ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΜΣ ΥΠΟΛΟΓΙΣΤΙΚΗ ΕΠΙΣΤΗΜΗ

Εργασία για το μάθημα: «*Αλγόριθμοι & Πολυπλοκότητα*»

Διδάσκων: *Ηλίας Κουτσουπιάς*

Χειμερινό Εξάμηνο 2006-2007

Ο Αλγόριθμος Buchberger

για την εύρεση βάσεων Groebner ιδεωδών πολυωνύμων

Κωνσταντίνα Ρουφικτού
k.royfiktoy@di.uoa.gr

Άγγελος Μαντζαφλάρης
amantzaf@math.uoa.gr

Ιανουάριος 2007

Περίληψη

Μια πληθώρα προβλημάτων καταλήγει σε συστήματα πολυωνύμων πολλών μεταβλητών. Η αντιμετώπιση τέτοιων συστημάτων δεν είναι εύκολη υπόθεση· μια πλήρης θεωρία για τη μελέτη τους είναι η θεωρία των βάσεων Groebner. Ο αλγόριθμος του Buchberger μετατρέπει ένα σύνολο πολυωνύμων σε κάποιο άλλο - τη βάση Groebner του συστήματος - το οποίο αποκαλύπτει όλη την κρυμμένη πληροφορία του αρχικού συστήματος και διευκολύνει τη μελέτη του, έως και την τελική επίλυση. Ένας τόσο ισχυρός αλγόριθμος δε μπορεί παρά να είναι (τουλάχιστον) εκθετικός. Παρόλα αυτά η αξία του είναι μεγάλη, τόσο από θεωρητική σκοπιά, όσο και στις εφαρμογές, που απλώνονται σε ρομποτική, θεωρία αποδείξεων, επιχειρησιακή έρευνα ή οπουδήποτε αλλού υπεισέρχονται πολυωνυμικές εξισώσεις.

I. Εισαγωγή

Οι απαρχές της άλγεβρας και των αλγορίθμων χρονολογούνται στον μακρινό ένατο αιώνα. Στη Βαγδάτη, ο μαθηματικός *Mohammed Ibn Musa al-Khawarizmi* ερευνούσε πολυωνυμικές εξισώσεις κι έγραψε το διάσημο βιβλίο του *Kita Al-jabr wa'l Muqabala*. Το βιβλίο αναφέρεται σε συμβολικές μεθόδους για επίλυση πολυωνυμικών εξισώσεων. Μάλιστα, οι λέξεις *άλγεβρα* και *αλγόριθμοι* έχουν προέλθει από τις λέξεις *Al-jabr* και *al-Khawarizmi'yah* αντίστοιχα. Έως τη δεκαετία του 1960, η έρευνα στη σύγχρονη άλγεβρα στράφηκε σε κατασκευαστικές μεθόδους, δηλαδή στην ανάπτυξη *αλγεβρικών αλγορίθμων*. Με την άνθηση της υπολογιστικής επιστήμης δημιουργήθηκε η ανάγκη για μελέτη των αλγεβρικών αλγορίθμων και από υπολογιστική σκοπιά, πχ μελέτη της αποτελεσματικότητάς τους, της υλοποίησής τους και των υπολογιστικών πόρων που χρειάζονται. Αυτό οδήγησε στην εδραίωση της *Υπολογιστικής Άλγεβρας*, ένα πεδίο μελέτης που απλώνεται τόσο στα μαθηματικά όσο και στην πληροφορική. Σήμερα η συμβολή της *Υπολογιστικής Άλγεβρας* στην υπολογιστική επιστήμη και τις εφαρμογές της είναι μεγάλη. Ένα εξαιρετικό παράδειγμα αυτής της συμβολής είναι η θεωρία και οι αλγόριθμοι για τις βάσεις Groebner.

Οι βάσεις Groebner είναι μια μέθοδος υπολογισμών με πολυώνυμα πολλών μεταβλητών. Γενικεύουν την απαλοιφή Gauss για επίλυση γραμμικών συστημάτων και τον αλγόριθμο του Ευκλείδη για την εύρεση του μέγιστου κοινού διαιρέτη πολυωνύμων μιας μεταβλητής. Φανταστείτε τους αλγορίθμους αυτούς να εφαρμόζονται με είσοδο όχι γραμμικά συστήματα ή πολυώνυμα μιας μεταβλητής, αλλά γενικά πολυώνυμα πολλών μεταβλητών. Η γενίκευση αυτή υπάρχει και λέγεται αλγόριθμος Buchberger: Ο αλγόριθμος έχει είσοδο ένα σύνολο πολυωνύμων $F = \{f_1, \ldots, f_n\}$ και δίνει στην έξοδο ένα διαφορετικό σύνολο πολυωνύμων $G = \{g_1, \ldots, g_m\}$, που καλείται βάση Groebner του συστήματος. Το σύνολο αυτό διατηρεί όλην την (αλγεβρική και γεωμετρική) πληροφορία του αρχικού συνόλου F(πχ το σύνολο των λύσεων του συστήματος παραμένει το ίδιο), και μάλιστα όλες οι πληροφορίες οι οποίες ήταν κρυμμένες στο F αποκαλύπτονται στο G.

Η ιδέα πίσω από τις βάσεις Groebner ξεκινά από την εποχή του David Hilbert. Ο Hilbert απέδειξε πως υπάρχουν τέτοια σύνολα σαν το G, όμως η απόδειξη που έδωσε δεν ήταν κατασκευαστική. Το κενό αυτό ήρθε να γεμίσει αργότερα ο Αυστριακός μαθηματικός Bruno Buchberger, όταν στη διδακτορική του διατριβή το 1965 διατύπωσε τον ομώνυμο αλγόριθμο. Η σημερινή μορφή της θεωρίας των βάσεων Groebner οφείλεται σε αυτόν 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.

Η πρωτότυπη εργασία [1] του Buchberger είναι γραμμένη στα γερμανικά, ενώ πρόσφατα δημοσιεύθηκε μια μετάφραση στα αγγλικά [2]. Μια μεταγενέστερη εργασία του ιδίου γραμμένη στα αγγλικά είναι η [3] . Ένα επιτυχημένο σύγγραμμα για τη θεωρία των βάσεων Groebner, στο οποίο παραπέμπουμε τον αναγνώστη για αποδείξεις των θεωρημάτων που παρουσιάζονται στα παρακάτω, είναι το [8].

Στην ενότητα II δίνουμε το απαραίτητο υπόβαθρο για την κατανόηση του αλγορίθμου, ενώ στην ενότητα III παρουσιάζουμε τον αλγόριθμο Buchberger με μια σύντομη μελέτη της ορθότητας και της πολυπλοκότητάς του. Τέλος, στην ενότητα IV δίνουμε μερικά παραδείγματα εφαρμογών, ώστε ο αναγνώστης να εκτιμήσει την αξία του αλγορίθμου.

