Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
Σχολή Θετικών Επιστημών

Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Διδακτορική Διατριβή

Μη–γραμμική επεξεργασία σήματος και εφαρμογές στην κρυπτογραφία

Νικόλαος Ε. Κολοκοτρώνης

Αθήνα, Δεκέμβριος 2003

Επιβλέπων

Ν. Καλουπτσίδης,	Καθηγητής Πανεπιστημίου Αθηνών

Τριμελής Επιτροπή

Ν. Καλουπτσίδης,	Καθηγητής Πανεπιστημίου Αθηνών
Θ. Σφηκόπουλος,	Καθηγητής Πανεπιστημίου Αθηνών
Δ. Μαρτάκος,	Αν. Καθηγητής Πανεπιστημίου Αθηνών

Επταμελής Επιτροπή

Ν. Καλουπτσίδης,	Καθηγητής Πανεπιστημίου Αθηνών
Θ. Σφηκόπουλος,	Καθηγητής Πανεπιστημίου Αθηνών
Δ. Μαρτάκος,	Αν. Καθηγητής Πανεπιστημίου Αθηνών
Κ. Χαλάτσης,	Καθηγητής Πανεπιστημίου Αθηνών
Λ. Μεράκος,	Καθηγητής Πανεπιστημίου Αθηνών
Η. Κουτσουπιάς,	Καθηγητής Πανεπιστημίου Αθηνών
Ι. Εμίρης,	Αν. Καθηγητής Πανεπιστημίου Αθηνών

Στους γονείς μου, Εμμανουήλ και Μαρία,
και στον αδελφό μου, Κωνσταντίνο.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμότερες ευχαριστίες στον επιβλέποντα καθηγητή μου κ. Ν. Καλουπτσίδη, Καθηγητή Πανεπιστημίου Αθηνών. Η αδιάκοπη επιστημονική του υποστήριξη, αλλά και η ηθική του συμπαράσταση, έπαιξαν τον πλέον καθοριστικό ρόλο στην πραγματοποίηση της παρούσας εργασίας. Η αστείρευτη επιστημονική του γνώση, ο ενθουσιασμός αλλά και η ικανότητα επίλυσης προβλημάτων συνδυάζοντας πληροφορίες διαφορετικών επιστημονικών περιοχών, αποτέλεσαν πηγή έμπνευσης και θαυμασμού. Ως υποψήφιος διδάκτορας, του οφείλω τα μέγιστα.

Θα ήθελα επίσης να ευχαριστήσω θερμά τον κ. Θ. Σφηκόπουλο, Καθηγητή Πανεπιστημίου Αθηνών, και τον κ. Δ. Μαρτάκο, Αν. Καθηγητή Πανεπιστημίου Αθηνών, που δέχτηκαν να αποτελέσουν μέλη της τριμελούς επιτροπής και να αξιολογήσουν την υποβαλλόμενη εργασία.

Επιπλέον, ευχαριστώ θερμά τους κ. Κ. Χαλάτση, Καθηγητή Πανεπιστημίου Αθηνών, κ. Λ. Μεράκο, Καθηγητή Πανεπιστημίου Αθηνών, κ. Η. Κουτσουπιά, Καθηγητή Πανεπιστημίου Αθηνών, και κ. Ι. Εμίρη, Αν. Καθηγητή Πανεπιστημίου Αθηνών, που δέχθηκαν να συμμετάσχουν στην επταμελή μου εξεταστική επιτροπή.

Ευχαριστώ θερμά τον υποψήφιο διδάκτορα Π. Ριζομυλιώτη για τις γόνιμες και ουσιαστικές συζητήσεις που αναπτύσσαμε στην ερευνητική περιοχή που πραγματεύεται η παρούσα εργασία. Η συνεργασία μου μαζί του υπήρξε άψογη. Επιπλέον, ευχαριστώ τον υποψήφιο διδάκτορα Γ. Γκαττ για τις χρήσιμες υποδείξεις του σε θέματα χρήσης ψευδοτυχαίων ακολουθιών για ταυτοποίηση γραμμικών και μη–γραμμικών συστημάτων.

Θα ήθελα επίσης να ευχαριστήσω το συνεργάτη Δρ. Π. Κανέλλη και την υποψήφια διδάκτορα Π. Παπαδοπούλου με τη βοήθεια και τις συμβουλές των οποίων

μελέτησα σε βάθος πρακτικές εφαρμογές της κρυπτογραφίας στην περιοχή του ηλεκτρονικού εμπορίου.

Τέλος, εκφράζω την ευγνωμοσύνη μου στην οικογένειά μου, για τη συνεχή συμπαράσταση που μου προσέφεραν, ψυχική και υλική, όλα αυτά τα χρόνια των σπουδών μου.

Ν. Κολοκοτρώνης

Περιεχόμενα

Κατάλογος σχημάτων

Κατάλογος πινάκων

Κατάλογος συντομογραφιών

AES	Advanced Encryption Standard
ARMA	Autoregressive Moving Average
BCH	Bose–Chaudhuri–Hocquenghem
CBC	Cipher Block Chaining
CFB	Cipher Feedback
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECB	Electronic Codebook
FEAL	Fast Data Encipherment Algorithm
FFT	Fast Fourier Transform
FIR	Finite Impulse Response
HTTP	Hypertext Transfer Protocol
IDEA	International Data Encryption Algorithm
IID	Independent & Identically Distributed
IP	Internet Protocol
KRG	Kolokotronis–Rizomiliotis–Gatt

LFSR	Linear Feedback Shift Register
NLSP	Network Layer Security Protocol
OFB	Output Feedback
OSI	Open Systems Interconnection
OFX	Open Financial Exchange
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standard
PPTP	Point–to–Point Tunneling Protocol
RSA	Rivest–Shamir–Adleman
SAFER	Secure And Fast Encryption Routine
SEAL	Software Optimized Encryption Algorithm
SET	Secure Electronic Transactions
S–HTTP	Secure Hypertext Transfer Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
SNR	Signal to Noise Ratio
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WAKE	Word Auto Key Encryption

Κατάλογος συμβολισμών

Ακολουθίες

D	Ο τελεστής κυκλικής ολίσθησης ακολουθιών προς τα αριστερά κατά μία θέση
L_x	Η γραμμική πολυπλοκότητα της ακολουθίας x
$\mathrm{PAC}_{\mathcal{F}}$	Η μέγιστη εκτός–φάσης αυτοσυσχέτιση της οικογένειας $\mathcal{F}$
$\mathrm{PC}_{\mathcal{F}}$	Η μέγιστη συσχέτιση της οικογένειας $\mathcal{F}$
$\mathrm{PCC}_{\mathcal{F}}$	Η μέγιστη ετεροσυσχέτιση της οικογένειας $\mathcal{F}$
$\mathrm{wc}_k(x)$	Η πολυπλοκότητα βάρους της ακολουθίας x με πραγματοποίηση k λαθών

Πίνακες

$\boldsymbol{A}^{-1}$	Ο αντίστροφος του πίνακα $\boldsymbol{A}$
$\boldsymbol{A}^{T}$	Ο ανάστροφος του πίνακα $\boldsymbol{A}$
$\boldsymbol{A}^{[m]}$	Η περιοδική επέκταση ή συρρίκνωση του ειδικής μορφής πίνακα $\boldsymbol{A}$ κατά m γραμμές και στήλες
$\boldsymbol{\Delta}$	Ο πίνακας που συνδέεται με το πολυώνυμο ανάδρασης ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης
$\boldsymbol{I}_m$	Ο $m \times m$ μοναδιαίος πίνακας
$\boldsymbol{J}_m$	Ο $m \times m$ πίνακας αντιστροφής διάταξης

Πολυώνυμα

$\deg(f)$	Ο βαθμός του πολυωνύμου f
$f^*(z)$	Το ανάστροφο του πολυωνύμου f, δηλ. $z^{\deg(f)} f(1/z)$
$\mathrm{ord}(f)$	Η τάξη του πολυωνύμου f, ίση με το βαθμό του μικροτέρου βαθμού διωνύμου που διαιρείται από το f

Στοιχεία

$n!$	Το παραγοντικό του ακεραίου n, δηλ. $1\,2\cdots n$
$n\|m$	Ο ακέραιος n διαιρεί το m
$\lfloor n \rfloor$	Το ακέραιο μέρος του n
$\binom{n}{m}$	Ο διωνυμικός συντελεστής, δηλ. $n!/m!(n-m)!$
$\gcd(z_1,\ldots,z_n)$	Ο μέγιστος κοινός διαιρέτης των στοιχείων $z_1,\ldots,z_n$
$\operatorname{lcm}(z_1,\ldots,z_n)$	Το ελάχιστο κοινό πολλαπλάσιο των στοιχείων $z_1,\ldots,z_n$
$\log_a n$	Ο λογάριθμος με βάση a του ακεραίου n
$\max(z_1,\ldots,z_n)$	Το μέγιστο των στοιχείων $z_1,\ldots,z_n$
$\min(z_1,\ldots,z_n)$	Το ελάχιστο των στοιχείων $z_1,\ldots,z_n$
$\bmod n$	Το υπόλοιπο της διαίρεσης με το στοιχείο n
$\operatorname{wt}(n)$	Το δυαδικό βάρος του ακεραίου n

Συναρτήσεις

$\mathrm{AC}_x()$	Η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας x
$\mathrm{CC}_{x,y}()$	Η συνάρτηση περιοδικής ετεροσυσχέτισης των ακολουθιών x και y
$\mathrm{cum}(z_1,\ldots,z_m)$	Η αθροιστική των στοιχείων $z_1,\ldots,z_m$ τάξης m
$\delta(m)$	Ο παλμός Dirac, είναι παντού μηδέν εκτός της θέσης m
$D_K(C)$	Η συνάρτηση αποκρυπτογράφησης, με κλειδί K, του κρυπτογραφήματος C
$E_K(M)$	Η συνάρτηση κρυπτογράφησης, με κλειδί K, του απλού κειμένου M
$\mathrm{E}(z_1\cdots z_m)$	Η αναμενόμενη τιμή (ροπή) του $z_1\cdots z_m$ τάξης m
$\varphi()$	Η συνάρτηση του Euler
$\mu()$	Η συνάρτηση του Möbius
$\mathrm{N}_{F/K}()$	Η νόρμα από το σώμα $F=\mathbb{F}_{p^n}$ στο $K=\mathbb{F}_p$
$\Pr(z=m)$	Η πιθανότητα η τυχαία μεταβλητή z να έχει τιμή m
$\mathrm{tr}_m^n()$	Η συνάρτηση ίχνους από το $\mathbb{F}_{2^n}$ στο $\mathbb{F}_{2^m}$ με $m\|n$

Σύνολα

$\|A\|$	Το πλήθος των στοιχείων του συνόλου A
A^*	Το σύνολο A εκτός του μηδενικού στοιχείου
$A\setminus B$	Αφαίρεση από το σύνολο A των κοινών στοιχείων του με το σύνολο B

$\mathbb{C}$	Το σύνολο των μιγαδικών αριθμών
C_m	Η κυκλοτομική κλάση του ακεραίου m
$\mathbb{F}_2$	Το πρωταρχικό σώμα $\{0, 1\}$ με δύο στοιχεία
$\mathbb{F}_{2^n}$	Το σώμα επέκταση του $\mathbb{F}_2$ με 2^n στοιχεία
I	Το σύνολο των επικεφαλείς κλάσεων
$\mathbb{N}$	Το σύνολο των φυσικών αριθμών
P_m	Το σύνολο των αντιμεταθέσεων του $\{1, 2, \ldots, m\}$
$\mathbb{Q}$	Το σύνολο των ρητών αριθμών
$\mathbb{R}$	Το σύνολο των πραγματικών αριθμών
R_m^n	Το σύνολο των διαμερίσεων του $\{1, 2, \ldots, m\}$ τάξης n
T_f	Το σύνολο των τριωνύμων ακολουθίας με ελάχιστο πολυώνυμο f
$\mathbb{Z}$	Το σύνολο των ακεραίων αριθμών
$\mathbb{Z}_m$	Το σύνολο $\{0, \ldots, m-1\}$ με m στοιχεία

Κεφάλαιο 1

Εισαγωγή

Τα συστήματα επεξεργασίας σήματος μετατρέπουν σήματα που παράγονται από τεχνικές ή φυσικές πηγές, σε μορφές κατάλληλες για την επίτευξη συγκεκριμένων στόχων. Παραδείγματα σημάτων είναι η φωνή, εικόνα, βίντεο, καθώς και δεδομένα ιατρικά, γεωφυσικά, κ.λπ. Μεταξύ άλλων, τυπικοί στόχοι αποτελούν η συλλογή, επεξεργασία, και εικονοποίηση των δεδομένων, η αποτελεσματική και αξιόπιστη μετάδοση και αποθήκευση δεδομένων, η ταυτοποίηση και βελτίωση της ποιότητας σημάτων [50].

