

Το Θεώρημα Κανονικής Μορφής και  
Απαρίθμησης (Kleene)  
και το Πρόβλημα Τερματισμού (Turing)

Βέργου Θεοδώρα  
Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

2 Οκτωβρίου 2017



Διπλωματική Εργασία

Επιβλέπων: Αρβανιτάκης Αλέξανδρος -Επίκουρος Καθηγητής Ε.Μ.Π

Τριμελής Εξεταστική Επιτροπή:

1. Αρβανιτάκης Αλέξανδρος (Επίκουρος Καθηγητής)
2. Χαραλαμπίδης Αντώνιος (Καθηγητής)
3. Στεφανέας Πέτρος (Επίκουρος Καθηγητής)

Αθήνα, Οκτώβριος 2017

# Μέρος I

## Εισαγωγικά

### 1 Λίγα λόγια

Η θεωρία των αναδρομικών συναρτήσεων, ως ξεχωριστός κλάδος των μαθηματικών, εμφανίστηκε τη δεκατία του 1930, μέσα από τις έρευνες των Kleene, Church και Turing. Ένα από τα βασικά της ορίσματα είναι τυπικοί χαρακτηρισμοί των μερικών συναρτήσεων τόσο από τους Turing και Kleene, όσο και από άλλους, που έχουνδειχθεί ίσοδύναμοι. Ο κάθε χαρακτηρισμός διαφέρει ως προς δομή και λεπτομέρεια, όλοι όμως δίνουν τυπικούς ορισμούς για αλγοριθμο / πρόγραμμα και εν συνεχεία τυπικούς ορισμούς για τις μερικές συναρτήσεις υπολογίσιμες από πρόγραμμα.

Στο παρόν σύγγραμμα, θα δούμε την τυπική μορφή που έδωσε ο Kleene για τις μερικές συναρτήσεις υπολογίσιμες από πρόγραμμα. Συγκεκριμένα στο θεώρημα Κανονικής Μορφής και Απαρίθμησης, ο Kleene, έδωσε έναν τρόπο υπολογισμού των αναδρομικών συναρτήσεων.

*"Κάθε αναδρομική συνάρτηση μπορεί να υπολογιστεί από τις βασικές συναρτήσεις (μηδέν, επομένου, ταυτοτική) με σύνθεση, πρωτογενή αναδρομή και ελαχιστοποίηση, χρησιμοποιώντας την τελευταία μόνο μια φορά"*

Περίπου το 1936 οι Church και Turing, έδειξαν ότι οι αναδρομικές συναρτήσεις όπως ορίστηκαν από τον Gödel, οι λ-υπολογίσιμες όπως ορίστηκαν από τον Church και οι συναρτήσεις που είναι υπολογίσιμες από μια μηχανή Turing ταυτίζονται. Μάλιστα διατύπωσαν την εξής θέση:

*"Η τυχαία μερική συνάρτηση στους φυσικούς είναι υπολογίσιμη αν και μόνο αν είναι αναδρομική"*

Επειδή η έννοια της υπολογισιμότητας είναι διαισθητική έννοια, η θέση δεν επιδέχεται αυστηρή απόδειξη. Μέχρι και σήμερα όμως δεν αμφισβητείται από τη μαθηματική κοινότητα.

Σε κάθε περίπτωση πάντως, η ταύτιση των αναδρομικών συναρτήσεων με τις υπολογίσιμες από μηχανή, είναι από μόνη της αρκετά ενδιαφέρουσα.

## Δομή

Το σύγγραμμα έχει τον εξής σκελετό:

Μαθηματικό Υπόβαθρο - Θεώρημα Κανονικής Μορφής - Απόδειξη Θεωρήματος - Το Πρόβλημα Τερματισμού.

-Στο μαθηματικό υπόβαθρο αρχικά θα δώσουμε τον ορισμό του αναδρομικού σχήματος και των πρωτογενώς αναδρομικών συνόλων, συναρτήσεων και προγραμμάτων.

Με την εισαγωγή του μ-σχήματος θα ορίσουμε τη διαδικασία της αναζήτησης και έπειτα τις ελαχιστικά-αναδρομικές συναρτήσεις. Στη συνέχεια θα κινηθούμε σε ένα καινούριο περιβάλλον, τις μερικές άλγεβρες, μέσα στο οποίο θα ορίσουμε γλώσσα που μπορεί να ερμηνευθεί και σαν γλώσσα προγράμματος. Εδώ γίνεται σιγά σιγά ξεκάθαρη η σχέση των αναδρομικών συναρτήσεων και αναδρομικών προγραμμάτων.

Τέλος θα ορίσουμε κωδικοποίηση. Την κωδικοποίηση (με τον τρόπο που θα οριστεί) την εισήγαγε για πρώτη φορά ο Gödel, και αποδίδει σε κάθε σύμβολο και κάθε σχέση μια τυπικής γλώσσας ένα μοναδικό φυσικό αριθμό (αριθμό Gödel).

-Θα διατυπώσουμε το Θεώρημα Κανονικής Μορφής του Kleene και θα δώσουμε μια ερμηνεία του.

-Θα προχωρήσουμε στην απόδειξη των επιμέρους ορισμάτων του θεωρήματος χρησιμοποιώντας όσα ορίσαμε στο Μαθηματικό Υπόβαθρο, και ειδικά στην Κωδικοποίηση.

-Τέλος θα παραθέσουμε το πρόβλημα τερματισμού του Turing και θα το αποδείξουμε, ως εφαρμογή του θεωρήματος του Kleene.

## 2 Μαθηματικό Υπόβαθρο

### 2.1 Συμβολισμοί

Παραθέτουμε μερικούς συμβολισμούς από τη λογική και τη συνολοθεωρία

$\&$ : και

$\vee$ : ή

$\neg$ : όχι

$\implies$ : συνεπάγεται

$\iff$ : αν και μόνο αν

$\forall$ : για κάθε

$\exists$ : υπάρχει

$\exists!$ : υπάρχει μοναδικό

$x \in A \iff$  το στοιχείο  $x$  ανήκει στο σύνολο  $A$

$A \subseteq B \iff$  κάθε μέλος του  $A$  είναι μέλος του  $B$

$\iff (\forall x)[x \in A \implies x \in B]$

$A = B \iff$  τα σύνολα  $A$  και  $B$  έχουν ακριβώς τα ίδια μέλη

$\iff A \subseteq B \& B \subseteq A$

$f : A \longrightarrow B \iff$  η  $f$  είναι συνάρτηση με πεδίο εισόδου (ορισμού) το σύνολο  $A$  και πεδίο εξόδου (τιμών) το σύνολο  $B$

$f : A \mapsto B \iff$  η  $f$  είναι μονοφορμισμός από το σύνολο  $A$  στο  $B$

$f : A \twoheadrightarrow B \iff$  η  $f$  είναι αντιστοιχία από το σύνολο  $A$  στο  $B$

$\{x|P(x)\} =$  το σύνολο όλων των  $x$  που έχουν την ιδιότητα  $P(x)$

$\{x \in A|P(x)\} = \{x|x \in A \& P(x)\}$

$A \times B = \{(a, b)|a \in A \text{ και } b \in B\}$

$A \times B \times C = \{(a, b, c)|a \in A, b \in B, c \in C\}$

## 2.2 Αναδρομή

**Λήμμα 2.1. Βασικό Λήμμα Αναδρομής** Για όλα τα σύνολα  $X, W$  και δοσμένες συναρτήσεις  $g: X \rightarrow W, h: W \times \mathbb{N} \times X \rightarrow W$ , υπάρχει ακριβώς μια συνάρτηση  $f: \mathbb{N} \times X \rightarrow W$  τέτοια ώστε

$$f(0, x) = g(x)$$

$$f(n+1, x) = h(f(n), n, x)$$

Θα δείξουμε με χρήση της Αρχής της Επαγωγής ότι η  $f$  όντως υπάρχει, είναι συνάρτηση και είναι μοναδική.

**Απόδειξη.** Οι συναρτήσεις στο Λήμμα είναι ορισμένες στα σύνολα  $\mathbb{N}, X, W$  αλλά το αναδρομικό σχήμα που περιγράφεται μπορεί να εφαρμοστεί και στα σύνολα  $\mathbb{N}, W$ . Καλούμε την πρώτη περίπτωση αναδρομικό σχήμα με παράμετρο και την δεύτερη αναδρομικό σχήμα χωρίς παράμετρο.

Χάρην ευκολίας θα ξεκινήσουμε την απόδειξη μας για το αναδρομικό σχήμα χωρίς παράμετρο:

$\forall w_0 \in W$  και  $\forall h: W \times \mathbb{N} \rightarrow W$  υπάρχει ακριβώς μια συνάρτηση  $f: \mathbb{N} \rightarrow W$  τέτοια ώστε

$$f(0) = w_0$$

$$f(n+1) = h(f(n), n)$$

Για την ύπαρξη της  $f: \mathbb{N} \rightarrow W$  θέτουμε

$$W^n = (w_0, \dots, w_{n-1}) | w_i \in W, n \in \mathbb{N},$$

και ορίζουμε το σύνολο των προσεγγίσεων της  $f: \mathbb{N} \times X \rightarrow W$  ως  $P(n, w) \in A$ :

$$P(n, w) \in A \iff P \text{ συνάρτηση } \& \text{Domain}(P) \subseteq \mathbb{N} \& \text{Image}(P) \subseteq W \& 0 \in \text{Domain}(P) \& P(0) = w_0 \& (\forall n \in \mathbb{N}) [S_n \in \text{Domain}(P) \Rightarrow n \in \text{Domain}(P) \& P(S_n) = h(P(n))]$$

όπου  $S_n$  η συνάρτηση του επομένου  $S_n = n + 1$

(Τα ζεύγη  $(n, w)$  είναι προσεγγίσεις της  $f(n) = w$  και έχουν πεδίο ορισμού υποσύνολα του  $\mathbb{N}$ )

Πρέπει να δείξουμε ότι υπάρχει ακριβώς μια συνάρτηση  $f: \mathbb{N} \rightarrow W$  που να ανήκει στο (μοναδικότητα).

Έστω λοιπόν δύο συναρτήσεις-προσεγγίσεις  $P_1, P_2$  στο  $A$ . Πεδία ορισμού έχουν υποσύνολα του  $\mathbb{N}$ .

Αρα για  $n \in \mathbb{N}$  θα δείξουμε ότι

$$n \in \text{Domain}(P_1) \cap \text{Domain}(P_2) \Rightarrow P_1(n) = P_2(n).$$

Δηλαδή στις τομές των πεδίων ορισμού τα ζεύγη  $(n, w)$  των προσεγγίσεων ταυτίζονται και αυτό συμβαίνει σε όλο το  $\mathbb{N}$ .

$$\text{Έστω } X = \{n \in \mathbb{N} | (\forall P_1, P_2 \in A) n \in \text{Domain}(P_1 \cap \text{Domain}(P_2)) \Rightarrow P_1(n) = P_2(n)\}$$

Προφανώς  $0 \in X$  αφού  $\forall P \in A \ 0 \in \text{Domain}(P) \ \& \ P(0) = w_0$   
 Έστω  $n \in X \ \& \ P_1, P_2 \in A \ \& \ Sn \in \text{Domain}(P_1) \cap \text{Domain}(P_2)$  τότε  
 $P_1(Sn) = h(P_1(n)) \ P_1 \in A$   
 $= h(P_2(n)) \ n \in X$   
 $= P_2(Sn) \ P_2 \in A$   
 Άρα  $n \in X \Rightarrow Sn \in X$   
 $X \equiv \mathbb{N}$ .

Άρα για όλα τα  $n \in \mathbb{N}$  οι τιμές των προσεγγίσεων  $P_i$  της  $f$  ταυτίζονται. Επομένως υπάρχει το πολύ μια  $f : \mathbb{N} \rightarrow W$  τέτοια ώστε  $f \in A$ . Αρκεί να δείξουμε ότι τουλάχιστον μια  $f$  υπάρχει (ύπαρξη).  
 Θέτουμε  $f = \cup A = \{(n, w) \mid (\exists P \in A)[n \in \text{Domain}(P) \ \& \ P(n) = w]\}$

1. Η  $f$  είναι συνάρτηση:

έστω  $(n, w) \in f \ \& \ (n, w') \in f \Rightarrow (\exists P_1, P_2 \in A)[(n, w) \in P_1 \ \& \ (n, w') \in P_2] \Rightarrow w = w' \ (P_1(n) = P_2(n) \ \forall n \in \mathbb{N})$

2.  $f \in A$  καθώς πληρεί τον ορισμό του:

$f$  συνάρτηση (1) & (για κάποιο  $P \in A$ )  $\text{Domain}(f) = \text{Domain}(P) \subseteq \mathbb{N} \ \& \ \text{Image}(f) \subseteq W \ \& \ 0 \in \text{Domain}(f) \ \& \ f(0) = P(0) = w_0 \ \& \ (\forall n \in \mathbb{N})[Sn \in \text{Domain}(f) \Rightarrow Sn \in \text{Domain}(P) \Rightarrow n \in \text{Domain}(P) \Rightarrow n \in \text{Domain}(f) \ \& \ f(Sn) = P(Sn) = h(P(n)) = h(f(n))]$

3.  $\text{Domain}(f) = \mathbb{N}$

Θα το δείξουμε κάνοντας ξανά χρήση της Αρχής της Επαγωγής.

$0 \in \text{Domain}(f)$  αφού  $0 \in \text{Domain}(P)$  για  $P \in A$

Αν  $n \in \text{Domain}(f) \Rightarrow \exists P_1 \in A : n \in \text{Domain}(P_1) \Rightarrow P_2 = P_1 \cup \{Sn \mid P_1(Sn) = h(P_1(n))\} \in A \Rightarrow Sn \in \text{Domain}(P_2) \subseteq \text{Domain}(f) \Rightarrow Sn \in \text{Domain}(f)$

Έχουμε δείξει την ύπαρξη και τη μοναδικότητα της  $f : \mathbb{N} \rightarrow W$ :

$$f(0) = w_0$$

$$f(n+1) = h(f(n))$$

Εάν στη θέση του  $w_0$  έχουμε τη συνάρτηση  $g(x) : X \rightarrow W$  που ορίζεται σε ένα σύνολο παραμέτρων  $X$ .

$\forall x \in X$  θέτουμε  $h_x : W \rightarrow \mathbb{N}$  ώστε  $h_x = h(x, w)$  (κρατάμε δηλαδή σταθερό το  $x$ )

Όπως δείξαμε υπάρχει μοναδική συνάρτηση  $f_x : \mathbb{N} \rightarrow W \times \mathbb{N}$  ώστε

$$f_x(0) = g(x)$$

$$f_x(n+1) = h_x(f(n)) = h(f(n), x)$$

Άρα η  $f(n, x) = f_x(n)$  ικανοποιεί την αναδρομή για παραμετρική μορφή.

□

Έχουμε πλέον διατυπώσει το Βασικό Λήμμα Αναδρομής και δείξει την μαθηματική του βάση.

Θα προχωρήσουμε στον ορισμό ενός πιο αυστηρού πλαισίου, αυτού των πρωτογενώς αναδρομικών συνόλων, με το οποίο μπορούμε να κωδικοποιούμε μαθηματικά αλγόριθμους.

### Πρωτογενώς Αναδρομικά Σύνολα

**Ορισμός 2.2.** Ένα σύνολο  $F$  πλειομελών συναρτήσεων στο  $\mathbb{N}$  είναι πρωτογενώς κλειστό αν:

i) η συνάρτηση του επομένου  $S(x) = x + 1$  ανήκει στο  $F$ .

ii) για κάθε  $n$  και  $q$ , η σταθερή συνάρτηση  $n$  μεταβλητών

$$C_q^n(x_1, \dots, x_n) = q$$

ανήκει στο  $F$

iii) για κάθε  $n$  και  $i$ ,  $1 \leq i \leq n$ , η προβολή

$$P_i^n(x_1, \dots, x_n) = x_i$$

ανήκει στο  $F$ .

iv) Το  $F$  είναι κλειστό για σύνθεση:

Αν η  $m$ -μελής συνάρτηση  $g(u_1, \dots, u_m)$  και οι  $m$ ,  $n$ -μελείς συναρτήσεις  $h_1(\vec{x}), \dots, h_m(\vec{x})$  ανήκουν στο  $F$ , με  $\vec{x} = (x_1, \dots, x_n)$ , τότε και η

$$f(\vec{x}) = g(h_1(\vec{x}), \dots, h_m(\vec{x})) \quad (1)$$

ανήκει στο  $F$ .

v) Το  $F$  είναι κλειστό για πρωτογενή αναδρομή:

Αν η  $n$ -μελής  $g$  και η  $(n+2)$ -μελής  $h$  ανήκουν στο  $F$ , και αν η  $(n+1)$ -μελής  $f$  ορίζεται από τις εξισώσεις

$$f(0, \vec{x}) = g(\vec{x})$$

$$f(y+1, \vec{x}) = h(f(y, \vec{x}), y, \vec{x}) \quad (2)$$

τότε και η  $f$  ανήκει στο  $F$ .

Στην περίπτωση που  $n = 0$  έχουμε πρωτογενή αναδρομή χωρίς παραμέτρους.

**Ορισμός 2.3. Πρωτογενώς Αναδρομική Συνάρτηση.** Μια συνάρτηση  $f$  είναι πρωτογενώς αναδρομική αν ανήκει σε κάθε πρωτογενώς αναδρομικό σύνολο.

Συμβολίζουμε  $R_p = \{f \mid \eta f \text{ είναι πρωτογενώς αναδρομική}\}$  το σύνολο των πρωτογενώς αναδρομικών συναρτήσεων.

