

## 6 Αναδρομικές συναρτήσεις

**Συμβολισμοί:** Με  $\mathbb{N} = \{0, 1, \dots, n \dots\}$  συμβολίζουμε το σύνολο των φυσικών αριθμών. Τα  $x, y, z, \dots, a, b, c, \dots$  δέχονται τιμές από το  $\mathbb{N}$ . Με  $F, G, H$  θα συμβολίζουμε τις αριθμητικές συναρτήσεις, δηλαδή, για κάποιο  $n$ , τις συναρτήσεις από το  $\mathbb{N}^n$  στο  $\mathbb{N}$  και με  $P, Q, R$  τα αριθμητικά κατηγορήματα ή σχέσεις, δηλαδή υποσύνολα του  $\mathbb{N}^n$ . Με  $\vec{x}$  θα συμβολίζουμε τη  $n$ -άδα  $\langle x_1, \dots, x_n \rangle$  (το  $n$  θα τεκμαίρεται πολλές φορές από τα συμφραζόμενα), με  $\forall \vec{x}$  το  $\forall x_1 \dots \forall x_n$  και αντίστοιχα με  $\exists \vec{x}$  το  $\exists x_1 \dots \exists x_n$ .

**Ορισμός 6.1** Η συνάρτηση  $F : \mathbb{N}^n \rightarrow \mathbb{N}$  είναι υπολογίσιμη εάν υπάρχει ένας (μηχανικός) αλγόριθμος ο οποίος αν τον τροφοδοτήσουμε με τους αριθμούς  $a_1, \dots, a_n$  να μας προμηθεύει, σε πεπερασμένο χρόνο, την τιμή  $F(a_1, \dots, a_n)$ : δηλαδή αν υπάρχει μια αποτελεσματική, μηχανική συνταγή υπολογισμού των τιμών της συνάρτησης.

**Παρατήρηση 6.2** Ο ανωτέρω ορισμός δεν είναι ένας αυστηρός μαθηματικός ορισμός. Αναφέρεται σε έννοιες, όπως αλγόριθμος, για τις οποίες δεν έχουν δοθεί μαθηματικοί ορισμοί. Αργότερα θα δούμε πώς μπορούμε να δώσουμε ένα αυστηρό μαθηματικό ανάλογο της έννοιας «υπολογίσιμη συνάρτηση».

**Ορισμός 6.3** Για  $P \subset \mathbb{N}^n$ , η χαρακτηριστική συνάρτηση του  $P$ , η  $C_P$ , ορίζεται ως εξής:

$$C_P = \begin{cases} 0 & \text{αν } P(\vec{x}) \\ 1 & \text{αν } \neg P(\vec{x}) \end{cases}$$

**Ορισμός 6.4** Το κατηγορήμα  $P$  είναι υπολογίσιμο εάν η χαρακτηριστική του συνάρτηση  $C_P$  είναι υπολογίσιμη.

**Ορισμός 6.5** Για κάθε  $n$  και κάθε  $i$  με  $1 \leq i \leq n$ , ορίζουμε τη συνάρτηση  $I_i^n : \mathbb{N}^n \rightarrow \mathbb{N}$  να είναι η  $I_i^n(x_1, \dots, x_n) = x_i$ . Η  $I_i^n$  λέγεται συνάρτηση προβολής.

Θα ορίσουμε κλάσεις αριθμητικών συναρτήσεων  $\Sigma$ , χρησιμοποιώντας τους ακόλουθους κανόνες:

**(R1)** Οι βασικές συναρτήσεις  $Z, \sigma, +, \cdot, C_<$  και  $I_i^n$  (για κάθε  $i, n$  με  $1 \leq i \leq n$ ), ανήκουν στο  $\Sigma$ , όπου  $+$  και  $\cdot$  είναι αντιστοίχως οι γνωστές συναρτήσεις της πρόσθεσης και του πολλαπλασιασμού και η  $C_<$  είναι η χαρακτηριστική συνάρτηση της σχέσης  $<$  στο  $\mathbb{N}$ ,  $Z : \mathbb{N} \rightarrow \mathbb{N}$ , με  $Z(x) = 0$ , για κάθε  $x$ , και  $\sigma : \mathbb{N} \rightarrow \mathbb{N}$ , με  $\sigma(x) = x + 1$  (η συνάρτηση του επόμενου).

**(R2)**[Αντικατάσταση]. Αν  $G, H_1, \dots, H_k \in \Sigma$  και  $F(\vec{x}) = G(H_1(\vec{x}), \dots, H_k(\vec{x}))$ , τότε  $F \in \Sigma$ .

(R3)[Αναδρομή] Αν  $G, H \in \Sigma$  και  $F$  ορίζεται από τις εξισώσεις

$$\begin{aligned} F(0, \vec{x}) &= G(\vec{x}) \\ F(y+1, \vec{x}) &= H(F(y, \vec{x}), y, \vec{x}) \end{aligned}$$

τότε  $F$  ανήκει στο  $\Sigma$ .

