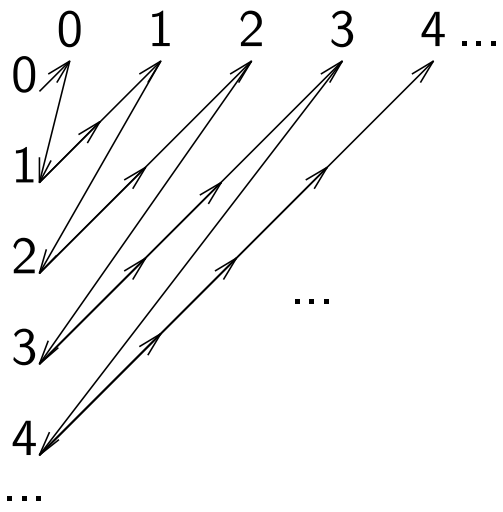
Απαρίθμηση ζευγών φυσικών αριθμών Ι



- $C(0,0) = 0$
- $C(2,1) = 7$ κωδικοποίηση κατά Cantor
- $D_1(7)$=2, $D_2(7)$=1 : αποκωδικοποίηση
- $C(m,n) = \frac{(n+m)(n+m+1)}{2} + m$, η C είναι 1-1 και επί.

Απαρίθμηση ζευγών φυσικών αριθμών II

Ορισμός

Μια **συνάρτηση σύζευξης** (pairing function) C είναι μια τεχνική αρίθμησης ζευγών για την οποία υπάρχουν οι αντίστροφες συναρτήσεις (D_1, D_2) που ικανοποιούν τις εξής συνθήκες για κάθε n, m, k:

$$D_1(C(n,m)) = n, \quad D_2(C(n,m)) = m, \quad C(D_1(k), D_2(k)) = k$$

Απαρίθμηση n-άδων φυσικών αριθμών

- $C^2 \equiv C$, $D_i^2 \equiv D_i$
- $C^3(a,b,c) = C^2(a, C^2(b,c))$
- $D_1^3(z) = D_1^2(z)$, $D_2^3(z) = D_1^2(D_2^2(z))$, $D_3^3(z) = D_2^2(D_2^2(z))$, κ.ο.κ.

και γενικά για $n \geqslant 3$:

$$C^n(a_1, a_2, \ldots, a_n) = C^2(a_1, C^{n-1}(a_2, \ldots, a_n))$$
$$D_1^n(z) = D_1^2(z) \quad \text{και για } i > 1 : D_i^n(z) = D_{i-1}^{n-1}(D_2^2(z))$$

Για κωδικοποίηση πεπερασμένων ακολουθιών:

$$C^{\mathrm{f}}(a_1, a_2, \ldots, a_n) = C^{n+1}(n, a_1, a_2, \ldots, a_n) \quad \text{κ.ο.κ.}$$

όπου n είναι το μήκος.

Gödelization (Γκεντελοποίηση)

Μέθοδος κωδικοποίησης κατα Gödel που βασίζεται στο *unique factorization property* των φυσικών αριθμών:

Παράδειγμα

$G(4,8,3) = 2^{4+1} \cdot 3^{8+1} \cdot 5^{3+1}$
$G(2,0) = 2^{2+1} \cdot 3^{1}$

Και γενικά:

$$G(a_0, \ldots, a_n) = p_0^{a_0+1} \ldots p_n^{a_n+1}$$

Παρατήρηση: Η παραπάνω κωδικοποίηση καθώς και η αποκωδικοποίηση μπορούν να γίνουν με προγράμματα LOOP.

Πρώτοι αριθμοί Ι

Ορισμός

Πρώτος αριθμός λέγεται ένας ακέραιος μεγαλύτερος του 1 που δεν έχει άλλους διαιρέτες εκτός από το 1 και τον εαυτό του, ειδάλλως λέγεται σύνθετος.

Πρόταση

Κάθε ακέραιος μεγαλύτερος του 1 είναι είτε πρώτος είτε γινόμενο πρώτων αριθμών.

Θεώρημα (Ευκλείδη)

Οι πρώτοι είναι άπειροι σε πλήθος.

Απόδειξη.

Έστω ότι οι πρώτοι είναι πεπερασμένοι σε πλήθος—συγκεκριμένα $p_1, p_2, \ldots, p_n$—τότε ο αριθμός $p_1 p_2 \ldots p_n + 1$ δε διαιρείται από κανένα πρώτο εκ τών $p_1, p_2 \ldots p_n$, άρα είναι πρώτος ή διαιρείται με άλλο πρώτο, κάτι που είναι άτοπο. □

Πρώτοι αριθμοί II

Θεώρημα (Θεμελιώδες Θεώρημα Αριθμητικής)

Κάθε αριθμός μπορεί να γραφεί με μοναδικό τρόπο σε γινόμενο πρώτων αριθμών (όχι απαραίτητα διαφορετικών ανά δύο).

Θεώρημα (Θεώρημα Τεσσάρων τετραγώνων του Lagrange)

Κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως άθροισμα τεσσάρων τετραγώνων.

Εικασία (Εικασία του Goldbach)

Κάθε άρτιος φυσικός μεγαλύτερος του δύο μπορεί να αναπαρασταθεί ως το άθροισμα δύο πρώτων.

Ορισμός

Αν ο p είναι πρώτος και ο $p+2$ είναι επίσης πρώτος τότε αυτοί λέγονται δίδυμοι πρώτοι.

