ΚΕΦΑΛΑΙΟ 1^{ο}

Εισαγωγή

Στην παρούσα εργασία θα προσπαθήσουμε να παρουσιάσουμε ορισμένους τρόπους και αλγορίθμους για την εύρεση του Μέγιστου Κοινού Διαιρέτη . Αρχικά θα παρουσιάσουμε ορισμένες , προκαταρτικές έννοιες και ορισμούς οι οποίοι είναι απαραίτητη για την περαιτέρω μελέτη μας . Στο πρώτο μέρος της παρούσας εργασίας θα παρουσιάσουμε πως υπολογίζουμε τον Μέγιστο Κοινό Διαιρέτη σε αριθμούς και θα ασχοληθούμε με τον Ευκλείδειο αλγόριθμο. Επιπρόσθετα , υπάρχουν και ορισμένοι άλλοι αλγόριθμοι οι οποίοι μας βοηθούν στην εύρεση του ΜΚΔ ακεραίων αριθμών.

Στο δεύτερο μέρος της παρούσας εργασίας θα παρουσιαστούν η έννοια του Μέγιστου Κοινού Διαιρέτη για τα πολυώνυμα της μίας μεταβλητής και μέθοδοι εύρεσής του. Παράλληλα θα παρουσιαστούν και θα αναλυθούν ορισμένοι αλγόριθμοι οι οποίοι έχουν προταθεί για τον υπολογισμό του ΜΚΔ. Σε ορισμένους από αυτούς τους αλγόριθμους , θα υπάρχουν και παραδείγματα για να γίνει πιο κατανοητή η ερμηνεία τους. Επιπρόσθετα , με τα παραπάνω θα γίνει και μια εισαγωγή στην «κατά προσέγγιση» έννοια του Μέγιστου Κοινού Διαιρέτη για πολυώνυμα μιας μεταβλητής και θα παρουσιαστούν και διάφορες μέθοδοι για τον υπολογισμό του. Τέλος, στο τρίτο μέρος της εργασίας θα παρουσιαστούν οι αλγόριθμοι για τον υπολογισμό του Μέγιστου Κοινού Διαιρέτη πολυωνύμων με δύο μεταβλητές.

Ο υπολογισμός του Μέγιστου Κοινού Διαιρέτη είναι ένα από τα θεμελιώδη προβλήματα των αλγεβρικών υπολογισμών. Η έννοια του Μέγιστου Κοινού Διαιρέτη ενός συνόλου από πολυώνυμα είναι μια από τις κεντρικές έννοιες κάποιου, ο οποίος εξετάζει τις δομικές ιδιότητες των γραμμικών συστημάτων . Ο υπολογισμός του ΜΚΔ προσελκύει πολλούς επιστήμονες να τον ερευνήσουν .

Οι αλγεβρικοί υπολογισμοί σε μοντέλα τα οποία περιέχουν παραμέτρους μη ακριβείς μπορούν να ταξινομηθούν σε κανονικούς και σε μη γεννεσιακούς (normal and generic) υπολογισμούς . Οι αριθμητικοί υπολογισμοί οι οποίοι ασχολούνται από πού προέρχεται (την καταγωγή της) μιας προσεγγιστικής τιμής μιας ιδιότητας ,μιας συνάρτησης , η οποία είναι μη γεννεσιακή σε ένα δοσμένο σύνολο μοντέλων , αναφέρονται σαν μη γεννεσιακοί υπολογισμοί . Η δυσκολία στον υπολογισμό του ΜΚΔ ενός συνόλου από πολυώνυμα είναι ότι η ύπαρξη μη τετριμμένης λύσης (διαφορετικής της μονάδας) είναι μη γεννεσιακή (non- generic).

Όταν κάποιος ασχολείται με μοντέλα μηχανικών συστημάτων (engineering system models) , έχει από τη μια την αβεβαιότητα των πραγματικών τιμών των παραμέτρων που εξετάζει και από την άλλη στρογγυλοποιεί τα υπολογιστικά σφάλματα .Αυτά τα δύο θέματα κάνουν τον υπολογισμό του ΜΚΔ ένα δύσκολο

θέμα. Στην πράξη , κάποιος ενδιαφέρεται για κατάλληλες προσεγγιστικές λύσεις , παρά ακριβείς (γεννεσιακές) οι οποίες θα είναι αποτέλεσμα υπολογισμών . Βέβαια , οι προσεγγιστικές αυτές λύσεις θα πρέπει να προκύπτουν , αν στα κατάλληλα βήματα μειώνονται μη σημαντικά λάθη.

ΚΕΦΑΛΑΙΟ 2^{ο}

Μέγιστος Κοινός Διαιρέτης

2.1 Ο μέγιστος κοινός διαιρέτης και η « Θεωρία Αριθμών »

Η ``Θεωρία αριθμών`` είναι ο κλάδος των καθαρών μαθηματικών που ασχολείται με τις ιδιότητες των ακεραίων , καθώς και με προβλήματα που προκύπτουν από την μελέτη αυτή.

Διαιρέτης ενός αριθμού x ,είναι ένας αριθμός y ,ο οποίος διαιρεί τον x. Για παράδειγμα ένας διαιρέτης του 6 είναι το 2. Ο αριθμός ένα , είναι ειδική περίπτωση , καθώς είναι διαιρέτης όλων των αριθμών. Αν κάποιος αριθμός έχει ακριβώς δύο διαιρέτες, · δηλαδή τον εαυτό του και την μονάδα , θα καλείται ***πρώτος*** (prime number). Ανάμεσα σε δύο ή παραπάνω αριθμούς , μπορούν να υπάρχουν ένας ή περισσότεροι κοινοί διαιρέτες (common divisors). Για παράδειγμα , οι διαιρέτες του 12 είναι το 1, το 2, το 3, το 4, το 6, και το 12, ενώ οι διαιρέτες του 15 είναι το 1 ,το 3, το 5 και το 15. Όπως είναι αντιληπτό, το 12 και το 15 , έχουν ένα ζευγάρι κοινών διαιρετών , τους αριθμούς 1 και 3. Από τα παραπάνω προκύπτει ότι ο μέγιστός κοινός διαιρέτης του 12 και του 15 , είναι ο αριθμός 3 .

Μέγιστος κοινός διαιρέτης (greatest common divisor -god) δύο φυσικών αριθμών είναι ο μεγαλύτερος φυσικό αριθμός , ο οποίος διαιρεί και τους δύο χωρίς να αφήνει υπόλοιπο. Διαφορετικά , τον μέγιστο κοινό διαιρέτη δύο αριθμών ορίζουμε να είναι ο μεγαλύτερος από τους κοινούς τους διαιρέτες. Στην ξενόγλωσση βιβλιογραφία , υπάρχουν και συνώνυμες εκφράσεις όπως : μέγιστος κοινός παράγοντας (**GCF** : greatest common factor) , μεγαλύτερος κοινός παράγοντας (**HCF** : highest common factor) και σαν τη μεγαλύτερη κοινή ποσότητα (**GCM** : greatest common measure). Ο μέγιστος κοινός διαιρέτης, δύο αριθμών a και b συμβολίζεται ***ΜΚΔ (α , β)*** ή πιο απλά **(α , β)**. Ο μέγιστος κοινός διαιρέτης τριών ή περισσοτέρων αριθμών ισούται με τον μεγαλύτερο από τους κοινούς θετικούς διαιρέτες τους . Επίσης ισχύει : $ΜΚΔ(α ,β ,γ) = ΜΚΔ(α,ΜΚΔ (β , γ))=ΜΚΔ(ΜΚΔ(α ,β), γ) =ΜΚΔ(ΜΚΔ(α,γ), β)$

Αν ΜΚΔ (α , β) = 1 τότε οι αριθμοί α και β λέμε ότι είναι ***πρώτοι μεταξύ τους***. Η παραπάνω ιδιότητα είναι ανεξάρτητη από το γεγονός ένα ο $α$ ή ο $β$ πρώτοι αριθμοί , από μόνοι τους. Για παράδειγμα ούτε ο αριθμός 8 , ούτε ο αριθμός 9 είναι πρώτος , καθώς οι διαιρέτες του 8 είναι το 1 , το 2 , το 4 και το 8 , ενώ αντίστοιχα οι διαιρέτες του 9 είναι το 1 , το 3 και το 9. Εν τούτοις , όμως , οι αριθμοί 8 και 9 είναι πρώτοι

μεταξύ τους , επειδή ΜΚΔ (8,9)=1. Αυτό συμβαίνει γιατί ο μέγιστος κοινός τους διαιρέτης είναι η μονάδα.

Ας είναι ΜΚΔ (α , β) = μ . Επιπρόσθετα , ας υποθέσουμε , ότι οι αριθμοί α , β είναι πολλαπλάσιοι του μ($\alpha = \mu \cdot \lambda$ και ο $\beta = \mu \cdot \nu$) και ότι δεν υπάρχει μεγαλύτερος αριθμός $M > \mu$. Τότε οι αριθμοί λ , ν θα είναι πρώτοι μεταξύ τους· δηλαδή: ΜΚΔ(λ , ν) = 1 . Εξαιτίας , αυτού , οποιοσδήποτε άλλος αριθμός φ, ο οποίος διαιρεί και τον α, και τον β (φ/α και φ/β) , τότε θα διαιρεί και τον μ. Από τα παραπάνω προκύπτει , ότι ο μέγιστος κοινός διαιρέτης μ των αριθμών α και β να είναι ο κοινός διαιρέτης ο οποίος είναι διαιρέσιμος από οποιοδήποτε άλλο κοινό διαιρέτη φ.

Παράλληλα με τα παραπάνω , ο μέγιστος κοινός διαιρέτης δύο αριθμών α και , β μπορεί να οριστεί σαν το γινόμενο των κοινών τους παραγόντων(common prime factors) και με τον κάθε παράγοντα υψωμένο στον μικρότερο εμφανιζόμενο εκθέτη, αν οι αριθμοί αυτοί γραφούν στην κανονική τους μορφή (γινόμενο πρώτων παραγόντων) . Για παράδειγμα το 56 γράφεται σαν γινόμενο πρώτων παραγόντων $56 = 2 \times 2 \times 2 \times 7$,και το 42 αντίστοιχα :$42 = 2 \times 3 \times 7$. Σύμφωνα με την παραπάνω πρόταση , ο μέγιστος κοινός διαιρέτης των 56 και 42 θα είναι ίσος με το γινόμενο των κοινών πρώτων παραγόντων, δηλαδή : $14 = 2 \times 7$. Σε περίπτωση που οι δύο αριθμοί δεν έχουν κοινούς πρώτους παράγοντες , τότε αυτοί θα είναι πρώτοι μεταξύ τους.

Από τα παραπάνω γίνεται αντιληπτό ότι ,οι εφαρμογές του μέγιστου κοινού διαιρέτη στα μαθηματικά και κυρίως στην Άλγεβρα είναι πολλές. Αξίζει να σημειωθεί ενδεικτικά η Μπεζουτιανή ιδιότητα (Bezout's identity) . Η ιδιότητα αυτή ασχολείται με τον μέγιστο κοινό διαιρέτη , και του παρέχει την ιδιότητα του γεννήτορα ενός ιδεώδους (generator of the ideal) . Αυτός ο ορισμός του ΜΚΔ οδήγησε στην μοντέρνα αφηρημένη έννοια του πρωτεύοντος ιδεώδους (principal ideal) , ο οποίος είναι ένας κλάδος που ασχολείται η σύγχρονη επιστημονική κοινότητα.

2.2 Ευκλείδειος αλγόριθμος και Μέγιστος Κοινός Διαιρέτης

Σε ορισμένες περιπτώσεις είναι αρκετά δύσκολο και χρονοβόρο να αναλύουμε έναν αριθμό σε γινόμενο πρώτων παραγόντων ή να βρίσκουμε όλους τους διαιρέτες του , με σκοπό την εύρεση του μέγιστου κοινού διαιρέτη . Ένας αλγόριθμος , ο οποίος μας βοηθάει στον ακριβή υπολογισμό του Μέγιστού Κοινού Διαιρέτη είναι ο ***Ευκλείδειος αλγόριθμος*** . Στα μαθηματικά ο Ευκλείδειος αλγόριθμος είναι μια αρχαία μέθοδος για τον υπολογισμό του μέγιστου κοινού διαιρέτη (ΜΚΔ). Ο αλγόριθμος αυτός είναι γνωστός και σαν αλγόριθμος του Ευκλείδη, ύστερα από την περιγραφή που κάνει ο αρχαίος Έλληνας μαθηματικός, στα βιβλία VII και X των ``Στοιχείων`` του.

Η παλαιότερη σωζόμενη περιγραφή του Ευκλείδειου αλγόριθμου υπάρχει στα ``Στοιχεία`` του Ευκλείδη (300π.Χ.) , και τον καθιστά αυτόματα , τον αρχαιότερο αριθμητικό αλγόριθμο , ο οποίος είναι σε ισχύ μέχρι και σήμερα. Ο αρχικός αλγόριθμος αναφερόταν μόνο σε φυσικούς αριθμούς και σε γεωμετρικά μήκη (πραγματικοί αριθμοί) . Τον 19^{ο} αιώνα γενικεύτηκε και σε άλλες μορφές αριθμών , όπως τους ακεραίους (Gaussian integers) και σε πολυώνυμα μιας μεταβλητής. Αυτό οδήγησε στις σημερινές μοντέρνες αφηρημένες αλγεβρικές έννοιες όπως τα ευκλείδεια πεδία (Euclidean domains). Αργότερα , ο ευκλείδειος αλγόριθμος γενικεύτηκε και σε άλλες μαθηματικές δομές , όπως τα πολυμεταβλητά πολυώνυμα και στους κόμβους (knots), που χρησιμοποιούμε στην Τοπολογία.

2.2.1 Περιγραφή του αλγορίθμου

Ο Ευκλείδειος αλγόριθμος είναι επαναληπτικός. Αυτό σημαίνει ότι η απάντηση στον υπολογισμό του ΜΚΔ θα βρεθεί μετά από μια αλληλουχία ορισμένων βημάτων. Το αποτέλεσμα – έξοδο το οποίο προκύπτει ύστερα από κάθε βήμα , θα χρησιμεύσει σαν είσοδο για το επόμενο βήμα. Στην συνέχεια θα περιγράψουμε την διαδικασία του Ευκλείδειου αλγόριθμου ,διότι είναι καθοριστική στην εξέλιξη της πορείας υπολογισμού του μέγιστου κοινού διαιρέτη , οποιασδήποτε μαθηματικής οντότητας .

Κάθε βήμα του αλγορίθμου ξεκινάει με δύο μη μηδενικά υπόλοιπα r_{k-1} και r_{k-2}. Καθώς ο αλγόριθμος εξασφαλίζει ότι τα υπόλοιπα μειώνονται σταθερά σε κάθε βήμα , το r_{k-1} είναι μικρότερο από το προκάτοχο υπόλοιπο r_{k-2}. Στόχος του αλγόριθμου είναι στο k^{στο} βήμα να βρεθεί ένα πηλίκο q_k και ένα υπόλοιπο r_k , τα οποία να ικανοποιούν την σχέση:

$$r_{k-2}=q_k r_{k-1}+r_k \qquad \text{με} \quad r_k < r_{k-1}.$$

Στο αρχικό βήμα του αλγορίθμου (k=0) τα υπόλοιπα r_{-2}και r_{-1} είναι ίσα με τους αριθμούς *a* , *b* , των οποίων ψάχνουμε το ΜΚΔ τους. Στο επόμενο βήμα (k=1) , τα υπόλοιπα είναι ίσα με το *b* και το υπόλοιπο r_0 από το αρχικό βήμα. Η διαδικασία συνεχίζεται ομοίως και για τα παρακάτω βήματα. Για αυτό το λόγο , ο αλγόριθμος μπορεί να γραφεί και να περιγραφεί , παράλληλα , με μια ακολουθία από εξισώσεις :

$a = q_0 \cdot b + r_0$

$b = q_1 r_0 + r_1$

$r_1 = q_3 r_2 + r_3$

……

Η παραπάνω διαδικασία γίνεται στην περίπτωση που ο *b* είναι μικρότερος από τον *a*. Σε διαφορετική περίπτωση αλλάζουν οι αριθμοί και η διαδικασία συνεχίζει αντίστοιχα. . Τα υπόλοιπα μειώνονται συνεχώς σε κάθε βήμα αλλά δεν γίνονται ποτέ αρνητικοί αριθμοί. Ο αλγόριθμος τερματίζει όταν κάποιο υπόλοιπο r_N γίνει ίσο με το μηδέν. Ο μέγιστος κοινός διαιρέτης των*a* και *b* είναι το τελευταίο μη μηδενικό υπόλοιπο (το r_{N-1} δηλαδή).

Παράδειγμα

Να βρεθεί ο ΜΚΔ των αριθμών *α=138* και *β=58*με την βοήθεια του Ευκλείδειου αλγόριθμου.

Εφαρμόζουμε διαδοχικά τον Ευκλείδειο αλγόριθμο και έχουμε:

$$138 = 2 \cdot 58 + 22$$

$$58 = 2 \cdot 22 + 14$$

$$22 = 1 \cdot 8 + 6$$

$$8 = 1 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

Οπότε έχουμε ότι ο *ΜΚΔ(138,58)=2* ,δηλαδή το τελευταίο μη μηδενικό υπόλοιπο**.**

■

2.2.2 Μερικοί αλγόριθμοι για τον ΜΚΔ αριθμών

Αλγόριθμος 1 (Ευκλείδη - επαναληπτικός)

```
function GCD(a, b)
  while b != 0
    if a > b then
      a := a - b
    else
      b := b - a
  return a
```

παράδειγμα

Έστω ότι θέλουμε να υπολογίσουμε το μέγιστο κοινό διαιρέτη των a=124 και b=24. Η διαδικασία φαίνεται παρακάτω:

GCD(124,24)

$1^{η}$ επανάληψη: a=100

$2^{η}$ επανάληψη: a=76

$3^{η}$ επανάληψη: a=52

$4^{η}$ επανάληψη: a=28

$5^{η}$ επανάληψη: a=4 το οποίο είναι και το τελικό αποτέλεσμα

Αλγόριθμος 2 (Ευκλείδη - αναδρομικός)

```
function GCD(a, b)
 if b = 0 then
   return a
 else
```

return GCD(b, a mod b)

Παράδειγμα

Έστω ότι θέλουμε να υπολογίσουμε το μέγιστο κοινό διαιρέτη των a=124 και b=24. Η αναδρομική διαδικασία φαίνεται παρακάτω:

GCD(124,24)-> GCD(24,4)->GCD(4,0) όπου και επιστρέφεται το 4 που είναι και η λύση.

Αλγόριθμος 3

function gcd(a,b)

t=min(a,b)

repeat

if (a mod t=0) then

if (b mod t =0) then

return t

t=t-1

until ((b mod (t+1) =0)and(a mod t =0))

παράδειγμα

Για τον υπολογισμό του gcd(124,24) η τιμή του t από 24 μειώνεται συνεχώς σε κάθε επανάληψη έως ότου t=4 όπου και τερματίζει η επανάληψη.

Αλγόριθμος 4 (Stein's Algorithm)

```
function gcd(a,b)
g = 1
while (a mod 2 =0) and (b mod 2 =0) then
        a = a/2
        b = b/2
        g = 2*g
while (a > 0)
        if (a mod 2 =0) then a = a/2
        else if (b mod 2=0) then b = b/2
        else
                t = |a-b|/2
                if a < b then
                        b = t
                else
                        a = t
return g*v
```

Αλγόριθμος 5

```
function gcd(a,b) {
if (a == b) return a;
if (a > b) return gcd(a-b, b);
if (a < b) return gcd(a, b-a);
}
```

παράδειγμα

gcd(124,24)->gcd(100,24)->gcd(76,24)->gcd(52,24)-> gcd (28,24)-> gcd (4,24)-> gcd (4,20)-> gcd (4,16)-> gcd (4,12)-> gcd (4,8)-> gcd (4,4)->4

Αλγόριθμος 6 (Knuth algorithm)

```
function gcd(a,b)
  If (a mod 2=0)and (b mod 2=0) then
    gcd(a, b) = 2 * gcd( a/2, b/2 )
  If (a mod 2=0)and (b mod 2=1) then
    gcd(a, b) = gcd( a/2, b )
  If (a mod 2=1)and (b mod 2=0) then
    gcd(a, b) = gcd( a, b/2 )
  If (a mod 2=1)and (b mod 2=1) then
    gcd(a, b) = gcd( (a-b)/2, b)
```

Παράδειγμα

Έστω ότι θέλουμε να υπολογίσουμε το μέγιστο κοινό διαιρέτη των a=124 και b=24. Η διαδικασία φαίνεται παρακάτω:

GCD(124,24)=2*GCD(62,12)=2*(2*GCD(31,6))=2*(2*(GCD(31,3)))= 2*(2*(GCD(14,3)))= 2*(2*(GCD(7,3)))= 2*(2*(GCD(4,3)))=2*(2*(GCD(2,3)))= 2*(2*(GCD(1,3)))

Αλλά ο μ.κ.δ. της μονάδας με έναν αριθμό είναι το 1 άρα το αποτέλεσμα είναι 2*2*1=4.

ΚΕΦΑΛΑΙΟ 3ο

Μέγιστος Κοινός Διαιρέτης Πολυωνύμων μίας μεταβλητής

3.1 Εισαγωγή

Ονομάζουμε ακέραιο πολυώνυμο του x ή πολυώνυμο μια μεταβλητής κάθε έκφραση της μορφής

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$$

, όπου $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ και $n \in \mathbb{N}$.

Οι αριθμοί $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n$ αποκαλούνται συντελεστές του πολυωνύμου και το α_0 αποκαλείται σταθερός όρος (είναι ο συντελεστής τουx^0). Οι εκφράσεις $\alpha_k x^k$, όπου $k \in \mathbb{Z}$ και $k \geq 0$, αποκαλούνται ακέραια μονώνυμα του x και αποτελούν τους όρους του πολυωνύμου. Πιο συγκεκριμένα, ο $\alpha_k x^k$, είναι ο πρώτος όρος και ο α_k ο πρώτος συντελεστής του πολυωνύμου. Το σύνολο των ακέραιων πολυωνύμων του x με μιγαδικούς συντελεστές θα το συμβολίζουμε με C[x] και τα στοιχεία του C[x], δηλαδή τα ακέραια πολυώνυμα του x, θα τα συμβολίζουμε με *P(x), Q(x), R(x), p(x)* κ.ο.κ.

Ας είναι $P(x)$ και $q(x)$ είναι δύο ακέραια πολυώνυμα του C[x]. Τότε λέμε ότι το $q(x)$ διαιρεί το $P(x)$, και θα γράφουμε $q(x)/P(x)$, αν και μόνο αν $q(x) \neq 0(x)$ (δηλαδή $q(x)$ είναι διαφορετικό από το μηδενικό πολυώνυμο) και υπάρχει ένα ακέραιο πολυώνυμο $r(x) \in$C[x], ώστε να ισχύει:

$$P(x) = q(x)r(x)$$

Σε αυτήν την περίπτωση ισχύει ότι το *P(x)* διαιρείται ή είναι διαιρετό από το *q(x)* ή ότι το *P(x)* είναι πολλαπλάσιο του *q(x)* ή ότι το *q(x)* είναι διαιρέτης του *P(x)* ή ότι το *q(x)* είναι παράγοντας του *P(x)* ή τέλος ότι το *q(x)* διαιρεί το *P(x).*

Παράλληλα με τα παραπάνω , ισχύει ότι το μηδενικό πολυώνυμο διαιρείται από κάθε μη μηδενικό πολυώνυμο και ότι οι μόνοι σίγουροι διαιρέτες ενός ακεραίου πολυωνύμου $P(x)$ είναι τα πολυώνυμα μηδενικού βαθμού , το ίδιο το πολυώνυμο $P(x)$, καθώς και όλα τα πολυώνυμα $cP(x)$. Οι διαιρέτες αυτοί αποκαλούνται προφανείς διαιρέτες του $P(x)$ και κάθε άλλος διαιρέτης του αποκαλείται γνήσιος διαιρέτης του $P(x)$.