**Ορισμός 6.6** Η κλάση των πρωτογενών αναδρομικών συναρτήσεων είναι η μικρότερη κλάση αριθμητικών συναρτήσεων που είναι κλειστή για τους κανόνες R1, R2 και R3. Δηλαδή είναι η μικρότερη κλάση συναρτήσεων που περιέχει τις βασικές συναρτήσεις και είναι κλειστή για τους κανόνες σχηματισμού συναρτήσεων R2 και R3.

**Παράδειγμα 6.7** Η εκθετική συνάρτηση  $x^y = \text{Exp}(y, x)$  είναι πρωτογενής αναδρομική, διότι

$$\begin{aligned} \text{Exp}(0, x) &= 1 = \sigma(Z(x)) \\ \text{Exp}(y+1, x) &= \text{Exp}(y, x) \cdot x = H(\text{Exp}(y, x), y, x) \end{aligned}$$

όπου  $H(a, b, c, ) = \cdot(I_1^3(a, b, c, ), I_3^3(a, b, c, ))$ .

**Λήμμα 6.8** Έστω η κλάση  $\Sigma$  ικανοποιεί τα R1 και R2 και έστω  $G \in \Sigma$ . Τότε, αν  $x_1, \dots, x_n$  είναι ξεχωριστές μεταβλητές και αν  $z_1, \dots, z_k$  ακολουθία μεταβλητών ώστε  $z_i \in \{x_1, \dots, x_n\}$ , ( $1 \leq i \leq k$ ) και εάν η  $F$  ορίζεται από  $F(x_1, \dots, x_n) = G(z_1, \dots, z_k)$  (είναι δυνατόν να έχουμε και  $k > n$ ), τότε  $F \in \Sigma$ .

**Απόδειξη** Έστω  $z_i = x_{j_i}$  για ( $1 \leq i \leq k$ ). Τότε έχουμε

$$F(x_1, \dots, x_n) = G(I_{j_1}^n(x_1, \dots, x_n), \dots, I_{j_k}^n(x_1, \dots, x_n))$$

□

Το λήμμα μας επιτρέπει, σε ορισμούς συναρτήσεων, για κλάσεις συναρτήσεων που ικανοποιούν τα R1, R2, να ταυτίζουμε, αντιμεταθέτουμε και να προσθέτουμε πλαστές μεταβλητές χωρίς να οδηγούμαστε εκτός της κλάσης  $\Sigma$ . Παραδείγματος χάριν, αν  $G(x_1, x_2, x_3) \in \Sigma$ , τότε όλες οι συναρτήσεις που ορίζονται με  $F_1(x_1, x_2) = G(x_1, x_2, x_1)$ ,  $F_2(x_2, x_1, x_3) = G(x_1, x_2, x_3)$  και  $F_3(x_1, x_2, x_3, x_4) = G(x_1, x_2, x_3)$  ανήκουν στο  $\Sigma$ .

**Ορισμός 6.9** Έστω  $P(\vec{x}, y)$  κατηγορημα και έστω ότι  $\forall \vec{x} \exists y P(\vec{x}, y)$  Τότε

$$\mu y P(\vec{x}, y) = \text{το ελάχιστο } y \text{ τέτοιο ώστε } P(\vec{x}, y).$$

(R4) [Τελεστής ελαχιστοποίησης] Εάν  $G \in \Sigma$  και εάν  $\forall \vec{y} \exists x G(\vec{y}, x) = 0$ . Τότε  $\mu x (G(\vec{y}, x) = 0) \in \Sigma$ .

**Ορισμός 6.10** Η κλάση των αναδρομικών συναρτήσεων είναι η μικρότερη κλάση αριθμητικών συναρτήσεων που είναι κλειστή για του κανόνες  $R1$ ,  $R2$  και  $R4$ . Αν μια συνάρτηση ανήκει στην κλάση αυτή λέμε ότι η συνάρτηση είναι (ολική) αναδρομική συνάρτηση.

**Ορισμός 6.11** Το κατηγορήμα  $P$  είναι αναδρομικό κατηγορήμα αν η χαρακτηριστική συνάρτηση  $C_P$  είναι αναδρομική συνάρτηση. Είναι πρωτογενές αναδρομικό κατηγορήμα αν η  $C_P$  είναι πρωτογενής αναδρομική συνάρτηση.

Στη συνέχεια θα δώσουμε κάποιους κανόνες κατασκευής νέων αναδρομικών συναρτήσεων και κατηγορημάτων.

(C1) Εάν  $Q$  αναδρομικό κατηγορήμα και  $F_1, \dots, F_k$  αναδρομικές συναρτήσεις και εάν  $P(\vec{x}) \leftrightarrow Q(F_1(\vec{x}), \dots, F_k(\vec{x}))$ , τότε το  $P$  είναι αναδρομικό κατηγορήμα.

**Απόδειξη** Επειδή  $C_P(\vec{x}) = C_Q(F_1(\vec{x}), \dots, F_k(\vec{x}))$ . □

(C2) Έστω  $P$  αναδρομικό κατηγορήμα και έστω  $\forall \vec{y} \exists x P(\vec{y}, x)$ . Τότε η συνάρτηση  $F(\vec{y}) = \mu x P(\vec{y}, x)$  είναι αναδρομική.

