ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αλγεβρικοί αλγόριθμοι και εφαρμογές στη γεωμετρία

ΗΛΙΑΣ Π. ΤΣΙΓΑΡΙΔΑΣ

ΑΘΗΝΑ
ΑΥΓΟΥΣΤΟΣ 2006

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αλγεβρικοί αλγόριθμοι και εφαρμογές στη γεωμετρία

Ηλίας Π. Τσιγαρίδας

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: **Ιωάννης Εμίρης**, Αναπληρωτής Καθηγητής ΕΚΠΑ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:

Ιωάννης Εμίρης, Αναπληρωτής Καθηγητής ΕΚΠΑ
Θεοχάρης Θεοχάρης, Αναπληρωτής Καθηγητής ΕΚΠΑ
Νικόλαος Μισυρλής, Καθηγητής ΕΚΠΑ

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Ιωάννης Εμίρης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Σέργιος Θεοδωρίδης,
Καθηγητής ΕΚΠΑ

Θεοχάρης Θεοχάρης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Νικόλαος Καλουπτσίδης,
Καθηγητής ΕΚΠΑ

Ηλίας Κουτσουπιάς,
Καθηγητής ΕΚΠΑ

Νικόλαος Μισυρλής,
Καθηγητής ΕΚΠΑ

Ευάγγελος Ράπτης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Ημερομηνία Εξέτασης: 29 Αυγούστου 2006

Περίληψη

Πραγματικοί αλγεβρικοί αριθμοί είναι οι πραγματικοί αριθμοί που προκύπτουν ως ρίζες πολυωνύμων σε μία μεταβλητή, με ακέραιους συντελεστές. Στόχος της παρούσας διατριβής είναι η ανάπτυξη, ανάλυση και αποτελεσματική υλοποίηση αλγορίθμων ακριβείας (exact algorithms), που βασίζονται σε αριθμητική ακεραίων απεριόριστης ακρίβειας και αφορούν υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς, καθώς και εφαρμογές αυτών σε προβλήματα και αλγορίθμους της μη γραμμικής υπολογιστικής γεωμετρίας.

Προκειμένου να κατασκευαστούν οι πραγματικοί αλγεβρικοί αριθμοί πρέπει να επιλυθεί, στους πραγματικούς, ένα πολυώνυμο με ακέραιους συντελεστές.

Ενοποιούμε και απλοποιούμε την θεωρία που αφορά τους αλγορίθμους επίλυσης, οι οποίοι βασίζονται στην υποδιαίρεση, και βελτιώνουμε την πολυπλοκότητα του αλγορίθμου που βασίζεται στα συνεχή κλάσματα. Επιτυγχάνεται, με νέο τρόπο, το καλύτερο γνωστό φράγμα πολυπλοκότητας. Επιπρόσθετα, αποδεικνύεται ότι το φράγμα αυτό ισχύει και για πολυώνυμα με τετράγωνα, ενώ με την ίδια πολυπλοκότητα υπολογίζουμε και την πολλαπλότητα των ριζών. Αποδεικνύουμε ένα νέο φράγμα για την αναμενόμενη πολυπλοκότητα της μεθόδου των συνεχών κλασμάτων. Οι αλγόριθμοι επίλυσης γενικεύονται και σε πολυωνυμικά συστήματα δύο μεταβλητών. Τα πειραματικά μας αποτελέσματα επιβεβαιώνουν την ταχύτητα των μεθόδων.

Οι αλγόριθμοι για τους πραγματικούς αλγεβρικούς αριθμούς αφορούν την κατασκευή, την σύγκριση και τον υπολογισμό του προσήμου ενός πολυωνύμου πάνω σε έναν και δύο πραγματικούς αλγεβρικούς αριθμούς, καθώς και το πρόβλημα της απαλοιφής ποσοδεικτών. Αν ο βαθμός του πολυωνύμου είναι μικρός (μέχρι 4 για μία μεταβλητή, μέχρι 2 για δύο μεταβλητές), προτείνουμε αλγορίθμους ειδικού σκοπού οι οποίοι έχουν σταθερή αριθμητική πολυπλοκότητα. Για όλους τους παραπάνω αλγορίθμους παρουσιάζεται υλοποίηση σε C++ και πειραματική μελέτη.

Στην υπολογιστική γεωμετρία μελετούνται τα κατηγορήματα που απαιτούνται στους αλγορίθμους υπολογισμού της διάταξης ελλειπτικών τόξων στο επίπεδο και στον υπολογισμό του διαγράμματος Voronoi ελλείψεων. Τέλος, δοθέντος ενός κυρτού πολυγώνου με ακέραιες κορυφές εξετάζουμε αλγορίθμους που μας επιτρέπουν να το διασπάσουμε σε δύο άλλα κυρτά πολύγωνα τέτοια ώστε το άθροισμά τους κατά Minkowski να ισούται με το αρχικό πολύγωνο.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Αλγεβρικοί αλγόριθμοι, Υπολογιστική γεωμετρία
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: πραγματικοί αλγεβρικοί αριθμοί, πραγματική επίλυση, επιλύουσα, διατάξεις, διάγραμμα Voronoi

Abstract

Real algebraic numbers are the real numbers that are real roots of univariate polynomials with integer coefficients. We study exact algorithms, from a theoretical and an implementation point of view, based on integer arithmetic of arbitrary precision, for computations with real algebraic numbers and applications of these algorithms on problems and algorithms in non linear computational geometry.

In order to construct a real algebraic number we must compute the real roots of a univariate polynomial with integer coefficients.

We unify and simplify the theory behind the subdivision based algorithms for real root isolation and we improve the complexity of the algorithm that is based on the continued fraction expansion of the real numbers. The best known complexity bound up today is achieved using new techniques. Moreover, we prove that the bound holds for non square-free polynomials and that in the same complexity bound we can compute the multiplicities of the real roots. We prove a new bound for the expected complexity of the algorithm based on continued fractions. We generalize the real root isolation algorithms to bivariate polynomial systems. Our experimental analysis proves the effectiveness of our methods.

The algorithms that we consider for computations with real algebraic numbers are construction, comparison, sign evaluation and quantifier elimination. If the degree of the polynomial is small, i.e. ≤ 4 in the univariate case and ≤ 2 in the bivariate case, we propose special purpose algorithms that have constant arithmetic complexity. For all the algorithms we present a C++ implementation and an experimental analysis.

In computational geometry we study the predicates needed by the algorithms for the arrangement of elliptic arcs in the plane and the computation of the Voronoi diagram of ellipses, also in the plane. Finally, given a convex lattice polygon we study algorithms for decomposing it to two other convex lattice polygons, such that their Minkowski sum is the original polygon.

SUBJECT AREA: Algebraic algorithms, Computational geometry
KEYWORDS: real algebraic numbers, real solving
resultant, arrangements, Voronoi diagram

Στο μπαμπά, στη μαμά και στην Άννα

Ευχαριστίες

Η εκπόνηση μιας διδακτορικής διατριβής είναι μια δύσκολη προσπάθεια. Είναι σίγουρο ότι δεν θα είχα καταφέρει να ολοκληρώσω τη διατριβή μου αν οι καθηγητές μου, οι φίλοι μου και η οικογένεια μου δεν με είχαν βοηθήσει. Τα λίγα λόγια που τους αφιερώνω εδώ είναι το ελάχιστο που μπορώ να κάνω. Άλλωστε η ευγνωμοσύνη δεν περιγράφεται.

Καταρχάς, θα ήθελα να ευχαριστήσω τον καθηγητή μου Γιάννη Εμίρη για την εμπιστοσύνη που μου έδειξε και για την ευκαιρία που μου έδωσε να ασχοληθώ με επιστημονικά ζητήματα που με ενδιέφεραν. Δεν θα ξεχάσω ποτέ ότι η πόρτα του γραφείου του ήταν πάντοτε ανοιχτή και ότι επέλεξε συνειδητά όχι να με 'χειριστεί', αλλά να με στηρίξει και με ενθαρρύνει. Ελπίζω να ανταποκρίθηκα στις προσδοκίες του και ο σεβασμός και η ευγνωμοσύνη μου να ανταποδίδουν σε κάποιο βαθμό τις προσπάθειές του.

Είμαι πολύ τυχερός που οι καθηγητές Σέργιος Θεοδωρίδης, Θεοχάρης Θεοχάρης, Νικόλαος Καλουπτσίδης, Ηλίας Κουτσουπιάς, Νικόλαος Μισυρλής και Ευάγγελος Ράπτης μου έκαναν την εξαιρετική τιμή να συμμετάσχουν στην επταμελή μου επιτροπή. Τους ευχαριστώ θερμά.

Θα ήθελα επίσης να ευχαριστήσω τον Bernard Mourrain, την Monique Teillaud και τον David Daney, από το INRIA Sophia-Antipolis, και τον Μενέλαο Καραβέλα, από το Πανεπιστήμιο της Κρήτης, για τη συνεργασία μας και την εμπιστοσύνη τους. Ιδιαίτερα ο Bernard λειτούργησε ως συνεπιβλέποντάς μου και με βοήθησε όσο περισσότερο μπορούσε. Τον ευχαριστώ για όλα.

Όταν ξεκινήσα την εκπόνηση της διδακτορικής μου διατριβής πίστευα ότι οι επιστημονικές προκλήσεις θα ήταν τα μόνα εμπόδια που συναντούσα. Κάτι τέτοιο όμως δεν ανταποκρίνεται στην πραγματικότητα, ή τουλάχιστον δεν ανταποκρίνεται στην πραγματικότητα που βιώσα εγώ. Η εκπόνηση μιας διατριβής απαιτεί να ξεπεράσεις και πολλά άλλα εμπόδια και είναι μια ψυχοφθόρα διαδικασία. Μια διαδικασία την οποία δεν θα είχα καταφέρει να φέρω εις πέρας χωρίς τη βοήθεια των φίλων μου και της οικογένειάς μου.

Στη Χρυσηίδα λέω απλά ευχαριστώ. Άλλωστε με καταλαβαίνει καλύτερα από τον καθένα και ό,τι και να γράψω θα ήταν πλεονασμός.

Ο Γιώργος Κ είναι ένας πολύ σημαντικός φίλος για μένα. Τον ευχαριστώ για την φιλία του και για τις ατελείωτες βόλτες που κάναμε προσπαθώντας να λύσουμε το γόρδιο δεσμό ενός ακόμα $f(x)$. Ίσως και με το Νίκο Π να καταφέρουμε να λύσουμε κάποιον.

Στους φίλους μου στο DI, ή πέριξ αυτού, Βασίλη, Κυριάκο, Γιώργο, Θανάση, Στρατή, Αντώνη, Μάριο, Γεράσιμο, Ευριπίδη, Δημήτρη και Χρήστο οφείλω, τουλάχιστον, ένα μεγάλο ευχαριστώ.

Τα τελευταία 3 χρόνια τις περισσότερες ώρες της ημέρας (μερικές φορές και της νύχτας) τις πέρασα με τους φίλους μου στα διπλανά 'γραφεία' (sic). Τη Μαρία, τον Ορέστη και το Γιώργο. Με

ανέχτηκαν και τους ανέχτηκα και μοιραστήκαμε τα κουτσομπολιά μας, τις χαρές και τις λύπες μας. Τους ευχαριστώ θερμά και θα τους είμαι ευγνώμων για πάντα.

Η απομόνωση κατά διαστήματα που απαιτεί μια διδακτορική διατριβή με έκανε να παραμελήσω πολλούς από τους φίλους μου εκτός του Πανεπιστημίου. Ο Παντελής Κ, ο Κώστας Π, η Σεβαστή Ν και οι κουμπάροι μου Νίκος και Βούλα πρέπει να έχουν τα μεγαλύτερα παράπονα. Τους ευχαριστώ για την κατανόησή τους και τους ζητώ να με συγχωρήσουν. Θα επανορθώσω στην πρώτη ευκαιρία.

Στο Βασίλη, στον Κώστα και στο Χρήστο θα τους εξηγήσω σε κάποιο άλλο αγώνα Champions League τι ερευνώ ακριβώς. Τους ευχαριστώ που με στήριξαν και ας μην καταλαβαίνουν γιατί μπήκα σε όλη αυτή τη διαδικασία.

Ο θείος μου ο Δημήτρης μου στάθηκε όσο περισσότερο μπορούσε και λίγο παραπάνω. Τον ευχαριστώ πολύ.

Η μητέρα μου και η αδελφή μου έκαναν ότι μπορούσαν για να με βοηθήσουν στην προσπάθειά μου. Αν ήξεραν και λίγα μαθηματικά παραπάνω ίσως να μου έλυναν και κάποια εξίσωση. Σε κάθε περίπτωση τους χρωστώ τα πάντα και τους αφιερώνω τη διατριβή μου ως το ελάχιστο που θα μπορώ να κάνω.

Ελπίζω να μην έχω ξεχάσει να αναφέρω κάποιον. Αν το έχω κάνει του ζητώ να με συγχωρήσει.

Ηλίας Π. Τσιγαρίδας
Αθήνα
Αύγουστος, 2006

Περιεχόμενα

Περιεχόμενα **13**

1 Εισαγωγή **15**

2 Αλγεβρικό υπόβαθρο **21**
2.1 Περί των αριθμών 22
2.2 Περί των πολυωνύμων 23
2.3 Πολυωνυμικές ακολουθίες υπολοίπων 30
2.4 Πολυώνυμα στη βάση Bernstein 42
2.5 Σύνοψη – Μελλοντικές επεκτάσεις 45

3 Πραγματική επίλυση πολυωνύμων σε μία μεταβλητή **47**
3.1 Μέτρο Mahler 50
3.2 Φράγματα στις ρίζες 52
3.3 Εύρεση πραγματικών ριζών πολυωνύμου 61
3.4 Ο αλγόριθμος του Kronecker 66
3.5 Αλγόριθμοι υποδιαίρεσης 68
3.6 Ο αλγόριθμος των συνεχών κλασμάτων 79
3.7 Σύνοψη – Μελλοντικές επεκτάσεις 88

4 Υπολογισμοί με πραγματικούς αλγεβρικούς αριθμούς **91**
4.1 Υπολογισμοί με έναν αλγεβρικό αριθμό 92
4.2 Υπολογισμοί με δύο αλγεβρικούς αριθμούς 98
4.3 Σύνοψη – Μελλοντικές επεκτάσεις 112

5 Αλγεβρικοί αριθμοί μικρού βαθμού **113**
5.1 Πολυώνυμα απομόνωσης και πραγματικές ρίζες 117
5.2 Πραγματική επίλυση 118
5.3 Σύγκριση αλγεβρικών αριθμών 132
5.4 Ο υπολογισμός προσήμου 135
5.5 Αποτίμηση προσήμου σε δύο μεταβλητές 139
5.6 Σύνοψη – Μελλοντικές επεκτάσεις 140

6 Περί της υλοποίησης **143**
6.1 Πειραματικά αποτελέσματα 147

7 Εφαρμογές στην γεωμετρία **165**
7.1 Περί των ελλείψεων 166
7.2 Διατάξεις κωνικών τομών στο επίπεδο 168
7.3 Διάγραμμα Voronoi ελλείψεων στο επίπεδο 173

8 Διάσπαση Minkowski **185**
8.1 Ορισμοί και προηγούμενες εργασίες 187
8.2 Προσθετέοι σταθερού μεγέθους 189
8.3 Υλοποίηση και πολύγωνα με ένα και κανένα εσωτερικό ακέραιο σημείο 196
8.4 Βελτίωση του γενικού αλγόριθμου διάσπασης 201
8.5 Μελλοντικές επεκτάσεις 203

Βιβλιογραφία **205**

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Αν θες να μάθεις για τη διαδρομή,
ρώτησε αυτούς που επιστρέφουν.

Κινέζικο γνωμικό

Πραγματικοί αλγεβρικοί αριθμοί είναι οι πραγματικοί αριθμοί που προκύπτουν ως ρίζες πολυωνύμων σε μία μεταβλητή, με ακέραιους συντελεστές. Σκοπός της παρούσας διατριβής είναι η ανάπτυξη, ανάλυση και αποτελεσματική υλοποίηση αλγορίθμων που βασίζονται σε αριθμητική ακριβείας[1] και αφορούν την επίλυση στους πραγματικούς πολυωνυμικών εξισώσεων, υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς καθώς και εφαρμογές αυτών σε προβλήματα και αλγορίθμους της μη γραμμικής υπολογιστικής γεωμετρίας.

Ας θεωρήσουμε το παρακάτω τμήμα ενός προγράμματος σε C++ το οποίο ορίζει δύο ακεραίους και τους συγκρίνει:

```
int a = 3;
int b = 5;

if ( a > b )  { execute algorithm A; }
if ( a < b )  { execute algorithm B; }
if ( a == b ) { execute algorithm C; }
```

Στόχος μας είναι να μελετήσουμε αλγορίθμους που να μας επιτρέπουν να γράψουμε αντίστοιχα προγράμματα όπου οι μεταβλητές είναι, αντί για ακέραιοι, πραγματικοί αλγεβρικοί αριθμοί και να μελετήσουμε την πολυπλοκότητα των αλγορίθμων αυτών. Για παράδειγμα, θα θέλαμε να έχουμε τη δυνατότητα να γράφουμε προγράμματα όπως:

[1] Σε όλη τη διατριβή, η λέξη *ακριβής* χρησιμοποιείται για την απόδοση του αγγλικού όρου *exact*. Όταν αναφερόμαστε σε *ακριβείς αλγορίθμους* (exact algorithms) ή σε *αριθμητική ακριβείας* (exact arithmetic) ή σε *ακριβείς υπολογισμούς* (exact computations) θα εννοούμε αλγορίθμους ή υπολογισμούς που βασίζονται σε αριθμητική ακεραίων ή ρητών αριθμών απεριόριστης ακρίβειας.

```
root_of a = solve( "x^3-2")[2];
root_of b = solve( "x^5-3")[2];

if ( a > b )  { execute algorithm A; }
if ( a < b )  { execute algorithm B; }
if ( a == b ) { execute algorithm C; }
```

Ο τύπος **root_of** είναι ο τύπος για τους πραγματικούς αλγεβρικούς αριθμούς και έχει αντικαταστήσει τον τύπο για τους ακεραίους (**int**) του προηγούμενου προγράμματος. Αντίστοιχη λειτουργικότητα με την αρχικοποίηση των ακεραίων έχει η συνάρτηση **solve**. Η συνάρτηση δέχεται ως είσοδο ένα πολυώνυμο και επιστρέφει μια λίστα (ή διάνυσμα) από πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του πολυωνύμου. Στο προηγούμενο πρόγραμμα επιλέξαμε (και στις δύο περιπτώσεις) τη δεύτερη μικρότερη ρίζα του αντίστοιχου πολυωνύμου. Οι τρεις τελευταίες γραμμές των προγραμμάτων είναι ακριβώς οι ίδιες. Και στις δύο περιπτώσεις, ανάλογα με τη διάταξη των αριθμών, εκτελείται κάποιος αλγόριθμος.

Ο ορισμός (ή αρχικοποίηση ή κατασκευή) πραγματικών αλγεβρικών αριθμών, που αντιστοιχεί στην επιλύση στους πραγματικούς ενός πολυωνύμου σε μία μεταβλητή με ακέραιους συντελεστές (ακέραιο πολυώνυμο) και η σύγκρισή τους είναι από τους πιο σημαντικούς υπολογισμούς, όπως επίσης και ο υπολογισμός του προσήμου ενός πολυωνύμου όταν αποτιμηθεί πάνω σε έναν αλγεβρικό αριθμό, η επίλυση συστημάτων πολυωνυμικών ανισώσεων σε μία μεταβλητή και οι αριθμητικές πράξεις με ρητούς και έναν πραγματικό αλγεβρικό αριθμό. Επίσης, οι πραγματικοί αλγεβρικοί αριθμοί μπορούν να κατασκευαστούν και κατά ζεύγη, όταν επιλύουμε στους πραγματικούς ένα πολυωνυμικό σύστημα σε δύο μεταβλητές. Έτσι προκύπτει η ανάγκη για υπολογισμούς όπου εμπλέκονται δύο πραγματικοί αλγεβρικοί αριθμοί.

Μια σημαντική παρατήρηση αφορά την πολυπλοκότητα των υπολογισμών. Οι πραγματικοί αλγεβρικοί αριθμοί προκύπτουν ως ρίζες ακέραιων πολυωνύμων, συνεπώς η πολυπλοκότητα των υπολογισμών εξαρτάται από κάποιο μέτρο της πολυπλοκότητας της αναπαράστασης των πολυωνύμων· το βαθμό τους και το μήκος της αναπαράστασης των συντελεστών τους.

Σε ποιούς αλγορίθμους εμφανίζονται οι πραγματικοί αλγεβρικοί αριθμοί; Εμφανίζονται όταν υπάρχουν μη γραμμικοί υπολογισμοί, πολυωνυμικής μορφής, όπως για παράδειγμα στη γεωμετρική σχεδίαση και μοντελοποίηση, στη ρομποτική, στην απαλοιφή ποσοδεικτών σε λογική πρώτης τάξης στο χώρο των πραγματικών αριθμών, στην (πραγματική) επίλυση πολυωνυμικών συστημάτων, καθώς αυτή ανάγεται στην επίλυση ενός πολυωνύμου σε μία μεταβλητή, σε αναδρομικές ακολουθίες πολυωνυμικών υπολογισμών (cascaded computations). Στη μη γραμμική υπολογιστική γεωμετρία, όπου ασχολούμαστε με πολυωνυμικές (αλγεβρικές) καμπύλες και επιφάνειες, οι υπολογισμοί με πραγματικούς αλγεβρικούς αριθμούς έχουν κεντρικό ρόλο. Πρέπει να τονίσουμε ότι οι μη γραμμικότητες δεν προκύπτουν μόνο από μη γραμμικά (γεωμετρικά) αντικείμενα όπως οι αλγεβρικές καμπύλες και επιφάνειες· μπορούν να προκύψουν και από γραμμικά αντικείμενα, όπως οι ευθείες και τα ευθύγραμμα τμήματα. Παραδείγματα τέτοιων προβλημάτων είναι ο υπολογισμός του διαγράμματος Voronoi ευθυγράμμων τμημάτων στο επίπεδο ή ευθειών στο χώρο. Ενθαρρύνουμε τον ενδιαφερόμενο αναγνώστη να ανατρέξει στην προσκεκλημένη ομιλία[2] του 22ου Ευρωπαϊκού Συνεδρίου Υπολογιστικής Γεωμετρίας, που αναφέρεται στη στενή

[2] www-sop.inria.fr/geometrica/team/Monique.Teillaud/talks/EWCG.pdf

σχέση της σύγχρονης υπολογιστικής γεωμετρίας, κυρίως μη γραμμικής, και της γεωμετρικής σχεδίασης με την επίλυση πολυωνύμων και πολυωνυμικών συστημάτων και υπολογισμών με πραγματικούς αλγεβρικούς αριθμούς. Επιπρόσθετα, όλοι οι παραπάνω υπολογισμοί πρέπει να πραγματοποιούνται με ακρίβεια προκειμένου αφενός μεν να αναγνωρίζουμε και να χειριζόμαστε εκφυλισμένες καταστάσεις (degeneracies), όπως για παράδειγμα την ισότητα πραγματικών αλγεβρικών αριθμών, την ύπαρξη πολλαπλών ριζών, την εφαπτομενική τομή καμπυλών και επιφανειών, αφετέρου δε να πιστοποιείται ότι υπολογίζουμε το σωστό αποτέλεσμα.

Οι πραγματικοί αλγεβρικοί αριθμοί μας επιτρέπουν να κάνουμε περισσότερους υπολογισμούς από ό,τι αν δουλεύαμε μόνο με τους ρητούς ή διαφορετικά μας επιτρέπουν να περιγράψουμε περισσότερα προβλήματα. Η σύνδεση των πραγματικών αλγεβρικών αριθμών με τη γεωμετρία έχει τις ρίζες της πολύ βαθιά στο χρόνο. Η μεγάλη μαθηματική και φιλοσοφική σχολή (αν ο διαχωρισμός μεταξύ μαθηματικών και φιλοσοφίας υφίσταται) του Πυθαγόρα του Σάμιου (περίπου 560–480 πΧ) πίστευε ότι, οι ολόκληροι αριθμοί (ακέραιοι) και οι λόγοι τους (ρητοί) μπορούσαν να περιγράψουν οποιαδήποτε γεωμετρική κατασκευή και άρα δεν υπήρχε ανάγκη για άλλους αριθμούς. Ο πυρήνας της φιλοσοφικής τους σκέψης ήταν η θεώρηση ότι οι ολόκληροι αριθμοί κυβερνούν τον κόσμο. Η μεγαλύτερη ανακάλυψη της σχολής ήταν, ίσως το πιο γνωστό μαθηματικό θεώρημα, το πυθαγόρειο θεώρημα. Αυτή ακριβώς η ανακάλυψη οδήγησε στη διάλυση της σχολής. Ο αριθμός που διέλυσε τον πυρήνα της πυθαγόρειας φιλοσοφικής σκέψης ήταν ο $\sqrt{2}$, ο οποίος ονομάζεται *σταθερά του Πυθαγόρα* και μπορεί να κατασκευαστεί (γεωμετρικά) ως η υποτείνουσα ενός ισοσκελούς ορθογωνίου τριγώνου με κάθετες πλευρές μήκους 1. Ο Πυθαγόρας απέδειξε ότι ο $\sqrt{2}$ δεν μπορεί να γραφτεί ως λόγος δύο ολόκληρων (ακεραίων) αριθμών. Συνεπώς, απέδειξε ότι υπάρχουν και άλλοι αριθμοί εκτός από τους ρητούς, γεγονός που ερχόταν σε ευθεία σύγκρουση με τη φιλοσοφική θεώρηση που πρέσβευε. Η απόδειξη αυτή, εκτός από τον Πυθαγόρα, είναι στενά συνδεδεμένη και με έναν άλλο φιλόσοφο που συμμετείχε στη σχολή του, τον Ίππασο τον Μεταπόντιο, ο οποίος γεννήθηκε, μάλλον, γύρω στο 500 πΧ στη Μεγάλη Ελλάδα. Κατά μία εκδοχή ήταν ο Ίππασος που βρήκε την απόδειξη για τον $\sqrt{2}$ κατά τη διάρκεια ενός θαλάσσιου ταξιδιού και τον σκότωσαν φανατικοί πυθαγόριοι πετώντας τον στη θάλασσα. Κατά μια άλλη εκδοχή ο Ίππασος διέδωσε την ύπαρξη του $\sqrt{2}$ εκτός του πυθαγόρειου κοινοβίου, γεγονός το οποίο οδήγησε στη θανάτωσή του, καθώς οι πυθαγόριοι έδιναν όρκο σιωπής κατά την είσοδό τους στη σχολή. Σε κάθε περίπτωση, ο Ίππασος πλήρωσε με τη ζωή του την ύπαρξη και άλλων αριθμών πέρα από τους ρητούς.

Σήμερα, τους αριθμούς που δεν μπορούν να γραφτούν ως ρητοί, δηλαδή ως κλάσμα δύο ακεραίων, τους ονομάζουμε άρρητους (irrational). Υπενθυμίζουμε ότι η ακολουθία των δεκαδικών ψηφίων των άρρητων αριθμών δεν τερματίζει και δεν γίνεται περιοδική. Δεν είναι εύκολο να αποδείξουμε ότι κάποιος αριθμός είναι άρρητος. Για παράδειγμα είναι ακόμα ανοιχτό πρόβλημα το αν ο αριθμός $\pi^{\sqrt{2}}$ είναι άρρητος. Η παρούσα διατριβή δεν ασχολείται με τους άρρητους αριθμούς, αλλά με ένα υποσύνολό τους, τους πραγματικούς αλγεβρικούς αριθμούς[3]. Ωστόσο, προκειμένου να βοηθήσουμε τον Πυθαγόρα στο *δίλημμά* του αφενός θεωρούμε ότι το θεμελιακό αριθμητικό αντικείμενο είναι οι ρητοί αριθμοί και κάνουμε υπολογισμούς μόνο με αυτούς, αφετέρου συνδέουμε τους πραγματικούς αλγεβρικούς αριθμούς με γεωμετρικά προβλήματα. Εφόσον

[3]Το σύνολο των πραγματικών αλγεβρικών αριθμών είναι υποσύνολο του συνόλου των άρρητων αριθμών μόνο αν του αφαιρέσουμε το σύνολο ρητών. Ελπίζουμε ο αναγνώστης να συγχωρέσει αυτή την παράλειψη.

ο $\sqrt{2}$ είναι πραγματικός αλγεβρικός αριθμός μπορούμε και αυτόν να τον χειριστούμε κάνοντας υπολογισμούς μόνο με ρητούς. *Ίσως*, αν ο Πυθαγόρας ήταν γνώστης αυτών των μαθηματικών, η δολοφονία του Ίππασου να είχε αποτραπεί.

Ποιό είναι το σύνολο των πραγματικών αλγεβρικών αριθμών; Θα συμβολίζουμε με $\mathbb{N}$ το σύνολο των φυσικών αριθμών, με $\mathbb{Z}$ το σύνολο των ακεραίων, με $\mathbb{Q}$ το σύνολο των ρητών, με $\mathbb{R}$ το σύνολο των πραγματικών και με $\mathbb{C}$ το σύνολο των μιγαδικών αριθμών. Μπορούμε να διατάξουμε τα σύνολα αυτά, ως εξής:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}_{alg} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Στην προηγούμενη σχέση έχουμε εισάγει ένα ακόμα σύνολο, το $\mathbb{R}_{alg}$, το οποίο είναι το σύνολο των πραγματικών αλγεβρικών αριθμών. Παρατηρούμε ότι δεν είναι όλοι οι πραγματικοί αριθμοί στοιχεία του $\mathbb{R}_{alg}$, καθώς δεν μπορούν όλοι οι πραγματικοί να εκφραστούν ως ρίζα κάποιου πολυωνύμου με ακέραιους συντελεστές. Για παράδειγμα ένας τέτοιος αριθμός είναι ο π. Αυτοί οι αριθμοί ονομάζονται *υπερβατικοί*. Τέτοιοι αριθμοί δεν θα μας απασχολήσουν στην παρούσα διατριβή. Στόχος είναι η ανάλυση και υλοποίηση υπολογισμών με στοιχεία του $\mathbb{R}_{alg}$ και εφαρμογές των υπολογισμών στην υπολογιστική γεωμετρία.

Αντί περιεχομένων

Αλγεβρικοί αλγόριθμοι ονομάζονται οι αλγόριθμοι για αλγεβρικά προβλήματα. Ή διαφορετικά, με τον όρο αλγεβρικοί αλγόριθμοι αναφερόμαστε στην αλγοριθμική προσέγγιση της άλγεβρας [5, 14, 38, 64, 66, 71, 112, 160, 187, 263, 275]. Οι εφαρμογές των αλγεβρικών αλγορίθμων περιλαμβάνουν τη συμβολική επεξεργασία, την αυτοματοποιημένη απόδειξη θεωρημάτων, την κρυπτογραφία, τη ρομποτική, την υπολογιστική γεωμετρία, την υπολογιστική βιολογία, τη σχεδίαση με υπολογιστή, τη γεωμετρική μοντελοποίηση και πολλές άλλες επιστημονικές περιοχές. Μερικά μόνο από τα προβλήματα που απασχολούν την επιστημονική περιοχή των αλγεβρικών αλγορίθμων είναι η αριθμητική με ακέραιους και ρητούς απεριόριστης ακρίβειας, οι υπολογισμοί σε χώρους πηλίκα (modulo ένα στοιχείο του χώρου), οι υπολογισμοί με πίνακες, οι υπολογισμοί με πολυώνυμα μίας και πολλών μεταβλητών, η επίλυση πολυωνύμων και πολυωνυμικών συστημάτων στους πραγματικούς ή/και στους μιγαδικούς, η παραγοντοποίηση ακεραίων και πολυωνύμων, η απαλοιφή ποσοδεικτών σε λογική πρώτης τάξης στους πραγματικούς αριθμούς· και φυσικά αλγόριθμοι και δομές δεδομένων για την αποθήκευση και τον χειρισμό των βασικών αντικειμένων, όπως τα πολυώνυμα, οι πίνακες, τα ιδεώδη και οι πραγματικοί αλγεβρικοί αριθμοί.

Τα σημαντικότερα ανοιχτά προβλήματα στην περιοχή των αλγεβρικών αλγορίθμων, που βασίζονται στην αριθμητική ακριβείας, αφορούν στην κατανόηση της θεωρητικής και πρακτικής πολυπλοκότητάς τους και τη σύγκρισή τους με τους αλγορίθμους της αριθμητικής ανάλυσης. Στόχος της περιοχής είναι να 'ανταγωνιστεί' τους αλγορίθμους που βασίζονται σε αριθμητική κινητής υποδιαστολής και να συμβάλλει σε μια υβρική προσέγγιση που θα στηρίζεται και στις δύο προσεγγίσεις (symbolic-numeric approach). Η παρούσα διδακτορική διατριβή εντάσσεται στο παραπάνω πλαίσιο και το περιεχόμενο και η συνεισφορά της συνοψίζονται ως εξής:

Στο Κεφ. 2 παρουσιάζουμε το απαραίτητο αλγεβρικό υπόβαθρο για την κατανόηση της διατριβής. Παρουσιάζουμε τις πολυπλοκότητες των βασικών υπολογισμών με ακέραια πολυώνυμα μιας μεταβλητής, την έννοια της επιλύουσας (resultant), τις πολυωνυμικές ακολουθίες υπολοίπων και

διάφορους αλγορίθμους για τον υπολογισμό τους. Τέλος, αναφερόμαστε συνοπτικά στην αναπαράσταση πολυωνύμων στη βάση Bernstein. Με την εξαίρεση της Πρότ. 2.36 τα αποτελέσματα του κεφαλαίου δεν είναι πρωτότυπα.

Στο Κεφ. 3 μελετάμε φράγματα στις πραγματικές ρίζες πολυωνύμων και αλγορίθμους για την απομόνωση των πραγματικών ριζών ακέραιων πολυωνύμων σε μία μεταβλητή. Τα πρωτότυπα αποτελέσματα αφορούν τη μελέτη της ποιότητας των φραγμάτων για τις θετικές πραγματικές ρίζες, ένα θεώρημα για τα σύνθετα φράγματα διαχωρισμού, την ενοποίηση και απλοποίηση της θεωρίας για τους αλγορίθμους επίλυσης πολυωνύμου, που βασίζονται στην υποδιαίρεση και τη βελτίωση της πολυπλοκότητας κατά δύο παράγοντες του αλγορίθμου των συνεχών φραγμάτων. Επιπρόσθετα, αποδεικνύουμε ότι το φράγμα πολυπλοκότητας ισχύει και για πολυώνυμα με τετράγωνα και ότι με την ίδια πολυπλοκότητα υπολογίζουμε και την πολλαπλότητα των ριζών.

Στο Κεφ. 4 μελετάμε αλγορίθμους για υπολογισμούς με έναν και δύο πραγματικούς αλγεβρικούς αριθμούς. Όσον αφορά στους υπολογισμούς με έναν αλγεβρικό αριθμό, αν και οι περισσότεροι αλγόριθμοι είναι γνωστοί, η πολυπλοκότητά τους δεν έχει μελετηθεί. Παρουσιάζουμε σε ενιαίο πλαίσιο τους αλγορίθμους για υπολογισμούς με έναν αλγεβρικό αριθμό και την πολυπλκοκότητά τους. Σε κάθε περίπτωση βελτιώνουμε τα φράγματα πολυπλοκότητας κατά δύο ή τρεις παράγοντες. Στη συνέχεια παρουσιάζουμε τις πολυπλοκότητες για τον υπολογισμό πολυωνυμικών ακολουθιών υπολοίπων, πολυωνύμων σε δύο μεταβλητές, δύο αλγόριθμους για την πραγματική επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές και αλγορίθμους για υπολογισμούς με δύο αλγεβρικούς αριθμούς. Όλοι οι αλγόριθμοι είναι καινούργιοι και τα προκύπτοντα φράγματα βελτιώνουν σε κάθε περίπτωση τα ήδη γνωστά.

Στο Κεφ. 5 παρουσιάζουμε αλγορίθμους για την επίλυση πολυωνυμικών εξισώσεων βαθμού ≤ 4 και πολυωνυμικών συστημάτων σε δύο μεταβλητές, όπου τα πολυώνυμα είναι βαθμού ≤ 2 καθώς επίσης και υπολογισμούς με πραγματικούς αλγεβρικούς αριθμούς βαθμού ≤ 4. Αποδεικνύουμε ότι όλοι οι παραπάνω υπολογισμοί έχουν πολυπλοκότητα $\mathcal{O}(1)$. Ας σημειωθεί ότι αφενός μεν δεν αναπαριστούμε τις ρίζες των πολυωνύμων με ριζικά αφετέρου δε οι υπολογισμοί εμπεριέχουν μόνο αριθμητική ακεραίων. Το σύνολο των αποτελεσμάτων είναι πρωτότυπο.

Στο Κεφ. 6 παρουσιάζουμε την υλοποίηση των αλγεβρικών αλγορίθμων που παρουσιάστηκαν στα κεφάλαια 3, 4 και 5 και αφορούν την πραγματική επίλυση ακέραιων πολυωνύμων και πολυωνυμικών συστημάτων και τη σύγκριση πραγματικών αλγεβρικών αριθμών. Η υλοποίησή μας είναι σε C++ και αποτελεί μέρος της αλγεβρικής βιβλιοθήκης SYNAPS [4]. Παρουσιάζουμε πειραματικά αποτελέσματα για πολυώνυμα βαθμού ≤ 4 αλλά και για πολυώνυμα βαθμού 1000 και δυαδικού μήκους συντελεστών 8000 bits.

Στο Κεφ. 7 παρουσιάζουμε δύο εφαρμογές των αλγεβρικών μεθόδων σε κατηγορήματα που απαιτούνται από τους αλγορίθμους υπολογισμού της διάταξης ελλειπτικών τόξων στο επίπεδο και στον υπολογισμό του διαγράμματος Voronoi ελλείψεων στο επίπεδο. Η υλοποίηση των αλγορίθμων είναι σε C++ και βασίζεται στην γεωμετρική βιβλιοθήκη CGAL [5]. Όλα τα αποτελέσματα είναι πρωτότυπα.

Στο Κεφ. 8 δοθέντος ενός κυρτού πολυγώνου με ακέραιες κορυφές στο επίπεδο (ακέραιο πολύγωνο), εξετάζουμε αλγορίθμους που μας επιτρέπουν να το διασπάσουμε σε δύο άλλα κυρτά

[4] www-sop.inria.fr/galaad/logiciels/synaps/
[5] www.cgal.org

πολύγωνα τέτοια ώστε το άθροισμά τους κατά Minkowski να είναι το αρχικό πολύγωνο. Κάθε πολυώνυμο σε δύο μεταβλητές αντιστοιχίζεται σε ένα ακέραιο πολύγωνο, το πολύγωνο (πολύτοπο) του Newton. Η διάσπαση του πολυτόπου του Newton είναι αναγκαία συνθήκη προκειμένου το αντίστοιχο πολυώνυμο να παραγοντοποιείται. Βελτιώνουμε τη μέχρι σήμερα γνωστή πολυπλοκότητα και παρουσιάζουμε βέλτιστους αλγορίθμους για την περίπτωση που ένας προσθετέος έχει σταθερό πλήθος ακμών.

ΚΕΦΑΛΑΙΟ 2

Αλγεβρικό υπόβαθρο

Τα μαθηματικά είναι η μουσική της αιτίας.

James Joseph Sylvester

Στα μαθηματικά δεν καταλαβαίνεις πράγματα. Απλά τα συνηθίζεις.

John von Neumann

Περίληψη

Παρουσιάζουμε συνοπτικά τη βασική θεωρία και τους αλγορίθμους που απαιτούνται για την κατανόηση των υπολοίπων κεφαλαίων της διατριβής. Καταρχάς παρουσιάζουμε την δυαδική πολυπλοκότητα των βασικών πράξεων μεταξύ πολυωνύμων. Ορίζουμε την έννοια του μέγιστου κοινού διαιρέτη και της επιλύσουσας δύο πολυωνύμων. Επίσης παρουσιάζουμε τις πολυωνυμικές ακολουθίες υπολοίπων, τη βασική θεωρία και ιδιότητες που τις διέπουν, διάφορους τρόπους κατασκευής τους και τη δυαδική πολυπλοκότητα των βασικών αλγορίθμων που τις εμπεριέχουν. Τέλος, αναφερόμαστε συνοπτικά στην αναπαράσταση πολυωνύμων στη βάση Bernstein.

Με την εξαίρεση της Πρότ. 2.36, η οποία παρουσιάστηκε στην εργασία [97] τα αποτελέσματα του κεφαλαίου δεν είναι πρωτότυπα.

Η πολυπλοκότητα ενός προβλήματος είναι συνάρτηση κάποιου μέτρου των δεδομένων της εισόδου και της εξόδου του. Τα προβλήματα τα οποία θα μας απασχολήσουν έχουν ως είσοδο ακέραιους ή ρητούς αριθμούς ή/και ακέραια ή ρητά πολυώνυμα. Στο μοντέλο υπολογισμού των αλγορίθμων που θα παρουσιάσουμε μπορούμε να αναπαραστήσουμε και να κάνουμε υπολογισμούς με ακεραίους απεριόριστης ακρίβειας, γι' αυτό και οι αλγόριθμοι ονομάζονται ακριβείς αλγόριθμοι (exact algorithms). Λόγω του γεγονότος ότι τα αντικείμενά μας δεν

έχουν καθορισμένη διάσταση, οι βασικές πράξεις με αυτά, όπως για παράδειγμα η πρόσθεση και ο πολλαπλασιασμός, δεν έχουν σταθερή πολυπλοκότητα αλλά εξαρτώμενη από το μήκος της αναπαράστασής τους.

Θα παρουσιάσουμε την πολυπλοκότητα των βασικών πράξεων ακεραίων αριθμών. Ακολούθως θα παρουσιάσουμε τη βασική θεωρία των πολυωνύμων και αλγορίθμους πάνω σε πολυώνυμα που θα μας χρειαστούν στα επόμενα κεφάλαια.

Χρησιμοποιούμε το συμβολισμό $\mathcal{O}$ για την αριθμητική και τον συμβολισμό $\mathcal{O}_B$ για την δυαδική (Boolean) πολυπλοκότητα. Ο συμβολισμός $\tilde{\mathcal{O}}$ και $\tilde{\mathcal{O}}_B$ αγνοεί τους λογαριθμικούς παράγοντες. Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία [57, 122].

2.1 Περί των αριθμών

Το βασικό αντικείμενο σε όλους τους αλγορίθμους είναι οι ακέραιοι αριθμοί, για τους οποίους υποθέτουμε ότι δίδονται σε δυαδική αναπαράσταση, δηλαδή αναπαρίστανται ως μία λίστα από 0 και 1. Ένας ρητός αριθμός αναπαρίσταται με δύο συνεχόμενες λίστες που αντιστοιχούν στον αριθμητή και στον παρανομαστή του, οι οποίες χωρίζονται από μία κενή θέση. Για έναν ακέραιο $a \in \mathbb{Z}$ ορίζουμε ως μήκος της δυαδικής αναπαράστασής του ή *δυαδικό μήκος* (bit size) την ποσότητα $\mathcal{L}(a) = 1 + \lceil \lg(|a|) + 1 \rceil$, όπου το $+1$ χρειάζεται για την αναπαράσταση του προσήμου. Αν $a = \frac{b}{c} \in \mathbb{Q}$ τότε $\mathcal{L}(a) = \max\{\mathcal{L}(b), \mathcal{L}(c)\}$. Με $|a|$ συμβολίζουμε το μέτρο του a, και αν $a \in \mathbb{Z}$ ή $a \in \mathbb{Q}$, τότε μέτρο είναι η απόλυτη τιμή του.

Θεώρημα 2.1

Έστω $a, b \in \mathbb{Z}$ τέτοιοι ώστε $\mathcal{L}(a) = \mathcal{L}(b) = \tau$. Η πολυπλοκότητα των πράξεων της πρόσθεσης και της αφαίρεσης ($a + b, a - b$) είναι $\Theta(\tau)$.

Αν $a, b \in \mathbb{Z}$ τότε θα συμβολίζουμε με $\mathsf{quo}(a, b)$ και $\mathsf{rem}(a, b)$ το πηλίκο και το υπόλοιπο, αντίστοιχα, της ακέραιας διαίρεσης των a και b.

Θεώρημα 2.2

Έστω $a, b \in \mathbb{Z}$ τέτοιοι ώστε $\mathcal{L}(a) = \mathcal{L}(b) = \tau$. Η πολυπλοκότητα των πράξεων του πολλαπλασιασμού, $a \cdot b$, της διαίρεσης με υπόλοιπο, $\mathsf{quo}(a, b) \wedge \mathsf{rem}(a, b)$, του τετραγωνισμού, a^2, και του αντιστρόφου, a^{-1}, είναι $\tilde{\mathcal{O}}_B(\mathsf{M}(\tau))$.

Σε ό,τι θα ακολουθήσει υποθέτουμε ότι γρήγοροι αλγόριθμοι πολλαπλασιασμού είναι διαθέσιμοι, για παράδειγμα αλγόριθμοι που βασίζονται στο Γρήγορο Μετασχηματισμό Fourier (Fast Fourier Transform, FFT). Συνεπώς, η πολυπλοκότητα του πολλαπλασιασμού και της διαίρεσης ακεραίων αριθμών είναι $\mathsf{M}(\tau) = \mathcal{O}_B(\tau \lg^c \tau) = \tilde{\mathcal{O}}_B(\tau)$. Για περισσότερες πληροφορίες καθώς και για τις αποδείξεις των θεωρημάτων ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία, δείτε για παράδειγμα [160, 263, 275].

2.2 Περί των πολυωνύμων

Σε ό,τι θα ακολουθήσει θα συμβολίζουμε με $\mathcal{K}$ ένα αλγεβρικά κλειστό σώμα, δηλαδή κάποια αλγεβρική δομή τέτοια ώστε όλα τα πολυώνυμα σε μία μεταβλητή με συντελεστές από το $\mathcal{K}$ να έχουν λύσεις στο $\mathcal{K}$. Με $\mathcal{R}$ θα συμβολίζουμε έναν υποδακτύλιο με μονάδα του $\mathcal{K}$ και με $\mathcal{F}$ το σώμα πηλίκων του $\mathcal{R}$. Ένα παράδειγμα μιας τέτοιας ιεραρχίας αλγεβρικών δομών είναι $\mathcal{R} = \mathbb{Z}$, $\mathcal{F} = \mathbb{Q}$ και $\mathcal{K} = \mathbb{C}$ [108, 258].

Αν $\mathcal{S}$ είναι κάποια αλγεβρική δομή τότε θα συμβολίζουμε με $\mathcal{S}[X_1, \ldots, X_k]$ το χώρο των πολυωνύμων με k μεταβλητές με συντελεστές από το $\mathcal{S}$. Το χώρο των πολυωνύμων πολλών μεταβλητών τα οποία θέλουμε να τα δούμε ως μιας μεταβλητής με συντελεστές πολυώνυμα σε πολλές (τις υπόλοιπες) μεταβλητές τον συμβολίζουμε ως $(\mathcal{S}[X_1, \ldots, X_{k-1}])[X_k]$.

Έστω ένα πολυώνυμο μιας μεταβλητής $f \in \mathcal{S}[X]$:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \tag{2.1}$$

αν $a_n \neq 0$ τότε ο βαθμός του πολυωνύμου είναι n, $\deg(f) = n$, και ο μεγιστοβάθμιος όρος του είναι $\mathrm{lead}(f) = a_n$. Όταν $\mathrm{lead}(f) = 1$ το πολυώνυμο ονομάζεται *μονικό* (monic). Ορίζουμε ως $f = 0$ το μηδενικό πολυώνυμο και εξ ορισμού $\deg(0) = -\infty$ και $\mathrm{lead}(0) = 1$.

Αν $f \in \mathcal{S}[X_1, \ldots, X_k]$ τότε με $\deg(f)$ δηλώνουμε το συνολικό βαθμό (total degree), ενώ με $\deg_{X_k}(f)$ συμβολίζουμε το βαθμό του f αν θεωρήσουμε ότι $f \in (\mathcal{S}[X_1, \ldots, X_{k-1}])[X_k]$.

Υποθέτουμε ότι $f \in \mathbb{C}[X]$ και ορίζουμε τις ακόλουθες μετρικές

$$\|f\|_\infty = \max\{|a_n|, \ldots, |a_1|, |a_0|\} \tag{2.2}$$

$$\|f\|_2 = \sqrt{|a_n|^2 + \cdots + |a_1|^2 + |a_0|^2} \tag{2.3}$$

για τις οποίες ισχύει η ανισότητα

$$\|f\|_\infty < \|f\|_2 < \sqrt{n+1}\,\|f\|_\infty \tag{2.4}$$

Για μια πληρέστερη και πιο εκτενή εισαγωγή στη θεωρία των πολυωνύμων ο αναγνώστης μπορεί να ανατρέξει, για παράδειγμα στους Cox et al. [59], Fraleigh [108], Prasolov [218], van der Waerden [258], Zippel [276].

Βασικές πράξεις

Θα μας απασχολήσουν κυρίως πολυώνυμα στο $\mathbb{Z}[X]$. Προκειμένου να αναπαραστήσουμε τα πολυώνυμα χρησιμοποιούμε την πυκνή αναπαράσταση, δηλαδή υποθέτουμε ένα διάνυσμα που περιέχει (σε δυαδική αναπαράσταση) τους συντελεστές του πολυωνύμου και ότι η πρόσβαση σε κάποιο συντελεστή έχει πολυπλοκότητα $\mathcal{O}(1)$. Όταν $f \in \mathbb{Z}[X]$ θα συμβολίζουμε με $\mathcal{L}(f)$ το μέγιστο δυαδικό μήκος των συντελεστών του f, δηλαδή $\mathcal{L}(f) = \lg(\|f\|_\infty)$. Επίσης, με τον όρο δυαδικό μήκος ενός πολυωνύμου θα υπονοούμε το μέγιστο δυαδικό μήκος των συντελεστών του.

Θεωρούμε $f, g \in \mathbb{Z}[X]$

$$\begin{aligned} f &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \\ g &= b_m X^m + b_{n-1} X^{m-1} + \cdots + b_1 X + b_0 \end{aligned} \tag{2.5}$$

τέτοια ώστε $\deg(f) = n \geq m = \deg(g)$, $\mathcal{L}(f) \leq \tau$, $\mathcal{L}(g) \leq \tau$ και έστω $c \in \mathbb{Z}$, $\mathcal{L}(c) = \sigma$.

Θα παρουσιάσουμε συνοπτικά την πολυπλοκότητα μερικών βασικών πράξεων. Ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία για περισσότερες λεπτομέρειες [25, 160, 212, 263, 275, 276].

Πρόσθεση και αφαίρεση

Το $h \in \mathbb{Z}[X]$, όπου $h = f \pm g$, υπολογίζεται με πολυπλοκότητα $\mathcal{O}_B(n\tau)$. Ισχύει $\deg(h) \leq n$ (ισότητα στην περίπτωση της πρόσθεσης) και $\mathcal{L}(h) \leq \tau + 1$.

