
HY 280 — Θεωρία Υπολογισμού

Ασκήσεις 1ης Διάλεξης
Χαράλαμπος Ε. Τσουρακάκης

Κοινή υπόθεση. Για τις ασκήσεις 1, 2 και 3 υποθέτουμε ότι διαθέτουμε έναν ελεγκτή $\text{HALT}(P, D)$ που τερματίζει πάντοτε και επιστρέφει **ΝΑΙ** αν το πρόγραμμα P τερματίζει με είσοδο D , και **ΟΧΙ** διαφορετικά. Γνωρίζουμε ότι τέτοιος γενικός αλγόριθμος δεν υπάρχει. Εδώ εξετάζουμε τι θα μπορούσαμε να κάνουμε *αν υπήρχε*. Τα προγράμματά μας δεν χρειάζονται είσοδο, οπότε γράφουμε $\text{HALT}(P, \varepsilon)$, όπου ε είναι η κενή είσοδος. Υποθέτουμε ακριβή αριθμητική ακεραίων, χωρίς προκαθορισμένο όριο μεγέθους.

Άσκηση 1 (Περιττοί τέλει αριθμοί). Ένας θετικός ακέραιος λέγεται **τέλειος** αν ισούται με το άθροισμα των θετικών διαιρετών του, εκτός του ίδιου. Για παράδειγμα,

$$6 = 1 + 2 + 3, \quad 28 = 1 + 2 + 4 + 7 + 14.$$

Η εικασία που εξετάζουμε είναι: **δεν υπάρχει περιττός τέλειος αριθμός**.

- (α') Περιγράψτε έναν πεπερασμένο έλεγχο για το αν ένας δεδομένος θετικός ακέραιος n είναι τέλειος.
- (β') Γράψτε πρόγραμμα P_1 που τερματίζει αν και μόνο αν υπάρχει περιττός τέλειος αριθμός. Αν βρει κάποιον, να τον εμφανίζει.
- (γ') Εξηγήστε πώς μία κλήση στον υποθετικό ελεγκτή τερματισμού θα προσδιόριζε αν η εικασία είναι αληθής ή ψευδής.

Άσκηση 2 (Η εικασία του Legendre). Η εικασία του Legendre λέει ότι ανάμεσα στα τετράγωνα δύο διαδοχικών θετικών ακεραίων υπάρχει πάντοτε τουλάχιστον ένας πρώτος αριθμός:

$$\forall n \geq 1 \exists p \text{ πρώτος} : \quad n^2 < p < (n+1)^2.$$

Για παράδειγμα, ανάμεσα στο 4 και στο 9 βρίσκεται ο πρώτος 5, ενώ ανάμεσα στο 9 και στο 16 βρίσκεται ο πρώτος 11. Υπενθυμίζεται ότι ένας ακέραιος $p \geq 2$ είναι πρώτος αν οι μόνοι θετικοί διαιρέτες του είναι το 1 και ο ίδιος.

- (α') Περιγράψτε πώς ελέγχουμε, σε πεπερασμένο χρόνο, αν η εικασία ισχύει για έναν συγκεκριμένο θετικό ακέραιο n .
- (β') Γράψτε πρόγραμμα P_2 που αναζητά αντιπαράδειγμα και τερματίζει αν και μόνο αν η εικασία είναι ψευδής.
- (γ') Εξηγήστε πώς χρησιμοποιούμε τον υποθετικό ελεγκτή τερματισμού για να προσδιορίσουμε αν η εικασία ισχύει.
- (δ') Γιατί ο έλεγχος των πρώτων 10^{12} τιμών του n δεν αποτελεί, από μόνος του, απόδειξη της εικασίας;

Άσκηση 3 (Το πρόβλημα Brocard--Ramanujan). Για έναν θετικό ακέραιο n , ορίζουμε το παραγοντικό $n! = 1 \cdot 2 \cdots n$. Εξετάζουμε την εξίσωση

$$n! + 1 = m^2, \quad n, m \in \mathbb{Z}_{>0}.$$

Έχουμε τις λύσεις

$$4! + 1 = 5^2, \quad 5! + 1 = 11^2, \quad 7! + 1 = 71^2.$$

Η εικασία που εξετάζουμε είναι: **οι παραπάνω είναι οι μοναδικές λύσεις σε θετικούς ακεραίους**.