**Απόδειξη** Επειδή  $F(\vec{y}) = \mu x (C_P(\vec{y}, x)) = 0$ . □

**Ορισμός 6.12** Ο ορισμός μιας συνάρτησης ή ενός κατηγορήματος λέγεται σαφής ορισμός από τα  $F_1, \dots, F_k$  και  $P_1, \dots, P_l$ , εάν ξεκινώντας από αυτά δίνουμε τον ορισμό χρησιμοποιώντας μόνον την αντικατάσταση και τον μ-τελεστή.

**Λήμμα 6.13** Αν  $F_1, \dots, F_k, P_1, \dots, P_l$  αναδρομικά, τότε κάθε ρητός ορισμός από αυτά δίνει αναδρομική συνάρτηση ή κατηγορήμα.

**Απόδειξη** Από τα C1, C2, R2, R4. □

(C3) Κάθε σταθερή συνάρτηση είναι αναδρομική.

**Απόδειξη** Για κάθε  $k \in \mathbb{N}$  έστω  $F_k(\vec{x}) = k$  η σταθερή συνάρτηση  $n$  μεταβλητών. Αποδεικνύουμε ότι κάθε  $F_k$  είναι αναδρομική με επαγωγή στο  $k$ .

$$F_0(\vec{x}) = \mu y (I_{n+1}^{n+1}(\vec{x}, y) = 0).$$

$$F_{k+1}(\vec{x}) = \mu y (F_k(\vec{x}, y) < y).$$

□

**Ορισμός 6.14** Εάν  $P$  και  $Q$  κατηγορήματα, ορίζουμε με προφανή τρόπο τα κατηγορήματα  $\neg P$ ,  $P \rightarrow Q$ ,  $P \vee Q$ ,  $P \wedge Q$  κ.λ.π. που προκύπτουν χρησιμοποιώντας τους λογικούς προτασιακούς συνδέσμους (συνδυασμοί Boole).

(C4) Εάν  $P$  και  $Q$  αναδρομικά τότε όλοι οι συνδυασμοί Boole των  $P$  και  $Q$  είναι αναδρομικά κατηγορήματα.

**Απόδειξη**

$$\begin{aligned} C_{\neg P}(\vec{x}) &= C_{<}(0, C_P(\vec{x})) \\ C_{P \vee Q}(\vec{x}) &= C_P(\vec{x}) \cdot C_Q(\vec{x}) \end{aligned}$$

Τα υπόλοιπα μπορούν να οριστούν συναρτήσσει των  $\neg$  και  $\vee$ , επειδή αυτά αποτελούν επαρκές σύνολο συνδέσμων.  $\square$

(C5) Τα κατηγορήματα  $<$ ,  $\leq$ ,  $>$ ,  $\geq$ ,  $=$  είναι αναδρομικά.

**Απόδειξη** Το  $<$  είναι αναδρομικό, από ορισμό. Για τα υπόλοιπα υπάρχουν οι ακόλουθοι ρητοί ορισμοί.

$$\begin{aligned} x \leq y &\leftrightarrow \neg(y < x) \\ x > y &\leftrightarrow y < x \\ x \geq y &\leftrightarrow y \leq x \\ x = y &\leftrightarrow x \leq y \wedge y \leq x \end{aligned}$$

$\square$

(C6) Η συνάρτηση  $\dot{-}$  που ορίζεται ως κάτωθι

$$x \dot{-} y = \begin{cases} x - y & \text{αν } x \geq y \\ 0 & \text{διαφορετικά, δηλαδή αν } x < y \end{cases}$$

είναι αναδρομική.

**Απόδειξη** Διότι έχει τον ρητό ορισμό,  $\dot{-} = \mu z(y + z = x \vee x < y)$ .  $\square$

**Ορισμός 6.15 (Φραγμένος τελεστής)** Έστω  $P(\vec{y}, x)$  οποιοδήποτε κατηγορήμα. Τότε ορίζουμε τη συνάρτηση  $\mu_{x < z} P(\vec{y}, x)$  ως εξής:

$$\mu_{x < z} P(\vec{y}, x) = \mu x (P(\vec{y}, x) \vee x = z)$$

Ας σημειωθεί ότι η συνάρτηση αυτή είναι πάντα ορισμένη και ότι το  $z$  ανήκει στις μεταβλητές της συνάρτησης. Η τιμή της συνάρτησης είναι το μικρότερο  $x$ , γνησίως μικρότερο του  $z$ , για το οποίο ισχύει  $P(\vec{y}, x)$ , με την προϋπόθεση ότι υπάρχει ένα τέτοιο  $x$ , διαφορετικά η τιμή είναι το  $z$ .

Είναι προφανές ότι αν  $P(\vec{y}, x)$  είναι αναδρομικό τότε η συνάρτηση  $\mu_{x < z} P(\vec{y}, x)$  είναι αναδρομική. Οπότε ισχύει και το παρακάτω.