Τα συστήματα επεξεργασίας σήματος χρησιμοποιούνται σε ένα ευρύ φάσμα εφαρμογών, όπως στην κατασκευαστική βιομηχανία (ρομποτική), στην επεξεργασία των ιατρικών σημάτων (ιατρική διάγνωση), και σε δίκτυα επικοινωνιών (ασφαλής μετάδοση δεδομένων). Μεταξύ των λειτουργιών που επιτελούν είναι οι ακόλουθες:

- συμπίεση για αύξηση της ταχύτητας μετάδοσης και μείωση του απαιτούμενου χώρου αποθήκευσης,
- κωδικοποίηση για την προστασία από λάθη κατά τη μετάδοση και αποθήκευση,
- κρυπτογράφηση για επίτευξη της εμπιστευτικότητας και διασφάλιση της αυθεντικότητας, και
- φιλτράρισμα για βελτίωση των χαρακτηριστικών και αφαίρεση θορύβου.

Η παρούσα διατριβή επικεντρώνεται κυρίως στις λειτουργίες κρυπτογράφησης που διασφαλίζουν το απόρρητο σημάτων ή δεδομένων προς αποθήκευση ή μετάδοση μέσω ανοικτών δικτύων, όπως το Διαδίκτυο. Εφαρμόζει τεχνικές επεξεργασίας σήματος για την ανάλυση και βελτίωση των χαρακτηριστικών τα οποία καθορίζουν το βαθμό ασφάλειας που αποδίδεται σε κρυπτογραφημένα σήματα [60], [62]–[65], [97], [98].

Το Διαδίκτυο έχει συνδυάσει μαζί υπηρεσίες εικόνας, ήχου, βίντεο, και δεδομένων. Συνεπώς, το γενικό πρόβλημα ασφάλειας δεν αφορά μόνο τον τομέα της κρυπτογράφησης, αλλά και της ακεραιότητας, πιστοποίησης ταυτότητας, και της ψηφιακής υπογραφής των δεδομένων προς μετάδοση. Λόγω της σπουδαιότητας της συγκεκριμένης θεματικής περιοχής, η παρούσα διατριβή περιλαμβάνει στο τέλος ένα κεφάλαιο το οποίο αναφέρεται στις εφαρμογές της κρυπτογραφίας στον τομέα του ηλεκτρονικού εμπορίου [54], [61], [77], [84], [88], [95].

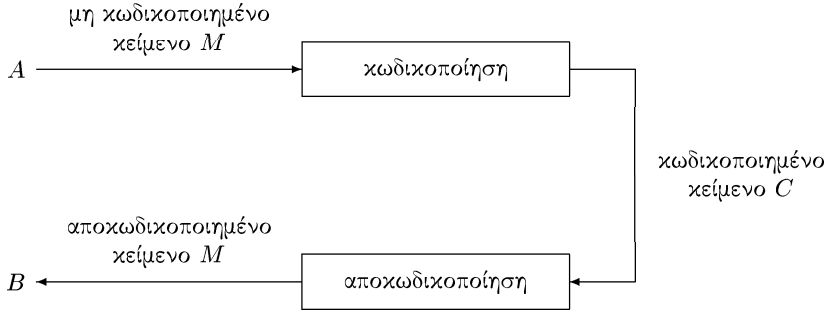
1.1 Βασικές έννοιες κρυπτογραφίας

Η συγκεκριμένη ενότητα έχει ως στόχο να εισάγει τις θεμελιώδεις έννοιες της κρυπτογραφίας ώστε στη συνέχεια (βλ. Ενότητα 1.2) να γίνει κατανοητό στον αναγνώστη το ακριβές πλαίσιο στο οποίο συνεισφέρει η παρούσα διατριβή.

Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται *απλό κείμενο*, ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται *κρυπτογράφημα*. Η διαδικασία κωδικοποίησης και αποκωδικοποίησης των δεδομένων απεικονίζεται στο Σχ. 1.1. Είναι σύνηθες, το απλό κείμενο και το κρυπτογράφημα να συμβολίζονται με M και C αντίστοιχα [109].

Κρυπτογράφηση είναι ο μετασχηματισμός του απλού κειμένου με σκοπό την παραγωγή ακατάληπτου μηνύματος (κρυπτογραφήματος) για τη διασφάλιση της εμπιστευτικότητάς του. Αντιθέτως, αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή του αντίστροφου αλγορίθμου. Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης συμβολίζονται με E και D αντίστοιχα.

Με μαθηματικούς συμβολισμούς, η διαδικασία παραγωγής του κρυπτογραφήματος C από το απλό κείμενο M συμβολίζεται με $E(M) = C$. Αντίστοιχα, η



Σχήμα 1.1. Κωδικοποίηση/αποκωδικοποίηση

διαδικασία ανάκτησης του απλού κειμένου M από το κρυπτογράφημα C συμβολίζεται με $D(C) = M$. Συνεπώς, ισχύει η ιδιότητα $D(E(M)) = M$.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα αποκρυπτογράφησης από τρίτο πρόσωπο. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, έαν μόνον τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος [3], [109], [112].

Γενικότερα, η κρυπτογραφία δύναται να ικανοποιήσει τους ακόλουθους στόχους [54], [84], [95].

- *εμπιστευτικότητα:* προστασία δεδομένων σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίηση τους.
- *αυθεντικότητα:* επιβεβαίωση της ταυτότητας ενός ατόμου ή η επιβεβαίωση της πηγής αποστολής των δεδομένων.
- *ακεραιότητα:* προστασία δεδομένων σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους.
- *μη–αποποίηση:* συνδυασμός της αυθεντικότητας και της ακεραιότητας που δεν επιτρέπει στον αποστολέα δεδομένων να αρνηθεί τη δημιουργία και αποστολή ενός μηνύματος.

Βασικό ρόλο για την παροχή των ανωτέρω υπηρεσιών διαδραματίζουν οι *αρχές πιστοποίησης* και οι *υποδομές δημοσίου κλειδιού*, που αναλύονται λεπτομερώς στο

Κεφάλαιο 7 [25], [88].

1.1.1 Συμμετρικοί και ασύμμετροι αλγόριθμοι

Ο αλγόριθμος κρυπτογράφησης χρησιμοποιεί ένα *κλειδί* για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν γίνει χρήση διαφορετικών κλειδιών. Το κλειδί συμβολίζεται με K.

Οι αλγόριθμοι των οποίων η ασφάλεια βασίζεται στη μη γνωστοποίηση των εσωτερικών τους μηχανισμών ονομάζονται *περιοριστικοί αλγόριθμοι* και έχουν ιστορική σημασία. Η ασφάλεια των σύγχρονων αλγορίθμων κρυπτογράφησης βασίζεται, μεταξύ άλλων, στη μη γνωστοποίηση του κλειδιού [109].

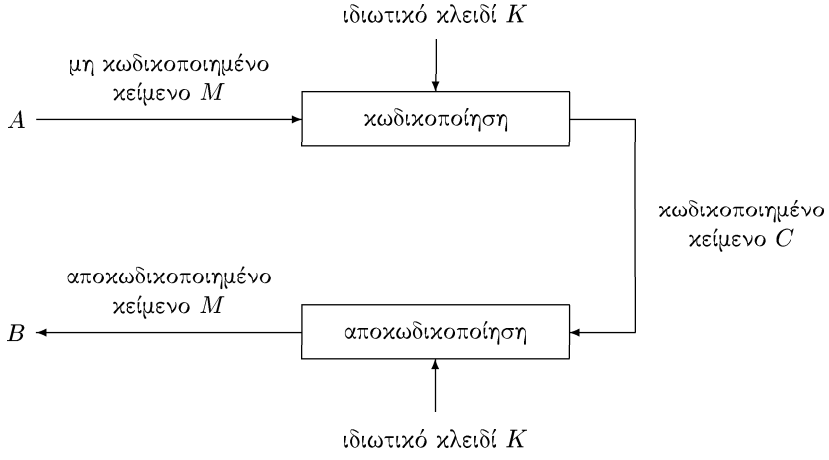
Οι περισσότεροι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν το ίδιο κλειδί κατά τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, και ονομάζονται *συμμετρικοί αλγόριθμοι*. Οι αλγόριθμοι που χρησιμοποιούν διαφορετικό κλειδί κατά την κρυπτογράφηση και αποκρυπτογράφηση ονομάζονται *ασύμμετροι αλγόριθμοι* [54], [95], [109].

Συμμετρική κρυπτογραφία

Η συμμετρική κρυπτογραφία *ή κρυπτογραφία ιδιωτικού κλειδιού* περιλαμβάνει τα κρυπτοσυστήματα που βασίζονται σε συμμετρικούς αλγορίθμους. Οι συμμετρικοί αλγόριθμοι, οι οποίοι ονομάζονται και *συμβατικοί αλγόριθμοι*, απαιτούν από τον αποστολέα A και τον παραλήπτη B ενός μηνύματος M να έχουν συμφωνήσει εκ των προτέρων το κλειδί που θα χρησιμοποιήσουν για την πραγματοποίηση ασφαλούς επικοινωνίας (Σχ. 1.2).

Ο αποστολέας A υπολογίζει και στέλνει την ποσότητα $E_K(M) = C$. Ομοίως, μετά την παραλαβή του κρυπτογραφήματος C, ο παραλήπτης B υπολογίζει και αποθηκεύει την ποσότητα $D_K(C) = D_K(E_K(M)) = M$.

Το σχήμα αυτό παρουσιάζει το μειονέκτημα ότι δεν είναι εύκολο να επεκταθεί για την εξυπηρέτηση μεγάλου πλήθους χρηστών και είναι δύσκολη η διαχείριση και διανομή των ιδιωτικών κλειδιών. Μεταξύ των αλγορίθμων κρυπτογράφησης που ανήκουν σε αυτή την κατηγορία είναι οι AES, DES, FEAL, IDEA, SAFER, RC2, RC5, SEAL, WAKE, και RC4 [84]–[86], [109].



Σχήμα 1.2. Κωδικοποίηση/αποκωδικοποίηση με κρυπτογραφία ιδιωτικού κλειδιού

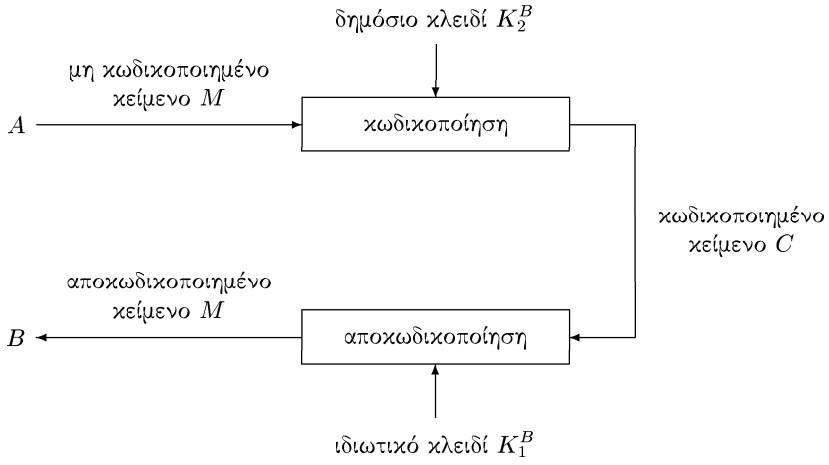
Ασύμμετρη κρυπτογραφία

Η ασύμμετρη κρυπτογραφία ή *κρυπτογραφία δημοσίου κλειδιού* περιλαμβάνει τα κρυπτοσυστήματα που βασίζονται σε ασύμμετρους αλγορίθμους. Οι ασύμμετροι αλγόριθμοι απαιτούν από τον αποστολέα A και τον παραλήπτη B ενός μηνύματος M να διατηρούν τα ζεύγη κλειδιών (K_1^A, K_2^A) και (K_1^B, K_2^B) αντίστοιχα (Σχ. 1.3) [87].

Τα κλειδιά K_1^A και K_1^B ονομάζονται *ιδιωτικά κλειδιά*, χρησιμοποιούνται μόνον από τον ιδιοκτήτη τους και δε γνωστοποιούνται ποτέ. Αντιθέτως, τα K_2^A και K_2^B ονομάζονται *δημόσια κλειδιά* και πρέπει να είναι γνωστά και διαθέσιμα. Κάθε ζεύγος κλειδιών δημιουργείται με τέτοιο τρόπο ώστε το ιδιωτικό κλειδί να είναι αδύνατο να παραχθεί από το δημόσιο με εύκολο τρόπο. Η κρυπτογραφία δημοσίου κλειδιού επιλύει τα προβλήματα επεκτασιμότητας και διανομής κλειδιών της κρυπτογραφίας ιδιωτικού κλειδιού [84].

Ο αποστολέας A υπολογίζει και στέλνει την ποσότητα $E_{K_2^B}(M) = C$. Ομοίως, μετά την παραλαβή του κρυπτογραφήματος C, ο παραλήπτης B υπολογίζει και αποθηκεύει την ποσότητα $D_{K_1^B}(C) = D_{K_1^B}(E_{K_2^B}(M)) = M$.

Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι ασύμμετρης κρυπτογραφίας



Σχήμα 1.3. Κωδικοποίηση/αποκωδικοποίηση με κρυπτογραφία δημοσίου κλειδιού

είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογραφίας. Μεταξύ των αλγορίθμων κρυπτογράφησης που ανήκουν σε αυτή την κατηγορία είναι οι DSA, RSA, Rabin, ElGamal, McEliece, και Knapsack [84], [109].

