήγησή τους με τη χρήση μη ντετερμινιστικών αλγορίθμων, οι οποίοι παράγουν κάποιον φυσικό αριθμό i με πιθανότητα p_i. Με βάση αυτά, θα περάσουμε στην a priori πιθανότητα m, η οποία προσάπτει στα αντικείμενας μας, για εμάς οι λέξεις του $\{0,1\}^{<\mathbb{N}}$, ένα μέτρο σχετικά με το κατά πόσο είναι πιθανό να προκύψουν από μια αλγοριθμική διαδικασία.

Στη δεύτερη ενότητα θα δούμε μια διαφορετική προσέγγιση της πολυπλοκότητας Kolmogorov, την οποία έδω αναφέρουμε ως προθεματική πολυπλοκότητα (συμβολισμός K), σε μια απόπειρα μετάφρασης του αγγλικού όρου prefix complexity. Παρά το γεγόνος ότι ο ορισμός της δεν είναι τόσο διαισθητικός όσο αυτός της C που είδαμε στο προηγούμενο κεφάλαιο, η προθεματική πολυπλοκότητα συνδέεται άμεσα με την έννοια του τυχαίου σε αλγοριθμικές διαδικάσιες, οπως θα δούμε σε αυτό αλλά και στο επόμενο κεφάλαιο, πράγμα που την καθιστά πιο χρήσιμη. Στόχος μας είναι να παρουσιάσουμε μερικές ιδιότητες της K, αλλά κυρίως να αποδείξουμε την, υπό μία έννοια δυική σχέση της με την a priori πιθανότητα m.

3.1 Ημιυπολογίσιμα Μέτρα στο $\mathbb{N}$ και a priori Πιθανότητα

Για να μιλήσουμε για ημιυπολογίσιμα μέτρα, είναι απαραίτητη η έννοια του υπολογίσιμου πραγματικού αριθμού. Αρχικά θα ταυτίζουμε το σύνολο των θετικών ρητών με το $\mathbb{N}^2$, δηλάδη τον ρήτο m/n με το ζευγάρι (m,n) (αυτός δεν είναι ο απόλυτα σωστός τρόπος να γίνει αυτό αφού τα (1,2) και (4,8) αντιπροσωπεύουν τον ίδιο ρητό, αλλά έμας μας ενδιαφέρει περισσότερο το γεγονός ότι μπορούμε να ορίζουμε αναδρομικές συνάρτησεις και στο $\mathbb{Q}$). Το σύνολο όλων των ρητών

αριθμών μπορούμε τότε να το θεώρουμε ως το $\{0,1\} \times \mathbb{N}^2$.

Μια συνάρτηση $f : \mathbb{N} \to \mathbb{Q}$, θα λέγεται υπολογίσιμη αν υπάρχουν υπολογίσιμες συναρτήσεις $r, h, g : \mathbb{N} \to \mathbb{N}$, έτσι ώστε $f(n) = (-1)^{r(n)} \frac{h(n)}{g(n)}$. Ένας $r \in \mathbb{R}$ καλείται υπολογίσιμος, αν υπάρχει υπολογίσιμη συνάρτηση $a : \mathbb{Q}^+ \to \mathbb{Q}$ έτσι ώστε για κάθε ρητό $\varepsilon > 0$ να ισχύει

$$|a(\varepsilon) - r| < \varepsilon.$$

Μια ασθενέστερη έννοια είναι αυτή της κάτω (αντίστοιχα άνω) ημιυπολογισιμότητας ένας πραγματικού αριθμού, η οποία θα μας είναι περισσότερο χρήσιμη σε αυτή την ενότητα. Ένας $r \in \mathbb{R}$ καλείται κάτω ημιυπολογίσιμος (αντίστοιχα άνω) αν υπάρχει υπολογίσιμη μη φθίνουσα (αντίστοιχα μη αύξουσα) ακολουθία ρητών $\{r_n\}_{n\in\mathbb{N}}$ τέτοια ώστε $\lim_n r_n = r$. Εμας μας ενδιαφέρουν σε αυτή την ενότητα ακολουθίες πραγματικών αριθμών οι οποίες είναι κάτω ημιυπολογίσιμες με έναν ομοιόμορφο τρόπο. Ξεκινάμε λοιπόν με τον επόμενο ορισμό.

Ορισμός 3.1.1. Έστω $\{r_i\}_{i\in\mathbb{N}}$ ακολουθία πραγματικών αριθμών. Η $\{r_i\}_{i\in\mathbb{N}}$ καλείται κάτω ημιυπολογίσιμη (lower semicomputable) αν υπάρχει υπολογίσιμη συνάρτηση $r : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ τέτοια ώστε:

(i) Για κάθε $i, n \in \mathbb{N}$, $r(i, n) \leq r(i, n + 1)$.

(ii) Για κάθε $i \in \mathbb{N}$, $\lim_n r(i, n) = r_i$.

Αξίζει να σημειωθεί, ότι στον πρηγούμενο ορισμό θα μπορούσαμε να θεωρήσουμε ότι η r δεν είναι απαραίτητα ολική, αλλά με κατάλληλο μετασχηματισμό της να κάναμε τις (i) και (ii) να έχουν νοήμα. Είμαστε έτοιμοι να δώσουμε τον ορισμό για ένα κάτω ημιυπολογίσιμο μέτρο και έπειτα να εξηγήσουμε πως προκύπτει.

Ορισμός 3.1.2. Έστω $\{p_i\}_{i\in\mathbb{N}}$ ακολουθία μη αρνητικών πραγματικών αριθμών. Η $\{p_i\}_{i\in\mathbb{N}}$ καλείται (κάτω) ημιυπολογίσιμο μέτρο (lower semicomputable measure) στο $\mathbb{N}$ αν ισχύουν τα εξής:

(i) Η $\{p_i\}_{i\in\mathbb{N}}$ είναι κάτω υμιυπολογίσιμη.

(ii) $\sum_{i\in\mathbb{N}} p_i \leq 1$.

Παρατηρούμε αρχικά από τον ορισμό 3.1.2 ότι η $\{p_i\}_{i\in\mathbb{N}}$ μοιάζει αρκέτα με ένα μέτρο πιθανότητας στο $\mathbb{N}$ με τη συνήθη σ-άλγερβα $\mathcal{P}(\mathbb{N})$, όμως απαιτούμε $\sum_{i\in\mathbb{N}} p_i \leq 1$, και όχι αυστηρή ισότητα όπως έχουμε στην περιπτώση των μέτρων πιθανότητας. Για το λόγο άυτο στην ξένη βιβλιογράφια συναντάται πιο συχνά ο όρος semimeasure, δηλαδή ημιμέτρο. Εμείς θα χρησιμοποιούμε τον όρο ημιυπολογίσιμο μέτρο εννοώντας πάντα μια ακολουθία πραγμάτικων σύμφωνα με

τον ορισμό 3.1.2. Επίσης αρκετές φορές θα συμβολίζουμε ένα ημιυπολογίσιμο μέτρο με κάποιο γράμμα π.χ. p, σαν αντικείμενο και με $p(i)$ τις τιμές του.

Για να γίνει περισσότερο κατανοήτη η έννοια του ημιυπολογίσιμου μέτρου, θεωρούμε τον εξής αλγόριθμο: Ρίξε ένα κέρμα έως ότου φέρεις γράμματα. Επίστρεψε τον αριθμό των κορώνων οι οποίες προηγήθηκαν και τερμάτισε. Ο συγκεκριμένος αλγόριθμος λειτουργεί χωρίς κάποια είσοδο και είναι μη ντετερμινιστικός, επιστρέφει τον αριθμό i με πιθανότητα $1/2^{i+1}$. Δεν είναι δύσκολο να δούμε ότι η ακολουθία $\{1/2^{i+1}\}_{i\in\mathbb{N}}$ αποτελεί ένα ημιυπολογίσιμο μέτρο στο $\mathbb{N}$.

Με βάση το προηγούμενο παράδειγμα, τα ημιυπολογίσιμα μέτρα προκύπτουν ως απάντηση στο εξής ερώτημα: Έστω μη ντετερμινιστικός αλγόριθμος ο οποίος με πιθανότητα p_i επιστρέφει τον φυσικό αριθμό i και τερματίζει (σε αυτή την περίπτωση, λέμε ότι ο αλγόριθμος παράγει την ακολουθία $\{p_i\}_{i\in\mathbb{N}}$). Τι ιδιότητες θα πρέπει να ικανοποιεί η ακολουθία $\{p_i\}_{i\in\mathbb{N}}$; Προφανώς θα πρέπει $\sum_i p_i = 1$, όμως έτσι δε λαμβάνουμε υπ᾽ όψιν το ενδεχόμενο ο αλγόριθμος μας να μην τερματίσει ποτέ, για το λόγο αύτο χαλαρώνουμε λίγο τη συγκεκριμένη απαίτηση σε $\sum_i p_i \leq 1$. Από την άλλη η (i) στον ορισμό 3.1.2 μας λέει χονδρικά, ότι ένας μη ντετερμινιστικός αλγόριθμος θα πρέπει να έχει στη διάθεση του ένα πρόγραμμα το οποίο να του υπολογίζει ολοένα και καλύτερες προσεγγίσεις για την τιμή p_i.

Ένα εύλογο ερώτημα είναι αν όλα τα ημιυπολογίσιμα μέτρα, παράγονται από ένα μη ντετερμινιστικό αλγόριθμο. Η απάντηση εδώ είναι καταφατική με βάση το επόμενο θεώρημα το οποίο παραθέτουμε για λόγους πληρότητας, χωρίς να το αποδείξουμε (βλ. [9]).

Θεώρημα 3.1.1. *Τα επόμενα είναι ισοδύναμα.*

(i) Η ακολουθία $\{p_i\}_{i\in\mathbb{N}}$ είναι ημιυπολογίσιμο μέτρο στο $\mathbb{N}$.

(ii) Υπάρχει μη ντετερμινιστικός αλγόριθμος, ο οποίος τρέχει χώρις είσοδο, επιστρέφει τον φυσικό αριθμό i με πιθανότητα p_i και τερματίζει.

Από το προηγούμενο θεώρημα έχουμε ότι, θα μπορούσαμε να ορίσουμε τα ημιυπολογίσιμα μέτρα με βάση το (ii). Ο λόγος που αναφερθήκαμε και σε αυτή την ισοδύναμη μορφή είναι κυρίως για την καλύτερη κατανόηση από τον αναγνώστη.

Με $\mathcal{M}$ θα συμβολίζουμε την κλάση όλων των ημιυπολογίσιμων μέτρων στο $\mathbb{N}$, δηλαδή

$$\mathcal{M} = \{p \in \mathbb{R}^{\mathbb{N}} \mid \{p(i)\}_{i\in\mathbb{N}} \text{ κάτω ημιυπολογίσιμη}, \sum_{i\in\mathbb{N}} p(i) \leq 1\}.$$

Σκόπος μας είναι να δείξουμε ότι η $\mathcal{M}$ περιέχει (τουλάχιστον) ένα στοιχείο m, το οποίο έχει έναν μεγιστικό χαρακτήρα, υπό την έννοια ότι για κάθε άλλο $p \in \mathcal{M}$, υπάρχει σταθερά c έτσι ώστε $cm(i) \geq p(i)$.

Με βάση τους ορισμούς 3.1.1 και 3.1.2 ένα $p \in \mathcal{M}$ προσδιορίζεται πλήρως από μια υπολογίσιμη συνάρτηση $r : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$, η οποία προσεγγίζει από κάτω τις τιμές $p(i)$. Όμως κάθε υπολογίσιμη συνάρτηση $h : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ δεν προσδιορίζει απαραίτητα ένα $p \in \mathcal{M}$, και αυτό θα αποτελέσει ένα πρόβλημα στην απόδειξη υπάρξης ενός "μεγιστικού" στοιχείου του $\mathcal{M}$. Γι' αυτό το λόγο χρειαζόμαστε το επόμενο λήμμα.

Λήμμα 3.1.1. *Κάθε υπολογίσιμη συνάρτηση $r : \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{Q}$ μπορεί να τροποποιηθεί με υπολογίσιμο τρόπο σε μια r', η οποία r' προσδιορίζει ένα ημιυπολογίσιμο μέτρο στο $\mathbb{N}$. Αν μία r προσδιορίζει ένα ημιυπολογίσιμο μέτρο p, τότε η r' προσδιορίζει και αυτή το p.*

Απόδειξη. Έστω r υπολογίσιμη συνάρτηση όπως στην εκφώνηση. Για να κατασκευάσουμε την r', θεωρούμε τις εξής δύο βοηθητικές συναρτήσεις,

$$T_r(i,n) = \begin{cases} r(i,n), & \text{αν } r(i,n)\downarrow \text{ σε } \leq n \text{ βήματα} \\ & \text{και } r(i,n) > 0. \\ 0, & \text{διαφορετικά.} \end{cases}$$

και

$$M_r(i,n) = \max\{T_r(i,0), T_r(i,1), \ldots, T_r(i,n)\},$$

Αρχικά η M_r ορίζεται για κάθε ζευγάρι (i,n) και $M_r(i,n) \leq M_r(i,n+1)$, αφού για $n+1$ θα πάρουμε το μέγιστο σε περισσότερα στοιχεία. Επίσης αν η r για κάποιο i ορίζεται για κάθε $n \in \mathbb{N}$ και $r(i,n) \leq r(i,n+1)$, τότε $\lim_n M_r(i,n) = \lim_n r(i,n)$. Ορίζουμε τώρα τη συνάρτηση r' με βάση τον παρακάτω αλγόριθμο.

1. Θέτουμε, $r'(i,0) = 0$, για κάθε $i \in \mathbb{N}$ και $k = 0$.

2. Αν έχουμε υπολογίσει τις τιμές $r'(0,n), \ldots, r'(n,n)$ για $k = n$, τότε θέτουμε $k = n+1$ και υπολογίζουμε τις τιμές $M_r(0,n+1), \ldots, M_r(n+1,n+1)$.

3. Αν,
$$\sum_{i=0}^{n+1} M_r(i,n+1) \leq 1,$$
τότε θέτουμε $r'(i,n+1) = M_r(i,n+1)$ για κάθε $i = 0,1,\ldots,n+1$ και επαναλαμβάνουμε το βήμα 2, διαφορετικά ο αλγόριθμος τερματίζει.

Αν μια r υπολογίζει το μέτρο p τότε η συνθήκη στο τρίτο βήμα του αλγορίθμου δεν θα παραβιαστεί πότε και από τον ορισμό της M_r θα έχουμε ότι $\lim_n r'(n,i) = p(i)$. Από την άλλη, αν παραβιαστεί για κάποιο k_0, τότε έχουμε ορίσει την r' ως, $r'(i,0) = 0$ για κάθε $i \in \mathbb{N}$ και για $0 \leq i \leq n$, $1 \leq n \leq k_0$, $r'(i,n) = M_r(i,n)$, ενώ για $n > k_0$, δεν ορίζονται οι τιμές $r'(i,n)$. Σε αυτή την περίπτωση η r' υπολογίζει το ημιυπολογίσιμο μέτρο p, το οποίο ορίζεται ως εξής,

$$p(i) = \begin{cases} M_r(i,k_0) & \text{αν } i \leq k_0. \\ 0 & \text{αν } i > k_0. \end{cases}$$

το οποίο ολοκληρώνει την απόδειξη. ◇

Έχοντας τώρα το λήμμα 3.1.1, αποδεικνύουμε το επόμενο θεώρημα.

Θεώρημα 3.1.2. *Υπάρχει $m \in \mathcal{M}$, το οποίο έχει την εξής ιδιότητα: για κάθε $p \in \mathcal{M}$, υπάρχει σταθερά c_p τέτοια ώστε $c_p m(i) \geq p(i)$ για κάθε $i \in \mathbb{N}$. Το m θα καλείται μεγιστικό ημιυπολογίσιμο μέτρο.*

Απόδειξη. Θεωρούμε υπολογίσιμη συνάρτηση $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, με τύπο,

$$\pi(n_1, n_2) = \frac{1}{2}(n_1 + n_2)(n_1 + n_2 + 1) + n_2,$$

η οποία είναι υπολογίσιμή, 1-1 και επί (η παραπάνω συνάρτηση ονομάζεται συνάρτηση ζεύγους του Cantor). Από το κεφάλαιο 1 έχουμε ότι υπάρχει υπολογίσιμη, συνάρτηση $\phi : \mathbb{N}^3 \rightharpoonup \mathbb{N}$, με $\phi(e, n_1, n_2) = \phi_e(n_1, n_2)$, όπου $\phi_e : \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{N}$ είναι η υπολογίσιμη συνάρτηση με κωδικό e. Κάθε συνάρτηση $r : \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{Q}$, μπορούμε να την δούμε και ως $r(i,n) = (r_1(i,n), r_2(i,n))$, οπού $r_1, r_2 : \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{N}$, υπολογίσιμες, όπού η r_1 αντιστοιχεί στον αριθμητή του ρητού $r(i,n)$ και η $r_2(i,n)$ στον παρονομαστή (πιο σώστα η r_1 λαμαβάνει τιμές στους ακεραίους, αλλά για την απόδειξη δεν έχει μεγαλή σημασία η υπόθεση μας).