(C7) Έστω  $P(\vec{y}, x)$  αναδρομικό (το  $x$  είναι διαφορετικό από τα  $\vec{y}$ ) και έστω  $H(\vec{y})$  είναι αναδρομική συνάρτηση. Τότε η συνάρτηση  $F(\vec{y}) = \mu_{x < H(\vec{y})} P(\vec{y}, x)$  είναι αναδρομική.

**Ορισμός 6.16 (Φραγμένοι ποσοδείκτες)** Έστω  $\cdots x \cdots$  μια ιδιότητα, ένα κατηγορήμα, που αναφέρεται στο  $x$ . Τότε οι φραγμένοι ποσοδείκτες ορίζονται ως ακολούθως:

$\exists x_{x < z} \cdots x \cdots \leftrightarrow$  υπάρχει  $x$ , γνησίως μικρότερο του  $z$ , ώστε το  $\cdots x \cdots$  να ισχύει.  
 $\forall x_{x < z} \cdots x \cdots \leftrightarrow$  για κάθε  $x$ , γνησίως μικρότερο του  $z$ , το  $\cdots x \cdots$  ισχύει.

(C8) Έστω  $P(\vec{y}, x)$  αναδρομικό κατηγορήμα (το  $x$  είναι διαφορετικό από τα  $\vec{y}$ ) και έστω  $H(\vec{y})$  αναδρομική συνάρτηση.

Αν το  $Q_1$  ορίζεται μέσω του ορισμού  $Q_1(\vec{y}) \leftrightarrow \exists x_{x < H(\vec{y})} P(\vec{y}, x)$  τότε είναι αναδρομικό διότι έχει τον σαφή ορισμό  $\mu x_{x < H(\vec{y})} (P(\vec{y}, x) < H(\vec{y}))$ .

Αν το  $Q_2$  ορίζεται μέσω του ορισμού  $Q_2(\vec{y}) \leftrightarrow \forall x_{x < H(\vec{y})} P(\vec{y}, x)$  τότε είναι αναδρομικό διότι έχει τον σαφή ορισμό  $\mu x_{x < H(\vec{y})} (\neg P(\vec{y}, x)) = H(\vec{y})$ .

(C9)[Ορισμός με περιπτώσεις] Έστω  $G_1(\vec{x}), \dots, G_k(\vec{x})$  αναδρομικές συναρτήσεις και έστω  $R_1(\vec{x}), \dots, R_k(\vec{x})$  αναδρομικά κατηγορήματα ώστε για κάθε  $\vec{x}$  ένα και μόνον ένα από τα  $R_1(\vec{x}), \dots, R_k(\vec{x})$  ισχύει. Τότε η συνάρτηση  $F$  που ορίζεται ως

$$F(\vec{x}) = \begin{cases} G_1(\vec{x}) & \text{αν } R_1(\vec{x}) \\ G_2(\vec{x}) & \text{αν } R_2(\vec{x}) \\ \vdots & \vdots \\ G_k(\vec{x}) & \text{αν } R_k(\vec{x}) \end{cases}$$

είναι αναδρομική.

**Απόδειξη** Διότι  $F(\vec{x}) = G_1(\vec{x}) \cdot C_{\neg R_1}(\vec{x}) + \cdots + G_k(\vec{x}) \cdot C_{\neg R_k}(\vec{x})$ .  $\square$

Αυτό μας επιτρέπει να δίνουμε αναδρομικούς ορισμούς του τύπου

$$F(\vec{x}) = \begin{cases} G_1(\vec{x}) & \text{αν } R_1(\vec{x}) \\ G_2(\vec{x}) & \text{διαφορετικά} \end{cases}$$

διότι το «διαφορετικά» σημαίνει  $\neg R_1$ . Γενικότερα, και στην περίπτωση του C9 μπορούμε αντί του  $R_k(\vec{x})$  να βάζουμε «διαφορετικά» διότι τότε το  $R_k(\vec{x})$  σημαίνει  $\neg(R_1(\vec{x}) \vee R_2(\vec{x}) \vee \cdots \vee R_{k-1}(\vec{x}))$ .

(C10) Έστω  $P_1(\vec{x}), \dots, P_k(\vec{x})$  αναδρομικά κατηγορήματα και έστω  $R_1(\vec{x}), \dots, R_k(\vec{x})$  αναδρομικά κατηγορήματα ώστε για κάθε  $\vec{x}$  ένα και μόνον ένα από τα  $R_1(\vec{x}), \dots, R_k(\vec{x})$  ισχύει. Τότε το κατηγορήμα  $Q$  που ορίζεται ως

$$Q(\vec{x}) \leftrightarrow \begin{cases} P_1(\vec{x}) & \text{αν } R_1(\vec{x}) \\ P_2(\vec{x}) & \text{αν } R_2(\vec{x}) \\ \vdots & \vdots \\ P_k(\vec{x}) & \text{αν } R_k(\vec{x}) \end{cases}$$

είναι αναδρομικό.

**Λήμμα 6.17** Υπάρχει αναδρομική συνάρτηση  $Pair : \mathbb{N}^2 \rightarrow \mathbb{N}$  η οποία είναι ένα προς ένα (μονομορφισμός).

