Εθνικο & Καποδιστριακο Πανεπιστημιο Αθηνων
Τμημα Πληροφορικης & Τηλεπικοινωνιων
ΠΜΣ Υπολογιστικη Επιστημη

Σημειώσεις Υπολογιστικής Άλγεβρας

Άγγελος Μαντζαφλάρης

Χειμερινό εξάμηνο 2006-2007

Οι παρούσες σημειώσεις προέρχονται από τις διαλέξεις των καθηγητών Ιωάννη Εμίρη(Τμήμα Πληροφορικής) και Ευάγγελου Ράπτη(Τμήμα Μαθηματικών) στα πλαίσια του μεταπτυχιακού μαθήματος *Υπολογιστική Άλγεβρα*, το οποίο διδάχθηκε κατά το χειμερινό εξάμηνο 2006-2007 στους φοιτητές του Προγράμματος Μεταπτυχιακών Σπουδών του Τμήματος Πληροφορικής και του Μεταπτυχιακού Προγράμματος στη Λογική και Θεωρία Αλγορίθμων.

Το κύριο θέμα του μαθήματος είναι η επίλυση συστημάτων πολυωνυμικών εξισώσεων πολλών μεταβλητών· γίνεται μια εισαγωγή στις ακολουθίες Sturm, στην κλασσική απαλοίφουσα, στις βάσεις Gröbner και στη θεωρία αραιής απαλοιφής. Τα θέματα παρουσιάζονται σαν αυτοτελή μαθήματα, περίπου όπως τα παρακολούθησε ο γράφων κατά τη διάρκεια του εξαμήνου. Οι παρατηρήσεις σας είναι ευπρόσδεκτες στην ηλεκτρονική διεύθυνση amantzaf@math.uoa.gr.

Άγγελος Μαντζαφλάρης
15 Οκτωβρίου 2007

Περιεχόμενα

Μάθημα 1

Εισαγωγή

Στο μάθημα αυτό θα ασχοληθούμε με μεθόδους εύρεσης ριζών πολυωνυμικών εξισώσεων και συστημάτων με χρήση αλγεβρικών αλγορίθμων. Οι αλγεβρικοί αλγόριθμοι αφορούν σε αλγεβρικά προβλήματα και, σε αντίθεση με αριθμητικές και αναλυτικές μεθόδους, χαρακτηρίζονται από απόλυτη ακρίβεια αποτελέσματος. Η απαίτηση αυτή καθιστά την υλοποίησή τους σε υπολογιστικές μηχανές πεπερασμένης ακρίβειας δύσκολη, όμως διάφορα υπολογιστικά πακέτα παρέχουν το απαραίτητο υπόβαθρο για να υλοποιηθούν τέτοιοι αλγόριθμοι. Το αντίτιμο είναι το σχετικά υψηλό υπολογιστικό κόστος λόγω της πιθανής έκρηξης του μεγέθους των (ενδιάμεσων) τιμών. Βέβαια το αν οι αριθμητικές μέθοδοι είναι ταχύτερες των αλγεβρικών αποτελεί τη μεγάλη πρόκληση(ανοικτό πρόβλημα) στην υλοποίηση τέτοιων αλγορίθμων.

Η περιοχή των αλγεβρικών αλγορίθμων ονομάζεται επίσης «άλγεβρα με υπολογιστή» (computer algebra), «υπολογιστική άλγεβρα» (computational algebra) ή «συμβολική επεξεργασία» (symbolic computation) διότι επεξεργάζεται σύμβολα: μεταβλητές x, y, πολυώνυμα κλπ.

1.1 Υπολογιστικά Μοντέλα και Ασυμπτωτικοί Συμβολισμοί

Η μελέτη διαφορετικών αλγόριθμων που επιλύουν το ίδιο πρόβλημα απαιτεί τη σύγκρισή τους με κάποιο κοινό μέτρο. Η μαθηματική εκτίμηση των υπολογιστικών πόρων που απαιτεί η εκτέλεση ενός αλγόριθμου ονομάζεται ανάλυση του αλγόριθμου.

Για τις ανάγκες του μαθήματος θα θεωρήσουμε δυο παραλλαγές του μοντέλου RAM(Random Access Machine - Μηχανή Άμεσης Προσπέλασης Μνήμης), στο οποίο οι εντολές εκτελούνται σειριακά και κάθε στοιχειώδες υπολογιστικό βήμα έχει μοναδιαίο κόστος. Σαν στοιχειώδη υπολογιστικά βήματα θεωρούμε τις βασικές αριθμητικές και λογικές πράξεις, την προσπέλαση της μνήμης για ανάγνωση ή εγγραφή καθώς και τις συγκρίσεις, τον υπολογισμό του ακέραιου μέρους, την εξαγωγή μιας τετραγωνικής ρίζας, ενίοτε τον υπολογισμό ενός πηλίκου ή υπολοίπου.

Real RAM (Arithmetic RAM). Στο μοντέλο αυτό κάθε πραγματικός αριθμός αναπαρίσταται με απόλυτη (απεριόριστη) ακρίβεια. Φυσικά κάτι τέτοιο είναι μη ρεαλιστικό. Εδώ το στοιχειώδες υπολογιστικό βήμα είναι η εκτέλεση μιας πράξης (όπως αυτές που αναφέρθηκαν παραπάνω) μεταξύ δυο πραγματικών αριθμών. Η αριθμητική πολυπλοκότητα συμβολίζεται με $O_A(\cdot)$.

Boolean RAM. Για μια ακριβέστερη μελέτη πολυπλοκότητας, χρησιμοποιούμε τη δυαδική RAM. Εδώ βλέπουμε κάθε στοιχείο $x \in \mathbb{Z}$ ως μια ακολουθία δυαδικών ψηφίων(bits) μήκους $\lceil \log_2 x \rceil$ στη μνήμη του υπολογιστή ή ακόμη και σαν ακολουθία από λέξεις(words) σε μια ορισμένη αναπαράσταση. Το στοιχειώδες υπολογιστικό βήμα είναι η πράξη μεταξύ δυο ψηφίων(ή λέξεων) της αναπαράστασης του αριθμού. Η δυαδική πολυπλοκότητα συμβολίζεται ως $O_B(\cdot)$.

Ένας αλγόριθμος θα λέμε ότι είναι γραμμικός, αν η πολυπλοκότητά του είναι γραμμική στο μέγεθος της εισόδου. Αντίστοιχα ορίζονται οι πολυωνυμικοί αλγόριθμοι, οι εκθετικοί κοκ. Παρατηρήστε εδώ πως αναλύοντας έναν αλγόριθμο με είσοδο έναν $x \in \mathbb{R}$ στο δυαδικό μοντέλο η είσοδος έχει μέγεθος $\lceil \log_2 x \rceil$, ενώ με χρήση του αριθμητικού μοντέλου η είσοδος έχει μέγεθος 1(ή κάποια σταθερά).

Κάποιες φορές μας ενδιαφέρουν οι μεγαλύτεροι μόνο από τους όρους του γινομένου που εμφανίζονται στην πολυπλοκότητα ενός αλγόριθμου. Τότε θα παραλείπουμε τους λογαριθμικούς παράγοντες και θα συμβολίζουμε

με $O_A^*(\cdot)$ ή $O_B^*(\cdot)$. Π.χ. Το γινόμενο δυο πολυωνύμων με τον αλγόριθμο FFT έχει πολυπλοκότητα $O_A(n \log n)$, δηλαδή $O_A^*(n)$(σημειώνεται πως τέτοιοι αλγόριθμοι καλούνται «σχεδόν γραμμικοί»).

Στα παραπάνω το $O(\cdot)$ είναι ο γνωστός συμβολισμός στην ανάλυση της ασυμπτωτικής συμπεριφοράς αλγορίθμων. Η ασυμπτωτική εκτίμηση εξετάζει την τάξη (χρονικού ή ακόμη και χωρικού) μεγέθους του αλγόριθμου, γι αυτό και πρακτικά ενδιαφέρεται για τον κυρίαρχο όρο της ακριβής καταμέτρησης μεγέθους, αγνοώντας τις σταθερές. Ακολουθούν οι τυπικοί ορισμοί των συνηθέστερων ασυμπτωτικών συμβολισμών. Το σύμβολο '=' εδώ δε σημαίνει ισότητα, καθώς όπως φαίνεται στους ορισμούς, δηλώνει ότι η f ανήκει σε μια κλάση συναρτήσεων(που περιέχει όλες της συναρτήσεις ίδιας τάξης μεγέθους με αυτήν):

$$f(n) = O(F(n)) \Leftrightarrow \exists N, \exists c : \forall n \geq N : f(n) \leq cF(n)$$

Π.χ.: $67 \ln n = O(\log_2 n), 562n^{34} = O(2^n), O(a+b) = O(\max\{a,b\})$.

$$f(n) = o(F(n)) \Leftrightarrow \lim_{n\to\infty}(f(n)/F(n)) = 0 \Leftrightarrow \forall \epsilon \exists N, \forall n > N, f(n) < \epsilon F(n)$$

Άρα θέτοντας $\epsilon = c$ βρίσκουμε $f(n) = O(F(n))$. Το αντίστροφο δεν ισχύει, δες π.χ. $13n^3 \lg n + 37n^{3.1} = O(n^{3.1})$. Ο συμβολισμός $o(\cdot)$ δηλώνει δηλαδή ένα άνω φράγμα που δεν είναι ακριβές(tight).

$$f(n) = \Omega(F(n)) \Leftrightarrow F(n) = O(f(n))$$

Παρόμοια με πριν ορίζεται και ο συμβολισμός $\omega(\cdot)$ για ένα κάτω φράγμα που δεν είναι ακριβές.

$$f(n) = \Theta(F(n)) \Leftrightarrow [\ f(n) = O(F(n))\ \&\ f(n) = \Omega(F(n))\ ]$$

Τέλος, για να αγνοούμε λογαριθμικές ποσότητες, ορίζουμε το «χαλαρό»(soft) όμικρον:

$$f(n) = O^*(F(n)) \Leftrightarrow [\ \exists\ c \in \mathbb{R} : f(n) = O((\log F(n))^c F(n))\ ]$$

Παρατηρήστε ότι μας ενδιαφέρει η ασυμπτωτική συμπεριφορά: το c μπορεί να είναι μια αρκετά μεγάλη δύναμη του λογαρίθμου κι όμως εδώ χαρακτηρίζεται αμελητέο.

1.2 Στοιχεία από την Άλγεβρα

Δίνουμε τώρα μερικούς ορισμούς από την Άλγεβρα, οι οποίοι θα εμφανιστούν στα επόμενα.

Ορισμός 1.1. *Ένα σύνολο $(G, \star)$, δηλαδή εφοδιασμένο με μια πράξη $\star : G \times G \to G$ καλείται* ομάδα*(group) αν ικανοποιεί:*

1. *Υπάρχει ουδέτερο στοιχείο, δηλ: $\exists e \in G$ ώστε $a \star e = e \star a = a,\ \forall a \in G$.*
2. *Για κάθε $a \in G$ υπάρχει $a' \in G$ ώστε $a \star a' = a' \star a = e$, όπου e το ουδέτερο στοιχείο.*
3. *Ισχύει η προσεταιριστική ιδιότητα, δηλ: $a \star (b \star c) = (a \star b) \star c,\ \forall a, b, c \in G$.*

Π.χ. η ομάδα $(\mathbb{Z}, +)$, της οποίας το ουδέτερο στοιχείο είναι το μηδέν.

Ορισμός 1.2. *Ένα σύνολο εφοδιασμένο δυο πράξεις $(R, +, *)$, όπου $+, * : R \times R \to R$ καλείται* δακτύλιος*(ring) αν ικανοποιεί τις ιδιότητες:*

1. *Οι πράξεις είναι προσεταιριστικές: $(a+b)+c = a+(b+c),\ (a*b)*c = a*(b*c),\ \forall a, b, c \in R$*
2. *$H\ +$ είναι αντιμεταθετική: $a + b = b + a,\ \forall a, b \in \mathbb{R}$*
3. *Υπάρχει $0 \in R$ ουδέτερο στοιχείο για τη $+$, δηλ: $a + 0 = 0 + a = a,\ \forall a \in \mathbb{R}$*

4. *Κάθε $a \in R$ έχει αντίστροφο, δηλ:* $\forall a \in R,\ \exists a' \in R$ *ώστε* $a + a' = a' + a = 0$*(συνήθως συμβολίζουμε τον αντίστροφο με* $-a$*).*

5. *Η* $+$ *είναι επιμεριστική ως προς* $*$*, δηλ:* $a * (b + c) = a * b + a * c,\ (b + c) * a = b * a + c * a$

Αν ο δακτύλιος έχει και ουδέτερο στοιχείο για την $*$, δηλαδή υπάρχει $1 \in R$ ώστε $1 * a = a * 1 = a,\ \forall a \in R$, τότε καλείται δακτύλιος με μονάδα. Αν επιπλέον ισχύει η μεταθετική ιδιότητα για την $*$ τότε έχουμε έναν *μεταθετικό δακτύλιο με μονάδα*.

Ο $(\mathbb{Z}, +, \cdot)$ είναι παράδειγμα μεταθετικού δακτυλίου με μονάδα, ενώ ο δακτύλιος $(\mathbb{R}^{2\times 2}, +, \cdot)$ των 2×2 πινάκων με τις συνήθεις πράξεις δεν είναι μεταθετικός.

Ορισμός 1.3. *Ένας μεταθετικός δακτύλιος* $R \neq \{0\}$ *με μονάδα, θα λέμε ότι είναι ακέραια περιοχή(integral domain) αν για κάθε* $a, b \in R$ *ισχύει η συνεπαγωγή* $a * b = 0 \Rightarrow a = 0$ *ή* $b = 0$*.*

Π.χ. ο $(\mathbb{Z}, +, \cdot)$ είναι ακέραια περιοχή, ενώ ο δακτύλιος $(\mathbb{Z}_6, +, \cdot)$ των ακεραίων modulo 6 δεν είναι, αφού $3 \cdot 4 \equiv 12 \equiv 0 \pmod 6$.

Ορισμός 1.4. Σώμα*(field) ονομάζεται ένας μεταθετικός δακτύλιος* $F \neq \{0\}$ *με μονάδα, αν για κάθε στοιχείο του διαφορετικό του* 0 *υπάρχει αντίστροφος ως προς* $*$*.*

Π.χ. με τις συνήθεις πράξεις τα $\mathbb{R},\ \mathbb{C},\ \mathbb{Q}$ είναι σώματα, ενώ το $\mathbb{Z}$ δεν είναι καθώς μόνο τα στοιχεία ± 1 έχουν πολλαπλασιαστικό αντίστροφο.

Ορισμός 1.5. *Αν* $(R, +, *)$ *ένας δακτύλιος, ένα μη κενό υποσύνολό του* $I \subseteq R$ *καλείται ιδεώδες του* R *αν ισχύουν:*

1. $a, b \in I \Rightarrow a - b \in I$*.*

2. *Αν* $c \in R$ *και* $a \in I$ *τότε* $c \cdot a, a \cdot c \in I$

Π.χ. τα πολλαπλάσια του 2(δηλαδή το $2\mathbb{Z}$), ή γενικά το $n\mathbb{Z}$ είναι ιδεώδη του $(\mathbb{Z}, +, \cdot)$.

Συνεχίζουμε με στοιχεία από την Θεωρία πραγματικών σωμάτων [Mis93].

Ορισμός 1.6. *Ένα σώμα (field)* K *καλείται* διατεταγμένο *όταν περιέχει ένα υποσύνολο θετικών αριθμών* R*, κλειστό ως προς τις* 2 *πράξεις* $(+, *)$*, τέτοιο ώστε για κάθε στοιχείο* $x \in K, x \neq 0$*, είτε* $x \in R$ *είτε* $-x \in R$*.*

Π.χ. $\mathbb{R}, \mathbb{Q}, \mathbb{R}(\epsilon), \mathbb{Q}(\epsilon)$ και $\mathbb{Q}(\sqrt[3]{2}) \equiv \mathbb{Q}[x]/\langle x^3 - 2\rangle$. Αντίθετα, το $\mathbb{C}$ δεν είναι διατεταγμένο. Σημειώστε πως το $0 < \epsilon \ll 1$ είναι ένας απειροελάχιστος (infinitesimal) θετικός δηλ. μπορούμε να θεωρήσουμε πως $\epsilon \to 0^+$. Το $1/\epsilon$, που ανήκει στο $\mathbb{R}(\epsilon)$, τείνει στο άπειρο.

Τα διατεταγμένα σώματα είναι αναγκαστικά άπειρα και μας παρέχουν την δυνατότητα να μελετήσουμε ανισότητες και διαστήματα. Δηλ. $a > b \Leftrightarrow a - b \in R$. Επίσης, $a > b \Rightarrow a + c > b + c, \forall c$, ενώ $a > b \Rightarrow ac > bc,\ \forall c \in R$.

Ορισμός 1.7. *Ένα σώμα* K *καλείται* κλειστό πραγματικό *όταν είναι διατεταγμένο, κάθε θετικός έχει μια θετική τετραγωνική ρίζα, και κάθε εξίσωση περιττού βαθμού στο* $K[x]$ *έχει μια ρίζα στο* K*.*

Π.χ. $\mathbb{R}, \mathbb{R}(\epsilon), \mathbb{R}(\epsilon_1, \epsilon_2)$, αλλά όχι το $\mathbb{Q}$ ούτε η αλγεβρική θήκη $\overline{\mathbb{Q}}$, ούτε το $\mathbb{Q}(\sqrt[3]{2})$.

Από τους ορισμούς προκύπτει πως για κάθε $p(x) \in K[x]$, όπου το K κλειστό πραγματικό, που είναι μη-παραγοντοποιήσιμο και μονικό (με μοναδιαίο μεγιστοβάθμιο συντελεστή) έπεται πως $\deg p \in \{1, 2\}$. Ειδικότερα, ένα δευτεροβάθμιο πολυώνυμο είναι ανάγωγο ανν η διακρίνουσα είναι αρνητική.

Λήμμα 1.8. *Το* K *είναι κλειστό πραγματικό ανν είναι διατεταγμένο και το* $K(\sqrt{-1})$ *είναι αλγεβρικά κλειστό.*

Θεώρημα 1.9 (Μέσης τιμής, Bolzano)**.** *Έστω* K *ένα κλειστό πραγματικό σώμα,* $p \in K[x]$*,* $a < b \in K$ *και* $p(a)p(b) < 0$*. Τότε υπάρχει* $c \in (a, b) : p(c) = 0$*.*

1.3 Επίλυση στους πραγματικούς

Η εύρεση των ριζών μιας πολυωνυμικής εξίσωσης ή ενός συστήματος τέτοιων εξισώσεων συναντά πλειάδα εφαρμογών σε τομείς όπως η υπολογιστική γεωμετρία, ο σχεδιασμός με υπολογιστή, η ρομποτική κοκ. Μια διάσημη μέθοδος για την εύρεση μιγαδικών ριζών είναι η μέθοδος Newton-Raphson. Εδώ θα ασχοληθούμε με την εύρεση πραγματικών ριζών με αλγεβρικές μεθόδους. Οι δυο κύριες κατηγορίες αλγορίθμων που θα εξεταστούν είναι

- Αλγόριθμοι υποδιαίρεσης: Χονδρικά οι αλγόριθμοι αυτοί δουλεύουν καταμετρώντας τον αριθμό των ριζών σε διαστήματα κατάλληλα μικρού πλάτους. Δηλαδή υποδιαιρούν την πραγματική ευθεία σε αρκούντως μικρά διαστήματα και εντοπίζουν σε ποια από αυτά υπάρχει(μοναδική) πραγματική ρίζα. Έτσι επιστρέφουν στην έξοδο αυτά τα «διαστήματα απομόνωσης». Τα βασικά στοιχεία ενός τέτοιου αλγόριθμου είναι ένα αρχικό φράγμα για τις πραγματικές ρίζες κι ένας τρόπος καταμέτρησης των ριζών. Για την ανάλυσή τους χρειαζόμαστε κι ένα κριτήριο για την απόσταση των ριζών. Η διάκριση τους γίνεται κυρίως με το δεύτερο χαρακτηριστικό τους, τον τρόπο καταμέτρησης των ριζών: πρόκειται κυρίως για μεθόδους Sturm και Descartes. Υπάρχουν επίσης διάφορα φράγματα για τις ρίζες, πχ το φράγμα του Cauchy, η αποτελεσματικότητα των οποίων εξαρτάται κι από την εξίσωση που επιλύεται.

- Αλγόριθμοι προσέγγισης: Αν και η έξοδος εδώ είναι πάλι κάποια διαστήματα, η μέθοδος που ακολουθείται είναι η προσέγγιση ενός πραγματικού αριθμού από ένα συνεχές κλάσμα(continued fraction) με ακέραιους συντελεστές.

Άνθιση γνωρίζουν και μέθοδοι που βασίζονται στην αριθμητική διαστημάτων(Interval Analysis), αλλά η ακρίβειά τους δεν είναι πάντα επαρκώς θεμελιωμένη.

Ένα πολυώνυμο $p(x)$ είναι *χωρίς τετράγωνα* εάν δεν έχει πολλαπλές ρίζες δηλ. εάν η παραγοντοποίησή του σε γραμμικά πολυώνυμα ($\in \mathbb{C}[x]$ ή, γενικότερα, ως προς την αλγεβρική θήκη του σώματος των συντελεστών) δεν περιλαμβάνει κανέναν παράγοντα υψωμένο σε δύναμη. Κάθε παράγων υψωμένος σε δύναμη $k > 1$ στο $p(x)$ εμφανίζεται στην δύναμη $k-1$ στην παράγωγο $p'(x)$. Για κάθε $p(x)$, το πολυώνυμο $p(x)/\text{ΜΚΔ}(p(x), p'(x))$ είναι χωρίς τετράγωνα και με το ίδιο σύνολο ριζών όπως το $p(x)$. Έτσι όταν μας ενδιαφέρει η εύρεση των ριζών, μπορούμε πάντα να δουλεύουμε (πιθανόν μετά από μια διαίρεση με το ΜΚΔ όπως παραπάνω) με πολυώνυμα χωρίς τετράγωνα.

1.4 Φράγματα ριζών

Το πρώτο ζητούμενο είναι ο εγκλωβισμός όλων των ριζών μιας εξίσωσης σε ένα αρχικό διάστημα. Όπως αναφέρθηκε, σε μια συγκεκριμένη εξίσωση άλλα φράγματα δίνουν μικρότερο διάστημα κι άλλα πιο ευρύ. Παρακάτω συνοψίζονται τα φράγματα που χρησιμοποιούν οι αλγόριθμοι (στο πρώτο τους στάδιο). Το θεώρημα αφορά σε όλες τις ρίζες, ακόμη κι αν αυτές είναι μιγαδικές. Η απαίτηση να είναι το πολυώνυμο μονικό δεν είναι περιοριστική, καθώς μπορούμε πάντα να διαιρέσουμε την εξίσωση με το συντελεστή του μεγιστοβάθμιου όρου.

Θεώρημα 1.10. *Κάθε ρίζα α του $p(x) = x^n + \cdots + c_0$, που είναι μονικό (δηλ. με μοναδιαίο μεγιστοβάθμιο συντελεστή $c_n = 1$), φράσσεται ως εξής:*

$$
\begin{aligned}
[\textit{Cauchy}1829]: \quad & |\alpha| < 1 + \max_{0\le i<n}\{|c_i|\}, \quad |\alpha| \le \max_{0\le i<n}\left\{|nc_i|^{\frac{1}{n-i}}\right\},\\
[\textit{Zassenhaus}]: \quad & |\alpha| \le 2\max_{0\le i<n}\left\{|c_i|^{\frac{1}{n-i}}\right\},\\
[\textit{Yap00, lect.VI}]: \quad & |\alpha| \le \frac{1}{\sqrt[n]{2}-1}\max_{0\le i<n}\left\{\left|\frac{\sqrt[n-i]{c_i}}{\binom{n}{n-i}}\right|\right\},\\
[\textit{Landau}]: \quad & |\alpha| \le \left(c_0^2 + \cdots + c_{n-1}^2\right)^{1/2}.
\end{aligned}
$$

Απόδειξη. Το 1ο φράγμα Cauchy, αν $|\alpha| \leq 1$, ισχύει τετριμμένα. Αλλιώς έχουμε

$$|\alpha|^n = |-c_{n-1}\alpha^{n-1} - \cdots - c_0| \leq \max\{|c_i|\}(|\alpha|^{n-1} + \cdots + 1) = \max\{|c_i|\}\frac{|\alpha|^n - 1}{|\alpha| - 1} < \frac{\max\{|c_i|\}|\alpha|^n}{|\alpha| - 1},$$

που δίνει το φράγμα. Οι υπόλοιπες αποδείξεις αφήνονται ως άσκηση. □

Άσκηση 1.1. Για κάθε φράγμα παραπάνω, βρείτε ένα πολυώνυμο για το οποίο το φράγμα αυτό είναι καλύτερο από τα υπόλοιπα.

Όταν θεωρούμε μόνο τις θετικές ρίζες, μια βελτίωση του 2ου φράγματος του Cauchy υπάρχει στο [Kiousteli-dis]: $\alpha \leq 2\max_{0\leq i<n, c_i<0}\left\{|c_i|^{\frac{1}{n-i}}\right\}$, όπου το μέγιστο λαμβάνεται από όλους τους αρνητικούς συντελεστές. Επιπλέον φράγματα υπάρχουν στην βιβλιογραφία, βλ. π.χ. [Tsi06, Zip93].

Ορίζουμε το ανάστροφο πολυώνυμο $q(x) = x^n p(1/x)$ και εξετάζουμε τις μη-μηδενικές ρίζες. Έστω ανώτερο φράγμα φ στη μέγιστη ρίζα του $q(x)$, την οποία συμβολίζουμε με α, δηλ. $q(\alpha) = 0 = \alpha^n p(1/\alpha) \Rightarrow 1/\varphi$ αποτελεί κατώτερο φράγμα στην ελάχιστη ρίζα $(= 1/\alpha)$ του $p(x)$.

Πόρισμα 1.11.

$$|\alpha| > \frac{|c_0|}{1 + \max_{1\leq i\leq n}\{|c_i|\}}, \quad |\alpha| \geq 1/\max_{1\leq i\leq n}\left\{\left|\frac{nc_i}{c_0}\right|^{\frac{1}{n-i}}\right\},$$
$$|\alpha| \geq \frac{1}{2}\max_{1\leq i\leq n}\left\{\left|\frac{c_i}{c_0}\right|^{\frac{1}{n-i}}\right\}, \quad |\alpha| \geq |c_0|/\left(c_1^2 + \cdots + c_n^2\right)^{1/2}.$$

Αφήνεται σαν άσκηση η «αναστροφή» του φράγματος του Yap.

Παράδειγμα 1.2. Δίνεται $p = x^3 + 2x - 3 = (x-1)(x + 1/2 + i\sqrt{11/2})(x + 1/2 - i\sqrt{11/2})$. Ανώτατα όρια στις πραγματικές ρίζες: Cauchy: $1 + \max\{2, 3\} = 4$, $\max\{6^{1/2}, 9^{1/3}\} = \max\{2.45, 2.0801\} = 2.45$ (που είναι και το καλύτερο άνω φράγμα), Zassenhaus: $2 \cdot \max\{1.414, 1.4423\} = 2.8845$.

Ανώτατα όρια στις ρίζες του $q(x) = x^3 p(1/x)$: Cauchy: $1 + \max\{1/3, 2/3\} = 5/3, \max\{1, 2\} = 2$. Zassenhaus: $2\max\{0.69, 2/3\} = 1.3867$. Επομένως το καλύτερο κατώτερο όριο που συνάγεται είναι $1/1.3867 = 0.7211$.

Αφήνεται σαν άσκηση η χρήση των φραγμάτων των Yap, Landau.

Η μέθοδος Sturm

Το θεώρημα του Sturm μας δίνει έναν τρόπο καταμέτρησης των πραγματικών ριζών ενός πολυωνύμου σε δοσμένο διάστημα που τηρεί κάποιες συνθήκες. Εισάγουμε την έννοια της ακολουθίας Sturm ενός πολυωνύμου, αποδεικνύουμε το σχετικό θεώρημα και κατόπιν δίνουμε αλγόριθμο εντοπισμού των πραγματικών ριζών.

2.1 Ακολουθίες Sturm

Έστω μια ακολουθία τιμών $(t_1, \ldots, t_k)$. Ορίζουμε ως το *πλήθος μεταβολών προσήμου* το πλήθος μεταβολών στην ακολουθία μη-μηδενικών προσήμων. Π.χ. πλήθος μεταβολών της $[-,+,+,-] = 2$, πλήθος μεταβολών της $[+,0,+,-] = 1$.

Έστω $a \in \mathbb{R} \cup \{-\infty, +\infty\}$ και μια ακολουθία πολυωνύμων $(p_1, \ldots, p_k)$. Ορίζουμε ως το *πλήθος μεταβολών προσήμου* της ακολουθίας στο σημείο a, και το συμβολίζουμε $V(a)$, το πλήθος μεταβολών προσήμου στην ακολουθία των τιμών $[p_1(a), \ldots, p_k(a)]$, όπου $p(\pm\infty) = \lim_{x\to\pm\infty} p(x)$.

Ορισμός 2.1. *Μια* ακολουθία Sturm *ενός πολυωνύμου $p \in K[x]$ στο $[a,b] \subset K \cup \{-\infty, +\infty\}$, όπου K κλειστό πραγματικό, είναι μια ακολουθία $(p_1, p_2, \ldots, p_k)$ με $p_1 = p$ εάν:*

1. $p(a)p(b) \neq 0$,
2. $\forall c \in [a,b], p_k(c) \neq 0$,
3. $\forall c \in [a,b] : p_j(c) = 0 \Rightarrow p_{j-1}(c)p_{j+1}(c) < 0, \quad j \in \{2, \ldots, k-1\}$
4. $\forall c \in [a,b] : p_1(c) = 0 \Rightarrow$ *υπάρχουν διαστήματα* $[c_1, c), (c, c_2]$ *τέτοια ώστε:* $u_1 \in [c_1, c) \Rightarrow p_1(u_1)p_2(u_1) < 0$ *και* $u_2 \in (c, c_2] \Rightarrow p_1(u_2)p_2(u_2) > 0$.

Το επόμενο θεώρημα δείχνει πως ο παραπάνω ορισμός δεν είναι κενός, δηλ. υπάρχει τουλάχιστον μια ακολουθία Sturm. Το θεώρημα ορίζει έτσι την απλή ακολουθία Sturm.

Θεώρημα 2.2 (Ύπαρξη ακολουθίας Sturm)**.** *Έστω μια ακολουθία $(p_1, p_2, \ldots, p_k)$ με $p_1 = p \in K[x]$ ένα πολυώνυμο χωρίς τετράγωνα και K κλειστό πραγματικό, $p_2 = p'$ (παράγωγος) και για $i = 3, \ldots, k$, $p_i = -(p_{i-2} \bmod p_{i-1})$. Η ακολουθία (p_i) είναι ακολουθία Sturm σε διάστημα $[a,b]$ όπου $p(a)p(b) \neq 0$ και καλείται απλή ακολουθία Sturm.*

Απόδειξη. (1) Κατ' επιλογή τα a, b δεν είναι ρίζες του p.