Μια συνάρτηση  $f$  είναι πρωτογενώς αναδρομική στο  $A$  για  $A$  σύνολο δοσμένων πλειομελών συναρτήσεων, αν η  $f$  ανήκει σε κάθε πρωτογενώς κλειστό σύνολο που περιέχει το  $A$ .

Αντίστοιχα  $R_p(A) = \{f \mid \eta f \text{ είναι πρωτογενώς αναδρομική στο } A\}$ .



Προφανώς  $R_p = R_p(\emptyset)$ .

**Ορισμός 2.4. Πρωτογενώς Αναδρομικό Πρόγραμμα** είναι η τυχαία ακολουθία πλειομελών συναρτήσεων

$$E = (f_0, f_1, \dots, f_n)$$

τέτοια που για κάθε  $j \leq n$  ισχύει ένα από τα εξής:

- i) η  $f_j$  είναι μια από τις βασικές πρωτογενώς αναδρομικές συναρτήσεις  $S, P_i^n, C_q^n$ .
- ii) η  $f_j$  ορίζεται με σύνθεση (1), όπου οι  $g, h_1, \dots, h_m$  είναι βασικές πρωτογενώς αναδρομικές συναρτήσεις ή εμφανίζονται στις ακολουθία  $f_0, \dots, f_{j-1}$ .
- iii) η  $f_j$  ορίζεται με πρωτογενή αναδρομή (2), όπου οι  $g, h$  είναι βασικές πρωτογενώς αναδρομικές συναρτήσεις ή εμφανίζονται στις ακολουθία  $f_0, \dots, f_{j-1}$ .

Όπως είχαμε αναφέρει, τα πρωτογενώς αναδρομικά σύνολα μας παρέχουν ένα πλαίσιο μέσα στο οποίο μπορούμε να κωδικοποιούμε αλγορίθμους.

Μια πρωτογενώς αναδρομική συνάρτηση είναι υπολογίσιμη από αλγόριθμο. Συγκεκριμένα

**Πρόταση 2.5.** : η τυχαία  $f : \mathbb{N}^k \rightarrow \mathbb{N}$  είναι πρωτογενώς αναδρομική αν και μόνο αν είναι  $f = f_n$  για κάποιο πρωτογενώς αναδρομικό πρόγραμμα  $(f_0, f_1, \dots, f_n)$ .

*Απόδειξη.* Ένα σύνολο συναρτήσεων  $F$  είναι πρωτογενώς κλειστό αν και μόνο αν

- i) περιέχει την συνάρτηση του επομένου  $S(x) = x + 1$  η οποία υπολογίζεται από το πρωτογενές αναδρομικό πρόγραμμα  $S$ .
- ii) περιέχει τη σταθερή συνάρτηση  $C_q^n(x_1, \dots, x_n) = q$  η οποία υπολογίζεται από το πρωτογενές αναδρομικό πρόγραμμα  $C_q^n$ .
- iii) περιέχει τη συνάρτηση-προβολή  $P_i^n(x_1, \dots, x_n) = x_i$  η οποία υπολογίζεται από το πρόγραμμα  $P_i^n$ .
- iv) είναι κλειστό για σύνθεση (1).

Έστω  $G(g_0, g_1, \dots, g_k)$  το πρόγραμμα που υπολογίζει την συνάρτηση  $g$ ,

$H_i(h_{i,0}, h_{i,1}, \dots, h_{i,n_i})$  το πρόγραμμα που υπολογίζει την  $h_i, 1 \leq i \leq m$ .

Τότε η  $f$ , σύνθεση των  $g$  και  $h$ , υπολογίζεται από το:

$$E(g_0, \dots, g_k, h_{1,0}, \dots, h_{1,n_1}, h_{2,0}, \dots, h_{2,n_2}, \dots, h_{m,0}, \dots, h_{m,n_m}, g_k(h_{1,n_1}, \dots, h_{m,n_m})).$$

v) είναι κλειστό για πρωτογενή αναδρομή (2).

Έστω πρόγραμμα  $G(g_0, \dots, g_k)$  που υπολογίζει τη συνάρτηση  $g(x)$ , και

πρόγραμμα  $H(h_0, \dots, h_l)$  που υπολογίζει τη συνάρτηση  $h(w, y, x)$ .

Τότε η  $f$  που προκύπτει από τις  $g, h$  με πρωτογενή αναδρομή (2) υπολογίζεται από το:

$$E(g_0, \dots, g_k, h_0, \dots, h_l, f_0 = g_k, f_1 = h_l(f_0, 0), \dots, f_n = h_l(f(n-1), n-1)).$$

Το ότι κάθε πρωτογενώς αναδρομική συνάρτηση υπολογίζεται από πρωτογενώς αναδρομικό πρόγραμμα, προκύπτει άμεσα με επαγωγή από τον ορισμό για τις περιγραφές των προγραμμάτων που δώσαμε.

Για το αντίστροφο:

Έστω  $D$  το σύνολο όλων των συναρτήσεων  $f$  για τις οποίες υπάρχει ακολουθία  $(f_0, \dots, f_n)$ . Προφανώς το  $D$  περιέχεται σε κάθε σύνολο  $F$  που είναι κλειστό για τα  $i-v$ .

Επιπλέον και το  $D$  είναι κλειστό για τα  $i-v$ .

Άρα το  $D$  συμπίπτει με την τομή όλων των  $F$  και είναι το ελάχιστο σύνολο στο οποίο ορίζεται  $f : \mathbb{N}^n \rightarrow \mathbb{N}$  πρωτογενώς αναδρομική.  $\square$

(Η έννοια του ελάχιστου συνόλου είναι πολύ σημαντική, καθώς μας δίνει τη δυνατότητα να εφαρμόζουμε επαγωγή).

Μέχρι στιγμής έχουμε δει πως μια συνάρτηση είναι πρωτογενώς αναδρομική αν γράφεται στη μορφή (2).

**Πρόταση 2.6.** Οι επόμενες συναρτήσεις είναι πρωτογενώς αναδρομικές:

#1. $x + y$	$x + 0 = 0$
	$x + Sy = S(x + y)$
#2. $x * y$	$x * 0 = 0$
	$x * Sy = x * y + x$
#3. $x^y$	$x^0 = 1$
	$x^{Sy} = x^y * x$
#4. $x!$	$0! = 1$
	$Sx = x! * x$
#5. $Pd(x)$	$Pd(0) = 0$
	$Pd(Sx) = x$
#6. $x \dot{\div} y$	$x \dot{\div} 0 = x$
	$x \dot{\div} Sy = Pd(x \dot{\div} y)$
#7. $min(x, y)$	$min(x, y) = y \dot{\div} (y \dot{\div} x)$
$min(x_1, \dots, x_n)$	$min(x_1, \dots, x_n) = min(\dots min(min(x_1, x_2), x_3), \dots, x_n)$
#8. $max(x, y)$	$max(x, y) = (x + y) \dot{\div} min(x, y)$
$max(x_1, \dots, x_n)$	$max(x_1, \dots, x_n) = max(\dots max(max(x_1, x_2), x_3), \dots, x_n)$
#9. $sg(x) = 0$ αν $x = 0$ , $1$ αν $x > 0$	$sg(x) = min(x, 1)$
#10. $\overline{sg}(x) = 1$ αν $x = 0$ , $0$ αν $x > 0$	$\overline{sg}(x) = 1 \dot{\div} x$
#11. $ x - y $	$ x - y  = (x \dot{\div} y) + (y \dot{\div} x)$
#12. $rm(x, y)$	$rm(0, y) = 0$
	$rm(Sn, y) = S(rm(x, y)) * sg( y - S(rm(x, y)) )$

#13.  $[x/y]$

$$[0/y] = 0$$

$$[Sx/y] = [x/y] + (1 \div y - S(\text{rm}(x, y)))$$

Έχουμε εξ' ορισμού ότι οι βασικές συναρτήσεις  $S, C_q^n, P_i^n$  είναι πρωτογενώς αναδρομικές.

Επίσης το σύνολο  $R_p(A)$  των πρωτογενώς αναδρομικών συναρτήσεων στο  $A$  περιέχει το  $A$  και είναι πρωτογενώς κλειστό.

Ένας άλλος τρόπος λοιπόν να δείξουμε ότι μια συνάρτηση  $f$  είναι πρωτογενώς αναδρομική είναι δίνοντας τον "ρητό ορισμό" της.

*Ρητός ορισμός* στην προκειμένη περίπτωση είναι μια έκφραση κατασκευασμένη χρησιμοποιώντας μόνο τις βασικές συναρτήσεις, πρωτογενώς αναδρομικές συναρτήσεις (από το  $A$ , ή που έχουν ορισθεί επίσης ρητά) και μεταβλητές, η οποία επιστρέφει για κάθε όρισμα την ίδια τιμή που επιστρέφει η  $f$ .

πχ1.  $f(x) = x + 1 = S(x)$

πχ2.  $f(x) = x = P_1^1(x)$

πχ3. για  $g(x, y) \in R_p(A)$

$$f(x, y) = g(x + 1, y) = g(S(P_1^2(x, y), P_2^2(x, y)))$$

Επίσης μπορούμε να θεωρούμε τις σταθερές πρωτογενώς αναδρομικές συναρτήσεις,  $C_q^n$  για  $n = 0$ .

Παρ'όλο που η έννοια των ρητών ορισμών μπορεί να φαίνεται τετριμμένη, είναι σημαντική καθώς καθιστά δυνατή την χρήση των δηλώντριων ή χαρακτηριστικών συναρτήσεων ως αριθμητικές συναρτήσεις.

**Ορισμός 2.7.** Η **χαρακτηριστική συνάρτηση** μιας σχέσης  $P(\vec{x})$  είναι η

$$\chi_{P(\vec{x})} = \begin{cases} 1, & \text{αν } P(\vec{x}) \\ 0, & \text{αλλιώς} \end{cases}$$

και η σχέση  $P(\vec{x})$  είναι πρωτογενώς αναδρομική αν η  $\chi_{P(\vec{x})}$  είναι πρωτογενώς αναδρομική.

Ομοίως για σύνολα: η χαρακτηριστική συνάρτηση του  $A \subseteq \mathbb{N}$  είναι η

$$\chi_A(x) = \begin{cases} 1, & \text{αν } x \in A \\ 0, & \text{αλλιώς} \end{cases}$$

και το  $A$  είναι πρωτογενώς αναδρομικό αν η  $\chi_A$  είναι πρωτογενώς αναδρομική.

Οπότε τώρα έχουμε ακόμα έναν τρόπο ορισμού πρωτογενώς αναδρομικών συναρτήσεων, αυτόν του ορισμού με περιπτώσεις.

**Πρόταση 2.8.** Αν η  $P(\vec{x})$  είναι πρωτογενώς αναδρομική σχέση, οι  $g(\vec{x})$  και  $h(\vec{x})$  πρωτογενώς αναδρομικές συναρτήσεις, και η  $f(\vec{x})$  ορίζεται από αυτές με περιπτώσεις

$$f(\vec{x}) = \begin{cases} g(\vec{x}), & \text{αν } P(\vec{x}) \\ h(\vec{x}), & \text{αλλιώς} \end{cases}$$

τότε η  $f(\vec{x})$  είναι πρωτογενώς αναδρομική.

*Απόδειξη.*  $f(\vec{x}) = \chi_{P(\vec{x})}g(\vec{x}) + (1 \div \chi_{P(\vec{x})})h(\vec{x})$ . □

Αντίστοιχα μπορούμε να ορίσουμε  $f$  πρωτογενώς αναδρομική με  $n$  περιπτώσεις, για κάθε  $n \geq 2$  :

Αν οι χαρακτηριστικές συναρτήσεις  $\chi_{P_i}, 1 \leq i \leq m$  είναι αμοιβαίως αποκλειόμενες, και  $\chi_{P_i}, g_i \in R_p(A)$  τότε η  $f(\vec{x}) = \chi_{P_1}(\vec{x})g_1(\vec{x}) + \dots + \chi_{P_m}(\vec{x})g_m(\vec{x}) + (1 \div \chi_{P_m}(\vec{x}))g_{m+1}(\vec{x})$  είναι επίσης πρωτογενώς αναδρομική στο  $A$ .

Με χρήση των τελευταίων ορισμών, μπορούμε να συμπληρώσουμε στις συναρτήσεις τις **Πρότασης 2.6** που θα θεωρούνται γνωστές ως πρωτογενώς αναδρομικές:

#14.  $x = y$

$$\chi_{=(x,y)} = \overline{sg} |x - y|$$

#15.  $x \leq y$

$$\chi_{\leq(x,y)} = 1 \div (x \div y)$$

#16.  $x|y$

$$\chi_{|(x,y)} = 1 \div rm(y,x)$$

**Πρόταση 2.9. a.** Το σύνολο των πρωτογενώς αναδρομικών σχέσεων είναι κλειστό για τους προτασιακούς τελεστές  $\neg, \vee, \&, \implies$

$$P(\vec{x}) = \neg Q(\vec{x})$$

$$\chi_{P(\vec{x})} = 1 \div \chi_{Q(\vec{x})}$$

$$P(\vec{x}) \iff Q(\vec{x}) \vee R(\vec{x})$$

$$\chi_{P(\vec{x})} = \min(\chi_{Q(\vec{x})} + \chi_{R(\vec{x})}, 1)$$

$$P(\vec{x}) \iff Q(\vec{x}) \& R(\vec{x})$$

$$\chi_{P(\vec{x})} = Pd(\chi_{Q(\vec{x})} + \chi_{R(\vec{x})})$$

$$P(\vec{x}) = Q(\vec{x})$$

$$\chi_{P(\vec{x})} = \chi_{Q(\vec{x})}$$

**b.** Αν  $Q(\vec{y})$  πρωτογενώς αναδρομική σχέση και  $f_1(\vec{x}), \dots, f_m(\vec{x})$  πρωτογενώς αναδρομικές συναρτήσεις, τότε και η σχέση

$$P(\vec{x}) \iff Q(f_1(\vec{x}), \dots, f_m(\vec{x}))$$

είναι πρωτογενώς αναδρομική.

(Προφανές αφού η χαρακτηριστική συνάρτηση της  $Q$  και οι  $f_i$  είναι πρωτογενώς αναδρομικές και ισχύει κλειστότητα για σύνθεση).

**c.** Αν η σχέση  $P(i, \vec{x})$  είναι πρωτογενώς αναδρομική και

$$Q(z, \vec{x}) \iff (\exists i \leq z) P(i, \vec{x})$$

$$R(z, \vec{x}) \iff (\forall i \leq z) P(i, \vec{x})$$

τότε και οι  $Q(z, \vec{x}), R(z, \vec{x})$  είναι πρωτογενώς αναδρομικές:

$$\chi_{Q(z, \vec{x})} = sg(\sum_{i=0}^z P(i, \vec{x}))$$

$$\chi_{R(z, \vec{x})} = \prod_{i=0}^z P(i, \vec{x})$$

Το ότι το πεπερασμένο άθροισμα πρωτογενώς αναδρομικών συναρτήσεων είναι πρωτογενώς αναδρομική συνάρτηση είναι εύκολο.

Θα δείξουμε όμως ότι ισχύει για το πεπερασμένο γινόμενο:

Έστω  $f(z, y)$  πρωτογενώς αναδρομική συνάρτηση. Τότε το πεπερασμένο γινόμενο ακολουθεί το σχήμα της πρωτογενούς αναδρομής:

$$\prod_{z < 0} f(z, y) = 1$$

$$\prod_{z < n+1} f(z, y) = [\prod_{z < n} f(z, y)] * f(n, y)$$

**d.** Αν η σχέση  $P(i, \vec{x})$  είναι πρωτογενώς αναδρομική και η συνάρτηση  $f(\vec{x})$  είναι επίσης πρωτογενώς αναδρομική, τότε και οι σχέσεις:

$$Q(\vec{x}) \iff (\exists i \leq f(\vec{x}))P(i, \vec{x})$$

$$R(\vec{x}) \iff (\forall i \leq f(\vec{x}))P(i, \vec{x})$$

(από b και c)

Έπεται ότι η σχέση

$$Prime(x) \iff \text{ο } x \text{ είναι πρώτος αριθμός}$$

είναι πρωτογενώς αναδρομική:

$$\#17.Pr(x) \quad \chi_{Pr(x)} = (x > 1) \& (1 - \chi(\exists a_{1 < a < x} [a|x]))$$

Στους αλγορίθμους εκτός από την έννοια του υπολογισμού, έχουμε και αυτή της αναζήτησης. Αυτή την λειτουργία πληρεί ο τελεστής της φραγμένης ελαχιστοποίησης  $\mu$  που ορίζουμε στη συνέχεια. Ο  $\mu$  παίρνει ως είσοδο ένα φράγμα  $z$  και μια σχέση  $R(i, \vec{x})$  και επιστρέφει τον μικρότερο φυσικό  $i < z$  για τον οποίο η  $R(i, \vec{x})$  ισχύει, ή, αν δεν υπάρχει τέτοιος, επιστρέφει  $z+1$  που σημαίνει αρνητική απάντηση στην αναζήτηση.

**Ορισμός 2.10.** Ο τελεστής **φραγμένης ελαχιστοποίησης** ορίζεται ως

$$(\mu i \leq z)R(i, \vec{x}) = \begin{cases} \text{ο ελάχιστος } i \leq z \text{ ώστε } R(i, \vec{x}), & \text{αν } (\exists i \leq z)R(i, \vec{x}) \\ z+1 & \text{αλλιώς} \end{cases}$$

**Πρόταση 2.11.** Για κάθε πρωτογενώς αναδρομική σχέση  $R(i, \vec{x})$ , η συνάρτηση

$$f(z, x) = (\mu i \leq z)R(i, \vec{x})$$

είναι πρωτογενώς αναδρομική.