Πρώτοι αριθμοί III

Εικασία (Εικασία των Διδύμων Πρώτων)

Υπάρχουν άπειρα το πλήθος ζευγάρια διδύμων πρώτων.

Θεώρημα (Θεώρημα Πρώτων Αριθμών (de la Valee Poussin, Hadamard))

Αν με $\pi(x)$ συμβολίσουμε το πλήθος των πρώτων αριθμών μικρότερων ή ίσων του x, τότε

$$\pi(x) \xrightarrow[x\to\infty]{} \frac{x}{\log x}$$

Θεώρημα (Vinogradov)

Υπάρχει ακέραιος N ώστε κάθε n περιττός αριθμός μεγαλύτερος του N γράφεται σαν άθροισμα τριών πρώτων αριθμών. Η καλύτερη γνωστή τιμή του N είναι $N = 3,33 \times 10^{43000}$.

Πρώτοι αριθμοί IV

Πόρισμα

Κάθε αριθμός μεγαλύτερος από την παραπάνω σταθερά μπορεί να γραφτεί ως άθροισμα τεσσάρων πρώτων.

Θεώρημα (Chen)

Υπάρχει ακέραιος N ώστε κάθε n άρτιος αριθμός μεγαλύτερος του N γράφεται σαν άθροισμα ενός πρώτου και ενός γινομένου το πολύ δύο πρώτων αριθμών.

Παρατήρηση: Πρόσφατα(2002) οι Saxena, Kayal και Agrawal απέδειξαν ότι το πρόβλημα PRIMES είναι στο P.

Άλλη μια συνάρτηση κωδικοποίησης

Παρακάτω περιγράφουμε μια ακόμη συνάρτηση σύζευξης, C:

$$C(n,m) = 2^n * (2m+1) - 1$$

Υπάρχει προφανώς πρόγραμμα loop που να υπολογίζει τη $C(n,m)$.

Ως προς τις αντίστροφες συναρτήσεις D_1, D_2, αν k είναι ένας φυσικός αριθμός, αποδεικνύεται ότι υπάρχει μοναδικό ζεύγος $n = D_1(k)$, $m = D_2(k)$, ώστε: $C(m,n) = k$.

Σημασιολογία προγραμμάτων LOOP

Program semantics (σημασιολογία): **specifications**, **formal verification**.

Υπάρχουν τρεις μαθηματικοί τρόποι να μιλήσουμε για σημασιολογία:

- **Operational semantics** (λειτουργική σημασιολογία)
- **Denotational semantics** (δηλωτική σημασιολογία)
- **Axiomatic semantics** (αξιωματική σημασιολογία)

Σημασιολογία προγραμμάτων LOOP

Λειτουργική σημασιολογία

Ορισμοί

- LOOP_n: το σύνολο των LOOP προγραμμάτων με μεταβλητές εκ των $x_1, x_2, \ldots, x_n$.
- **Configuration** είναι ένα στοιχείο του $\mathbb{N}^n$,συγκεκριμένα οι τιμές των μεταβλητών $x_1, x_2, \ldots, x_n$.
- **Computation** είναι ένα στοιχείο του $(\mathbb{N}^n)^*$: συγκεκριμένα μια ακολουθία από διαδοχικές διαμορφώσεις.

Ορισμός (Λειτουργική σημασιολογία)

$$S_o : \mathrm{LOOP}_n \times \mathbb{N}^n \to (\mathbb{N}^n)^*$$

(η S_o μπορεί να οριστεί με πρωταρχική αναδρομή)

Σημασιολογία προγραμμάτων LOOP

Δηλωτική σημασιολογία

Ορισμός (Δηλωτική σημασιολογία)

$$S_{\mathrm{d}} : \mathsf{LOOP}_n \times \mathbb{N}^n \to \mathbb{N}^n$$

Σημασιολογία προγραμμάτων LOOP

Αξιωματική σημασιολογία

Assertions, Invariants

Παράδειγμα 1:
(1) x:=y; (2) **for** w:=1 **to** z **do** (3) x:=succ x (4) **end** (5)

1. $y = a_1 \wedge z = a_2$. Βεβαίωση εισόδου.
2. $y = a_1 \wedge z = a_2 \wedge x = a_1$.
3. $y = a_1 \wedge z = a_2 \wedge x = a_1 + w - 1 \wedge w \leqslant a_2$. Αναλλοίωτη βρόχου.
4. $y = a_1 \wedge z = a_2 \wedge x = a_1 + w$.
5. $y = a_1 \wedge z = a_2 \wedge x = a_1 + a_2$. Βεβαίωση εξόδου.

Σημασιολογία προγραμμάτων LOOP

Αξιωματική σημασιολογία

Παράδειγμα 2 (Pascal):
(1) z:=0; u:=x; (2) **repeat** (3) z:=z+y (4) u:=u-1 (5) **until** u=0 (6)

Βεβαιώσεις:

1. $x > 0 \wedge y > 0$. Βεβαίωση εισόδου.
2. $z = 0 \wedge u = x \wedge x > 0 \wedge y > 0$.
3. $z + u * y = x * y \wedge u > 0$. Αναλλοίωτη βρόχου.
4. $(z - y) + u * y = x * y \wedge u > 0$.
5. $(z - y) + (u + 1) * y = x * y \wedge u \geqslant 0$.
6. $z + u * y = x * y \wedge u \geqslant 0$ (δηλαδή $z = x * y \wedge u = 0$). Βεβαίωση εξόδου.

u: **συνθήκη τερματισμού** (termination condition) μια γνησίως φθίνουσα συνάρτηση που εγγυάται τον τερματισμό όταν $u = 0$.