II. Θεωρία βάσεων Groebner

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 με n αγνώστους(μεταβλητές):

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

όπου $f_i \in \mathbb{F}[x_1, x_2, ..., x_n]$, δηλαδή πολυώνυμα με μεταβλητές $x_1, x_2, ..., x_n$ και συντελεστές από κάποιο σύνολο $\mathbb{F}$ (πχ $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

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

α) Αν το σύστημα είναι γραμμικό, δηλαδή αποτελείται από γραμμικά πολυώνυμα*, τότε η επίλυση μπορεί να γίνει αποτελεσματικά με τη μέθοδο απαλοιφής του Gauss.

β) Αν το σύστημα έχει μόνο μία μεταβλητή, δηλαδή $n = 1$, ουσιαστικά έχουμε να βρούμε τις ρίζες ενός πολυωνύμου, του ΜΚΔ$(f_1, \ldots, f_m)$. Το τελευταίο υπολογίζεται με τον αλγόριθμο του Ευκλείδη, και υπάρχουν αλγόριθμοι για τον εντοπισμό των ριζών του.

Μια βάση Groebner στην περίπτωση γραμμικών συστημάτων είναι τα πολυώνυμα(τριγωνικό σύστημα) που βρίσκουμε εκτελώντας απαλοιφή Gauss, ενώ στην περίπτωση πολυωνύμων μιας μεταβλητής, μια βάση Groebner είναι ο μέγιστος κοινός διαιρέτης του συστήματος.

Ορισμός 1. *Έστω το σύνολο $\mathbb{F}[x_1, x_2, ..., x_n]$ των πολυωνύμων με n μεταβλητές. 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

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

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. Λέμε ότι το μονώνυμο $\underset{\sim}{x}{}^{\alpha}$ *διαιρεί* το $\underset{\sim}{x}{}^{\beta}$ αν το $\underset{\sim}{x}{}^{\beta}$ γράφεται σαν $\underset{\sim}{x}{}^{\gamma} \cdot \underset{\sim}{x}{}^{\alpha}$ για κάποιο τρίτο μονώνυμο $\underset{\sim}{x}{}^{\gamma}$(προσέξτε ότι στον ορισμό του μονωνύμου δεν επιτρέπονται αρνητικοί εκθέτες).

Διαίρεση σε πολλές μεταβλητές

Η πράξη της διαίρεσης μεταξύ πολυωνύμων πολλών μεταβλητών είναι καθοριστικής σημασίας για τα επόμενα. Υπενθυμίζουμε ότι στα πολυώνυμα μιας μεταβλητής, για να γίνει η διαίρεση χρειαζόμαστε ένα διαιρετέο $f(x) \in \mathbb{F}[x]$ και ένα διαιρέτη $g(x) \in \mathbb{F}[x]$ με $g(x) \neq 0$. Αφού διατάξουμε τα μονώνυμα του διαιρετέου και τα μονώνυμα του διαιρέτη χρησιμοποιώντας την φυσική διάταξη των δυνάμεων των μονωνύμων, εκτελούμε τη γνωστή μας διαδικασία και λαμβάνουμε

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

Κάτι που πρέπει να τονισθεί ιδιαίτερα εδώ είναι ότι το πηλίκο $\pi(x)$ και το υπόλοιπο $\upsilon(x)$ είναι μοναδικά.

Στα πολυώνυμα μιας μεταβλητής δεν υπάρχει αμφιβολία για το ποιος είναι ο μεγιστοβάθμιος όρος. Όμως ποιος είναι ο μεγιστοβάθμιος του $f(x, y) = y^3x + x^3y$; Για τη διαίρεση πολυωνύμων με n μεταβλητές θα χρειαστεί να ορίσουμε έναν μεγιστοβάθμιο όρο σε κάθε πολυώνυμο. Έτσι χρειαζόμαστε κάποια διάταξη στα μονώνυμά του. Η πιο απλή διάταξη είναι η «λεξικογραφική».

*Ένα γραμμικό πολυώνυμο με n μεταβλητές είναι της μορφής $\alpha_1x_1 + \alpha_2x_2 + \cdots + \alpha_nx_n$

Ορισμός 2. *Στο σύνολο* $\mathbb{Z}^n_{\geq 0} = \{(\alpha_1, \alpha_2, ..., \alpha_n) | \ \alpha_i \in \{0, 1, ...\}\}$ *ορίζουμε την απλή λεξικογραφική διάταξη ως εξής:* $(\alpha_1, \alpha_2, ..., \alpha_n) >_{\lambda\varepsilon\xi} (\beta_1, \beta_2, ..., \beta_n) \Leftrightarrow \alpha_1 > \beta_1$ *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.*

Επιλέγοντας μια διάταξη στις μεταβλητές, πχ θεωρώντας $x > y$, επάγεται μια λεξικογραφική διάταξη στα μονώνυμα, πχ $1 <_{\lambda\varepsilon\xi} y <_{\lambda\varepsilon\xi} y^2 <_{\lambda\varepsilon\xi} y^3 <_{\lambda\varepsilon\xi} \cdots <_{\lambda\varepsilon\xi} x <_{\lambda\varepsilon\xi} xy <_{\lambda\varepsilon\xi} \cdots <_{\lambda\varepsilon\xi} x^2 \ldots$. Παρατηρήστε πως σε πολυώνυμα μιας μεταβλητής υπήρχε μια και μοναδική διάταξη που μπορούσαμε να χρησιμοποιήσουμε. Εδώ οι επιλογές είναι αρκετά περισσότερες. Μια άλλη διάταξη είναι η βαθμωτή:

Ορισμός 3. *Στο σύνολο* $\mathbb{Z}^n_{\geq 0} = \{(\alpha_1, \alpha_2, ..., \alpha_n) | \ \alpha_i \in \{0, 1, ...\}\}$ *ορίζουμε τη βαθμωτή λεξικογραφική διάταξη ως:*

$$(\alpha_1, \alpha_2, ..., \alpha_n) >_{\beta\alpha\vartheta} (\beta_1, \beta_2, ..., \beta_n) \iff \sum \alpha_i > \sum \beta_i \ \ \eta \ \ \sum \alpha_i = \sum \beta_i \ \ \& \ \ \alpha >_{\lambda\varepsilon\xi} \beta$$

δηλαδή λαμβάνουμε ένα επιπλέον κριτήριο πρώτα, τον ολικό βαθμό του μονωνύμου, πχ αν $x > y$ είναι $1 <_{\beta\alpha\vartheta} y <_{\beta\alpha\vartheta} x <_{\beta\alpha\vartheta} y^2 <_{\beta\alpha\vartheta} xy <_{\beta\alpha\vartheta} x^2 \ldots$

Ορισμός 4. *Σε κάθε πολυώνυμο* $f \in \mathbb{F}[\underset{\sim}{x}]$ *έχουμε ένα μεγιστοβάθμιο όρο (σύμφωνα με τη διάταξη που εφαρμόζουμε) και τον συμβολίζουμε* $MO(f)$.