**Απόδειξη.** Έστω  $q(i, \vec{x})$  η χαρακτηριστική συνάρτηση της  $R(i, \vec{x})$ . Έχουμε ισοδύναμα

$$(\mu i \leq z)q(i, \vec{x}) = \begin{cases} 0 & \text{ελάχιστος } i \leq z \text{ ώστε } q(i, \vec{x}) = 1, \text{ αν } \exists i \leq z \text{ τέτοιο} \\ 0 & \text{αλλιώς} \end{cases}$$

$$(\mu i \leq 0)q(i, \vec{x}) = 0$$

$$(\mu i \leq z+1)q(i, \vec{x}) = \begin{cases} 0, & \text{αν } \nexists i \leq z+1 \text{ } q(i, \vec{x}) = 1 \\ (\mu i \leq z)q(i, \vec{x}), & \text{αν } \exists i \leq z \text{ } q(i, \vec{x}) = 1 \\ z+1, & \text{αν } q(z+1, \vec{x}) = 1 \text{ \& } \nexists i \leq z \text{ } q(i, \vec{x}) = 1 \end{cases}$$

□

Με εφαρμογή του **2.9.b** στην τελευταία πρόταση έχουμε και ότι για  $R(i, \vec{x}, g(\vec{x}))$  πρωτογενώς αναδρομικές, η συνάρτηση

$$f(z, x) = (\mu i \leq g(\vec{x}))R(i, \vec{x})$$

είναι επίσης πρωτογενώς αναδρομική.

Μέχρι στιγμής έχουμε μελετήσει της πρωτογενώς αναδρομικές συναρτήσεις, που όπως είδαμε υπολογίζονται από πρωτογενώς αναδρομικά προγράμματα.

**Λήμμα 2.12.** Οι  $S, C_q^n, P_i^n$ , η σύνθεση και ο ορισμός με περιπτώσεις είναι ολικές συναρτήσεις. Ως εκ τούτου πρωτογενώς αναδρομικές συναρτήσεις που ορίζονται μόνο με χρήση αυτών, είναι ολικές συναρτήσεις.

**Λήμμα 2.13.** Οι πρωτογενώς αναδρομικές συναρτήσεις είναι υποσύνολο των ολικών συναρτήσεων που είναι αριθμησιμο.

Είδαμε στην πρόταση 2.5 ότι κάθε πρωτογενώς αναδρομική συνάρτηση υπολογίζεται από κάποιο πρωτογενώς αναδρομικό πρόγραμμα. Θα δούμε παρακάτω (Κεφάλαιο Κωδικοποίησης) ότι υπάρχει πρωτογενώς αναδρομική κωδικοποίηση (και) κάθε τέτοιου προγράμματος στους φυσικούς. Ορίζοντας αρίθμηση για τους κωδικούς, που είναι φυσικοί αριθμοί, μπορούμε να αριθμήσουμε τα προγράμματα που υπολογίζουν πρωτογενώς αναδρομικές συναρτήσεις (κάθε συνάρτηση μπορεί να καταγράφεται πάνω από μια φορά αλλά εδώ μας ενδιαφέρει η αριθμησιμότητα. Επίσης κάθε πλειομελής συνάρτηση μπορεί να αντιστοιχίσει σε συνάρτηση μιας μεταβλητής (currying)).

Άρα έχουμε

	0	1	2	...	j	...
[f <sub>0</sub> ]	f <sub>0</sub> (0)	f <sub>0</sub> (1)	f <sub>0</sub> (2)	...	f <sub>0</sub> (j)	...
[f <sub>1</sub> ]	f <sub>1</sub> (0)	f <sub>1</sub> (1)	f <sub>1</sub> (2)	...	f <sub>1</sub> (j)	...
[f <sub>2</sub> ]	f <sub>2</sub> (0)	f <sub>2</sub> (1)	f <sub>2</sub> (2)	...	f <sub>2</sub> (j)	...
⋮						
[f <sub>i</sub> ]	f <sub>i</sub> (0)	f <sub>i</sub> (1)	f <sub>i</sub> (2)	...	f <sub>i</sub> (j)	...
⋮						

Τέλος, η κωδικοποίηση μας επιτρέπει από κάθε κωδικό  $[f_n]$  να ανακτίσουμε και τον τερματικό υπολογισμό του πρωτογενώς αναδρομικού προγράμματος που υπολογίζει την  $f$  για κάθε όρισμα (ολική). Άρα μπορούμε να ανακτίσουμε και την τιμή στο  $f_n(n)$ .

Ορίζουμε την  $d(n, m) = f_n(m) + 1 \forall n, m$ .

Η  $d(n, m)$  είναι "υπολογίσιμη", με την έννοια ότι μπορώ να υπολογίσω την τιμή κάθε  $f_n$  για κάθε όρισμα, και να προσθέσω 1.

Αλλά δεν είναι πρωτογενώς αναδρομική. Όντως, έστω ότι  $d(n, m)$  πρωτογενώς αναδρομική, άρα εμφανίζεται στην αρίθμηση και είναι  $d(n, m) = f_n(m)$  για κάποιο  $n$ .

Όμως τότε  $f_n(n) = d(n, n) = f_n(n) + 1$ , άτοπο.

Παρατηρούμε ότι η μέθοδος της διαγωνιοποίησης (Cantor 1874) είναι τόσο ισχυρή που αν περιοριστούμε στις πρωτογενώς αναδρομικές συναρτήσεις δε μπορούμε να αποφύγουμε το παραπάνω αποτέλεσμα.

Ο τρόπος να αποφύγουμε την αντίφαση  $f_n(n) = f_n(n) + 1$  είναι να επιτρέψουμε μερικές συναρτήσεις, δηλαδή συναρτήσεις που δεν είναι απαραίτητα ορισμένες σε όλο το  $\mathbb{N}$ , και δεν εμφανίζονται στην παραπάνω αρίθμηση.

**Ορισμός 2.14. Μερική συνάρτηση** από το πεδίο εισόδου  $A$  στο πεδίο τιμών  $B$

$$f : A \longrightarrow B$$

είναι η τυχαία συνάρτηση

$$f : A_0 \longrightarrow B$$

όπου  $A_0 = \text{Domain}(f) \subseteq A$ , το πεδίο σύγκλισης της  $f$ .

Ισοδύναμα είναι η τυχαία συνάρτηση

$$f : A \longrightarrow B \cup \perp$$

όπου  $\perp$  κάποιο συμβατικά επιλεγμένο αντικείμενο που δεν ανήκει στο  $B$ .

Έτσι η  $f$  παίρνει τιμές από το  $B$  στο πεδίο ορισμού της και την "τιμή"  $\perp$  στα στοιχεία του  $\mathbb{N}$  για τα οποία δεν ορίζεται:  
Λέμε ότι η  $f$  συγκλίνει στο  $\vec{x}$ ,

$$f(\vec{x}) \downarrow \iff \vec{x} \in \text{Domain}(f) \iff f(\vec{x}) \in B$$

και ότι η  $f$  αποκλίνει στο  $\vec{x}$ ,

$$f(\vec{x}) \uparrow \iff \vec{x} \notin \text{Domain}(f) \iff f(\vec{x}) = \perp$$

Προφανώς οι  $S$ ,  $C_q^m$ ,  $P_i^n$  είναι μερικές συναρτήσεις που ορίζονται σε όλο το  $\mathbb{N}$ .

Η σύνθεση και η πρωτογενής αναδρομή ερμηνεύονται για μερικές συναρτήσεις με το φυσικό τρόπο του υπολογισμού τους:

**Σύνθεση** αν  $f : A \rightarrow B, g : G^m \rightarrow D, h_i : H \rightarrow G$ :

$$f(\vec{x}) = g(h_1(\vec{x}), \dots, h_m(\vec{x})) = w$$

$$\iff \exists u_i \in G : h_i(\vec{x}) = u_i \quad \text{και} \quad g(u_1, \dots, u_m) = w \in D \cap B$$

αν συγκλίνει.

Αν για κάποιο  $i$ ,  $h_i(\vec{x}) \uparrow$ , ή  $g(h_1(\vec{x}), \dots, h_m(\vec{x})) \uparrow$ , τότε  $f(\vec{x}) = \perp$ .

**Πρωτογενής Αναδρομή**

$$\begin{cases} f(0, \vec{x}) = g(\vec{x}) \\ f(y+1, \vec{x}) = h(f(y, \vec{x}), y, \vec{x}) \end{cases}$$

αν  $g, h$  μερικές συναρτήσεις στο  $\mathbb{N}$  τότε για  $y, \vec{x}, w \in \mathbb{N}$ :

$$f(y, \vec{x}) = w$$

$$\iff (\exists w_0, \dots, w_y \in \mathbb{N}) [w_0 = g(\vec{x})$$

$$\& (\forall i, 0 \leq i \leq y) [w_i = h(w_{i-1}, i-1, \vec{x})] \quad \& \quad w_y = w]$$

Προφανώς αν  $g(\vec{x}) \uparrow, f(y, \vec{x}) \uparrow \forall y$ .

**Ορισμός 2.15.** Έστω  $n$ -μελής συναρτήσεις  $f, g : A \rightarrow B$ . Ορίζουμε

$$f \sqsubseteq g \iff (\forall \vec{x}) [f(\vec{x}) \downarrow \implies f(\vec{x}) = g(\vec{x})]$$

Μένει τώρα να ορίσουμε τελεστή για τη διαδικασία της αναζήτησης. Είχαμε δει στις πρωτογενώς αναδρομικές συναρτήσεις τον τελεστή της φραγμένης ελαχιστοποίησης. Ενώ και αυτός συνεχίζει να ισχύει στις μερικές συναρτήσεις, έχουμε πλέον τη δυνατότητα (αφού έχουμε ενσωματώσει στη γλώσσα μας την περίπτωση μια συνάρτηση/υπολογισμός/πρόγραμμα να αποκλίνει) για μη φραγμένη ελαχιστοποίηση.

**Ορισμός 2.16.** Η **ελαχιστοποίηση** της μερικής συνάρτησης  $g(i, \vec{x})$  είναι η μερική συνάρτηση

$$f(y, \vec{x}) = (\mu i \geq y) [g(i, \vec{x}) = 0]$$

= ο ελάχιστος  $w \geq y$ , ώστε  $g(w, \vec{x}) = 0 \& (\forall i) [y \leq i \leq w \implies g(i, \vec{x}) > 0]$



Όπως και στη φραγμένη ελαχιστοποίηση, η  $f(y, \vec{x})$  αναζητά  $i$  ώστε  $g(i, \vec{x}) = 0$ . Η  $g$  μπορεί και εδώ να είναι δείκτρια αν είναι ολική. Όπως και να έχει ο τελεστής  $\mu$  επιστρέφει ελάχιστη λύση. Η διαφορά εδώ είναι ότι δεν υπάρχει φράγμα, οπότε η αναζήτηση συνεχίζεται μέχρι να βρεθεί όρισμα που ικανοποιεί τη σχέση, ή επ' άπειρον.

Το τελευταίο σημαίνει ότι η  $f$  αποκλίνει, δηλαδή δεν είναι ορισμένη στο  $\vec{x}$ .

Αυτό μπορεί να συμβαίνει είτε αν η  $g(i, \vec{x})$  δεν μηδενίζεται ποτέ, είτε αν η  $g(i, \vec{x})$  αποκλίνει σε κάποια είσοδο πριν βρεθεί  $i : g(i, \vec{x}) = 0$ .

Έχουμε πλέον ο,τι χρειάζεται για να ορίσουμε την επόμενη ευρύτερη κλάση υπολογίσιμων συναρτήσεων (στις οποίες ανήκει λχ. η  $d(n)$  παραπάνω).

**Ορισμός 2.17.** Η τυχαία μερική συνάρτηση  $f : \mathbb{N}^n \rightarrow \mathbb{N}$  είναι **ελαχιστικά αναδρομική** (ή  $\mu$ -αναδρομική) στο σύνολο μερικών συναρτήσεων  $A$ , αν η  $f$  ανήκει σε κάθε σύνολο που περιέχει το  $A$  και είναι πρωτογενώς κλειστό και κλειστό για ελαχιστοποίηση.

Συμβολίζουμε

$$R_\mu(A) = \{f \mid \eta \ f \ \text{είναι } \mu\text{-αναδρομική στο } A\}$$

Ισχύει κι εδώ αντίστοιχα, ότι μια σχέση  $P(\vec{x})$  είναι ελαχιστικά αναδρομική αν η χαρακτηριστική της συνάρτηση είναι ελαχιστικά αναδρομική.

Και, όπως προκύπτει από τον ορισμό:

$$\begin{aligned} R_\mu &= R_\mu(\emptyset) \\ R_p(A) &\subseteq R_\mu(A) \end{aligned}$$

Θα προχωρήσουμε δείχνοντας την κλειστότητα του  $R_\mu$  για τον τελεστή της διακλάδωσης, για ορισμούς με περιπτώσεις. Πλέον όμως πρέπει να ενσωματώσουμε και την περίπτωση απόκλισης, καθώς και να εξετάσουμε τη συνθήκη σύγκλισης.

**Ορισμός 2.18.** Η **διακλάδωση** τριών, δοσμένων μερικών συναρτήσεων  $c(\vec{x}), g(\vec{x}), h(\vec{x})$  είναι η μερική συνάρτηση

$$\begin{aligned} f(\vec{x}) &= \text{αν } (c(\vec{x}) = 0) \quad \text{τότε } g(\vec{x}) \text{ αλλιώς } h(\vec{x}) \\ &= \begin{cases} g(\vec{x}), & \text{αν } c(\vec{x}) = 0, \\ h(\vec{x}), & \text{αν } c(\vec{x}) \downarrow \ \& c(\vec{x}) \neq 0 \\ \perp, & \text{αν } c(\vec{x}) \uparrow \end{cases} \end{aligned}$$

**Πρόταση 2.19.** Η ελαχιστοποίηση

$$f(y, \vec{x}) = (\mu i \geq y)[g(i, \vec{x}) = 0]$$

τυχαίας μερικής συνάρτησης  $g$  είναι η  $\sqsubseteq$ -ελάχιστη λύση της αναδρομικής εξίσωσης

$$(10) \quad p(y, \vec{x}) = \text{αν } (g(y, \vec{x}) = 0) \text{ τότε } y, \text{ αλλιώς } p(y+1, \vec{x})$$

δηλαδή:

a) η σχέση (10) ισχύει για όλα τα  $y, \vec{x}$  αν θέσουμε  $p := f$ .

b) αν η σχέση (10) ισχύει για όλα τα  $y, \vec{x}$  για κάποια  $p$ , τότε  $f \sqsubseteq p$ .

**Απόδειξη.** (a) Θα δείξουμε ότι για όλα τα  $y, \vec{x}$ ,

$$f(y, \vec{x}) = \text{αν } (g(y, \vec{x}) = 0) \text{ τότε } y, \text{ αλλιώς } f(y+1, \vec{x})$$

Διακρίνουμε τις εξής περιπτώσεις για την  $f$ :

1.  $f(y, \vec{x}) \downarrow$

δηλαδή για κάποιο  $y$   $g(y, \vec{x}) = 0$ .

Τότε  $f(y, \vec{x}) = y$ , για αυτό το πρώτο  $y$  που μηδενίζει την  $g$ . Όμως και  $p(y, \vec{x}) = y$  για το ίδιο  $y$ .

Άρα  $p = f$ .

2.  $f(y, \vec{x}) \uparrow$

Η  $f$  αποκλίνει αν η  $g(y, \vec{x}) \uparrow$  ή αν  $g(y, \vec{x}) > 0$  για όλα τα  $y$ .

Αν  $g(y, \vec{x}) \uparrow$ , τότε και  $p(y, \vec{x}) \uparrow$ .

Άρα  $p = f$ .

Αν  $g(y, \vec{x}) > 0$  για όλα τα  $y$ , τότε  $p(y, \vec{x}) = \perp = p(y+1, \vec{x}) \forall y$ .

Άρα και πάλι  $p = f$ .

(b) Θα δείξουμε ότι  $\forall \vec{x}$ , για όλα τα  $y$  και  $w \geq y$ ,

$$f(y, \vec{x}) = w \implies p(y, \vec{x}) = w$$

με επαγωγή στη διαφορά  $w - y$ .

**Επαγωγική Βάση:**  $w - y = 0 \implies w = y$ .

$$f(y, \vec{x}) = w = y \implies g(y, \vec{x}) = 0 \implies p(y, \vec{x}) = y = w$$

**Επαγωγικό Βήμα:** έστω  $w > y$  και  $g(y, \vec{x}) > 0$ ,

αν  $f(y, \vec{x}) = w$  τότε:

$$w = f(y, \vec{x})$$

$$= f(y+1, \vec{x}) \quad (\forall i \geq y \quad f(i, \vec{x}) = f(y, \vec{x}) \text{ (από ορισμό f)})$$

$$= p(y+1, \vec{x}) \quad (w - (y+1) = (w-y) - 1 \text{ (άρα ισχύει επαγωγική υπόθεση)})$$

$$= p(y, \vec{x}) \quad (\text{ορισμός } p \text{ για } g(y, \vec{x}) > 0)$$

□

### 2.3 Γενική Αναδρομή

Χαρακτηριστικό παράδειγμα μερικής άλγεβρας είναι η βασική δομή της αριθμητικής

$$\mathbb{N}_0 = (\mathbb{N}, 0, 1, S, Pd)$$

όπου  $S$  και  $Pd$  είναι οι συναρτήσεις του επόμενου και του προηγούμενου στους φυσικούς αριθμούς, και όπου έχουμε προβάλλει τις αληθοτιμές  $0, 1$ .