Πολλαπλασιασμός

Το $h \in \mathbb{Z}[X]$, όπου $h = f \cdot g$, υπολογίζεται με πολυπλοκότητα $\mathcal{O}_B(\mathsf{M}(n, \tau))$. Ισχύει $\deg(h) = mn$ και $\mathcal{L}(h) \leq 2\tau + \lg n$. Όπως και στην περίπτωση του πολλαπλασιασμού ακεραίων θα υποθέσουμε γρήγορους αλγορίθμους πολλαπλασιασμού πολυωνύμων βασισμένους στο γρήγορο μετασχηματισμό Fourier, οπότε $\mathcal{O}_B(\mathsf{M}(n, \tau)) = \widetilde{\mathcal{O}}_B(n\tau)$ [212, 240].

Απεικονίσεις-μετασχηματισμοί

- Αντιστροφή: $h = \mathcal{R}(f)(X) := X^n f(\frac{1}{X})$

  Η πολυπλοκότητα του μετασχηματισμού είναι $\mathcal{O}(n)$ ή $\mathcal{O}_B(n\tau)$. Ωστόσο, με κατάλληλη αναπαράσταση του πολυωνύμου μπορούμε να επιτύχουμε πολυπλοκότητα $\mathcal{O}(1)$. Επιπρόσθετα $\deg(h) = n$ και $\mathcal{L}(h) = \tau$. Θεωρούμε ότι $a_0 \neq 0$.

- Μετατόπιση: $h = \mathcal{T}_c(f)(X) := f(X + c)$

  Η πολυπλοκότητα του μετασχηματισμού είναι $\mathcal{O}_B(\mathsf{M}\left(n^2 \lg n + n\tau + n^2\sigma\right))$ ή παραλείποντας τους (πολυ-) λογαριθμικούς παράγοντες $\widetilde{\mathcal{O}}_B(n^2 \lg n + n\tau + n^2\sigma)$ [262]. Επιπρόσθετα $\deg(h) = n$ και $\mathcal{L}(h) = \mathcal{O}(\tau + n\sigma)$.

  Η μετατόπιση είναι από τους πιο σημαντικούς μετασχηματισμούς. Οι γρήγοροι αλγόριθμοι για αυτή την πράξη στην βιβλιογραφία αναφέρονται και με τον όρο *fast Taylor shifts*.

- Ομοθεσία: $h = \mathcal{H}_c(f)(X) := f(cX)$ και $h = \mathcal{H}'_c(f)(X) := c^n f(\frac{X}{c}) = \mathcal{R}(\mathcal{H}_c(\mathcal{R}(f)))(X)$

  Η πολυπλοκότητα του μετασχηματισμού είναι $\mathcal{O}_B(n\,\mathsf{M}(\max\{\tau, n\sigma\}))$ ή $\widetilde{\mathcal{O}}_B(n\,\max\{\tau, n\sigma\})$. Επιπρόσθετα $\deg(h) = n$ και $\mathcal{L}(h) = \mathcal{O}(\tau + n\sigma)$.

- Παράγωγος: Συμβολίζουμε με $f^{(k)}$ την k παράγωγο του f. Η αποτίμηση όλων των παραγώγων πάνω σε κάποιο αριθμό c έχει την ίδια πολυπλοκότητα με τη μετατόπιση. Πολλές φορές μας ενδιαφέρει η αποτίμηση των κανονικοποιημένων παραγώνων, $f^{(k)}(X)/k!$ (normalized derivatives), πράξη η οποία είναι (σχεδόν) ισοδύναμη με την μετατόπιση, καθώς εμφανίζονται στην ανάπτυξη κατά Taylor του $f(x + c)$ [25, 212, 243, 262].

Αποτίμηση

Ο ομομορφισμός εκτίμησης $\phi_c : \mathbb{Z}[X] \to \mathbb{Z}$, όπου $f \mapsto f(c)$, για κάθε $f \in \mathbb{Z}[X]$, θα ονομάζεται *αποτίμηση* (του f) πάνω στο c. Ο υπολογισμός της αποτίμησης $f(c)$, με τη βοήθεια του σχήματος Horner έχει πολυπλοκότητα $\mathcal{O}_B(n\,\mathsf{M}(\max\{\tau, n\sigma\}))$ και $\mathcal{L}(f(c)) \leq \tau + n\sigma + \lg n$. Ο υπολογισμός της αποτίμησης του f πάνω σε ένα σύνολο από n διαφορετικούς ακεραίους, $c_1, \ldots, c_n$, όπου $\mathcal{L}(c_i) \leq \sigma$, έχει πολυπλοκότητα $\mathcal{O}_B(n\,\lg^2 n\,\mathsf{M}(\max\{\tau, n\sigma\}))$ ή $\widetilde{\mathcal{O}}_B(n \max\{\tau, n\sigma\})$ [25, 263, 275] και βασίζεται στην τεχνική 'διαίρει και βασίλευε'. Επίσης, την ίδια πολυπλοκότητα έχει ο υπολογισμός της αποτίμησης όλων των παραγώγων του f πάνω στο c, δηλαδή $\widetilde{\mathcal{O}}_B(n \max\{\tau, n\sigma\})$ [25, 212, 243, 262].

Διαίρεση

Αν οι συντελεστές των πολυωνύμων ανήκουν σε κάποιο σώμα τότε μπορούμε να ορίσουμε και τη διαίρεση των πολυωνύμων:

Θεώρημα 2.3 (Διαίρεση πολυωνύμων)
Έστω $f, g \in \mathcal{F}[X]$ και $g \neq 0$. Υπάρχουν μοναδικά πολυώνυμα $Q, R \in \mathcal{F}[X]$ τέτοια ώστε

$$f = gQ + R$$

και $\deg(R) < \deg(g)$. Το Q, αντίστοιχα R, ονομάζεται πηλίκο, αντίστοιχα υπόλοιπο και συμβολίζεται με $\mathsf{quo}(f, g)$, αντίστοιχα $\mathsf{rem}(f, g)$.

Ωστόσο, αν οι συντελεστές δεν ανήκουν σε σώμα, π.χ $f, g \in \mathbb{Z}[X]$, τότε η διαίρεση δεν μπορεί να οριστεί. Προκειμένου να οριστεί η διαίρεση για κάθε αντιμεταθετικό δακτύλιο ο Jacobi [138] εισήγαγε την έννοια της ψευδο-διαίρεσης.

Θεώρημα 2.4 (Ψευδο-διαίρεση πολυωνύμων)
Έστω $f, g \in \mathcal{R}[X]$. Υπάρχουν μοναδικά πολυώνυμα $Q, R \in \mathcal{R}[X]$ τέτοια ώστε

$$\mathsf{lead}(g)^{\delta-1} f = gQ + R$$

και $\deg(R) < \deg(g)$, όπου $\delta = \max\{1, \deg(f) - \deg(g)\}$. Το Q, αντίστοιχα R, ονομάζεται ψευδο-πηλίκο, αντίστοιχα ψευδο-υπόλοιπο, και συμβολίζεται με $\mathsf{pquo}(f, g)$, αντίστοιχα $\mathsf{prem}(f, g)$.

Η πολυπλοκότητα της ψευδο-διαίρεσης είναι $\mathcal{O}_B(m\,\mathsf{M}(n\tau))$ ή $\widetilde{\mathcal{O}}_B(m\,n\,\tau)$ και $\mathcal{L}(\mathsf{prem}(f, g)) = \mathcal{O}(n\,\tau)$, $\mathcal{L}(\mathsf{pquo}(f, g)) = \mathcal{O}(n\,\tau)$ [25, 263, 275].

Θα λέμε ότι το $g \in \mathcal{R}[X]$ διαιρεί ακριβώς το $f \in \mathcal{R}[X]$ αν $\mathsf{rem}(f, g) = 0$ ή $\mathsf{prem}(f, g) = 0$. Για το δυαδικό μήκος των διαιρετών ενός πολυωνύμου ισχύει το φράγμα του Mignotte [188, 189]. Πιο συγκεκριμένα, αν $f = g \cdot Q$ και $f, g, Q \in \mathbb{Z}[X]$ τότε $\mathcal{L}(Q) = \mathcal{O}(n\,\mathcal{L}(f))$ και το ίδιο ισχύει για το g.

Μέγιστος κοινός διαιρέτης

Η αμέσως επόμενη πράξη, η οποία είναι πολύ μεγάλης σημασίας, είναι ο υπολογισμός του μέγιστου κοινού διαιρέτη (ΜΚΔ) δύο πολυωνύμων. Ο ΜΚΔ δύο πολυωνύμων είναι το πολυώνυμο που διαιρεί ακριβώς τόσο τα δύο πολυώνυμα όσο και κάθε άλλο πολυώνυμο που τα διαιρεί ακριβώς. Αν $\mathcal{R}$ είναι μια περιοχή μοναδικής ανάλυσης (UFD, Unique Factorization Domain), για παράδειγμα αν $\mathcal{R} = \mathbb{Z}$ ή $\mathcal{R} = \mathbb{Z}[Y]$, τότε το $\mathcal{R}[X]$ είναι επίσης UFD [108, 258]. Κατά συνέπεια, μπορούμε να ορίσουμε τον μέγιστο κοινό διαιρέτη (ΜΚΔ) δύο πολυωνύμων $f, g \in \mathcal{R}[X]$, τον οποίο συμβολίζουμε ως $\gcd(f, g)$.

Ο ΜΚΔ είναι εξέχουσας σημασίας καθώς επιτρέπει, πέρα των άλλων, να δώσουμε απαντήσεις σε προβλήματα όπως αυτό της εύρεσης των διαφορετικών ριζών ενός πολυωνύμου ή όπως του υπολογισμού των κοινών ριζών δύο πολυωνύμων. Πιο συγκεκριμένα ισχύουν τα ακόλουθα:

- Ο αριθμός των κοινών ριζών των $f, g \in \mathcal{R}[X]$ είναι $\deg(\gcd(f, g))$.
- Ο αριθμός των διαφορετικών ριζών του $f \in \mathcal{R}[X]$ είναι $\deg(f) - \deg(\gcd(f, f'))$.

Ο υπολογισμός του μέγιστου κοινού διαιρέτη έχει πολυπλοκότητα σχεδόν όσο και η ψευδοδιαίρεση, δηλαδή $\widetilde{\mathcal{O}}_B(n\,m\,\tau)$ και $\mathcal{L}(\gcd(f, g)) = \mathcal{O}(n\,\tau)$. Λόγω της πολύ μεγάλης σημασίας αυτού του υπολογισμού θα επανέλθουμε σε επόμενες παραγράφους.

Επιλύουσα δύο πολυωνύμων

Ένα από τα πιο βασικά εργαλεία στους αλγεβρικούς αλγορίθμους, και όχι μόνο, είναι η επιλύουσα (resultant). Η επιλύουσα είναι στενά συνδεδεμένη τόσο με τη θεωρία της απαλοιφής (elimination), γι' αυτό ονομάζεται και *απαλοίφουσα* (eliminant), όσο και με τον υπολογισμό του ΜΚΔ και την εύρεση μιγαδικών ριζών. Για περισσότερες λεπτομέρειες σχετικά με την απαλοίφουσα και για τις αποδείξεις των θεωρημάτων που παραλείπουμε ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [5, 14, 38, 59, 66, 114, 160, 178, 187, 190, 251, 263, 275, 276].

Μπορούμε να διατυπώσουμε το ακόλουθο θεώρημα [114, 249, 251]:

Θεώρημα 2.5 (Επιλύουσα)

Θεωρούμε δύο πολυώνυμα $f, g \in \mathcal{K}[X]$ όπως στην Εξ. (2.5) τέτοια ώστε $a_n\, b_m \neq 0$. Υπάρχει ένα μοναδικό, εκτός από το πρόσημο, ανάγωγο πολυώνυμο $\mathtt{res}(f, g) \in \mathbb{Z}[a_n, \ldots, a_1, a_0, b_m, \ldots, b_1, b_0]$ το οποίο είναι μηδέν όταν τα $f(X)$ και $g(X)$ έχουν κάποιου κοινό παράγοντα. Επιπρόσθετα, το $\mathtt{res}(f, g)$ είναι ομογενές και $\deg(\mathtt{res}(f, g)) = \deg(f) + \deg(g) = m + n$.

Το πολυώνυμο αυτό ονομάζεται επιλύουσα (resultant).

Ο ορισμός και η ύπαρξη της επιλύουσας μπορεί να επεκταθεί και σε συστήματα πολυωνύμων πολλών μεταβλητών, δείτε για παράδειγμα [60, 114, 251]. Στη γενική περίπτωση η επιλύουσα είναι η 'ελάχιστη' συνθήκη επιλυσιμότητας (minimum condition of solvability) πάνω στους συντελεστές. Δηλαδή είναι η *ελάχιστη*, ικανή και αναγκαία, συνθήκη, πάνω στους συντελεστές, για την ύπαρξη μιγαδικών λύσεων ενός συστήματος $\ell + 1$ πολυωνυμικών εξισώσεων σε ℓ μεταβλητές. Στην παρούσα διατριβή δεν θα μας απασχολήσουν προβλήματα όπου $\ell > 1$, εκτός από την Εν. 7.3 όπου θα χρησιμοποιήσουμε την επιλύουσα προκειμένου να απαλείψουμε κάποιες μεταβλητές.

Στην περίπτωση πολυωνύμων σε μία μεταβλητή μπορούμε να εκφράσουμε την επιλύουσα δύο πολυωνύμων ως την ορίζουσα ενός πίνακα, του πίνακα Sylvester. Αν τα πολυώνυμα είναι πολλών μεταβλητών τότε δεν γνωρίζουμε έναν τέτοιο πίνακα στη γενική περίπτωση, αν και υπάρχουν αποτελέσματα για την περίπτωση τριών εξισώσεων και δύο μεταβλητών [154] και άλλων ειδικών περιπτώσεων [72, 73].

Ορισμός 2.6 (Πίνακας Sylvester). *Έστω* $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{m} b_i X^i \in \mathcal{K}[X]$. *Ο πίνακας Sylvester των* f *και* g, $\mathtt{Syl}(f,g)$, *είναι ο παρακάτω πίνακας διαστάσεων* $(m+n)\times(m+n)$

$$\mathtt{Syl}(f,g) := \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_m & b_{m-1} & \dots & b_0 \end{pmatrix} \begin{matrix} X^{m-1}f \\ X^{m-2}f \\ \vdots \\ X^0 f \\ X^{n-1}g \\ X^{n-2}g \\ \vdots \\ X^0 g \end{matrix}$$

όπου υπάρχουν m *γραμμές με τους συντελεστές* a_i *του* f, n *γραμμές με τους συντελεστές* b_i *του* g *και οι άδειες θέσεις περιέχουν μηδενικά.*

Θεώρημα 2.7 (Επιλύουσα δύο πολυωνύμων)

Αν θεωρήσουμε τους συντελεστές των f *και* g *ως παραμέτρους, με την προϋπόθεση ότι* $a_n b_m \neq 0$, *τότε, για οποιαδήποτε τιμή των παραμέτρων, η επιλύουσα των* f *και* g *ως προς* X *ισούται με την ορίζουσα του πίνακα Sylvester,*

$$\mathtt{res}(f,g) = \det(\mathtt{Syl}(f,g))$$

Η επιλύουσα συμβολίζεται ως $\mathtt{res}_X(f,g)$ όταν τα f και g είναι πολυώνυμα πολλών μεταβλητών, π.χ $f, g \in \mathcal{K}[Y_1, \dots, Y_k, X]$, και θέλουμε να δηλώσουμε ότι αναφερόμαστε στην επιλύουσά τους θεωρώντας τα πολυώνυμα μιας μεταβλητής ως προς X, δηλαδή $f, g \in (\mathcal{K}[Y_1, \dots, Y_k])[X]$.

Μπορούμε επίσης να διατυπώσουμε το επόμενο θεώρημα:

Θεώρημα 2.8

Έστω $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{m} b_i X^i$, $f, g \in \mathcal{K}[X]$. *Τα επόμενα είναι ισοδύναμα:*

1. *Τα* f *και* g *έχουν κάποια κοινή ρίζα στο* $\mathcal{K}$.
2. $\deg(\gcd(f,g)) = k > 0$.
3. *Υπάρχουν* $A, B \in \mathcal{K}[X]$, *τέτοια ώστε* $\deg(A) < m-k$ *και* $\deg(B) < n-k$, *από τη σχέση Bézout, τέτοια ώστε να μην είναι και τα δύο μηδέν και* $A\,f + B\,g = 0$.
4. $\mathtt{res}(f,g) = \det(\mathtt{Syl}(f,g)) = 0$

Παράδειγμα 2.9. *Έστω*

$$\begin{aligned} f &= a_2X^2 + a_1X + a_0 \\ g &= b_2X^2 + b_1X + b_0 \end{aligned}$$

Ο πίνακας Sylvester των f και g είναι

$$\mathtt{Syl}(f,g) = \begin{bmatrix} a_2 & a_1 & a_0 & 0 \\ 0 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 \\ 0 & b_2 & b_1 & b_0 \end{bmatrix}$$

και η επιλύουσα είναι

$$\mathtt{res}(f,g) = a_2^2b_0^2 + a_2b_1^2a_0 - a_2b_1a_1b_0 - 2\,a_2b_2b_0a_0 + b_2a_1^2b_0 - b_2a_1b_1a_0 + b_2^2a_0^2$$

Παρατηρούμε ότι $\deg(\mathtt{res}(f,g)) = \deg(f) + \deg(g) = 2 + 2 = 4$. *Η επιλύουσα είναι η βέλτιστη συνθήκη για την επιλυσιμότητα και συνεπώς ο συνολικός βαθμός του* $\mathtt{res}(f,g) \in \mathbb{Z}[a_2, a_1, a_0, b_2, b_1, b_0]$, *ο οποίος είναι 4, είναι βέλτιστος. Ή διαφορετικά, στη γενική περίπτωση, εκτός από την επιλύσουσα δεν υπάρχει άλλο πολυώνυμο ως προς τους συντελεστές των f και g, με συνολικό βαθμό ≤ 4, ο μηδενισμός του οποίου να μας εξασφαλίζει την ύπαρξη κοινών λύσεων των f και g.*

Επίσης, παρατηρούμε ότι η επιλύσουσα είναι ένα εκέραιο πολυώνυμο ως προς τους συντελεστές των f και g και δεν περιέχει την μεταβλητή X. Δηλαδή η επιλύουσα (απαλοίφουσα) έχει απαλείψει από το σύστημα $f = g = 0$ την μεταβλητή X.

Παρουσιάζουμε μερικές ιδιότητες της επιλύουσας.

Λήμμα 2.10. *Έστω $f, g, h \in \mathcal{K}[X]$ τέτοια ώστε $\deg(f) = n$, $\deg(g) = m$ και $\alpha, \beta \in \mathcal{K}$.*

1. $\mathtt{res}(\alpha, f) = \alpha^n$.
2. $\mathtt{res}(X - \alpha, f) = f(\alpha)$.
3. $\mathtt{res}(f,g) = (-1)^{mn}\, res(g,f)$.
4. $\mathtt{res}(\alpha f, g) = \alpha^n\, \mathtt{res}(f,g)$.
5. $\mathtt{res}(f \cdot h, g) = \mathtt{res}(f,g) \cdot \mathtt{res}(h,g)$.
6. *Αν $f = gQ + R$ και $\deg(R) = r$, $m \geq n > r$, τότε*

$$\mathtt{res}(f,g) = (-1)^{n(m-r)}\, a_n^{m-r}\, \mathtt{res}(R,g) = (-1)^{mn}\, a_n^{m-r}\, \mathtt{res}(g,R)$$

Το προηγούμενο λήμμα οδηγεί στον ακόλουθο χαρακτηρισμό της επιλύουσας:

Θεώρημα 2.11

Έστω $f, g \in \mathcal{R}[x]$, όπως στην Εξ. (2.5), με ρίζες $\alpha_1, \ldots, \alpha_n$ και $\beta_1 \ldots, \beta_m \in \mathcal{K}$. Ισχύουν τα ακόλουθα:

$$\mathtt{res}(f,g) \;=\; a_n^m\, b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn}\, b_m^n \prod_{i=1}^{m} f(\beta_i)$$

Ο πίνακας Bézout

Στην περίπτωση δύο πολυωνύμων σε μία μεταβλητή υπάρχει και άλλος τρόπος να υπολογίσουμε την επιλύουσα ως ορίζουσα κάποιου πίνακα. Η κατασκευή βασίζεται στον πίνακα Bézout των f και g και οφείλεται στους Bézout και Cayley.

Δοθέντων δύο πολυωνύμων f και g, όπως στην (2.5), ο πίνακας Bézout [14, 187, 190, 276] των f και g είναι ο συμμετρικός πίνακας

$$\mathtt{Bz}(f,g) = \begin{pmatrix} c_{0,0} & \ldots & c_{0,n-1} \\ \vdots & & \vdots \\ c_{n-1,0} & \ldots & c_{n-1,n-1} \end{pmatrix} \tag{2.6}$$

όπου τα $c_{i,j}$ ορίζονται από την έκφραση Cayley

$$\frac{f(X)\,g(Y) - f(Y)\,g(X)}{X - Y} = \sum_{i,j=0}^{n-1} c_{i,j}\, X^i\, Y^j.$$

Ο πίνακας Bézout είναι στενά συνδεδεμένος με τον πίνακα Sylvester. Η ορίζουσα του πίνακα Bézout είναι η επιλύουσα των f και g. Δηλαδή

$$\mathtt{res}(f,g) = \det(\mathtt{Bz}(f,g)).$$

Η διάσταση του πίνακα Bézout είναι $n \times n$ όπου $n = \max\{\deg(f), \deg(g)\}$ και είναι μικρότερη από αυτή του πίνακα Sylvester. Επίσης, μπορούμε να υπολογίσουμε τον πίνακα Bézout και στην περίπτωση που έχουμε $\ell + 1$ πολυώνυμα σε ℓ μεταβλητές. Σε αυτή την περίπτωση, η ορίζουσα του πίνακα μας δίνει κάποιο πολλαπλάσιο της επιλύουσας του συστήματος. Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [20, 21, 86].

Διακρίνουσα

Στενά συνδεδεμένη με την έννοια της επιλύουσας είναι η έννοια της διακρίνουσας.

Ορισμός 2.12 (Διακρίνουσα). *Έστω $f = \sum_{i=0}^{n} a_i X^i \in \mathcal{R}[X]$, $n \geq 2$ και $\gamma_1, \ldots, \gamma_n \in \mathcal{K}$ οι ρίζες του. Ορίζουμε ως διακρίνουσα (discriminant) του A την πόσοτητα*

$$\mathsf{disc}(f) := a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\gamma_i - \gamma_j)^2$$

Παράδειγμα 2.13. *Αν* $f = a\,x^2 + b\,x + c$ *τότε* $\mathsf{disc}(f) = b^2 - 4\,a\,c$.

Ο ορισμός της διακρίνουσας δεν παρέχει κάποιον τρόπο υπολογισμού της, κάτι που επιτυγχάνεται με το ακόλουθο θεώρημα από το οποίο επίσης προκύπτει ότι $\mathsf{disc}(f) \in \mathcal{R}[a_n, \ldots, a_1, a_0]$.

Θεώρημα 2.14
Έστω $f = \sum_{i=0}^{n} a_i X^i \in \mathcal{R}[X]$, *τότε*

$$\mathtt{res}(f, f') = \pm\, a_n\, \mathsf{disc}(f) = (-1)^{\frac{n(n-1)}{2}}\, a_n\, \mathsf{disc}(f)$$

Παρατηρούμε ότι ο ο ορισμός της διακρίνουσας δεν απαιτεί την ύπαρξη (μόνο) διαφορετικών ριζών. Κατά συνέπεια $\mathsf{disc}(f) = 0$ αν και μόνο αν το f έχει πολλαπλές ρίζες ή ισοδύναμα $\mathtt{res}(f, f') = 0$ αν και μόνο αν το f έχει πολλαπλές ρίζες. Αν $f \in \mathbb{Z}[X]$ και δεν έχει πολλαπλές ρίζες τότε $\mathsf{disc}(f) \geq 1$. Ένα άνω φράγμα στη διακρίνουσα μας παρέχει το επόμενο θεώρημα, όπου $\mathcal{M}(f)$ είναι το μέτρο Mahler του f (Ορ. 3.2), το οποίο θα ορίσουμε στο επόμενο κεφάλαιο.

Θεώρημα 2.15
Αν $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ *με* $\deg(f) = n$ *τότε*

$$|\mathsf{disc}(f)| \leq n^n\, \mathcal{M}(f)^{2(n-1)} \leq n^n\, \|f\|_2^{2(n-1)}$$

2.3 Πολυωνυμικές ακολουθίες υπολοίπων

Ας υποθέσουμε ότι $\mathcal{R}$ είναι μια περιοχή μοναδικής ανάλυσης, π.χ $\mathcal{R} = \mathbb{Z}$ ή $\mathcal{R} = \mathbb{Z}[Y]$. Έστω $A, B \in \mathcal{R}[X]$ τέτοια ώστε

$$\begin{array}{rcl} A(X) & = & a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0 \\ B(X) & = & b_q X^q + b_{q-1} X^{q-1} + \cdots + b_1 X + b_0 \end{array} \tag{2.7}$$

όπου $\deg(A) = p \geq q = \deg(B) > 0$. Αν $\mathcal{R} = \mathbb{Z}$ τότε θεωρούμε ότι $\mathcal{L}(A), \mathcal{L}(B) \leq \tau$.

Επιστρέφουμε στο πρόβλημα του υπολογισμού του ΜΚΔ δύο πολυωνύμων. Προκειμένου να υπολογίσουμε το $\gcd(A, B)$ μπορούμε να θεωρήσουμε ότι $A, B \in \mathcal{F}[X]$ και να εφαρμόσουμε τον αλγόριθμο του Ευκλείδη, δείτε για παράδειγμα [160, 263, 275]. Πιο συγκεκριμένα, θεωρούμε $P_{q+1} = A$, $P_q = B$, $Q_i = \mathsf{quo}(P_{i+1}, P_i)$ και $P_{i-1} = \mathsf{rem}(P_{i+1}, P_i)$, οπότε

$$\begin{array}{rcll} P_{q+1} & = & Q_q P_q + P_{q-1} & \deg(P_{q-1}) < \deg(P_q) \\ P_q & = & Q_{q-1} P_{q-1} + P_{q-1} & \deg(P_{q-2}) < \deg(P_{q-1}) \\ & \vdots & & \\ P_{h+2} & = & Q_{h+1} P_{h+1} + P_h & \deg(P_h) < \deg(P_{h+1}) \\ P_{h+1} & = & Q_h P_h + 0 & \end{array} \tag{2.8}$$

όπου $\gcd(A, B) = P_h$. Ο αλγόριθμος τερματίζει καθώς ο βαθμός μειώνεται σε κάθε βήμα.

Ωστόσο, όταν $\mathcal{R} = \mathbb{Z}$ και $\mathcal{F} = \mathbb{Q}$ η προσέγγιση που ακολουθήσαμε για τον υπολογισμό του ΜΚΔ εισάγει ρητούς αριθμούς τους οποίους θέλουμε να αποφύγουμε γιατί οι πράξεις με ρητούς έχουν (πολύ) μεγάλη πολυπλοκότητα. Χαρακτηριστικά αναφέρουμε ότι η πρόσθεση δύο ακεραίων αυξάνει το δυαδικό μήκος του αποτελέσματος κατά 1, ενώ η πρόσθεση δύο ρητών διπλασιάζει το δυαδικό μήκος του αποτελέσματος. Συνεπώς, επιθυμούμε όχι μόνο γρήγορους αλγορίθμους για τον υπολογισμό του ΜΚΔ αλλά και αλγορίθμους που απαιτούν πράξεις μόνο στο $\mathcal{R}$ και στο $\mathcal{R}[X]$. Προκειμένου να επιτύχουμε τους στόχους μας θα ορίσουμε πιο αυστηρά την ακολουθία πολυωνύμων $(P_{q+1}, P_q, \ldots, P_h)$ και θα αναδείξουμε την άμεση συσχέτιση των συντελεστών των P_i με συγκεκριμένες υποορίζουσες του πίνακα Sylvester των A και B.

Η παρουσίασή μας βασίζεται στους von zur Gathen and Lücking [264] και Yap [275] αλλά είναι πιο απλοποιημένη. Θα χρειαστούμε τους ακόλουθους ορισμούς:

Το *περιεχόμενο* (*content*) του A είναι ο ΜΚΔ των συντελεστών του και το συμβολίζουμε ως $\mathsf{content}(A)$. Το *πρωταρχικό μέρος* (*primitive part*) του A προκύπτει αν διαιρέσουμε το A με το $\mathsf{content}(A)$ και το συμβολίζουμε με $\mathsf{pp}(A)$. Αν στο $\mathcal{R}$ δεν ορίζεται ο ΜΚΔ τότε $\mathsf{content}(A) = 1$. Δύο πολυώνυμα A, B είναι όμοια όταν $\mathsf{pp}(A) = \mathsf{pp}(B)$ και συμβολίζουμε $A \sim B$.

Ορισμός 2.16 (Πολυωνυμική ακολουθία υπολοίπων). *Έστω A, B όπως στην Εξ. (2.7). Ορίζουμε ως πολυωνυμική ακολουθία υπολοίπων (polynomial remainder sequence) των A και B την ακολουθία $\mathbf{PRS}(A, B) = (R_{q+1} = A, R_q = B, R_{q-1}, \ldots, R_h)$, για την οποία ισχύει*

$$\mathfrak{a}_i R_{i+1} = Q_i R_i + \mathfrak{b}_i R_{i-1} \tag{2.9}$$

όπου $\deg(R_{i-1}) < \deg(R_i)$, $q \geq i \geq h+1$. Απαιτούμε $\mathfrak{a}_i, \mathfrak{b}_i \in \mathcal{R}$ και $R_i \in \mathcal{R}[X]$. Επίσης ορίζουμε και την αντίστοιχη ακολουθία πηλίκων $\mathbf{PQS}(A, B) = (Q_q, Q_{q-1}, \ldots, Q_h, R_h)$.

Το μήκος της ακολουθίας είναι $q - h + 2$.

Αν ισχύει $p < q$, τότε η ακολουθία είναι $\mathbf{PRS}(A, B) = (R_{p+2} = A, R_{p+1} = B, R_p = A, \ldots, R_h)$. Υποθέτουμε $p \geq q$ προκειμένου να διευκολυνθούμε στην αριθμητική των δεικτών.

Η $\mathbf{PRS}$ είναι *πλήρης* (complete) αν η (2.9) ικανοποιείται για $i = h$ και ισχύει $R_{h-1} = 0$. Όλες οι ακολουθίες που θα θεωρήσουμε θα είναι πλήρεις, εκτός αν ρητά αναφέρεται το αντίθετο. Η $\mathbf{PRS}$ ονομάζεται κανονική (normal ή regular) αν $\deg(R_i) - \deg(R_{i+1}) = 1$, διαφορετικά ονομάζεται ελαττωματική (defective). Όταν η $\mathbf{PRS}$ είναι πλήρης και κανονική τότε $h = 0$, το μήκος της ακολουθίας είναι $q + 2$ και ο δείκτης σε κάθε πολυώνυμο R_i δηλώνει το βαθμό του.

Αξίζει να παρατηρήσουμε ότι μπορούμε να ορίσουμε μια ακολουθία υπολοίπων με μοναδικό τρόπο αν υποθέσουμε κάποια ακολουθία ζευγών $(\mathfrak{a}_i, \mathfrak{b}_i)$ ή κάποιο τρόπο υπολογισμού τους. Στην περίπτωση αυτή τα R_{i-1} και Q_i ορίζονται μοναδικά επιλύοντας ένα γραμμικό συστήμα. Ωστόσο, προκειμένου να διευκολύνουμε τον αναγνώστη, σε όλους τους κανόνες υπολογισμού πολυωνυμικών ακολουθιών υπολοίπων που θα παρουσιάσουμε, θα δίνουμε και τον τρόπο υπολογισμού των R_{i-1} και Q_i.

Ευκλείδια ακολουθία

Στην περίπτωση που ισχύει $\mathcal{R} = \mathcal{F}$ και $(\mathfrak{a}_i, \mathfrak{b}_i) = (1, 1)$ τότε η ακολουθία υπολοίπων είναι ακριβώς η ακολουθία υπολοίπων που εμφανίζεται κατά τη διάρκεια του αλγορίθμου του Ευκλείδη για τον

υπολογισμό του $\gcd(A, B)$, Εξ. (2.8), με τη μόνη διαφορά είναι ότι η αρίθμηση των δεικτών είναι στην περίπτωση της **PRS** φθίνουσα. Συνεπώς, το τελευταίο πολυώνυμο της ακολουθίας είναι ο ΜΚΔ των A και B. Την ακολουθία αυτή θα τη συμβολίσουμε με $\mathbf{Euclid-PRS}(A, B)$ και οι (αναδρομικοί) κανόνες ορισμού της είναι:

$$\mathbf{Euclid-PRS}(A, B) \quad \left\{ \begin{array}{rcl} (\mathfrak{a}_i, \mathfrak{b}_i) & = & (1, 1) \\ R_{i-1} & = & \mathsf{rem}\,(R_{i+1}, R_i) \\ Q_i & = & \mathsf{quo}\,(R_{i+1}, R_i) \end{array} \right\} \tag{2.10}$$

Οι κανόνες της (2.10) είναι στην ουσία ένας αλγόριθμος υπολογισμού της **Euclid – PRS**. Το ίδιο ισχύει και για τους επόμενους κανόνες που θα παρουσιάσουμε.

Στη χειρότερη περίπτωση υπάρχουν $\Omega(q)$ πολυώνυμα στην ακολουθία, τα οποία έχουν βαθμούς $\Omega(p)$. Κατά συνέπεια ο συνολικός αριθμός των συντελεστών όλων των πολυωνύμων στην ακολουθία είναι $\Omega(pq)$ και άρα ένα κάτω φράγμα για την αριθμητική πολυπλοκότητα υπολογισμού της ακολουθίας είναι $\Omega(pq)$. Αν $\mathcal{R} = \mathbb{Z}$ και $\mathcal{L}(A), \mathcal{L}(B) \leq \tau$ τότε το δυαδικό μήκος των πολυωνύμων στην ακολουθία φράσσεται από $\mathcal{O}(p^2\tau)$ [175]. Σε αυτό το σημείο αξίζει να επισημάνουμε ότι το άθροισμα των βαθμών των Q_i είναι $\mathcal{O}(q)$ και άρα το πλήθος των συντελεστών των πολυωνύμων που ανήκουν στην ακολουθία των πηλίκων είναι $\mathcal{O}(q)$.

Ακολουθίες κατά Sturm

Εξέχουσας σημασίας είναι η πολυωνυμική ακολουθία υπολοίπων κατά Sturm [248], η οποία διαφέρει κατά ένα πρόσημο από την Ευκλείδια ακολουθία. Οι κανόνες ορισμού της είναι:

$$\mathbf{Sturm}(A, B) \quad \left\{ \begin{array}{rcl} (\mathfrak{a}_i, \mathfrak{b}_i) & = & (1, -1) \\ R_{i-1} & = & \mathsf{rem}\,(R_{i+1}, R_i) \\ Q_i & = & \mathsf{quo}\,(R_{i+1}, R_i) \end{array} \right\} \tag{2.11}$$

Ο Sturm [248] χρησιμοποίησε την ακολουθία $\mathbf{Sturm}(A, A')$ για να απομονώσει τις πραγματικές ρίζες του A, η οποία και ονομάζεται *ακολουθία Sturm*.

Οι ακολουθίες κατά Sturm ορίζονται με πιο γενικό τρόπο ως ακολούθως:

Ορισμός 2.17. *Μια ακολουθία πραγματικών πολυωνύμων $(p_k, p_{k-1}, \ldots, p_1, p_0)$ είναι ακολουθία κατά Sturm στο διάστημα (a, b), όπου τα a και b μπορούν να είναι και $\pm\infty$, αν $\forall\, c \in (a, b)$, ισχύουν*

(i) $p_k(a)\, p_k(b) \neq 0$

(ii) *Αν* $p_k(c) = 0$ *τότε* $\exists\, \epsilon \in \mathbb{R}$ *τέτοιο ώστε* $\forall u \in (c - \epsilon, c)$, *αντίστοιχα* $\forall u \in (c, c + \epsilon)$, *να ισχύει* $p_k(u)\, p_{k-1}(u) < 0$, *αντίστοιχα* $p_k(u)\, p_{k-1}(u) > 0$.

(iii) *Αν* $p_i(c) = 0$, $0 \leq i \leq k - 1$, *τότε* $p_{i-1}(c)\, p_{i+1}(c) < 0$.

(iv) $p_0(c) \neq 0$.

Ένας από τους τρόπους υπολογισμού (υπάρχουν άπειροι) μιας ακολουθίας κατά Sturm παρουσιάζεται στην (2.11). Σε επόμενες παραγράφους θα γενικεύσουμε τον ορισμό της ακολουθίας κατά Sturm.

Ψευδο-Ευκλείδια ακολουθία

Όταν $\mathcal{R} \neq \mathcal{F}$ τότε δεν ορίζεται πάντοτε η διαίρεση και γι' αυτό το λόγο έχει εισαχθεί η ψευδο-διαίρεση (Θεωρ. 2.4). Η ακολουθία πολυωνυμικών υπολοίπων που ορίζεται με τη βοήθεια της ψευδο-διαίρεσης ονομάζεται *ψευδο-Ευκλείδια* (pseudo-Euclidean) και συμβολίζεται με $\mathbf{EPRS}(A, B)$. Θα χρησιμοποιήσουμε τον συμβολισμό $\mathfrak{r}_i = \mathsf{lead}(R_i)$ και $\delta_i = \max\{1, \deg(R_{i+1}) - \deg(R_i)\}$. Οι κανόνες της $\mathbf{EPRS}$ είναι:

$$\mathbf{EPRS}(A, B) \quad \left\{ \begin{array}{l} (\mathfrak{a}_i, \mathfrak{b}_i) = \left(\mathfrak{r}_i^{\delta_i+1}, 1\right) \\ R_{i-1} = \mathsf{rem}(\mathfrak{a}_i R_{i+1}, R_i) \\ Q_i = \mathsf{quo}(\mathfrak{a}_i R_{i+1}, R_i) \end{array} \right\} \tag{2.12}$$

όπου ο υπολογισμός των R_{i-1} και Q_i εμπεριέχει μόνο ακριβείς (χωρίς υπόλοιπο) διαιρέσεις με τους συντελεστές. Την αντίστοιχη ακολουθία πηλίκων τη συμβολίζουμε με $\mathbf{EPQS}(A, B)$. Παρατηρούμε ότι $R_{i-1} = \mathsf{rem}(\mathfrak{a}_i R_{i+1}, R_i) = \mathsf{prem}(R_{i-1}, R_i)$ και $Q_i = \mathsf{quo}(\mathfrak{a}_i R_{i+1}, R_i) = \mathsf{pquo}(R_{i-1}, R_i)$.

Η ψευδο-Ευκλείδια ακολουθία είναι ο πιο εύκολος και προφανής τρόπος υπολογισμού μιας πολυωνυμικής ακολουθίας υπολοίπων και κατά συνέπεια του ΜΚΔ δύο πολυωνύμων. Η αριθμητική πολυπλοκότητα του υπολογισμού της είναι $\mathcal{O}(pq)$ και άρα βέλτιστη. Επιπρόσθετα, μπορεί να δειχτεί ότι οποιαδήποτε άλλη ακολουθία που ικανοποιεί τις απαιτήσεις της (2.9) παράγει πολυώνυμα τα οποία είναι όμοια με αυτά της $\mathbf{EPRS}$.

Ωστόσο, το δυαδικό μήκος των πολυωνύμων στην $\mathbf{EPRS}(A, B)$ αυξάνεται εκθετικά σε σχέση το μήκος της ακολουθίας. Μπορεί να δειχτεί [160, 178, 263, 264, 275] ότι το R_i μπορεί να έχει δυαδικό μήκος μεγαλύτερο κατά ένα παράγοντα $(1+\sqrt{2})^i$ σε σχέση με το δυαδικό μήκος των A και B. Συνεπώς η $\mathbf{EPRS}$ απαιτεί εκθετικό αριθμό δυαδικών πράξεων και άρα δεν έχει μεγάλη πρακτική σημασία.

Πρωταρχική ακολουθία

Προκειμένου να αντιμετωπίσουμε την εκθετική συμπεριφορά της $\mathbf{EPRS}$ η πιο προφανής λύσης είναι να αντικαταστήσουμε κάθε R_{i-1} στην $\mathbf{EPRS}$ με το πρωταρχικό του μέρος. Δηλαδή να θέσουμε $\mathfrak{b}_i = \mathsf{content}(R_{i-1})$. Η ακολουθία που σχηματίζεται με αυτόν το τρόπο ονομάζεται *πρωταρχική ακολουθία πολυωνυμικών υπολοίπων* (primitive polynomial remainder sequence) και θα τη συμβολίζουμε με $\mathbf{PPRS}$. Οι κανόνες της είναι:

$$\mathbf{PPRS}(A, B) \quad \left\{ \begin{array}{l} (\mathfrak{a}_i, \mathfrak{b}_i) = \left(\mathfrak{r}_i^{\delta_i+1}, \mathsf{content}(\mathsf{prem}(R_{i-1}, R_i))\right) \\ R_{i-1} = \mathsf{rem}(\mathfrak{a}_i R_{i+1}, R_i) / \mathfrak{b}_i \\ Q_i = \mathsf{quo}(\mathfrak{a}_i R_{i+1}, R_i) \end{array} \right\} \tag{2.13}$$

όπου ο υπολογισμός των R_{i-1} και Q_i εμπεριέχει μόνο ακριβείς διαιρέσεις με τους συντελεστές. Η αντίστοιχη ακολουθία πηλίκων συμβολίζεται με $\mathbf{PPQS}(A, B)$.

Η ακολουθία $\mathbf{PPRS}(A, B)$ είναι ό,τι καλύτερο μπορούμε να περιμένουμε σχετικά με το δυαδικό μήκος των πολυωνύμων της ακολουθίας. Ωστόσο, ο υπολογισμός της απαιτεί σε κάθε βήμα τον υπολογισμό του περιεχομένου ενός πολυωνύμου, πράξη η οποία είναι αρκετά χρονοβόρα. Είναι πολύ δύσκολο να υπολογίσουμε θεωρητικά τη δυαδική πολυπλοκότητα του υπολογισμού της

πρωταρχικής ακολουθίας, καθώς δεν μπορούμε να προβλέψουμε τον συσχετισμό των συντελεστών των πολυωνύμων που εμφανίζονται στην ακολουθία, αν και μπορεί να δειχτεί ότι αν η ακολουθία υπολογιστεί συμβολικά οι συντελεστές των πολυωνύμων της ακολουθίας (που είναι πολυώνυμα ως προς τους συντελεστές των αρχικών πολυωνύμων) είναι ανάγωγα πολυώνυμα και μεταξύ τους πρώτα [83]. Για τον υπολογισμό όλης της ακολουθίας απαιτούνται $\mathcal{O}(p\,q)$ πράξεις, καθώς τόσο είναι το πλήθος των συντελεστών. Υπάρχουν $\mathcal{O}(q)$ πολυώνυμα στην ακολουθία. Αν κάνουμε την ασθενή υπόθεση ότι απαιτείται ένας υπολογισμός ΜΚΔ για κάθε πολυώνυμο της ακολουθίας, τότε απαιτούνται τουλάχιστον $\mathcal{O}(p\,q^2)$ αριθμητικές πράξεις. Όπως θα παρουσιάσουμε στην επόμενη παράγραφο που θα αναφερθούμε στις υπο-επιλύουσες, το δυαδικό μήκος των συντελεστών της ακολουθίας είναι τουλάχιστον $\mathcal{O}(p\,\tau)$. Άρα, η δυαδική πολυπλοκότητα υπολογισμού της **PPRS** είναι τουλάχιστον $\tilde{\mathcal{O}}_B(p\,q^2\,\mathsf{M}\,(p\,\tau))$. Οι αλγόριθμοι που θα παρουσιάσουμε στη συνέχεια έχουν καλύτερη πολυπλοκότητα, αν και η σπουδαιότητα της πρωταρχικής ακολουθίας δεν πρέπει να υποτιμάται τουλάχιστον σε υπολογισμούς με πολυώνυμα σχετικά μικρού βαθμού.

Σε κάθε περίπτωση γεννάται το ερώτημα σχετικά με το πως θα μπορούσαμε να υπολογίσουμε το περιεχόμενο ενός πολυωνύμου της **EPRS**, ή έστω κάποιου αρκετά μεγάλου διαιρέτη του, χωρίς να καταφύγουμε στους χρονοβόρους υπολογισμούς του μέγιστου κοινού διαιρέτη πολλών αριθμών. Επιπρόσθετα, θα επιθυμούσαμε το δυαδικό μήκος των συντελεστών να πλησιάζει όσο το δυνατόν περισσότερο αυτό της πρωταρχικής ακολουθίας, δηλαδή στη χειρότερη περίπτωση να αυξάνεται γραμμικά.

Πιο συγκεκριμένα αν $\mathbf{EPRS}(A,B) = (R_{q+1}, R_q, \ldots, R_h)$ σκοπός μας είναι να υπολογίσουμε μια άλλη ακολουθία $(P_{q+1}, P_q, \ldots, P_h)$, τέτοια ώστε $R_i \sim P_i$ και $P_i = R_i/\beta_i$, όπου $\beta_i \in \mathcal{R}$ και η διαίρεση είναι χωρίς υπόλοιπο.

Υπο-επιλύουσες (subresultants)

Προκειμένου να αντιμετωπιστεί το πρόβλημα της εκθετική αύξησης του δυαδικού μήκους των συντελεστών στην ψευδο-Ευκλείδια ακολουθία και ταυτόχρονα να αποφευχθεί ο υπολογισμός της πρωταρχικής ακολουθίας που εμπεριέχει πολλούς υπολογισμούς αρχικά ο Collins [54] και στη συνέχεια οι Brown and Traub [35] (ξανα-)ανακάλυψαν τις πολυωνυμικές υπο-επιλύουσες (ή υπο-απαλοίφουσες) (polynomials subresultants) οι οποίες ορίζονται ως ορίζουσες κάποιας παραλλαγής του πίνακα Sylvester, δείτε επίσης [34, 36, 37, 178]. Ο Habicht [125] ήδη από το 1948 είχε εισαγάγει αυτή την προσέγγιση. Ο αναγνώστης μπορεί να ανατρέξει στην εργασία των Ho and Yap [133] για την μοντέρνα εκδοχή της προσέγγισης του Habicht.

Ο αναγνώστης μπορεί να ανατρέξει στους von zur Gathen and Lücking [264] οι οποίοι παρουσιάζουν με ενοποιημένο τρόπο τις διάφορες παραλλαγές σχετικά με τις υπο-επιλύουσες ή στον El Kahoui [83] όπου η έννοια της υπο-επιλύσουσας γενικεύεται για κάθε αβελιανό δακτύλιο. Για πιο σύγχρονες εκδοχές των υπο-επιλυουσών ο αναγνώστης μπορεί να ανατρέξει στους Basu et al. [14], González-Vega et al. [118, 119], Lickteig and Roy [174, 175], Lombardi et al. [176], von zur Gathen and Gerhard [263], Yap [275] όπου επίσης περιέχονται και οι αποδείξεις των θεωρημάτων που παρουσιάζουμε.

Έστω k πολυώνυμα $A_i = \sum_{j=0}^{n_i} a_{ij} X^j \in \mathcal{R}[X]$, $1 \leq i \leq k$ και $\ell = 1 + \max_{1\leq i\leq k} n_i$. Θεωρούμε

τον πίνακα

$$mat(A_1, \ldots, A_k) = [a_{i,\ell-j}]$$

του οποίου η i γραμμή περιέχει τους συντελεστές του A_i και $a_{ij} = 0$ αν $j > n_j = \deg(A_i)$. Ο πίνακας έχει διαστάσεις $k \times \ell$.

Ορισμός 2.18. *Έστω $M \in \mathcal{R}^{k\times\ell}$, $\ell \leq k$. Το πολυώνυμο ορίζουσας (determinant polynomial) του M είναι:*

$$detpol(M) := \det(M^{(k)})X^{\ell-k} + \cdots + \det(M^{(\ell)})$$

όπου $M^{(i)}$ είναι ένας τετραγωνικός υποπίνακας του M, ο οποίος αποτελείται από τις πρώτες $k-1$ στήλες και την i στήλη ($\ell \leq i \leq k$).

Ορισμός 2.19 (subresultants). *Έστω $A, B \in \mathcal{R}[X]$, όπως στην Εξ. (2.7).*

- *Η k (πολυωνυμική) υπο-επιλύουσα (k^{th} subresultant) των A και B είναι το πολυώνυμο*

  $$\mathbf{SR}_k(A, B) = detpol(M_k)$$

  όπου $M_k = mat(X^{q-k-1}A, \ldots, A, X^{p-k-1}B, \ldots, B)$.

- *Η ακολουθία υπο-επιλυουσών (subresultant chain) των A και B είναι:*

  $$\mathbf{SR}(A, B) = (\mathbf{SR}_{q+1} = A, \mathbf{SR}_q = B, \mathbf{SR}_{q-1}, \ldots, \mathbf{SR}_0)$$

- *Ο $k-$οστός πρωτεύων συντελεστής της υπο-επιλύσουσας (k^{th} principal subresultant coefficient) των A και B είναι*

  $$\mathbf{psc}_k(A, B) = \det(M_k^{(k)}), \quad 0 \leq k \leq q$$

  όπου $\mathbf{psc}_{q+1} = 1$.

Αν δεν υπάρχει ο κίνδυνος σύγχυσης τότε θα συμβολίζουμε $\mathbf{SR}_i(A, B) = \mathbf{SR}_i$ και $\mathbf{psc}_i(A, B) = \mathbf{psc}_i = \mathbf{sr}_i$.

Οι υπο-επιλύουσες δεν είναι τίποτα άλλο από κάποια υλοποίηση πολυωνυμικών ακολουθιών υπολοίπων με τις επιπλέον ιδιότητες ότι τα πολυώνυμα της ακολουθίας είναι στο $\mathcal{R}[X]$, ότι συμπεριφέρονται καλά κάτω από ομομορφισμούς εκτίμησης και ότι αν $\mathcal{R} = \mathbb{Z}$ η αύξηση στο δυαδικό μήκος των πολυωνύμων είναι το πολύ γραμμική.

Παρατηρούμε ότι ο πίνακας $M_0 = mat(X^{q-1}A, \ldots, A, X^{p-}B, \ldots, B)$ είναι ο πίνακας Sylvester των A και B, δηλαδή ισχύει $\mathtt{Syl}(A, B) = M_0$. Πιο συγκεκριμένα ισχύει το ακόλουθο θεώρημα:

Θεώρημα 2.20

Το πολυώνυμο $\mathbf{SR}_0(A, B)$ είναι (εκτός ίσως από το πρόσημό του) η επιλύουσα των A και B, δηλαδή $\mathbf{SR}_0(A, B) = \pm\mathtt{res}(A, B)$.

Από την ακολουθία $\mathbf{SR}(A, B)$ μπορούμε να υπολογίσουμε τον ΜΚΔ των A και B. Πιο συγκεκριμένα ισχύει ότι:

$$\mathbf{SR}_k(A, B) = \gcd(A, B) \Leftrightarrow \begin{cases} \mathbf{psc}_0(A, B) = \cdots = \mathbf{psc}_{k-1}(A, B) = 0 \\ \mathbf{psc}_k(A, B) \neq 0 \end{cases}$$

και $\deg(\gcd(A, B)) = k$.