Ο μέγιστος κοινός διαιρέτης δύο πολυωνύμων $p(x)$ και $q(x)$ είναι το « μεγαλύτερο » πολυώνυμο που διαιρεί και το $p(x)$ και $q(x)$. Ο ορισμός αυτός είναι βασισμένος στον ορισμό του μέγιστου κοινού διαιρέτη των ακεραίων αριθμών, όπου είναι ο μεγαλύτερος ακέραιος, ο οποίος διαιρεί και τους δύο αριθμούς και αφήνει μηδενικό υπόλοιπο. Για τα πολυώνυμα όμως , αυτή η συνθήκη είναι λίγο μπερδεμένη , γιατί δεν υπάρχει η έννοια του μεγαλύτερου σε αυτά. Εξ' αιτίας αυτού ,έχει επιλεχτεί να είναι ΜΚΔ το πολυώνυμο εκείνο , του οποίου ο βαθμός είναι ο μέγιστος

δυνατός και ο αντίστοιχος συντελεστής του μεγιστοβάθμιου(leading coefficient) όρου να είναι μονάδα .

Θα προσπαθήσουμε στην συνέχεια να δώσουμε έναν επίσημο μαθηματικό ορισμό για τον μέγιστο κοινό διαιρέτη δύο πολυωνύμων. Ας είναι $p(x)$ και $q(x)$ πολυώνυμα , όχι και τα δύο μηδενικά , με συντελεστές σε ένα σώμα F.

Ο μέγιστος κοινός διαιρέτης των $p(x)$ και $q(x)$ ορίζουμε να είναι το monic πολυώνυμο (ο συντελεστής του μεγιστοβάθμιου όρου του είναι μονάδα) $d(x)$ για το οποίο ισχύουν :

- ✓ είναι κοινός διαιρέτης των $p(x)$ και $q(x)$
- ✓ να διαιρείται από κάθε άλλο κοινό διαιρέτη των $p(x)$ και $q(x)$.

Ακόμα μπορούμε να ορίσουμε τον ΜΚΔ των $p(x)$ και $q(x)$ να είναι το πολυώνυμο εκείνο με τον μεγαλύτερο βαθμό ανάμεσα στους κοινούς διαιρέτες των δύο πολυωνύμων.

Συμβολίζουμε τον ΜΚΔ των $p(x)$ και $q(x)$ γράφοντας $MK\Delta(p(x), q(x))$. Το σώμα F μπορεί να είναι το σώμα των μιγαδικών αριθμών $\mathbb{C}$ ή των πραγματικών αριθμών $\mathbb{R}$ ή ακόμα και το σώμα των ρητών αριθμών $\mathbb{Q}$.

Αν είναι $p(x) = q(x) = 0$ τότε κάθε πολυώνυμο είναι κοινός διαιρέτης των $p(x) και\ q(x)$.Σε αυτή περίπτωση δεν υπάρχει ΜΚΔ .

Ο αριθμός 1 , είναι πάντα κοινός διαιρέτης των $p(x)\ και\ q(x)$. Αν $MK\Delta\ (p(x), q(x)) = 1$ τότε τα πολυώνυμα $p(x)$ και $q(x)$ είναι πρώτα μεταξύ τους και επομένως ο μέγιστος κοινός διαιρέτης είναι το σταθερό πολυώνυμο 1.

Ας δούμε ορισμένες ιδιότητες του Μέγιστου Κοινού Διαιρέτη των πολυωνύμων .

- Ο ΜΚΔ δύο πολυωνύμων , όχι αναγκαστικά και τα δύο μηδενικά , με συντελεστές από ένα σώμα , πάντα θα υπάρχει και θα είναι μοναδικός.
- Αν $r(x)$ είναι κάποιος κοινός διαιρέτης των $p(x)$ και $q(x)$,τότε θα διαιρεί και τον ΜΚΔ τους.
- $MK\Delta(\ p(x), q(x)) = MK\Delta\ (q(x), p(x))$
- $MK\Delta(p(x), q(x)) = MK\Delta(p(x), p(x) + q(x))$
- Για οποιοδήποτε $k \in$ F τότε $MK\Delta(p(x), q(x)) = MK\Delta(p(x), kq(x))$
- Ομοίως,
  $MK\Delta(p(x), q(x)) = MK\Delta(a_1 p(x) + b_1 q(x), a_2 p(x) + b_2 q(x))$
  για οποιαδήποτε $a_1, b_1, a_2, b_2, a_1 b_2 - a_2 b_1$ δεν είναι ίσα με το μηδέν.
- Παρομοίως , αν $MK\Delta(\ p(x), r(x)) = 1$ τότε $MK\Delta(\ p(x), q(x)) = MK\Delta(p(x), q(x) r(x))$.
- Ο ΜΚΔ δύο πολυωνύμων $p(x)$ και $q(x)$ είναι το μικρότερο σε βαθμό πολυώνυμο , το οποίο μπορεί να γραφεί σαν γραμμικός συνδυασμός των

$p(x)$ και $q(x)$. Δηλαδή υπάρχουν κάποια πολυώνυμα $r(x)$ και $s(x)$, όχι απαραίτητα μοναδικά, τα οποία ανήκουν στο ίδιο σώμα F με τα $p(x)$ και $q(x)$, για τα οποία ισχύει :
$d(x) = p(x)r(x) + q(x)s(x)$.

- Είναι δυνατόν να ορίσουμε τον ΜΚΔ τριών ή περισσοτέρων πολυωνύμων επαγωγικά .Δηλαδή :

$$MK\Delta\big(p(x), q(x), r(x)\big) = MK\Delta(p(x), MK\Delta\big(q(x), r(x)\big)$$

και γενικότερα:

$$MK\Delta\big(p_1(x), p_2(x), \dots, p_n(x)\big) = MK\Delta(p_1(x), MK\Delta\big(p_2(x), \dots p_n(x)\big).$$

3.2 Μέθοδοι εύρεσης ΜΚΔ πολυωνύμων μιας μεταβλητής

Υπάρχουν διάφοροι τρόποι για να υπολογίσει τον μέγιστο κοινό διαιρέτη δύο πολυωνύμων .Δύο από τις πιο βασικές και απλές μεθόδους είναι η παραγοντοποίηση και ο Ευκλείδειος αλγόριθμος . Παρακάτω θα επεκταθούμε εκτενέστερα και σε άλλες μεθόδους .

Στην παραγοντοποίηση αρχικά αναλύουμε το κάθε πολυώνυμο σε παράγοντες και στην συνέχεια επιλέγουμε τους κοινούς παράγοντες. Αφού επιλέξουμε τους κοινούς παράγοντες από τα δύο πολυώνυμα , παίρνουμε το γινόμενο τους. Το γινόμενο τους όμως , υπάρχει περίπτωση να μην είναι monic πολυώνυμο, και για αυτό τον λόγο το πολλαπλασιάζουμε με έναν κατάλληλο αριθμό . Με αυτόν τον τρόπο πετυχαίνουμε την εύρεση του ΜΚΔ των δύο πολυωνύμων , αφού περιέχει όλους τους κοινούς παράγοντες και ο συντελεστής του μεγιστοβάθμιου όρου είναι μονάδα.

Παράδειγμα

Να βρεθεί ο ΜΚΔ των πολυωνύμων $P(x) = x^4 + 2x^3 - x^2 - 2x$ και $Q(x) = x^3 - 4x^2 - 5x - 6$.

Έχουμε ότι :

$$P(x) = x^4 + 2x^3 - x^2 - 2x = x^2(x^2 - 1) + 2x(x^2 - 1)$$
$$= x(x + 2)(x - 1)(x + 1)$$

Και $Q(x) = x^3 - 4x^2 - 5x - 6 = x^3 - x^2 - 3x^2 + 2x^2 - 3x - 2x - 6 = x(x^2 - x - 2) + 3(x^2 - x - 2) = (x + 3)(x + 2)(x - 1)$

Άρα ο ΜΚΔ των $P(x)$ και $Q(x)$ είναι $d(x) = (x + 2)(x - 1) = x^2 + x - 2$.

■

Όπως είπαμε και παραπάνω ένας άλλος απλός τρόπος για τον υπολογισμό του ΜΚΔ δύο πολυωνύμων μιας μεταβλητής είναι ο Ευκλείδειος αλγόριθμος. Πρόκειται

για μια γρήγορη μέθοδο η οποία δουλεύει για οποιαδήποτε πολυώνυμα. Πραγματοποιεί διαδοχικές πολυωνυμικές ευκλείδειες διαιρέσεις , όπως ακριβώς και στον Ευκλείδειο αλγόριθμο για τους ακέραιους αριθμούς. Οι αριθμοί που παίρνουν μέρος σε κάθε βήμα του αλγορίθμου μειώνονται . Αντιστοίχως ισχύει και στα πολυώνυμα . Δηλαδή σε κάθε βήμα ο βαθμός των πολυωνύμων μειώνεται .Το τελευταίο μη μηδενικό υπόλοιπο είναι ο μέγιστος κοινός διαιρέτης των δύο πολυωνύμων .Αρκεί βέβαια το υπόλοιπο αυτό να είναι ένα monic πολυώνυμο. Σε διαφορετική περίπτωση θα πρέπει να το μετατρέψουμε όπως και προηγουμένως καταλλήλως , πολλαπλασιάζοντας με τον κατάλληλο αριθμό.

Παράδειγμα

Να βρεθεί ο ΜΚΔ των πολυωνύμων $P(x) = x^2 + 7x + 6$ και $Q(x) = x^2 - 5x - 6$.

Κάνοντας την Ευκλείδεια διαίρεση του πολυωνύμων $P(x)$ με το $Q(x)$ προκύπει :

$$x^2 + 7x + 6 = (x^2 - 5x - 6)(1) + (x + 1)$$

$$x^2 - 5x - 6 = (x + 1)(x - 6) + 0$$

Επομένως το τελευταίο μη μηδενικό υπόλοιπο του παραπάνω αλγορίθμου είναι ο ΜΚΔ των πολυωνύμων $P(x) = x^2 + 7x + 6$ και $Q(x) = x^2 - 5x - 6$

■

Διάφοροι αριθμητικοί αλγόριθμοι έχουν προταθεί για τον υπολογισμό του Μέγιστου Κοινού Διαιρέτη (ΜΚΔ) δύο ή περισσοτέρων πολυωνύμων μίας μεταβλητής. Μερικοί από αυτοί βασίζονται στον Ευκλείδειο αλγόριθμο και στις γενικεύσεις του και άλλοι από αυτοί βασίζονται πρότυπες διαδικασίες εμπεριέχοντας πίνακες (matrix – based methods) . Συχνά , είναι άσκοπο να προσπαθούμε να υπολογίσουμε τον ακριβή ΜΚΔ των πολυωνύμων και έτσι οι κατά προσέγγιση λύσεις είναι περισσότερο κατάλληλες , για την μελέτη των αντίστοιχων προβλημάτων ,κάθε φορά. Εξαιτίας της σπουδαιότητας και της βαρύτητας των εφαρμογών που προκύπτουν από τις « κατά προσέγγιση » έννοιες , πολλοί ερευνητές έχουν ασχοληθεί με το θέμα αυτό.

Οι Pace και Barnett (1972) περιγράφουν διάφορες μεθόδους για τον υπολογισμού ΜΚΔ όπως μια παλαιότερη μέθοδο οφειλομένη στον Fryer , η οποία είναι κατά βάση ισοδύναμη με τον Ευκλείδειο αλγόριθμο και χρησιμοποιεί έναν αλγόριθμο με την βοήθεια της διάταξης του Routh. Παράλληλα , περιγράφουν την μέθοδο Weinstock η οποία σχηματίζει μία επαναληπτική μέθοδο , η οποία περιέχει πολυωνυμικές διαιρέσεις και πολλαπλασιασμούς χρησιμοποιώντας τα αρχικά πολυώνυμα με σκοπό να υπολογίσει ένα νέο πολυώνυμο το οποίο να έχει τον μικρότερο δυνατό βαθμό . Τέλος , παρουσιάζουν μια διαφορετική μέθοδο η οποία προτάθηκε από τον Blankinship (1963) , στην οποία ο ΜΚΔ και τα πολλαπλάσια προσδιορίζονται εκτελώντας στοιχειώδεις μετασχηματισμούς στις σειρές ενός

πίνακα, μέχρι να υπάρχει ένα μη μηδενικό στοιχείο στην πρώτη στήλη του πίνακα. Ο πίνακας αυτός προκύπτει από τα δοσμένα αρχικά πολυώνυμα Η εισαγωγή της χρήσης των πινάκων στο πρόβλημα υπολογισμού του ΜΚΔ πολυωνύμων , συνεχίστηκε και αργότερα από τον Barnett (1971) , ο οποίος αναπτύσσει μία τεχνική υπολογισμού του βαθμού και των συντελεστών του ΜΚΔ χρησιμοποιώντας συνοδεύον πίνακες (companion matrices) και πίνακες του Sylvester (Sylvester matrices).

Ο Καρκανιάς μελέτησε το 1987 τις ιδιότητες του ΜΚΔ, με αποτέλεσμα το 1990 στην ανάπτυξη της μεθόδου ERES, στην οποία εκτελεί εκτεταμένους μετασχηματισμούς και μετατρέπει έναν πίνακα απευθείας από τους συντελεστές των πολυωνύμων. Με την μέθοδο ERES εισάγεται για πρώτη φορά μια συστηματική προσπάθεια για τον υπολογισμό του « κατά προσέγγιση » ΜΚΔ για πολυώνυμα .

Όπως προαναφέραμε και παραπάνω , η διαδικασία εύρεση του ΜΚΔ δεν είναι μια εύκολη υπόθεση. Ο Ευκλείδειος αλγόριθμος για την εύρεση του ΜΚΔ των ακεραίων , παράγει μία αυστηρά φθίνουσα ακολουθία από θετικούς ακεραίους , και έτσι τα βήματα της διαίρεσης γίνονται ολοένα και πιο εύκολα καθώς προχωράει η διαδικασία υπολογισμού. Αντίθετα , στην περίπτωση των πολυωνύμων δεν συμβαίνει αυτό. Μολονότι , γίνονται αλλεπάλληλες μειώσεις στον βαθμό των πολυωνύμων · οι συντελεστές τους τείνουν να αυξάνονται και έτσι κάθε επόμενο βήμα δυσκολεύει , σε σχέση με το προηγούμενο του.

3.2 Περιγραφή αλγορίθμων για τον ακριβή υπολογισμό του ΜΚΔ πολυωνύμων μίας μεταβλητής

Οποιαδήποτε από τις παρακάτω μεθόδους και αν διαλέξει κανείς , θα καταλάβει ότι αναφέρονται στον υπολογισμό του ΜΚΔ δύο πολυωνύμων . Βέβαια, αυτό μπορεί να επεκταθεί και σε παραπάνω από δύο.

3.2.1 Αλγόριθμος με την βοήθεια του πίνακα του Routh (Routh array algorithm)

Οι Pace και Barnett το 1972 περιγράφουν διάφορες μεθόδους για τον υπολογισμό του ΜΚΔ δύο πολυωνύμων μιας μεταβλητής στο σώμα τον πραγματικών αριθμών , οι οποίες είναι ισοδύναμες με τον Ευκλείδειο αλγόριθμο.

Θεωρούμαι δύο πολυώνυμα :

$$a(\lambda)=a_1\lambda^m+a_2\lambda^{m-1}+\cdots+a_m\lambda+a_{m+1}$$

και

$$b(\lambda)=b_1\lambda^n+b_2\lambda^{n-1}+\cdots+b_n\lambda+b_{n+1} \quad (1)$$

με αντίστοιχους βαθμούς m και n , αντίστοιχα $m \geq n$.

Σημειώνουμε g(λ) τον ΜΚΔ των δύο παραπάνω πολυωνύμων, και έχουμε :

$$g(\lambda)=g_1\lambda^k+g_2\lambda^{k-1}+\cdots+g_k\lambda+g_{k+1} \quad (2)$$

όπου k ο βαθμός του g(λ).

Το πολυώνυμο g(λ) γράφεται σαν γραμμικός συνδυασμός των α(λ) και b(λ) ως εξής : $g(\lambda)=x(\lambda)a(\lambda)+y(\lambda)b(\lambda)$ (3)

, όπου $x(\lambda)=x_1\lambda^{n-1}+x_2\lambda^{n-2}+\cdots+x_{n-1}\lambda+x_n$

και $y(\lambda)=y_1\lambda^{m-1}+y_2\lambda^{m-2}+\cdots+y_{m-1}\lambda+y_m$ (4)

τα μοναδικά πολλαπλάσια των α(λ) και b(λ) αντίστοιχα , τέτοια ώστε να ισχύει η (3).

Ο Fryer το 1959 με την βοήθεια του πίνακα του Routh, παρουσιάζει , όπως προαναφέραμε μια τεχνική για τον υπολογισμό τουΜΚΔ , η οποία είναι ισοδύναμη με τον Ευκλείδειο αλγόριθμο.

Η τεχνική έχει ως εξής :

1η γραμμή	a_1	a_2	a_3	.	.	.	.	.	a_m	a_{m+1}
2η γραμμή	b_1	b_2	b_3	.	.		b_n	b_{n+1}		
3η γραμμή	c_1	c_2	c_3	.	.					
4η γραμμή	d_1	d_2	d_3	.	.					
.		.								
.		.								
.		.								

Όπου $c_j = -\frac{\begin{vmatrix} a_1 & a_{j+1} \\ b_1 & b_{j+1} \end{vmatrix}}{b_1}$ και $d_j = -\frac{\begin{vmatrix} b_1 & b_{j+1} \\ c_1 & c_{j+1} \end{vmatrix}}{c_1}$ με j =1,2,….κτλ.

Η διαδικασία του κριτηρίου τερματίζει όταν προκύψει μία σειρά μόνο με μηδενικά. Στην περίπτωση αυτή η προηγούμενη σειρά μας δείχνει τους συντελεστές του μέγιστου κοινού διαιρέτη $g_1, g_2, g_3, \dots, g_{k+1}$. Οι δυσκολίες προκύπτουν στην περίπτωση στην οποία όταν το πρώτο ή περισσότερα στοιχεία από οποιαδήποτε σειρά είναι μηδέν . Αυτό το εμπόδιο ξεπερνιέται , αν μετακινήσουμε κατάλληλα ολόκληρη την σειρά προς τα αριστερά μέχρι να εμφανιστεί ο πρώτος μη μηδενικός αριθμός στην πρώτη θέση. Ο υπολογισμός στην συνέχεια συνεχίζει κανονικά.

Έχοντας δύο σειρές του πίνακα του Routh με m+1 στοιχεία a_j και n+1 στοιχεία b_j αντίστοιχα , (με $m \geq n$) τότε απαιτούνται n πολλαπλασιασμοί και n διαιρέσεις για να προκύψει η τρίτη σειρά στοιχείων c_j μέχρι $c_j = \frac{a_{j+1} - a_1 b_{j+1}}{b_1}$

Τέλος, μπορεί να αποδειχθεί ότι για την κατασκευή του πίνακα του Routh απαιτούνται $mn - k^2 + k$ πολλαπλασιασμοί και διαιρέσεις.

Παράδειγμα

Να υπολογιστεί ο ΜΚΔ των πολυωνύμων $p(x) = x^2 + 6x + 9$ και $q(x) = x + 3$.

Σύμφωνα με το κριτήριο – πίνακα του Routh έχουμε αντίστοιχα :

1η γραμμή	9	6	1
2η γραμμή	3	1	
3η γραμμή	3	1	
4η γραμμή	0		

Οι αριθμοί της τρίτης γραμμής του πίνακα του Routh προκύπτουν :

$$c_1 = -\frac{\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}}{b_1} = -\frac{\begin{vmatrix} 9 & 6 \\ 3 & 1 \end{vmatrix}}{3} = -\frac{-9}{3} = 3$$

$$c_2 = -\frac{\begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}}{b_1} = -\frac{\begin{vmatrix} 9 & 1 \\ 3 & 0 \end{vmatrix}}{3} = -\frac{-3}{3} = 1$$

Ομοίως, έχουμε και τους αριθμούς της 4ης γραμμής . Οπότε :

$$d_1 = -\frac{\begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix}}{c_1} = -\frac{\begin{vmatrix} 3 & 1 \\ 3 & 1 \end{vmatrix}}{3} = -\frac{0}{3} = 0$$

Άρα, σύμφωνα με το κριτήριο του Routh και την βοήθεια του παραπάνω πίνακα καταλαβαίνουμε ότι ο ΜΚΔ των πολυωνύμων p(x) και q(x) είναι το πολυώνυμο που έχει συντελεστές τους αριθμούς , 3 ,1 αντίστοιχα.
Οπότε ΜΚΔ $\{p(x), q(x)\} = x + 3$.

■

3.2.2 Αλγόριθμος με την βοήθεια του συνοδεύον πίνακα (Barnett)

Το πρόβλημα εύρεσης του ΜΚΔ με την χρήση των πινάκων μπορεί να περιγραφεί από διάφορα θεωρήματα του Barnett . Ας συμβολίσουμε το πολυώνυμο α(λ) από την (1) με $\alpha_1 = 1$ και επίσης ας είναι

$$b_i(\lambda) = b_{i1}\lambda^{m-1} + b_{i2}\lambda^{m-2} + \cdots + b_{im}$$

, όπου ένα ή περισσότερα από τα b_{ij} μπορεί να είναι μηδέν. Ο συνοδεύον πίνακας (companion matrix) του πολυωνύμου $a(\lambda)$ είναι :

$$A = \begin{bmatrix} 0 & 0 & . & 0 & -\alpha_{m+1} \\ 1 & 0 & . & 0 & -a_m \\ 0 & 1 & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & 0 & -a_3 \\ 0 & 0 & . & 1 & -a_2 \end{bmatrix}$$

Έχει αποδειχθεί ότι ο βαθμός k του ΜΚΔ των πολυωνύμων $\alpha(\lambda), b_1(\lambda), \ldots, b_i(\lambda)$ είναι $k = m - rank\ R$, όπου $R = [F, AF, A^2F, \ldots, A^{m-1}F]$ και

$$F = \begin{bmatrix} b_{1m} & b_{2m} & . & . & b_{lm} \\ b_{1m-1} & . & . & . & . \\ . & . & . & . & . \\ b_{l1} & . & . & . & b_{ll} \end{bmatrix}$$

Επιπροσθέτως με τα παραπάνω , οι τελευταίες m-k σειρές του πίνακα R είναι γραμμικά ανεξάρτητες , και αν οι πρώτες k σειρές είναι γραμμένες στην μορφή :

$$r_i = \sum_{j=k+1}^{m} z_{ij} r_j, \quad i = 1, 2, \ldots, k \qquad (5)$$

(r_i, r_j είναι η i και η j σειρά αντίστοιχα) .

Τότε ο ΜΚΔ με τον συντελεστή του μεγιστοβάθμιου όρου να είναι μονάδα , (monic GCD) των $\alpha(\lambda)$ και $b_i(\lambda)$ έχει συντελεστές :

$$g_{i+1} = z_{k+1-i,k+1} \text{ με } i = 1,2,3 \dots, k \text{ και } g_1 = 1 \quad (6)$$

Αυτή η λύση στο πρόβλημα είναι αρκετά ξεκάθαρο ότι βασίζεται στην λύση της γραμμικής εξίσωσης (5). Αν ο πίνακας R διαμερίζεται ως

$$:R = \begin{bmatrix} R_1(k \times ml - m + k) & \vdots & R_2(k \times m - k) \\ \cdots\cdots\cdots\cdots\cdots\cdots & \vdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ R_3(m - k \times ml - m + k) & \vdots & R_4(m - k \times m - k) \end{bmatrix} \quad (7)$$

τότε ο R μπορεί να αναλυθεί σε γινόμενο δύο πινάκων οι οποίοι προκύπτουν από την απαλοιφή του Gauss τέτοιοι ώστε:

$$J_{m-k}J_{m-k-1} \cdots\cdots J_2J_1R = L \quad (8)$$

όπου $J_i = \begin{bmatrix} 1 & \cdots & 0 & \cdots & -z_{1,m+1-i} & \cdots & 0 \\ & \ddots & & & \vdots & & \vdots \\ & & 1 & & -z_{m-i,m+1-i} & & \\ & & & & \ddots & \vdots & \\ & & & & & 1 & 0 \\ & & & & & & \ddots \\ 0 & & & & & & 1 \end{bmatrix}$

και $L = \begin{bmatrix} 0 & \vdots & 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots & \vdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ L_1(m - k \times ml - m + k) & \vdots & L_2(m - k \times m - k) \end{bmatrix}$.