1.1.2 Τμηματικοί και σειριακοί αλγόριθμοι

Οι συμμετρικοί αλγόριθμοι διαχωρίζονται σε δύο κατηγορίες, τους *τμηματικούς αλγόριθμους* και τους *σειριακούς αλγόριθμους*. Βασικά χαρακτηριστικά και διαφορές των δύο κατηγοριών αναφέρονται στις ακόλουθες ενότητες. Αναλυτικές περιγραφές περιλαμβάνονται στις αναφορές [84], [109].

Τμηματικοί αλγόριθμοι

Οι τμηματικοί αλγόριθμοι ανήκουν στην κλάση αλγορίθμων συμμετρικής κρυπτογράφησης και εφαρμόζουν μία σταθερή χρονικά συνάρτηση σε μεγάλα τμήματα δεδομένων. Μετατρέπουν ένα τμήμα απλού κειμένου M_i, καθορισμένου μήκους, σε ένα τμήμα κρυπτογραφήματος C_i του ιδίου μήκους, βάσει του κλειδιού K. Τα συνήθη μεγέθη τμημάτων τα οποία επεξεργάζονται οι τμηματικοί αλγόριθμοι είναι 64, 128, και 256 bits.

Πίνακας 1.1. Ρυθμοί λειτουργίας τμηματικών αλγορίθμων

ρυθμός	κρυπτογράφηση	αποκρυπτογράφηση
ECB	$C_i = E_K(M_i)$	$M_i = D_K(C_i)$
CBC	$C_i = E_K(M_i + C_{i-1})$	$M_i = D_K(C_i) + C_{i-1}$
CFB	$C_i = M_i + K_i,\ K_i = E_K(C_{i-1})$	$M_i = C_i + K_i,\ K_i = E_K(C_{i-1})$
OFB	$C_i = M_i + K_i,\ K_i = E_K(K_{i-1})$	$M_i = C_i + K_i,\ K_i = E_K(K_{i-1})$

Οι τμηματικοί αλγόριθμοι λειτουργούν επαναληπτικά μετασχηματίζοντας ένα τμήμα διαδοχικά με συγκεκριμένο αριθμό επαναλήψεων. Σε κάθε επανάληψη, εφαρμόζεται ο ίδιος μετασχηματισμός. Το πλήθος των επαναλήψεων είναι ανάλογο του επιθυμητού επιπέδου ασφάλειας. Ειδική κατηγορία των τμηματικών αλγορίθμων αποτελούν οι αλγόριθμοι τύπου Feistel [51], [52], π.χ. ο αλγόριθμος DES [85]. Σημαντικό χαρακτηριστικό τους είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημη με την κρυπτογράφηση [109].

Οι τμηματικοί αλγόριθμοι έχουν τέσσερις ρυθμούς λειτουργίας (ECB, CBC, CFB, και OFB) οι οποίοι συνδυάζουν το βασικό αλγόριθμο με ένα συγκεκριμένο τρόπο ανάδρασης και απλές λογικές πράξεις. Στον Πίνακα 1.1 φαίνεται ο τρόπος με τον οποίο γίνεται η κρυπτογράφηση και αποκρυπτογράφηση. Στους ρυθμούς CFB και OFB, K_i συμβολίζει το *τρέχον κλειδί*. Ο ρυθμός λειτουργίας ECB είναι ο απλούστερος και ταχύτερος, ενώ οι τρεις τελευταίοι απαιτούν επιπλέον τη χρήση διανύσματος αρχικοποίησης [86].

Μεγάλο πλήθος τμηματικών αλγορίθμων έχουν δημοσιευτεί ορισμένοι εκ των οποίων έχουν προτυποποιηθεί ή εφαρμοστεί στην πράξη. Μεταξύ των αλγορίθμων κρυπτογράφησης που ανήκουν σε αυτή την κατηγορία είναι οι AES, DES, FEAL, IDEA, SAFER, RC2, και RC5 [109].

Σειριακοί αλγόριθμοι

Οι σειριακοί αλγόριθμοι ανήκουν στην κλάση αλγορίθμων συμμετρικής κρυπτογράφησης και εφαρμόζουν μία μεταβαλλόμενη χρονικά συνάρτηση σε μικρά τμήματα δεδομένων (χαρακτήρες ή συνήθως σε ένα bit). Μετατρέπουν ένα τμήμα απλού κειμένου m_i, καθορισμένου μήκους, σε ένα τμήμα κρυπτογραφήματος c_i του ιδίου μήκους, βάσει του κλειδιού k [54], [99], [109].

Γενικά, οι σειριακοί αλγόριθμοι είναι ταχύτεροι από τους τμηματικούς, έαν

Πίνακας 1.2. Κατηγορίες σειριακών αλγορίθμων

τύπος	κρυπτογράφηση	αποκρυπτογράφηση	τρέχον κλειδί
SYN	$c_i = h(m_i, k_i)$	$m_i = h^{-1}(c_i, k_i)$	$k_i = f_k(z_i)$, $z_i = g_k(z_{i-1})$
ASYN	$c_i = h(m_i, k_i)$	$m_i = h^{-1}(c_i, k_i)$	$k_i = f_k(z_i)$, $z_i = (c_{i-1}, \ldots, c_{i-t})$

υλοποιηθούν σε υλικό, λόγω των απλούστερων απαιτούμενων κυκλωμάτων. Επιπλέον, είναι πιο κατάλληλοι, και σε ορισμένες περιπτώσεις αναγκαίοι (π.χ. σε εφαρμογές τηλεπικοινωνιών), έαν η χρήση ενδιάμεσης μνήμης είναι περιορισμένη ή τα μικρά τμήματα δεδομένων πρέπει να επεξεργάζονται καθώς λαμβάνονται. Χαρακτηρίζονται από ελάχιστη έως μηδενική διάδοση σφαλμάτων, και συνεπώς η χρήση τους είναι επωφελής σε κανάλια επικοινωνίας με μεγάλη πιθανότητα εμφάνισης σφαλμάτων μετάδοσης [84].

Οι σειριακοί αλγόριθμοι διακρίνονται σε *σύγχρονους (SYN)* και *ασύγχρονους (ASYN)* ή *αυτο–συγχρονιζόμενους*. Στον Πίνακα 1.2 φαίνεται ο τρόπος με τον οποίο γίνεται η κρυπτογράφηση και αποκρυπτογράφηση. Τυπική περίπτωση σύγχρονων σειριακών αλγορίθμων είναι ο *δυαδικός προσθετικός*, όπου $c_i = m_i + k_i$, f_k *η συνάρτηση εξόδου*, και g_k *η συνάρτηση επόμενης κατάστασης* [84].

Στην πράξη, η δομή των περισσοτέρων σειριακών αλγορίθμων είναι απόρρητη, και συνεπώς μικρό πλήθος εξ΄ αυτών έχει δημοσιευτεί. Μεταξύ των αλγορίθμων κρυπτογράφησης που ανήκουν σε αυτή την κατηγορία είναι οι SEAL, WAKE, και RC4 [88], [109].

1.2 Αντικείμενο της διατριβής

Η Ενότητα 1.1 παρουσίασε τους βασικούς στόχους της κρυπτογραφίας και τις βασικές κατηγορίες αλγορίθμων κρυπτογράφησης. Η έρευνα της παρούσας διατριβής επικεντρώνεται στη θεματική περιοχή των *δυαδικών προσθετικών σύγχρονων σειριακών κρυπτοσυστημάτων*. Τα κρυπτοσυστήματα αυτής της κατηγορίας αποτελούνται από ένα *γεννήτορα τρέχοντος κλειδιού* του οποίου η ακολουθία εξόδου προστίθεται δυαδικά με τα bits του απλού κειμένου. Η ασφάλεια του συγκεκριμένου κρυπτοσυστήματος βασίζεται στο βαθμό τυχαιότητας της ακολουθίας

κλειδιών που παράγεται από το γεννήτορα τρέχοντος κλειδιού [54], [84], [95].

Ο θεμελιώδης στόχος κατά την κατασκευή σειριακών κρυπτοσυστημάτων είναι η παραγωγή *ψευδο–τυχαίων ακολουθιών κλειδιών* των οποίων τα χαρακτηριστικά προσομοιάζουν εκείνα των πραγματικά τυχαίων ακολουθιών που λαμβάνονται από φυσικές πηγές. Μία τέτοια ακολουθία δύναται να θεωρηθεί ως τυχαία έαν είναι αδύνατο να

- προσδιοριστούν υποδείγματα στα ψηφία της ακολουθίας,
- γίνει επιτυχής πρόβλεψη μεταγενέστερων ψηφίων της ακολουθίας δοθέντων των ψηφίων που έχουν παραχθεί, και να
- παραχθεί απλή περιγραφή του συστήματος που γεννά την ακολουθία.

Συνεπώς, ο ανωτέρω στόχος οδηγεί σε ανάγκη για την κατασκευή σειριακών κρυπτοσυστημάτων που παράγουν ψευδο–τυχαίες ακολουθίες κλειδιών μέσω των οποίων καθίσταται αδύνατη η εύρεση περιγραφής του συστήματος και του αντίστοιχου κλειδιού.

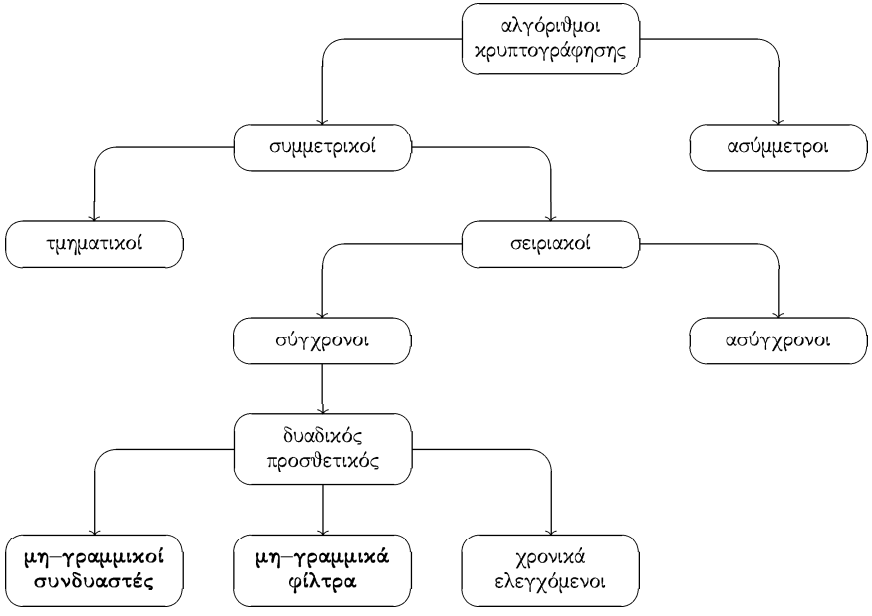
Πλήθος κατασκευών γεννητόρων τρέχοντος κλειδιού βασίζονται στους *καταχωρητές ολίσθησης με (γραμμική) ανάδραση*. Χαρακτηριστικά αναφέρουμε τους (Σχ. 1.4)

- *γεννήτορες μη–γραμμικού συνδυασμού*,
- *γεννήτορες μη–γραμμικού φίλτρου*, και
- *χρονικά ελεγχόμενους γεννήτορες*.

Ιδιότητες των ακολουθιών που παράγονται από τους αναφερόμενους γεννήτορες περιγράφονται στο Κεφάλαιο 3.

Τα ερευνητικά αποτελέσματα της διατριβής συνεισφέρουν στο σχεδιασμό γεννητόρων ψευδο–τυχαίων ακολουθιών, τύπου μη–γραμμικών συνδυαστών και μη–γραμμικών φίλτρων, ώστε να προσομοιάζουν πραγματικά τυχαίες ακολουθίες [60], [62]–[65], [97], [98].

Η δυνατότητα αξιοποίησης των ερευνητικών αποτελεσμάτων δεν περιορίζεται μόνο στο σχεδιασμό σειριακών κρυπτοσυστημάτων, καθώς ο βαθμός ασφάλειας πλήθους άλλων κρυπτοσυστημάτων βασίζεται στη χρήση τυχαίων ακολουθιών. Μεταξύ άλλων, παραδείγματα αποτελούν παράμετροι ασύμμετρων αλγορίθμων, όπως RSA και DSA, κλειδιά τμηματικών αλγορίθμων, όπως AES και DES,



Σχήμα 1.4. Θεματικές περιοχές συνεισφοράς της διατριβής

και ψευδο–τυχαία δεδομένα που χρησιμοποιούνται σε πρωτόκολλα *πρόκλησης–απόκρισης*, όπως SSL και TLS [54], [84], [85], [95].