Από τον ορισμό του πρωτεύοντος συντελεστή της υπο-επιλύουσας προκύπτει ότι μπορεί να είναι και μηδέν! Δηλαδή ο πρωτεύων συντελεστής δεν είναι απαραίτητα και ο μεγιστοβάθμιος όρος της υπο-επιλύουσας. Στη γενική περίπτωση ισχύει $\mathsf{lead}\left(\mathbf{SR}_i\right) \neq \mathbf{psc}_i$ και $\deg(\mathbf{SR}_i) \leq i$. Όταν $\forall i$ ισχύει $\mathbf{psc}_i \neq 0$, δηλαδή $\deg(\mathbf{SR}_i) = i$, τότε η ακολουθία είναι κανονική (normal ή regular) αλλιώς είναι ελαττωματική (defective). Οι ορισμοί είναι ακριβώς οι ίδιοι με αυτούς των πολυωνυμικών ακολουθιών υπολοίπων. Επίσης, αν $\deg(\mathbf{SR}_j) = k < j$, τότε $\mathbf{SR}_i = 0$ για $j+1 \geq i > k$ και $\deg(\mathbf{SR}_k) = k$ και $\mathbf{SR}_j \sim \mathbf{SR}_k$. Αυτό είναι και το κλασικό θεώρημα δομής για τις υπο-επιλύουσες (gap structure theorem of subresultants) [54, 178].

Πρέπει να προσθέσουμε ότι θα μπορούσαμε να είχαμε χρησιμοποιήσει τον πίνακα Bézout προκειμένου να ορίσουμε την ακολουθία υπο-επιλυουσών [20, 21, 136].

Προκειμένου οι ακολουθίες υπο-επιλυουσών να υπακούουν τον Ορ. (2.9) θεωρούμε ότι έχουμε απομακρύνει τα μηδενικά πολυώνυμα που βρίσκονται στις ενδιάμεσες θέσεις της $\mathbf{SR}(A, B)$ και επεκτείνουμε τον ορισμό έτσι ώστε να επιτρέπουμε να υπάρχουν δύο, συνεχόμενα, ίδιου βαθμού πολυώνυμα στην ακολουθία.

Τόσο οι υπο-επιλύουσες όσο και οι συντελεστές τους προκύπτουν ως ορίζουσες κάποιων υποπινάκων του πίνακα Sylvester και γι' αυτό έχουν πολύ καλή συμπεριφορά κάτω από ομομορφισμούς εκτίμησης, δείτε για παράδειγμα [118, 119, 120, 178]. Δηλαδή, μπορούμε να θεωρήσουμε τους συντελεστές των πολυωνύμων ως παραμέτρους, να υπολογίζουμε τις υπο-επιλύουσες συμβολικά και στη συνέχεια να αποδώσουμε τιμές στους παραμέτρους έχοντας την εγγύηση ότι θα υπολογίσουμε το ίδιο αποτέλεσμα με το αν είχαμε αντικαταστήσει τις παραμέτρους στην αρχή και στη συνέχεια υπολογίζαμε την ακολουθία των υπο-επιλυουσών.

Επίσης, το γεγονός ότι ορίζονται από ορίζουσες μας επιτρέπει να φράξουμε το δυαδικό μήκος των πολυωνύμων της ακολουθίας χρησιμοποιώντας την ανισότητα του Hadamard, δείτε για παράδειγμα [275, 276], και πιο συγκεκριμένα αν $\mathcal{R} = \mathbb{Z}$ τότε ισχύει ότι $\mathcal{L}\left(\mathbf{SR}_i\right) = \mathcal{O}(p\tau)$.

Ωστόσο, προκειμένου να υπολογίσουμε τις υπο-επιλύουσες δεν υπολογίζουμε ορίζουσες. Ο λόγος είναι ότι η πολυπλόκοτητα του υπολογισμού της ορίζουσας είναι $\mathcal{O}(p^3)$ και καθώς έχουμε $\mathcal{O}(q)$ πολυώνυμα στην ακολουθία θα καταλήγαμε σε έναν αλγόριθμο με πολυπλοκότητα $\mathcal{O}(p^3 q)$ που απέχει πολύ από το βέλτιστο που είναι $\mathcal{O}(pq)$. Οι αλγόριθμοι που υπολογίζουν υπο-επιλύουσες εκμεταλλεύονται την ειδική μορφή του πίνακα Sylvester και συνάγουν διάφορα θεωρήματα που αφορούν διαιρέτες του περιεχομένου των πολυωνύμων της ακολουθίας των υπο-επιλυουσών και χρησιμοποιούν ψευδο-διαιρέσεις. Το πιο γνωστό θεώρημα είναι το εξής:

Θεώρημα 2.21

Για $0 < k < q$, $k < q-1$, το ψευδο-υπόλοιπο των $\mathbf{SR}_{k+1}$ και $\mathbf{SR}_k$ είναι πολλαπλάσιο του $\mathbf{SR}_{k-1}$, δηλαδή

$$\mathbf{SR}_{k-1} = \mathsf{prem}\left(\mathbf{SR}_{k+1}, \mathbf{SR}_k\right) / \mathsf{lead}\left(\mathbf{SR}_{k+1}\right)$$

Το προηγούμενο θεώρημα μας παρέχει ένα αλγόριθμο υπολογισμού της ακολουθίας ο οποίος είναι πολυπλοκότητας $\mathcal{O}(p\,q)$ ή $\mathcal{O}_B(p\,q\,\mathsf{M}\left(p\,\tau\right))$, όταν $\mathcal{R} = \mathbb{Z}$.

Η παρουσίαση και άλλων θεωρημάτων είναι πέρα πό τις επιδιώξεις της παρούσας διατριβής. Ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία [54, 175, 176, 263, 264] για περισότε-

ρες λεπτομέρειες. Για λόγους πληρότητας θα παρουσιάσουμε χωρίς απόδειξη μερικούς ακόμα κανόνες υπολογισμού ακολουθιών πολυωνυμικών υπολοίπων ή ακολουθιών υπο-επιλυουσών:

$$[54]\quad \mathbf{reduced-PRS}(A,B)\quad \left\{\begin{array}{rcl} \mathfrak{a}_{q+1} &=& 1\\ (\mathfrak{a}_i,\mathfrak{b}_i) &=& \left(\mathfrak{r}_i^{\delta_i+1},\mathfrak{a}_{i+1}\right)\\ R_{i-1} &=& \mathsf{rem}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)/\mathfrak{b}_i\\ Q_i &=& \mathsf{quo}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)\end{array}\right\} \tag{2.14}$$

$$[34,\,54]\quad \mathbf{Subresultant-PRS}(A,B)\quad \left\{\begin{array}{rcll} \mathfrak{r}_{q+1} &=& 1 & \\ (\mathfrak{a}_i,\mathfrak{b}_i) &=& \left(\mathfrak{r}_i^{\delta_i+1},-\mathfrak{r}_{i+1}\,\psi_i^{\delta_i+1}\right) & \\ \psi_i &=& \left\{\begin{array}{ll} -1 & i=q\\ (-\mathfrak{r}_{i+1})^{\delta_{i+1}}\,\psi_{i+1}^{1-\delta_{i+1}} & \text{αλλιώς}\end{array}\right. & \\ R_{i-1} &=& \mathsf{rem}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)/\mathfrak{b}_i & \\ Q_i &=& \mathsf{quo}\left(\mathfrak{a}_i\,R_{i+1},R_i\right) & \end{array}\right\} \tag{2.15}$$

$$[36,\,37]\quad \mathbf{improved-PRS}(A,B)\quad \left\{\begin{array}{rcll} \mathfrak{r}_{q+1} &=& 1 & \\ (\mathfrak{a}_i,\mathfrak{b}_i) &=& \left(\mathfrak{r}_i^{\delta_i+1},-\mathfrak{r}_{i+1}\,\psi_i^{\delta_i+1}\,\mu_{i+1}^{-\delta_i-1}\right)\mu_i & \\ \psi_i &=& \left\{\begin{array}{ll} -1 & i=q\\ (-\mu_{i+2}\,\mathfrak{r}_{i+1})^{\delta_{i+1}}\,\psi_{i+1}^{1-\delta_{i+1}} & \text{αλλιώς}\end{array}\right. & \\ R_{i-1} &=& \mathsf{rem}\left(\mathfrak{a}_i\,R_{i+1},R_i\right)/\mathfrak{b}_i & \\ Q_i &=& \mathsf{quo}\left(\mathfrak{a}_i\,R_{i+1},R_i\right) & \end{array}\right\} \tag{2.16}$$

όπου τα μ_i είναι τέτοια ώστε να ικανοποιείται η Εξ. (2.9). Ο Brown [36, 37] προτείνει $\mu_i = \mathsf{gcd}\left(\mathsf{lead}\left(A\right),\mathsf{lead}\left(B\right)\right)$.

Ακολουθίες Sturm-Habicht

Υπάρχουν επίσης και οι ακολουθίες Sylvester-Habicht, οι οποίες συμβολίζονται με $\mathbf{StHa}(A,B)$ και οι οποίες αν $B=A'$ ονομάζονται ακολουθίες Sturm-Habicht [14, 118, 119, 175, 176]. Οι ακολουθίες αυτές είναι εξ ορισμού προσημασμένες (δείτε τον Ορ. 2.3) και όταν η ακολουθία είναι κανονική είναι, εκτός από κάποιο πρόσημο, οι ίδιες με την $\mathbf{SR}(A,B)$. Όταν όμως η ακολουθία είναι ελαττωματική τότε τα πολυώνυμα που την αποτελούν έχουν μικρότερους συντελεστές.

Όσον αφορά του κανόνες υπολογισμού της, υποθέτουμε ότι έχουμε δύο συνεχόμενα πολυώνυμα R_j και R_{j-1} της ακολουθίας και θέλουμε να υπολογίσουμε τα δύο επόμενα, δηλαδή τα R_k και R_{k-1}. Οι κανόνες είναι

1. $h_k\,R_{j-1} = \mathfrak{r}_{j-1}\,R_k$, όπου $h_k = (-1)^{(j-k)(j-k+1)/2}\,\dfrac{\mathfrak{r}_{j-1}^{j-k}}{\mathfrak{r}_j^{j-k-1}}$.
2. $R_\ell = 0$, για $k<\ell<j$.

3. $\mathfrak{r}_j^2\, R_{k-1} = -\,\mathsf{rem}\,(\mathfrak{r}_{j-1}\, h_k\, R_j, R_{j-1})$.

όπου ο υπολογισμός του υπολοίπου στην τελευταία σχέση εμπεριέχει μόνο ακριβείς διαιρέσεις με τους συντελεστές του διαιρέτη και του διαιρετέου. Αν $\deg(R_{j-1}) = j-1$ τότε $k = j-1$ και η ακολουθία είναι κανονική. Την ακολουθία αυτή έχουμε χρησιμοποιήσει στις υλοποιήσεις μας.

Γενικευμένες ακολουθίες Sturm

Οι γενικευμένες ακολουθίες Sturm [275] αποτελούν γενίκευση των ακολουθιών κατά Sturm, Εξ. (2.11).

Ορισμός 2.22 (Γενικευμένες ακολουθίες Sturm). *Έστω $A, B \in \mathbb{R}[X]$ όπως στην Εξ. (2.7). Ορίζουμε ως γενικευμένη ακολουθία Sturm (generalized Sturm sequence) ή προσημασμένη πολυωνυμική ακολουθία υπολοίπων (signed polynomial remainder sequence) ή προσημασμένη ακολουθία υπο-επιλυουσών (signed subresultant chain) των A και B την ακολουθία $\mathbf{St}(A,B) = (R_{q+1} = A, R_q = B, R_{q-1}, \ldots, R_h)$, για την οποία ισχύει*

$$\mathfrak{a}_i\, R_{i+1} = Q_i\, R_i + \mathfrak{b}_i\, R_{i-1} \qquad a_i b_i < 0 \tag{2.17}$$

όπου $\mathfrak{a}_i \mathfrak{b}_i < 0$, $q \geq i \geq h+1$ και το μήκος της ακολουθίας της ακολουθίας είναι $q-h+2$. Απαιτούμε $\mathfrak{a}_i, \mathfrak{b}_i \in \mathcal{R}$ και $R_i \in \mathcal{R}[X]$. Επίσης θεωρούμε και την ακολουθία πηλίκων $\mathbf{StQ}(A,B) = (Q_q, Q_{q-1}, \ldots, Q_h, A_h)$.

Οι ακολουθίες υπο-επιλυουσών που παρουσιάσαμε σε προηγούμενες παραγράφους μπορούν να γίνουν προσημασμένες είτε προσαρμόζοντας κατάλληλα τους κανόνες υπολογισμού τους είτε μετά τον υπολογισμό τους να χρησιμοποιήσουμε το αλγόριθμο του Yap [275], ο οποίος είναι γραμμικός, ώστε να τις καταστήσουμε προσημασμένες. Επίσης, όλα τα θεωρήματα που ισχύουν για τις υπο-επιλύουσες ισχύουν και αν είναι προσημασμένες.

Σημείωση 2.23. *Σε ό,τι θα ακολουθήσει θα θεωρήσουμε μόνο προσημασμένες ακολουθίες υπο-επιλυουσών και όταν αναφερόμαστε σε υπο-επιλύουσες θα εννοούμε προσημασμένες υπο-επιλύουσες.*

Προκειμένου να μην επιβαρύνουμε περαιτέρω τον συμβολισμό θα θεωρήσουμε $\mathbf{SR} = \mathbf{St}$ και $\mathbf{SRQ} = \mathbf{StQ}$.

Αν $\mathbf{SR}(A,B)$ είναι μια (προσημασμένη) ακολουθία υπο-επιλυουσών τότε συμβολίζουμε με $\mathbf{SR}(A, B\,;\, \mathsf{a})$ την ακολουθία που προκύπτει αν αποτίμησουμε όλα τα πολυώνυμα της ακολουθίας στο a, δηλαδή

$$\mathbf{SR}(A, B\,;\, \mathsf{a}) = (\mathbf{SR}_{q+1}(\mathsf{a}), \mathbf{SR}_q(\mathsf{a}), \ldots, \mathbf{SR}_1(\mathsf{a}), \mathbf{SR}_0(\mathsf{a}))$$

Ορισμός 2.24. *Έστω η ακολουθία $\mathtt{a} = (a_0, a_1, \ldots, a_k) \in \mathbb{R}^k$. Ορίζουμε το πλήθος των εναλλαγών προσήμων στην ακολουθία $\mathtt{a}$, το οποίο συμβολίζουμε $\mathtt{VAR}(\mathtt{a})$, αναγωγικά στο k ως:*

$$\begin{aligned} \mathtt{VAR}(a_1) &= 0 \\ \mathtt{VAR}(a_1, \ldots, a_k) &= \begin{cases} \mathtt{VAR}(a_1, \ldots, a_{k-1}) + 1 & \text{αν } \mathsf{sign}(a_{k-1} a_k) = -1 \\ \mathtt{VAR}(a_1, \ldots, a_{k-1}) & \text{αλλιώς} \end{cases} \end{aligned}$$

Σημείωση 2.25. *Αν* $f = \sum_{i=0}^{n} a_i X^i$ *τότε* $\mathtt{VAR}(f) = \mathtt{VAR}(a_n, \ldots, a_1, a_0)$.

Τα παρακάτω θεωρήματα αναδεικνύουν τη μεγάλη σημασία των προσημασμένων ακολουθιών:

Θεώρημα 2.26

Έστω $A, B \in \mathbb{R}[X]$ *σχετικά πρώτα μεταξύ τους. Αν* $\mathsf{a} < \mathsf{b}$, $\mathsf{a}, \mathsf{b} \in \mathbb{R} \cup \{\pm\infty\}$ *δεν είναι ρίζες του* A *τότε*

$$\begin{aligned} \mathtt{VAR}\left(\mathbf{SR}(A, B\,;\,[\mathsf{a},\mathsf{b}])\right) &:= \mathtt{VAR}\left(\mathbf{SR}(A, B\,;\,\mathsf{a})\right) - \mathtt{VAR}\left(\mathbf{SR}(A, B\,;\,\mathsf{b})\right) \\ &= \sum_{\substack{\gamma \mid A(\gamma)=0 \\ \mathsf{a}<\gamma<\mathsf{b}}} \operatorname{sign}\left(A'(\gamma)B(\gamma)\right) \end{aligned}$$

Η αποτίμηση στο $\pm\infty$ πραγματοποιείται θεωρώντας το όριο στο $\pm\infty$. Αν στο προηγούμενο θεώρημα αντικαταστήσουμε το $B = A'$ τότε η ποσότητα $\mathtt{VAR}\left(\mathbf{SR}(A, A'\,;\,[\mathsf{a},\mathsf{b}])\right)$ μας δίνει το πλήθος των πραγματικών ριζών του A στο διάστημα (a, b). Το επόμενο πόρισμα οφείλεται στον Sturm [248].

Πόρισμα 2.27. *Έστω* $A \in \mathbb{R}[X]$. *Αν* $\mathsf{a} < \mathsf{b}$, $\mathsf{a}, \mathsf{b} \in \mathbb{R} \cup \{\pm\infty\}$ *δεν είναι ρίζες του* A *τότε*

$$\mathtt{VAR}\left(\mathbf{SR}(A, A'\,;\,\mathsf{a})\right) - \mathtt{VAR}\left(\mathbf{SR}(A, A'\,;\,\mathsf{b})\right) = \#\{\gamma \mid A(\gamma) = 0 \wedge \mathsf{a} < \gamma < \mathsf{b}\}$$

Το προηγούμενο πόρισμα μπορεί να προκύψει θεωρώντας $B = 1$ στο παρακάτω θεώρημα:

Θεώρημα 2.28

Έστω $A, B \in \mathbb{R}[X]$ *σχετικά πρώτα μεταξύ τους. Αν* $\mathsf{a} < \mathsf{b}$, $\mathsf{a}, \mathsf{b} \in \mathbb{R}$ *δεν είναι ρίζες του* A *τότε*

$$\mathtt{VAR}\left(\mathbf{SR}(A, A'B\,;\,\mathsf{a})\right) - \mathtt{VAR}\left(\mathbf{SR}(A, A'B\,;\,\mathsf{b})\right) = \sum_{\substack{\gamma \mid A(\gamma)=0 \\ \mathsf{a}<\gamma<\mathsf{b}}} \operatorname{sign}\left(B(\gamma)\right)$$

Σημείωση 2.29. *Αν χρησιμοποιούσαμε τις ακολουθίες Sylvester-Habicht ή Sturm-Habicht τότε ο ορισμός του* $\mathtt{VAR}\left(\mathbf{StHa}(A, B\,;\,\mathsf{a})\right)$ *θα πρέπει να τροποποιηθεί ελαφρά. Πιο συγκεκριμένα, αφού διαγράψουμε τα μηδενικά πολυώνυμα, αποτιμούμε την ακολουθία πάνω στο* a *και προκειμένου να μετρήσουμε τις εναλλαγές προσήμων, μετράμε 1 εναλλαγή για κάθε ομάδα προσήμων* $[+, 0, 0, -]$ *και* $[-, 0, 0, +]$ *και 2 εναλλαγές για κάθε ομάδα* $[+, 0, 0, +]$ *και* $[-, 0, 0-]$.

Σε ό,τι θα ακολουθήσει θα συμβολίζουμε με $\mathbf{SR}(A)$ την ακολουθία $\mathbf{SR}(A, A')$.

Πολυπλοκότητα υπολογισμών με υπο-επιλύουσες

Θεωρούμε ότι $\mathcal{R} = \mathbb{Z}$ και $A, B, \in \mathbb{Z}[X]$ για A και B όπως στην Εξ. (2.7).

Υπάρχουν πολλοί αλγόριθμοι [14, 77, 176, 263, 275] για τον υπολογισμό προσημασμένων ακολουθιών υπο-επιλυουσών οι οποίοι βασίζονται, ως επί το πλείστον, στους κανόνες που έχουμε αναφέρει. Με την εξαίρεση του αλγορίθμου του Ducos [77], οι αλγόριθμοι προσπαθούν να είναι όσο το δυνατόν κοντύτερα στην ψευδο-Ευκλείδια ακολουθία και να υπολογίσουν διαιρέτες του περιεχομένου των πολυωνύμων της ακολουθίας.

Μπορούμε να διατυπώσουμε το ακόλουθο θεώρημα [14, 77, 176, 222]:

Θεώρημα 2.30

Έστω $A, B \in \mathbb{Z}[X]$ τέτοια ώστε $\deg(A) = p \geq q = \deg(B)$ και $\mathcal{L}(A) = \mathcal{L}(B) = \tau$. Η πολυπλοκότητα υπολογισμού της ακολουθίας $\mathbf{SR}(A, B)$ είναι $\mathcal{O}_B(pq\,\mathsf{M}(p\tau))$, ή $\widetilde{\mathcal{O}}_B(p^2q\tau)$. Επιπρόσθετα $\mathcal{L}(\mathbf{SR}_j(A, B)) = \mathcal{O}(p\tau)$.

Η παραπάνω πολυπλοκότητα είναι σχεδόν βέλτιστη, με την εξαίρεση κάποιων σταθερών και λογαριθμικών παραγόντων, καθώς: Υπάρχουν $\Omega(q)$ πολυώνυμα στην ακολουθία, τα οποία έχουν βαθμούς $\Omega(p)$, κατά συνέπεια ο συνολικός αριθμός των συντελεστών που εμφανίζονται στην ακολουθία είναι $\Omega(pq)$. Αυτή η παρατήρηση μας επιτρέπει να επιχειρηματολογήσουμε ότι η αριθμητική πολυπλοκότητα $O(pq)$ που επιτυγχάνεται από τους αλγορίθμους είναι βέλτιστη. Εφόσον το μέγιστο δυαδικό μήκος των συντελεστών είναι $\Omega(p\tau)$ με παρόμοιο τρόπο συνάγουμε και ότι η δυαδική πολυπλοκότητα είναι βέλτιστη.

Ωστόσο, το φράγμα πολυπλοκότητας αφορά το σύνολο της ακολουθίας $\mathbf{SR}(A, B)$. Όταν για παράδειγμα δεν ενδιαφερόμαστε για όλη την ακολουθία (π.χ μας ενδιαφέρει κάποιο συγκεκριμένο πολυώνυμο της ακολουθίας) ή όταν ο τελικός στόχος είναι η αποτίμηση της ακολουθίας πάνω σε έναν αριθμό τότε υπάρχουν και πιο γρήγοροι αλγόριθμοι. Η βασική τους ιδέα είναι να αναπαραστήσουν την $\mathbf{SR}(A, B)$ εμμέσως με τη χρήση της αντίστοιχης πολυωνυμικής ακολουθίας πηλίκων, $\mathbf{SRQ}(A, B)$.

Οι αλγόριθμοι είναι *διαίρει-και-βασίλευε* και βασίζονται πάνω στην δομή του αλγορίθμου HALF-GCD [247, 275]. Στην σύγχρονη μορφή τους οι αλγόριθμοι παρουσιάστηκαν από τον Reischert [222] και τους Lickteig and Roy [175], δείτε επίσης [263].

Αν $\mathbf{SRQ}(A, B) = (Q_0, Q_1, \ldots, Q_{k-1}, \mathbf{SR}_k)$ είναι η ακολουθία πηλίκων που αντιστοιχεί στην $\mathbf{SR}(A, B)$ όπου $\mathbf{SR}_k \neq 0$, τότε μπορούμε να διατυπώσουμε το ακόλουθο θεώρημα [14, 175, 222, 263]:

Θεώρημα 2.31

Έστω $A, B \in \mathbb{Z}[X]$ τέτοια ώστε $\deg(A) = p \geq q = \deg(B))$ και $\mathcal{L}(A) = \mathcal{L}(B) = \tau$. Ο υπολογισμός της ακολουθίας $\mathbf{SRQ}(A, B)$, της επιλύουσας, $\mathtt{res}(A, B)$, και του ΜΚΔ, $\gcd(A, B)$, έχει πολυπλοκότητα $\mathcal{O}_B(q \lg q \mathsf{M}(p\tau))$ ή $\widetilde{\mathcal{O}}_B(p\,q\,\tau)$. Επιπρόσθετα, $\mathcal{L}(\mathtt{res}(A, B)) = \mathcal{L}(\gcd(A, B)) = \mathcal{O}(p\,\tau)$.

Παρατηρούμε ότι το πλήθος των συντελεστών της $\mathbf{SRQ}(A, B)$ είναι $\mathcal{O}(q)$ και ότι έχουν μέγιστο δυαδικό μήκος $\mathcal{O}(p\tau)$ [14, 222]. Όσον αφορά στον υπολογισμό κάποιου πολυωνύμου της ακολουθίας $\mathbf{SR}(A, B)$ και στον υπολογισμό του $\gcd(A, B)$, η πολυπλοκότητα του Θεωρ. 2.31 είναι

βέλτιστη, με την εξαίρεση κάποιων σταθερών και πολυλογαριθμικών παραγόντων. Αυτό προκύπτει από το γεγονός ότι στη γενική περίπτωση ο βαθμός των πολυωνύμων στην ακολουθία είναι $\mathcal{O}(q)$ και οι συντελεστές τους έχουν δυαδικό μήκος $\mathcal{O}(p\tau)$. Δεν συμβαίνει το ίδιο και με τον υπολογισμό του $\mathtt{res}(A, B)$. Στη γενική περίπτωση το δυαδικό μήκος όλων των συντελεστών του $\mathtt{res}(A, B)$ είναι $\mathcal{O}(p\tau)$, για παράδειγμα αν $\mathtt{res}(A, B) \in \mathbb{Z}$.

Μπορούμε να χρησιμοποιήσουμε την ακολουθία πηλίκων προκειμένου να υπολογίσουμε την αποτίμηση της $\mathbf{SR}(A, B)$ πάνω σε κάποιο αριθμό [65, 241, 247]. Η αποτίμηση πρέπει να αρχίσει από το τελευταίο στοιχείο της ακολουθίας υπολοίπων. Το επόμενο θεώρημα [175, 222] μας παρέχει την πολυπλοκότητα αυτού του υπολογισμού.

Θεώρημα 2.32

Ο υπολογισμός της αποτίμησης της $\mathbf{SR}(A, B)$ *πάνω σε ένα αριθμό* $\mathsf{a} \in \mathbb{Q} \cup \{\pm\infty\}$, $\mathcal{L}(\mathsf{a}) = \sigma$, $\mathbf{SR}(A, B\,;\, \mathsf{a})$, *έχει πολυπλοκότητα* $\mathcal{O}_B(q\,\lg(q)\,\mathsf{M}(\max(p\tau, q\sigma)))$ *ή* $\mathcal{O}_B(q\,\mathsf{M}(\max(p\tau, q\sigma)))$ *εάν η* $\mathbf{SRQ}(A, B)$ *δεν είναι ήδη υπολογισμένη.*

Και στις δύο περιπτώσεις η πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(q\max\{p\tau, q\sigma\})$.

Σημείωση 2.33. *Σε πολλές περιπτώσεις (π.χ απομόνωση πραγματικών ριζών, σύγκριση πραγματικών αλγεβρικών αριθμών) χρειάζεται να υπολογίσουμε την αποτίμηση* $\mathbf{SR}(A, B\,;\, \mathsf{a})$, *όπου* $\mathcal{L}(\mathsf{a}) = \mathcal{O}(p\tau)$. *Εάν υπολογίσουμε την αποτίμηση εφαρμόζοντας διαδοχικά τον κανόνα του Horner τότε αφού υπάρχουν* $\Omega(q^2)$ *συντελεστές στην ακολουθία και πρέπει να πολλαπλασιάσουμε αριθμούς δυαδικού μήκους* $\mathcal{O}(p\tau)$ *και* $\mathcal{O}(p^2\tau)$, *η συνολική πολυπλοκότητα είναι* $\widetilde{\mathcal{O}}_B(p^2q^2\tau)$.

Ωστόσο, ακόμα και όταν υπάρχει η ανάγκη υπολογισμού της ακολουθίας $\mathbf{SR}(A, B)$ *η ακολουθία* $\mathbf{SRQ}(A, B)$ *μπορεί να υπολογιστεί με την ίδια πολυπλοκότητα [14, 222]. Οπότε μπορούμε πάντοτε να χρησιμοποιήσουμε την ακολουθία πηλίκων για αποτιμήσεις.*

Το $A \in \mathcal{R}[X]$ λέμε ότι είναι χωρίς τετράγωνα αν $\deg(\gcd(A, A')) = 0$. Ή διαφορετικά, το A δεν έχει ρίζες πολλαπλότητας > 1 στο $\mathcal{K}$. Ορίζουμε το χωρίς τετράγωνα μέρος του A ως

$$A_{red} = \frac{A}{\gcd(A, A')}$$

Παρατηρούμε ότι η διαίρεση είναι καλώς ορισμένη στο $\mathcal{R}[X]$, δηλαδή είναι μια τέλεια διαίρεση χωρίς υπόλοιπο. Για τον υπολογισμό του χωρίς τετράγωνα μέρους του A, ισχύει το ακόλουθο θεώρημα [14, Algorithm 10.17, p. 326]:

Θεώρημα 2.34

Αν $A \in \mathbb{Z}[X]$ *τέτοιο ώστε* $\deg(A) = p$ *και* $\mathcal{L}(A) = \tau$, *τότε το χωρίς τετράγωνα μέρος του* A, A_{red}, *μπορεί να υπολογιστεί από την ακολουθία* $\mathbf{SR}(A, A')$, *με πολυπλοκότητα* $\mathcal{O}_B(p\lg p\mathsf{M}(p\tau))$ *ή* $\widetilde{\mathcal{O}}_B(p^2\tau)$. *Επιπρόσθετα,* $\mathcal{L}(A_{red}) = \mathcal{O}(p + \tau)$.

Σημείωση 2.35. *Υπάρχει ένα βήμα κανονικοποίησης [14] στον υπολογισμό του τελευταίου στοιχείου της ακολουθίας* $\mathbf{SR}(A, A^{'})$ *και γι' αυτό επιτυγχάνουμε* $\mathcal{L}\left(A_{red}\right) = \mathcal{O}(p + \tau)$. *Εάν χρησιμοποιούσαμε το γενικό φράγμα για τις ακολουθίες υπο-επιλυουσών ή το φράγμα του Mignotte [187] σχετικά με το δυαδικό μήκος των συντελεστών των διαιρετών ενός πολυωνύμου τότε θα συν άγαμε ότι* $\mathcal{L}\left(A_{red}\right) = \mathcal{O}(p\tau)$.

2.4 Πολυώνυμα στη βάση Bernstein

Όλα τα πολυώνυμα βαθμού $\leq d$ στο $\mathbb{R}[X]$ αποτελούν ένα διανυσματικό χώρο διάστασης d πάνω στο $\mathbb{R}$. Η συνήθης αναπαράσταση των πολυωνύμων, Εξ. (2.1), είναι κάποιος γραμμικός συνδυασμός των στοιχειωδών πολυωνύμων $\{1, X, \ldots, X^d\}$. Αυτά τα στοιχειώδη πολυώνυμα αποτελούν και (μία) βάση του διανυσματικού χώρου η οποία ονομάζεται *βάση δυνάμεων* (power basis).

Ωστόσο, μπορούμε να αναπαραστήσουμε τα πολυώνυμα χρησιμοποιώντας άλλες βάσεις. Στην παρούσα παράγραφο παρουσιάσουμε συνοπτικά τη βάση Bernstein για την αναπαράσταση των πολυωνύμων. Η αναπαράσταση σε βάση Bernstein είναι αριθμητικά ευσταθής σε αντίθεση με τη βάση δυνάμεων που είναι αριθμητικά ασταθής. Αυτός είναι και ο λόγος που έχει πολύ μεγάλη πρακτική σημασία. Θα πρέπει ωστόσο να τονίσουμε ότι η διαδικασία μετατροπής από τη βάση των δυνάμεων στη βάση Bernstein και το αντίστροφο είναι διαδικασίες αριθμητικά ασταθείς. Για περισσότερες λεπτομέρειες και για μια πιο εκτενή περιγραφή της βάσης Bernstein και των ιδιοτήτων της ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία, π.χ [102, 103, 104].

Έστω $\mathbb{R}[X]_d$ το σύνολο των πραγματικών πολυωνύμων βαθμού $\leq d$. Έστω $a < b \in \mathbb{R}$, συμβολίζουμε με

$$\mathfrak{B}_d^i(X; a, b) = \binom{d}{i} \frac{(X-a)^i (b-X)^{d-1}}{(b-a)^d} \quad i = 0, \ldots, d$$

τη βάση Bernstein των $\mathbb{R}[X]_d$ στο διάστημα $[a, b]$.

Για κάθε πολυώνυμο $f \in \mathbb{R}[X]_d = \sum_{i=0}^{d} b_i \mathfrak{B}_d^i(X; a, b)$, το οποίο αναπαρίσταται στη βάση Bernstein, οι συντελεστές $\mathbf{b} = (b_i)_{i=0,\ldots,d}$ ονομάζονται *συντελεστές ελέγχου* (*control coefficients*) του f. Συμβολίζουμε με $\mathtt{VAR}(f) \equiv \mathtt{VAR}(\mathbf{b})$, το πλήθος των εναλλαγών προσήμου. στην ακολουθία $\mathbf{b}$ των συντελεστών (αφού αφαιρέσουμε τα μηδενικά).

Δοθέντος πολυωνύμου f με αναπαράσταση στη βάση Bernstein στο διάστημα $\mathcal{I} = [a, b]$, ο αλγόριθμος του de Casteljau, δείτε για παράδειγμα [14, 205], μας επιτρέπει να υπολογίσουμε την αναπαράσταση του f σε δύο υποδιαστήματα του $\mathcal{I}$, $\mathcal{I}_L = [a, (1-t)a + tb]$ και $\mathcal{I}_R = [(1-t)a + tb, b]$, όπου $0 \leq t \leq 1$. Πιο συγκεκριμένα, $\mathbf{b}_L = (b_0^i)_{i=0,\ldots,d}$ (αντίστοιχα $\mathbf{b}_R = (b_i^{d-i})_{i=0,\ldots,d}$) είναι οι συντελεστές ελέγχου του f στο I_L (αντίστοιχα I_R), όπου $b_i^0 = b_i, i = 0, \ldots, d$, και

$$b_i^r = (1-t)\, b_i^{r-1} + t\, b_{i+1}^{r-1}(t), \quad 0 \leq i \leq d-r,\ 0 \leq r \leq d. \tag{2.18}$$

Προκειμένου να αναλύσουμε την πολυπλοκότητα του αλγορίθμου του de Casteljau αναφέρουμε μερικούς πολυωνυμικούς μετασχηματισμούς που σχετίζονται με αναπαράσταση στη βάση

Bernstein. Ο αναγνώστης μπορεί να ανατρέξει στους Mourrain et al. [205] για περισσότερες λεπτομέρειες.

Έστω $\mathbb{R}[X,Y]_{[d]}$ το σύνολο όλων των ομογενών πολυωνύμων βαθμού d με μεταβλητές (X,Y). Για κάθε $f \in \mathbb{R}[X]_d$, συμβολίζουμε με $\overline{f}$ την ομογενοποίηση του f στο βαθμό d. Για $\lambda \neq 0, \mu \in \mathbb{R}$ θεωρούμε τις ακόλουθες απεικονίσεις $\mathbb{R}^2 \to \mathbb{R}^2$:

- $\mathcal{R} : (X,Y) \mapsto (Y,X)$,
- $\mathcal{H}_\lambda : (X,Y) \mapsto (\lambda X, Y)$,
- $\mathcal{H}'_\lambda : (X,Y) \mapsto (X, \lambda Y)$,
- $\mathcal{T}_\mu : (X,Y) \mapsto (X - \mu Y, Y)$,
- $\mathcal{T}'_\mu : (X,Y) \mapsto (X, Y - \mu X)$.

Η σύνθεση των παραπάνω απεικονίσεων με το $\overline{f}$ παράγει αντιστρέψιμες απεικονίσεις πάνω στο σύνολο των πολυωνύμων βαθμού d και οι αντίστοιχες απεικονίσεις στα μη ομογενή πολυώνυμα τις οποίες και θα συμβολίσουμε με τα ίδια σύμβολα είναι, $\forall f \in \mathbb{R}[X]_d$:

- $\mathcal{R}(f) = X^d f(1/X)$,
- $\mathcal{H}_\lambda(f) = f(\lambda X)$,
- $\mathcal{H}'_\lambda(f) = f(\lambda^{-1} X)$,
- $\mathcal{T}_\mu(f) = f(X - \mu)$,
- $\mathcal{T}'_\mu(f) = (1 - \mu\, X)^d f(\frac{X}{1-\mu\, X})$.

Για κάθε πολυώνυμο $f(X) = \sum_{i=0}^d b_i \mathfrak{B}_d^i(X;a,b)$, έχουμε

$$\mathcal{R} \circ \mathcal{T}_1 \circ \mathcal{R} \circ \mathcal{H}_{b-a} \circ \mathcal{T}_{-a}(f) = \sum_{i=0}^{d} \binom{d}{i} b_i X^i.$$

Ας θεωρήσουμε ένα διάστημα $[c,d]$. Η αναπαράσταση του f στη βάση Bernstein στο $[c,d]$ είναι $f(X) = \sum_{i=0}^d b'_i \mathfrak{B}_d^i(X;c,d)$. Η απεικόνιση η οποία μετασχηματίζει το f από τη βάση Bernstein στο διάστημα $[a,b]$ στη βάση Bernstein στο διάστημα $[c,d]$, δηλαδή από το $\sum_{i=0}^d \binom{d}{i} b_i X^i$ στο $\sum_{i=0}^d \binom{d}{i} b'_i X^i$ είναι

$$\mathcal{R} \circ \mathcal{T}_1 \circ \mathcal{R} \circ \mathcal{H}_{d-c} \circ \mathcal{T}_{-c} \circ \mathcal{T}_a \circ \mathcal{H}_{\frac{1}{b-a}} \circ \mathcal{R} \circ \mathcal{T}_{-1} \circ \mathcal{R} = \mathcal{T}'_1 \circ \mathcal{H}_{d-c} \circ \mathcal{T}_{a-c} \circ \mathcal{H}_{\frac{1}{b-a}} \circ \mathcal{T}'_{-1} \tag{2.19}$$

Αν θεωρήσουμε $[a,b] = [0,1]$ και $[c,d] = [0,\frac{1}{2}]$ τότε η απεικόνιση (2.19) γίνεται: $\mathcal{R} \circ \mathcal{T}_{-1} \circ \mathcal{R} \circ \mathcal{H}_{\frac{1}{2}} \circ \mathcal{R} \circ \mathcal{T}_1 \circ \mathcal{R}$. Μετά από απλοποιήσεις, έχουμε

$$\mathcal{S}_L : \overline{f} \mapsto \overline{f}\left(X + \frac{Y}{2}, \frac{Y}{2}\right) = \overline{f} \circ \mathcal{T}_{-1} \circ \mathcal{H}'_{\frac{1}{2}}. \tag{2.20}$$

Αν θεωρήσουμε τη συμμετρική περίπτωση, δηλαδή $[a,b] = [0,1]$ και $[c,d] = [\frac{1}{2},1]$ τότε η απεικόνιση (2.19) γίνεται: $\mathcal{R}\circ\mathcal{T}_{-1}\circ\mathcal{R}\circ\mathcal{H}_{\frac{1}{2}}\circ\mathcal{T}_{-\frac{1}{2}}\circ\mathcal{R}\circ\mathcal{T}_1\circ\mathcal{R}$. Η οποία αντιστοιχεί στην ακόλουθη απεικόνιση στα ομογενή πολυώνυμα:

$$\mathcal{S}_R : \overline{f} \mapsto \overline{f}\left(\frac{X}{2}, \frac{X}{2}+Y\right) = \overline{f}\circ\mathcal{T}'_{-1}\circ\mathcal{H}_{\frac{1}{2}}. \tag{2.21}$$

Και στις δύο περιπτώσεις, αν πολλαπλασιάσουμε με 2^d παράγουμε την απεικόνιση $\overline{\mathcal{S}}_R : \overline{p} \mapsto \overline{p}(X, X+2Y)$, (αντίστοιχα $\overline{\mathcal{S}}_L : \overline{p} \mapsto \overline{p}(2X+Y, Y)$), η οποία ενεργεί σε πολυώνυμα με ακέραιους συντελεστές.

Η επόμενη πρόταση μας επιτρέπεινα υλοποιήσουμε τη διάσπαση ενός πολυωνύμου σε δύο υποδιαστήματα με την εφαρμογή μετασχηματισμών μετατόπισης.

Πρόταση 2.36. *Έστω $(b_i)_{i=0,\ldots,d} \in \mathbb{Z}^{d+1}$ οι συντελεστές ενός πολυωνύμου f στη βάση Bernstein στο διάστημα $[a,b]$, και έστω ν ένα φράγμα στο δυαδικό μήκος των συντελεστών. Η πολυπλοκότητα του υπολογισμού των συντελεστών στη βάση Bernstein του f πάνω στα δύο υποδιαστήματα $[a, \frac{a+b}{2}]$ και $[\frac{a+b}{2}, b]$ φράσσεται από $\widetilde{\mathcal{O}}_B(d(d+\nu))$ και το δυαδικό μήκος των συντελεστών από $d+\nu$.*

Απόδειξη: Χρησιμοποιώντας το σχήμα του de Casteljau, Εξ. (2.18) με $t = \frac{1}{2}$, αποδεικνύουμε με επαγωγή ότι οι συντελεστές $b_i^r = \frac{(b_i^{r-1} + b_{i+1}^{r-1})}{2}$ είναι της μορφής $\frac{\overline{b}_i^r}{2^i}$, όπου $\overline{b}_i^r \in \mathbb{Z}$ είναι δυαδικού μήκους $\leq \nu + r$. Θέτοντας τον ίδιο παρανομαστή 2^d προκύπτουν ακέραιοι συντελεστές μήκους $\leq \nu + d$.

Συμβολίζουμε με ν' το μήκος των συντελεστών $\left(\binom{d}{i} b_i\right)_{i=0,\ldots,d}$ όπου $(b_i)_{i=0,\ldots,d}$ είναι οι συντελεστές του f στη βάση Bernstein $(\mathfrak{B}_d^i(X;a,b))_{i=0,\ldots,d}$. Παρατηρούμε ότι $\nu' \leq \nu + d$.

Για τον υπολογισμό των συντελεστών του f στα διαστήματα $[a, \frac{a+b}{2}]$ και $[\frac{a+b}{2}, b]$, εφαρμόζουμε τις ίδιες απεικονίσεις όπως όταν υπολογίζαμε τους συντελεστές ενός πολυωνύμου στη βάση Bernstein στα διαστήματα $[0, \frac{1}{2}]$ και $[\frac{1}{2}, 1]$, δοθέντος της αναπαράστασης σε βάση Bernstein στο διάστημα $[0,1]$.

Σύμφωνα με την Εξ. (2.20), η εκτέλεση του αλγόριθμου de Casteljau αντιστοιχεί αρχικά στον πολλαπλασιασμό με τους διωνυμικούς συντελεστές, στη συνέχεια σε μια μετατόπιση $Y \to X+Y$, σε μια κλιμάκωση της μιας μεταβλητής του ομογενούς πολυωνύμου $\overline{f}$ κατά $\frac{1}{2}$ και τέλος σε μια διαίρεση με τους διωνυμικούς συντελεστές[1].

Εφόσον το δυαδικό μήκος των δυωνυμικών συντελεστών φράσσεται από d (το άθροισμά τους είναι 2^d), πολλαπλασιάζοντας τους με b_i κοστίζει το πολύ $\widetilde{\mathcal{O}}_B(d(\nu+d))$. Η μετατόπιση κατά 1 ενός πολυωνύμου βαθμού d με συντελεστές δυαδικού μήκους $\leq \nu + d$ απαιτεί $\widetilde{\mathcal{O}}_B(d(d+\nu))$ [262] και παράγει ένα πολυώνυμο με συντελεστές μήκους $\mathcal{O}(\nu+d)$. Συνεπώς η μετατόπιση του πολυωνύμου κατά $\frac{1}{2}$ και ο υπολογισμός του πηλίκου με τους διωνυμικούς συντελεστές απαιτεί $\widetilde{\mathcal{O}}_B(d(\nu+d))$ δυαδικές πράξεις..

Κατά συνέπεια, η πολυπλοκότητα του υπολογισμού των συντελεστών Bernstein του f στο υποδιάστημα $[a, \frac{a+b}{2}]$ φράσσεται από $\widetilde{\mathcal{O}}_B(d(\nu+d))$. Εκ συμμετρίας, αντιστρέφοντας τους συντελεστές του f, προκύπτει το ίδιο φράγμα για τους συντελεστές του f στο $[\frac{a+b}{2}, b]$.

Έτσι ολοκληρώνεται η απόδειξη. ΟΕΔ

2.5 Σύνοψη – Μελλοντικές επεκτάσεις

Το κεφάλαιο περιέχει τις βασικές αλγεβρικές και αλγοριθμικές έννοιες που απαιτούνται για την κατανόηση της διατριβής. Παρουσιάμε την πολυπλοκότητα των βασικών πράξεων με ακέραιους αριθμούς και πολυώνυμα σε μία μεταβλητή, την έννοια της επιλύουσας και της διακρίνουσας και τις ακολουθίες πολυωνυμικών υπολοίπων. Τέλος, παρουσιάσαμε συνοπτικά την αναπαράσταση των πολυωνύμων στη βάση Bernstein και αποδείξαμε ότι δοθέντος ενός πολυωνύμου στη βάση Bernstein σε κάποιο διάστημα, ο υπολογισμός των συντελεστών του σε δύο υποδιαστήματα του αρχικού διαστήματος ανάγεται σε δύο μετατοπίσεις κατά 1 και άρα η πολυπλοκότητά του είναι αυτή της μετατόπισης.

Όπως γίνεται εύκολα κατανοητό από τον αναγνώστη η περιοχή των (προσημασμένων) πολυωνυμικών ακολουθιών υπολοίπων είναι τεράστια με πολλούς, μερικές φορές αντικρουόμενους, ορισμούς και δεκάδες θεωρήματα. Θεωρούμε ως μεγάλη επιστημονική πρόκληση τη πρόταση μιας θεωρίας που να ενοποιεί και να απλοποιεί τις παρούσες προσεγγίσεις. Επίσης μια ενδελεχής πειραματική μελέτη των διαφόρων αλγορίθμων υπολογισμού των ακολουθιών υπολοίπων πρέπει να είναι από τις πρώτες προτεραιότητες.

Το μεγαλύτερο ανοιχτό πρόβλημα αφορά τον υπολογισμό της επιλύουσας δύο πολυωνύμων. Δοθέντων δύο πολυωνύμων βαθμού d και δυαδικού μήκους τ, οι καλύτεροι μέχρι σήμερα αλγόριθμοι υπολογίζουν την επιλύουσα με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2\tau)$ [175, 222]. Ωστόσο, η επιλύουσα έχει δυαδικό μήκος $\mathcal{O}(d\tau)$ στη χειρότερη περίπτωση. Υπάρχει αλγόριθμος, έστω και πιθανοτικός, που να υπολογίζει την επιλύουσα δύο πολυωνύμων με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d\tau)$;

ΚΕΦΑΛΑΙΟ 3

Πραγματική επίλυση πολυωνύμων σε μία μεταβλητή

> Ομαδοποίησε τους υπολογισμούς. Ταξινόμησέ τους ανάλογα με την πολυπλοκότητά τους και όχι σύμφωνα με τη μορφή τους. Αυτή νομίζω είναι η αποστολή των μελλοντικών μαθηματικών.
>
> Evariste Galois

Περίληψη

Δοθέντος ενός ακέραιου πολυωνύμου, όχι απαραίτητα χωρίς τετράγωνα, σε μία μεταβλητή παρουσιάζουμε αλγορίθμους για τον υπολογισμό διαστημάτων με ρητά άκρα που απομονώνουν τις πραγματικές ρίζες του και υπολογίζουν τις πολλαπλότητές τους.

Τα πρωτότυπα αποτελέσματα του κεφαλαίου αφορούν τη μελέτη της ποιότητας των φραγμάτων για τις θετικές πραγματικές ρίζες, ένα θεώρημα για τα σύνθετα φράγματα διαχωρισμού, την ενοποίηση και απλοποίηση της θεωρίας για τους αλγορίθμους επίλυσης πολυωνύμου που βασίζονται στην υποδιαίρεση και τη βελτίωση της πολυπλοκότητας κατά δύο παράγοντες του αλγορίθμου των συνεχών φραγμάτων. Επιπρόσθετα, για όλους τους αλγορόιθμους επίλυσης, αποδεικνύουμε ότι το φράγμα πολυπλοκότητας ισχύει και για πολυώνυμα με τετράγωνα και ότι με την ίδια πολυπλοκότητα υπολογίζουμε και την πολλαπλότητα των ριζών. Μέρος των αποτελεσμάτων παρουσιάστηκε στις εργασίες [97, 252, 253].

Η επίλυση πολυωνυμικών εξισώσεων είναι ένα από τα παλαιότερα και πιο γνωστά προβλήματα στα μαθηματικά. Οι προσπάθειες επίλυσης της πολυωνυμικής εξίσωσης αποτέλεσαν τη γεννησιουργό αιτία για πολλές από τις πιο σημαντικές μαθηματικές έννοιες. Ενδεικτικά αναφέρουμε τους άρρητους και τους μιγαδικούς αριθμούς, τη θεωρία ομάδων, την έννοια του σώματος και του ιδεώδους, τη θεωρία των συμμετρικών συναρτήσεων και την επιλύουσα.

Στη σύγχρονη ιστορία των μαθηματικών η επίλυση της πολυωνυμικής εξίσωσης δεν κατέχει τον κεντρικό ρόλο που κατείχε στους περασμένους αιώνες, αν και εξακολουθεί να αποτελεί το κεντρικό πρόβλημα για τους ερευνητές στις περιοχές της αριθμητικής ανάλυσης και της υπολογιστικής άλγεβρας, τουλάχιστον. Ο αναγνώστης που ενδιαφέρεται για την ιστορική εξέλιξη της επίλυσης της πολυωνυμικής εξίσωσης, κυρίως από τη σκοπιά της αριθμητικής ανάλυσης, μπορεί να ανατρέξει στις εργασίες του Pan [210, 211]. Επίσης σχεδόν όλες οι εργασίες σχετικά με την επίλυση πολυωνυμικών εξισώσεων περιέχονται στην ιστοσελίδα του John Michael McNamee[1], δείτε επίσης [183, 184, 185].

Τα τελευταία 20 με 30 χρόνια η επίλυση, ή πιο σωστά, οι αλγόριθμοι επίλυσης της πολυωνυμικής εξίσωσης βρίσκονται ξανά στο επίκεντρο καθώς πολλές επιστημονικές περιοχές, όπως η μη γραμμική υπολογιστική γεωμετρία, η σχεδίαση με υπολογιστή, η γεωμετρική μοντελοποίηση, τα συστήματα γεωγραφικών πληροφοριών και η ρομποτική έχουν επικεντρωθεί σε προβλήματα με καμπύλα αντικείμενα ή/και σε προβλήματα που περιέχουν μη γραμμικότητες πολυωνυμικής μορφής. Σε τέτοια προβλήματα η επίλυση της πολυωνυμικής εξίσωσης παίζει πολύ σημαντικό ρόλο τόσο από θεωρητική όσο από πρακτική άποψη.