(2) $\text{ΜΚΔ}(p, p') =$ μη μηδενική σταθερά διότι το p δεν έχει τετράγωνα. Το p_k είναι πολλαπλάσιο του $\text{ΜΚΔ}(p, p')$ επί μια μη μηδενική σταθερά άρα $p_k =$ σταθερά. Εδώ χρησιμοποιείται η υπόθεση πως το πολυώνυμο είναι χωρίς τετράγωνα.

(3) $\exists q_i \in K[x] : p_{i-1} = p_i q_i - p_{i+1} \Rightarrow p_{i-1}(c) = 0 - p_{i+1}(c)$. Εάν $p_{i-1}(c) = 0 = p_{i+1}(c)$ τότε $\forall j > i-2, p_j(c) = 0$: άτοπο για $j = k$.

(4) Για c τέτοιο ώστε $p(c) = 0$ έχουμε $p'(c) \neq 0$ (διότι p χωρίς τετράγωνα) άρα υπάρχει διάστημα (c_1, c_2) που περιέχει το c όπου το p' έχει σταθερό πρόσημο ενώ το p αλλάζει πρόσημο στο c, δεδομένου ότι πρόκειται για απλή ρίζα. □

Πόρισμα 2.3. *Κάθε ακολουθία* $(p_i) = (p, p', \dots)$ *όπου* $a_i p_i = b_i p_{i-2} + p_{i-1} q_{i+1}$ *για* $a_i, b_i \in K,\ a_i b_i < 0$, *όπου το* $p(x) \in K[x]$ *είναι χωρίς τετράγωνα και το* K *κλειστό πραγματικό, είναι ακολουθία Sturm στο* $[a, b]$ *όπου* $p(a)p(b) \neq 0$.

Απόδειξη. Όπως παραπάνω: άσκηση. □

Λήμμα 2.4. *Μία ακολουθία προσήμων* $(\sigma, \tau, -\sigma)$ *έχει 1 αλλαγή προσήμου για κάθε* $\sigma, \tau \in \{+, -\}$.

2.2 Το Θεώρημα Sturm

Είμαστε τώρα έτοιμοι να διατυπώσουμε το βασικό θεώρημα της ενότητας, που θα μας επιτρέψει να μετράμε τις διαφορετικές πραγματικές ρίζες ενός πολυωνύμου σε ένα διάστημα, χωρίς όμως να υπολογίζουμε τις πολλαπλότητές τους.

Θεώρημα 2.5 (Sturm). *Έστω μια ακολουθία Sturm* $(p_i) = (p_1, \dots, p_k)$ *στο* $[a, b] \subset K \cup \{-\infty, +\infty\}$, *όπου* $p = p_1 \in K[x]$ *και* K *κλειστό πραγματικό. Το πλήθος των διαφορετικών πραγματικών ριζών του* $p_1(x)$ *στο* $[a, b]$ *ισούται με* $V(a) - V(b)$, *όπου* $V(\cdot)$ *το πλήθος μεταβολών προσήμου της* (p_i).

Απόδειξη. Έστω $a_1 < \cdots < a_m$ οι ρίζες $\in (a, b)$ ΟΛΩΝ των πολυωνύμων στην (p_i), δηλαδή όλες οι τιμές στο διάστημα στις οποίες κάποιο πολυώνυμο της ακολουθίας μηδενίζεται. Θα αποδείξουμε επαγωγικά πως η διαφορά $V(a) - V(c_i)$ ισούται με το πλήθος των πραγματικών ριζών στο (a, c_i) για τυχαίο $c_i \in (a_i, a_{i+1})$, $i = 0, \dots, m$, όπου $a_0 = a, a_{m+1} = b$.

Βάση της επαγωγής: Έστω $c_0 \in (a_0, a_1)$. Αν $p_i(a_0) \neq 0,\ i = 2, \dots, k-1$ τότε προφανώς από το θεώρημα μέσης τιμής του Bolzano σε ένα διάστημα $(a_0 - \varepsilon, c_0)$, για κάποιο $\varepsilon > 0$, κάθε πολυώνυμο διατηρεί το πρόσημό του, δηλαδή $V(a) = V(c_0) \Rightarrow V(a) - V(c_0) = 0$.

Ακόμη κι αν υπάρχει $i \in \{2, \dots, k-1\}$ με $p_i(a) = 0$, η ιδιότητα (3) της ακολουθίας Sturm δίνει $p_{i-1}(a)p_{i+1}(a) < 0$, άρα η τριάδα συνεισφέρει στο $V(a)$ κατά 1, επειδή η ακολουθία προσήμων είναι της μορφής $[\cdots, \sigma, 0, -\sigma, \cdots]$, $\sigma, \tau \in \{+, -\}$ στις θέσεις $i-1, i, i+1$. Καθώς στο διάστημα (a, c_0) δεν υπάρχουν ρίζες, η ακολουθία προσήμων στο c_0 είναι της μορφής $[\cdots, \sigma, \tau, -\sigma, \cdots]$ στις ίδιες θέσεις, άρα σύμφωνα με το Λήμμα 2.4 συνεισφέρει στο $V(c_0)$ κατά 1. Αν υπάρχει κι άλλος τέτοιος δείκτης i, με το ίδιο επιχείρημα φθάνουμε στην ίδια μεταβολή των αλλαγών προσήμου, άρα τελικά $V(a) - V(c_0) = 0$.

Επαγωγικό βήμα: Υποθέτοντας $V(a) - V(c_i) =$πλήθος ριζών $\in (a, c_i)$ θα το αποδείξουμε για c_{i+1} όπου $c_i < a_{i+1} < c_{i+1} < a_{i+2}$. Διακρίνουμε δυο περιπτώσεις ανάλογα με το αν $p(a_{i+1}) \neq 0$ ή $p(a_{i+1}) = 0$:

1. Έστω $p(a_{i+1}) \neq 0$. Τότε $p_j(a_{i+1}) = 0$, για κάποιο $j \in \{2, \dots, k-1\}$. Χάριν της ιδιότητας (3) των ακολουθιών Sturm, $p_{j+1}(a_{i+1})p_{j-1}(a_{i+1}) < 0$, συνεπώς έχουμε τις ακολουθίες προσήμων

$$\begin{aligned} [p_{j-1}(c_i), p_j(c_i), p_{j+1}(c_i)] &= [\sigma, \tau_0, -\sigma], \\ [p_{j-1}(c_{i+1}), p_j(c_{i+1}), p_{j+1}(c_{i+1})] &= [\sigma, \tau_1, -\sigma] \end{aligned}$$

   για $\sigma, \tau_0, \tau_1 \in \{+, -\}$. Σύμφωνα με το Λήμμα 2.4, υπάρχει ακριβώς μία αλλαγή προσήμου σε καθεμιά από τις 2 ακολουθίες. Άρα, αν μόνο το p_j μηδενίζεται στο a_{i+1}, έχουμε $V(c_{i+1}) = V(c_i)$. Αν υπάρχει κι άλλο πολυώνυμο που μηδενίζεται στο a_{i+1} το ίδιο επιχείρημα δείχνει πως τελικά $V(c_{i+1}) = V(c_i)$.

   Αφού οι ρίζες του p δεν αυξήθηκαν στο διάστημα (c_i, c_{i+1}), ο ισχυρισμός αποδείχθηκε.

2. Έστω $p(a_{i+1}) = 0$. Χάριν της ιδιότητας (4) των ακολουθιών Sturm, τα $p_1,\ p_2$ έχουν διαφορετικό πρόσημο στο c_i και το ίδιο στο c_{i+1}. Επίσης, από την ιδιότητα (3) για $j = 2$, έχουμε $p_2(a_{i+1}) = 0 \Rightarrow p_1(a_{i+1}) \neq 0$, το οποίο είναι άτοπο. Άρα από θ.Bolzano το p_2 διατηρεί το πρόσημό του στο (a_i, a_{i+2}), δηλαδή οι ακολουθίες προσήμων στα c_i και c_{i+1} είναι:

$$\begin{aligned} [p_1(c_i), p_2(c_i), \dots] &= [-\rho, \rho, \cdots], \\ [p_1(c_{i+1}), p_2(c_{i+1}), \dots] &= [\rho, \rho, \cdots] \end{aligned}$$

όπου $\rho \in \{+, -\}$.

Αν κανένα άλλο πολυώνυμο με δείκτη $j > 2$ δε μηδενίζεται στο a_{i+1} βλέπουμε ότι $V(c_{i+1}) = V(c_i) - 1$.

Αν τώρα για $j > 2$, υπάρχει p_j με $p_j(a_{i+1}) = 0$ ακολουθούμε ακριβώς την ίδια διαδικασία όπως στην περίπτωση 1 πιο πάνω, για να δείξουμε ότι για την υπακολουθία $[p_2, p_3, \ldots, p_k]$ είναι $V^\star(c_{i+1}) = V^\star(c_i)$, δηλαδή ισχύει και πάλι $V(c_{i+1}) = V(c_i) - 1$.

Τελικά βλέπουμε ότι $V(a) - V(c_{i+1}) = V(a) - V(c_i) + 1$ άρα από επαγωγική υπόθεση φθάνουμε στο ζητούμενο(δεδομένου ότι οι ρίζες του p έχουν αυξηθεί κατά μία στο διάστημα (c_i, c_{i+1})).

□

Άσκηση 2.1. Η έννοια της ακολουθίας Sturm γενικεύεται με το να αναιρέσουμε την προϋπόθεση (1) του ορισμού 2.1. Τότε τα διαστήματα στην προϋπόθεση (4) πρέπει να ανήκουν στο διάστημα $[a, b]$, δηλ. η προϋπόθεση (4) απλοποιείται στην περίπτωση που $c = a$ ή $c = b$. Αποδείξτε πως το θεώρημα 2.5 ισχύει.

Στόχος είναι η απομόνωση όλων των ριζών δηλ. ο υπολογισμός ρητών διαστημάτων που καθένα περιέχει μια μοναδική ρίζα. Περιορίζουμε το διάστημα όπου βρίσκονται οι (πραγματικές) ρίζες του $p(x)$ χρησιμοποιώντας το θεώρημα 1.10 και το πόρισμά του.

Παράδειγμα 2.2. Δίνεται $p = x^3 + 2x - 3 = (x-1)(x+1/2+i\sqrt{11/2})(x+1/2-i\sqrt{11/2})$. Ακολουθία Sturm:

$$p_1 = p,\ p_2 = p' = 3x^2 + 2,\ p_3 = -(p_1 \mod p_2) = -(4/3)x + 3,\ p_4 = -(p_2 \mod p_3) = -275/16.$$

Στο παράδειγμα 1.2 υπολογίστηκε το αρχικό διάστημα $(0.7211,\ 2.45)$, το οποίο περιέχει όλες τις ρίζες του p. Προκύπτει λοιπόν ο παρακάτω πίνακας, όπου μετά το αρχικό διάστημα $(0, 3)$ επελέγησαν τα σημεία $3/2, 3/4, 9/8$ με αυτή τη σειρά.

$a =$	0	3/4	**1**	9/8	3/2	3
$p_1(a)$	−	−	**0**	+	+	+
$p_2(a)$	+	+	**+**	+	+	+
$p_3(a)$	+	+	**+**	+	+	−
$p_4(a)$	−	−	−	−	−	−
$V(a) =$	2	2	**1**	1	1	1

Άσκηση 2.3. Έστω πολυώνυμο $f = x^3 - 13x + 12$. Δίνεται η ταυτότητα $f'(x = 18/13) = -1225/169$. Υπολογίστε μια ακολουθία Sturm και απομονώστε τις ρίζες.

Απάντηση: $p_1 = f, p_2 = f' = 3x^2 - 13, p_3 = 26x/3 - 12, p_4 > 0$. Ρίζες $= 1, 3, 4$.

2.3 Ο αλγόριθμος Sturm

Δίνουμε τώρα τον αλγόριθμο Sturm για εύρεση πραγματικών ριζών ενός πολυωνύμου με απλές ρίζες σε ψευδοκώδικα:

Αλγόριθμος STURM

▷ *Είσοδος:* Ένα πολυώνυμο $p \in \mathbb{R}[x]$ χωρίς τετράγωνα.
▷ *Έξοδος:* Ένα σύνολο R με στοιχεία διαστήματα απομόνωσης των πραγματικών ριζών του p.

```
1  I_0 ← Cauchy(p)
2  Υπολόγισε ακολουθία Sturm S = (p_1, ..., p_k) στο I_0
3  Q ← {I_0}, R ← ∅
4  όσο Q ≠ ∅
5          I ←εξαγωγή(Q)
6          roots ← VARS(S, a) − VARS(S, b)
7          αν roots = 1, R ← R ∪ I
8          αν roots > 1, Q ← Q ∪ {I_L, I_R}
9  επέστρεψε R
```

Όπου $I = [a, b]$, και συμβολίζουμε $I_L = [a, \frac{a+b}{2}],\ I_R = [\frac{a+b}{2}, b]$. Τα σύνολα Q, R μπορούν να υλοποιηθούν με κάποια δομή δεδομένων, πχ στοίβα ή ουρά. Η εντολή **Cauchy**(p) επιστρέφει το διάστημα $I_0 = [-B, B]$, όπου B το φράγμα ριζών του p από τον τύπο του Cauchy. Ο παραπάνω αλγόριθμος δεν λαμβάνει υπόψιν την περίπτωση κάποιο από τα άκρα των I_L, I_R να είναι ρίζα του $p(x)$, όμως ένας τέτοιος έλεγχος είναι εύκολο να προστεθεί και δεν επιβαρύνει σημαντικά τον αλγόριθμο.

Δίνεται και η ρουτίνα VARS(S, r), η οποία εκτελεί την αποτίμηση της ακολουθίας Sturm σε δοσμένη τιμή και μετρά τις εναλλαγές προσήμων στην ακολουθία που προκύπτει:

Αλγόριθμος VARS

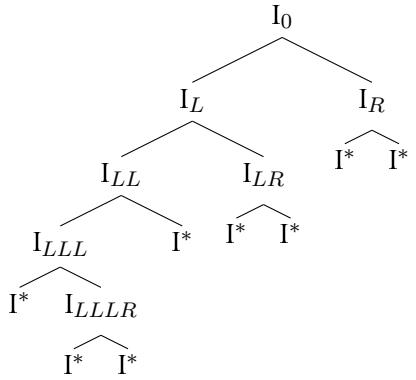
▷ *Είσοδος:* Μια ακολουθία πολυωνύμων $S = (p_1, p_2, \ldots, p_k)$ και μια τιμή $r \in \mathbb{Q}$
▷ *Έξοδος:* Το πλήθος των αλλαγών προσήμου της $S(r) = (p_1(r), p_2(r), \ldots, p_k(r))$

```
1  V ← 0
2  σ ←πρόσημο(p_1(r))
3  για i = 2 μέχρι k
4          τ ←πρόσημο(p_i(r))
5          αν στ = −1, V ← V + 1
6          αν τ ≠ 0, σ ← τ
7  επέστρεψε V
```

Όπου η εντολή **πρόσημο**() επιστρέφει 1 αν το όρισμα είναι θετικό, -1 αν είναι αρνητικό, ή 0 αν το όρισμα είναι το 0.

Προχωράμε στην ανάλυση του αλγορίθμου. Έστω d ο βαθμός του p, $p(x) = \sum_{i=0}^{d} c_i x^i$, κι έστω ότι οι συντελεστές του έχουν μήκος $O_B(\tau)$. Για την ώρα θα δεχθούμε ότι το βήμα 2 στον αλγόριθμο STURM, δηλαδή ο υπολογισμός μιας ακολουθίας Sturm[1], έχει πολυπλοκότητα $O_B^*(d^3\tau)$ και ότι οι συντελεστές κάθε πολυωνύμου p_i έχουν μήκος $O_B(d\tau)$. Επειδή $B = 1 + \max_{0 \le i \le d} \left|\frac{c_i}{c_d}\right|$, το B έχει μήκος $O_B(\tau)$, δηλαδή $B \cong 2^\tau$.

Οι υποδιαιρέσεις(διχοτομήσεις) διαστημάτων που γίνονται δημιουργούν ένα νοητό δυαδικό δέντρο, με φύλλα τα διαστήματα απομόνωσης των ριζών του p, τα οποία συμβολίζονται στο παρακάτω παράδειγμα με I^*.



Στο δέντρο αυτό κάθε κόμβος-διάστημα χαρακτηρίζεται από το ύψος $h(I)$ στο οποίο βρίσκεται, και μάλιστα είναι

$$h(I) = \lg \frac{|I_0|}{|I|} \tag{2.1}$$

όπου με $|I|$ συμβολίζουμε το μήκος του διαστήματος. Η σχέση προκύπτει άμεσα αν σκεφτούμε πως σε κάθε επίπεδο το μήκος υποδιπλασιάζεται, κι έτσι είναι $|I| = 2^{-h(I)}|I_0|$.

[1] Η βέλτιστη αυτή τιμή επιτυγχάνεται με την ακολουθία Habicht και μπορεί να μειωθεί περισσότερο αν υπολογιστεί μια ακολουθία πηλίκων, αντί για τα υπόλοιπα..

Όταν χρησιμοποιούμε κατάλληλη ακολουθία Sturm, η αποτίμησή της σε έναν ρητό με μήκος[2] $O_B(\sigma)$ έχει πολυπλοκότητα $O_B^*(d^2(\tau+\sigma))$. Αυτή είναι και η πολυπλοκότητα της ρουτίνας VARS όταν η είσοδος είναι $O_B(\sigma)$, καθώς οι υπόλοιπες πράξεις μεταξύ προσήμων είναι αμελητέες. Τι μήκος έχουν όμως οι ρητοί στους οποίους εφαρμόζουμε τη ρουτίνα; Όπως φαίνεται και στο παραπάνω δέντρο, σε βάθος $h \equiv h(I)$ τα άκρα του διαστήματος I προκύπτουν με h διαδοχικές διαιρέσεις με το 2 ποσοτήτων ανάλογων των άκρων του I_0, άρα θα έχουν μήκος $O_B(\tau+h)$. Έτσι τελικά η VARS τρέχει σε χρόνο $O_B^*(d^2(\tau+h))$.

Για να βρούμε τη συνολική πολυπλοκότητα του αλγορίθμου πρέπει να εκτιμήσουμε πόσες φορές θα εκτελεστεί η επανάληψη στα βήματα 4-8, το οποίο είναι ανάλογο του αριθμού των υποδιαιρέσεων που θα γίνουν στο διάστημα I(βήμα 8). Τέλος, ο αριθμός των επαναλήψεων θα πολλαπλασιαστεί με την πολυπλοκότητα της ρουτίνας VARS για να έχουμε το τελικό αποτέλεσμα.

Υπενθυμίζουμε το μέτρο Mahler του πολυωνύμου $p(x)$

$$M = |c_d| \prod_{i=1}^{d} \max\{1, |\rho_i|\} \tag{2.2}$$

όπου $\rho_i,\ i = 1, \ldots, d$ οι μιγαδικές ρίζες του p. Για το μέτρο Mahler ισχύει το φράγμα

$$M \leq \sqrt{c_0^2 + c_1^2 \cdots + c_d^2} \leq 2^\tau \sqrt{d+1} \tag{2.3}$$

Για να φράξουμε το πλήθος των υποδιαιρέσεων C που εκτελεί ο αλγόριθμος χρειαζόμαστε και το παρακάτω

Θεώρημα 2.6. *(Davenport-Mahler-Mignotte) Αν $p(x) \in \mathbb{Z}[x]$ και $\{a_1, \ldots, a_k\},\ \{b_1, \ldots, b_k\}$ δυο σύνολα ριζών του, με $|a_i| > |a_{i+1}|$, $|b_i| > |b_{i+1}|$ και $|a_i| > |b_i|$ τότε ισχύει*

$$\prod_{i=1}^{k} |a_i - b_i| \geq \frac{\left(\sqrt{3}/d\right)^k}{M^{d-1} \cdot d^{d/2}}$$

όπου M το μέτρο Mahler του $p(x)$.

Ας θεωρήσουμε τώρα το σύνολο $\mathcal{S} = \{I :$ υπάρχει ακριβώς μια ρίζα στο I_L και ακριβώς μια στο $I_R\}$, δηλαδή το $\mathcal{S}$ περιέχει τα διαστήματα του δέντρου που έχουν 2 φύλλα(στο παράδειγμα είναι τα I_R, I_{LR}, I_{LLLR}). Επειδή τα φύλλα είναι το πολύ d, έχουμε ότι το πλήθος των στοιχείων του είναι

$$|\mathcal{S}| \leq \frac{d}{2} \tag{2.4}$$

Το θεώρημα (2.6) ισχύει για $k = |\mathcal{S}|$ και a_i, b_i οι ρίζες στο $I_i \in \mathcal{S}$. Λογαριθμώντας παίρνουμε

$$-\log \prod_{i=1}^{|\mathcal{S}|} |a_i - b_i| \leq (d-1)\log M + \frac{d}{2}\log d + |\mathcal{S}|\log d - \frac{|\mathcal{S}|}{2}\log 3$$

και λαμβάνοντας υπόψιν από τις (2.3), (2.4) ότι $\log M = O(\tau + \log d)$ και $|\mathcal{S}| = O(d)$, είναι τελικά

$$-\log \prod_{i=1}^{|\mathcal{S}|} |a_i - b_i| = O(d\tau + d\log d) \tag{2.5}$$

[2] δυαδικό μήκος(bit complexity) ρητού ορίζουμε τη μέγιστη τιμή από το δυαδικό μήκος του αριθμητή και του παρονομαστή του

Έχοντας κατά νου όλα τα παραπάνω, μπορούμε να φράξουμε το C ως εξής:

$$\begin{aligned}
C &\leq \sum_{I\in\mathcal{S}} h(I) \\
&\overset{(2.1)}{=} \sum_{I\in\mathcal{S}} \lg \frac{|I_0|}{|I|} \\
&= |\mathcal{S}| \lg |I_0| - \sum_{I\in\mathcal{S}} \lg |I| \\
&< |\mathcal{S}| \lg(2B) - \sum_{I\in\mathcal{S}} \lg(a_i - b_i) \\
&\prec |\mathcal{S}|\tau - \sum_{I\in\mathcal{S}} \log(a_i - b_i) \\
&\overset{(2.4)}{<} d\tau - \log \prod_{i=1}^{|\mathcal{S}|} |a_i - b_i| \\
&\overset{(2.5)}{\prec} d\tau + d\tau + d\log d \\
&= O_B(d\tau + d\log d) = O_B^*(d\tau)
\end{aligned}$$

Μια παρατήρηση είναι εδώ ότι $h \leq C$, άρα το φράγμα για την πολυπλοκότητα της VARS είναι $O_B^*(d^3\tau)$. Τελικά ο αλγόριθμος έχει συνολική πολυπλοκότητα $O_B^*(C \cdot d^3\tau) = O_B^*(d^4\tau^2)$.

Απαλοίφουσα και Διακρίνουσα

Σε αυτήν την ενότητα θα συναντήσουμε δυο σημαντικές έννοιες που συνδέονται με τα πολυώνυμα μιας(ή και πολλών) μεταβλητής· την απαλοίφουσα και τη διακρίνουσα. Η απαλοίφουσα συνδέεται με τις ακολουθίες Sturm μέσω της ακολουθίας Sturm-Habicht, η οποία είναι μια εξαιρετικά αποδοτική ακολουθία Sturm, με την έννοια ότι οι συντελεστές των πολυωνύμων που την αποτελούν έχουν αρκετά μικρό δυαδικό μήκος και, όπως έχουμε αναφέρει, ο υπολογισμός της είναι σχετικά ταχύς.

3.1 Παραγοντοποίηση και μέγιστος κοινός διαιρέτης

Στο *Μάθημα 1* είδαμε πως ένας δακτύλιος χωρίς μηδενοδιαιρέτες[1] ονομάζεται ακέραια περιοχή. Συνεχίζουμε ορίζοντας περιοχές μοναδικής παραγοντοποίησης και περιοχές με διαίρεση:

Ορισμός 3.1. *Έστω R ένας δακτύλιος και $a, b \in R$.*
(α) Θα λέμε ότι το a διαιρεί το b (συμβολισμός $a|b$) αν υπάρχει $c \in R$ τέτοιο ώστε $b = ac$.
(β) Τα a και b ονομάζονται συντροφικά(associate) στον R αν $a = ub$ για κάποιο αντιστρέψιμο $u \in R$.

Πχ τα μόνα συντροφικά στοιχεία του 5 στο $\mathbb{Z}$ είναι το 5 και το -5. Τα συντροφικά στοιχεία του $g(x) \in F[x]$ όπου F σώμα, είναι τα $ug(x)$ όπου $u \in F - \{0\}$.

Ορισμός 3.2. *Έστω R μια ακέραια περιοχή και $u \in R$. Το u ονομάζεται ανάγωγο(irreducible) στην R αν*
(α) το u δεν είναι μηδέν και δεν είναι αντιστρέψιμο, και
(β) Αν $u = ab$ με $a, b \in R$ τότε το a ή το b είναι αντιστρέψιμο.

Πχ τα ανάγωγα στοιχεία του $\mathbb{Z}$ είναι οι πρώτοι αριθμοί, ενώ τα ανάγωγα πολυώνυμα του $\mathbb{R}[x]$ είναι τα πρωτοβάθμια και τα δευτεροβάθμια με αρνητική διακρίνουσα.

Ορισμός 3.3. *Μια ακέραια περιοχή R καλείται περιοχή μοναδικής παραγοντοποίησης (unique factorization domain) ανν κάθε στοιχείο επιδέχεται «μοναδικής» παραγοντοποίησης. Πιο τυπικά,*
(α) κάθε μη μηδενικό και μη αντιστρέψιμο $a \in R$ παραγοντοποιείται ως $a = c_1 \cdots c_n$, όπου τα c_i ανάγωγα,
(β) αν υπάρχει κι άλλη παραγοντοποίηση $a = d_1 \cdots d_m$, τότε $m = n$ και υπάρχει μια 1-1 αντιστοίχιση των c_i, d_i τέτοια ώστε τα c_i, d_i να είναι συντροφικά(ή αλλιώς $c_i|d_i$ και $d_i|c_i$).

Ορισμός 3.4. Ευκλείδειος δακτύλιος *(Euclidean ring) λέγεται κάθε αντιμεταθετικός δακτύλιος D όπου ορίζεται μια συνάρτηση «διαβάθμισης» $\phi : D \to \mathbb{N}$, τέτοια ώστε $ab \neq 0 \Rightarrow \phi(ab) \leq \phi(a)$ και ορίζεται η διαίρεση $a = bq + r$ με υπόλοιπο r, όπου $r = 0$ ή $\phi(r) < \phi(b)$.*

Ένας ευκλείδειος δακτύλιος που είναι και ακέραια περιοχή λέγεται Ευκλείδεια περιοχή (Euclidean domain).

πχ το $\mathbb{Z}$ είναι Ευκλείδεια περιοχή με συνάρτηση διαβάθμισης την απόλυτο τιμή. Έστω σώμα K. Το K είναι Ευκλείδεια περιοχή με συνάρτηση διαβάθμισης $K \mapsto 1$. Επίσης το $K[x]$ είναι Ευκλείδεια περιοχή με συνάρτηση διαβάθμισης τον βαθμό πολυωνύμου.

Αποδεικνύεται πως κάθε Ευκλείδεια περιοχή είναι περιοχή μοναδικής παραγοντοποίησης. Συνεπώς, μια ιεραρχία δακτυλίων είναι: Αντιμεταθετικοί δακτύλιοι, Ακέραιες περιοχές, Περιοχές μοναδικής παραγοντοποίησης, Ευκλείδειες περιοχές, σώματα.

[1] μηδενοδιαιρέτες ενός δακτυλίου είναι δυο μη μηδενικά στοιχεία α, β αυτού, για τα οποία $\alpha\beta = 0$. Αν ο δακτύλιος δεν είναι μεταθετικός διακρίνουμε αριστερούς και δεξιούς μηδενοδιαιρέτες.

Ορισμός 3.5. *Ο* μέγιστος κοινός διαιρέτης *ΜΚΔ*(a,b) *σε μια Ευκλείδειο περιοχή είναι το μέγιστο(ως προς τη συνάρτηση διαβάθμισης) στοιχείο της που διαιρεί τα* a *και* b*. Στους ακέραιους πρόκειται για το μέγιστο θετικό, στα πολυώνυμα μίας μεταβλητής, αυτό με μέγιστο βαθμό. Το* ελάχιστο κοινό πολλαπλάσιο *ΕΚΠ*(a,b) *είναι το μικρότερο στοιχείο που διαιρεί τα* a,b*.*

Σημαντική είναι η εξής ιδιότητα: ΕΚΠ(a,b) ΜΚΔ$(a,b) = ab$.

Ο Αλγόριθμος του Ευκλείδη για την εύρεση του ΜΚΔ είναι ο αρχαιότερος αλγόριθμος σε χρήση σήμερα: Δεδομένων δυο στοιχείων $a,b \in D$ θέτουμε $c_0 = a, c_1 = b$. Για $i = 2,3,\dots$ εκτελούμε τις διαιρέσεις με υπόλοιπο: $c_{i-2} = c_{i-1}q_i + c_i$, δηλαδή το επόμενο στοιχείο στην ακολουθία c_i είναι το υπόλοιπο της προηγούμενης διαίρεσης. Η ακολουθία τερματίζεται όταν $c_k = 0$ οπότε και ο ΜΚΔ$(a,b) = c_{k-1}$.

3.2 Ο πίνακας Sylvester

Έστω $p_1 = a_{d_1}x^{d_1} + \cdots + a_0$ και $p_2 = b_{d_2}x^{d_2} + \cdots + b_0$ δυο πολυώνυμα, $p_1, p_2 \in D[x]$, όπου D μια Ευκλείδεια περιοχή. Ο πίνακας Sylvester των p_1, p_2 είναι ένας πίνακας $S \in D^{(d_1+d_2)\times(d_1+d_2)}$ του οποίου οι στήλες αντιστοιχούν σε δυνάμεις της μεταβλητής x και οι γραμμές σε πολλαπλάσια των πολυωνύμων ως εξής[2]:

$$S := \begin{array}{c} \\ p_1 \\ xp_1 \\ \vdots \\ x^{d_2-1}p_1 \\ p_2 \\ xp_2 \\ \vdots \\ x^{d_1-1}p_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & x & x^2 & \dots & \dots & \dots & x^{d_1+d_2-1} \end{array} \\ \begin{bmatrix} a_0 & a_1 & \cdots & a_{d_1} & & & \\ & a_0 & a_1 & \cdots & a_{d_1} & & \mathbf{0} \\ \mathbf{0} & & \ddots & \ddots & \ddots & \ddots & \\ & & & a_0 & a_1 & \cdots & a_{d_1} \\ b_0 & b_1 & \cdots & b_{d_2} & & & \\ & b_0 & b_1 & \cdots & b_{d_2} & & \mathbf{0} \\ \mathbf{0} & & \ddots & \ddots & \ddots & \ddots & \\ & & & b_0 & b_1 & \cdots & b_{d_2} \end{bmatrix} \end{array}$$

Παρατηρήστε πως ο S αποτελείται από δυο υποπίνακες(blocks), οι οποίοι έχουν όλες τις διαγωνίους τους σταθερές. Τέτοιοι πίνακες ονομάζονται πίνακες Toeplitz:

Ορισμός 3.6. *Ενας πίνακας* T*, διάστασης* $n \times m$ *καλείται Toeplitz εάν τα έχει σταθερές διαγωνίους. Δηλαδή ο πίνακας ορίζεται από δυο διανύσματα* $(d, t_1, \cdots, t_{m-1})$ *και* $(\tau_1, \tau_2, \dots, \tau_{n-1})$*:*

$$T = \begin{bmatrix} d & t_1 & t_2 & \dots & \dots & t_{m-1} \\ \tau_1 & d & t_1 & \ddots & & \vdots \\ \tau_2 & \tau_1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & t_1 & t_2 \\ \vdots & & \ddots & \tau_1 & d & t_1 \\ \tau_{n-1} & \dots & \dots & \tau_2 & \tau_1 & d \end{bmatrix}$$

Οι πίνακες Toeplitz αλλά και οι block(κατά ομάδες) Toeplitz έχουν ενδιαφέρουσες ιδιότητες:

- Ο πολλαπλασιασμός $T\underset{\sim}{w}$ ενός $n \times n$, κάτω τριγωνικού πίνακα Toeplitz από δεξιά με ένα διάνυσμα $\underset{\sim}{w}$ εκφράζει τον πολλαπλασιασμό πολυωνύμων, όπου οι συντελεστές των πολυωνύμων βρίσκονται στην πρώτη στήλη του T και στα στοιχεία του $\underset{\sim}{w}$ αντίστοιχα. Όμοια και για το γινόμενο $\underset{\sim}{w}^t T$, όπου T άνω τριγωνικός.