Αποτίμηση του βαθμού τυχαιότητας ακολουθιών πραγματοποιείται εφαρμόζοντας διάφορους στατιστικούς ελέγχους. Ως παράδειγμα αναφέρουμε τους ελέγχους *ισοκατανομής* τάξης k, $k \geq 1$, *αυτοσυσχέτισης*, και *καθολικότητας*. Οι στατιστικοί έλεγχοι μεταφράζονται στην πράξη σε ιδιότητες που πρέπει να έχει μία ψευδο–τυχαία ακολουθία [33]:

- μεγάλη περίοδο,
- μεγάλη γραμμική πολυπλοκότητα, και
- επιθυμητές στατιστικές ιδιότητες (ισοκατανομή μονάδων και μηδενικών, ιδανική αυτοσυσχέτιση, κ.λπ.).

Η διατριβή επεκτείνει τις υπάρχουσες μεθοδολογίες ανάλυσης και σχεδιασμού ακολουθιών με μεγάλη γραμμική πολυπλοκότητα στο Κεφάλαιο 4. Επιπλέον,

εισάγει την έννοια της *προσέγγισης* ακολουθιών παραγόμενων από μη–γραμμικά φίλτρα ως ιδιότητα τυχαιότητας και παρέχει τρόπους σχεδιασμού στο Κεφάλαιο 5. Τέλος, εισάγει την έννοια της *τυχαιότητας υψηλότερης τάξης* και προτείνει ακολουθίες παραγόμενες από μη–γραμμικούς συνδυαστές που την ικανοποιούν στο Κεφάλαιο 6.

1.3 Δομή της διατριβής

Η παρούσα διατριβή αποτελείται από οκτώ κεφάλαια και δύο παραρτήματα, η δομή των οποίων (εκτός του παρόντος κεφαλαίου) περιγράφεται στη συνέχεια.

Κεφάλαιο 2: Δίνονται βασικές έννοιες της Άλγεβρας και θεωρίας πεπερασμένων σωμάτων, ενώ επιπλέον εισάγονται οι συμβολισμοί που χρησιμοποιούνται στην παρούσα διατριβή. Παρατίθενται τρόποι κατασκευής και αναπαράστασης στοιχείων των πεπερασμένων σωμάτων ως προς την εκθετική, πολυωνυμική, και κανονική μορφή κάνοντας χρήση της πολυωνυμικής και δυϊκής βάσης. Τέλος, εισάγεται η έννοια του ελαχίστου πολυωνύμου και των απεικονίσεων ίχνους και νόρμας, που χρησιμοποιούνται σε μεγάλο βαθμό στα επόμενα κεφάλαια.

Κεφάλαιο 3: Παρουσιάζονται βασικές έννοιες που χρησιμοποιούνται στη θεωρία ανάλυσης ψευδο–τυχαίων ακολουθιών, όπως η αναπαράσταση ίχνους και η τυπική αναπαράσταση δυναμοσειράς. Συνδέονται οι αναπαραστάσεις με κυκλώματα παραγωγής ακολουθιών (καταχωρητές ολίσθησης) και γραμμική άλγεβρα. Αναφέρονται ιδιότητες των ακολουθιών μεγίστου μήκους, ο μετασχηματισμός Fourier αυτών, και οι συναρτήσεις αυτο– και ετερο– συσχέτισης. Τέλος, ορίζεται η έννοια της γραμμικής πολυπλοκότητας.

Κεφάλαιο 4: Επεκτείνονται οι τεχνικές των E. L. Key και R. A. Rueppel για την ανάλυση της γραμμικής πολυπλοκότητας ακολουθιών που παράγονται από το μη–γραμμικό φιλτράρισμα ακολουθιών μεγίστου μήκους. Δίνονται τύποι που καθιστούν δυνατό τον πλήρη προσδιορισμό της αναπαράστασης ίχνους της ακολουθίας εξόδου σε σχέση με το μη–γραμμικό φίλτρο. Τέλος, περιγράφονται μέθοδοι για την εύρεση μη–γραμμικών φίλτρων που παράγουν ακολουθίες καθορισμένης γραμμικής πολυπλοκότητας.

Κεφάλαιο 5: Επιλύεται το πρόβλημα παραγωγής ακολουθιών κατά προσέγγιση εισάγοντας τρεις διαφορετικές μεθόδους. Παρουσιάζονται οι μέθοδοι των διαδοχικών διαιρέσεων, εξισώσεων ισοδυναμίας, και συγχρονισμού φάσεων. Οι μέθοδοι αυτές βασίζονται στον αλγόριθμο του Ευκλείδη, σε τρόπους επίλυσης

συνόλου εξισώσεων ισοδυναμίας, και στην αναπαράσταση ίχνους της ακολουθίας εισόδου αντίστοιχα. Τέλος, δίνονται σύνδεσμοι μεταξύ των διαφορετικών μεθόδων, καθώς και ιδιότητες για το σχεδιασμό ακολουθιών που είναι ανθεκτικές σε επιθέσεις προσέγγισης.

Κεφάλαιο 6: Διερευνώνται γνωστές κλάσεις δυαδικών ακολουθιών (μεγίστου μήκους, Gold, και δυϊκές BCH) ως προς το βαθμό προσομοίωσης σημάτων λευκού θορύβου ανωτέρας τάξης. Αποδεικνύεται ότι οι ακολουθίες μεγίστου μήκους δεν είναι κατάλληλες για την προσομοίωση σημάτων λευκού θορύβου τάξης μεγαλύτερης του 2. Ορίζεται η νέα κλάση ακολουθιών KRG, με ιδιότητες οι οποίες επιτρέπουν πλήρη έλεγχο της συμπεριφοράς τους σε ροπές ανωτέρας τάξης. Τέλος, δίνονται συγκριτικά αποτελέσματα πειραμάτων προσομοίωσης επιδεικνύοντας την ποιότητα των προτεινόμενων δυαδικών ακολουθιών στην ταυτοποίηση διγραμμικών μοντέλων εισόδου–εξόδου.

Κεφάλαιο 7: Δίνονται εφαρμογές της κρυπτογραφίας σε δίκτυα επικοινωνιών και εντοπίζονται σημεία όπου συνεισφέρουν τα θεωρητικά αποτελέσματα της διατριβής. Συγκεκριμένα, εισάγεται η έννοια των ψηφιακών υπογραφών, των αρχών πιστοποίησης, και των υποδομών δημοσίων κλειδιών. Αναλύεται η σημαντικότητα αυτών για την επίτευξη ασφαλούς επικοινωνίας μέσω του Διαδικτύου και την ανάπτυξη του ηλεκτρονικού εμπορίου. Επιπλέον, περιγράφονται βασικά πρωτόκολλα και τεχνικές για την ανάπτυξη στρατηγικών ασφάλειας που χρησιμοποιούνται ευρέως σε εφαρμογές.

Κεφάλαιο 8: Συνοψίζονται τα αποτελέσματα της διατριβής και περιγράφονται κατευθύνσεις για μελλοντική έρευνα.

Τέλος, τα **Παραρτήματα Α** και **Β** περιλαμβάνουν λίστες πρωταρχικών πολυωνύμων και αναλύσεις στατιστικών αντίστοιχα.

Κεφάλαιο 2

Πεπερασμένα σώματα

Η θεωρία των πεπερασμένων σωμάτων είναι κλάδος της μοντέρνας Άλγεβρας που γνωρίζει ιδιαίτερη άνθιση τα τελευταία 50 χρόνια λόγω του πλήθους εφαρμογών της, μεταξύ άλλων, σε προβλήματα συνδυαστικής, θεωρίας κωδίκων, και μαθηματικής ανάλυσης κυκλωμάτων.

Οι βάσεις της θεωρίας πεπερασμένων σωμάτων θεμελιώθηκαν από διαπρεπείς μαθηματικούς, όπως οι Leonhard Euler, Adrien–Marie Legendre, Joseph–Louis Lagrange, και Pierre de Fermat συνεισφέροντας στη θεωρία των πεπερασμένων πρωταρχικών σωμάτων. Η γενική θεωρία διατυπώθηκε πρώτη φορά μέσα από τις εργασίες των Carl Friedrich Gauss και Evariste Galois, αλλά απέκτησε ιδιαίτερο ενδιαφέρον στα εφαρμοσμένα μαθηματικά τις τελευταίες δεκαετίες λόγω της ανάπτυξης των διακριτών μαθηματικών.

Τα πεπερασμένα σώματα χρησιμοποιούνται στην ανάλυση των περισσοτέρων γνωστών κατασκευών ψευδοτυχαίων ακολουθιών και των περιόδων τους, των συναρτήσεων περιοδικής (αυτο– και ετερο–) συσχέτισης, της γραμμικής πολυπλοκότητας καταχωρητών ολίσθησης γραμμικής ανάδρασης και μη–γραμμικά παραγόμενων ακολουθιών. Επιπλέον, διαδραματίζουν ιδιαίτερο ρόλο σε ένα μεγάλο πλήθος κρυπτοσυστημάτων, όπως το πρωτόκολλο ανταλλαγής κλειδιών Diffie–Hellman, το πρότυπο ψηφιακών υπογραφών (DSS), κρυπτοσυστήματα δημοσίου κλειδιού ElGamal, και κρυπτοσυστήματα δημοσίου κλειδιού ελλειπτικών καμπύλων. Το παρόν κεφάλαιο συνοψίζει τις κυριότερες ιδιότητες των πεπερασμένων σωμάτων. Εκτενείς αναλύσεις περιλαμβάνονται στις αναφορές [15], [59], [72], [117].

2.1 Αλγεβρικές δομές

Στην ενότητα αυτή ορίζονται οι αλγεβρικές δομές των ομάδων, δακτυλίων, σωμάτων, και πολυωνύμων. Συμβολίζουμε με $\mathbb{N}$ το σύνολο των φυσικών αριθμών, με $\mathbb{Z}$ το σύνολο των ακεραίων, με $\mathbb{Q}$ το σύνολο των ρητών, με $\mathbb{R}$ το σύνολο των πραγματικών, και με $\mathbb{C}$ το σύνολο των μιγαδικών.

2.1.1 Ομάδες

Ας θεωρήσουμε το μη–κενό σύνολο S και έστω $S \times S$ είναι το σύνολο όλων των διατεταγμένων ζευγών (s, t) με $s, t \in S$. Τότε, κάθε απεικόνιση από το σύνολο $S \times S$ στο S ονομάζεται *(δυαδική) πράξη* πάνω στο σύνολο S.

Ορισμός 2.1. Ένα τυχαίο μη–κενό σύνολο S μαζί με μία ή περισσότερες πράξεις, κλειστές πάνω στο S, ονομάζεται *αλγεβρική δομή*.

Ορισμός 2.2. Η *ομάδα* είναι ένα μη–κενό σύνολο G μαζί με μία δυαδική πράξη $*$ κλειστή πάνω στο G, η οποία συμβολίζεται ως $(G, *)$, τέτοια ώστε να ισχύουν οι ακόλουθες τρεις ιδιότητες

i. Η πράξη $*$ είναι προσεταιριστική, δηλ. για κάθε $a, b, c \in G$ ισχύει

$$a * (b * c) = (a * b) * c.$$

ii. Υπάρχει στοιχείο $e \in G$, που ονομάζεται *μοναδιαίο στοιχείο*, τέτοιο ώστε για κάθε $a \in G$ ισχύει

$$a * e = e * a = a.$$

iii. Για κάθε $a \in G$, υπάρχει ένα *αντίστροφο στοιχείο* $a^{-1} \in G$ τέτοιο ώστε

$$a * a^{-1} = a^{-1} * a = e.$$

Έαν η ομάδα $(G, *)$ ικανοποιεί επιπλέον την ιδιότητα

iv. Η πράξη $*$ είναι αντιμεταθετική, δηλ. για κάθε $a, b \in G$ ισχύει

$$a * b = b * a$$

τότε ονομάζεται *αβελιανή ή αντιμεταθετική ομάδα*.

Παρατήρηση 2.3. Συχνά, αντί του συμβολισμού $(G, *)$ γράφουμε $(G, *, e)$, όπου e το μοναδιαίο στοιχείο της πράξης $*$.

Για λόγους απλοποίησης, χρησιμοποιούμε στη συνέχεια το σύμβολο του πολλαπλασιασμού για να προσδιορίσουμε την πράξη σε μία ομάδα, γράφοντας ab αντί του $a * b$. Επιπλέον, έαν η ομάδα G είναι αντιμεταθετική, τότε γράφουμε $a + b$ και $-a$ αντί του $a * b$ και a^{-1} αντίστοιχα, δηλ. χρησιμοποιούμε συμβολισμούς της πρόσθεσης.

Η προσεταιριστική ιδιότητα διασφαλίζει ότι εκφράσεις της μορφής $a_1 a_2 \cdots a_n$, με $a_j \in G$, υπολογίζονται με σαφήνεια ανεξάρτητα του τρόπου τοποθέτησης των παρενθέσεων, και πάντοτε αναπαριστούν το ίδιο στοιχείο της ομάδας G. Έαν $n \in \mathbb{N}$, τότε το στοιχείο της ομάδας G που προκύπτει από τις πράξεις

$$\underbrace{a\, a\, \cdots\, a}_{n \text{ στοιχεία}} \quad \text{ή} \quad \underbrace{a + a + \cdots + a}_{n \text{ στοιχεία}}$$

συμβολίζεται με a^n ή na, χρησιμοποιώντας τον πολλαπλασιαστικό ή αθροιστικό συμβολισμό αντίστοιχα. Συγκεκριμένα, το στοιχείο a^n ονομάζεται n–στή δύναμη του $a \in G$.