LOOP-υπολογισιμότητα

Ορισμός

Μια συνάρτηση $f\colon \mathbb{N}^n \to \mathbb{N}$ λέγεται **LOOP-υπολογίσιμη** (LOOP-computable) εάν υπάρχει ένα LOOP_{n+m} πρόγραμμα

$$\pi(x_1, \ldots, x_n, \ldots, x_{n+m})$$

και ένα $i \leqslant m + n$ έτσι ώστε για κάθε $a_1, a_2, \ldots, a_n \in \mathbb{N}$:

$$f(a_1, a_2, \ldots, a_n) = S_{d,i}(\pi)[a_1, \ldots, a_n, 0, \ldots, 0]\,.$$

Πρωταρχικές αναδρομικές συναρτήσεις Ι

Ορισμός

Η κλάση $\mathcal{P}$ των **πρωταρχικών αναδρομικών** συναρτήσεων είναι η μικρότερη κλάση συναρτήσεων που:

1. περιέχει τις εξής **αρχικές συναρτήσεις**: S, P, Z, U_i^n (για όλα τα n και $i \leqslant n$) και
2. είναι κλειστή ως προς τα σχήματα της **σύνθεσης** και της **πρωταρχικής αναδρομής**.

Πρωταρχικές αναδρομικές συναρτήσεις II

Εξηγήσεις:
$S(x) = x + 1$, $P(x + 1) = x$, $P(0) = 0$, $Z(x) = 0$,
$U_i^n(x_1, x_2, \ldots, x_n) = x_i$, $1 \leqslant i \leqslant n$

Σύνθεση: $f(x) = h(g(x))$
γενικά $f(x_1, x_2, \ldots, x_n) = h(g_1(x_1, x_2, \ldots, x_n), \ldots, g_m(x_1, x_2, \ldots, x_n))$

Πρωταρχική Αναδρομή: $\begin{cases} f(0) = C \\ f(Sy) = h(y, f(y)) \end{cases}$

Γενικά:

$$\begin{cases} f(x_1, x_2, \ldots, x_n, 0) = g(x_1, x_2, \ldots, x_n) \\ f(x_1, x_2, \ldots, x_n, Sy) = h(x_1, x_2, \ldots, x_n, y, f(x_1, x_2, \ldots, x_n, y)) \end{cases}$$

Πρωταρχικές αναδρομικές συναρτήσεις III

Παραδείγματα:

1. $\begin{cases} add(x,0) = U_1^1(x) \\ add(x,Sy) = h(x,y,add(x,y)) \end{cases}$ όπου $h(x,y,z) = S(U_3^3(x,y,z))$
2. $\begin{cases} mult(x,0) = Z(x) \\ mult(x,Sy) = h(x,y,mult(x,y)) \end{cases}$
   όπου $h(x,y,z) = add(U_1^3(x,y,z), U_3^3(x,y,z))$
3. $mult2(x) = mult(S(S(Z(x))), U_1^1(x))$
4. $\begin{cases} pow2(0) = 1 \\ pow2(Sy) = h(y,pow2(y)) \end{cases}$ όπου $h(y,z) = mult2(U_2^2(y,z))$
5. Αν η $g(x,y)$ είναι πρωταρχικά αναδρομική, τότε είναι και η f:
   $f(x) = g(x,x) = g(U_1^1(x), U_1^1(x))$ (ταυτοποίηση ορισμάτων)
6. Αν η $g(x,y)$ είναι πρωταρχικά αναδρομική, τότε είναι και η f:
   $f(x,y) = g(y,x) = g(U_2^2(x,y), U_1^2(x,y))$ (εναλλαγή ορισμάτων)
7. $abs(x-y) = (x \dot{-} y) + (y \dot{-} x)$

Πρωταρχικές αναδρομικές συναρτήσεις IV

8. προσημοσυναρτήσεις $(sg, \overline{sg})$
9. $eq(x, y) = \overline{sg}(abs(x - y))$

Παρατήρηση

Οι sg, $\overline{sg}$ και eq είναι χαρακτηριστικές συναρτήσεις.

Ορισμός

Μια σχέση $R \subseteq \mathbb{N}^n$ είναι πρωταρχική αναδρομική, αν η χαρακτηριστική συνάρτηση χ_R είναι πρωταρχική αναδρομική, όπου

$$\chi_R(x_1, \ldots, x_n) = \begin{cases} 1, & \text{αν } (x_1, \ldots, x_n) \in R \\ 0, & \text{αλλιώς} \end{cases}$$

Άλλα είδη αναδρομής Ι

Ακολουθία Fibbonaci:

$$\begin{cases} f(0) = 1 \\ f(1) = 1 \\ f(SSn) = f(n) + f(Sn) \end{cases}$$

Αυτό το σχήμα είναι αναδρομή αλλά δεν είναι πρωταρχική αναδρομή!