**Απόδειξη** Ορίζουμε  $Pair(x, y) = (x + y)(x + y) + x + 1$ . Η συνάρτηση είναι προφανώς αναδρομική. Θα αποδείξουμε ότι είναι και ένα προς ένα. Έστω  $Pair(x, y) = Pair(x', y')$ . Θέλουμε  $x = x'$  και  $y = y'$ . Ας υποθέσουμε ότι  $x + y < x' + y'$ . Τότε  $Pair(x, y) = (x + y)^2 + x + 1 \leq (x + y + 1)^2 \leq (x' + y')^2 < Pair(x', y')$ . Άρα θα πρέπει  $x + y = x' + y'$ , εκ του οποίου  $x = x'$  και βέβαια  $y = y'$ .  $\square$

**Λήμμα 6.18 (Η  $\beta$ -συνάρτηση του Gödel.)** Υπάρχει συνάρτηση δύο μεταβλητών  $\beta(x, y)$  τέτοια ώστε:

1.  $\beta(x, y) \leq x - 1$
2. Για κάθε  $n$  και κάθε ακολουθία  $a_0, \dots, a_{n-1}$  υπάρχει  $a$  ώστε  $\beta(a, i) = a_i, \forall i < n$ .

**Απόδειξη** Αργότερα.

Στην συνέχεια θα υποθέσουμε ότι συνάρτηση  $\beta$  υπάρχει. Τότε

$$\begin{aligned}\beta(0, y) &= 0 \\ \beta(x, y) &< x, \quad \forall x > 0.\end{aligned}$$

**Ορισμός 6.19** Για κάθε  $n$  ορίζουμε συνάρτηση  $\langle \dots \rangle : \mathbb{N}^n \rightarrow \mathbb{N}$ , ως εξής:

$$\langle y_0, \dots, y_{n-1} \rangle = \mu x (\beta(x, 0) = n \wedge \beta(x, 1) = y_0 \wedge \dots \wedge \beta(x, n) = y_{n-1})$$

Ο αριθμός  $\langle y_0, \dots, y_{n-1} \rangle$  ονομάζεται αριθμός ακολουθίας της  $n$ -άδας  $y_0, \dots, y_{n-1}$ .

**Λήμμα 6.20** Οι ακόλουθες συναρτήσεις είναι αναδρομικές.

1. Το «μήκος του  $x$ »,  $lh(x) = \beta(x, 0)$ .
2. Η « $i + 1$  συνιστώσα του  $x$ »,  $(x)_i = \beta(x, i + 1)$ .
3. Το κατηγορημα  $Seq(x)$ , όπου  $Seq(x) \leftrightarrow x$  είναι αριθμός ακολουθίας κάποιων  $a_0, \dots, a_{n-1}$ .

**Απόδειξη** του 3: Για κάθε  $x$  και για  $\beta(x, 0) = n = lh(x)$ , ικανοποιείται η εξίσωση

$$\beta(x, 0) = n \wedge \beta(x, 1) = (x)_0 \wedge \dots \wedge \beta(x, n) = (x)_{n-1}. \quad (*)$$

Για να είναι το  $x$  ένας αριθμός ακολουθίας, δηλαδή να είναι  $x = \langle (x)_0, \dots, (x)_{n-1} \rangle$ , θα πρέπει να είναι ο μικρότερος  $x$  που ικανοποιεί την εξίσωση (\*). Άρα μπορούμε να δώσουμε τον ακόλουθο ρητό ορισμό:

$$seq(x) \leftrightarrow \forall y_{y < x} (lh(y) = lh(x) \rightarrow \exists i_{i < lh(x)} ((y)_i \neq (x)_i))$$

□

Έχουμε πάντα  $lh(\langle a_0, \dots, a_{n-1} \rangle) = n$  και  $(\langle a_0, \dots, a_{n-1} \rangle)_i = a_i$  ( $i < n$ ).  
Επιτρέπουμε (για το μήκος της κενής ακολουθίας)  $n = 0$ . Τότε θα έχουμε  $\langle \emptyset \rangle = \langle \ \rangle = 0$ .

Επίσης αν  $a \neq \langle \ \rangle$ , τότε  $lh(a) < a$  και  $(a)_i < a$ .

**Ορισμός 6.21** Ορίζουμε αναδρομική συνάρτηση  $Red(x, y)$  ώστε να έχει την χαρακτηριστική ιδιότητα  $Red(\langle y_0, \dots, y_{n-1} \rangle, i) = \langle y_0, \dots, y_{i-1} \rangle$ ,  $i \leq n$ . Ο ρητός ορισμός είναι

$$Red(x, i) = \mu y (lh(y) = i \wedge \forall j_{j < i} ((y)_j = (x)_j))$$

Σημείωση:  $Seq(x) \wedge lh(x) = n \rightarrow x = \langle (x)_0, \dots, (x)_{n-1} \rangle$

**Ορισμός 6.22** Για κάθε συνάρτηση  $F(y, \vec{x})$  ορίζουμε την  $\bar{F}$ , τη συνάρτηση ιστορίας της  $F$ , ως εξής:

$$\bar{F}(y, \vec{x}) = \langle F(0, \vec{x}), F(1, \vec{x}), \dots, F(y-1, \vec{x}) \rangle$$

Θα είναι  $\bar{F}(0, \vec{x}) = \langle \ \rangle = 0$ .