Χρησιμοποιώντας τους συμβολισμούς του πολλαπλασιασμού και της πρόσθεσης αντίστοιχα έχουμε τις ακόλουθες ιδιότητες:

$$\begin{aligned} a^{-n} &= (a^{-1})^n, & (-n)a &= n(-a), \\ a^n a^m &= a^{n+m}, & na + ma &= (n+m)a, \\ (a^n)^m &= a^{nm}, & m(na) &= (mn)a. \end{aligned}$$

Έαν ο φυσικός αριθμός n είναι ίσος με το μηδέν, τότε θεωρούμε ότι $a^0 = e$ και $0a = 0$, όπου το τελευταίο μηδενικό αναπαριστά το μοναδιαίο στοιχείο της ομάδας G, χρησιμοποιώντας τον πολλαπλασιαστικό και αθροιστικό συμβολισμό αντίστοιχα.

Παράδειγμα 2.4. Τα $(\mathbb{Z}, +, 0)$, $(\mathbb{R}, +, 0)$, και $(\mathbb{R}^*, \cdot, 1)$ είναι ομάδες, όπου $\mathbb{R}^*$ είναι το σύνολο των πραγματικών εκτός του μηδενικού στοιχείου. □

Χρησιμοποιούμε το $\mathbb{Z}_n$ για να συμβολίσουμε το σύνολο των υπολοίπων της διαίρεσης όλων των ακεραίων με το n, όπου n είναι θετικός ακέραιος, δηλ.

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Το σύνολο $\mathbb{Z}_n^*$ περιέχει όλα τα μη–μηδενικά στοιχεία του $\mathbb{Z}_n$. Στο εξής, συμβολίζουμε με $a \bmod n$ το υπόλοιπο της διαίρεσης του ακεραίου a με το n. Για απλοποίηση γράφουμε $a+b$ και ab αντί του $a+b \bmod n$ και $ab \bmod n$, όπου $+$ και $\cdot$ συμβολίζουν τις συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού αντίστοιχα.

Παράδειγμα 2.5. Οι αλγεβρικές δομές

α΄. $(\mathbb{Z}_2, +, 0)$, $(\mathbb{Z}_5, +, 0)$, και $(\mathbb{Z}_6, +, 0)$ είναι ομάδες με πράξη την πρόσθεση.

β΄. $(\mathbb{Z}_5^*, \cdot, 1)$ είναι ομάδα με πράξη τον πολλαπλασιασμό. □

Στη συνέχεια θα αποδείξουμε ορισμένες βασικές ιδιοτήτες των ομάδων. Για το λόγο αυτό παραθέτουμε το ακόλουθο αποτέλεσμα.

Γεγονός 2.6. Έστω p πρώτος αριθμός και a ακέραιος με $0 < a < p$. Επειδή $\gcd(a, p) = 1$, υπάρχουν ακέραιοι u, v τέτοιοι ώστε $au + pv = 1$, όπου $0 < u < p$.

Πρόταση 2.7. *Έστω n τυχαίος θετικός ακέραιος και p τυχαίος πρώτος αριθμός. Τότε ισχύουν τα ακόλουθα [72]:*

i. $(\mathbb{Z}_n, +, 0)$ *είναι ομάδα, και ονομάζεται προσθετική ομάδα των ακεραίων modulo n.*

ii. $(\mathbb{Z}_p^*, \cdot, 1)$ *είναι ομάδα, και ονομάζεται πολλαπλασιαστική ομάδα των ακεραίων modulo p.*

Ορισμός 2.8. Η πολλαπλασιαστική ομάδα G ονομάζεται *κυκλική* έαν υπάρχει στοιχείο $a \in G$ τέτοιο ώστε για κάθε $b \in G$ υπάρχει ακέραιος i με $b = a^i$. Το στοιχείο a ονομάζεται *γεννήτορας* της κυκλικής ομάδας G, και θα γράφουμε $G =< a >$.

Παράδειγμα 2.9. Για τις ομάδες

α΄. $(\mathbb{Z}, +, 0)$, το 1 και το -1 είναι γεννήτορες.

β΄. $(\mathbb{Z}_6, +, 0)$, το 1 και το 5 είναι γεννήτορες.

γ΄. $(\mathbb{Z}_3^*, \cdot, 1)$, το 2 είναι γεννήτορας.

δ΄. $(\mathbb{Z}_5^*, \cdot, 1)$, το 2 και το 3 είναι γεννήτορες. □

Ορισμός 2.10. Μία ομάδα ονομάζεται *πεπερασμένη* (αντ. *άπειρη*) έαν περιέχει πεπερασμένο (αντ. άπειρο) πλήθος στοιχείων. Ο αριθμός των στοιχείων σε μία πεπερασμένη ομάδα G ονομάζεται *τάξη* της ομάδας, και συμβολίζεται με $|G|$.

2.1.2 Δακτύλιοι και σώματα

Το μεγαλύτερο πλήθος των ευρέως γνωστών αριθμητικών συστημάτων, όπως των ακεραίων, ρητών, και πραγματικών αριθμών, χρησιμοποιούν τις δυαδικές πράξεις της πρόσθεσης και του πολλαπλασιασμού. Στη συνέχεια, ορίζουμε την αλγεβρική δομή του δακτυλίου, η οποία έχει βασικές κοινές ιδιότητες με τα προαναφερθέντα αριθμητικά συστήματα.

Ορισμός 2.11. Ο *δακτύλιος* $(R, +, \cdot)$ είναι ένα σύνολο R, μαζί με δύο δυαδικές πράξεις, που συμβολίζονται με $+$ και $\cdot$, τέτοιες ώστε:

i. Το σύνολο R είναι αντιμεταθετική ομάδα ως προς την πράξη $+$.

ii. Η πράξη $\cdot$ είναι προσεταιριστική, δηλ. ισχύει $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, για κάθε $a, b, c \in R$.

iii. Ισχύει η επιμεριστική ιδιότητα, δηλ. για κάθε $a, b, c \in R$ έχουμε $a \cdot (b + c) = a \cdot b + a \cdot c$ και $(b + c) \cdot a = b \cdot a + c \cdot a$.

Παράδειγμα 2.12. Οι αλγεβρικές δομές

α΄. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, και $(\mathbb{C}, +, \cdot)$ είναι δακτύλιοι.

β΄. $(\mathbb{Z}_n, +, \cdot)$ είναι δακτύλιος, ο οποίος ονομάζεται *δακτύλιος κλάσεων υπολοίπων modulo* n. □

Ορισμός 2.13. Ο δακτύλιος $(R, +, \cdot)$ ονομάζεται

i. *δακτύλιος με μοναδιαίο στοιχείο* έαν υπάρχει στοιχείο $e \in R$ τέτοιο ώστε για κάθε $a \in R$ να ισχύει $ae = ea = a$.

ii. *αντιμεταθετικός δακτύλιος* έαν η πράξη του πολλαπλασιασμού είναι αντιμεταθετική.

iii. *ακέραια περιοχή* έαν είναι αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο, και έαν επιπλέον για κάθε $a, b \in R$ με $ab = 0$ ισχύει $a = 0$ ή $b = 0$.

iv. *δακτύλιος διαίρεσης* έαν τα μη–μηδενικά στοιχεία του R αποτελούν ομάδα ως προς την πράξη του πολλαπλασιασμού.

Ορισμός 2.14. *Σώμα* είναι ένας δακτύλιος $(F, +, \cdot)$ τέτοιος ώστε το σύνολο F^* μαζί με την πράξη του πολλαπλασιασμού $\cdot$ να αποτελεί αντιμεταθετική ομάδα.

Σύμφωνα με τον ορισμό, *σώμα* είναι ένα σύνολο F στο οποίο ορίζονται δύο δυαδικές πράξεις, η πρόσθεση και ο πολλαπλασιασμός, και το οποίο περιέχει δύο διακριτά στοιχεία 0 και 1 (συμβολίζουμε το πολλαπλασιαστικό μοναδιαίο στοιχείο e με 1) με $0 \neq 1$. Επιπρόσθετα, το $(F, +)$ είναι αντιμεταθετική ομάδα ως προς την πρόσθεση με το 0 ως μοναδιαίο στοιχείο, ενώ το $(F^*, \cdot)$ είναι αντιμεταθετική ομάδα ως προς τον πολλαπλασιασμό με το 1 ως μοναδιαίο στοιχείο.

Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού συνδέονται μέσω της επιμεριστικής ιδιότητας $a(b+c) = ab+ac$. Η δεύτερη επιμεριστική ιδιότητα $(b+c)a = ba+ca$ απορρέει από την αντιμεταθετικότητα του πολλαπλασιασμού. Το στοιχείο 0 ονομάζεται *μηδενικό στοιχείο* και το 1 ονομάζεται *πολλαπλασιαστικό μοναδιαίο στοιχείο* ή απλά *μονάδα*.

Ορισμός 2.15. *Πεπερασμένο σώμα* είναι ένα σώμα το οποίο περιέχει πεπερασμένο αριθμό στοιχείων, και ο αριθμός αυτός ονομάζεται *τάξη* του σώματος. Τα πεπερασμένα σώματα ονομάζονται και *σώματα Galois*.

Παρατήρηση 2.16. Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Παράδειγμα 2.17. Οι αλγεβρικές δομές

α΄. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, και $(\mathbb{C}, +, \cdot)$ είναι σώματα.

β΄. $(\mathbb{Z}_5, +, \cdot)$ είναι πεπερασμένο σώμα.

γ΄. $(\mathbb{Z}_2, +, \cdot)$ είναι πεπερασμένο σώμα. Τα στοιχεία του συγκεκριμένου σώματος, τάξης 2, είναι τα 0 και 1, και οι πίνακες που αντιστοιχούν στις πράξεις της πρόσθεσης και του πολλαπλασιασμού έχουν την ακόλουθη μορφή

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

όπου τα 0 και 1 ονομάζονται *δυαδικά στοιχεία*. □

Πρόταση 2.18. *Έαν ο ακέραιος p είναι πρώτος, τότε η αλγεβρική δομή $(\mathbb{Z}_p, +, \cdot)$ είναι σώμα.*

Απόδειξη. Από την Πρόταση 2.7, οι αλγεβρικές δομές $(\mathbb{Z}_p, +)$ και $(\mathbb{Z}_p^*, \cdot)$ είναι αντιμεταθετικές ομάδες. Οι ακέραιοι ικανοποιούν την επιμεριστική ιδιότητα, και τελικά ισχύει $a(b+c) = ab+ac$ για κάθε $a, b, c \in \mathbb{Z}_p$, δηλ. τα υπόλοιπα της

διαίρεσης του αριστερού και δεξιού μέλους της επιμεριστικής ιδιότητας με το p είναι ίσα. Συνεπώς, το $\mathbb{Z}_p$ ικανοποιεί την επιμεριστική ιδιότητα. Σύμφωνα με τον Ορισμό 2.14, το $(\mathbb{Z}_p, +, \cdot)$ είναι σώμα. □

Στη συνέχεια, το σώμα $(\mathbb{Z}_p, +, \cdot)$, που ονομάζεται *σώμα κλάσεων υπολοίπων modulo p*, συμβολίζεται απλά ως $\mathbb{Z}_p$ ή $\mathbb{F}_p$, και αποτελεί το πρώτο παράδειγμα πεπερασμένου σώματος [93], [94].

2.1.3 Πολυώνυμα

Στην παρούσα ενότητα παραθέτουμε αποτελέσματα σχετικά με πολυώνυμα πάνω σε δακτύλιους και σώματα. Συγκεκριμένα, θεωρούμε ένα δακτύλιο R. Ένα *πολυώνυμο* πάνω στο R είναι μία έκφραση της μορφής

$$f(z) = \sum_{i=0}^{n} a_i z^i = a_0 + a_1 z + \cdots + a_n z^n \tag{2.1}$$

όπου ο ακέραιος n είναι μη–αρνητικός, οι συντελεστές a_i, $0 \leq i \leq n$, είναι στοιχεία του δακτυλίου R, και z είναι η ανεξάρτητη μεταβλητή. Θεωρούμε ότι οι όροι $a_i z^i$ με $a_i = 0$ δεν είναι απαραίτητο να συμπεριλαμβάνονται στην (2.1). Συνεπώς, το πολυώνυμο $f(z)$ γράφεται στην ισοδύναμη μορφή

$$f(z) = a_0 + a_1 z + \cdots + a_n z^n + 0 z^{n+1} + \cdots + 0 z^{n+h}$$

όπου h είναι θετικός ακέραιος. Συμπεραίνουμε ότι κατά τη σύγκριση πάνω στο R δύο τυχαίων πολυωνύμων $f(z)$ και $g(z)$ μπορούμε δίχως βλάβη της γενικότητας να υποθέσουμε ότι περιλαμβάνουν τις ίδιες δυνάμεις της μεταβλητής z. Τα πολυώνυμα

$$f(z) = \sum_{i=0}^{n} a_i z^i \quad \text{και} \quad g(z) = \sum_{i=0}^{n} b_i z^i$$

είναι ίσα έαν και μόνον έαν $a_i = b_i$ για κάθε $0 \leq i \leq n$. Η πρόσθεση δύο πολυωνύμων $f(z)$ και $g(z)$ ορίζεται ως εξής

$$f(z) + g(z) = \sum_{i=0}^{n} (a_i + b_i) z^i.$$

Αντίστοιχα, το γινόμενο των $f(z) = \sum_{i=0}^{n} a_i z^i$ και $g(z) = \sum_{j=0}^{m} b_j z^j$ ορίζεται από τις σχέσεις

$$f(z)g(z) = \sum_{k=0}^{nm} c_k z^k \quad \text{με} \quad c_k = \sum_{i+j=k} a_i b_j$$

όπου το άθροισμα διατρέχει όλους τους ακεραίους $0 \leq i \leq n$ και $0 \leq j \leq m$. Προφανώς, το σύνολο των πολυωνύμων πάνω στο R με τις πράξεις τις πρόσθεσης και του πολλαπλασιασμού, όπως ορίστηκαν προηγουμένως, αποτελεί δακτύλιο [117].