Αμοιβαία (Mutual) Πρωταρχική Αναδρομή

$$\begin{cases} f_1(0) = 1 \\ f_1(Sn) = f_1(n) + f_2(n) \end{cases} \qquad \begin{cases} f_2(0) = 0 \\ f_2(Sn) = f_1(n) \end{cases}$$

$$f_1 : 1, 1, 2, 3, 5, 8, \ldots \qquad f_2 : 0, 1, 1, 2, 3, 5, \ldots$$

Άλλα είδη αναδρομής II

Γενικά: για $j = 1, \ldots, m$:

$$\begin{cases} f_j(x_1, x_2, \ldots, x_n, 0) & = g_j(x_1, \ldots, x_n) \\ f_j(x_1, x_2, \ldots, x_n, Sy) & = h_j(x_1, \ldots, x_n, y, f_1(x_1, x_2, \ldots, x_n, y), \ldots \\ & \qquad , f_m(x_1, x_2, \ldots, x_n, y)) \end{cases}$$

Λήμμα

Αν όλες οι συναρτήσεις g_j και h_j είναι πρωταρχικές αναδρομικές, τότε και οι συναρτήσεις f_j, όπως ορίζονται από το παραπάνω σχήμα, είναι επίσης πρωταρχικές αναδρομικές.

Άλλα είδη αναδρομής III

Απόδειξη.

Χρησιμοποιούμε κωδικοποίηση και αποκωδικοποίηση κατά (π.χ.) Cantor. Σημειωτέον ότι αυτές (C^m και D_i^m) είναι πρωταρχικές αναδρομικές.

$$\begin{cases} f(x_1, x_2, \ldots, x_n, 0) = C^m(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) \\ f(x_1, x_2, \ldots, x_n, Sy) = \\ \quad C^m(h_1[x_1, \ldots, x_n, y, D_1^m(f(x_1, x_2, \ldots, x_n, y)), \ldots, D_m^m(f(x_1, x_2, \ldots, x_n, y))], \\ \quad \ldots, h_m[x_1, \ldots, x_n, y, D_1^m(f(x_1, x_2, \ldots, x_n, y)), \ldots, D_m^m(f(x_1, x_2, \ldots, x_n, y))]) \end{cases}$$

Η f ορίζεται με πρωταρχική αναδρομή, είναι άρα πρωταρχική αναδρομική. $f_j(x_1, x_2, \ldots, x_n, y) = D_j^m(f(x_1, x_2, \ldots, x_n, y))$ και συνεπώς και οι συναρτήσεις f_j είναι επίσης πρωταρχικές αναδρομικές. □

Ισοδυναμία πρωταρχικών αναδρομικών και LOOP συναρτήσεων Ι

Θεώρημα

Κάθε πρωταρχική αναδρομική συνάρτηση είναι LOOP-υπολογίσιμη.

Απόδειξη: Με επαγωγή στη δομή της συνεπαγωγικής ακολουθίας των πρωταρχικών αναδρομικών συναρτήσεων.

Παρατήρηση

Η επαγωγική απόδειξη ιδιότητας σε επαγωγικό πεδίο συνεπάγεται:

1. απόδειξη της ιδιότητας για τα αρχικά στοιχεία
2. απόδειξη της ιδιότητας για "νέα" στοιχεία που δημιουργούνται με πράξεις κλεισίματος και με "παλιά" στοιχεία για τα οποία υποθέτουμε ότι *έχουν* την ιδιότητα.

Ισοδυναμία πρωταρχικών αναδρομικών και LOOP συναρτήσεων II

1. **Αρχικές συναρτήσεις**

αρχικές συναρτήσεις	Loop-πρόγραμμα	μεταβλητή εξόδου
S	$x := \text{succ } x$	x
P	$x := \text{pred } x$	x
Z	$x := 0$	x
U_i^n	κενό πρόγραμμα	x_i

2. **Σχήματα κλεισίματος**
   1. **Σύνθεση**: Έστω ότι δίνονται τα $m+1$ προγράμματα για:
      - $y_1 := g_1(x_1, x_2, \ldots, x_n)$
      - $\ldots$
      - $y_m := g_m(x_1, x_2, \ldots, x_n)$ και
      - $z := h(y_1, y_2, \ldots, y_n)$.

      Τότε η f που ορίζεται με σύνθεση από τις g_1, g_2, ..., g_m και h, με το σχήμα δηλαδή:

      $$f(x_1, x_2, \ldots, x_n) = h(g_1(x_1, x_2, \ldots, x_n), \ldots, g_m(x_1, x_2, \ldots, x_n))$$

      μπορεί να υπολογιστεί με το εξής πρόγραμμα:
      "$y_1 := g_1(x_1, x_2, \ldots, x_n)$"; $\ldots$; "$y_m := g_m(x_1, x_2, \ldots, x_n)$"; "$z := h(y_1, y_2, \ldots, y_m)$"

Ισοδυναμία πρωταρχικών αναδρομικών και LOOP συναρτήσεων III

2. **Πρωταρχική Αναδρομή**: Έστω ότι δίνονται προγράμματα για "$y := g(x_1, \ldots, x_n)$" και "$y := h(x_1, \ldots, x_n, u, y)$".
   Τότε η f που ορίζεται με πρωταρχική αναδρομή από τις συναρτήσεις g και h, με το σχήμα δηλαδή:

$$\begin{cases} f(x_1, x_2, \ldots, x_n, 0) = g(x_1, \ldots, x_n) \\ f(x_1, x_2, \ldots, x_n, Sy) = h(x_1, \ldots, x_n, y, f(x_1, x_2, \ldots, x_n, y)) \end{cases}$$

   μπορεί να υπολογιστεί με το εξής πρόγραμμα:
   $z := x_{n+1}$; "$y := g(x_1, x_2, \ldots, x_n)$"; **for** $u := 1$ **to** z **do** "$y := h(x_1, x_2, \ldots, x_n, u - 1, y)$" **end**

Ισοδυναμία πρωταρχικών αναδρομικών και LOOP συναρτήσεων Ι

Θεώρημα

Κάθε LOOP-υπολογίσιμη συνάρτηση είναι πρωταρχική αναδρομική.