Όπως συνηθίζεται και στα πολυώνυμα μιας μεταβλητής, μπορούμε να διατάξουμε τους όρους ενός πολυωνύμου πολλών μεταβλητών κατά φθίνοντα βαθμό. Επιπλέον σε κάθε πολυώνυμο f επισυνάπτεται ένας βαθμός $\deg(f) = (\delta_1, \ldots, \delta_n)$, και μπορούμε να συγκρίνουμε δυο πολυώνυμα ως προς το βαθμό τους.

Ίσως χρησιμοποιήσουμε και τις συντομογραφίες $M\Sigma(f)$ και $MM(f)$ για το μεγιστοβάθμιο συντελεστή και το μεγιστοβάθμιο μονώνυμο του f αντίστοιχα, δηλαδή θα είναι $MO(f) = M\Sigma(f) \cdot MM(f)$.

Ορίζουμε τώρα μία διαδικασία διαίρεσης έτσι ώστε δοθέντων των πολυωνύμων g και $f_1, f_2, \ldots, f_m$(με συγκεκριμένη σειρά), κι αφού σταθεροποιήσουμε μια διάταξη στις μεταβλητές, ο αλγόριθμος να δίνει μια γραφή του πολυωνύμου g ως $g = \pi_1 f_1 + \pi_2 f_2 + \cdots + \pi_m f_m + \upsilon$. Το πολυώνυμο $\upsilon(\underset{\sim}{x})$ καλείται *υπόλοιπο της διαίρεσης* και η διατεταγμένη m-άδα πολυωνύμων $(\pi_1, \pi_2, \ldots, \pi_m)$ *πηλίκο της διαίρεσης*. Ο αλγόριθμος είναι:

1. Αρχικοποίησε $\pi_i = 0, \ i = 1, \ldots, m$ και $\upsilon = 0$
2. Για $i = 1 \ldots n$,
3. Όσο $MO(f_i)$ διαιρεί $MO(g)$ θέσε $u = MO(g)/MO(f_i)$, $\pi_i = \pi_i + u$, $g = g - u f_i$
4. διαφορετικά θέσε $\upsilon = \upsilon + MO(g)$, $g = g - MO(g)$
5. Επανέλαβε τα 2,3,4 έως ότου $g = 0$

Για να γίνει πιο κατανοητή η διαδικασία παραθέτουμε μια τέτοια διαίρεση(με δυο μεταβλητές). Θεωρούμε την απλή λεξικογραφική διάταξη, με $x > y$. Διατάσσουμε τους όρους των πολυωνύμων κατά φθίνουσα σειρά σύμφωνα με τη διάταξη αυτή και ακολουθούμε τον αλγόριθμο ως εξής:

	$g(x,y) = \ 3x^{14}y^{10} + 5xy^3 - 6y^7 + 1$	$-2x^{12} + 4x^2y^4$	$= f_1(x,y)$
$\left[\frac{3x^{14}y^{10}}{-2x^{12}} = -\frac{3}{2}x^2y^{10}\right]$	$-3x^{14}y^{10} + 6x^4y^{14}$	$x^2 - y^{11}$	$= f_2(x,y)$
$\left[-2x^{12}\right.$ δε διαιρεί $\left.6x^4y^{14}\right]$	$6x^4y^{14} + 5xy^3 - 6y^7 + 1$	$-\frac{3}{2}x^2y^{10}$	$= \pi_1(x,y)$
$\left[\frac{6x^4y^{14}}{x^2} = 6x^2y^{14}\right]$	$-6x^4y^{14} + 6x^2y^{25}$	$6x^2y^{14} + 6y^{25}$	$= \pi_2(x,y)$
	$6x^2y^{25} + 5xy^3 - 6y^7 + 1$	$5xy^3 + 6y^{36} - 6y^7 + 1$	$= \upsilon(x,y)$
$\left[\frac{6x^2y^{25}}{x^2} = 6y^{25}\right]$	$-6x^2y^{25} + 6y^{36}$		
	$5xy^3 + 6y^{36} - 6y^7 + 1$		
$\left[x^2\right.$ δε διαιρεί $\left.5xy^3$ κτλ..$\right]$	0		

Άρα τελικά είναι

$$g(x,y) = (-\frac{3}{2}x^2y^{10}) \cdot f_1(x,y) + (6x^2y^{14} + 6y^{25}) \cdot f_2(x,y) + (5xy^3 + 6y^{36} - 6y^7 + 1)$$

Ο αλγόριθμος δεν είναι μονοσήμαντα ορισμένος: εξαρτάται από τη διάταξη ως προς την οποία επιλέγουμε τους μεγιστοβάθμιους όρους. Βλέπουμε ότι:

α) Ο αλγόριθμος τερματίζει, καθώς ο βαθμός του g στα βήματα 2,3 φθίνει γνήσια. Αν έχει σταθερό όρο, στο τελευταίο βήμα αφαιρείται και αυτός, και έχουμε $g = 0$.

β) Αν θεωρήσουμε το αποτέλεσμα της διαίρεσης, $g = \pi_1 f_1 + \pi_2 f_2 + \cdots + \pi_m f_m + \upsilon$, η διαδικασία δείχνει ότι $\deg(g) \geq \deg(\pi_i f_i), \quad \forall\ i = 1, 2, \ldots, m$.

γ) Το υπόλοιπο της διαίρεσης είναι και αυτό ένα πολυώνυμο. Σημειώστε πως αντίθετα με τα πολυώνυμα μιας μεταβλητής, εδώ δεν μπορούμε να εγγυηθούμε **μοναδικότητα του υπολοίπου**, αν αλλάξουμε τη σειρά των διαιρετών(πχ τροποποιώντας το βήμα 2 ως «Για $i = n \ldots 1$»).