- (α') Περιγράψτε πώς ελέγχουμε σε πεπερασμένο χρόνο αν ένας θετικός ακέραιος N είναι τέλειο τετράγωνο.
- (β') Γράψτε πρόγραμμα P_3 που τερματίζει αν και μόνο αν η εξίσωση έχει λύση με $n \notin \{4, 5, 7\}$. Αν βρει τέτοια λύση, να την εμφανίζει.
- (γ') Εξηγήστε τι θα σήμαινε καθεμία από τις δύο απαντήσεις του υποθετικού ελεγκτή τερματισμού για το P_3 .

Άσκηση 4 (Η αναπαράσταση αλλάζει το μέγεθος της εισόδου). Στη **μοναδιαία αναπαράσταση**, ο θετικός ακέραιος N γράφεται ως μια ακολουθία από N μονάδες. Για παράδειγμα, το 5 γράφεται ως 11111.

- (α') Γράψτε το 13 σε μοναδιαία, δυαδική και δεκαδική αναπαράσταση. Πόσα σύμβολα χρησιμοποιεί καθεμία;
- (β') Έστω $N = 2^k$, όπου $k \geq 1$. Ποιο είναι το μήκος της μοναδιαίας και ποιο της δυαδικής αναπαράστασής του;
- (γ') Ένας αλγόριθμος εκτελεί ακριβώς N επαναλήψεις. Εκφράστε το πλήθος των επαναλήψεων ως συνάρτηση του μήκους της εισόδου, για καθεμία από τις δύο αναπαράστασεις.
- (δ') Μπορούμε να μετατρέψουμε κάθε δυαδική αναπαράσταση μήκους n στην αντίστοιχη μοναδιαία σε χρόνο πολυωνυμικό ως προς n ; Υποθέστε ότι σε κάθε βήμα γράφουμε το πολύ ένα σύμβολο εξόδου.

Άσκηση 5 (Δυαδική αναπαράσταση). Ένας θετικός ακέραιος N έχει δυαδική αναπαράσταση με ακριβώς n bits, χωρίς αρχικά μηδενικά.

1. Ποια είναι η μικρότερη και ποια η μεγαλύτερη δυνατή τιμή του N ;
2. Πόσα bits απαιτούνται για την αναπαράσταση του $2N$; Πώς προκύπτει από τη δυαδική αναπαράσταση του N ;
3. Πότε ο αριθμός $N + 1$ χρειάζεται περισσότερα bits από τον N ;
4. Ένας αλγόριθμος εκτελεί ακριβώς N βήματα με είσοδο τη δυαδική αναπαράσταση του N . Είναι γραμμικός ως προς το **μήκος της εισόδου**; Αιτιολογήστε την απάντησή σας.

Άσκηση 6 (Μία απάντηση ή μία γενική μέθοδος;). Έστω $f : \mathbb{N} \rightarrow \{0, 1\}$ μια ολική συνάρτηση. Γράφουμε $P(x) \downarrow = y$ όταν το πρόγραμμα P τερματίζει με είσοδο x και επιστρέφει y .

Συγκρίνετε τις προτάσεις:

$$(A) \quad \forall x \in \mathbb{N} \exists P : P(x) \downarrow = f(x),$$

$$(B) \quad \exists P \forall x \in \mathbb{N} : P(x) \downarrow = f(x).$$

- (α') Εξηγήστε τη διαφορά τους με λόγια. Σε ποια πρόταση μπορεί το πρόγραμμα να εξαρτάται από το x ;
- (β') Δείξτε ότι η (A) ισχύει για κάθε τέτοια συνάρτηση f , ακόμη και αν η f δεν είναι υπολογίσιμη. Υπόδειξη: αρκούν δύο προγράμματα σταθερής εξόδου.
- (γ') Ποια πρόταση εκφράζει την υπολογισσιμότητα της f ;

(δ') Γράψτε την άρνηση της (B), χρησιμοποιώντας το κατηγορημα

$C(P, x) : \quad \text{«το } P(x) \text{ τερματίζει και επιστρέφει } f(x)\text{»}.$

Εξηγήστε τους δύο τρόπους με τους οποίους μπορεί να αποτύχει το $C(P, x)$.