[2] Στη βιβλιογραφία μπορεί να συναντήσετε τον ορισμό του S ως τον ανάστροφο του πίνακα που δίνεται εδώ

- Όταν ο T είναι block Toeplitz, ο ο πολλαπλασιασμός με ένα πολυώνυμο με συντελεστές $\underset{\sim}{w}$ εκφράζει το άθροισμα γινομένων πολυωνύμων.
- Η αντιμετάθεση στηλών(και γραμμών εφόσον δεν παραβιάζεται η block μορφή) δίνει ένα νέο πίνακα Toeplitz κατά block, ο οποίος έχει τις ίδιες ιδιότητες με τον αρχικό.

3.3 Η Απαλοίφουσα δυο πολυωνύμων

Υπάρχουν αρκετοί τρόποι να ορίσεις την απαλοίφουσα. Για τις ανάγκες του μαθήματος δίνουμε τον παρακάτω

Ορισμός 3.7. *Αν $p_1, p_2 \in D[x]$ καλούμε απαλοίφουσα την ορίζουσα του πίνακα Sylvester: $R(p_1,p_2) := \det S$.*

Επειδή ο πίνακας Sylvester έχει στοιχεία από το D, η απαλοίφουσα ανήκει στο D. Επίσης από τη μορφή του S προκύπτει πως η απαλοίφουσα έχει βαθμό d_2 και d_1 ως προς τους συντελεστές του p_1 και του p_2 αντίστοιχα.

Με τις γνωστές ιδιότητες των οριζουσών μπορεί να δειχθεί η ιδιότητα $R[(x-r)p_1(x), p_2(x)] = p_2(r)R[p_1,p_2]$. Γενικότερα με επαγωγή αποδεικνύεται η λεγόμενη μορφή Poisson(Poisson formula):

$$R(p_1,p_2) = a_{d_1}^{d_2} \prod_{i=1}^{d_2} p(r_i) \tag{3.1}$$

όπου r_i οι d_2 ρίζες του p_2 στην αλγεβρική θήκη του D.

Θεώρημα 3.8. *Η απαλοίφουσα είναι μηδέν ανν τα p_1, p_2 έχουν κοινή ρίζα, με άλλα λόγια ισχύει η ισοδυναμία*

$$R(p_1,p_2) = 0 \iff \deg[\mathit{MK\Delta}(p_1,p_2)] \geq 1$$

Απόδειξη. ($\Leftarrow$) Έστω r κοινή ρίζα των p_1, p_2. Αρκεί ο πίνακας S να είναι ιδιάζων. Ισοδύναμα, αρκεί να υπάρχει μη μηδενικό διάνυσμα στον $\ker S$. Θέτουμε $\underset{\sim}{w} = \begin{bmatrix} 1 & r & \cdots & r^{d_1+d_2} \end{bmatrix}^t$. Λόγω της πρώτης συντεταγμένης, $\underset{\sim}{w} \neq 0$, όμως

$$S\underset{\sim}{w} = \begin{bmatrix} p_1(r) \\ \vdots \\ r^{d_2-1}p_1(r) \\ p_2(r) \\ \vdots \\ r^{d_1-1}p_2(r) \end{bmatrix} = \underset{\sim}{0} \quad \Rightarrow \quad \underset{\sim}{w} \in \ker S$$

($\Rightarrow$) Έστω ότι $\det S = 0$. Τότε στον αριστερό πυρήνα θα υπάρχει μη μηδενικό διάνυσμα: $\exists \underset{\sim}{v} \neq 0,\ \underset{\sim}{v} \in \ker S^T$. Έστω $\underset{\sim}{v} = [\kappa_0\ \kappa_1\ \cdots\ \kappa_{d_2-1}\ \lambda_0\ \lambda_1\ \cdots\ \lambda_{d_1-1}]^t$. Αν $q_1(x) = \sum_{i=0}^{d_2-1} \kappa_i x^i,\ q_2(x) = \sum_{i=0}^{d_1-1} \lambda_i x^i$, σύμφωνα με ιδιότητα των block Toelpitz πινάκων:

$$\underset{\sim}{v}^t S = \underset{\sim}{0} \ \Rightarrow\ q_1(x)p_1(x)+q_2(x)p_2(x) = 0 \ \Rightarrow\ q_1(x)p_1(x) = -q_2(x)p_2(x) \ \Rightarrow\ \deg \text{ΕΚΠ}[p_1,p_2] \leq d_1+d_2-1$$

Γνωρίζουμε όμως ότι $\text{ΜΚΔ}[p_1,p_2]\text{ΕΚΠ}[p_1,p_2] = p_1p_2 \Rightarrow \deg \text{ΕΚΠ}[p_1,p_2] + \deg \text{ΜΚΔ}[p_1,p_2] = d_1+d_2$. Τελικά

$$\deg \text{ΜΚΔ}[p_1,p_2] = d_1+d_2-\deg \text{ΕΚΠ}[p_1,p_2] \geq d_1+d_2-d_1-d_2+1 = 1$$

δηλαδή τα p_1, p_2 έχουν κοινή ρίζα. □

Με χρήση της απαλοίφουσας μπορούμε να κατασκευάσουμε άθροισμα, γινόμενο, πηλίκο κτλ αλγεβρικών αριθμών. Ένας αλγεβρικός αριθμός ορίζεται ως η ρίζα ενός πολυωνύμου σε ένα διάστημα απομόνωσης αυτής.

Παραδείγματος χάριν έστω οι: $a = \{p(x) = 0\ , x \in [t_1,t_2]\},\ b = \{q(x) = 0\ , x \in [r_1,r_2]\}$. Αν θέσουμε $b = a+y$, τότε τα $p(x),\ q(x+y)$ έχουν κοινή ρίζα (αν θεωρηθούν ως πολυώνυμα με μεταβλητή το x) το a, άρα η διαφορά είναι ρίζα της $R(y) \equiv R[p(x), q(x+y)] = 0$. Έτσι τελικά $b-a = \{R(y) = 0,\ y \in [r_1-t_2, r_2-t_1]\}$.

Μια άλλη εφαρμογή είναι στην απόδειξη του παρακάτω

Θεώρημα 3.9. *Έστω s η απόσταση δυο οποιονδήποτε ριζών ενός πολυωνύμου $p \in \mathbb{R}[x]$ βαθμού d με συντελεστές μήκους $O_B(\tau)$. Τότε είναι $-\log s = O_B(d\tau)$.*

Απόδειξη. Αν θέσουμε όπως πριν $b = a + y$, με $s = |y|$, θα είναι $R(y) \equiv R[p(x), p(x+y)] = 0$. Έστω $R(y) = c_r y^r + \cdots + c_1 y + c_0$, όπου $r \leq d^2$ από τον ορισμό της απαλοίφουσας ως ορίζουσας διάστασης $2d$. Έτσι $c_i = O_B(d^2 2^{d\tau})$. Από το (αντίστροφο) φράγμα του Cauchy τώρα

$$s \geq \frac{c_r}{1 + \max\limits_{0 \leq i \leq r} |c_i|} \succ \frac{1}{\max\limits_{0 \leq i \leq r} |c_i|}$$

Για $s \leq 1$, και αν c_{i_0} ο μέγιστος κατ' απόλυτο τιμή συντελεστής, παίρνουμε τελικά $-\lg s \geq \lg |c_{i_0}| - \lg 1 \cong 2 \lg d + d\tau = O_B(d\tau)$. □

Η ορίζουσα του S δεν αλλάζει αν προσθέσουμε την j-οστή στήλη της, πολλαπλασιασμένη με x^{j-1} για $j = 2, \ldots, d_1 + d_2$, στην πρώτη στήλη. Όμως ο πίνακας έχει αλλάξει καθόσον η πρώτη στήλη περιέχει τα πολυώνυμα $p_1(x), \ldots, x^{d_2-1} p_1(x), p_2(x), \ldots, x^{d_1-1} p_2(x)$. Με βάση αυτήν την παρατήρηση, ορίζουμε:

Ορισμός 3.10. *Η μηδενική υπο-απαλοίφουσα R_0 είναι η απαλοίφουσα $R(p_1, p_2) = \det S$.*

Για $0 < i \leq \min\{d_1, d_2\}$, η i-οστή υπο-απαλοίφουσα είναι η ορίζουσα R_i.

Για $i = \min\{d_1, d_2\}$, η υπο-απαλοίφουσα R_i είναι η ορίζουσα του πίνακα που περιέχει μόνο συντελεστές του πολυωνύμου με το μεγαλύτερο βαθμό. Η πρώτη γραμμή της ξεκινά με το διάνυσμα των συντελεστών του μεγιστοβάθμιου πολυωνύμου και κατόπιν μηδενικά.

Για $\min\{d_1, d_2\} < i < \max\{d_1, d_2\}$ ορίζουμε $R_i = 0$. Σχηματικά:

$$R_i(p_1, p_2) = \left| \begin{array}{c:cccc} p_1(x) & a_{i+1} & \cdots & a_{d_1} & & \mathbf{0} \\ \vdots & \vdots & \ddots & & \ddots & \\ x^{d_2-i-1} p_1(x) & a_{2i-d_2+2} & \cdots & a_{i+1} & \cdots & a_{d_1} \\ p_2(x) & b_{i+1} & \cdots & b_{d_2} & & \\ \vdots & \vdots & \ddots & & \ddots & \mathbf{0} \\ x^{d_1-i-1} p_2(x) & b_{2i-d_1+2} & \cdots & a_{i+1} & \cdots & b_{d_2} \end{array} \right| \quad , \quad i = 0, 1, \ldots, \min\{d_1, d_2\}$$

όπου ορίζουμε $a_k,\ b_k = 0$ για $k < 0$.

Η ορίζουσα R_i προκύπτει από εκείνη του μετασχηματισμένου πίνακα S, αν αφαιρέσουμε τις τελευταίες i γραμμές που περιέχουν συντελεστές του p_1, τις τελευταίες i γραμμές (που περιέχουν συντελεστές του p_2), τις τελευταίες i στήλες (οι οποίες πλέον περιέχουν μόνο μηδενικά) και, τέλος, τις i αριστερότερες στήλες που βρίσκονται δεξιά της πρώτης. Για $i = 0$ δεν αφαιρούμε γραμμές ή στήλες. Η διάσταση της ορίζουσας είναι προφανώς $(d_1 + d_2 - 2i) \times (d_1 + d_2 - 2i)$.

Χάριν ευκολίας στην παρουσίαση επιτρέψαμε αρνητικούς δείκτες, ερμηνεύοντας τα αντίστοιχα a_k ως μηδενικά. Εξαρτάται από το τον αριθμό των γραμμών/στηλών που θα αφαιρέσουμε αν θα υπάρχουν ή όχι μηδενικά στο κάτω αριστερά κομμάτι κάθε υποπίνακα του R_i. Παρατηρήστε επίσης ότι για $\kappa < \lambda$, η R_κ είναι υποορίζουσα της R_λ. Έτσι όλες οι υπο-απαλοίφουσες προκύπτουν από την αρχική R_0(σε κουτιά οι γραμμές της i-οστής

υπο-απαλοίφουσας):

$$R_0(p_1,p_2)=\begin{vmatrix} p_1(x) & a_1 & \cdots & a_{i+1} & \cdots & a_{d_1} & & \\ \vdots & a_0 & & \ddots & & \ddots & & \mathbf{0} \\ \vdots & \mathbf{0} & \ddots & & \ddots & & \ddots & \\ x^{d_2-i-1}p_1(x) & & & a_0 & \cdots & a_{i+1} & \cdots & a_{d_1} \\ p_2(x) & b_1 & \cdots & b_{i+1} & \cdots & b_{d_1} & & \\ \vdots & b_0 & & \ddots & & \ddots & & \mathbf{0} \\ \vdots & & \ddots & & \ddots & & \ddots & \\ x^{d_1-i-1}p_2(x) & \mathbf{0} & & b_0 & \cdots & b_{i+1} & \cdots & b_{d_2} \end{vmatrix}$$

Αν αναπτύξουμε την R_0 ως προς την πρώτη στήλη, συνάγεται η εξής ιδιότητα:

$$R_0(p_1,p_2)\equiv R(p_1,p_2)=p_1(x)t_0(x)+p_2(x)s_0(x),\ \text{όπου}\ \deg t_0=d_2-1,\ \deg s_0=d_1-1$$

Όπως ήδη γνωρίζουμε $\deg R_0(x)=0$. Αν $i=d_2<d_1$, ο αντίστοιχος πίνακας είναι κάτω τριγωνικός και $R_{d_2}(x)=p_2(x)a_{d_2}^{d_1-d_2-1}$, άρα $\deg R_{d_2}(x)=d_2$. Γενικότερα ισχύει το παρακάτω

Θεώρημα 3.11. *Ο βαθμός της υπο-απαλοίφουσας είναι* $\deg R_i(x)\le i$ *για* $i=0,\ldots,\min\{d_1,d_2\}$.

Ενδέχεται βέβαια κάποιες υπο-απαλοίφουσες να έχουν τον ίδιο βαθμό ή ο βαθμός δυο διαδοχικών υπο-απαλοιφουσών να διαφέρει περισσότερο από 1.

Η βασική ιδιότητα των υπο-απαλοιφουσών είναι η παρακάτω ισοδυναμία:

Θεώρημα 3.12. *Εφόσον τα* $p_1,p_2\in K[x]$ *για* K *μια περιοχή μοναδικής παραγοντοποίησης με μονάδα:*

$$\text{τα } p_1,p_2 \text{ έχουν έναν κοινό διαιρέτη βαθμού } k \iff R_i=0,\ \forall i<k \text{ και } R_k\neq 0$$

3.4 Διακρίνουσα πολυωνύμου

Ορισμός 3.13. *Έστω* D *ακέραια περιοχή και* $p(x)=\sum_{i=0}^{d}c_ix^i$ *με συντελεστές* $c_i\in D, c_d\neq 0$ *και* $r_i\in\overline{D}$*(αλγεβρική θήκη του* D*),*$i=1,\ldots,d$ *οι ρίζες του* p*. Ορίζεται η διακρίνουσα:*

$$\Delta:=c_d^{2d-2}\prod_{i<j}(r_i-r_j)^2 \tag{3.2}$$

Λήμμα 3.14. $\Delta=0$ *τότε και μόνο τότε αν υπάρχει πολλαπλή ρίζα του* p*.*

Απόδειξη. $\Delta=0\iff\exists i\neq j:\ r_j=r_i\iff$ το r_i έχει πολλαπλότητα τουλάχιστον 2. □

Λήμμα 3.15. *Η διακρίνουσα συνδέεται με την απαλοίφουσα με τον τύπο* $c_d\Delta=(-1)^{\binom{d}{2}}R(p,p')$.

Απόδειξη. Έστω $p(x)=c_d\prod_{i=1}^{d}(x-r_i)$. Τότε παραγωγίζοντας με χρήση του κανόνα Leibnitz

$$p'(x)=c_d\left[\prod_{i=1}^{d}(x-r_i)\right]'=c_d\sum_{j=1}^{d}\prod_{i\neq j}(x-r_i)\quad\Rightarrow\quad p'(r_j)=c_d\prod_{i\neq j}(r_j-r_i)$$

Από τη μορφή Poisson (3.1) έχουμε:

$$R(p,p')=c_d^{d-1}\prod_{i=1}^{d}p'(r_i)$$

αντικαθιστώντας

$$R(p,p') = c_d^{d-1}\prod_{i=1}^{d} c_d \prod_{i\neq j}(r_j - r_i) = c_d^{2d-1}\prod_{i<j}\left[(-1)(r_i-r_j)^2\right] = (-1)^{\binom{d}{2}} c_d^{2d-1}\prod_{i<j}(r_i-r_j)^2 = (-1)^{\binom{d}{2}} c_d\Delta$$

τελικά, $c_d\Delta = (-1)^{\binom{d}{2}} R(p,p')$. □

Λήμμα 3.16. *Η διακρίνουσα ανήκει στην ευκλείδεια περιοχή D.*

Απόδειξη. Με χρήση ιδιοτήτας της ορίζουσας, βγάζουμε κοινό παράγοντα το c_d από την τελευταία στήλη:

$$R(p,p') = \begin{vmatrix} c_0 & c_1 & \cdots & c_d & & \\ & c_0 & c_1 & \cdots & c_d & \mathbf{0} \\ \mathbf{0} & & \ddots & \ddots & \ddots & \ddots \\ & & & c_0 & c_1 & \cdots & c_d \\ c_1 & 2c_2 & \cdots & dc_d & & \\ & c_1 & 2c_2 & \cdots & dc_d & \mathbf{0} \\ \mathbf{0} & & \ddots & \ddots & \ddots & \ddots \\ & & & c_1 & 2c_2 & \cdots & dc_d \end{vmatrix} = \left|\begin{array}{ccccccc} c_0 & c_1 & \cdots & c_d & & \mathbf{0} & \\ & c_0 & c_1 & \cdots & c_d & & \mathbf{0} \\ \mathbf{0} & & \ddots & \ddots & \ddots & \ddots & \\ & & & c_0 & c_1 & \cdots & 1 \\ c_1 & 2c_2 & \cdots & dc_d & & \mathbf{0} & \\ & c_1 & 2c_2 & \cdots & dc_d & & \mathbf{0} \\ \mathbf{0} & & \ddots & \ddots & \ddots & \ddots & \\ & & & c_1 & 2c_2 & \cdots & d \end{array}\right| c_d$$

άρα $c_d \big| R(p,p') \Rightarrow \dfrac{R(p,p')}{c_d} \in D \Rightarrow (-1)^{\binom{d}{2}}\dfrac{R(p,p')}{c_d} \in D \Rightarrow \Delta \in D$. □

Το επόμενο λήμμα συνδέει τη διακρίνουσα με μια ορίζουσα Vandermonde των ριζών του πολυωνύμου.

Λήμμα 3.17. *Το γινόμενο που εμφανίζεται στη διακρίνουσα μπορεί να εκφραστεί σαν το τετράγωνο μιας ορίζουσας Vandermonde, συγκεκριμένα $\prod_{i<j}(r_i - r_j) = \pm V(r_1,\ldots,r_d)$, όπου*

$$V(r_1,\ldots,r_d) := \begin{vmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_d \\ r_1^2 & r_2^2 & \cdots & r_d^2 \\ \vdots & \vdots & & \vdots \\ r_1^{d-1} & r_2^{d-1} & \cdots & r_d^{d-1} \end{vmatrix}$$

Απόδειξη. Θα δείξουμε πως τα δυο μέλη έχουν τον ίδιο βαθμό σαν πολυώνυμα των r_i και ότι διαιρούν το ένα το άλλο. Είναι

$$\deg\prod_{i<j}(r_i - r_j) = \binom{d}{2} = \frac{d!}{2!(d-2)!} = \frac{d(d-1)}{2}\ ,\ \deg V(r_1,\ldots,r_d) = (d-1)+(d-2)+\cdots+2+1 = \frac{d(d-1)}{2}$$

Αν $\prod_{i<j}(r_i - r_j) = 0$, τότε $r_i = r_j,\ i \neq j$. Η ορίζουσα Vandermonde έχει δυο στήλες ίδιες, δηλαδή γραμμικά εξαρτημένες άρα $V(r_1,\ldots,r_d) = 0 \Rightarrow \prod_{i<j}(r_i - r_j) \big| V(r_1,\ldots,r_d)$.

Αντίστροφα, αν $V(r_1,\ldots,r_d) = 0$ αναπτύσσοντας την ορίζουσα βλέπουμε ότι
$\prod_{i<j}(r_i - r_j) | V(r_1,\ldots,r_d) \Rightarrow V(r_1,\ldots,r_d) \big| \prod_{i<j}(r_i - r_j)$. □

Το αποτέλεσμα αυτό, σε συνδυασμό με το φράγμα Hadamard που ακολουθεί, χρησιμοποιούνται στην απόδειξη του Θεωρήματος Davenport-Mahler-Mignotte (2.6). Για την απόδειξη χρησιμοποιούμε το παρακάτω φράγμα στην ορίζουσα Vandermonde. Κατόπιν με γραμμοπράξεις σχηματίζουμε τις διαφορές και τα γινόμενα που θέλουμε:

Λήμμα 3.18. *(Φράγμα Hadamard) Αν* $A = [\underline{u}_1 \ \cdots \ \underline{u}_n] = [\underline{w}_1 \ \cdots \ \underline{w}_n]^T$ *ισχύει* $|\det A| \leq \prod_{i=1}^{n} \|\underline{u}_i\|_2 = \prod_{i=1}^{n} \|\underline{w}_i\|_2$.

Η ισότητα επιτυγχάνεται όταν οι στήλες(ή γραμμές) είναι ορθογώνιες, πχ $\left|\begin{array}{cc} 1 & c \\ c & -1 \end{array}\right| = 1+c^2 = \sqrt{1+c^2}\sqrt{c^2+1}$.

3.5 Ακολουθία Sturm-Habicht(Subresultant Sequence)

Ας δούμε τώρα πως συνδέεται η ακολουθία υπο-απαλοιφουσών με τις ακολουθίες Sturm. Υπενθυμίζουμε σύντομα την ψευδοδιαίρεση: Στον Ευκλείδειο αλγόριθμο η αύξηση του μεγέθους των (ενδιάμεσων) συντελεστών είναι εκθετική. Για το λόγο αυτό έχουν μελετηθεί μέθοδοι που γενικεύουν τη βασική σχέση, βασισμένες στην ψευδο-διαίρεση:

Ορισμός 3.19. *Στην* ψευδο-διαίρεση $\alpha p(x) = q(x)s(x) + r(x)$, *όπου* $p(x), s(x) \in \mathbb{Z}[x]$ *με* $\deg(p(x)) > \deg(r(x))$, *έχουμε* $\alpha = c_d^{\delta} \in \mathbb{Z}$, *όπου* $\delta = \deg(p(x)) - \deg(s(x)) + 1$ *και* c_d *ο μεγιστοβάθμιος συντελεστής του* p. *Έτσι το* ψευδο-πηλίκο $q(x) \in \mathbb{Z}[x]$, *συνεπώς και το* ψευδο-υπόλοιπο $r(x)$ *ανήκουν στο* $\mathbb{Z}[x]$. *Τα* $q(x), r(x)$ *είναι μοναδικά.*

Έστω $p_0(x) = a(x), p_1(x) = b(x)$ και για $i \geq 2$: $\alpha_i p_{i-2}(x) = p_{i-1}(x)q_i(x) + \beta_i p_i(x)$ όπου α_i και β_i σταθερές. Μερικές περιπτώσεις είναι:

- $\alpha_i = \beta_i = 1$ στον *Ευκλείδειο* αλγόριθμο: δίνει το ελάχιστο β_i αλλά το μέγιστο μέγεθος συντελεστών, δηλ. εκθετικό στην χειρότερη περίπτωση [Zip93].
- $\beta_i p_i(x) =$ ψευδο-υπόλοιπο στη διαίρεση που έγινε στο προηγούμενο βήμα, όπου το β_i είναι ο ΜΚΔ των συντελεστών του ψευδο-υπολοίπου (άρα υπολογίζεται ως ένα ΜΚΔ ακεραίων), δηλ. το $p_i(x)$ είναι ένα *πρωτογενές (primitive)* πολυώνυμο: μέγιστο β_i, ελάχιστο μέγεθος πολυωνυμικών συντελεστών, αλλά υψηλό υπολογιστικό κόστος. Αυτός ο αλγόριθμος εφαρμόζεται επαγωγικά και με πολλές μεταβλητές $\mathbb{Z}[x_1, \ldots, x_n]$.
- Το β_i δίνεται σε συνάρτηση των α_j, β_j για $j < i$ ενώ τα πολυώνυμα δίνονται από κάποια υπο-απαλοίφουσα(subresultant). Συγκεκριμένα, $\alpha_i = c^{d_{i-2}-d_{i-1}+1}$, όπου c ο μεγιστοβάθμιος συντελεστής του $p_{i-1}(x)$ και $\deg p_i = d_i$. Η θεωρία των Habicht, Collins, Brown αποδεικνύει πως το β_i διαιρεί το ψευδο-υπόλοιπο των $p_{i-2}(x), p_{i-1}(x)$. Επιτυγχάνονται ενδιάμεσες τιμές β_i και ενδιάμεσο μέγεθος συντελεστών των p_i σε σχέση με τις άλλες μεθόδους. Συγκεκριμένα, οι συντελεστές των p_i έχουν μήκος $O_B^*(d\tau)$, όπου τ το μέγεθος των συντελεστών στα δεδομένα πολυώνυμα. Η μέθοδος αυτή πετυχαίνει βέλτιστη δυαδική πολυπλοκότητα $O_B^*(d^3\tau)$ για τον υπολογισμό *ολόκληρης* της ακολουθίας [Lombardi-Roy-ElDin, Reischert].

Το παρακάτω θεώρημα συνδέει τις υπο-απαλοίουσες με την ακολουθία Sturm-Habicht:

Θεώρημα 3.20. *Έστω* $p_0, p_1 \in \mathbb{Z}[x]$. *Το σύνολο των υπο-απαλοιφουσών προκύπτει σαν ένα σύνολο μιας ακολουθίας ψευδο-υπολοίπων, δηλαδή*

$$\{R_0(x), R_1(x), \ldots\} = \{p_i(x) \ : \ b_i p_{i-1}(x) = q_i(x)p_i(x) + c_i^{\delta_i+1} p_{i+1}(x) \ , \ i = 2, \ldots\}$$

με $b_i, c_i \in D$, c_i *ο μεγιστοβάθμιος όρος του* p_i *και* $\delta_i = \deg q_i(x)$.

Το θεώρημα Bézout

Στο μάθημα αυτό θα γενικεύσουμε την απαλοίφουσα δυο πολυωνύμων μιας μεταβλητής στη γενική περίπτωση, δηλαδή θα ορίσουμε την απαλοίφουσα $n+1$ πολυωνύμων n μεταβλητών. Στόχος είναι η εύρεση όλων των μιγαδικών λύσεων του συστήματος με μεθόδους της γραμμικής άλγεβρας. Το κλειδί για αυτήν την προσέγγιση είναι η απαλοίφουσα. Το πλεονέκτημα της έναντι της προσέγγισης με βάσεις Gröbner, οι οποίες θα παρουσιαστούν αργότερα, είναι οι αποτελεσματικοί αλγόριθμοι που έχουμε για λύση γραμμικών συστημάτων.

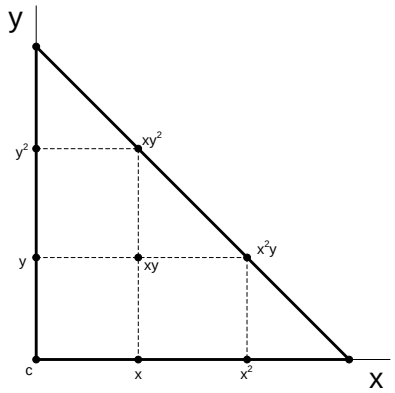
Από τον ορισμό της απαλοίφουσας που δόθηκε στα προηγούμενα λείπει μια σημαντική παράμετρος· δεν καθορίζεται ο χώρος των λύσεων, στον οποίο η απαλοίφουσα εκφράζει επιλυσιμότητα. Θα δούμε πως ο χώρος αυτός είναι ο προβολικός χώρος $\mathbb{P}^1$ στην περίπτωση μιας μεταβλητής. Στη γενική περίπτωση, το θεώρημα Bézout θα μας προσδιορίσει τον αριθμό των λύσεων στον αντίστοιχο προβολικό χώρο.

4.1 Γενικά πολυώνυμα

Σε δεδομένο πρόβλημα, ένα σύνολο δεδομένων καλείται *γενικό* (generic), ισοδύναμα δεν αποτελούν *ειδικά ή εκφυλισμένα* (degenerate, singular) δεδομένα, όταν λειτουργούν σε αυτό το πρόβλημα όπως τα περισσότερα τέτοια σύνολα. Στην πράξη γενικά δεδομένα υπολογίζονται με μεγάλη πιθανότητα χρησιμοποιώντας τυχαία επιλογή. Στα παρακάτω θα θεωρήσουμε συστήματα με πολυώνυμα που έχουν συμβολικούς συντελεστές, δηλαδή οι συντελεστές τους είναι κι αυτοί μεταβλητές που παίρνουν τιμές σε κάποιο χώρο συντελεστών. Έτσι θα μιλάμε για γενικά(generic) πολυώνυμα, που δεν είναι εξαρτημένα μεταξύ τους και οι συμβολικοί συντελεστές τους δεν είναι γενικά μηδενικοί. Ένα γενικό πολυώνυμο n μεταβλητών συνολικού βαθμού d, θα έχει

$$\binom{n+d}{n}$$

όρους, όπως φαίνεται εύκολα με ένα συνδυαστικό επιχείρημα(είναι ο αριθμός των μη αρνητικών ακέραιων λύσεων της $a_1 + a_2 + \cdots + a_n \leq d$). Αν οι συντελεστές λάβουν τιμές και «αρκετές» από αυτές είναι μηδενικές τότε θα μιλάμε για *ειδικά ή εκφυλισμένα* πολυώνυμα. Π.χ. αν θεωρήσουμε ένα γενικό πολυώνυμο συνολικού βαθμού 3 με δυο μεταβλητές και απεικονίσουμε τα μονώνυμά του σε ένα σύστημα αξόνων:



ένας κανόνας γενικότητας θα μπορούσε να είναι να μην λάβουν τιμή μηδέν οι συντελεστές των μονωνύμων που βρίσκονται στις κορυφές του τριγώνου. Τελικά ο χαρακτηρισμός γενικό πολυώνυμο είναι κάπως ασαφής και

εξαρτάται από τη γενική ιδιότητα του πολυωνύμου που θέλουμε κάθε φορά να διατηρήσουμε(πχ ένα σύστημα να μην έχει πολλαπλές ρίζες) και η οποία δεν ισχύει σε εκφυλισμένες περιπτώσεις.