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

Ιδεώδη πολυωνύμων και βάσεις Groebner

Είναι εύκολο να δούμε ότι τα δυο παρακάτω συστήματα[†] έχουν το ίδιο σύνολο λύσεων:

$$(\Sigma)\begin{cases} g(x_1, x_2, ..., x_n) = 0 \\ f_1(x_1, x_2, ..., x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, ..., x_n) = 0 \end{cases} \quad , \quad (\Sigma')\begin{cases} \upsilon(x_1, x_2, ..., x_n) = 0 \\ f_1(x_1, x_2, ..., x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, ..., x_n) = 0 \end{cases}$$

όπου υ το υπόλοιπο της διαίρεσης του g δια $(f_1, \ldots, f_m)$. Θα θέλαμε να συνεχίσουμε τις διαιρέσεις και τις απλοποιήσεις με έναν συστηματικό τρόπο, ώστε να αναπαραστήσουμε το σύστημα με μια απλούστερη μορφή, για να το επιλύσουμε πιο εύκολα. Σαν πρώτο βήμα για το σκοπό αυτό, ορίζουμε το *ιδεώδες*:

Ορισμός 5. *Το υποσύνολο $I \neq \varnothing$ του $\mathbb{F}[\underset{\sim}{x}]$ καλείται ιδεώδες πολυωνύμων, και συμβολίζουμε $I \lhd \mathbb{F}[\underset{\sim}{x}]$ εάν ισχύουν τα ακόλουθα :*

(α′) $f, g \in I \Rightarrow f - g \in I$

(β′) *Αν* $f \in I, h \in \mathbb{F}[\underset{\sim}{x}]$, *τότε* $f \cdot h \in I$

Θα λέμε ότι το ιδεώδες I παράγεται από τα $f_1, \ldots, f_m$, αν

$$I = \left\{ h_1 f_1 + h_2 f_2 + \cdots + h_m f_m \mid h_i \in \mathbb{F}[\underset{\sim}{x}] \right\}$$

Το σύνολο $\{f_1, \ldots, f_m\}$ καλείται μια *βάση* του I και συμβολίζουμε $I = \langle f_1, \ldots, f_m \rangle$.

Σκεφτείτε το ιδεώδες αυτό ως το «σύστημα» όλων των (απείρων) πολυωνύμων που μπορείτε να σκεφτείτε, έτσι ώστε το «σύστημα» να είναι ισοδύναμο με το αρχικό. Παρατηρήστε ότι αν διαιρέσουμε πχ το f_1 με τα επόμενα πολυώνυμα, δηλαδή

$$f_1 = h_2 f_2 + h_3 f_3 + \cdots + h_n f_n + \upsilon$$

και κατόπιν αντικαταστήσουμε στη βάση μας το f από το υπόλοιπο υ της διαίρεσης, βρίσκουμε μια άλλη βάση του ίδιου ιδεώδους, $I = \langle \upsilon, f_2, \ldots, f_m \rangle$. Αυτό αντανακλά την παρατήρηση που κάναμε στην αρχή.

[†]Παρατηρήστε πως στην περίπτωση που $n = 1$, η παρατήρηση αυτή οδηγεί στο γνωστό αποτέλεσμα ότι το σύστημα έχει λύσεις της ρίζες του ΜΚΔ$(f_1, \ldots, f_m)$, όπως φαίνεται από τον Ευκλείδειο αλγόριθμο εύρεσης του ΜΚΔ.

Συμπεραίνουμε ότι η μελέτη ενός πολυωνυμικού συστήματος ανάγεται στη μελέτη του ιδεώδους που παράγεται από τα πολυώνυμα του συστήματος. Αυτό που θα κάνουμε είναι να περιγράψουμε το ιδεώδες αυτό χρησιμοποιώντας, όχι τα αρχικά πολυώνυμα, αλλά βρίσκοντας μια διαφορετική βάση του ιδεώδους. Αυτή θα μας επιτρέψει να προσδιορίσουμε πιο εύκολα το σύνολο λύσεων του αρχικού συστήματος και γενικότερα να εξάγουμε εύκολα διάφορα συμπεράσματα για αυτό.

Το ερώτημα που γεννιέται είναι αν όλα τα ιδεώδη(χωρίς να τα υποθέτουμε παραγόμενα από κάποιο πεπερασμένο σύνολο) έχουν μια πεπερασμένη βάση. Απάντηση σε αυτό δίνει το περίφημο *θεώρημα βάσης του Hilbert*. Πριν το διατυπώσουμε ας δούμε μια σημαντική ειδική περίπτωση:

Ορισμός 6. *Έστω $\mathbb{F}[\underset{\sim}{x}]$ το σύνολο των πολυωνύμων n μεταβλητών, με συντελεστές από το σύνολο $\mathbb{F}$. Ένα* ***ιδεώδες μονωνύμων*** *του $\mathbb{F}[\underset{\sim}{x}]$, ένα ιδεώδες που παράγεται από μονώνυμα, δηλαδή*

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

Ένα μονώνυμο ανήκει σε ένα ιδεώδες μονωνύμων αν υπάρχει ένα άλλο μονώνυμο στη βάση του ιδεώδους που διαιρεί το μονώνυμο αυτό. Όπως φαίνεται στον ορισμό, τα μονώνυμα που παράγουν το I ενδέχεται να είναι άπειρα. Το *λήμμα του Dickson* μας λέει ότι πάντα υπάρχει ένα πεπερασμένο σύνολο γεννητόρων:

Λήμμα 1. *(Dickson) Έστω I ένα ιδεώδες μονωνύμων. Τότε το I έχει μια πεπερασμένη βάση από μονώνυμα, δηλαδή υπάρχουν k μονώνυμα: $\underset{\sim}{x}^{\beta_1}, \underset{\sim}{x}^{\beta_2}, \ldots, \underset{\sim}{x}^{\beta_k}$, που παράγουν το I, συμβολικά $I = \langle \underset{\sim}{x}^{\beta_1}, \underset{\sim}{x}^{\beta_2}, \ldots, \underset{\sim}{x}^{\beta_k} \rangle$.*

Μπορούμε τώρα να ορίσουμε τις βάσεις Groebner και να μελετήσουμε τις ιδιότητές τους. Η σημασία των βάσεων αυτών θα φανεί από τις ιδιότητες που έχουν. 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 (1)* 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 1. *(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 7. *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 (1) 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 2. *Έστω* $G = \{g_1, g_2, ..., g_\kappa\}$ *μια βάση Groebner ενός ιδεώδους* $I \lhd \mathbb{F}[\underset{\sim}{x}]$ *και* $f \in \mathbb{F}[\underset{\sim}{x}]$. *Τότε εκτελώντας τη διαίρεση του* f *δια* G *με οποιαδήποτε σειρά των* g_i*:*

$$f = h_1 g_1 + h_2 g_2 + \cdots + h_\kappa g_\kappa + \upsilon$$

το $\upsilon(\underset{\sim}{x})$ *είναι πάντα το ίδιο πολυώνυμο.*

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 σειρά 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. *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 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 3. *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).

Εφαρμογές των βάσεων Groebner

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 2. *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($\pi\chi\ x_1 > \cdots > x_n$) 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 4. *Ένα σύστημα πολυωνύμων F είναι αδύνατο(δεν έχει λύσεις) αν και μόνο αν η ανηγμένη βάση Groebner είναι το μονοσύνολο $\{1\}$, δηλαδή $I = \langle F \rangle = \langle 1 \rangle = \mathbb{F}[\underset{\sim}{x}]$.*

III. Ο Αλγόριθμος του Buchberger

Είδαμε ότι κάθε ιδεώδες έχει μια βάση Groebner. Πως όμως μπορεί να προσδιοριστεί μια τέτοια βάση;

Ορισμός 10. *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 3. *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 5. *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.