Άρα σε κάθε $r : \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{Q}$, αντιστοιχίζουμε μια $\tilde{r} : \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{N}$, με $\tilde{r} = \pi \circ (r_1, r_2)$, και έτσι μέσω της ϕ να έχουμε μια απαρίθμηση όλων των συναρτήσεων $r : \mathbb{N} \times \mathbb{N} \rightharpoonup \mathbb{Q}$, με $r^{(0)}, r^{(1)}, r^{(2)} \ldots$. Εφαρμόζοντας το λήμμα 3.1.1 σε κάθε $r^{(0)}, r^{(1)}, \ldots$ παίρνουμε μια υπολογίσιμη απαρίθμηση όλων των συναρτήσεων που προσδιορίζουν τα στοιχεία του $\mathcal{M}$, δηλάδη $p^{(0)}, p^{(1)}, \ldots$.

Για να κατασκευάσουμε το ζητούμενο m, θα χρησιμοποιήσουμε την παραπάνω απαρίθμηση των στοιχείων του $\mathcal{M}$. Θεωρούμε $\{\lambda_k\}_{k \in \mathbb{N}}$ υπολογίσιμη ακολουθία ρητών τέτοια ώστε $\sum_k \lambda_k \leq 1$ (π.χ. $\lambda_k = 1/2^{k+1}$), και θέτουμε

$$m(i) = \sum_{k \in \mathbb{N}} \lambda_k p^{(k)}(i).$$

Αρχικά έχουμε ότι επειδή οι ποσότητες λ_k και $p^{(k)}(i)$ είναι μη αρνητικές,

$$\sum_{i=\in\mathbb{N}} m(i) = \sum_{k\in\mathbb{N}}\sum_{i\in\mathbb{N}} \lambda_k p^{(k)}(i) = \sum_{k\in\mathbb{N}} \lambda_k \sum_{i\in\mathbb{N}} p^{(k)}(i) \leq \sum_{k\in\mathbb{N}} \lambda_k \leq 1,$$

όπου η πρώτη ανισότητα προκύπτει από το γεγονός ότι $p^{(k)} \in \mathcal{M}$. Επίσης για κάθε $p \in \mathcal{M}$ είναι προφανές από τον ορισμό του m ότι $c_p m(i) \geq p(i)$ (η σταθερά είναι όρος λ_k που αντιστοιχεί στη σειρά με την οποία απαριθμείται το p). Τέλος η ακολουθία $\{m(i)\}_{i\in\mathbb{N}}$ είναι κάτω ημιυπολογίσιμη, αφού η συνάρτηση

$$r_m(i,n) = \sum_{k=0}^{n} \lambda_k r^{(k)}(i,n)$$

είναι υπολογίσιμη, αύξουσα ως προς n και για κάθε $i \in \mathbb{N}$,

$$\lim_n r_m(i,n) = \sum_{k\in\mathbb{N}} \lambda_k \lim_n r^{(k)}(n,i) = \sum_{k\in\mathbb{N}} \lambda_k p^{(k)}(i) = m(i).$$

Άρα το m είναι το ζητούμενο ημιυπολογίσμο μέτρο. ◇

Είναι φανερό από την απόδειξη ότι το m δεν είναι μοναδικό, στην πραγματικότητα υπάρχουν αριθμήσιμα άπειρα το πλήθός με την ιδίοτητα του θεωρήματος 3.1.2. Για το λόγο αυτό δίνουμε τον παρακάτω ορισμό.

Ορισμός 3.1.3. Θεωρούμε ένα συγκεκριμένο και σταθερό από εδώ και στο εξής, μεγιστικό ημιυπολογίσιμο μέτρο στο $\mathbb{N}$. Η ποσότητα $m(i)$ καλείται η a priori πιθανότητα του αριθμού i.

Έχοντας υπόψιν ότι κάθε ημιυπολογίσιμο μέτρο p αντιστοιχεί σε έναν μη ντετερμινιστικό αλγόριθμο, η ποσότητα m μας δίνει μια πρώτη εκτίμηση για το κατα πόσο ο αριθμός i είναι πιθανό να προκύψει από μια τυχαία αλγοριθμική διαδικασία. Για να γίνει πιο ξεκάθαρη η συγκεκριμένη ερμηνεία της ποσότητας m, ας περάσουμε πάλι στις λέξεις του $\{0,1\}^{<\mathbb{N}}$. Έστω $x \in \{0,1\}^{<\mathbb{N}}$ και έστω ότι η x εμφανίζεται στην n-οστή θέση της λεξικογραφικής διάταξης, θα εννοούμε με $m(x)$ την a priori πιθανότητα του φυσικού αριθμού n. Αυτός φυσικά δεν είναι ο μοναδικός τρόπος να αντιστοιχίζουμε ημιυπολογίσιμα μέτρα στο $\mathbb{N}$ σε αντίστοιχα σε λέξεις, αφού με βάση το θεώρημα 3.1.1 δεν είναι δύσκολο να τροποποιήσουμε έναν μη ντετερμινιστικό αλγόριθμο που μας επιστρέφει φυσικούς αριθμούς σε έναν άλλο αλγόριθμο, ο οποίος επιστρέφει λέξεις. Το σημαντικό είναι ότι ο αλγοριθμός μας θα πρέπει να επιστρέφει μια λέξη ολόκληρη και έπειτα να τερματίζει, και όχι να παράγει τη λέξη ψηφίο ψηφίο, χώρις έμεις να γνωρίζουμε πότε ο αλγόριθμος θα τερματίσει και αν τερματίσει, επιστρέφοντας το τελευταίο ψηφίο της λέξης.

Ας υποθέσουμε τώρα μια μηχανή, η οποία δεν γνωρίζουμε με τι τρόπο λειτουργεί (ντετερμινιστικό ή μη), η οποία επιστρέφει λέξεις του $\{0,1\}^{<\mathbb{N}}$, και επίσης έστω ότι η μας επιστρέφει μια λέξη η οποία αποτελείται από 50 μηδενικά. Αν υποθέταμε ότι τα 0 και 1 επιλέγονται ομοιόμορφα τότε η πιθάνοτητα να δούμε αυτή τη λέξη είναι $2^{-50} \approx 10^{-15}$, όμως δεν μπορούμε να χαρακτηρίσουμε μια λέξη με ένα τόσο ξεκάθαρο μοτίβο ως τυχαία. Θα υποθέταμε τότε ότι η μηχανή που την παρήγαγε δεν λειτουργεί με κάποιον τυχαίο τρόπο, αλλά μάλλον με μια απλή αλγοριθμική διαδικασία. Είναι φυσιολογικό άλλωστε, απλά μοτίβα και μεγάλες κανονικότητες να προκύπτουν από απλές διαδικασίες και συνεπώς να προκύπτουν πιο συχνά, ενώ μοτιβά που μπορούν να παραχθούν μόνο από πολύπλοκες διαδικάσιες είναι σχετικά απίθανα. Η πόσοτητα m μας δίνει λοιπόν ένα πρώτο μέτρο σχετικά με το πόσο πιθανό είναι προκύψει μια λέξη από μια τυχαία διαδικασία. Το σημαντικό μειονέκτημα όμως είναι ότι δεν μπορούμε να υπολόγισουμε τις τιμές της m, παρά μόνο να τις προσεγγίζουμε από κάτω, αφού αποδεικνύεται ότι κάθε μεγιστικό ημιυπολογίσιμο μέτρο δεν είναι υπολογίσιμο.

Τον παραπάνω τρόπο για να δώσουμε ένα νόημα στην ποσότητα m, τον έχουμε δανειστεί ουσιαστικά από την επομένη ενότητα, όπου θα αποδείξουμε την σχέση, $K(x) = -\log m(x) + O(1)$, όπου K είναι η προθεματική πολυπλοκότητα.

3.2 Προθεματική Πολυπλοκότητα

Για να ορίσουμε την προθεματική πολυπλοκότητα, θα χρειαστεί να ορίσουμε δύο κατηγορίες υπολογίσιμων συναρτήσεων. Πριν από αυτό, για $x, y \in \{0,1\}^{<\mathbb{N}}$, θα συμβολίζουμε με $x \sqsubseteq y$ αν η x είναι πρόθεμα της y, δηλαδή,

$$x \sqsubseteq y \iff l(x) \leq l(y) \ \& \ \forall i \leq l(x)(x(i) = y(i)).$$

Επίσης θα λέμε ότι δύο λέξεις x, y είναι ασυμβίβαστες και θα συμβολίζουμε με $x \perp y$, αν δεν είναι καμία πρόθεμα της άλλης, δηλαδή,

$$x \perp y \iff \exists i(x(i) \neq y(i)).$$

Ορισμός 3.2.1. Έστω υπολογίσιμη συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$. Η f καλείται:

(i) prefix stable αν ισχύει η συνεπαγωγή:

$$f(x)\downarrow \ \& \ x \sqsubseteq y \Rightarrow f(y)\downarrow \ \& \ f(x) = f(y).$$

(ii) prefix free αν ισχύει η συνεπαγωγή:

$$x, y \in Dom(f) \Rightarrow x \perp y.$$

Σημειώνουμε ότι και οι δύο έννοιες έμειναν αμετάφραστες, λόγω της δυσκολίας εύρεσης κατάλληλων όρων στα ελλήνικα. Θα ορίσουμε δύο διαφορετικές ποσότητες πολυπλοκότητας, μια βασιζόμενη σε prefix stable συναρτήσεις, την οποία θα συμβολίζουμε με K, και μια βασιζόμενοι σε prefix free συναρτήσεις συμβολίζοντας την με K'. Ιστορικά η ιδέα της προθεματικής πολυπλοκότητας αναπτύχθηκε παράλληλα από τον Leonid Levin, χρησιμοποιώντας prefix stable συναρτήσεις και από τον Gregory Chaitin, οποίος χρησιμοποίησε prefix free. Οπώς θα δούμε παρακάτω ισχύει ότι $K(x) = K'(x) + O(1)$, επομένως το ποια από τις δύο χρησιμοποιεί κανείς δεν έχει μεγάλη σημασία.

Ξεκινάμε με την K, και περιοριζόμαστε σε prefix stable συνάρτησεις. Αν λοιπόν $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ είναι prefix stable τότε κατ' αναλογία του ορισμού 2.1.1 θα συμβολίζουμε με $K_f(x)$ την εξής ποσότητα,

$$K_f(x) = \begin{cases} \min\{l(y) \mid f(y) = x\}, & \text{αν } x \in Rng(f). \\ +\infty, & \text{αν } x \notin Rng(f). \end{cases}$$

Σκόπος μας είναι να δείξουμε ότι ακόμα και αν περιοριστούμε μόνο σε prefix stable συναρτήσεις, μπορούμε και πάλι να βρούμε μια ασυμπτωτικά βέλτιστη συνάρτηση D, η οποία θα είναι prefix stable. Για το σκοπό αυτό έχουμε το επόμενο λήμμα.

Λήμμα 3.2.1. *Κάθε υπολογίσιμη συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, μπορεί να τροποποιηθεί με υπολογίσιμο τρόπο σε μια $\tilde{f}$ η οποία είναι prefix stable. Επίσης αν η f είναι prefix stable τότε $f = \tilde{f}$.*

Απόδειξη. Έστω $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ υπολογίσιμη συνάρτηση. Το γράφημα της f, $Gr(f) = \{(x,y) \mid f(x) = y\}$ είναι αναδομικά απαριθμητό, επομένως υπάρχει αλγόριθμος ο οποίος μας απαριθμεί τα ζεύγη $\{(x_i, y_i)\}_{i\in\mathbb{N}}$. Για να καταλήξουμε στην εν λόγω $\tilde{f}$ θα διαγράψουμε κάποια στοιχεία από το γράφημα της f. Διαγράφουμε το ζεύγος (x_i, y_i) αν υπάρχει ζεύγος (x_j, y_j) με: $x_j \sqsubseteq x_i$ είτε $x_i \sqsubseteq x_j$ και $y_j \neq y_i$, για κάποιο $j < i$.

Έχοντας τώρα την απαρίθμηση όλων των ζευγών (x_i, y_i) τα οποία επέζησαν από την παραπάνω διαδικασία, για να υπολογίζουμε την τιμή $\tilde{f}(x)$, εργαζόμαστε ως εξής, περιμένουμε έως ότου εμφανιστεί ζεύγος (x_i, y_i), με $x_i \sqsubseteq x$, και θέτουμε $\tilde{f}(x) = y_i$.

Η $\tilde{f}$ είναι prefix stable. Πράγματι έστω $\tilde{f}(x) = y$ και $x \sqsubseteq x'$. Από την κατασκευή της $\tilde{f}(x)$ υπάρχει ζεύγαρι (x_i, y_i) με $x_i \sqsubseteq x$ και $y_i = y$. Παρατηρούμε ότι $x_i \sqsubseteq x'$, και υπολογίζοντας την τιμή $\tilde{f}(x')$ με βάση τα παραπάνω, έχουμε είτε ότι $\tilde{f}(x') = y_i = \tilde{f}(x)$, είτε $\tilde{f}(x') = y_j$, όπου (x_j, y_j) είναι ζευγάρι με $x_j \sqsubseteq x'$ και $j < i$. Τότε εφόσον και τα δύο ζεύγη $(x_i, y_i), (x_j, y_j)$ δεν έχουν διαγραφεί από την παραπάνω διαδικάσια έχουμε ότι $y_j = y_i = y$. Τέλος είναι άμεσο ότι αν η f είναι prefix stable τότε κανένα ζεύγος δεν θα διαγραφεί από το γράφημα της και θα έχουμε $f = \tilde{f}$. ◇

Αξίζει να σημειωθεί ότι αν για κάποια $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, έχουμε ότι $0, 1 \in Dom(f)$ τότε η $\tilde{f}$ του προηγούμενου λήμματος θα παίρνει μόνο δύο τιμές. Αυτό δε μας απασχολεί, δίοτι εμάς μας ενδιαφέρει περισσότερο το γεγονός ότι prefix stable συναρτήσεις παραμένουν αναλοίωτες.

Θεώρημα 3.2.1. *Η κλάση όλων των prefix stable υπολογίσιμων συναρτήσεων περιέχει μια ασυμπτωτικά βέλτιστη. Δηλαδή υπάρχει υπολογίσιμη prefix stable συνάρτηση $D : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, τέτοια ώστε για κάθε άλλη υπολογίσιμη prefix stable συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ να ισχύει ότι,*

$$K_D(x) \leq K_f(x) + O(1), \quad \forall x \in \{0,1\}^{<\mathbb{N}}.$$

Απόδειξη. Αντίστοιχα με την απόδειξη του θεωρήματος 2.1.1 θέτουμε

$$D(\langle e, x\rangle) = \tilde{f}_e(x),$$

όπου $\langle e, x\rangle = \overline{bin(e)}01x$, f_e είναι η υπολογίσιμη συνάρτηση με κωδικό e και $\tilde{f}_e$, η prefix stable μορφή της με βάση το λήμμα 3.2.1. Η D είναι υπολογίσιμη όπως πρόκυπτει από την απόδειξη του θεωρήματος 2.1.1. Μένει να δείξουμε ότι είναι prefix stable και ασυμπτωτικά βέλτιστη στην κλάση όλων των prefix stable συναρτήσεων.

Δείχνουμε πρώτα ότι είναι prefix stable. Αρχικά παρατηρούμε ότι αν για κάποιες λέξεις ισχύει ότι $\overline{x}01 \sqsubseteq \overline{y}01$, τότε $x = y$. Αυτό προκύπτει από το γεγονός ότι το τέλος 01 και των δύο λέξεων είναι τα μοναδικά ψηφία που δεν είναι διπλά. Έστω τώρα $\langle e_1, x_1\rangle \sqsubseteq \langle e_2, x_2\rangle$. Θα πρέπει να δείξουμε ότι $D(\langle e_1, x_1\rangle) = D(\langle e_2, x_2\rangle)$. Επειδή οι λέξεις $\overline{bin(e_1)}01$, $\overline{bin(e_2)}01$ είναι και οι δύο προθέματα της λέξης $\langle e_2, x_2\rangle$, από την παρατήρηση που κάναμε αρχικά έχουμε ότι θα πρέπει $bin(e_1) = bin(e_2)$, δηλαδή $e_1 = e_2$. Εφόσον θα πρέπει $bin(e_1) = bin(e_2)$, από την υπόθεση μας προκύπτει ότι θα πρέπει $x_1 \sqsubseteq x_2$. Άρα αφού η $\tilde{f}_{e_1} (= \tilde{f}_{e_2})$ είναι prefix stable, έχουμε ότι $\tilde{f}_{e_1}(x_1) = \tilde{f}_{e_1}(x_2)$, επόμενως και

$$D(\langle e_1, x_1\rangle) = \tilde{f}_{e_1}(x_1) = \tilde{f}_{e_2}(x_2) = D(\langle e_2, x_2\rangle).$$

Τέλος αν θεωρήσουμε f μια prefix stable υπολογίσιμη συνάρτηση με κωδικό e, και λέξεις x, y με $f(y) = x$ και $K_f(x) = l(y)$, τότε η λέξη $\langle e, y\rangle$ είναι μια D-περιγραφή για το x, άρα,

$$K_D(x) \leq 2\log(e) + l(y) + O(1) = K_f(x) + O(1),$$

και η D είναι πράγματι βέλτιστη. ◇

Δίνουμε τώρα τον ορισμό της προθεματικής πολυπλοκότητας K (με βάση prefix stable συναρτήσεις).