Εφεξής θεωρούμε πως οι δεδομένες εξισώσεις είναι ανεξάρτητες και πως οι συντελεστές είναι γενικοί(συμβολικοί). Στα (μη) γραμμικά συστήματα:

- Πλήθος εξισώσεων $>$ πλήθος μεταβλητών (υπερ-προσδιορισμένο) $\Rightarrow$ γενικά δεν υπάρχουν ρίζες.
- Πλήθος εξισώσεων = πλήθος μεταβλητών (καλώς ορισμένο) $\Rightarrow$ γενικά υπάρχει πεπερασμένο πλήθος ριζών, το οποίο φράσσεται από τα διάφορα όρια (στα γραμμικά συστήματα μοναδική ρίζα).Η διάσταση του αλγεβρικού συνόλου είναι 0.
- Πλήθος εξισώσεων $<$ πλήθος μεταβλητών (υπο-προσδιορισμένο) $\Rightarrow$ απειρία λύσεων, διάσταση συνόλου > 0.

4.2 Ομογενοποίηση

Η χρησιμότητα της ομογενοποίησης θα φανεί στα επόμενα, όταν μιλήσουμε για τον προβολικό χώρο. Αρχικά εισάγουμε την έννοια του ομογενούς πολυωνύμου:

Ορισμός 4.1. *Ένα πολυώνυμο $F \in \mathbb{F}[x_0, x_1, \cdots, x_n]$ καλείται ομογενές βαθμού d(ή απλά ομογενές), όπου $d = \deg F$ ο συνολικός βαθμός του πολυωνύμου, αν για κάθε $\lambda \in \mathbb{F}$ ισχύει $F(\lambda \underline{x}) = \lambda^d F(\underline{x}), \quad \forall \underline{x} \in \mathbb{F}^{n+1}$.*

Ισοδύναμα, για κάθε μονώνυμο $\underline{x}^{(\alpha_0,\alpha_1,\ldots,\alpha_n)}$ του F ισχύει $\sum_{k=0}^{n} \alpha_k = d$, δηλαδή ο συνολικός βαθμός κάθε όρου του πολυωνύμου ισούται με το βαθμό του πολυωνύμου.

Έστω $f \in \mathbb{F}[x_1, \cdots, x_n]$. Μπορούμε να εισάγουμε μια επιπλέον μεταβλητή x_0(ομογενοποιητική μεταβλητή) σε κάθε όρο του f, σε δύναμη τέτοια ώστε να προκύψει ένα ομογενές πολυώνυμο $F \in \mathbb{F}[x_0, x_1, \cdots, x_n]$ βαθμού $\deg f$, δηλαδή $F(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. Η διαδικασία αυτή λέγεται *ομογενοποίηση* του f και το F ομογενές πολυώνυμο που αντιστοιχεί στο f.

Στην πράξη θα συναντήσουμε πολυώνυμα(όπως πχ η απαλοίφουσα ενός συστήματος) τα οποία είναι ομογενή όχι μόνο ως προς το σύνολο των μεταβλητών, αλλά και ως προς μικρότερες ομάδες μεταβλητών. Συγκεκριμένα:

Ορισμός 4.2. *Έστω μια διαμέριση των μεταβλητών σε m υποσύνολα $X_1, \ldots, X_m$. Ένα πολυώνυμο f καλείται* πολυ-ομογενές*(multihomogenous) ή m-ομογενές αν είναι ομογενές(βαθμού $d_i = \deg_{X_i} f$) ως προς κάθε υποσύνολο X_i για $i = 1, \ldots, m$.*

Με άλλα λόγια, ένα πολυώνυμο πολυ-ομογενοποιείται με την εισαγωγή μιας τεχνητής μεταβλητής για κάθε υποσύνολο X_i. Παρατηρήστε πως το πολυώνυμο είναι συνεπώς και ομογενές. Ένα σύστημα που αποτελείται από πολυ-ομογενή πολυώνυμα, ως προς την ίδια διαμέριση μεταβλητών, καλείται m-ομογενές(m-homogeneous).

Παράδειγμα 4.1. Το $f = c_{110}x_1x_2y_0 + c_{201}x_1^2y_1 + c_{111}x_1x_2y_1 + c_{001}x_0^2y_1$ είναι πολυ-ομογενές ως προς τα $X_1 = (x_0, x_1, x_2)$, $X_2 = (y_0, y_1)$ με $m = 2$, όπου $n_1 = 2, n_2 = 1$ και $d_1 = 2, d_2 = 1$.

4.3 Προβολική απαλοίφουσα και όριο Bézout

Σε αυτήν την παράγρραφο γενικεύουμε τον ορισμό της απαλοίφουσας για ένα σύστημα $n+1$ πολυωνύμων $f_i \in \mathbb{F}[x_1, \ldots, x_n],\ i = 0, \ldots, n$. Όπως και στην περίπτωση του πίνακα Sylvester, η απαλοίφουσα (ή επιλύουσα: resultant or eliminant) παρέχει μια συνθήκη ύπαρξης ριζών στο υπερ-προσδιορισμένο σύστημα $\{f_i = 0 \ : \ i = 0, \ldots, n\}$.

Για συστήματα δύο πολυωνύμων με $n = 1$, η απαλοίφουσα είναι η ορίζουσα του πίνακα Sylvester. Θυμίζουμε το θεώρημα (3.8):

Θεώρημα 3.8. *Έστω δυο πολυώνυμα $p_1, p_2 \in \mathbb{Z}[x]$. Τότε $R = \det S = 0$ ανν τα πολυώνυμα έχουν κοινή ρίζα.*

Δίνουμε έναν ορισμό της απαλοίφουσας για τη γενική περίπτωση:

Ορισμός 4.3. *Η απαλοίφουσα R του συστήματος $n+1$ πολυωνύμων σε n μεταβλητές και με συμβολικούς συντελεστές είναι ένα πολυώνυμο με ακέραιους συντελεστές και μεταβλητές τους συμβολικούς συντελεστές του αρχικού συστήματος. Όταν οι συμβολικοί συντελεστές λάβουν συγκεκριμένες τιμές, $R = 0$ αν και μόνο αν το αρχικό σύστημα έχει λύση.*

Μέχρι τώρα δεν έχουμε διευκρινίσει το χώρο των λύσεων στον οποίο αναφέρεται το κριτήριο αυτό, δηλαδή δεν έχουμε πει **πού** ακριβώς η απαλοίφουσα εκφράζει επιλυσιμότητα.

Παράδειγμα 4.2. Αν $f_0, f_1 \in \mathbb{F}[x]$ με συμβολικούς συντελεστές και θεωρήσουμε το σύστημα $\begin{cases} f_0 = c_{00} + c_{01}x = 0 \\ f_1 = c_{10} + c_{11}x = 0 \end{cases}$ στη γενική περίπτωση μπορούμε να λύσουμε το $f_0 = 0$ και να έχουμε μοναδική ρίζα $x = -\dfrac{c_{00}}{c_{01}}$. Το σύστημα έχει λύση ανν $c_{10} - \dfrac{c_{00}}{c_{01}}c_{11} = 0$ και άρα η απαλοίφουσα του συστήματος είναι $R = c_{01}c_{10} - c_{00}c_{11}$. Παρατηρήστε πως όταν οι συντελεστές λάβουν τιμές στο $\mathbb{F}$ η απαλοίφουσα $R \in \mathbb{Z}[c_{ij}]$ ισούται με την ορίζουσα του πίνακα Sylvester.

Ο ορισμός (4.3) είναι επίσης ασαφής ως προς τον χώρο των λύσεων. Στην ουσία είναι ο χώρος των λύσεων που μας καθορίζει την απαλοίφουσα. Έτσι ορίζεται η προβολική (κλασική) απαλοίφουσα όταν ο χώρος των λύσεων είναι ο προβολικός χώρος $\mathbb{P}^n$, ή η τορική απαλοίφουσα, η οποία εκφράζει την ύπαρξη ριζών σε ένα τορικό αλγεβρικό σύνολο. Εδώ θα μιλήσουμε για την προβολική απαλοίφουσα.

Η ιδέα πίσω από τον προβολικό χώρο είναι να αντικαταστήσουμε τις συντεταγμένες $(x_1, \ldots, x_n)$ ενός σημείου με τους λόγους $\dfrac{x_1}{x_0}, \ldots, \dfrac{x_n}{x_0}$, όπου x_0 μια καινούρια συντεταγμένη. Έτσι το σημείο παρίσταται ως $(x_0 : x_1 : \cdots : x_n)$ με την έννοια ότι μόνο οι λόγοι των συντεταγμένων έχουν σημασία. Δηλαδή $(\lambda x_0 : \lambda x_1 : \cdots : \lambda x_n) = (x_0 : x_1 : \cdots : x_n)$. Για κάθε μη μηδενικό x_0 ένα τέτοιο σημείο αντιστοιχεί σε ένα σημείο στον $\mathbb{F}^n$, ενώ τα σημεία με $x_0 = 0$ αναπαριστούν σημεία στο άπειρο. Μιλώντας πιο αυστηρά, ο προβολικός χώρος πάνω σε ένα σώμα $\mathbb{F}$ ορίζεται ως το πηλίκο

$$\mathbb{P}^n_{\mathbb{F}} = (\mathbb{F}^{n+1} - \{\underline{0}\})/_{\sim}$$

όπου $\sim$ η σχέση ισοδυναμίας στον $\mathbb{F}^{n+1}$: $\underline{x} \sim \lambda\underline{x}$, για κάθε $\lambda \in \mathbb{F}^*$.

Ορισμός 4.4. *Ο προβολικός χώρος $\mathbb{P}^n_{\mathbb{C}}$, ή απλούστερα $\mathbb{P}^n$, είναι το σύνολο, διάστασης n, των κλάσεων ισοδυναμίας των διανυσμάτων στο $\mathbb{C}^{n+1}$ που έχουν τουλάχιστον ένα μη μηδενικό στοιχείο, όπου ταυτίζουμε διανύσματα που διαφέρουν κατά ένα μη μηδενικό σταθερό πολλαπλάσιο:*

$$\mathbb{P}^n := \{(\alpha_0 : \cdots : \alpha_n) \in \mathbb{C}^{n+1} | (\alpha_0 : \cdots : \alpha_n) \neq \underline{0}, (\alpha_0 : \cdots : \alpha_n) \sim (\lambda\alpha_0 : \cdots : \lambda\alpha_n), \lambda \in \mathbb{C}^*\}.$$

Ο προβολικός χώρος $\mathbb{P}^n$ προβάλλεται με 1-1 αντιστοιχία στον $\mathbb{C}^n$ εάν θέσουμε $\alpha_{n+1} = 1$, και προβάλλεται στο άπειρο εάν θέσουμε $\alpha_{n+1} = 0$.

Παράδειγμα 4.3. Ας θεωρήσουμε τη σχέση $(x_0 : x_1) \sim (\lambda x_0 : \lambda x_1)$ όπου $x_i \in \mathbb{C}$. Αν $x_0 = 0 \neq x_1$ έχουμε μια κλάση ισοδυναμίας με εκπρόσωπο $(0 : 1)$. Η κλάση αυτή είναι το προβολικό άπειρο. Αν $x_0 = 1$, παίρνουμε κλάσεις με εκπροσώπους $(1 : x_1)$, κάθε μια από τις οποίες αντιστοιχεί στο μιγαδικό $x_1 \in \mathbb{C}$.

Το πλεονέκτημα του $\mathbb{P}^n$ είναι ότι συμπεριλαμβάνει τις «ρίζες στο άπειρο». Έτσι έχουμε γνωστό πλήθος ριζών, το οποίο δίνεται από το παρακάτω

Θεώρημα 4.5. [Béz79] *Το πλήθος των κοινών ριζών στο $\mathbb{P}^n_{\mathbb{C}}$ για σύστημα πολυωνύμων $f_1, \ldots, f_n$ με n μεταβλητές και δεδομένους συνολικούς βαθμούς* $\deg f_i$ *φράσσεται από το*

$$\prod_{i=1}^{n} \deg\ f_i,$$

όπου οι πολλαπλές ρίζες μετρούνται με την πολλαπλότητά τους. Εάν οι συντελεστές είναι γενικοί (δηλ. αρκετά τυχαίοι) τότε το όριο είναι ακριβές.

Παράδειγμα 4.4. Έστω οι παράλληλες ευθείες $3x-2y+5=0$ και $3x-2y+1=0$. Το σύστημα είναι αδύνατο, όμως αν ομογενοποιήσουμε θα είναι $3x-2y+5z=0$ και $3x-2y+z=0$. Με απαλοιφή του z παίρνουμε $2y=3x$, $z=0$. Άρα στο προβολικό επίπεδο υπάρχει σημείο τομής, το $(x,y,z)=(2,3,0)$ που δηλώνει ρίζα στο άπειρο.

Αν πάρουμε $3x-2y+5=0$ και $4x-7y+2=0$, ομογενοποιούμε σε $3x-2y+5z=0$ και $4x-7y+2z=0$. Απαλοίφοντας το z είναι $14x=31y$, $z=-\frac{13}{31}x$ και η προβολική ρίζα είναι $(31,14,-13)$, η οποία αντιστοιχεί στη συνήθη ρίζα $\left(\frac{-31}{13},\frac{-14}{13}\right)$.

Υπάρχουν βελτιώσεις επί του θεωρήματος όταν το σύστημα είναι πολυ-ομογενές: Έστω η διαμέριση των μεταβλητών $X_1,\ldots,X_m$, όπου το υποσύνολο X_i περιέχει n_i μεταβλητές και $n_1+\cdots+n_m=n$ το σύνολο των μεταβλητών. Έστω ένα m-ομογενές σύστημα n πολυωνύμων, όπου το i-στό πολυώνυμο έχει βαθμό d_{ij} ως προς τις μεταβλητές X_j, κατόπιν ομογενοποίησης με την εισαγωγής της μεταβλητής με αριθμό n_j+1. Τότε ισχύει,

Θεώρημα 4.6. *[m-Bézout] Το πολυομογενές φράγμα m-Bézout φράσσει το πλήθος των απομονωμένων ριζών στο* $\mathbb{P}^{n_1}\times\cdots\times\mathbb{P}^{n_m}$ *από τον* συντελεστή *του* $y_1^{n_1}\cdots y_m^{n_m}$ *στο νέο πολυώνυμο*

$$\prod_{i=1}^{n}(d_{i1}y_1+\cdots+d_{im}y_m)$$

Για πολυώνυμα με τυχαίους συντελεστές, το φράγμα είναι ακριβές.

Τα πολυ-ομογενή πολυώνυμα προσφέρουν μια ενδιάμεση θεώρηση μεταξύ της κλασικής προβολικής θεωρίας και της θεωρίας αραιής απαλοιφής που γενικεύει όλα τα παραπάνω όρια [CLO05].

Για την περίπτωση μιας μεταβλητής, έχουμε αποδείξει τη μορφή Poisson (3.1). Ο τύπος γενικεύεται με το παρακάτω

Θεώρημα 4.7. *Τύπος Poisson:* $R=C\prod_{\alpha\in A}f_k(\alpha)$, *όπου* A *είναι το σύνολο κοινών ριζών των* $f_1,\ldots,f_{k-1}$, $f_{k+1},\ldots,f_{n+1}$ *και* C *μια σταθερά ανεξάρτητη από τους συντελεστές του* f_k.

Πόρισμα 4.8. *Ο βαθμός της απαλοίφουσας ως προς τους συντελεστές του* $f_k(x)$ *δίνεται από το όριο στο πλήθος κοινών ριζών των* $f_1,\ldots,f_{k-1},f_{k+1},\ldots,f_{n+1}$.

Η κλασική απαλοίφουσα [Euler,Cayley,Sylvester,Bézout] αφορά στις προβολικές μιγαδικές ρίζες συνεπώς ο βαθμός της ως προς τους συμβολικούς συντελεστές του αρχικού συστήματος εξαρτάται από το όριο Bézout, ενώ στον τύπο Poisson το A περιλαμβάνει όλες τις μιγαδικές προβολικές ρίζες. Άρα:

- $\deg_{f_i}R=\prod_{j=0,j\neq i}^{n}\deg f_i$ = πλήθος προβολικών ριζών του $f_0=\cdots=f_{i-1}=f_{i+1}=\cdots=f_n=0$.
- Η απαλοίφουσα είναι ομογενές πολυώνυμο $R\in\mathbb{Z}[c_{ij}]$, συνολικού βαθμού $\deg R=\sum_{i=0}^{n}\deg_{f_i}R$.

4.4 Η απαλοίφουσα γραμμικού συστήματος $n+1$ πολυωνύμων

Σε γραμμικό σύστημα $n+1$ πολυωνύμων που γράφεται ως $M\underline{x}=b,\underline{x}\in\mathbb{C}^n$, υπάρχει ρίζα αν και μόνο αν το σταθερό διάνυσμα $\underline{b}$ ανήκει στο πεδίο των στηλών του πίνακα συντελεστών M των $n+1$ πολυωνύμων, ισοδύναμα η τάξη του $(n+1)\times(n+1)$ πίνακα M των συντελεστών επαυξημένο με τη στήλη b είναι $\mathrm{rank}<n+1$, ή αλλιώς $\det M=0$.

Έστω M_{ij} ο υποπίνακας $n \times n$ που προκύπτει από το M σβήνοντας τη γραμμή και τη στήλη που περιέχουν το στοιχείο (i,j). Όταν $\det M_{(n+1)(n+1)} \neq 0$ τότε λύνουμε το αντίστοιχο υποσύστημα με τον κανόνα Cramer και η j-οστή συνιστώσα της λύσης δίνεται από τον τύπο

$$\alpha_j = \frac{(-1)^j \det M_{(n+1)j}}{\det M_{(n+1)(n+1)}}$$

Αυτή είναι ρίζα και της τελευταίας εξίσωσης αν και μόνο αν

$$\begin{array}{rrcl} & c_{(n+1)1}\alpha_1 + \ldots + c_{(n+1)n}\alpha_n & = & b_{n+1} \\ \iff & c_{(n+1)1}(-1)\det M_{(n+1)1} + \ldots + c_{(n+1)n}(-1)^n \det M_{(n+1)n} & = & b_{n+1}\det M_{(n+1)(n+1)} \\ \iff & \det M & = & 0 \end{array}$$

επειδή παρατηρούμε πως πρόκειται για το ανάπτυγμα της $\det M$ ως προς την τελευταία σειρά.

Σημειώστε ότι $\deg_{f_i} R = 1$ και $\deg R = n+1$.

Παράδειγμα 4.5. $x+2y=-1,\ 2x+3y=0,\ x+y=1$. Έχουμε $\operatorname{rank}(M)=2$ και η κοινή ρίζα είναι η $(3,-2)$.

Αυτή η ορίζουσα $\det M$ ισούται με την απαλοίφουσα του γραμμικού συστήματος. Οι στήλες του M αντιστοιχούν στα γραμμικά μονώνυμα, ενώ οι γραμμές περιέχουν τα πολυώνυμα f_i. Αν $\operatorname{rank}(M) = n$ τότε υπάρχει μοναδική ρίζα, αλλιώς απειρία λύσεων.

Αν $\underline{\nu} = [1, \alpha_0, \ldots, \alpha_n]^t$, το γινόμενο $M\underline{\nu}$ είναι το διάνυσμα των τιμών πολυωνύμων στο σημείο $\underline{\nu}$ άρα (ανάμεσα) στα μη-μηδενικά διανύσματα που βρίσκονται στον πυρήνα του M υπάρχει το διάνυσμα $\underline{\nu}$ που αποτελείται από τις συντεταγμένες της κοινής ρίζας.

Αντίθετα με τις ειδικές περιπτώσεις μίας μεταβλητής και γραμμικών συστημάτων, δεν υπάρχει γενικός τύπος για την απαλοίφουσα σε συνάρτηση των συντελεστών.

Υπολογισμός απαλοίφουσας

Ο προσδιορισμός της απαλοίφουσας σε τυχόν πολυωνυμικό σύστημα είναι το πραγματικό ζητούμενο, αφού εκεί το σύνολο των λύσεων μας είναι γενικά άγνωστο. Σε γραμμικά συστήματα είδαμε ότι η απαλοίφουσα είναι ο πίνακας των συντελεστών. Στη γενική περίπτωση αρκούμαστε στον υπολογισμό πολλαπλασίων της, με τη μορφή οριζουσών πινάκων που γενικεύουν τον πίνακα συντελεστών γραμμικού συστήματος και τον πίνακα Sylvester. Έτσι σε αυτά τα πολλαπλάσια υπεισέρχεται ένας *παρασιτικός παράγοντας*.

Επιδιώκουμε συνεπώς να κατασκευάσουμε τετράγωνους πίνακες M για τους οποίους:

(i) η ορίζουσα $\det M$ δεν είναι γενικά μηδέν,

(ii) η ορίζουσα $\det M$ διαιρείται από την απαλοίφουσα, άρα αποτελεί μια αναγκαία συνθήκη ύπαρξης ριζών,

(iii) ο πίνακας M έχει το μικρότερο δυνατό μέγεθος και οι επιπλέον παρασιτικές ρίζες που μηδενίζουν την $\det M$ χωρίς να είναι ρίζες του συστήματος είναι σημειακές δηλ. διάστασης$= 0$ (ειδάλλως απαιτούνται ειδικές επιπρόσθετες πράξεις πινάκων).

Υπάρχουν οι εξής βασικοί τύποι πινάκων για την προσέγγιση της απαλοίφουσας:

Bézout ή Dixon [Dix08, EM00], όπου τα στοιχεία είναι πολυώνυμα ως προς τους συμβολικούς αρχικούς συντελεστές, επομένως έχουν μικρότερο μέγεθος και συχνά λιγότερες εξαιρέσεις.

Sylvester που στην γενική περίπτωση ερευνήθηκε από το [Mac02] για την κλασική απαλοίφουσα και τους [Stu93, Stu94, CLO05] για την αραιή(sparse).

Υβριδικός αποτελεί συνδυασμό των 2 παραπάνω, π.χ. [DD01].

Για τον πίνακα M που υπολογίζεται είναι $\det M = P \cdot R$, όπου $P \in \mathbb{Z}[c_{ij}]$ ο παρασιτικός παράγοντας. Εδώ θα ασχοληθούμε κυρίως με πίνακες τύπου Sylverster.

5.1 Πίνακες τύπου Sylvester

Οι πίνακες τύπου Sylvester κατασκευάζονται εισάγοντας γραμμές που περιέχουν τους συντελεστές των $\underset{\sim}{x}^{\alpha} f_i$ για κάποια μονώνυμα $\underset{\sim}{x}^{\alpha} \in \mathbb{F}[x_1, \ldots, x_n]$. Οι στήλες αντιστοιχούν στα μονώνυμα των αντίστοιχων συντελεστών. Έτσι πρόκειται για μια κατασκευή παρόμοια με αυτήν του πίνακα Sylvester με τη διαφορά ότι τώρα δεν έχουμε συγκεκριμένο τρόπο να επιλέξουμε τα μονώνυμα $\underset{\sim}{x}^{\alpha}$. Οι περιορισμοί όμως σε αυτήν την επιλογή(ώστε να έχουμε πίνακα απαλοίφουσας) είναι:

- Πρέπει να υπάρχει η αντίστοιχη στήλη για κάθε μονώνυμο που εμφανίζεται στα $\underset{\sim}{x}^{\alpha} f_i$, ώστε να τοποθετηθεί ο αντίστοιχος συντελεστής σε αυτήν.
- Ο πίνακας που θα προκύψει πρέπει να είναι τετράγωνος, με ορίζουσα όχι ταυτοτικά μηδέν.

Για κάθε επιλογή μονωνύμων που τηρεί τους περιορισμούς αυτούς παίρνουμε έναν πίνακα τύπου Sylvester. Άρα χρειαζόμαστε $n+1$ ομάδες γραμμών, μία ανά πολυώνυμο, και κατ' επέκταση $n+1$ σύνολα μονωνύμων $B_i,\ i = 0, \ldots, n$, όπου τα μονώνυμα του B_i πολλαπλασιάζονται με το f_i και δίνουν $|B_i|$ γραμμές στον πίνακα.

Θα συμβολίζουμε την ομάδα γραμμών που περιέχει τους συντελεστές του f_i με $B_i * f_i$. Οι στήλες στον πίνακα αντιστοιχούν στα μονώνυμα C, έτσι ώστε

$$\sum_{i=0}^{n} |B_i| = |C|$$

Η συνθήκη αυτή εξασφαλίζει ότι ο πίνακας είναι τετράγωνος. Τελικά ένας πίνακας τύπου Sylvester έχει τη μορφή

$$M = \begin{bmatrix} B_0 * f_0 \\ \hdashline B_1 * f_1 \\ \hdashline \vdots \\ \hdashline B_n * f_n \end{bmatrix}$$

όπου οι στήλες αντιστοιχούν στα μονώνυμα του συνόλου

$$C = \{\underset{\sim}{x}^{\alpha} \ : \ \text{υπάρχει πολυώνυμο-γραμμή στην οποία εμφανίζεται συντελεστής του } \underset{\sim}{x}^{\alpha}\}$$

Ο πίνακας τύπου Sylvester έχει την γνωστή ιδιότητα πολλαπλασιασμού με διάνυσμα από δεξιά: έστω $\underset{\sim}{v}$ ένα διάνυσμα που περιέχει τις τιμές των μονωνύμων C σε κάποιο $n-$διάστατο σημείο $\underset{\sim}{\xi}$. Τότε $M\underset{\sim}{v}$ εκφράζει τις τιμές των πολυωνύμων των γραμμών στο $\underset{\sim}{\xi}$. Εάν το $\underset{\sim}{\xi}$ είναι κοινή ρίζα των $n+1$ πολυωνύμων, τότε $\underset{\sim}{v}$ ανήκει στον πυρήνα του M.

Λήμμα 5.1. *Έστω τετράγωνος πίνακας M τύπου Sylvester, δηλ. με γραμμές που αντιστοιχούν σε γινόμενα των $n+1$ πολυωνύμων επί μονώνυμα στις n μεταβλητές. Αν υπάρχει $\underset{\sim}{\xi} \in \mathbb{C}^n$ κοινή ρίζα του συστήματος $\{f_i = 0,\ i = 0, \ldots, n\}$ τότε υπάρχει μη μηδενικό διάνυσμα $\underset{\sim}{v}$ στον πυρήνα $\ker M$. Ισοδύναμα $\det M = 0$.*

Απόδειξη. Κατασκευάζουμε το διάνυσμα $\underset{\sim}{v}$ που περιέχει τις τιμές των μονωνύμων των στηλών στο $\underset{\sim}{\xi}$. Αυτό είναι μη μηδενικό στη γενική περίπτωση. Το γινόμενο $M\underset{\sim}{v}$ περιέχει τις τιμές των πολυωνύμων $\underset{\sim}{x}^{\alpha_i} f_i$ (όπου τα $\underset{\sim}{x}^{\alpha_i}$ είναι τα μονώνυμα του B_i) στο $\underset{\sim}{\xi}$, άρα πρόκειται για το μηδενικό διάνυσμα:

$$M \cdot \underset{\sim}{v} = \begin{bmatrix} \underset{\sim}{\xi}^{\alpha_0} f_0(\underset{\sim}{\xi}) \\ \hdashline \underset{\sim}{\xi}^{\alpha_1} f_1(\underset{\sim}{\xi}) \\ \hdashline \vdots \\ \hdashline \underset{\sim}{\xi}^{\alpha_n} f_n(\underset{\sim}{\xi}) \end{bmatrix} = \underset{\sim}{0}$$

τελικά $\underset{\sim}{v} \in \ker M$. □

Ομοίως από αριστερά θεωρούμε πως το $\underset{\sim}{v}^t$ περιέχει τους συντελεστές $n+1$ πολυωνύμων q_i σε αντιστοιχία με τα μονώνυμα B_i. Το $\underset{\sim}{v}^t M$ περιέχει τους συντελεστές του $\sum_{i=0}^{n} f_i q_i$ σε αντιστοιχία με τα μονώνυμα του C.

Αυτή η ιδιότητα φανερώνει μια γενικευμένη δομή Toeplitz. Ο πίνακας τύπου Sylvester περιέχει $n+1$ υποπίνακες με δομή μη-γραμμική Toeplitz, άρα είναι μη-γραμμικός Toeplitz κατά ομάδες γραμμών όπου κάθε ομάδα αντιστοιχεί σε ένα πολυώνυμο, και καλείται quasi-Toeplitz. Παρατηρούμε πως η αντιμετάθεση στηλών (και γραμμών εφόσον δεν παραβιάζεται η ομαδοποίηση) δίνει ένα νέο πίνακα quasi-Toeplitz, με τις ίδιες ιδιότητες.

Πόρισμα 5.2. *Η ορίζουσα $\det M$ διαιρείται από την απαλοίφουσα του συστήματος: $R \big| \det M$.*

Απόδειξη. Αν $R = 0$, υπάρχει κοινή ρίζα, άρα από το προηγούμενο λήμμα $\det M = 0 \Rightarrow R \big| \det M$. □

Παρατηρήστε ότι δε μπορούμε να ισχυριστούμε το αντίστροφο, όπως στην περίπτωση μιας μεταβλητής, λόγω του παρασιτικού παράγοντα.

Γνωρίζοντας ότι η $\det M$ είναι πολλαπλάσιο της απαλοίφουσας, μπορούμε να δώσουμε ένα κάτω φράγμα για τον αριθμό των στηλών που περιέχουν συντελεστές καθενός f_i:

Πόρισμα 5.3. *Είναι* $|B_i| \geq \prod_{j=0, j\neq i}^{n} \deg f_i, \quad i = 0, \ldots, n.$

Απόδειξη. Το $|B_i|$ είναι ο βαθμός της $\det M$ ως προς του συντελεστές του f_i. Άρα

$$|B_i| = \deg_{f_i}[\det M] \geq \deg_{f_i} R \geq \prod_{j=0, j\neq i}^{n} \deg f_i$$

όπου χρησιμοποιήθηκε το προηγούμενο πόρισμα και το θεώρημα Bézout (4.6). □

Βλέπουμε ότι η βέλτιστη (δηλ. ελάχιστη) διάσταση των πινάκων αυτών ισούται με τον συνολικό βαθμό της απαλοίφουσας. Σε αυτήν την περίπτωση η ορίζουσά τους δίνει την απαλοίφουσα ως πολυώνυμο στους αρχικούς συντελεστές. Έτσι, στις ειδικές περιπτώσεις που έχουμε δει, ο πίνακας των συντελεστών γραμμικού συστήματος και ο πίνακας Sylvester είναι οι μικρότεροι δυνατοί.

5.2 Η Μέθοδος Macaulay

Η μέθοδος που αναπτύχθηκε από τον Macaulay(1902) κατασκευάζει έναν αρκετά καλό πίνακα M τύπου Sylvester και επίσης ορίζει έναν υποπίνακα M', η ορίζουσα του οποίου είναι ο παρασιτικός παράγοντας, δηλαδή

$$R = \frac{\det M}{\det M'}$$

Αρχικά ορίζουμε την ομαλότητα(regularity) του M ως εξής

$$\rho := \left(\sum_{i=0}^{n} \deg f_i \right) - n$$

και λαμβάνουμε

$$C = \{\underset{\sim}{x}^{\alpha} \ : \ \deg \underset{\sim}{x}^{\alpha} \leq \rho\}$$

Γνωρίζουμε ότι $|C| = \binom{\rho + n}{n}$, άρα αυτή θα είναι και η διάσταση του M.