**Ορισμός 2.20. Μερική άλγεβρα** είναι η τυχαία δομή

$$\mathbf{M} = (M, 0, 1, f_1, \dots, f_n),$$

όπου το  $M$  είναι σύνολο,  $0, 1 \in M$  και  $0 \neq 1$  και για  $i = 1, \dots, K$ , η

$$f_i : M^n \rightarrow M$$

είναι μερική συνάρτηση πλειομέλειας  $n_i$ . Για  $n_i = 0$ , η  $f_i$  είναι σταθερά, κάποιο μέλος του  $M$  ή ο πάτος  $\perp$ .

**Ορισμός 2.21. Τυπική γλώσσα  $R(\mathbf{M})$ .**

#### **A. Σύνταξη**

Σε κάθε μερική άλγεβρα  $\mathbf{M}$  αντιστοιχούμε την τυπική της γλώσσα  $R = R(\mathbf{M})$ , της οποίας το αλφάβητο αποτελείται από τα εξής **σύμβολα**:

τις ατομικές μεταβλητές:	$v_0, v_1, \dots,$
τις ατομικές σταθερές:	$x (x \in M)$
τις συναρτησιακές σταθερές:	$f_1, \dots, f_K$
τα σύμβολα για τη διακλάδωση:	αν τότε αλλιώς
τα σημεία στίξεως:	, ( )
το σύμβολο της ισότητας:	=

Απ'αυτά τα σύμβολα ξεχωρίζουμε το **λεξιλόγιο**

$$(f_1, \dots, f_K) \quad (arity(f_i) = n_i)$$

που παρέχει συμβολισμό για τις δοσμένες μερικές συναρτήσεις της  $\mathbf{M}$ , ενώ τα υπόλοιπα σύμβολα είναι κοινά για όλες τις μερικές άλγεβρες στο σύνολο  $M$ .

**Λέξεις** στο σύνολο είναι οι πεπερασμένες ακολουθίες από στοιχεία του  $M$ . Η παράθεση δύο λέξεων είναι η παράθεση των συμβόλων τους. Ισότητα  $\equiv$  λέξεων είναι η ταύτιση τους στοιχείο προς στοιχείο.

Συμβολίζουμε με  $\Lambda$  την **κενή λέξη** και ισχύει:

$$\Lambda \alpha \equiv \alpha \Lambda \equiv \alpha$$

**Όροι** της  $R$  είναι το ελάχιστο σύνολο λέξεων που ορίζεται αναδρομικά ως εξής:

(A1) Κάθε  $x \in M$  (και ιδιαίτερα τα 0 και 1) και κάθε ατομική μεταβλητή  $v_i$  είναι όροι.

(A2) Αν οι λέξεις  $A_1, \dots, A_{n_i}$  είναι όροι, τότε όρος είναι και η λέξη

$$f_i(A_1, \dots, A_{n_i})$$

(A3) Αν οι λέξεις  $A_1, A_2, A_3$  είναι όροι, τότε όρος είναι και η λέξη

$$(\text{αν } (A_1 = 0) \text{ τότε } A_2 \text{ αλλιώς } A_3)$$

Ο όρος  $A$  είναι **κλειστός** αν δεν εμφανίζεται σ' αυτόν καμία ατομική μεταβλητή  $v_i$  και **αγνός** αν οι μόνες ατομικές σταθερές που μπορεί να εμφανίζονται στον  $A$  είναι το 0 ή το 1.

### **Λήμμα 2.22. Μοναδική αναγνωσιμότητα όρων**

a) Σε κάθε όρο  $A$ , το πλήθος των αριστερών παρενθέσεων '(' είναι ίσο με το πλήθος των δεξιών παρενθέσεων ')'.  
b) Κανένα γνήσιο αρχικό τμήμα όρου δεν είναι όρος.

[ $\alpha, \beta, \gamma$  λέξεις,  $\beta \neq \Lambda$ ,  $\gamma \neq \Lambda$ :  $\alpha$  γνήσιο αρχικό τμήμα της  $\beta$  αν  $\beta \equiv \alpha\gamma$ ]

c) Αν η λέξη  $A \equiv \alpha_1 \dots \alpha_n$  είναι όρος, τότε πληρεί ακριβώς μια από τις περιπτώσεις  $A_1, A_2, A_3$  του ορισμού του συνόλου των Όρων.

*Απόδειξη.* a) Κάθε όρος  $A$  είναι:

είτε σταθερά -καμία δεξιά ή αριστερή παρένθεση,

είτε μεταβλητή -καμία δεξιά ή αριστερή παρένθεση,

είτε της μορφής  $f_i(A_1, \dots, A_{n_i})$  -ίσος αριθμός αριστερών δεξιών παρενθέσεων,

είτε της μορφής (αν  $(A_1 = 0)$  τότε  $A_2$  αλλιώς  $A_3$ ) -ίσος αριθμός αριστερών δεξιών παρενθέσεων,

είτε συνδιασμός των παραπάνω. Άρα επαγωγικά έχει ίσο αριθμό αριστερών δεξιών παρενθέσεων,

b) Αν  $A$  σταθερά ή μεταβλητή, το αρχικό του τμήμα είναι η  $\Lambda$  που δεν είναι όρος. Αν  $A$  προκύπτει από  $A_2$  ή  $A_3$  το αρχικό του τμήμα δεν έχει ίσο αριθμό παρενθέσεων, αφού  $\gamma \neq \Lambda$ , άρα από a) δεν είναι όρος.

c) Επειδή το σύνολο Όροι είναι το ελάχιστο που ορίζεται αναδρομικά από  $A_1, A_2, A_3$  αν μια λέξη είναι όρος θα πληρεί τουλάχιστον μια από τις περιπτώσεις. Προφανώς μια σταθερά δεν μπορεί να είναι μεταβλητή. Αν  $A = \alpha_1 \dots \alpha_n$  προκύπτει από  $A_2$  τότε  $\alpha_1 = f_i$  για κάποια συναρτησιακή σταθερά, άρα δε μπορεί να γραφεί και ως σταθερά, μεταβλητή ή στη μορφή  $A_3$ . Ομοίως για  $A_3$ .  $\square$

Από τις λέξεις από το αλφάβητο της  $R(\mathbf{M})$  διακρίνουμε ως συντακτικά ορθές εκφράσεις τους όρους και τις εξισώσεις όρων, δηλαδή λέξεις της μορφής  $A = B$ , όπου  $A$  και  $B$  όροι.

## B. Δηλωτική σημασιολογία.

Η τιμή  $\text{val}_M(A)$   $\mathbf{M}$  :

(B1)  $\text{val}_M(x) = x, x \in M$ .

(B2) Αν  $\text{val}_M(A_j = w_j) j = 1, \dots, n_i, \text{val}_M(f_i(A_1, \dots, A_{n_i})) = f_i(w_1, \dots, w_{n_i})$

(B3) Αν  $\text{val}_M(A) = a, \text{val}_M(B) = b, \text{val}_M(C) = c, \text{val}_M((=)C) = (=)bc$ .

όπου στο B2 η  $f_i$  είναι η μερική συνάρτηση της  $\mathbf{M}$  που εκπροσωπεί η συναρτησιακή σταθερά  $f_i$   $f_i(w_1, \dots, w_{n_i})$  τότε  $\text{val}_M(f_i(A_1, \dots, A_{n_i})) = \perp$ .

Στην περίπτωση των ατομικών μεταβλητών η τιμή  $\text{val}_M(v_i)$ .

Εξετάζουμε όμως την περίπτωση αντικατάστασης μεταβλητής από όρο:

Αν οι ατομικές μεταβλητές που εμφανίζονται στον όρο  $A$  είναι στη λίστα  $v_1, \dots, v_n$  και  $w_1, \dots, w_n$  είναι κλειστοί όροι και έχουμε

$$\text{val}_M(B_1) = w_1 \in M, \dots, \text{val}_M(B_n) = w_n \in M$$

τότε

$$\text{val}_M(A\{v_1 \equiv B_1, \dots, v_n \equiv B_n\}) = \text{val}_M(A\{v_1 \equiv w_1, \dots, \text{text } v_n \equiv w_n\})$$

**Ορισμός 2.23. Αποτίμηση** στο  $M$  είναι η τυχαία συνάρτηση

$$\pi : \{v_0, v_1, \dots\} \longrightarrow M$$

που αναθέτει σε κάθε ατομική μεταβλητή μια τιμή  $\pi(v_i)$  στο  $M$ .

Αν οι ατομικές μεταβλητές που εμφανίζονται στον όρο  $A$  είναι στη λίστα  $v_1, \dots, v_n$ ,

$$\text{val}_M(A, \pi) = \text{val}_M(A\{v_0 \equiv \pi(v_0), \dots, v_n \equiv \pi(v_n)\})$$

**Ορισμός 2.24. Προγραμματιστική γλώσσα  $R(\mathbf{M})$ .**

### A. Σύνταξη

Εισάγουμε στους όρους της  $R$  τις **συναρτησιακές μεταβλητές**

$$\zeta_0^n, \zeta_1^n, \dots \quad (\text{arity}(\zeta_i^n) = n, \quad n = 0, 1, \dots).$$

Το λεξιλόγιο της  $R$  πλέον είναι το σύνολο  $(f_1, \dots, f_K, \zeta_0^n, \zeta_1^n, \dots)$ .

**Τυπική αναδρομική εξίσωση** είναι η τυχαία εξίσωση όρων

$$\zeta(v_0, \dots, v_n) = A$$

όπου  $\zeta$  συναρτησιακή μεταβλητή,  $v_0, \dots, v_n$  διαφορετικές ατομικές μεταβλητές.

Ο όρος  $A$  πρέπει να είναι αγνός στον οποίο όσες ατομικές μεταβλητές εμφανίζονται ανήκουν στη λίστα  $v_0, \dots, v_n$ , ώστε η εξίσωση να είναι αναδρομική καλά ορισμένη.

Αν καμία συναρτησιακή μεταβλητή  $\zeta$  δεν εμφανίζεται στον όρο  $A$  η εξίσωση καλείται **ρητή**.

**Αναδρομικό πρόγραμμα** της μερικής άλγεβρα  $\mathbf{M}$  είναι το τυχαίο σύστημα αναδρομικών εξισώσεων

$$\zeta_0(\vec{V}_0) = E_0$$

⋮

$$\zeta_k(\vec{V}_k) = E_k$$

όπου  $\zeta_0, \dots, \zeta_k$  διαφορετικές συναρτησιακές μεταβλητές και οι μόνες που εμφανίζονται στους όρους  $E_0, \dots, E_k$ .

Έτσι ξεκαθαρίζει και ο ορισμός/χρήση των συναρτησιακών μεταβλητών. Η κάθε  $\zeta_i$  ορίζεται και υπολογίζεται μέσα στο πρόγραμμα μέσω των όρων (ακόμα και άλλων συναρτήσεων  $\zeta$ ) της εξίσωσής της, που με τη σειρά τους υπολογίζονται από το σύνολο των εξισώσεων του συστήματος.

Οι εξισώσεις του  $E$  καλούνται **ορισμοί** των συναρτησιακών μεταβλητών  $\zeta_0, \dots, \zeta_k$ .

Έτσι, ενώ οι συναρτησιακές μεταβλητές από συντακτική απόψη μοιάζουν με τις συναρτησιακές σταθερές  $f_1, \dots, f_K$  που ονομάζουν τις (δεδομένες) μερικές συναρτήσεις της  $\mathbf{M}$ , οι συναρτησιακές μεταβλητές δεν αντιστοιχούν σε δεδομένες μερικές συναρτήσεις, αλλά αντιστοιχούν σε μερικές συναρτήσεις που εξαρτώνται από το εκάστοτε πρόγραμμα  $E$ .

Κάθε πρόγραμμα  $E$  αντιστοιχίζει και υπολογίζει κάθε μια από τις συναρτήσεις  $\zeta_i$  που εμφανίζεται σε αυτό, σε μια μερική συνάρτηση

$$\bar{\zeta}_i : M^{k_i} \rightarrow M \quad (k_i = \text{arity}(\zeta_i))$$

ώστε οι  $\bar{\zeta}_0, \dots, \bar{\zeta}_k$  να ικανοποιούν το  $E$  στη  $\mathbf{M}$ .

Τα σύνολα μερικών συναρτήσεων που ικανοποιούν το  $E$  μπορεί να είναι πολλά. Όπως θα δούμε στη συνέχεια όμως, υπάρχει, για κάθε πρόγραμμα που έχει λύση, ελάχιστη λύση και αυτή θα αντιστοιχίσει η υπολογιστική σημασιολογία της  $R(\mathbf{M})$  στο  $E$ .

Η υπολογιστική σημασιολογία της  $R(\mathbf{M})$  πατώντας στην προγραμματιστική γλώσσα όπως την ορίσαμε και ένα σύνολο κανόνων υπολογισμού, μας δίνει μια μηχανή (**αναδρομική μηχανή**) η οποία πραγματοποιεί την αντιστοιχία

$$(E, \zeta) \longrightarrow \bar{\zeta}$$

Δίνουμε αρχικά τους ακόλουθους δυο ορισμούς, που θέτουν το πλαίσιο λειτουργίας αυτής της μηχανής.

**Ορισμός 2.25. Σύστημα μεταβάσεων** είναι η τυχαία τριάδα

$$\mathcal{T} = (S, \rightarrow, T)$$

όπου

i) το  $S$  είναι μη-κενό σύνολο, οι καταστάσεις του  $\mathcal{T}$

ii) το  $\rightarrow$  είναι μια διμελής σχέση μετάβασης στο  $S$ .

iii) το  $T \subseteq S$  είναι το σύνολο των *τερματικών* καταστάσεων και για κάθε τερματική κατάσταση

$$s \in T \implies (\forall s') [s \not\rightarrow s']$$

Μια κατάσταση  $s$  που ικανοποιεί την τελευταία σχέση αλλά δεν είναι τερματική καλείται *άγονη*.

Το  $\mathcal{T}$  είναι **αιτιοκρατικό** αν κάθε κατάσταση  $s$  έχει το πολύ μια επόμενη. Για παράδειγμα

$$m \rightarrow_1 n \Leftrightarrow m > n \quad , \quad m \rightarrow_2 n \Leftrightarrow m = n + 1$$

το σύστημα  $(\mathbb{N}, \rightarrow_1, 0)$  δεν είναι αιτιοκρατικό, ενώ το  $(\mathbb{N}, \rightarrow_2, 0)$  είναι.

**Ορισμός 2.26. Μερικός υπολογισμός** του συστήματος μεταβάσεων  $\mathcal{T}$  είναι κάθε πεπερασμένο μονοπάτι

$$Y = (s_0 \rightarrow s_1 \rightarrow \dots \rightarrow s_n)$$

στο γράφημα  $(S, \rightarrow)$ . Ο  $Y$  είναι *τερματικός* αν η τελευταία κατάσταση  $s_n$  είναι τερματική, και *άγονος* αν η  $s_n$  είναι *άγονη*.

*Άπειρος* υπολογισμός είναι κάθε άπειρο μονοπάτι

$$Y = (s_0 \rightarrow s_1 \rightarrow \dots).$$

Προφανώς ένας άπειρος υπολογισμός είναι *αποκλίνων*.

*Αποκλίνων* είναι και ένας υπολογισμός με *άγονη* τερματική κατάσταση (άγονος).

Το *μήκος* πεπερασμένου υπολογισμού είναι το πλήθος το καταστάσεων στο μονοπάτι  $(n+1)$ .

Το σύστημα μετάβασης  $\mathcal{T}$  υπολογίζει τη μερική συνάρτηση  $\pi : S \rightarrow T$  αν, για όλα τα  $s \in S, t \in T$

$$\pi(s) = t \Leftrightarrow (\exists (s_0, \dots, s_n) \in C(\mathcal{T})) [s_0 = s \& s_n = t]$$

όπου

$C(\mathcal{T}) =$  το σύνολο των τερματικών υπολογισμών του  $\mathcal{T}$

Κάθε αιτιοκρατικό σύστημα μεταβάσεων  $\mathcal{T}$  υπολογίζει ακριβώς μια τέτοια συνάρτηση  $\pi : S \rightarrow T$ , και για κάθε κατάσταση  $s$  υπάρχει ακριβώς ένας τερματικός (αν  $\pi(s) \downarrow$ ), άγονος ή άπειρος (αν  $\pi(s) \uparrow$ ) υπολογισμός.

Παρατηρούμε ότι για  $\mathcal{T}$  αιτιοκρατικό κάθε υπολογισμός μπορεί να οριστεί με το αναδρομικό σχήμα:

$$s_0 = s$$

$$s_{n+1} = \begin{cases} \text{η μοναδική } s' \text{ τέτοια ώστε } s_n \rightarrow s', & \text{αν υπάρχει} \\ \perp, & \text{αλλιώς} \end{cases}$$

Θα δούμε στη συνέχεια πώς μπορούμε να υπολογίσουμε μια αναδρομική μερική συνάρτηση  $f : A \rightarrow B$  μέσω του αναδρομικού σχήματος του υπολογισμού ενός συστήματος μεταβάσεων.

Κατ'αρχάς για να υπολογίσουμε μια μερική συνάρτηση  $f : A \rightarrow B$  με κάποιο σύστημα μεταβάσεων  $\mathcal{T}$ , πρέπει να έχουμε κάποιον τρόπο εισαγωγής στοιχείων από το  $A$  στο  $\mathcal{T}$  και κάποιον τρόπο εξαγωγής τιμών από το  $\mathcal{T}$  στο  $B$ .