Πώς ορίζεται όμως η πολυωνυμική εξίσωση και τί εννούμε με τον όρο επίλυση;

Σε ό,τι θα ακολουθήσει θα θεωρήσουμε το πολυώνυμο $A \in \mathcal{R}[X]$, όπου $\mathcal{R}$ κάποιος υποδακτύλιος του $\mathbb{C}$, και

$$A(X) = a_d\, X^d + a_{d-1}\, X^{d-1} + \cdots + a_1\, X + a_0 \tag{3.1}$$

Προκειμένου να αποφύγουμε εκφυλισμένες περιπτώσεις θεωρούμε $a_d\, a_0 \neq 0$. Αν $A \in \mathbb{Z}[X]$ τότε $\mathcal{L}(A) = \tau$. Η πολυωνυμική εξίσωση είναι η εξίσωση

$$A(X) = 0$$

Με τον όρο επίλυση εννοούμε τον υπολογισμό αριθμών γ, τέτοιων ώστε να ισχύει $A(\gamma) = 0$. Αυτοί οι αριθμοί ονομάζονται ρίζες (roots) της πολυωνυμικής εξίσωσης. Το θεμελιώδες θεώρημα της άλγεβρας (Fundamental theorem of algebra), το οποίο διατυπώθηκε αρχικά από τον Descartes και του οποίου η πρώτη (ημιτελής) απόδειξη παρουσιάστηκε στη διδακτορική διατριβή του Gauss, μας εξασφαλίζει ότι το πολυώνυμο έχει ακριβώς τόσες (μιγαδικές) ρίζες όσες και ο βαθμός του, αν μετρήσουμε και τις πολλαπλότητές τους. Δηλαδή υπάρχουν μιγαδικοί αριθμοί $\gamma_1, \ldots, \gamma_d \in \mathbb{C}$ τέτοιοι ώστε η (3.1) να γράφεται ως

$$A(X) = a_d \prod_{i=1}^{d} (X - \gamma_i)$$

Αν ενδιαφερόμαστε για τον υπολογισμό μόνο των πραγματικών ριζών τότε χρησιμοποιούμε τον όρο πραγματική επίλυση. Σχετικά με το θεμελιώδες θεώρημα της άλγεβρας ο αναγνώστης μπορεί να ανατρέξει για παράδειγμα στους van der Waerden [258] και Uspensky [255].

Στην παρούσα διατριβή θα ασχοληθούμε με την πραγματική επίλυση ακέραιων πολυωνύμων, δηλαδή $A \in \mathbb{Z}[X]$. Οι αριθμοί που προκύπτουν ως λύσεις ακεραίων πολυωνύμων ονομάζονται αλγεβρικοί αριθμοί και αν είναι πραγματικοί τότε ονομάζονται πραγματικοί αλγεβρικοί αριθμοί. Πιο συγκεκριμένα

[1] www1.elsevier.com/homepage/sac/cam/mcnamee/

Ορισμός 3.1. *Ένας πραγματικός αριθμός ονομάζεται πραγματικός αλγεβρικός αριθμός αν είναι ρίζα κάποιου πολυωνύμου με ακέραιους συντελεστές.*

Το σύνολο των πραγματικών αλγεβρικών αριθμών είναι σώμα και το συμβολίζουμε με $\mathbb{R}_{alg}$. Το $\mathbb{R}_{alg}$ είναι αριθμήσιμο και ισχύει

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}_{alg} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Αν $\gamma \in \mathbb{R}_{alg}$ τότε από όλα τα πολυώνυμα $A \in \mathbb{Z}[X]$ για τα οποία ισχύει $A(\gamma) = 0$, εκείνα με τον ελάχιστο βαθμό ονομάζονται ελαχιστικά (minimal) πολυώνυμα του γ. Αν επιπλέον απαιτήσουμε το πολυώνυμο να είναι πρωταρχικό (primitive) τότε ονομάζεται ελάχιστο (minimum) πολυώνυμο του γ. Ο βαθμός του γ, $\deg(\gamma)$, είναι ο βαθμός του ελάχιστου πολυωνύμου του και αν $\gamma = 0$ τότε εξ ορισμού το ελάχιστο πολυώνυμο είναι το $A = 0$ και $\deg(\gamma) = -\infty$. Αν το A έχει και άλλες (μιγαδικές) ρίζες εκτός από το γ τότε αυτοί οι αριθμοί ονομάζονται συζυγείς (conjugate) του γ.

Κατά συνέπεια το πρόβλημα της επίλυσης της πολυωνυμικής εξίσωσης είναι (σχεδόν) ισοδύναμο με το πρόβλημα της κατασκευής των στοιχείων του $\mathbb{R}_{alg}$. Οπότε τίθεται το ερώτημα: Πώς αναπαριστούμε τα στοιχεία του $\mathbb{R}_{alg}$ ή ισοδύναμα ποιά είναι η έξοδος των αλγορίθμων πραγματικής επίλυσης πολυωνυμικών εξισώσεων;

Για να απαντήσει στα παραπάνω ερωτήματα, η αλγεβρική προσέγγιση υπολογίζει τις λύσεις μιας πολυωνυμικής εξίσωσης με τη βοήθεια των βασικών πράξεων και ριζικών. Η προσέγγιση αυτή στη γενική περίπτωση, όπως απέδειξαν οι εργασίες των Abel και Galois δεν μπορεί να επιλύσει πολυώνυμα βαθμού μεγαλύτερου από 4.

Η αριθμητική προσέγγιση υπολογίζει κάποια προσέγγιση στις ρίζες μέχρι κάποια ακρίβεια, η οποία είτε είναι είσοδος στον αλγόριθμο είτε είναι το φράγμα διαχωρισμού (Εν. 3.2) και βασίζεται σε αριθμούς κινητής υποδιαστολής. Χαρακτηριστικά παραδείγματα αυτής της προσέγγισης είναι οι εργασίες των Pan [210, 213, 214], Renegar [223], Schönhage [239]. Ο αναγνώστης μπορεί επίσης να ανατρέξει στους Henrici [131], Marden [181], Obreschkoff [207], Ostrowski [209], Ralston and Rabinowitz [221], Stetter [246] για περισσότερα αποτελέσματα σχετικά με μεθόδους και αλγορίθμους αριθμητικής επίλυσης.

Οι αλγόριθμοι πραγματικής επίλυσης ακέραιων πολυωνύμων σε μία μεταβλητή, που θα μας απασχολήσουν, έχουν ως έξοδο διαστήματα με άκρα ρητούς αριθμούς που θα περιέχουν μία και μόνο μία ρίζα του $A(X)$ και εμπεριέχουν πράξεις μόνο με ακεραίους απεριόριστης ακρίβειας. Τα διαστήματα αυτά ονομάζονται *διαστήματα απομόνωσης* και οι αλγόριθμοι ονομάζονται *αλγόριθμοι απομόνωσης*. Ο διαχωρισμός του προβλήματος της προσέγγισης από το πρόβλημα της απομόνωσης των (πραγματικών) ριζών ενός πολυωνύμου, πιθανόν οφείλεται στον Lagrange [167], χωρίς ωστόσο να παραγνωρίσουμε τη συμβολή των Fourier [107], Sturm [248], Vincent [261]. Στη σύγχρονη εκδοχή τους οι αλγόριθμοι απομόνωσης παρουσιάστηκαν από τους Uspensky [255], Collins and Loos [55] και Collins and Akritas [52]. Θα επανέλθουμε στις σχετικές εργασίες για αλγορίθμους απομόνωσης στη συνέχεια του κεφαλαίου. Επιπρόσθετα, οι αλγόριθμοι που θα παρουσιάσουμε υπολογίζουν και τις πολλαπλότητές των πραγματικών ριζών εκτός από τα διαστήματα απομόνωσης τους. Όσον αφορά στην αναπαράσταση των στοιχείων του $\mathbb{R}_{alg}$ θα την παρουσιάσουμε αναλυτικά στο επόμενο κεφάλαιο.

Συνοψίζοντας και υιοθετώντας την ορολογία του Yap [275], το παρόν κεφάλαιο ασχολείται με το *θεμελιώδες υπολογιστικό πρόβλημα της άλγεβρας*.

Τι θα ακολουθήσει

Αρχικά παρουσιάζουμε το μέτρο Mahler για πολυώνυμα και πραγματικούς αλγεβρικούς αριθμούς και διαφόρων ειδών φράγματα στις πραγματικές και μιγαδικές ρίζες ενός πολυωνύμου. Στη συνέχεια παρουσιάζουμε ένα αλγόριθμο για τον υπολογισμό των πολλαπλοτήτων των πραγματικών ριζών ενός πολυωνύμου. Τέλος, παρουσιάζουμε αλγορίθμους για την απομόνωση των πραγματικών ριζών. Πιο συγκεκριμένα παρουσιάζουμε τον αλγόριθμο του Kronecker, τους αλγορίθμους υποδιαίρεσης STURM, DESCARTES και BERNSTEIN και τον αλγόριθμο των συνεχών κλασμάτων CF.

3.1 Μέτρο Mahler

Θα παρουσιάσουμε το μέτρο Mahler [180] πολυωνύμων και αλγεβρικών αριθμών. Για τις αποδείξεις των θεωρημάτων που παραλείπουμε ο αναγνώστης μπορεί να ανατρέξει στους Mignotte [187] και Mignotte and Stefanescu [190].

Ορισμός 3.2 (μέτρο Mahler). *[180] Έστω $A \in \mathbb{C}[X] \setminus \mathbb{C}$, τέτοιο ώστε*

$$A = \sum_{i=0}^{d} a_i X^i = a_d (X - \gamma_1) \cdots (X - \gamma_d)$$

όπου $a_d \neq 0$. Το μέτρο Mahler του A, το οποίο συμβολίζουμε ως $\mathcal{M}(A)$, ορίζεται ως

$$\mathcal{M}(A) = |a_d| \prod_{j=1}^{d} \max\{1, |\gamma_j|\}$$

Για το μέτρο Mahler ισχύουν οι ακόλουθες ιδιότητες:

Λήμμα 3.3. *Έστω $A, B \in \mathbb{C}[X] \setminus \mathbb{C}$, τέτοια ώστε το μέτρο Mahler να ορίζεται, $\deg(A) = d$ και $k \in \mathbb{N}^*$, τότε*

1. $\mathcal{M}\left(X^d A(\frac{1}{X})\right) = \mathcal{M}(A(X))$
2. $\mathcal{M}(A \cdot B) = \mathcal{M}(A) \cdot \mathcal{M}(B)$
3. $\mathcal{M}\left(A(X^k)\right) = \mathcal{M}(A(X))$

Απόδειξη: Θεωρούμε, χωρίς βλάβη της γενικότητας, ότι τα A και B δεν έχουν ούτε το 0 ως ρίζα, ούτε κάποια ρίζα μέτρου 1. Έστω $A = \sum_{i=0}^{d} a_i X^i$ και $B = \sum_{i=0}^{p} b_i X^i$ των οποίων οι (μιγαδικές) ρίζες είναι:

$$\begin{array}{ccccccccccccc} |\alpha_1| & \leq & \ldots & \leq & |\alpha_k| & < & 1 & < & |\alpha_{k+1}| & \leq & \ldots & \leq & |\alpha_d| \\ |\beta_1| & \leq & \ldots & \leq & |\beta_l| & < & 1 & < & |\beta_{l+1}| & \leq & \ldots & \leq & |\beta_p| \end{array}$$

Προκειμένου να αποδείξουμε την πρώτη ανισότητα, υπενθυμίζουμε ότι οι συντελεστές του πολυωνύμου είναι συμμετρικές πολυωνυμικές συναρτήσεις των ριζών [187, 190, 275] και ως εκ τούτου ο σταθερός όρος είναι το γινόμενο των (μιγαδικών) ριζών, αν το πολυώνυμο είναι μονικό.

Συνεπώς για το A ισχύει ότι $\prod_{i=1}^{d} |\alpha_i| = \left|\frac{a_0}{a_d}\right|$. Επίσης, το $X^d A(\frac{1}{X}) = a_0\, X^d + \cdots + a_{d-1}X + a_d$ έχει (μιγαδικές) ρίζες

$$\frac{1}{|\alpha_d|} \leq \cdots \leq \frac{1}{|\alpha_{k+1}|} < 1 < \frac{1}{|\alpha_k|} \leq \cdots \leq \frac{1}{|\alpha_1|}$$

Άρα

$$\begin{aligned} \mathcal{M}(A) &= |a_d| \cdot |\alpha_{k+1}| \cdots |\alpha_d| \\ &= |a_d| \left|\frac{a_0}{a_d}\right| \left|\frac{1}{\alpha_1}\right| \cdots \left|\frac{1}{\alpha_k}\right| \quad = |a_0| \left|\frac{1}{\alpha_1}\right| \cdots \left|\frac{1}{\alpha_k}\right| \\ &= \mathcal{M}\left(X^d A\left(\frac{1}{X}\right)\right) \end{aligned}$$

Όσον αφορά τη δεύτερη ανισότητα, οι μιγαδικές ρίζες του $A \cdot B$ είναι $\{\alpha_i\}_{1\leq i\leq d} \cup \{\beta_j\}_{1\leq j\leq p}$. Επίσης ισχύει ότι $\mathsf{lead}(A \cdot B) = a_d \cdot b_p$. Συνεπώς

$$\mathcal{M}(A \cdot B) = a_d b_p \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \prod_{j=1}^{p} \max\{1, |\beta_j|\} = \mathcal{M}(A) \cdot \mathcal{M}(B)$$

Η τελευταία ανισότητα είναι τετριμμένη. ΟΕΔ

Η δεύτερη ιδιότητα του Λημ. 3.4 αναδεικνύει και την σπουδαιότητα του μέτρου Mahler καθώς, σε αντίθεση με άλλες μετρικές, είναι συμβατό με τον πολλαπλασιασμό πολυωνύμων. Επίσης, το ακόλουθο λήμμα φράσσει το μέτρο Mahler και είναι εξαιρετικής σημασίας:

Λήμμα 3.4 (Landau). *Αν $A \in \mathbb{C}[X]$ δεν είναι μονώνυμο τότε $\mathcal{M}(A) \leq \|A\|_2$. Αν $A \in \mathbb{Z}[X]$ και $\mathcal{L}(A) = \tau$ τότε*

$$\mathcal{M}(A) \leq \|A\|_2 \leq 2^{\tau}\sqrt{d+1} \tag{3.2}$$

Ορισμός 3.5 (Μέτρο Mahler αλγεβρικού αριθμού). *Το μέτρο Mahler ενός αλγεβρικού αριθμού γ, το οποίο θα συμβολίζουμε ως $\mathcal{M}(\gamma)$, είναι το μέτρο $\mathcal{M}(A)$ οποιουδήποτε ελάχιστου πολυωνύμου $A \in \mathbb{Z}[X]$ του γ.*

Το ελάχιστο πολυώνυμο, που ανήκει στο $\mathbb{Z}[X]$, ενός αλγεβρικού αριθμού είναι μοναδικό, με την εξαίρεση του πολλαπλασιασμού με -1. Κατά συνέπεια αν υποθέσουμε ότι θεωρούμε τον μεγιστοβάθμιο όρο ενός πολυωνύμου πάντα θετικό τότε το $\mathcal{M}(\gamma)$ είναι καλώς (μοναδικά) ορισμένο. Επίσης ισχύουν οι παρακάτω ανισότητες, η απόδειξη των οποίων βασίζεται στον ορισμό 3.2.

Πρόταση 3.6. *Έστω α και β δύο αλγεβρικοί αριθμοί τέτοιοι ώστε $\deg(\alpha) = m$ και $\deg(\beta) = n$.*

Τότε ισχύουν οι παρακάτω σχέσεις:

$$\begin{aligned}
\frac{1}{\mathcal{M}(\alpha)} &\leq |\alpha| \leq \mathcal{M}(\alpha) \\
\mathcal{M}(\alpha \cdot \beta) &\leq \mathcal{M}(\alpha)^n \cdot \mathcal{M}(\beta)^m \\
\mathcal{M}(\alpha + \beta) &\leq 2^{m\,n} \mathcal{M}(\alpha)^n \cdot \mathcal{M}(\beta)^m \\
\mathcal{M}\left(\alpha^{\frac{1}{k}}\right) &\leq \mathcal{M}(\alpha) \qquad\qquad \forall\, k \in \mathbb{N}^* \\
\mathcal{M}\left(\alpha^{-1}\right) &= \mathcal{M}(\alpha) \\
\mathcal{M}\left(\alpha^{k}\right) &\leq \mathcal{M}(\alpha)^k \qquad\qquad \forall\, k \in \mathbb{N}^*
\end{aligned}$$

3.2 Φράγματα στις ρίζες

Απόλυτα φράγματα

Αν $A \in \mathbb{C}[X]$ σκοπός μας είναι να υπολογίσουμε ένα δίσκο $D \subset \mathbb{C}$, ως συνάρτηση των συντελεστών, ο οποίος περιέχει όλες τις ρίζες του A. Αν θεωρήσουμε ότι το D έχει κέντρο το μηδέν τότε αρκεί να υπολογίσουμε μια ακτίνα η οποία να έχει μέτρο μεγαλύτερο από το μέτρο της μεγαλύτερης (κατά μέτρο) ρίζας του A. Τέτοιου είδους φράγματα ονομάζονται *απόλυτα φράγματα* ή *φράγματα εγκλεισμού*.

Για τις αποδείξεις των θεωρημάτων που παραλείπουμε ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [131, 187, 190, 192, 233, 233, 238, 245, 257, 275].

Θεώρημα 3.7 (Cauchy 1829)

Έστω $A \in \mathbb{C}[X]$ και έστω $r[A]$ η μοναδική θετική ρίζα του

$$\mathcal{C}_A(X) = |a_d|\, X^d - |a_{d-1}|\, X^{d-1} - \cdots - |a_1|\, X - |a_0| \ \in \mathbb{C}[X]$$

Όλες οι (μιγαδικές) ρίζες του A περιέχονται στο δίσκο $|X| \leq r[A]$. Το $\mathcal{C}_A[X]$ ονομάζεται πολυώνυμο Cauchy του A.

Τα περισσότερα απόλυτα φράγματα προσπαθούν να προσεγγίσουν όσο το δυνατόν καλύτερα το $r[A]$, δηλαδή υπολογίζουν κάποιο ξ τέτοιο ώστε $r[A] \leq \xi$. Οι καλύτερες προσεγγίσεις επιτυγχάνονται με το παρακάτω θεώρημα:

Θεώρημα 3.8 (M. Fujiwara, 1926)

Έστω $A \in \mathbb{C}[X]$ και $\lambda_0, \ldots, \lambda_{d-1} \in (0, \infty)$ τέτοια ώστε $\frac{1}{\lambda_0} + \cdots + \frac{1}{\lambda_{d-1}} \leq 1$, τότε όλες οι (μιγαδικές) ρίζες του A περιέχονται στο δίσκο $|X| \leq F_\lambda(A)$, όπου

$$F_\lambda(A) = \max_{0 \leq k \leq d-1} \left\{ \left(\lambda_k \left| \frac{a_k}{a_d} \right| \right)^{\frac{1}{d-k}} \right\}$$

Το επόμενο φράγμα, το οποίο οφείλεται στο Kuniyeda, δίνει συνήθως χειρότερα αποτελέσματα από το αυτό του Fujiwara, αλλά το παρουσιάζουμε για λόγους πληρότητας.

Θεώρημα 3.9 (M. Kuniyeda, 1916)
Έστω $A \in \mathbb{C}[X]$ και $p, q > 0$ τέτοια ώστε $\frac{1}{p} + \frac{1}{q} = 1$ τότε όλες οι (μιγαδικές ρίζες του A περιέχονται στο δίσκο $|X| \leq \xi$, όπου

$$\xi = \left(1 + \left(\sum_{j=0}^{d-1} \left| \frac{a_j}{a_d} \right|^p \right)^{\frac{q}{p}} \right)^{\frac{1}{q}}$$

Τα παρακάτω φράγματα προκύπτουν από το Θεωρ. 3.8 με κατάλληλη επιλογή των λ_i.

Πόρισμα 3.10. *Αν γ είναι η μεγαλύτερη κατά μέτρο ρίζα του $A \in \mathbb{C}[X]$ τότε*

$$\textit{(Cauchy)} \qquad |\gamma| \leq 1 + \frac{\max\{|a_0|, \ldots, |a_{d-1}|\}}{|a_d|}$$

$$|\gamma| \leq \frac{1}{\sqrt[d]{2} - 1} \max\left\{ \frac{|a_{d-1}|}{\binom{d}{1}|a_d|}, \sqrt{\frac{|a_{d-2}|}{\binom{d}{2}|a_d|}}, \sqrt[3]{\frac{|a_{d-3}|}{\binom{d}{3}|a_d|}}, \ldots, \sqrt[d]{\frac{|a_0|}{\binom{d}{d}|a_d|}} \right\}$$

$$\textit{(Cauchy)} \qquad |\gamma| \leq \max\left\{ \frac{d|a_{d-1}|}{|a_d|}, \sqrt{\frac{d|a_{d-2}|}{|a_d|}}, \sqrt[3]{\frac{d|a_{d-3}|}{|a_d|}}, \ldots, \sqrt[d]{\frac{d|a_0|}{|a_d|}} \right\}$$

Αν $A \in \mathbb{Z}[X]$ και χρησιμοποιώντας την ανισότητα (2.4) τότε το πρώτο φράγμα του Πορ. 3.10 γίνεται

$$|\gamma| \leq 1 + \frac{\|A\|_\infty}{|a_d|} \leq 1 + \frac{\|A\|_2}{|a_d|}$$

όπου η δεύτερη ανισότητα ονομάζεται φράγμα Landau [275], δείτε επίσης το Λημ. 3.4. Τα φράγματα του Πορ. 3.10 είναι βέλτιστα, δηλαδή υπάρχουν πολυώνυμα των οποίων η μεγαλύτερη ρίζα είναι κάποιο από τα φράγματα, συνεπώς είναι μεταξύ τους (θεωρητικά) ισοδύναμα. Επιπρόσθετα, η μέγιστη τιμή τους είναι 2^τ και η ελάχιστη $2^{-\tau}$, αν $A \in \mathbb{Z}[X]$.

Σημείωση 3.11. *Θεωρούμε ένα αλγόριθμο* absoluteRootBound *ο οποίος υλοποιεί κάποιο από τα παραπάνω απόλυτα φράγματα. Η πολυπλοκότητα του υπολογισμού όλων των φραγμάτων αν $A \in \mathbb{Z}[X]$, $\deg(A) = d$ και $\mathcal{L}(A) = \tau$ είναι $\widetilde{\mathcal{O}}_B(d\tau)$.*

Προκειμένου να υπολογίσουμε ένα κάτω απόλυτο φράγμα στις ρίζες του A θεωρούμε το πολυώνυμο $\mathcal{R}(A)(X)$, του οποίου οι ρίζες είναι $\frac{1}{\gamma}$. Υπολογίζουμε κάποιο απόλυτο φράγμα στις ρίζες του $\mathcal{R}(A)(X)$, οπότε έχουμε ότι $\frac{1}{|\gamma|} \leq$ absoluteRootBound$(\mathcal{R}(A))$ ή $|\gamma| \geq 1/$absoluteRootBound$(\mathcal{R}(A))$.

Δηλαδή θεωρούμε τον αλγόριθμο lowerAbsoluteRootBound*, για τον οποίο ισχύει ότι*

$$\text{lowerAbsoluteRootBound}(A) = 1/\text{absoluteRootBound}(\mathcal{R}(A))$$

και ο οποίος έχει την ίδια πολυπλοκότητα με τον absoluteRootBound.

Θετικά φράγματα

Τα απόλυτα φράγματα υπολογίζουν έναν δίσκο στο μιγαδικό επίπεδο που περιέχει όλες τις ρίζες. Ωστόσο, σε πολλές περιπτώσεις, όπως για παράδειγμα στην απομόνωση των πραγματικών ριζών με τον αλγόριθμο των συνεχών κλασμάτων, χρειαζόμαστε φράγματα που αφορούν μόνο τις θετικές πραγματικές ρίζες. Τέτοιου είδους φράγματα θα τα ονομάσουμε *θετικά φράγματα*. Αν και μπορούμε να χρησιμοποιήσουμε τα απόλυτα φράγματα, η ελπίδα είναι ότι μπορούμε να υπολογίσουμε πιο σφιχτά φράγματα γιατί ενδιαφερόμαστε για μια ειδική περίπτωση. Δεν υπάρχει μεγάλη βιβλιογραφία για τα θετικά φράγματα. Οι πιο σημαντικές εργασίες οφείλονται στους Kioustelidis [157] και Stefanescu [244].

Θεώρημα 3.12

[157] Έστω $A \in \mathbb{R}[X]$ και U_A το σύνολο των δεικτών των αρνητικών συντελεστών του A, δηλαδή $U_A := \{k \mid k \leq d \wedge a_k < 0\}$. Έστω το πολυώνυμο

$$\mathcal{C}_A^+(X) := a_d\, X^d + \sum_{k \in U_A} a_k\, X^k$$

Το $\mathcal{C}_A^+$ έχει μία μοναδική θετική ρίζα, που συμβολίζουμε με $r^+[A]$ και οποία και αποτελεί ένα άνω φράγμα στις θετικές πραγματικές ρίζες του A (αν υπάρχουν).

Απόδειξη: Αν το $\mathcal{C}_A^+$ έχει το μηδέν ως σταθερό όρο τότε το διαιρούμε με την κατάλληλη δύναμη του X έτσι ώστε ο σταθερός όρος να είναι διάφορος του μηδενός. Υποθέτουμε ότι ο σταθερός όρος δεν είναι μηδέν. Παρατηρούμε ότι $\mathtt{VAR}(\mathcal{C}_A^+) = 1$, άρα το $\mathcal{C}_A^+$ έχει μία μοναδική θετική ρίζα, σύμφωνα με τον κανόνα προσήμων του Descartes (Θεωρ. 3.28).

Αν το A δεν έχει θετικές πραγματικές ρίζες τότε το θεώρημα ισχύει. Έστω $\gamma > 0$ η μεγαλύτερη θετική ρίζα του A. Τότε ισχύει ότι

$$\begin{aligned} a_d\,\gamma^d = -\sum_{i=0}^{d-1} a_i\,\gamma^i \leq -\sum_{k \in U_A} a_k\,\gamma^k \;\Leftrightarrow \\ a_d\,\gamma^d + \sum_{k \in U_A} a_k\,\gamma^k \leq 0 \\ \mathcal{C}_A^+(\gamma) \leq 0 \end{aligned}$$

Παρατηρούμε ότι $\mathcal{C}_A^+(0) < 0$ και $\mathcal{C}_A^+(+\infty) > 0$, οπότε το γ είναι μικρότερο ή ίσο από $r^+[A]$. ΟΕΔ

Αν και το $\mathcal{C}_A^+$ εξαρτάται από κάποιο υποσύνολο του συνόλου των συντελεστών του A, το επαγόμενο φράγμα είναι χειρότερο από αυτό που προκύπτει από τη θετική ρίζα του πολυωνύμου Cauchy (Θεωρ. 3.7), όπως δείχνει το επόμενο λήμμα. Η χρησιμότητά του θα φανεί στη συνέχεια όταν παρουσιάσουμε το Λημ. 3.17.

Λήμμα 3.13. *Ισχύει $r[A] \leq r^+[A]$.*

Απόδειξη: Παρατηρούμε ότι $\mathcal{C}_A(0) < 0$ και $\mathcal{C}_A(+\infty) > 0$ και ότι

$$\begin{aligned}\mathcal{C}_A(r^+[A]) &= a_d(r^+[A])^d + \sum_{k\in U_A} a_k\,(r^+[A])^k + \sum_{k\notin U_A} a_k\,(r^+[A])^k \\ &= 0 + \sum_{k\notin U_A} a_k\,(r^+[A])^k \geq 0\end{aligned}$$

ΟΕΔ

Μπορούμε τώρα να ορίσουμε ένα φράγμα ανάλογο με αυτό το Fujiwara για την περίπτωση των θετικών πραγματικών ριζών. Το επόμενο θεώρημα οφείλεται στον Kioustelidis [157].

Θεώρημα 3.14

Έστω $A = \sum_{i=0}^{d} a_i X^d \in \mathbb{R}[X]$ και έστω ένα σύνολο μη αρνητικών αριθμών $\mu = \{\mu_k\}_{k\in U_A}$, τέτοιο ώστε $\sum_{k\in U_A} \frac{1}{\mu_k} \leq 1$. τότε

(1) η ποσότητα

$$N_\mu(A) := \max_{k\in U_A}\left\{\left(\mu_k\left|\frac{a_k}{a_d}\right|\right)^{\frac{1}{d-k}}\right\}$$

είναι ένα άνω φράγμα στις θετικές πραγματικές ρίζες του A.

(2) Η ελάχιστη τιμή του $N_\mu(A)$, αν θεωρεί ως συνάρτηση των μ_k, είναι η μοναδική θετική ρίζα του $\mathcal{C}_A^+$, δηλαδή $r^+[A] = \min_\mu N_\mu(A)$.

Απόδειξη: Αρκεί να δειχτεί ότι $r^+[A] \leq N_\mu(A)$. Θα το δείξουμε με αναγωγή σε άτοπο. Έστω $r^+[A] > N_\mu(A)$. Τότε $\forall\, k \in U_A$ ισχύει

$$r^+[A] > \left(\mu_k\left|\frac{a_k}{a_d}\right|\right)^{\frac{1}{d-k}} \Rightarrow \frac{1}{\mu_k} a_d\,(r^+[A])^d > |a_k|\,(r^+[A])^k$$

και αθροίζοντας πάνω σε όλα τα $k \in U_A$ έχουμε

$$\begin{aligned} a_d\,(r^+[A])^d \sum_{k\in U_A}\frac{1}{\mu_k} &> \sum_{k\in U_A}|a_k|(r^+[A])^k \\ a_d\,(r^+[A])^d \sum_{k\in U_A}\frac{1}{\mu_k} &> a_d(r^+[A])^d \\ \sum_{k\in U_A}\frac{1}{\mu_k} &> 1 \qquad\qquad \text{ΑΤΟΠΟ!}\end{aligned}$$

Για την απόδειξη του δεύτερης ιδιότητας αρκεί να θεωρήσουμε

$$\mu_k = \frac{a_d}{a_k}\,\left(r^+[A]\right)^{d-k}$$

όπου $k \in U_A$.

ΟΕΔ

Αν και αποδείξαμε (Λημ. 3.13) ότι $r[A] \leq r^+[A]$ τα φράγματα που λαμβάνουμε για το θετικό πολυώνυμο Cauchy είναι καλύτερα από αυτά που λαμβάνουμε από το θεώρημα του Fujiwara. Δηλαδή ισχύει $N_\mu(A) \leq F_\lambda(A)$.

Λήμμα 3.15. *Αν $F_\lambda(A)$ κάποιο άνω φράγμα στις θετικές ρίζες του A, τότε μπορούμε πάντοτε να επιλέξουμε μια ακολουθία $\mu \subset \lambda$, τέτοια ώστε $N_\mu(A) \leq F_\lambda(A)$.*

Απόδειξη: Έστω ένα φράγμα $F_\lambda(A)$. Από το Θεωρ. 3.8 έχουμε ότι $\sum_{j=0}^{d-1} \frac{1}{\lambda_j} \leq 1$ και $\lambda_j > 0$. Συνεπώς οποιοδήποτε υποσύνολο των αντιστρόφων έχει άθροισμα ≤ 1. Επιλέγουμε ακολουθία μ τέτοια ώστε $\mu_k = \lambda_j$ και $k \in U_A$. Τότε ισχύει

$$\left\{ \left(\mu_k \left| \frac{a_k}{a_d} \right| \right)^{\frac{1}{d-k}} \right\}_{k \in U_A} \subseteq \left\{ \left(\lambda_j \left| \frac{a_j}{a_d} \right| \right)^{\frac{1}{d-j}} \right\}_{0 \leq j \leq d-1}$$

οπότε συνάγουμε ότι $N_\mu(A) \leq F_\lambda(A)$. ΟΕΔ

Λήμμα 3.16. *Έστω $A = \sum_{i=0}^{d} a_i X^d \in \mathbb{R}[X]$. Το συναρτησοειδές*

$$N_2(A) := 2 \max_{k \in U_A} \left\{ \left| \frac{a_k}{a_d} \right|^{\frac{1}{d-k}} \right\} \tag{3.3}$$

αποτελεί ένα άνω φράγμα στις θετικές ρίζες του A και ισχύει $r^+[A] \leq N_2(A) \leq 2\, r^+[A]$.

Απόδειξη: Σύμφωνα με το Θεωρ. 3.14, επιλέγοντας $\mu_k = 2^{d-k}$, έχουμε $r^+[A] \leq N_2(A)$. Εφόσον $r^+(A)$ είναι ρίζα του $\mathcal{C}_A^+$ ισχύει

$$\mathcal{C}_A^+ \left(r^+[A] \right) = a_d \left(r^+[A] \right)^d + \sum_{k \in U_A} a_k \left(r^+[A] \right)^k = 0 \quad \Leftrightarrow$$

$$1 = \sum_{k \in U_A} \left| \frac{a_k}{a_d} \right| \left(r^+[A] \right)^{k-d}$$

Παρατηρούμε ότι στην τελεταία ισότητα, όλες οι ποσότητες του αθροίσματος είναι θετικές, συνεπώς κάθε μια από αυτές πρέπει να είναι ≤ 1. Δηλαδή ισχύει

$$\left| \frac{a_k}{a_d} \right| \left(r^+[A] \right)^{k-d} \leq 1 \quad \Leftrightarrow \quad \left| \frac{a_k}{a_d} \right| \leq \left(r^+[A] \right)^{d-k}$$

Συνδυάζοντας την τελευταία ανισότητα με την (3.3) συμπεραίνουμε ότι $N_2(A) \leq 2\, r^+[A]$. ΟΕΔ

Το παρακάτω λήμμα μας δίνει μια ένδειξη για την ποιότητα του φράγματος $N_2(A)$, στη χειρότερη περίπτωση.

Λήμμα 3.17. *Αν $A \in \mathbb{C}[X]$ και γ μια θετική του ρίζα τότε $\gamma \leq N_2(A) \leq 2\, d \cdot \gamma$.*

Απόδειξη: Η αριστερή ανισότητα είναι προφανής. Από την εργασία του van der Sluis [257] ξέρουμε ότι $F_2(A) \leq 2\,d \cdot \gamma$ και από το προηγούμενο λήμμα ότι $N_2(A) \leq F_2(A)$. ΟΕΔ

Στηριζόμενοι στο Θεωρ. 3.14 μπορούμε να συνάγουμε καινούργια φράγματα για τις θετικές ρίζες ενός (πραγματικού) πολυωνύμου, παρόμοια με αυτά του Πορ. 3.10.

Πόρισμα 3.18. *Αν γ είναι η μεγαλύτερη πραγματική θετική ρίζα του $A \in \mathbb{R}[X]$ και $\ell \geq 1$, τότε*

1. $|\gamma| \leq \max_{k \in U_A} \left\{ \sqrt[d-k]{\ell \left| \frac{a_k}{a_d} \right|} \right\}$
2. *Αν ρ η (μοναδική) θετική ρίζα του $X^d - \sum_{k \in U_A} X^k$ τότε* $|\gamma| \leq \max_{k \in U_A} \left\{ \rho \sqrt[d-k]{\left| \frac{a_k}{a_d} \right|} \right\}$
3. $|\gamma| \leq \frac{1}{\sqrt[d]{2}-1} \max_{k \in U_A} \left\{ \sqrt[d-k]{\frac{|a_k|}{\binom{d}{k}|a_d|}} \right\}$

Απόδειξη: Η απόδειξη στηρίζεται στο Θεωρ. 3.14 με κατάλληλη επιλογή των μ_k.

1. Επιλέγουμε $\mu_k = \ell$ για $k \in U_A$. Αν $\ell = |U_A|$, τότε το φράγμα είναι γνωστό ως κανόνας του Cauchy. Θα μπορούσαμε επίσης να επιλέξουμε $\ell = d = \deg(A)$.
2. Παρατηρούμε ότι $\rho > 1$ και επιλέγουμε $\mu_k = \rho^k$ για $k \in U_A$.
3. Επιλέγουμε $\mu_k^{-1} = \binom{d}{k}(2^{1/d} - 1)^k$ για $k \in U_A$.

ΟΕΔ

Το ακόλουθο φράγμα δεν προκύπτει από το Θεωρ. 3.14. Οφείλεται στον Stefanescu [244] και αν μπορεί να εφαρμοστεί δίνει σχεδόν πάντα καλύτερα φράγματα. Το θεώρημα που παρουσιάζουμε έχει πιο ασθενείς υποθέσεις από αυτό που παρουσίασε ο Stefanescu. Η απόδειξη είναι ακριβώς η ίδια και γι' αυτό την παραλείπουμε.

Θεώρημα 3.19

[244] Έστω $A \in \mathbb{R}[X]$ τέτοιο ώστε να μπορεί να γραφτεί ως

$$A(X) = c_1 X^{d_1} - b_1 X^{m_1} + c_2 X^{d_2} - b_2 X^{m_2} + \cdots + c_k X^{d_k} - b_k X^{m_k} + g(X)$$

όπου $g(X) \in \mathbb{R}_+[X]$, $c_i > 0$, $b_i > 0$, $d_i > m_i$ για $1 \leq i \leq k$. Τότε ο αριθμός

$$\max\left\{ \left(\frac{b_1}{c_1}\right)^{1/(d_1-m_1)}, \ldots, \left(\frac{b_k}{c_k}\right)^{1/(d_k-m_k)} \right\}$$

είναι ένα άνω φράγμα στις θετικές ρίζες του A.

Σημείωση 3.20. *Θεωρούμε έναν αλγόριθμο* positiveRootBound *ο οποίος υλοποιεί κάποιο από τα παραπάνω φράγματα. Η πολυπλοκότητα του υπολογισμού όλων των φραγμάτων αν $A \in \mathbb{Z}[X]$, $\deg(A) = d$ και $\mathcal{L}(A) = \tau$ είναι $\widetilde{\mathcal{O}}_B(d\tau)$.*

Αντίστοιχα με την περίπτωση των απολύτων φραγμάτων (Σημ. 3.11) θεωρούμε τον αλγόριθμο positiveLowerBound *ο οποίος υπολογίζει ένα κάτω φράγμα στις θετικές ρίζες του A και ο οποίος έχει την ίδια πολυπλοκότητα με του* positiveRootBound.

Σύνθετα φράγματα και φράγματα διαχωρισμού

Ορισμός 3.21. *Έστω $A \in \mathbb{C}[X]$ και $\gamma_1, \ldots, \gamma_d$ οι (μιγαδικές) ρίζες του, ορίζουμε ως φράγμα διαχωρισμού (separation bound) των ριζών του A την ποσότητα*

$$\Delta(A) := \min_{i \neq j} |\gamma_i - \gamma_j|$$

Πρόταση 3.22. *Έστω $A = \sum_{i=0}^{d} a_i X^i \in \mathbb{C}[X]$ χωρίς τετράγωνα, τότε*

$$\Delta(A) > \sqrt{\frac{3|\mathsf{disc}(A)|}{d^{d+2}}} \|A\|_2^{1-d} \geq \sqrt{\frac{3|\mathsf{disc}(A)|}{d^{d+2}}} \mathcal{M}(A)^{1-d}$$

Αν ενδιαφερόμαστε για το φράγμα διαχωρισμού μεταξύ πραγματικών ριζών τότε υπάρχει το φράγμα του Rump [276], το οποίο είναι λίγο καλύτερο από τα προηγούμενα φράγματα

Πρόταση 3.23. *Έστω $A \in \mathbb{C}[X]$ χωρίς τετράγωνα τότε*

$$\Delta_{real}(A) > \sqrt{\frac{8}{d^{d+2}}} \frac{1}{1 + \|A\|_\infty^d}$$

Σημείωση 3.24. *Τα φράγματα διαχωρισμού είναι βέλτιστα, με την εξαίρεση κάποιων σταθερών. Τα πολυώνυμα Mignotte [187, 189, 190]*

$$f = X^d - 2(aX - 1)^2$$

όπου $d \geq 3$, $a \in \mathbb{Q}$ και $a \geq 3$, τα οποία είναι ανάγωγα στο $\mathbb{Q}[X]$, έχουν δύο πραγματικές ρίζες πολύ κοντά στο $1/a$ και ισχύει ότι $\Delta(f) < 2\,a^{-(d+2)/2}$. Συνεπώς το δυαδικό μήκος ενός (ρητού) αριθμού που βρίσκεται ανάμεσα σε δύο πραγματικές ρίζες ενός πολυωνύμου είναι στη γενική περίπτωση $\mathcal{O}(d\tau)$.

Ωστόσο, στη γενική περίπτωση τα φράγματα διαχωρισμού είναι πολύ άσχημα. Για παράδειγμα το θεωρητικό φράγμα διαχωρισμού για το πολυώνυμο Wilkinson $\sum_{i=0}^{20}(X - i)$ είναι περίπου 10^{-344} ενώ στην πραγματικότητα είναι 1!

Σημείωση 3.25. *Αν και η εκτίμηση του φράγματος διαχωρισμού με τη χρήση της νόρμας $\|\cdot\|_2$ είναι πιο ακριβής καθώς εξαρτάται από το πολυώνυμο το οποίο εξετάζουμε, όταν μελετούμε την ασυμπτωτική πολυπλοκότητα το δυαδικό μηκός όλων των φραγμάτων είναι το ίδιο, δηλαδή $\Delta(A) = 2^{-\mathcal{O}(d\tau)}$.*

Θα αποδείξουμε ένα θεώρημα το οποίο αφορά το γινόμενο διαφορών (μιγαδικών) ριζών ενός πολυωνύμου. Ένα παρόμοιο θεώρημα πρωτοπαρουσιάστηκε από τον Davenport [65] αλλά αφορούσε μόνο τις πραγματικές ρίζες και απαιτούσε πιο ισχυρές προϋποθέσεις. Μια άλλη παραλλαγή του θεωρήματος παρουσιάστηκε από τον Johnson [139], δείτε επίσης [163], η οποία αφορούσε και τις μιγαδικές ρίζες και χαλάρωνε τις υποθέσεις αρκετά. Στην πιο γενική του μορφή το θεώρημα παρουσιάστηκε από τον Mignotte [191] και επίσης από τους Du et al. [76].

Θεώρημα 3.26 (Davenport-Mahler bound)

Έστω $\{\alpha_1, \ldots, \alpha_k\}$ και $\{\beta_1, \ldots, \beta_k\}$ υποσύνολα διαφορετικών (μιγαδικών) ριζών του f (όχι απαραίτητα χωρίς τετράγωνα) τέτοια ώστε $\beta_i \notin \{\alpha_1, \ldots, \alpha_i\}$ και $|\beta_i| \leq |\alpha_i|$, για όλα τα $i \in \{1, \ldots, k\}$. Τότε

$$\prod_{i=1}^{k} |\alpha_i - \beta_i| \geq \mathcal{M}(f)^{-d+1} d^{-\frac{d}{2}} \left(\frac{\sqrt{3}}{d}\right)^k$$

Το φράγμα ισχύει και όταν $\alpha_1 > \beta_1 = \alpha_2 > \beta_2 = \ldots \alpha_k > \beta_k := \alpha_{k+1}$, είναι διαφορετικές πραγματικές ρίζες του f.

Η παραλλαγή, που αποδεικνύουμε στη συνέχεια, βασίζεται σε ένα θεώρημα του Mignotte [187], δείτε επίσης [190], αλλά η απόδειξη είναι πιο απλή και οι ανισότητες εμπεριέχουν το μέτρο Mahler. Αν και αντικαθιστούμε το παράγοντα d^d με τον παράγοντα 2^{d^2}, όταν $d = \mathcal{O}(\tau)$ τότε τα φράγματα είναι ισοδύναμα. Επιπρόσθετα, χαλαρώνουμε στο ελάχιστο τις υποθέσεις του θεωρήματος και άρα διευρύνουμε τη χρήση του, όπως θα γίνει σαφές και στην ανάλυση των αλγορίθμων απομόνωσης. Τέλος, αποδεικνύουμε και ένα άνω φράγμα [252].

Θεώρημα 3.27 (Davenport-Mahler-Mignotte revisited)

Έστω $A \in \mathbb{Z}[X]$ τέτοιο ώστε $\deg(A) = d$ και $\mathcal{L}(A) = \tau$. Έστω Ω ένα σύνολο από k ζεύγη (i, j) τέτοια ώστε $1 \leq i < j \leq d$. Θεωρούμε τις μη μηδενικές (μιγαδικές) ρίζες του A σε αύξουσα διάταξη κάτα μέτρο, δηλαδή $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_d|$. Τότε

$$2^k \mathcal{M}(A)^k \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{k - \frac{d(d-1)}{2}} \mathcal{M}(A)^{1-d-k} \sqrt{\mathsf{disc}(A)}$$

Απόδειξη: Έστω $\overline{\Omega}$ το πολυσύνολο $\overline{\Omega} = \{j \mid (i, j) \in \Omega\}$ και $|\overline{\Omega}| = k$.

Θα χρησιμοποιήσουμε την ανισότητα

$$|a - b| \leq 2 \max\{|a|, |b|\} \quad a, b \in \mathbb{C} \tag{3.4}$$

και το γεγονός ότι για κάθε ρίζα του A ισχύει $\frac{1}{\mathcal{M}(A)} \leq |\gamma_i| \leq \mathcal{M}(A)$ (Πρότ. 3.6).

Προκειμένου να δείξουμε την αριστερή ανισότητα του θεωρήματος

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \leq 2^k \prod_{j\in\overline{\Omega}} |\gamma_j| \leq 2^k \max_{j\in\overline{\Omega}} |\gamma_j|^k \leq 2^k \mathcal{M}(A)^k.$$

Η διακρίνουσα του A (Ορ. 2.12) είναι $\mathsf{disc}(A) = \mathsf{lead}\,(A)^{2d-2} \prod_{i<j} (\gamma_i - \gamma_j)^2$. Προκειμένου να δείξουμε τη δεξιά ανισότητα του θεωρήματος θεωρούμε την απόλυτη τιμή της διακρίνουσας του A:

$$\begin{aligned} |\mathsf{disc}(A)| &= |\,\mathsf{lead}\,(A)\,|^{2d-2} \prod_{i<j} |\gamma_i - \gamma_j|^2 \\ &= |\,\mathsf{lead}\,(A)\,|^{2d-2} \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j|^2 \prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j|^2 \qquad \Leftrightarrow \\ \sqrt{|\mathsf{disc}(A)|} &= |\,\mathsf{lead}\,(A)\,|^{d-1} \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j| \end{aligned}$$

Θεωρούμε το γινόμενο $\prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j|$ και εφαρμόζουμε $\frac{d(d-1)}{2} - k$ φορές την ανισότητα (3.4). Τότε

$$\begin{aligned} \prod_{(i,j)\notin\Omega} |\gamma_i - \gamma_j| &\leq 2^{\frac{d(d-1)}{2}-k} |\gamma_1|^0 |\gamma_2|^1 \cdots |\gamma_d|^{d-1} \Big(\prod_{j\in\overline{\Omega}} |\gamma_j|\Big)^{-1} \\ &\leq 2^{\frac{d(d-1)}{2}-k} \mathcal{M}(A)^{d-1} |\,\mathsf{lead}\,(A)\,|^{1-d} \mathcal{M}(A)^k \end{aligned}$$

όπου επίσης χρησιμοποιήσαμε την ανισότητα $|\gamma_1|^0 |\gamma_2|^1 \cdots |\gamma_d|^{d-1} \leq |\mathcal{M}(A)/\,\mathsf{lead}\,(A)\,|^{d-1}$, και το γεγονός ότι αφού $\forall i$, $|\gamma_i| \geq \mathcal{M}(A)^{-1}$, από Πρότ. 3.6, τότε $\prod_{j\in\overline{\Omega}} |\gamma_j| \geq |\gamma_1|^k \geq \mathcal{M}(A)^{-k}$. Και η απόδειξη ολοκληρώθηκε. ΟΕΔ

Φράγματα στο πλήθος των πραγματικών ριζών

Τα θεωρήματα τα οποία θα παρουσιάσουμε φράσσουν το πλήθος των πραγματικών ριζών ενός πολυωνύμου A. Συνήθως μας προσφέρουν μια υπερεκτίμηση και δεν είναι ακριβή όπως για παράδειγμα το Πορ. 2.27.

Θεώρημα 3.28 (Descartes' rule of sign)

Ο αριθμός των πραγματικών ριζών, έστω R, ενός πολυωνύμου $A \in \mathbb{R}[X]$ στο $(0,\infty)$ φράσσεται από $\mathtt{VAR}(A)$ και πιο συγκεκριμένα $R \equiv \mathtt{VAR}(A) \mod 2$.

Σημείωση 3.29. *Στη γενική περίπτωση ο κανόνας προσήμων του Descartes παρέχει μια υπερεκτίμηση στο πλήθος των πραγματικών ριζών. Ωστόσο, εάν ξέρουμε ότι το πολυώνυμο είναι υπερβολικό, δηλαδή έχει μόνο πραγματικές ρίζες, ή εάν οι εναλλαγές προσήμων είναι 0 ή 1, τότε μας δίνει το ακριβές πλήθος των πραγματικών ριζών.*

Ο κανόνας προσήμων του Descartes είναι ανεξάρτητος από τη βάση στην οποία αναπαρίστανται τα πολυώνυμα. Κατά συνέπεια ισχύει και όταν τα πολυώνυμα είναι στη βάση Bernstein (Εν. 2.4), δηλαδή ισχύει το ακόλουθο θεώρημα [14]:

Πρόταση 3.30. *Έστω πραγματικό πολυώνυμο A στην αναπαράσταση στη βάση Bernstein στο διάστημα $[a, b]$. Ο αριθμός R των πραγματικών ριζών του A στο $[a, b]$ φράσσεται από $\mathtt{VAR}(A)$. Επιπλέον $R \equiv \mathtt{VAR}(A) \mod 2$.*

Ο κανόνας προσήμων του Descartes μπορεί να προκύψει από το επόμενο θεώρημα το οποίο οφείλεται στον Budan. Για την απόδειξη ο αναγνώστης μπορεί να ανατρέξει στη βιβλιογραφία, π.χ [5, 187].

Θεώρημα 3.31 (Budan)

Έστω $A \in \mathbb{R}[X]$, τέτοιο ώστε $\deg(A) = d$ και έστω $a < b$, με $a, b \in \mathbb{R}$. Έστω A_a, αντίστοιχα A_b, το πολυώνυμο που παράγεται αφού εφαρμόσουμε στο A του μετασχηματισμό $X \mapsto X + a$, αντίστοιχα $X \mapsto X + b$. Τότε ισχύουν τα ακόλουθα:

1. $\mathtt{VAR}(A_a) \geq \mathtt{VAR}(A_b)$.
2. $\#\{\gamma \in (a, b) | A(\gamma) = 0\} \leq \mathtt{VAR}(A_a) - \mathtt{VAR}(A_b)$.
3. $\#\{\gamma \in (a, b) | A(\gamma) = 0\} \equiv \mathtt{VAR}(A_a) - \mathtt{VAR}(A_b) \mod 2$.