Ορισμός 3.2.2. Θεωρούμε D μια ασυμπτωτικά βέλτιστη (συγκεκριμένη και σταθερή από εδώ και στο εξής) prefix stable υπολογίσιμη συνάρτηση και λέξη $x \in \{0,1\}^{<\mathbb{N}}$, η ποσότητα,

$$K(x) = \min\{l(y) \mid D(y) = x\}, \tag{3.1}$$

ονομάζεται προθεματική πολυπλοκότητα (Prefix Complexity) της λέξης x.

Για την περίπτωση των prefix free συναρτήσεων και τον ορισμό της K' με βάση αυτες, η διαδικάσια είναι ανάλογη. Χρειαζόμαστε αρχικά ένα αντίστοίχο του λήμματος 3.2.1.

Λήμμα 3.2.2. *Κάθε υπολογίσιμη συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, μπορεί να τροποποιηθεί με υπολογίσιμο τρόπο σε μια $\check{f}$ η οποία είναι prefix free. Επίσης αν η f είναι prefix free τότε $f = \check{f}$.*

Απόδειξη. Η απόδειξη χρησιμοποιεί την ίδια λογική με αυτή του λήμματος 3.2.1. Η μόνη διαφορά είναι ότι στην prefix free περίπτωση που μας ενδιαφέρει εδώ, διαγράφουμε το ζεύγος (x_i, y_i) αν υπάρχει ζεύγος (x_j, y_j) με $x_j \sqsubseteq x_i$ ή $x_i \sqsubseteq x_j$ για κάποιο $j < i$. Για τον υπολογισμό της τιμής $\check{f}(x)$, περιμένουμε έως ότου η απαρίθμηση των ζευγών μας εμφανίζει ένα (x_i, y_i), με $x_i = x$, και θέτουμε $\check{f}(x) = y_i$ (αν δεν υπάρχει τέτοιο ζεύγος δίοτι διαγράφηκε τότε η $\check{f}(x) \uparrow$).

Είναι εύκολο να διαπιστώσουμε ότι η $\check{f}$ είναι prefix free και αν η f είναι prefix free, τότε $\check{f} = f$. ◇

Θα συμβολίζουμε με K' την αντιστοιχή πολυπλοκότητα για prefix free συνάρτησείς, δηλαδή αν $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ είναι prefix free υπολογίσιμη συνάρτηση, τότε θα συμβολίζουμε με $K'_f(x)$ την εξής ποσότητα,

$$K'_f(x) = \begin{cases} \min\{l(y) \mid f(y) = x\}, & \text{αν } x \in Rng(f). \\ +\infty, & \text{αν } x \notin Rng(f). \end{cases}$$

Επίσης με ανάλογο τρόπο του θεωρήματος 3.2.1 αποδεικνύεται η υπάρξη ασυμπτωτικά βέλτιστης υπολογισιμής συνάρτησεις D, στην κλάση όλων των prefix free συναρτήσεων. Πιο συγκεκριμένα έχουμε το παρακάτω.

Θεώρημα 3.2.2. *Η κλάση όλων των prefix free υπλογίσιμων συναρτήσεων περιέχει μια ασυμπτωτικά βέλτιστη. Δηλαδή υπάρχει υπολογίσιμη prefix free συνάρτηση $D : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, τέτοια ώστε για κάθε άλλη υπολογίσιμη prefix free συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ να ισχύει ότι,*

$$K'_D(x) \leq K'_f(x) + O(1), \quad \forall x \in \{0,1\}^{<\mathbb{N}}.$$

Άντιστοιχά με τον ορισμό 3.2.2 έχουμε τον ορισμό για την ποσότητα K', της προθεματικής πολυπλοκότητας με βάση της prefix free συναρτήσεις.

Τίθεται εύλογα λοιπόν το ερώτημα ποια από τις δύο ποσότητες K, K' είναι η καταλληλότερη για την χρήση της ως προθεματική πολυπλοκότητας. Η απάντηση είναι ότι η κάθε μια έχει τα πλεονεκτήματα της σε σύγκριση με την άλλη. Επίσης όπως θα δούμε στην πορεία η K, K' διαφέρουν κατα μια σταθερά, επομένως δεν έχει και μεγάλη σημασία ποια θα χρησιμοποιούμε, εφόσον την πολυπλοκότητα μιας λέξης μπορουμε να την προσδιορίσουμε με κάποιο σφάλμα και όχι ακριβως. Η επιλογή λοιπόν εξαρτάται από το πρόβλημα που αντιμετωπίζει κάνεις και το αν κάποια από τις δύο διευκολύνει κάποιους ισχυρισμούς που ενδεχομένως να χρειάζονται.

Συνέχιζουμε αποδεικνύοντας δύο πολύ απλές ιδιότητες της K.

Πρόταση 3.2.1. *Ισχύει ότι:*

(i) Για κάθε λέξή $x \in \{0,1\}^{<\mathbb{N}}$,

$$C(x) \leq K(x) + O(1). \tag{3.2}$$

(ii) Για κάθε $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, *υπολογίσιμη συνάρτηση και για κάθε* $x \in Dom(f)$,

$$K(f(x)) \leq K(x) + O(1). \tag{3.3}$$

Στις παραπάνω σχέσεις μπορουμε να αντικαταστήσουμε την K *με την* K'.

Απόδειξη. (i) Έστω D η ασυμπτωτικά βέλτιστη prefix stable υπολογίσιμη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της K. Από το θέωρημα 2.1.1 έχουμε ότι,

$$C(x) \leq C_D(x) + O(1),$$

όμως $C_D(x) = K(x)$, από το οποίο προκύπτει το ζητούμενο.
(ii) Έστω $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, υπολογίσιμη συνάρτηση και D η συνάρτηση που χρησιμοποιήσαμε στον ορισμό της K. Θεωρούμε τη συνάρτηση $f \circ D$, η οποία είναι υπολογίσιμη ως σύνθεση υπολογίσιμων συναρτήσεων και επίσης είναι prefix stable. Πράγματι έστω ότι η τιμή $f(D(x))$ ορίζεται και λέξη y, με $x \sqsubseteq y$. Εφόσον η D είναι prefix stable έχουμε ότι $D(y) = D(x)$, επομένως και $f(D(x)) = f(D(y))$.

Έστω τώρα $x, y \in \{0,1\}^{<\mathbb{N}}$ με $x \in Dom(f)$ και $K(x) = l(y)$. Τότε $D(y) = x$, άρα $f(D(y)) = f(x)$, δηλαδή η λέξη y είναι μια $f \circ D$-περιγραφή για τη λέξη $f(x)$, άρα $K_{f\circ D}(f(x)) \leq l(y)$. Από το θεώρημα 3.2.1 έχουμε,

$$K(f(x)) \leq K_{f\circ D}(f(x)) + O(1) \leq l(y) + O(1) = K(x) + O(1).$$

Για τις αντίστοιχες σχέσεις για την K' εργαζόμαστε ανάλογα. ◇

Όπως έχουμε ήδη αναφέρει, θα αποδείξουμε ότι $K(x) = K'(x) = -\log m(x)$ (modulo) μια σταθερά. Οι περισσότερες από τις ιδιότητες της προθεματικής πολυπλόκοτητας αποδεικνύονται με πολύ απλό τρόπο μέσω της σχέσης που την συνδέει με την a priori πιθανότητα. Για να καταλήξουμε λοιπόν σε αυτό, θα αποδείξουμε κύκλικά πως η κάθε ποσότητα φράσσεται από την επόμενη της. Κάνουμε την αρχή με το επόμενο θεώρημα.

Θεώρημα 3.2.3. *Για κάθε $x \in \{0,1\}^{<\mathbb{N}}$ ισχύει ότι,*

$$K(x) \leq K'(x) + O(1). \tag{3.4}$$

Απόδειξη. Έστω D η prefix free υπολογίσιμη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της K'. Θα κατασκευάσουμε από την D μια επέκταση της η οποία είναι prefix stable. Έστω $y \in \{0,1\}^{<\mathbb{N}}$, θέτουμε,

$$\tilde{D}(y) = x \iff \exists y' \sqsubseteq y (D(y') = x).$$

Αρχικά, η $\tilde{D}$ είναι καλά ορισμένη, δίοτι αν υπάρχει $y' \sqsubseteq y$ με $D(y') = x$, τότε αυτό θα είναι μοναδικό, αφού η D είναι prefix free. Επίσης είναι υπολογίσιμη, πράγματι για να υπολογίσουμε την $\tilde{D}(y)$, για κάποια λέξη y, υπολογίζουμε παράλλήλα τις τιμές $D(y')$, για κάθε $y' \sqsubseteq y$, έως ότου βρούμε κάποιο y' με $D(y') \downarrow$, διαφορετικά το $\tilde{D}(y)$ δεν ορίζεται.

Τέλος, η $\tilde{D}$ είναι prefix stable, αφού αν υποθέσουμε ότι για τη λέξη x, ισχύει ότι $\tilde{D}(x) \downarrow$ και $x \sqsubseteq y$, τότε υπάρχει μοναδικό $x' \sqsubseteq x$, με $D(x') = \tilde{D}(x)$. Προφανώς $x' \sqsubseteq y$, επομένως αφού η D είναι prefix free και από τον ορισμό της $\tilde{D}$, έπεται ότι $\tilde{D}(y) \downarrow$ και $\tilde{D}(y) = D(x)$.

Για να καταλήξουμε στην 3.4 έστω $x, y \in \{0,1\}^{<\mathbb{N}}$, με $D(y) = x$ και $K'(x) = l(y)$. Τότε $\tilde{D}(y) = x$, άρα από το θεώρημα 3.2.1 έχουμε ότι,

$$K(x) \leq K_{\tilde{D}}(x) + O(1) \leq l(y) + O(1) = K'(x) + O(1),$$

άρα η 3.4 ισχύει. ◇

Πριν συνεχίσουμε σημειώνουμε ότι δεν ισχύει για την προθεματική πολυπλοκότητα ότι $K(x) \leq l(x) + O(1)$, και αυτό γιατι η ταυτοτική απεικόνιση δεν είναι prefix stable ούτε και prefix free. Μπορούμε όμως να βρούμε φράγματα για την K τα οποία εμπλέκουν είτε το μήκος των λέξεων είτε την απλή πολυπλοκότητα τους. Πιο συγκεκριμένα, μπορούμε να όρισουμε ως f, την εξής, $f(\overline{x}01) = x$, ή οποία είναι prefix free, και έχουμε ότι,

$$K'(x) \leq K'_f(x) + O(1) = 2l(x) + O(1).$$

Μπορούμε να βέλτιωσουμε το παραπάνω φράγμα, θεωρώντας την f αυτή τη φορά ως

$$f(\overline{bin(l(x))}01x) = x,$$

η οποία είναι επίσης prefix free, επομένως,

$$K'(x) \leq l(x) + 2\log l(x) + O(1), \tag{3.5}$$

με την 3.5 να ισχύει και για την K, λόγω του θεωρήματος που μόλις αποδείξαμε. Μπορούμε επίσης εύκολα να αποδείξουμε την επόμενη πρόταση.

Πρόταση 3.2.2. *Για κάθε $x \in \{0,1\}^{<\mathbb{N}}$ ισχύει ότι,*

$$K(x) \leq C(x) + 2\log C(x) + O(1). \tag{3.6}$$

Στην παραπάνω σχέση μπορούμε να αντικαταστήσουμε την K με την K'.

Απόδειξη. Έστω D η ασυμπτωτικά βέλτιστη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της C, και λέξη $x \in \{0,1\}^{<\mathbb{N}}$. Έστω επίσης $y \in \{0,1\}^{<\mathbb{N}}$ με $D(y) = x$ και $C(x) = l(y)$. Εφόσον η D είναι υπολογίσιμη από την σχέση 3.3 έχουμε ότι,

$$\begin{aligned} K(x) = K(D(y)) &\leq K(y) + O(1) \\ &\leq l(y) + 2\log l(y) + O(1) \\ &= C(x) + 2\log C(x) + O(1), \end{aligned}$$

το οποίο αποδεικνύει την 3.6. ◇

Πριν συνέχισουμε, θα χρειαστεί να αναφέρουμε λίγα πράγματα για τον χώρο μέτρου $\{0,1\}^{\mathbb{N}}$, όλων τον άπειρων ακολουθιών από 0 και 1. Κατ᾽ αρχάς με για μια λέξη $q \in \{0,1\}^{<\mathbb{N}}$, θα συμβολίζουμε με V_q, το σύνολο όλων των στοιχείων του $\{0,1\}^{\mathbb{N}}$, τα οποία έχουν ως αρχικό τμήμα τη λέξη q, δηλαδή,

$$V_q = \{\omega \in \{0,1\}^{\mathbb{N}} \mid q(i) = \omega(i), \forall i \leq l(q) - 1\}.$$

Θεώρουμε το $\{0,1\}^{\mathbb{N}}$ εφοδιασμένο με τη σ-άλγεβρα η οποία παράγεται από την οικογένεια $\{V_q \mid q \in \{0,1\}^{<\mathbb{N}}\}$, και προσάπτουμε στα V_q μέτρο, $\mu(V_q) = 2^{-l(q)}$, το οποίο αντιστοιχεί σαν μοντέλο, στις άπειρες ρίψεις ένος τίμιου νομίσματος. Είναι προφανές ότι $\mu(\{0,1\}^{\mathbb{N}}) = 1$, αφού $\{0,1\}^{\mathbb{N}} = V_0 \cup V_1$.

Τα παραπάνω αναφέρθηκαν γιατί θα τα χρησιποποίησουμε και στο να αποδείξουμε ότι $-\log m(x) \leq K(x) + O(1)$, και $K'(x) \leq -\log m(x) + O(1)$. Συνεχίζουμε με το επόμενο σύντομο λήμμα.

Λήμμα 3.2.3. *Έστω ακολουθία λέξεων $x_0, x_1, \ldots$ του $\{0,1\}^{<\mathbb{N}}$ τέτοιες ώστε για κάθε $n \neq k$, $x_n \perp x_k$. Τότε*

$$\sum_{n \in \mathbb{N}} 2^{-l(x_n)} \leq 1.$$

Απόδειξη. Παρατηρούμε ότι αν $x_n \perp x_k$, τότε $V_{x_n} \cap V_{x_k} = \emptyset$, δίοτι αν για κάποιο i_0 υποθέσουμε ότι $x_n(i_0) \neq x_k(i_0)$, τότε κανένα $\omega \in \{0,1\}^{\mathbb{N}}$ δεν μπορεί να έχει ως αρχικό του τμήμα και τις δύο λέξεις. Επομένως η $\{V_{x_n}\}_{n\in\mathbb{N}}$, αποτελείται από ξένα ανά δύο σύνολα, άρα,

$$\mu(\bigcup_{n\in\mathbb{N}} V_{x_n}) = \sum_{n\in\mathbb{N}} \mu(V_{x_n}) = \sum_{n\in\mathbb{N}} 2^{-l(x_n)} \leq 1,$$

το οποίο είναι και το ζητούμενο. ◇

Με βάση αυτή την πολύ απλή παρατήρηση, έχουμε το επόμενο θεώρημα.