**Ορισμός 2.27. Αφηρημένη Μηχανή** με πεδίο εισόδου  $A$  και πεδίο εξόδου  $B$  είναι η τυχαία πεντάδα

$$\mathcal{M} = \mathcal{T}(input, output) = (S, \rightarrow, T, input, output)$$

όπου  $\mathcal{T} = (S, \rightarrow, T)$  ένα σύστημα μεταβάσεων, και

input:  $A \rightarrow S$  μια συνάρτηση εισόδου

output:  $T \rightarrow B$  μια συνάρτηση εξόδου.

Η  $\mathcal{T}(input, output)$  υπολογίζει τη μερική συνάρτηση  $f : A \rightarrow B$  αν για όλα τα  $x \in A$  και  $w \in B$

$$f(x) = w \Leftrightarrow (\exists (s_0, \dots, s_n) \in C(S, \rightarrow, T)) [s_0 = input(x) \& output(s_n) = w]$$

Προφανώς για να είναι η  $f$  καλά ορισμένη (σε κάθε input αντιστοιχεί ένα output) το  $\mathcal{T}$  πρέπει να είναι αιτιοκρατικό.

Έχουμε πλέον ο,τι χρειαζόμαστε για να ορίσουμε την **αναδρομική μηχανή** που θα πραγματοποιεί την αντιστοιχία  $(E, \zeta) \rightarrow \bar{\zeta}$ .



(pass)	$\alpha x : \beta \rightarrow \alpha : x \beta (x \in M)$
(e-call) (e-cal) για την $\mathbf{N}_0$	$\alpha f_i : \vec{x} \beta \rightarrow \alpha : f_i(\vec{x}) \beta$ $\alpha S : x \beta \rightarrow \alpha : x + 1 \beta$ $\alpha Pd : x \beta \rightarrow \alpha : x - 1 \beta$
(i-call)	$\alpha \zeta_i : \vec{x} \beta \rightarrow \alpha E_i \{ \vec{v}_i \} ::= \vec{x} : \beta$
(comp) (br) (br0) (br1)	$\alpha h(A_1, \dots, A_n) : \beta \rightarrow \alpha h \ A_1 \dots \ A_n : \beta$ $\alpha \text{αν}(A = 0) \text{τότε Βαλλιώς } C : \beta \rightarrow \alpha B \ C \ ? \ A : \beta$ $\alpha B \ C \ ? : 0 \beta \rightarrow \alpha B \ : \beta$ $\alpha B \ C \ ? : y \beta \rightarrow \alpha C : \beta \quad (y \neq 0)$

Πίνακας 1: Πίνακας Μεταβάσεων

**Ορισμός 2.28. Αναδρομικές μηχανές.** Για κάθε πρόγραμμα  $E$  της  $R(\mathbf{M})$  ορίζουμε ένα σύστημα μεταβάσεων  $\mathcal{T}(E) = \mathcal{T}(E, \mathbf{M})$  ως εξής:

i) Οι καταστάσεις του  $\mathcal{T}(E)$  είναι όλες οι λέξεις  $s$  της μόρφης

$$\alpha_0 \dots \alpha_{m-1} : \beta_0 \dots \beta_{n-1}$$

όπου

- κάθε  $\alpha_i$  είναι συναρτησιακό σύμβολο ή κλειστός όρος ή το σύμβολο ?
- κάθε  $\beta_j$  είναι ατομική σταθερά
- οι υπογεγραμμένες λέξεις είναι αυτές που αλλάζουν σε κάθε μετάβαση
- $\vec{x} = x_1, \dots, x_n$  είναι  $n$ -άδα ατομικών σταθερών
- στην εξωτερική κλίση (e-call)  $f = f_i$  είναι μερική συνάρτηση της  $\mathbf{M}$  με  $arity(f_i) = n_i = n$
- στην εσωτερική κλίση (i-call) η  $\zeta_i$  είναι  $n$ -μελής συναρτησιακή μεταβλητή του προγράμματος  $E$  που ορίζεται από την εξίσωση  $\zeta_i(\vec{x}) = E_i$
- στη μετάβαση σύνθεσης (comp) η  $h$  είναι συναρτησιακό σύμβολο με  $arity(h) = n$

ii) Η σχέση μετάβασης του  $\mathcal{T}(E)$  ορίζεται στις περιπτώσεις του Πίνακα Μεταβάσεων .

iii) Οι τερματικές καταστάσεις του  $\mathcal{T}(E)$  είναι οι λέξεις της μορφής

$$: w$$

Το σύστημα  $\mathcal{T}(E)$  είναι προφανώς αιτιοκρατικό -κάθε κατάσταση  $s$  στον πίνακα έχει μια  $s'$  ώστε  $s \rightarrow s'$  και αυτές είναι οι μόνες περιπτώσεις που ορίζεται η σχέση μετάβασης.

Όλες οι μηχανές που στηρίζονται στο  $\mathcal{T}(E)$  έχουν συνάρτηση εξόδου την

$$\text{output}( : w) = w$$

που παίρνει σαν ορίσματα καταστάσεις της μορφής  $: w$  (τερματικές) και επιστρέφει  $w$ .

Για κάθε  $n$ -μελή συναρτησιακή μεταβλητή του  $E$ , η **αναδρομική μηχανή**  $\mathcal{T}(E, \zeta)$  παράγεται από το σύστημα μεταβάσεων  $\mathcal{T}(E)$  με την προσθήκη της κοινής συνάρτησης εξόδου  $\text{output}()$  και την προσθήκης της συνάρτησης εισόδου για της εκάστοτε  $\zeta$  :

$$\text{input}(\vec{x}) \equiv \zeta : \vec{x}$$

και υπολογίζει την μερική συνάρτηση  $\bar{\zeta} = \bar{\zeta}_E : M^n \rightarrow M$ .

Παρατηρούμε ότι η  $\bar{\zeta}$  εξαρτάται τόσο από το πρόγραμμα  $E$  όσο και από την μερική άλγεβρα  $\mathbf{M}$ .

Επίσης όπως προκύπτει από την Αναδρομική Μηχανή, κάθε πρόγραμμα  $E$  υπολογίζει τη συνάρτηση του  $\text{input}$ , δηλαδή την συναρτησιακή μεταβλητή που ορίζεται "πρώτη"  $\zeta_0$ .

### **Ορισμός 2.29. M-αναδρομικό.**

Η τυχαία  $n$ -μελής συνάρτηση  $f : M^n \rightarrow M$  είναι **M-αναδρομική** αν και μόνο αν υπολογίζεται από κάποιο αναδρομικό πρόγραμμα της  $\mathbf{M}$ . Δηλαδή έχουμε  $f = \bar{\zeta}_E$  για πρόγραμμα  $E$  της  $\mathbf{M}$ .

Η τυχαία σχέση  $P(\vec{x})$  στο  $M$  είναι **M-αναδρομική** αν η χαρακτηριστική της συνάρτηση είναι **M-αναδρομική**.

Το τυχαίο σύνολο  $A \subseteq M$  είναι **M-αναδρομικό** αν η χαρακτηριστική του συνάρτηση είναι **M-αναδρομική**.

Θέτουμε

$$\mathcal{R}(\mathbf{M}) = \{f : M^n \rightarrow M \mid f \text{ είναι } \mathbf{M}\text{-αναδρομική}\}$$

Συγκεκριμένα για την άλγεβρά  $\mathbf{N}_0$  και τις επεκτάσεις της

$$\mathcal{R} = \mathcal{R}(\mathbf{N}, 0, 1, S, Pd) = \{f : \mathbb{N}^n \rightarrow \mathbb{N} \mid f \text{ είναι } \mathbf{N}_0\text{-αναδρομική}\}$$

Για σύνολο  $\Psi$  πλειομελών μερικών συναρτήσεων στο  $\mathbb{N}$

$$\mathcal{R}(\Psi) = \{f : \mathbb{N}^n \rightarrow \mathbb{N} \mid f(\mathbf{N}_0, f_1, \dots, f_K) \text{ -- αναδρομική για } f_1, \dots, f_K \in \Psi\}$$

Στη συνέχεια θα δείξουμε ότι οι λύσεις που υπολογίζονται από την  $R(\mathbf{M})$  ικανοποιούν όντως το εκάστοτε πρόγραμμα  $E$ .

**Λήμμα 2.30.** Για κάθε μερικό υπολογισμό

$$\alpha_0 : \beta_0 \rightarrow \alpha_1 : \beta_1 \rightarrow \dots \rightarrow \alpha_m : \beta_m$$

στο σύστημα  $\mathcal{T}(E, \mathbf{M})$  και λέξεις  $\alpha^*, \beta^*$  τέτοιες ώστε

$$\alpha * \alpha_0 : \beta_0 \beta^*$$

να είναι κατάσταση, ο

$$\alpha * \alpha_0 : \beta_0 \beta^* \rightarrow \alpha * \alpha_1 : \beta_1 \beta^* \rightarrow \dots \rightarrow \alpha * \alpha_m : \beta_m \beta^*$$

είναι επίσης μερικός υπολογισμός του  $\mathcal{T}(E, \mathbf{M})$ .

*Απόδειξη.* Με επαγωγή στο  $m \geq 0$ . Η επαγωγική βάση για  $m = 0$  είναι τετριμμένη από την υπόθεση. Έστω ότι

$$\alpha * \alpha_0 : \beta_0 \beta^* \rightarrow \alpha * \alpha_1 : \beta_1 \beta^* \rightarrow \dots \rightarrow \alpha * \alpha_m : \beta_m \beta^*$$

μερικός υπολογισμός. Παρατηρούμε ότι οποιαδήποτε περίπτωση του Πίνακα Μεταβάσεων δικαιολογεί τη μετάβαση

$$\alpha_m : \beta_m \rightarrow \alpha_{m+1} : \beta_{m+1}$$

δικαιολογεί και την μετάβαση

$$\alpha * \alpha_m : \beta_m \beta^* \rightarrow \alpha * \alpha_{m+1} : \beta_{m+1} \beta^*$$

Έπεται ότι αν ο

$$\alpha_0 : \beta_0 \rightarrow \alpha_1 : \beta_1 \rightarrow \dots$$

είναι αποκλείων υπολογισμός, θα είναι και ο

$$\alpha * \alpha_0 : \beta_0 \beta^* \rightarrow \alpha * \alpha_1 : \beta_1 \beta^* \rightarrow \dots$$

□

**Θεώρημα 2.31. Υπολογιστική Εγκυρότητα της  $R(\mathbf{M})$**

Για τυχαίο αναδρομικό πρόγραμμα  $E$  στην  $\mathbf{M} = (M, 0, 1, f_1, \dots, f_K)$  με συναρτησιακές μεταβλητές  $\zeta_0, \dots, \zeta_k$ , θέτουμε

$$\bar{\mathbf{M}} = (\mathbf{M}, \bar{\zeta}_0, \dots, \bar{\zeta}_k) = (M, 0, 1, f_1, \dots, f_K, \zeta_0, \dots, \zeta_k)$$

Οι μερικές συναρτήσεις  $\bar{\zeta}_0, \dots, \bar{\zeta}_k$  ικανοποιούν το σύστημα  $E$  στη μερική άλγεβρα  $\mathbf{M}$ .

**Απόδειξη.** Κατ'αρχάς θα δείξουμε ότι για δοσμένο, κλειστό όρο  $A$  αν  $\mathbf{val}(A) \uparrow$  τότε ο υπολογισμός  $\text{comp}_{\mathcal{T}}(A :)$  του  $\mathcal{T}(E, \mathbf{M})$  με αρχική κατάσταση  $A :$  είναι άπειρος ή άγονος, ενώ αν  $\mathbf{val}(A) = w$  τότε ο υπολογισμός  $\text{comp}_{\mathcal{T}}(A :)$  του  $\mathcal{T}(E, \mathbf{M})$  με αρχική κατάσταση  $A :$  συγκλίνει με τερματική κατάσταση  $: w$ .

Όντως με επαγωγή στις περιπτώσεις για τον όρο  $A$  έχουμε:

(1)  $A \equiv x \in M$ , τότε  $\mathbf{val}(A) = x$  και  $\text{comp}_{\mathcal{T}}(A :)$  :

$x$ : (pass)

$:x$

(2)  $A \equiv f_i(A_1, \dots, A_{n_i})$  για κάποια δοσμένη μερική συνάρτηση  $f_i$  της  $\mathbf{M}$ , τότε ο  $\text{comp}_{\mathcal{T}}(A :)$  αρχίζει με τη μετάβαση

$f_i(A_1, \dots, A_{n_i}) :$  (comp)  $f_i \quad A_1, \dots, A_{n_i}$

Θεωρούμε τρεις περιπτώσεις

(2α) Για κάποιο  $j$ ,  $\mathbf{val}(A_j) \uparrow$ , οπότε και  $\mathbf{val}(A) \uparrow$ . Αν το  $j$  είναι το μέγιστο  $\leq n_i$  με αυτή την ιδιότητα τότε με επίκληση της επαγωγικής υπόθεσης ο υπολογισμός  $\text{comp}(A :)$  αρχίζει

$f_i(A_1, \dots, A_{n_i}) :$  (comp)

$f_i \quad A_1, \dots, A_{n_i} :$  (επαγ. υπ.)

$\vdots$

$f_i \quad A_1, \dots, A_{n_i-1} : w_{n_i}$

$\vdots$

$f_i \quad A_1, \dots, A_j : w_{j+1} \dots w_{n_i}$

Όμως αφού  $\mathbf{val}(A_j) \uparrow$  από το Λήμμα 2.30 ο  $\text{comp}(A_j :)$  επίσης αποκλίνει, άρα και ο  $\text{comp}(A :)$ .

(2β) Υπάρχουν  $w_1, \dots, w_j \in M$  τέτοια ώστε  $\mathbf{val}(A_j) = w_j$  για  $j = 1, \dots, n_i$ , αλλά  $f_i(w_1, \dots, w_{n_i}) \uparrow$ . Εδώ από επαγωγική υπόθεση ο υπολογισμός  $\text{comp}(A :)$  έχει ως εξής:

$f_i(A_1, \dots, A_{n_i}) :$  (comp)

$f_i \quad A_1, \dots, A_{n_i} :$  (επαγ. υπ.)

$\vdots$

$f_i \quad A_1, \dots, A_{n_i-1} : w_{n_i}$

$\vdots$

$f_i : w_1 w_2 \dots w_{n_i}$

και πάλι από το Λήμμα 2.30 σταματά άγονα.

(2γ)  $\mathbf{val}(f_i(A_1, \dots, A_{n_i})) = w$ , έτσι ώστε υπάρχουν στοιχεία  $w_1, \dots, w_{n_i}$  στο  $M$  με  $\mathbf{val}(A_j) = w_j$  για  $j = 1, \dots, n_i$  και  $f_i(w_1, \dots, w_{n_i}) = w$ . Από την επαγωγική υπόθεση και το Λήμμα 2.30 ο υπολογισμός  $\text{comp}(A :)$  είναι

$f_i(A_1, \dots, A_{n_i}) :$  (comp)

$f_i \quad A_1, \dots, A_{n_i} :$  (επαγ. υπ.)

$\vdots$

$f_i \ A_1, \dots, A_{n_i-1} : w_{n_i}$

⋮

$f_i : w_1 w_2 \dots w_{n_i}$   
:  $f_i(w_1, \dots, w_{n_i})$

(3)  $A \equiv \zeta_i(A_1, \dots, A_{n_i})$  για κάποια  $n$ -μελ συναρτησιακή μεταβλητή  $\zeta_i$  του  $E$ , τότε ο υπολογισμός  $\text{comp}(A)$  αρχίζει με τη μετάβαση

$\zeta_i(A_1, \dots, A_{n_i})$  : (comp)

$\zeta_i \ A_1, \dots, A_{n_i}$  :

Θεωρούμε τρεις περιπτώσεις όπως και στο (2):

(3α) Για κάποιο  $j$ ,  $\mathbf{val}(A_j) \uparrow$ , οπότε και  $\mathbf{val}(A) \uparrow$ .

Απόδειξη ίδια με το (2α).

(3β) Υπάρχουν  $w_1, \dots, w_j \in M$  τέτοια ώστε  $\mathbf{val}(A_j) = w_j$  για  $j = 1, \dots, n_i$ , αλλά  $\zeta_i(w_1, \dots, w_{n_i}) \uparrow$ .

$\zeta_i(A_1, \dots, A_{n_i})$  : (comp)

$\zeta_i \ A_1, \dots, A_{n_i}$  : (επαγ. υπ.)

⋮

$\zeta_i \ A_1, \dots, A_{n_i-1} : w_{n_i}$

⋮

$\zeta_i : w_1 w_2 \dots w_{n_i}$

όπου το τελευταίο αποκλίνει.

(3γ)  $\mathbf{val}(\zeta_i(A_1, \dots, A_{n_i})) = w$ , έτσι ώστε υπάρχουν στοιχεία  $w_1, \dots, w_{n_i}$  στο  $M$  με  $\mathbf{val}(A_j) = w_j$  για  $j = 1, \dots, n_i$  και  $\bar{\zeta}_i(w_1, \dots, w_{n_i}) = w$ . Κι εδώ όπως πριν

$\zeta_i(A_1, \dots, A_n)$  : (comp)

$\zeta_i \ A_1, \dots, A_n$  : (επαγ. υπ.)

⋮

$\zeta_i \ A_1, \dots, A_{n-1} : w_n$  (επαγ. υπ.)