**Λήμμα 6.23** Η  $F(y, \vec{x})$  είναι αναδρομική αν και μόνο αν η  $\bar{F}(y, \vec{x})$  είναι αναδρομική.

**Απόδειξη**  $\Rightarrow$ :  $\bar{F}(y, \vec{x}) = \mu z (lh(z) = y \wedge \forall i_{i < y} ((z)_i = F(i, \vec{x})))$  (ρητός ορισμός).

$\Leftarrow$ : Η  $F$  έχει το ρητό ορισμό  $F(y, \vec{x}) = (\bar{F}(y+1, \vec{x}))_y$ .

□

**Θεώρημα 6.24** Εάν  $G$  αναδρομική και  $F$  ορίζεται από  $F(y, \vec{x}) = G(\bar{F}(y, \vec{x}), y, \vec{x})$ , τότε  $F$  είναι αναδρομική.

**Απόδειξη** Γράφουμε ένα ρητό ορισμό για τη συνάρτηση  $H$ .

$$H(y, \vec{x}) = \mu z (Seq(z) \wedge lh(z) = y \wedge \forall i_{i < y} ((z)_i = G(Red(z, i), i, \vec{x})))$$

Θα αποδείξουμε ότι η  $H(y, \vec{x})$  ταυτίζεται με την  $\bar{F}(y, \vec{x})$ . Η απόδειξη θα γίνει με επαγωγή. Υποθέτουμε ότι (E.Y.), για κάθε  $i < y$  ισχύει  $\bar{F}(i, \vec{x}) = H(i, \vec{x})$ , δηλαδή  $H(i, \vec{x}) = \langle F(0, \vec{x}), \dots, F(i-1, \vec{x}) \rangle$ . Θα αποδείξουμε ότι τότε  $\bar{F}(y, \vec{x}) = H(y, \vec{x})$ .

Έστω  $\bar{F}(y, \vec{x}) = \langle F(0, \vec{x}), \dots, F(y-1, \vec{x}) \rangle = z$ . Από E.Y.  $Red(z, i) = H(i, \vec{x})$ , για κάθε  $i < y$ . Το  $z$  είναι ο μικρότερος αριθμός ο οποίος είναι αριθμός ακολουθίας, έχει  $lh(z) = y$  και για κάθε  $i < y$  ισχύει ότι  $(z)_i = F(i, \vec{x})$ . Αλλά από τον ορισμό του  $F$ ,  $F(i, \vec{x}) = G(\bar{F}(i, \vec{x}), i, \vec{x})$  και από την E.Y.,  $G(\bar{F}(i, \vec{x}), i, \vec{x}) = G(H(i, \vec{x}), i, \vec{x}) = G(Red(z, i), i, \vec{x})$ , δηλαδή έχουμε  $(z)_i = G(Red(z, i), i, \vec{x})$ , για κάθε  $i < y$ . Αυτό σημαίνει ότι το  $z$  είναι ο μικρότερος αριθμός που ικανοποιεί τις απαιτήσεις του αναδρομικού ορισμού του  $H(y, \vec{x})$  και συνεπώς έχουμε ότι  $z = H(y, \vec{x}) = \bar{F}(y, \vec{x})$ . □

**Πόρισμα 6.25** Η κλάση των αναδρομικών συναρτήσεων είναι κλειστή για το σχήμα  $R3$ , δηλαδή αν  $G$  και  $H$  είναι αναδρομικές, τότε η  $F$  που ορίζεται από

$$\begin{aligned} F(0, \vec{x}) &= G(\vec{x}) \\ F(y+1, \vec{x}) &= H(F(y, \vec{x}), y, \vec{x}) \end{aligned}$$

είναι αναδρομική.

**Απόδειξη** Η  $F$  έχει τον εξής ρητό ορισμό.

$$F(y, \vec{x}) = \begin{cases} G(\vec{x}) & \text{αν } y = 0 \\ H((\bar{F}(y, \vec{x}))_{y-1}, y, \vec{x}) & \text{διαφορετικά} \end{cases}$$

□

**Παράδειγμα 6.26** Η ακολουθία Fibonacci, η  $u_n$ , που ορίζεται ως

$$\begin{aligned} u_0 &= u_1 = 1 \\ u_{n+2} &= u_n + u_{n+1} \end{aligned}$$

είναι αναδρομική συνάρτηση  $F(n) = u_n$ , διότι έχει τον αναδρομικό ορισμό

$$F(x) = \begin{cases} 1 & \text{αν } x = 0 \vee x = 1 \\ (\bar{F}(x))_{x-1} + (\bar{F}(x))_{x-2} & \text{διαφορετικά} \end{cases}$$