Θα ορίσουμε τώρα μια διαμέριση του C σε $n+1$ σύνολα:

$$\begin{aligned}
C_1 &= \{\underset{\sim}{x}^{\alpha} \in C \ : \ \alpha_1 \geq d_1\} \\
C_2 &= \{\underset{\sim}{x}^{\alpha} \in (C - C_1) \ : \ \alpha_2 \geq d_2\} \\
&\vdots \\
C_i &= \left\{ \underset{\sim}{x}^{\alpha} \in \left(C - \bigcup_{j=1}^{i-1} C_j \right) \ : \ \alpha_i \geq d_i \right\} \\
&\vdots \\
C_n &= \left\{ \underset{\sim}{x}^{\alpha} \in \left(C - \bigcup_{j=1}^{n-1} C_j \right) \ : \ \alpha_n \geq d_n \right\} \\
C_0 &= C - \bigcup_{j=1}^{n} C_j
\end{aligned}$$

όπου $d_i = \deg f_i$. Οι συνθήκες $\alpha_i \geq d_i$ θα μπορούσαν να γραφούν ισοδύναμα ως $x_i^{d_i} | \underset{\sim}{x}^{\alpha}$.

Τα μονώνυμα που θα πολλαπλασιάσουν τα f_i στις γραμμές του M είναι:

$$\begin{aligned} B_i &:= \left\{ \frac{\underset{\sim}{x}^{\alpha}}{x_i^{d_i}} \ : \ x^{\alpha} \in C_i \right\} \quad , \quad i = 1, 2, \ldots, n \\ B_0 &:= C_0 \end{aligned}$$

Σημειώνουμε πως αν είχαμε ομογενοποιήσει τα πολυώνυμα, το B_0 θα εντασσόταν στο γενικό τύπο, δηλαδή θα ήταν τα μονώνυμα του C_0 διαιρεμένα με την ομογενοποιητική μεταβλητή υψωμένη στον $\deg f_0$.

Παράδειγμα 5.1. Έστω $f_0, f_1 \in \mathbb{F}[x]$. Η ομαλότητα είναι $\rho = d_0 + d_1 - 1$, και $\dim M = \binom{\rho+1}{1} = \rho + 1 = d_0 + d_1$. Τελικά $\det R = \det S$, όπου S ο πίνακας Sylvester. Εκ κατασκευής του πίνακα Macaulay συμπεραίνουμε πως $M = S$.

Παράδειγμα 5.2. Έστω $f_i \in \mathbb{F}[x_1, \ldots, x_n]$ γραμμικά πολυώνυμα. Είναι $\rho = (n+1) - n = 1$ άρα το C θα περιέχει τα γραμμικά μονώνυμα και τη μονάδα. Είναι $C_i = \{x_i\} \Rightarrow B_i = \{1\}$ και $C_0 = \{1\}$. Τελικά βλέπουμε πως ο πίνακας Macaulay συμπίπτει με τον πίνακα των συντελεστών.

Στα δυο παραπάνω παραδείγματα, η μέθοδος του Macaulay μας έδωσε το βέλτιστο ως προς διάσταση πίνακα και μάλιστα προσέγγισε ακριβώς την απαλοίφουσα, χωρίς παρασιτικό παράγοντα.

Ο πίνακας αυτός καλείται πίνακας Macaulay. Θα αποδείξουμε ότι πρόκειται για πίνακα τύπου Sylvester:

- Τα μονώνυμα των γραμμών $B_i * f_i$ εμφανίζονται στο C: Πράγματι τα μονώνυμα αυτά ανήκουν εκ κατασκευής στα C_i, τα οποία είναι διαμέριση του C.

  Συγκεκριμένα, αν $\underset{\sim}{x}^{\alpha} \in B_i, \ i = 1, \ldots, n$, θα είναι $\deg \underset{\sim}{x}^{\alpha} \leq \rho - d_i$. Επειδή πολλαπλασιάζονται με το f_i ο μέγιστος βαθμός στο $B_i * f_i$ είναι ρ.

  Για το $B_0 = \{\underset{\sim}{x}^{\alpha} \ : \ 0 \leq \alpha_i \leq d_i - 1\}$ έχουμε (αθροίζοντας τις ανισότητες) $\sum_{i=1}^{n} \alpha_i \leq \sum_{i=1}^{n} d_i - n$. Όταν πολλαπλασιάσουμε επί f_0 παίρνουμε πολυώνυμα βαθμού $\sum_{i=0}^{n} \alpha_i - n = \rho$.

- Προφανώς ο M είναι τετράγωνος πίνακας. Θα δείξουμε πως η ορίζουσά του $\det M \in \mathbb{Z}[c_{ij}]$ δεν είναι ταυτοτικά μηδέν.

  Έστω V το σύνολο των λύσεων της $\det M = 0$, και D το πλήθος όλων των c_{ij}. Θα είναι $\det M \equiv 0$ ανν $V = \mathbb{C}^D$, ισοδύναμα ανν $\dim V = D$. Θα δείξουμε πως αυτό δε συμβαίνει, βρίσκοντας ένα ανοιχτό σύνολο στον $\mathbb{C}^D$ στο οποίο $\det M \neq 0$.

  Θέτουμε $f_0 = 1, \ f_i = x_i^{d_i}$ για $i = 1, \ldots, n$. Η επιλογή αυτή δεν είναι παρά ένα σημείο $\underset{\sim}{c}$ στο χώρο των συντελεστών. Είναι $B_i = \{1\}, \ i = 0, \ldots, n$, άρα ο πίνακας Macaulay είναι $M = I_{n+1}$(μοναδιαίος διάστασης $n+1$). Έτσι $\det M = 1 \neq 0$. Μένει να βρούμε μια ανοικτή περιοχή του σημείου $\underset{\sim}{c} \in \mathbb{C}^D$ των συντελεστών όπου η ορίζουσα δεν είναι μηδενική. Διαταράσσουμε τους μηδενικούς συντελεστές των πολυωνύμων κατά αρκούντως μικρό $\varepsilon > 0$. Τότε παίρνουμε έναν πίνακα με μονάδες στη διαγώνιο και ε αλλού. Η ορίζουσα είναι $\det M = 1 + O(\varepsilon) \cong 1 \neq 0$. Άρα στην ανοικτή μπάλα με κέντρο $\underset{\sim}{c}$ και ακτίνα ε η ορίζουσα δεν είναι μηδενική.

Λήμμα 5.4. *Στη γενική περίπτωση, κάθε κύρια υπο-ορίζουσα του πίνακα M είναι μη μηδενική.*

Απόδειξη. Όμοια με πριν, λαμβάνοντας $f_0 = 1, \ f_i = x_i^{d_i}$ για $i = 1, \ldots, n$. □

Στην κατασκευή Macaulay, βλέπουμε ότι $B_0 = \{\underset{\sim}{x}^{\alpha} \ : \ 0 \leq \alpha_i \leq d_i - 1\}$. Έτσι, $|B_0| = \prod_{i=1}^{n} d_i = \deg_{f_0} R$. Η επιλογή αυτή είναι βέλτιστη, σύμφωνα με το *Πόρισμα (5.3)*. Ας συμβολίσουμε M_j τον πίνακα Macaulay που προκύπτει αν θελήσουμε να να επιλέξουμε με βέλτιστο τρόπο το σύνολο B_j, όπως έγινε παραπάνω με το

B_0. Στην περίπτωση των γραμμικών πολυωνύμων παρατηρήστε ότι για κάθε j έχουμε $|B_j| = 1$, άρα οι M_j προκύπτουν από αντιμεταθέσεις γραμμών του M_0 και συμπίπτουν μέχρι προσήμου. Στη γενική περίπτωση αυτό δεν ισχύει.

Θεώρημα 5.5. *Ισχύει* $R = \mathit{ΜΚΔ}(\det M_0, \det M_1, \ldots, \det M_n)$.

Απόδειξη. Είναι $|B_0| = \prod_{i=1}^{n} d_i = \deg_{f_0} R$, άρα $\deg_{f_0}[\det M_0] = \deg_{f_0} R$.

Επίσης, $R \big| \det M_0 \Rightarrow \forall i,\ \deg_{f_i} R \leq \deg_{f_i}[\det M_0]$.

Γενικότερα, $R \big| \det M_j$ και $|B_j| = \prod_{i=0, i\neq j}^{n} d_i = \deg_{f_j} R$, δηλαδή είναι

$$\deg_{f_j} R = \deg_{f_j}[\det M_j] \quad \text{και} \quad \forall i,\ \deg_{f_i} R \leq \deg_{f_i}[\det M_j],\ j = 0, 1, \ldots, n$$

Άρα $\deg_{f_i}[\text{ΜΚΔ}(\det M_0, \det M_1, \ldots, \det M_n)] = \deg_{f_i} R$, όμως $R \big| \text{ΜΚΔ}(\det M_0, \det M_1, \ldots, \det M_n)$ και η ισότητα έπεται. □

Επίλυση συστήματος με χρήση της απαλοίφουσας

Σε αυτό το μάθημα θα δούμε πως μπορούμε να λύσουμε το καλώς προσδιορισμένο σύστημα n πολυωνύμων με n μεταβλητές με χρήση του πίνακα Macaulay. Για να εφαρμόσουμε τη θεωρία της απαλοίφουσας πρέπει να μετατρέψουμε το σύστημα σε υπερπροσδιορισμένο. Αυτό γίνεται με δυο τρόπους:

- Προσθέτουμε ένα ακόμη πολυώνυμο(γραμμική μορφή), με συμβολικούς συντελεστές: $f_0 = u_0 + u_1x_1 + \cdots + u_nx_n$.

  Προσθέτουμε μια γραμμική εξίσωση $p_0 = x_1u_1 + \cdots + x_nu_n + u_0$ όπου τα $u_1, \ldots, u_n$ είναι τυχαίες σταθερές (ή παράμετροι) και το u_0 είναι μια παράμετρος στο σώμα των συντελεστών, άρα τα στοιχεία του πίνακα της απαλοίφουσας είναι σταθερές και το u_0 (ή και τα $u_1, \ldots, u_n$). Το πολυώνυμο p_0 λέγεται u-πολυώνυμο και η αντίστοιχη απαλοίφουσα λέγεται u-απαλοίφουσα. Άρα $M(u_0) = M_0 + M_1u_0$ όπου M_0, M_1 περιέχουν μόνο σταθερές.

  Πλεονέκτημα: διαχωρίζει τις πολλαπλές ρίζες ως προς κάποιο x_i του αρχικού συστήματος εφόσον $p_0(\alpha) \neq p_0(\alpha')$, για διαφορετικές ρίζες $\alpha \neq \alpha'$. Μειονέκτημα: αυξάνει τον αριθμό των εξισώσεων.

- Θεωρούμε μια από τις μεταβλητές του συστήματος, πχ τη x_1, ως παράμετρο των συντελεστών, δηλαδή βλέπουμε τα πολυώνυμα ως πολυώνυμα $n-1$ μεταβλητών, $f_i \in (\mathbb{F}[x_1])[x_2, \ldots, x_n]$.

  Κρύβουμε τη μεταβλητή x_n στο πεδίο των συντελεστών ώστε τα n πολυώνυμα θεωρούνται μέλη του δακτυλίου $(\mathbb{C}[x_n])[x_1, \ldots, x_{n-1}]$ δηλ. σε $n-1$ μεταβλητές. Τα στοιχεία του πίνακα είναι σταθερές ή πολυώνυμα του x_n βαθμού μέχρι d, οπότε ο πίνακας γράφεται $M(x_n) = M_0 + M_1x_n + \cdots + M_dx_n^d$ όπου οι πίνακες M_i περιέχουν μόνο σταθερά στοιχεία. Προφανώς αντί για το x_n μπορούμε να επιλέγουμε κάποια άλλη μεταβλητή.

Με τις παραπάνω ιδέες προκύπτουν διαφορετικές μέθοδοι επίλυσης ενός συστήματος με χρήση της απαλοίφουσας.

6.1 Ανάλυση σε γραμμμικούς παράγοντες

Θεωρούμε $f_0 = u_0 + u_1x_1 + \cdots + u_nx_n$. Η απαλοίφουσα του υπερπροσδιορισμένου συστήματος είναι πολυώνυμο με μεταβλητές τα u_i. Από τον τύπο του Poisson έχουμε

$$R(u_0, \ldots, u_n) = C \prod_{\underline{\alpha} \in A} f_0(\underline{\alpha})$$

όπου A το σύνολο των ριζών του συστήματος $f_1 = \cdots = f_n = 0$ και C μια σταθερά που εξαρτάται από τους συντελεστές των $f_1, \ldots, f_n$.

Έτσι αν παραγοντοποιήσουμε την $R(u_0, \ldots, u_n)$ σε γραμμικούς παράγοντες, θα εμφανιστούν οι (προβολικές) λύσεις του συστήματος σαν συντελεστές των u_i:

$$R = C \prod_{\underline{\alpha} \in A} (u_0\alpha_0 + u_1\alpha_1 + \cdots + u_n\alpha_n)$$

Αν θέσουμε πχ $f_0 = u_0 + u_ix_i$, η παραγοντοποίηση σαν γινόμενο $\prod(u_i - \alpha_i)$ θα μας δώσει τις τιμές της $i-$συντεταγμένης των ριζών του συστήματος.

Όμως η παραγοντοποίηση είναι μια υπολογιστικά δύσκολη διαδικασία. Ακόμη και αν με παραγοντοποίηση σε μια μεταβλητή, τη u_i, βρούμε τα σύνολα $\{\alpha_i\}$ των $i-$οστών συντεταγμένων των ριζών, έχουμε να λύσουμε ένα πρόβλημα ταιριάσματος για να φτάσουμε στις λύσεις $(\alpha_1, \ldots, \alpha_n)$ πράγμα το οποίο είναι εξίσου υπολογιστικά δύσκολο.

Είδαμε ότι μπορούμε να υπολογίσουμε μια συντεταγμένη κάθε πραγματικής ρίζας λύνοντας ένα πολυώνυμο σε μια μεταβλητή. Ο υπολογισμός των υπόλοιπων συντεταγμένων με « ανύψωση » προτάθηκε από τον Canny [**?**] και είναι σήμερα γνωστή ως μέθοδος του Πρωτογενούς στοιχείου (primitive element) ή ως Ρητή Μονοδιάστατη Αναπαράσταση (Rational Univariate Representation), βλ. και [Rou99].

6.2 Αναγωγή σε πρόβλημα ιδιοδιανυσμάτων

Μπορούμε να χρησιμοποιήσουμε χρησιμοποιήσουμε τη γραμμική μορφή f_0 πιο αποδοτικά.

$$\left[\begin{array}{c|c} M_{11} & M_{12} \\ \hline M_{21} & M_{22} \end{array}\right] \left[\begin{array}{c} \underset{\sim}{v} \\ \hline \underset{\sim}{w} \end{array}\right] = \left[\begin{array}{c} f_0(\underset{\sim}{\alpha})\underset{\sim}{v} \\ \hline \underset{\sim}{0} \end{array}\right]$$

Για ένα διάνυσμα $\left[\begin{array}{cc} \underset{\sim}{v} & \underset{\sim}{w} \end{array}\right]^t$ στον πυρήνα του M, το οποίο είναι τα μονώνυμα των στηλών του M υπολογισμένα στις συντεταγμένες μιας λύσης του συστήματος $\underset{\sim}{\alpha}$, θα έχουμε:

$$\left[\begin{array}{c|c} M_{11} & M_{12} \\ \hline M_{21} & M_{22} \end{array}\right] \left[\begin{array}{c} \underset{\sim}{v} \\ \hline \underset{\sim}{w} \end{array}\right] = \left[\begin{array}{c} f_0(\underset{\sim}{\alpha})\underset{\sim}{v} \\ \hline \underset{\sim}{0} \end{array}\right]$$

όπου το f_0 εξαρτάται από το u. Αν πολλαπλασιάσουμε και τα δυο μέλη από αριστερά με τον πίνακα $\left[\begin{array}{cc} I_3 & -M_{12}M_{22}^{-1} \\ \mathbf{0} & I_3 \end{array}\right]$ παίρνουμε

$$\left[\begin{array}{c|c} M_{11} - M_{12}M_{22}^{-1}M_{21} & \mathbf{0} \\ \hline M_{21} & M_{22} \end{array}\right] \left[\begin{array}{c} \underset{\sim}{v} \\ \hline \underset{\sim}{w} \end{array}\right] = \left[\begin{array}{c} f_0(\underset{\sim}{\alpha})\underset{\sim}{v} \\ \hline \underset{\sim}{0} \end{array}\right]$$

δηλαδή

$$(M_{11} - M_{12}M_{22}^{-1}M_{21})\underset{\sim}{v} = f_0(\underset{\sim}{\alpha})\underset{\sim}{v}$$

Συμπεραίνουμε ότι το $f_0(\underset{\sim}{\alpha})$ είναι ιδιοτιμή του $M_{11} - M_{12}M_{22}^{-1}M_{21}$ και έχει ιδιοδιάνυσμα με συντεταγμένες τις τιμές των πρώτων 2 μονωνύμων του M σε μια λύση του συστήματος. Άρα το πρόβλημα εύρεσης των λύσεων ανάγεται στον υπολογισμό των ιδιοδιανυσμάτων αυτού του πίνακα,

Ας θυμηθούμε ότι

$$\left[\begin{array}{cc} M_{11} & M_{12} \\ M_{21} & M_{22} \end{array}\right] \left[\begin{array}{c} \underset{\sim}{v_j} \\ \underset{\sim}{w_i} \end{array}\right] = \left[\begin{array}{c} M_{11}\underset{\sim}{v_j} + M_{12}\underset{\sim}{w_i} \\ M_{21}\underset{\sim}{v_j} + M_{22}\underset{\sim}{w_i} \end{array}\right] = \left[\begin{array}{c} f_0(\underset{\sim}{\alpha})\underset{\sim}{v} \\ \underset{\sim}{0} \end{array}\right]$$

όπου $\underset{\sim}{v_i}$, $i = 1, 2$ τα ιδιοδιανύσματα που βρήκαμε και $\underset{\sim}{w_i}$ το διάνυσμα που περιέχει τα επόμενα 4 μονώνυμα των στηλών του M υπολογισμένα στις συντεταγμένες των λύσεων $\underset{\sim}{\alpha}$ για $i = 1$ και $\underset{\sim}{\beta}$ για $i = 2$. Άρα

$$M_{21}\underset{\sim}{v_i} + M_{22}\underset{\sim}{w_i} = \underset{\sim}{0} \Rightarrow M_{22}\underset{\sim}{w_i} = -M_{21}\underset{\sim}{v_i}$$

Οι συντεταγμένες α_1, β_1 των ριζών μπορούν να βρεθούν από τα αντίστοιχα διανύσματα $\underset{\sim}{w_i}$, δηλαδή ο υπολογισμός τους ανάγεται στην επίλυση του παραπάνω γραμμικού συστήματος.

$$\underset{\sim}{w_i} = -M_{22}^{-1}M_{21}\underset{\sim}{v_i}$$

6.3 Μέθοδος απόκρυψης μεταβλητής

Για να αναχθούμε σε ένα υπερπροσδιορισμένο σύστημα, θεωρούμε τα πολυώνυμα ως $f_1, \ldots, f_n \in (\mathbb{F}[x_1])[x_2, \ldots, x_n]$, δηλαδή *κρύβουμε* τη μεταβλητή x_1 στο σώμα των συντελεστών. Υπολογίζουμε τον πίνακα Macaulay, για τον οποίο ισχύει $\det M(x_1) = R(x_1) \cdot P(x_1)$, όπου $P(x_1)$ ο παρασιτικός παράγοντας. Αν ο βαθμός του συστήματος ως προς τη x_1 είναι d, ο πίνακας αναλύεται ως:

$$M(x_1) = M_0 + x_1 M_1 + \cdots + x_1^{d-1} M_{d-1} - x_1^d M_d$$

Περίπτωση 1: Ο πίνακας M_d είναι αντιστρέψιμος.

$$M_d^{-1} M(x_1) = M_d^{-1} M_0 + x_1 M_d^{-1} M_1 + \cdots + x_1^{d-1} M_d^{-1} M_{d-1} - x_1^d I$$

$$C = \begin{bmatrix} 0 & I & \cdots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & I \\ M_d^{-1} M_0 & M_d^{-1} M_1 & \ddots & M_d^{-1} M_{d-1} \end{bmatrix}$$

M_d αντιστρέψιμος: Εάν $d = 1, M(x) = 0$ ισοδυναμεί με $\det(-M_1^{-1} M_0 - Ix) = 0$ οπότε οι ρίζες του ξ ανήκουν στο σύνολο των ιδιοτιμών του $-M_1^{-1} M_0$ διάστασης m. Για μεγαλύτερα d, έχουμε $M(x) = M_d x^d + \cdots + M_1 x + M_0$. Η υπόθεση $|M_d| \neq 0$ οδηγεί στο:

$$\det M(x) = \det M_d \det(I_N x^d + \cdots + M_d^{-1} M_1 x + M_d^{-1} M_0)$$

και ο $M(x)$ είναι μη-αντιστρέψιμος ανν το x ισούται με τις ιδιοτιμές του συντροφικού πίνακα (companion matrix) C, διάστασης dm. Το ίδιο πρόβλημα γράφεται $\det(C_0 + C_1 x) = 0$ με $\det C_1 \neq 0$, δηλ. $\det(-C_1^{-1} C_0 - Ix) = 0$. Τα ιδιοδιανύσματα v_α του αρχικού πίνακα αντιστοιχούν στα ιδιοδιανύσματα του C ως εξής, όπου β μια ιδιοτιμή του αρχικού πίνακα:

$$M(\beta) v_\alpha = 0 \Leftrightarrow \left(\begin{bmatrix} 0 & I_N & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & I_N \\ -M_d^{-1} M_0 & \cdots & \cdots & -M_d^{-1} M_{d-1} \end{bmatrix} - \beta I_{Nd} \right) \begin{bmatrix} v_\alpha \\ \beta v_\alpha \\ \vdots \\ \beta^{d-1} v_\alpha \end{bmatrix} = 0.$$

Περίπτωση 2: Ο πίνακας M_d είναι ιδιάζων.

Οι συντεταγμένες των ριζών του συστήματος μπορούν να βρεθούν σαν λόγοι των συντεταγμένων ενός ιδιοδιανύσματος $\underline{v}$ στο μηδενοχώρο του $M(x_1) = M_0 - x_1 M_1$.

$$\left(\begin{bmatrix} \mathbf{0} & I_3 \\ S_0 & \mathbf{0} \end{bmatrix} - y \begin{bmatrix} I_3 & \mathbf{0} \\ -S_1 & -S_2 \end{bmatrix} \right) \begin{bmatrix} \underline{u} \\ y\underline{u} \end{bmatrix} = (A_0 - yA_1)\underline{v} = \underline{0}$$

$\det M_d = 0$: τα x στα οποία μηδενίζεται η $\det(M_0 + M_1 x) = 0$, για $d = 1$, λέγονται γενικευμένες ιδιοτιμές και υπολογίζονται αριθμητικά με κόστος μια κυβική συνάρτηση της διάστασης, αλλά με ψηλότερη σταθερά και χειρότερη αριθμητική ακρίβεια απ' ό,τι οι απλές ιδιοτιμές. Για μεγαλύτερα d, ορίζονται πίνακες A_0, A_1 διάστασης dm, τέτοιοι ώστε το ίδιο πρόβλημα γενικευμένων ιδιοτιμών γράφεται $\det(A_0 + A_1 x) = 0$, με $\det A_1 = 0$. Για μια ιδιοτιμή β και το αντίστοιχο ιδιοδιάνυσμα v_α έχουμε:

$$M(\beta) v_\alpha = 0 \Leftrightarrow \left(\begin{bmatrix} 0 & I_N & & \\ & & \ddots & \\ & & & I_N \\ -M_0 & -M_1 & \cdots & -M_{d-1} \end{bmatrix} - \beta \begin{bmatrix} I_N & & & \\ & \ddots & & \\ & & I_N & \\ & & & M_d \end{bmatrix} \right) \begin{bmatrix} v_\alpha \\ \beta v_\alpha \\ \vdots \\ \beta^{d-1} v_\alpha \end{bmatrix} = 0.$$

Παράδειγμα 6.1. Παρουσιάζουμε ένα παράδειγμα όπου κρύβουμε τη μεταβλητή x για δυο δεδομένα πολυώνυμα σε δυο αγνώστους: $p_1 = y(x+1)+x^2+2x-1, p_2 = -y^2+2y+x^2+3x-1 \in (\mathbb{Z}[x])[y]$. Ο πίνακας Sylvester δίνεται παρακάτω κι έχει δεξιό πυρήνα της μορφής $(1, y, y^2)$:

$$S = \begin{bmatrix} x^2+2x-1 & x+1 & 0 \\ 0 & x^2+2x-1 & x+1 \\ x^2+3x-1 & 2 & -1 \end{bmatrix} \Rightarrow \det S = -x^3-2x^2+3x \Rightarrow x \in \{0,-3,1\}.$$

Για κάθε λύση του x ο πυρήνας του αντίστοιχου πίνακα δίνει $y = 1, 1, -1$.

Εφόσον το φράγμα Bézout είναι 4, αυτό σημαίνει πως υπάρχει προβολική ρίζα του συστήματος που βρίσκεται στο προβολικό άπειρο $\mathbb{P}^2 \setminus \mathbb{C}^2$, δηλ. για $z = 0$ όπου z η μεταβλητή ομογενοποίησης. Με άλλα λόγια, ψάχνουμε τις ρίζες όταν μηδενίζονται οι μεγιστοβάθμιοι όροι κάθε εξίσωσης, $xy+x^2 = -y^2+x^2 = 0$. Αν $x = 0 \Rightarrow y = 0$ που δεν αποτελεί δεκτή λύση. Αν $x \neq 0 \Rightarrow y = -x$ και οι λύσεις στο άπειρο είναι $(x : -x : 0)$, δηλ. ένα μονοδιάστατο σύνολο.

Με βάση τη θεωρία της απαλοίφουσας, μας ενδιαφέρουν οι τιμές της παραμέτρου ή της κρυμμένης μεταβλητής για τις οποίες μηδενίζεται η ορίζουσα του πίνακα της απαλοίφουσας. Και οι 2 μέθοδοι ενοποιούνται και ανάγουν την επίλυση του αρχικού συστήματος στην επίλυση του γραμμικού συστήματος $M(x) = M_0+M_1x+\cdots+M_dx^d$, ($d = 1$ στην πρώτη περίπτωση), όπου έστω m η διάστασή του. Διαπιστώνουμε εδώ το πλεονέκτημα της μεθόδου της απαλοίφουσας για την επίλυση συστημάτων.

Στα παρακάτω, έστω I ο μοναδιαίος πίνακας της διάστασης που απαιτείται. Οι τιμές του x που μηδενίζουν την ορίζουσα $\det M(x)$ είναι οι τιμές του u_0 ή του x_n στις ρίζες του αρχικού συστήματος.

Πώς βρίσκουμε τώρα τα υπόλοιπα στοιχεία των διανυσμάτων που αποτελούν ρίζες του αρχικού συστήματος; Χρησιμοποιούμε την ιδιότητα του πίνακα της απαλοίφουσας σχετικά με τον πολλαπλασιασμό επί διάνυσμα από δεξιά, που μας οδηγεί στον υπολογισμό του πυρήνα του $m \times m$ πίνακα $M(x)$. Ενοποιούμε τις περιπτώσεις για κάθε d γράφοντας το πρόβλημα ισοδύναμα ως τον υπολογισμό των διανυσμάτων v τέτοια ώστε $(C_0+C_1x)v = 0$, όπου διάσταση πινάκων $= md$.

Έστω v στον πυρήνα δηλ. $(-C_1^{-1}C_0 - Ix)v = 0$ εφόσον ο C_1 είναι αντιστρέψιμος, οπότε αρκεί ο υπολογισμός των ιδιοδιανυσμάτων του $-C_1^{-1}C_0$, διάστασης md. Αν $\det C_1 = 0$ τότε υπολογίζουμε τα γενικευμένα ιδιοδιανύσματα $(C_0 + C_1x)v = 0$.

Τέλος, τα στοιχεία του v είναι τύπου α^b για μονώνυμο b, άρα μπορούμε να υπολογίσουμε τις συντεταγμένες της ρίζας α με ορισμένες διαιρέσεις. Π.χ.: για $2-$διάστατο α, παίρνουμε δύο στοιχεία με εκθέτες $(1, 2)$ και $(1, 3)$, άρα το πηλίκο δίνει την 2η συντεταγμένη.

Τα διανύσματα α που υπολογίζουμε από τα (γενικευμένα) ιδιοδιανύσματα είναι συνήθως περισσότερα από τις ρίζες του αρχικού συστήματος, διότι ο πίνακας της απαλοίφουσας δεν έχει συνήθως την βέλτιστη (δηλ. ελάχιστη) διάσταση. Επομένως υπολογίζουμε τις τιμές των αρχικών πολυωνύμων στα α που έχουμε υπολογίσει και απορρίπτουμε αυτά στα οποία τα πολυώνυμα δε μηδενίζονται.

6.4 Πίνακες πολλαπλασιασμού

Ο πίνακας της απαλοίφουσας δίνει περαιτέρω πληροφορία. Μια σημαντική πληροφορία αφορά στον πίνακα πολλαπλασιασμού (multiplication table) στον δακτύλιο πηλίκο $K[x]/I$, όπου $K[x]$ ο αρχικός δακτύλιος των πολυωνύμων και I το ιδεώδες που ορίζουν τα $f_1, \ldots, f_n$.

Ας περιοριστούμε, προς το παρόν, στην περίπτωση που η διάσταση του αλγεβρικού συνόλου $V(I)$ είναι μηδέν και το I είναι ριζικό, δηλ. $I = \sqrt{I}$. Ισοδύναμα, το σύστημα $f_1 = \cdots = f_n = 0$ έχει μεμονωμένες ρίζες και απλές. Ο δακτύλιος πηλίκο $K[x]/I$ γράφεται και $K[x] \bmod I$ και περιέχει τις κλάσεις ισοδυναμίας των υπολοίπων κατά την διαίρεση με το I. Από την αντιμεταθετική άλγεβρα γνωρίζουμε πως, όταν $\dim V(I) = 0$, το $K[x]/I$ είναι διανυσματικός χώρος πάνω στο K.

Θεώρημα 6.1. *Υποθέτουμε πως $I = \sqrt{I}$, $\dim V(I) = 0$. Έστω $f_0 \in K[x]$ τ.ώ. να έχει διαφορετικές τιμές στις ρίζες του συστήματος $f_1 = \cdots = f_n = 0$. Έστω $B_0 \in \mathbb{N}^n$ το σύνολο μονωνύμων που πολλαπλασιάζουν το f_0 στην κατασκευή Macaulay. Τότε το B_0 είναι βάση του διανυσματικού χώρου $K[x]/I$ πάνω στο K.*

Απόδειξη. Έστω $m = \prod_{i=1}^{n} \deg(f_i)$ το φράγμα Bézout του συστήματος. Τότε $|B_0| = m$ και θέτουμε $B_0 = \{b_1, \ldots, b_m\}$.

Θα χρησιμοποιήσουμε τον πίνακα M', μεγέθους $m \times m$, που προκύπτει από το συμπλήρωμα Schur στον πίνακα Macaulay, όπως είδαμε παραπάνω. Θυμηθείτε πως οι ιδιοτιμές του M' είναι της μορφής $f_0(\alpha)$, όπου $\alpha \in \mathbb{C}^n$ μια ρίζα του καλώς ορισμένου συστήματος.