Άσκηση 7 (Τερματισμός με χρονικό όριο). Ένας φοιτητής προτείνει τον εξής ελεγκτή: «Προσομοιώνω το $P(D)$ για 10^{12} βήματα. Αν τερματίσει, απαντώ ΝΑΙ. Διαφορετικά, απαντώ ΟΧΙ».

(α') Γιατί αυτός ο ελεγκτής δεν λύνει το γενικό πρόβλημα του τερματισμού;

(β') Θεωρήστε τώρα το διαφορετικό πρόβλημα:

«Το $P(D)$ τερματίζει μέσα σε το πολύ t βήματα;»

Η είσοδος περιλαμβάνει τα P, D, t . Δώστε αλγόριθμο που το αποφασίζει.

(γ') Εξηγήστε γιατί η λύση του (β) δεν αντιφάσκει με τη μη αποφασισιμότητα του γενικού προβλήματος.

(δ') Ένας δεύτερος φοιτητής προτείνει: «Αντί για σταθερό όριο, υπολογίζω από τα P, D ένα όριο $B(P, D)$. Κάθε εκτέλεση που πρόκειται να τερματίσει θα τερματίζει μέσα σε αυτό το όριο».

Αποδείξτε ότι δεν υπάρχει ολικός αλγόριθμος που υπολογίζει ένα τέτοιο όριο για όλα τα P, D .

Άσκηση 8 (Το πρόβλημα του τερματισμού χωρίς είσοδο). Γνωρίζουμε ότι δεν υπάρχει αλγόριθμος που να αποφασίζει, για κάθε πρόγραμμα P και είσοδο D , αν το $P(D)$ τερματίζει.

Κάποιος ισχυρίζεται ότι το πρόβλημα γίνεται αποφασίσιμο αν περιοριστούμε σε προγράμματα που δεν δέχονται είσοδο. Υποθέτει ότι υπάρχει ελεγκτής $H_0(Q)$ που τερματίζει πάντοτε και απαντά σωστά αν το πρόγραμμα $Q()$ τερματίζει.

(α') Δοθέντων των P, D , κατασκευάστε ένα πρόγραμμα $Q_{P,D}$ χωρίς είσοδο, το οποίο έχει ενσωματωμένα στον κώδικά του τα P, D και ικανοποιεί:

$Q_{P,D}() \text{ τερματίζει} \iff P(D) \text{ τερματίζει}.$

(β') Εξηγήστε πώς θα χρησιμοποιούσατε το H_0 για να λύσετε το γενικό πρόβλημα του τερματισμού.

(γ') Συμπληρώστε τη σωστή κατεύθυνση της αναγωγής:

_____ $\leq$ _____.

(δ') Για να κατασκευάσουμε το $Q_{P,D}$, χρειάζεται να εκτελέσουμε πρώτα το $P(D)$; Γιατί έχει σημασία η απάντηση;

Άσκηση 9 (Μια γεύση αλγορίθμων από το Λύκειο: Ορθότητα και τερματισμός του Ευκλείδη). Για θετικούς ακεραίους a, b , θεωρούμε τον αλγόριθμο:

```
Euclid(a, b):  
  όσο b ≠ 0:  
    r = a mod b  
    a = b  
    b = r  
  επέστρεψε a
```

Το $a \bmod b$ είναι το υπόλοιπο της διαίρεσης του a με το b . Οι αναθέσεις εκτελούνται με τη σειρά που γράφονται.

(α') Εκτελέστε τον αλγόριθμο για $(a, b) = (252, 105)$, καταγράφοντας τα διαδοχικά ζεύγη (a, b) .

(β') Αποδείξτε ότι, για $b > 0$, ο ΜΚΔ $\gcd(a, b)$ (greatest common divisor) των a, b ικανοποιεί

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Υπόδειξη: γράψτε $a = qb + r$ και συγκρίνετε τους κοινούς θετικούς διαιρέτες των δύο ζευγών.

(γ') Αποδείξτε ότι ο αλγόριθμος τερματίζει.

(δ') Συνδυάστε τα προηγούμενα για να αποδείξετε ότι επιστρέφει τον ΜΚΔ των αρχικών αριθμών. Γιατί το ερώτημα (β) δεν αρκεί από μόνο του;