Θεώρημα 3.2.4. *Για κάθε $x \in \{0,1\}^{<\mathbb{N}}$ ισχύει ότι,*

$$-\log m(x) \leq K(x) + O(1). \tag{3.7}$$

Απόδειξη. Θεωρούμε την απεικόνιση $x \mapsto 2^{-K(x)}$. Αντίστοιχα με την απόδειξη του θεωρήματος 2.1.3 προκύπτει ότι η συνάρτηση K είναι άνω ημιυπολογίσιμη, επομένως η $-K$ είναι προφανώς κάτω ημιυπολογίσιμη, και το ίδιο και η $2^{-K(x)}$. Ισχυριζόμαστε ότι,

$$\sum_{x\in\{0,1\}^{<\mathbb{N}}} 2^{-K(x)} \leq 1.$$

Πράγματι έστω $x \in \{0,1\}^{<\mathbb{N}}$, και q_x να είναι η βέλτιστη D-περιγραφή του x, όπου D είναι η prefix stable ασυμπτωτικά βέλτιστη συνάρτηση που χρησιμοποιήσαμε στον ορισμό της K. Αν $x, y \in \{0,1\}^{<\mathbb{N}}$ με $x \neq y$, τότε αφού $D(q_x) = x \neq y = D(q_y)$, και η D prefix stable, έπεται ότι $q_x \perp q_y$. Άρα από το λήμμα 3.2.3,

$$\sum_{x\in\{0,1\}^{<\mathbb{N}}} 2^{-K(x)} = \sum_{x\in\{0,1\}^{<\mathbb{N}}} 2^{-l(q_x)} \leq 1.$$

Επομένως η ποσότητα $2^{-K(x)}$ αποτελεί ένα ημιυπολογίσιμο μέτρο, άρα από το θεώρημα 3.1.2 υπάρχει σταθερά c_K τέτοια ώστε,

$$c_K m(x) \geq 2^{-K(x)}, \tag{3.8}$$

και λογαριθμίζοντας τη σχέση 3.8 έχουμε ότι $\log c_K + \log m(x) \geq -K(x)$, από το οποίο προκύπτει το ζητούμενο. ◇

Για να καταλήξουμε ότι $K(x) = -\log m(x) + O(1)$, μας έχει μείνει να δείξουμε ότι $K'(x) \leq -\log m(x) + O(1)$, το οποίο σε συνδιασμό με τα θεωρήματα 3.2.3 και 3.2.4 θα μας οδηγήσουν στο ζητούμενο. Για το λόγο αυτό έχουμε το επόμενο λήμμα, ένα " αντίστροφο " του λήμματος 3.2.3 το οποίο στη βιβλιογραφία συναντάται μερικές φορές ως Kraft-Chaitin.

Λήμμα 3.2.4. *Έστω $l_0, l_1, \ldots,$ υπολογίσιμη ακολουθία φυσικών τέτοια ώστε,*

$$\sum_{n\in\mathbb{N}} 2^{-l_n} \leq 1.$$

Τότε υπάρχει υπολογίσιμη ακολουθία λέξεων $x_0, x_1, \ldots,$ τέτοια ώστε για κάθε $n \neq k$, $x_n \perp x_k$ και για κάθε $n \in \mathbb{N}$, $l(x_n) = l_n$.

Απόδειξη. Παραθέτουμε αρχικά τον τρόπο με τον οποίο επιλέγουμε την ακολουθία $\{x_n\}_{n\in\mathbb{N}}$. Κατ᾽ αρχάς, για δεδομένη λέξη x, θα συμβολίζουμε με I_x το σύνολο των λέξεων που συγγρίνονται με αυτήν, δηλαδή,

$$I_x = \{y \in \{0,1\}^{<\mathbb{N}} \mid y \sqsubseteq x \text{ ή } x \sqsubseteq y\},$$

το οποίο είναι αναδρομικό, αφού αν γνωρίζουμε το x, για να αποφανθούμε αν $y \in I_x$ ή όχι, ελέγχουμε αν $x(i) = y(i)$ για κάθε $i \leq \min\{l(x)-1, l(y)-1\}$. Ο αλγόριθμος για την επιλογή των x_n είναι ο εξής.

1. Θέτουμε $x_0 = \underbrace{000\ldots0}_{l_0 \text{ φορές}}$ και $A_0 = \{0,1\}^{<\mathbb{N}} \backslash I_{x_0}$.

2. Αν έχουμε επιλέξει τις πρώτες n λέξεις, $x_0, x_1, \ldots, x_{n-1}$, τότε επιλέγουμε για x_n την πρώτη λέξη στη λεξικογραφική διάταξη, μήκους l_n, για την οποία ισχύει ότι, $x_n \in A_{n-1}$. Θέτουμε $A_n = A_{n-1} \backslash I_{x_n}$ και επαναλαμβάνουμε το βήμα 2.

Παρατηρούμε ότι κάθε A_i είναι αναδρομικό, ως διαφορά αναδρομικών συνόλων, επομένως η επιλογή του x_n γίνεται ως εξής: έχοντας το l_n ξεκινάμε από τα αριστερά προς τα δεξία του δέντρου $\{0,1\}^{<\mathbb{N}}$, στο επίπεδο l_n και υπολογίζουμε κάθε φορά την χαρακτηριστική συνάρτηση, χ_{A_i} στην αντίστοιχη λέξη, με το που βρούμε λέξη x, με $\chi_{A_i}(x) = 1$, θέτουμε $x_n = x$.

Θα πρέπει όμως να επιβεβαιώσουμε ότι υπάρχει αρκετός " χώρος " που απομένει σε κάθε βήμα ώστε να έχουμε τη δυνάτοτητα στο επόμενο να επιλέξουμε τη λέξη με τα χαρακτηριστικά που μας ενδιαφερούν. Η ιδέα είναι ότι κάθε λέξη x_n που βρίσκουμε, καταλαμβάνει ένα τμήμα του $\{0,1\}^{\mathbb{N}}$, μέσω του αντίστοιχου V_{x_n}. Αν καταφέρουμε να δείξουμε ότι σε κάθε βήμα, το μέτρο του σύνολού που περισσεύει είναι μεγαλύτερο από το $2^{-l_{n+1}}$, τότε ο άλγοριθμός πάντα θα μπορεί να βρίσκει την επόμενη λέξη. Πριν συνεχίσουμε αν $A \subset \{0,1\}^{<\mathbb{N}}$, με $[A]$ θα συμβολίζουμε το εξής σύνολο,

$$[A] = \{\omega \in \{0,1\}^{\mathbb{N}} \mid \exists x \in A, x(i) = \omega(i), 0 \leq i \leq l(x)-1\}.$$

Είναι άμεσο ότι $[I_x] = V_x$. Αποδεικνύουμε τώρα τον παρακάτω ισχυρισμό.

Για κάθε A_i, υπάρχουν ασυμβίβαστες λέξεις $t_1, t_2, \ldots, t_{m_i}$, τέτοιες ώστε,

$$[A_i] = V_{t_1} \cup V_{t_2} \cup \cdots \cup V_{t_{m_i}} \quad \text{και} \quad l(t_1) > l(t_2) > \cdots > l(t_{m_i}) \tag{3.9}$$

με $l(t_{m_i}) \geq l_{i+1}$.

Θα αποδείξουμε το παραπάνω επαγωγικά. Έστω λοιπόν ότι έχουμε επιλέξει τις λέξεις $x_0, x_1, \ldots, x_{n-1}$ και έχουμε ότι τα αντίστοιχα A_i έχουν την εν λόγω ιδιότητα. Άρα από την 3.9 για το A_{n-1} έχουμε ότι,

$$\mu(V_{t_j}) \leq \frac{1}{2}\mu(V_{t_{j+1}}),$$

άρα για το συνολικό μέτρο των V_{t_j} στον $\{0,1\}^{\mathbb{N}}$, έχουμε ότι,

$$\sum_{j=1}^{m_{n-1}} \mu(V_{t_j}) \leq \mu(V_{t_{m_{n-1}}}) \sum_{j=1}^{m_{n-1}} \frac{1}{2^j} < 2\mu(V_{t_{m_{n-1}}}).$$

Θέλουμε τώρα να " χωρέσουμε " μια λέξη μήκους l_n. Από υπόθεση έχουμε ότι $\sum_{i=0}^{n} 2^{-l_i} \leq 1$, και ισοδύναμα,

$$\begin{aligned} 2^{-l_n} \leq \sum_{i=0}^{n-1} 2^{-l_i} &= \mu(\{0,1\}^{\mathbb{N}} \backslash (\bigcup_{i=0}^{n-1} V_{x_i})) \\ &= \mu(V_{t_1} \cup \cdots \cup V_{t_{m_{n-1}}}) \\ &< 2\mu(V_{t_{m_{n-1}}}). \end{aligned}$$

Επομένως,

$$2^{-l_n} \leq \mu(V_{t_{m_{n-1}}}) = 2^{-l(t_{m_{n-1}})},$$

από το οποίο προκύπτει ότι $l_n \geq l(t_{m_{n-1}})$. Άρα ο άλγοριθμός μας θα βρει λέξη μήκους l_n, η οποία θα ανήκει στο A_{n-1}.

Για να δούμε ότι και το $A_n = A_{n-1} \backslash I_{x_n}$ θα ικανοποιεί την 3.9, παρατηρούμε ότι είτε $l_n = l(t_j)$ είτε $l(t_{j-1}) < l_n < l(t_j)$ για κάποιο j. Στην πρώτη περίπτωση, είναι εύκολο να δούμε ότι $x_n = t_j$, και άρα το A_n θα ικανοποιεί την 3.9. Αν τώρα $l(t_{j-1}) < l_n < l(t_j)$, τότε η λέξη που θα επιλεγεί απο τον αλγόριθμο είναι η

$$x_n = t_{j-1} \underbrace{0 \ldots 0}_{d \text{ φορές}}, \quad d = l_n - l(t_{j-1}),$$

και δεν είναι δύσκολο να διαπιστώσουμε ότι και πάλι το A_n θα γράφεται ως ένωση διαστημάτων, όπως στην 3.9. ◇

Πιο συγκεκριμένα, θα μας είναι χρήσιη μια εναλλακτική μορφή του λήμματος που μολις αποδείξαμε, το οποίο αναφέρουμε με το επόμενο σύντομο πόρισμα.

Πόρισμα 3.2.1. *Έστω $l_0, l_1, \ldots,$ υπολογίσιμη ακολουθία φυσικών τέτοια ώστε,*

$$\sum_{n\in\mathbb{N}} 2^{-l_n} \leq 1.$$

Τότε για κάθε $n \in \mathbb{N}$, $K'(n) \leq l_n + O(1)$.

Απόδειξη. Από το λήμμα 3.2.4, υπάρχει υπολογίσιμη ακολουθία $\{x_n\}_{n\in\mathbb{N}}$, από λέξεις οι οποίες είναι ανά δύο ασυμβίβαστες και για κάθε n, $l(x_n) = l_n$. Άρα υπάρχει $\phi : \mathbb{N} \to \{0,1\}^{<\mathbb{N}}$, υπολογίσιμη, ολική συνάρτηση με $\phi(n) = x_n$. Επειδή η ϕ είναι ολική, δεν είναι δύσκολο να διαπιστώσουμε ότι η ϕ^{-1} είναι επίσης υπολογίσιμη, και αφού $Dom(\phi^{-1}) = \{x_n\}_{n\in\mathbb{N}}$, έχουμε ότι η ϕ^{-1} είναι prefix free. Άρα, από το θεώρημα 3.2.2 έχουμε ότι,

$$K'(n) \leq K'_{\phi^{-1}}(n) + O(1) = l(x_n) + O(1) = l_n + O(1),$$

το οποίο είναι το ζητούμενο. ◇

Έχοντας το πόρισμα 3.2.1 αποδεικνύουμε τώρα το επομένο θεώρημα.

Θεώρημα 3.2.5. *Για κάθε $x \in \{0,1\}^{<\mathbb{N}}$ ισχύει ότι,*

$$K'(x) \leq -\log m(x) + O(1). \tag{3.10}$$

Απόδειξη. Έστω r_m η υπολογίσιμη συνάρτηση η οποία προσεγγίζει την m από κάτω. Θεωρούμε την εξής συνάρτηση,

$$r'_m(x,i) = \begin{cases} \min\{1/2^k \mid k \in \mathbb{N}, r_m(x,i) \leq 1/2^k\}, & \text{αν } r_m(x,i) > 0. \\ 0 & \text{αν } r_m(x,i) \leq 0. \end{cases}$$

Η r'_m είναι υπολογίσιμη, δίοτι η r_m είναι υπολογίσιμη και έτσι μπορούμε να υπολογίσουμε την τιμή $r'_m(x,i)$ συγκρίνοντας την πόσοτητα $r_m(x,i)$ με τις 1, 1/2, 1/4, ..., και το πρώτο k το οποίο θα βρούμε $r_m(x,i) > 1/2^k$, επιστρέφουμε $r'_m(x,i) = 1/2^{k-1}$. Επίσης είναι προφανες ότι $r'_m(x,i)$ είναι αύξουσα ως προς i, αφού η $r_m(x,i)$ είναι αύξουσα ως προς i. Τέλος, ισχύει ότι

$$r_m(x,i) \leq r'_m(x,i) \leq 2r_m(x,i),$$

η πρώτη ανισότητα είναι προφανης, για τη δεύτερη, αν ίσχυε $1/2^{k_0} > 2r_m(x,i)$, με $r'_m(x,i) = 1/2^{k_0}$, τότε και $1/2^{k_0+1} > r_m(x,i)$, και έτσι το $1/2^{k_0}$ δεν θα ήταν η ελάχιστη δύναμη του 1/2 με την εν λόγω ιδιότητα.

Για δική μας ευκολία, θα λέμε ένα ζευγάρι (x,i) γνήσιο αν ισχύει ότι $r'_m(x,i) > r'_m(x,i-1)$ για $i \geq 1$, και για $i = 0$, αν $r'_m(x,0) > 0$. Για σταθερό $x \in \{0,1\}^{<\mathbb{N}}$ θεωρούμε το σύνολο,

$$J_x = \{i \in \mathbb{N} \mid (x,i) : \text{γνήσιο}\},$$

και παρατηρούμε τα παρακάτω. Αρχικά, από την μεγιστική ιδιότητα της m έχουμε ότι $J_x \neq \emptyset$, για κάθε x. Επίσης για κάθε $x \in \{0,1\}^{<\mathbb{N}}$, το J_x είναι πεπερασμένο, αυτό προκύπτει από το γεγονός ότι αν $i_0 = \min J_x$, με $r'_m(x, i_0) = 1/2^{k_0}$, για κάποιο φυσικό k_0, τότε επειδή η r'_m είναι μη φθίνουσα ως προς i, μπορεί να κάνει το πολύ k_0 ‘‘άλματα’’, όσα και οι υποψήφιες δυνάμεις του $1/2$, που είναι μεγαλύτερες του $1/2^{k_0}$, και επομένως $|J_x| \leq k_0 + 1$.

Ισχυριζόμαστε τώρα ότι για κάθε λέξη $x \in \{0,1\}^{<\mathbb{N}}$, ισχύει ότι,

$$\sum_{i \in J_x} r'_m(x, i) \leq 4m(x). \tag{3.11}$$

Για να αποδείξουμε την σχέση 3.11, παρατηρούμε ότι, από τον τροπό που χαρακτηρίσαμε τα γνήσια ζεύγη, και το ότι η $r'_m(x, i)$ είναι αύξουσα ως προς i, προκύπτει η εξής σχέση,

$$r'_m(x, i_{j+1}) \geq 2r'_m(x, i_j),$$

υποθέτοντας ότι $J_x = \{i_0 < i_1 < \cdots < i_N\}$. Άρα υπολογίζοντας το άθροισμα έχουμε,

$$\begin{aligned}
\sum_{i \in J_x} r'_m(x, i) &\leq \sum_{j=0}^{N} \frac{1}{2^j} r'_m(x, i_N) \\
&= (2 - \frac{1}{2^N}) r'_m(x, i_N) \\
&\leq 2(2r_m(x, i_N)) \\
&\leq 4m(x),
\end{aligned}$$

άρα η 3.11 ισχύει.

Συνεχίζουμε παρατηρώντας ότι, το $B = \{(x, i) \mid (x, i) : \text{γνήσιο}\}$, είναι αναδρομικό, αφού για να απαφανθούμε αν το ζευγάρι (x, i) είναι γνήσιο ή όχι απλά ελέγχουμε τη συνθήκη $r'_m(x, i) > r'_m(x, i-1)$, και η r'_m είναι υπολογίσιμη. Επομένως έχουμε μία υπολογίσιμη ακολουθία από γνήσια ζεύγη (x_n, i_n), η οποία τα περιλαμβάνει όλα από μια φόρα ακριβώς. Με βάση αυτή την ακολουθία θεωρούμε ακολουθία φυσικών $\{l_n\}_{n \in \mathbb{N}}$, τέτοια ώστε,

$$2^{-l_n} = \frac{r'_m(x_n, i_n)}{4},$$

η οποία είναι υπολογίσιμη διότι τόσο η ακολουθία των ζευγαριών (x_n, i_n) όσο

και η r'_m είναι υπολογίσιμες. Από την σχέση 3.11 έχουμε ότι,

$$\begin{aligned}\sum_{n\in\mathbb{N}} 2^{-l_n} &= \frac{1}{4}\sum_{n\in\mathbb{N}} r'_m(x_n, i_n)\\ &= \frac{1}{4}\sum_{n\in\mathbb{N}}\sum_{i\in J_{x_n}} r'_m(x_n, i)\\ &\leq \frac{1}{4}\sum_{n\in\mathbb{N}} 4m(x_n) \leq 1.\end{aligned}$$

Από το πόρισμα 3.2.1 ισχύει ότι $K'(n) \leq l_n + O(1)$, δηλαδή

$$K'(n) \leq -\log r'_m(x_n, i_n) + 2 + O(1),$$

και εφόσον το x_n υπολογίζεται δοθέντος του n (υπολογίζουμε το ζεύγος (x_n, i_n) και επιστρέφουμε την πρώτη συντεταγμένη) έπεται ότι,

$$K'(x_n) \leq K'(n) + O(1) \leq -\log r'_m(x_n, i_n) + O(1). \tag{3.12}$$

Όπως ήδη αναφέραμε για κάθε $x \in \{0,1\}^{<\mathbb{N}}$, υπάρχει i τέτοιο ώστε το (x, i) να είναι γνήσιο, επόμενως κάθε x εμφανίζεται στην ακολουθία των γνήσιων ζευγών (x_n, i_n). Για να καταλήξουμε στο ζητούμένη σχέση 3.10, θεωρούμε λέξη x για την οποία από τα παραπάνω, ισχύει ότι ότι $x = x_n$ για κάποιο n, και επομένως η σχέση 3.12 αληθεύει. Θέτουμε $i_x = \max J_x$, και είναι προφανές ότι, $r_m(x, i) \leq r'_m(x, i_x)$ για κάθε $i \in \mathbb{N}$, άρα και $m(x) \leq r'_m(x, i_x)$, από την 3.12 έχουμε τώρα,

$$K'(x) \leq -\log r'_m(x, i_x) + O(1) \leq -\log m(x) + O(1),$$

το οποίο είναι το ζητούμενο. ◇

Είναι άμεσο τώρα το επόμενο θεώρημα.