Εξ υποθέσεως οι ιδιοτιμές $f_0(\alpha)$ είναι διαφορετικές, άρα υπάρχουν m ιδιοδιανύσματα γραμμικώς ανεξάρτητα της μορφής $[\alpha^{b_1}, \ldots, \alpha^{b_m}]$. Δεδομένου ότι το συνολικό πλήθος ιδιοδιανυσμάτων είναι m, έπεται πως όλα τα ιδιοδιανύσματα είναι της μορφής $[\alpha^{b_1}, \ldots, \alpha^{b_m}]$.

Αν το B_0 δεν είναι βάση του διανυσματικού χώρου, τότε υπάρχουν $k_1, \ldots, k_m \in K$ τέτοια ώστε $\sum_{i=1}^{m} k_i x^{b_i} = 0 \pmod{I}$, άρα για κάθε ρίζα α έπεται πως $\sum_{i=1}^{m} k_i \alpha^{b_i} = 0$. Θεωρήστε τον πίνακα με στήλες τα ιδιοδιανύσματα του M', ο οποίος είναι αντιστρέψιμος λόγω ανεξαρτησίας των στηλών του. Η παραπάνω σχέση σημαίνει πως αν πολλαπλασιαστεί κάθε γραμμή με k_i, το άθροισμά τους μηδενίζεται, δηλ. ο πίνακας δεν είναι αντιστρέψιμος, πράγμα άτοπο. □

Άσκηση 6.2. Μελετήστε τον πίνακα Macaulay στην περίπτωση της u-απαλοίφουσας. Αποδείξτε πως με απαλοιφή κατά Gauss προκύπτει τετράγωνος πίνακας διάστασης ίσης με το φράγμα Bézout του αρχικού καλώς προσδιορισμένου συστήματος, ο οποίος εκφράζει τον πολλαπλασιασμό πολυωνύμου mod το ιδεώδες του συστήματος.

Αλγεβρικά σύνολα και Αλγόριθμος διαίρεσης

Σε αυτήν την ενότητα θα ασχοληθούμε με πολυώνυμα πολλών μεταβλητών, και μάλιστα με συστήματα τέτοιων πολυωνύμων. Ενδιαφερόμαστε φυσικά για το σύνολο των λύσεων των συστημάτων αυτών, στο οποίο θα αναφερόμαστε και ως «αλγεβρικό σύνολο». Σημαντικό ρόλο στη μελέτη του συνόλου αυτού παίζει η διαίρεση μεταξύ τέτοιων πολυωνύμων, την οποία θα ορίσουμε παρακάτω. Τέλος, απαραίτητο στοιχείο για την κατανόησή τους είναι και η έννοια του ιδεώδους. Ο ορισμός του ιδεώδους έχει δοθεί στο *Μάθημα 1*, υπενθυμίζουμε:

Ορισμός 7.1. *Έστω R ένας δακτύλιος. Το υποσύνολο I του R καλείται ιδεώδες του R, και συμβολίζουμε $I \lhd R$ εάν ισχύουν τα ακόλουθα :*

(α') $0 \in I$

(β') $a, b \in I \Rightarrow a - b \in I$

(γ') $a \in I, x \in R \Rightarrow ax, xa \in I$

Αν ο δακτύλιος R έχει μοναδιαίο στοιχείο 1_R, τότε η συνθήκη *(β')* μπορεί να αντικατασταθεί από την $a, b \in I \Rightarrow a + b \in I$. Επίσης η συνθήκη *(α')* μπορεί να αντικατασταθεί με τη συνθήκη το I να είναι μη κενό, επειδή τότε από την *(γ')* έχουμε $0 \in I$.

7.1 Αλγεβρικά σύνολα(Varieties)

Μας ενδιαφέρει το σύνολο

$$V(f_1, f_2, ..., f_\mu) := \{(\xi_1, \xi_2, ..., \xi_n) \in \mathbb{F}^n \mid f_i(\xi_1, \xi_2, ..., \xi_n) = 0, \forall i = 1, 2, ..., \mu\}.$$

δηλαδή το σύνολο των λύσεων του συστήματος $\{f_i = 0, \quad i = 1, \ldots, \mu\}$. Έτσι ορίζουμε:

Ορισμός 7.2. *Το σύνολο $V(f_1, f_2, ..., f_\mu)$, το ονομάζουμε* ***αλγεβρικό σύνολο ή αλγεβρική πολλαπλότητα (algebraic variety)*** *αντίστοιχη στο σύνολο των πολυωνύμων $\{f_1, f_2, ..., f_\mu\}$.*

Γενικεύοντας τον παραπάνω ορισμό, με την έννοια ότι βλέπουμε κι ένα ιδεώδες του $\mathbb{F}[x_1, \ldots, x_n]$ ως ένα σύστημα (άπειρων) πολυωνύμων, ορίζουμε

Ορισμός 7.3. *Αν $I \lhd \mathbb{F}[x_1, x_2, ..., x_n]$, τότε το σύνολο*

$$V(I) = \{(\xi_1, \xi_2, ..., \xi_n) \in \mathbb{F}^n \mid f_i(\xi_1, \xi_2, ..., \xi_n) = 0, \forall f_i \in I\}$$

θα λέγεται αλγεβρικό υποσύνολο του $\mathbb{F}^n$.

Π.χ. τα αλγεβρικά υποσύνολα του $\mathbb{F}$ είναι τα μη κενά πεπερασμένα υποσύνολά του (διότι ένα μη-μηδενικό μή σταθερό πολυώνυμο με συντελεστές από το $\mathbb{F}$ έχει πεπερασμένες ρίζες), το $\mathbb{F}$ ως σύνολο ριζών του μηδενικού πολυωνύμου και το κενό σύνολο ως σύνολο ριζών ενός σταθερού μη-μηδενικού πολυωνύμου.

Μερικά αλγεβρικά υποσύνολα του $\mathbb{F}^n$ είναι το κενό σύνολο (ως σύνολο λύσεων ενός γραμμικού συστήματος, το οποίο είναι αδύνατο), οι υπόχωροι (ως σύνολο λύσεων ενός ομογενούς γραμμικού συστήματος με ν αγνώστους), τα σύνολα της μορφής $\{(\omega_1, \omega_2, \cdots, \omega_n) + A\}$ όπου A ένας υπόχωρος του $\mathbb{F}^n$ και $(\omega_1, \omega_2, \cdots, \omega_n)$ μία μερική λύση του συστήματος. Θα δούμε πως αυτά δεν είναι τα μόνα αλγεβρικά υποσύνολα του $\mathbb{F}^n$.

Διάσταση του αλγεβρικού συνόλου καλείται η γεωμετρική διάστασή του, δηλαδή για μη κενά σύνολα είναι ένας ακέραιος μεταξύ 0 (πεπερασμένο σύνολο σημείων) έως n (αν και μόνο αν αλγεβρικό σύνολο ισούται με το $\mathbb{C}^n$). Π.χ. η διάσταση ενός πεπερασμένου συνόλου ευθειών(επιπέδων) είναι 1, η διάσταση υπερεπιπέδου στο n-διάστατο χώρο είναι$n-1$. Θα συμβολίζουμε τη διάσταση του V ως $\dim V$.

Πρόταση 7.4. *Αν* $f_1(x)=\lambda_2(x)f_2(x)+\lambda_3(x)f_3(x)+\cdots+\lambda_\mu(x)f_\mu(x)$, *τότε* $V(f_1,f_2,...,f_\mu)=V(f_2,f_3,...,f_\mu)$.

Απόδειξη. Έστω $(\xi_1,\xi_2,...,\xi_n)\in V(f_1,f_2,...,f_\mu)\Rightarrow(\xi_1,\xi_2,...,\xi_n)\in V(f_2,f_3,...,f_\mu)$ και αντίστροφα. □

Πρόταση 7.5. *Έστω* I *το ιδεώδες του* $\mathbb{F}[x_1,x_2,...,x_n]$ *που παράγεται*[1] *από τα* $f_1,f_2,...,f_\mu$. *Τότε*

$$V(f_1,f_2,...,f_\mu)=V(I)$$

Απόδειξη. Έστω $(\xi_1,\xi_2,...,\xi_n)\in V(f_1,f_2,...,f_\mu)$ και $g(x_1,x_2,...,x_n)\in I$. Όπως είναι γνωστό $g=\lambda_1f_1+\lambda_2f_2+\cdots+\lambda_\mu f_\mu$, με $\lambda_i\in\mathbb{F}[x_1,x_2,...,x_n]$. Έτσι $(\xi_1,\xi_2,...,\xi_n)\in V(g,f_1,f_2,...,f_\mu)$ ή $V(f_1,f_2,...,f_\mu)\subseteq V(I)$.

Αντίστροφα, αν $(\xi_1,\xi_2,...,\xi_n)\in V(I)$ προφανώς μηδενίζονται τα f_i ως στοιχεία του ιδεώδους, άρα $V(I)\subseteq V(f_1,f_2,...,f_\mu)$. Τελικά $V(f_1,f_2,...,f_\mu)=V(I)$. □

Σύμφωνα με την παραπάνω πρόταση, η μελέτη του πολυωνυμικού συστήματος ανάγεται στη μελέτη του ιδεώδους που παράγεται από τα πολυώνυμα του συστήματος. Αυτό που θα κάνουμε είναι να περιγράψουμε το ιδεώδες αυτό όχι χρησιμοποιώντας τα αρχικά πολυώνυμα, αλλά βρίσκοντας μια βάση του ιδεώδους η οποία θα μας επιτρέψει να προσδιορίσουμε πιο εύκολα το σύνολο λύσεων του συστήματος.

Πρόταση 7.6. *Έστω* V_1 *και* V_2 *δυο αλγεβρικά υποσύνολα του* $\mathbb{F}^n$. *Τότε ισχύουν :*

(i) $V_1\cup V_2$ *είναι αλγεβρικό σύνολο.*

(ii) $V_1\cap V_2$ *είναι αλγεβρικό σύνολο.*

Απόδειξη. Έστω $V_1=V(f_1,f_2,...,f_\mu)$ και $V_2=V(g_1,g_2,...,g_\lambda)$.
(**i**)Θεωρούμε το σύνολο των πολυωνύμων $C=\{f_1g_1,...,f_1g_\lambda,f_2g_1,...,f_2g_\lambda,...,f_\mu g_1,...,f_\mu g_\lambda\}$.

Αν $(\xi_1,\xi_2,...,\xi_n)\in V(C)$ τότε $(\xi_1,\xi_2,...,\xi_n)\in V_1$ ή $(\xi_1,\xi_2,...,\xi_n)\in V_2$ και αντίστροφα, άρα $V(C)=V_1\cup V_2$.
(**ii**)Είναι εύκολο να δει κανείς ότι $V(f_1,f_2,...,f_\mu,g_1,...,g_\lambda)=V_1\cap V_2$. □

7.2 Διατάξεις μονωνύμων

Για τη διαίρεση πολυωνύμων με n μεταβλητές θα χρειαστεί να ορίσουμε έναν μεγιστοβάθμιο όρο σε κάθε πολυώνυμο. Έτσι χρειαζόμαστε κάποια διάταξη στα μονωνύμά του. Η πιο απλή διάταξη είναι η «λεξικογραφική».

Ορισμός 7.7. *Έστω ο δακτύλιος* $\mathbb{F}[x_1,x_2,...,x_n]$. *Μονώνυμο καλείται κάθε έκφραση της μορφής* ${x_1}^{\alpha_1}{x_2}^{\alpha_2}\cdots{x_n}^{\alpha_n}$, *όπου* $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{Z}_{\geq 0}$. *Αν* $\alpha_i=0$ *τότε ορίζουμε* ${x_i}^{\alpha_i}:=1$.

Κάθε μονώνυμο ${x_1}^{\alpha_1}{x_2}^{\alpha_2}\cdots{x_n}^{\alpha_n}$ καθορίζεται πλήρως από το διάνυσμα $\alpha:=(\alpha_1,\alpha_2,\ldots,\alpha_n)$. Για συντομία θα συμβολίζουμε και

$$\underset{\sim}{x}^{\alpha}:={x_1}^{\alpha_1}{x_2}^{\alpha_2}\cdots{x_n}^{\alpha_n}$$

Πολυώνυμο του $\mathbb{F}[x_1,x_2,...,x_n]$ καλούμε κάθε πεπερασμένο γραμμικό συνδυασμό μονωνύμων του ίδιου δακτυλίου. Έτσι κάθε έκφραση της μορφής $\xi\cdot\underset{\sim}{x}^{\alpha}$, με $\xi\in\mathbb{F}$ και $\alpha\in\mathbb{Z}^n_{\geq 0}$, καλείται μονώνυμο με συντελεστή ξ ή, εφόσον εμφανίζεται σε κάποιο πολυώνυμο, όρος του πολυωνύμου.

Ορισμός 7.8. *Στο σύνολο* $\mathbb{Z}^n{}_{\geq 0}=\{(\alpha_1,\alpha_2,...,\alpha_n)|\ \alpha_i\in\{0,1,...\}\}$ *ορίζουμε τη λεξικογραφική διάταξη ως εξής:* $(\alpha_1,\alpha_2,...,\alpha_n)>(\beta_1,\beta_2,...,\beta_n)\Leftrightarrow\alpha_1>\beta_1$ *ή* $\alpha_1=\beta_1$ *&* $\alpha_2>\beta_2$ *ή* $\alpha_1=\beta_1$ *&* $\alpha_2=\beta_2$ *&* $\alpha_3>\beta_3$ *κ.ο.κ.*

[1] θα συμβολίζουμε και $I=\langle f_1,f_2,...,f_\mu\rangle$

Έτσι επιλέγοντας μια διάταξη στις μεταβλητές, π.χ. $x_1 > x_2 > \cdots > x_n$, επάγεται μια λεξικογραφική διάταξη στα μονώνυμα.

Ορισμός 7.9. *Σε κάθε πολυώνυμο $f \in \mathbb{F}[x_1, x_2, ..., x_n]$ έχουμε ένα μεγιστοβάθμιο όρο (σύμφωνα με τη λεξικογραφική διάταξη που εφαρμόζουμε) και τον συμβολίζουμε $MO(f)$.*

Ίσως χρησιμοποιήσουμε και τις συντομογραφίες $\text{ΜΣ}(f)$ και $\text{ΜΜ}(f)$ για το μεγιστοβάθμιο συντελεστή και το μεγιστοβάθμιο μονώνυμο του f αντίστοιχα, δηλαδή θα είναι $\text{ΜΟ}(f) = \text{ΜΣ}(f) \cdot \text{ΜΜ}(f)$.

7.3 Αλγόριθμος της διαίρεσης

Η πράξη της διαίρεσης στον δακτύλιο $\mathbb{F}[x_1, x_2, \cdots, x_n]$, όπου $\mathbb{F}$ είναι ένα σώμα, είναι καθοριστικής σημασίας για τα επόμενα. Υπενθυμίζουμε ότι στον δακτύλιο των πολυωνύμων μιας μεταβλητής για να γίνει η διαίρεση χρειαζόμαστε:

1) Να έχουμε ένα διαιρετέο $f(x) \in \mathbb{F}[x]$ και ένα διαιρέτη $g(x) \in \mathbb{F}[x]$ με $g(x) \neq 0$

2) Να διατάξουμε τα μονώνυμα του διαιρετέου και τα μονώνυμα του διαιρέτη χρησιμοποιώντας την φυσική διάταξη των δυνάμεων των μονωνύμων.

Μετά την εκτέλεση της διαίρεσης έχουμε

$$f(x) = g(x)\pi(x) + \upsilon(x) \quad \text{με} \quad \begin{cases} \upsilon(x) = 0 \\ \text{ή} \\ \upsilon(x) \neq 0 \text{ και } \deg(\upsilon(x)) < \deg(g(x)) \end{cases}$$

Κάτι που πρέπει να τονισθεί ιδιαίτερα εδώ είναι ότι το πηλίκο $\pi(x)$ και το υπόλοιπο $\upsilon(x)$ είναι μοναδικά. Σε όλες τις περιπτώσεις[2] αν $I = \langle f(x), g(x) \rangle$ είναι το ιδεώδες του δακτυλίου $\mathbb{F}[x]$ που παράγεται από τα δύο πολυώνυμα $f(x), g(x)$ θα έχουμε ότι $\upsilon(x) \in I$.

Θα μπορούσαμε να πούμε ότι κατά την εύρεση του υπολοίπου, η προσπάθειά μας επικεντρώνεται στην εύρεση ενός πολυωνύμου μέσα στο ιδεώδες $I = \langle f(x), g(x) \rangle$, το οποίο να έχει τον ελάχιστο βαθμό. Θυμηθείτε ότι κάθε στοιχείο $h(x) \in I$ είναι της μορφής $h(x) = \kappa(x)f(x) + \lambda(x)g(x)$ $\kappa(x), \lambda(x) \in \mathbb{F}[x]$.

Ορίζουμε τώρα μία διαδικασία διαίρεσης στον δακτύλιο $\mathbb{F}[x_1, x_2, \cdots, x_n]$ έτσι ώστε δοθέντων των πολυωνύμων $g(x_1, x_2, \cdots, x_n), f_1(x_1, x_2, \cdots, x_n), f_2(x_1, x_2, \cdots, x_n)$, $f_3(x_1, x_2, \cdots, x_n), \cdots, f_\mu(x_1, x_2, \cdots, x_n)$, κι αφού σταθεροποιήσουμε μια διάταξη στις μεταβλητές, ο αλγόριθμος να δίνει:

1. Μία έκφραση του πολυωνύμου $g(x_1, x_2, \cdots, x_n)$ ως $g(x_1, x_2, \cdots, x_n) = \pi_1(x_1, x_2, \cdots, x_n)f_1(x_1, x_2, \cdots, x_n) +$

   $\pi_2(x_1, x_2, \cdots, x_n)f_2(x_1, x_2, \cdots, x_n) + \cdots + \pi_\mu(x_1, x_2, \cdots, x_n)f_\mu(x_1, x_2, \cdots, x_n) + \upsilon(x_1, x_2, \cdots, x_n)$.

2. Το πολυώνυμο $\upsilon(x_1, x_2, \cdots, x_n)$, το οποίο θα το λέμε **υπόλοιπο** της διαίρεσης και τη διατεταγμένη μ-άδα πολυωνύμων $(\pi_1(x_1, x_2, \cdots, x_n), \pi_2(x_1, x_2, \cdots, x_n), \cdots, \pi_\mu(x_1, x_2, \cdots, x_n))$, την οποία θα λέμε **πηλίκο** της διαίρεσης.

Δίνουμε τον αλγόριθμο της διαίρεσης σε ψευδοκώδικα:

[2] Υπενθυμίζουμε εδώ από την Άλγεβρα, ότι στο μηδενικό πολυώνυμο δεν επισυνάπτουμε βαθμό και τα σταθερά μη-μηδενικά πολυώνυμα έχουν βαθμό μηδέν

Αλγόριθμος POLYDIV

▷ *Είσοδος:* Ένας διαιρετέος $\Delta \in \mathbb{F}[x_1, \ldots, x_n]$ και μια μ-άδα διαιρετών $(\delta_1, \ldots, \delta_\mu) \in \mathbb{F}[x_1, \ldots, x_n]^\mu$.
▷ *Έξοδος:* Το πηλίκο $(\pi_1, \ldots, \pi_\mu)$ και το υπόλοιπο $\upsilon \in \mathbb{F}[x_1, \ldots, x_n]$ της διαίρεσης Δ δια $(\delta_1, \ldots, \delta_\mu)$.

$\upsilon \leftarrow 0, \quad \pi_i \leftarrow 0, i = 1, \ldots, \mu$
όσο $\Delta \neq 0$
    $j \leftarrow 1$
    τέλος $\leftarrow$ λάθος
    όσο $j \leq \mu$ & τέλος=λάθος
        αν $\mathrm{MO}(\Delta) \mod \mathrm{MO}(\pi_j) = 0$
            $\pi_j \leftarrow \pi_j + \mathrm{MO}(\Delta)/\mathrm{MO}(\delta_i)$
            $\Delta \leftarrow \Delta - [\mathrm{MO}(\Delta)/\mathrm{MO}(\delta_i)] \cdot \delta_i$
            τέλος $\leftarrow$ σωστό
        αλλιώς
            $j \leftarrow j + 1$
    αν τέλος=λάθος
        $\upsilon \leftarrow \upsilon + \mathrm{MO}(\Delta)$
        $\Delta \leftarrow \Delta - \mathrm{MO}(\Delta)$
επέστρεψε $(\pi_1, \pi_2, \ldots, \pi_\mu), \upsilon$

• **Ο αλγόριθμος τερματίζει.** Αυτό αποδεικνύεται ως εξής: Κάθε μονώνυμο $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$ (χωρίς τον συντελεστή του) όπως είπαμε παραπάνω βρίσκεται σε 1-1 και επί αντιστοιχία με τις διατεταγμένες n-άδες μη αρνητικών ακεραίων. Ισχύει το παρακάτω θεώρημα:

Θεώρημα 7.10. *Έστω Α το σύνολο των διατεταγμένων n-άδων μη αρνητικών ακεραίων.Τότε*

i) Η λεξικογραφική διάταξη είναι σχέση ολικής διάταξης δηλαδή εάν $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ *και* $(\xi_1, \xi_2, \cdots, \xi_n)$ *δύο στοιχεία του Α, τότε ισχύει ένα από τα παρακάτω*

$(\lambda_1, \lambda_2, \cdots, \lambda_n) > (\xi_1, \xi_2, \cdots, \xi_n)$ *ή*

$(\xi_1, \xi_2, \cdots, \xi_n) > (\lambda_1, \lambda_2, \cdots, \lambda_n)$ *ή*

$(\lambda_1, \lambda_2, \cdots, \lambda_n) = (\xi_1, \xi_2, \cdots, \xi_n)$

ii) Κάθε μη κενό υποσύνολο του Α έχει ελάχιστο στοιχείο

Απόδειξη. i) Έστω $(\xi_1, \xi_2, \cdots, \xi_n)$ και $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ δύο στοιχεία του Α. Θεωρούμε τους μη αρνητικούς ακεραίους ξ_1 και λ_1. Αυτοί συγκρίνονται. Αν $\xi_1 > \lambda_1$ τότε $(\xi_1, \xi_2, \cdots, \xi_n) > (\lambda_1, \lambda_2, \cdots, \lambda_n)$. Αν $\xi_1 < \lambda_1$ τότε $(\xi_1, \xi_2, \cdots, \xi_n) < (\lambda_1, \lambda_2, \cdots, \lambda_n)$. Αν $\xi_1 = \lambda_1$ συνεχίζουμε ελέγχοντας αντίστοιχα τα ξ_2, λ_2. Συνεχίζουμε επίσης για τα ξ_3, λ_3 κτλ. Η διαδικασία αυτή τερματίζει το πολύ στον έλεγχο των ξ_n, λ_n

ii) Η απόδειξη της ύπαρξης ελαχίστου σε κάθε μη κενό υποσύνολο του Α στηρίζεται στην ύπαρξη ελαχίστου σε κάθε μη κενο υποσύνολο των φυσικών. □

Τώρα η απόδειξη ότι ο αλγόριθμος τερματίζει είναι ως εξής: βλέποντας τα ενδιάμεσα υπόλοιπα παρατηρούμε ότι ο μεγιστοβάθμιος όρος αυτών συνεχώς μειώνεται γνήσια.Μετά από πεπερασμένα βήματα θα φθάσει σε ένα ελάχιστο και δεν θα μπορεί να μειώνεται άλλο. Αυτό σημαίνει ότι τερματίζει.

• **Το υπόλοιπο.** Από τον αλγόριθμο της διαίρεσης έχουμε τα εξής:

1. Το υπόλοιπο της διαίρεσης είναι και αυτό ένα πολυώνυμο, δηλαδή ένα στοιχείο του ιδίου δακτυλίου. Σημειώστε πως αντίθετα με τα πολυώνυμα μιας μεταβλητής, εδώ δεν μπορούμε να εγγυηθούμε μοναδικότητα του υπολοίπου, αν αλλάξουμε τη διάταξη των διαιρετών.

2. Δεν υπάρχει μη μηδενικός όρος του υπολοίπου που να διαιρείται από τον μεγιστοβάθμιο όρο κάποιου πολυωνύμου που βρίσκεται στον διαιρέτη.

3. Αν Θεωρούμε το αποτέλεσμα της διαίρεσης $g(x_1, x_2, \cdots, x_n)$ ως $g = \pi_1 f_1 + \pi_2 f_2 + \cdots + \pi_\mu f_\mu + \upsilon$, η διαδικασία δείχνει ότι $\deg(g) \geq \deg(\pi_i f_i), \quad \forall\, i = 1, 2, \cdots \mu$.

• **Το σύστημα.** Το αποτέλεσμα του αλγορίθμου της διαίρεσης οδηγεί στην αντιμετώπιση του κυρίου προβλήματος, που διαπραγματευόμαστε. Αφήνεται ως άσκηση η παρακάτω σημαντική παρατήρηση:

Άσκηση 7.1. Τα δυο παρακάτω συστήματα έχουν το ίδιο σύνολο λύσεων:

$$(\Sigma)\left\{\begin{array}{c} g(x_1, x_2, ..., x_n) = 0 \\ f_1(x_1, x_2, ..., x_n) = 0 \\ f_2(x_1, x_2, ..., x_n) = 0 \\ \vdots \\ f_\mu(x_1, x_2, ..., x_n) = 0 \end{array}\right\} \quad , \quad (\Sigma')\left\{\begin{array}{c} \upsilon(x_1, x_2, ..., x_n) = 0 \\ f_1(x_1, x_2, ..., x_n) = 0 \\ f_2(x_1, x_2, ..., x_n) = 0 \\ \vdots \\ f_\mu(x_1, x_2, ..., x_n) = 0 \end{array}\right\}$$

όπου υ το υπόλοιπο της διαίρεσης του g δια $(f_1, \ldots, f_m)$.

Παρατηρήστε πως στην περίπτωση που $n = 1$, η παραπάνω άσκηση μας λέει ότι το σύστημα

$$(\Sigma)\left\{\begin{array}{c} f_1(x) = 0 \\ f_2(x) = 0 \\ \vdots \\ f_m(x) = 0 \end{array}\right\}$$

έχει λύσεις της ρίζες του ΜΚΔ$(f_1, \ldots, f_m)$, όπως φαίνεται από τον Ευκλείδειο αλγόριθμο εύρεσης του ΜΚΔ.

Εισαγωγή στις Βάσεις Groebner

Η σημερινή μορφή της θεωρίας των βάσεων Groebner οφείλεται στον Αυστριακό μαθηματικό Bruno Buchberger και η ονομασία που τους έδωσε είναι προς τιμήν του καθηγητή του, Wolfgang Gröbner(ο Hironaka, την ίδια περίπου εποχή, τις ονομάζει Standard bases). Εκτός από τη θεωρητική θεμελίωση, ο Buchberger ανέδειξε την αλγοριθμική όψη των βάσεων Groebner. Με την υπολογιστική ισχύ που διαθέτουμε σήμερα, αυτή η όψη είναι εξαιρετικά σημαντική, καθώς δίνει στην άλγεβρα ένα νέο πεδίο εφαρμογών στα εφαρμοσμένα μαθηματικά και την υπολογιστική επιστήμη.

Θα εισάγουμε τις βάσεις Groebner ως εργαλείο για την ανάλυση και ανάπτυξη αλγορίθμων για τη λύση του παρακάτω προβλήματος:

Να λυθεί το πολυωνυμικό σύστημα m εξισώσεων n αγνώστους(μεταβλητές):

$$(\Sigma)\left\{\begin{array}{c} f_1(x_1,x_2,...,x_n)=0 \\ f_2(x_1,x_2,...,x_n)=0 \\ \vdots \\ f_\mu(x_1,x_2,...,x_n)=0 \end{array}\right\}$$

όπου $f_i \in \mathbb{F}[x_1,x_2,...,x_n]$, και το $\mathbb{F}$ είναι σώμα.

Μερικές ειδικές περιπτώσεις του παραπάνω, στις οποίες έχουμε ικανοποιητικό αλγόριθμο για τη λύση είναι:

1. Αν το παραπάνω σύστημα είναι γραμμικό, δηλαδή αποτελείται από γραμμικά πολυώνυμα[1], τότε η Γραμμική Άλγεβρα είναι η κατάλληλη μαθηματική θεωρία για την εύρεση των λύσεών του, π.χ. με τη μέθοδο απαλοιφής του Gauss.

2. Αν το παραπάνω σύστημα έχει μόνο μία μεταβλητή, δηλαδή $n=1$, ουσιαστικά έχουμε να βρούμε τις ρίζες ενός πολυωνύμου, του ΜΚΔ$(f_1,\ldots,f_\mu)$. Αφού υπολογίσουμε τον ΜΚΔ με τον αλγόριθμο του Ευκλείδη, μπορούμε να εφαρμόσουμε τον αλγόριθμο Sturm κατά τα γνωστά.

Οι κύριες προσεγγίσεις για την αντιμετώπιση του προβλήματος στη γενική περίπτωση είναι δυο:

1. Αλγεβρικές, μελέτη δηλαδή της δομής του δακτυλίου πολυωνύμων $\mathbb{F}[x_1,x_2,...,x_n]$. Εδώ θα συναντήσουμε και θα ασχοληθούμε με τα θεωρήματα **Hilbert**.

2. Γεωμετρικές, μελέτη δηλαδή της δομής του συνόλου λύσεων πολυωνυμικών συστημάτων π.χ. μελέτη επιφανειών, γραμμών, σημείων τομής. Υπενθυμίζουμε εδώ ότι το σύνολο λύσεων ενός ομογενούς γραμμικού συστήματος είναι ένας υπόχωρος. Το τελευταίο είναι ένα αρκετά σημαντικό αποτέλεσμα, διότι μπορούμε έτσι βρίσκοντας μία βάση να κατανοήσουμε πλήρως τη δομή του συνόλου των λύσεων.

Θυμίζουμε ότι το αλγεβρικό σύνολο $V(f_1,\ldots,f_\mu)$ που αναζητούμε περιγράφεται από το ιδεώδες I του συστήματος. Έτσι ένα πρόβλημα που τίθεται είναι το *πρόβλημα του ανήκειν(ideal membership problem)*, δηλαδή η απάντηση στο αν το τυχόν $g \in \mathbb{F}[x_1,x_2,...,x_n]$ ανήκει στο I.

Θα δούμε πως η θεωρία των βάσεων Groebner μας δίνει τρόπο να αποφανθούμε άμεσα για το πρόβλημα του ανήκειν. Επίσης μας επιτρέπει να εφαρμόσουμε μεθόδους ανάλογες με εκείνες της απαλοιφής Gauss στα γραμμικά συστήματα, δηλαδή μας βοηθά να μετατρέψουμε το σύστημά μας σε «άνω τριγωνικό», με τη γενικότερη έννοια του όρου.