Από τον τύπο (8) προκύπτει ότι $R = [J_{m-k}J_{m-k-1} \cdots\cdots J_2J_1]^{-1}L$ (10).

$$[J_{m-k}J_{m-k-1} \cdots\cdots J_2J_1]^{-1} = \begin{bmatrix} 1 & \cdots & 0 & \cdots & z_{1,k+1} & \cdots & 0 \\ & & & & \vdots & & \\ & \ddots & & & z_{k,k+1} & & \\ & & 1 & & & & \\ & & & \ddots & & 0 & \\ & & & & 1 & & \\ 0 & & & \cdots & & & 1 \end{bmatrix} =$$

$$\begin{bmatrix} I & \vdots & U_1(k \times m - k) \\ \cdots\cdots\cdots\cdots\cdots\cdots & \vdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ 0(m - k \times k) & \vdots & U_2(m - k \times m - k) \end{bmatrix} \quad (11)$$

,όπου U_2 είναι μοναδιαίος πάνω διαγώνιος (όπου όλα τα στοιχεία της κύρια διαγωνίου είναι μονάδες) .Χρησιμοποιώντας τις σχέσεις (7), (9) ,(10) και (11) παίρνουμε τις σχέσεις :

$[R_1 \ \vdots \ \mathrm{R}_2] = U_1[L_1 \ \vdots \ \mathrm{L}_2]$

και

$[\,R_3 \ \vdots \ \mathrm{R}_4] = U_2[L_1 \ \vdots \ \mathrm{L}_2]$.

Από τις παραπάνω σχέσεις προκύπτει ότι : $[R_1 \ \vdots \ \mathrm{R}_2] = U_1U_2^{-1}[R_3 \ \vdots \ \mathrm{R}_4]$.

Το αποτέλεσμα του Barnett υποδηλώνει ότι η πρώτη στήλη του πίνακα $U_1U_2^{-1}$ δίνει τους συντελεστές του monic μέγιστου κοινού παράγοντα. Καθώς ο πίνακας U_2 είναι πάνω τριγωνικός αρα και ο U_2^{-1} θα είναι πάνω τριγωνικός, οπότε η πρώτη στήλη του $U_1U_2^{-1}$ θα είναι απλά η πρώτη στήλη του U_1. Συνεπώς εφαρμόζοντας τεχνικές για να ορίσουμε την τάξη του πίνακα R (άρα και τον βαθμό του ΜΚΔ) ταυτόχρονα ορίζουμε και τους συντελεστές του ΜΚΔ.

Ο Barnett , απέδειξε την σχέση μεταξύ του πίνακα R και του αντίστοιχου πίνακα του Sylvester , για δύο πολυώνυμα . Αυτό που απέδειξε είναι ισοδύναμο με το θεώρημα του Laidacker(1969) όπου αναφέρει ότι : εάν ο πίνακας του Sylvester έχει τις στήλες του κλιμακωτά φτιαγμένες, τότε η τελευταία μη μηδενική στήλη δίνει του συντελεστές του ΜΚΔ.

Για δύο πολυώνυμα τα παραπάνω αποτελέσματα μπορούν να επεκταθούν με τον προσδιορισμό των πολλαπλάσιων συγχρόνως με την εύρεση του ΜΚΔ. Αν θεωρήσουμε ξανά τις εξισώσεις:

$g(\lambda) = x(\lambda)\alpha(\lambda) + y(\lambda)b(\lambda)$,

όπου $x(\lambda) = x_1\lambda^{n-1} + x_2\lambda^{n-2} + \cdots + x_{n-1}\lambda + x_n$

και $y(\lambda) = y_1\lambda^{m-1} + y_2\lambda^{m-2} + \cdots + y_{m-1}\lambda + y_m$.

Αν εξισώσουμε τους συντελεστές και τους γράψουμε στην μορφή πινάκων έχουμε : $\boldsymbol{Sa} = \boldsymbol{g}$, όπου S είναι ο πίνακας του Sylvester

$$S = \begin{bmatrix} a_{m+1} & 0 & . & . & 0 & \vdots & b_{m+1} & 0 & . & . & 0 \\ a_m & a_{m+1} & . & . & . & \vdots & b_m & b_{m+1} & . & . & . \\ . & a_m & & & . & \vdots & . & b_m & & & . \\ . & . & . & & . & \vdots & . & . & . & & . \\ . & . & & & . & \vdots & . & . & & & . \\ . & . & & . & 0 & \vdots & . & . & & . & 0 \\ a_2 & . & & & a_{m+1} & \vdots & b_2 & . & & & b_{m+1} \\ a_1 & a_2 & & & . & \vdots & b_1 & b_2 & & & . \\ 0 & a_1 & & & . & \vdots & 0 & b_1 & & & . \\ . & 0 & . & . & . & \vdots & . & 0 & . & . & . \\ . & & & . & a_2 & \vdots & . & . & & . & b_2 \\ 0 & . & . & . & a_1 & \vdots & 0 & . & . & . & b_1 \end{bmatrix} \qquad (12)$$

$\boldsymbol{a}^T = [x_n, x_{n-1}, \ldots, x_2, x_1, y_m, y_{m-1}, \ldots, y_2, y_1]$ και $\boldsymbol{g}^T = [g_{k+1}, g_k, \ldots, g_2, g_1, 0, \ldots, 0]$.

Εξαιτίας της σχέσης που υπάρχει μεταξύ του S και του αντίστοιχου R, έχουμε ότι $k = m + n - rank\ S$.Εκτελώντας μια ανάλυση στον πίνακα S, όμοια με αυτήν που είχαμε κάνει προηγουμένως στην (8) ,προκύπτει :

$$S = \begin{bmatrix} S_1 & S_2 \\ S_3 & S_4 \end{bmatrix} = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix} [L_1 \quad L_2] \tag{13}$$

όπου ο πίνακας U_2 είναι μοναδιαίος πάνω τριγωνικός και η πρώτη στήλη του πίνακα

$$\begin{bmatrix} U_1 \\ U_2 \end{bmatrix}$$

αποτελεί τους συντελεστές του ΜΚΔ .

Από την (13) έχουμε:

$$\left[\frac{U_1}{U_2}\right] = S[L_1 \quad \vdots \quad L_2]^+$$

, όπου το + υποδηλώνει τον γενικευμένο αντίστροφο Moore-Penrose και εδώ το L_2 έχει πλήρη τάξη (full rank) . Έχουμε :

$$[L_1 \quad \vdots \quad L_2]^+ = [L_1 \quad \vdots \quad L_2]^T\{[L_1 \quad \vdots \quad L_2]^T\}^{-1}$$

Έτσι λοιπόν ,

$$\boldsymbol{g} = c_1\left[\frac{U_1}{U_2}\right] = Sc_1\{[L_1 \quad \vdots \quad L_2]^+\}$$

,όπου $c_1[X]$ σημειώνουμε την πρώτη στήλη από κάθε πίνακα X. Άρα έχουμε :

$$\boldsymbol{g} = S\boldsymbol{\alpha} = Sc_1\{[L_1 \quad \vdots \quad L_2]^+\}$$

Οπότε:

$$\boldsymbol{\alpha} = c_1\{[L_1 \quad \vdots \quad L_2]^+\}$$

Η παραπάνω επέκταση της μεθόδου του Barnett, να υπολογίζουμε τα πολλαπλάσια ,δυστυχώς , δεν μπορεί να εφαρμοστεί σε περισσότερα από δύο πολυώνυμα , καθώς οι βαθμοί των πολλαπλάσιων δεν μπορούν να προσδιοριστούν εκ των προτέρων

3.2.3 Αλγόριθμος του Blankinship με την βοήθεια πινάκων.

Μια διαφορετική μέθοδος είναι αυτή του Blankinship (1963) η οποία υπολογίζει τον ΜΚΔ g(λ) ενός συνόλου πολυωνύμων $\alpha_i(\lambda)\ i = 1,2,\dots,n$ μαζί με τα πολλαπλάσια $x_i(\lambda)$ δηλαδή

$$\sum_{i=1}^{n} x_i(\lambda)\,\alpha_i(\lambda) = g(\lambda) \tag{14}$$

Ο ΜΚΔ και τα πολλαπλάσια ορίζονται εκτελώντας στοιχειώδεις μετασχηματισμούς στις γραμμές του πίνακα

$$[\boldsymbol{\alpha} \quad \vdots \quad I_n\ ] \tag{15}$$

, όπου $\boldsymbol{\alpha}^T = [\alpha_1, \alpha_2, \dots, \alpha_n]$ και ο I_n είναι ο μοναδιαίος πίνακας τάξης n. Οι στοιχειώδεις μετασχηματισμοί εκτελούνται στον πίνακα μέχρι να υπάρχει ένα μη

μηδενικό στοιχείο στην πρώτη στήλη . Αυτό δίνει ξεκάθαρα τον ΜΚΔ , καθώς :$MK\Delta[\alpha_1, \alpha_2, \dots, \alpha_n] = MK\Delta\left[\alpha_1 + \kappa\alpha_j, \alpha_2, \dots, \alpha_n\right]$.

Αυτές οι διαδικασίες μπορούν να παρασταθούν από τους μη μοναδιαίους πίνακες M_iκαθώς το τελικό αποτέλεσμα είναι της μορφής :

$$\dots M_3 M_2 M_1 [\boldsymbol{\alpha} \ \vdots \ I_n] = \begin{bmatrix} 0 & \vdots & \cdots & \cdots \\ \vdots & \vdots & & \vdots \\ g(\lambda) & \vdots & M & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & \vdots & \cdots & \cdots \end{bmatrix} = [M\boldsymbol{\alpha} \ \vdots \ M] \qquad (16)$$

, όπου M είναι το γινόμενο των M_i. Εάν ο ΜΚΔ σημειώνεται στην j^{η} γραμμή τότε από την σχέση (16) προκύπτει ότι :

$$g(\lambda) = r_j[M]\boldsymbol{\alpha},$$

όπου $r_i[M]$ ορίζουμε να είναι η j^{η} γραμμή του πίνακα M.

3.2.4 Μια επαναληπτική μέθοδος (Weinstock method).

Η Weinstock μέθοδος (1960) σχηματίζει μια επαναληπτική μέθοδος , η οποία περιέχει πολλαπλασιασμούς και διαιρέσεις πολυωνύμων , στο αρχικό σύνολο των πολυωνύμων των οποίων ζητάμε να βρούμε τον ΜΚΔ τους , με σκοπό να υπολογιστεί τελικά ένα καινούριο πολυώνυμο , το οποίο θα έχει τον ελάχιστο δυνατό βαθμό και θα είναι βέβαια , ο ζητούμενος ΜΚΔ .Η παραπάνω μέθοδος βασίζεται σε ένα θεώρημα το οποίο αναφέρει ότι για οποιαδήποτε πολυώνυμα $\alpha_i(\lambda)$, $i = 1,2, \dots, n$, - των οποίων αναζητούμε τον μέγιστο κοινό διαιρέτη τους - ,το πολυώνυμο $g(\lambda)$ της μορφής :

$$\sum_{i=1}^{n} x_i(\lambda)\, \alpha_i(\lambda) = g(\lambda)$$

, το οποίο έχει τον ελάχιστο δυνατό βαθμό είναι ο ΜΚΔ των $\alpha_1(\lambda), \dots, \alpha_n(\lambda)$.

Ο αλγόριθμος ξεκινάει με ένα αυθαίρετο σύνολο από πολυώνυμα $x_1^0(\lambda), \dots, x_n^0(\lambda)$ τέτοια ώστε $x_1^0(\lambda)\alpha_1(\lambda) + \cdots + x_n^0(\lambda)\alpha_n(\lambda) = r_0(\lambda)$. Γενικά , ισχύει ότι $r_0(\lambda) \neq g(\lambda)$. Είναι εύκολο να αποδείξει κανείς ότι το $g(\lambda)$ είναι παράγοντας του $r_0(\lambda)$. Υπάρχει τουλάχιστον ένα $\alpha_j(\lambda)$ τέτοιο ώστε

$$\alpha_j(\lambda) = q(\lambda) r_0(\lambda) + r_1(\lambda)$$

με $\deg r_1(\lambda) < \deg r_0(\lambda)$ και $r_1(\lambda) \neq 0$.

Οπότε έχουμε ότι:

$$[-x_1^0(\lambda)q(\lambda)]a_1(\lambda) + [-x_2^0(\lambda)q(\lambda)]a_2(\lambda) + \cdots + \left[1 - x_j^0(\lambda)q(\lambda)\right]a_j(\lambda) + \cdots + [-x_n^0(\lambda)q(\lambda)]a_n(\lambda) = r_1(\lambda)$$

ή ισοδύναμα έχουμε:

$$x_1^1(\lambda)a_1(\lambda) + \cdots + x_n^1(\lambda)a_n(\lambda) = r_1(\lambda).$$

Η διαδικασία επαναλαμβάνεται μέχρι να προκύψει το $r_k(\lambda)$ το οποίο διαιρεί όλα τα πολυώνυμα $a_i(\lambda)$. Τότε αυτό το πολυώνυμο είναι ο ζητούμενος ΜΚΔ και τα $x_i^k(\lambda)$ είναι τα αντίστοιχα πολλαπλάσια.

3.2.5 Η μέθοδος ERES.

Οι περισσότερες από τις διαδικασίες εύρεσης του ΜΚΔ έως και το 1987 , εμπεριείχαν την χρήση του γενικευμένου τεστ του Βαρδουλάκη ή κάποιες εκδόσεις – παραλλαγές του Ευκλείδειου αλγόριθμου. Για μεγάλο αριθμό πολυωνύμων με πολύ υψηλή τάξη , οι παραπάνω μέθοδοι οδηγούσαν σε « υπολογιστική έκρηξη» . Μια εναλλακτική μέθοδο για τον υπολογισμό του ΜΚΔ προτάθηκε από τον Καρκανιά το 1978 . Η μέθοδος αυτή είναι βασισμένη στην ιδιότητα , του μέγιστου κοινού διαιρέτη , να παραμένει αναλλοίωτος μετά από στοιχειώδεις γραμμοπράξεις και μετατοπίσεις (μετατόπιση είναι μια διαδικασία χωρίς αριθμητικό σφάλμα) στον πίνακα της βάσης που συσχετίζεται με τα πολυώνυμα. Έτσι μετατρέπει τον υπολογισμό του ΜΚΔ στην τριγωνιοποίηση ενός συνόλου από πίνακες μικρότερων διαστάσεων. Η παραπάνω μέθοδος είναι γνωστή σαν μέθοδος ERES (*Extended Row Equivalence and Shifting)* και αποτελεί μια αποτελεσματική αριθμητική μέθοδο , εάν χρησιμοποιηθεί με τον κατάλληλο τρόπο καθώς δεν επηρεάζεται από τον αριθμό και την τάξη των πολυωνύμων.

Με κάθε σύνολο από m πολυώνυμα με μέγιστο βαθμό d (θα τα συμβολίζουμε $P_{m,d}$), θα τα συσχετίζουμε με έναν πίνακα βάσης P_m. Η κυριότερη ιδιότητα στην οποία στηρίχθηκε η θεωρητική διαδικασία του αλγόριθμου ERES (Καρκανιάς 1987) , ήταν όπως είπαμε και παραπάνω, ότι ο ΜΚΔ παραμένει αναλλοίωτος ύστερα από

στοιχειώδεις γραμμοπράξεις και μετατοπίσεις στον πίνακα P_m . Ένα από τα βασικότερα βήματα του θεωρητικού αλγόριθμου είναι η εκλογή του πίνακα P_r για τον χώρο των γραμμών του $P_{m,d}$, και στην συνέχεια ο μετασχηματισμός του σε άνω τριγωνιοποιήσιμη μορφή ή σε Ερμιτιανή μορφή $P_{r,d}^H$, μετά από στοιχειώδεις γραμμοπράξεις. Κάνοντας μετατοπίσεις και αλλεπάλληλες τριγωνιοποιήσεις στον πίνακα $P_{r,d}^H$, ο βαθμός των πινάκων που προκύπτουν κάθε φορά συνεχώς ελαττώνεται και τελικά αποκτάμε έναν πίνακα P_r . Ο πίνακας αυτός έχει βαθμίδα ίση με ένα (rank $P_r = 1$) και από αυτόν ορίζουμε τους συντελεστές του ΜΚΔ του συνόλου των πολυωνύμων $P_{m,d}$. Για να περιγραφεί ο αλγόριθμος θα χρειαστεί να αναφερθούν και να εξηγηθούν ορισμένα σύμβολα τα οποία θα χρησιμοποιηθούν παρακάτω.

Ας είναι λοιπόν :

$P_{m,d} := \{p_i(s): p_i(s) \in \mathbb{R}[s]\ , i \in m\ , d_i = \deg\{p_i(s)\}, d = \max\{d_i\ , i \in m\}\}$
$< P_{m,d} >:= \{P_{m_i,d'}, m_i \in \mathbb{Z}^+, d' \leq d\ , d \in \mathbb{Z}^+\}$.

Για οποιοδήποτε σύνολο $P_{m,d}$ ορίζουμε το διάνυσμα αντιπροσώπευσης (VR) $\boldsymbol{p}_m(s)$, και τον πίνακα βάσης (BM) P_m σαν :

$\boldsymbol{p}_m(s) = [\boldsymbol{p}_1(s), \boldsymbol{p}_2(s), \dots, \boldsymbol{p}_m(s)]^t = [\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_d] = P_m \boldsymbol{e}_d(s)$, όπου $P_m \in \mathbb{R}^{m\,x\,(d+1)}$ και $\boldsymbol{e}_d(s) = [1, s, \dots, s^d]^t$. Με $MK\Delta\ \{P_{m,d}\} = \varphi(s)$ θα ορίζουμε να είναι ο ΜΚΔ του συνόλου. Αν c είναι ακέραιος για τον οποίο ισχύει : $\boldsymbol{p_0} = \boldsymbol{p}_1 = \cdots = \boldsymbol{p}_{c-1} = 0$, $\boldsymbol{p}_c \neq 0$ τότε $c = \omega(P_{m,d})$,και θα ονομάζουμε την τάξη του $P_{m,d}$. Επιπρόσθετα , σαν s^c θα ονομάζεται ο στοιχειώδης διαιρέτης του ΜΚΔ .Το σύνολο $P_{m,d}$ θα ονομάζεται γνήσιο (proper) αν $c = 0$ και μη γνήσιο (non-proper) αν το $c \geq 1$, αντίστοιχα. Στην συνέχεια θα οριστούν και οι εξής πράξεις – διαδικασίες, οι οποίες είναι γνωστές και σαν μετασχηματισμοί ERES :

i. *Στοιχειώδες πράξεις γραμμών (γραμμοπράξεις) στον πίνακα* P_m
ii. *Πρόσθεση ή απαλοιφή μηδενικών γραμμών του πίνακα* P_m
iii. *Αν* $\boldsymbol{a}^t = [0, \dots, 0, a_\varepsilon, \dots a_{d+1}] \in \mathbb{R}^{1\,x\,(d+1)}, a_\varepsilon \neq 0$ *είναι μια γραμμή του* P_m *ορίζουμε την πράξη της μετατόπισης (shifting operation) shf:* $shf(\boldsymbol{a}^t) = \boldsymbol{a}^{*t} = [a_\varepsilon, \dots, a_{d+1}, 0, \dots, 0] \in \mathbb{R}^{1\,x\,(d+1)}$.

Οι παραπάνω πράξεις ερμηνεύονται διαφορετικά στα διάφορα πολυώνυμα, και για αυτόν τον λόγο θα γίνει προσπάθεια να εξηγηθούν. Με τον πρώτο (*i*) τύπο πράξεων , υποδηλώνεται ότι μπορεί να αναδιαταχθεί η σειρά στον πίνακα P_m , να πολλαπλασιαστούν οι συντελεστές του με μη μηδενικούς αριθμούς και να αντικατασταθεί το πολυώνυμο με έναν γραμμικό συνδυασμό όλων των πολυωνύμων του συνόλου. Αντίθετα , ο δεύτερος (*ii*) τύπος πράξεων , επιτρέπει να απαλειφθούν όλα τα μηδενικά πολυώνυμα από τον πίνακα P_m ,ή και να προστεθούν αντίστοιχα . Τέλος, ο τρίτος τύπος (*iii*) πράξεων υποδηλώνει ότι εάν ένα πολυώνυμο του συνόλου γράφεται $p(s) = s^c p'(s)$, τότε μπορεί να το αντικατασταθεί με το πολυώνυμο $p'(s)$, το οποίο έχει μικρότερο βαθμό από το αρχικό. Με τον συμβολισμό $shf(P_{m,d}) := P^*_{m,d}$, συμβολίζεται το σύνολο , το οποίο προκύπτει από το $P_{m,d}$, εκτελώντας μετατοπίσεις σε κάθε πολυώνυμο του.

Έτσι λοιπόν , σύμφωνα με τα παραπάνω προκύπτουν ορισμένες ιδιότητες για τον ΜΚΔ (Karcanias et al.,1993) .

ΘΕΩΡΗΜΑ 2.5.1 Για οποιοδήποτε σύνολο $P_{m,d}$ με πίνακα βάσης (ΒΜ) P_m , $\rho(P_m) = r$ και $\varphi(s) = MK\Delta\{P_{m,d}\}$ προκύπτουν οι ακόλουθες ιδιότητες :

i. *Εάν R είναι ο γραμμοχώρος του* P_m *, τότε το φ(s) είναι αναλλοίωτο από το R. Επιπλέον , αν* $r = dim R = d + 1$ *τότε* $\varphi(s) = 1$

ii. *Εάν* $\omega(P_{m,d}) = c \geq 1$ *και* $shf(P_{m,d}) = P^*_{m,d}$ *τότε*

$$\varphi(s) = MK\Delta\{P_{m,d}\} = s^c \cdot MK\Delta\{P^*_{m,d}\}$$

iii. *Εάν* $P_{m,d}$ *είναι γνήσιο σύνολο (proper) , τότε ο* $\varphi(s)$ *είναι αναλλοίωτος μετά από τις παραπάνω πράξεις.*

Συνοψίζοντας τις παραπάνω ιδιότητες ,προκύπτουν τα παρακάτω σημεία, που αξίζει να σημειωθούν , για την μεθοδολογία εύρεσης και υπολογισμού του ΜΚΔ πολυωνύμων:

i. *Δεν χρειάζονται όλα τα πολυώνυμα του* $P_{m,d}$ *για τον υπολογισμό του ΜΚΔ, αλλά μόνο ένα υποσύνολο του το οποίο έχει την ιδιότητα να παρέχει τον γραμμοχώρο R του πίνακα* P_m.

ii. *Ο υπολογισμός του ΜΚΔ μπορεί να μετατραπεί στην εύρεση του ΜΚΔ ενός γνήσιου συνόλου (proper set) ,εάν έχουμε εφαρμόσει μετατοπίσεις στο αρχικό σύνολο.*

iii. *Για ένα γνήσιο σύνολο* $P_{m,d}$ *,μια επιτυχημένη εφαρμογή τριγωνιοποίησης του πίνακα* P_m *με τους μετασχηματισμούς ERE ,οδηγεί σε μείωση του βαθμού από το αρχικό σύνολο.*

iv. *Αν για ένα σύνολο* $P_{m,d}$, $\rho(P_m) = 1$ *τότε οποιοδήποτε πολυώνυμο του* $P_{m,d}$ *ορίζει τον ΜΚΔ.*

Η θεωρητική διαδικασία ERES για τον υπολογισμό του ΜΚΔ $\varphi(s) = \{P_{m,d}\}$ ενός συνόλου $P_{m,d}$, με πίνακα βάσης (ΒΜ) P_m , $\rho(P_m) = r$ και $\omega(P_{m,d}) = c \geq 1$, μπορεί να περιγραφεί από τον παρακάτω αλγόριθμο.