Ορθότητα

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 5.

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 (1), 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.

Πολυπλοκότητα

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 [10].

Οι Mayr & Meyer έδειξαν το 1982 ότι το πρόβλημα του ανήκειν είναι EXPSPACE-complete[11]. 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)[12]:

Θεώρημα 6. *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 (1)). 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 (6) 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.

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 [6].

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$(\text{MO}(p), \text{MO}(p))$ 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 [7].

γ) Παρατήρηση Buchberger II: Αν τα $\text{MM}(p)$ και $\text{MM}(q)$ 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 $\text{MO}(h)$ διαιρεί το ΕΚΠ$(\text{MO}(p), \text{MO}(q))$

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.

IV. Εφαρμογές

Πέρασαν αρκετά χρόνια από την ανακάλυψη του αλγορίθμου μέχρι να γίνει γνωστή η χρησιμότητά του σε μια πληθώρα διαφορετικών προβλημάτων. Μόλις τη δεκαετία του ΄90 η θεωρία άρχισε να εφαρμόζεται σε άλλους κλάδους πέρα από την *Αλγεβρική Γεωμετρία* και τη *Μεταθετική Άλγεβρα*. Μέχρι σήμερα έχουν δημοσιευθεί εκατοντάδες εργασίες, κάθε μια από τις οποίες προσθέτει μια νέα εφαρμογή στον αλγόριθμο Buchberger.

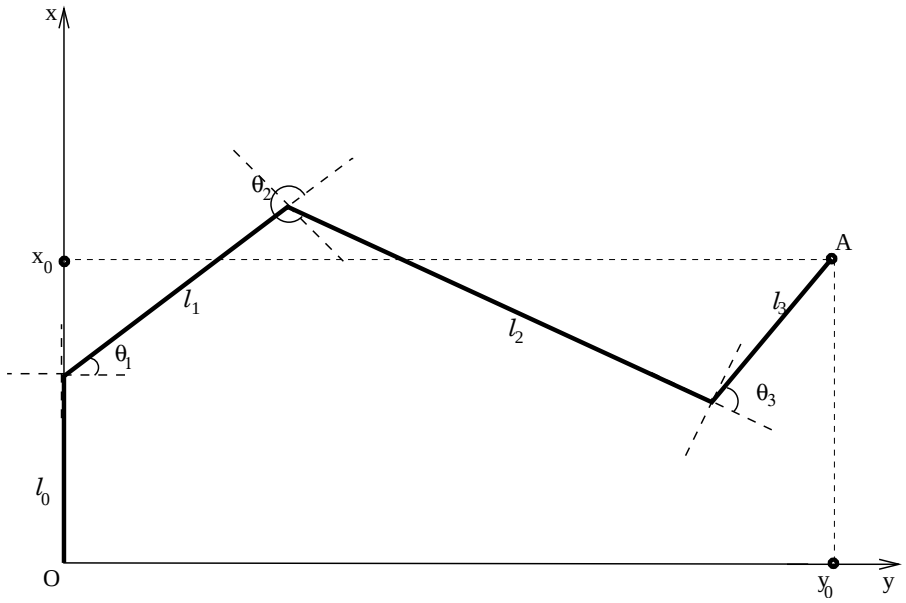
Θα δούμε τρεις από αυτές τις εφαρμογές, από τρεις φαινομενικά ασύνδετους κλάδους: ρομποτική, θεωρία αποδείξεων, επιχειρησιακή έρευνα.

Ρομποτική: Ευθύ κινηματικό πρόβλημα

Στο ευθύ κινηματικό πρόβλημα(forward kinematic problem) μας δίνεται ένα ρομπότ και ένα σημείο του χώρου. Ζητείται η θέση του ρομπότ ώστε το άκρο του να φτάσει το σημείο αυτό. Στην εφαρμογή θα ασχοληθούμε με ένα «επίπεδο» ρομπότ, με έναν σταθερό βραχίονα μήκους l_0 και άλλους τρεις $l_1,\ l_2,\ l_3$ που μπορούν να κινηθούν ελεύθερα.

Θεωρούμε ένα κύριο σύστημα συντεταγμένων Oxy και ένα σταθερό βραχίονα, με μήκος l_0 κάθετο στον x-άξονα, ο οποίος στηρίζεται στο σημείο O. Επίσης στο άκρο κάθε βραχίονα l_1, l_2 θεωρούμε κινητά συστήματα συντεταγμένων με αρχή το άκρο του βραχίονα και τον x_i-άξονα παράλληλο στο l_i.

Θα μελετήσουμε το ευθύ κινηματικό πρόβλημα, δηλαδή δεδομένων των συντεταγμένων (x_0, y_0) ενός σημείου A στο κύριο σύστημα συντεταγμένων, ποια θέση πρέπει να πάρει κάθε βραχίονας ώστε το άκρο του l_3 να συμπέσει με το δοσμένο σημείο. Για το σκοπό αυτό θεωρούμε την γωνία που σχηματίζει κάθε βραχίονας με τον x_i-άξονα του προηγούμενου βραχίονα, κατά τη θετική φορά. Η κατάσταση φαίνεται στο παρακάτω σχήμα.



Σημειώνουμε πως στο άκρο του l_0 θεωρούμε απλώς τη μεταφορά του κύριου συστήματος Oxy κατά ένα διάνυσμα $(0, l_0)$.

Με στοιχειώδη τριγωνομετρία βρίσκουμε τις συντεταγμένες του (x_0, y_0) συναρτήσει των γωνιών $\theta_1, \theta_2, \theta_3$:

$$\begin{aligned} x_0 &= l_1\cos\theta_1 + l_2\cos(\theta_1+\theta_2) + l_3\cos(\theta_1+\theta_2+\theta_3) \\ y_0 &= l_0 + l_1\sin\theta_1 + l_2\sin(\theta_1+\theta_2) + l_3\sin(\theta_1+\theta_2+\theta_3) \end{aligned}$$

Άρα η κατάσταση του ρομπότ καθορίζεται πλήρως από τις γωνίες $\theta_1,\ \theta_2,\ \theta_3$, ενώ για να πραγματοποιηθεί μια κίνηση από τη θέση A σε μια νέα θέση B, με γωνίες ϕ_1, ϕ_2, ϕ_3 αρκεί να υπολογιστούν οι γωνίες

αυτές(αν υπάρχουν) και κατόπιν να πραγματοποιηθεί στροφή κάθε βραχίονα l_i κατά γωνία $\phi_i - \theta_i$. Η θέση B δεν είναι εφικτή από το ρομπότ αν δεν υπάρχουν τέτοιες γωνίες, ώστε το άκρο του να συμπίπτει με το σημείο B.