⋮

$\zeta_i : w_1 w_2 \dots w_n$  (ορισμός της  $\bar{\zeta}_i$ )

⋮

:  $\bar{\zeta}_i(w_1, \dots, w_n)$

:  $w$

Από τον ορισμό της αναδρομικής μηχανής έχουμε

$$\bar{\zeta}_i(\vec{x}) = w \Leftrightarrow \zeta_i : \vec{x} \rightarrow E_i\{\vec{x} \equiv \vec{x}\} \rightarrow s_1 \rightarrow \dots \rightarrow w$$

και από τον Πίνακα Μεταβάσεων

$\zeta_i : \vec{x}$  (i-call)

$E_i\{\vec{v} \equiv \vec{x}\}$  :

Σύμφωνα με τα παραπάνω σε όποια περίπτωση (1),(2γ),(3γ) και να εμπίπτουν τα ορίσματα του  $E_i$  ο υπολογισμός πραγματοποιείται και ισχύει

$$E_i\{\vec{x} \equiv \vec{x}\} : \rightarrow s_1 \rightarrow \dots \rightarrow : w \Leftrightarrow \mathbf{val}(E_i\{\vec{v} \equiv \vec{x}\}) = w$$

Άρα έχουμε το ζητούμενο  $\bar{\zeta}_i(\vec{x}) = w \Leftrightarrow \mathbf{val}(E_i\{\vec{v} \equiv \vec{x}\}) = w$ . □

**Θεώρημα 2.32.** Το σύνολο των **M**-αναδρομικών μερικών συναρτήσεων περιλαμβάνει τις δοσμένες μερικές συναρτήσεις  $f_1, \dots, f_K$  της **M**, τις προβολές

$$P_i^n(x_1, \dots, x_n) = x_i \quad (i = 1, \dots, n)$$

και τις σταθερές  $C_0(\vec{x}) = 0$  και  $C_1(\vec{x}) = 1$ , και είναι κλειστό για σύνθεση και διακλάδωση.

*Απόδειξη.* Για τις δοσμένες μερικές συναρτήσεις, παρατηρούμε ότι για το πρόγραμμα  $E_{f_i}$ :  $\zeta(\vec{x}) = f_i(\vec{x})$  έχουμε:

$$\zeta(\vec{x}) : \rightarrow \zeta : \vec{x} \rightarrow E_i\{\vec{v}_i \equiv \vec{x}\} : \rightarrow f_i(\vec{x}) : \rightarrow : f_i(\vec{x})$$

Για την προβολή  $P_i^n$  χρησιμοποιούμε το πρόγραμμα  $\zeta(\vec{x}) = x_i$

και για τις σταθερές συναρτήσεις  $C_0, C_1$  χρησιμοποιούμε τα  $\zeta(\vec{x}) = 0$  και  $\zeta(\vec{x}) = 1$  αντίστοιχα.

Για τη σύνθεση έστω  $E_f$  και  $E_g$  προγράμματα της **M** που υπολογίζουν τις  $f$  και  $g$ . Τότε η σύνθεση  $f \circ g$  υπολογίζεται από το πρόγραμμα:

$$E = E_f + E_g + \{\zeta(\vec{x}) = f(g(\vec{x}))\}$$

Για τη διακλάδωση έστω τα  $E_c, E_g, E_h$  προγράμματα της **M** που υπολογίζουν τις  $\bar{c}, \bar{g}$  και  $\bar{h}$  αντίστοιχα. Αλλάζοντας το όνομα τυχόν κοινών συναρτησιακών μεταβλητών ώστε κάθε σύμβολο να εμφανίζεται σε ένα μόνο από τα προγράμματα  $E_c, E_g, E_h$  και να διατηρείται η αιτιοκρατία έχουμε:

$$E = E_c + E_g + E_h + \{\zeta(\vec{x}) = \text{αν } (c(\vec{x}) = 0) \text{ τότε } g(\vec{x}) \text{ αλλιώς } h(\vec{x})\}$$

□

**Πόρισμα 2.33.** Για κάθε μερική άλγεβρα  $\mathbf{M} = \{M, 0, 1, f_1, \dots, f_K\}$  και τυχαίες  $g : M^n \rightarrow M, f : M^m \rightarrow M$ ,

$$[g \in \mathcal{R}(\mathbf{M}) \ \& \ f \in \mathcal{R}(\mathbf{M}, g)] \Rightarrow f \in \mathcal{R}(\mathbf{M})$$

*Απόδειξη.* Εφόσον η  $g \in \mathcal{R}(\mathbf{M})$  το πρόγραμμα που υπολογίζει την  $g$  χρησιμοποιεί το λεξιλόγιο της **M**. Άρα αν το  $E_g$  χρησιμοποιεί  $N$  από τα  $K_i$  που υπολογίζουν τις αντίστοιχες  $f_i$  και προγράμματα

$E_{\bar{P}_i^n}, E_{\bar{C}_0}, E_{\bar{C}_1}$  προγράμματα σύνθεσης έστω  $E_o$  και διακλάδωσης  $E_d$  έχουμε ότι

$$E_g = \sum_{i=1}^N E_i + E_{\bar{P}_i^n} + E_{\bar{C}_0} + E_{\bar{C}_1} + E_o + E_d + \{\zeta_g(x_1, \dots, x_n) = g(x_1, \dots, x_n)\}$$

Για  $f \in \mathcal{R}(\mathbf{M}, g)$  έχουμε ότι το πρόγραμμα  $E_f$  που υπολογίζει την  $f$  χρησιμοποιεί  $M$  από τα  $K_i$  που υπολογίζουν τις αντίστοιχες  $f_i$  και προγράμματα  $E_{\bar{P}_i^n}, E_{\bar{C}_0}, E_{\bar{C}_1}$  προγράμματα σύνθεσης έστω  $E_o$  και διακλάδωσης  $E_d$  και το πρόγραμμα που υπολογίζει την  $g$ . Άρα

$$\begin{aligned} E_f &= \sum_{i=1}^M E_i + E_{\bar{P}_i^n} + E_{\bar{C}_0} + E_{\bar{C}_1} + E_o + E_d + E_g + \{\zeta_f(x_1, \dots, x_m) = f(x_1, \dots, x_m)\} \\ &= \sum_{i=1}^N E_i + \sum_{i=1}^M E_i + E_{\bar{P}_i^n} + E_{\bar{C}_0} + E_{\bar{C}_1} + E_o + E_d + \{\zeta_g(\vec{x}_n) = g(\vec{x}_n)\} + \{\zeta_f(\vec{x}_m) = f(\vec{x}_m)\} \end{aligned}$$

Δεδομένου ότι σε ένα πρόγραμμα επιπλέον ορίσματα απλώς αγνοούνται (δεν χρησιμοποιούνται στους υπολογισμούς), μπορούμε να γράψουμε:

$$E_f = \sum_{i=1}^K E_i + E_{\bar{P}_i^n} + E_{\bar{C}_0} + E_{\bar{C}_1} + E_o + E_d + \{\zeta_g(\vec{x}_n) = g(\vec{x}_n)\} + \{\zeta_f(\vec{x}_m) = f(\vec{x}_m)\}$$

Οπώς φαίνεται το  $E_f$ , δηλαδή όλα τα επιμέρους προγράμματα που το ορίζουν, καλούν μόνο τα δοσμένα προγράμματα της  $\mathbf{M}$ . Άρα η  $f$  είναι  $\mathbf{M}$ -αναδρομική :  $f \in \mathcal{R}(\mathbf{M})$ . □

Θα δείξουμε τώρα πως σε κάθε πρόγραμμα  $E$  η υπολογιστική σημασιολογία της  $\mathcal{R}(\mathbf{M})$  αντιστοιχίζει τις ελάχιστες λύσεις - "κανονικές".

### Θεώρημα 2.34. Ελάχιστων Σταθερών Σημείων

Για κάθε πρόγραμμα  $E$  στη μερική άλγεβρα  $\mathbf{M}$  με συναρτησιακές μεταβλητές  $\zeta_0, \dots, \zeta_K$  οι μερικές συναρτήσεις  $\bar{\zeta}_0, \dots, \bar{\zeta}_K$  που υπολογίζει το σύστημα μεταβάσεων  $\mathcal{T}(E)$  είναι οι  $\sqsubseteq$ -ελάχιστες μερικές συναρτήσεις που ικανοποιούν τις εξισώσεις του  $E$ .

Απόδειξη. Οι  $\bar{\zeta}_0, \dots, \bar{\zeta}_k$  ικανοποιούν το σύστημα  $E$  από το Θεώρημα 2.31. Άρα, από τον ορισμό του αρχικού τμήματος, αρκεί να δείξουμε ότι αν οι τυχαίες  $\zeta'_0, \dots, \zeta'_k$  ικανοποιούν τις εξισώσεις του  $E$ , τότε

$$\bar{\zeta}_i(\vec{x}) = w \Rightarrow \zeta'_i(\vec{x}) = w \quad (i = 0, \dots, k)$$

Υποθέτουμε ότι οι  $\zeta'_0, \dots, \zeta'_k$  ικανοποιούν τις εξισώσεις του  $E$ , και θεωρούμε

$$\bar{\mathbf{M}} = (\mathbf{M}, \bar{\zeta}_0, \dots, \bar{\zeta}_k), \quad \mathbf{M}' = (\mathbf{M}, \zeta'_0, \dots, \zeta'_k)$$

Από το Θεώρημα 2.31 ξέρουμε ότι για κάθε κλειστό όρο  $A$  στο λεξιλόγιο  $(f_1, \dots, f_K, \zeta_0, \dots, \zeta_k)$ , αν  $\mathbf{val}_{\mathbf{M}}(A) = w$ , τότε ο υπολογισμός  $\text{comp}(A:)$  της  $\mathcal{T}(E)$  είναι τερματικός με τελευταία κατάσταση την  $: w$ . Θα δείξουμε με επαγωγή στο μήκος του υπολογισμού  $m$ , ότι για κάθε  $A$  και για κάθε  $w$ ,

(a) αν  $A : \rightarrow \alpha_1 : \beta_1 \rightarrow \dots \alpha_{m-1} : \beta_{m-1} \rightarrow : w$ , τότε  $\mathbf{val}_{\mathbf{M}'}(A) = w$ .

Συγκεκριμένα μας ενδιαφέρει η περίπτωση  $A \equiv \zeta_i(x_1, \dots, x_n)$ , οπότε

$$\bar{\zeta}_i(\vec{x}) = w \Rightarrow \mathbf{val}_{\mathbf{M}'}(\zeta_i(\vec{x})) \Rightarrow \zeta'_i(\vec{x}) = w.$$

Για την απόδειξη της (a) εξετάζουμε τη μορφή του όρου  $A$ , και το επιχείρημα είναι τετριμμένο σε όλες τις περιπτώσεις εκτός από την  $\zeta_i(A_1, \dots, A_n)$ , όπου ο υπολογισμός έχει τη μορφή:

$\zeta_i(A_1, \dots, A_n) :$

$\zeta_i A_1, \dots, A_n :$

$\vdots$

$\zeta_i A_1, \dots, A_{n-1} : w_n$

$\vdots$

$\zeta_i : w_1 \dots w_n$

$E_i\{\vec{v} \equiv \vec{w}\} :$

$\vdots$

$: w$

Σημειώνουμε ότι έχουμε και χρησιμοποιούμε δεδομένο μήκος υπολογισμού.

Η επαγωγική υπόθεση τώρα συνεπάγεται ότι

$$\mathbf{val}_{\mathbf{M}'}(A_1) = w_1, \dots, \mathbf{val}_{\mathbf{M}'}(A_n) = w_n, \mathbf{val}_{\mathbf{M}'}(E_i\{\vec{v} \equiv \vec{w}\}) = w$$

επειδή οι υπολογισμοί που αντιστοιχούν σ'αυτές τις τιμές έχουν μικρότερο μήκος. Άρα

$$\begin{aligned} \mathbf{val}_{\mathbf{M}'}(\zeta_i(A_1, \dots, A_n)) &= \zeta'_i(\mathbf{val}_{\mathbf{M}'}(A_1) = w_1, \dots, \mathbf{val}_{\mathbf{M}'}(A_n)) \\ &= \zeta_i(w_1, \dots, w_n) = \mathbf{val}_{\mathbf{M}'}(E_i\{\vec{v} \equiv \vec{w}\}) = w \end{aligned}$$

□

Έχουμε πλέον ορίσει τις αναδρομικές συναρτήσεις και έχουμε δώσει σύστημα υπολογισμού τους και δείξει την εγκυροτητά του.



Έχουμε ορίσει το σύνολο των μερικών συναρτήσεων που είναι αναδρομικές σε ένα σύνολο  $\Psi$  πλειομελών, αναδρομικών συναρτήσεων στους φυσικούς:

$$\mathcal{R}(\Psi) = \{f : \mathbb{N}^n \rightarrow \mathbb{N} \mid f \text{ } (\mathbf{N}_0, f_1, \dots, f_K)\text{-αναδρομική για } f_1, \dots, f_K \in \Psi\}$$

**Θεώρημα 2.35.** Το σύνολο  $\mathcal{R}(\Psi)$  είναι πρωτογενώς κλειστό και κλειστό για ελαχιστοποίηση, με

$$\mathcal{R}_\mu(\Psi) \subseteq \mathcal{R}(\Psi).$$

Έχουμε ότι κάθε ελαχιστικά αναδρομική μερική συνάρτηση είναι αναδρομική.

*Απόδειξη.* Από Θεώρημα 2.32 το  $\mathcal{R}(\Psi)$  στους φυσικούς περιέχει τις προβολές, τις σταθερές 0 και 1, τις δοσμένες μερικές συναρτήσεις  $S(x)$ ,  $Pd(x)$  και είναι κλειστό για σύνθεση και διακλάδωση. Θα δείξουμε ότι το σύνολο  $\mathcal{R}(\Psi)$  είναι κλειστό για ελαχιστοποίηση. Δηλαδή αν  $g \in \mathcal{R}(\Psi)$  και

$$f(y, \vec{x}) = (\mu i \geq y)[g(i, \vec{x}) = 0],$$

τότε  $f \in \mathcal{R}(\Psi)$ . Από Πρόταση 2.20 η  $f$  είναι η ελάχιστη λύση της αναδρομικής εξίσωσης

$$f(y, \vec{x}) = \text{αν } (g(y, \vec{x}) = 0) \text{ τότε } y \text{ αλλιώς } f(y + 1, \vec{x})$$

η οποία από μόνη της είναι πρόγραμμα.

Από το Θεώρημα 2.34 έχουμε ότι η  $f$  υπολογίζεται από αυτό ο πρόγραμμα και  $f \in \mathcal{R}(\Psi \cup \{g\})$ . Αλλά από Πρόταση 2.33 για  $g \in \mathcal{R}(\Psi)$  καταλήγουμε ότι  $f \in \mathcal{R}(\Psi)$ . Άρα  $\mathcal{R}_\mu(\Psi) \subseteq \mathcal{R}(\Psi)$ . □

Επίσης από τον Ορισμό 2.18 έχουμε  $\mathcal{R}_p(\Psi) \subseteq \mathcal{R}_\mu(\Psi)$ .

## 2.4 Κωδικοποίηση

Γενικά **κωδικοποίηση** ενός συνόλου  $A$  σε ένα σύνολο  $C$  είναι η τυχαία ένα-προς-ένα συνάρτηση  $c : A \rightarrow C$ , που μας επιτρέπει να ανακτήσουμε ένα τυχαίο στοιχείο  $x \in A$  από τον κωδικό  $c(x)$ .

Έστω  $\mathbb{N}^*$  το σύνολο όλων των πεπερασμένων ακολουθιών φυσικών αριθμών, ώστε  $\Lambda, (1), (1, 4), (2, 3, 4), \dots \in \mathbb{N}^*$ , όπου  $\Lambda$  η κενή ακολουθία.

Η τυχαία κωδικοποίηση

$$\langle \rangle : \mathbb{N}^* \rightarrow \mathbb{N}$$

του  $\mathbb{N}^*$  είναι **πρωτογενώς αναδρομική**, αν για κάθε ακολουθία φυσικών αριθμών  $u_0, \dots, u_{n-1}$ :

i)  $u_i < \langle u_0, \dots, u_{n-1} \rangle$  ( $i < n$ ).

ii) η σχέση  $Seq(u) \Leftrightarrow u = \langle u_0, \dots, u_{n-1} \rangle$  για κάποια  $u_0, \dots, u_{n-1}$  είναι πρωτογενώς αναδρομική.

iii) για κάθε  $n$  η  $n$ -μελής συνάρτηση  $f_n(u_0, \dots, u_{n-1}) = \langle u_0, \dots, u_{n-1} \rangle$  είναι πρωτογενώς αναδρομική

και

iv) υπάρχουν πρωτογενώς αναδρομικές συναρτήσεις που ικανοποιούν τα έξης:

$$\begin{aligned} lh(\langle u_0, \dots, u_{n-1} \rangle) &= n \text{ (μήκος)} \\ proj(\langle u_0, \dots, u_{n-1} \rangle, i) &= (\langle u_0, \dots, u_{n-1} \rangle)_i = u_i \quad (i < n) \text{ (προβολή)} \\ append(\langle u_0, \dots, u_{n-1} \rangle, y) &= \langle u_0, \dots, u_{n-1}, y \rangle. \text{ (προσθήκη)} \end{aligned}$$

Για τεχνικούς λόγους απαιτούμε

$$[\neg Seq(u) \vee i \geq lh(u)] \Rightarrow lh(u) = (u)_i = 0.$$

το οποίο μαζί με το (i) δίνει ότι

$$u > 0 \Rightarrow (u_i) < u.$$

**Πρόταση 2.36.** Υπάρχουν πρωτογενώς αναδρομικές συναρτήσεις  $u \upharpoonright i$  και  $u * v$ , τέτοιες που

$$\langle u_0, \dots, u_{n-1} \rangle \upharpoonright i = \langle u_0, \dots, u_{i-1} \rangle \quad (i \leq n)$$

$$\langle u_0, \dots, u_{n-1} \rangle * \langle v_0, \dots, v_{m-1} \rangle = \langle u_0, \dots, u_{n-1}, v_0, \dots, v_{m-1} \rangle$$

Όντως η πρώτη είναι σύνθεση των πρωτογενώς αναδρομικών συναρτήσεων  $Seq$  και  $append$ , ενώ η δεύτερη των  $Seq$  και  $lh$ .