Αλγόριθμος ERES

If $c \geq 1$ **then**

$P^*_{m,d} := shf(P_{m,d}), P^*_{m,d}$ γνήσιο

$\varphi(s) := s^c \cdot MK\Delta\{P^*_{m,d}\}$

while $P_{m,d}$ είναι γνήσιο **do**

if $r = d + 1$ **then**

$P_{m,d}$ είναι πρώτο (coprime), **quit**

else

if $r < d + 1$ **then**

if $r = 1$ **then**

$\varphi(s) :=$ όποιο μη μηδενικό πολυώνυμο του $P_{m,d}$, **quit**

else

if $r > 1$ **then**

όρισε το μέγιστο γραμμικό ανεξάρτητο σύνολο που αποτελείται από τα r διανύσματα των γραμμών του P_m

$P_{m,d} := P_{r,d}, P_r :=$ ο ΒΜ του $P_{m,d}$

$P^H_r :=$ η αριστερή κλιμακωτή μορφή (Left Echelon Form) του P_r

$t(s) := 1 + a_1 s + \cdots + a_\delta s^\delta$ το μικρότερο σε βαθμό πολυώνυμο του $shf(P^H_{r,d})$

If $\delta = 0$ **then**

$P_{m,d}$ είναι πρώτο (coprime) , **quit**

Else

If $\delta = 1,2$ **then**

Υπολόγισε τα μηδενικά του $t(s)$ και έλεγξε εάν είναι ή αν δεν είναι μηδενικά ενός διανύσματος αντιπροσώπευσης(VR) του $P_{m,d}$.

Διαμόρφωσε το $\varphi(s)$ από αυτές τις ρίζες

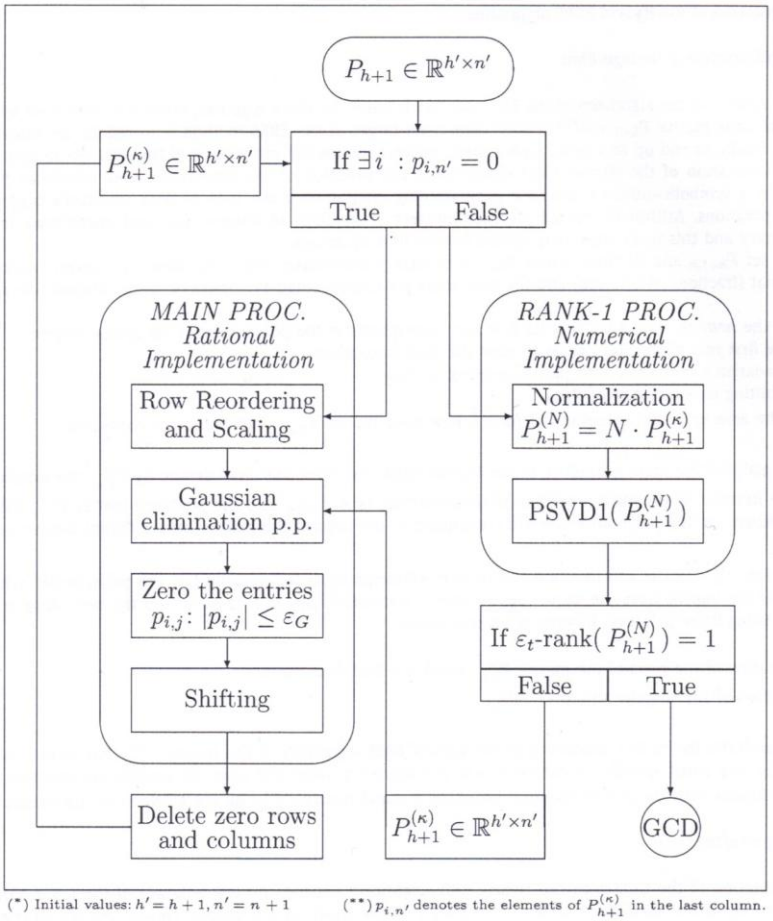
Else

If $\delta \geq 3$ **then**

$P^*_{m,d}$:=το αποτέλεσμα της εφαρμογής των μετασχηματισμών ERES στον $P^*_{m,d}$

$P_{m,d} := P^*_{r,d}$

Η παραπάνω διαδικασία θα τερματιστεί εξαιτίας ότι θα μειώνονται και η διάσταση (m) και ο βαθμός (d) των ισοδύναμων πολυωνύμων.



Επιπροσθέτως , αξίζει να τονισθεί ότι η διαδικασία ERES μειώνει τον βαθμό των πολυώνυμων που προκύπτουν κάθε φορά και τελειώνει , μόνο όταν ο τελικός πίνακα βάσης έχει βαθμίδα ίση με ένα. Για αυτόν τον λόγο καθώς επίσης και για διάφορους

άλλους (η χρήση μεθόδων για την τριγωνιοποίηση των πινάκων κ.α.) παρουσιάζεται ένας ανεπτυγμένος αριθμητικός αλγόριθμος που μας επιτρέπει τον υπολογισμό του ΜΚΔ πολυωνύμων (Karcanias et al.,1993).

Ας είναι $P_m \in \mathbb{R}^{m\,x\,n}, n = d + 1$ ένας πίνακας βάσης του $P_{m,d}$, $\varphi(P_m) = r, c \geq 0$ η τάξη του $P_{m,d}$, σ_i , $i = 1,2, \dots, \min\{m, n\}$ οι ιδιοτιμές του P_m, και $\varepsilon, \varepsilon_1$ δοσμένες ανοχές .

ΒΗΜΑ 1 **If** P_m είναι μη γνήσιος (non-proper) $(c \geq 1)$ **then**

$P_m \coloneqq [0_{m,c}, \overline{P_m}]$

s^c είναι ένας στοιχειώδης διαιρέτης του $\varphi(s)$ για s=0

$\varphi(s) \coloneqq s^c \cdot \overline{\varphi(s)}$ είναι ο ΜΚΔ του γνήσιου σύνολο που ορίζεται από το (ΒΜ) $\overline{P_m}$

$P_m = \overline{P_m}$

else

P_m είναι γνήσιος $(c = 0)$

Η πρώτη στήλη του P_m είναι μη μηδενική

$\varphi(0) \neq 0$

ΒΗΜΑ 2 **If** $\rho_\varepsilon(P_m) = n$ **then**

Τα πολυώνυμα είναι πρώτα μεταξύ τους

$\varphi(s) \coloneqq 1$,**quit**

Else

If $\rho_\varepsilon(P_m) = 1$ **then**

Οποιαδήποτε μη μηδενική γραμμή του P_m δίνει τους συντελεστές του $\varphi(s)$, **quit**

If $\rho_\varepsilon(P_m) \neq m$ **then**

Ψάξε να βρεις την καλύτερη βάση $\rho_\varepsilon(P_m) = r$ διανύσματα ανάμεσα στις γραμμές του πίνακα P_m και $P_r \in \mathbb{R}^{r\,x\,n}, r \leq n$ αντίστοιχος υποπίνακας του P_m

$P_m \coloneqq P_r$

ΒΗΜΑ 3 3.1 Αναδιέταξε τις γραμμές του P_mσε φθίνουσα σειρά σύμφωνα με τον αριθμό των μηδενικών σε αυτές.

3.2 **If** $\{\deg\{p_i(s)\}$ είναι το ίδιο για όλα τα $i = 1,2, \dots, m\}$ **then**

Ψάξε $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_m$ τις ιδιοτιμές του P_m

If $\{\sigma_1 \triangleq m$ και $\sigma_i \leq \varepsilon, i = 1,2,\dots,m\}$ **then**

Οποιαδήποτε σειρά του P_mδίνει τους συντελεστές του $\varphi(s)$, **quit**

3.3 Χρησιμοποίησε παραγοντοποίηση Gauss με μερική οδήγηση στον P_m και μετασχημάτισε τον σε πάνω τραπεζοειδή ή τριγωνική μορφή P_m^G.

$P_m := P_m^G$

3.4 $P_m :=$ η κανονικοποιημένη μορφή του P_m

3.5 Χρησιμοποίησε την πράξη της μετατόπισης στον P_m

3.6 Επανέλαβε το βήμα 3

Παράλληλα με τα παραπάνω αξίζει να σημειωθεί σε αυτό το σημείο ότι η μέθοδος ERES , εισάγει για πρώτη φορά την έννοια του «κατά προσέγγιση» ΜΚΔ (approximate GCD) για ένα σύνολο από πολυώνυμα. Η εισαγωγή της έννοιας «κατά προσέγγιση» γίνεται στην ανάγκη εφαρμογής της θεωρητικής διαδικασίας .Η ανάγκη αυτή οδηγεί στη χρήση αριθμητικών εργαλείων τα οποία θα αποφεύγουν μη σημαντικά αριθμητικά σφάλματα και θα επινοούν κατάλληλα κριτήρια τερματισμού του αλγορίθμου.

3.2.6 Ο SVD αλγόριθμος (Singular Value Decomposition)

Το 1995 εισάγετε ένας νέος αλγόριθμος για τον υπολογισμό του ΜΚΔ πολυωνύμων μια μεταβλητής (Corless et al.,1995). Ο αλγόριθμος αυτός είναι γνωστός σαν SVD αλγόριθμος (Singular Value Decomposition) ή αν προσπαθήσουμε να τον αποδώσουμε στα Ελληνικά ως αλγόριθμος με την βοήθεια ανάλυσης των χαρακτηριστικών τιμών ενός πίνακα. Ο αλγόριθμος αυτός σύμφωνα με τον Corless είναι πιο απλός και πιο έγκυρος, από διάφορους άλλους .

Για να μπορέσει κανείς να κατανοήσει τον αλγόριθμο , είναι σκόπιμο να αναφερθούν και να εξηγηθούν ορισμένες έννοιες που χρησιμοποιούνται στον αλγόριθμο. Αρχικά ας παρουσιάσουμε την (SVD) ανάλυση των χαρακτηριστικών τιμών ενός πίνακα. Για να αναλύσουμε έναν πίνακα Α με την βοήθεια των χαρακτηριστικών τιμών του εργαζόμαστε ως εξής :

- ✓ Υπολογίζουμε αρχικά τον ανάστροφο του πίνακα Α , δηλαδή τον A^T ·και στην συνέχεια το γινόμενο $A^T A$

- ✓ Στην συνέχεια υπολογίζουμε τις ιδιοτιμές του πίνακα A^TA και τις τοποθετούμε σε φθίνουσα σειρά , κατά απόλυτη τιμή. Οι χαρακτηριστικές τιμές του πίνακα A , είναι οι τετραγωνικές ρίζες των παραπάνω ιδιοτιμών.
- ✓ Κατασκευάζουμε τον διαγώνιο πίνακα Σ ο οποίος έχει στην κύρια διαγώνιο του ,τις παραπάνω χαρακτηριστικές τιμές τοποθετημένες σε φθίνουσα σειρά. Στην συνέχεια υπολογίζουμε τον αντίστροφο του Σ , δηλαδή τον Σ^{-1}
- ✓ Από το 2ο βήμα χρησιμοποιούμε τις ιδιοτιμές του πίνακα A^TA και υπολογίζουμε τα ιδιοδιανύσματα του. Έτσι κατασκευάζουμε τον V πίνακα , ο οποίος έχει σαν στήλες τα αντίστοιχα ιδιοδιανύσματα .Στην συνέχεια υπολογίζουμε τον ανάστροφο του V ,δηλαδή τον V^T.
- ✓ Τέλος υπολογίζουμε τον πίνακα U, όπου $U = AV\Sigma^{-1}$. Για να υπολογίσουμε την SVD ανάλυση γράφουμε τον A σαν $A = U\Sigma V^T$

Σε αυτό το σημείο αξίζει να σημειωθεί η διαφορά των ιδιοτιμών από τις χαρακτηριστικές τιμές ενός πίνακα. Συνήθως συγχέονται και ταυτίζονται αυτές οι δύο έννοιες, πράγμα το οποίο είναι λάθος. Αν ο πίνακας A είναι συμμετρικός θετικά ορισμένος , τότε και μόνο οι ιδιοτιμές ταυτίζονται με τις χαρακτηριστικές τιμές. Επιπρόσθετα με τα παραπάνω , αν μας δοθούν δύο πολυώνυμα

$p(x) = p_0 + p_1x + p_2x^2 + \cdots + p_mx^m$ και $q(x) = q_0 + q_1x + q_2x^2 + \cdots + q_nx^n$,

τότε ο πίνακας του Sylvester των p και q θα είναι ένας πίνακας $(n+m)\ x\ (n+m)$ διαστάσεων συμπληρωμένος ως εξής:

$$S = \begin{bmatrix} p_m & p_{m-1} & \cdot & \cdot & \cdot & p_1 & p_0 & 0 & \cdot & \cdot & 0 \\ 0 & p_m & p_{m-1} & \cdot & \cdot & \cdot & p_1 & p_0 & 0 & \cdot & 0 \\ 0 & 0 & p_m & \cdot & \cdot & \cdot & \cdot & p_1 & p_0 & 0 & \cdot \\ \cdot & \cdot & \cdot & & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & 0 & p_m & \cdot & & \cdot & \cdot & p_1 & p_0 & 0 \\ 0 & \cdot & & 0 & p_m & & \cdot & \cdot & & p_1 & p_0 \\ q_n & q_{n-1} & \cdot & \cdot & q_0 & 0 & 0 & \cdot & & & 0 \\ 0 & q_n & & & \cdot & q_0 & 0 & 0 & & & 0 \\ 0 & 0 & q_n & & \cdot & \cdot & q_0 & 0 & & & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & & \cdot & & \cdot & \cdot & \cdot \\ 0 & & & \cdot & & & \cdot & \cdot & & q_0 & 0 \\ 0 & \cdot & \cdot & 0 & q_n & q_{n-1} & 0 & \cdot & \cdot & q_1 & q_0 \end{bmatrix}$$

Με την βοήθεια όσων προαναφέραμε , μπορούμε τώρα να περιγράψουμε τον SVD αλγόριθμο. (Corless et al.,1995).

SVD αλγόριθμος

ΕΙΣΟΔΟΣ (Input) τα πολυώνυμα p και q με $\deg[p(x)] \geq \deg[q(x)]$ και περιθώριο ανοχής σφάλματος $\varepsilon > 0$

Διαδικασία:

Βήμα 1. Σχημάτισε τον πίνακα του Sylvester S ,για τα δύο πολυώνυμα p και q.

Βήμα 2. Άναλυσε τον πίνακα S με την βοήθεια των χαρακτηριστικών του τιμών (SVD) $S = U\Sigma V^T$

Βήμα 3. Βρες το μεγαλύτερο k τέτοιο ώστε $\sigma_k > \varepsilon\sqrt{m+n}$ και $\sigma_{k+1} \leq \varepsilon$ (αν όλα τα $\sigma_j > \varepsilon\sqrt{m+n}$ καθόρισε $d = 1$, και αν δεν ισχύει κάτι τέτοιο βγάλε λάθος) . Ο δείκτης k δηλώνει την τάξη του πίνακα S ($k = rankS$) και ο βαθμός του d θα είναι $n_d = n - k$.

Βήμα 4. Υπολόγισε το d με έναν από τους παρακάτω τρόπους:

(i) Υπολόγισε το d με τον συνηθισμένο τρόπο του Ευκλείδειου αλγόριθμου, και τερματισέ τον όταν ο βαθμός του υπολοίπου γίνει ίσο με n_d.

(ii) (Αυτή η λογική μέθοδος είναι αναπόδεικτη .) Συγκρότησε τις k γραμμές από επάνω του πίνακα $U^T S$ ή ισοδύναμα του ΣV^T. Υπολόγισε την κλιμακωτή διάταξη αυτού του πίνακα χρησιμοποιώντας απαλοιφή Gauss με μερική οδήγηση

(iii) Λύσε το πρόβλημα της παρακάτω ελαχιστοποίησης με βασικές τεχνικές βελτιστοποίησης .(Corless et al.,1995) Ο «κοντινός-ΜΚΔ» αποτελεί λύση του προβλήματος ελαχιστοποίησης $min_d \| C_p(d) q_1 - p2 + Cqd(q2 - q2$, όπου Cpd είναι ο $n+1 \; x \; n-nd+1$ πίνακας Cauchy ορισμένος από τους άγνωστους συντελεστές του «κοντινού-ΜΚΔ» d , βαθμού n_d. Αντίστοιχα , $C_q(d)$ είναι ο $(m+1)x\,(m - nd+1$ πίνακας Cauchy. Τέλος , $q1$ και $q2$ είναι τα άγνωστα διανύσματα των συντελεστών που προκύπτουν από το πηλίκο των πολυωνύμων. Το πρόβλημα αυτό λύνετε σαν ένα μη γραμμικό πρόβλημα ελαχίστων τετραγώνων και έτσι βρίσκετε το $d(x)$.

3.2.7 Matrix pencil αριθμητική μέθοδος για τον υπολογισμό του ΜΚΔ.

Το 1994 ο Καρκανιάς εισάγει μια καινούρια μέθοδο για τον υπολογισμό του μέγιστου κοινού διαιρέτη ενός συνόλου m πολυωνύμων $P_{m,d}$, μέγιστου βαθμού d. Η παραπάνω μέθοδος βασίζεται στην ιδιότητα ότι ο μέγιστος κοινός διαιρέτης του $P_{m,d}$ είναι τα αποσυζευτικά μηδενικά εξόδου (output decoupling zeros) του ενός γραμμικού συστήματος $S(\hat{A}, \hat{C})$, το οποίο συνδέεται με το $P_{m,d}$ (Karcanias et al.,1994). Ο υπολογισμός του ΜΚΔ μετατρέπεται στην εύρεση των μηδενικών των $sW - AW$, όπου W είναι ο μη παρατηρήσιμος υποχώρος του $S(\hat{A}, \hat{C})$. Το 2006, (Karcanias et al.,2006) ο Καρκανιάς εξετάζει όλες τις matrix pencil μεθόδους για τον υπολογισμό του ΜΚΔ χρησιμοποιώντας στην ανάπτυξη των αλγορίθμων συμβολικό και αριθμητικό προγραμματισμό , που τα αναφέρει σαν «υβριδικούς υπολογισμούς» (hybrid computations). Ο συνδυασμός των αριθμητικών διαδικασιών με τον συμβολικό προγραμματισμό βελτιώνει την φύση του αλγόριθμου και εγγυάται την σταθερότητα του.

Αλγόριθμος standard matrix pencil

Βήμα 1. Υπολόγισε τον πίνακα βάσης M για τον δεξιό μηδενοχώρο $N_r(P_m)$ χρησιμοποιώντας τον SVD (Singular Value Decomposition) αλγόριθμο.

Βήμα 2. Δημιούργησε τον M_1 διαγράφοντας την τελευταία σειρά του M.

Βήμα 3. Υπολόγισε τον πίνακα $\hat{C}$ τέτοιο ώστε $\hat{C}M = 0$

Βήμα 4. Δημιούργησε τον πίνακα παρατηρησιμότητας $Q(\hat{A}, \hat{C}) = \left[\hat{C}^t, \hat{A}^t\hat{C}^t, \ldots, (\hat{A}^t)^{d-1}\hat{C}^t \right]^t$

Βήμα 5. Υπολόγισε τον δεξιό μηδενοχώρο $W = N_r\left(Q(\hat{A}, \hat{C})\right)$ χρησιμοποιώντας τον SVD (Singular Value Decomposition).

Βήμα 6. Δημιούργησε pencil matrix $Z(s) = sW - \hat{A}W$. Οποιοσδήποτε μικρότερου βαθμού μέγιστης τάξης $Z(s)$ ορίζει τον ΜΚΔ των πολυωνύμων.

Resultant matrix pencil μέθοδος

Βήμα 1. Υπολόγισε τον πίνακα βάσης $\widetilde{M}$ για τον δεξιό μηδενοχώρο του πίνακα του Sylvester S.

Βήμα 2. Όρισε τον ΜΚΔ pencil matrix $\tilde{Z}(s) = s\widetilde{M_1} - \widetilde{M_2}$, όπου $\widetilde{M_1}$ και $\widetilde{M_2}$ είναι οι πίνακες οι οποίοι προκύπτουν από τον $\widetilde{M}$, αν διαγράψουμε την τελευταία και την πρώτη σειρά από το $\widetilde{M}$, αντίστοιχα.

Βήμα 3. Υπολόγισε οποιοδήποτε μη μηδενική ελάσσων ορίζουσα $d(s)$ του $\tilde{Z}(s)$ και έτσι βρίσκουμε τον ΜΚΔ . Δηλαδή $MK\Delta = d(s)$.

Στην συνέχεια παρουσιάζεται ένα παράδειγμα το οποίο θα βοηθήσει τον αναγνώστη να καταλάβει και να κατανοήσει πλήρως τους δύο παραπάνω αλγορίθμους.

Παράδειγμα:

Να υπολογίσετε τον ΜΚΔ των πολυωνύμων :

$$\begin{cases} p_1(s) = s^3 - 6s^2 + 11s - 6 \\ p_2(s) = s^2 - 3s + 2 \\ p_3(s) = s^2 - 2s + 1 \\ p_4(s) = s^2 - 4s + 3 \end{cases}$$

Όπως παρατηρούμε παραπάνω πρόκειται ένα σύνολο από τέσσερα πολυώνυμα , με μέγιστο βαθμό 3 , και δεύτερο μέγιστο βαθμό 2.

Standard matrix pencil μέθοδος .

Ο πίνακας βάσης P_m είναι :

$$P_m = \begin{bmatrix} -6 & 11 & -6 & 1 \\ 2 & -3 & 1 & 0 \\ 1 & -2 & 1 & 0 \\ 3 & -4 & 1 & 0 \end{bmatrix} \epsilon \mathbb{R}^{4\times 4}$$

Όπου ο πίνακας των χαρακτηριστικών τιμών του πίνακα P_m χρησιμοποιώντας τον SVD αλγόριθμο , έχουμε από το MATLAB ([U,S,V]=svd(a)) τον πίνακα των χαρακτηριστικών τιμών

$$S = \begin{bmatrix} 15.4156 & 0 & 0 & 0 \\ 0 & 1.5221 & 0 & 0 \\ 0 & 0 & 0.2088 & 0 \\ 0 & 0 & 0 & 0.0000 \end{bmatrix}$$

και τον πίνακα V να είναι

$$V = \begin{bmatrix} 0.4541 & -05807 & 0.4535 & 0.5000 \\ -0.7944 & 0.0714 & 0.3373 & 0.5000 \\ 0.3979 & 0.7685 & 0.0335 & 0.5000 \\ -0.0586 & -0.2591 & -0.8243 & 0.5000 \end{bmatrix}$$

Όπου η ανοχή που χρησιμοποιήσαμε είναι 10^{-15}.Η τελευταία χαρακτηριστική τιμή είναι πολύ μικρή και μπορεί να θεωρηθεί μηδέν . Οι στήλες του V οι οποίες αντιστοιχούν στην μηδενική χαρακτηριστική τιμή S είναι η τελευταία , και έτσι ο πίνακας M είναι

$$M = \begin{bmatrix} 0.5000 \\ 0.5000 \\ 0.5000 \\ 0.5000 \end{bmatrix}$$

και ο αντίστοιχος M_1 διαγράφοντας την τελευταία σειρά είναι

$$M_1 = \begin{bmatrix} 0.5000 \\ 0.5000 \\ 0.5000 \end{bmatrix}$$

Στην συνέχεια πρέπει να υπολογίσουμε τον πίνακα $\hat{C}$ τέτοιος ώστε $\hat{C}M_1 = 0$. Όπου θα τον υπολογίσουμε αν εφαρμόσουμε SVD ανάλυση στον ανάστροφο πίνακα του M_1 και ο $\hat{C}$ θα είναι ο βάση για τον μηδενοχώρο του M_1^T.

Έτσι προκύπτει ότι

$$\hat{C} = \begin{bmatrix} 0.5774 & 0.7887 & -0.2113 \\ 0.5774 & -0.2113 & 0.7887 \end{bmatrix}$$

Για το πολυώνυμο $p_1(s)$ ο συνοδεύον πίνακας (companion matrix) και ο πίνακας παρατηρησιμότητας είναι αντίστοιχα

$$\hat{A} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 6 & -11 & 6 \end{bmatrix}$$

και έτσι $Q(\hat{A}, \hat{C}) = \begin{bmatrix} 0.5774 & 0.7887 & -0.2113 \\ 0.5774 & -0.2113 & 0.7887 \\ -1.2678 & 2.9017 & -0.4791 \\ 4.7322 & -8.0983 & 4.5209 \\ -2.8746 & 4.0023 & 0.0271 \\ 27.1254 & -44.9977 & 19.0271 \end{bmatrix}$

Από όπου προκύπτει ο πίνακας W , ο οποίος είναι ο δεξιός μηδενοχώρος του πίνακα $Q(\hat{A}, \hat{C})$. Επομένως , έχουμε :

$$W = \begin{bmatrix} -0.8313 \\ -0.5456 \\ -0.1059 \end{bmatrix}$$

Και έτσι pencil πίνακας είναι :

$$Z(s) = sW - \hat{A}W = \begin{bmatrix} -0.8313s + 0.5456 \\ -0.5456s + 0.5456 \\ -0.1059s + 0.1059 \end{bmatrix}$$

Από όπου η ελάχιστη ορίζουσα είναι $Det\big(Z(s)\big) = -0.5456s + 0.5456 = -0.5456(s-1)$

Άρα ο ΜΚΔ των $\{p_1(s), p_2(s), p_3(s), p_4(s)\}$ είναι ο $MK\Delta = s - 1$.