Θα προσεγγίσουμε το ευθύ κινηματικό πρόβλημα ορίζοντας κατάλληλες μεταβλητές ώστε να αναγάγουμε το πρόβλημα ύπαρξης και εύρεσης των γωνιών $\theta_1,\ \theta_2,\ \theta_3$ στην επίλυση ενός πολυωνυμικού συστήματος. Θέτουμε:

$$\begin{aligned} x_1 &= \sin\theta_1 & y_1 &= \cos\theta_1 \\ x_2 &= \sin\theta_2 & y_2 &= \cos\theta_2 \\ x_3 &= \sin\theta_3 & y_3 &= \cos\theta_3 \end{aligned}$$

και χρησιμοποιούμε τις τριγωνομετρικές ταυτότητες του αθροίσματος γωνιών:

$$\begin{aligned} \cos(\theta_1+\theta_2) &= y_1y_2 - x_1x_2 \\ \sin(\theta_1+\theta_2) &= x_1y_2 + x_2y_1 \\ \cos(\theta_1+\theta_2+\theta_3) &= y_3\cos(\theta_1+\theta_2) - x_3\sin(\theta_1+\theta_2) \\ &= y_3(y_1y_2 - x_1x_2) - x_3(x_1y_2 + x_2y_1) \\ \sin(\theta_1+\theta_2+\theta_3) &= y_3\sin(\theta_1+\theta_2) + x_3\cos(\theta_1+\theta_2) \\ &= y_3(x_1y_2 + x_2y_1) + x_3(y_1y_2 - x_1x_2) \end{aligned}$$

Αντικαθιστώντας:

$$\begin{aligned} x_0 &= l_1y_1 + l_2(y_1y_2 - x_1x_2) + l_3(y_3y_1y_2 - y_3x_1x_2 - x_3x_1y_2 - x_3x_2y_1) \\ y_0 &= l_0 + l_1x_1 + l_2(x_1y_2 + x_2y_1) + l_3(y_3x_1y_2 + y_3x_2y_1 + x_3y_1y_2 - x_3x_1x_2) \end{aligned}$$

και μετά από πράξεις:

$$\begin{aligned} x_0 &= -l_3x_1x_2y_3 - l_2x_1x_2 - l_3x_1x_3y_2 - l_3x_2x_3y_1 + l_3y_1y_2y_3 + l_2y_1y_2 + l_1y_1 \\ y_0 &= -l_3x_1x_2x_3 + l_3x_1y_2y_3 + l_2x_1y_2 + l_1x_1 + l_3x_2y_1y_3 + l_2x_2y_1 + l_3x_3y_1y_2 + l_0 \end{aligned}$$

Λαμβάνοντας υπόψιν την τριγωνομετρική σχέση $\sin^2\theta + \cos^2\theta = 1$ παίρνουμε τις σχέσεις:

$$\begin{aligned} x_1^2 + y_1^2 &= 1 \\ x_2^2 + y_2^2 &= 1 \\ x_3^2 + y_3^2 &= 1 \end{aligned}$$

Τελικά φθάνουμε στο εξής πολυωνυμικό σύστημα:

$$(\Sigma)\begin{cases} f_1 = -l_3x_1x_2y_3 - l_2x_1x_2 - l_3x_1x_3y_2 - l_3x_2x_3y_1 + l_3y_1y_2y_3 + l_2y_1y_2 + l_1y_1 - x_0 = 0 \\ f_2 = -l_3x_1x_2x_3 + l_3x_1y_2y_3 + l_2x_1y_2 + l_1x_1 + l_3x_2y_1y_3 + l_2x_2y_1 + l_3x_3y_1y_2 + l_0 - y_0 = 0 \\ f_3 = x_1^2 + y_1^2 - 1 = 0 \\ f_4 = x_2^2 + y_2^2 - 1 = 0 \\ f_5 = x_3^2 + y_3^2 - 1 = 0 \end{cases}$$

η λύση του οποίου(στους πραγματικούς) με συγκεκριμένες παραμέτρους $l_0,\ l_1,\ l_2,\ l_3,\ x_0,\ y_0$ δίνει απάντηση στο ευθύ κινηματικό πρόβλημα.

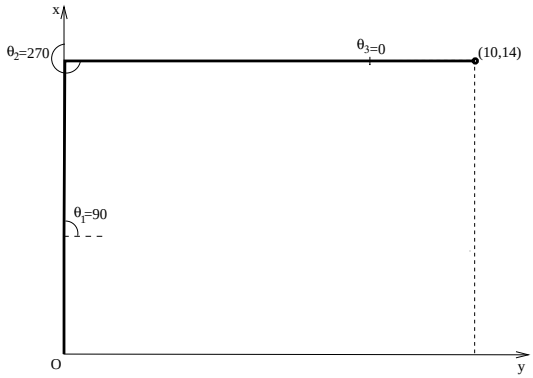
Συνεχίζουμε με ένα παράδειγμα. Με δεδομένα $(l_0, l_1, l_2, l_3) = (4, 6, 10, 4)$ χρησιμοποιήσαμε το υπολογιστικό πακέτο Maple για τον υπολογισμό της Ανηγμένης βάσης Groebner και την επίλυση του συστήματος.

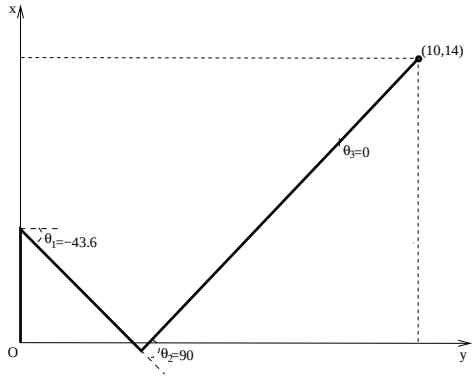
Παρακάτω φαίνονται μερικές απαντήσεις που πήραμε για συγκεκριμένα σημεία (x_0, y_0):

- $(x_0, y_0) = (14, 10)$. Πήραμε τις πραγματικές λύσεις:

$$(x_1, x_2, x_3, y_1, y_2, y_3) = (1, -1, 0, 0, 0, 1) \quad \text{ή} \quad (\frac{-20}{29}, 1, 0, \frac{21}{29}, 0, 1)$$

άρα έχουμε δυο τρόπους να φτάσουμε το $(14, 10)$. Μεταφράζοντας τις λύσεις σε γωνίες παίρνουμε $(\theta_1, \theta_2, \theta_3) = (90, -90, 0)$ και $(\theta_1, \theta_2, \theta_3) = (-43.6, 90, 0)$.