Ορισμός 2.19. Ο δακτύλιος που σχηματίζεται από τα πολυώνυμα πάνω στο R με τις ανωτέρω πράξεις ονομάζεται *πολυωνυμικός δακτύλιος πάνω στο* R και συμβολίζεται με $R[z]$, δηλ.

$$R[z] = \left\{ \sum_{i=0}^{n} a_i z^i : \ a_i \in R, n \geq 0 \right\}.$$

Το μηδενικό στοιχείο του $R[z]$ είναι το πολυώνυμο του οποίου όλοι οι συντελεστές είναι ίσοι με μηδέν, ονομάζεται *μηδενικό πολυώνυμο*, και συμβολίζεται με 0.

Ορισμός 2.20. Ας θεωρήσουμε ότι το $f(z)$ δεν είναι το μηδενικό πολυώνυμο πάνω στο R, ώστε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι $a_n \neq 0$. Τότε, τα a_0 και a_n ονομάζονται *σταθερός όρος* και *μεγιστοβάθμιος συντελεστής* του $f(z)$ αντίστοιχα, ενώ το n ονομάζεται *βαθμός* του $f(z)$ και συμβολίζεται με

$$n = \deg(f(z)) = \deg(f).$$

Θέτουμε $\deg(0) = -\infty$, ενώ τα πολυώνυμα μηδενικού βαθμού ονομάζονται *σταθερά πολυώνυμα*. Έαν το R είναι σώμα, και έαν επιπλέον ο μεγιστοβάθμιος συντελεστής του $f(z)$ είναι 1, τότε το $f(z)$ ονομάζεται *μονικό πολυώνυμο* [117].

Στη συνέχεια, εξετάζουμε πολυώνυμα τα οποία είναι ορισμένα πάνω σε σώματα.

Θεώρημα 2.21. *Έστω ότι τα πολυώνυμα $f(z)$ και $g(z)$ ανήκουν στο δακτύλιο $F[z]$. Τότε, ισχύουν οι ακόλουθες ιδιότητες:*

i. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$, *και*

ii. $\deg(fg) = \deg(f) + \deg(g)$.

Απόδειξη. Η απόδειξη βασίζεται στον υπολογισμό του μεγιστοβάθμιου συντελεστή του αθροίσματος και γινομένου αντίστοιχα των δύο πολυωνύμων. □

Έστω $f(z), g(z), h(z) \in F[z]$. Είναι γνωστό από τη βιβλιογραφία ότι το πολυώνυμο $g(z)$ διαιρεί το $f(z)$ έαν υπάρχει πολυώνυμο $h(z)$ τέτοιο ώστε $f(z) = g(z)h(z)$. Το πολυώνυμο $g(z)$ ονομάζεται *διαιρέτης* του $f(z)$. Αντίστοιχα, το πολυώνυμο $f(z)$ ονομάζεται *πολλαπλάσιο* του $g(z)$ ή ισοδύναμα λέμε ότι το $f(z)$ διαιρείται από το $g(z)$.

Θεώρημα 2.22 (Αλγόριθμος διαίρεσης). *Ας θεωρήσουμε το μη–μηδενικό πολυώνυμο $g(z) \in F[z]$, και έστω $f(z), q(z), r(z) \in F[z]$. Τότε, για κάθε πολυώνυμο $f(z)$ υπάρχουν μονοσήμαντα ορισμένα $q(z), r(z)$ τέτοια ώστε [72]*

$$f(z) = q(z)g(z) + r(z)$$

όπου $\deg(r) < \deg(g)$.

Ορισμός 2.23. Έστω τα πολυώνυμα $f(z), g(z) \in F[z]$ τα οποία δεν είναι και τα δύο ταυτόχρονα ίσα με 0. Έαν το $d(z) \in F[z]$ ικανοποιεί τις συνθήκες

i. το πολυώνυμο $d(z)$ διαιρεί τα $f(z)$ και $g(z)$, και

ii. κάθε πολυώνυμο $c(z) \in F[z]$ που διαιρεί τα $f(z)$ και $g(z)$ θα διαιρεί και το $d(z)$

τότε, το $d(z)$ ονομάζεται *μέγιστος κοινός διαιρέτης* των πολυωνύμων $f(z)$ και $g(z)$, και συμβολίζεται με $d(z) = \gcd(f(z), g(z))$. Έαν $d(z) = 1$, τα πολυώνυμα $f(z)$ και $g(z)$ ονομάζονται *σχετικά πρώτα*.

Θεώρημα 2.24. *Έστω $d(z) = \gcd(f(z), g(z))$ και $d(z), f(z), g(z) \in F[z]$. Τότε, το πολυώνυμο $d(z)$ γράφεται στην ακόλουθη μορφή*

$$d(z) = u(z)f(z) + g(z)v(z)$$

με $u(z), v(z) \in F[z]$.

Ορισμός 2.25. Το πολυώνυμο $p(z) \in F[z]$ ονομάζεται *ανάγωγο* στο σώμα F έαν έχει βαθμό μεγαλύτερο του μηδενός και έαν

$$p(z) = b(z)c(z), \qquad b(z), c(z) \in F[z]$$

ο μοναδικός μη–μηδενικός συντελεστής των $b(z)$ ή $c(z)$ είναι ο σταθερός όρος. Διαφορετικά, το πολυώνυμο $p(z)$ ονομάζεται *αναγώγιμο* στο σώμα F.

Τα ανάγωγα πολυώνυμα έχουν εξαιρετική σημασία για τη δομή του δακτυλίου $F[z]$, ή ισοδύναμα για τη δομή ακολουθιών παραγόμενων από καταχωρητές ολίσθησης γραμμικής ανάδρασης. Αυτό οφείλεται στη μοναδικότητα ανάλυσης πολυωνύμων του $F[z]$ ως γινομένων αναγώγων πολυωνύμων σύμφωνα με το ακόλουθο θεώρημα.

Θεώρημα 2.26 (Μοναδικότητα Παραγοντοποίησης). *Κάθε πολυώνυμο $f(z) \in F[z]$ βαθμού μεγαλύτερου του μηδενός παραγοντοποιείται ως*

$$f(z) = a\, p_1(z)^{e_1} p_2(z)^{e_2} \cdots p_k(z)^{e_k} \tag{2.2}$$

όπου $a \in F$, $p_1(z), \ldots, p_k(z)$ είναι διαφορετικά μονικά ανάγωγα πολυώνυμα στο $F[z]$, και $e_1, \ldots, e_k$ είναι θετικοί ακέραιοι. Επιπλέον, η παραγοντοποίηση (2.2) είναι μοναδική, με εξαίρεση τη διάταξη των παραγόντων.

Απόδειξη. Η απόδειξη του θεωρήματος αναπτύσσεται στο [72]. □

Ορισμός 2.27. Το στοιχείο $b \in F$ ονομάζεται *ρίζα* ή *μηδενικό* του πολυωνύμου $f(z) \in F[z]$ έαν ισχύει $f(b) = 0$.

2.2 Βασική θεωρία πεπερασμένων σωμάτων

Στην παρούσα ενότητα παρουσιάζουμε αποτελέσματα που σχετίζονται με βασικές ιδιότητες των πεπερασμένων σωμάτων, όπως η χαρακτηριστική, οι γεννήτορες, και αναπαραστάσεις των στοιχείων τους.

2.2.1 Χαρακτηριστική πεπερασμένου σώματος

Ορισμός 2.28. Έστω F πεπερασμένο σώμα και έστω θετικός ακέραιος m τέτοιος ώστε $m\alpha = 0$ για κάθε $\alpha \in F$. Τότε, ο ελάχιστος θετικός ακέραιος με αυτήν την ιδιότητα ονομάζεται *χαρακτηριστική* του σώματος F, ή ισοδύναμα, λέμε ότι το σώμα F έχει χαρακτηριστική m.

Θεώρημα 2.29. *Η χαρακτηριστική ενός πεπερασμένου σώματος F είναι πρώτος αριθμός.*

Ένα σώμα είναι δυνατό να περιέχει υποσώματα. Το υποσύνολο K του σώματος F, το οποίο είναι σώμα ως προς τις πράξεις του F ονομάζεται *υπόσωμα* του F. Αντίστοιχα, το F ονομάζεται *επέκταση* του σώματος K. Έαν $K \subset F$, τότε λέμε ότι το K είναι *γνήσιο υπόσωμα* του F. Συνεπώς, το σώμα $\mathbb{F}_{p^n}$ έχει χαρακτηριστική p και περιέχει το $\mathbb{F}_p$ ως υπόσωμα. Πρόσθετες ιδιότητες αναφέρονται στην ενότητα 2.5.

2.2.2 Δομές πεπερασμένου σώματος

Θεώρημα 2.30. *Ας θεωρήσουμε το πεπερασμένο σώμα F με $|F| = q$ στοιχεία και χαρακτηριστική p. Τότε, θα ισχύει $F = \mathbb{F}_p$ έαν $q = p$, ή το σώμα F είναι n–διάστατος διανυσματικός χώρος στο $\mathbb{F}_p$ έαν $q > p$, δηλ. $q = p^n$.*

Απόδειξη. Έστω $q = p$. Αφού $\mathbb{F}_p$ υπόσωμα του F, λαμβάνουμε $F = \mathbb{F}_p$. Έστω τώρα $q > p$. Επιλέγουμε ένα μέγιστο σύνολο στοιχείων του F τα οποία είναι γραμμικά ανεξάρτητα στο $\mathbb{F}_p$, έστω το $\{\alpha_0, \ldots, \alpha_{n-1}\}$. Τότε, το σώμα F περιέχει όλα τα στοιχεία της μορφής

$$a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1}, \qquad a_i \in \mathbb{F}_p$$

και μόνον αυτά. Συνεπώς, το σώμα F είναι n–διάστατος διανυσματικός χώρος στο $\mathbb{F}_p$, και περιέχει $q = p^n$ στοιχεία. □

Σύμφωνα με το Θεώρημα 2.30, έαν F είναι πεπερασμένο σώμα τάξης q και p είναι η χαρακτηριστική του F, τότε ισχύει $q = p$ ή $q = p^n$ με $n \geq 1$. Δύο πεπερασμένα σώματα F και G ονομάζονται *ισόμορφα* έαν υπάρχει ένα–προς–ένα και επί απεικόνιση από το F στο G η οποία διατηρεί τις πράξεις της πρόσθεσης και του πολλαπλασιασμού [72].

Όλα τα πεπερασμένα σώματα τάξης p^n είναι ισόμορφα μεταξύ τους. Συνεπώς, διακρίνουμε μόνο δύο τύπους πεπερασμένων σωμάτων. Ο πρώτος είναι ο $\mathbb{F}_p$, το πρωταρχικό σώμα κλάσσεων υπολοίπων modulo p, ενώ ο δεύτερος είναι ο $\mathbb{F}_{p^n}$, η επέκταση που λαμβάνεται προσαρτώντας μία από τις ρίζες ενός πολυωνύμου βαθμού n ανάγωγου στο $\mathbb{F}_p$. Στη συνέχεια, συμβολίζουμε συχνά το σώμα F τάξης q με F_q.

Έαν F είναι πεπερασμένο σώμα, τότε συμβολίζουμε με F^* την πολλαπλασιαστική ομάδα των μη–μηδενικών στοιχείων του F. Ας θεωρήσουμε το στοιχείο $\alpha \in F$, και έστω r είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $\alpha^r = 1$. Ο

ακέραιος r ονομάζεται *τάξη* του στοιχείου α, και συμβολίζεται με $r = \mathrm{ord}(\alpha)$. Το ακόλουθο αποτέλεσμα είναι απαραίτητο για την απόδειξη σημαντικών ιδιοτήτων των πεπερασμένων σωμάτων.

Γεγονός 2.31. Ας θεωρήσουμε τα στοιχεία $\alpha, \beta \in F^*$ της πολλαπλασιαστικής ομάδας του σώματος F, με $\mathrm{ord}(\alpha) = r$ και $\mathrm{ord}(\beta) = s$. Τότε ισχύουν τα εξής

i. $\mathrm{ord}(\alpha^m) = r/\gcd(r, m)$. Έαν επιπλέον ισχύει $\gcd(r, m) = 1$, τότε είναι $\mathrm{ord}(\alpha^m) = \mathrm{ord}(\alpha)$.

ii. Έαν ισχύει $\gcd(r, s) = 1$, τότε $\mathrm{ord}(\alpha\beta) = rs$.