■

Να σημειώσουμε σε αυτό το σημείο ότι ο αλγόριθμος δουλεύει ομοίως και ανάλογα και με την Resultant matrix pencil μέθοδο. Η διαφορά τους είναι ότι στον δεύτερο πίνακα υπολογίζουμε τον πίνακα του Sylvester . Σε σχέση με τον πίνακα P_m ο πίνακας του Sylvester S, είναι μεγαλύτερου μεγέθους και έτσι οι πράξεις θα ήταν σαφώς πιο πολύπλοκες .

3.2.8 ΜΚΔ και το Generalized Resultant θεώρημα.

Αν θεωρήσουμε το σύνολο των πολυωνύμων :

$$P_{h+1,n} = \{a(s), b_i(s) \in \mathbb{R}[s] , n = \deg\{a(s)\} , n \geq \deg\{b_i(s)\}, i = 1,2, \dots, h\}$$

και

$$p = \max\{\deg\{b_i(s)\} , i = 1, \dots, h\}.$$

Αναπαριστάνουμε τα πολυώνυμα $a(s), b_i(s)$ σε σχέση με τους μέγιστους βαθμούς τους n και p , αντίστοιχα ως εξής:

$$a(s) = s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0$$

και

$$b_i(s) = b_{i,p}s^p + \cdots + b_{i,1}s + b_{i,0}, \ i = 1,2, \dots, h.$$

Το σύνολο $P_{h+1,n}$ θα λέγεται (n,p) τάξης πολυωνυμικό σύνολο ή θα το παρουσιάζουμε συντετμημένα σαν P. Τον μέγιστο κοινό διαιρέτη του P θα τον συμβολίζουμε με $\varphi(s)$.

Επιπρόσθετα με τα παραπάνω ,για κάθε σύνολο P ορίζουμε το διάνυσμα αντιπροσώπευσης $\boldsymbol{p_{h+1}}(s) = [a(s), b_1(s), \dots, b_h(s)]^t$ και τον πίνακα βάσης P_{h+1}.

Θεωρώντας όλα τα παραπάνω μπορούμε να ορίσουμε έναν πίνακα $p \times (n+p)$, ο οποίος θα συνδέεται με τον πολυώνυμο $\alpha(s)$ ως εξής:

$$S_0 = \begin{bmatrix} 1 & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & 1 & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & a_{n-1} & \cdots & \cdots & a_1 & a_0 \end{bmatrix}$$

και τον $n \times (n+p)$ πίνακα , αντίστοιχα ο οποίος συνδέεται με τα πολυώνυμα $b_i(s), i = 1,2, \dots, h$ ως εξής :

$$S_i = \begin{bmatrix} b_{i,p} & b_{i,p-1} & b_{i,p-2} & \cdots & b_{i,1} & b_{i,0} & 0 & \cdots & \cdots & 0 \\ 0 & b_{i,p} & b_{i,p-1} & \cdots & \cdots & b_{i,1} & b_{i,0} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & b_{i,p} & b_{i,p-1} & \cdots & \cdots & \cdots & b_{i,1} & b_{i,0} \end{bmatrix}$$

για κάθε $i = 1,2, \dots h$.

Παράλληλα , ο εκτεταμένος πίνακας Sylvester (extended Sylvester matrix) ή διαφορετικά ο γενικευμένος resultant (generalized resultant matrix) για το σύνολο *P* , ορίζεται ως εξής: $S_p = \begin{bmatrix} S_0 \\ S_1 \\ \vdots \\ S_h \end{bmatrix} \in \mathbb{R}^{(p+hn)\times(n+p)}$.

Ο πίνακας S_p ,είναι ο πίνακας βάσης για το σύνολο των πολυωνύμων ,

$$S[P] = \{a(s), sa(s), \dots, s^{p-1}a(s); b_1(s), \dots b_h(s), sb_h(s), \dots s^{n-1}b_h(s)\}$$

ο οποίος είναι γνωστός και σαν Sylvester resultant σύνολο (Sylvester resultant set) ενός δοσμένου συνόλου *P*.

Σύμφωνα με όλα τα παραπάνω , καθώς επίσης και με (Karcanias et al.,2004) , (Vardulakis et al.,1978) διατυπώνεται το γενικευμένο Resultant θεώρημα (Generalized Resultant Theorem) το οποίο βοηθάει πολύ στον υπολογισμό του μέγιστου κοινού διαιρέτη .

Θεώρημα 1. Γενικευμένο Resultant θεώρημα (Generalized Resultant Theorem)
Δίνοντας ένα σύνολο από πολυώνυμα $\alpha(s)$ και $b_i(s)$, το οποίο έχει εκτεταμένο πίνακα Sylvester (generalized resultant) S_p , ισχύουν οι παρακάτω ιδιότητες:

i. *Μια ικανή και αναγκαία συνθήκη για να είναι πρώτο (coprime) μεταξύ τους , ένα σύνολο από πολυώνυμα, είναι να ισχύει :*

$$\rho(S_p) = n + p$$

,όπου $\rho(S_p)$*: η τάξη του πίνακα* S_p.

ii. *Αν είναι* $\varphi(s)$ *ο ΜΚΔ του συνόλου P, τότε :*

$$\rho(S_p) = n + p - \deg\{\varphi(s)\}.$$

iii. *Αν μετατρέψουμε τον πίνακα* S_p *σε κλιμακωτή μορφή , χρησιμοποιώντας στοιχειώδες γραμμοπράξεις , τότε η τελευταία μη μηδενική σειρά , ορίζει τους συντελεστές του ΜΚΔ του συνόλου των πολυωνύμων.*

3.2.9 Ακολουθία πολυωνυμικών υπολοίπων (PRS)

Ένας από τους πιο γνωστούς αλγορίθμους για τον υπολογισμό του ΜΚΔ πολυωνύμων μιας μεταβλητής είναι η ακολουθία πολυωνυμικών υπολοίπων (Polynomial Remainder Sequence – PRS). Ο παραπάνω αλγόριθμος αποτελεί μια γενίκευση του ευκλείδειου αλγορίθμου και είναι πολύ απλός στην χρήση του. Φαινομενικά δεν υπάρχει πρόβλημα στην χρήση του , αντίθετα όμως στην πράξη είναι αρκετά δύσκολο. Στις περισσότερες πρακτικές εφαρμογές , οι συντελεστές των πολυωνύμων είναι αριθμοί κινητής υποδιαστολής , και κάνουμε αυθαίρετα αποκοπές οι οποίες επηρεάζουν το ακριβές αποτέλεσμα του αλγορίθμου.

Αλγόριθμος PRS (Noda et al., 1991)

Είσοδος : *Πολυώνυμα* P_1 *και* P_2 *με συντελεστές ρητούς αριθμούς , όπου* $deg(P_1) \geq deg\ (P_2)$

Έξοδος : *Μέγιστος Κοινός Διαιρέτης των* P_1 *και* P_2 *:* $ΜΚΔ(\ P_1, P_2)$

Μέθοδος : $i \coloneqq 2;$

while $P_i \neq 0$ ***do***

begin

$P_{i+1} \coloneqq υπόλοιπο\ (\ P_{i-1}, P_i);$

$i \coloneqq i + 1$

end

return $pp(P_{i-1})$

Όπου $pp(P_{i-1})$ συμβολίζουμε το αρχικό μέρος του πολυωνύμου (primitive part).

3.3 Ο κατά προσέγγιση ΜΚΔ (approximate GCD).

Όπως αναφέραμε και παραπάνω η έννοια του Μέγιστου Κοινού Διαιρέτη των πολυωνύμων , χαρακτηρίζεται από την ιδιότητα ότι ο υπολογισμός του είναι non-generic. Η ανάγκη ορισμού εννοιών όπως «σχεδόν μηδέν» ή «κατά προσέγγιση ΜΚΔ» (appropriate GCD) ,έχει αναγνωριστεί σαν σημαντική σε πολλές εφαρμογές. Το πρόβλημα του «κατά προσέγγιση» ΜΚΔ εγείρεται κάθε φορά , που πρέπει χειριστούμε «μη τελείως γνωστά» πολυώνυμα, όταν οι συντελεστές προκύπτουν μετά από μετρήσεις ή όταν έχουμε πράξεις πολυωνύμων με συντελεστές κινητής υποδιαστολής (floating point coefficients) στον υπολογιστή. Ο υπολογισμός του ΜΚΔ είναι ένα μη ευσταθές πρόβλημα. Μια πολύ μικρή διαταραχή στο πολυώνυμο μπορεί να αλλάξει ολόκληρη την απάντηση.

Για να υπολογίσουμε τον ακριβή ΜΚΔ για n πολυώνυμα , είναι αρκετό να ξέρουμε να υπολογίζουμε τον ΜΚΔ για δύο πολυώνυμα. Για τον « κατά προσέγγιση » ΜΚΔ , ο υπολογισμός είναι τελείως διαφορετικός (Rupprecht ,1998). Με το θέμα του «κατά προσέγγιση» ΜΚΔ έχουν ασχοληθεί οι Schoenhage (1985) , Noda και Sasaki (1996) , Karmarkar και Lakshman (1996) , οι οποίοι εξετάζουν το θέμα στο γενικότερο ευρύτερο πλαίσιο της Ευκλείδειας διαίρεσης και για την περίπτωση των δύο πολυωνύμων. Ο Chin (Chin et al. , 1998) μελετάει και προτείνει μεθόδους για τον υπολογισμό του βαθμού του ΜΚΔ χρησιμοποιώντας SVD (ανάλυση χαρακτηριστικών τιμών) σε πίνακες Sylvester . Παράλληλα , προτείνει βελτιστοποιημένες στρατηγικές για τον υπολογισμό του «κατά προσέγγιση» ΜΚΔ. Η ουσία των παραπάνω μεθόδων για την παρουσίαση του «κατά προσέγγιση» ΜΚΔ είναι η «χαλάρωση» των χαρακτηριστικών ιδιοτήτων και συνθηκών , οι οποίες διέπουν τον ακριβή ΜΚΔ. Η δυσκολία σε όλες τις μεθόδου υπολογισμού του «κατά προσέγγιση» ΜΚΔ είναι , να εγγυηθούν το πόσο καλή προσέγγιση είναι αυτή που προσφέρουν.

Στην συνέχεια της εργασίας θα παραταθούν ορισμένοι αλγόριθμοι για τον υπολογισμό του «κατά προσέγγιση» ΜΚΔ πολυωνύμων , αλλά δεν θα επεκταθούμε

στο παρών θέμα. Ο αναγνώστης μπορεί να ανατρέξει στην παραπάνω προτεινόμενη βιβλιογραφία για περαιτέρω προσέγγιση του θέματος.

3.3.1 Ο «κατά προσέγγιση» ΜΚΔ και ο matrix pencil αλγόριθμος.

Ο resultant pencil πίνακας τροποποιημένος κατάλληλα , μπορεί να χρησιμοποιηθεί για την «κατά προσέγγιση» έννοια του ΜΚΔ για πολυώνυμα. Αυτό συμβαίνει γιατί οι συντελεστές των αρχικών πολυωνύμων του συνόλου όπου θέλουμε να υπολογίσουμε τον ΜΚΔ ,συνήθως προκύπτουν από πειράματα ή από αριθμητικούς υπολογισμούς. Για παράδειγμα γίνεται συχνά, αντί για 0.9999 να χρησιμοποιούμε το 1 στους συντελεστές.

Κάνοντας τον SVD αλγόριθμο στον πίνακα Sylvester είναι πιθανό όλες οι χαρακτηριστικές τιμές να είναι θετικές. Αυτό σημαίνει ότι ο δεξιός μηδενοχώρος του S θα είναι ένας άδειος πίνακας και δεν θα υπάρχει ακριβώς ΜΚΔ για τα πολυώνυμα , και έτσι θα είναι πρώτα. Σε αυτή την περίπτωση πρέπει να υπολογίσουμε τον «κατά προσέγγιση» ΜΚΔ(Karcanias et al. , 2006) . Ο παρακάτω αλγόριθμος εφαρμόζεται στον Sylvester resultant και χρησιμοποιεί την έννοια του «κοντινός μηδενοχώρου» ενός πίνακα. Ένα προτέρημα του συγκεκριμένου αλγορίθμου είναι ότι τεστάρει την «ποιότητα» του ΜΚΔ που προκύπτει. $(colspan\{\widetilde{M_1}\} \neq colspan\{\widetilde{M_2}\})$

Βήμα 1. *Όρισε ένα 'ξεκίνημα' (threshold)* $t > 0$ *. Εφάρμοσε SVD ανάλυση στον πίνακα* S^**. Όρισε μια βάση M για τον δεξιό «κοντινό μηδενοχώρο» του πίνακα του Sylvester* S^**.*

Βήμα 2. *Όρισε τον ΜΚΔ pencil matrix* $\tilde{Z}(s) = s\widetilde{M_1} - \widetilde{M_2}$ *, όπου* $\widetilde{M_1}$ *και* $\widetilde{M_2}$ *είναι οι πίνακες οι οποίοι προκύπτουν από τον* $\tilde{M}$ *, αν διαγράψουμε την τελευταία και την πρώτη σειρά από το* $\tilde{M}$ *, αντίστοιχα.*

Βήμα 3. *Κατασκεύασε έναν πίνακα με στοιχεία όλα τις μη μηδενικές ελάσσων ορίζουσες του* $\tilde{Z}(s)$ *και υπολόγισε την βάση του* $\tilde{B}$*.*

Βήμα 4. *Χρησιμοποίησε τον SVD αλγόριθμο στον πίνακα* $\tilde{B}$*:* $\tilde{B} = \tilde{U}^T \tilde{\Sigma} \tilde{V}$*. Η στήλη του* $\tilde{V}$*, η οποία αντιστοιχεί στην μεγαλύτερη χαρακτηριστική τιμή δίνει τους συντελεστές του ΜΚΔ.*

Βήμα 5. *Υπολόγισε την space angle των* $\widetilde{M_1}$ *και* $\widetilde{M_2}$ *για να κρίνει πόσο καλή είναι η προσέγγιση που έκανες.*

3.3.2 Ένας απλός αλγόριθμος για τον «κατά προσέγγιση» ΜΚΔ.

Οι Noda και Sasaki (Noda et al., 1991) ορίζουν τον «κατά προσέγγιση» ΜΚΔ πολυωνύμων με την βοήθεια της ακρίβεια ε .Στην συνέχεια παρουσιάζεται ο αλγόριθμός .

Αλγόριθμος για τον «κατά προσέγγιση» ΜΚΔ

Είσοδος : Κανονικά πολυώνυμα $P_1(x)$ και $P_2(x), \deg(P_1) \geq \deg(P_2)$; ένας μικρός θετικός αριθμός ε $0 < \varepsilon \ll 1$

Έξοδος : Ο «κατά προσέγγιση» ΜΚΔ των $P_1(x)$ και $P_2(x)$, με ακρίβεια μικρότερη από *ε;*

Μέθοδος : Υπολόγισε την πολυωνυμική ακολουθία υπολοίπων (PRS)

$$\left(P_1, P_2, \ldots, P_k \neq 0(cutoff\ \varepsilon), P_{k+1} = 0\ (cutoff\ \varepsilon)\right)$$

με την επαναληπτική μέθοδο

$$Q_i = \pi\eta\lambda\iota\kappa\acute{o}\ (P_{i-1}, P_i);$$

$$P_{i-1} = Q_i P_i + \max\{1, mmc(Q_i)\} \times P_{i+1}\ ,\ i = 2,3, \ldots, k$$

return P_k.

$mmc(P)$: ο μεγαλύτερος σε απόλυτη τιμή συντελεστής P.

Δηλαδή $mmc(P) = \max\{|a_1|, \ldots, |a_n|\}$, όπου a_i οι συντελεστές του πολυωνύμου P.

ΚΕΦΑΛΑΙΟ 4ο
Μέγιστος Κοινός Διαιρέτης Πολυωνύμων Δύο Μεταβλητών

4.1 Εισαγωγή

Τα πολυώνυμα μπορούν να κατηγοριοποιηθούν εξαιτίας πολλών διαφορετικών ιδιοτήτων. Μία από τις κατηγοριοποιήσεις είναι βασισμένες στον αριθμό των μεταβλητών που έχει κάθε πολυώνυμο. Το πολυώνυμο με μία μεταβλητή ονομάζεται πολυώνυμο μιας μεταβλητής (univariate polynomial) , ενώ με περισσότερες μεταβλητές ονομάζεται πολυμεταβλητό πολυώνυμο (multivariate polynomial).

Ορίζουμε ***πολυώνυμο*** (Cox et al. , 1996) f **με μεταβλητές** $x_1, x_2, x_3, \dots, x_n$ και συντελεστές από το k σώμα , να είναι πεπερασμένος γραμμικός συνδυασμός μονωνύμων. Θα γράφουμε το πολυώνυμο f στην μορφή

$$f = \sum_a a_a \, x^a \quad , a \in k$$

όπου το άθροισμα είναι ένας πεπερασμένος αριθμός ν-άδων $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$. Το σύνολο όλων των πολυωνύμων με μεταβλητές $x_1, x_2, x_3, \dots, x_n$ και συντελεστές από το k το συμβολίζουμε $k[x_1, \dots, x_n]$.

Για παράδειγμα το πολυώνυμο :

$$f = 2x^2y^5z - \frac{4}{5}z^8 + xy - x^3$$

Είναι ένα πολυώνυμο στο σώμα $\mathbb{Q}[x, y, z]$. Ας παραθέσουμε ορισμένα βασικά από τα πολυώνυμα τα οποία θα τα χρειαστούμε παρακάτω :

Ας είναι $f = \sum_a a_a \, x^a$ ένα πολυώνυμο στο $k[x_1, \dots, x_n]$.

i. Θα ονομάζουμε α_α συντελεστή του μονώνυμου x^a.

ii. Αν $\alpha_\alpha \neq 0$ τότε τον $\alpha_\alpha x^a$ θα τον ονομάζουμε όρο του πολυωνύμου f.

iii. Ο συνολικός βαθμός (total degree) ενός πολυωνύμου f , συμβολίζεται $\boldsymbol{t}\deg(f)$ και είναι μέγιστο των εκθετών συμπεριλαμβανομένου και του αθροίσματος των εκθετών σε όρο του πολυωνύμου που περιέχει το γινόμενο των μεταβλητών.

Για παράδειγμα το πολυώνυμο $f = 2x^2y^5z - \frac{4}{5}z^8 + xy - x^3$, το οποίο είδαμε παραπάνω έχει τέσσερις όρους και έχει ολικό βαθμό οκτώ , ενώ το πολυώνυμο $f = 2x^{12} - 2x^7y^2z + yz^4 - 4y^6$, έχει ολικό βαθμό 12.

Τα πολυώνυμα όπως αναφέραμε και παραπάνω μπορούν να περιέχουν και παραπάνω από μία μεταβλητή. Αυτά είναι τα πολυμεταβλητά πολυώνυμα. Οι πολυωνυμικοί δακτύλιοι με πεπερασμένο αριθμό μεταβλητών είναι μια από τις βασικές έννοιες οι οποίες χρησιμοποιούνται στην αλγεβρική γεωμετρία (algebraic geometry). Η αλγεβρική γεωμετρία είναι ένας κλάδος των μαθηματικών ο οποίος συνδυάζει τεχνικές από την αφηρημένη άλγεβρα , και ειδικότερα από την αντιμεταθετική άλγεβρα με την γλώσσα και τα προβλήματα της γεωμετρίας .
Ένα από τα θέματα που εξετάζουν όσοι ασχολούνται με τα πολυμεταβλητά πολυώνυμα είναι ο υπολογισμό του ΜΚΔ των πολυωνύμων αυτών .

4.2 Μέγιστος Κοινός Διαιρέτης Πολυωνύμων Δύο μεταβλητών

Ο υπολογισμός του Μέγιστου Κοινού Διαιρέτη πολυωνύμων δύο μεταβλητών ,αποτελεί σημείο μελέτης για πολλούς ερευνητές. Η μελέτη των αλγορίθμων αυτών έχει μια πολύ μακριά ιστορία .Η ιδέα γενίκευσης του Ευκλείδειου αλγόριθμου για ΜΚΔ ακεραίων σε ΜΚΔ πολυωνύμων εμφανίζεται τον 16^{ο} αιώνα . Ωστόσο το 1967 ο Collins προσπαθεί να κάνει μια ανάλυση του Ευκλείδειου αλγόριθμου για τον ΜΚΔ πολυμεταβλητών πολυωνύμων. Αργότερα υπάρχουν αρκετοί οι οποίοι ασχολήθηκαν με αυτό . Ο υπολογισμός του ΜΚΔ πολυμεταβλητών πολυωνύμων , άρα και κατ' επέκταση και πολυωνύμων με δύο μεταβλητές είναι από τις πιο σημαντικές διαδικασίες στην Υπολογιστική Άλγεβρα (computer algebra) και επομένως αναζητάμε τους πιο αποδοτικούς αλγορίθμους .

Στην συνέχεια θα προσπαθήσουμε να παρουσιάσουμε τους πιο σημαντικούς αλγορίθμους για την εύρεση του ΜΚΔ πολυωνύμων με δύο μεταβλητές. Στους περισσότερους αλγόριθμους έχει γίνει αναγωγή του αρχικού αλγορίθμου για πολυώνυμα με δύο μεταβλητές . Επιπρόσθετα αναφέρουμε και τρόπους υπολογισμού «κατά προσέγγιση» ΜΚΔ .

4.2.1 Υπολογισμός ΜΚΔ με παρεμβολή.

Ας υποθέσουμε ότι έχουμε n πολυώνυμα $p_i(x,y) \in \mathbb{R}[x,y], i = 0,1,\dots,n-1$. Αυτά τα πολυώνυμα μπορούν να γραφούν στην μορφή (Karampetakis et al.,2007) :

$$p_i(x,y) = p_{i,x}(x)g_x(x)p_{i,x,y}(x,y)g_{x,y}(x,y)p_{i,y}(y)g_y(y)$$

$$= \sum_{m=0}^{M_1}\sum_{j=0}^{M_2} p_{i,m,j}x^m y^j \in \mathbb{R}[x,y] \quad , i = 0,1,\dots,n-1 \qquad (1)$$

Για λόγους ευκολίας που θα χρησιμοποιήσουμε παρακάτω συμβολίζουμε: $p'_{i,x}(x) = p_{i,x}(x)g_x(x), p'_{i,x,y}(x,y) = p_{i,x,y}(x,y)g_{x,y}(x,y), p'_{i,y}(y) = p_{i,y}(y)g_y(y)$.

Συμβολίζουμε M_1 την μεγαλύτερη δύναμη του x στο $p_i(x,y)$, και M_2 αντίστοιχα την μεγαλύτερη δύναμη του y στο $p_i(x,y)$. Παράλληλα ,τα πολυώνυμα $p_{i,x}(x) \in \mathbb{R}[x]$ είναι πρώτα μεταξύ τους. Ομοίως τα $p_{i,y}(y) \in \mathbb{R}[y]$ είναι πρώτα μεταξύ τους, και τα $p_{i,x,y}(x,y) \in \mathbb{R}[x,y]$ είναι πρώτα όχι μόνο με παράγοντες του x και του y (δηλαδή δεν υπάρχουν κοινοί παράγοντες $p_{i,x,y}(x,y)$). Επιπρόσθετα με τα παραπάνω σαν $g_x(x)$ συμβολίζουμε τον ΜΚΔ των $p'_{i,x}(x)$, σαν $g_y(y)$ τον ΜΚΔ των $p'_{i,y}(y)$ και σαν $g_{x,y}(x,y)$ τον ΜΚΔ των $p'_{i,x,y}(x,y)$.