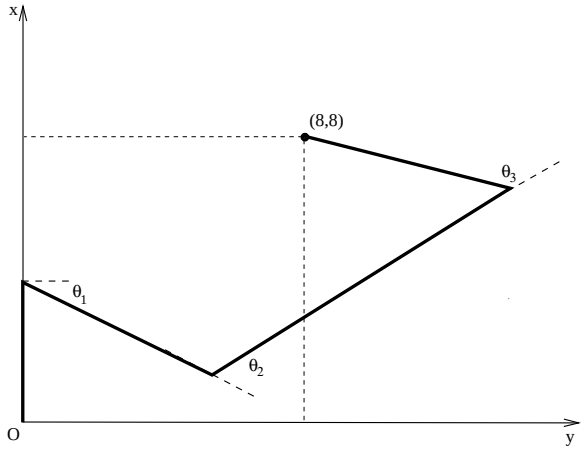




- $(x_0, y_0) = (8, 8)$. Πήραμε τις λύσεις:

$$\begin{aligned}(x_1, x_2, x_3, y_1, y_2, y_3) \quad = \quad & \left(\frac{3}{5}, \frac{-4}{5}, \frac{-4}{5}, \frac{-4}{5}, \frac{-3}{5}, \frac{3}{5}\right) \quad \text{ή} \quad \left(\frac{-3}{5}, \frac{4}{5}, \frac{-4}{5}, \frac{4}{5}, \frac{-3}{5}, \frac{-3}{5}\right) \\ & \text{ή} \quad \left(-1, \frac{4}{5}, \frac{4}{5}, 0, \frac{-3}{5}, \frac{3}{5}\right) \quad \text{ή} \quad \left(1, \frac{-4}{5}, \frac{4}{5}, 0, \frac{-3}{5}, \frac{-3}{5}\right)\end{aligned}$$

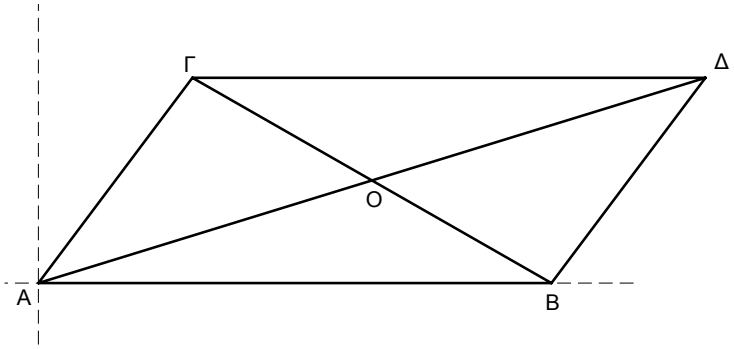
οπότε βρίσκουμε(προσεγγιστικά) τις γωνίες $(\theta_1, \theta_2, \theta_3) = (-33.7, 50, -53.1)$ ή $(-36.9, -50, 50)$ ή $(-90, -50, 53.1)$ ή $(90, 50, -50)$.



- $(x_0, y_0) = (5, 5)$. Η βάση Groebner είναι $G = \{1\}$, άρα δεν υπάρχουν λύσεις. Το σημείο δεν είναι εφικτό από το ρομπότ.

Θεωρία Αποδείξεων: Αυτοματοποιημένη απόδειξη γεωμετρικών θεωρημάτων

Θα εξετάσουμε αν ισχύει το θεώρημα: *Οι διαγώνιες του παραλληλογράμμου διχοτομούνται.*



Έστω $AB\Gamma\Delta$ ένα τυχόν παραλληλόγραμμο. Θα εκφράσουμε τις υποθέσεις και τα θεωρήματα με τη μορφή πολυωνύμων. Θεωρούμε σύστημα συντεταγμένων με αρχή το A. Είναι $B = (u_1, 0)$, $\Gamma = (u_2, u_3)$. Η κορυφή Δ ορίζεται μονοσήμαντα από τα άλλα τρία σημεία, άρα είναι $\Delta = (x_1, x_2)$, όπου τα x_1, x_2 είναι συναρτήσεις των u_i. Μια υπόθεση είναι ότι οι απέναντι πλευρές είναι παράλληλες, άρα οι ευθείες που τις περιέχουν θα έχουν τον ίδιο συντελεστή διεύθυνσης:

$$AB//\Gamma\Delta \Longrightarrow 0 = \frac{x_2 - u_3}{x_1 - u_2}$$

$$A\Gamma//B\Delta \Longrightarrow \frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1}$$

απαλοίφοντας τους παρονομαστές φτάνουμε στα πολυώνυμα

$$\begin{aligned} h_1 &= x_2 - u_3 = 0 \\ h_2 &= (x_1 - u_1)u_3 - x_2u_2 = 0 \end{aligned}$$

Επίσης τα A, O, Δ και B, O, Γ είναι συνευθειακά, αφού το O είναι η τομή των δυο διαγωνίων άρα,αν $O = (x_3, x_4)$, φτάνουμε στις σχέσεις:

$$AO//O\Delta \Longrightarrow \frac{x_4}{x_3} = \frac{u_3}{x_1}$$

$$BO//O\Gamma \Longrightarrow \frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1}$$

και τελικά

$$\begin{aligned} h_3 &= x_4x_1 - x_3u_3 = 0 \\ h_4 &= x_4(u_2 - u_1) - (x_3 - u_1)u_3 = 0 \end{aligned}$$

Το σύστημα $\{h_1, h_2, h_3, h_4\}$ αποτελεί μια αναπαράσταση των υποθέσεων του θεωρήματος.

Εκφράζουμε και τα συμπεράσματα του θεωρήματος σαν πολυώνυμα, με χρήση του Πυθαγορείου Θεωρήματος

$$AO = O\Delta \Longrightarrow x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2$$

$$BO = O\Gamma \Longrightarrow (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2$$

μετά από πράξεις τα συμπεράσματα είναι:

$$\begin{aligned} g_1 &= x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2 = 0 \\ g_2 &= 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 = 0 \end{aligned}$$

Το θεώρημα θα ισχύει, αν $g_1, g_2 \in \langle h_1, h_2, h_3, h_4 \rangle$. Καθώς όμως τα u_i επιλέχθηκαν τυχαία, θα θεωρήσουμε ως μεταβλητές μόνο τα x_i, δηλαδή βλέπουμε τα u_i σαν παραμέτρους των συντελεστών. Υπολογίζουμε την ανηγμένη βάση Groebner των $h_i \in \mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$:

$$G = \{-u_3 + 2x_4, 2 * x_3 - u_1 - u_2, x_2 - u_3, -u_1 - u_2 + x_1\}$$

και βλέπουμε ότι $\overline{g_1}^G = 0$ και $\overline{g_2}^G = 0$. Συμπεραίνουμε ότι το θεώρημα είναι ορθό.