Απόδειξη: Με επαγωγή στη δομή των προγραμμάτων LOOP:

1. **Αρχικά προγράμματα (αναθέσεις)**

Αρχικό πρόγρ. (αναθέσεις)	Πρωτ. Αναδρ. Συναρτ.
$y := x_i$ (μετ. εξόδου y)	$U_i^n(x_1, x_2, \ldots, x_n)$
$y := \mathrm{succ}\, x_i$	$S(U_i^n(x_1, x_2, \ldots, x_n))$
$y := \mathrm{pred}\, x_i$	$P(U_i^n(x_1, x_2, \ldots, x_n))$
$y := 0$	$Z(U_i^n(x_1, x_2, \ldots, x_n))$
κενό π (μετ. εξόδου x_j)	$U_j^n(x_1, x_2, \ldots, x_n)$

Ισοδυναμία πρωταρχικών αναδρομικών και LOOP συναρτήσεων II

2. **Δομές Ελέγχου ροής προγράμματος**
   1. **Παράθεση (;):** Έστω ότι το π_1 υπολογίζει τις πρωταρχικές αναδρομικές συναρτήσεις g_1 (μεταβλητή εξόδου: x_1), g_2 (μεταβλητή εξόδου: x_2), ..., g_n (μεταβλητή εξόδου: x_n) και ότι το π_2 υπολογίζει την πρωταρχική αναδρομική συνάρτηση h (μεταβλητή εξόδου: x_j). Τότε το πρόγραμμα $\pi_1; \pi_2$ υπολογίζει:
   $$h_j(g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n)$$
   που είναι πρωταρχική αναδρομική λόγω του κλεισίματος ως προς σύνθεση συναρτήσεων.
   2. **βρόχος for:** Έστω ότι το π υπολογίζει τις πρωταρχικές αναδρομικές συναρτήσεις h_1 (μεταβλητή εξόδου: x_1), h_2 (μεταβλητή εξόδου: x_2), ..., h_n (μεταβλητή εξόδου: x_n) και χωρίς βλάβη της γενικότητας ας υποθέσουμε ότι ούτε η μεταβλητή ελέγχου w ούτε το άνω όριο z δεν εμφανίζονται στο π (αλλιώς μετατρέψτε το π σε ισοδύναμο· δες εξήγηση παρακάτω).
   Τότε το πρόγραμμα **for** $w := 1$ **to** z **do** π **end** υπολογίζει τις συναρτήσεις f_j $(1 \leqslant j \leqslant n)$:
   $$\begin{cases} f_j(x_1, x_2, \ldots, x_n, 0) = U_j^n(x_1, \ldots, x_n) \\ f_j(x_1, x_2, \ldots, x_n, Sz) = h_j(f_1(x_1, \ldots, x_n, z), \ldots, f_n(x_1, x_2, \ldots, x_n, z)) \end{cases}$$
   που είναι πρωταρχικές αναδρομές λόγω του κλεισίματος ως προς αμοιβαία πρωταρχική αναδρομή.

Ισοδυναμία πρωταρχικών αναδρομικών και LOOP συναρτήσεων III

Εξήγηση: Αν η μεταβλητή ελέγχου (έστω x_k) και το άνω όριο (έστω x_m) εμφανίζονται στο π, μετατρέπουμε το πρόγραμμα **for** $x_k := 1$ **to** x_m **do** π **end** στο ακόλουθο ισοδύναμο πρόγραμμα π' (ισοδύναμο πρόγραμμα ως προς τις μεταβλητές x_1, x_2, ..., x_n, του π): $x_k := 1$; $z := x_m$; **for** $w := 1$ **to** z **do** (* w, z νέες μεταβλητές *) π; $x_k := x_k + 1$ end
Βασιζόμενοι τώρα στις προηγούμενες αποδείξεις για την παράθεση προγραμμάτων και το βρόχο **for**, μπορούμε εύκολα να δείξουμε ότι κάθε μια από τις f_j $(1 \leqslant j \leqslant n)$ τις οποίες υπολογίζει το π' είναι πρωταρχική αναδρομή. Επομένως, και κάθε f_j του ισοδύναμου προγράμματος **for** $x_k := 1$ **to** x_m **do** π **end** είναι πρωταρχική αναδρομική.

Σταθερά σημεία Ι

Ορισμοί

$M^k = \underbrace{M \times \cdots \times M}_{k \text{ φορές}}$

N^M: *σύνολο των ολικών συναρτήσεων* από το M στο N.

χ: *χαρακτηριστική συνάρτηση* στο M: $\chi : M \to \{0, 1\}$

χ_S: *χαρακτηριστική συνάρτηση συνόλου* $S \subseteq M$: $\chi_S(a) = \begin{cases} 1, & a \in S \\ 0, & \text{αλλιώς} \end{cases}$

Το σύνολο των χαρακτηριστικών συναρτήσεων στο M είναι ισομορφικό του δυναμοσυνόλου του M ($\{0, 1\}^M \cong \mathrm{Pow}(M)$).

Ορισμός

Αν $\underline{M}, \underline{N}$ αλγεβρικές δομές τότε μία συνάρτηση $f : \underline{M} \to \underline{N}$ ονομάζεται **ομομορφισμός** όταν είναι 1-1 και συμβατή με τις πράξεις.