**Πρόταση 2.37.** Υπάρχει πρωτογενώς αναδρομική κωδικοποίηση του  $\mathbb{N}^*$ , συγκεκριμένα η "κλασσική" κωδικοποίηση

$$\langle u_0, \dots, u_{n-1} \rangle = p_0^{u_0+1} * p_1^{u_1+1} * \dots * p_{n-1}^{u_{n-1}+1}$$

όπου  $p_0 = 2, p_1 = 3, p_2 = 5, \dots$  πρώτοι. Θέτουμε  $\langle \Lambda \rangle = 1$ .

Απόδειξη.

$$\langle \Lambda \rangle = 1$$

$$\langle u_0, \dots, u_{n+1} \rangle = \langle u_0, \dots, u_n \rangle * p_{n+1}^{u_{n+1}+1}$$

□

Είχαμε δει στο πρώτο κεφάλαιο, ότι η σχέση

$$Prime(x) \Leftrightarrow \exists d \mid x \text{ είναι πρώτος αριθμός}$$

είναι πρωτογενώς αναδρομική.

**Λήμμα 2.38.** Για την "κλασσική" κωδικοποίηση, οι εξής συναρτήσεις είναι πρωτογενώς αναδρομικές

$$maxseq(n) = max\{\langle u_0, \dots, u_{m-1} \rangle \mid m, u_0, \dots, u_{m-1} \leq n\}$$

$$seq(u, i, j) = \begin{cases} \langle (u)_i, (u)_{i+1}, \dots, (u)_{j-1} \rangle, & \text{αν } Seq(u) \text{ (} 0 \leq i < j \leq lh(u) \text{)} \\ 0, & \text{αλλιώς} \end{cases}$$

Έστω τώρα φυσικός αριθμός  $c(u)$  κωδικός ακολουθίας. Για να ανακτήσουμε το  $i$ -οστό στοιχείο της ακολουθίας αρκεί να πάρουμε τον  $i$ -οστό πρώτο και να ανακτήσουμε τον εκθέτη του.

Υπάρχει πρόγραμμα που επιστρέφει τον  $i$ -οστό πρώτο:

$$p(0) = 2$$

$$p(n+1) = \{ \mu k > p(n) : (Prime(k)) \}$$

Έστω  $p_i$ . Τότε με  $c(u) \div p_i = y$  είναι

$$u_i = \log_{p_i}(y) + 1.$$

Φυσικά και μπορούμε να έχουμε ακολουθίες ακολουθιών. Χάρην ευκολίας θέτουμε

$$(u)_{i,j} = ((u)_i)_j, \quad (u)_{i,j,k} = (((u)_i)_j)_k \quad \text{κτλ}$$

$$\text{first}(u) = (u)_0, \text{ το πρώτο στοιχείο της } u_0, \dots, u_{n-1}$$

$$\text{last}(u) = (u)_{lh(u)-1}, \text{ το τελευταίο στοιχείο της } u_0, \dots, u_{n-1}$$

Η "κλασσική" κωδικοποίηση του  $\mathbb{N}^*$  δεν είναι η πιο αποτελεσματική, τουλάχιστον από άποψη πολυπλοκότητας. Από άποψη υπολογισιμότητας όμως, όλες οι κωδικοποιήσεις του  $\mathbb{N}^*$  είναι ισοδύναμες.

**Πρόταση 2.39.** Έστω πρωτογενώς αναδρομικές συναρτήσεις

$$\langle \cdot \rangle_1, \langle \cdot \rangle_2 : \mathbb{N}^* \rightarrow \mathbb{N}.$$

Τότε υπάρχει πρωτογενώς αναδρομική συνάρτηση  $s : \mathbb{N} \rightarrow \mathbb{N}$ , τέτοια που

$$s(\langle \vec{x} \rangle_1) = \langle \vec{x} \rangle_2 \quad (\vec{x} \in \mathbb{N}^*)$$

**Απόδειξη.** Για  $u = (u_0, \dots, u_k)$  ορίζουμε συνάρτηση  $g(u, n)$  :

$$g(\langle u \rangle_1, 0) = \langle \quad \rangle_2$$

$$g(\langle u \rangle_1, n+1) = g(\langle u \rangle_1, n) * \langle (\langle u \rangle_1)_{n+1} \rangle_2 \quad m+1 \leq k$$

Τότε  $s = g(\langle u \rangle_1, lh(u))$ . □

Από δω και στο εξής θα χρησιμοποιούμε τη "κλασσική" κωδικοποίηση και τα συμπεράσματα, συμφωνα με την παραπάνω Πρόταση, θα ισχύουν για οποιαδήποτε κωδικοποίηση στο  $\mathbb{N}$ .

Χρησιμοποιώντας την "κλασσική" κωδικοποίηση ακολουθιών θα ορίσουμε κωδικούς για τα βασικά σύνολα αντικειμένων στη θεωρία της προγραμματιστικής γλώσσας R.

Συμβολίζοντας  $[X]_A$  τον κωδικό του αντικειμένου  $X$ , οι ορισμοί που ακολουθούν μας δίνουν ένα-προς-ένα συναρτήσεις  $\llbracket \cdot \rrbracket_A : A \rightarrow \mathbb{N}$ , για κάθε σύνολο  $A$ .

Έχουμε τα εξής 6 συνολα και για  $i = 1, \dots, 6$  θα συμβολίζουμε με  $\llbracket \cdot \rrbracket_i$  τον κωδικό του αντίστοιχού συνόλου.

### **i=1. Σύμβολα**

Θέτουμε

$$[v_i]_1 = \langle 0, 0, 1 \rangle, \quad [n]_1 = \langle 0, 1, n \rangle, \quad [S]_1 = \langle 1, 1, 0 \rangle,$$

$$[Pd]_1 = \langle 1, 1, 1 \rangle, \quad [\zeta_i^n]_1 = \langle 1, n, 2 + i \rangle.$$

και για τα σύμβολα διακλάδωσης

$$[\alpha v]_1 = \langle 2, 0 \rangle, \quad [\tau \acute{o} \tau \epsilon]_1 = \langle 2, 1 \rangle \quad [\alpha \lambda \lambda \iota \acute{o} \varsigma]_1 = \langle 2, 2 \rangle,$$

$$[\ ]_1 = \langle 2, 3 \rangle, \quad [(\ ]_1 = \langle 2, 4 \rangle, \quad [)]_1 = \langle 2, 5 \rangle. \quad [=]_1 = \langle 2, 6 \rangle, \quad [?]_1 = \langle 2, 7 \rangle.$$

### **i=2. Λέξεις**

Για κάθε λέξη (ακολουθία από σύμβολα)  $\alpha \equiv \alpha_0, \alpha_1, \dots, \alpha_n$  θέτουμε

$$[\alpha_0, \alpha_1, \dots, \alpha_n]_2 = \langle [\alpha_0]_1, [\alpha_1]_1, \dots, [\alpha_n]_1 \rangle.$$

Για παράδειγμα,

$$\begin{aligned} [\zeta_1^2(v_1, 5)] &= \langle [\zeta_1^2]_1, [(\ ]_1, [v]_1, [\ ]_1, [5]_1, [)]_1 \rangle \\ &= \langle \langle 1, 2, 3 \rangle, \langle 2, 4 \rangle, \langle 0, 0, 1 \rangle, \langle 2, 3 \rangle, \langle 0, 1, 5 \rangle, \langle 2, 5 \rangle \rangle. \end{aligned}$$

Ο ορισμός αυτός αναθέτει κωδικούς στους όρους της R.

Πρέπει να προσέχουμε πότε οι μεταβλητές  $v_i$  και οι σταθερες  $n$  είναι σύμβολα και πότε όροι και να χρησιμοποιούμε την κωδικοποίηση  $\llbracket \cdot \rrbracket_1, \llbracket \cdot \rrbracket_2$  αντίστοιχα.

### **i=3. Αναδρομικές εξισώσεις**

Η τυχαία τυπική εξίσωση καθορίζεται από το αριστερό και το δεξί μέλος της που είναι όροι. Θέτουμε

$$[\zeta(\vec{v})]_3 = \langle [\zeta(\vec{v})]_2, [1]_2 \rangle$$

#### **i=4. Αναδρομικά προγράμματα**

Αν  $E = (e_0, \dots, e_k)$ , όπου  $e_i$  κωδικός αναδρομικής εξίσωσης, θέτουμε

$$[E]_4 = \langle [e_0]_3, \dots, [e_k]_3 \rangle.$$

#### **i=5. Καταστάσεις**

Μια κατάσταση έχει τη μορφή  $\alpha_0 \dots \alpha_{m-1} : \beta_0 \dots \beta_{n-1}$ , όπου  $\alpha_i$  κλειστός όρος ή συναρτησιακό σύμβολο ή ? και  $\beta_i$  αριθμητικές σταθερές. Θέτουμε

$$[\alpha_0 \dots \alpha_{m-1} : \beta_0 \dots \beta_{n-1}]_5 = \langle \langle [\alpha_0]_*, \dots, [\alpha_{m-1}]_* \rangle, \langle [\beta_0]_1, \dots, [\beta_{n-1}]_1 \rangle \rangle,$$

όπου

$$[\alpha_i]_* = \begin{cases} [\alpha_i]_1, & \text{αν } \alpha_i \text{ συναρτησιακό σύμβολο ή ?} \\ [\alpha_i]_2, & \text{αν } \alpha_i \text{ κλειστός όρος} \end{cases}$$

#### **i=6. Υπολογισμοί**

Για κάθε ακολουθία καταστάσεων  $s = (s_0, \dots, s_k)$ , θέτουμε

$$[s_0, \dots, s_k]_6 = \langle [s_0]_5, \dots, [s_k]_5 \rangle.$$

Η τελευταία σχέση κωδικοποιεί όλες τις ακολουθίες καταστάσεων, και ιδιαίτερα τους τερματικούς υπολογισμούς για οποιοδήποτε αναδρομικό πρόγραμμα.

## Μέρος II

# Θεώρημα Κανονική Μορφής

Με το ακόλουθο θεώρημα ο Kleene (c.1943) έδειξε ότι μπορούμε να μεταφράζουμε από αναδρομή σε πρωτογενή αναδρομή, και μάλιστα υπάρχουν κανονικοί κανόνες μετάφρασης.

### Θεώρημα 2.40. Θεώρημα Κανονικής Μορφής και Απαρίθμησης (Kleene)

Υπάρχει πρωτογενώς αναδρομική συνάρτηση  $U(y)$ , κα πρωτογενώς αναδρομικές σχέσεις  $T_n(e, x_1, \dots, x_n, y)$  ( $n \geq 1$ ) και συναρτήσεις  $S_n^m(e, z_1, \dots, z_m)$  ( $n, m \geq 1$ ), για τις οποίες ισχύουν τα εξής:

a) Η τυχαία  $n$ -μελής μερική συνάρτηση  $f(\vec{x})$  στους φυσικούς είναι αναδρομική αν και μόνον αν υπάρχει κάποιος αριθμός  $e$  τέτοιος που

$$f(\vec{x}) = U(\mu y T_n(e, \vec{x}, y)) \quad (\vec{x} = x_1, \dots, x_n \in \mathbb{N})$$

b) Για όλα τα  $e, y, \vec{z} = z_1, \dots, z_m$  και  $\vec{x} = x_1, \dots, x_n$ ,

$$U(\mu y T_{m+n}(e, \vec{z}, \vec{x}, y)) = U(\mu y T_n(S_n^m(e, \vec{z}), \vec{x}, y)).$$

Επιπλέον οι συναρτήσεις  $S_n^m(e, \vec{z})$  είναι ένα προς ένα.

Για το νόημα του (a) έχουμε τη σχέση

$$T_n(e, x_1, \dots, x_n, y) \Leftrightarrow$$

"ο  $e$  είναι κωδικός κάποιου αναδρομικού προγράμματος  $E$ , και ο  $y$  είναι κωδικός τερματικού υπολογισμού του  $E$  στη είσοδο  $\zeta_0 : x_1, \dots, x_n$ ". να είναι πρωτογενώς αναδρομική.

Και υπάρχει πρωτογενώς αναδρομική  $U(y)$ , τέτοια που αν  $y$  κωδικός τερματικού υπολογισμού, τότε

$U(y) =$  η τιμή εξόδου από τον τερματικό υπολογισμό  $y$ .

Από την κανονική μορφή (a) συνεπάγεται ότι κάθε αναδρομική μερική συνάρτηση "παράγεται" από πρωτογενώς αναδρομικές συναρτήσεις με μόνο μια βλακώδη αναζήτηση.

Έστω π.χ. η "κλασσική" κωδικοποίηση. Η  $U$  παίρνει τον εκθέτη του μεγαλύτερου πρώτου και 'μετράει' τους πρώτους που τον διαιρούν μια φορά.

Φαίνεται επίσης ότι κάθε αναδρομική μερική συνάρτηση είναι ελαχιστικά αναδρομική.

Τέλος αν θέσουμε

$$\phi_e^n = U(\mu y T_n(e, \vec{x}, y)),$$

$\phi$ ,  $n$ -μελής συνάρτηση με κωδικό  $e$ . Τότε η κανονική μορφή (a) συνεπάγεται ότι, για κάθε  $n$ , η ακολουθία

$$\phi_0^n, \phi_1^n, \dots$$

απαριθμεί όλες τις  $n$ -μελής αναδρομικές μερικές συναρτήσεις και μάλιστα με τέτοιο τρόπο ώστε η  $(n+1)$ -μελής συνάρτηση

$$\phi^n(e, \vec{x}) = \phi_e^n(\vec{x})$$

να είναι αναδρομική.

Μας δίνει δηλαδή και μια απαρίθμηση όλων των αναδρομικών συναρτήσεων.

Το μέρος (b) του θεωρήματος δείχνει ότι μια συγκεκριμένη κατασκευή αναδρομικών προγραμμάτων είναι πρωτογενώς αναδρομική στους κωδικούς. Συγκεκριμένα, αν ο  $e$  είναι κωδικός της  $f(\vec{z}, \vec{x})$ , τότε, για κάθε  $\vec{z}$ , ο  $S_n^m(e, \vec{z})$  είναι κωδικός της μερικής συνάρτησης  $f_{\vec{z}}(\vec{x})$ .

Με χρήση αυτού του θεωρήματος (θεώρημα  $S_n^m$ ) φαίνεται πώς πιο πολύπλοκα προγράμματα (προγράμμα πάνω σε κωδικούς άλλων προγραμμάτων πχ) είναι επίσης πρωτογενώς αναδρομικά στους κωδικούς.

### Μέρος III

## Απόδειξη Θεωρήματος Κανονικής Μορφής

Για την απόδειξη του πρώτου μέρους (α) του Θεωρήματος θα παραθέσουμε μια σειρά από σχέσεις, οι οποίες με χρήση της κωδικοποίησης όπως ορίστηκε στο προηγούμενο κεφάλαιο μας δίνουν πρωτογενώς αναδρομικούς ορισμούς.