Επιχειρησιακή έρευνα: ακέραιος προγραμματισμός

Στα προβλήματα ακέραιου προγραμματισμού θέλουμε να ελαχιστοποιήσουμε(ή να μεγιστοποιήσουμε) την τιμή ενός γραμμικού πολυωνύμου ενώ απαιτούμε οι τιμές των μεταβλητών να είναι ακέραιοι και να ικανοποιούν κάποιους περιορισμούς που εκφράζονται με γραμμικά πολυώνυμα. Θα δούμε πως μπορούμε να πετύχουμε κάτι τέτοιο χρησιμοποιώντας τις βάσεις Groebner με ένα παράδειγμα:

Ας θεωρήσουμε το πρόβλημα της αναπαράστασης ενός ποσού, πχ 117 ευρώ, με το μικρότερο αριθμό νομισμάτων, αν διαθέτουμε νομίσματα των 1, 5, 10, 20 ευρώ. Επειδή πρόκειται για αδιαίρετα νομίσματα, η λύση πρέπει να είναι μια τετράδα μη αρνητικών ακεραίων με ελάχιστο συνολικό άθροισμα. Έστω e ο αριθμός των νομισμάτων του ενός ευρώ, x τα παντάευρα, y τα δεκάευρα και z τα εικοσάευρα που θα χρησιμοποιήσουμε. Το πρόβλημα είναι ένα πρόβλημα ακέραιου προγραμματισμού:

$$\begin{aligned} \text{ελαχιστοποίηση της} \quad & e + x + y + z \\ \text{υπό τους περιορισμούς} \quad & e + 5x + 10y + 20z = 117 \\ & e, x, y, z \in \mathbb{Z}_{\geq 0} \end{aligned}$$

Ας θεωρήσουμε τις βασικές σχέσεις μεταξύ των νομισμάτων σαν ένα σύνολο πολυωνύμων του $\mathbb{Z}[e, x, y, z]$. Δηλαδή:

$$F = \{e^5 - x, e^{10} - y, e^{20} - z\}$$

πχ το $e^5 - x$ σημαίνει ότι 5 μονόευρα είναι ίσα με ένα πεντάευρο. Παρατηρήστε ότι πρόκειται για πολυώνυμα με δυο μονώνυμα το καθένα(διώνυμα). Σε αυτήν την περίπτωση η βάση Groebner θα αποτελείται κι αυτή από διώνυμα. Η ανηγμένη βάση Groebner του $I = \langle F \rangle$ είναι:

$$G = \{e^5 - x, x^2 - y, y^2 - z\}$$

Βλέπουμε ότι η G είναι ένα σύνολο άλλων κανόνων μεταξύ των νομισμάτων, το οποίο είναι ισοδύναμο με το αρχικό, πχ $y^2 - z$ σημαίνει ότι 2 δεκάευρα είναι ίσα με ένα εικοσάευρο. Ας θεωρήσουμε τώρα μια εφικτή λύση του προβλήματος, έστω $(17, 10, 5, 0)$, πράγματι $17 \cdot 1 + 10 \cdot 5 + 5 \cdot 10 + 0 \cdot 20 = 117$. Με τη μορφή μονωνυμου είναι το $e^{17}x^{10}y^5$. Θα χρησιμοποιήσουμε τους κανόνες της βάσης G έτσι ώστε με τοπικές μετακινήσεις προς καλύτερες αναπαραστάσεις του ποσού να φτάσουμε στο ολικό βέλτιστο(παρατηρήστε ότι η χρήση των Βάσεων Groebner εδώ είναι ανάλογη με την εκτέλεση του αλγορίθμου Simplex για γραμμικό προγραμματισμό). Είναι

$$e^{17}x^{10}y^5 \xrightarrow{e^5=x} e^2x^{13}y^5 \xrightarrow{x^2=y} e^2xy^{11} \xrightarrow{y^2=z} e^2xyz^5$$

Συμπεραίνουμε ότι η βέλτιστη λύση είναι $(2, 1, 1, 5)$.

Βιβλιογραφία

[1] B. Buchberger, *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal(German)*, Phd thesis, University of Innsbruck (Austria), 1965.

[2] B. Buchberger, *An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*(thesis english translation), Journal of Symbolic Computation, Volume 41, Issues 3-4, March-April 2006, pp. 475-511

[3] B. Buchberger *Groebner-Bases: An Algorithmic Method in Polynomial Ideal Theory*, Multidimensional Systems Theory - Progress, Directions and Open Problems in Multidimensional Systems, N.K. Bose (ed.), Chapter 6, pp. 184-232, 1985

[4] B. Buchberger, *An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations (German)*, Aequationes Mathematicae, vol. 4, no. 3, 1970, pp. 374383. English translation in [5].

[5] B. Buchberger, and F. Winkler, eds. *Grobner Bases and Applications*, volume 251 of London Mathematical Society Series. Proc. of the International Conference 33 Years of Groebner Bases. Cambridge University Press, 1998

[6] B. Buchberger, *A Criterion for Detecting Unnecessary Reductions in the Construction of Grobner Bases*, Lecture Notes in Computer Science, vol. 72. Springer-Verlag, 1979.

[7] A. Giovinni, T. Mora, G. Niesi, L. Robbiano, C. Traverso, *One sugar cube, please, or selection strategies in the Buchberger algorithm*, In S.M. Watt, editor, Proc. ISSAC'91, pp. 49-54. ACM Press, 1991

[8] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, 1996

[9] Δ. Βάρσος,Δ. Δεριζιώτης, Μ. Μαλιάκας, Σ. Παπασταυρίδης, Ε. Ράπτης, Ο. Ταλέλλη, *Μια εισαγωγή στην Άλγεβρα*, Σοφία, 2003

[10] C. Papadimitriou, *Computational Complexity*, Addison-Wesley, 1994.

[11] Mayr,*Membership in Polynomial Ideals over $\mathbb{Q}$ Is Exponential Space Complete*. TR 6/88, Fachbereich Informatik, Universitat Frankfurt, November 1988. Also in: Proceedings of STACS "89 (Paderborn, February 1618, 1989).

[12] Mayr, *On polynomial ideals, their complexity, and applications*. Technical Report TUM-I9520, Institut fur Informatik, TU Munchen (May 1995). Also in: Proceedings of 10th International Conference on Fundamentals of Computation Theory, FCT"95 (Dresden, August 1995). LNCS 965, pp. 89 105.

[13] Mayr, *It is on the boundary: Complexity considerations for polynomial ideals*. Proceedings of the International Conference on Theoretical Computer Science Exploring New Frontiers of Theoretical Informatics, IFIP TCS"2000 (Sendai, Japan, August 2000). LNCS 1872, p. 99.

[14] B. Kutzler & S. Stifter, *On the Application of Buchberger's Algorithm to Automated Geometry Theorem Proving*, Journal of Symbolic Computation, 2, pp.389–397.