Ορισμός

Ένας **ισομορφισμός** είναι μία συνάρτηση με τις ιδιότητες: 1-1, επί, ομομορφισμού. (Επίσης ονομάζεται και *αντιστοιχία*.)

Σταθερά σημεία II

Λήμμα (Επανάληψης)

Έστω $a \in \mathbb{N}$ *και* $g\colon \mathbb{N} \to \mathbb{N}$.
Υπάρχει ακριβώς μία συνάρτηση $f\colon \mathbb{N} \to \mathbb{N}$ *τέτοια ώστε:*

$$\begin{array}{ll} \textit{Σχήμα Επανάληψης} & \begin{cases} f(0) & = a \\ f(Sx) & = g(f(x)) \end{cases} \\ \textit{(Scheme of Iteration)} & \end{array} \qquad (*)$$

Απόδειξη.

Χρησιμοποιώντας επαγωγή κατασκευάζουμε διαδοχικά συναρτήσεις f_0, f_1, ..., f_i, ... με $\mathrm{dom}(f_i) = \{0, 1, \ldots, i\}$, τέτοια ώστε $f_i(0) = a$ και $f_i(n+1) = g(f_i(n))$, για κάθε $n < i$.
Όλες οι f_i έχουν τις ίδιες τιμές στο κοινό πεδίο ορισμού τους (συμβολισμός $f_0 \sqsubseteq f_1 \sqsubseteq f_2 \sqsubseteq \ldots$).
Ορίζουμε: $f(n) = f_n(n)$, $\forall n \in \mathbb{N}$. Η f ικανοποιεί την $(*)$, άρα αποδείξαμε την ύπαρξη.
Έστω τώρα f' άλλη λύση της $(*)$. Η f' περιορισμένη σε οποιοδήποτε $\{0, 1, \ldots, n\}$ πρέπει να έχει τις ίδιες τιμές με την f_n. Επομένως, $f'(n) = f_n(n) = f(n)$, για κάθε $n \in \mathbb{N}$, άρα αποδείξαμε και την μοναδικότητα. □

Σταθερά σημεία III

Ας δούμε την παραπάνω απόδειξη συνολοθεωρητικά. Μία συνάρτηση είναι ένα σύνολο ζευγών: $F = \{(x, y) \mid y = f(x)\} \subseteq \mathbb{N} \times \mathbb{N}$. Τότε το $(*)$ γίνεται

$$F = \{(0, a)\} \cup \{(x + 1, y) \mid \exists z\colon y = g(z) \wedge (x, z) \in F\}.$$

Το δεξιό μέλος το συμβολίζουμε με $\tau_0(F)$. Ο τελεστής τ_0 είναι το σχήμα ορισμού.

Ο ισχυρισμός του λήμματος επανάληψης είναι ο εξής: $F = \tau_0(F)$, δηλαδή το τ_0 έχει *σταθερό σημείο*.

Το λήμμα επανάληψης είναι συνέπεια του εξής γενικότερου θεωρήματος:

Ορισμός (Συνεχής τελεστής)

Έστω $U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots$ μία *αλυσίδα* (chain) υποσυνόλων του M. Λέμε ότι ο τελεστής $\tau\colon \mathrm{Pow}(M) \to \mathrm{Pow}(M)$ είναι **συνεχής** αν για κάθε αλυσίδα $U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots$ στο $\mathrm{Pow}(M)$ ισχύει $\tau(\bigcup_i \{U_i\}) = \bigcup_i \{\tau(U_i)\}$.

Σταθερά σημεία IV

Θεώρημα (Σταθερού σημείου: Tarski-Knaster, Kleene)

Κάθε συνεχής τελεστής $\tau : Pow(M) \to Pow(M)$ *έχει σταθερό σημείο την*

$$F = \bigcup\{\tau^i(\varnothing) \mid i \in \mathbb{N}\}.$$

Παράδειγμα: Έστω η συνάρτηση:

$$\begin{cases} \text{fact}(0) & = 1 \\ \text{fact}(Sn) & = (n+1) * \text{fact}(n) \end{cases}$$

Συνολοθεωρητικά έχουμε:

$$\text{FACT} = \{(0,1)\} \cup \{(n+1, (n+1) * k) \mid (n,k) \in \text{FACT}\}$$

ή σύντομα: $\text{FACT} = \tau(\text{FACT})$, όπου:

$$\tau(X) = \{(0,1)\} \cup \{(n+1, (n+1) * k) \mid (n,k) \in X\}.$$

Σταθερά σημεία V

Με χρήση του θεωρήματος σταθερού σημείου λαμβάνουμε:

$$\begin{aligned}
&\tau^0(\varnothing) = \varnothing \\
&\tau^1(\varnothing) = \tau(\varnothing) = \{(0,1)\} \\
&\tau^2(\varnothing) = \tau(\tau(\varnothing)) = \tau(\{(0,1)\}) = \{(0,1)\} \cup \{(1,1)\} \\
&\tau^3(\varnothing) = \tau(\tau(\tau(\varnothing))) = \{(0,1)\} \cup \{(1,1),(2,2)\} \\
&\tau^4(\varnothing) = \tau(\tau(\tau(\tau(\varnothing)))) = \{(0,1)\} \cup \{(1,1),(2,2),(3,6)\} \\
&\quad \ldots
\end{aligned}$$