Θεώρημα 2.32. *Για κάθε πεπερασμένο σώμα F, η πολλαπλασιαστική ομάδα F^* είναι κυκλική.*

Απόδειξη. Έστω $|F| = q$. Πρέπει να δείξουμε ότι υπάρχει στοιχείο του F^* τάξης $q - 1$. Πρώτα αποδεικνύουμε ότι έαν υπάρχει στοιχείο $\alpha \in F$ του οποίου η τάξη r είναι η μέγιστη δυνατή, τότε η τάξη s ενός τυχαίου στοιχείου $\beta \in F$ διαιρεί το r.

Από το Γεγονός 2.31, και την υπόθεση για το r, ισχύει ότι $\gcd(r, s) \neq 1$. Συνεπώς, είναι δυνατό να γράψουμε $r = p_1^d a$ και $s = p_1^e b$, όπου οι ακέραιοι a και b δε διαιρούνται από το p_1. Σύμφωνα με το Γεγονός 2.31, έχουμε $\mathrm{ord}(\alpha^{p_1^d}) = a$, $\mathrm{ord}(\beta^b) = p_1^e$, και $\mathrm{ord}(\alpha^{p_1^d}\beta^b) = p_1^e a$. Ως αποτέλεσμα, $e \leq d$ διαφορετικά η τάξη του r δεν θα ήταν μέγιστη. Τελικά συμπεραίνουμε ότι κάθε πρώτη δύναμη η οποία είναι διαιρέτης του s είναι επίσης διαιρέτης του r, και συνεπώς $s|r$.

Στη συνέχεια, αποδεικνύουμε ότι $r = q - 1$. Είναι προφανές ότι $r \leq q - 1$. Ας ορίσουμε το πολυώνυμο

$$g(z) = \sum_{\beta \in F^*} (z - \beta)$$

το οποίο έχει βαθμό $q - 1$. Επειδή $s|r$, κάθε στοιχείο $\beta \in F^*$ ικανοποιεί την εξίσωση $z^r - 1 = 0$. Συνεπώς, το πολυώνυμο $z^r - 1$ διαιρείται από το $g(z)$, απ΄ όπου καταλήγουμε στη σχέση $q - 1 = \deg(g) \leq \deg(z^r - 1) = r$. Από την $r \leq q - 1$, λαμβάνουμε $r = q - 1$, και τελικά ισχύει $F^* =< \alpha >$. □

Ορισμός 2.33. Ο γεννήτορας της κυκλικής ομάδας $\mathbb{F}_{p^n}^*$ ονομάζεται *πρωταρχικό στοιχείο* του $\mathbb{F}_{p^n}$. Το πολυώνυμο με ρίζες πρωταρχικά στοιχεία ονομάζεται *πρωταρχικό πολυώνυμο* [50].

Είναι σημαντικό να παρατηρήσουμε ότι δεν είναι όλα τα ανάγωγα πολυώνυμα πρωταρχικά, π.χ. το $1+z+z^3+z^4$ είναι ανάγωγο, και δύναται να χρησιμοποιηθεί για την κατασκευή του πεπερασμένου σώματος $\mathbb{F}_{2^4}$, αλλά δεν είναι πρωταρχικό πολυώνυμο. Σύμφωνα με τον Ορισμό 2.33, έαν F είναι σώμα τάξης p^n, τότε το στοιχείο $\alpha \in F$ είναι πρωταρχικό έαν η τάξη του είναι $p^n - 1$. Στο Παράρτημα Α δίνονται πρωταρχικά πολυώνυμα των πεπερασμένων σωμάτων $\mathbb{F}_{2^n}$, όπου $2 \leq n \leq 31$ [72].

Πόρισμα 2.34. *Κάθε πεπερασμένο σώμα περιέχει πρωταρχικά στοιχεία.*

Απόδειξη. Κάθε γεννήτορας της κυκλικής ομάδας F^* είναι πρωταρχικό στοιχείο. □

Το ακόλουθο πόρισμα είναι άμεση συνέπεια του Θεωρήματος 2.32.

Πόρισμα 2.35 (Θεώρημα του Fermat). *Κάθε στοιχείο α του πεπερασμένου σώματος F τάξης p^n ικανοποιεί την ταυτότητα $\alpha^{p^n} = \alpha$, ή ισοδύναμα, είναι ρίζα της εξίσωσης $z^{p^n} = z$. Συνεπώς, ισχύει*

$$z^{p^n} - z = \sum_{\alpha \in F} (z - \alpha).$$

Λήμμα 2.36. *Σε κάθε σώμα χαρακτηριστικής p, ισχύει $(a+b)^p = a^p + b^p$.*

Απόδειξη. Αναπτύσσοντας το διώνυμο $(a+b)^p$ λαμβάνουμε

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p.$$

αφού $\binom{p}{0} = \binom{p}{p} = 1$. Έαν $0 < k < p$, τότε $\gcd(k!, p) = 1$. Συνεπώς

$$\binom{p}{k} = p \frac{(p-1)\cdots(p-k+1)}{k!} \equiv 0 \pmod{p}.$$ □

Πόρισμα 2.37. *Σε κάθε σώμα χαρακτηριστικής p ισχύει $(a+b)^{p^m} = a^{p^m} + b^{p^m}$, για κάθε $m \geq 1$.*

Απόδειξη. Εφαρμόζεται επαγωγικά το Λήμμα 2.36. □

Πίνακας 2.1. Αναπαραστάσεις του πεπερασμένου σώματος $\mathbb{F}_{2^3}$ όπως ορίζεται από το πολυώνυμο $f(z) = 1 + z + z^3$

πολυωνυμική βάση			κανονική βάση			εκθετική
α^0	α^1	α^2	α^3	α^6	α^5	α^i
0	0	0	0	0	0	∞
1	0	0	1	1	1	0
0	1	0	0	1	1	1
0	0	1	1	0	1	2
1	1	0	1	0	0	3
0	1	1	1	1	0	4
1	1	1	0	0	1	5
1	0	1	0	1	0	6

2.2.3 Αναπαράσταση στοιχείων

Σύμφωνα με το Θεώρημα 2.30, το πεπερασμένο σώμα $\mathbb{F}_{p^n}$ είναι n–διάστατος διανυσματικός χώρος στο $\mathbb{F}_p$. Κάθε σύνολο n γραμμικώς ανεξάρτητων στοιχείων δύνανται να χρησιμοποιηθούν ως βάση του διανυσματικού χώρου. Διακρίνουμε δύο ιδιαίτερα σημαντικές βάσεις του $\mathbb{F}_{p^n}$. Η πρώτη είναι η *πολυωνυμική βάση*

$$\left\{1, \alpha, \ldots, \alpha^{n-1}\right\} \tag{2.3}$$

που χρησιμοποιείται για την κατασκευή του $\mathbb{F}_{p^n}$ από ένα ανάγωγο πολυώνυμο $f(z)$ στο $\mathbb{F}_p$ βαθμού n με $f(\alpha) = 0$. Η δεύτερη είναι η *κανονική βάση*

$$\left\{\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}\right\} \tag{2.4}$$

στην περίπτωση που τα ανωτέρω στοιχεία είναι γραμμικά ανεξάρτητα στο $\mathbb{F}_p$. Είναι γνωστό στη βιβλιογραφία ότι σε κάθε πεπερασμένο σώμα $\mathbb{F}_{p^n}$ υπάρχει τουλάχιστον μία κανονική βάση [72]. Αναγκαία, αλλά όχι ικανή, συνθήκη ώστε τα στοιχεία της (2.4) να είναι γραμμικώς ανεξάρτητα στο $\mathbb{F}_p$ είναι η [72]

$$\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}} \neq 0.$$

Σύμφωνα με το Θεώρημα 2.32, η πολλαπλασιαστική ομάδα $\mathbb{F}^*_{p^n}$ είναι κυκλική. Έστω $\alpha \in \mathbb{F}_{p^n}$ πρωταρχικό στοιχείο του $\mathbb{F}_{p^n}$, και έστω $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ βάση του $\mathbb{F}_{p^n}$ στο $\mathbb{F}_p$. Τότε, μπορούμε να γράψουμε το σώμα $\mathbb{F}_{p^n}$, σύμφωνα με τη διανυσματική και την εκθετική αναπαράσταση αντίστοιχα ($\beta\lambda$. Πίνακα 2.1), ως

εξής

$$\begin{aligned}\mathbb{F}_{p^n} &= \left\{a_0\alpha_0 + \cdots + a_{n-1}\alpha_{n-1} :\ a_i \in \mathbb{F}_p\right\} \\ &= \left\{\alpha^i :\ 0 \le i \le p^n - 2 \text{ ή } i = \infty\right\}\end{aligned}$$

όπου χρησιμοποιούμε το συμβολισμό $0 = \alpha^\infty$.

2.3 Κατασκευές του $\mathbb{F}_{p^n}$

Στην παρούσα ενότητα, παραθέτουμε τον τρόπο κατασκευής του πεπερασμένου σώματος $\mathbb{F}_{p^n}$. Σύμφωνα με την ανάλυση που προηγήθηκε στην ενότητα 2.1, το $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ είναι πεπερασμένο σώμα τάξης p, όπου p πρώτος αριθμός, και οι πράξεις της πρόσθεσης $+$ και του πολλαπλασιασμού $\cdot$ πραγματοποιούνται modulo p.

Ας θεωρήσουμε το θετικό ακέραιο n. Για να κατασκευάσουμε το πεπερασμένο σώμα $\mathbb{F}_{p^n}$, τάξης p^n, επιλέγουμε ένα πολυώνυμο $f(z) \in \mathbb{F}_p[z]$ βαθμού n το οποίο είναι ανάγωγο στο $\mathbb{F}_p$. Επιπλέον, υποθέτουμε ότι α είναι στοιχείο τέτοιο ώστε $f(\alpha) = 0$. Τότε, ορίζουμε

$$\mathbb{F}_{p^n} = \left\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} :\ a_i \in \mathbb{F}_p\right\}.$$

Στη συνέχεια, ορίζονται οι πράξεις της πρόσθεσης $+$ και του πολλαπλασιασμού $\cdot$ αντίστοιχα στο $\mathbb{F}_{p^n}$. Έαν τα στοιχεία $g(\alpha), h(\alpha) \in \mathbb{F}_{p^n}$ δίνονται από τις σχέσεις

$$g(\alpha) = \sum_{i=0}^{n-1} a_i\alpha^i \quad \text{και} \quad h(\alpha) = \sum_{j=0}^{n-1} b_j\alpha^j$$

τότε ορίζουμε

$$\begin{aligned}g(\alpha) + h(\alpha) &= \sum_{i=0}^{n-1}(a_i + b_i)\alpha^i \in \mathbb{F}_{p^n}, \\ g(\alpha) \cdot h(\alpha) &= r(\alpha) \in \mathbb{F}_{p^n}.\end{aligned}$$

Το στοιχείο $r(\alpha)$ υπολογίζεται βάσει των ακολούθων βημάτων:

α΄. Πολλαπλασιασμός των στοιχείων $g(\alpha)$ και $h(\alpha)$ σύμφωνα με τον τρόπο πολλαπλασιασμού πολυωνύμων, δηλ.

$$g(\alpha) \cdot h(\alpha) = \left(\sum_{i=0}^{n-1} a_i\alpha^i\right) \cdot \left(\sum_{j=0}^{n-1} b_j\alpha^j\right) = \sum_{k=0}^{2n} c_k\alpha^k = c(\alpha)$$

όπου $c_k = \sum_{i+j=k} a_i b_j$.

β΄. Διαίρεση του $c(\alpha)$ με το $f(\alpha)$, απ΄ όπου λαμβάνουμε τα δύο στοιχεία $q(\alpha)$ και $r(\alpha)$ τέτοια ώστε

$$c(\alpha) = q(\alpha)f(\alpha) + r(\alpha), \quad \text{με } \deg(r) < n.$$

Επειδή $f(\alpha) = 0$, έχουμε $c(\alpha) = r(\alpha) \in \mathbb{F}_{p^n}$.

Θεώρημα 2.38. *Το σύνολο $\mathbb{F}_{p^n}$ με τις πράξεις της πρόσθεσης $+$ και πολλαπλασιασμού $\cdot$, όπως ορίστηκαν παραπάνω, αποτελεί πεπερασμένο σώμα τάξης p^n.*

Απόδειξη. Είναι εύκολο να δείξουμε ότι τα κριτήρια του Ορισμού 2.11 ικανοποιούνται, και ότι η αλγεβρική δομή $(\mathbb{F}_{p^n}, +, \cdot)$ αποτελεί δακτύλιο. Η μοναδική ιδιότητα που πρέπει να αποδείξουμε είναι ότι για κάθε στοιχείο $g \in \mathbb{F}_{p^n}^*$, υπάρχει $g^{-1} \in \mathbb{F}_{p^n}^*$ τέτοιο ώστε $gg^{-1} = 1$.