Θεώρημα 3.2.6 (Levin)**.** *Για κάθε $x \in \{0,1\}^{<\mathbb{N}}$ ισχύει ότι,*

$$K(x) = -\log m(x) + O(1). \tag{3.13}$$

Απόδειξη. Προκύπτει άμεσα από τις σχέσεις 3.4, 3.7 και 3.9. ◇

Με βάση τα θεώρηματα 3.2.3 εώς 3.2.6 οι ποσότητες $K(x), K'(x)$ και $-\log m(x)$, διαφέρουν μεταξύ τους κατά μία σταθερά. Αυτό έχει ως πρώτη συνέπεια για εμάς να μην κάνουμε τη διάκριση ανάμεσα στις K, K' και να τις θεωρούμε πλέον ως μέτρο για την ίδια ποσότητα, την προθεματική πολυπλοκότητα. Θα χρησιμοποιούμε είτε την prefix stable μορφή της, είτε την prefix

free, ανάλογα με το ποια από τις δύο μας διευκολύνει, χώρις αυτό να έχει κάποια ιδιαίτερη επίπτωση στην ισχύ των ισχυρισμών μας.

Η 3.12 επιβεβαιώνει τα όσα αναφέραμε για την a priori πιθανότητα m στο τέλος της προηγούμενης ενότητας. Μια λέξη x έχει μεγάλη πολυπλοκότητα K αν και μόνο αν έχει μικρή a priori πιθανότητα $m(x)$, δηλαδή υπό μία έννοια δεν είναι τόσο πιθανό να προκύψει από μια αλγοριθμική διαδικασία.

Στο υπόλοιπο αυτής της ενότητας θα αποδείξουμε μερικές ιδιότητες της K χρησιμοποιώντας την 3.13. Κατ᾽ αρχάς, για δύο λέξεις $x, y \in \{0,1\}^{<\mathbb{N}}$, η ποσότητα $K(x,y)$ ορίζεται με τον ίδιο τρόπο όπως είχαμε δεί στην ενότητα 2.2 για την απλή πολυπλοκότητα C. Μάλιστα, είχαμε δει στην πρόταση 2.2.2 ότι για την απλή πολυπλοκότητα δεν ισχύει μιας μορφής τριγωνικής ανισότητας $C(x,y) \leq C(x) + C(y) + O(1)$, διότι υπάρχει και ένας όρος τάξης $\log C(x)$. Η επομένη πρόταση αποδεικνύει ότι κάτι τέτοιο ισχύει όμως για την K.

Πρόταση 3.2.3. *Για κάθε $x, y \in \{0,1\}^{<\mathbb{N}}$, ισχύει ότι,*

$$K(x,y) \leq K(x) + K(y) + O(1). \tag{3.14}$$

Απόδειξη. Έστω $x, y \in \{0,1\}^{<\mathbb{N}}$, με $[x,y]$, συμβολίζουμε και εδώ την κωδικοποίηση του ζεύγους (x,y) σε μία λέξη, όπως και στην ενότητα 2.2. Θεωρούμε $p : \{0,1\}^{<\mathbb{N}} \to \mathbb{R}$, ως εξής,

$$p(z) = \begin{cases} m(x)m(y), & \text{αν } z = [x,y] \\ 0, & \text{αν } \forall x,y(z \neq [x,y]). \end{cases}$$

Εφόσον η m είναι κάτω ημιυπολογίσιμη, τότε και η p είναι, δίοτι αν r_m είναι η υπολογίσιμη συνάρτηση που προσεγγίζει την m από κάτω, τότε μπορούμε να ορίσουμε την ανττίστοιχη r_p, ως

$$r_p([x,y],n) = r_m(x,n)r_m(y,n),$$

και $r_p(z,n) = 0$, για κάθε n, αν το z δεν αποτελεί κωδικοποίηση κάποιου ζεύγους. Τότε η r_p είναι υπολογίσιμη, είναι αύξουσα ως προς n και προφανώς $\lim_n r_p(z,n) = p(z)$.

Παρατηρούμε επίσης ότι,

$$\begin{aligned} \sum_{z \in \{0,1\}^{<\mathbb{N}}} p(z) &= \sum_{x,y \in \{0,1\}^{<\mathbb{N}}} m(x)m(y) \\ &= \sum_{x \in \{0,1\}^{<\mathbb{N}}} m(x) \cdot \sum_{y \in \{0,1\}^{<\mathbb{N}}} m(y) \leq 1 \cdot 1, \end{aligned}$$

επομένως η p είναι ένα ημιυπολογίσιμο μέτρο. Άρα υπάρχει σταθερά c_p, τέτοια ώστε $c_p m(z) \geq p(z)$, για κάθε z. Επομένως για το $[x, y]$ έχουμε,

$$\log c_p + \log m([x, y]) \geq \log m(x) + \log m(y),$$

και ισοδύναμα από την σχέση 3.13,

$$K(x, y) \leq K(x) + K(y) + O(1),$$

άρα η 3.14 ισχύει. ◇

Αξίζει να σημειωθεί ότι η προηγούμενη πρόταση μπορεί να αποδειχθεί χωρίς την χρήση της m.

Συνεχίζουμε με κάποιες ιδίοτητες της συνάρτησης K. Αρχικά, δεν είναι δύσκολο να διαπιστώσουμε ότι κάθε υπολογίσιμο κάτω φράγμα για την K, θα πρέπει αναγκαστικά να είναι φραγμένο. Ένας πολύ σύντομος τρόπος για να το δούμε αυτό, είναι το γεγονός ότι, με αντίστοιχο τρόπο με αυτόν που καταλήξαμε στην σχέση 3.5, μπορούμε να συμπεράνουμε ότι $K(x) \leq 2l(x) + O(1)$, και συνεπώς $K(x) \leq 2C(x)+O(1)$. Αν υποθέταμε ότι υπήρχε κάποιο μη φραγμένο, υπολογίσιμο κάτω φράγμα για την K, αυτό θα μας έδινε και ένα αντίστοιχο για την C, το οποίο όμως είναι αδύνατο σύμφωνα με το θεώρημα 2.1.2. Επίσης με εντελώς παρομοίο τρόπο, με αυτόν στην περίπτωση της C, αποδεικνύεται ότι η K είναι άνω ημιυπολογίσιμη. Μάλιστα ισχύει το παρακάτω.

Θεώρημα 3.2.7. *Έστω άνω ημιυπολογίσιμη συνάρτηση $\kappa : \{0,1\}^{<\mathbb{N}} \to \mathbb{N}$, τέτοια ώστε*

$$\sum_{x \in \{0,1\}^{<\mathbb{N}}} 2^{-\kappa(x)} < \infty.$$

Τότε για κάθε $x \in \{0,1\}^{<\mathbb{N}}$, ισχύει ότι $K(x) \leq \kappa(x) + O(1)$.

Απόδειξη. Θεωρούμε τη συνάρτηση $p(x) = c2^{-\kappa(x)}$, όπου c είναι σταθερά με, $c \leq 1/\sum_x 2^{-\kappa(x)}$. Εφόσον η κ είναι άνω ημιυπολογίσιμη, έχουμε ότι η p είναι κάτω ημιυπολογίσιμη και επίσης $\sum_x p(x) \leq 1$, δηλαδή η p είναι ημιυπολογίσιμο μέτρο. Επομένως υπάρχει σταθερά c_p, τέτοια ώστε $c_P m(x) \geq p(x)$, για κάθε x, άρα,

$$\log c_p + \log m(x) \geq \log c - \kappa(x),$$

και από την 3.13 έχουμε ότι $K(x) \leq \kappa(x) + O(1)$. ◇

Το προηγούμενο αποδεικνύει ουσιαστικά ότι οι ιδιότητες $\sum_x 2^{-\kappa(x)} < \infty$ και $K(x) \leq \kappa(x) + O(1)$ είναι ισοδύναμες.

Ολοκληρώνοντας το κεφάλαιο αυτό θα θέλαμε να συγκρίνουμε λίγο τις ποσότητες K και C. Για το λόγο αυτό, θα πρέπει να λάβουμε υπόψιν όχι μόνο πως σχετίζονται πάνω σε συγκεκριμένες λέξεις x, αλλά και το πως κατανέμονται οι τιμές της σε λέξεις δεδομένου μήκους ή πόσες λέξεις περιμένουμε να έχουν μικρότερη πολυπλοκότητα από κάποιο n. Πιο συγκεκριμένα ισχύει το επομένο.

Πρόταση 3.2.4. *Για κάθε $n \in \mathbb{N}$, ισχύει ότι,*

$$|\{x \in \{0,1\}^{<\mathbb{N}} \mid K(x) < n\}| \leq 2^{n-K(n)+O(1)}.$$

Απόδειξη. Έστω $a_n = |\{x \in \{0,1\}^{<\mathbb{N}} \mid K(x) < n\}|$. Αρχικά η ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ είναι κάτω ημιυπολογίσιμη. Πράγματι, εφόσον η K είναι άνω ημιυπολογίσιμη, έχουμε ότι κάθε $\{x \in \{0,1\}^{<\mathbb{N}} \mid K(x) < n\}$ είναι αναδρομικά απαριθμήτο, επομένως μπορώ να προσεγγίζω την τιμή a_n από κάτω, απαριθμώντας τα στοιχεία του αντίστοιχου συνόλου.

Με βάση το λήμμα 3.2.3 είδαμε ότι, $\sum_x 2^{-K(x)} \leq 1$, επομένως από τον τρόπο που ορίστηκε η a_n, έχουμε ότι,

$$\sum_{n\in\mathbb{N}}(a_{n+1} - a_n)2^{-n} = \sum_{x\in\{0,1\}^{<\mathbb{N}}} 2^{-K(x)} \leq 1. \tag{3.15}$$

Αναπτύσσοντας τους πρώτους όρους της πρώτης σειράς στην 3.15, έχουμε ότι

$$\sum_{n\in\mathbb{N}}(a_{n+1} - a_n)2^{-n} = \sum_{n\in\mathbb{N}}(2^{-n+1} - 2^{-n})a_n = \sum_{n\in\mathbb{N}} a_n 2^{-n},$$

άρα η ποσότητα $a(n) = a_n 2^{-n}$ αποτελεί ένα ημιυπολογίσιμο μέτρο. Επομένως υπάρχει σταθερά c_a, έτσι ώστε $c_a m(n) \geq a_n 2^{-n}$, από το οποίο προκύπτει άμεσα ότι $a_n \leq c_a m(n) 2^n$, άρα από την σχέση 3.13 έχουμε ότι

$$a_n \leq c_a 2^n 2^{-K(n)+O(1)} \leq 2^{n-K(n)+O(1)},$$

το οποίο ολοκληρώνει την απόδειξη. ◇

Ολοκληρώνουμε αυτή την ενότητα αποδεικνύοντας έναν διαφορετικό τρόπο, από έκεινον της σχέσης 3.6, εκτίμησης της K, μέσω της C.

Πρόταση 3.2.5. *Για κάθε $x \in \{0,1\}^{<\mathbb{N}}$, ισχύει ότι,*

$$K(x) \leq C(x) + K(C(x)) + O(1). \tag{3.16}$$

Απόδειξη. Θα αποδείξουμε αρχικά ότι για κάθε λέξη x ισχύει ότι,

$$K(x) \leq l(x) + K(l(x)) + O(1).$$

Θεωρούμε την συνάρτηση $p(x) = 2^{-l(x)} m(l(x))$. Η p είναι κάτω ημιυπολογίσιμη και επίσης

$$\sum_{x:l(x)=n} p(x) = 2^n 2^{-n} m(n) = m(n),$$

από έπεται ότι $\sum_{x\in\{0,1\}^{<\mathbb{N}}} p(x) \leq 1$. Κατά τα γνωστά, υπάρχει σταθερά c_p, έτσι ώστε $c_p m(x) \geq p(x)$, και λογαριθμίζοντας έχουμε ότι,

$$-l(x) + \log m(l(x)) \leq \log m(x) + \log c_p,$$

και από την 3.13 έχουμε το ζητούμενο. Για να καταλήξουμε στην 3.16 θεωρούμε D τη συνάρτηση με βάση την οποία ορίσαμε την C και την σχέση 3.3. $\diamond$

Πριν συνεχίσουμε στο επόμενο κεφάλαιο, σημειώνουμε ότι αντίστοιχα με την περίπτωση της δεσμευμένης πολυπλοκότητας $C(x|y)$, ορίζεται και $K(x|y)$, με μερικές τροποποιήσεις στο ορισμό των prefix stable και preefix free συναρτήσεων, αλλά εμάς για την εφαρμογή της K, που θα δούμε στο επόμενο κεφάλαιο δε θα μας χρειαστεί. Για περισσότερα πάνω στο θέμα ο αναγνώστης μπορεί να συμβουλευτεί τα [5] και [9].

Κεφάλαιο 4

Τυχαιότητα Martin-Löf

Στο τελευταίο κεφάλαιο της εργασίας αυτής θα δούμε μια εφαρμογή της προθεματικής πολυπλοκότητας στον χαρακτηρισμό των τυχαίων άπειρων ακολουθιών από 0 και 1, αποδεικνύοντας το Θεώρημα Levin-Schnorr, στην δεύτερη ενότητα του κεφαλαίου αυτού.

Θα αναρωτηθεί κανείς βέβαια, τι εννοούμε ακριβώς όταν λέμε ότι μια ακολουθία είναι τυχαία, και ο σκόπος της πρώτης ενότητας είναι ακριβώς αυτός, να απαντήσουμε σε αυτό το ερώτημα παρουσιάζοντας την έννοια της τυχαίας ακολουθίας κατά Martin-Löf. Τα δύο κύρια χαρακτηριστικά της τυχαιότητας είναι η μη προβλεψιμότητα και η ομοιομορφία στην συχνότητα εμφάνισης των γεγονότων, υπό την έννοια ότι κανένα από τα ενδεχόμενα που παρατηρούμε δεν εμφανίζεται συστηματικά πιο συχνά από τα υπόλοιπα. Με βάση αυτα τα κριτήρια έχουν προταθεί διάφοροι ορισμοί γι αυτό που αποκαλούμε τυχαίο, από τους Richard von Mises, Alonzo Church και Claus Schnorr, αλλά ο τρόπος του Per Martin-Löf, απότελει ίσως τον πιο ικανοποιητικό.

Για να γίνουν πιο κατανοητά τα παραπάνω, έστω ότι μας δίνεται μια πεπερασμένη ακολουθία από εκατό 0 και 1, για την οποία γνωρίζουμε ότι από το πεμπτο ψηφίο και μέτα εμφανίζονται μόνο μηδενικά. Είναι δυνατόν η συγκεκριμένη ακολουθία να προέκυψε από ένα τίμιο νόμισμα; Είναι, αλλά η διαίσθηση μας λέει ότι δεν γίνεται να έχει παραχθεί από ενα τίμιο παιχνίδι κορώνας-γράμματα, και αυτό γιατί υπάρχει μια κανονικότητα στη συγκεκριμένη ακολουθία που είναι δύσκολο για εμάς να πιστέψουμε ότι είναι τυχαία. Ας σημειώσουμε, ότι με βάση τη θεωρία πιθανοτήτων, η πιθανότητα να παρατηρήσουμε τη συγκεκριμένη ακολουθία είναι 2^{-100}, όπως και οποιαδήποτε άλλη ακολουθία από εκατό 0 και 1. Επομένως η θεωρία πιθανοτήτων αδυνάτει να ποσοτικοποιήσει, αύτο το οποίο ο ανθρώπινος εγκέφαλος χαρακτηρίζει ως τυχαιότητα. Η βασική ιδέα του Martin-Löf όπως θα δούμε, ήταν ουσιάστικα με τη χρήση υπολογίσιμων διαδικάσιων να ελέγχουμε την τυχαιότητα ή μη ενός αντικειμένου.