Τα ακόλουθα θεωρήματα είναι το αντίστροφο του κανόνα των προσήμων του Descartes και είναι εξαιρετικά χρήσιμα για την απόδειξη τερματισμού των αλγορίθμων απομόνωσης των πραγματικών ριζών ενός πολυωνύμου, που θα παρουσιάσουμε στη συνέχεια. Πιο συγκεκριμένα εξασφαλίζουν προϋποθέσεις, κάτω από τις οποίες, το πλήθος των εναλλαγών προσήμων να μας δίνει ακριβώς το πλήθος των πραγματικών ριζών. Για τις αποδείξεις των παραπάνω θεωρημάτων ο αναγνώστης μπορεί να ανατρέξει στην βιβλιογραφία [14, 53, 162, 163].

Θεώρημα 3.32 (Το θεώρημα του ενός κύκλου)

Έστω $f \in \mathbb{R}[X]$, $\mathcal{I} = [a, b] \in \mathbb{R}^2$. Εάν ο δίσκος $D = (\frac{a+b}{2}, \frac{|\mathcal{I}|}{2})$ δεν περιέχει καμία ρίζα του f τότε $\mathtt{VAR}(f) = 0$.

Θεώρημα 3.33 (Το θεώρημα των δύο κύκλων)

Έστω $f \in \mathbb{R}[X]$, $\mathcal{I} = [a, b] \in \mathbb{R}^2$. Εάν η ένωση των δίσκων $D_1 = \left(i\frac{\sqrt{3}}{6}|\mathcal{I}|, \frac{|\mathcal{I}|}{2}\right)$ και $D_2 = \left(-i\frac{\sqrt{3}}{6}|\mathcal{I}|, \frac{|\mathcal{I}|}{2}\right)$ περιέχει μία και μόνο ρίζα του f (η οποία είναι κατά συνέπεια πραγματικός αριθμός) τότε $\mathtt{VAR}(f) = 1$.

3.3 Εύρεση πραγματικών ριζών πολυωνύμου

Οι βιβλιογραφικές αναφορές που παρουσιάζουμε για το πρόβλημα είναι μόνο η κορυφή του παγόβουνου και γι' αυτό ενθαρρύνουμε τον αναγνώστη να ανατρέξει στη βιβλιογραφία για περισσότερες πληροφορίες.

Καταρχάς πρέπει να υπενθυμίσουμε ότι ενδιαφερόμαστε μόνο για τις πραγματικές ρίζες ενός ακέραιου πολυωνύμου και ότι με τον όρο επίλυση εννοούμε τον υπολογισμό διαστημάτων απομόνωσης των πραγματικών ριζών. Επίσης, μας ενδιαφέρουν *μόνο* ακριβείς αλγόριθμοι, δηλαδή αλγόριθμοι που χρησιμοποιούν (μόνο) αριθμητική ακεραίων απεριόριστης ακρίβειας. Αν d είναι ο βαθμός του πολυωνύμου και τ το δυαδικό του μήκος, σε ό,τι θα ακολουθήσει θα θεωρήσουμε $N = \max\{d, \tau\}$.

Οι πιο γνωστοί και πιο συχνά χρησιμοποιούμενοι στην πράξη αλγόριθμοι για την απομόνωση των πραγματικών ριζών είναι οι αλγόριθμοι υποδιαίρεσης. Αυτοί οι οι αλγόριθμοι μιμούνται τη φιλοσοφία του αλγόριθμου της δυαδικής αναζήτησης. Πιο συγκεκριμένα ελέγχουν σε ένα αρχικό διάστημα το πλήθος των ριζών που περιέχει, στη συνέχεια το διαιρούν σε δύο ίσα υποδιαστήματα και ο αλγόριθμος επαναλαμβάνεται μέχρι να υπάρξει κάποια πιστοποίηση ότι το διάστημα το οποίο ελέγχουν περιέχει μία ή καμία ρίζα.

Οι πιο γνωστοί αλγόριθμοι και τους οποίους θα εξετάσουμε κάτω από ένα ενιαίο πρίσμα είναι οι αλγόριθμοι DESCARTES, BERNSTEIN και STURM.

Ο αλγόριθμος DESCARTES, ο οποίος βασίζεται στον κανόνα προσήμων του Descartes, παρουσιάστηκε στην σύγχρονη εκδοχή του από τους Collins and Akritas [52] και των οποίων η ανάλυση πέτυχε πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^6\tau^2)$. Στην συνέχεια ο Johnson [139] βελτίωσε την πολυπλοκότητα σε $\widetilde{\mathcal{O}}_B(d^5\tau^2)$ χωρίς να χρησιμοποιήσει γρήγορους αλγορίθμους για την μετατόπιση πολυωνύμου. Ωστόσο, η απόδειξη του Johnson [139] περιείχε κάποια κενά τα οποία διόρθωσε ο Krandick [162] ο οποίος επιπλέον παρουσίασε έναν διαφορετικό τρόπο διάσχισης του δένδρου αναζήτησης του αλγορίθμου. Οι Rouillier and Zimmermann [230] παρουσίασαν ένα ενοποιημένο πλαίσιο για όλες τις παραλλαγές του αλγορίθμου Descartes με βέλτιστη διαχείριση μνήμης και επιπλέον παρουσίασαν μια πολύ γρήγορη υλοποίηση. Η ορθότητα και ο τερματισμός του αλγορίθμου στηρίζονται στο θεώρημα του Vincent (Θεωρ. 3.43) ή/και στα θεωρήματα του ενός και των δύο κύκλων τα οποία παρουσιάστηκαν από τους Collins and Johnson [53] και στη συνέχεια έγιναν πιο σφιχτά από τους Krandick and Mehlhorn [163] χωρίς ωστόσο να επηρεάσουν την ασυμπτωτική πολυπλοκότητα.

Ο αλγόριθμος BERNSTEIN βασίζεται επίσης στον κανόνα προσήμων του Descartes αλλά και στις ιδιότητες της αναπαράστασης των πολυωνύμων στη βάση Bernstein. Ο αλγόριθμος παρουσιάστηκε από τους Lane and Riesenfeld [169] αλλά η ανάλυσή του πρωτοπαρουσιάστηκε από τους Mourrain et al. [203]. Ο αναγνώστης μπορεί να ανατρέξει και στους Mourrain et al. [205] για μια παραλλαγή με βέλτιστη διαχείριση μνήμης και για τη σύνδεση με τον αλγόριθμο DESCARTES. Στο ίδιο πλαίσιο οι Eigenwillig et al. [80] παρουσίασαν έναν πιθανοτικό αλγόριθμο για πολυώνυμα χωρίς τετράγωνα με συντελεστές που δεν είναι γνωστοί ακριβώς (bit stream coefficients). Η πολυπλοκότητα όλων των προσεγγίσεων είναι $\widetilde{\mathcal{O}}_B(d^6\tau^2)$.

Σχετικά πρόσφατα η πολυπλοκότητα τόσο για τον αλγόριθμο DESCARTES όσο και για τον BERNSTEIN βελτιώθηκε σε $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ από τους Eigenwillig et al. [81], δείτε επίσης [97] για μια πιο απλή προσέγγιση όπου επιπρόσθετα το πολυώνυμο δεν είναι απαραίτητα χωρίς τετράγωνα.

Ο αλγόριθμος STURM εισήχθη από τον Sturm [248] αλλά η ανάλυσή του και η γενίκευσή του έτσι ώστε να εμπεριέχει μόνο πράξεις με ακέραιους αριθμούς πρωτοπαρουσιάστηκε από τον Heindel [129], δείτε επίσης [55], και η πολυπλοκότητα του αλγορίθμου ήταν $\widetilde{\mathcal{O}}_B(d^7\tau^3)$. Ο Davenport [65] παρουσιάζει μια πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$, αλλά αν και αποδεικνύει ότι το πλήθος των βημάτων του αλγορίθμου είναι $\mathcal{O}(d\tau)$ δεν παρουσίασε το κόστος του κάθε βήματος, προφα-

νώς γιατί οι γρήγοροι αλγόριθμοι αποτίμησης προσημασμένων ακολουθιών υπο-επιλυουσών δεν ήταν γνωστοί εκείνη την εποχή. Γι' αυτό άλλωστε στο βιβλίο των Davenport, Siret, and Tournier [66] που ακολούθησε αναφέρεται ότι η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^6\tau^3)$. Οι Du et al. [76] δίνοντας ένα επιχείρημα απόσβεσης (amortized argument) πέτυχαν μια πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ για πολυώνυμα χωρίς τετράγωνα. Τέλος οι Emiris and Tsigaridas [91], δείτε επίσης [97], απλοποίησαν και συμπλήρωσαν τα κενά στην προσέγγιση του Davenport [65].

Ένας διαφορετικός ακριβής αλγόριθμος για την απομόνωση των πραγματικών ριζών ενός πολυωνύμου είναι ο αλγόριθμος των συνεχών κλασμάτων (continued fractions), τον οποίο θα συμβολίζουμε με CF. Διαφέρει από τους αλγορίθμους υποδιαίρεσης στο ότι αντί να υποδιαιρεί ένα αρχικό διάστημα που περιέχει όλες τις πραγματικές ρίζες του πολυωνύμου, υπολογίζει την ανάπτυξη σε συνεχές κλάσμα των ριζών.

Η πρώτη διατύπωση του αλγορίθμου οφείλεται στον Vincent [261]. ο αναγνώστης μπορεί επίσης να ανατρέξει στον Akritas [1, 5] για ιστορικές αναφορές. Ο αλγόριθμος του Vincent βασιζόταν σε ένα θεώρημα που διατύπωσε ο ίδιος (είναι το Θεωρ. 3.43 χωρίς τις συνθήκες τερματισμού) το οποίο εξασφαλίζει ότι επαναλαμβανόμενοι μετασχηματισμοί ενός πολυωνύμου τελικά δίνουν ένα πολυώνυμο με μία ή καμία εναλλαγή προσήμων στη λίστα των συντελεστών του. Κατά συνέπεια, από τον κανόνα προσήμων του Descartes προκύπτει ότι το μετασχηματισμένο πολυώνυμο έχει μία, αντίστοιχα καμία, πραγματική ρίζα στο $(0, \infty)$. Εάν καταλήξουμε με μία εναλλαγή προσήμων τότε οι αντίστροφοι μετασχηματισμοί μπορούν να εφαρμοστούν προκειμένου να υπολογίσουμε το διάστημα το οποίο απομονώνει την πραγματική ρίζα του αρχικού πολυωνύμου. Επιπρόσθετα, τα $c_i \in \mathbb{Z}$ που χρησιμοποιούνται ως μετατοπίσεις στους διάφορους μετασχηματισμούς αντιστοιχούν στα μερικά πηλίκα της ανάπτυξης σε συνεχή κλάσματα της πραγματικής ρίζας που απομονώσαμε.

Ωστόσο, ο αλγόριθμος του Vincent έχει εκθετική πολυπλοκότητα [52]. Αυτό συμβαίνει γιατί ο υπολογισμός των c_i στους μετασχηματισμούς του Θεωρ. 3.43 πραγματοποιείται με επαναλαμβανόμενες μετατοπίσεις της μορφής $X \mapsto X + 1$. Συνεπώς αν ένα από τα c_i (ή το το άθροισμά τους) είναι μέτρου, έστω, 2^τ τότε απαιτείται εκθετικό πλήθος βημάτων για τον υπολογισμό τους. Ο Uspensky [255] επέκτεινε το θεώρημα του Vincent υπολογίζοντας ένα άνω φράγμα στο πλήθος των μετασχηματισμών που απαιτούνται προκειμένου να απομονωθούν οι πραγματικές ρίζες, αλλά δεν κατάφερε να αντιμετωπίσει τον εκθετικό χαρακτήρα του αλγορίθμου. Ο αναγνώστης μπορεί επίσης να ανατρέξει στους Cantor et al. [47], Rosen and Shallit [228] όπου επιπρόσθετα εξετάζεται το πρόβλημα της προσέγγισης των πραγματικών αλγεβρικών αριθμών. Χρησιμοποιώντας το θεώρημα του Vincent οι Collins and Akritas [52] πρότειναν τον αλγόριθμο DESCARTES.

Ο Akritas [2, 5] αντιμετώπισε την εκθετική συμπεριφορά του αλγορίθμου, υπολογίζοντας τα c_i που εμφανίζονται στους μετασχηματισμούς ως θετικά κάτω φράγματα των πραγματικών ριζών. Ο Akritas πέτυχε μια πολυπλοκότητα της τάξης του $\widetilde{\mathcal{O}}_B(d^5\tau^3)$ ή $\widetilde{\mathcal{O}}_B(N^8)$, χωρίς να χρησιμοποιήσει γρήγορους αλγορίθμους μετατόπισης (Εν. 2.2). Ωστόσο, δεν είναι σαφές το πως και αν η προσέγγισή του λαμβάνει υπόψιν το γεγονός ότι το δυαδικό μήκος των συντελεστών ενός πολυώνυμου αυξάνει αν του εφαρμόσουμε έναν μετασχηματισμό μετατόπισης $X \mapsto b + X$. Ένα άλλο σημαντικό σημείο είναι το μέτρο των c_i. Η Εξ. (3.9) υποδηλώνει ότι το μέτρο των μερικών πηλίκων είναι μη φραγμένο. Ο αλγόριθμος CF είναι ο αλγόριθμος που χρησιμοποιείται από το MATHEMATICA [4] για την απομόνωση των πραγματικών ριζών. Ο αναγνώστης μπορεί να ανατρέξει στους Akritas and Strzebonski [3] για μια πειραματική μελέτη των διαφόρων αλγορίθμων απομόνωσης

με υλοποιήσεις βασισμένες στο MATHEMATICA.

Μια άλλη κατηγορία αλγορίθμων, τους οποίους δεν θα μελετήσουμε, είναι οι αριθμητικοί (numerical) αλγόριθμοι, όπου ο όρος *αριθμητικός* χρησιμοποιείται με την έννοια της αριθμητικής ανάλυσης [210, 214, 239]. Οι αλγόριθμοι αυτοί απαιτούν υπολογισμούς με αριθμούς κινητής υποδιαστολής απεριόριστης ακρίβειας (multiprecision floats) και υπολογίζουν προσεγγίσεις σε όλες τις ρίζες, πραγματικές και μιγαδικές, του πολυωνύμου προς επίλυση μέχρι κάποια ακρίβεια ϵ. Προκειμένου να αναγνωριστούν και να απομονωθούν οι πραγματικές ρίζες θα πρέπει να θέσουμε το ϵ ίσο με το φράγμα διαχωρισμού.

Οι βέλτιστοι αλγόριθμοι χρησιμοποιούν την τεχνική 'διαίρει και βασίλευε' και σε γενικές γραμμές η βασική ιδέα είναι η εξής: Δοθέντος ενός πολυωνύμου υπολογίζονται δύο δίσκοι (splitting circles) στο μιγαδικό επίπεδο που περιέχουν περίπου ίσο αριθμό (μιγαδικών) ριζών. Το πολυώνυμο παραγοντοποιείται προσεγγιστικά σε δύο πολυώνυμα οι ρίζες των οποίων είναι (προσεγγιστικά, μέχρι ακρίβεια ϵ) ίσες με τις ρίζες που περιέχονται στους κύκλους. Ο αλγόριθμος επαναλαμβάνεται για καθένα από τα δύο πολυώνυμα και σταματά όταν γίνουν γραμμικά. Η πολυπλοκότητα των αριθμητικών αλγορίθμων είναι σχεδόν βέλτιστη και πιο συγκεκριμένα $\widetilde{\mathcal{O}}_B(d^3\tau)$ ή $\widetilde{\mathcal{O}}_B(N^4)$ [214, 239] αλλά αποτελεσματικές υλοποιήσεις αυτών είναι ακόμα ζητούμενο. Αξίζει επίσης να αναφέρουμε και τον αριθμητικό αλγόριθμο ABERTH [22, 23] για τον οποίο υπάρχει μια πολύ αποτελεσματική υλοποίηση και ο οποίος έχει πολύ καλά πρακτικά αποτελέσματα αλλά για τον οποίο η δυαδική πολυπλοκότητα δεν είναι γνωστή. Στο ίδιο πλαίσιο εντάσσεται και ο αλγόριθμος του Sebastiano e Silva του οποίου η ανάλυση παρουσιάστηκε από τον Cardinal [49].

Όλοι οι παραπάνω αλγόριθμοι υποθέτουν πολυώνυμα χωρίς τετράγωνα.

Στις επόμενες παραγράφους θα παρουσιάσουμε ένα γενικό αλγόριθμο που δέχεται ως είσοδο πολυώνυμα όχι απαραίτητα χωρίς τετράγωνα και υπολογίζει τα διαστήματα απομόνωσης και τις πολλαπλότητες των πραγματικών ριζών. Θα παρουσιάσουμε ένα ενιαίο πλαίσιο για όλους τους αλγορίθμους υποδιαίρεσης, το οποίο απλοποιεί την ανάλυση των αλγορίθμων DESCARTES, BERNSTEIN και STURM. Στο πλαίσιο αυτό μπορούν να ενταχθούν όλοι οι αλγόριθμοι οι οποίοι βασίζονται στην υποδιαίρεση ενός αρχικού διαστήματος, όπως για παράδειγμα ο αλγόριθμος αποκλεισμού των Dedieu and Yakoubsohn [68]. Επίσης, θα βελτιώσουμε την πολυπλοκότητα του αλγορίθμου CF κατά ένα παράγοντα $d\,\tau$ ή N^2. Τέλος, για όλους τους αλγορίθμους απομόνωσης, θα δείξουμε ότι το φράγμα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ ισχύει και για πολυώνυμα τα οποία δεν είναι χωρίς τετράγωνα και στην ίδια πολυπλοκότητα θα υπολογίσουμε και τις πολλαπλότητες των πραγματικών ριζών.

Ο γενικός αλγόριθμος

Παρουσιάζουμε έναν γενικό αλγόριθμο απομόνωσης των πραγματικών ριζών και υπολογισμού των πολλαπλοτήτων τους, ενός πολυωνύμου $A \in \mathbb{Z}[X]$. Ο ψευδο-κώδικας, REALROOTSOLVER, παρουσιάζεται στον Αλγ. 1.

Η είσοδος του αλγορίθμου είναι ένα πολυώνυμο $A \in \mathbb{Z}[X]$ με $\deg(A) = d$ και $\mathcal{L}(A) = \tau$. Η έξοδος του αλγορίθμου είναι μία λίστα (ή διάνυσμα) που περιέχει διαστήματα απομόνωσης των πραγματικών ριζών $L = [[a_1, b_1], \ldots, [a_k, b_k]]$, όπου $a_i, b_i \in \mathbb{Q}$, και μία λίστα με τις πολλαπλότητές τους $M = [m_1, \ldots, m_k]$, όπου $m_i \in \mathbb{N}$, k είναι το πλήθος των πραγματικών ριζών του A_{red} και $\sum_{i=1}^{k} m_i = d$.

Algorithm 1: realRootSolver (A)

Input: $A \in \mathbb{Z}[X]$

Output: Μια λίστα με τα διαστήματα απομόνωσης και μία με τις πολλαπλότητες των ριζών

1 $A_{red} \leftarrow$ squareFreePart(A)
2 $B \leftarrow$ absoluteRootBound(A_{red})
3 $\mathbb{J}_0 = [-B, B]$
4 $L \leftarrow$ realRootIsolator$(A_{red}, \mathbb{J}_0)$
5 $M \leftarrow$ computeMultiplicities(A_{red}, L)
6 return L, M

Αρχικά ο αλγόριθμος υπολογίζει το χωρίς τετράγωνα μέρος του A, καλώντας τη συνάρτηση squareFreePart. Στη συνέχεια υπολογίζει ένα διάστημα που περιέχει όλες τις πραγματικές ρίζες του A_{red}, καλώντας τον αλγόριθμο absoluteRootBound. Τέλος, καλεί κάποιον αλγόριθμο υπολογισμού των διαστημάτων απομόνωσης των πραγματικών ριζών, realRootIsolator, και υπολογίζει τις πολλαπλότητες καλώντας την συνάρτηση computeMultiplicities.

Στη συνέχεια περιγράφουμε και αναλύουμε την πολυπλοκότητα των διαφόρων συναρτήσεων (αλγορίθμων) που χρησιμοποιεί ο αλγόριθμος realRootSolver.

- squareFreePart
  Έστω A_{red} το χωρίς τετράγωνα μέρος του A. Παρατηρούμε ότι $\deg(A_{red}) = \mathcal{O}(d)$ και $\mathcal{L}(A_{red}) = \mathcal{O}(d + \tau)$. Η πολυπλοκότητα αυτού του υπολογισμού είναι $\widetilde{\mathcal{O}}_B(d^2\tau)$ αν χρησιμοποιήσουμε τους γρήγορους αλγορίθμους για τον υπολογισμό ακολουθιών πολυωνυμικών υπολοίπων. Δείτε Θεωρ. 2.34.

- absoluteRootBound
  Μπορούμε να χρησιμοποιήσουμε ένα από τα απόλυτα φράγματα που παρουσιάστηκαν στην Εν. 3.2, δείτε και Σημ. 3.11. Όλα τα φράγματα έχουν, ασυμπτωτικά, το ίδιο δυαδικό μήκος, συνεπώς μπορούμε να υποθέσουμε ότι $B = 2^\tau$ και $\mathbb{J}_0 = [\mathsf{a}, \mathsf{b}] = [-2^\tau, 2^\tau]$.

  Η πολυπλοκότητα του βήματος αυτού είναι $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B(d(d + \tau)) = \widetilde{\mathcal{O}}_B(d^2 + d\tau)$.

- computeMultiplicites
  Προκειμένου να υπολογίσουμε τις πολλαπλότητες των πραγματικών ριζών του A πρέπει καταρχάς να υπολογίσουμε την *ελεύθερη τετραγώνων παραγοντοποίηση* του. Αυτή η παραγοντοποίηση συνίσταται από πολυώνυμα $(g_1, g_2, \ldots, g_m)$ τέτοια ώστε $A = g_1 g_2^2 \cdots g_m^m$, $g_m \neq 1$, τα g_i είναι πρώτα μεταξύ τους και χωρίς τετράγωνα. Για τον υπολογισμό της παραγοντοποίησης χρησιμοποιούμε τον αλγόριθμο του Yun [263] ο οποίος έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2\tau)$. Μάλιστα προκειμένου να είμαστε πιο ακριβής μπορούμε να πούμε ότι το κόστος της παραγοντοποίησης είναι δύο φορές το κόστος υπολογισμού του $\mathbf{SR}(A, A')$ [112]. Επιπλέον, ισχύει $\deg(g_j) = \delta_j \leq d$ και $\mathcal{L}(g_j) = O(d\tau)$, όπως προκύπτει από το φράγμα του Mignotte [187, 188, 189], όπου $1 \leq j \leq m$.

Κάθε διάστημα απομόνωσης περιέχει μία και μόνο μία πραγματική ρίζα του A_{red} και άρα το A_{red} αλλάζει πρόσημο αν αποτιμηθεί στα άκρα του κάθε διαστήματος, δηλαδή ισχύει $A_{red}(\mathsf{a}_i)A_{red}(\mathsf{b}_i) < 0$, $1 \leq i \leq k$, σύμφωνα με το θεώρημα του Bolzano.

Παρατηρούμε ότι ένα και μόνο ένα από τα πολυώνυμα g_j πρέπει να αλλάζει πρόσημο σε κάθε διάστημα απομόνωσης καθώς είναι χωρίς τετράγωνα και πρώτα μεταξύ τους. Αν κάποιο g_j αλλάζει πρόσημο σε κάποιο από τα διαστήματα απομόνωσης τότε η πολλαπλότητα της πραγματικής ρίζας που περιέχεται στο διάστημα αυτό είναι j. Κάθε g_j μπορεί να αποτιμηθεί σε κάποιο άκρο ενός διαστήματος απομόνωσης με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(\delta_i^2\, d\, \tau)$, αν χρησιμοποιήσουμε τον κανόνα του Horner. Μπορούμε ωστόσο να το αποτιμήσουμε πάνω σε όλα τα άκρα (το πλήθος τους είναι το πολύ $d+1$) σε χρόνο $\widetilde{\mathcal{O}}_B(\delta_i\, d^2\, \tau)$ [263, 275] (δείτε Εν. 2.2).

Εφόσον $\sum_{i=1}^{m} \delta_i \leq d$ η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$.

Αν το πλήθος των διαστημάτων που περιέχει η λίστα L είναι k τότε κατασκευάζουμε μία λίστα M, μεγέθους k, τέτοια ώστε αν $M[j] = m_j \in \mathbb{N}$, τότε η πραγματική ρίζα του A που περιέχεται στο j-οστό διάστημα απομόνωσης της L έχει πολλαπλότητα m_j.

Από τα παραπάνω προκύπτει ότι η συνολική πολυπλοκότητα του αλγορίθμου realRootSolver είναι το μέγιστο ανάμεσα στο $\widetilde{\mathcal{O}}_B(d^3\tau)$ και στην πολυπλοκότητα του αλγορίθμου realRootIsolator.

3.4 Ο αλγόριθμος του Kronecker

Ο Kronecker [166], δείτε επίσης [55], παρουσίασε έναν αλγόριθμο για την απομόνωση των πραγματικών ριζών ενός πολυωνύμου χωρίς τετράγωνα. Ο αλγόριθμος βασίζεται στον θεώρημα του Bolzano, δηλαδή ότι αν σε ένα διάστημα περιέχεται μία και μόνο πραγματική ρίζα ενός πολυωνύμου τότε το πολυώνυμο έχει διαφορετικό πρόσημο στα άκρα του διαστήματος. Ο αλγόριθμος είναι απλός αλλά όχι πολυωνυμικός. Τον παρουσιάζουμε προκειμένου να εισάγουμε τον αναγνώστη στους ακριβείς αλγορίθμους απομόνωσης των πραγματικών ριζών αλλά και για να απαντήσουμε σε ένα ερώτημα των Collins and Loos [55] σχετικά με το αναμενόμενο πλήθος των διαστημάτων που εξετάζει ο αλγόριθμος.

Ο ψευδο-κώδικας του αλγορίθμου kronecker παρουσιάζεται στον Αλγ. 2. Η είσοδος του αλγορίθμου είναι ένα πολυώνυμο A_{red} χωρίς τετράγωνα και η έξοδός του είναι μία λίστα L με τα διαστήματα απομόνωσης των πραγματικών ριζών.

Καταρχάς, ο αλγόριθμος υπολογίζει ένα απόλυτο φράγμα στις ρίζες (Εν. 3.2). Όλα τα φράγματα έχουν, ασυμπτωτικά, το ίδιο δυαδικό μήκος, συνεπώς μπορούμε να υποθέσουμε ότι $B = 2^\tau$. Το βήμα αυτό μπορεί να μην εκτελεστεί αν υποθέσουμε ότι έχει προηγηθεί ο αλγόριθμος realRootIsolator. Στη συνέχεια υπολογίζει το φράγμα διαχωρισμού, έστω Δ (Εν. 3.2).

Ακολούθως χωρίζει το διάστημα $[-B, B]$ σε διαστήματα μήκους Δ και ελέγχει, με το θεώρημα του Bolzano, αν κάποιο από αυτά περιέχει κάποια πραγματική ρίζα του A_{red}. Η συνάρτηση add$(L, [\mathsf{a}, \mathsf{b}])$, εισάγει το διάστημα $[\mathsf{a}, \mathsf{b}]$ στη λίστα L των διαστημάτων απομόνωσης.

Η ανάλυση της πολυπλοκότητας του αλγορίθμου βασίζεται στο πόσες φορές εκτελείται ο βρόγχος **while** (Γραμμή 6), δηλαδή εξαρτάται από το πόσα διαστήματα εξετάζει. Εφόσον το

Algorithm 2: KRONECKER (A_{red})

Input: $A_{red} \in \mathbb{Z}[X]$
Output: Μια λίστα από διαστήματα απομόνωσης

$L \leftarrow \emptyset$
$B \leftarrow$ ABSOLUTEROOTBOUND(A_{red})
$\Delta \leftarrow$ SEPARATIONBOUND(A_{red})
$\mathsf{a} \leftarrow -B$
$s_L \leftarrow \mathrm{sign}(A_{red}(\mathsf{a}))$
while $\mathsf{a} < B$ **do**
  $\mathsf{b} \leftarrow \mathsf{a} + \Delta$
  $s_R \leftarrow \mathrm{sign}(A_{red}(\mathsf{b}))$
  if $s_R = 0$ **then** $L \leftarrow$ ADD$(L, [\mathsf{b}, \mathsf{b}])$
  if $s_L \cdot s_R < 0$ **then** $L \leftarrow$ ADD$(L, [\mathsf{a}, \mathsf{b}])$
  $\mathsf{a} \leftarrow \mathsf{b}$
  $s_L \leftarrow s_R$
RETURN L

αρχικό διάστημα είναι $[-2^\tau, 2^\tau]$ έχει μήκος $2^{\tau+1}$. Επίσης $\Delta = 2^{-\mathcal{O}(d\tau)}$, δείτε Εν. 3.2. Επομένως, ο αλγόριθμος εξετάζει $2^{\mathcal{O}(d\tau)}$ διαστήματα.

Σε κάθε βήμα υπολογίζει την αποτίμηση του A_{red} πάνω σε ένα ρητό αριθμό δυαδικού μήκους το πολύ $\mathcal{O}(d\tau)$. Η πολυπλοκότητα της αποτίμησης είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Εν. 2.2).

Συνεπώς μπορούμε να διατυπώσουμε το παρακάτω θεώρημα:

Θεώρημα 3.34 (KRONECKER)
Έστω πολυώνυμο $A_{red} \in \mathbb{Z}[X]$ χωρίς τετράγωνα, τέτοιο ώστε $\deg(A_{red}) = d$ και $\mathcal{L}(A_{red}) = \tau$. Ο αλγόριθμος KRONECKER *απομονώνει τις πραγματικές ρίζες του A_{red} σε χρόνο $\widetilde{\mathcal{O}}_B(2^{d\tau}d^3\tau)$.*

Υπάρχει μια προφανής βελτίωση του αλγορίθμου KRONECKER. Αντί να υπολογίζουμε κάθε φορά τα πρόσημα στα άκρα ενός διαστήματος θα μπορούσαμε να υπολογίζουμε το πρόσημο στα άκρα d διαστημάτων, ταυτόχρονα, με την ίδια πολυπλοκότητα (Εν. 2.2). Δυστυχώς αυτή η παραλλαγή δεν βελτιώνει την εκθετική πολυπλοκότητα του αλγορίθμου καθώς τα διαστήματα που πρέπει να εξεταστούν είναι $2^{\mathcal{O}(d\tau)}/d = 2^{\mathcal{O}(d\tau)}$.

Αν χρησιμοποιήσουμε τον αλγόριθμο KRONECKER ως REALROOTISOLATOR στον Αλγ. 1 τότε η πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(2^{d\,\tau}d^3\tau + d^3\tau)$ ή $\widetilde{\mathcal{O}}_B(2^{d\,\tau}d^3\tau)$ για τον υπολογισμό και των πολλαπλοτήτων των πραγματικών ριζών.

Οι Collins and Loos [55] έθεσαν το ερώτημα σχετικά με το πόσα διαστήματα κατά μέσο όρο εξετάζει ο αλγόριθμος KRONECKER. Θα προσπαθήσουμε να απαντήσουμε σε αυτό το ερώτημα κάνοντας την υπόθεση ότι κάθε διάστημα έχει την ίδια πιθανότητα να περιέχει μία πραγματική ρίζα του A_{red}.

Αν υποθέσουμε ότι το πλήθος των πραγματικών ριζών, έστω R, δεν είναι γνωστό και ότι $R < d$, τότε ο αλγόριθμος, πάντοτε, εξετάζει όλα τα διαστήματα, καθώς δεν μπορεί να γνωρίζει πότε πρέπει να σταματήσει.

Ας υποθέσουμε λοιπόν ότι γνωρίζουμε το ακριβές πλήθος των πραγματικών ριζών, $R \leq d$. Έστω K όλα τα διαστήματα προς εξέταση. Όλες οι δυνατές θέσεις των ριζών είναι $\binom{K}{R}$. Το πόσα διαστήματα θα εξεταστούν εξαρτάται από τη θέση της μεγαλύτερης ρίζας, η οποία μπορεί να βρίσκεται από τη θέση R έως και τη θέση K. Αν βρίσκεται στην ℓ θέση, όπου $R \leq \ell \leq K$, τότε εξετάζονται ℓ διαστήματα και υπάρχουν $\binom{\ell-1}{R}$ τέτοιες περιπτώσεις. Συνεπώς η μέση τιμή του πλήθους των εξεταζόμενων διαστημάτων είναι

$$\frac{\sum_{\ell=R}^{K} \binom{\ell-1}{R-1} \ell}{\binom{K}{R}} = \frac{R\,(K+1)}{R+1}$$

Αν $R = 1$, τότε προφανώς δεν χρειάζεται να εκτελεστεί ο αλγόριθμος KRONECKER καθώς έχουμε, από κατασκευής, ένα διάστημα απομόνωσης, το $[-B, B]$. Αν παρ' όλα αυτά ο αλγόριθμος εκτελεστεί, για παράδειγμα αν θέλουμε να υπολογίσουμε ένα, μικρού μήκους, διάστημα που να περιέχει την πραγματική ρίζα, τότε το αναμενόμενο πλήθος των εξεταζόμενων διαστημάτων είναι $\frac{K+1}{2}$. Το οποίο προφανώς συμπίπτει με τον αναμενόμενο πλήθος πλήθος συγκρίσεων κατά τη σειριακή αναζήτηση ενός στοιχείου σε ένα πίνακα [161].

3.5 Αλγόριθμοι υποδιαίρεσης

Στην παρούσα παράγραφο θα εξειδικεύσουμε τον αλγόριθμο REALROOTISOLATOR με αλγορίθμους υποδιαίρεσης, τους οποίους θα συμβολίσουμε με $\text{SUBDIVISIONSOLVER}_{\text{SM}}$. Θα θεωρήσουμε ότι το πολυώνυμο, A_{red} που εξετάζουμε είναι χωρίς τετράγωνα και ότι $\deg(A_{red}) = d$ και $\mathcal{L}(A_{red}) = \tau$. Υπενθυμίζουμε ότι οι αλγόριθμοι υποδιαίρεσης για την απομόνωση των πραγματικών ριζών είναι παρόμοιοι με αυτόν της δυαδικής αναζήτησης.

Ο ψευδοκώδικας του γενικού αλγορίθμου υποδιαίρεσης παρουσιάζεται στον Αλγ. 3. Η είσοδος είναι το πολυώνυμο $A_{red} \in \mathbb{Z}[X]$ χωρίς τετράγωνα και ένα διάστημα $\mathcal{I}_0$ στο οποίο θέλουμε να απομονώσουμε τις πραγματικές ρίζες του A_{red}. Συνήθως το $\mathcal{I}_0$ περιέχει όλες τις πραγματικές ρίζες του A_{red}. Ο αλγόριθμος χρησιμοποιεί μια στοίβα Q η οποία περιέχει ζεύγη της μορφής $\{f, \mathcal{I}\}$. Η σημασιολογία του ζεύγους είναι ότι απαιτείται να απομονώσουμε τις πραγματικές ρίζες του f στο διάστημα $\mathcal{I}$.

Στον Αλγ. 3 εμφανίζονται κλήσεις σε μερικές βοηθητικές, εξωτερικές, συναρτήσεις (αλγορίθμους). Καταρχάς εμφανίζονται δύο συναρτήσεις που αφορούν τη στοίβα Q. Η συνάρτηση $\text{PUSH}(Q, \{f, \mathcal{I}\})$, η οποία εισάγει το ζεύγος $\{f, \mathcal{I}\}$ στην κορυφή της στοίβας και η συνάρτηση $\text{POP}(Q)$ η οποία επιστρέφει το ζεύγος που βρίσκεται στην κορυφή της στοίβας Q και ταυτόχρονα το διαγράφει από αυτήν. Επίσης η συνάρτηση $\text{ADD}(L, \mathcal{I})$, εισάγει το διάστημα $\mathcal{I}$ στη λίστα L των διαστημάτων απομόνωσης.

Τέλος, υπάρχουν τρεις εξωτερικές συναρτήσεις με δείκτη SM οι οποίες επιδέχονται διαφορετικής υλοποίησης ανάλογα με τον αλγόριθμο υποδιαίρεσης που χρησιμοποιείται. Καταρχάς, η συνάρτηση $\text{INITIALIZATION}_{\text{SM}}$ εκτελεί κάποιες διαδικασίες αρχικοποίησης ανάλογα με τον αλγόριθμο υποδιαίρεσης. Η συνάρτηση $\text{COUNT}_{\text{SM}}(f, \mathcal{I})$ επιστρέφει το πλήθος (ή ένα άνω φράγμα στο

Algorithm 3: SUBDIVISIONSOLVER$_{\text{SM}}(A_{red}, \mathcal{I}_0)$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I}_0 = [\mathsf{a}, \mathsf{b}]$
Output: Μια λίστα από διαστήματα απομόνωσης

```
1  INITIALIZATION_SM(A_red, I_0)
2  L ← ∅
3  Q ← ∅
4  Q ← PUSH(Q, {A, I_0})
5  while Q ≠ ∅ do
6      {f, I} ← POP(Q)
7      V ← COUNT_SM(f, I)
8      switch V do
9          case V = 0 continue
10         case V = 1 L ← ADD(L, I)
11         case V > 1
12             {f_L, I_L}, {f_R, I_R} ← SPLIT_SM(f, I)
13             Q ← PUSH(Q, {f_L, I_L})
14             Q ← PUSH(Q, {f_R, I_R})
15 RETURN L
```

πλήθος) των πραγματικών ριζών του f στο $\mathcal{I}$. Τέλος η συνάρτηση $\text{SPLIT}_{\text{SM}}(f, \mathcal{I})$ υποδιαιρεί το διάστημα $\mathcal{I}$ σε δύο ίσα υποδιαστήματα και ανάλογα με τον αλγόριθμο ενδεχομένως υποδιαιρεί και το f.

Παρατηρούμε ότι η πολυπλοκότητα του αλγορίθμου υποδιαίρεσης εξαρτάται από το πόσες φορές εκτελείται ο βρόγχος while (Γραμμή 5 στον Αλγ. 3) και από το κόστος των συναρτήσεων $\text{COUNT}_{\text{SM}}(f, \mathcal{I})$ και $\text{SPLIT}_{\text{SM}}(f, \mathcal{I})$. Επίσης, σε κάθε βήμα του αλγορίθμου, αφού το προς εξέταση διάστημα χωρίζεται σε δύο ίσα υποδιαστήματα, μπορούμε να υποθέσουμε ότι το δυαδικό μήκος των άκρων του διαστήματος αυξάνεται κατά ένα. Πιο συγκεκριμένα αν υποθέσουμε ότι τα άκρα του αρχικού διαστήματος $\mathcal{I}_0$, έχουν μήκος τ, τότε στο h βήμα του αλγορίθμου το δυαδικό μήκος των άκρων του προς εξέταση διαστήματος $\mathcal{I} \subseteq \mathcal{J}_0$ είναι $\tau + h$.

Οι διάφοροι αλγόριθμοι υποδιαίρεσης χαρακτηρίζονται ανάλογα με το πως υλοποιούν τις τρεις αυτές συναρτήσεις. Θα εξετάσουμε τρεις τέτοιους αλγορίθμους:

- τον αλγόριθμο STURM ή $\text{SUBDIVISIONSOLVER}_{\text{STURM}}$,
- τον αλγόριθμο DESCARTES ή $\text{SUBDIVISIONSOLVER}_{\text{DESCARTES}}$, και
- τον αλγόριθμο BERNSTEIN ή $\text{SUBDIVISIONSOLVER}_{\text{BERNSTEIN}}$.

Σημείωση 3.35. *Στον Αλγ. 3 θα πρέπει να προστεθεί ένας έλεγχος σχετικά με το αν το μέσο κάποιου προς εξέταση διαστήματος $\mathcal{I}$ αποτελεί ρίζα του f. Ο έλεγχος αυτός δεν επηρεάζει την πολυπλοκότητα του αλγορίθμου και γι' αυτό τον παραλείπουμε για λόγους απλότητας.*

Επιπρόσθετα, ο Αλγ. 3 μπορεί εύκολα να τροποποιηθεί έτσι ώστε να απομονώσει τις πραγματικές ρίζες του A_{red} σε κάποιο διάστημα $\mathcal{J} \subseteq \mathcal{I}_0$.

Ο αλγόριθμος STURM

Ο αλγόριθμος STURM μοιάζει περισσότερο από όλους τους αλγορίθμους υποδιαίρεσης με αυτόν της δυαδικής αναζήτησης. Χρησιμοποιεί αποτιμήσεις της προσημασμένης ακολουθίας υποεπιλθουσών $\mathbf{SR}(A_{red})$ προκειμένου να μετρήσει το πλήθος των πραγματικών ριζών του A_{red} που περιέχονται σε ένα διάστημα $\mathcal{I}$ (Θεωρ. 2.27).

Παρατηρούμε ότι το Θεωρ. 2.27 μας επιτρέπει να μετρήσουμε τις ρίζες ενός πολυωνύμου σε ένα διάστημα ακόμα και αν αυτό δεν είναι χωρίς τετράγωνα. Δηλαδή, θα μπορούσαμε να χρησιμοποιήσουμε την ακολουθία $\mathbf{SR}(A)$ αντί της $\mathbf{SR}(A_{red})$. Ωστόσο, προκειμένου να επιτύχουμε ομοιόμορφη παρουσίαση για όλους τους αλγορίθμους υποδιαίρεσης θα υποθέσουμε ότι η είσοδος είναι ένα πολυώνυμο χωρίς τετράγωνα, καθώς αυτή η υπόθεση (τελικά) δεν επηρεάζει σημαντικά τον υπολογισμό της πολυπλοκότητας.

Το ότι ο αλγόριθμος τερματίζει, εξασφαλίζεται από το ότι το $\mathbb{Q}$ είναι Αρχιμήδειο σώμα [14]. Ένα σώμα είναι Αρχιμήδειο αν μπορεί να οριστεί σε αυτό διάταξη, και άρα απόλυτη τιμή, και αν για κάθε στοιχείο του, έστω x, υπάρχει ένας φυσικός αριθμός n τέτοιος ώστε $|x| < n$. Κατά συνέπεια, οι συνεχείς υποδιαιρέσεις μικραίνουν τα διαστήματα, τα οποία τελικά γίνονται τόσο μικρά όσο το φράγμα διαχωρισμού. Προφανώς, σε διαστήματα με μήκος τόσο μικρό όσο το φράγμα διαχωρισμού περιέχεται μία ή καμία πραγματική ρίζα.

Algorithm 4: INITIALIZATION$_{\text{STURM}}(A_{red}, \mathcal{I})$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: $\mathbf{StHa}(A)$

1 COMPUTE $\mathbf{SR}(A_{red})$

Algorithm 5: COUNT$_{\text{STURM}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Το πλήθος των (διαφορετικών) πραγματικών ριζών του f στο $[\mathsf{a}, \mathsf{b}]$

1 RETURN VAR$(\mathbf{SR}(A\,;\,\mathsf{a}) - \text{VAR}(\mathbf{SR}(A\,;\,\mathsf{b}))$

Algorithm 6: SPLIT$_{\text{STURM}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Διαμέριση του διαστήματος $\mathcal{I}$ και του f

1 $\mathsf{m} \leftarrow \frac{\mathsf{a}+\mathsf{b}}{2}$
2 $\mathcal{I}_L \leftarrow [\mathsf{a}, \mathsf{m}]$
3 $\mathcal{I}_R \leftarrow [\mathsf{m}, \mathsf{b}]$
4 RETURN $\{f, \mathcal{I}_L\}, \{f, \mathcal{I}_R\}$

Παρουσιάζουμε τώρα την ανάλυση πολυπλοκότητας των διαφόρων συναρτήσεων που εμπλέκονται στην εκτέλεση του αλγορίθμου.

- INITIALIZATION$_{\text{STURM}}$ (Αλγ. 4)
  Η αρχικοποίηση του αλγορίθμου συνίσταται στο να υπολογίσουμε την ακολουθία $\mathbf{SR}(A_{red})$. Η πολυπλοκότητα της συνάρτησης είναι $\widetilde{\mathcal{O}}_B(d^2\tau)$ (Θεωρ. 2.31).

- SPLIT$_{\text{STURM}}$ (Αλγ. 6)
  Η συνάρτηση αυτή υπολογίζει το μέσον του $\mathcal{I}$ και επιστρέφει δύο υποδιαστήματα. Η πολυπλοκότητα της συνάρτησης είναι $\mathcal{O}_B(\tau + h)$.

- COUNT$_{\text{STURM}}$ (Αλγ. 5)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση διάστημα είναι το $\mathcal{I}$. Τα άκρα του $\mathcal{I}$ έχουν δυαδικό μήκος φραγμένο από $\tau + h$.

  Το κόστος της συνάρτησης εξαρτάται από το κόστος αποτίμησης της ακολουθίας $\mathbf{SR}(A_{red})$ πάνω στα άκρα του $\mathcal{I}$, το οποίο είναι $\widetilde{\mathcal{O}}_B\left(d^2(\tau + h)\right)$ (Θεωρ. 2.32).

  Υπενθυμίζουμε ότι η συνάρτηση COUNT$_{\text{STURM}}(f, \mathcal{I})$ μετρά *ακριβώς* το πλήθος των πραγματικών ριζών του f στο $\mathcal{I}$.

Σημείωση 3.36. *Παρατηρούμε ότι δεν χρειάζεται να περνάμε ως παράμετρο κάποιο πολυώνυμο f στις συναρτήσεις* SPLIT$_{\text{STURM}}$ *και* COUNT$_{\text{STURM}}$. *Παρ'όλα αυτά το κάνουμε προκειμένου ο ψευδοκώδικας να είναι ο ίδιος σε όλους τους αλγορίθμους υποδιαίρεσης. Επίσης, σε όλη τη διάρκεια του αλγορίθμου $f \equiv A_{red}$.*

Ο αλγόριθμος DESCARTES

Algorithm 7: INITIALIZATION$_{\text{DESCARTES}}(A_{red}, \mathcal{I}_0)$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I}_0 = [\mathsf{a}, \mathsf{b}]$
Output: Το A_{red} μετασχηματίζεται έτσι ώστε όλες οι ρίζες του στο $\mathcal{I}_0$ να είναι στο $(0, 1)$

1 $A_{red} \leftarrow A_{red}\left((\mathsf{b} - \mathsf{a})X + \mathsf{a}\right)$

Algorithm 8: COUNT$_{\text{DESCARTES}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$
Output: Ένα άνω φράγμα στις πραγματικές ρίζες του f στο $(0, 1)$

1 $g \leftarrow \mathcal{T}_{-1}(\mathcal{R}(f))(X)$
2 RETURN VAR(g)

Algorithm 9: SPLIT$_{\text{DESCARTES}}(f, \mathcal{I})$

Input: $f \in \mathbb{Z}[X]$
Output: Διαμέριση του διαστήματος $\mathcal{I}$ και του f

1 $\mathsf{m} \leftarrow \frac{\mathsf{a}+\mathsf{b}}{2}$
2 $\mathcal{I}_L \leftarrow [\mathsf{a}, \mathsf{m}]$
3 $\mathcal{I}_R \leftarrow [\mathsf{m}, \mathsf{b}]$
4 $f_L \leftarrow \mathcal{H}_2'(f)(X)$
5 $f_R \leftarrow \mathcal{T}_{-1}(\mathcal{H}_2'(f))(X)$
6 RETURN $\{f_L, \mathcal{I}_L\}, \{f_R, \mathcal{I}_R\}$

Ο αλγόριθμος DESCARTES, όπως ήδη έχουμε αναφέρει, βασίζεται στον κανόνα προσήμων του Descartes (Θεωρ. 3.28).

Αρχικά το A_{red} μετασχηματίζεται έτσι ώστε όλες οι ρίζες του στο $\mathcal{I}_0$ να περιέχονται πλέον στο $(0,1)$. Στο βήμα h του αλγορίθμου πρέπει να εξεταστεί το ζεύγος $\{f, \mathcal{I}\}$. Οι ρίζες του προς εξέταση πολυωνύμου f στο $(0,1)$ αντιστοιχούν στις ρίζες του A_{red} στο $\mathcal{I}$. Αν το f έχει περισσότερες από μία ρίζες τότε υπολογίζονται δύο υποδιαστήματα του $\mathcal{I}$, τα $\mathcal{I}_L$ και $\mathcal{I}_R$, όπως επίσης και δύο πολυώνυμα, f_L και f_R, τέτοια ώστε οι ρίζες του f_L, αντίστοιχα f_R, στο $(0,1)$ να αντιστοιχούν στις ρίζες του A_{red} στο $\mathcal{I}_L$, αντίστοιχα $\mathcal{I}_R$, και ο αλγόριθμος επαναλαμβάνεται.

Παρατηρούμε ότι ο κανόνας προσήμων του Descartes δίνει στη γενική περίπτωση μια υπερεκτίμηση για το πλήθος των θετικών πραγματικών ριζών. Κατά συνέπεια οι υποδιαιρέσεις συνεχίζονται μέχρι τα προς εξέταση διαστήματα να έχουν μήκος τόσο όσο υποδηλώνουν τα θεωρήματα του ενός και των δύο κύκλων (Θεωρ. 3.32 και Θεωρ. 3.33) προκειμένου να εξασφαλίσουμε ότι θα έχουμε μία ή καμία εναλλαγή προσήμων και άρα ο κανόνας των προσήμων θα υπολογίσει ακριβώς το πλήθος των θετικών πραγματικών ριζών. Το γεγονός ότι το $\mathbb{Q}$ είναι Αρχιμήδειο σώμα εξασφαλίζει ότι από τις υποδιαιρέσεις τελικώς θα προκύψουν τέτοια (μικρά) διαστήματα και άρα ο αλγόριθμος θα τερματίσει.

Παρουσιάζουμε τώρα την ανάλυση πολυπλοκότητας των διαφόρων συναρτήσεων που εμπλέκονται στην εκτέλεση του αλγορίθμου.

- $\text{INITIALIZATION}_{\text{DESCARTES}}$ (Αλγ. 7)
  Η αρχικοποίηση του αλγορίθμου συνίσταται στο να μετασχηματίσουμε το A_{red} σε ένα πολυώνυμο $\overline{A}_{red}$ τέτοιο ώστε οι ρίζες του A_{red} στο $\mathcal{I}_0$ να αντιστοιχούν στις ρίζες του $\overline{A}_{red}$ στο $(0,1)$. Αυτό επιτυγχάνεται με τον μετασχηματισμό $\phi(X) = (\mathsf{b}-\mathsf{a})X + \mathsf{a}$. Θεωρούμε ότι $\mathcal{L}(\mathsf{a}) = \mathcal{L}(\mathsf{b}) = \tau$ και άρα η πολυπλοκότητα της αρχικοποίησης είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Εν. 2.2). Παρατηρούμε ότι για το $\overline{A}_{red}$ ισχύει $\deg(\overline{A}_{red}) = d$ και $\mathcal{L}\left(\overline{A}_{red}\right) = \mathcal{O}(d\tau)$.

  Προκειμένου να μην επιβαρύνουμε τον συμβολισμό θα συμβολίσουμε το $\overline{A}_{red}$ πάλι με A_{red}.

- $\text{COUNT}_{\text{DESCARTES}}$ (Αλγ. 8)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Οι ρίζες του f στο $(0,1)$ αντιστοιχούν στις ρίζες του αρχικού πολυωνύμου στο $\mathcal{I}$. Παρατηρούμε ότι τα άκρα του $\mathcal{I}$ έχουν δυαδικό μήκος φραγμένο από $\tau + h$. Επίσης το προς εξέταση πολυώνυμο έχει δυαδικό μήκος $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$, όπως προκύπτει από την συνάρτηση SPLIT.