Η μεγαλύτερη τιμή που μπορούν να πάρουν οι μεταβλητές x και y του ΜΚΔ $p(x,y)$ δίνονται από τον τύπο:

$$\deg_x\big(p(x,y)\big) = b_1 := (\leq \min_{i=0,1,\dots,n-1}\{\deg_x\big(p_i(x,y)\big)\}) ,$$

και

$$\deg_y\big(p(x,y)\big) = b_2 := (\leq \min_{i=0,1,\dots,n-1}\{\deg_y\big(p_i(x,y)\big)\}) \qquad (2)$$

Έτσι ο ΜΚΔ γράφεται

$$p(x,y) = \sum_{k_1=0}^{b_1}\sum_{k_2=0}^{b_2}\big(p_{k_1,k_2}\big)(x^{k_1}y^{k_2})$$

Από όλα τα παραπάνω ο υπολογισμός του ΜΚΔ πολυωνύμων δύο μεταβλητών, μετατράπηκε σε ένα πρόβλημα υπολογισμού ΜΚΔ μιας μεταβλητής , με την χρήση της παρεμβολής. Ο αριθμός των σημείων της παρεμβολής (x_i, y_i) που θα χρησιμοποιήσουμε για να υπολογίσουμε το $p(x,y)$, ή ισοδύναμα τους συντελεστές p_{k_1,k_2} είναι ίσος με

$$R_1 = (b_1 + 1)(b_2 + 1).$$

Συνοψίζοντας όλα τα παραπάνω θα προκύψει ο επόμενος αλγόριθμος.

Υπολογισμός ΜΚΔ με παρεμβολή

Βήμα 1. Υπολόγισε τους ΜΚΔ $\tilde{p}_k(x, y_k)$ των πολυωνύμων $p_i(x, y_k)$ χρησιμοποιώντας κάποια από τις τεχνικές υπολογισμού ΜΚΔ πολυωνύμων μιας μεταβλητής , όπως είδαμε προηγουμένως. Όπου y_k , $k = 0,1, \dots, b_2$ είναι τα $b_2 + 1$ ξεχωριστά σημεία παρεμβολής.

Βήμα 2. Χρησιμοποίησε τις τιμές των $b_1 + 1$ ξεχωριστών σημείων παρεμβολής x_j , $j = 0,1, \dots, b_1$ στα πολυώνυμα $\tilde{p}_k(x, y_k)$ με σκοπό να υπολογίσουμε τις τιμές του «κατά προσέγγιση» ΜΚΔ $\tilde{p}(x, y_k)$ στα σημεία (x_j, y_k). Δηλαδή $\tilde{p}(x_j, y_k) = \tilde{p}_k(x_j, y_k)$, $j = 0,1, \dots, b_1$

Βήμα 3. Βρες το πολυώνυμο με δύο μεταβλητές $\tilde{p}(x, y_k)$ το οποίο διέρχεται από τα R_1 σημεία παρεμβολής $\left(x_j, y_k, \tilde{p}_k(x_j, y_k)\right)$.Έτσι το πολυώνυμο $\tilde{p}(x, y_k)$ θα είναι η εκτίμηση του $p(x, y)$ με παρεμβολή.

Από τον παραπάνω αλγόριθμο τα μόνα μειονεκτήματα που πρέπει να ξεπεραστούν είναι δύο :

i. Υπάρχει περίπτωση στην οποία για τα πολυώνυμα $p_{i,x,y}(x, y)$ να υπάρχουν (x_k, y_k) τέτοια ώστε $p_{i,x,y}(x_k, y_k) = 0$, για κάθε i. Έτσι για αυτές τις τιμές των y_k , οι ΜΚΔ $\tilde{p}_k(x, y_k)$ των πολυωνύμων μιας μεταβλητής $p_i(x, y_k)$ θα έχουν έναν ακόμα παράγοντα ,τον $(x - x_k)$, καθώς όλα τα πολυώνυμα $p_i(x, y_k)$θα μηδενίζονται στο $x = x_k$. Έτσι λοιπόν , ο ΜΚΔ $\tilde{p}_k(x, y_k)$ θα έχει ακόμα έναν παράγοντα του x, εκτός από $g_x(x)g_{x,y}(x, y_k)$ που θα προκύπτουν από τους παράγοντες του $p_{i,x,y}(x, y)$.

ii. Καθώς υπολογίζουμε τα πολυώνυμα μιας μεταβλητής $\tilde{p}_k(x, y_k)$ να είναι monic (δηλαδή ο συντελεστής του μεγιστοβάθμιου όρου να είναι μονάδα) ,χάνουμε πληροφορίες από τους παράγοντες $p'_{i,y}(y)$ και έτσι ο εκτιμώμενος ΜΚΔ θα έχει την μορφή $p(x, y) = g_x(x)g_{x,y}(x, y)g_y(y)$,δηλαδή χάνεται το μέρος $g_y(y)$.

Έτσι σύμφωνα με (Karampetakis et al. ,2007) για να ξεπεράσουμε τα παραπάνω προβλήματα κάνουμε τα παρακάτω :

i. Επιλέγουμε τα σημεία παρεμβολής y_i (αντίστοιχα x_i) να είναι όσο το δυνατό πιο τυχαία γίνεται.

ii. Όταν υπολογίζουμε τον ΜΚΔ των πολυωνύμων μιας μεταβλητής $\tilde{p}_k(x, y_k)$, θα παίρνουμε το γινόμενο των μεγιστοτάξιων συντελεστών των πολυωνύμων $p_i(x, y_k)$ με σκοπό να διατηρήσουμε όλες τις πληροφορίες και από το πολυώνυμο $f_y(y)$ ($f_y(y)$ είναι το γινόμενο όλων των παραγόντων των πολυωνύμων $p_i(x, y)$, οι οποίοι εξαρτώνται μόνο από το y.

Παράδειγμα

Να βρεθεί ο ΜΚΔ των παρακάτω πολυωνύμων με παρεμβολή

$$\begin{cases} p_1(s) = 4x^3 + 2x^2y + 4xy + 2y \\ p_2(s) = 4xy^2 + 4x + 2y^3 + 2y \end{cases}$$

4.2.2 Υπολογισμός ΜΚΔ με την χρήση DFT.

Ο Καραμπετάκης το 2007 (Karampetakis et al. ,2007) παρουσιάζει έναν αλγόριθμο ο οποίος υπολογίζει τον ΜΚΔ πολυωνύμων δύο μεταβλητών με την χρήση του διακριτού μετασχηματισμού Fourier (Discrete Fourier Transform – DFT).

Ας θεωρήσουμε την πεπερασμένη ακολουθία $X(k_1, k_2)$ και $\tilde{X}(r_1, r_2), i = 1,2$ και $k_i, r_i = 0,1, \dots, M_i$. Με σκοπό οι δύο ακολουθίες $X(k_1, k_2)$ και $\tilde{X}(r_1, r_2)$ να αποτελούν ένα DFT ζευγάρι , πρέπει να ισχύουν οι παρακάτω σχέσεις :

$$\tilde{X}(r_1, r_2) = \sum_{k_1=0}^{M_1} \sum_{k_2=0}^{M_2} X(k_1, k_2) W_1^{-k_1 r_1} W_2^{-k_2 r_2} \quad (3)$$

$$X(k_1, k_2) = \frac{1}{R} \sum_{r_1=0}^{M_1} \sum_{r_2=0}^{M_2} \tilde{X}(r_1, r_2) W_1^{k_1 r_1} W_2^{k_2 r_2} \quad (4)$$

όπου

$$W_i = e^{\frac{2\pi I}{M_i+1}}, \forall\, i = 1,2 \quad (5)$$

$$R = (M_1 + 1)(M_2 + 1) \quad (6)$$

και I συμβολίζουμε την φανταστική μονάδα. Η σχέση (3) είναι ο προς τα εμπρός Μετασχηματισμός Fourier (forward Fourier transform) της $X(k_1, k_2)$.

Η σχέση (4) είναι ο αντίστροφος Μετασχηματισμό Fourier της $\tilde{X}(r_1, r_2)$. Καθορίζουμε δύο τυχαίους πραγματικούς αριθμούς c_1 και c_2 και πολλαπλασιάζουμε τα σημεία $W_i^k = e^{\frac{2\pi kI}{b_i+1}}$, $i = 1,2$ και $k = 0,1, \dots, b_i$,αντίστοιχα.

Λήμμα 1. Θεωρούμε να είναι $\tilde{W}_i^k = c_i W_i^k$, $i = 1,2$ και $k = 0,1, \dots, M_i$ όπου τα σημεία W_i^k ορίζονται από την σχέση (5) .Τότε οι σχέσεις

$$\tilde{X}'(r_1, r_2) = \sum_{k_1=0}^{M_1} \sum_{k_2=0}^{M_2} X(k_1, k_2) \tilde{W}_1^{-k_1 r_1} \tilde{W}_2^{-k_2 r_2} \quad (7)$$

$$X(k_1, k_2) = \frac{1}{R} \sum_{r_1=0}^{M_1} \sum_{r_2=0}^{M_2} \tilde{X}'(r_1, r_2) \tilde{W}_1^{k_1 r_1} \tilde{W}_2^{k_2 r_2} \quad (8)$$

αποτελούν τον προς τα εμπρός και τον αντίστροφο μετασχηματισμό Fourier ,αντίστοιχα.

Απόδειξη

Έχουμε για το

$\tilde{X}'(r_1, r_2) =$

$\sum_{k_1=0}^{M_1} \sum_{k_2=0}^{M_2} X(k_1, k_2) \tilde{W}_1^{-k_1 r_1} \tilde{W}_2^{-k_2 r_2} =$

k1=0M1k2=0M2Xk1,k2c1W1k1−r1

c2W2k2−r2=c1−r1c2−r2k1=0M1k2=0M2Xk1,k2W1−k1r1W2−k2r2=c1−r

1c2−r2Xr1,r2 (9)

,όπου $\tilde{X}(r_1, r_2)$ ορίστηκε παραπάνω από την σχέση (3).

Στην συνέχεια χρησιμοποιώντας την σχέση (9) και την σχέση (4) , θα αποδείξουμε τη σχέση (8) . Οπότε έχουμε :

$$\frac{1}{R}\sum_{r_1=0}^{M_1}\sum_{r_2=0}^{M_2}\tilde{X}'(r_1,r_2)\tilde{W}_1^{r_1k_1}\tilde{W}_2^{r_2k_2}=\frac{1}{R}\sum_{r_1=0}^{M_1}\sum_{r_2=0}^{M_2}\left[\,c_1^{-r_1}c_2^{-r_2}\tilde{X}(r_1,r_2)\right]\tilde{W}_1^{r_1k_1}\tilde{W}_2^{r_2k_2}$$

$$=\frac{1}{R}\sum_{r_1=0}^{M_1}\sum_{r_2=0}^{M_2}c_1^{-r_1}c_2^{-r_2}\tilde{X}(r_1,r_2)\left(c_1W_1^{k_1}\right)^{r_1}\left(c_2W_2^{k_2}\right)^{r_2}$$

$$=\sum_{r_1=0}^{M_1}\sum_{r_2=0}^{M_2}c_1^{-r_1}c_2^{-r_2}\tilde{X}(r_1,r_2)c_1^{r_1}c_2^{r_2}W_1^{k_1r_1}W_2^{k_2r_2}$$

$$=\sum_{r_1=0}^{M_1}\sum_{r_2=0}^{M_2}\tilde{X}(r_1,r_2)W_1^{k_1r_1}W_2^{k_2r_2}=X(k_1,k_2)$$

■

Σύμφωνα με το Λήμμα 1 , μπορούμε να αλλάξουμε τα σημεία παρεμβολής $y_k=W_2^k$ (αντίστοιχα $x_k=W_1^k$) να ανήκουν σε έναν μοναδιαίο κύκλο με κέντρο την αρχή των αξόνων και τα σημεία $\tilde{y}_k=c_2W_2^k$ (αντίστοιχα $\tilde{x}_k=c_1W_1^k$) να ανήκουν σε έναν κύκλο με ακτίνα $\|c_1\|$ (αντίστοιχα $\|c_2\|$) και να έχουν το ίδιο κέντρο.

Ας θεωρήσουμε n πολυώνυμα $p_i(x,y)\in\mathbb{R}[x,y], i=0,1,\dots,n-1$ της μορφής (1) και ορίζουμε να είναι $\tilde{b}_i$, $i=1,2$

$$\deg_x\big(p(x,y)\big)=\tilde{b}_1:=\big(\leq\min_{i=0,1,\dots,n-1}\{\deg_x\big(p_i(x,y)\big)\}\big),$$

και

$$\deg_y\big(p(x,y)\big)=\tilde{b}_2:=\big(\leq\textstyle\sum_{i=0}^{n-1}\{\deg_y\big(p_i(x,y)\big)\}\big)$$

(10)

για τον ΜΚΔ.

Στην συνέχεια θα παραταθεί ένας αλγόριθμος για τον υπολογισμό του πολυωνύμου

$$\bar{p}(x,y)=g_x(x)g_{xy}(x,y)\textstyle\prod_{i=0}^{n-1}p'_{i,y}(y)=\sum_{k_1=0}^{\tilde{b}_1}\sum_{k_2=0}^{\tilde{b}_2}\big(\bar{p}_{k_1,k_2}\big)\big(x^{k_1}y^{k_2}\big)\qquad(11)$$

για τον ΜΚΔ των πολυωνύμων $p_i(x,y), i=0,1,\dots,n-1$ χρησιμοποιώντας τον διακριτό μετασχηματισμό Fourier.

Τα πολυώνυμα $\bar{p}(x,y)$ μπορούν να υπολογιστούν με παρεμβολή χρησιμοποιώντας τα $R_1=\big(\tilde{b}_1+1\big)\big(\tilde{b}_2+1\big)$ σημεία . Τα σημεία αυτά είναι τα :

$$u_i\big(r_j\big)=c_iW_i^{r_j}\ , i=1,2\ \text{ και } r_j=0,1,\dots,\tilde{b}_i\ ,\ W_i=c_ie^{\frac{2\pi I}{\tilde{b}_i+1}}$$

(12)

,όπου c_i , $i = 1,2$ είναι τυχαίοι πραγματικοί αριθμοί.

Με σκοπό να υπολογίσουμε τους συντελεστές $\bar{p}_{k_1,k_2}$ εργαζόμαστε ως εξής :

i. *Ορίζουμε τον ΜΚΔ* $\tilde{p}_{r_2}\left(x, u_2(r_2)\right), r_2 = 0,1, \dots, \tilde{b}_2$ *των πολυωνύμων* $p_i\left(x, u_2(r_2)\right)$, $i = 1,2, \dots, n-1$ *χρησιμοποιώντας κάποιους από τους αλγορίθμους για τον υπολογισμό του ΜΚΔ για πολυώνυμα με μία μεταβλητή , που περιγράψαμε παραπάνω.*

ii. *Για να προκύψουν τα πολυώνυμα* $\bar{p}_{r_2}\left(x, u_2(r_2)\right)$ *πολλαπλασιάζουμε κάθε πολυώνυμο* $\tilde{p}_{r_2}\left(x, u_2(r_2)\right)$ *με το γινόμενο των συντελεστών των μεγαλύτερων τάξεων των πολυωνύμων* $p_i\left(x, u_2(r_2)\right)$. *Με αυτόν τον τρόπο θα πάρουμε το γινόμενο* $\prod_{i=0}^{n-1} p'_{i,y}$

Στην συνέχεια θα χρησιμοποιήσουμε το $u_1(r_1)$, $r_1 = 0,1, \dots, \tilde{b}_1$ στα παραπάνω πολυώνυμα , θα πάρουμε

$$\tilde{p}_{r_1,r_2} = \bar{p}\left(u_1(r_1), u_2(r_2)\right).$$

(13)

Από τις σχέσεις (11) και (13) προκύπτει

$$\tilde{p}_{r_1,r_2} = \frac{1}{R_1} \sum_{l_1=0}^{\tilde{b}_1} \sum_{l_2=0}^{\tilde{b}_2} \left(\bar{p}_{l_1,l_2}\right)\left(W_1^{-r_1 l_1} W_2^{-r_2 l_2}\right)$$

Να σημειωθεί ότι τα $\left[\bar{p}_{l_1,l_2}\right]$ και $\left[\tilde{p}_{r_1 r_2}\right]$ σχηματίζουν ένα ζευγάρι Διακριτού Μετασχηματισμού Fourier (DFT) , και έτσι χρησιμοποιώντας την σχέση (4) υπολογίζουμε τους συντελεστές του (11) ,δηλαδή

$$\bar{p}_{l_1 l_2} = \frac{1}{R} \sum_{r_1=0}^{\tilde{b}_1} \sum_{r_2=0}^{\tilde{b}_2} \tilde{p}_{r_1 r_2} W_1^{r_1 l_1} W_2^{r_2 l_2}$$

(14)

όπου $l_i = 0, \dots, \tilde{b}_i$, $i = 1,2$.

<u>Αλγόριθμος για τον υπολογισμό του</u> $\bar{p}(x,y) = g_x(x) g_{xy}(x,y) \prod_{i=0}^{n-1} p'_{i,y}(y)$

Βήμα 1. Υπολόγισε τον αριθμό των σημείων παρεμβολής

$$R = \left(\tilde{b}_1 + 1\right)\left(\tilde{b}_2 + 1\right)$$

Βήμα 2. Υπολόγισε τα σημεία R_1 παρεμβολής $\left(u_1(r_1), u_2(r_2)\right)$ για $r_i = 0,1, \dots, \tilde{b}_i$, $i = 1,2$ όπως ορίζονται από την σχέση (12).

Βήμα 3. Υπολόγισε τα πολυώνυμα $\bar{p}_{r_2}\left(x, u_2(r_2)\right)$, $r_2 = 0,1, \dots, \tilde{b}_2$.

Βήμα 4. Υπολόγισε τις τιμές $\tilde{p}_{r_1,r_2} = \bar{p}\left(u_1(r_1), u_2(r_2)\right) = \bar{p}_{r_2}\left(u_1(r_1), u_2(r_2)\right)$, $r_i = 0,1, \dots, \tilde{b}_i$

Βήμα 5. Χρησιμοποίησε τον αντίστροφο DFT (14) για τα σημεία $\tilde{p}_{r_1,r_2}$ με σκοπό να υπολογίσουμε τις τιμές $\bar{p}_{i_1,i_2}$.

Βήμα 6. Υπολόγισε το πολυώνυμο

$\bar{p}(x,y) =$

$g_x(x) g_{x,y}(x,y) \prod_{i=0}^{n-1} p'_{i,y}(y) = \sum_{k_1=0}^{\tilde{b}_1} \sum_{k_2=0}^{\tilde{b}_2} \left(\bar{p}_{k_1,k_2}\right)\left(x^{k_1} y^{k_2}\right)$

Ομοίως με προηγουμένως μπορούμε να ορίσουμε το πολυώνυμο

$$\bar{q}(x,y) = \left(\prod_{i=0}^{n-1} p'_{i,x}(x)\right) g_{x,y}(x,y) g_y(x) = \sum_{k_1=0}^{\tilde{b}_1} \sum_{k_2=0}^{\tilde{b}_2} \left(\bar{q}_{k_1,k_2}\right)\left(x^{k_1} y^{k_2}\right).$$

Σε αυτόν τον υπολογισμό στο βήμα 3 της προηγούμενης μεθόδου , ορίζουμε αρχικά τα πολυώνυμα $\tilde{q}_{r_1}(u_1(r_1), y)$, $r_1 = 0,1, \dots, \tilde{b}_1$ τα οποία είναι οι Μέγιστοι Κοινοί Διαιρέτες των πολυωνύμων με μία μεταβλητή $p_i(u_1(r_1), y)$. Στην συνέχεια πολλαπλασιάζουμε κάθε πολυώνυμο $\tilde{q}_{r_1}(u_1(r_1), y)$ με το γινόμενο των μεγιστοβάθμιων συντελεστών των πολυωνύμων $p_i(u_1(r_1), y)$ με σκοπό να υπολογίσουμε τα πολυώνυμα $\bar{q}(r_1(u_1(r_1), y)$. Στο επόμενο βήμα ,αντικαθιστούμε τις τιμές του y με $u_2(r_2)$ και θα έχουμε $\tilde{q}_{r_1,r_2} = \bar{q}\left(u_1(r_1), u_2(r_2)\right) = \bar{q}_{r_1}\left(u_1(r_1), u_2(r_2)\right)$. Τέλος , χρησιμοποιώντας τον αντίστροφο Μετασχηματισμό Fourier, βρίσκουμε τους συντελεστές $\bar{q}_{k_1,k_2}$.

Συνοψίζοντας όλα τα παραπάνω , εάν γνωρίζουμε τα πολυώνυμα $\bar{p}(x,y)$ και $\bar{q}(x,y)$ μπορούμε να ορίσουμε εύκολα τον ΜΚΔ για τα πολυώνυμα $p_i(x,y)$.

Πρόταση. Ας θεωρήσουμε n πολυώνυμα με δύο μεταβλητές

$p_i(x,y) = p_{i,x}(x) g_x(x) p_{i,x,y}(x,y) g_{x,y}(x,y) p_{i,y}(y) g_y(y)$, $i = 0,1, \dots, n-1$.

Για λόγους ευκολίας που θα χρησιμοποιήσουμε παρακάτω συμβολίζουμε: $p'_{i,x}(x) = p_{i,x}(x)g_x(x), p'_{i,x,y}(x,y) = p_{i,x,y}(x,y)g_{x,y}(x,y), p'_{i,y}(y) = p_{i,y}(y)g_y(y)$.

Αν ορίσουμε

$$\bar{p}(x,y) = g_x(x)g_{x,y}(x,y)\prod_{i=0}^{n-1} p'_{i,y}(y)$$

$$\bar{q}(x,y) = \left(\prod_{i=0}^{n-1} p'_{i,x}(x)\right) g_{x,y}(x,y)g_y(x)$$

τότε ο ΜΚΔ τους είναι

$$p(x,y) = \bar{q}(x,y)\frac{\bar{p}(x,c)}{\bar{q}(x,c)} = \bar{p}(x,y)\frac{\bar{q}(c,y)}{\bar{p}(c,y)}$$

όπου c ένας αυθαίρετος αριθμός

Απόδειξη:

Έχουμε ότι

$$\frac{\bar{q}(x,c)}{\bar{p}(x,c)} = \frac{C_2 g_{x,y}(x,c)\prod_{i=0}^{n-1} p'_{i,x}(x)}{g_x(x)g_{x,y}(x,c)C_1} = \frac{C_2}{C_1}\frac{\prod_{i=0}^{n-1} p'_{i,x}(x)}{g_x(x)} = \frac{C_2}{C_1}\frac{p'_{0,x}\prod_{i=0}^{n-1} p'_{i,x}}{g_x(x)}$$

$$= \frac{C_2}{C_1}\frac{p'_{o,x}(x)g_x(x)\prod_{i=0}^{n-1} p'_{i,x}}{g_x(x)} = \frac{C_2}{C_1}p_{0,x}(x)\prod_{i=0}^{n-1} p'_{i,x}.$$

Όπου $\bar{p}(x,c)$ και $\bar{q}(x,c)$ πολυώνυμα με μόνη μεταβλητή το x. Έτσι λοιπόν ο ΜΚΔ θα είναι :

$$p(x,y) = \bar{q}(x,y)\frac{\bar{p}(x,c)}{\bar{q}(x,c)}$$

$$= \left[g_y(y)g_{x,y}(x,y)\prod_{i=0}^{n-1} p'_{i,x}(x)\right]\left[\frac{C_1}{C_2}\frac{1}{p_{0,x}(x)\prod_{i=0}^{n-1} p'_{i,x}(x)}\right]$$

$$= \frac{C_1}{C_2}g_y(y)g_{x,y}(x,y)g_x(x)p_{0,x}(x)\prod_{i=0}^{n-1} p'_{i,x}(x)\frac{1}{p_{0,x}(x)\prod_{i=0}^{n-1} p'_{i,x}(x)}$$

$$= \frac{C_1}{C_2}g_y(y)g_{x,y}(x,y)g_x(x).$$

Η διαίρεση η διενεργείται παραπάνω είναι η γνωστή Ευκλείδεια διαίρεση .