Όπως αναφέραμε και στην αρχή, τα αντικείμενα σε αυτο το κεφάλαιο, θα

είναι οι άπειρες ακολουθίες απο 0 και 1, μια βολική γενίκευση για να μελετάμε ακολουθίες οσοδήποτε (πολύ) μεγάλου μήκους.

4.1 Σύνολα Μηδενικού Μέτρου στον $\{0,1\}^{\mathbb{N}}$

Σε αυτή την ενότητα θα ασχοληθούμε με στοιχεία του $\{0,1\}^{\mathbb{N}}$, γνωστο και ως σύνολο Cantor. Προς αποφυγή σύγχυσης σε αυτό το κεφάλαιο, τα στοιχεία του $\{0,1\}^{\mathbb{N}}$, δηλαδή της άπειρες ακολουθίες από 0 και 1, θα τις συμβολίζουμε με ελληνικους χαρακτήρες όπως χ, ψ, ω, ενώ τα στοιχεία του $\{0,1\}^{<\mathbb{N}}$, με λατινικούς, όπως s, t, u.

Όπως έχουμε ήδη αναφέρει με V_t, για $t \in \{0,1\}^{<\mathbb{N}}$, θα συμβολίζουμε τα βάσικα ανοικτά του $\{0,1\}^{\mathbb{N}}$, δηλαδή

$$V_t = \{\omega \in \{0,1\}^{\mathbb{N}} \mid t(i) = \omega(i), \forall i \leq l(t) - 1\}.$$

Επίσης θα χρειαστούμε την έννοια του μέτρου σε αυτή την ενότητα, για αυτό τον λόγο, θα θεωρούμε τον $\{0,1\}^{\mathbb{N}}$ εφοδιασμένο με την Borel σ-άλγεβρα, δηλάδη την σ-άλγεβρα που παράγεται από την οικογένεια, $\{V_t \mid t \in \{0,1\}^{<\mathbb{N}}\}$, και με μέτρο θα εννοούμε ένα πραγματικό, πεπερασμένο (ή πιθανότητας) σ-αθροιστικό μέτρο στον παραπάνω μετρήσιμο χώρο. Τέλος σε κάθε μέτρο μ στον $\{0,1\}^{\mathbb{N}}$, αντιστοιχίζουμε την εξής συνάρτηση $p_\mu : \{0,1\}^{<\mathbb{N}} \to \mathbb{R}^+$, με $p_\mu(s) = \mu(V_s)$.

Ξεκινάμε με τον ορισμό του υπολογίσιμου μέτρου, ο οποίος θα μας είναι χρήσιμος παρακάτω.

Ορισμός 4.1.1. Έστω μέτρο μ στον $\{0,1\}^{\mathbb{N}}$. Το μ θα καλείται υπολογίσιμο μέτρο (computable measure), αν υπάρχει υπολογίσιμη $r : \{0,1\}^{<\mathbb{N}} \times \mathbb{Q}^+ \to \mathbb{Q}^+$, τέτοια ώστε, για κάθε $t \in \{0,1\}^{<\mathbb{N}}$ και $\varepsilon \in \mathbb{Q}^+$ να ισχύει,

$$|r(t,\varepsilon) - p_\mu(t)| < \varepsilon. \tag{4.1}$$

Δίνουμε τώρα τον ορισμό των effectively null υποσυνόλων του $\{0,1\}^{\mathbb{N}}$, ως προς κάποιο μέτρο μ. Εμείς θα τα καλούμε E-μηδενικά σύνολα, λόγω της δυσκολίας μετάφρασης στα ελλήνικα του όρου effectively null set.

Ορισμός 4.1.2. Έστω $A \subset \{0,1\}^{\mathbb{N}}$ και μέτρο μ στον $\{0,1\}^{\mathbb{N}}$. Το A θα καλείται E-μηδενικό (effectively null set) για το μέτρο μ, αν υπάρχει υπολογίσιμη συνάρτηση $t : \mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$, τέτοια ώστε για κάθε $\varepsilon \in \mathbb{Q}^+$ να ισχύουν,

(i) $A \subset \bigcup_{n\in\mathbb{N}} V_{t(n,\varepsilon)}$.

(ii) $\sum_{n\in\mathbb{N}} p_\mu(t(n,\varepsilon)) < \varepsilon$.

Δηλαδή ένα Ε-μηδεινκό υποσύνολο του $\{0,1\}^{\mathbb{N}}$, είναι ένα σύνολο μέτρου μηδέν με τη συνήθη έννοια, του οποίου όμως τα αντίστοιχά καλύμματα μπορούν να βρεθούν με έναν υπολογίσιμο τρόπο. Για παράδειγμα, έστω $\omega \in \{0,1\}^{\mathbb{N}}$, υπολογίσιμη ακολουθία, και έστω $f : \mathbb{N} \to \{0,1\}^{<\mathbb{N}}$, υπολογίσιμη συνάρτηση με $f(n) = \omega_{|n}$. Τότε το $\{\omega\}$ είναι Ε-μηδενικό, αφού ορίζοντας τη συνάρτηση,

$$t(n,\varepsilon) = \begin{cases} f(k_\varepsilon), & \text{αν } n = 0 \\ \text{δεν ορίζεται}, & \text{αν } n \geq 1 \end{cases}$$

όπου $k_\varepsilon = \min\{k \in \mathbb{N} \mid 2^{-k} < \varepsilon\}$, είναι άμεσο ότι ικανοποιείται ο ορισμός 4.1.2.

Ας υποθέσουμε τώρα ότι έχουμε μια συνάρτηση $t : \mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$, για την οποία για κάθε $\varepsilon \in \mathbb{Q}^+$, ισχύει ότι, $\sum_{n\in\mathbb{N}} p_\mu(t(n,\varepsilon)) < \varepsilon$. Η t προσδιορίζει με ένα φυσιολογικό τρόπο ένα Ε-μηδενικό σύνολο στον $\{0,1\}^{\mathbb{N}}$ ως εξής,

$$W = \bigcap_{\varepsilon\in\mathbb{Q}^+} \bigcup_{n\in\mathbb{N}} V_{t(n,\varepsilon)},$$

καθώς και κάθε υποσύνολο του W θα είναι επίσης Ε-μηδενικό. Είναι προφανές λοιπόν ότι κάθε Ε-μηδενικό σύνολο θα πρέπει να είναι είτε της μορφής του W, είτε να είναι υποσύνολο κάποιου τέτοιου W. Αυτή η παρατήρηση είναι σημαντική για να αποδείξουμε ότι υπάρχει ένα Ε-μηδενικό υποσύνολο του $\{0,1\}^{\mathbb{N}}$, με την ιδιότητα ότι περιέχει οποιοδήποτε άλλο Ε-μηδενικό σύνολο, ένα αποτέλεσμα το οποίο οφείλεται στον Martin-Löf. Για να αποδείξουμε κάτι τέτοιο χρειαζόμαστε το επόμενο λήμμα.

Λήμμα 4.1.1. *Έστω μ υπολογίσιμο μέτρο στον $\{0,1\}^{\mathbb{N}}$. Τότε κάθε υπολογίσιμη συνάρτηση $t : \mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$, μπορεί να τροποποιηθεί με υπολογίσιμο τρόπο σε μια $\tilde{t}$, για την οποία ισχύει το εξής: για κάθε $J \subset \mathbb{N}$, πεπερασμένο και για κάθε $\varepsilon \in \mathbb{Q}^+$,*

$$\sum_{n\in J} p_\mu(\tilde{t}(n,\varepsilon)) < \varepsilon$$

(με την προϋπόθεση φυσικά, ότι οι όροι που εμφανίζονται στο άθροισμα ορίζονται).

Απόδειξη. Έστω $r : \{0,1\}^{<\mathbb{N}} \times \mathbb{Q}^+ \to \mathbb{Q}^+$, η υπολογίσιμη συνάρτηση που προσεγγίζει το μ, και υπολογίσιμη συνάρτηση $t : \mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$. Περιγράφουμε τώρα τον αλγόριθμο που χρειαζόμαστε.

Έστω $\varepsilon \in \mathbb{Q}^+$, στο k βήμα του αλγορίθμού μας υπολογίζουμε παράλληλα τις τιμές,

$$t(0,\varepsilon), t(1,\varepsilon), \ldots, t(k-1,\varepsilon).$$

Κάθε φορά που η παραπάνω διαδικασία υπολογίζει ένα $t(n_l, \varepsilon)$, πραγματοποιούμε τον εξής έλεγχο: αν $t(n_1, \varepsilon), t(n_2, \varepsilon) \ldots, t(n_l, \varepsilon)$ είναι οι τιμές που έχουμε υπολογίσει μέχρι το συγκεκριμένο βήμα, τότε για $j \in \mathbb{N}$ υπολογίζουμε τις ποσότητες,

$$r(t(n_i, \varepsilon), \frac{1}{(i+1)^j}), \quad i = 1, 2, \ldots l,$$

έως ότου για κάποιο j να ισχύει ότι,

$$\sum_{i=1}^{l} r(t(n_i, \varepsilon), \frac{1}{(i+1)^j}) \leq \varepsilon - \sum_{i=1}^{l} \frac{1}{(i+1)^j}. \tag{4.2}$$

Δηλαδή για $j = 1$ υπολογίζουμε τις προσεγγίσεις,

$$r(t(n_1, \varepsilon), \frac{1}{2}), r(t(n_2, \varepsilon), \frac{1}{3}), \ldots, r(t(n_l, \varepsilon), \frac{1}{l+1}),$$

αν η 4.2 δεν ικανοποιείται, τότε υπολογίζουμε τις αντίστοιχες ποσότητες για $j = 2$, κ.ο.κ.. Αν για κάποιο j η διαδικάσια που περιγράψαμε τερματίσει, τότε θέτουμε $\tilde{t}(n_l, \varepsilon) = t(n_l, \varepsilon)$, αν από την άλλη η διαδικασία δεν τερματίσει πότε, δίοτι για παράδειγμα $p_\mu(t(n_l, \varepsilon)) > \varepsilon$, τότε η $\tilde{t}$ θα έχει οριστεί μόνο για τα ζεύγη $(n_1, \varepsilon), \ldots, (n_{l-1}, \varepsilon)$ με τις υπόλοιπες τιμές για το συγκεκριμένο ε να μην ορίζονται.

Η 4.2 εξασφαλίζει ότι αν η $\tilde{t}$ έχει οριστεί για τα $(n_1, \varepsilon), \ldots, (n_l, \varepsilon), \ldots$ τότε για κάθε πεπερασμένο $J \subset \mathbb{N}$ και για κατάλληλο j, ισχύει ότι,

$$\begin{aligned} \sum_{i \in J} p_\mu(\tilde{t}(n_i, \varepsilon)) &< \sum_{i \in J} \frac{1}{(i+1)^j} + \sum_{i \in J} r(t(n_i, \varepsilon), \frac{1}{(i+1)^j}) \\ &\leq \sum_{i \in J} \frac{1}{(i+1)^j} + \varepsilon - \sum_{i \in J} \frac{1}{(i+1)^j} = \varepsilon. \end{aligned}$$

Τέλος είναι άμεσο ότι αν μια t ικανοποιεί το συμπέρασμα του λήμματος, τότε ο έλεγχος στον οποίο την υποβάλει ο αλγόριθμός μας, θα τερματίζει για κάθε νέα τιμή που προσθέτουμε και επομένως $t = \tilde{t}$. ◇

Σημειώνουμε ότι αν για μια υπολογίσιμη συνάρτηση $t : \mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$, ισχύει ότι για κάθε $\varepsilon \in \mathbb{Q}^+$ και για κάθε πεπερασμένο $J \subset \mathbb{N}$,

$$\sum_{n \in J} p_\mu(t(n, \varepsilon)) < \varepsilon,$$

τότε είναι προφανές ότι,

$$\sum_{n \in \mathbb{N}} p_\mu(t(n, \varepsilon)) \leq \varepsilon,$$

όπου το άθροισμα εννοείται σε όλα τα n για τα οποία $(n, \varepsilon) \in Dom(t)$. Ουσιαστικά λοιπόν, το λήμμα 4.1.1 μας λέει ότι κάθε υπολογίσιμη συνάρτηση τύπου $\mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$, μπορεί να τροποποιηθεί αλγοριθμικά, ώστε να προσδιορίζει ένα Ε-μηδενικό υποσύνολο του $\{0,1\}^{\mathbb{N}}$ επιλέγοντας $\varepsilon' < \varepsilon$.

Είμαστε έτοιμοι τώρα να διατυπώσουμε και να αποδείξουμε το επόμενο θεώρημα.

Θεώρημα 4.1.1 (Martin-Löf)**.** *Έστω μ υπολογίσιμο μέτρο στον $\{0,1\}^{\mathbb{N}}$. Τότε υπάρχει Ε-μηδενικό σύνολο $U \subset \{0,1\}^{\mathbb{N}}$, με την ιδιότητα ότι για κάθε άλλο Ε-μηδενικό σύνολο $W \subset \{0,1\}^{\mathbb{N}}$, να ισχύει ότι $W \subset U$.*

Απόδειξη. Θα χρησιμοποιήσουμε το γεγονός ότι υπάρχει υπολογίσιμη συνάρτηση $\phi : \mathbb{N} \times \mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$, με $\phi(e, n, \varepsilon) = \phi_e(n, \varepsilon)$, όπου ϕ_e είναι η υπολογίσιμη συνάρτηση $\phi_e : \mathbb{N} \times \mathbb{Q}^+ \rightharpoonup \{0,1\}^{<\mathbb{N}}$, με κωδικό e. Με βάση το λήμμα 4.1.1 μπορούμε να έχουμε την τροποποιημένη μορφή της ϕ_e, $\tilde{\phi}_e$. Άρα η συναρτήσεις $\tilde{\phi}_e$, απαριθμούνται μέσω της ϕ, ως $\tilde{\phi}^{(0)}, \tilde{\phi}^{(1)}, \ldots$.

Όπως έχουμε ήδη αναφέρει κάθε μία από τις $\tilde{\phi}^{(i)}$, προσδιορίζει ένα Ε-μηδενικό σύνολο, W_i, ως εξής,

$$W_i = \bigcap_{\varepsilon \in \mathbb{Q}^+} \bigcup_{n \in \mathbb{N}} V_{\tilde{\phi}^{(i)}(n,\varepsilon)}.$$

Ισχυριζόμστε τώρα ότι, το $U = \bigcup_{i \in \mathbb{N}} W_i$ είναι το ζητούμενο Ε-μηδενικό σύνολο. Το μόνο που έχουμε να δείξουμε είναι ότι το U είναι Ε-μηδενικό, αφού είναι προφανές ότι θα περιέχει κάθε άλλο Ε-μηδενικό σύνολο.

Έστω λοιπόν $\varepsilon \in \mathbb{Q}^+$ και επιλέγουμε $\varepsilon' \in \mathbb{Q}^+$ με $\varepsilon' < \varepsilon$ (π.χ. $\varepsilon' = \varepsilon/2$). Η ιδέα είναι να συνδιάσουμε το $\varepsilon'/2$ κάλυμμα του W_0, με το $\varepsilon'/4$ κάλυμμα του W_1, κοκ. Για τον σκοπό αυτό, θεωρούμε $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, υπολογίσιμη αντιστοιχία (1-1 και επί) ανάμεσα στα δύο σύνολα (όπως στην απόδειξη του θεωρήματος 3.1.2), και θέτουμε

$$t_U(\pi(n,i), \varepsilon') = \tilde{\phi}^{(i)}(n, \varepsilon'/2^{i+1}),$$

η οποία είναι υπολογίσιμη. Για κάθε $i \in \mathbb{N}$ έχουμε ότι $W_i \subset \bigcup_{n \in \mathbb{N}} V_{\tilde{\phi}^{(i)}(n,\varepsilon'/2^{i+1})}$, από το οποίο έπεται ότι,

$$U \subset \bigcup_{i \in \mathbb{N}} \bigcup_{n \in \mathbb{N}} V_{\tilde{\phi}^{(i)}(n,\varepsilon'/2^{i+1})},$$

και ισοδύναμα,

$$U \subset \bigcup_{(n,i) \in \mathbb{N}^2} V_{t_U(\pi(n,i),\varepsilon')}.$$

Τέλος, αφού κάθε $\tilde{\phi}^{(i)}$, ικανοποιεί το συμπέρασμα του λήμματος 4.1.1, έχουμε ότι,

$$\sum_{(n,i)\in\mathbb{N}^2} p_\mu(t_U(\pi(n,i),\varepsilon')) \leq \varepsilon' < \varepsilon,$$

άρα το U είναι Ε-μηδενικό σύνολο. ◇

Έχοντας τώρα το U, που προκύπτει από το θεώρημα 4.1.1, δίνουμε τον ορισμό της τυχαίας ακολουθίας κατα Martin-Löf.