  Προκειμένου να μετρήσουμε τις ρίζες του f στο $(0,1)$ υπολογίζουμε το πολυώνυμο $g = \mathcal{T}_{-1} \circ \mathcal{R} \circ f$. Οι ρίζες του g στο $(0,\infty)$ αντιστοιχούν στις ρίζες του f στο $(0,1)$.

  Προκειμένου να μετρήσουμε τις ρίζες χρησιμοποιούμε τον κανόνα προσήμων του Descartes (Θεωρ. 3.28), άρα αρκεί να υπολογίσουμε τις αλλαγές προσήμων στους συντελεστές του g.

  Ο μετασχηματισμός αντιστροφής, $\mathcal{R}$, δεν αλλάζει το μέγιστο δυαδικό μήκος των συντελεστών και απαιτεί $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B\left(d(d\tau + dh)\right)$ (Εν. 2.2).

  Ο μετασχηματισμός $\mathcal{T}_{-1} \circ \mathcal{R} \circ f$ έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2 \lg d + d(d\tau + dh) + d^2)$ και $\mathcal{L}(g) = \mathcal{O}(d\tau + (d+1)h)$ (Εν. 2.2).

  Η συνάρτηση $\mathtt{VAR}(g)$ απαιτεί $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B\left(d(d\tau + (d+1)h)\right)$.

Συνεπώς το συνολικό κόστος της συνάρτησης είναι $\widetilde{\mathcal{O}}_B(d^2 \lg d + d^2\tau + d^2 h)$.

- SPLIT$_{\text{DESCARTES}}$ (Αλγ. 9)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Παρατηρούμε ότι τα άκρα του $\mathcal{I}$ έχουν δυαδικό μήκος φραγμένο από $\tau + h$. Επίσης το προς εξέταση πολυώνυμο έχει δυαδικό μήκος $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$.

  Υπολογίζουμε το μέσον του διαστήματος $\mathcal{I}$ με πολυπλοκότητα $\mathcal{O}_B(\tau + h)$.

  Εφόσον $f_L = \mathcal{H}_2^{'}(f)(X)$ ο υπολογισμός του απαιτεί $\mathcal{O}(d)$ πράξεις ολίσθησης και $\mathcal{L}(f_L) = \mathcal{O}(d\tau + dh + d)$ (Εν. 2.2).

  Παρατηρούμε ότι $f_R = \mathcal{T}_{-1}(\mathcal{H}_2^{'}(f) = \mathcal{T}_{-1}(f_L)(X)$. Συνεπώς ο υπολογισμός του έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^2 \lg d + d(d\tau + (d+1)h + d) + d^2)$ και $\mathcal{L}(f_R) = \mathcal{O}(d\tau + dh + 2d)$ (Εν. 2.2).

  Συμπεραίνουμε ότι η συνολική πολυπλοκότητα της συνάρτησης είναι $\widetilde{\mathcal{O}}_B(d^2 \lg d + d^2\tau + d^2 h)$ και ότι $\mathcal{L}(f_L) = \mathcal{L}(f_R) = \mathcal{O}(d\tau + dh)$.

  Μια σημαντική παρατήρηση αφορά το μέγιστο δυαδικό μήκος των συντελεστών των f_L και f_R. Αρχικά $\mathcal{L}(A_{red}) = d\tau$. Σε κάθε βήμα του αλγορίθμου υπόκειται (το πολύ) σε μια ομοθεσία και σε μία μετατόπιση και άρα οι συντελεστές του αυξάνουν (το πολύ) κατά έναν προσθετικό παράγοντα d. Γι' αυτό υποθέτουμε ότι στο h βήμα του αλγορίθμου $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$.

Ο αλγόριθμος BERNSTEIN

Algorithm 10: INITIALIZATION$_{\text{BERNSTEIN}}(A_{red}, \mathcal{I}_0)$

Input: $A_{red} \in \mathbb{Z}[X]$, $\mathcal{I}_0 = [\mathsf{a}, \mathsf{b}]$
Output: Το A_{red} μετασχηματίζεται στη βάση Bernstein στο διάστημα $\mathcal{I}_0$

1 $A_{red} \leftarrow \sum_{i=0}^{d} b_i \mathfrak{B}_d^i(X; \mathsf{a}, \mathsf{b})$

Algorithm 11: COUNT$_{\text{BERNSTEIN}}(f, \mathcal{I})$

Input: $f = \sum_{i=0}^{d} b_i \mathfrak{B}_i^d(X)$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Ένα άνω φράγμα στις πραγματικές ρίζες του f στο $\mathcal{I}$

1 RETURN VAR$(b_0, \ldots, b_d)$

Algorithm 12: SPLIT$_{\text{BERNSTEIN}}(f, \mathcal{I})$

Input: $f = \sum_{i=0}^{d} b_i \mathfrak{B}_i^d(X)$, $\mathcal{I} = [\mathsf{a}, \mathsf{b}]$
Output: Διαμέριση του διαστήματος $\mathcal{I}$ και του f

1 $\mathsf{m} \leftarrow \frac{\mathsf{a}+\mathsf{b}}{2}$
2 $\mathcal{I}_L \leftarrow [\mathsf{a}, \mathsf{m}]$
3 $\mathcal{I}_R \leftarrow [\mathsf{m}, \mathsf{b}]$
4 $f_L \leftarrow \overline{\mathcal{S}}_L(f)(X)$
5 $f_R \leftarrow \overline{\mathcal{S}}_R(f)(X)$
6 RETURN $\{f_L, \mathcal{I}_L\}, \{f_R, \mathcal{I}_R\}$

Μια απλή παρατήρηση που μπορεί να γίνει στον αλγόριθμο του DESCARTES είναι ότι είναι ανεξάρτητος από το βάση στην οποία αναπαρίσταται το πολυώνυμο. Στον αλγόριθμο DESCARTES που παρουσιάσαμε υποθέσαμε ότι τα πολυώνυμα είναι στη βάση των δυνάμεων. Ο αλγόριθμος BERNSTEIN υποθέτει πολυώνυμα στη βάση Bernstein (Εν. 2.4). Ο λόγος χρησιμοποίησης αυτής της αναπαράστασης είναι ότι η αριθμητική ευστάθεια των πολυωνύμων στη βάση αυτή είναι πολύ καλή και έτσι τα αποτελέσματα του αλγορίθμου αν υλοποιηθεί με αριθμούς κινητής υποδιαστολής ή και με αριθμητική διαστημάτων είναι αριθμητικά ευσταθή. Επιπρόσθετα, οι βρόγχοι των διαφόρων υπολογισμών που εμπλέκονται στην υλοποίηση του αλγορίθμου είναι πιο σφιχτοί από ότι στον αλγόριθμο DESCARTES και συνεπώς πιο γρήγοροι στην πράξη. Τέλος, ο έλεγχος για το πλήθος των ριζών είναι πολύ πιο απλοποιημένος από αυτόν του DESCARTES.

Κατά τα λοιπά ο αλγόριθμος ομοιάζει με τον DESCARTES. Αρχικά το πολυώνυμο αναπαρίσταται στη βάση Bernstein στο διάστημα $\mathcal{I}_0$. Στο βήμα h του αλγορίθμου πρέπει να εξεταστεί το ζεύγος $\{f, \mathcal{I}\}$. Οι ρίζες του προς εξέταση πολυωνύμου f στο $\mathcal{I}$ αντιστοιχούν στις ρίζες του A_{red} στο $\mathcal{I}$. Αν το f έχει περισσότερες από μία ρίζες τότε υπολογίζονται δύο υποδιαστήματα του $\mathcal{I}$, τα $\mathcal{I}_L$ και $\mathcal{I}_R$ και η αναπαράσταση του f στη βάση Bernstein στα δύο αυτά υποδιαστήματα χρησιμοποιώντας τις απεικονίσεις (2.20) και (2.21) και ο αλγόριθμος επαναλαμβάνεται.

Το ότι ο αλγόριθμος τερματίζει εξασφαλίζεται, όπως και στην περίπτωση του DESCARTES, από τα θεωρήματα του ενός και των δύο κύκλων (Θεωρ. 3.32 και Θεωρ. 3.33) και από το ότι το $\mathbb{Q}$ είναι Αρχιμήδειο.

- INITIALIZATION$_{\text{BERNSTEIN}}$ (Αλγ. 10)
  Η αρχικοποίηση του αλγορίθμου συνίσταται στο να αναπαραστήσουμε το A_{red} στη βάση Bernstein στο διάστημα $\mathcal{I}$. Η μετατροπή απαιτεί $\mathcal{O}(d^2)$ αριθμητικές πράξεις και οι συντελεστές του νέου πολυωνύμου έχουν δυαδικό μήκος $\mathcal{O}(d\tau)$, δείτε Εν. 2.4 και [203, 205].

  Άρα το κόστος της αρχικοποίησης είναι φραγμένο από $\widetilde{\mathcal{O}}_B(d^3\tau)$. Το νέο πολυώνυμο στη βάση Bernstein θα το συμβολίσουμε ξανά με A_{red} προκειμένου να μην επιβαρύνουμε τον συμβολισμό.

- COUNT$_{\text{BERNSTEIN}}$ (Αλγ. 11)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Για το f ισχύει ότι $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$.

  Η συνάρτηση $\texttt{VAR}(f) = \texttt{VAR}(b_0, \ldots, b_d)$ απαιτεί $\mathcal{O}(d)$ αριθμητικές πράξεις ή $\widetilde{\mathcal{O}}_B\left(d(d\tau + dh)\right)$.

- SPLIT$_{\text{BERNSTEIN}}$ (Αλγ. 12)
  Θεωρούμε ότι βρισκόμαστε σε βάθος h στο δένδρο διαμέρισης και έστω ότι το προς εξέταση ζεύγος είναι $\{f, \mathcal{I}\}$. Για το f ισχύει ότι $\mathcal{L}(f) = \mathcal{O}(d\tau + dh)$, όπως ακριβώς και στον αλγόριθμο DESCARTES.

  Υπολογίζουμε τις αναπαραστάσεις του f στη βάση Bernstein για τα διαστήματα $\mathcal{I}_L$ και $\mathcal{I}_R$, f_L και f_R, χρησιμοποιώντας τις απεικονίσεις (2.20) και (2.21), με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d(d + d\tau + d\,h)) = \widetilde{\mathcal{O}}_B(d^3 + d^2\tau + d^2h)$ (Πρότ. 2.36).

Το δένδρο διαμέρισης

Προκειμένου να ολοκληρώσουμε την ανάλυση πολυπλοκότητας των αλγορίθμων υποδιαίρεσης πρέπει να υπολογίσουμε το πλήθος των βημάτων που εκτελούν. Υπενθυμίζουμε ότι αλγόριθμοι υποδιαίρεσης ακολουθούν τη φιλοσοφία του αλγορίθμου της δυαδικής αναζήτησης. Κατά συνέπεια, μπορούμε να υποθέσουμε ένα δυαδικό δένδρο, έστω T, ανάλογο με αυτό της δυαδικής αναζήτησης, το οποίο στη ρίζα του έχει το αρχικό διάστημα, $\mathcal{I}_0$ που περιέχει όλες τις πραγματικές ρίζες του A_{red} και το οποίο υποδιαιρείται κατά την εκτέλεση των αλγορίθμων. Το δένδρο αυτό το ονομάζουμε *δένδρο διαμέρισης*. Ο αριθμός των βημάτων που εκτελούν οι αλγόριθμοι υποδιαίρεσης ισούται με το πλήθος των κόμβων του δένδρου διαμέρισης, το οποίο συμβολίζουμε με $\#(T)$. Σε κάθε κόμβο του T αντιστοιχούμε ένα υποδιάστημα του $\mathcal{I}_0$. Παρατηρούμε ότι τα διαστήματα που αντιστοιχούν σε κόμβους στο ίδιο βάθος του δένδρου έχουν για άκρα ρητούς αριθμούς με το ίδιο δυαδικό μήκος καθώς έχουν προκύψει μετά από ίσο αριθμό υποδιαιρέσεων. Επίσης, τα φύλλα του δένδρου περιέχουν διαστήματα που περιέχουν είτε μία είτε καμία πραγματική ρίζα του f και το μήκος τους (των διαστημάτων) δεν είναι μικρότερο από το διάστημα απομόνωσης. Στόχος μας είναι να φράξουμε το $\#(T)$.

Έστω $\mathfrak{I}$ το σύνολο των διαστημάτων τα οποία έχουν δύο παιδιά φύλλα στο δένδρο διαμέρισης. Εκ κατασκευής, αν $\mathcal{I} \in \mathfrak{I}$ τότε $\text{COUNT}_{\text{SM}}(f, \mathcal{I}) \geq 2$, γιατί αλλιώς δεν υπήρχε λόγος να το υποδιαιρέσουμε περαιτέρω. Ωστόσο, για τα δύο παιδιά του $\mathcal{I}$, έστω $\mathcal{I}_L$ και $\mathcal{I}_R$, ισχύει $\text{COUNT}_{\text{SM}}(f_L, \mathcal{I}_L) \in \{0, 1\}$, αντίστοιχα $\text{COUNT}_{\text{SM}}(f_R, \mathcal{I}_R) \in \{0, 1\}$, επειδή είναι φύλλα στο δένδρο διαμέρισης. Αν ενδιαφερόμαστε μόνο για τον αλγόριθμο STURM τότε ισχύουν οι πιο αυστηρές σχέσεις $\text{COUNT}_{\text{STURM}}(f, \mathcal{I}) = 2$ και $\text{COUNT}_{\text{STURM}}(f_L, \mathcal{I}_L) = \text{COUNT}_{\text{STURM}}(f_R, \mathcal{I}_R) = 1$, επειδή ο αλγόριθμος αυτός μετρά ακριβώς το πλήθος των ριζών σε κάποιο διάστημα.

Παρατηρούμε ότι $|\mathfrak{I}|$ είναι μικρότερο ή ίσο από $\text{COUNT}_{\text{SM}}(A_{red}, \mathcal{I}_0)$, καθώς σε κάθε διαμέριση το άθροισμα των εναλλαγών προσήμων του f δεν αυξάνεται και για τους τρεις αλγορίθμους. Ειδικά για τον αλγόριθμο BERNSTEIN, δείτε [14, 203, 205]. Πιο συγκεκριμένα ισχύει $|\mathfrak{I}| \leq \text{COUNT}_{\text{SM}}(A_{red}, \mathcal{I}_0) \leq d$.

Αν για κάποια (μιγαδική) ρίζα του f, έστω α, το πραγματικό της μέρος ανήκει σε ένα διάστημα $\mathcal{I}$, $\Re(\alpha) \in \mathcal{I}$, τότε θα τη συμβολίζουμε με $\alpha_{\mathcal{I}}$. Μπορούμε να αποδείξουμε την ακόλουθη πρόταση, η οποία είναι σημαντική από μόνη της και θα μας βοηθήσει στο να φράξουμε το πλήθος των διαμερίσεων.

Πρόταση 3.37. *Έστω $\mathcal{I} \in \mathfrak{I}$. Υπάρχουν δύο διαφορετικές (μιγαδικές) ρίζες $\alpha_{\mathcal{I}} \neq \beta_{\mathcal{I}}$ του f τέτοιες ώστε $|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| < 2\,|\mathcal{I}|$.*

Απόδειξη: Θεωρούμε ένα διάστημα $\mathcal{I} \in \mathfrak{I}$, τα δύο παιδιά του $\mathcal{I}_L$ και $\mathcal{I}_R$ στο δένδρο διαμέρισης και τα πολυώνυμα f_L και f_R που αντιστοιχούν σε αυτά. Υπάρχουν οι ακόλουθες περιπτώσεις σχετικά με τις εναλλαγές προσήμων των f_L και f_R στα δύο υποδιαστήματα $\mathcal{I}_L$ και $\mathcal{I}_R$:

- $(1, 1)$: για όλους τους αλγορίθμους, υπάρχουν δύο, διαφορετικές μεταξύ τους, πραγματικές ρίζες $\alpha \in \mathcal{I}_L$ και $\beta \in \mathcal{I}_R$ στο διάστημα $\mathcal{I}$. Συνεπώς $|\alpha - \beta| \leq |\mathcal{I}|$. Αυτή είναι και η μοναδική περίπτωση για τον αλγόριθμο STURM.

- $(0, 0)$: αυτή η περίπτωση μπορεί να παρουσιαστεί μόνο στους αλγορίθμους DESCARTES και BERNSTEIN. Εφόσον ισχύει $\text{COUNT}_{\text{SM}}(f, \mathcal{I}) \geq 2$, από το θεώρημα του ενός κύκλου

(Θεωρ. 3.32) συνεπάγεται ότι υπάρχουν δύο συζυγείς μιγαδικές ρίζες $\beta, \overline{\beta}$ στον δίσκο $D(m(\mathcal{I}), \frac{|\mathcal{I}|}{2})$. Συνεπώς $|\beta - \overline{\beta}| \leq |\mathcal{I}|$.

- $(1,0)$ ή $(0,1)$: αυτή η περίπτωση μπορεί να παρουσιαστεί μόνο στους αλγορίθμους DESCARTES και BERNSTEIN. Υπάρχει μία πραγματική ρίζα α στο $\mathcal{I}$. Εφόσον $\text{COUNT}_{\text{SM}}(f, \mathcal{I}) \geq 2$, από το θεώρημα των δύο κύκλων (Θεωρ. 3.33) υπάρχουν δύο συζυγείς μιγαδικές ρίζες $\beta, \overline{\beta}$ στην ένωση των δίσκων $D(m(\mathcal{I}) \pm \frac{1}{2\sqrt{3}}\mathbf{i}|\mathcal{I}|, \frac{1}{\sqrt{3}}|\mathcal{I}|)$. Η ένωση περιέχεται στο δίσκο με διάμετρο $2\,|\mathcal{I}|$. Συνεπώς $|\beta - \alpha| < 2|\mathcal{I}|$.

Και η πρόταση αποδείχτηκε. ΟΕΔ

Πρόταση 3.38. *Οι αλγόριθμοι διαμέρισης εκτελούν $\mathcal{O}(d^2 + d\,\tau)$ βήματα.*

Απόδειξη: Ο αριθμός των βημάτων που εκτελούν οι αλγόριθμοι διαμέρισης ισούται με το πλήθος των κόμβων του δένδρου διαμέρισης, τον οποίο θα συμβολίσουμε με $\#(T)$.

Παρατηρούμε ότι το $\#(T)$ είναι μικρότερο ή ίσο από δύο φορές το άθροισμα των κόμβων που περιέχονται στο μονοπάτι από κάθε $\mathcal{I} \in \mathfrak{I}$ στη ρίζα του δένδρου. Επιπρόσθετα το πλήθος των κόμβων στο μονοπάτι από $\mathcal{I} \in \mathfrak{I}$ στη ρίζα του δένδρου διαμέρισης είναι $\lg \frac{|\mathcal{I}_0|}{|\mathcal{I}|}$. Συνεπώς

$$\begin{aligned}
\#(T) &\leq 2 \sum_{\mathcal{I} \in \mathfrak{I}} \lg \frac{|\mathcal{I}_0|}{|\mathcal{I}|} \\
&\leq 2\,|\mathfrak{I}|\ \lg|\mathcal{I}_0| - 2 \sum_{\mathcal{I} \in \mathfrak{I}} \lg|\mathcal{I}| \\
&\leq 2\,|\mathfrak{I}|\ \lg|\mathcal{I}_0| + |\mathfrak{I}| - \sum_{\mathcal{I} \in \mathfrak{I}} \lg|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| \\
&\leq 2\,|\mathfrak{I}|\ \lg|\mathcal{I}_0| + |\mathfrak{I}| - \lg \prod_{\mathcal{I} \in \mathfrak{I}} |\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}|
\end{aligned} \tag{3.5}$$

όπου στην προτελευταία ανισότητα χρησιμοποιήσαμε το γεγονός ότι από την Εν. 3.37 ισχύει

$$|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| \leq 2\,|\mathcal{I}| \Rightarrow 1 - \lg|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}| \geq -\lg|\mathcal{I}|$$

Για το αρχικό διάστημα $\mathcal{I}_0$, χρησιμοποιώντας ένα από τα απόλυτα φράγματα εγκλεισμού όλων των (πραγματικών) ριζών (Εν. 3.2), ισχύει

$$\mathcal{I}_0 = [-2^\tau, 2^\tau] \Rightarrow \lg|\mathcal{I}_0| = \tau + 1 \tag{3.6}$$

Επίσης, καθώς σε κάθε επίπεδο του δένδρου διαμέρισης δεν μπορούμε να έχουμε περισσότερα από d διαστήματα προς εξέταση, ισχύει

$$|\mathfrak{I}| \leq d \tag{3.7}$$

Προκειμένου να εφαρμόσουμε το Θεωρ. 3.27 στην (3.5), πρέπει να αναδιατάξουμε την ποσότητα $\prod_{\mathcal{I} \in \mathfrak{I}} |\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}|$ έτσι ώστε οι απαιτήσεις για τους δείκτες των ριζών να ικανοποιούνται. Οι προϋποθέσεις του θεωρήματος δεν ικανοποιούνται αν εμφανίζονται συμμετρικά γινόμενα.

Θεωρούμε τη χειρότερη περίπτωση, να εμφανίζονται *μόνο* συμμετρικά γινόμενα, δηλαδή η ποσότητά μας είναι της μορφής $\prod|(\alpha_{\mathcal{I}}-\beta_{\mathcal{I}})(\beta_{\mathcal{I}}-\alpha_{\mathcal{I}})|$. Κατά συνέπεια, θεωρούμε το τετράγωνο της ανισότητας του Θεωρ. 3.27 αντικαθιστώντας την ποσότητα k με $\frac{|\mathcal{I}|}{2}$ και λαμβάνοντας υπ' όψιν ότι $\mathsf{disc}(A_{red})\geq 1$ (αφού το A_{red} είναι χωρίς τετράγωνα), έχουμε

$$\begin{aligned}\prod_{\mathcal{I}\in\mathfrak{I}}|\alpha_{\mathcal{I}}-\beta_{\mathcal{I}}| \;&\geq\; \left(2^{\frac{|\mathcal{I}|}{2}-\frac{d(d-1)}{2}}\,\mathcal{M}(f)^{1-d-\frac{|\mathcal{I}|}{2}}\right)^2\\ -\lg\prod_{I\in\mathfrak{I}}|\alpha_{\mathcal{I}}-\beta_{\mathcal{I}}| \;&\leq\; d^2-d+|\mathfrak{I}|+(2d+|\mathfrak{I}|-2)\lg\mathcal{M}(f)\end{aligned}\tag{3.8}$$

Λαμβάνοντας υπόψιν ότι $\lg\mathcal{M}(f)\leq\tau+\frac{1}{2}\lg(d+1)$ (Λημ. 3.4) και συνδυάζοντας τις εξισώσεις (3.6), (3.7) και (3.8) με την εξίσωση (3.5) έχουμε ότι

$$\#(T)\leq 2\,d\,(\tau+1)+d+d^2+(3d-1)(\tau+\frac{1}{2}\lg(d+1))$$

Και τελικά $\#(T)=\mathcal{O}(d^2+d\tau+d\lg d)$. ΟΕΔ

Σημείωση 3.39. *Μπορεί να αποδειχτεί ότι $\#(T)=\mathcal{O}(d\tau+d\lg d)$, χρησιμοποιώντας το Θεωρ. 3.26 και έτσι να γλυτώσουμε έναν παράγοντα d^2 [65, 76, 81, 91, 97]. Ωστόσο η απόδειξη είναι πολύ πιο δύσκολη σε αυτή την περίπτωση καθώς απαιτείται να αποδείξουμε ότι πάντοτε μπορούμε να αναδιατάξουμε τα γινόμενα των ριζών στην* (3.8) *με τέτοιο τρόπο ώστε οι απαιτήσεις του Θεωρ. 3.26 να ικανοποιούνται. Επιπρόσθετα, ο παράγοντας d^2 δεν παίζει κανένα ρόλο όταν $d=\mathcal{O}(\tau)$ ή όταν το πολυώνυμο που επιλύουμε δεν είναι χωρίς τετράγωνα.*

Πολυπλοκότητα των αλγορίθμων υποδιαίρεσης

Θα αποδείξουμε ότι η πολυπλοκότητα των αλγορίθμων υποδιαίρεσης είναι $\widetilde{\mathcal{O}}_B(d^4\tau^2)$. Υποθέτουμε (καταρχάς) $d=\mathcal{O}(\tau)$ για να απλοποιήσουμε τον συμβολισμό.

Θεώρημα 3.40 (SUBDIVISIONSOLVER**)**

Έστω $A_{red}\in\mathbb{Z}[x]$ χωρίς τετράγωνα, τέτοιο ώστε $\deg(A_{red})=d$ και $\mathcal{L}(A_{red})=\tau$. Οι αλγόριθμοι υποδιαίρεσης STURM, DESCARTES *και* BERNSTEIN *για την απομόνωση των πραγματικών ριζών του A_{red} έχουν πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\,\tau^2)$.*

Επιπρόσθετα το δυαδικό μήκος των ρητών αριθμών που είναι άκρα των διαστημάτων απομόνωσης φράσσεται από $\mathcal{O}(d\,\tau)$.

Απόδειξη: Τα άκρα των διαστημάτων απομόνωσης έχουν δυαδικό μήκος το πολύ $\mathcal{O}(d\tau)$, όπως προκύπτει από το φράγμα διαχωρισμού (Σημ. 3.24). Υπενθυμίζουμε ότι το πλήθος των βημάτων και για τους τρεις αλγορίθμους είναι $\mathcal{O}(d^2+d\tau)$. Εξετάζουμε κάθε αλγόριθμο ξεχωριστά.

- STURM

  Στη χειρότερη περίπτωση πρέπει να αποτιμήσουμε την $\mathbf{SR}(A_{red})$ πάνω σε κάποιο ρη-

τό αριθμό δυαδικού μήκους $\mathcal{O}(d\tau)$. Η πολυπλοκότητα της αποτίμησης είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Θεωρ. 2.32). Εφόσον χρειάζεται να εκτελέσουμε το πολύ $\mathcal{O}(d^2+d\tau)$ τέτοιες αποτιμήσεις (Πρότ. 3.38), το συνολικό κόστος του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^5\tau+d^4\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

- DESCARTES
  Το κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^2\lg d+d^2\tau+d^2h)$ για την συνάρτηση COUNT και $\widetilde{\mathcal{O}}_B(d^2\lg d+d^2\tau+d^2h)$ για τη συνάρτηση SPLIT (Εν. 3.5). Το συνολικό κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^2\lg d+d^2\tau+d^2h)$.

  Αθροίζοντας πάνω σε όλα τα βήματα του αλγορίθμου που είναι $\sum h = \widetilde{\mathcal{O}}_B(d^2+d\tau)$ (Πρότ. 3.38), συμπεραίνουμε ότι η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^6+d^5\tau+d^4\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

- BERNSTEIN
  Το κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^2\tau+d^2h)$ για τη συνάρτηση COUNT και $\widetilde{\mathcal{O}}_B(d^3+d^2\tau+d^2h)$ για τη συνάρτηση SPLIT (Εν. 3.5). Το συνολικό κόστος στο βήμα h είναι $\widetilde{\mathcal{O}}_B(d^3+d^2\tau+d^2h)$.

  Αθροίζοντας πάνω σε όλα τα βήματα του αλγορίθμου που είναι $\sum h = \widetilde{\mathcal{O}}_B(d^2+d\tau)$ (Πρότ. 3.38), συμπεραίνουμε ότι η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(d^6+d^5\tau+d^4\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

Και το θεώρημα αποδείχτηκε. ΟΕΔ

Όταν πρέπει να απομονώσουμε τις πραγματικές ρίζες ενός πολυωνύμου A, το οποίο δεν είναι χωρίς τετράγωνα και/ή θέλουμε να υπολογίσουμε τις πολλαπλότητες των πραγματικών ριζών τότε μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο REALROOTSOLVER (Αλγ. 1) αντικαθιστώντας τη συνάρτηση REALROOTISOLATOR με κάποιον από τους αλγορίθμους STURM, DESCARTES ή BERNSTEIN. Η πολυπλοκότητα του REALROOTSOLVER είναι το μέγιστο ανάμεσα στην πολυπλοκότητα του REALROOTISOLATOR και του $\widetilde{\mathcal{O}}_B(d^3\tau)$. Επιπρόσθετα θα πρέπει να λάβουμε υπόψιν μας ότι το δυαδικό μήκος του A_{red} είναι $\mathcal{O}(d+\tau)$ (Θεωρ. 2.34) καθώς αντιπροσωπεύει το μέγιστο δυαδικό μήκος των συντελεστών του χωρίς τετράγωνα μέρους του πολυωνύμου A.

Μπορούμε να διατυπώσουμε το ακόλουθο πιο γενικό θεώρημα.

Θεώρημα 3.41 (REALROOTSOLVER)

Έστω $A\in\mathbb{Z}[X]$ τέτοιο ώστε $\deg(A)=d$ και $\mathcal{L}(A)=\tau$, όχι απαραίτητα χωρίς τετράγωνα. Η πολυπλοκότητα του αλγορίθμου REALROOTSOLVER *για την απομόνωση και τον υπολογισμό των πολλαπλοτήτων των πραγματικών ριζών του A, χρησιμοποιώντας ως* REALROOTISOLATOR *οποιουδήποτε από τους αλγορίθμους* STURM, DESCARTES *και* BERNSTEIN *είναι $\widetilde{\mathcal{O}}_B(d^6+d^5\,\tau+d^4\,\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ αν $d=\mathcal{O}(\tau)$.*

Επιπρόσθετα, το δυαδικό μήκος των ρητών αριθμών που είναι άκρα των διαστημάτων απομόνωσης φράσσεται από $\mathcal{O}(d\,\tau)$.

Σημείωση 3.42. *Αν θεωρήσουμε ότι* $N = \max\{d, \tau\}$*, τότε η πολυπλοκότητα των παραπάνω αλγορίθμων είναι* $\widetilde{\mathcal{O}}_B(N^6)$*. Υπενθυμίζουμε ότι η πολυπλοκότητα των αριθμητικών (προσεγγιστικών) αλγορίθμων είναι* $\widetilde{\mathcal{O}}_B(d^3\tau) = \widetilde{\mathcal{O}}_B(N^4)$*.*

Όσον αφορά τους αλγορίθμους DESCARTES και BERNSTEIN θα μπορούσαμε να μην υπολογίσουμε το χωρίς τετράγωνα μέρος του A_{red}. Σε αυτή την περίπτωση θα βασιζόμασταν σε μια γενίκευση του θεωρήματος του Vincent (Θεωρ. 3.43), η οποία οφείλεται στο Wang [6]. Χρησιμοποιώντας αυτό το θεώρημα μπορούμε να συνεχίσουμε τις υποδιαιρέσεις μέχρι να φτάσουμε το φράγμα διαχωρισμού. Τότε ο αριθμός των εναλλαγών προσήμων θα υποδήλωνε την πολλαπλότητα της πραγματικής ρίζας που θα είχαμε απομονώσει.

Η προσέγγιση αυτή αν και σημαντική γιατί καταρρίπτει την μέχρι σήμερα γνωστή υπόθεση ότι οι οι αλγόριθμοι που στηρίζονται στον κανόνα προσήμων του Descartes πρέπει να απαιτούν πολυώνυμο χωρίς τετράγωνα, δεν συνίσταται για πρακτικές εφαρμογές καθώς είναι πολύ δαπανηρό υπολογιστικά να απαιτήσουμε να υποδιαιρέσεις μέχρι το θεωρητικό φράγμα διαχωρισμού, δείτε Σημ. 3.24.

3.6 Ο αλγόριθμος των συνεχών κλασμάτων

Εισαγωγή στα συνεχή κλάσματα

Παρουσιάζουμε μια γρήγορη επισκόπηση των συνεχών κλασμάτων η οποία αν και απέχει παρασάγκας από το να χαρακτηριστεί πλήρης ικανοποιεί τις ανάγκες μας. Η παρουσίασή μας ακολουθεί τον van der Poorten [256]. Για μια πιο λεπτομερή παρουσίαση ο αναγνώστης μπορεί να ανατρέξει για παράδειγμα στους Akritas [5], Bombieri and van der Poorten [31], Khintchine [155], van der Poorten [256], Yap [275].

Ένα *απλό συνεχές κλάσμα* (*simple or regular continued fraction*) είναι μια (πιθανά άπειρη) έκφραση της μορφής

$$c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \dots}} = [c_0, c_1, c_2, \dots]$$

όπου οι αριθμοί c_i ονομάζονται *μερικά πηλίκα* (*partial quotients*), $c_i \in \mathbb{Z}$ και $c_i \geq 1$ για $i > 0$. Παρατηρούμε ότι το c_0 μπορεί να είναι είτε θετικός είτε αρνητικός αριθμός, ωστόσο για τον αλγόριθμο που θα παρουσιάσουμε μπορούμε να υποθέσουμε ότι $c_0 \geq 0$. Θεωρώντας τις αναδρομικές σχέσεις

$$\begin{aligned} P_{-1} &= 1, \quad P_0 = c_0, \quad P_{n+1} = c_{n+1}\,P_n + P_{n-1} \\ Q_{-1} &= 0, \quad Q_0 = 1, \quad Q_{n+1} = c_{n+1}\,Q_n + Q_{n-1} \end{aligned}$$

μπορεί να δειχτεί με επαγωγή ότι $R_n = \frac{P_n}{Q_n} = [c_0, c_1, \dots, c_n]$, για $n = 0, 1, 2, \dots$ και επίσης ότι

$$\begin{aligned} P_n\,Q_{n+1} - P_{n+1}\,Q_n &= (-1)^{n+1} \\ P_n\,Q_{n+2} - P_{n+2}\,Q_n &= (-1)^{n+1} c_{n+2} \end{aligned}$$

Αν $\gamma = [c_0, c_1, \dots]$ τότε

$$\gamma = c_0 + \frac{1}{Q_0 Q_1} - \frac{1}{Q_1 Q_2} + \cdots = c_0 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{Q_{n-1} Q_n}$$

και καθώς η προηγούμενη σχέση είναι μια σειρά από αριθμούς που συνεχώς μειώνονται και έχουν εναλλασσόμενα πρόσημα, συμπεραίνουμε ότι συγκλίνει σε έναν πραγματικό αριθμό γ. Ένα πεπερασμένο τμήμα $R_n = \frac{P_n}{Q_n} = [c_0, c_1, \dots, c_n]$ ονομάζεται $n-$οστό *αναγώγημα* (*convergent* ή *approximant*) του γ και η ουρά $\gamma_{n+1} = [c_{n+1}, c_{n+2}, \dots]$ είναι γνωστή ως *ολικό πηλίκο* (*complete quotients*). Δηλαδή ισχύει $\gamma = [c_0, c_1, \dots, c_n, \gamma_{n+1}]$ για $n = 0, 1, 2, \dots$. Υπάρχει μία '1-1' αντιστοιχία μεταξύ των πραγματικών αριθμών και συνεχών κλασμάτων, όπου τα πεπερασμένα συνεχή κλάσματα αντιστοιχούν σε ρητούς αριθμούς.

Είναι γνωστό ότι $Q_n \geq F_{n+1}$ και ότι $F_{n+1} < \phi^n < F_{n+2}$, όπου F_n είναι ο $n-$οστός όρος Fibonacci και $\phi = \frac{1+\sqrt{5}}{2}$ ο *χρυσός λόγος* (*golden ratio*). Τα συνεχή κλάσματα είναι η καλύτερη (για δεδομένο μέτρο παρανομαστή) προσέγγιση, δηλαδή

$$\frac{1}{Q_n(Q_{n+1} + Q_n)} \leq \left| \gamma - \frac{P_n}{Q_n} \right| \leq \frac{1}{Q_n Q_{n+1}} \leq \frac{1}{Q_n^2} < \phi^{-2n}$$

Ισχύει επίσης και η λιγότερο ακριβής σχέση:

$$\left| \gamma - \frac{P_n}{Q_n} \right| < \frac{1}{c_{n+1} Q_n^2}$$

Έστω $\gamma = [c_0, c_1, \dots]$ η ανάπτυξη σε συνεχές κλάσμα ενός πραγματικού αριθμού. Η κατανομή Gauss-Kuzmin [31, 224] δηλώνει ότι για σχεδόν όλους τους πραγματικούς αριθμούς γ (το σύνολο των εξαιρέσεων έχει Lebesque μέτρο μηδέν) η πιθανότητα ένας θετικός ακέραιος δ να εμφανίζεται στην ανάπτυξη σε συνεχές κλάσμα του γ είναι

$$\mathbf{Prob}[c_i = \delta] = \lg \frac{(\delta+1)^2}{\delta(\delta+2)}, \quad i > 0 \tag{3.9}$$

Η κατανομή Gauss-Kuzmin δεν μας επιτρέπει να φράξουμε τη μέση τιμή των μερικών πηλίκων ή με άλλα λόγια η αναμενόμενη τιμή (μέσος όρος) των μερικών πηλίκων αποκλίνει, δηλαδή

$$\mathbf{E}[c_i] = \sum_{\delta=1}^{\infty} \delta \, \mathbf{Prob}[c_i = \delta] = \infty,$$

για κάθε $i > 0$. Παρ' όλα αυτά ο γεωμετρικός αλλά και ο αρμονικός μέσος όχι μόνο φράσσονται ασυμπτωτικά αλλά φράσσονται και από μία σταθερά. Για την περίπτωση του γεωμετρικού μέσου αυτή η σταθερά είναι η περίφημη σταθερά Khintchine [155], όπου

$$\lim_{n \to \infty} \sqrt[n]{\prod_{i=1}^{n} c_i} = \mathcal{K} = 2.685452001\ldots$$

και για την οποία σταθερά δεν είναι γνωστό αν είναι άρρητος ή υπερβατικός αριθμός. Ο αναγνώστης μπορεί να ανατρέξει στην εργασία των Bailey et al. [12] όπου υπάρχει μια εμπεριστατωμένη

μελέτη των λεγόμενων *Khintchine's means*. Η αναμενόμενη τιμή του δυαδικού μήκους των μερικών πηλίκων είναι σταθερή για σχεδόν όλους τους αλγεβρικούς αριθμούς, όταν $n \to \infty$ ή n αρκετά μεγάλο [155, 224]. Ακολουθώντας προσεκτικά τους Richtmyer et al. [224], έχουμε:

$$\mathbf{E}[\ln c_i] = \frac{1}{n}\sum_{i=1}^{n} \ln c_i = \ln K = 0.98785...,$$

καθώς $n \to \infty$, $\forall i > 0$. Αν $\mathcal{L}(c_i) \triangleq b_i$, τότε

$$\mathbf{E}[b_i] = \mathcal{O}(1) \tag{3.10}$$

Ένας πραγματικός αριθμός έχει (τελικά) περιοδική ανάπτυξη σε συνεχές κλάσμα αν και μόνο αν είναι πραγματική ρίζα ενός πολυωνύμου δευτέρου βαθμού. Το σύνολο των πραγματικών αλγεβρικών αριθμών είναι Lebesque μέτρου 0 και ενδεχομένως τόσο η κατανομή Gauss–Kuzmin όσο και ο νόμος του Khintchine να μην ισχύει στο $\mathbb{R}_{alg}$. Όπως τονίζουν οι Brent, van der Poorten, and Riele [33]: "There is no reason to believe that the continued fraction expansions of non-quadratic algebraic irrationals generally do anything other than faithfully follow Khintchine's law"[2]. Επιπρόσθετα, ένα πλήθος πειραματικών αποτελεσμάτων [31, 224, 228] επιβεβαιώνει τον ισχυρισμό, ότι τόσο η κατανομή Gauss-Kuzmin όσο και ο νόμος του Khintchine είναι εν ισχύ στην ανάπτυξη σε συνεχές κλάσμα των πραγματικών αλγεβρικών αριθμών, βαθμού > 2. Αποτελεί τεράστια μαθηματική πρόκληση η θεωρητική κατάρριψη ή απόδειξη του ισχυρισμού. Σχετικά με το μεγαλύτερο αριθμό που μπορεί να εμφανιστεί στην ανάπτυξη σε συνεχές κλάσμα ενός ρητού αριθμού ο αναγνώστης μπορεί να ανατρέξει στην εργασία του Hensley [132].

Αξίζει να τονίσουμε ότι αν και στηριζόμαστε στην εικασία ότι τα μερικά πηλίκα των πραγματικών αλγεβρικών αριθμών είναι μη φραγμένου μέτρου, αυτή είναι η χειρότερη δυνατή περίπτωση. Αν αποδειχτεί ότι φράσσονται τότε αυτό μπορεί να οδηγήσει μόνο σε βελτίωση της πολυπλοκότητας του αλγορίθμου CF που εξετάζουμε.

Περιγραφή του αλγορίθμου CF

Ο αλγόριθμος CF εξαρτάται από το ακόλουθο θεώρημα, το οποίο παρουσιάστηκε από τον Vincent το 1836 [261]. Το αντίστροφο του Θεωρ. 3.43 εξασφαλίζει τον τερματισμό του CF και ο αναγνώστης μπορεί να ανατρέξει στους Akritas [5], Collins and Loos [55], Mignotte [187]. Ένα πολύ ενδιαφέρον ερώτημα είναι εάν τα θεωρήματα του ενός και των δύο κύκλων (Θεωρ. 3.32 και Θεωρ. 3.33) που χρησιμοποιούνται για την ανάλυση του τερματισμού των αλγορίθμων υποδιαίρεσης μπορούν να χρησιμοποιηθούν και ίσως να βελτιώσουν την πολυπλοκότητα του CF. Η απόδειξη του Θεωρ. 3.43 υπάρχει στις εργασίες των Akritas [5], Alesina and Galuzzi [6], Uspensky [255]. Για μια πιο σύγχρονη και κομψή εκδοχή του θεωρήματος του Vincent, ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στους Alesina and Galuzzi [6].

Θεώρημα 3.43

Έστω $A_{red} \in \mathbb{Z}[X]$, χωρίς τετράγωνα, τέτοιο ώστε $\deg(A_{red}) = d$ *και έστω* $\Delta > 0$ *το φράγμα*

[2] Ελεύθερη μετάφραση: Δεν συντρέχει κανένας λόγος που να μας κάνει να πιστεύουμε ότι οι μη τετραγωνικοί αλγεβρικοί αριθμοί δεν ακολουθούν πιστά τον νόμο του Khintchine.

Algorithm 13: CF (A, M, L)

Input: $A \in \mathbb{Z}[X]$, $M(X) = \frac{kX+l}{mX+n}$, $k, l, m, n \in \mathbb{Z}$
Output: A list of isolating intervals

```
1  if A(0) = 0 then
2      L ← ADD(L, [M(0), M(0)]) ;
3      A ← A(X)/X;
4      CF(A, M, L);
5  V ← VAR(A);
6  if V = 0 then RETURN ;
7  if V = 1 then
8      L ← ADD(L, [M(0), M(∞)]) ;
9      RETURN ;
10 b ← PLB(A) // PLB ≡ POSITIVELOWERBOUND ;
11 if b > 1 then A ← A(b + X), M ← M(b + X) ;
12 A_1 ← A(1 + X), M_1 ← M(1 + X) ;
13 CF(A_1, M_1, L) // Looking for real roots in (1, +∞);
14 A_2 ← A(1/(1+X)), M_2 ← M(1/(1+X)) ;
15 CF(A_2, M_2, L) // Looking for real roots in (0, 1) ;
16 RETURN ;
```

διαχωρισμού του. Έστω n ο μεγαλύτερος δείκτης, τέτοιος ώστε

$$F_{n-1}\Delta > 2 \quad \textit{και} \quad F_{n-1}F_n\Delta > 1 + \frac{1}{\epsilon_d}$$

όπου F_n είναι ο n-οστός όρος της ακολουθίας Fibonnaci και $\epsilon_d = \left(1 + \frac{1}{d}\right)^{\frac{1}{d-1}} - 1$. Η απεικόνιση $X \mapsto [c_0, c_1, \ldots, c_n, X]$, όπου $c_0, c_1, \ldots, c_n$ είναι μια αυθαίρετη ακολουθία θετικών ακεραίων μετασχηματίζει το $A_{red}(X)$ στο $A_n(X)$, το οποίο δεν έχει παραπάνω από μία εναλλαγή προσήμων.

Σημείωση 3.44. *Καθώς ισχύει ότι $\frac{3}{4d^2} < \epsilon_d < \frac{4}{d^2}$ [55] συνάγουμε ότι $\frac{1}{\epsilon_d} + 1 < 2d^2$ για $d \geq 2$. Κατά συνέπεια, εάν $d \geq 2$ μπορούμε να αντικαταστήσουμε τις δύο συνθήκες του Θεωρ. 3.43 από την $F_{n-1}\Delta \geq 2d^2$, καθώς $F_n \geq F_{n-1} \geq 1$ και $F_{n-1}F_n\Delta \geq F_{n-1}\Delta \geq 2d^2 > 2$.*

Το Θεώρ. 3.43 μπορεί να χρησιμοποιηθεί προκειμένου να απομονώσουμε τις θετικές πραγματικές ρίζες ενός πολυωνύμου A_{red}, χωρίς τετράγωνα. Προκειμένου να απομονώσουμε τις αρνητικές πραγματικές ρίζες εφαρμόζουμε τον μετασχηματισμό $X \mapsto -X$ στο πολυώνυμο και επαναλαμβάνουμε τον αλγόριθμο. Συνεπώς σε ό,τι ακολουθεί θα υποθέσουμε ότι αναφερόμαστε μόνο στις θετικές πραγματικές ρίζες του A_{red}.

Η παραλλαγή του Vincent για τον αλγόριθμο CF είναι η ακόλουθη: Ένα πολυώνυμο A μετασχηματίζεται σε A_1 με την απεικόνιση $X \mapsto 1 + X$ και αν $\mathtt{VAR}(A_1) = 0$ ή $\mathtt{VAR}(A_1) = 1$ τότε το A έχει 0, αντίστοιχα 1, πραγματική ρίζα μεγαλύτερη από 1 (Θεώρ. 3.28 και Σημ. 3.29). Αν $\mathtt{VAR}(A_1) < \mathtt{VAR}(A)$ τότε (πιθανώς) υπάρχουν πραγματικές ρίζες του A στο $(0, 1)$, όπως προκύπτει από το Θεώρημα του Budan (Θεωρ. 3.31). Το A_2 παράγεται εφαρμόζοντας την απεικόνιση $X \mapsto 1/(1+X)$ στο A, αν $\mathtt{VAR}(A_2) = 0$ ή $\mathtt{VAR}(A_2) = 1$ τότε το A έχει 0, αντίστοιχα 1, πραγματική ρίζα μεγαλύτερη από 1 (Θεώρ. 3.28 και Σημ. 3.29).

Η παραλλαγή του Uspensky [255] για τον αλγόριθμο CF, δείτε επίσης [228], σε κάθε βήμα παράγει και τα δύο πολυώνυμα A_1 και A_2, πιθανώς όπως αναφέρει ο Akritas [1], επειδή δεν γνώριζε το Θεώρημα του Budan (Θεώρ. 3.31). Και στις δύο παραλλαγές, αν το μετασχηματισμένο πολυώνυμο έχει παραπάνω από μία ενναλλαγή προσήμων τότε επαναλαμβάνουμε τη διδαδικασία.

Ας θεωρήσουμε την όλη διαδικασία του CF αλγορίθμου ως ένα άπειρο δυαδικό δένδρο του οποίου η ρίζα αντιστοιχεί στο αρχικό πολυώνυμο A_{red}. Μια διακλάδωση από ένα κόμβο σε ένα δεξί παιδί αντιστοιχεί στον μετασχηματισμό $X \mapsto X + 1$, ενώ προς σε ένα αριστερό παιδί στον μετασχηματισμό $X \mapsto \frac{1}{1+X}$. Παρατηρούμε ότι μια ακολουθία από c μετασχηματισμούς $X \mapsto 1 + X$ ακολουθούμενη από έναν του τύπου $X \mapsto 1/(1 + X)$ είναι ισοδύναμη με δύο μετασχηματισμούς: έναν του τύπου $X \mapsto c + 1/X$ ακολουθούμενο από $X \mapsto 1 + X$. Κατά συνέπεια ο αλγόριθμος του Vincent (και του Uspensky) είναι μια ακολουθία από μετασχηματισμούς όπως αυτοί του Θεώρ. 3.43 και άρα το δένδρο είναι πεπερασμένο. Στα φύλλα, του δυαδικού δένδρου που έχουμε υποθέσει, αντιστοιχούν (μετασχηματισμένα) πολυώνυμα τα οποία έχουν το πολύ μία εναλλαγή προσήμων, αν το Θεώρ. 3.43 ισχύει. Ο Akritas [2], δείτε επίσης [5], αντικατέστησε μια σειρά από μετασχηματισμούς $X \mapsto X + 1$ με έναν μετασχηματισμό του τύπου $X \mapsto X + b$, όπου το b είναι ένα θετικό κάτω φράγμα (PLB) στις θετικές πραγματικές ρίζες του πολυωνύμου που εξετάζουμε. Το φράγμα αυτό υπολογίζεται με κάποιον από τους τύπους της Εν. 3.2. Με αυτό τον τρόπο, ο αριθμός των βημάτων του CF αλγόριθμου είναι πολυωνυμικός και η πολυπλοκότητά του είναι $\widetilde{\mathcal{O}}_B(d^5\tau^3)$. Ωστόσο, δεν είναι προφανές εάν και πώς η ανάλυση της πολυπλοκότητας λαμβάνει υπόψιν της ότι οι συντελεστές του πολυωνύμου μεγαλώνουν μετά από ένα μετασχηματισμό μετατόπισης. Ένα ακόμα σημαντικό ζήτημα είναι το μέτρο και το δυαδικό μήκος των c_i (μερικών πηλίκων) που εμφανίζονται κατά τη διάρκεια του αλγορίθμου και χρησιμοποιούνται ως παράμετροι μετατόπισης.

Για εκείνα τα πολυώνυμα που έχουν μόνο μία εναλλαγή προσήμου χρειάζεται να υπολογίσουμε το διάστημα όπου κείται η πραγματική ρίζα του αρχικού πολυωνύμου A_{red}. Ας θεωρήσουμε ένα πολυώνυμο A_n το οποίο αντιστοιχεί σε ένα φύλλο του δυαδικού δένδρου του αλγορίθμου και το οποίο έχει μία εναλλαγή προσήμου. Παρατηρούμε ότι το A_n έχει παραχθεί από μετασχηματισμούς σαν και αυτούς του Θεώρ. 3.43, με τη βοήθεια μιας ακολουθίας θετικών ακεραίων $c_0, c_1, \ldots, c_n$. Αυτοί οι μετασχηματισμοί μπορούν να γραφτούν σε πιο συμπαγή μορφή με τη χρήση αναγωγημάτων:

$$M : X \mapsto \frac{P_n X + P_{n-1}}{Q_n X + Q_{n-1}} \tag{3.11}$$

όπου $\frac{P_{n-1}}{Q_{n-1}}$ και $\frac{P_n}{Q_n}$ είναι συνεχόμενα αναγωγήματα του συνεχούς κλάσματος $[c_0, c_1, \ldots, c_n]$. Παρατηρούμε ότι η (3.11) είναι ένας μετασχηματισμός Möbius, για περισσότερες λεπτομέρειες δείτε [5, 275]. Εφόσον το A_n έχει μία εναλλαγή προσήμου. συνεπάγεται ότι έχει μία πραγματική ρίζα στο $(0, \infty)$, συνεπώς προκειμένου να υπολογίσουμε το διάστημα απομόνωσης που αντιστοιχεί στο

αρχικό πολυώνυμο A_{red} αποτιμούμε το δεξί μέλος της (3.11) στο 0 και στο ∞. Τα άκρα (πιθανώς μη διατεταγμένα) του διαστήματος απομόνωσης είναι $\frac{P_{n-1}}{Q_{n-1}}$ και $\frac{P_n}{Q_n}$.