[1]Ένα γραμμικό πολυώνυμο με ν μεταβλητές είναι της μορφής $\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n$

8.1 Ιδεώδη μονωνύμων

Ορισμός 8.1. *Έστω $\mathbb{F}[x_1, x_2, ..., x_n]$ ο δακτύλιος των πολυωνύμων ν μεταβλητών, με συντελεστές από το σώμα $\mathbb{F}$. Τότε θα καλούμε **ιδεώδες μονωνύμων** του $\mathbb{F}[x_1, x_2, ..., x_n]$, ένα ιδεώδες που παράγεται από μονώνυμα, δηλαδή*

$$I = \langle \underset{\sim}{x}^{\alpha_1}, \underset{\sim}{x}^{\alpha_2}, \underset{\sim}{x}^{\alpha_3}, ... \rangle \quad , \quad \alpha_i \in \mathbb{Z}^n_{\geq 0}$$

Όπως φαίνεται στον ορισμό, τα μονώνυμα που παράγουν το I ενδέχεται να είναι άπειρα(θα δούμε όμως παρακάτω πως κάθε ιδεώδες μονωνύμων έχει μια πεπερασμένη βάση). Μπορεί να δειχθεί τα στοιχεία του ιδεώδες είναι όλοι οι γραμμικοί συνδυασμοί των μονωνύμων της βάσης με συντελεστές από το $\mathbb{F}$. Η παρακάτω πρόταση χαρακτηρίζει τα μονώνυμα του του ιδεώδους:

Πρόταση 8.2. *Έστω $I = \langle \underset{\sim}{x}^{\alpha_1}, \underset{\sim}{x}^{\alpha_2}, \ldots \rangle$ ένα ιδεώδες μονωνύμων και $\underset{\sim}{x}^{\beta} \in I$. Τότε το $\underset{\sim}{x}^{\beta}$ διαιρείται από κάποιο $\underset{\sim}{x}^{\alpha_i}$.*

Απόδειξη. Το I είναι διανυσματικός χώρος (άπειρης διάστασης) επί του $\mathbb{F}$ (Τα μονώνυμα του I είναι γραμμικά ανεξάρτητα). Άρα το $\underset{\sim}{x}^{\beta}$ γράφεται $\underset{\sim}{x}^{\beta} = \xi_1 \underset{\sim}{x}^{\alpha_1} + \cdots + \xi_n \underset{\sim}{x}^{\alpha_n}$. Από τη γραμμική ανεξαρτησία τ Επειδή το $x_1^{\gamma_{\rho 1}} x_2^{\gamma_{\rho 2}} \cdots x_n^{\gamma_{\rho n}} \in I$, τότε αυτό είναι γραμμικός συνδυασμός μονωνύμων της μορφής $x_1^{a_{i1}} x_2^{a_{i2}} ... x_n^{a_{in}}$. □

Πρόταση 8.3. *Τα ιδεώδη μονωνύμων του $\mathbb{F}[x]$, όπου $\mathbb{F}$ είναι σώμα, είναι της μορφής $\langle x^{\lambda} \rangle$, $\lambda \in \mathbb{Z}_{\geq 0}$.*

Απόδειξη. Αν I=$\{0\}$, ο ισχυρισμός είναι προφανής.

Έστω I$\neq \{0\}$. Επειδή έχουμε μια μόνο μεταβλητή, δηλαδή ν=1, είναι $I = \langle x^{\xi_1}, x^{\xi_2}, ..., x^{\xi_i}, ... \rangle$. Θεωρούμε το σύνολο $\Xi = \{\xi_1, \xi_2, \xi_3, ...\} \subseteq \mathbb{Z}_{\geq 0}$. Στο Ξ υπάρχει ελάχιστο στοιχείο, έστω ξ. Θα αποδείξουμε ότι $I = \langle x^{\xi} \rangle$.

Θεωρούμε το ιδεώδες $A = \langle x^{\xi} \rangle$. Τότε $x^{\xi} \in I$ και έτσι $A = \langle x^{\xi} \rangle \subseteq I$. Έστω $x^{\lambda} \in I$. Εκτελούμε τη διαίρεση του λ δια του ξ και έχουμε ότι $\lambda = \pi\xi + \upsilon$. Αν $\upsilon \neq 0$, τότε $x^{\upsilon} = x^{\lambda} x^{-\pi\xi} \in I$ και οδηγούμαστε σε άτοπο, διότι το ξ είναι ο ελάχιστος θετικός ακέραιος με $x^{\xi} \in I$. Άρα $\upsilon = 0$ και τελικά $x^{\lambda} \in I$ και $I \subseteq A$ άρα $A = I$. □

Π.χ. το ιδεώδες $I = \langle x^2 + x \rangle$ δεν είναι ιδεώδες μονωνύμων, διότι αν ήταν θα έπρεπε $I = \langle x^{\lambda} \rangle$, το οποίο είναι άτοπο αφού δεν υπάρχει πολυώνυμο $h(x)$, τέτοιο ώστε $x^2 + x = x^{\lambda} h(x)$.

Το ερώτημα που γεννιέται είναι αν όλα τα ιδεώδη μονωνύμων (χωρίς να τα υποθέτουμε παραγόμενα από κάποιο πεπερασμένο σύνολο) έχουν μια πεπερασμένη βάση.

Θεώρημα 8.4. *(Dickson) Έστω $I = \langle \underset{\sim}{x}^{\alpha_1}, \underset{\sim}{x}^{\alpha_2}, \underset{\sim}{x}^{\alpha_3}, \ldots \rangle$, $\alpha_i \in \mathbb{Z}^n_{\geq 0}$ ένα ιδεώδες μονωνύμων. Τότε το I είναι πεπερασμένα παραγόμενο, δηλαδή υπάρχουν n μονώνυμα: $\underset{\sim}{x}^{\beta_1}, \underset{\sim}{x}^{\beta_2}, \ldots, \underset{\sim}{x}^{\beta_n}$, που παράγουν το I.*

Απόδειξη. Στα παρακάτω για ένα διάνυσμα $\alpha \in \mathbb{Z}^{\kappa}_{\geq 0}$ θα συμβολίζουμε $\alpha^* \in \mathbb{Z}^{\kappa-1}_{\geq 0}$ την προβολή του α στις πρώτες $\kappa - 1$ συντεταγμένες. Έστω ένα τυχόν $I = \langle \underset{\sim}{x}^{\alpha_i},\ i \in K \rangle$, με K ένα σύνολο δεικτών. Εφαρμόζουμε επαγωγή στο πλήθος n των μεταβλητών.

• Για $n = 1$ ισχύει, όπως αποδείξαμε στην *Πρόταση (8.3)*.

• Έστω ότι ισχύει για $n = \kappa - 1$. Θα αποδείξουμε ότι ισχύει για $n = \kappa$.

Θεωρούμε το ιδεώδες μονωνύμων J του $\mathbb{F}[x_1, x_2, ..., x_{\kappa-1}]$, $J = \langle \underset{\sim}{x}^{\gamma^*} \ : \ \underset{\sim}{x}^{\gamma} \in I \rangle$, $\gamma \in \mathbb{Z}^{\kappa}_{\geq 0}$ δηλαδή το J παράγεται από την προβολή των όλων των μονωνύμων του I στις πρώτες $\kappa - 1$ μεταβλητές.

Από την υπόθεση της επαγωγής έχουμε ότι το J είναι πεπερασμένα παραγόμενο, άρα

$$J = \langle \underset{\sim}{x}^{\rho_i^*} \ , \ i = 1, \ldots, \lambda \rangle \quad , \quad \rho_i^* \in \mathbb{Z}^{\kappa-1}_{\geq 0}$$

Εξ ορισμού του J, τα $\underset{\sim}{x}^{\rho_i^*}$ προέρχονται από κάποια μονώνυμα $\underset{\sim}{x}^{\rho_i} \in I$, και έστω m_i η κ-οστή συντεταγμένη του $\underset{\sim}{x}^{\rho_i}$, $i = 1, \ldots, \lambda$. Θέτουμε $m = \max\{m_i \ , \ 1 \leq i \leq \lambda\}$. Για $r = 1, \ldots, m-1$ θεωρούμε τα ιδεώδη

$$J_r = \langle \underset{\sim}{x}^{\delta^*} \ : \ \underset{\sim}{x}^{\delta} \in I \text{ και η } x_{\kappa} \text{ είναι υψωμένη στην } r \rangle \quad , \quad \delta \in \mathbb{Z}^{\kappa}_{\geq 0}$$

άρα πρόκειται για τα ιδεώδη του $\mathbb{F}[x_1, \ldots, x_{\kappa-1}]$ που παράγονται από την προβολή όλων των μονωνύμων του I που περιέχουν το x_{κ}^r. Από υπόθεση αυτά είναι πεπερασμένα παραγόμενα:

$$J_r = \langle \underset{\sim}{x}^{\rho_{ir}^*} \ : \ i = 1, \ldots, \lambda_r \rangle \quad , \quad \rho_{ir}^* \in \mathbb{Z}^{\kappa-1}_{\geq 0}$$

και τα μονώνυμα $\underset{\sim}{x}^{\rho_{ir}}$ ανήκουν στο I.

Ισχυριζόμαστε ότι $I = \langle B \rangle$, όπου $B := \{\underset{\sim}{x}^{\rho_i} \ : \ i = 1, \ldots, \lambda\} \cup \{\underset{\sim}{x}^{\rho_{ir}} \ : \ r = 1 \ldots, m-1 \text{ και } i = 1 \ldots, \lambda_r\}$.

Πράγματι, αν $\underset{\sim}{x}^{\alpha} \in I, \ \alpha = (\alpha_1, \ldots, \alpha_\kappa)$, διακρίνουμε δυο περιπτώσεις:

$\alpha_\kappa \geq m$: Τότε $\underset{\sim}{x}^{\alpha^*} \in J$, και για κάποιο i, $\underset{\sim}{x}^{\rho_i} \big| \underset{\sim}{x}^{\alpha}$ επειδή το m είναι μέγιστο.

$\alpha_\kappa < m$: Τότε $\alpha_\kappa = r$, για κάποιο r. Έτσι $\underset{\sim}{x}^{\alpha^*} \in J_r$, άρα $\underset{\sim}{x}^{\rho_{ir}} \big| \underset{\sim}{x}^{\alpha}$ για κάποιο $i \in \{1 \ldots, \lambda_r\}$. □

8.2 Βάσεις Groebner

Θα προσδιορίσουμε μια κλάση βάσεων του τυχόντος ιδεώδους $I \lhd \mathbb{F}[x_1, \ldots, x_n]$, τις οποίες θα ονομάσουμε βάσεις Groebner. Η σημασία των βάσεων αυτών θα φανεί από τις ιδιότητες που θα δούμε ότι έχουν. Για να φτάσουμε σε μια τέτοια βάση ακολουθούμε την εξής διαδικασία: Για να φτάσουμε σε μια τέτοια βάση κάνουμε τους εξής συλλογισμούς:

α) Θεωρούμε το σύνολο $\mathrm{MO}(I) := \{MO(f) \ : \ f \in I\}$ των μεγιστοβαθμίων όρων όλων των πολυωνύμων του I. Αξίζει να παρατηρήσουμε ότι το σύνολο $MO(I)$ είναι άπειρο, εάν $I \neq \{0\}$. Φυσικά το σύνολο αυτό δεν είναι ιδεώδες, ούτε έχει κάποια άλλη αλγεβρική δομή.

β) Θεωρούμε το ιδεώδες μονωνύμων $\langle \mathrm{MO}(I) \rangle$. Γνωρίζουμε από το *λήμμα του Dickson (8.4)* ότι παράγεται από πεπερασμένα μονώνυμα του συνόλου $\mathrm{MO}(I)$. Δηλαδή $\langle \mathrm{MO}(I) \rangle = \langle \underset{\sim}{x}^{\alpha_1}, \ldots, \underset{\sim}{x}^{\alpha_\kappa} \rangle$. Επειδή $\underset{\sim}{x}^{\alpha_i} = \mathrm{MM}(g_i)$ για κάποια πολυώνυμα $g_i \in I$, μπορούμε χωρίς βλάβη να πολλαπλασιάσουμε κάθε στοιχείο της βάσης με τον αντίστοιχο συντελεστή $\mathrm{M\Sigma}(g_i)$ και να έχουμε $\langle \mathrm{MO}(I) \rangle = \langle \mathrm{MO}(g_1), \ldots, \mathrm{MO}(g_\kappa) \rangle$

Θεώρημα 8.5. *(Βάσης του Hilbert) Μια βάση του I είναι η $\{g_1, g_2, ..., g_\kappa\}$. Άρα κάθε ιδεώδες $I \lhd \mathbb{F}[\underset{\sim}{x}]$ είναι πεπερασμένα παραγόμενο.*

Ορισμός 8.6. *Έστω I ιδεώδες του $\mathbb{F}[\underset{\sim}{x}]$. Αν*

$$\langle MO(I) \rangle = \langle MO(g_1), MO(g_2), \ldots, MO(g_\kappa) \rangle$$

*τότε το σύνολο $\{g_1, g_2, ..., g_\kappa\}$ λέγεται **βάση Groebner** του ιδεώδους I.*

Μπορούμε να δούμε ότι μια τυχαία βάση δεν έχει την ιδιότητα του ορισμού: Έστω $I = \langle x^3 + 1, x^2 y + x \rangle$. Το πολυώνυμο

$$h(x, y) = x(x^2 y + x) - y(x^3 + 1) = x^2 - y$$

ανήκει στο I και έχει μεγιστοβάθμιο όρο(θεωρούμε διάταξη $x > y$) $\mathrm{MO}(h) = x^2$, όμως $x^2 \notin \langle x^3, x^2 y \rangle$ αφού δε διαιρείται με κανένα από αυτά.

Από το θεώρημα (8.4) γνωρίζουμε ότι κάθε ιδεώδες έχει μια βάση Groebner. Επίσης από την επιλογή των g_i φαίνεται πως η βάση δεν είναι μοναδική. Ο τρόπος εύρεσης μιας βάσης Groebner δεν είναι προφανής, όμως θα δούμε παρακάτω πως υπάρχει αλγόριθμος που την υπολογίζει. Γενικότερα ισχύουν:

- Κάθε ιδεώδες έχει (συνήθως) αρκετές βάσεις Groebner.
- Αν εισάγουμε πολυώνυμα που ανήκουν στο ιδεώδες σε μια βάση Groebner, το νέο σύνολο είναι επίσης βάση Groebner.
- Η βάση Groebner εξαρτάται από τη διάταξη των μονωνύμων που έχουμε επιλέξει.

Είδαμε ότι στον αλγόριθμο της διαίρεσης το υπόλοιπο δε μένει το ίδιο αν διαιρέσουμε με μια μετάθεση του διαιρέτη. Για τη διαίρεση όμως με μια βάση Groebner ισχύει το παρακάτω

Θεώρημα 8.7. *Έστω $G = \{g_1, g_2, ..., g_\kappa\}$ μια βάση Groebner ενός ιδεώδους $I \lhd \mathbb{F}[x_1, ..., x_n]$, και $f, \upsilon_1, \upsilon_2 \in \mathbb{F}[x_1, ..., x_n]$, όπου υ_1, υ_2 τα υπόλοιπα της διαίρεσης f δια $(g_1, g_2, ..., g_\kappa)$ και $(g_2, g_1, ..., g_\kappa)$ αντίστοιχα. Τότε $\upsilon_1 = \upsilon_2$.*

Απόδειξη. Έστω $\upsilon_1 - \upsilon_2 = 0$, τότε ισχύει το ζητούμενο.

Εάν όμως θεωρήσουμε ότι $\upsilon_1 - \upsilon_2 \neq 0$, τότε η διαφορά $\upsilon_1 - \upsilon_2$ αποτελεί συνδυασμό των $\{g_2, g_1, ..., g_\kappa\}$ και άρα έχουμε $\upsilon_1 - \upsilon_2 \in \langle g_2, g_1, ..., g_\kappa \rangle$. Αλλά το σύνολο $\{g_2, g_1, ..., g_\kappa\}$ είναι μια βάση Groebner του I. Έτσι ο $\mathrm{MO}(\upsilon_1 - \upsilon_2)$ διαιρείται από τουλάχιστον ένα μέγιστο όρο από τα $g_2, g_1, ..., g_\kappa$. Άτοπο διότι ο $\mathrm{MO}(\upsilon_1 - \upsilon_2)$ έχει βαθμό μικρότερο από κάθε $\mathrm{MO}(g_i)$ ως διαφορά υπολοίπων της διαίρεσης με $g_1, g_2, ..., g_\kappa$. □

Έτσι όταν διαιρούμε με μια βάση Groebner μπορούμε να γράφουμε $f \mod \{g_1, g_2, ..., g_\kappa\}$ αφού το υπόλοιπο δεν εξαρτάται από τη διάταξη των g_i που θα χρησιμοποιήσουμε στον αλγόριθμο της διαίρεσης. Θα συμβολίζουμε και

$$\overline{f}^{\{g_1, g_2, ..., g_\kappa\}} := f \mod \{g_1, g_2, ..., g_\kappa\}$$

Παρατηρήσαμε πως μια βάση Groebner δεν είναι μοναδική. Ο παρακάτω ορισμός μας δίνει μια πιο μικρή κλάση βάσεων Groebner:

Ορισμός 8.8. *Ελάχιστη(minimal) βάση Groebner του ιδεώδους I είναι μια βάση Groebner $G = \{g_1, g_2, ..., g_\kappa\}$ με τις επιπλέον ιδιότητες:*

(α') Οι αριθμητικοί συντελεστές των $MO(g_i)$ είναι ίσοι με 1.

(β') Για κάθε $i = 1, 2, ...\kappa$, ισχύει ότι $MO(g_i) \notin \langle MO(g_1), \ldots, MO(g_{i-1}), MO(g_{i+1}), \ldots, MO(g_\kappa) \rangle$.

Σύμφωνα με τον ορισμό μπορούμε εύκολα να μετατρέψουμε μια τυχούσα βάση Groebner σε ελάχιστη διαιρώντας τα στοιχεία της με τους αντίστοιχους μεγιστοβάθμιους συντελεστές(ώστε οι μεγιστοβάθμιοι να γίνουν 1) και ελέγχοντας αν υπάρχουν μεγιστοβάθμιοι όροι που διαιρούνται μεταξύ τους· τα αντίστοιχα πολυώνυμα αφαιρούνται από το σύνολο και τότε η βάση Groebner είναι ελάχιστη(μπορείτε να διαπιστώσετε εύκολα ότι το σύνολο που απομένει είναι πράγματι βάση Groebner).

Είναι φανερό ότι η ελάχιστη βάση είναι πιο βολική για τους υπολογισμούς, αφού έχει ελάχιστο αριθμό στοιχείων. Το τελικό βήμα είναι να βρούμε μια ακόμα «καλύτερη» βάση Groebner, η οποία θα έχει την σπουδαία ιδιότητα να είναι μοναδική για κάθε ιδεώδες:

Ορισμός 8.9. *Ανηγμένη(reduced) βάση Groebner είναι μια ελάχιστη βάση Groebner $G = \{g_1, g_2, ..., g_\kappa\}$ με την επιπλέον ιδιότητα να μην υπάρχει μονώνυμο του g_i $(i = 1, ..., \kappa)$ που να διαιρείται από κάποιο $MO(g_j)$, $j \neq i$.*

Θεώρημα 8.10. *Κάθε ιδεώδες I έχει μοναδική ανηγμένη βάση Groebner.*

Αν έχουμε μια ελάχιστη βάση Groebner μπορούμε εύκολα να φτάσουμε στην ανηγμένη βάση Groebner του ιδεώδους ακολουθώντας τον ορισμό: παίρνουμε τα g_i που δεν ικανοποιούν την ιδιότητα *(β')* και τα αντικαθιστούμε με το υπόλοιπο $g_i \mod (G - \{g_i\})$. Το τελευταίο υπολογίζεται από τον αλγόριθμο της διαίρεσης, και είναι βέβαιο πως ικανοποιεί την ιδιότητα *(β')*. Η διαδικασία που μετατρέπει μια τυχαία βάση πρώτα σε ελάχιστη και κατόπιν στην ανηγμένη λέγεται αυτοαναγωγή(autoreduction).

8.3 Προβλήματα και λύσεις

Στην επόμενη ενότητα παρουσιάζουμε τον αλγόριθμο που υπολογίζει μια βάση Groebner ενός ιδεώδους. Ας δούμε ποια σημαντικά προβλήματα μπορούν να λυθούν με έναν τέτοιο αλγόριθμο.

α) Από τη μοναδικότητα της ανηγμένης βάσης Groebner έχουμε έναν αλγόριθμο για να εξετάζουμε ισότητα ιδεωδών(άρα και ισοδυναμία δυο πολυωνυμικών συστημάτων):

1. Βρες τις ανηγμένες βάσεις Groebner, των δυο ιδεωδών.
2. Αν έχουν την ίδια ανηγμένη βάση Groebner απάντησε ΝΑΙ αλλιώς απάντησε ΟΧΙ.

β) Πολύ σημαντικό στις εφαρμογές είναι το *πρόβλημα του ανήκειν*: «δοθέντος ενός συνόλου πολυωνύμων $F = \{f_1, \ldots, f_n\}$ και ενός πολυωνύμου h, ανήκει το h στο ιδεώδες που παράγεται από το F;». Από το παρακάτω

Λήμμα 8.11. *Έστω $G = \{g_1, \ldots, g_\kappa\}$ μια βάση Groebner του I. Τότε $h \in I \Leftrightarrow h \bmod G = 0$.*

έχουμε άμεσα τον εξής αλγόριθμο:

1. Βρες μια βάση Groebner, $G = \{g_2, g_1, ..., g_\kappa\}$ του ιδεώδους.
2. Εκτέλεσε τη διαίρεση του h δια G, με οποιαδήποτε σειρά.
3. Αν $\overline{f}^G = 0$ απάντησε ΝΑΙ αλλιώς απάντησε ΟΧΙ.

γ) Η χρησιμότητα των βάσεων Groebner στη μελέτη και επίλυση αλγεβρικών συστημάτων είναι μεγάλη, ακόμη κι αν πρόκειται για υπερ- ή υπό-προσδιορισμένα συστήματα. Η βασική ιδιότητα είναι πως το σύνολο λύσεων του αρχικού συστήματος ισούται με το σύνολο λύσεων της βάσης, αφού πρόκειται για το ίδιο ιδεώδες. Η βάση Groebner έχει την *ιδιότητα της απαλοιφής*(elimination property): Αν έχουμε μια βάση Groebner σύμφωνα με μια λεξικογραφική διάταξη(πχ $x_1 > \cdots > x_n$) και το σύστημα έχει πεπερασμένες λύσεις, τότε υπάρχει πολυώνυμο στη βάση στο οποίο εμφανίζεται μόνο η x_n. Λύνουμε το τελευταίο ως προς x_n και αντικαθιστούμε τις λύσεις στα υπόλοιπα. Για κάθε τιμή του x_n, βρίσκουμε πολυώνυμο στη βάση με μεταβλητή μόνο την x_{n-1} κοκ. Πρόκειται για μια γενίκευση της αντίστοιχης διαδικασίας που γίνεται στα γραμμικά συστήματα, όταν επιλύουμε με προς τα πίσω αντικατάσταση(back-substitution). Στο τέλος έχουμε όλες τις λύσεις του συστήματος.

Αν το σύστημα έχει άπειρες λύσεις μπορούμε παρόμοια να αφήσουμε κάποιες ελεύθερες μεταβλητές, και να έχουμε μια περιγραφή όλων των λύσεων. Απάντηση στο ερώτημα «έχει το σύστημα λύσεις;» δίνει το περίφημο Θεώρημα Nullstellensatz του Hilbert(1890):

Θεώρημα 8.12. *Ένα σύστημα πολυωνύμων F είναι αδύνατο(δεν έχει λύσεις) αν και μόνο αν η ανηγμένη βάση Groebner είναι το μονοσύνολο $\{1\}$, δηλαδή $I = \langle F \rangle = \langle 1 \rangle = \mathbb{F}[\underline{x}]$.*

Αλγόριθμος Buchberger

Είδαμε ότι κάθε ιδεώδες έχει μια βάση Groebner. Πως όμως μπορεί να προσδιοριστεί μια τέτοια βάση; Την απάντηση έδωσε ο B. Buchberger, όταν στη διδακτορική του διατριβή το 1965 διατύπωσε τον ομώνυμο αλγόριθμο. Ξεκινάμε με έναν ορισμό:

Ορισμός 9.1. *Για δυο πολυώνυμα $f_1, f_2 \in \mathbb{F}[\underset{\sim}{x}]$ καλούμε S-πολυώνυμο των f_1, f_2 το*

$$S(f_1, f_2) := \frac{\underset{\sim}{x}^{\gamma}}{MO(f_1)} f_1 - \frac{\underset{\sim}{x}^{\gamma}}{MO(f_2)} f_2$$

όπου $\underset{\sim}{x}^{\gamma}$ το ελάχιστο κοινό πολλαπλάσιο των $MM(f_1)$ και $MM(f_2)$, δηλαδή το γ_i είναι η μέγιστη δύναμη στην οποία εμφανίζεται η x_i στα δυο μονώνυμα.

Για παράδειγμα, $S(x^3+2, x^2-x+1) = x^2-x+2$, $S(x^2y-y, xy^2+x) = -x^2-y^2$, $S(\underset{\sim}{x}^{(2,1,2)}+\underset{\sim}{x}^{(2,1,1)}, \underset{\sim}{x}^{(1,2,2)}) = \underset{\sim}{x}^{(2,2,1)}$. Παρατηρούμε ότι το $S-$πολυώνυμο δεν έχει απαραίτητα μικρότερο βαθμό απ' ότι τα f, g.

Η βασική ιδιότητα του $S(f, g)$ είναι ότι οι $\mathrm{MO}(f), \mathrm{MO}(g)$ δεν εμφανίζονται σε αυτό. Αν τα f, g ήταν γραμμικά και αντιστοιχούσαν σε γραμμές κάποιου πίνακα, τότε το $S(f, g)$ θα ήταν ο γραμμικός συνδυασμός των αντίστοιχων γραμμών, τον οποίο υπολογίζει ο αλγόριθμος απαλοιφής του Gauss. Το παρακάτω λήμμα δείχνει ότι κάθε πιθανή απλοποίηση μεγιστοβαθμίων όρων σε γραμμικούς συνδυασμούς πολυωνύμων εκφράζεται από κάποιο σύνολο S-πολυωνύμων:

Λήμμα 9.2. *Έστω $f_i = MO(f_i) + h_i,\ i = 1, \ldots, \kappa$ πολυώνυμα, στα οποία έχουμε ξεχωρίσει τους μεγιστοβάθμιους όρους(ως προς μια διάταξη), και $MM(f_i) = x^{\delta}$.*

Για κάθε γραμμικό συνδυασμό $q = \sum_{i=1}^{\kappa} c_i f_i$, $c_i \in \mathbb{F}$, τέτοιο ώστε ο βαθμός του q να είναι μικρότερος από το δ(σύμφωνα με την ίδια διάταξη), υπάρχουν $S-$πολυώνυμα και συντελεστές $a_i \in \mathbb{F}$ ώστε

$$q = \sum_{i=1}^{\kappa-1} a_i S(f_i, f_{i+1})$$

Επίσης κάθε $S-$πολυώνυμο που εμφανίζεται έχει βαθμό μικρότερο του δ.

Αυτή η ιδιότητα των $S-$πολυωνύμων μας δίνει τη δυνατότητα να ξεπεράσουμε ένα σημαντικό πρόβλημα που εμφανίστηκε στις βάσεις ιδεωδών· υπάρχουν σύνολα F που παράγουν ένα ιδεώδες, όμως μέσα σε αυτό το ιδεώδες εμφανίζονται πολυώνυμα με μεγιστοβάθμιους όρους που δεν διαιρούνται με κανένα στοιχείο του $\mathrm{MO}(F)$, όπως είναι το q. Γνωρίζουμε τώρα ότι όλα αυτά τα πολυώνυμα μπορούν να εκφραστούν σαν γραμμικοί συνδυασμοί $S-$πολυωνύμων. Άρα το κλειδί για να φτάσουμε σε μια βάση Groebner είναι τα $S-$πολυώνυμα.

Η παρατήρηση αυτή μας οδηγεί στο *Κριτήριο Buchberger* που χαρακτηρίζει τις βάσεις Groebner ενός ιδεώδους.

Θεώρημα 9.3. *Έστω $I = \langle g_1, g_2, ..., g_\kappa \rangle$. Το $G = \{g_1, g_2, ..., g_\kappa\}$ είναι βάση Groebner ως προς μια συγκεκριμένη διάταξη μονωνύμων αν και μόνο αν $\overline{S(g_i, g_j)}^{G} = 0,\ \forall i \neq j$, ως προς τη διάταξη που έχουμε επιλέξει.*

Παρατηρήστε ότι πρόκειται για αλγοριθμικό κριτήριο, το οποίο απαντάει στην ερώτηση: «Είναι το G βάση Groebner;».

Μπορούμε τώρα να διατυπώσουμε τον αλγόριθμο του Buchberger. Με είσοδο ένα σύνολο $F = \{f_1, \ldots, f_m\}$, ο αλγόριθμος υπολογίζει μια βάση Groebner $G = \{g_1, \ldots, g_\kappa\}$ του ιδεώδους $I = \langle f_1, \ldots, f_m\rangle$ τέτοια ώστε $F \subseteq G$. Δηλαδή ο αλγόριθμος απλώς προσθέτει πολυώνυμα στο αρχικό σύνολο. Τα πολυώνυμα που προστίθενται είναι τα μη μηδενικά υπόλοιπα της διαίρεσης $S-$πολυωνύμων δια του F. Αν αυτή η διαδικασία της προσθήκης τερματίσει(δηλαδή κάποια στιγμή ικανοποιηθεί το κριτήριο Buchberger), ο αλγόριθμος θα δώσει στην έξοδο μια βάση Groebner, που συνήθως δεν είναι η ανηγμένη. Θυμηθείτε όμως ότι από μια τυχούσα βάση μπορούμε να υπολογίσουμε ανηγμένη βάση Groebner(αυτοαναγωγή). Ο αλγόριθμος είναι:

1. Θέσε $G = F$.
2. Για κάθε ζεύγος $\{p, q\} \subseteq G$, Αν $s = \overline{S(p,q)}^G$ είναι μη μηδενικό, θέσε $F = F \cup \{s\}$
3. Αν $G = F$ (δηλαδή στο βήμα 2 δεν προστέθηκε τίποτα καινούριο) τότε επέστρεψε το G, διαφορετικά ξεκίνα πάλι από το βήμα 1.

Για παράδειγμα, έστω $F = \{f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x\}$. Θεωρούμε τη βαθμωτή διάταξη. Το F δεν είναι βάση Groebner διότι το $f_3 := \overline{S(f_1, f_2)}^F = -x^2$ έχει αρχικό μονώνυμο $x^2 \notin \langle x^3, x^2y\rangle$. Άρα θέτουμε $G = \{f_1, f_2, f_3\}$. Υπολογίζουμε

$$f_4 := \overline{S(f_1, f_3)}^G = -2xy, \;\; f_5 := \overline{S(f_2, f_3)}^G = -2y^2 + x$$

και διαπιστώνουμε πως πλέον όλα τα S-πολυώνυμα μηδενίζονται $\mathrm{mod}\{f_1, \ldots, f_5\}$. Το $G = \{f_1, \ldots, f_5\}$ είναι βάση Groebner σύμφωνα με το Κριτήριο Buchberger.

Παρατηρήστε πως $\mathrm{MO}(f_1) \in \langle \mathrm{MO}(f_2), \ldots, \mathrm{MO}(f_5)\rangle$. Αυτό σημαίνει πως μια μικρότερη βάση Grobner είναι το σύνολο $\{f_2, \ldots, f_5\}$. Επιπλέον $\mathrm{MO}(f_2) \in \langle \mathrm{MO}(f_3), \mathrm{MO}(f_4), \mathrm{MO}(f_5)\rangle$ άρα μια ακόμη μικρότερη βάση Groebner είναι το $\{f_3, f_4, f_5\}$. Πρόκειται για μια *ελάχιστη* βάση Groebner αν διαιρέσουμε με τους μεγιστοβάθμιους συντελεστές.