Ας υποθέσουμε τώρα ότι  $\mathcal{E}(\bar{C}_P(y, \vec{x}))$  είναι ένας ρητός ορισμός, από το κατηγορήμα  $P$  και από άλλες συναρτήσεις και κατηγορήματα που είναι αναδρομικά. Τότε το κατηγορήμα  $P$ , με ορισμό

$$P(y, \vec{x}) \leftrightarrow \mathcal{E}(\bar{C}_P(y, \vec{x}))$$

είναι αναδρομικό, διότι η χαρακτηριστική του έχει τον αναδρομικό ορισμό

$$C_P(y, \vec{x}) = \begin{cases} 0 & \text{αν } \mathcal{E}(\bar{C}_P(y, \vec{x})) \\ 1 & \text{διαφορετικά} \end{cases}$$

Άρα μπορούμε να ορίσουμε αναδρομικά ένα  $P$  με

$$P(y, \vec{x}) \leftrightarrow \begin{cases} R_1(\vec{x}) & \text{αν } y = 0 \\ R_2(\vec{x}) & \text{αν } y = 0 \wedge P(y-1, \vec{x}) \\ R_3(\vec{x}) & \text{διαφορετικά} \end{cases}$$

διότι  $P(y-1, \vec{x}) \leftrightarrow (\bar{C}_P(y, \vec{x}))_{y-1} = 0$ .

Μπορούμε επίσης να ορίσουμε μια συνάρτηση  $F$  με

$$F(x, y) = \begin{cases} F(H_1(x), y) & \text{αν } H_1(x) < x \\ H_2(x, y) & \text{διαφορετικά} \end{cases}$$

διότι η πρώτη γραμμή του ορισμού μπορεί να αντικατασταθεί με

$(\bar{F}(x, y))_{H_1(x)}$  αν  $H_1(x) < x$ .

**Γενικός κανόνας:** Ο αναδρομικός ορισμός μιας συνάρτησης  $F(y, \bar{x})$  (ή ενός κατηγορήματος) είναι σωστός με την προϋπόθεση ότι, όταν το  $F(w, \bar{x})$  εμφανίζεται στο δεξιό μέρος του ορισμού, μπορούμε να αποδείξουμε ότι  $w < y$ .

Στη συνέχεια θα αποδείξουμε το λήμμα 6.18, δηλαδή την ύπαρξη της συνάρτησης  $\beta$ . Για να διευκολυνθούμε στην απόδειξη, αποδεικνύουμε πρώτα την ύπαρξη μιας, παρόμοιας με τη  $\beta$ , συνάρτησης  $\delta$ .

**Πρόταση 6.27** Υπάρχει αναδρομική συνάρτηση  $\delta(x, y, z)$ , τέτοια ώστε:

1.  $\delta(x, y, z) \leq x$ .
2. Για κάθε  $a_0, \dots, a_{n-1}$ , υπάρχουν αριθμοί  $b$  και  $c$  ώστε  $\delta(b, c, i) = a_i$  για κάθε  $i < n$ .

Πρίν προχωρήσουμε στην απόδειξη του 6.27, θα δείξουμε ότι η ύπαρξη της συνάρτησης  $\delta$  συνεπάγεται την ύπαρξη της συνάρτησης  $\beta$ .

**Πρόταση 6.28** Η ύπαρξη της συνάρτησης  $\delta$  συνεπάγεται την ύπαρξη της συνάρτησης  $\beta$ .

**Απόδειξη** Ισχύει ότι  $x, y < \text{Pair}(x, y)$ . Ορίζουμε αναδρομικές συναρτήσεις  $l$  (αριστερή συνιστώσα) και  $r$  (δεξιά συνιστώσα), ως εξής:

$$\begin{aligned} l(x) &= \mu y_{y < x} \exists z_{z < x} (x = \text{Pair}(y, z)) \\ r(x) &= \mu y_{y < x} \exists z_{z < x} (x = \text{Pair}(z, y)) \end{aligned}$$

Ορίζουμε την αναδρομική συνάρτηση  $\beta$  ως ακολούθως:

$$\beta(x, i) = \begin{cases} \delta(l(x), r(x), i) & \text{αν } x = \text{Pair}(l(x), r(x)) \\ 0 & \text{διαφορετικά} \end{cases}$$

Είναι φανερό ότι  $\beta(x, i) = \delta(l(x), r(x), i) \leq l(x) < x$ , εάν  $x = \text{Pair}(l(x), r(x))$  (δηλαδή εάν το  $x$  ανήκει στο πεδίο τιμών της  $\text{Pair}$ ). Άρα, επειδή σε κάθε άλλη περίπτωση η τιμή είναι μηδέν, θα έχουμε πάντα  $\beta(x, i) \leq x - 1$ .