Ο ψευδο-κώδικας του αλγορίθμου CF παρουσιάζεται στον Αλγ. 13.

Η αρχική είσοδος του αλγορίθμου είναι ένα πολυώνυμο $A_{red}(X)$ χωρίς τετράγωνα, ο τετριμμένος μετασχηματισμός $M(X) = X$ και μια κενή λίστα L όπου θα τοποθετηθούν τα διαστήματα απομόνωσης. Χρειαζόμαστε το συναρτησοειδές M προκειμένου να κρατάμε τους μετασχηματισμούς που λαμβάνουν χώρα κατά την εκτέλεση του αλγορίθμου και έτσι να παράγουμε τα διαστήματα απομόνωσης. Η συνάρτηση PLB(A) υπολογίζει ένα θετικό κάτω φράγμα στις θετικές πραγματικές ρίζες του A. Παρατηρούμε ότι οι Γραμμές 14 και 15 στον αλγόριθμο θα έπρεπε να εκτελούνται μόνο όταν $\mathtt{VAR}(A_1) < \mathtt{VAR}(A_2)$, σύμφωνα με το θεώρημα του Budan (Θεωρ. 3.31), αλλά προκειμένου να απλοποιήσουμε την παρουσίαση το παραλείπουμε, καθώς απλά διπλασιάζουν την πολυπλοκότητα.

Σημείωση 3.45. *Υπάρχουν δύο πολύ απλές αλλά πολύ σημαντικές παρατηρήσεις που αφορούν το Θεωρ. 3.43. Όταν το μετασχηματισμένο πολυώνυμο έχει μία εναλλαγή προσήμου, τότε το διάστημα με άκρα $\frac{P_{n-1}}{Q_{n-1}} = [c_0, c_1, \ldots, c_{n-1}]$ και $\frac{P_n}{Q_n} = [c_0, c_1, \ldots, c_n]$ (πιθανώς όχι σε διάταξη) απομονώνουν μια πραγματική ρίζα του A_{red}, έστω γ_i. Τότε, προκειμένου το Θεωρ. 3.43 να ισχύει μπορούμε να θεωρήσουμε αντί του ελάχιστου φράγματος διαχωρισμού Δ, την ποσότητα $|\gamma_i - \gamma_{c_i}|$, όπου γ_{c_i} είναι η (μιγαδική) ρίζα του A_{red} που βρίσκεται πιο κοντά στην ρίζα γ_i.*

Ομοίως, όταν το μετασχηματισμένο πολυώνυμο δεν έχει καμία εναλλαγή προσήμου και τα $\frac{P_{n-1}}{Q_{n-1}}$ και $\frac{P_n}{Q_n}$ απομονώνουν το θετικό πραγματικό μέρος μιας μιγαδικής ρίζας γ_i, τότε επίσης μπορούμε να αντικαταστήσουμε το Δ με $|\gamma_i - \gamma_{c_i}|$.

Θεώρημα 3.46

Ο αλγόριθμος CF *εκτελεί το πολύ $\mathcal{O}(d^2 + d\tau)$ βήματα.*

Απόδειξη: Έστω $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_k|$, $k \leq d$ οι (μιγαδικές) ρίζες του A_{red} με θετικό πραγματικό μέρος και έστω γ_{c_i} η ρίζα του A_{red} που είναι η πλησιέστερη στην γ_i.

Θεωρούμε το δυαδικό δένδρο T που παράγεται από την εκτέλεση του αλγορίθμου CF. Ο αριθμός των βημάτων του αλγορίθμου αντιστοιχεί στο πλήθος των κόμβων του T, και το οποίο πλήθος συμβολίζουμε με $\#(T)$. Θα χρησιμοποιήσουμε μερικά επιχειρήματα και το συμβολισμό από τους Eigenwillig et al. [81] προκειμένου να κλαδέψουμε το δένδρο.

Σε κάθε κόμβο v του T αντιστοιχούμε ένα μετασχηματισμό Möbius, $M_v : X \mapsto \frac{kX+l}{mX+n}$, ένα πολυώνυμο A_v και εμμέσως ένα διάστημα $\mathcal{I}_v$ με πιθανώς μη διατεγμένα άκρα, τα οποία και υπολογίζονται αν αποτιμήσουμε το M_v στο 0 και στο ∞.

Υπενθυμίζουμε ότι το A_v παράγεται εφαρμόζοντας τον μετασχηματισμό M_v στο A_{red}. Στη ρίζα του (δένδρου) T αντιστοιχούμε τα A_{red}, $M(X) = X$ (όπου $k = n = 1, l = m = 0$) και εμμέσως το διάστημα $(0, \infty)$.

Θεωρούμε ότι ένα φύλλο u του T είναι **type-i** αν το (αντίστοιχο) διάστημα $\mathcal{I}_u$ περιέχει $i \geq 0$ πραγματικές ρίζες. Εφόσον ο αλγόριθμος τερματίζει τα φύλλα του δένδρου είναι είτε type-0 είτε type-1. Θα κλαδέψουμε κάποια φύλλα του T προκειμένου να προκύψει ένα συγκεκριμένο

υποδένδρο, έστω T', όπου θα είναι εύκολο να μετρήσουμε τον αριθμό των κόμβων του. Καταρχάς απομακρύνουμε κάθε φύλλο του οποίου ο αδελφός κόμβος δεν είναι φύλλο. Στη συνέχεια θεωρούμε όλα τα φύλλα τα οποία έχουν αδελφούς κόμβους που είναι φύλλα. Εάν και τα δύο (αδελφά) φύλλα είναι type-1 τότε απομακρύνουμε τυχαία ένα από αυτά. Εάν το ένα από αυτά είναι τύπου type-1, τότε απομακρύνουμε το άλλο. Εάν είναι και τα δύο type-0, τότε αυτό σημαίνει ότι στον πατέρα τους αντιστοιχεί ένα πολυώνυμο με τουλάχιστον δύο εναλλαγές προσήμου και ότι προσπαθούμε να απομονώσουμε το θετικό πραγματικό μέρος μιας μιγαδικής ρίζας. Κρατάμε το φύλλο το οποίο περιέχει το θετικό πραγματικό μέρος της μιγαδικής ρίζας. Κατά συνέπεια $\#(T) < 2\,\#(T')$.

Στη συνέχεια θεωρούμε τα φύλλα του T'. Όλα είναι type-0 ή type-1. Και στις δύο περιπτώσεις στο αντίστοιχο διάστημα $\mathcal{I}_v$, περιέχεται το θετικό πραγματικό μέρος μιας ρίζας του A_{red} και ισχύει $|\mathcal{I}_v| \geq |\gamma_i - \gamma_{c_i}|$ (Σημ. 3.45). Επίσης, ο αριθμός των κόμβων από ένα φύλλο μέχρι τη ρίζα του δένδρου είναι n_i, ο οποίος είναι τέτοιος ώστε να ικανοποιείται η συνθήκη της Σημ. 3.44. Καθώς το n_i είναι ο μικρότερος δείκτης τέτοιος ώστε η συνθήκη της Σημ. 3.44 να ικανοποιείται, εάν μειώσουμε το n_i κατά ένα τότε η ανισότητα δεν ισχύει πλέον. Συνεπώς

$$F_{n_i-2}|\gamma_i - \gamma_{c_i}| \leq 2d^2 \Rightarrow \phi^{n_i-3}|\gamma_i - \gamma_{c_i}| < 2d^2 \Rightarrow n_i < 4 + 2\lg d - \lg|\gamma_i - \gamma_{c_i}|$$

Αθροίζουμε πάνω σε όλα τα n_i προκειμένου να φράξουμε το πλήθος των κόμβων του T', οπότε

$$\#(T') \leq \sum_{i=1}^{k} n_i \leq 2k(2 + \lg d) - \sum_{i=1}^{k} \log|\gamma_i - \gamma_{c_i}| \leq 2k(2 + \lg d) - \log\prod_{i=1}^{k}|\gamma_i - \gamma_{c_i}| \qquad (3.12)$$

Προκειμένου να εφαρμόσουμε το Θεωρ. 3.27 πρέπει να αναδιατάξουμε την ποσότητα $\prod_{\mathcal{I}\in\mathcal{J}}|\alpha_{\mathcal{I}} - \beta_{\mathcal{I}}|$ έτσι ώστε οι απαιτήσεις για τους δείκτες των ριζών να ικανοποιούνται. Οι προϋποθέσεις του θεωρήματος δεν ικανοποιούνται αν εμφανίζονται συμμετρικά γινόμενα. Θεωρούμε τη χειρότερη περίπτωση, να εμφανίζονται *μόνο* συμμετρικά γινόμενα, δηλαδή η ποσότητά μας είναι της μορφής $\prod|(\alpha_{\mathcal{I}} - \beta_{\mathcal{I}})(\beta_{\mathcal{I}} - \alpha_{\mathcal{I}})|$. Κατά συνέπεια θεωρούμε το τετράγωνο της ανισότητας του Θεωρ. 3.27 αντικαθιστώντας την ποσότητα $\frac{k}{2}$ με k και λαμβάνοντας υπ' όψιν ότι $\mathrm{disc}(A_{red}) \geq 1$, αφού το A_{red} είναι χωρίς τετράγωνα. Συνεπώς

$$\begin{aligned} \prod_{i=1}^{k}|\gamma_i - \gamma_{c_i}| \;&\geq\; \left(2^{\frac{k}{2}-\frac{d(d-1)}{2}}\,\mathcal{M}(A)^{1-d-\frac{k}{2}}\right)^2 \\ -\log\prod_{i=1}^{d}|\gamma_i - \gamma_{c_i}| \;&\leq\; d^2 - d - k + (2d + k - 2)\lg\mathcal{M}(A) \end{aligned} \qquad (3.13)$$

Η (3.12) γίνεται $\#(T') \leq 2k(2 + \lg d) + d^2 - d - k + (2d + k - 2)\lg\mathcal{M}(A)$. Ωστόσο, για το μέτρο Mahler είναι γνωστό ότι $\mathcal{M}(A) \leq 2^\tau\sqrt{d+1} \Rightarrow \lg\mathcal{M}(A) \leq \tau + \lg d$, για $d \geq 2$ (Λημ. 3.4), και έτσι $\#(T') \leq 2k(2 + \lg d) + d^2 - d - k + (2d + k - 2)(\tau + \lg d)$. Εφόσον $\#(T) < 2\,\#(T')$ και $k \leq d$, συμπεραίνουμε ότι $\#(T) = \mathcal{O}(d^2 + d\,\tau + d\lg d)$. ΟΕΔ

Η πολυπλοκότητα του CF

Προκειμένου να ολοκληρώσουμε την ανάλυση του CF αλγορίθμου πρέπει να υπολογίσουμε το κόστος κάθε βήματος. Στην χειρότερη περίπτωση κάθε βήμα απαιτεί τον υπολογισμό του θετικού κάτω φράγματος, b, στις θετικές πραγματικές ρίζες (Γραμμή 10) και τρεις μετασχηματισμούς, $X \mapsto b + X$, $X \mapsto 1 + X$ και $X \mapsto \frac{1}{1+X}$ (Γραμμές 11, 12 και 14 στον Αλγ. 13). Η αντιστροφή έχει πολυπλοκότητα $\mathcal{O}(d)$. Συνεπώς η πολυπλοκότητα του αλγορίθμου εξαρτάται από το κόστος των μετατοπίσεων (Γραμμή 11 στον Αλγ. 13) με την προϋπόθεση ότι απαιτείται ένας μικρός αριθμός από κλήσεις της PLB προκειμένου να υπολογιστεί ένα μερικό πηλίκο. Προς το παρόν δεχόμαστε αυτή την υπόθεση και θα την τεκμηριώσουμε στη συνέχεια.

Προκειμένου να υπολογίσουμε την συνολική πολυπλοκότητα πρέπει να φράξουμε το μέγεθος των $\mathcal{L}(c_k) \triangleq b_k, 0 \leq k \leq n_i$, δείτε επίσης την (3.10).

Αρχικά το A_{red} έχει βαθμό d και δυαδικό μήκος τ. Προφανώς ένας μετασχηματισμός μετατόπισης δεν αλλάζει το βαθμό του. Μια μετατόπιση με έναν ακέραιο, δυαδικού μήκος b_h, αυξάνει το δυαδικό μήκος του πολυωνύμου κατά ένα προσθετικό παράγοντα $d\, b_h$, στη χειρότερη περίπτωση (Εν. 2.2). Στο h βήμα του αλγορίθμου το πολυώνυμο έχει δυαδικό μήκος $\mathcal{O}(\tau + d\sum_{i=1}^{h} b_i)$ και εκτελούμε μια μετατόπιση με έναν ακέραιο μήκους b_{h+1}. Τα αποτελέσματα της Εν. 2.2 (Fast Taylor Shifts) μας υποδεικνύουν ότι αυτή η μετατόπιση μπορεί να γίνει με πολυπλοκότητα $\mathcal{O}_B\left(\mathsf{M}\left(d^2 \lg d + d^2 b_{h+1} + d(\tau + d\sum_{i=1}^{h} b_i)\right)\right)$ ή $\mathcal{O}_B\left(\mathsf{M}\left(d^2 \lg d + d\tau + d^2 \sum_{i=1}^{h+1} b_i\right)\right)$.

Απομένει να φράξουμε την ποσότητα $\sum_{i=1}^{h+1} b_i$. Γι' αυτό το σκοπό χρησιμοποιούμε την (3.10), η οποία φράσσει το $\mathbf{E}[b_i]$. Χρησιμοποιώντας την γραμμικότητα της αναμενόμενης τιμής προκύπτει ότι $\mathbf{E}[\sum_{i=1}^{h+1} b_i] = \mathcal{O}(h)$. Εφόσον $h \leq \#(T) = \mathcal{O}(d^2 + d\tau)$ (Θεωρ. 3.46), το αναμενόμενο κόστος, στη χειρότερη περίπτωση, στο βήμα h είναι $\mathcal{O}_B(\mathsf{M}\left(d^2 \lg d + d\tau + d^2(d^2 + d\tau)\right))$ ή $\widetilde{\mathcal{O}}_B(d^2(d^2 + d\tau))$.

Τέλος, πολλαπλασιάζοντας με τον αριθμό των βημάτων, $\#(T)$, συμπεραίνουμε ότι η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(d^6 + d^5\tau + d^4\tau^2)$, ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ εάν $d = \mathcal{O}(\tau)$, ή $\widetilde{\mathcal{O}}_B(N^6)$, όπου $N = \max\{d, \tau\}$.

Προκειμένου να απομονώσουμε τις αρνητικές πραγματικές ρίζες εφαρμόζουμε στο A_{red} τον μετασχηματισμό $X \mapsto -X$ και επαναλαμβάνουμε τον αλγόριθμο.

Όταν πρέπει να απομονώσουμε τις πραγματικές ρίζες ενός πολυωνύμου A, το οποίο δεν είναι ελεύθερο τετραγώνων και/ή θέλουμε να υπολογίσουμε τις πολλαπλότητες των πραγματικών ριζών τότε, όπως και στην περίπτωση των αλγορίθμων υποδιαίρεσης, μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο REALROOTSOLVER (Αλγ. 1) αντικαθιστώντας τη συνάρτηση REALROOTISOLATOR με τον αλγόριθμο CF.

Η προηγούμενη συζήτηση μας επιτρέπει να διατυπώσουμε το ακόλουθο θεώρημα:

Θεώρημα 3.47

Έστω $A \in \mathbb{Z}[X]$, όχι απαραίτητα χωρίς τετράγωνα, τέτοιο ώστε $\deg(A) = d > 2$ και $\mathcal{L}(A) = \tau$. Η αναμενόμενη πολυπλοκότητα του αλγορίθμου REALROOTSOLVER *για την απομόνωση και τον υπολογισμό των πολλαπλοτήτων των πραγματικών ριζών του A, χρησιμοποιώντας ως* REALROOTISOLATOR *του αλγόριθμο* CF*, είναι $\widetilde{\mathcal{O}}_B(d^6 + d^5\,\tau + d^4\,\tau^2)$ ή $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ αν $d = \mathcal{O}(\tau)$.*

Επιπρόσθετα το δυαδικό μήκος των ρητών αριθμών που είναι άκρα των διαστημάτων απομόνωσης φράσσεται από $\mathcal{O}(d\,\tau)$.

Σημείωση 3.48. *Η υπόθεση $d > 2$ δύναται να αντικατασταθεί από $d > 4$, καθώς μπορούμε να επιλύσουμε στους πραγματικούς πολυώνυμα βαθμού μέχρι 4 σε χρόνο $\mathcal{O}(1)$ ή $\widetilde{\mathcal{O}}_B(\tau)$ [92].*

Σημείωση 3.49. *Μπορούμε να δείξουμε ότι και η πολυπλοκότητα στη χειρότερη περίπτωση του* CF *είναι $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ διαφοροποιώντας ελάχιστα τον αλγόριθμο. Σε κάθε βήμα του αλγορίθμου διαμερίζουμε το A_1 σε δύο άλλα πολυώνυμα $A_{1,1}$ και $A_{1,2}$ χρησιμοποιώντας την συνάρτηση* $\text{SPLIT}_{\text{DESCARTES}}$. *Με αυτή την μικρή τροποποίηση ο* CF *είναι σχεδόν ο ίδιος με του αλγόριθμο* DESCARTES *και άρα έχει στην χειρότερη περίπτωση την ίδια πολυπλοκότητα.*

Εναλλακτικά μπορούμε επίσης να να χρησιμοποιήσουμε το γεγονός ότι στη χειρότερη περίπτωση πρέπει να κάνουμε κάποια μετατόπιση με έναν αριθμό δυαδικού μήκους το πολύ $\mathcal{O}(d\tau)$ όπως προκύπτει από το φράγμα διαχωρισμού και να συνάγουμε την πολυπλοκότητα στη χειρότερη περίπτωση.

Ρητοί αριθμοί και η υλοποίηση του PLB

Υπάρχουν δύο σημεία στον αλγόριθμο CF τα οποία χρήζουν μεγαλύτερης ανάλυσης και τα οποία η βιβλιογραφία έχει παραβλέψει.

Το πρώτο αφορά τους ρητούς αριθμούς. Αν το προς επίλυση πολυώνυμο A έχει κάποιους ρητούς αριθμούς για ρίζες τότε η ανάπτυξη σε συνεχή κλάσματα αυτών των ριζών δεν ακολουθεί ούτε την κατανομή Gauss-Kuzmin ούτε το νόμο του Khintchine. Ωστόσο, αν ένας ρητός αριθμός, $\frac{p}{q}$ είναι ρίζα του A τότε ο p διαιρεί τον a_0 και ο q διαιρεί τον a_d. Συνεπώς στη χειρότερη περίπτωση $\mathcal{L}(p/q) = \mathcal{O}(\tau)$ και άρα οι ρητοί αριθμοί απομονώνονται πολύ νωρίς στην εκτέλεση του αλγορίθμου. Το γεγονός ότι τους μεταχειριζόμαστε όπως τους αλγεβρικούς αριθμούς βαθμού μεγαλύτερου από δύο είναι μια υπερεκτίμηση.

Το δεύτερο σημείο αφορά τον αριθμό των κλήσεων της συνάρτησης PLB που απαιτούνται προκειμένου να υπολογιστεί ένα μερικό πηλίκο. Στην Εν. 3.6 κάναμε την παραδοχή ότι ο αριθμός αυτός είναι μικρός. Στην πράξη είναι σχεδόν πάντοτε έτσι εκτός από μία πολύ ειδική περίπτωση, όταν το πολυώνυμο έχει μόνο ρητούς αριθμούς για ρίζες οι οποίες είναι $\gg 1$. Η μη καλή συμπεριφορά του αλγορίθμου CF οφείλεται στο γεγονός ότι η συνάρτηση PLB πρέπει να κληθεί αρκετές φορές. Οι Richtmyer et al. [224] προκειμένου να αντιμετωπίσουν τέτοια προβλήματα πραγματοποιούν ένα μικρό αριθμό από επαναλήψεις Newton για να υπολογίσουν μια καλή προσέγγιση του μερικού πηλίκου. Οι Akritas [2], Akritas and Strzebonski [3], Akritas et al. [4] επιλύουν (πρακτικώς) το πρόβλημα εφαρμόζοντας την ομοθεσία $X \mapsto bX$, όπου b είναι το υπολογισμένο φράγμα, όταν $b \geq 16$.

Η παρατήρηση ότι ο αριθμός των κλήσεων της PLB είναι μικρός ενισχύεται από την (3.9), από την οποία προκύπτει ότι η πιθανότητα ένα μερικό πηλίκο να είναι μέτρου ≤ 10 είναι ~ 0.87. Γι' αυτό στην πράξη τα μερικά πηλίκα είναι πολύ μικρού δυαδικού μήκους. Επιπρόσθετα, η σχέση

$$\left|\gamma - \frac{P_n}{Q_n}\right| < \frac{1}{c_{n+1}\, Q_n^2}$$

μας λέει ότι η εμφάνιση ενός μερικού πηλίκου ασυνήθιστα μεγάλου μέτρου σημαίνει ότι η *προηγούμενη* προσέγγιση του αλγεβρικού αριθμού ήταν πάρα πολύ καλή.

Προκειμένου να θεμελιώσουμε θεωρητικά τη συμπεριφορά του CF θα χρησιμοποιήσουμε τα αποτελέσματα για την ποιότητα των φραγμάτων στις θετικές πραγματικές ρίζες που παρουσιάσαμε στην Εν. 3.2.

Το φράγμα που χρησιμοποιούμε για την υλοποίηση του PLB είναι το N_2, δείτε Εξ. (3.3). Αν b είναι το υπολογισθέν φράγμα και γ η κοντινότερη σε αυτό ρίζα, την οποία προσπαθούμε να απομονώσουμε, τότε από το Λημ. 3.17 ισχύει ότι $b \leq \gamma \leq d\,b$. Υπενθυμίζουμε ότι το κάτω φράγμα υπολογίζεται αρχικά ως άνω φράγμα στο αντίστροφο πολυώνυμο, το οποίο στη συνέχεια αντιστρέφεται, δείτε Σημ. 3.20.

Συνεπώς, κάποιος από τους ακεραίους στο διάστημα $[b, d\,b]$ αντιστοιχεί στο μερικό πηλίκο του γ που προσπαθούμε να υπολογίσουμε. Μπορούμε να χρησιμοποιήσουμε δυαδική αναζήτηση σε συνδυασμό με το θεώρημα του Budan (Θεωρ. 3.31) προκειμένου να βρούμε ένα διάστημα $[c, c+1] \subseteq [b, d\,b]$ στο οποίο περιέχεται το γ και όπου το $c \in \mathbb{Z}$ είναι μερικό πηλίκο που αναζητούμε. Το θεώρημα του Budan υλοποιείται με 2 μετατοπίσεις, οπότε η δυαδική αναζήτηση απαιτεί, για τον υπολογισμό του μερικού πηλίκου c, το πολύ $\mathcal{O}(\lg d + \lg b)$ μετατοπίσεις.

Όμως $b \leq c \Rightarrow \mathcal{L}(b) \leq \mathcal{L}(c) = \mathcal{O}(1)$, καθώς το c είναι μερικό πηλίκο στην ανάπτυξη του γ σε συνεχές κλάσμα, και άρα το δυαδικό του μήκος υπακούει το νόμο του Khintchine, Εξ. (3.10). Συνεπώς, σε κάθε βήμα του αλγορίθμου πρέπει να εκτελεστούν το πολύ $\mathcal{O}(\lg d)$ μετατοπίσεις, αντί για 2 που είχαμε υποθέσει. Δηλαδή, η πολυπλοκότητα του αλγορίθμου πρέπει να πολλαπλασιαστεί με ένα παράγοντα $\lg d$, ο οποίος δεν αλλάζει το φράγμα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$.

Στην πράξη η ποιότητα των φραγμάτων είναι πάρα πολύ καλή και ποτέ δεν κάνουμε δυαδική αναζήτηση προκειμένου να υπολογίσουμε το μερικό πηλίκο!

3.7 Σύνοψη – Μελλοντικές επεκτάσεις

Το παρόν κεφάλαιο επικεντρώνεται ρίζες των ακέραιων πολυωνύμων. Αρχικά παρουσιάσαμε απόλυτα, θετικά, σύνθετα φράγματα και φραγματα διαχωρισμού για τις πραγματικές και μιγαδικές ρίζες. Όσον αφορά τα θετικά φράγματα ενοποιήσαμε τα ήδη γνωστά φράγματα, προτείναμε κάποια καινούργια και αποδείξαμε κάποια αποτελέσματα για την ποιότητά τους.

Η ενασχόλησή μας με τα θετικά φράγματα και τα φράγματα διαχωρισμού συνεχίζεται. Θεωρούμε ότι είναι εξαιρετικά ενδιαφέρουσα μια συνολική θεωρία για τα θετικά φράγματα, όπως αυτή του van der Sluis [257] για τα απόλυτα φράγματα. Επίσης ενδιαφέρουσα είναι η απόδειξη κάποιου αποτελέσματος για την ποιότητα του φράγματος του Stefanescu (Θεωρ. 3.19).

Το σημείο αναφοράς του κεφαλαίου είναι απομόνωση των πραγματικών ριζών ενός ακέραιου πολυωνύμου, βαθμού d και δυαδικού μήκους τ, και ο υπολογισμός των πολλαπλοτήτων τους. Ενοποιήσαμε τους αλγορίθμους υποδιαίρεσης και βελτιώσαμε την πολυπλοκότητα του αλγορίθμου των συνεχών κλασμάτων κατά δύο παράγοντες, όπου επιπρόσθετα οριστικοποιήσαμε την θεωρητική του θεμελίωση. Η πολυπλοκότητα όλων των αλγορίθμων είναι $\widetilde{\mathcal{O}}_B(d^4\,\tau^2)$. Αποδείξαμε ότι το φράγμα της πολυπλοκότητας ισχύει και για πολυώνυμα με τετράγωνα και ότι στην ίδια πολυπλοκότητα μπορούμε να υπολογίσουμε τις πολλαπλότητες ριζών.

Υπενθυμίζουμε στον αναγνώστη ότι η πολυπλοκότητα των αριθμητικών (προσεγγιστικών) αλγορίθμων [213, 214, 239] είναι $\widetilde{\mathcal{O}}_B(d^3\,\tau)$ ή $\widetilde{\mathcal{O}}_B(N^4)$, όπου $N = \max\{d, \tau\}$. Ένα από τα μεγαλύτερα ανοιχτά ερωτήματα είναι αν οι ακριβείς αλγόριθμοι μπορούν να επιτύχουν αυτό το φράγμα πολυπλοκότητας. Επίσης, ποιό είναι το κάτω φράγμα των αλγορίθμων απομόνωσης; Παρατηρούμε ότι η έξοδος των αλγορίθμων είναι $\mathcal{O}(d)$ διαστήματα απομόνωσης με άκρα δυαδικού μήκους $\mathcal{O}_B(d\,\tau)$, οπότε ένα κάτω φράγμα είναι το $\mathcal{O}_B(d^2\tau)$. Είναι το φράγμα βέλτιστο; Από την άλλη αν μας δοθεί ένα πολυώνυμο και $\mathcal{O}(d)$ διαστήματα απομόνωσης των πραγματικών ριζών του, με άκρα δυαδικού μήκους $\mathcal{O}_B(d\,\tau)$, μπορούμε να υπολογίσουμε τις πολλαπλότητες των ριζών με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\,\tau)$, η οποία είναι βέλτιστη. Μήπως αυτό είναι το βέλτιστο κάτω φράγμα;

Όσον αφορά τους αλγορίθμους υποδιαίρεσης δεν υπάρχει ελπίδα για πολυπλοκότητα $\widetilde{\mathcal{O}}_B(N^4)$, καθώς τόσο ο αριθμός των βημάτων που εκτελούν όσο και το κόστος του κάθε βήματος είναι βέλτιστο. Το αμέσως επόμενο βήμα θα πρέπει να είναι η ένταξη στους αλγορίθμους υποδιαίρεσης του αλγορίθμου αποκλεισμού (exclusion algorithm) των Dedieu and Yakoubsohn [68] και η βελτίωση της πολυπλοκότητάς του. Για τον αλγόριθμο των συνεχών κλασμάτων πιστεύουμε ότι, με κάποιες μικρές τροποποιήσεις, μπορούμε να επιτύχουμε (αναμενόμενη) πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\tau)$. Αν αλλάξουμε την αναπαράσταση των πραγματικών ριζών και αντί για διαστήματα απομόνωσης υιοθετήσουμε την κωδικοποίηση Thom [58], τότε χρησιμοποιώντας τον αλγόριθμο του Canny [44] μπορούμε να προτείνουμε έναν αλγόριθμο με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(N^5)$.

Τέλος, οι ακριβείς αλγόριθμοι στην πράξη είναι πολύ γρήγοροι και σπάνια επιτυγχάνουν το φράγμα πολυπλοκότητας της χειρότερης περίπτωσης. Ποιά είναι η αναμενόμενη πολυπλοκότητα των αλγορίθμων;

Στα παραπάνω προβλήματα ευελπιστούμε ότι θα μπορέσουμε να παρουσιάσουμε αποτελέσματα στο άμεσο μέλλον.

ΚΕΦΑΛΑΙΟ 4

Υπολογισμοί με πραγματικούς αλγεβρικούς αριθμούς

Ο Θεός έφτιαξε τους ακέραιους,
όλοι οι υπόλοιποι αριθμοί είναι
δημιουργήματα του ανθρώπου.

Leopold Kronecker

Περίληψη

Το παρόν κεφάλαιο ασχολείται με αλγορίθμους που αφορούν υπολογισμούς με ένα και δύο πραγματικούς αλγεβρικούς αριθμούς. Πιο συγκεκριμένα παρουσιάζονται αλγόριθμοι για την αναπαράσταση πραγματικών αλγεβρικών αριθμών, για τον υπολογισμό του προσήμου της αποτίμησης ενός πολυωνύμου πάνω σε έναν και δύο αλγεβρικούς αριθμούς και για το πρόβλημα των ταυτόχρονων ανισώσεων. Τέλος, παρουσιάζουμε δύο αλγορίθμους για την πραγματική επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές. Όλοι αλγόριθμοι βασίζονται στις προσημασμένες ακολουθίες πολυωνυμικών υπολοίπων.

Όσον αφορά στους υπολογισμούς με έναν αλγεβρικό αριθμό, αν και οι περισσότεροι αλγόριθμοι είναι γνωστοί, η πολυπλοκότητά τους δεν έχει μελετηθεί. Παρουσιάζουμε σε ενιαίο πλαίσιο τους αλγορίθμους για υπολογισμούς με έναν αλγεβρικό αριθμό και την πολυπλκοκότητά τους. Σε κάθε περίπτωση βελτιώνουμε τα φράγματα πολυπλοκότητας κατά δύο ή τρεις παράγοντες. Στη συνέχεια παρουσιάζουμε τις πολυπλοκότητες για τον υπολογισμό πολυωνυμικών ακολουθιών υπολοίπων, πολυωνύμων σε δύο μεταβλητές, δύο αλγόριθμους για την πραγματική επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές και αλγορίθμους για υπολογισμούς με δύο αλγεβρικούς αριθμούς. Τα προκύπτοντα φράγματα πολυπλοκότητας βελτιώνουν σε κάθε περίπτωση τα ήδη γνωστά. Μέρος των αποτελεσμάτων έχει παρουσιαστεί στις εργασίες [87, 91, 97].

Το σύνολο των πραγματικών αλγεβρικών αριθμών, το οποίο είναι σώμα, το συμβολίζουμε με $\mathbb{R}_{alg}$. Προκειμένου να περιγράψουμε και να αναλύσουμε αλγορίθμους που αφορούν υπολογισμούς με αλγεβρικούς αριθμούς πρέπει να επιλέξουμε μια αναπαράστασή τους. Επιλέγουμε την αναπαράσταση διαστήματος απομόνωσης (isolating interval representation).

Ορισμός 4.1. *Η αναπαράσταση με διάστημα απομόνωσης ενός πραγματικού αλγεβρικού αριθμού,* $\gamma \in \mathbb{R}_{alg}$*, συμβολίζεται με* $\gamma \cong (A(X), \mathcal{I})$*, όπου* $A \in \mathbb{Z}[X]$ *είναι χωρίς τετράγωνα,* $A(\gamma) = 0$*,* $\gamma \in \mathcal{I}$*,* $\mathcal{I} = [a, b]$*,* $a, b, \in \mathbb{Q}$ *και το* A *δεν έχει άλλη πραγματική ρίζα στο* $\mathcal{I}$*.*

Η αναπαράσταση με διάστημα απομόνωσης δεν είναι μοναδική. Καταρχάς δεν απαιτούμε το A να είναι το ελάχιστο πολυώνυμο του γ. Αν και υπάρχουν αλγόριθμοι που υπολογίζουν το ελάχιστο πολυώνυμο, θέλουμε να τους αποφύγουμε λόγω της μεγάλης θεωρητικής και πρακτικής πολυπλοκότητάς τους. Ακόμη και στην περίπτωση που το ελάχιστο πολυώνυμο είναι γνωστό, το διάστημα απομόνωσης δεν μπορεί να οριστεί μοναδικά.

Παράδειγμα 4.2. *Αν* $\gamma = \sqrt{2}$ *τότε οι αναπαραστάσεις* $\gamma \cong (X^2 - 2, [0, 3])$*,* $\gamma \cong (X^2 - 2, [1, 2])$ *και* $\gamma \cong ((X^2 - 2)(X - 10), [0, 9])$ *είναι ισοδύναμες αναπαραστάσεις του* γ*.*

Εκτός από την αναπαράσταση με διάστημα απομόνωσης, υπάρχουν και άλλες αναπαραστάσεις για τους πραγματικούς αλγεβρικούς αριθμούς. Ο αναγνώστης μπορεί να ανατρέξει για παράδειγμα, στους Cohen [51], Mishra [193], Yap [275] για περισσότερες λεπτομέρειες. Αξίζει ωστόσο να αναφέρουμε την αναπαράσταση με κωδικοποίηση κατά Thom την οποία εισήγαγαν οι Coste and Roy [58], όπου οι πραγματικές ρίζες ενός ακέραιου πολυωνύμου χαρακτηρίζονται (μοναδικά) από το πρόσημο όλων των παραγώγων του πολυωνύμου πάνω σε αυτές. Η προσέγγιση αυτή είναι καθαρά συμβολική, δεν εξαρτάται από τα φράγματα διαχωρισμού και είναι νόμιμη όχι μόνο για ακέραια πολυώνυμα αλλά και για πολυώνυμα σε σε οποιοδήποτε κλειστό αλγεβρικό σώμα. Για την πολυπλοκότητα των υπολογισμών αυτών ο αναγνώστης μπορεί να ανατρέξει στους Coste and Roy [58], Roy and Szpirglas [231] αλλά και στους Cucker et al. [63], Mishra and Pedersen [194], όπου παρουσιάζονται αποτελέσματα πολυπλοκότητας στην κλάση NC. Δεν θα ασχοληθούμε με αυτή την προσέγγιση.

Το υπόλοιπο του κεφαλαίου χωρίζεται σε δύο ενότητες. Η πρώτη αφορά υπολογισμούς με έναν πραγματικό αλγεβρικό αριθμό και η δεύτερη με δύο.

4.1 Υπολογισμοί με έναν αλγεβρικό αριθμό

Σε ό,τι θα ακολουθήσει θα παρουσιάσουμε έναν αλγόριθμο που κατασκευάζει πραγματικούς αλγεβρικούς αριθμούς. Επίσης, αλγορίθμους που συγκρίνουν πραγματικούς αλγεβρικούς αριθμούς, που υπολογίζουν το πρόσημο ενός πολυωνύμου αν αποτιμηθεί πάνω σε έναν πραγματικό αλγεβρικό αριθμό, έναν αλγόριθμο για τον υπολογισμό ενδιάμεσων σημείων σε μία διατεταγμένη λίστα από πραγματικούς αλγεβρικούς αριθμούς και τέλος έναν αλγόριθμο για το πρόβλημα των ταυτόχρονων ανισώσεων.

Ο Canny [46] αλλά και ο Rump [232] προτείνουν, αφενός μεν οι πραγματικοί αλγεβρικοί αριθμοί να αναπαρίστανται με διάστημα απομόνωσης, αφετέρου δε οι υπολογισμοί με αυτούς να γίνονται με συνεχείς εκλεπτύνσεις των διαστημάτων απομόνωσης, βασιζόμενοι στις ιδιότητες της αριθμητικής διαστημάτων και στα φράγματα διαχωρισμού πολυωνυμικών συστημάτων [46, 275]. Με άλλα λόγια οι υπολογισμοί πραγματοποιούνται με προσεγγίσεις των πραγματικών αλγεβρικών αριθμών οι οποίες βελτιώνονται αν δεν είναι ικανοποιητικές. Για παράδειγμα, προκειμένου

να υπολογιστεί το πρόσημο μιας (πολυωνυμικής) έκφρασης που περιέχει πραγματικούς αλγεβρικούς αριθμούς, αντικαθιστούμε τους πραγματικούς αλγεβρικούς αριθμούς με τα διαστήματα απομόνωσής τους και εκτελούμε τις πράξεις χρησιμοποιώντας αριθμητική διαστημάτων. Αν το αποτέλεσμα, το οποίο είναι ένα διάστημα, δεν περιέχει το 0, τότε μπορούμε να αποφασίσουμε το πρόσημό του. Αν περιέχει το 0 τότε εκλεπτύνουμε τα διαστήματα απομόνωσης, χρησιμοποιώντας τα πολυώνυμα που ορίζουν τους αλγεβρικούς αριθμούς, μέχρι το διάστημα του αποτελέσματος να μην περιέχει το 0 ή μέχρι να ξεπεράσουμε το φράγμα διαχωρισμού της έκφρασης, οπότε και το αποτέλεσμα είναι 0. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι μπορεί να υλοποιηθεί, σχετικά εύκολα, με αριθμούς κινητής υποδιαστολής, είτε στην ακρίβεια της μηχανής είτε απεριόριστης ακρίβειας και επίσης όταν η έκφρασή δεν είναι μηδέν τότε είναι πάρα πολύ αποτελεσματική. Από την άλλη μεριά αν το αποτέλεσμα της έκφρασης είναι 0 ή πολύ κοντά στο 0, τότε προκειμένου να αποφασίσουμε το πρόσημο της έκφρασης πρέπει το διάστημα του αποτελέσματος να είναι μικρότερο από το φράγμα διαχωρισμού. Τα φράγματα διαχωρισμού αντικατοπτρίζουν τη χειρότερη δυνατή περίπτωση και όπως έχουμε αναφέρει και στην περίπτωση της μιας μεταβλητής είναι στη γενική περίπτωση πολύ κακής ποιότητας, δείτε Εν. 3.2. Στο ίδιο πλαίσιο κινείται η προσέγγιση του Johnson [140], οι αλγόριθμοι που παρουσιάζουν οι Basu et al. [14] και η ακόμα πιο γενική προσέγγιση των Burnikel et al. [40, 42], Li and Yap [172], Pion and Yap [216] οι οποίοι παρουσιάζουν το γενικό θεωρητικό υπόβαθρο αυτής της πρόσεγγισης και για τις τέσσερις βασικές πράξεις. Δείτε επίσης τις εργασίες των Li et al. [173], Yap [274].

Οι αλγόριθμοι που παρουσιάζουμε χρησιμοποιούν την αναπαράσταση με διάστημα απομόνωσης αλλά επιπρόσθετα βασίζονται στις προσημασμένες πολυωνυμικές ακολουθίες υπολοίπων προκειμένου να αποφύγουμε την εκλέπτυση των διαστημάτων.

Μια τέτοια προσέγγιση προτείνουν οι Schwartz and Sharir [241] και επίσης χρησιμοποιεί ο Rioboo [225, 226, 227]. Μάλιστα η υλοποίηση του Rioboo [225, 226] στο μαθηματικό λογισμικό AXIOM είναι η μοναδική μέχρι σήμερα, που επιτρέπει όλες τις πράξεις μεταξύ πραγματικών αλγεβρικών αριθμών, χωρίς να χρησιμοποιεί προσεγγίσεις τους. Αλγόριθμοι που αφορούν όλες τις βασικές πράξεις παρουσιάζονται από τον Loos [177], δείτε επίσης [193, 218, 275]. Η αλγοριθμική προσέγγιση που ομοιάζει περισσότερο στη δική μας είναι αυτή του Sakkalis [234]. Όσον αφορά τους υπολογισμούς με έναν πραγματικό αλγεβρικό αριθμό, οι περισσότεροι από τους αλγορίθμους που παρουσιάζουμε δεν είναι κανούργιοι. Ωστόσο, περιέργως πως, η πολυπλοκότητά τους δεν παρουσιάζεται στην βιβλιογραφία. Σε κάθε περίπτωση βελτιώνουμε την πολυπλοκότητα κατά 2 ή 3 παράγοντες.

Αν και γενικώς πιστεύεται ότι η πρώτη προσέγγιση είναι η καλύτερη στην πράξη, αυτό δεν είναι πάντοτε αληθές. Μια προσεκτική υλοποίηση των αλγορίθμων που παρουσιάζουμε μπορεί να οδηγήσει σε λογισμικό που μπορεί να επιλύσει πολύ γρήγορα πολλά από τα προβλήματα που παρουσιάζονται στις εφαρμογές. Επιπρόσθετα, το μεγάλο πλεονέκτημα της προσέγγισής μας είναι η θεωρήτική της πληρότητα, η οποία μας επιτρέπει να μελετήσουμε θεωρητικά τους αλγορίθμους υπολογισμού και να συνάγουμε φράγματα πολυπλοκότητας τα οποία είναι πολύ καλύτερα από οποιαδήποτε άλλη προσέγγιση. Ίσως το πιο σημαντικό πλεονέκτημα της προσέγγισή μας είναι το γεγονός ότι αν ο βαθμός των πραγματικών αλγεβρικών αριθμών είναι σταθερός, τότε η αριθμητική πολυπλοκότητα όλων των αλγορίθμων που παρουσιάζουμε, με την εξαίρεση του αλγορίθμου κατασκευής, είναι $\mathcal{O}(1)$, καθώς δεν εξαρτώμαστε από το φράγμα διαχωρισμού.

Κατασκευή

Δοθέντος ενός πολυωνύμου $A \in \mathbb{Z}[X]$,τέτοιου ώστε $\deg(A) = d$ και $\mathcal{L}(A) = \tau$, ο αλγόριθμος που υπολογίζει τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του A παρουσιάζεται στον Αλγ. 14. Για να απομονώσουμε τις ρίζες χρησιμοποιούμε τον αλγόριθμο readRootSolver (Αλγ. 1) με κάποιον από τους αλγορίθμους sturm, descartes, bernstein ή cf. Το κόστος επίλυσης είναι $\widetilde{\mathcal{O}}_B(d^6 + d^4\tau^2)$. Το πολυώνυμο που ορίζει τους αλγεβρικούς αριθμούς είναι το χωρίς τετράγωνα μέρος του A, το οποίο έχει δυαδικό μήκος $\mathcal{O}(d+\tau)$. Το δυαδικό μήκος των άκρων των διαστημάτων απομόνωσης είναι $\mathcal{O}(d\tau)$. Παρατηρούμε ότι πρέπει να ταξινομήσουμε τα διαστήματα απομόνωσης πριν κατασκευάσουμε τους αλγεβρικούς αριθμούς. Το κόστος της ταξινόμησης είναι $\mathcal{O}(d^2 \lg d)$ ή $\widetilde{\mathcal{O}}_B(d^3\,\tau)$, χρησιμοποιώντας για παράδειγμα τον αλγόριθμο quick-sort [57].

Η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(d^6 + d^4\tau^2)$.

Algorithm 14: construct (A)

Input: $A \in \mathbb{Z}[X]$
Output: Μια λίστα με τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του A και τις πολλαπλότητές τους.

```
1 R ← ∅
2 L, M ← realRootSolver(A)
3 sort([L, M])
4 foreach 𝕀 ∈ L do
5     R ← (A_red, 𝕀)
6 return R, M
```

Σημείωση 4.3. *Αν $\gamma \equiv (A, \mathbb{I} = [\mathsf{a}, \mathsf{b}])$, το $\mathbb{I}$ περιέχει μόνο μία πραγματική ρίζα του A και συνεπώς το A αλλάζει πρόσημο στα άκρα του $\mathbb{I}$, εκτός από την περίπτωση που $\mathsf{a} = \mathsf{b}$ οπότε και ισχύει $A(\mathsf{a}) = A(\mathsf{b}) = 0$. Μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι $0 \notin (\mathsf{a}, \mathsf{b})$, εκτός αν $\gamma = \mathsf{a} = \mathsf{b} = 0$.*

Παρατηρούμε επίσης ότι το πρόσημο του γ μπορεί να εξαχθεί εύκολα από το πρόσημο των a *και* b.

Στη συνέχεια θα παρουσιάσουμε αλγορίθμους (και την πολυπλοκότητά τους) για μερικές πολύ βασικές πράξεις με πραγματικούς αλγεβρικούς αριθμούς. Οι αλγεβρικοί αριθμοί θα έχουν την αναπαράσταση $\gamma \cong (A, \mathbb{I}) = [\mathsf{a}, \mathsf{b}]$, όπου το A είναι χωρίς τετράγωνα και $\deg(A) = d$, $\mathcal{L}(A) = \tau$ και $\mathcal{L}(\mathsf{a}) = \mathcal{L}(\mathsf{b}) = \mathcal{O}(d\tau)$, εκτός αν ρητά αναφέρεται το αντίθετο.

Υπολογισμός προσήμου

Ο αλγόριθμος υπολογισμού προσήμου, sign_at(f, γ) (Αλγ. 15), υπολογίζει το πρόσημο της αποτίμησης ενός πολυωνύμου f πάνω στον πραγματικό αλγεβρικό αριθμό γ. Θεωρούμε ότι $\deg(f) \leq d$ και $\mathcal{L}(f) = \sigma$.

Για να υπολογίσουμε το πρόσημο χρησιμοποιούμε το Θεωρ. 2.26 και έτσι έχουμε

$$\mathtt{VAR}(\mathbf{SR}(A, f\,;\,[\mathsf{a},\mathsf{b}])) = \mathrm{sign}\left(f(\gamma)\cdot A'(\gamma)\right)$$

Όμως $\mathrm{sign}(A'(\gamma)) = \mathrm{sign}(A(\mathsf{b}) - A(\mathsf{a}))$, οπότε συμπεραίνουμε ότι

$$\mathrm{sign}(f(\gamma)) = \mathtt{VAR}(\mathbf{SR}(A, f\,;\,[\mathsf{a},\mathsf{b}]))\cdot \mathrm{sign}(A(\mathsf{b}) - A(\mathsf{a}))$$

Το κόστος του υπολογισμού $\mathtt{VAR}(\mathbf{SR}(A, f\,;\,[\mathsf{a},\mathsf{b}]))$ είναι δύο φορές το κόστος υπολογισμού του $\mathbf{SR}(A, f\,;\,\mathsf{a})$, το οποίο είναι $\widetilde{\mathcal{O}}_B(d^2\max\{\sigma, d\tau\})$ (Θεωρ. 2.32). Το κόστος των αποτιμήσεων $A(\mathsf{a})$ και $A(\mathsf{b})$ είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$ (2.2), αν και μπορεί να θεωρηθεί ότι το πρόσημό τους είναι ήδη γνωστό.

Algorithm 15: SIGN_AT (f, γ)

Input: $f \in \mathbb{Z}[X], \gamma \cong (A, \mathcal{I} = [\mathsf{a},\mathsf{b}])$
Output: $\mathrm{sign}(f(\gamma))$

1 RETURN $\mathrm{sign}\left(\mathtt{VAR}(\mathbf{SR}(A, f\,;\,[\mathsf{a},\mathsf{b}]))\cdot \mathrm{sign}(A'(\gamma))\right)$

Πόρισμα 4.4. *Έστω $f(X) \in \mathbb{Z}[X]$, όπου $\deg(f) \le d$ και $\mathcal{L}(f) = \sigma$, και έστω ένας πραγματικός αλγεβρικός αριθμός $\gamma \cong (A, [\mathsf{a},\mathsf{b}])$, όπου $\deg(A) = d$, $\mathcal{L}(A) = \tau$ και $\mathcal{L}(\mathsf{a}) = \mathcal{L}(\mathsf{b}) = \mathcal{O}(d\tau)$. Η πολυπλοκότητα του* SIGN_AT(f, γ) *είναι $\widetilde{\mathcal{O}}_B(d^2\max\{\sigma, d\tau\})$.*

Η υπόθεση $\deg(f) \le d$ είναι χωρίς βλάβη της γενικότητας καθώς αν $\deg(f) > d$, τότε μπορούμε να υπολογίσουμε το SIGN_AT$(A, \mathrm{prem}(f, A))$ καθώς

$$\left|\mathrm{lead}(A)^{\deg(f)-\deg(A)+1}\right| \; f = A\cdot \mathrm{pquo}(f, A) + \mathrm{prem}(f, A) \Rightarrow f(\gamma) = \mathrm{prem}(f, A)(\gamma)$$

Σύγκριση

Ο αλγόριθμος σύγκρισης, COMPARE(γ_1, γ_2), δύο πραγματικών αλγεβρικών αριθμών $\gamma_1 \cong (A_1, \mathcal{I}_1 = [\mathsf{a}_1, \mathsf{b}_1])$ και $\gamma_2 \cong (A_2, \mathcal{I}_2 = [\mathsf{a}_2, \mathsf{b}_2])$ παρουσιάζεται στον Αλγ. 16. Αν τα διαστήματα $\mathcal{I}_1$ και $\mathcal{I}_2$ είναι ξένα μεταξύ τους ή αν μόνο ένας από τους γ_1 και γ_2 ανήκει στο $\mathcal{I}_1 \cap \mathcal{I}_2$ τότε μπορούμε εύκολα να τους συγκρίνουμε. Αν και οι δύο ανήκουν στο $\mathcal{J} = \mathcal{I}_1 \cup \mathcal{I}_2$ τότε

$$\gamma_1 \ge \gamma_2 \Leftrightarrow A_2(\gamma_1)\cdot A_2'(\gamma_2) \ge 0$$

Το πρόσημο της αποτίμησης $A_2(\gamma_1)$ μπορούμε να το υπολογίσουμε με τον αλγόριθμο SIGN_AT(A_2, γ_1) και το κόστος της, το οποίο είναι και το κόστος του αλγορίθμου COMPARE, είναι $\widetilde{\mathcal{O}}_B(d^3\tau)$.