Απόδειξη ότι  $T_n(e, \vec{x}, y)$  είναι πρωτογενώς αναδρομική

**ΑρΜετ**( $v$ )  $\iff$  ο  $v$  είναι κωδικός κάποιος μεταβλητής  $v_i$

$$\iff v = \langle 0, 0, (v)_2 \rangle$$

**ΑρΣταθ**( $c$ )  $\iff$  ο  $c$  είναι κωδικός αριθμού

$$\iff c = \langle 0, 1, (c)_2 \rangle$$

**ΣυνΜετ**( $f$ )  $\iff$  ο  $f$  είναι κωδικός κάποιας  $\zeta_i^n$

$$\iff f = \langle 1, (f)_1, (f)_2 \rangle \& (f)_1 \geq \& (f)_2 \geq 2$$

**ΣυνΣταθ**( $f$ )  $\iff$  ο  $f$  είναι κωδικός του S ή του Pd

$$\iff f = [S]_1 \vee f = [Pd]_1$$

**ΣυνΣυμβ**( $f$ )  $\iff$  ΣυνΜετ( $f$ )  $\vee$  ΣυνΣταθ( $f$ )

$arity(f)$  = η πλειομέλεια του συναρτησιακού συμβόλου  $f$ , αν ΣυνΣυμβ( $f$ ) = ( $f$ )<sub>1</sub>

**Όρος**( $u$ )  $\iff$  ο  $u$  είναι κωδικός όρου

**ΚλΌρος**( $u$ )  $\iff$  ο  $u$  είναι κωδικός κλειστού όρου

$$\iff \text{Όρος}(u) \& (\forall i < lh(u)) \neg \text{ΑρΜετ}((u)_i)$$

**ΣυνθΌρος**( $u$ )  $\iff$  ο  $u$  είναι κωδικός όρου  $\zeta_i^n(A_1, \dots, A_n)$

$$\iff \text{Όρος}(u) \& \text{ΣυνΜετ}(\text{first}u)$$

**ΥποΌρος**( $u, v$ )  $\iff$  ο  $v$  είναι κωδικός υποόρου του όρου με κωδικό  $u$

$$\iff \text{Όρος}(u) \& \text{Όρος}(v) \& (\exists i, j \leq lh(u)) [i < j \& v = \text{seg}(u, i, j)]$$

**ΑπλΌρος**( $u$ )  $\iff$  ο  $u$  είναι κωδικός όρου  $\zeta_i^n(v_1, \dots, v_n)$

$$\iff \text{ΣυνθΌρος}(u) \& (\forall v < u) [\text{ΥποΌρος}(u, v) \Rightarrow \text{ΑρΜετ}(v)]$$

**Εξίσωση**( $e$ )  $\iff$  ο  $e$  είναι κωδικός αναδρομικής εξίσωσης

$$\iff e = \langle \text{first}(e), \text{last}(e) \rangle$$

$$\& \text{ΑπλΌρος}(\text{first}(e)) \& \text{Όρος}(\text{last}(e))$$

$$\& (\forall i < lh(\text{last}(e))) [\text{ΑρΜετ}((\text{last}(e))_i)]$$

$$\Rightarrow (\exists j < lh(\text{first}(e))) [(\text{last}(e))_i = (\text{first}(e))_j]$$

**Προγρ**( $e$ )  $\iff$  ο  $e$  είναι κωδικός προγράμματος

$$\iff \text{Seq}(e) \& lh(e) > 0 \& (\forall i < lh(e)) [\text{Εξίσωση}((e)_i)]$$

$$(\forall i < lh(e)) (\forall j < lh((e)_{i,1}) [\text{ΣυνΜετ}((e)_{i,1,j}) \Rightarrow (\exists k < lh(e)) [(e)_{i,1,j} = (e)_{k,0,0}]]$$

**Κατ**( $s$ )  $\iff$  ο  $s$  είναι κωδικός κατάστασης



$\Leftrightarrow s = \langle (s)_0, (s)_1 \rangle$   
 $\& (\forall i < lh((s)_0) [\text{ΣυνΣυμβ}((s)_0, i) V (s)_0, i = [?]_1 V \text{Κλορος}((s)_0, i)] \quad \& (\forall j < lh((s)_1) \text{ΑρΣταθ}((s)_1, j))$   
**ΤερμΚατ** (s)  $\Leftrightarrow$  ο s είναι κωδικός τερματικής κατάστασης  
 $\Leftrightarrow \text{Κατ}(s) \& lh((s)_0) = 0 \& lh((s)_1) = 1$   
**Αντ**(u, j, x) = το αποτέλεσμα της αντικατάστασης της μεταβλητής με κωδικό j=[v<sub>i</sub>] με τη σταθερά x στον όρο με κωδικό u  
**ΠΛΑντ** (u, v, w) = το αποτέλεσμα της αντικατάστασης των μεταβλητών με κωδικούς (v)<sub>0</sub>, ..., last(v) με τις σταθερές (w)<sub>0</sub>, ..., last(w) στον όρο με κωδικό u  
**ΜετΑπλορου** (u) =  $\langle [v_{i_1}]_1, \dots, [v_{i_n}]_1 \rangle$  (αν u =  $[\zeta^n(v_1, \dots, v_{i_n})]_2$ )  
**Μετάβαση** (e, s, s')  $\Leftrightarrow$  Προγρ(e) & Κατ(s) & Κατ(s')  
 $\& s \rightarrow s'$  στο T(E) για e = [E]<sub>4</sub>  
**Υπολ** (e, y)  $\Leftrightarrow$  ο y είναι κωδικός τερματικού υπολογισμού στο T(E) για e = [E]<sub>4</sub>  
 $\Leftrightarrow (\forall i < lh(y) \div 1) [\text{Μετάβαση}(e, (y)_i, (y)_{i+1})$   
 ΤερμΚατ (last (y))  
**T<sub>n</sub>**(e,  $\vec{x}$ , y)  $\Leftrightarrow$  Προγρ(e) & Υπολ(e, y)  
 first(first (y)) =  $\langle$  first(first(first(e))) $\rangle$   
 last(first (y)) =  $[x_1 x_2 \dots x_n]_2$

**Λήμμα 2.41.** Η σχέση Ορος(u) είναι πρωτογενώς αναδρομική.

*Απόδειξη.* Αν ο n είναι φυσικός αριθμός, με "n" συμβολίζουμε την αποκωδικοποίηση του.

Θα ορίσουμε μια σχέση Ορος\* (u), η οποία ανάγει τη ισχύ ή όχι της Ορος(u) στους υποόρους της.

Συγκεκριμένα ορίζουμε

Ορος(u)  $\Leftrightarrow$  Ορος<sub>1</sub>  $\vee$  Ορος<sub>2</sub>  $\vee$  Ορος<sub>3</sub>  $\vee$  Ορος<sub>4</sub>  
 όπου

Ορος<sub>1</sub>  $\Leftrightarrow$  για κάποια μεταβλητή v<sub>i</sub>, u = [v<sub>i</sub>]<sub>2</sub>  $\Leftrightarrow$  u =  $\langle \langle 0, 0, (u)_{0,2} \rangle \rangle$

Ορος<sub>2</sub>  $\Leftrightarrow$  u = [n]<sub>2</sub> για κάποιον αριθμό n  $\Leftrightarrow$  u =  $\langle \langle 0, 1, (u)_{0,2} \rangle \rangle$

Οι πιο δύσκολες περιπτώσεις είναι της διακλάδωσης και της σύνθεσης. Εδώ απλώς ενδιαφερόμαστε αν υπάρχουν φυσικοί αριθμοί πιθανοί κωδικοί όρων, ώστε χρησιμοποιώντας τους στην κωδικοποίηση ο u να παρουσιάζει μορφή όρου.

Συγκεκριμένα ορίζουμε:

Ορος<sub>4</sub>  $\Leftrightarrow$

για κάποιους αριθμούς a, b, c : u = [ αν (" = 0) τότε "b" αλλιώς "c" ]<sub>2</sub>  
 $\Leftrightarrow (\exists a, b, c < u) (u = [(\text{αν}(\ ]_2 * * [= 0) \text{ τότε} ]_2 * b * [ \text{αλλιώς} ]_2 * c * [ ]_2)$

Παρατήρηση: Η Ορος<sub>4</sub> δε συνεπάγεται (αντίθετα από τις Ορος<sub>1</sub>( $u$ ), Ορος<sub>2</sub>( $u$ )) ότι ο  $u$  είναι κωδικός όρου. Η συνεπαγωγή είναι αληθής αν οι  $a, b, c$  είναι κωδικοί όρου.

Για την περίπτωση της σύνθεσης, θέλουμε να ελέγξουμε αν ο  $u$  είναι κωδικός όρου της μορφής  $f(A_0, \dots, A_n)$ . Εδώ έχουμε ένα επιπρόσθετο πρόβλημα, τις τελίτσες "...", για τις οποίες θα χρησιμοποιήσουμε πρωτογενή αναδρομή. Ούτε εδώ θα ελέγξουμε αν στην αποκωδικοποίηση οι φυσικοί αριθμοί  $\alpha_0, \dots, \alpha_n$  που αντιστοιχούν στους  $A_0, \dots, A_n$  είναι πράγματι κωδικοί όρων. Έτσι ουσιαστικά θα ορίσουμε

$$\text{Ορος}_3(u) \Leftrightarrow \exists \alpha_0, \dots, \alpha_n : u = [f(" \alpha_0 ", \dots, " \alpha_n ") ]_2$$

Θα χρησιμοποιήσουμε τον υπαρξιακό ποσοδείκτη για τον κωδικό  $\alpha = \langle \alpha_0, \dots, \alpha_n \rangle \leq \text{maxseq}(n)$ .

Για να ανασχηματίσουμε το  $[f(" \alpha_0 ", \dots, " \alpha_n ") ]_2$ , ώστε να συγκρίνουμε με το  $u$ , ορίζουμε τις εξής πρωτογενώς αναδρομικές συναρτήσεις:

$$h(0, u, \alpha) = \langle (u)_0 \rangle * [ ]_2 * \langle (\alpha)_0 \rangle$$

$$h(t+1, u, \alpha) = h(t, u, \alpha) * [ , ]_2 * \langle (\alpha)_{t+1} \rangle$$

Τότε αν  $u = [f(" \alpha_0 ", \dots, " \alpha_n ") ]_2$  (1) και  $t \leq n$ :

$$h(t, u, \alpha) = [f(" \alpha_0 ", \dots, " \alpha_t ") ]_2.$$

Επειδή αν ο  $u$  είναι της μορφής (1),  $(u)_{0,1}$  είναι η πλειομέλια (arity) της  $f$ , έπεται ότι η  $g(u, v) = h((u)_{0,1}, u, \alpha) * [ ]_2$  θα είναι ακριβώς ο αριθμός  $[f(" \alpha_0 ", \dots, " \alpha_n ") ]_2$ .

Άρα μπορούμε να ορίσουμε:

$$\text{Ορος}_3(u) \Leftrightarrow \text{Seq}(u) \& \text{ΣυνΣυμβ}((u)_0) \& (\exists \alpha \leq \text{maxseq}(u)) [u = g(u, \alpha)]$$

Οι σχέσεις Ορος<sub>3</sub>, Ορος<sub>4</sub> θα χρειαστούν κάποια συνάρτηση εξόδου που δίνει κωδικούς, που με τη σειρά τους πρέπει να ελεγχθούν αν έχουν τη μορφή όρων. Θέτουμε

$$\text{output}(\text{Ορος}_4)(u) = (\mu \alpha \leq \text{maxseq}(u)) (u = [(\text{αν } [ ]_2 * \langle (\alpha)_2 \rangle * [ ])_2])$$

$$\text{output}(\text{Ορος}_3)(u) = (\mu \alpha \leq \text{maxseq}(u)) [u = g(u, \alpha)]$$

όπου η συνάρτηση  $g$  ορίστηκε πιο πάνω.

Τέλος ορίζουμε αναδρομικά τη συνάρτηση  $h(w)$  η οποία "θυμάται" ποιοι κωδικοί είναι πραγματικοί όροι. Η μορφή της εξόδου της σε κάποιο  $w$  είναι  $\langle t_0, \dots, t_{w-1} \rangle$ , όπου για  $i w - 1$ , ο  $i$  είναι κωδικός όρου αν και μόνο αν  $t_i = 1$ , διαφορετικά  $t_i = 0$ .

$$h(0) = \langle \quad \rangle$$

$$h(w+1) = \begin{cases} h(w) * \langle 1 \rangle, & \text{αν } (\text{Ορος}_1(w) \vee \text{Ορος}_2(w) \vee \{\text{Ορος}_3(w) \\ & \&\forall i \leq lh(\text{output}(\text{Ορος}_3)(w)) [h(w)_{\text{output}(\text{Ορος}_3)(w)_i} = 1]\} \\ & \vee \{\text{Ορος}_4(w) \&\forall i \leq lh(\text{output}(\text{Ορος}_4)(w)) \\ & [h(w)_{\text{output}(\text{Ορος}_4)(w)} = 1]\} \\ h(w) * \langle 0 \rangle, & \text{αλλιώς} \end{cases}$$

Έπεται ότι  $\text{Ορος}(u) \Leftrightarrow (h(u+1))_u = 1$ .

□

*Απόδειξη ότι  $U(y)$  είναι πρωτογενώς αναδρομική*

Έχοντας δείξει ότι η κωδικοποίηση και αποκωδικοποίηση στο  $\mathbb{N}$  είναι πρωτογενώς αναδρομική, έπεται άμεσα ότι είναι και η  $U(y)$  για  $y$  κωδικό τερματικού υπολογισμού:

$$U(y) = \text{last}(y)_{1,0,2}$$

Για την απόδειξη του δεύτερου μέρους (b) τους θεωρήματος, βλέπουμε ότι η σχέση  $T_{m+n}(e, \vec{z}, \vec{x}, y) = T(S_n^m(e, \vec{z}), \vec{x}, y)$  σημαίνει ότι τα προγράμματα που υπολογίζουν την πρωτογενώς αναδρομική  $T$  στο δεξί και αριστερό μέρος της ισότητας είναι ισοδύναμα.

Δηλαδή το πρόγραμμα με κωδικό  $e$  και όρισμα  $(\vec{z}, \vec{x})$  και το πρόγραμμα με κωδικό  $S_n^m(e, \vec{z})$  και όρισμα  $(\vec{x})$  επιστρέφουν τον ίδιο τερματικό υπολογισμό με κωδικό  $y$ .

Αρκεί να υπολογίσουμε μονοσήμαντα τον κωδικό  $S_n^m(e, \vec{z})$  από τον κωδικό  $e$  και το δοσμένο  $\vec{z}$ . (Είναι σα να σταθεροποιούμε το όρισμα  $\vec{z}$  και να 'τρέχουμε' το πρόγραμμα για τυχόν όρισμα  $\vec{x}$ ).

Έστω

$$g(\vec{z}, \vec{x})$$

η μερική συνάρτηση που υπολογίζει το πρόγραμμα  $E$  με κωδικό  $e$ , και

$$f(\vec{x}) = g(\vec{z}, \vec{x})$$

η συνάρτηση που υπολογίζει το πρόγραμμα  $E_{\vec{z}}$  με κωδικό  $S_n^m(e, \vec{z})$ . Προφανώς το πρώτο συναρτησιακό σύμβολο του  $E$  είναι η  $g$ , και το πρώτο συναρτησιακό σύμβολο του  $E_{\vec{z}}$  η  $f$ .

Για τον ορισμό του  $E_{\vec{z}}$ , εφόσον  $f(\vec{x}) = g(\vec{z}, \vec{x})$ , αρκεί να προσθέσουμε στην αρχή του προγράμματος  $E$  τη συναρτησιακή μεταβλητή  $f$ . Ο υπολογισμός του κωδικού  $S_n^m(e, \vec{z})$  θα χρησιμοποιεί τον κωδικό της  $f$ .

Έχουμε από την κωδικοποίηση ότι ο κωδικός της συναρτησιακής μεταβλητής που ορίζεται στην πρώτη εξίσωση του  $E$  είναι

$$[\zeta_i^{m+n}] = (e)_{0,0,0}$$

και οι κωδικοί των αριθμητικών μεταβλητών στην πρώτη εξίσωση

$$[V_i] = (e)_{0,0,2+2i} \quad (i = 0, \dots, m + n - 1).$$

Παρατηρούμε ότι ο αριθμός

$$f^*(e) = \langle 1, n, \max\{(e)_{i,0,0,2} + 1 \mid i < lh(e)\} \rangle$$

είναι κωδικός συναρτησιακής μεταβλητής που δεν εμφανίζεται στο  $E$ , καθώς είναι γνήσια μεγαλύτερος κάθε κωδικού που εμφανίζεται στο  $E$ .

Μπορούμε τώρα θα θέσουμε

$$S_n^m(e, \vec{z}) = \langle \langle f^*(e), [(), g_2(e, m), ()], \dots, g_2(e, m + n - 1), () \rangle \rangle \\ \langle g_1(e), [z_1]_1, \dots, [ ]_1, \dots, [ ]_1, [z_m]_1, [ ]_1 \rangle \rangle * e$$

Για να είναι καλά ορισμένη συνάρτηση, θέτουμε στην περίπτωση που  $\neg \text{Προγρ}(e)$ :

$$S_n^m(e, \vec{z}) = \langle 0, e, \vec{z} \rangle$$

καθώς από την κωδικοποίηση καμία ακολουθία αυτής της μορφής δεν είναι κωδικός προγράμματος (ισοδύνα επιστρέφει  $\perp$ ).

Τέλος από τη 'κλασική' κωδικοποίηση, η συναρτήσεις  $S_n^m(e, \vec{z})$  είναι ένα-προς-ένα.

**Πόρισμα 2.42.** Η μερική συνάρτηση  $f : \mathbb{N}^n \rightarrow \mathbb{N}$  είναι αναδρομική τότε και μόνο αν είναι ελαχιστικά αναδρομική.

*Απόδειξη.* Οι ελαχιστικά αναδρομικές μερικές συναρτήσεις είναι αναδρομικές από Θεώρημα 2.36 και από το Θεώρημα Κανονικής Μορφής προκύπτει ότι κάθε αναδρομική μερική συνάρτηση είναι ελαχιστικά αναδρομική.

□

## Μέρος IV

# Το Πρόβλημα Τερματισμού

### Θεώρημα 2.43. Turing

Η σχέση τερματισμού

$$H(e, x) \Leftrightarrow \phi_e(x) \downarrow$$

δεν είναι αναδρομική.

Απόδειξη. Από τον ορισμό της  $H(e, x)$  έχουμε:

$$\begin{aligned} H(e, x) &\Leftrightarrow \phi_e(x) \downarrow \\ &\Leftrightarrow (\exists y) T_1(e, x, y) \\ &\Leftrightarrow \text{Προγρ}(e) \ \& \ \text{η αναδρομική μηχανή με κωδικό } e \\ &\quad \text{τερματίζει στην είσοδο } x \end{aligned}$$

Έστω ότι η  $H(e, x)$  είναι αναδρομική. Τότε αναδρομική είναι και η ολική συνάρτηση

$$f(x) = \begin{cases} \phi_x(x) + 1, & \text{αν } H(x, x) \\ 0, & \text{αλλιώς} \end{cases}$$

Από το θεώρημα κανονικής μορφής για  $f$  αναδρομική έχουμε  $f = U(\mu y T_1(e, x, y)) = \phi_e(x)$ , για κάποιο κωδικό αναδρομικού προγράμματος  $e$ .

Άρα για κάποιο  $e$ , αν  $H(x, x): \phi_e(x) = \phi_x(x) + 1$  για κάθε δυνατή είσοδο  $x$ .

Άτοπο για  $x = e$ .

□

## **Βιβλιογραφία**

- 1 Αναδρομή και Υπολογισιμότητα - Γιάννης Ν. Μοσχοβάκης
- 2 Introduction to Metamathematics - S.C.Kleene
- 3 Theory of Recursive Functions and Effective Computability - Hartley Rogers,Jr.