■

Αλγόριθμος με χρήση DFT για τον υπολογισμό του ΜΚΔ 2D-πολυωνύμων

Βήμα 1. Υπολογίζουμε το πολυώνυμο $\bar{p}(x,y)$ από την σχέση (4)

$$\bar{p}(x,y) = g_x(x)g_{x,y}(x,y)\prod_{i=0}^{n-1} p'_{i,y}(y).$$

Βήμα 2. Υπολογίζουμε το πολυώνυμο $\bar{q}(x,y)$ με μετατροπή της σχέσης (4) . Άρα :

$$\bar{q}(x,y) = g_y(y)g_{x,y}(x,y)\prod_{i=0}^{n-1} p'_{i,x}(x).$$

Βήμα 3. Ο ΜΚΔ θα είναι

$$p(x,y) = \bar{q}(x,y)\frac{\bar{p}(x,c)}{\bar{q}(x,c)} = \bar{p}(x,y)\frac{\bar{q}(c,y)}{\bar{p}(c,y)}$$

όπου c ένας αυθαίρετος πραγματικός αριθμός .

Παράδειγμα

4.2.3 Υπολογισμός του «κατά προσέγγιση» ΜΚΔ

Το 2008 ο Kaltofen (Kaltofen et al. , 2008 – Shuhong et al. ,2004) παραθέτει έναν αλγόριθμο για τον υπολογισμό του «κατά προσέγγιση» ΜΚΔ πολυμεταβλητών πολυωνύμων .Παρακάτω γίνεται η αναγωγή του στις δύο διαστάσεις (δηλαδή για πολυώνυμα με δύο μεταβλητές) , χωρίς περιορισμό της γενικότητας που παρουσιάζεται στον αρχικό αλγόριθμο.

AMVGCD : Approximate Multivariate GCD – «κατά προσέγγιση» ΜΚΔ

Είσοδος : g και h πολυώνυμα στο $\mathbb{C}[x_1, x_2]$

Έξοδος : d : μη μεταβλητός «κατά προσέγγιση» ΜΚΔ για τα πολυώνυμα g και h

Βήμα 1. Όρισε τον βαθμό k του «κατά προσέγγιση» ΜΚΔ των g και h , με έναν από τους παρακάτω δύο τρόπους :

i. Σχημάτισε τον πίνακα $S = S_1(g,h)$ του γραμμικού συστήματος $ug + vh = 0$, όπου $g, h \in \mathbb{C}[x_1, x_2]$ και $\mathbf{t}\deg(u) \leq \mathbf{t}\deg(h)$ και $\mathbf{t}\deg(v) \leq \mathbf{t}\deg(g)$ (όπου $\mathbf{t}deg(f_i)$ εννοούμε τον συνολικό βαθμό του f_i). Βρες το μεγαλύτερο κενό (largest gap) στις χαρακτηριστικές τιμές του S και συμπέρανε τον βαθμό k από την τάξη του πίνακα S.

ii. *Υπολόγισε τους ΜΚΔ από διάφορες τυχαίες προβολές των g και h (θεωρώντας τα πολυώνυμα , σαν πολυώνυμα μιας μεταβλητής) , χρησιμοποιώντας την τάξη των αντίστοιχων μιας μεταβλητής πινάκων Sylvester .*

Βήμα 2. Δημιούργησε ξανά τον πίνακα S σαν $S_k(g,h)$ υπό τον περιορισμό όμως $\deg(u) = \deg(h) - k$ και $\deg(v) = \deg(g) - k$ για τα u και v του γραμμικού συστήματος , του πρώτου βήματος. Ο καινούριος πίνακας που θα προκύψει S θα έχει διάσταση 1 μηδενοχώρου.

Βήμα 3. Υπολόγισε μια βάση για τον μηδενοχώρο του S χρησιμοποιώντας το χαρακτηριστικό διάνυσμα που αντιστοιχεί στην μικρότερη χαρακτηριστική τιμή του πίνακα S. Αυτό το διάνυσμα δίνει μια λύση $[u, v]^T$.

Βήμα 4. Βρες το d, το κατά προσέγγιση πηλίκο των h και u (ή των g και v) ,εναλλακτικά ελαχιστοποίησε την ποσότητα $\|h - du\|_2^2 + \|g + dv\|_2^2$ χρησιμοποιώντας την μέθοδο ελαχίστων τετραγώνων.

Αν κάποιος θέλει να καθορίσει μια ανοχή (tolerance) , τότε μόνο το πρώτο βήμα του αλγορίθμου επηρεάζεται . Σε αυτή την περίπτωση , είναι πιθανό ο υπολογισμό του βαθμού να είναι $k = 0$ και τελικά το αποτέλεσμα του «κατά προσέγγιση» ΜΚΔ να είναι $d = 1$.

Πρέπει να σημειωθεί σε αυτό το σημείο ότι οι γενικευμένοι πίνακες του Sylvester είναι διαφορετικοί στον Gao και διαφορετικοί στον Zeng-Dayton. Ο αλγόριθμος του Gao δεν χρειάζεται μια ανοχή (tolerance) ε σε αντίθεση με τον Zeng-Dayton (Sanuki , 2007).

4.2.3 Ο Modular αλγόριθμος .

Με τον Modular αλγόριθμο για την εύρεση του ΜΚΔ πολυμεταβλητών πολυωνύμων ,το πρόβλημα υπολογισμού του μετατρέπεται στον υπολογισμό του ΜΚΔ πολυωνύμων με μία μεταβλητή (Zhi et al. ,?). Αυτή η διαδικασία γίνεται επανειλημμένως χρησιμοποιώντας υπολογισμούς ομομορφισμών για να εξαλείψουν μεταβλητές και να κατασκευάσουν τον ΜΚΔ των αρχικών δοσμένων πολυωνύμων αυτών των ``εικόνων`` χρησιμοποιώντας την διαδικασία της παρεμβολής . Υπάρχουν δύο είδη modular μεθόδων : οι «πυκνές» (dense) και οι «αραιές» (sparse) μέθοδοι (Li et al. , 2005) . Για τον dense modular αλγόριθμο ο αριθμός των ομομορφισμών

είναι εκθετικός ως προς το πλήθος των μεταβλητών που περιέχει το πολυώνυμο. Συνήθως αυτό ο αριθμός είναι πολύ μεγάλος . Η μέθοδος αυτή υπολογίζει τον βαθμό του ΜΚΔ με τυχαίους ομομορφισμούς και κάνει παρεμβολή σε μη μηδενικούς συντελεστές . Ο Corless (Corless et al. , 1995) μετατρέπει τον sparse modular αλγόριθμο για τον υπολογισμό του «κατά προσέγγιση» ΜΚΔ πολυωνύμων με δύο μεταβλητές.

4.2.3.1 Περιγραφή του αλγορίθμου

Ας θεωρήσουμε ότι έχουμε δύο πολυώνυμα p και q και ότι ο βαθμός των δοσμένων πολυωνύμων ως προς x είναι μικρότερος από τον βαθμό ως προς y. Στην συνέχεια θεωρούμε μια τυχαία τιμή του x .Ας είναι $x = a$. Με αυτό τον τρόπο, ανάγουμε τον υπολογισμό του ΜΚΔ πολυωνύμων με δύο μεταβλητές στον υπολογισμό του ΜΚΔ των $p(a, y)$ και $q(a, y)$. Για να υπολογίσουμε τους συγκεκριμένους ΜΚΔ χρησιμοποιούμε τον SVD αλγόριθμο που περιγράφτηκε παραπάνω για πολυώνυμα με μία μεταβλητή (Corless et al., 1995). Επειδή η λήψη της τιμής του $x = \alpha$ είναι τυχαία, θα προκύψει να έχουμε υπολογίσει το βαθμό του σωστού ΜΚΔ σαν πολυώνυμο ως προς y. Αυτή η πρόβλεψη είναι αρκετά αξιόπιστη (πιθανότητα ίση με τη μονάδα).

Στην συνέχεια θα κάνουμε την αντίθετη διεργασία. Δηλαδή θα θεωρήσουμε το x σαν την βασική μας μεταβλητή και θα διαλέξουμε έναν βέβαιο αριθμό για τις τυχαίες τιμές β_i που θα πάρει το y. Για κάθε β_i θα υπολογίσουμε τον ΜΚΔ των $p(x, \beta_i)$ και $q(x, \beta_i)$. Οι παραπάνω ΜΚΔ που θα υπολογιστούν , θα είναι monic πολυώνυμα, καθώς επίσης ότι οι συντελεστές (leading coefficients) των μεγιστοβάθμιων όρων του κάθε πολυωνύμου θα έχουν x και y. Συνεπώς οι συντελεστές του ΜΚΔ θα είναι ρητές συναρτήσεις του β. Ωστόσο μπορούμε να τα πάρουμε τους παρανομαστές από αυτές τις συναρτήσεις να είναι ίδιοι για κάθε συντελεστή. Αυτό μας επιτρέπει να κάνουμε sparse παρεμβολή και επομένως παίρνοντας περισσότερα σημεία από τα απαιτούμενα έχουμε πιο σωστές απαντήσεις για αυτό που αναζητάμε.

Στους ακριβείς υπολογισμούς (exact computation) κάθε συντελεστής μπορεί να παρεμβληθεί ξεχωριστά. Στους «κατά προσέγγιση» υπολογισμούς (approximate computation) παρεμβάλλουμε όλους τους συντελεστές ταυτόχρονα.

Υποθέτουμε ότι υπάρχουν T_x μη μηδενικοί όροι σε κάθε ΜΚΔ των $p(x,\beta_i)$ και $q(x,\beta_i)$. Παράλληλα , υποθέτουμε ότι γνωρίζουμε ότι ο ΜΚΔ των $p(a,y)$ και $q(a,y)$ έχει T_y μη μηδενικούς όρους των οποίων γνωρίζουμε και τις δυνάμεις.
Στην συνέχεια πρέπει να είμαστε ικανοί να εφαρμόσουμε ρητές συναρτήσεις $p_i(y)/p_0(y)$ στους T_x όρους των ΜΚΔ των $p(x,\beta_i)$ και $q(x,\beta_i)$. Επιπρόσθετα , ο συντελεστής του monic όρου είναι $p_0(y)/p_0(y)$ και συνεπάγεται ότι για κάθε β_i θα έχουμε $T_x - 1$ εξισώσεις στους $T_x T_y$ μη γνωστούς συντελεστές των πολυωνύμων που παρεμβάλουμε. Από εδώ προκύπτει ότι εάν έχουμε $T_x = 1$ προκύπτει ότι υπάρχει ένας όρος του x του οποίου γνωρίζουμε την δύναμη. Οπότε το πρόβλημά μας μετατρέπεται στο να υπολογίσουμε τον ΜΚΔ των πολυωνύμων για $x = 1$ και στην συνέχεια να πολλαπλασιάσουμε το αποτέλεσμά που θα προκύψει με το x^l, όπου l είναι η γνωστή δύναμη του ΜΚΔ . Διαφορετικά αν $T_x > 1$ μπορούμε να πάρουμε έναν αριθμό M ο οποίος να είναι μεγαλύτερος ή ίσος από την ποσότητα $T_x T_y/(T_x - 1)$. Αν κάνουμε αυτό έχουμε να λύσουμε M προβλήματα $MK\Delta$ με $n-1$ μεταβλητές.

Στην συνέχεια θα περιγράψουμε με βήματα την παραπάνω μεθοδολογία του αλγορίθμου.

<u>Ο Modular αλγόριθμος</u>

Είσοδος : Δύο πολυώνυμα p και q με $\deg_x\{p,q\} > \deg_y\{p,q\}$

Έξοδος : «κατά προσέγγιση» ΜΚΔ των p και q.

Βήμα 1. Διάλεξε τυχαίους υπολογισμούς α, β_i για τα $\mathbf{x}$ και $\mathbf{y}$ για να υπολογίσεις τους T_x μη μηδενικούς όρους του $MK\Delta\big(F(x,\beta_i), G(x,b_i)\big)$ και τον T_y μη μηδενικό όρο του $MK\Delta\big(F(a,y), G(a,y)\big)$.

Βήμα 2. Λύσε M monic $MK\Delta\big(F(x,\beta_i), G(x,\beta_i)\big)$ για τυχαία επιλεγμένα β_i, όπου:

$$M \geq \frac{T_x T_y}{T_x - 1}$$

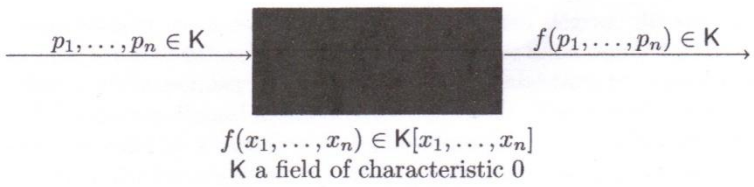
Βήμα 3. Κάνε παρεμβολή για όλους του συντελεστές ταυτόχρονα.

Όπως αναφέρθηκε και προηγουμένως ο sparse modular αλγόριθμος μπορεί να υπολογίσει ``μικρούς`` ΜΚΔ πολύ γρήγορα .Σε διαφορετικές περιπτώσεις όμως

υπάρχει περίπτωση να μην είμαστε τυχεροί ή να χρειαζόμαστε μεγάλο αριθμό ομομορφισμών σε περίπτωση που ο ΜΚΔ είναι «αραιός» (dense).

4.2.4 Ο Black Box αλγόριθμος

Ξεκινώντας την περιγραφή του black box αλγορίθμου θα ήταν σκόπιμο αρχικά να αναφερθούμε εν συντομία για το τι είναι ``black box`` στην Υπολογιστική Άλγεβρα. Στην συνέχεια θα εισάγουμε τον αλγόριθμο για τον υπολογισμό του ΜΚΔ πολυωνύμων με δύο μεταβλητές. Ταυτόχρονα με τον υπολογισμό του ΜΚΔ ο παρακάτω αλγόριθμος μεταχειρίζεται επιδέξια τα πολυμεταβλητά πολυώνυμα όταν αυτά δίνονται από «μαύρα κουτιά». Το «μαύρο κουτί» είναι ένα αντικείμενο το οποίο δέχεται σαν είσοδο μία τιμή για κάθε μεταβλητή του πολυωνύμου και στην συνέχεια παράγει την τιμή του (Kaltofen ,1988). Δηλαδή ,η black box αναπαράσταση ενός πολυμεταβλητού πολυωνύμου είναι μια συνάρτηση η οποία δέχεται σαν είσοδο μια τιμή για κάθε μεταβλητή του και στην συνέχεια παράγει την τιμή του πολυωνύμου (εικόνα 1).



Εικόνα 1: Η "black box" αναπαράσταση ενός πολυωνύμου.

Στην συνέχεια θα περιγράψουμε τον αλγόριθμος για πολυώνυμα με δύο μεταβλητές.

Black Box αλγόριθμος

Είσοδος : Μια black box αναπαράσταση για τα πολυώνυμα $f_i(x_1, x_2) \in K[x_1, x_2]$, $i = 1,2, \ldots, r \geq 2$, και Κ είναι ένα σώμα.

Έξοδος : Ένα πρόγραμμα το οποίο θα καλεί την black box αναπαράσταση των f_i και θα έχει την επόμενη ιδιότητα. Το πρόγραμμα δέχεται δύο στοιχεία p_1, p_2 και θα υπολογίζει το $g(p_1, p_2) \in K[x_1, x_2]$, όπου $g = MK\Delta_{1 \leq i \leq r}(f_i)$.

Βήμα 1. *Διάλεξε τυχαία πεπερασμένα στοιχεία*

$$a_2, b_2, c_3, \dots c_r$$

από ένα υποσύνολο $R \subseteq K$. *Η πληθικότητα αυτού του συνόλου δίνεται σε σχέση με τον* $\deg(f_i)$, *για* $1 \le i \le r$. *Ας συμβολίσουμε με την γραμμή* $\bar{}$ *να είναι η προβολή , για οποιοδήποτε* $h \in K[x_1, x_2]$

$$\bar{h}(X, Y) = h(X, Y(p_2 - a_2 p_1 - b_2) + a_2 X + b_2) \ .$$

Σημειώνουμε ότι $\bar{h}(p_1, 1) = h(p_1, p_2)$. *Θα χρησιμοποιήσουμε τα πολυώνυμα με δύο μεταβλητές* $\bar{f_0}(X, Y) = \bar{f_2}(X, Y) + \sum_{i=3}^{r} c_i \bar{f_i}(X, Y)$, $\bar{f_1}(X, Y)$,

$$\gamma(X, Y) = MK\Delta\left(\bar{f_0}(X, Y), \bar{f_1}(X, Y)\right)$$

Επίσης θα χρησιμοποιήσουμε τους ΜΚΔ για τα πολυώνυμα

$$\bar{\gamma}_e(X) = MK\Delta\left(\bar{f_0}(X, e), \bar{f_1}(X, e)\right), \text{για } e \in K.$$

Βήμα 2. *Με την standard παρεμβολή υπολογίζουμε*

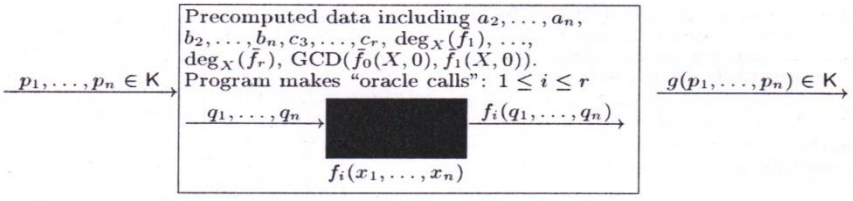
$$\bar{f_0}(X, 0) = f_2(X, a_2 X + b_2) + \sum_{i=3}^{r} c_i f_i(X, a_2 X + b_2)$$

και $$\bar{f_1}(X, 0) = f_1(X, a_2 X + b_2)$$

Στην συνέχεια υπολογίζουμε $\bar{\gamma}_0(X) = MK\Delta\left(\bar{f_0}(X, 0), \bar{f_1}(X, 0)\right)$.

Πρέπει να γνωρίζουμε $\deg_X(\bar{f_i})$ *για όλα τα* $1 \le i \le r$. *Ο βαθμός ή ένα πάνω φράγμα μπορεί να έχει δοθεί από τα δεδομένα μας ή διαφορετικά μπορεί να υπολογιστεί με τον παρακάτω τρόπο.*

Διάλεξε $B \in R$ *και υπολόγισε* $\bar{f_i}(X, B)$ *ορίζοντας μια αλληλουχία πολυωνύμων* $\bar{f_i}^{(d)}(X, B)$ *για* $d = 1,2,3 \dots$ *μέχρι* $\bar{f_i}^{(d)}(X, B) = \bar{f_i}(X, B)$.*Όπου* $\bar{f_i}^{(d)}(X, B)$ *είναι η παρεμβολή στα* $X = 0,1, \dots, d$ *των* $\bar{f_i}(X, B)$. *Ελέγχουμε αν ισχύει η ισότητα* $\bar{f_i}^{(d)}(X, B) = \bar{f_i}(X, B)$ *υπολογίζοντας στο τυχαίο* $A \in R$ *: αν* $\bar{f_i}^{(d)}(A, B) = \bar{f_i}(A, B)$ *τότε δηλώνουμε ότι* $\bar{f_i}^{(d)}(X, B) = \bar{f_i}(X, B)$ *και* $\deg_X(\bar{f_i}) = d$, *διαφορετικά συνεχίζουμε την παρεμβολή.*



4.2.5 Αλγόριθμος τύπου black-box για τον υπολογισμό του ΜΚΔ

Ο αλγόριθμος που προτείνει ο Zeng to 2004 (Zeng et al. , 2004) υπολογίζει τον «κατά προσέγγιση» ΜΚΔ για πολυμεταβλητά πολυώνυμα των οποίων οι συντελεστές δεν είναι ακριβείς αριθμοί (inexact) . Ο αλγόριθμος που προτείνουν είναι τύπου black-box και αποτελείται από τρία στάδια .Στην συνέχεια θα παρουσιαστούν και θα αναλυθούν τα τρία στάδια που απαρτίζουν τον αλγόριθμο.

Αλγόριθμος

Στάδιο Ι: Υπολογισμός του βαθμού του «κατά προσέγγιση» ΜΚΔ

Είσοδος: Πολυώνυμα p και q με ανοχή (tolerance) ε

- Δημιούργησε ένα τυχαίο διάνυσμα $s = (s_1, s_2)^T$.
- **for** $j = 1,2$ **do**
  - Σχημάτισε τα ζευγάρια πολυωνύμων μιας μεταβλητής
    $$\{p_1(t) = p_1(t, s_2), q_1(t) = q_1(t, s_2)\}$$
    $$\{p_2(t) = p_2(s_1, t), q_2(t) = q_2(s_1, t)\}$$
  - Χρησιμοποίησε τον υπολογισμό του «κατά προσέγγιση» ΜΚΔ πολυωνύμων μιας μεταβλητής (Zeng , 2004) για να υπολογίσεις τους ΜΚΔ u_j για τα ζευγάρια (p_j, q_j)
  - Θέσε $k_j = \deg(u_j)$

end do

Έξοδος : $\boldsymbol{k} = [k_1, k_2]$

Στάδιο ΙΙ : Υπολογισμός των παραγόντων του «κατά προσέγγιση» ΜΚΔ.

Είσοδος: $p\ , q, \boldsymbol{k}$

- Σχημάτισε τον πίνακα $S_k(p, q) = [\ C_{m-k}(q)\ \ \vdots\ \ C_{n-k}(p)\ ]$, όπου τα δύο blocks $C_{m-k}(q)$ και $C_{n-k}(p)$ είναι οι πίνακες συνέλιξης (Zeng et al. ,2004 - παράρτημα) με $m = \deg(p)$ και $n = \deg(q)$.
- Κάνε QR παραγοντοποίηση στον πίνακα S_k , $QR = S_k(p, q)$
- **for** $l = 0,1, \ldots,$ **do**
  - Υπολόγισε ρ_l και $\boldsymbol{y}_l$ από
    $$\begin{cases} \boldsymbol{y}_{i+1} = \boldsymbol{y}_i - \begin{bmatrix} 2r\boldsymbol{y}_i^H \\ R \end{bmatrix}^+ \begin{bmatrix} r\boldsymbol{y}_i^H\boldsymbol{y}_i - r \\ R\boldsymbol{y}_i \end{bmatrix} \\ \text{ομαλοποίησε } \boldsymbol{y}_i \text{ , και θέσε } \rho_i = \|R\boldsymbol{y}_i\|_2 \text{ , } i = 0,1, \ldots, r = \|R\|_\infty \end{cases}$$
    όπου $[A]^H$ είναι ο Hermitian συζυγής πίνακας του A και $[\ A]^+ = (A^H A)^{-1} A^H$
  - **if** $\|\boldsymbol{y}_l - \boldsymbol{y}_{l-1}\|$ σταματάει να μειώνεται **then**
    θέσε $\boldsymbol{y} = \boldsymbol{y}_l$, σταμάτα **do loop**

  End do
- Υπολόγισε τα **v** και $\boldsymbol{w}$ από το $\boldsymbol{y}$ (Zeng et al. ,2004 – παράρτημα)
- Λύσε το γραμμικό σύστημα $C_{\boldsymbol{k}}(v)\boldsymbol{u} = \boldsymbol{p}$ ως προς $\boldsymbol{u}$.
- Υπολόγισε την εγγύτητα (nearness) $\theta = \sqrt{\|C_{\boldsymbol{k}}(v)\boldsymbol{u} - \boldsymbol{p}\|_2^2 + \|C_{\boldsymbol{k}}(w)\boldsymbol{u} - \boldsymbol{q}\|_2^2}$

Έξοδος : $\boldsymbol{k} = [k_1, k_2]$

Στάδιο ΙΙΙ : Βελτίωση και επιβεβαίωση των παραπάνω παραγόντων.