Πόρισμα 4.5. *Έστω πραγματικοί αλγεβρικοί αριθμοί $\gamma_1 \cong (A_1, \mathcal{I}_1 = [\mathsf{a}_1, \mathsf{b}_1])$ και $\gamma_2 \cong (A_2, \mathcal{I}_2 = [\mathsf{a}_2, \mathsf{b}_2])$ όπου $\deg(A_{1,2}) = d$, $\mathcal{L}(A_{1,2}) = \tau$ και $\mathcal{L}(\mathsf{a}_{1,2}) = \mathcal{L}(\mathsf{b}_{1,2}) = \mathcal{O}(d\tau)$. Η σύγκρισή τους με τον αλγόριθμο* COMPARE *έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\tau)$.*

Algorithm 16: COMPARE (γ_1, γ_2)

Input: $\gamma_1 \cong (A_1, \mathcal{I}_2 = [\mathsf{a}_1, \mathsf{b}_1]), \gamma_2 \cong (A_2, \mathcal{I}_2 = [\mathsf{a}_2, \mathsf{b}_2])$
Output: Σύγκριση των γ_1 και γ_2

```
1  J ← I1 ∩ I2 = [c, d]
2  if J = ∅ then
3  |   if I1 < I2 then RETURN −1
4  |   else RETURN 1
5  if γ1 ∉ J then
6  |   if I1 < J then RETURN −1
7  |   else RETURN 1
8  if γ2 ∉ J then
9  |   if I2 < J then RETURN 1
10 |   else RETURN −1
11 RETURN SIGN_AT(A2, γ1) · sign(A2'(γ2))
```

Ενδιάμεσα σημεία

Σε πολλές περιπτώσεις, δοθέντων πραγματικών αλγεβρικών αριθμών (σε διάταξη) που είναι ρίζες ενός πολυωνύμου A χρειάζεται να υπολογίσουμε ρητά σημεία ανάμεσα στους αριθμούς. Αυτό μπορεί να γίνει διατρέχοντας τη λίστα L που επιστρέφει ο αλγόριθμος CONSTRUCT(A) και για κάθε ζεύγος διαστημάτων να θεωρήσουμε το μέσο του πάνω άκρου του πρώτου διαστήματος και του κάτω άκρου του δεύτερου διαστήματος. Το πρώτο (τελευταίο), ενδιάμεσο σημείο το υπολογίζουμε αφαιρώντας (προσθέτοντας) 1 στο κάτω (άνω) άκρο του πρώτου (τελευταίου) διαστήματος απομόνωσης. Τον αλγόριθμο αυτό θα τον συμβολίσουμε με INTERMEDIATE_POINTS και η πολυπλοκότητα του είναι $\widetilde{\mathcal{O}}_B(d^2\,\tau)$ ή $\widetilde{\mathcal{O}}_B(R\,d\,\tau)$, όπου R είναι το πλήθος των πραγματικών ριζών του A.

Το πρόβλημα των ταυτόχρονων ανισώσεων

Έστω $f, A_1, \ldots, A_{n_1}, B_1, \ldots, B_{n_2}, C_1, \ldots, C_{n_3} \in \mathbb{Z}[X]$, όπου συνολικός τους βαθμός φράσσεται από d και το δυαδικό τους μήκος από τ. Θέλουμε να υπολογίσουμε το πλήθος αλλά και τις πραγματικές ρίζες, γ, του f για τις οποίες ισχύει $A_i(\gamma) > 0$, $B_j(\gamma) < 0$ και $C_k(\gamma) = 0$ και $1 \le i \le n_1, 1 \le j \le n_2, 1 \le k \le n_3$. Έστω $n = n_1 + n_2 + n_3$.

Το παραπάνω πρόβλημα ονομάζεται *πρόβλημα των ταυτόχρονων ανισώσεων* (simultaneous inequalities) ή SI για συντομία.

Οι Ben-Or, Kozen, and Reif [15] παρουσίασαν τον αλγόριθμο BKR για την επίλυση του προβλήματος στην πιο γενική του μορφή, όπου τα πολυώνυμα είναι πολλών μεταβλητών. Ωστόσο, στις πολλές μεταβλητές ο BKR είχε εκθετική συμπεριφορά. Στη συνέχεια ο Canny [45] παρουσίασε μια παραλλαγή του BKR η οποία έχει ψευδο-πολυωνυμική πολυπλοκότητα στις πολλές μεταβλητές και η οποία έχει καλύτερη πολυπλοκότητα στην περίπτωση της μιας μεταβλητής. Πιο συγκεκριμένα, η αριθμητική πολυπλοκότητα του SI στην περίπτωση της μιας μεταβλητής είναι

$\mathcal{O}(n(R\,d\,\lg(R)\,\lg^2(d)+R^{2.376}))$, όπου R είναι το πλήθος των πραγματικών ριζών του A.

Οι Coste and Roy [58] εισήγαγαν την κωδικοποίηση των πραγματικών ριζών ενός πολυωνύμου κατά Thom, όπου οι ρίζες χαρακτηρίζονται και αναπαρίστανται από το πρόσημο (όλων) των παραγώγων του f πάνω σε αυτές. Βασιζόμενοι σε αυτή την αναπαράσταση παρουσίασαν ένα αλγόριθμο, βασισμένο στον BKR, για το πρόβλημα SI. Η προσέγγισή τους, όπως και οι προσεγγίσεις των Ben-Or et al. [15] και Canny [45], είναι συμβολική και ο αλγόριθμος τους είναι νόμιμος για πολυώνυμα ορισμένα σε οποιοδήποτε πραγματικό κλειστό σώμα. Η πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(N^8)$, όπου $N=\max\{d,n,\tau,R\}$, αλλά δεν χρησιμοποιούν τους γρήγορους αλγορίθμους για τον υπολογισμό ακολουθιών υπο-επιλυουσών.

Τέλος, οι Basu et al. [14], δείτε επίσης [231], παρουσιάζουν έναν αλγόριθμο για το SI, όπου γίνεται η παραδοχή ότι οι πραγματικοί αλγεβρικοί αριθμοί είναι σε αναπαράσταση με διάστημα απομόνωσης, ο οποίος έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(nd^6\tau^2)$ ή $\widetilde{\mathcal{O}}_B(N^9)$. Χρησιμοποιούν συνεχείς εκλεπτύνσεις των διαστημάτων απομόνωσης και δεν υποθέτουν γρήγορους αλγορίθμους για τον πολλαπλασιασμό.

Ο αλγόριθμός που παρουσίαζουμε βελτιώνει την πολυπλοκότητα του προβλήματος κατά δύο ή τρεις παράγοντες και είναι πολύ πιο απλός από όλες τις μέχρι τώρα προσεγγίσεις.

Πόρισμα 4.6. *Υπάρχει αλγόριθμος για το πρόβλημα των ταυτόχρονων ανισώσεων (SI) με πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(d^4\tau\max\{n,\tau\})$.

Απόδειξη: Αρχικά υπολογίζουμε τις πραγματικές ρίζες του f σε αναπαράσταση με διάστημα απομόνωσης με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (Θεωρ. 3.41). Υπάρχουν το πολύ d πραγματικές ρίζες. Για κάθε πραγματική ρίζα γ του f και για κάθε πολυώνυμο A_i, B_j και C_k, υπολογίζουμε το πρόσημο $\mathrm{sign}\left(A_i(\gamma)\right)$, $\mathrm{sign}\left(B_j(\gamma)\right)$ και $\mathrm{sign}\left(C_k(\gamma)\right)$. Ο υπολογισμός του προσήμου έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Πορ. 4.4) και στη χειρότερη περίπτωση πρέπει να επαναλάβουμε αυτή τη διαδικασία n φορές. Συνεπώς, η συνολική πολυπλοκότητα είναι $\widetilde{\mathcal{O}}_B(\max\{nd^4\tau, d^4\tau^2\})$. ΟΕΔ

Υπολογισμοί σε σώμα επέκτασης

Έστω $\gamma\cong(A,\mathbb{J})$. Ας υποθέσουμε προς τη στιγμή ότι το A είναι το ελάχιστο πολυώνυμο του γ. Αν στο $\mathbb{Q}$ επισυνάψουμε το γ τότε το καινούργιο σύνολο το συμβολίζουμε με $\mathbb{Q}(\gamma)$ και το ονομάζουμε σώμα επέκτασης. Η αλγεβρική δομή $\mathbb{Q}(\gamma)$ είναι ένας διανυσματικός χώρος πάνω στο $\mathbb{Q}$ και μία βάση του είναι η $\{1,\gamma,\ldots,\gamma^{d-1}\}$. Κατά συνέπεια τα στοιχεία $\beta\in\mathbb{Q}(\alpha)$ είναι πολυώνυμα ως προς γ βαθμού το πολύ $d-1$ με ακέραιους συντελεστές. Παρατηρούμε ότι πάντοτε μπορούμε να απαλείψουμε τους παρανομαστές με το ΕΚΠ.

Οι πράξεις της πρόσθεσης, της αφαίρεσης και του πολλαπλασιασμού υλοποιούνται όπως ακριβώς και στα πολυώνυμα μιας μεταβλητής (Παρ. 2.2). Η πιο βασική πράξη είναι ο υπολογισμός τους προσήμου, $\mathrm{sign}(\beta)$, $\beta\in\mathbb{Q}(\gamma)$. Ωστόσο, ο β είναι αναπαρίσταται με ένα πολυώνυμο μιας μεταβλητής ως προς γ, έστω f, συνεπώς $\mathrm{sign}(\beta)=\textsc{sign_at}(A,f)$. Προκειμένου να συγκρίνουμε $\beta_1,\beta_2\in\mathbb{Q}(a)$, αρκεί να υπολογίσουμε το $\mathrm{sign}(\beta_1-\beta_2)$.

Το γεγονός ότι όλες οι πράξεις υλοποιούνται είτε ως πράξεις πολυωνύμων είτε με τη χρήση των ακολουθιών υπο-επιλυουσών μας επιτρέπει να μην απαιτήσουμε το ελάχιστο πολυώνυμο

του γ, αλλά ένα οποιοδήποτε πολυώνυμο το οποίο έχει το γ ως ρίζα. Ωστόσο, χρειάζεται ειδική προσοχή στη διαίρεση β_1/β_2 [195]. Μια άλλη προσέγγιση [49] χρησιμοποιεί τη βάση Horner για να αναπαραστήσει τα πολυώνυμα που ορίζουν το $\beta \in \mathbb{Q}(\gamma)$.

4.2 Υπολογισμοί με δύο αλγεβρικούς αριθμούς

Θα παρουσιάσουμε αλγορίθμους που αφορούν υπολογισμούς με δύο αλγεβρικούς αριθμούς και την επίλυση πολυωνυμικών συστημάτων με δύο μεταβλητές. Όλοι οι αλγόριθμοι που θα παρουσιάσουμε βασίζονται στις προσημασμένες ακολουθίες υπο-επιλυουσών.

Αρχικά θα επεκτείνουμε τα αποτελέσματα της Εν. 2.3, που αφορούν υπολογισμούς με υπο-επιλύουσες με πολυνώνυμα σε μία μεταβλητή, σε πολυώνυμα με πολλές μεταβλητές. Στη συνέχεια θα παρουσιάσουμε έναν αλγόριθμο για τον υπολογισμό του προσήμου της αποτίμησης ενός πολυωνύμου (σε δύο μεταβλητές) πάνω σε δύο πραγματικούς αλγεβρικούς αριθμούς. Τέλος, θα παρουσιάσουμε δύο αλγορίθμους για την επίλυση πολυωνυμικών συστημάτων σε δύο μεταβλητές και έναν αλγόριθμο για το πρόβλημα των ταυτόχρονων ανισώσεων.

Υπο-επιλύουσες πολυωνύμων σε δύο μεταβλητές

Στους αλγορίθμους που θα παρουσιάσουμε θα χρησιμοποιήσουμε συστηματικά την τεχνική της *δυαδικής τμηματοποίησης* (binary segmentation) [24, 25, 159, 222, 263], η πρώτη παραλλαγή της οποίας πιθανώς οφείλεται στον Kronecker. Η ιδέα της δυαδικής τμηματοποίησης είναι η εξής: Εφαρμόζουμε έναν κατάλληλο ομομορφισμό εκτίμησης σε ένα ακέραιο πολυώνυμο, δηλαδή το αποτιμούμε πάνω σε έναν κατάλληλο ακέραιο αριθμό και προφανώς το αποτέλεσμα είναι ένας ακέραιος αριθμός. Στη συνέχεια, εφαρμόζουμε τον αλγόριθμο που μας ενδιαφέρει στον ακέραιο που είναι το απολέσμα της αποτίμησης και τέλος στο αποτέλεσμα (που είναι επίσης αριθμός) εφαρμόζουμε τον αντίστροφο ομομορφισμό εκτίμησης έτσι ώστε να πάρουμε το αποτέλεσμα. Ιδιαίτερη προσοχή απαιτείται έτσι ώστε ο αριθμός πάνω στον οποίο, αρχικά, θα αποτιμήσουμε το πολυώνυμό μας να είναι αρκετά μεγάλος έτσι ώστε στο τελικό αποτέλεσμα να είναι δυνατόν να εφαρμοστεί ο αντίστροφος ομομορφισμός. Οι διάφορες παραλλαγές αυτής της τεχνικής χαρακτηρίζονται ανάλογα με τον αλγόριθμο κωδικοποίησης, δηλαδή ανάλογα με το πως επιλέγουν τους ακεραίους που χρησιμοποιούν για τις αποτιμήσεις. Για το λόγο αυτό, το ακόλουθο λήμμα, που οφείλεται στον Klose [159] είναι πολύ σημαντικό, καθώς μέσω ενός ομομορφισμού εκτίμησης απεικονίζει πολυώνυμα σε ακεραιίους αριθμούς και εξασφαλίζει την ύπαρξη της αντίστροφης απεικόνισης.

Λήμμα 4.7. *Έστω $n, \lambda \in \mathbb{N}$. Αν $n \geq 2$ τότε $D \in \mathbb{N}$ αλλιώς $D = \infty$. Έστω $\nu = (\nu_1, \nu_2, \ldots, \nu_n)$ με $\nu_i = (\lambda+1)(D^{i-1} + D^{i-2} + \cdots + D + 1)$, $1 \leq i \leq n$. Ο ομομορφισμός εκτίμησης*

$$\begin{aligned} \phi_\nu : P_{\lambda,D} &\to \mathbb{Z} \\ f &\mapsto f(2^{\nu_1}, \ldots, 2^{\nu_n}) \end{aligned}$$

όπου $P_{\lambda,D} = \{f \in \mathbb{Z}[X_1, \ldots, X_n] \,|\, \mathcal{L}(f) \leq \lambda \wedge \deg(f) \leq D\}$, είναι $1-1$ και υπάρχει η αντίστροφη απεικόνιση, $\phi_\nu^{-1} : \phi_\nu(\mathbb{Z}) \to \mathbb{Z}[X_1, \ldots, X_n]$.

Επιπρόσθετα αν $f \in P_{\lambda,D}$ και $\deg(f) = p \leq D$ και $\mathcal{L}(f) = \sigma \leq \lambda$, τότε $\mathcal{L}(\phi_\nu(f)) \leq \nu_n p + \sigma + 1$.

Με απλά λόγια το Λημ. 4.7 μας εξασφαλίζει ότι αν επιλέξουμε ακεραίους σύμφωνα με τους κανόνες του τότε οι αποτιμήσεις διαφορετικών πολυωνύμων του $P_{\tau,D}$ δίνουν διαφορετικό αποτέλεσμα. Το επόμενο παράδειγμα αναδεικνύει τη χρήση του Λημ. 4.7.

Παράδειγμα 4.8. *Έστω το πολυώνυμο* $f = X^2 + 3X + 1 \in \mathbb{Z}[X]$. *Αντικαθιστώντας όπου* X *το* $2^2 = 4$ *έχουμε ότι* $\phi_1(f) = 4^2 + 3\cdot 4 + 1 = 29$. *Από το* 29 *προκύπτει το* f *ως εξής. Παρατηρούμε ότι* $\left(\mathsf{rem}\left(29, 4^2\right), \mathsf{quo}\left(29, 4^2\right)\right) = (13, 1)$ *οπότε ο μεγιστοβάθμιος συντελεστής είναι* 1. *Στη συνέχεια* $\left(\mathsf{rem}\left(13, 4^1\right), \mathsf{quo}\left(13, 4^1\right)\right) = (1, 3)$ *οπότε ο συντελεστής του γραμμικού όρου είναι* 3 *και τέλος αφού* $\left(\mathsf{rem}\left(1, 4^0\right), \mathsf{quo}\left(1, 4^0\right)\right) = (0, 1)$, *ο σταθερός όρος είναι* 1.

Επίσης παρατηρήστε ότι $(29)_{10} = (01\,11\,01)_2$. *Τα δύο πρώτα ψηφία της δυαδικής αναπαράστασης είναι ο συντελεστής του* X^2, *τα δύο επόμενα του* X *και τα δύο τελευταία του σταθερού όρου.*

Το επόμενο θεώρημα είναι η επέκταση του Θεωρ. 2.30 για πολυώνυμα σε πολλές μεταβλητές.

Θεώρημα 4.9

Έστω $f, g \in (\mathbb{Z}[Y_1, \ldots, Y_n])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ *και* $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. *Επιπρόσθετα, έστω* $\deg_{Y_i}(f) \leq d$ *και* $\deg_{Y_i}(g) \leq d$, *όπου* $1 \leq i \leq n$. *Ο υπολογισμός της ακολουθίας* $\mathbf{SR}(f, g)$ *ως προς* X, *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(2^{n-1}\, p^{n+2}\, q\, d^n\, \tau)$.

Απόδειξη: Θα χρησιμοποιήσουμε το Λημ. 4.7. Θεωρούμε τον ομομορφισμό εκτίμησης $\phi = \phi_n$, όπου $\nu_i = (\lambda+1)(D^{i-1}+\cdots+D+1)$, $\lambda = \max\{\mathcal{L}(\mathbf{SR}_j(f, g))\}$, και $D \geq \max\{\deg(\mathbf{SR}_j(f, g))\}$, όπου $1 \leq i \leq n$ και $0 \leq j \leq q$.

Τα πολυώνυμα $\phi(f)$ και $\phi(g)$ είναι μιας μεταβλητής, δηλαδή $\phi(f), \phi(g) \in \mathbb{Z}[X]$. Επίσης, $\deg(\phi(f)) = p \leq q = \deg(\phi(g))$ και τα $\mathcal{L}(\phi(f)) = \mathcal{L}(\phi(g))$ φράσσονται από

$$\mathcal{O}(d \cdot \lambda \cdot \sum_{i=1}^{n} \nu_i + \tau) = \mathcal{O}(d \cdot \lambda \cdot D^{n-1})$$

Από το Θεωρ. 2.30 η ακολουθία $\mathbf{SR}(\phi(f), \phi(g))$ υπολογίζεται σε $\mathcal{O}\left(p\, q\, \mathsf{M}\left(p \cdot d \cdot \lambda \cdot D^{n-1}\right)\right)$.

Απομένει να επιλέξουμε τα D και λ τα οποία εξαρτώνται από το βαθμό και το δυαδικό μήκος των πολυωνύμων $\mathbf{SR}_j \in \mathbb{Z}[X]$. Προκειμένου να φράξουμε το βαθμό των $\mathbf{SR}_j$ χρησιμοποιούμε τον ορισμό τους ως πολυώνυμα οριζουσών (Ορ. 2.19) και την ανισότητα του Hadamard [14] και συμπεραίνουμε ότι $\deg(\mathbf{SR}_j(f, g)) \leq d(p + q - 2j)$. Οπότε επιλέγουμε $D = 2dp$. Με την ίδια τεχνική φράσσουμε και το δυαδικό τους μήκος. Πιο συγκεκριμένα

$$\mathcal{L}(\mathbf{SR}_j(f, g)) \leq (\tau + \mathcal{L}(p + q))(p + q - 2j) + n\,\mathcal{L}((p + q)d + 1)$$

οπότε επιλέγουμε $\lambda = \mathcal{O}(p\tau + (p + n)\lg(pd))$ ή $\lambda = \widetilde{\mathcal{O}}(p\tau)$. Κατά συνέπεια ο υπολογισμός της ακολουθίας $\mathbf{SR}(\phi(f), \phi(g))$ έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(2^{n-1}\, p^{n+2}\, q\, d^n\, \tau)$.

Προκειμένου να υπολογίσουμε την ακολουθία $\mathbf{SR}(f, g)$ ως προς X, αρκεί να εφαρμόσουμε τον μετασχηματισμό ϕ^{-1} στα πολυώνυμα της ακολουθίας $\mathbf{SR}(\phi(f), \phi(g))$. ΟΕΔ

Ο Reischert [222] για την απόδειξη του Θεωρ. 4.9 χρησιμοποιεί επαναληπτική δυαδική τμηματοποίηση κατά Kronecker, δείτε επίσης [263]. Ωστόσο, ο μετασχηματισμός του Λημ. 4.7 έχει πιο εύκολο αλγόριθμο κωδικοποίησης και αποκωδικοποίησης [159]. Η δε αριθμητική πολυπλοκότητά του είναι γραμμική ως προς την έξοδο και απαιτεί μόνο προσθέσεις και ολισθήσεις [159] και σε καμία περίπτωση δεν επηρεάζει την πολυπλοκότητα όλων των αλγορίθμων που παρουσιάζουμε. Η πολυπλοκότητα υπολογισμού της ακολουθίας **SR**, Θεωρ. 4.9, που παρουσιάσαμε είναι ίδια με αυτή που παρουσίασε ο Reischert [222] και είναι καλύτερη κατά ένα παράγοντα 2 (και κάποιους πολυ-λογαριθμικούς παράγοντες) από αυτή που παρουσίασε ο Klose [159].

Το επόμενο θεώρημα επεκτείνει το Θεωρ. 2.31 και αφορά τον υπολογισμό της ακολουθίας **SRQ** σε πολυώνυμα πολλών μεταβλητών. Το φράγμα πολυπλοκλότητας που επιτυγχάνεται είναι το ίδιο με αυτό του Reischert [222].

Θεώρημα 4.10

Έστω $f, g \in (\mathbb{Z}[Y_1, \ldots, Y_n])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ *και* $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. *Επιπρόσθετα, έστω* $\deg_{Y_i}(f) \leq d$ *και* $\deg_{Y_i}(g) \leq d$, *όπου* $1 \leq i \leq n$.

Ο υπολογισμός της ακολουθίας $\mathbf{SRQ}(f, g)$, *οποιουδήποτε πολυωνύμου της ακολουθίας* $\mathbf{SR}(f, g)$, *του* $\mathtt{res}(f, g)$ *και του* $\gcd(f, g)$ *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(2^{n-1}\, p^{n+1}\, q\, d^n\, \tau)$.

Απόδειξη: Χρησιμοποιούμε τον ίδιο μετασχηματισμό, όπως και στην απόδειξη του Θεωρ. 4.9. Έτσι έχουμε $\phi(f), \phi(g) \in \mathbb{Z}[X]$ όπου $\deg(f) = p \geq q = \deg(g)$ και $\mathcal{L}(f) = \mathcal{L}(q) = \mathcal{O}(d \cdot \lambda \cdot D^{n-1})$. Ο υπολογισμός $\mathbf{SRQ}(\phi(f), \phi(g))$ έχει πολυπλοκότητα $\widetilde{\mathcal{O}}_B(p\, q\, d\, \lambda\, D^{n-1})$ (Θεωρ. 2.31). Αντικαθιστώντας $\lambda = \widetilde{\mathcal{O}}(p\tau)$ και $D = 2\, d\, p$ προκύπτει η ζητούμενη πολυπλοκότητα.

Καθώς τα $\mathtt{res}(f, g)$ και $\gcd(f, g)$ είναι στοιχεία της ακολουθίας **SRQ**, το θεώρημα αποδείχτηκε. ΟΕΔ

Με την εξαίρεση του υπολογισμού της επιλύουσας, η πολυπλοκότητα του προηγούμενου θεωρήματος είναι βέλτιστη. Αυτό δεν ισχύει μόνο για την περίπτωση της επιλύουσας.

Για πολυώνυμα σε δύο μεταβλητές τα δύο προηγούμενα θεωρήματα μας οδηγούν στα ακόλουθα πορίσματα:

Πόρισμα 4.11. *Έστω* $f, g \in (\mathbb{Z}[Y])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$, $\deg_Y(f) \leq d$, $\deg_Y(g) \leq d$ *και* $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. *Ο υπολογισμός της ακολουθίας* $\mathbf{SR}(f, g)$ *ως προς* X *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(p^3\, q\, d\, \tau)$.

Επιπρόσθετα $\mathcal{L}(\mathbf{SR}_j(f, g)) = \mathcal{O}(p\tau)$ *και* $\deg_Y(\mathbf{SR}_j(f, g)) \leq 2\, d\, p$.

Πόρισμα 4.12. *Έστω* $f, g \in (\mathbb{Z}[Y])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ $\deg_Y(f) \leq d$, $\deg_Y(g) \leq d$ *και* $\mathcal{L}(F) \leq \mathcal{L}(G) \leq \tau$. *Ο υπολογισμός της ακολουθίας* $\mathbf{SRQ}(f, g)$, *ως προς* X, *οποιουδήποτε πολυωνύμου στην ακολουθία* $\mathbf{SR}(f, g)$, *του* $\mathtt{res}(f, g)$ *και του* $\gcd(f, g)$ *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(p^2\, q\, d\, \tau)$.

Επιπρόσθετα $\deg_Y(\mathtt{res}(f, g)) \leq 2\, d\, p$.

Το επόμενο πόρισμα, περιέργως πως, δεν παρουσιάζεται στην βιβλιογραφία.

Πόρισμα 4.13. *Έστω* $f, g \in (\mathbb{Z}[Y])[X]$, *όπου* $\deg_X(f) = p \geq q = \deg_X(g)$ $\deg_Y(f) \leq d$, $\deg_Y(g) \leq d$ *και* $\mathcal{L}(F), \mathcal{L}(G) \leq \tau$. *Ο υπολογισμός της αποτίμησης* $\mathbf{SR}(f, g\,;\, \mathsf{a})$, *ως προς* X, *όπου* $\mathcal{L}(\mathsf{a}) = \sigma$, *έχει πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(q\ \max\{p^2\, d\, \tau, q\, \sigma\})$.

Επιπρόσθετα $\mathbf{SR}_j(\mathsf{a}) \in \mathbb{Z}[Y]$, $\deg_Y(\mathbf{SR}_j(\mathsf{a})), \deg(\mathbf{SR}_j(\mathsf{a})) \leq 2\, d\, p$ *και* $\mathcal{L}(\mathbf{SR}_j(\mathsf{a})) = \mathcal{O}(\max\{p\, \tau, d\, \sigma\})$.

Απόδειξη: Θα χρησιμοποιήσουμε το Λημ. 4.7. Θεωρούμε τον ομομορφισμό εκτίμησης $\phi = \phi_1$, όπου $\nu_1 = \nu = (L+1)$, $L = \max\{\mathcal{L}(\mathbf{SR}_j(f, g))\} = \mathcal{O}(p\, \tau)$, $0 \leq j \leq d$. Για τα πολυώνυμα $\phi(f), \phi(g) \in \mathbb{Z}[X]$ ισχύει $\mathcal{L}(\phi(f)) = \mathcal{L}(\phi(g)) = \mathcal{O}(d\, L + \tau) = \mathcal{O}(d\, L)$.

Υπολογίζουμε την αποτίμηση $\mathbf{SR}(\phi(f), \phi(g)\,;\, \mathsf{a})$ με πολυπλοκότητα $\widetilde{\mathcal{O}}_B(q\ \max\{p\, d\, L, q\, \sigma\})$ ή $\widetilde{\mathcal{O}}_B(q\ \max\{p^2\, d\, \tau, q\, \sigma\})$ (Θεωρ. 2.32). Για κάθε ένα $\mathbf{SR}_j(\phi(f), \phi(g)\,;\, \mathsf{a}) \in \mathbb{Z}$, $0 \leq j \leq q$, εφαρμόζουμε τον μετασχηματισμό ϕ^{-1} προκειμένου να πάρουμε το $\mathbf{SR}_j(f, g\,;\, \mathsf{a}) \in \mathbb{Z}[X]$.

Προκειμένου να φράξουμε το βαθμό των $\mathbf{SR}_j$ ως προς Y χρησιμοποιούμε τον ορισμό τους ως πολυώνυμα οριζουσών (Ορ. 2.19) και την ανισότητα του Hadamard [14] και συμπεραίνουμε ότι $\deg_Y(\mathbf{SR}_j(\mathsf{a})) = \deg(\mathbf{SR}_j(\mathsf{a})) \leq 2\, d\, p$. Και με την ίδια τεχνική, εφόσον $\mathcal{L}(\mathbf{SR}_j(f, g)) = \mathcal{O}(p\, \tau)$ συνάγουμε ότι $\mathcal{L}(\mathbf{SR}_j(f, g\,;\, \mathsf{a})) = \mathcal{O}(\max\{p\, \tau, d\, \sigma\})$ (Εν. 2.2). ΟΕΔ

Το γεγονός ότι οι (προσημασμένες) ακολουθίες υπο-επιλυουσών (signed subresultant sequences) έχουν καλή συμπεριφορά ακόμα κι όταν οι συντελεστές των πολυωνύμων είναι παράμετροι, δείτε [118, 119] και Εν. 2.3, βρίσκει εφαρμογή όταν απαιτούνται υπολογισμοί με πολυώνυμα πολλών μεταβλητών (στην περίπτωσή μας με δύο μεταβλητές). Αν f και g είναι δύο πολυώνυμα με παραμετρικούς συντελεστές, τέτοια ώστε ο βαθμός τους να μην μεταβάλλεται για οποιαδήποτε τιμή των παραμέτρων, ο υπολογισμός της ακολουθίας $\mathbf{SR}(f, g)$ μας εγγυάται ότι για οποιαδήποτε τιμή των παραμέτρων η ακολουθία είναι ορθή. Θα χρησιμοποιήσουμε αυτή την ιδιότητα, στην περίπτωση που τα f και g είναι πολυώνυμα σε δύο μεταβλητές, προκειμένου να υπολογίσουμε την $\mathbf{SR}(f, g)$ ως προς Y (ή ως προς X) θεωρώντας ότι τα πολυώνυμα ανήκουν στο $(\mathbb{Z}[X])[Y]$ (ή στο $(\mathbb{Z}[Y])[X]$).

Η επόμενη υπόθεση είναι πολύ χρήσιμη για τη συνέχεια.

Ορισμός 4.14 (Υπόθεση της γενικής θέσης). *Δύο πολυώνυμα* $f, g \in \mathcal{R}[X, Y]$ *είναι σε γενική θέση αν* $\mathsf{lead}_Y(f) \neq 0$, $\mathsf{lead}_Y(g) \neq 0$ *και για κάθε* $(\alpha_1, \beta), (\alpha_2, \beta) \in \mathcal{K}^2$ *τέτοια ώστε* $f(\alpha_1, \beta) = g(\alpha_1, \beta) = 0$ *και* $f(\alpha_2, \beta) = g(\alpha_2, \beta) = 0$ *να ισχύει* $\alpha_1 \neq \alpha_2$.

Με άλλα λόγια, η υπόθεση της γενικής θέσης απαιτεί οι λύσεις του συστήματος $f = g = 0$ με κοινή τεταγμένη να έχουν διαφορετική τετμημένη και οι μεγιστοβάθμιοι όροι ως προς Y να μην μηδενίζονται. Το ακόλουθο θεώρημα, το οποίο βασίζεται στην υπόθεση της γενικής θέσης, είναι εξέχουσας σημασίας:

Θεώρημα 4.15

[14, 116, 117] Έστω $f, g \in \mathcal{R}[X, Y]$ *τα οποία είναι σχετικά πρώτα αν τα θεωρήσουμε πολυώνυμα ως προς* Y *και ικανοποιούν την υπόθεση της γενικής θέσης. Έστω*

$$\mathbf{SR}_j(f, g) = \mathbf{sr}_j(X) Y^j + \mathbf{sr}_{j,i-1}(X) Y^{j-1} + \cdots + \mathbf{sr}_{j,0}(X) \quad \in (\mathcal{R}[X])[Y]$$

τα πολυώνυμα της ακολουθίας $\mathbf{SR}(f, g)$ *ως προς* Y, *όπου* $\mathbf{sr}_j = \mathbf{psc}_j$. *Αν* $(\alpha, \beta) \in \mathcal{K}^2$, *τέτοιο ώστε* $f(\alpha, \beta) = g(\alpha, \beta) = 0$ *τότε υπάρχει δείκτης* k *τέτοιος ώστε*

$$\mathbf{sr}_0(\alpha) = \cdots = \mathbf{sr}_{k-1}(\alpha) = 0, \quad \mathbf{sr}_k(\alpha) \neq 0, \quad \beta = -\frac{1}{k} \frac{\mathbf{sr}_{k,k-1}(\alpha)}{\mathbf{sr}_k(\alpha)}$$

Απόδειξη: Έστω ότι για κάποια ρίζα $\alpha \in \mathcal{K}$ του $\mathbf{sr}_0 = \mathbf{SR}_0 \in \mathcal{R}[X]$ ισχύει $\mathbf{sr}_0(\alpha) = \mathbf{sr}_1(\alpha) = 0, \ldots, \mathbf{sr}_{k-1}(\alpha) = 0$ και $\mathbf{sr}_k(\alpha) \neq 0$. Στην ακολουθία $\mathbf{SR}(f, g)$, η οποία είναι ως προς Y, κάνουμε την αντικατάσταση $X = \alpha$. Την προκύπτουσα ακολουθία, η οποία έχει πολυώνυμα στον χώρο $(\mathbb{Z}[\alpha])[Y]$, τη συμβολίσουμε $\widetilde{\mathbf{SR}}$. Λόγω των καλών ιδιοτήτων των ακολουθιών υποεπιλυουσών, είμαστε βέβαιοι ότι η ακολουθία είναι η ίδια με αυτή που θα είχαμε υπολογίσει αν είχαμε κάνει την αντικατάσταση $X = \alpha$ μόνο στα f και g και ακολούθως είχαμε υπολογίσει την ακολουθία.

Εφόσον ο πρώτος μη μηδενικός πρωταρχικός συντελεστής της $\widetilde{\mathbf{SR}}$ έχει δείκτη k, ο ΜΚΔ των $\widetilde{f}, \widetilde{g} \in (\mathbb{Z}[\alpha])[Y]$ είναι το πολυώνυμο $\widetilde{\mathbf{SR}}_k$, το οποίο έχει βαθμό k, και άρα τα $\widetilde{f}, \widetilde{g}$ έχουν k κοινές ρίζες (Θεωρ. 2.20). Με άλλα λόγια οι Y συντεταγμένες των λύσεων του συστήματος $f = g = 0$, που έχουν για X συντεταγμένη το α, είναι οι ρίζες του $\widetilde{\mathbf{SR}}_k$. Ωστόσο, τα f και g είναι σε γενική θέση, συνεπώς κάθε λύση του συστήματος έχει διαφορετική X συντεταγμένη. Κατά συνέπεια το $\widetilde{\mathbf{SR}}_k$ πρέπει να έχει μία και μόνο μία ρίζα και επειδή είναι βαθμού k, έχει μία πραγματική ρίζα πολλαπλότητας k.

Άρα $\widetilde{\mathbf{SR}}_k = (k \cdot \mathbf{sr}_k(\alpha)\, Y + \mathbf{sr}_{k,k-1}(\alpha))^k$ και συνεπώς η ρίζα του είναι $-\frac{1}{k}\frac{\mathbf{sr}_{k,k-1}(\alpha)}{\mathbf{sr}_k(\alpha)}$. ΟΕΔ

Υπολογισμός προσήμου

Algorithm 17: SIGN_AT(F, α, β)

Input: $F \in \mathbb{Z}[X, Y], \alpha \cong (A, \mathbb{J}_1 = [\mathsf{a}_1, \mathsf{b}_1]), \beta \cong (B, \mathbb{J}_2 = [\mathsf{a}_2, \mathsf{b}_2])$
Output: $\mathrm{sign}(F(\alpha, \beta))$

1 $Q_1 \leftarrow \emptyset$
2 $L_1 \leftarrow \mathbf{SR}_X(A, F\,;\, \mathsf{a}_1)$
3 **foreach** $f \in L_1$ **do** $Q_1 \leftarrow$ ADD$(Q_1,$ SIGN_AT$(f, \beta))$
4 $Q_2 \leftarrow \emptyset$
5 $L_2 \leftarrow SR_X(A, F\,;\, \mathsf{b}_1)$
6 **foreach** $f \in L_2$ **do** $Q_2 \leftarrow$ ADD$(Q_2,$ SIGN_AT$(f, \beta))$
7 RETURN $(\mathrm{VAR}(Q_1) - \mathrm{VAR}(Q_2)) \cdot \mathrm{sign}(A'(\alpha))$

Όπως και στην περίπτωση των υπολογισμών με έναν πραγματικό αλγεβρικό αριθμό, ο πιο σημαντικός υπολογισμός είναι το πρόσημο της αποτίμησης. Πιο συγκεκριμένα, θεωρούμε $F \in \mathbb{Z}[X, Y]$, $\alpha \cong (A(x), \mathbb{J}_1)$ και $\beta \cong (B(X), \mathbb{J}_2)$ όπου $\mathbb{J}_1 = [a_1, b_1]$, $\mathbb{J}_2 = [a_2, b_2]$. Θέλουμε να υπολογίσουμε το πρόσημο της αποτίμησης $F(\alpha, \beta)$. Τον υπολογισμό αυτό θα τον συμβολίσουμε με SIGN_AT(F, α, β). Ο ψευδο-κώδικας του αλγορίθμου παρουσιάζεται στον Αλγ. 17.

Θεώρημα 4.16

Έστω $F \in \mathbb{Z}[X, Y]$ τέτοιο ώστε $\deg_X(F) = \deg_Y(F) = n_1$ και $\mathcal{L}(F) = \sigma$ και δύο πραγματικοί

αλγεβρικοί αριθμοί $\alpha \cong (A, \mathcal{I}_\alpha) = [\mathsf{a}_1, \mathsf{b}_1]$, $\beta \cong (B, \mathcal{I}_\beta) = [\mathsf{a}_2, \mathsf{b}_2]$ *όπου* $A, B \in \mathbb{Z}[X]$, $\deg(A) = \deg(B) = n_2$, $\mathcal{L}(A) = \mathcal{L}(B) = \sigma$ *και* $\mathcal{I}_\alpha, \mathcal{I}_\beta \in \mathbb{Q}^2$ *και το δυαδικό μήκος των άκρων τους φράσσεται από* $\mathcal{O}(n_2\,\sigma)$.

Μπορούμε να υπολογίσουμε το πρόσημο της αποτίμησης του F *πάνω στους* α *και* β, *δηλαδή* SIGN_AT(F, α, β), *χρησιμοποιώντας του Αλγ. 17 με πολυπλοκότητα* $\widetilde{\mathcal{O}}_B(n_1^3\, n_2^3\, \sigma)$, *υποθέτουτας ότι* $n_1 \leq n_2$.

Απόδειξη: Αρχικά θεωρούμε το F ως πολυώνυμο ως προς X με συντελεστές πολυώνυμα ως προς Y, δηλαδή $F \in (\mathbb{Z}[Y])[X]$ και προσπαθούμε να υπολογίσουμε το πρόσημό του αν το αποτιμήσουμε πάνω στο α, όπως ακριβώς κάναμε και στην περίπτωση της μίας μεταβλητής (Αλγ. 15).

Υπολογίζουμε την αποτίμηση της ακολουθίας $\mathbf{SR}(A, F)$ ως προς X, πάνω στο a_1, δηλαδή την ακολουθία $\mathbf{SR}(A, F\,;\, \mathsf{a}_1)$ (Γραμμή 2 στον Αλγ. 17). Ο υπολογισμός αυτός κοστίζει $\widetilde{\mathcal{O}}_B(n_1^2\, n_2^2\, \sigma)$ (Πορ. 4.13). Η ακολουθία $\mathbf{SR}(A, F\,;\, \mathsf{a}_1)$ (L_1 στον Αλγ. 17) περιέχει $\mathcal{O}(n_1)$ πολυώνυμα στο $\mathbb{Z}[Y]$ με βαθμούς $\mathcal{O}(n_1\, n_2)$ και δυαδικό μήκος $\mathcal{O}(n_1\, n_2\, \sigma)$.

Για κάθε ένα πολυώνυμο στην $\mathbf{SR}(A, F\,;\, \mathsf{a}_1)$, υπολογίζουμε το SIGN_AT$(\mathbf{SR}_j(A, F\,;\, \mathsf{a}_1), \beta)$ (Γραμμή 3 στον Αλγ. 17) και μετράμε τις εναλλαγές προσήμων. Ο υπολογισμός SIGN_AT$(\mathbf{SR}_j(A, F\,;\, \mathsf{a}_1), \beta)$ κοστίζει $\widetilde{\mathcal{O}}_B(n_1^2\, n_2^3\, \sigma)$ (Θεωρ. 2.32) και καθώς χρειαζόμαστε $\mathcal{O}(n_1)$ τέτοιους υπολογισμούς, το συνολικός κόστος είναι $\widetilde{\mathcal{O}}_B(n_1^3\, n_2^3\, \sigma)$.

Κάνουμε το ίδιο για το δεξί άκρο του $\mathcal{I}_\alpha$ το b_1 και αφαιρούμε τις εναλλαγές προσήμων. Ο υπολογισμός του $\mathrm{sign}(A'(\alpha))$ γίνεται όπως στον Αλγ. 15 και κοστίζει $\widetilde{\mathcal{O}}_B(n_2^3\, \sigma)$.

Συμπεραίνουμε ότι η συνολική πολυπλοκότητα του αλγορίθμου είναι $\widetilde{\mathcal{O}}_B(n_1^3\, n_2^3\, \sigma)$. ΟΕΔ

Από όσο είμαστε σε θέση να γνωρίζουμε η πολυπλοκότητα του προηγούμενου θεωρήματος δεν ήταν γνωστή μέχρι σήμερα. Μπορούμε να γενικεύσουμε το Θεώρημα στον υπολογισμό προσήμου της αποτίμησης ενός πολυωνύμου με k μεταβλητές πάνω σε k πραγματικούς αλγεβρικούς αριθμούς, ακολουθώντας την προσέγγιση του Sakkalis [234]. Ωστόσο, το γεγονός ότι χρησιμοποιούμε ακολουθίες υπο-επιλυουσών, αντί για προσημασμένες Ευκλείδιες ακολουθίες, βελτιώνει τόσο τη θεωρητική [14] όσο και την πρακτική πολυπλοκότητα [66, 87, 275].

Δύο αλγόριθμοι για την επίλυση συστημάτων

Θεωρούμε το σύστημα

$$\begin{cases} F = \displaystyle\sum_{1 \leq i \leq d} \sum_{1 \leq j \leq d} a_{i,j} X^i Y^j = 0 \\ G = \displaystyle\sum_{1 \leq i \leq d} \sum_{1 \leq j \leq d} d_{i,j} X^i Y^j = 0 \end{cases} \tag{4.1}$$

Υποθέτουμε ότι τα πολυώνυμα του συστήματος $F, G \in \mathbb{Z}[X, Y]$ είναι σχετικά πρώτα και ότι $\deg(F) = \deg(G) = n$ και $\mathcal{L}(F) = \mathcal{L}(G) = \sigma$. Θα παρουσιάσουμε δύο αλγορίθμους και την ανάλυσή τους που αφορούν την πραγματική επίλυση του παραπάνω συστήματος. Οι ιδέα και των δύο αλγορίθμων είναι να προβάλλουμε το σύστημα στον X και στον Y άξονα, να υπολογίσουμε

τις συντεταγμένες των λύσεων και στη συνέχεια με κάποιο τρόπο να τις ταιριάξουμε. Η διαφορά των αλγορίθμων έγκειται στον τρόπο ταιριάσματος. Οι προβολές του συστήματος στους άξονες επιτυγχάνονται με την βοήθεια της επιλύουσας. Υπενθυμίζουμε, δείτε Εν. 2.2, ότι η επιλύουσα δύο πολυωνύμων σε δύο μεταβλητές *απαλείφει* τη μία μεταβλητή. Η έξοδος των αλγορίθμων είναι μια λίστα με ζεύγη πραγματικών αλγεβρικών αριθμών, που είναι λύσεις του συστήματος και αν είναι δυνατόν μια λίστα με τις πολλαπλότητες.

Αν και το πρόβλημα της επίλυσης συστημάτων είναι μια από τις πιο ενεργές επιστημονικές περιοχές στην κοινότητα των αλγεβρικών αλγορίθμων, ο κύριος όγκος των εργασιών επικεντρώνεται σε πολυωνυμικά συστήματα με k μεταβλητές, δείτε για παράδειγμα[1] [46, 84, 95, 168, 197, 198, 199, 200]. Αυτός είναι ο λόγος που αποτελέσματα σε πολυωνυμικά συστήματα 2 μεταβλητών είναι αρκετά περιορισμένα.

Ο απλός αλγόριθμος (NAIVE_SOLVE)

Algorithm 18: NAIVE_SOLVE(F, G)

Input: $F, G \in \mathbb{Z}[X, Y]$

Output: Οι πραγματικές λύσεις του συστήματος $F = G = 0$

```
1  R_x ← res_y(F, G)
2  L_x, M_x ← CONSTRUCT(R_x)
3  R_y ← res_x(F, G)
4  L_y, M_y ← CONSTRUCT(R_y)
5  Q ← ∅
6  foreach α ∈ L_x do
7      foreach β ∈ L_y do
8          if SIGN_AT(F, α, β) = 0 ∧ SIGN_AT(G, α, β) = 0 then
9              Q ← ADD(Q, {α, β})
10 RETURN Q
```

Ο αλγόριθμος NAIVE_SOLVE, ο ψευδο-κώδικας του οποίου παρουσιάζεται στον Αλγ. 18, είναι ο πλέον προφανής. Υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις X και Y συντεταγμένες των πραγματικών λύσεων του συστήματος ως λύσεις των προβολών $\mathtt{res}_Y(F, G)$ και $\mathtt{res}_Y(F, G)$ και στη συνέχεια τις ταιριάζουμε χρησιμοποιώντας τον αλγόριθμο SIGN_AT (Αλγ. 17).

Η είσοδος του αλγορίθμου είναι τα δύο πολυώνυμα $F, G \in \mathbb{Z}[X, Y]$ και η έξοδος του είναι μία λίστα από ζεύγη πραγματικών αλγεβρικών αριθμών σε αναπαράσταση με διάστημα απομόνωσης, η οποία συμβολίζεται με Q στον Αλγ. 18.

Η ορθότητα του αλγορίθμου προκύπτει από το γεγονός ότι αφενός μεν όλες οι πραγματικές λύσεις του συστήματος προκύπτουν από ως πραγματικές λύσεις των $\mathtt{res}_x(F, G)$ και $\mathtt{res}_y(F, G)$

[1] Η βιβλιογραφία για τα πολυωνυμικά συστήματα πολλών μεταβλητών που παρουσιάζουμε είναι ενδεικτική.

και αφετέρου δε από το γεγονός ότι ένα ζεύγος $(\alpha, \beta) \in \mathbb{R}^2_{alg}$ είναι λύση του συστήματος αν και μόνο αν $F(\alpha, \beta) = G(\alpha, \beta) = 0$.

Το επόμενο θεώρημα περιγράφει αναλυτικά τα βήματα του αλγορίθμου και αναλύει την πολυπλοκότητά τους.

Θεώρημα 4.17 (NAIVE_SOLVE)

Έστω $F, G \in \mathbb{Z}[X, Y]$ σχετικά πρώτα, με συνολικό βαθμό που φράσσεται από n και μέγιστο δυαδικό μήκος συντελεστών που φράσσεται από σ. Η πραγματική επίλυση του συστήματος $F = G = 0$ με τον αλγόριθμο NAIVE_SOLVE *έχει πολυπλοκότητα $\tilde{\mathcal{O}}_B(n^{14}\,\sigma)$, με την υπόθεση ότι $\sigma = \mathcal{O}(n^4)$.*

Απόδειξη: Καταρχάς υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις X συντεταγμένες των πραγματικών λύσεων του συστήματος, υπολογίζοντας την επιλύουσα των F και G ως προς Y, R_x, (Γραμμή 1 στον Αλγ. 18). Η πολυπλοκότητα του βήματος είναι $\tilde{\mathcal{O}}_B(n^4\sigma)$ (Πορ. 4.12). Παρατηρούμε ότι $\deg(R_x) = \mathcal{O}(n^2)$ και $\mathcal{L}(R_X) = \mathcal{O}(n\,\sigma)$. Υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που είναι ρίζες του R_x, με αναπαράσταση διαστήματος απομόνωσης (Γραμμή 2 στον Αλγ. 18) με πολυπλοκότητα $\tilde{\mathcal{O}}_B(n^{10}\sigma^2)$ (Θεωρ. 3.41) και τους τοποθετούμε στη λίστα L_x.

Ομοίως και με την ίδια πολυπλοκότητα, υπολογίζουμε τους πραγματικούς αλγεβρικούς αριθμούς που αντιστοιχούν στις Y συντεταγμένες των λύσεων του συστήματος (Γραμμές 3 και 4 στον Αλγ. 18) και τους τοποθετούμε στη λίστα L_y.

Η αναπαράσταση των πραγματικών αλγεβρικών αριθμών που έχουμε υπολογίσει, περιέχει το χωρίς τετράγωνα μέρος του R_x ή του R_y. Και στις δύο περιπτώσεις το δυαδικό μήκος του πολυωνύμου είναι $\mathcal{O}(n + n\,\sigma) = \mathcal{O}(n\,\sigma)$ (Θεωρ. 2.34). Τα διαστήματα απομόνωσης έχουν άκρα ρητούς αριθμούς με δυαδικό μήκος $\mathcal{O}(n^3\,\sigma)$ (Σημ. 3.24). Τέλος, τόσο το μέγεθος της L_x όσο και της L_y είναι $\mathcal{O}(n^2)$.

Σχηματίζουμε όλα τα δυνατά ζεύγη πραγματικών αλγεβρικών αριθμών και ελέγχουμε αν μηδενίζουν τόσο το F όσο και το G (Γραμμή 8 στον Αλγ. 18). Αυτό επιτυγχάνεται με τον αλγόριθμο SIGN_AT (Αλγ. 17). Πρέπει να πραγματοποιήσουμε το πολύ $\mathcal{O}(n^4)$ τέτοιους υπολογισμούς και κάθε ένας από αυτούς κοστίζει $\tilde{\mathcal{O}}_B(n^{10}\sigma)$ (Θεωρ. 4.16).

Συνεπώς, η συνολική πολυπλοκότητα είναι $\tilde{\mathcal{O}}_B(n^{14}\sigma)$. ΟΕΔ

Ο αλγόριθμος που παρουσιάσαμε, αν και προφανής, δεν έχει αναλυθεί μέχρι σήμερα. Το μειονέκτημα του αλγορίθμου NAIVE, εκτός από τη μεγάλη θεωρητική του πολυπλοκότητα είναι ότι δεν υπολογίζει τις πολλαπλότητες των λύσεων. Επίσης, η πολυπλοκότητα στην πράξη του αλγορίθμου SIGN_AT (Αλγ. 17) είναι πολύ μεγάλη. Από την άλλη η απλότητά του το κάνει πολύ εύκολα υλοποιήσιμο και ιδιαίτερα ελκυστικό. Μια παραλλαγή του αλγορίθμου NAIVE_SOLVE, όπου ο έλεγχος για το αν ένα ζεύγος είναι λύση του συστήματος πραγματοποιείται με συνεχώς βελτιούμενες προσεγγίσεις των πραγματικών αλγεβρικών αριθμών, χρησιμοποιείται πολύ συχνά στην πράξη.