Ορισμός 4.1.3. Έστω μ υπολογίσιμο μέτρο στον $\{0,1\}^{\mathbb{N}}$. Ένα $\omega \in \{0,1\}^{\mathbb{N}}$ καλείται τυχαίο κατά Martin-Löf (Martin-Löf random) ή για συντομία ML-τυχαίο για το μ, αν $\omega \notin U$ (όπου U το σύνολο που προκύπτει από το θεώρημα 4.1.1).

Μια ισοδύναμη μορφή του προηγούμενου ορισμού είναι: ένα $\omega \in \{0,1\}^{\mathbb{N}}$ καλείται ML-τυχαίο αν το $\{\omega\}$ δεν είναι Ε-μηδενικό.

Σε μια προσπάθεια κατανόησης του παραπάνω ορισμού, ας επικαλεστούμε λίγο τη διαίσθηση μας. Ας υποθέσουμε ότι μας δίνεται μια άπειρη ακολουθία από 0 και 1, και μας ζητά κάποιος τη γνώμη μας αν θεωρούμε τη συγκεκριμένη ακολουθία τυχαία ή όχι. Σε μία προσπάθεια μας να τη χαρακτηρίσουμε, θα ψάχναμε να βρούμε κάποια κανονικότητα στον τρόπο με τον οποίο κατανέμονται τα ψηφία 0 και 1. Για παράδειγμα αν σε κάθε άρτια θέση υπήρχε 1, τότε αύτη η ιδιαιτερότητα της, είναι πολύ πιθανό να μας έκανε να την χαρακτηρίσουμε ως μη τυχαία.

Μπορούμε να φανταστούμε την ιδιότητα " κάθε άρτιο ψηφίο της ακολουθίας είναι 1 " ως ένα Ε-μηδενικό σύνολο, έτσι ο ορισμός 4.1.3 μας λέει ότι θα χαρακτηρίζαμε μια ακολουθία ως τυχαία, αν δεν μπορούσαμε να αναγνωρίσουμε μέσα σε αυτήν κανένα χαρακτηριστικό το οποίο να την ξεχωρίζει από τις υπόλοιπες και το οποίο κατέχουν " λιγοστές " μόνο ακολουθίες. Αντίθετως ένα χαρακτηριστικό όπως " η ακολουθία ξεκινά με δύο μηδενικά " δεν μπορεί να θεωρήθει ως κάτι το ιδιαίτερο, αφού 1 στις 4 ακολουθίες έχει αυτή την ιδιότητα (υποθέτοντας ότι τα 0 και 1 επιλέγονται ομοιόμορφα).

Αξίζει να αναφέρουμε ότι ο αρχικός ορισμός του Martin-Löf όπως αυτός εμφανίζεται στο [6], ήταν διαφορετικός και βασιζόταν στην έννοια effectively open set. Ένα $W \subset \{0,1\}^{\mathbb{N}}$, καλείται effectively open, αν υπάρχει υπάρχει υπολογίσιμη συνάρτηση $f : \mathbb{N} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, τέτοια ώστε $W = \bigcup_{n\in\mathbb{N}} V_{f(n)}$. Μια ακολουθία $\{W_n\}_{n\in\mathbb{N}}$, υποοσυνόλων του $\{0,1\}^{\mathbb{N}}$, καλείται ομοιόμορφα effectively open, αν κάθε W_n είναι effectively open και το σύνολο $\{(x,n) \mid x \in W_n\}$ είναι αναδρομικά απαριθμητό.

Με βάση τα παραπάνω, ο Martin-Löf όρισε την έννοια του effectively null set ως εξής: Ένα $A \subset \{0,1\}^{\mathbb{N}}$ καλείται effectively null set, ως προς κάποιο

υπολογίσιμο μέτρο μ αν υπάρχει ακολουθία $\{W_n\}_{n\in\mathbb{N}}$ ομοιόμορφα effectively open, τέτοια ώστε,

$$W_{n+1} \subset W_n,\ \mu(W_n) \leq 2^{-n} \ \text{ και } A \subset \bigcap_{n\in\mathbb{N}} W_n.$$

Δεν είναι δύσκολο να διαπιστώσει κανείς οτι ο παραπάνω ορισμός και ο 4.1.2 είναι ισοδύναμοι. Κάθε ομοιόμορφα effectively open ακολουθία $\{W_n\}_{n\in\mathbb{N}}$ με $W_{n+1} \subset W_n$ και $\mu(W_n) \leq 2^{-n}$ καλείται ένα ML-test.

Το αντίστοιχο του θεωρήματος 4.1.1, με την παραπάνω ορολογία είναι το εξής: Υπάρχει ML-test, $\mathcal{U} = \{U_n\}_{n\in\mathbb{N}}$, τέτοιο ώστε για κάθε άλλο ML-test, $\{W_n\}_{n\in\mathbb{N}}$, να ισχύει ότι,

$$U_{n+c} \subset W_n, \quad \forall n \in \mathbb{N},$$

όπου c είναι σταθερά που εξάρταται από το ML-test $\{W_n\}_{n\in\mathbb{N}}$. Το test $\mathcal{U}$ καλείται universal.

Για κάθε ML-test, και κάθε $\omega \in \{0,1\}^{\mathbb{N}}$, ορίζεται η εξής ποσότητα,

$$d_W(\omega) = \max\{n \in \mathbb{N} \mid \omega \in W_n\},$$

και στην περίπτωση του universal ML-test $\mathcal{U}$, η ποσότητα $d_{\mathcal{U}}$ καθορίζει αν ένα ω είναι τυχαίο ή όχι ως εξής, ένα $\omega \in \{0,1\}^{\mathbb{N}}$ είναι ML-τυχαίο αν $d_{\mathcal{U}}(\omega) < \infty$, με τη συμβαση ότι $U_0 = \{0,1\}^{\mathbb{N}}$, ώστε η $d_{\mathcal{U}}$ να είναι πάντα μεγαλύτερη η ίση του μηδεν. Η ποσότητα $d_{\mathcal{U}}(\omega)$ μέτρα αν θέλετε το κατά πόσο απέχει το ω, από την τυχαιότητα.

Κλείνουμε την αναφόρα αυτή, και συνεχίζουμε με ένα πόρισμα του θεωρήματος 4.1.1.

Πόρισμα 4.1.1. *Έστω $A \subset \{0,1\}^{\mathbb{N}}$. Το A είναι Ε-μηδενικό ως προς κάποιο υπολογίσιμο μέτρο μ, αν και μόνο αν κάθε $\omega \in A$ δεν είναι ML-τυχαίο.*

Απόδειξη. Αν το A είναι Ε-μηδενικό, τότε $A \subset U$ από το θεώρημα 4.1.1 και συνεπώς κάθε $\omega \in A$ δεν είναι ML-τυχαίο, αφού ανήκει στο U.

Αντίστροφα, αν κάθε $\omega \in A$ δεν είναι ML-τυχαίο, τότε $A \subset U$, άρα το A είναι Ε-μηδενικό. ◇

Δηλαδή η προσθήκη ενός ML-τυχαίου ω σε ένα οποιοδήποτε Ε-μηδενικό σύνολο, αρκεί ώστε το συγκεκριμένο σύνολο να πάψει να είναι Ε-μηδενικό.

Ας υποθέσουμε ότι έχουμε το ομοιόμορφο μέτρο Bernoulli στον $\{0,1\}^{\mathbb{N}}$, δηλαδή $\mu(V_t) = 2^{-l(t)}$, και $\omega \in \{0,1\}^{\mathbb{N}}$ μια όχι ML-τυχαία ακολουθία ως προς το μ. Θεωρούμε τώρα την ακολουθία $\psi = 0^\frown\omega$, και έστω $\varepsilon \in \mathbb{Q}^+$. Αφού το $\{\omega\}$ είναι Ε-μηδενικό, υπάρχει υπολογίσιμη συνάρτηση t, τέτοια ώστε

$$\omega \in \bigcup_{n\in\mathbb{N}} V_{t(n,\varepsilon)} \quad \text{και} \quad \sum_{n\in\mathbb{N}} p_\mu(t(n,\varepsilon)) < \varepsilon.$$

Αν $r(n,\varepsilon) = 0^\frown t(n,\varepsilon)$, τότε η r είναι υπολογίσιμη και είναι εύκολο να διαπιστώσει κανείς ότι παράγει ένα κάλυμμα για την ψ, με $\sum_{n\in\mathbb{N}} p_\mu(r(n,\varepsilon)) < \varepsilon/2$. Άρα η ψ είναι ML-τυχαία. Παρομοίως αν θεώρησούμε την $\chi = \omega_1\omega_2\ldots$, δηλαδή από την ω αφαιρέσαμε το πρώτο ψηφίο, τότε παίρνοντας ένα κάλυμμα για την ω για $\varepsilon' = \varepsilon/2$, καταλήγουμε ότι η χ δεν είναι ML-τυχαία.

Επαγωγικά έχουμε ότι προσθέτοντας λέξεις στην άρχη μιας όχι ML-τυχαίας ακολουθίας, είτε διαγράφωντας τα πρώτα n ψηφία της τότε η ακολουθία που προκύπτει δεν είναι ML-τυχαία. Με βάση αυτό, προκύπτει ότι μεταβάλλοντας ψηφία σε πεπερασμένες το πλήθος θέσεις της ω, επίσης το αποτέλεσμα δεν είναι μια ML-τυχαία ακολουθία.

Με βάση τα παραπάνω ουσιαστικά αποδείξαμε την επόμενη πρόταση.

Πρόταση 4.1.1. *Έστω $\omega \in \{0,1\}^{\mathbb{N}}$ μια όχι ML-τυχαία ακολουθία ως προς το ομοιόμορφο μέτρο Bernoulli. Τότε οποιαδήποτε ακολουθία ψ με,*

$$|\{i \in \mathbb{N} \mid \omega(i) \neq \psi(i)\}| < \infty,$$

δεν είναι ML-τυχαία.

Παρά το γεγόνος ότι το μέτρο του συνόλου των ML-τυχαίων ακολουθίων ισούται με 1, αφού $\mu(U) = 0$, δεν είναι εύκολο να δώσει κανείς παραδείγματα ακολουθιών οι οποίες είναι ML-τυχαίες. Ισως το πιο γνώστο παράδειγμα ML-τυχαίας ακολουθίας είναι η σταθερά Ω, του Chaitin, η οποία αντιπροσωπεύει, πολύ χονδρικά, την πιθανότητα ένα τυχαία κατασκευασμένο πρόγραμμα να τερματίσει.

Αναφέρουμε τέλος ότι αποδεικνύεται ότι κάθε ML-τυχαία ακολουθία ως προς το ομοιόμορφο μέτρο Bernoulli, έχει οριακή συχνότητα των ψηφιών 1, 1/2, δηλαδή για κάθε ML-τυχαία ακολουθία ως προς το συγκεκριμένο μέτρο, $\omega = \omega_0\omega_1\ldots$, ισχύει ότι,

$$\lim_{n\to\infty} \frac{\omega_0 + \omega_1 + \cdots + \omega_{n-1}}{n} = \frac{1}{2}.$$

4.2 Θεώρημα Levin-Schnorr

Ολοκληρώνουμε την εργασία αυτή, παρουσιάζοντας μια εφαρμογή της προθεματικής πολυπλοκότητας στον χαρακτηρισμό των ML-τυχαίων στοιχείων του $\{0,1\}^{\mathbb{N}}$. Σκοπός μας είναι να παρουσιάσουμε το θεώρημα Levin-Schnorr το οποίο αποδείχθηκε από τον Claus Schnorr στο [8]. Ιστορικά οι Levin και Chaitin, όπως αναφέραμε, παρουσιάσαν πρώτοι την προθεματική πολυπλοκότητα, με βάση την οποία ένα $\omega \in \{0,1\}^{\mathbb{N}}$ καλείται αλγοριθμικά τυχαίο αν υπάρχει σταθερά d, έτσι ώστε για κάθε $n \in \mathbb{N}$, $K(\omega_{|n}) \geq n - d$. Ο Schnorr το 1973

απέδειξε ότι ένα ω είναι ML-τυχαίο ως προς το ομοιόμορφο μέτρο Bernoulli αν και μόνο αν είναι αλγοριθμικά τυχαίο. Έμεις στην τελευταία ενότητα θα αποδείξουμε μια γενικότερη μορφή αυτού του αποτελέσματος, για οποιοδήποτε υπολογίσιμο μέτρο στο $\{0,1\}^{\mathbb{N}}$.

Για να αποδείξουμε το εν λόγω θεώρημα θα χρειαστούμε αρκετά από όσα παρουσιάσαμε στο προηγούμενο κεφάλαιο και μερικά σύντομα λήμματα. Ξεκινάμε με το πρώτο.

Λήμμα 4.2.1. *Έστω $\{p_i\}_{i\in\mathbb{N}}$ ημιυπολογίσιμο μέτρο στο $\mathbb{N}$. Τότε υπάρχει υπολογίσιμη prefix free συνάρτηση $f : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$, τέτοια ώστε για κάθε $i \in N$,*

$$K_f(i) \leq -\log p_i + 2.$$

Απόδειξη. Η απόδειξη ακολουθεί αυτήν του θεωρήματος 3.2.5, για το λόγο αυτό παρουσιάζεται συνοπτικα. Έστω r_p η υπολογίσιμη συνάρτηση που προσεγγίζει τις τιμές p_i. Ορίζουμε τότε

$$r'_p(i,n) = \begin{cases} \min\{1/2^k \mid k \in \mathbb{N}, r_p(i,n) \leq 1/2^k\}, & \text{αν } r_p(i,n) > 0 \\ 0, & \text{αν } r_p(i,n) \leq 0. \end{cases}$$

Για να έχει νόημα το συμπέρασμα προφανώς $p_i > 0$ για κάθε i, επομένως αν

$$J_i = \{n \in \mathbb{N} \mid r'_p(i,n) > r'_p(i,n-1)\},$$

τότε για κάθε i ισχύει ότι $J_i \neq \emptyset$, $|J_i| < \infty$ και $\sum_{n\in J_i} r'_p(i,n) \leq 4p_i$. Το $J = \bigcup_{i\in\mathbb{N}}\{i\} \times J_i$ είναι αναδρομικό, και έστω (i_k, n_k) μια απαρίθμηση των στοιχείων του. Επιλέγοντας τώρα φυσικούς αριθμούς l_k, ως εξής,

$$2^{-l_k} = \frac{r'_p(i_k,n_k)}{4},$$

τότε $\sum_k 2^{-l_k} \leq 1$. Από το πόρισμα 3.2.1 (απόδειξη) υπάρχει υπολογίσιμη h τέτοια ώστε $K_h(k) = l_k = -\log r'_p(i_k,n_k) + 2$, άρα και $K_h(k) \leq -\log p_{i_k} + 2$, και αφού το i_k προκύπτει από το k με υπολογίσιμο τρόπο, έστω $g(k) = i_k$, τότε για $f = g \circ h$ έχουμε ότι, $K_f(i_k) \leq -\log p_{i_k} + 2$, από το οποίο προκύπτει το ζητούμενο, διότι για κάθε i υπάρχει k με $i = i_k$. ◇

Λήμμα 4.2.2. *Κάθε αναδρομικά απαριθμητή ακολουθία λέξεων $t_0, t_1, \ldots$, μπορεί να τροποποιηθεί με υπολογίσιμο τρόπο σε μία $\tilde{t}_0, \tilde{t}_1, \ldots$, τέτοια ώστε για $i \neq j$, $\tilde{t}_i \perp \tilde{t}_j$ και $\bigcup_{i\in\mathbb{N}} V_{t_i} = \bigcup_{i\in\mathbb{N}} V_{\tilde{t}_i}$.*

Απόδειξη. Απαριθμόντας τα στοιχεία της ακολουθίας μέσω κάποιου αλγορίθμου, υποθέτουμε ότι έχουμε ορίσει τα $\tilde{t}_j$ για $j < i$. Έστω ότι η i-οστή λέξη

είναι η t_i, τότε υπάρχουν τρία ενδεχόμενα. Η λέξη t_i είτε είναι ασυμβίβαστη με τις i το πλήθος λέξεις $\tilde{t}_j$, που έχουν εμφανιστεί ήδη κατά την απαρίθμηση, είτε έχει προηγηθεί λέξη $\tilde{t}_j$, με $\tilde{t}_j \sqsubseteq t_i$, ή $t_i \sqsubseteq \tilde{t}_j$. Στην πρώτη περίπτωση $\tilde{t}_i = t_i$. Στην δεύτερη, η λέξη t_i, δεν συνεισφέρει κάτι στην ένωση των $V_{\tilde{t}_i}$, δίοτι $V_{t_i} \subset V_{\tilde{t}_j}$, επομένως η t_i " διαγράφεται " από την ακολουθία, και για να ορίζουμε την $\tilde{t}_i$, περιμένουμε την επόμενη λέξη από την ακολουθία, που θα επιστρέψει ο αλγόριθμος, και επαναλαμβάνουμε την διαδικασία. Τέλος, αν $t_i \sqsubseteq \tilde{t}_j$, τότε θεωρούμε τις λέξεις $s_0, s_1, \ldots, s_{N-1}$, όπου $N = 2^{l(\tilde{t}_j)-l(t_i)} - 1$, μήκους $l(\tilde{t}_j)$, για τις οποίες ισχύει ότι $t_i \sqsubseteq s_m$, και

$$\exists k \geq l(t_i)(s_m(k) \neq \tilde{t}_j(k)),$$

για κάθε $m \leq N-1$. Οι s_m κατασκευάζονται ως εξής, αν $u(k) = 1 - \tilde{t}_j(k)$, τότε,

$$s_0 = t_i^\frown u(l(t_i))\tilde{t}_j(l(t_i)+1)\ldots\tilde{t}_j(l(\tilde{t}_j)-1)),$$
$$s_1 = t_i^\frown \tilde{t}_j(l(t_i))u(l(t_i)+1)\ldots\tilde{t}_j(l(\tilde{t}_j)-1)),\ \text{κ.ο.κ.}$$

Τότε είναι εύκολο να διαπιστώσουμε ότι οι λέξεις s_m είναι ανά δύο ασυμβίβαστες και

$$V_{t_i} \backslash V_{\tilde{t}_j} = \bigcup_{m=0}^{N-1} V_{s_m}.$$

Σε αυτή την περίπτωση λοιπόν αντικάθιστουμε την t_i με τις $s_0, \ldots, s_{N-1}$, και έχουμε ορίσει ουσιαστικά τις $\tilde{t}_i = s_0, \tilde{t}_{i+1} = s_1, \ldots, \tilde{t}_{i+N} = s_{N-1}$.