$\mathbf{FACT} = \bigcup_i \tau^i(\varnothing) = \tau^0(\varnothing) \cup \tau^1(\varnothing) \cup \ldots = \{(0,1),(1,1),(2,2),(3,6),\ldots\}.$

Σταθερά σημεία VI

Προκειμένου να εφαρμόσουμε βέβαια το θεώρημα σταθερού σημείου θα πρέπει να δείξουμε ότι ο τελεστής τ είναι συνεχής. Πράγματι:

$$\begin{aligned}
\tau(\bigcup_i X_i) &= \{(0,1)\} \cup \{(n+1,(n+1)*k) \mid (n,k) \in \bigcup_i X_i\} \\
&= \{(0,1)\} \cup \{(n+1,(n+1)*k) \mid \exists i\colon (n,k) \in X_i\} \\
&= \{(0,1)\} \cup \bigcup_i \{(n+1,(n+1)*k) \mid (n,k) \in X_i\} \\
&= \bigcup_i \{(0,1)\} \cup \{(n+1,(n+1)*k) \mid (n,k) \in X_i\} \\
&= \bigcup_i \tau(X_i)
\end{aligned}$$

Σταθερά σημεία VII

Ένας άλλος τρόπος χρήσης του θεωρήματος σταθερού σημείου είναι για να δείξουμε ότι "η μικρότερη κλάση που περιέχει ... και είναι κλειστή ως προς ..." ορίζει μονοσήμαντα μία κλάση $\mathcal{P}$: Έστω C μία οποιαδήποτε κλάση συναρτήσεων. Έστω $\gamma(C)$ η κλάση των συναρτήσεων που λαμβάνουμε αν εφαρμόσουμε μία φορά το σχήμα της σύνθεσης σε συναρτήσεις από το C. Έστω $\rho(C)$ η κλάση των συναρτήσεων που λαμβάνουμε αν εφαρμόσουμε μία φορά το σχήμα πρωταρχικής αναδρομής σε συναρτήσεις από το C. Έστω A η κλάση των αρχικών συναρτήσεων: $A = \{S, P, Z, U_i^n\}$.

Τότε η $\mathcal{P}$ είναι το ελάχιστο σταθερό σημείο της

$$\mathcal{P} = A \cup \gamma(\mathcal{P}) \cup \rho(\mathcal{P}).$$

Το $\mathcal{P}$ κατασκευάζεται με επαναληπτική εφαρμογή των γ και ρ:

$$\mathcal{P} = A \cup \gamma(A) \cup \rho(A) \cup \gamma(A \cup \gamma(A) \cup \rho(A)) \cup \rho(A \cup \gamma(A) \cup \rho(A)) \cup \ldots$$

Υπολογισιμότητα

Θεώρημα

Υπάρχουν "υπολογίσιμες" συναρτήσεις που δεν είναι πρωταρχικές αναδρομικές.

Απόδειξη: Διαγωνιοποίηση.

- Μηχανιστική απαρίθμηση πρωταρχικών αναδρομικών συναρτήσεων: φ_0, φ_1, φ_2, ...
- Ορίζουμε: $f(x) = \varphi_x(x) + 1$
  Η f είναι "υπολογίσιμη".
- Έστω ότι η f είναι πρωταρχική αναδρομική, άρα εμφανίζεται στην παραπάνω μηχανιστική απαρίθμηση. Έστω π.χ. ότι ένας δείκτης της f είναι y, δηλαδή $\varphi_y = f$. Εφάρμοσε την f σε όρισμα y:

$$\varphi_y(y) = f(y) = \varphi_y(y) + 1 \qquad \text{Άτοπο}$$

□

Υπολογισιμότητα

Παράδειγμα μιας **ολικής** (ορισμένης για όλους τους φυσικούς αριθμούς) υπολογίσιμης συνάρτησης που όμως δεν είναι πρωταρχική αναδρομική είναι η εξής συνάρτηση f:

$$\begin{cases} f(x,y,0) = Sy \\ f(x,0,1) = x, \quad f(x,0,2) = 0, \quad f(x,0,SSSn) = 1 \\ f(x,Sy,Sn) = f(x,f(x,y,Sn),n) \end{cases}$$

Η παραπάνω συνάρτηση f συγγενεύει με την περίφημη συνάρτηση του Ackermann A:

$$\begin{cases} A(0,n) = n+1 \\ A(m,0) = A(m-1,1) \\ A(m,n) = A(m-1,A(m,n-1)) \end{cases}$$

Ανάγκη να επεκταθούμε απο ολικές σε μερικές συναρτήσεις

Ο τρόπος να αποφύγουμε την αντίφαση ($\varphi_x(x) = \varphi_x(x) + 1$) της διαγωνιοποίησης είναι να επιτρέψουμε **μερικές** (partial) συναρτήσεις, δηλαδή συναρτήσεις που δεν είναι κατά ανάγκη ορισμένες για όλους τους φυσικούς αριθμούς $\mathbb{N}$.