9.1 Ορθότητα & πολυπλοκότητα

Εκ κατασκευής $F \subseteq G$. Τα $S-$πολυώνυμα είναι στοιχεία του ιδεώδους, άρα $G \subseteq I$. Άρα το G παράγει το ιδεώδες. Εάν τερματίσει ο αλγόριθμος, τότε τα υπόλοιπα των $S-$πολυωνύμων δια G είναι όλα μηδέν, άρα πρόκειται για μια βάση Groebner σύμφωνα με το θεώρημα 9.3.

Θα δείξουμε ότι ο αλγόριθμος τερματίζει. Έστω $\underset{\sim}{x}^{t_i}$ το μεγιστοβάθμιο μονώνυμο του $i-$οστού πολυωνύμου που εισάγει ο αλγόριθμος στη βάση, $i = 1, 2, \ldots$. Παρατηρούμε ότι στην ακολουθία $\underset{\sim}{x}^{t_1}, \underset{\sim}{x}^{t_2}, \underset{\sim}{x}^{t_3}, \ldots$, για κάθε j, το μονώνυμο $\underset{\sim}{x}^{t_j}$ δεν είναι πολλαπλάσιο κανενός από τα $\underset{\sim}{x}^{t_1}, \underset{\sim}{x}^{t_2}, \ldots, \underset{\sim}{x}^{t_{j-1}}$, διότι έχουμε εκτελέσει τη διαίρεση με τα πολυώνυμα της βάσης, μέσα στην οποία υπάρχουν πολυώνυμα με μεγιστοβάθμια μονώνυμα αυτά ακριβώς τα μονώνυμα. Από το Λήμμα του Dickson (8.4), μια τέτοια ακολουθία δε μπορεί παρά να είναι πεπερασμένη: Πράγματι ένα άπειρο σύνολο από τέτοια μονώνυμα θα ήταν βάση ενός ιδεώδους μονωνύμων, το οποίο δε θα είχε καμία πεπερασμένη βάση, καθώς κάθε επόμενο στοιχείο της άπειρης βάσης δεν θα μπορούσε να παρασταθεί με χρήση των προηγουμένων, άτοπο.

Αν πειραματιστούμε με οποιαδήποτε υλοποίηση του αλγορίθμου θα διαπιστώσουμε πως είναι έντονο το φαινόμενο της ενδιάμεσης διόγκωσης των υπολογισμών(intermediate expression swell): Ξεκινώντας με είσοδο πολυώνυμα μικρού βαθμού και με μικρούς συντελεστές, ο αλγόριθμος παράγει πολυώνυμα με μεγάλο βαθμό και τεράστιους συντελεστές. Αυτή η παρατήρηση είναι αρκετά κακός οιωνός για τα αποτελέσματα που αναμένουμε σχετικά με το χρόνο του αλγορίθμου. Για περισσότερα από τριάντα χρόνια από τη δημοσίευση του αλγορίθμου(1965), η πολυπλοκότητά του παρέμεινε άγνωστη. Αρκετά ερωτήματα είναι ανοικτά ακόμη και σήμερα. Η ανάλυση που παρουσιάζουμε οφείλεται στον Mayr και τους συνεργάτες του.

Υπενθυμίζουμε σύντομα από τη Θεωρία Πολυπλοκότητας την κλάση προβλημάτων στην οποία θα εντάξουμε τον αλγόριθμο: Η κλάση EXPSPACE είναι το σύνολο των προβλημάτων απόφασης που μπορούν να επιλυθούν

με χρήση εκθετικού χώρου μνήμης. Τα προβλήματα EXPSPACE-complete είναι εξαιρετικά δύσκολα και συνήθως έχουν διπλά εκθετικό χρόνο, $O(2^{2^n})$, τουλάχιστον για κάποια στιγμιότυπα. Για περισσότερες λεπτομέρειες παραπέμπουμε στο [;].

Οι Mayr & Meyer έδειξαν το 1982 ότι το πρόβλημα του ανήκειν είναι EXPSPACE-complete[;]. Γνωρίζουμε ότι το πρόβλημα αυτό ανάγεται στον υπολογισμό μιας βάσης Groebner, άρα το αντίστοιχο πρόβλημα απόφασης «είναι το G βάση Groebner» είναι EXPSPACE-hard. Το παρακάτω αποτέλεσμα οφείλεται στους Mayr(1989) και Kühnle & Mayr(1996)[;]:

Θεώρημα 9.4. *Το πρόβλημα εύρεσης της ανηγμένης βάσης Groebner είναι EXPSPACE-complete.*

Έχει δειχθεί επίσης(Mayr 1995) ότι για ομογενή ιδεώδη(δηλαδή παραγόμενα από ομογενή πολυώνυμα) το πρόβλημα του ανήκειν είναι PSPACE-complete, ενώ ο υπολογισμός μιας βάσης Groebner παραμένει EXPSPACE-complete. Πρώτος ο Hilbert απέδειξε(1890) ότι το πρόβλημα του ανήκειν είναι αποφασίσιμο(θεώρημα (8.5)). Η Hermann το 1926 έδωσε μια κατασκευαστική μέθοδο για την αναπαράσταση οποιουδήποτε $f \in \langle f_1, \ldots, f_n \rangle$ ως πολυωνυμικό συνδυασμό

$$f = \sum_{i=1}^{n} q_i f_i$$

Έδειξε ότι οι βαθμοί των q_i φράσσονται από μια διπλά εκθετική ποσότητα. Ειδικότερα οι βαθμοί των πολυωνύμων μιας ανηγμένης βάσης Groebner φράσσονται από

$$2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}$$

όπου n ο αριθμός των μεταβλητών και $\deg f_i \leq d$. Το φράγμα δεν εξαρτάται από τον αριθμό των πολυωνύμων ή το μέγεθος των συντελεστών. Είναι πολυωνυμικό ως προς το βαθμό των πολυωνύμων και διπλά εκθετικό ως προς τον αριθμό των μεταβλητών. Υπάρχουν ιδεώδη που έχουν βάσεις Groebner με τουλάχιστον $2^{2^{cn}}$ στοιχεία, με βαθμό τουλάχιστον $2^{2^{sn}}$,όπου $c, s \in \mathbb{R}$. Για παράδειγμα, αν $F = \{x^{n+1} - yz^{n-1}w, xy^{n-1} - z^n, x^n z - y^n w\}$, έχει αποδειχθεί ότι το πολυώνυμο $z^{n^2+1} - y^{n^2}w$ υπάρχει στην ανηγμένη βάση Groebner του $\langle F \rangle$, σύμφωνα με κάποια διάταξη.

Ο χρόνος χειρότερης περίπτωσης του αλγορίθμου του Buchberger δεν είναι γνωστός, όμως από το θεώρημα (9.4) έχουμε ένα κάτω φράγμα για αυτόν. Το αποτέλεσμα αυτό είναι αρκετά απαισιόδοξο, όμως υπάρχει αντίλογος: Το φράγμα αυτό έχει αποδειχθεί με στιγμιότυπα περισσότερο συνδυαστικά παρά γεωμετρικά. Τα περισσότερα πρακτικά προβλήματα όμως έχουν γεωμετρική υφή. Οι Kühnle & Mayr θεωρούν τον ίδιο υπολογιστικό χρόνο για κάθε πολυώνυμο με δεδομένο βαθμό και αριθμό μεταβλητών, πράγμα το οποίο δεν ανταποκρίνεται στην πραγματικότητα. Ενδεχομένως τα πραγματικά (συνήθως γεωμετρικά) προβλήματα που εμφανίζονται στην πράξη να είναι πιο εύκολα από ότι τα συνδυαστικά κατασκευασμένα προβλήματα.

9.2 Βελτιώσεις στον αλγόριθμο

Είδαμε τη βασική ιδέα του αλγορίθμου και συνεχίζουμε με κάποιες παρατηρήσεις που βελτιώνουν τον αρχικό αλγόριθμο του Buchberger. Όλο το υπολογιστικό βάρος του αλγορίθμου πέφτει στις διαιρέσεις του βήματος 2. Θα δούμε πως κάποιες από αυτές μπορούν να παραλειφθούν. Σημαντικό ρόλο παίζει η σειρά με την οποία διαλέγουμε τα $\{p, q\}$, κι έχουν αναπτυχθεί διάφορες στρατηγικές για το πως είναι καλύτερα να γίνει αυτό. Ένας άλλος βαθμός ελευθερίας που έχουμε είναι στη διάταξη που εφαρμόζουμε, η οποία επηρεάζει την ταχύτητα του αλγορίθμου της διαίρεσης για δεδομένο στιγμιότυπο.

Οι τρεις *παρατηρήσεις Buchberger* που αναφέρονται παρακάτω εμφανίζονται πρώτη φορά στο [;].

α) Αν κάποιο $S-$πολυώνυμο $S(p, q)$ αφήσει υπόλοιπο 0 κατά τη διαίρεση σε κάποιο βήμα, ο παραπάνω αλγόριθμος υπολογίζει πάλι το υπόλοιπο στις επόμενες επαναλήψεις. Αυτό δε θα έπρεπε να γίνεται, καθώς το υπόλοιπο θα παραμείνει 0 όταν προσθέσουμε επιπλέον πολυώνυμα στη βάση.

β) Παρατήρηση Buchberger I: Η στρατηγική αυτή προτείνει να επιλεγούν πρώτα εκείνα τα $\{p, q\}$ με το μικρότερο ΕΚΠ(ΜΟ(p), ΜΟ(p)) μεταξύ των ζευγών, σύμφωνα με τη διάταξη που έχουμε καθορίσει. Αυτή η επιλογή ενδέχεται να βελτιώσει την ταχύτητα του αλγορίθμου.

Μια άλλη στρατηγική για την επιλογή των ζευγών(sugar strategy), η οποία φαίνεται να έχει καλύτερα αποτελέσματα τις περισσότερες περιπτώσεις, παρουσιάζεται στο [**;**].

γ) Παρατήρηση Buchberger II: Αν τα ΜΜ(p) και ΜΜ(q) είναι σχετικά πρώτα, τότε $\overline{S(p,q)}^F = 0$. Άρα μπορούμε να αγνοήσουμε τα ζεύγη $\{p, q\}$ τα οποία έχουν την ιδιότητα αυτή.

δ) Παρατήρηση Buchberger III: Αν υπάρχει πολυώνυμο h στη βάση τέτοιο ώστε

- Τα $S(p, h)$ και $S(q, h)$ έχουν ήδη υπολογιστεί και
- Ο ΜΟ(h) διαιρεί το ΕΚΠ(ΜΟ(p), ΜΟ(q))

τότε $\overline{S(p,q)}^F = 0$, και το ζεύγος $\{p, q\}$ μπορεί να αγνοηθεί.

ε) Η έξοδος του αρχικού αλγορίθμου δεν είναι η ανηγμένη βάση Groebner, δηλαδή υπάρχουν πλεονάζοντα πολυώνυμα τα οποία μπορούν να αφαιρεθούν. Αναφέραμε τη διαδικασία της αυτοαναγωγής, για να φτάσουμε στην ανηγμένη βάση σαν ένα τελικό βήμα. Είναι πιο αποτελεσματικό η διαδικασία αυτή να γίνεται online σε κάθε επανάληψη του αλγορίθμου. Έτσι με κατάλληλη τροποποίηση του αλγορίθμου μπορούμε να πάρουμε στην έξοδο την ανηγμένη βάση Groebner.

Θεωρία αραιής απαλοιφής

Παρακάτω εξετάζουμε τη θεωρία της αραιής απαλοιφής (sparse, or toric, elimination) που γενικεύει όλα τα παραπάνω όρια [CLO05].

Ορισμός 10.1. *Έστω πολυώνυμο n μεταβλητών με m μη-μηδενικούς όρους. Θεωρούμε τα ακέραια διανύσματα των m εκθετών ως σημεία στον $n-$διάστατο χώρο. Το κυρτό περίβλημα των m σημείων (μικρότερο κυρτό πολύεδρο που περιλαμβάνει τα σημεία) καλείται* πολύεδρο του Νεύτωνα *του πολυωνύμου.*

Συνεπώς το πολύεδρο του Νεύτωνα εξαρτάται μόνο από ένα υποσύνολο των μη μηδενικών όρων, αλλά όχι από την ακριβή τιμή των συντελεστών τους. Το πολύεδρο του Νεύτωνα εκφράζει την «πολυπλοκότητα» του πολυωνύμου, με μεγαλύτερη ακρίβεια απ'ό,τι ο συνολικός βαθμός.

Παράδειγμα 10.1. Στο πολυώνυμο $P(x,y) = 3x^2 - y + 2xy + 5x^2y + 6x^2y^2 - 2x^3y^2$ αντιστοιχούμε το σύνολο των εκθετών που εμφανίζονται $\{(2,0),(0,1),(1,1),(2,1),(2,2),(3,2)\}$.

Έστω μια εξίσωση $f = c_0 + c_1x + \cdots + c_bx^b$ ως προς x, βαθμού b. Το πολύεδρο του Νεύτωνα εδώ είναι το ευθύγραμμο τμήμα $[0,b]$ και ο όγκος του ισούται με το μήκος b. Γνωρίζουμε από το Θεμελιώδες Θεώρημα της Άλγεβρας πως το πλήθος των μιγαδικών ριζών της εξίσωσης $f = 0$ ισούται με b. Αν έχουμε 2 εξισώσεις με 2 αγνώστους x, y, οι οποίες έχουν το ίδιο πολύεδρο του Νεύτωνα (το οποίο ονομάζουμε P), τότε το διπλάσιο του όγκου του πολυέδρου ισούται με το πλήθος των κοινών μιγαδικών ριζών του συστήματος, δηλ. το πλήθος των ζευγών (x,y) για τα οποία και οι 2 εξισώσεις μηδενίζονται.

φιγυρε=φιγς/τηεσε/αΝεωτον.πς,ωιδτη=5cμ

Σχήμα 10.1: Πολύγωνο του Νεύτωνα για αραιό πολυώνυμο 2 μεταβλητών συνολικού βαθμού 4 και αντίστοιχο πολύγωνο του Νεύτωνα για αντίστοιχο πυκνό πολυώνυμο με τον ίδιο συνολικό βαθμό.

Γενικά, ένα σύστημα n εξισώσεων με n αγνώστους, όπου όλα τα πολύεδρα του Νεύτωνα είναι ίδια, έχει το πολύ $n!V$ μιγαδικές ρίζες, όπου V ο όγκος του πολυέδρου του Νεύτωνα. Αυτό αποτελεί ειδική περίπτωση του παρακάτω θεωρήματος 10.2.

Γενικότερα, υπάρχουν όρια στο πλήθος ριζών συστήματος πολυωνύμων σε συνάρτηση του Μεικτού όγκου των αντίστοιχων πολυέδρων του Νεύτωνα, ακριβέστερα από τα κλασικά όρια του Bézout, τα οποία αποτελούν συνάρτηση του συνολικού βαθμού. Για να δούμε πώς το πολύγωνο του Νεύτωνα δίνει ακριβέστερη πληροφορία από τον συνολικό βαθμό, θεωρήστε το παράδειγμα στο σχήμα 10.1. Είναι σαφές πως το πολύγωνο αυτό είναι πολύ μικρότερο από το αντίστοιχο πολύγωνο (τρίγωνο) του Νεύτωνα για πυκνό πολυώνυμο συνολικού βαθμού 4, το οποίο φαίνεται με διακεκομμένες γραμμές.

Παράδειγμα 10.2. Έστω τα πολυώνυμα $c_0 + c_1x + c_2x^2y + c_3xy, b_0 + b_1x + b_2y + b_3xy$, και οποιαδήποτε μη-μηδενικά c_i, b_i. Το σχ. 10.2 δείχνει τα αντίστοιχα πολύγωνα του Νεύτωνα.

φιγυρε=φιγς/τηεσε/ιν13μ.πς,ωιδτη=5cμ

Σχήμα 10.2: Δύο πολύγωνα Νεύτωνα, άθροισμα Μινκοωσκι, μικτή υποδιαίρεση, και υπολογισμός μικτού όγκου.

Διανυσματικό άθροισμα (ή άθροισμα Minkowski) $A+B$ δύο συνόλων (πεπερασμένων ή άπειρων) ακέραιων διανυσμάτων είναι $\{\alpha+\beta : \alpha \in A, \beta \in B\}$. Εάν A, B κυρτά σύνολα τότε $A+B$ κυρτό. Ορίζεται επίσης ο μικτός όγκος των πολυέδρων, ο οποίος μπορεί να υπολογιστεί μέσω του αθροίσματος Μινκοωσκι. Το άθροισμα

Μινκοωσκι δύο σημειοσυνόλων A, B είναι το σημειοσύνολο $A+B$ που περιέχει όλα τα διανυσματικά αθροίσματα $a+b$ για κάθε $a \in A, b \in B$. Το άθροισμα Minkowski 2 πολυγώνων φαίνεται στο σχήμα 10.2 παρακάτω. Στο ίδιο σχήμα δείχνουμε και μια «μικτή υποδιαίρεση» του αθροίσματος Minkowski με την οποία υπολογίζουμε το Μικτό όγκο και, τελικά, ένα φράγμα στο πλήθος ριζών των αντίστοιχων πολυωνύμων. Στο παράδειγμα (σχήμα 10.2) ο Μικτός όγκος ισούται με 3.

Θεώρημα 10.2. [Ber75] *Ο μικτός όγκος των n πολυέδρων Νεύτωνα των πολυωνύμων φράσσει το πλήθος των κοινών ριζών στο $(\mathbb{C}-\{0\})^n$ για οποιοδήποτε σύστημα με δεδομένους τους μη-μηδενικούς όρους. Οι πολλαπλότητες συνυπολογίζονται, ενώ σπάνια προσμετρούνται ρίζες στο άπειρο. Εάν οι συντελεστές είναι γενικοί τότε το όριο είναι ακριβές.*

Το όριο Bernstein είναι επίσης γνωστό ως όριο Bernstein-Khovanskii-Kushnirenko.

Η χρησιμότητα του ορίου δικαιολογείται από 2 παράγοντες: (α) Τυπικά είναι πολύ κατώτερο του ορίου Bézout, (β) εξαρτάται μόνο από τα πολύεδρα του Νεύτωνα των πολυωνύμων οπότε είναι συνάρτηση της δομής των πολυωνύμων και της αραιότητάς τους (καλείται και αραιό όριο).

Για απολύτως πυκνά πολυώνυμα (μη μηδενικοί όλοι οι δυνατοί όροι) τα όρια Bernstein και Bézout συμπίπτουν. Υπάρχει μια επέκταση [ΗΣ97] στο ^{n}.

Παράδειγμα 10.3. Στη δομική βιολογία, μελετάμε τις διαμορφώσεις του κυκλοεξανίου, δηλ. ενός δακτυλίου έξι σημειακών μαζών, με 6 περιστρεφόμενους βαθμούς ελευθερίας. Από την γεωμετρία αποστάσεων ή την Ευκλείδειο γεωμετρία, κατασκευάζουμε ένα σύστημα 3×3 που περιγράφει τις δυνατές διαμορφώσεις:

$$f_i = \beta_{i1} + \beta_{i2}t_j^2 + \beta_{i3}t_k^2 + \beta_{i4}t_jt_k + \beta_{i5}t_j^2t_k^2, \qquad \{i,j,k\} = 0,1,2.$$

Οι μεταβλητές t_0, t_1, t_2 αντιστοιχούν στην εφαπτόμενη της μισής γωνίας των 3 αλγεβρικώς ανεξάρτητων γωνιών, οι οποίες καθορίζουν μια διαμόρφωση.

Το φράγμα Βέζουτ ισούται με $4^3 = 64$.

Το πολυομογενές φράγμα μ-Βέζουτ φράσσει το πλήθος ριζών στο $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. Οι βαθμοί των πολυωνύμων στις μεταβλητές t_0, t_1, t_2 είναι αντίστοιχα $(0,2,2), (2,0,2), (2,2,0)$. Το φράγμα ισούται με τον συντελεστή του $y_1y_2y_3$ στο

$$\prod_i (d_{i1}y_1 + d_{i2}y_2 + d_{i3}y_3) = \cdots + (2y_2+2y_3)(2y_1+2y_3)(2y_1+2y_2) + \cdots = \cdots + 2y_2 \cdot 2y_1 \cdot 2y_3 + 2y_3 \cdot 2y_1 \cdot 2y_2 + \cdots$$

δηλ. το φράγμα είναι 16.

Τέλος, θεωρούμε τα 3 πολύεδρα του Νεύτωνα Q_0, Q_1, Q_2. Είναι και τα 3 τετράγωνα, με μήκος ακμής 2, που βρίσκονται σε διαφορετικά επίπεδα, δηλ. στο επίπεδο των t_1t_2, των t_0t_2 και των t_0t_1 αντίστοιχα. Το άθροισμα Μινκοωσκι $Q_0 + Q_1 + Q_2$ είναι κύβος με μήκος ακμής 4 και όγκο $4^3 = 64$. Ο Μικτός Όγκος των 3 πολυέδρων είναι, από τον τύπο εγκλεισμού-αποκλεισμού,

$$V(Q_0+Q_1+Q_2) - \sum_{i \neq j} V(Q_i+Q_j) + \sum_i V(Q_i) = 4^3 - 3 \cdot 4 \cdot 2 \cdot 2 + 0 = 16,$$

όπου κάθε άθροισμα $Q_i + Q_j$ είναι ορθογώνιο παραλληλεπίπεδο με μήκος ακμών $4, 2, 2$.

Ορισμός 10.3. *Η κλασική απαλοίφουσα [Euler,Cayley,Sylvester,Bézout] αφορά στις προβολικές μιγαδικές ρίζες συνεπώς ο βαθμός της ως προς τους συμβολικούς συντελεστές του αρχικού συστήματος εξαρτάται από το όριο Βέζουτ, ενώ στον τύπο Ποισσον το A περιλαμβάνει όλες τις μιγαδικές προβολικές ρίζες.*

Στη θεωρία αραιής απαλοιφής, μελετάμε τορικά αλγεβρικά σύνολα T που ορίζονται από τα πολύεδρα του Νεύτωνα. Γενικά, κάθε T περιέχει το $(\mathbb{C}-\{0\})^n$ ως πυκνό υποσύνολο και βρίσκεται μέσα στο $\mathbb{P}^N$, όπου N το πλήθος όψεων στο άθροισμα Μινκοωσκι των πολυέδρων του Νεύτωνα. Άρα το T μπορεί να τέμνει τον προβολικό χώρο στο άπειρο για συγκεκριμένους, μη γενικούς συντελεστές.

Ορισμός 10.4. [CLO05, GKZ94, PS93] *Η αραιή απαλοίφουσα εκφράζει την ύπαρξη ριζών σε ένα τορικό αλγεβρικό σύνολο T συνεπώς ο βαθμός της συναρτάται από το όριο Βερνστειν ενώ $A \subset T$.*

$$M_s = \begin{bmatrix}
c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 & 0 & 0 & 0 & 0 \\
0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 \\
0 & 0 & 0 & 0 & 0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} \\
c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23}
\end{bmatrix}$$

Πίνακες της τορικής απαλοίφουσας

Μελετάμε αλγόριθμους κατασκευής πινάκων Newton για την τορική απαλοίφουσα. Οι γραμμές στην ομάδα $i = 1, \ldots, n+1$ ορίζονται από τα B_i, όπου B_i ανήκει στο διανυσματικό άθροισμα των πολυέδρων του Νεύτωνα των άλλων n πολυωνύμων. Οι στήλες αντιστοιχούν στα μονώνυμα C, υποσύνολο του διανυσματικού αθροίσματος όλων των $n+1$ πολυέδρων του Νεύτωνα.

Ο αλγόριθμος [**?**, **?**] χρησιμοποιεί το διανυσματικό άθροισμα των πολυέδρων του Νεύτωνα και κατασκευάζει πίνακες με διάσταση ίση με το πλήθος των ακέραιων σημείων σε μια απειροελάχιστη διατάραξη αυτού του αθροίσματος. Υπάρχει επίσης η βελτίωση των [CP93, Stu94].

Ο αλγόριθμος [**?**] είναι αυξητικός (incremental) και δοκιμάζει διαδοχικούς ορθογώνιους πίνακες μέχρι να βρεθεί κάποιος με πλήρη τάξη (rank) για γενικούς συντελεστές, οπότε και επιλέγεται ένας τετράγωνος υποπίνακας γενικά μη αντιστρέψιμος. Τυπικά, ο αυξητικός δίνει μικρότερους πίνακες από τον προηγούμενο αλγόριθμο.

Ο πίνακας Newton ταυτίζεται με τον πίνακα των συντελεστών, τον πίνακα Sylvester ή Macaulay εάν, αντίστοιχα, το σύστημα είναι γραμμικό, περιέχει 2 πολυώνυμα, ή τα πολυώνυμα είναι απολύτως πυκνά.

Παράδειγμα 10.4. (συνέχεια παραδείγματος 10.3) Μελετάμε τις διαμορφώσεις του κυκλοεξανίου με αλγεβρικό σύστημα 3×3 (παρατηρήστε την αρίθμηση των εξισώσεων f_1, f_2, f_3):

$$f_i = \beta_{i1} + \beta_{i2} t_j^2 + \beta_{i3} t_k^2 + \beta_{i4} t_j t_k + \beta_{i5} t_j^2 t_k^2, \qquad \{i, j, k\} = 1, 2, 3.$$

Για τη χρήση της απαλοίφουσας θεωρούμε τα 3 πολυώνυμα ως πολυώνυμα σε 2 μεταβλητές t_1, t_2 και συντελεστές $c_{ij} \in [t_3]$:

$$\begin{aligned}
f_1 &= c_{11} + c_{12} t_2 + c_{13} t_2^2 = 0, \\
f_2 &= c_{21} + c_{22} t_1 + c_{23} t_1^2 = 0, \\
f_3 &= c_{31} + c_{32} t_2^2 + c_{33} t_1 t_2 + c_{34} t_1^2 + c_{35} t_1^2 t_2^2 = 0.
\end{aligned} \tag{10.1}$$

Ο βαθμός της αραιής απαλοίφουσας στα c_{1j} είναι $\mathrm{MO}(f_2, f_3) = 4$, όπου τα αντίστοιχα πολύεδρα Νεύτωνα είναι ένα ευθύγραμμο τμήμα κι ένα τετράγωνο στο ^{2}. Ομοίως και για το βαθμό στα c_{2j}. Ο βαθμός της αραιής απαλοίφουσας στα c_{3j} είναι 4 διότι τα f_1, f_2 έχουν πολύγωνα Νεύτωνα 2 κάθετα ευθύγραμμα τμήματα. Αρα ο βέλτιστος πίνακας τύπου Σψλεστερ θα είχε μέγεθος 12×12.

Και οι 2 παραπάνω αλγόριθμοι (με χρήση υποδιαίρεσης του αθροίσματος Μινκοωσκι κι ο αυξητικός) παράγουν τον παρακάτω πίνακα 16×16:

Οι στήλες του πίνακα αντιστοιχούν στους εξής όρους:

$$\left[1, t_2, t_2^2, t_2^3, t_1, t_1t_2, t_1t_2^2, t_1t_2^3, t_1^2, t_1^2t_2, t_1^2t_2^2, t_1^2t_2^3, t_1^3, t_1^3t_2, t_1^3t_2^2, t_1^3t_2^3\right].$$

Κλείνουμε την ενότητα με στοιχεία χρήσιμα για τον αυξητικό αλγόριθμο, ειδικά τον έλεγχο ενός υποψήφιου πίνακα για το αν αποτελεί πίνακα της αραιής απαλοίφουσας. Έστω ορθογώνιος πίνακας M διαστάσεων $a \times c$, $a \geq c$, κατασκευασμένος από τον αυξητικό αλγόριθμο με πλήρη τάξη ο οποίος συνεπώς μας παρέχει έναν πίνακα Newton $c \times c$. Έστω T ένας αντιστρέψιμος πίνακας $t \times a$. Τότε ο $t \times c$ πίνακας TM έχει τις ιδιότητες ενός πίνακα απαλοίφουσας και επίσης παρέχει έναν πίνακα Newton. Θυμηθείτε (ενότητες **;;**, **;;**) πως $\mu(\lambda)|\chi(\lambda) = \det(M - \lambda I)$ ενώ τα δυο πολυώνυμα (ελάχιστο και χαρακτηριστικό) ισούνται αν και μόνο αν όλες οι ιδιοτιμές έχουν μοναδιαία πολλαπλότητα. Φυσικά, $\det A = 0$ αν και μόνο αν είναι μηδέν ο σταθερός όρος του $\chi(x)$ ή, ισοδύναμα, του $\mu(x)$.

Βιβλιογραφία

[Ber75] D.N. Bernstein. The number of roots of a system of equations. *Funct. Anal. and Appl.*, 9(2):183–185, 1975. Translated from *Funktsional'nyi Analiz i Ego Prilozheniya,* 9(3):1–4, 1975.

[Béz79] E. Bézout. Théorie générale des équations algébriques. Paris, 1779.

[CLO05] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Number 185 in GTM. Springer, New York, 2nd edition, 2005.

[CP93] J. Canny and P. Pedersen. An algorithm for the Newton resultant. Technical Report 1394, Comp. Science Dept., Cornell University, 1993.

[DD01] C. D'Andrea and A. Dickenstein. Explicit formulas for the multivariate resultant. *J. Pure Appl. Algebra*, 164(1-2):59–86, 2001.

[Dix08] A.L. Dixon. The eliminant of three quantics in two independent variables. *Proc. London Math. Society*, 6:49–69, 209–236, 1908.

[EM00] M. Elkadi and B. Mourrain. Algorithms for residues and Lojasiewicz exponents. *J. Pure & Appl. Algebra*, 153:27–44, 2000.

[GKZ94] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser, Boston, 1994.

[HS97] B. Huber and B. Sturmfels. Bernstein's theorem in affine space. *Discr. and Computational Geometry*, 17(2):137–142, March 1997.

[Mac02] F.S. Macaulay. Some formulae in elimination. *Proc. London Math. Soc.*, 1(33):3–27, 1902.

[Mis93] B. Mishra. *Algorithmic Algebra*. Springer-Verlag, New York, 1993.

[PS93] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Zeitschrift*, 214:377–396, 1993.

[Rou99] F. Rouillier. Solving zero-dimensional polynomial systems through the rational univariate representation. *Applic. Algebra in Engineering, Communic. and Computing*, 9(5):433–461, 1999.

[Stu93] B. Sturmfels. Sparse elimination theory. In D. Eisenbud and L. Robbiano, editors, *Proc. Computat. Algebraic Geom. & Commut. Algebra 1991*, pages 264–298, Cortona, Italy, 1993. Cambridge Univ. Press.

[Stu94] B. Sturmfels. On the Newton polytope of the resultant. *J. of Algebr. Combinatorics*, 3:207–236, 1994.

[Tsi06] E.P. Tsigaridas. *Algebraic algorithms and applications in computational geometry*. PhD thesis, Dept. Informatics & Telecoms, National U. Athens, Greece, 2006. In greek.

[Yap00] C.K. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, New York, 2000.

[Zip93] R. Zippel. *Effective Polynomial Computation*. Kluwer Academic Publishers, Boston, 1993.