Είναι εύκολο να διαπιστώσουμε ότι σε κάθε περιπτώση η ένωση των πρώτων i το πλήθος, V_t δεν έχει μεταβληθεί με την προηγούμενη διαδικάσια, από το οποίο προκύπτει το ζητούμενο. ◇

Διατυπώνουμε και αποδεικνύουμε τώρα το τελευταίο αποτέλεσμα στην εργασία αυτή.

Θεώρημα 4.2.1 (Levin-Schnorr). *Ένα $\omega \in \{0,1\}^{\mathbb{N}}$ είναι ML-τυχαίο ως προς το υπολογίσιμο μέτρο μ αν και μόνο αν υπάρχει σταθερά c, τέτοια ώστε για κάθε $n \in \mathbb{N}$ να ισχύει ότι,*

$$K(\omega_{|n}) \geq -\log p_\mu(\omega_{|n}) - c. \tag{4.3}$$

Απόδειξη. Για την απόδειξη θα χρησιμοποιήσουμε την prefix free εκδοχή της K. Αποδεικνύουμε αρχικά το ευθύ, δείχνοντας ότι αν για κάποιο ω, η διαφορά $-\log p_\mu(\omega_{|n}) - K(\omega_{|n})$ είναι μη φραγμένη, τότε το ω δεν είναι ML-τυχαίο. Έστω λοιπόν $\omega \in \{0,1\}^{\mathbb{N}}$, τέτοιο ώστε για κάθε $n \in \mathbb{N}$, να υπάρχει $M \in \mathbb{N}$ έτσι ώστε, $-\log p_\mu(\omega_{|n}) - K(\omega_{|n}) > M$. Για δεδομένο M, θεωρούμε το σύνολο

$$T_M = \{t \in \{0,1\}^{<\mathbb{N}} \mid -\log p_\mu(t) - K(t) > M\},$$

το οποίο από υπόθεση είναι μη κενό, και επίσης είναι αναδρομικά απαριθμητό, δίοτι η συνάρτηση $-\log p_\mu - K$ είναι κάτω ημιυπολογίσιμη.

Αν με $[T_M]$, συμβολίσουμε το εξής σύνολο,

$$[T_M] = \{\psi \in \{0,1\}^{\mathbb{N}} \mid \exists t \in T_M (t \sqsubseteq \psi)\},$$

είναι προφανές από την υπόθεση μας ότι $\omega \in [T_M]$, και ισχυριζόμαστε τότε ότι $\mu([T_M]) < 2^{-M}$. Αρχικά το $[T_M]$, είναι μετρήσιμο, δίοτι, αν

$$T'_M = \{t \in T_M \mid \nexists s \in T_M (s \sqsubseteq t, s \neq t)\},$$

τότε είναι εύκολο να διαπιστώσουμε ότι $[T_M] = \bigcup_{t \in T'_M} V_t$. Για κάθε $t \in T'_M$, θεωρούμε $q_t \in \{0,1\}^{<\mathbb{N}}$, την βέλτιστη D-περιγραφή του t, όπου D είναι η υπολογίσιμη prefix free συνάρτηση που χρησιμοποιήσαμε στον ορισμό της K. Άρα, από υπόθεση έχουμε ότι, $K(t) = l(q_t) < -\log p_\mu(t) - M$, από το οποίο προκύπτει άμεσα ότι

$$2^{-l(q_t)} > p_\mu(t) 2^M = \mu(V_t) 2^M. \tag{4.4}$$

Εφόσον, $[T_M] = \bigcup_{t \in T'_M} V_t$, από την 4.4, προκύπτει ότι,

$$\mu([T_M]) = \mu(\bigcup_{t \in T'_M} V_t) \leq \sum_{t \in T'_M} \mu(V_t) < \sum_{t \in T'_M} \frac{2^{-l(q_t)}}{2^M} \leq 2^{-M}.$$

Το ζήτημα είναι ότι παρότι το T_M είναι αναδρομικά απαριθμητό, δεν ισχύει το ίδιο απαραίτητα για το T'_M, γι αυτό το λόγο χρειαζόμαστε το λήμμα 4.2.2. Αν $t_0, t_1, \ldots,$ είναι μια απαρίθμηση του T_M, τότε υπάρχει απαριθμητή ακολουθία λέξεων $\tilde{t}_0, \tilde{t}_1, \ldots,$ ανα δύο ασυμβίβαστων με, $\bigcup_{i \in \mathbb{N}} V_{t_i} = \bigcup_{i \in \mathbb{N}} V_{\tilde{t}_i}$. Επομένως για ένα σταθερό $M \in \mathbb{N}$, έχουμε κατασκευάσει μια απαριθμητή ακολουθία από λέξεις με,

$$\{\omega\} \subset \bigcup_{i \in \mathbb{N}} V_{\tilde{t}_i} \quad \text{και} \quad \sum_{i \in \mathbb{N}} p_\mu(\tilde{t}_i) < 2^{-M},$$

και αφού η παραπάνω διαδικάσια γίνεται για κάθε M, δοθέντος $\varepsilon \in \mathbb{Q}^+$, μπορούμε να επιλέξουμε M, με $2^{-M} < \varepsilon$, από το οποίο προκύπτει ότι το $\{\omega\}$ είναι E-μηδενικό για το μ, και άρα το ω δεν είναι ML-τυχαίο.

Για το αντίστροφο, θα δείξουμε πάλι, ότι αν ένα $\{\omega\}$ είναι ένα E-μηδενικό σύνολο για το μ, τότε η διαφορά $-\log p_\mu(\omega_{|n}) - K(\omega_{|n})$ είναι μη φραγμένη. Έστω λοιπόν $\omega \in \{0,1\}^{\mathbb{N}}$ με το $\{\omega\}$, E-μηδενικό. Έστω $n \in \mathbb{N}$, μπορούμε λοιπόν να έχουμε μια αναδρομικά απαριθμητή ακολουθία από λέξεις $t(0, 2^{-n}), t(1, 2^{-n}), \ldots,$ με

$$\{\omega\} \subset \bigcup_{i \in \mathbb{N}} V_{t(i, 2^{-n})} \quad \text{και} \quad \sum_{i \in \mathbb{N}} p_\mu(t(i, 2^{-n})) < 2^{-n}.$$

Θεωρούμε την ακολουθία, $p_i = 2^n p_\mu(t(i, 2^{-n}))$, $i \in \mathbb{N}$, η οποία είναι υπολογίσιμη και $\sum_{i\in\mathbb{N}} p_i \leq 1$. Από το λήμμα 4.2.1, υπάρχει υπολογίσιμη prefix free συνάρτηση f, τέτοια ώστε $K_f(i) \leq -\log p_i + 2$, και αφού η απεικόνιση $i \mapsto t(i, 2^{-n})$ είναι υπολογίσιμη, θεωρώντας F_n τη σύνθεση των δύο απεικονίσεων, $t_i = t(i, 2^{-n})$ και από τον ορισμό του p_i έχουμε ότι,

$$K_{F_n}(t_i) \leq -\log p_\mu(t_i) - n + 2.$$

Θα πρέπει τώρα να συνδιάσουμε όλες τις F_n (σημειώνουμε ότι κάθε F_n είναι prefix free) με κάποιον τρόπο. Θεωρούμε, την $D : \{0,1\}^{<\mathbb{N}} \rightharpoonup \{0,1\}^{<\mathbb{N}}$ ως εξής,

$$D(\overline{bin(n)}01u) = v \iff F_n(u) = v,$$

και δεν είναι δύσκολο να διαπιστώσουμε ότι η D είναι υπολογίσιμη και prefix free. Επομένως από τον ορίσμο της D προκύπτει ότι,

$$K(t_i) \leq -\log p_\mu(t_i) - n + O(\log n),$$

άρα $-\log p_\mu(t_i) - K(t_i) \geq n - O(\log n)$, και αφού το $\{\omega\} \subset \bigcup_{i\in\mathbb{N}} V_{t(i,2^{-n})}$, για κάθε $n \in \mathbb{N}$, δηλαδή για κάθε n το ω έχει αρχικά τμήματα μέσα στην ενώση $\bigcup_{i\in\mathbb{N}} V_{t(i,2^{-n})}$ από το οποίο προκύπτει ότι προκύπτει το ζητούμενο. ◇

Στην περίπτωση του ομοιόμορφου μέτρου Bernoulli, έχουμε την εξής ειδική περίπτωση.

Πόρισμα 4.2.1. *Ένα $\omega \in \{0,1\}^{\mathbb{N}}$ είναι ML-τυχαίο ως προς το ομοιόμορφο μέτρο Bernoulli αν και μόνο αν υπάρχει σταθερά c, τέτοια ώστε για κάθε $n \in \mathbb{N}$ να ισχύει ότι,*

$$K(\omega_{|n}) \geq n - c. \tag{4.5}$$

Απόδειξη. Προκύπτεί άμεσα από το θεώρημα 4.2.1, δίοτι αν μ είναι το ομοιόμορφο μέτρο Bernoulli, τότε για $t \in \{0,1\}^{<\mathbb{N}}$, $-\log p_\mu(t) = l(t)$. ◇

Συμπεράσματα

Ολοκληρώνοντας την εργάσια αυτή θα θέλαμε να σχολιάσουμε όσα είδαμε κυριώς στα δύο τελευταία κεφάλαια και το πώς συνδέεται η πολυπλοκότητα ενός αντικειμένου x, με την εσωτερική δομή του αντικειμένου αυτού. Είδαμε αρχικά ότι $K(x) \simeq -\log m(x)$, το οποίο ερμηνεύσαμε ως: όσο πιο μεγάλη είναι η προθεματική πολυπλοκότητα μιας λέξης x, τόσο πιο απίθανο είναι να προκύψει η λέξη x, από μια αλγοριθμική διαδικασία. Η αλήθεια είναι ότι η πόσοτητα m που συναντήσαμε στο τρίτο κεφάλαιο προκύπτει και διαφορετικά. Αν D είναι μια καθολική prefix free υπολογίσιμη συνάρτηση, τότε η $m(x)$, ορίζεται και ως η πιθάνοτητα η D να μας παράγει το x, όταν την τροφοδωτούμε με λέξεις από 0 και 1, οι οποίες προκύπτουν τυχαία, π.χ. με το στρήψιμο ενός νομίσματος, δηλαδή,

$$m(x) = \sum_{p:D(p)=x} 2^{-l(p)}.$$

Έτσι ο κυρίαρχος όρος του παραπάνω αθροίσματος είναι φανερό ότι είναι ο $2^{-K(x)}$, και συνεπώς για μία λέξη ισχύει ότι, όσο πιο πολύπλοκη περιγράφη έχει τόσο πιο απίθανο είναι να την παράξει τυχαία ένα πρόγραμμα. Βέβαια και οι δύο ποσότητες K και m, δεν είναι υπολογίσιμες, παρ᾽ όλα αυτά είναι δυνατόν να τις προσεγγίζουμε με υπολογίσιμες συνάρτησεις, όπως είδαμε. Για περισσότερα πάνω στην a priori πιθανότητα και τις εφαρμογές της, ο αναγνώστης μπορεί να συμβουλευτεί το [5].

Στο τέταρτο κεφάλαιο, συνδέσαμε την προθεματική πολυπλοκότητα με την τάση που έχει ο ανθρώπινος νους να χαρακτηρίζει τα αντικείμενα που συναντά ως τυχαία ή όχι. Αξίζει να σημειωθεί ότι σπουδαίοι μαθηματικοί, είχαν κάνει την παρατήρηση αυτή, δηλαδή ότι υπάρχει κάτι το διαφορετικό ανάμεσα στις ακολουθίες 00000000... και 01011110..., αλλά δεν είχαν αναπτυχθεί ακόμη τα κατάλληλα εργαλεία ώστε να διατυπώθουν με μαθηματική αυστηρότητα αυτές οι ιδέες. Απαραίτητο μέσο για να εκφραστούν μαθηματικά αυτές οι ιδέες, όπως είδαμε, είναι η θεωρία υπολογισιμότητας, και γενικότερα η έννοια του αλγορίθμου.

Καταλήξαμε έτσι σε μια ικανή και αναγκαία συνθήκη τυχαιότητας με βάση την πολυπλοκότητα, το θεώρημα Levin-Schnorr το οποίο αποτελεί μια μαθημα-

τική διατύπωση αυτού που έχουμε στο μυαλό μας λίγο πολύ όλοι, ότι αν κάτι γίνεται όλο και πιο δύσκολο να περιγραφεί ή να προβλεφθεί, τότε δεν μπορεί παρά αυτό το κάτι να είναι τυχαίο.

Τέλος, αξίζει να αναφέρουμε ότι, πριν μερικά χρόνια αποδείχθηκε από τους Miller J.S. και Yu L. ένα αντίστοιχο κριτήριο τυχαιότητας για το ομοιόμορφο μέτρο Bernoulli, χρησιμοποιώντας την απλή πολυπλοκότητα Kolmogorov, το οποίο λέει συγκεκριμένα το εξής.

Θεώρημα (Miller-Yu). *Ένα $\omega \in \{0,1\}^{\mathbb{N}}$ είναι ML-τυχαίο ως προς το ομοιόμορφο μέτρο Bernoulli αν και μόνο αν για κάθε υπολογίσιμη ολική συνάρτηση $f : \mathbb{N} \to \mathbb{N}$, με $\sum_{n\in\mathbb{N}} 2^{-f(n)} < \infty$, υπάρχει σταθερά c, τέτοια ώστε για κάθε $n \in \mathbb{N}$ να ισχύει ότι,*

$$C(\omega_{|n}) \geq n - f(n) - c.$$

Το μειονέκτημα του παραπάνω αποτελέσματος, είναι προφανώς η ύπαρξη του ποσοδείκτη "... για κάθε υπολογίσιμη f...". Αποδεικνύεται ότι αν θέλει κανείς να απαλλαγεί από αυτό, αρκεί να επιστρέψει στην προθεματική πολυπλοκότητα K και να διαπιστώσει αν ισχύει για κάποια σταθερά c, και για κάθε n, ότι,

$$C(\omega_{|n}) \geq n - K(n) - c.$$

Βιβλιογραφία

[1] Boolos G.S., Burgess J.P. & Jeffrey R.C.: Computability and Logic (Fifth Edition). Cambridge University Press, 2007.

[2] Chaitin G.J.: A Theory of Program Size Formally Identical to Information Theory. Journal of the ACM Vol.22, 1975.

[3] Kolmogorov A.N.: Three Approaches to the Quantitative Definition of Information. Problems Of Information Transition 1, 1965.

[4] Levin L.A. & Zvonkin A.K.: The Complexity of Finite Objects and the Development of the Concepts of Information and Randomness by Means of the Theory of Algorithms. Russian Mathematical Surveys Vol. 25, 1970.

[5] Li M. & Vitanyi P.M.B.: An Introduction to Kolmogorov Complexity and Its Applications (Third Edition). Springer-Verlag New York, 2008.

[6] Martin-Löf P.: The Definition of a Random Sequence. Information And Control Vol. 9, 1966.

[7] Moschovakis G.N.: Recursion and Computability. διαδικτυακές σημειώσεις, http://www.math.ucla.edu/ ynm/lectures/nirt.pdf.

[8] Schnorr C.P.: Process Complexity and Effective Random Tests. Journal of Computer and System Sciences Vol. 7, 1973.

[9] Shen A., Uspensky V.A. & Vereshchagin N.: Kolmogorov Complexity and Algorithmic Randomness. American Mathematical Society, 2017.