Μάθημα 4

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.

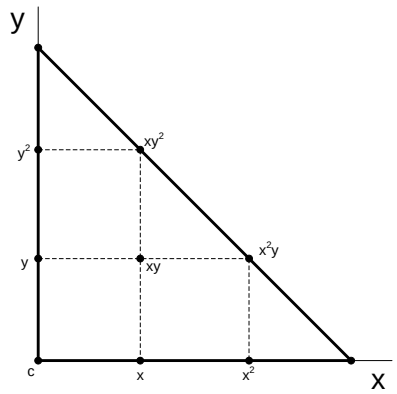
Από τον ορισμό της απαλοίφουσας που δόθηκε στα προηγούμενα λείπει μια σημαντική παράμετρος· δεν καθορίζεται ο χώρος των λύσεων, στον οποίο η απαλοίφουσα εκφράζει επιλυσιμότητα. Θα δούμε πως ο χώρος αυτός είναι ο προβολικός χώρος $\mathbb{P}^1$ στην περίπτωση μιας μεταβλητής. Στη γενική περίπτωση, το 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) ⇒ γενικά δεν υπάρχουν ρίζες.
- Πλήθος εξισώσεων = πλήθος μεταβλητών (καλώς ορισμένο) ⇒ 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) ⇒ 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 $F(\lambda \underline{x}) = \lambda^d F(\underline{x}), \ \ \forall \underline{x} \in \mathbb{F}^{n+1}$.*

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 παράγραφο 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 (3.1):

Θεώρημα 3.1. *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 4.1. [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* $\deg f_i$ *φράσεται 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 $14x = 31y$, $z = -\dfrac{13}{31}x$ και η προβολική ρίζα είναι $(31, 14, -13)$, η οποία αντιστοιχεί στη συνήθη ρίζα $\left(\dfrac{-31}{13}, \dfrac{-14}{13}\right)$.

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 4.2. *[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 4.3. *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 4.1. *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 $M\underset{\sim}{x} = b, \underset{\sim}{x} \in \mathbb{C}^n$, υπάρχει ρίζα αν και μόνο αν το σταθερό διάνυσμα $\underset{\sim}{b}$ 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 $\text{rank} < n+1$, 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 $\text{rank}(M) = 2$ 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 $\text{rank}(M) = n$ τότε υπάρχει μοναδική ρίζα, αλλιώς απειρία λύσεων.

Αν $\underset{\sim}{v} = [1, \alpha_0, \ldots, \alpha_n]^t$, το γινόμενο $M\underset{\sim}{v}$ είναι το διάνυσμα των τιμών πολυωνύμων στο σημείο v άρα (ανάμεσα) στα μη-μηδενικά διανύσματα που βρίσκονται στον πυρήνα του M υπάρχει το διάνυσμα $\underset{\sim}{y}$ 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.