Είσοδος: $\boldsymbol{p}\ , \boldsymbol{q}, (u_0, v_0, w_0), \boldsymbol{r}$

- Σχημάτισε τους πίνακες $F(\boldsymbol{z}_0) = \begin{bmatrix} \boldsymbol{r}^H\boldsymbol{u} - 1 \\ C_{m-k}(v)\boldsymbol{u} \\ C_{n-k}(w)\boldsymbol{u} \end{bmatrix}$, $\boldsymbol{z}_0 = \begin{bmatrix} u_0 \\ v_o \\ w_0 \end{bmatrix}$,

$$\boldsymbol{b} = \begin{bmatrix} 0 \\ \boldsymbol{p} \\ \boldsymbol{q} \end{bmatrix}, \boldsymbol{r}, \boldsymbol{u} \in \mathbb{C}^K, \boldsymbol{v} \in \mathbb{C}^{m-k}, \boldsymbol{w} \in \mathbb{C}^{n-k}, \boldsymbol{p} \in \mathbb{C}^M, \boldsymbol{q} \in \mathbb{C}^N$$

- **for** $j = 0,1, \ldots$ **do**
  - Λύσε την εξίσωση $J(\boldsymbol{z_j})\boldsymbol{d_j} = F(\boldsymbol{z_j}) - \boldsymbol{b}$ για $\boldsymbol{d_j}$ λύση ελαχίστων τετραγώνων ,όπου $J(\boldsymbol{z_j})$ η Ιακωβιανή της $F(\boldsymbol{z_j})$.

    Γενικά $J(z) = \begin{bmatrix} \boldsymbol{r'^H} \\ C_k(v) \quad C_{m-k}(u) \\ C_{n-k}(w) \quad\quad\quad C_{(n-k)(u)} \end{bmatrix}$
  - Θέσε $\boldsymbol{z}_{j+1} = \boldsymbol{z}_j - \boldsymbol{d}_j$
  - Υπολόγισε την εγγύτητα $\theta_{j+1} = \|F(\boldsymbol{z}_{j+1} - \boldsymbol{b}\|_2$
  - Αν η εγγύτητα θ_{j+1} σταματήσει να μειώνεται ,τότε

    Θέσε $\boldsymbol{z} = \boldsymbol{z}_j, \theta = \theta_j$ σταμάτα **do loop**

    end if
- Βγάλε τα (u, v, w) από $\boldsymbol{z}$

Έξοδος : (u, v, w) και την εγγύτητα θ.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι ο συγκεκριμένος αλγόριθμος βρίσκει ‘’εφαρμογή’’ και στο προγραμματιστικό περιβάλλον της MATLAB. Ο Zeng στο διαδίκτυο αναφέρει για το toolbox της MATLAB, το Apalab το οποίο απευθύνεται σε συμβολικούς και αριθμητικούς υπολογισμούς στην «κατά προσέγγιση» πολυωνυμική Άλγεβρα. Αν κάποιος χρήστης επισκεφτεί την ιστοσελίδα στο διαδίκτυο μπορεί να κατεβάσει το συγκεκριμένο toolbox και να το χρησιμοποιήσει. Υπάρχουν πολλές συναρτήσεις οι οποίες μπορούν να σου υπολογίσουν εύκολα μέγιστους κοινούς διαιρέτες πολυωνύμων μιας ή παραπάνω μεταβλητών.

4.2.6 Ο Subresultant αλγόριθμος για τον ΜΚΔ πολυωνύμων δύο μεταβλητών

Όπως έχουμε αναφέρει και παραπάνω ο Subresultant PRS αλγόριθμος είναι διαθέσιμος και για τον υπολογισμό του ΜΚΔ πολυωνύμων με δύο μεταβλητές. Ο Subresultant PRS αλγόριθμος είναι ο Ευκλείδειος αλγόριθμος χρησιμοποιώντας την «ψευδοδιαίρεση» σε έναν πολυωνυμικό δακτύλιο (Li et al. ,2005) .

Ας θεωρήσουμε τα πολυώνυμα $F(x,y)$ και $G(x,y)$ όπου $F, G \in \mathbb{C}[x,y]$.

$$F = f_m x^m + \cdots + f_0, \qquad f_m \neq 0,$$
$$G = g_n x^n + \cdots + g_0, \qquad g_n \neq 0,$$

Όπου $f_i, g_i \in \mathbb{C}[x,y]$, $i = 0,1,\ldots$, και $\deg(F) \geq \deg(G)$.

Στην συνέχεια θα τροποποιήσουμε τον Ευκλείδειο αλγόριθμο για να υπολογίσουμε τον «κατά προσέγγιση» ΜΚΔ των πολυωνύμων με δύο μεταβλητές (Noda et al., 1991) . Ο συμβατικός αλγόριθμος υπολογίζει μια ακολουθία πολυωνυμικών υπολοίπων (PRS)

$$\{P_1 = F, P_2 = G, \ldots, P_k \neq 0, P_{k+1} = 0\} \tag{1}$$

σύμφωνα με την επαναληπτική διαδικασία

$$\beta_i P_{i+1} = \upsilon\pi\acute{o}\lambda o\iota\pi o(\alpha_i P_{i-1}, P_i)\ , i = 2,3,\ldots$$

Όπου $\alpha_i, \beta_i \in \mathbb{C}[x,y]$. Σύμφωνα με την θεωρία PRS $,P_i\ , i \geq 3$ μπορούν να παρασταθούν τα F, G και οι συντελεστές του σαν :

$$P_i = \lambda_i \begin{vmatrix} f_m & f_{m-1} & & \cdots & \cdots & f_{2j-n+2} & x^{n-j-1}F \\ & \ddots & & & & & \vdots \\ & & f_m & f_{m-1} & \cdots & f_{j+1} & x^0 F \\ g_n & g_{n-1} & & \cdots & \cdots & g_{2j-m+2} & x^{m-j-1}G \\ & \ddots & & & & \vdots & \vdots \\ & & g_n & g_{n-1} & \cdots & g_{j+1} & x^0 G \end{vmatrix},$$

όπου $\lambda_i \in \mathbb{C}[x,y], \deg(P_{i-1}) = j+1$ και $f_k = g_k$ αν $k < 0$. Η παραπάνω ορίζουσα ονομάζεται $j^{\sigma\tau\eta}$ *τάξη* ορίζουσα των πολυωνύμων F και G.

Παράλληλα με τα παραπάνω $|\lambda_i| = 1$ αν διαλέξουμε

$$\alpha_i = lc(P_i)^{d_i+1}, d_i = \deg(P_{i-1}) - \deg(P_i),$$
$$\beta_2 = 1, \qquad \gamma_2 = 1,$$
$$\beta_i = lc(P_{i-1})\gamma_i^{d_i-1}\ , \gamma_i = lc(P_{i-1})^{d_{i-1}}\gamma_{i-1}^{1-d_{i-1}}\ , i \geq 3$$

Με $lc(P)$ συμβολίζουμε τον συντελεστή (leading coefficient) του μεγιστοβάθμιου όρου του P. Η παραπάνω επιλογή των α_i και β_i ονομάζεται *subresultant-PRS* αλγόριθμος. Ο συγκεκριμένος αλγόριθμος δημιουργήθηκε για πολυώνυμα με συντελεστές κινητής υποδιαστολής (floating point coefficients) .

Όμως υπάρχουν δύο κρίσιμα βήματα για τον παραπάνω αλγόριθμο:

i. *Ομαλοποίηση των υπολοίπων στην ακολουθία των πολυωνυμικών υπολοίπων (normalization of remainders in PRS).* Ας είναι F, G πολυώνυμα στο $\mathbb{C}[x,y]$, με $\deg(F) \geq \deg(G)$. Ας είναι $\tilde{R}$ και $\tilde{Q}$ πολυώνυμα τέτοια ώστε:

$$\tilde{R} = lc(g)^{d+1}F - \tilde{Q}G\ , d = deg(F) - deg(G), \deg\left(\tilde{R}\right) < \deg(G).$$

Τα πολυώνυμα $\tilde{R}$ και $\tilde{Q}$ ονομάζονται «ψευδό – υπόλοιπο» και «ψευδό – πηλίκο», αντίστοιχα. Ορίζουμε σαν ομαλοποιημένο «ψευδό – υπόλοιπο» το

$$R = \frac{\tilde{R}}{\max\{mmc[lc(G)^{d+1}], mmc(\tilde{Q})\}},$$

όπου $mmc(P)$ ορίζουμε να είναι η απόλυτη τιμή του μεγαλύτερου αριθμητικού συντελεστή του P (maximum magnitude numeric coefficient) ή διαφορετικά την μεγαλύτερη νόρμα του διανύσματος των συντελεστών του P.

ii. *Στρογγυλοποίηση του P_k (Rounding of P_k).* Ας είναι P_k ένα στοιχείο από την ακολουθία PRS που περιγράψαμε παραπάνω (1) τέτοιο ώστε $P_k = const.\times MK\Delta(P_1, P_2, \varepsilon)$. Στην συνέχεια , μετά την ομαλοποίηση του P_k με $mmc(P_k) = 1$,στρογγυλοποιούμε τους συντελεστές του P_k στο $O(\varepsilon)$ και σημειώνουμε το αποτέλεσμα σαν $roundoff(P_k, \varepsilon)$

Επομένως σύμφωνα με τα παραπάνω κρίσιμα βήματα του αλγορίθμου μπορούμε να περιγράψουμε τον αλγόριθμο με βήματα

<u>Αλγόριθμος PRS για τον υπολογισμό του «κατά προσέγγιση»</u> $MK\Delta(P_1, P_2, \varepsilon)$

Είσοδος : Ομαλοποιημένα πολυώνυμα $P_1, P_2 \in \mathbb{C}[x, y]$ με $\deg(P_1) \geq \deg(P_2)$. Ένας μικρός αριθμός ε_0 , $0 \leq \varepsilon_0 \leq 1$

Έξοδος : $D = MK\Delta(P_1, P_2, \varepsilon)$ και ε

Βήμα 1. $k := 2\ ; \gamma := 1\ ; P_3 := prem'(P_1, P_2);$

Βήμα 2. $d_k := \deg(P_k) - \deg(P_{k-1})\ ;$

Βήμα 3. **If** $mmc(P_{k+1}) < \varepsilon_0$ **then goto** Βήμα4;

If $\deg(P_{k+1}) = 0$ **then** return $(1, \varepsilon_0)$;

$k := k + 1\ ; \gamma := lc(P_{k-1})^{d_{k-1}}\gamma^{1-d_{k-1}};$

$\beta := ομαλοποίησε(lc(P_{k-1})\gamma^{d_{k-1}});$

$P_{k+1} := prem'(P_{k-1}, P_k)/\beta$ **goto** Βήμα2;

Βήμα 4. $\varepsilon := mmc(P_{k+1}); P_k := P_k/mmc(P_k);$

$P_k := roundoff(P_k, 2\varepsilon);$

Βήμα 5. $C_1 := cont(P_1, 2\varepsilon), C_2 := cont(P_2, 2\varepsilon);$

return $(pp(P_k, 2\varepsilon) \times$ *«κατά προσέγγιση»*$MK\Delta(C_1, C_2, 2\varepsilon))$.

Στο Βήμα 5 του παραπάνω αλγορίθμου σαν $cont$ και pp ορίζουμε να είναι οι πράξεις της διάστασης και του αρχικό μέρος του πολυωνύμου, αντίστοιχα:

$$cont(F, \varepsilon) = [\ll \text{κατά προσέγγιση} \gg \text{ ΜΚΔ των συντελεστών του } F\,]$$

και

$$pp(F, \varepsilon) = [\ll \kappa\alpha\tau\acute{\alpha}\ \pi\rho o\sigma\acute{\varepsilon}\gamma\gamma\iota\sigma\eta \gg\ \pi\eta\lambda\acute{\iota}\kappa o\ \tau o\upsilon\ F\ \kappa\alpha\iota\ cont(F, \varepsilon)]$$

Παράλληλα με τον παραπάνω αλγόριθμο στην βιβλιογραφία υπάρχουν και άλλοι αλγόριθμοι οι οποίοι στηρίζονται στον PRS αλγόριθμο για τον υπολογισμό του ΜΚΔ για πολυμεταβλητά πολυώνυμα , οπότε και για πολυώνυμα με δύο μεταβλητές. Ένας από αυτούς είναι ο «κατά προσέγγιση» PC-PRS αλγόριθμος (Sanuki , 2007).

Παράδειγμα

Να βρεθεί ο «κατά προσέγγιση» ΜΚΔ των πολυωνύμων :

4.2.7 Αλγόριθμος του Hensel

Η παρακάτω μέθοδος για τον υπολογισμό του ΜΚΔ πολυμεταβλητών πολυωνύμων εν ολίγοις περιγράφει τον EZ-GCD (Sanuki , 2007) χρησιμοποιώντας τον Hensel αλγόριθμο. Στην συνέχεια θα αναχθεί ο συγκεκριμένος αλγόριθμος για την εύρεση του ΜΚΔ για πολυώνυμα με δύο μεταβλητές .

Όταν χρησιμοποιούμε τον αλγόριθμο του Hensel για τον υπολογισμό του ΜΚΔ πολυωνύμων με δύο μεταβλητές ,τότε τα δοσμένα πολυώνυμα μετατρέπονται σε δύο πολυώνυμα με μία μεταβλητή ,των οποίων ο Μέγιστος Κοινός τους Διαιρέτης μετατρέπεται ξανά στο πεδίο με δύο μεταβλητές χρησιμοποιώντας generalized Newton επαναλήψεις . Απεικονιστικά ο αλγόριθμος του Hensel έχει ως εξής

$$\begin{array}{ccccc} \mathrm{R}[\mathbf{x}_1,\mathbf{x}_2] & \times & \mathrm{R}[\mathbf{x}_1,\mathbf{x}_2] & \xrightarrow{\text{ΜΚΔ}} & \mathrm{R}[\mathbf{x}_1,\mathbf{x}_2] \\ \text{mod I} & \downarrow & & & \downarrow \text{mod I} \\ \mathrm{R}[\mathbf{x}_1] & \times & \mathrm{R}[\mathbf{x}_1] & \xrightarrow{\text{ΜΚΔ}} & \mathrm{R}[\mathbf{x}_1] \end{array}$$

Όπου $I = (x_2 - a_2)$.

Αλγόριθμος του Hensel

Βήμα 1. Διάλεξε την κύρια μεταβλητή του πολυωνύμου. Ας υποθέσουμε ότι είναι x_1. Βρες έναν κατάλληλο ομομορφισμό $I = (x_2 - a_2)$.

Βήμα 2. Θεώρησε $F_1 = F \ mod \ I$, $G_1 = G \ mod \ I$. Υπολόγισε $C_1 = MK\Delta \ (F_1, G_1)$ και τις ελάσσων ορίζουσες $\widetilde{F_I}, \widetilde{G_I}$.

Βήμα 3. Αν υπάρχει μία από τις ελάσσων ορίζουσες , η οποία να είναι πρώτη (prime) με το C_I, τότε χρησιμοποίησε την πολυμεταβλητή κατασκευή του Hensel για να ``ανυψώσουμε`` (lift) το C_I και την ελάσσων ορίζουσα. Διαφορετικά εκτέλεσε μια square – free ανάλυση είτε για το F είτε για το G.

Από τα παραπάνω βήματα το τελευταίο είναι το πιο κρίσιμο για την πορεία του αλγορίθμου (Li et al., 2005). Ας υποθέσουμε ότι έχουμε το πολυώνυμο P με μεταβλητές x_1, x_2 και με συντελεστή του μεγιστοβάθμιου όρου (leading coefficient) $p_m(a_2) \neq 0$. Ας είναι $x = x_1 , u = x_2 , G^{(0)}$ και $H^{(0)}$ είναι πρώτα πολυώνυμα ικανοποιώντας την εξίσωση

$$P(x,u) = G^{(0)}(x)H^{(0)}(x).$$

Η πολυμεταβλητή κατασκευή του Hensel είναι να υπολογίσουμε τα πολυώνυμα $G^{(k)}(x,u)$ και $H^{(k)}(x,u)$ που να ικανοποιούν την σχέση

$$P(x,u) = G^{(k)}(x)H^{(k)} mod \ I^{k+1}$$

Ο βασικός υπολογισμός που περιέχεται στην πολυμεταβλητή κατασκευή του Hensel είναι η λύση πολυωνυμικών Διοφαντικών εξισώσεων για τα σταθερά πολυώνυμα (fixed polynomials) $G^{(0)}(x)$ και $H^{(0)}(x)$. Αν τα πολυώνυμα $G^{(0)}(x)$ και $H^{(0)}(x)$ είναι πρώτα (relative prime) , τότε για οποιοδήποτε πολυώνυμο $R(x)$ με

$\deg\big(R(x)\big) < \deg\Big(G^{(0)}(x)\Big) + \deg\Big(H^{(0)}(x)\Big)$ υπάρχουν μοναδικά πολυώνυμα $A(x)$ και $B(x)$ τέτοια ώστε

$$A(x)G^{(0)}(x) + B(x)H^{(0)}(x) = R(x)$$

και

$$\deg\big(A(x)\big) < \deg\Big(H^{(0)}(x)\Big)\,, \deg\big(B(x)\big) < \deg\Big(G^{(0)}(x)\Big).$$

Υποθέτουμε ότι

$$G^{(0)}(x) = g_s x^s + g_{s-1}x^{s-1} + \cdots + g_1 x + g_0\,, g_s \neq 0$$
$$H^{(0)}(x) = h_t x^t + h_{t-1}x^{t-1} + \cdots + h_1 x + h_0\,, h_t \neq 0$$

Πρόκειται να λύσουμε τις γραμμικές εξισώσεις

$$Mx = r$$

όπου r είναι το διάνυσμα των συντελεστών του πολυωνύμου $R(x)$, M είναι ο πίνακας του Sylvester για τα πολυώνυμα $G^{(0)}(x)$ και $H^{(0)}(x)$. Για την λύση των παραπάνω γραμμικών εξισώσεων μπορούν να εφαρμοστούν διάφοροι τρόποι , όμως είναι προτιμότερο να χρησιμοποιήσουμε την QR παραγοντοποίηση καθώς είναι εύκολο αξιοποιήσουμε την δομή του πίνακα M του Sylvester . Καθώς , ο πίνακας του Sylvester αποτελείται από δύο υποπίνακες G και H (Toeplitz πίνακες) ,ξεκινάμε την QR παραγοντοποίηση με Given περιστροφή και υπολογίζουμε τα στοιχεία κάτω από τις πρώτες t στήλες , και στην συνέχεια εφαρμόζουμε τον μετασχηματισμό Hausholder για τον κάτω $s \times s$ υποπίνακα (υποθέτουμε ότι $s \geq t$).

Επιπρόσθετα , στην Hensel κατασκευή είναι πολύ σημαντικό να αποφασίσουμε που θα σταματήσουμε .Είναι φανερό ότι η διαδικασία σταματάει καθώς $\left\|\Delta P^{(k)}\right\| = \left\|P - G^{(k)}H^{(k)}\right\| = O(\varepsilon)$. Επίσης είναι δυνατό ότι ο $\Delta P^{(k)}$ μπορεί να έχει ακόμα μερικούς συντελεστές των οποίων οι απόλυτες τιμές να μην είναι $O(\varepsilon)$ όταν ο k είναι ο μεγαλύτερος από τον συνολικό βαθμό της μεταβλητής u στο P. Σε αυτήν την περίπτωση , πρέπει να ελέγξουμε και να αποφασίσουμε αν αυτό προέρχεται από λάθος ή αν το πολυώνυμο P έχει πράγματι κατά προσέγγιση παράγοντες . Αν πολλοί συντελεστές του $\Delta P^{(k)}$ είναι σχετικοί πολλοί περισσότερο από ε ,τότε μπορεί τα πολυώνυμα F και G να μην έχουν «κατά προσέγγιση» ΜΚΔ. Διαφορετικά μπορούμε να χρησιμοποιήσουμε μια μέθοδο βελτιστοποίησης για να βελτιώσουμε τον αρχικό «κατά προσέγγιση» ΜΚΔ μιας μεταβλητής και τις ελάσσων ορίζουσες του $G^{(0)}(x)$ και $H^{(0)}(x)$ ή να αυξήσουμε τον αριθμό των ψηφίων που χρησιμοποιούμε στους

υπολογισμού κινητής υποδιαστολής . Υπάρχει περίπτωση όμως και οι δύο μέθοδοι να μην είναι αποδοτικές .

Αν το $\Delta P^{(k)}$ είναι λογικά μικρό , τότε στρογγυλοποιούμε $G^{(k)}$ και $H^{(k)}$ σε G και H, αντίστοιχα. Τα G και H επιλέχτηκαν να είναι υποψήφιοι παράγοντες του P. Αν $\|P - GH\|$ δεν είναι πολύ μεγάλο , σχηματίζουμε το πρόβλημα ελαχιστοποίησης

$$\min_{\Delta G, \Delta H} \|P - GH - G\Delta H - \Delta GH\|.$$

4.2.8 Υπολογισμός ΜΚΔ με την Grobner Basis μέθοδο.

Ο παρακάτω αλγόριθμος , ο οποίος θα παρουσιαστεί υπολογίζει μια Grobner Basis του ιδεώδες (P_1, P_2) στο $K[y][x]$. Δηλαδή αντιμετωπίζουμε τα P_1 και P_2 σαν πολυώνυμα της μεταβλητής x με συντελεστές στο $K[y]$. Η Grobner Basis στο $K[y]$ είναι ισάξια και ισοδύναμη με την Grobner Basis $K[x, y]$.
Ο αλγόριθμος που θα παρουσιαστεί παρακάτω βασίζεται στο επόμενο θεώρημα (Sasaki et al. ,1988).

Θεώρημα . Ας είναι $\Gamma = \{P_1, P_2, \dots, P_s\}$ μια Grobner Basis του ιδεώδες (P_1, P_2) στο $K[y, \dots, z][x]$. Επίσης ας συμβολίσουμε με $\deg(P_i) = d_i$, $i = 1, \dots, s$,τον βαθμό του πολυωνύμου P_i. Ακόμα ας είναι d_k η μικρότερη τιμή από τις $\{d_1, d_2, \dots, d_s\}$. Τότε υπάρχει ένα πολυώνυμο $C, C \in K[y, \dots, z]$ τέτοιο ώστε $P_k = C \cdot MK\Delta\ (P_1, P_2)$.

Απόδειξη:
Ας θεωρήσουμε ότι $G = MK\Delta(P_1, P_2)$. Καθώς $P_k \in (P_1, P_2), P_k = A_k P_1 + B_k P_2$ για κάποια A_k και $B_k \in K[y, \dots, z][x]$.
Ακόμα όμως ισχύει ότι υπάρχει πολυώνυμο A και B , $A, B \in K(y, \dots, z)[x]$ τέτοιο ώστε $G = AP_1 + BP_2$.Πολλαπλασιάζοντας με $\tilde{C}$ ($\tilde{C}$ ΕΚΠ των παρανομαστών των Α και Β) αυτή την εξίσωση, έχουμε : $\tilde{C}G \in MK\Delta(P_1, P_2)$. Καθώς όμως $\deg(\tilde{C}G) = \deg(G)$ και $\tilde{C}G$ πρέπει να είναι Μ-μειωμένο σε 0 επι Γ, έχουμε $\deg(P_k) \leq \deg(\tilde{C}G) = \deg(G)$. Άρα $C \in K[y, \dots, z]$.

■

Το παραπάνω θεώρημα μας αποφέρει τον επόμενο αλγόριθμο για την εύρεση του ΜΚΔ πολυωνύμων δύο μεταβλητών.

Αλγόριθμος για τον ΜΚΔ χρησιμοποιώντας την Grobner Basis μέθοδο

Βήμα 1. Υπολόγισε την Grobner Basis $\Gamma = \{P_1, P_2, \dots, P_s\}$ του ιδεώδες (P_1, P_2) στο $K[y, \dots, z][x]$

Βήμα 2. Αν P_k είναι το ελάχιστο βαθμού στοιχείο του Γ και αν $\deg(P_k) = 0$, τότε βγάλε 1, αλλιώς $pp(P_k)$, όπου $pp(P_k)$ είναι το αρχικό μέρος του P (primitive part of P)

Από τον παραπάνω αλγόριθμο το $pp(P_k)$ μπορεί να υπολογιστεί ικανοποιητικά ως εξής :

- Υπολόγισε το $g = MK\Delta\left(lc\,(P_1), lc(P_2)\right)$, όπου $lc(P)$ εννοούμε τον συντελεστή του μεγιστοβάθμιου όρου της κύριας μεταβλητής (της x) του πολυωνύμου P.
- Κατασκεύασε το $\tilde{P} = \frac{gP_k}{lc(P_k)}$.
- Υπολόγισε το $pp(\tilde{P})$.