Έστω τώρα, δοθέντων των  $a_0, \dots, a_{n-1}$ , τα  $b$  και  $c$  έχουν βρεθεί ώστε  $\delta(b, c, i) = a_i$ ,  $\forall i < n$ . Τότε εάν  $a = \text{Pair}(b, c)$  θα έχουμε ότι  $\beta(a, i) = \delta(l(a), r(a), i) = a_i$ , για κάθε  $i < n$ . Άρα η  $\beta$  θα ικανοποιεί τις απαιτήσεις του ορισμού της στο λήμμα 6.18. □

Για να αποδείξουμε την ύπαρξη της συνάρτησης  $\delta$  θα χρειαστούμε τα ακόλουθα δύο λήμματα.

**Λήμμα 6.29 (Κινέζικο θεώρημα υπολοίπων)** Έστω  $d_0, \dots, d_{n-1}$  αριθμοί ανά δύο πρώτοι (προς αλλήλους) και έστω  $a_0, \dots, a_{n-1}$  τέτοια ώστε  $a_i < d_i, \forall i < n$ . Τότε υπάρχει  $b$  ώστε  $a_i = b \bmod d_i$ , για κάθε  $i < n$ : το  $x \bmod y$  συμβολίζει το υπόλοιπο της διαίρεσης του  $x$  από το  $y$ , άρα έχουμε και  $x \bmod y < y$ .

**Απόδειξη** Έστω  $q = \prod_{i < n} d_i = d_0 \cdot d_1 \cdots d_{n-1}$ . Επειδή τα  $d_i$  είναι ανά δύο πρώτα, το  $q$  είναι ο μικρότερος αριθμός που διαιρείται από όλα τα  $d_i$ . Έστω τώρα  $x$  τυχών αριθμός. Ορίζουμε  $[x] = \langle x \bmod d_0, \dots, x \bmod d_{n-1} \rangle$  να είναι η  $n$ -άδα των υπολοίπων της διαίρεσης του  $x$  από τα  $d_0, \dots, d_{n-1}$ . Το μέγιστο δυνατό πλήθος αυτών των  $n$ -άδων είναι  $d_i = d_0 \cdot d_1 \cdots d_{n-1}$ , δηλαδή  $q$ . Έστω τώρα  $x, y < q$  με  $x \neq y$ . Τότε  $[x] \neq [y]$ , διότι αν  $\langle x \bmod d_0, \dots, x \bmod d_{n-1} \rangle = \langle y \bmod d_0, \dots, y \bmod d_{n-1} \rangle$  τότε θα είχαμε ότι  $d_i \mid |x - y|$ , για κάθε  $i < n$ . Επειδή  $|x - y| < q$ , αυτό είναι δυνατό μόνον αν  $x = y$ . Άρα το  $[x]$  παίρνει όλες τις δυνατές τιμές όταν το  $x$  κινείται στα  $0, 1, \dots, q - 1$ . Άρα αν πάρουμε μια  $n$ -άδα  $a_0, \dots, a_{n-1}$  με  $a_i < d_i$ , τότε θα υπάρχει  $b$  ώστε  $[b] = \langle a_0, \dots, a_{n-1} \rangle$ .  $\square$

**Λήμμα 6.30** Για κάθε αριθμό  $n$ , οι  $n + 1$  αριθμοί

$$1 + n!, 1 + 2(n!), 1 + 3(n!), \dots, 1 + (n + 1)(n!)$$

είναι ανά δύο πρώτοι προς αλλήλους

**Απόδειξη** Έστω ότι υπάρχουν  $i, j \in \{1, \dots, (n + 1)\}$  τέτοια ώστε  $1 + i(n!)$  και  $1 + j(n!)$  έχουν κοινό παράγοντα, έστω τον πρώτο αριθμό  $p$ . Τότε ο  $p$  διαιρεί τον  $|i - j| \cdot n!$ . Επειδή  $p \nmid n!$  (διότι τότε θα διαιρούσε και το 1) έχουμε ότι  $p \mid |i - j|$ . Αλλά  $|i - j| \leq n < p$ , ( $n < p$  διότι  $p \nmid n!$ ). Άρα  $p \mid |i - j|$  μόνο στην περίπτωση  $i = j$ .  $\square$

**Απόδειξη** της πρότασης 6.27.

Ορίζουμε τη  $\delta$  ως εξής:

$$\delta(x, y, z) = x \bmod (1 + (z + 1)y).$$

Η  $\delta$  είναι αναδρομική διότι έχει τον ακόλουθο αναδρομικό ορισμό

$$\delta(x, y, z) = \mu w (\exists t_{t < x+1} (x = t(1 + (z + 1)y) + w)).$$

Έστω τώρα  $a_0, \dots, a_{k-1}$  αριθμοί και έστω  $n = \max\{a_1, \dots, a_k, k\}$ . Παίρνουμε  $c = n!$ . Τότε από το λήμμα 6.30 οι αριθμοί  $1 + (i + 1) \cdot c$ , για όλα τα  $i \leq n$ , είναι ανά δύο πρώτοι προς αλλήλους.

Από λήμμα 6.29 (θέτοντας  $d_i = 1 + (i + 1)c$ ), υπάρχει  $b$  τέτοιο ώστε  $a_i = b \bmod (1 + (i + 1)c)$ , για κάθε  $i < n$ . Δηλαδή  $\delta(d, c, i) = a_i, \forall i < n$ .