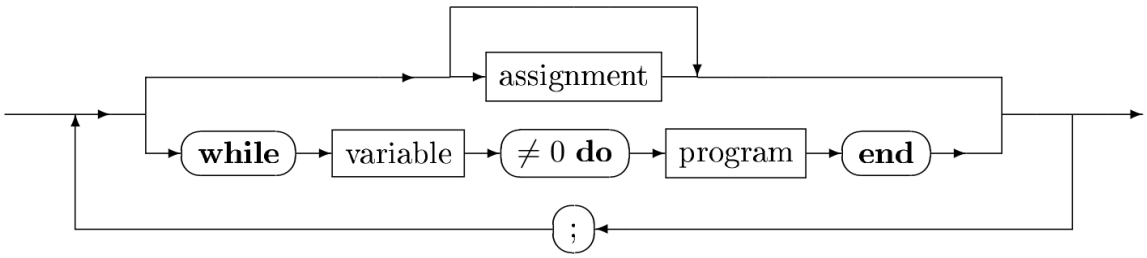
Συνήθως χρησιμοποιούμε τους ακόλουθους συμβολισμούς όταν η συνάρτηση f δεν είναι ορισμένη για το όρισμα x:

> *Η f **αποκλίνει** (diverges) για το x, $f(x)\uparrow$, ή ακόμα το πρόγραμμα για την f δεν σταματάει.*

Τα σχήματα σύνθεσης και πρωταρχικής αναδρομής γενικεύονται κατα προφανή τρόπο.

Προγράμματα WHILE και μερικές αναδρομικές συναρτήσεις I

- Οι assignments ακριβώς ίδιες όπως στη γλώσσα LOOP.
- program:



Προγράμματα WHILE και μερικές αναδρομικές συναρτήσεις II

Όπως είναι γνωστό, είναι δυνατόν η εκτέλεση ενός προγράμματος WHILE να μην σταματάει ποτέ.

Παράδειγμα

Η $\sqrt{x} : \mathbb{N} \to \mathbb{N}$, ως μερική συνάρτηση, ορίζεται (σταματάει) μόνο αν το x είναι τέλειο τετράγωνο:
$y := 0$; $z := \mathrm{abs}(x - y^2)$; **while** $z \neq 0$ **do** $y := y + 1$; $z := \mathrm{abs}(x - y^2)$ **end**

Σημασιολογία για προγράμματα WHILE και ακολούθως η έννοια της WHILE-υπολογίσιμης συνάρτησης μπορούν να οριστούν με παρόμοιο τρόπο, όπως και για τα LOOP-προγράμματα. Η κλάση των WHILE-υπολογίσιμων συναρτήσεων συμπεριλαμβάνει και όλες τις LOOP-υπολογίσιμες συναρτήσεις.

μ-σχήμα

Θα εισαγάγουμε τώρα ένα νέο σχήμα, το **μ-σχήμα** ή σχήμα **απεριόριστης ελαχιστοποίησης** (unbounded minimization).

Παράδειγμα

$\sqrt{x} = \mu y[\text{abs}(x - y^2) = 0]$, δηλαδή το μικρότερο y, ώστε $\text{abs}(x - y^2) = 0$, αν υπάρχει τέτοιο y, ειδάλλως η τιμή δεν είναι ορισμένη.

Γενικώς: $f(x_1, \ldots, x_n) = \mu y[h(x_1, \ldots, x_n, y) = 0]$.

Η f μπορεί να μην είναι ορισμένη για δύο λόγους: είτε η h δεν είναι ποτέ $= 0$, είτε η h δεν είναι κάπου ορισμένη πριν να βρεθεί ένα y για το οποίο $h = 0$.

Μερικές αναδρομικές συναρτήσεις

Ορισμός

Η κλάση $\mathcal{PR}$ των **μερικών αναδρομικών συναρτήσεων** (partial recursive functions) είναι η μικρότερη κλάση που:

α) περιλαμβάνει τις **αρχικές συναρτήσεις**: S, P, Z, U_i^n

β) είναι κλειστή ως προς τη **σύνθεση**, την **πρωταρχική αναδρομή** και το μ-**σχήμα**.

Μερικές αναδρομικές συναρτήσεις Ι

Θεώρημα

Μια μερική συνάρτηση είναι WHILE-υπολογίσιμη ανν είναι μερική αναδρομική.

Απόδειξη (σκελετός):
Με επαγωγή, παρομοίως με τις προηγούμενες αποδείξεις της ισοδυναμίας των LOOP-υπολογίσιμων και των πρωταρχικών αναδρομικών συναρτήσεων.

Πρόσθετες ιδέες:

$\Leftarrow$: $f(x_1, \ldots, x_n) = \mu z[h(x_1, \ldots, x_n, z) = 0]$
μπορεί να υπολογιστεί με το πρόγραμμα:
$z := 0$; "$y := h(x_1, \ldots, x_n, z)$"; **while** $y \neq 0$ **do** $z := \operatorname{succ} z$; "$y := h(x_1, \ldots, x_n, z)$" **end**

Μερικές αναδρομικές συναρτήσεις II

$\Rightarrow$: **while** $x_k \neq 0$ **do** π **end**
υπολογίζει την $f_i(x_1, \ldots, x_n, v(x_1, \ldots, x_n))$ [σύνθεση], όπου για $1 \leqslant i \leqslant n$:

$$\begin{cases} f_i(x_1, \ldots, x_n, 0) = U_i^n(x_1, \ldots, x_n) [\text{αμοιβαία πρωταρχική αναδρομή}] \\ f_i(x_1, \ldots, x_n, Sz) = h_i(f_1(x_1, \ldots, x_n, z), \ldots, f_n(x_1, \ldots, x_n, z)) \end{cases}$$

$[z = \text{αριθμός επαναλήψεων βρόχου}]$

και $v(x_1, \ldots, x_n) = \mu z[f_k(x_1, \ldots, x_n, z) = 0]$