Επειδή το πολυώνυμο $f(z)$, βαθμού n, είναι ανάγωγο στο $\mathbb{F}_p$, και $\deg(g) < n$, το $g(z)$ είναι σχετικά πρώτο με το $f(z)$. Σύμφωνα με το Θεώρημα 2.24, υπάρχουν πολυώνυμα $u(z), v(z) \in \mathbb{F}_p[z]$ τέτοια ώστε

$$g(z)u(z) + f(z)v(z) = 1.$$

Θέτοντας όπου $z = \alpha$, λαμβάνουμε

$$g(\alpha)u(\alpha) + f(\alpha)v(\alpha) = 1 \Leftrightarrow g(\alpha)u(\alpha) = 1$$

αφού $f(\alpha) = 0$. Έαν $\deg(u) \geq n$, τότε εφαρμόζοντας τον αλγόριθμο της διαίρεσης στα πολυώνυμα $u(z)$ και $f(z)$ λαμβάνουμε

$$u(z) = q_1(z)f(z) + r_1(z), \quad \text{με } \deg(r_1) < n.$$

Για $z = \alpha$, έχουμε $u(\alpha) = r_1(\alpha) \in \mathbb{F}_{p^n}$. Συνεπώς, μπορούμε να υποθέσουμε ότι ισχύει $\deg(u) < n$. Τελικά, συμπεραίνουμε ότι $g^{-1} = u(\alpha) \in \mathbb{F}_{p^n}$. □

Τα $f(z)$ και α ονομάζονται *ορίζον πολυώνυμο* και *ορίζον στοιχείο* αντίστοιχα του $\mathbb{F}_{p^n}$ στο $\mathbb{F}_p$. Από τον τρόπο κατασκευής του πεπερασμένου σώματος $\mathbb{F}_{p^n}$ έχουμε ότι $f(\alpha) = 0$, δηλ. το στοιχείο α είναι ρίζα του $f(z)$ στο $\mathbb{F}_{p^n}$. Συχνά λέμε ότι το $\mathbb{F}_{p^n}$ παράγεται από το $\mathbb{F}_p$ προσαρτώντας στο $\mathbb{F}_p$ μία ρίζα του πολυωνύμου $f(z)$, ή ότι το $\mathbb{F}_{p^n}$ είναι *πεπερασμένη επέκταση* του $\mathbb{F}_p$ [50].

Πίνακας 2.2. Τα στοιχεία του σώματος $\mathbb{F}_{2^3}$, που ορίζεται από το πολυώνυμο $f(z) = 1 + z + z^3$ και $f(\alpha) = 0$

ως διάνυσμα	ως πολυώνυμο	ως δυνάμεις
000	0	0
100	1	1
010	α	α
001	α^2	α^2
110	$1+\alpha$	α^3
011	$\alpha+\alpha^2$	α^4
111	$1+\alpha+\alpha^2$	α^5
101	$1+\alpha^2$	α^6

Παράδειγμα 2.39. Ας θεωρήσουμε τον ακέραιο $p = 2$ και το πολυώνυμο $f(z) = 1+z+z^3$, το οποίο είναι ανάγωγο στο $\mathbb{F}_2$. Επιπλέον, υποθέτουμε ότι το στοιχείο α είναι ρίζα του πολυωνύμου $f(z)$, και θεωρούμε το πεπερασμένο σώμα $\mathbb{F}_{2^3}$ που ορίζεται από τη σχέση

$$\mathbb{F}_{2^3} = \left\{ a_0 + a_1\alpha + a_2\alpha^2 : \ a_i \in \mathbb{F}_2 \right\}.$$

Από τον Πίνακα 2.2 παρατηρούμε ότι $\mathbb{F}_{2^3}^* =< \alpha >$, δηλ. τα μη–μηδενικά στοιχεία του $\mathbb{F}_{2^3}$ αποτελούν κυκλική ομάδα τάξης 7 με γεννήτορα το στοιχείο α, όπου $\alpha^7 = 1$. □

Παράδειγμα 2.40. Ας θεωρήσουμε τον ακέραιο $p = 2$ και το πολυώνυμο $f(z) = 1+z+z^4$, το οποίο είναι ανάγωγο στο $\mathbb{F}_2$. Επιπλέον, υποθέτουμε ότι το στοιχείο α είναι ρίζα του πολυωνύμου $f(z)$, και θεωρούμε το πεπερασμένο σώμα $\mathbb{F}_{2^4}$ που ορίζεται από τη σχέση

$$\mathbb{F}_{2^4} = \left\{ a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 : \ a_i \in \mathbb{F}_2 \right\}.$$

Από τον Πίνακα 2.3 παρατηρούμε ότι $\mathbb{F}_{2^4}^* =< \alpha >$, δηλ. τα μη–μηδενικά στοιχεία του $\mathbb{F}_{2^4}$ αποτελούν κυκλική ομάδα τάξης 15 με γεννήτορα το στοιχείο α, όπου $\alpha^{15} = 1$. Έστω ότι τα στοιχεία $1+\alpha$ και $\alpha+\alpha^3$ χρειάζεται να προστεθούν

$$(1+\alpha) + (\alpha+\alpha^3) = 1+\alpha^3$$

και να πολλαπλασιαστούν

$$(1+\alpha)\cdot(\alpha+\alpha^3) = \alpha^4\alpha^9 = \alpha^{4+9} = \alpha^{13} = 1+\alpha^2+\alpha^3$$

Πίνακας 2.3. Τα στοιχεία του σώματος $\mathbb{F}_{2^4}$, που ορίζεται από το πολυώνυμο $f(z) = 1 + z + z^4$ και $f(\alpha) = 0$

ως διάνυσμα	ως πολυώνυμο	ως δυνάμεις
0000	0	0
1000	1	1
0100	α	α
0010	α^2	α^2
0001	α^3	α^3
1100	$1 + \alpha$	α^4
0110	$\alpha + \alpha^2$	α^5
0011	$\alpha^2 + \alpha^3$	α^6
1101	$1 + \alpha + \alpha^3$	α^7
1010	$1 + \alpha^2$	α^8
0101	$\alpha + \alpha^3$	α^9
1110	$1 + \alpha + \alpha^2$	α^{10}
0111	$\alpha + \alpha^2 + \alpha^3$	α^{11}
1111	$1 + \alpha + \alpha^2 + \alpha^3$	α^{12}
1011	$1 + \alpha^2 + \alpha^3$	α^{13}
1001	$1 + \alpha^3$	α^{14}

όπου παρατηρήσαμε ότι $1 + \alpha = \alpha^4$ και $\alpha + \alpha^3 = \alpha^9$. Συνεπώς, η πολυωνυμική αναπαράσταση βολεύει για την πρόσθεση, ενώ η εκθετική αναπαράσταση για τον πολλαπλασιασμό. □

2.4 Ελάχιστα πολυώνυμα

Από το θεώρημα του Fermat ($\beta\lambda$. Πόρισμα 2.35) συμπεραίνουμε ότι κάθε στοιχείο $\alpha \in \mathbb{F}_q$, όπου $q = p^n$, ικανοποιεί την εξίσωση [93], [94]

$$z^q - z = 0. \tag{2.5}$$

Το ανωτέρω πολυώνυμο έχει όλους τους συντελεστές στο πρωταρχικό σώμα $\mathbb{F}_p$, και είναι μονικό. Όμως, είναι πιθανό το α να ικανοποιεί μία εξίσωση μικροτέρου βαθμού από τον αντίστοιχο της (2.5).

Ορισμός 2.41. Το *ελάχιστο πολυώνυμο* στο $\mathbb{F}_p$ του στοιχείου α είναι το ελαχίστου βαθμού μονικό πολυώνυμο $m(z) \in \mathbb{F}_p[z]$ τέτοιο ώστε $m(\alpha) = 0$.

Παράδειγμα 2.42. Έαν θεωρήσουμε ότι το στοιχείο $\alpha \in \mathbb{F}_{2^4}$ ικανοποιεί τη σχέση $\alpha^4 + \alpha + 1 = 0$, όπου τα ελάχιστα πολυώνυμα έχουν συντελεστές ίσους με

Πίνακας 2.4. Ελάχιστα πολυώνυμα του πεπερασμένου σώματος $\mathbb{F}_{2^4}$

στοιχείο	ελάχιστο πολυώνυμο
0	z
1	$1+z$
α	$1+z+z^4$
α^3	$1+z+z^2+z^3+z^4$
α^5	$1+z+z^2$
α^7	$1+z^3+z^4$

0 ή 1, τότε ισχύει $\alpha^7 = \alpha^{-1}$. Τα ελάχιστα πολυώνυμα του $\mathbb{F}_{2^4}$ που αντιστοιχούν σε στοιχεία του πεπερασμένου σώματος φαίνονται στον Πίνακα 2.4. □

Στη συνέχεια της παρούσας ενότητας παρατίθενται ιδιότητες των ελαχίστων πολυωνύμων, συζυγών ριζών, κυκλοτομικών κλάσεων, ενώ δίνεται στο τέλος αλγόριθμος εύρεσης ελαχίστων πολυωνύμων. Ας υποθέσουμε ότι $m(z)$ είναι το ελάχιστο πολυώνυμο του στοιχείου $\alpha \in \mathbb{F}_{p^n}$.

Ιδιότητα 2.43. Το πολυώνυμο $m(z)$ είναι ανάγωγο.

Απόδειξη. Έστω ότι το πολυώνυμο $m(z)$ δεν είναι ανάγωγο. Τότε, υπάρχουν μη–μηδενικά πολυώνυμα $g(z), h(z) \in \mathbb{F}_p[z]$ τέτοια ώστε $m(z) = g(z)h(z)$. Από τη σχέση $m(\alpha) = g(\alpha)h(\alpha) = 0$ συμπεραίνουμε ότι $g(\alpha) = 0$ ή $h(\alpha) = 0$, το οποίο έρχεται σε αντίθεση με το ελάχιστο της επιλογής του πολυωνύμου $m(z)$ με ρίζα το στοιχείο α. □

Ιδιότητα 2.44. Για κάθε πολυώνυμο $f(z) \in \mathbb{F}_p[z]$, έαν $f(\alpha) = 0$ τότε $m(z)|f(z)$.

Απόδειξη. Εφαρμόζουμε τον αλγόριθμο διαίρεσης του Θεωρήματος 2.22 για να διαιρέσουμε το πολυώνυμο $f(z)$ με το $m(z)$. Τότε, υπάρχουν πολυώνυμα $q(z)$, $r(z) \in \mathbb{F}_p[z]$ τέτοια ώστε

$$f(z) = q(z)m(z) + r(z), \qquad \text{με } \deg(r) < \deg(m).$$

Έαν θέσουμε $z = \alpha$, λαμβάνουμε $0 = 0 + r(\alpha)$, και συνεπώς το πολυώνυμο $r(z)$ έχει ρίζα το στοιχείο α και βαθμό μικρότερο από το βαθμό του $m(z)$. Αυτό έρχεται σε αντίθεση με το ελάχιστο της επιλογής του πολυωνύμου $m(z)$, εκτός έαν $r(z) = 0$. □

Ιδιότητα 2.45. Το ελάχιστο πολυώνυμο $m(z)$ διαιρεί το $z^{p^n} - z$.

Απόδειξη. Από το Πόρισμα 2.35, συμπεραίνουμε ότι το στοιχείο $\alpha \in \mathbb{F}_{p^n}$ ικανοποιεί τη σχέση $\alpha^{p^n} - \alpha = 0$. Εφαρμόζοντας την Ιδιότητα 2.44, λαμβάνουμε ότι $m(z)|z^{p^n} - z$. □

Ιδιότητα 2.46. Ο βαθμός του ελαχίστου πολυωνύμου $m(z)$ είναι μικρότερος ή ίσος με n.

Απόδειξη. Επειδή το πεπερασμένο σώμα $\mathbb{F}_{p^n}$ είναι n–διάστατος διανυσματικός χώρος στο $\mathbb{F}_p$, κάθε $n+1$ στοιχεία, π.χ. τα $\{1, \alpha, \ldots, \alpha^n\}$, είναι γραμμικώς εξαρτημένα. Συνεπώς, υπάρχουν συντελεστές $a_i \in \mathbb{F}_p$, όχι όλοι μηδέν, τέτοιοι ώστε

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Άρα το πολυώνυμο $a_0 + a_1 z + \cdots + a_n z^n \in \mathbb{F}_p[z]$, βαθμού μικρότερου ή ίσου με n έχει ρίζα το στοιχείο α, απ΄ όπου προκύπτει ότι $\deg(m) \leq n$. □

Ιδιότητα 2.47. Το ελάχιστο πολυώνυμο ενός πρωταρχικού στοιχείου του σώματος $\mathbb{F}_{p^n}$ έχει βαθμό n.

Απόδειξη. Έστω α πρωταρχικό στοιχείο του σώματος $\mathbb{F}_{p^n}$ με ελάχιστο πολυώνυμο $m(z)$ βαθμού d. Το πολυώνυμο $m(z)$ δύναται να χρησιμοποιηθεί για την κατασκευή ενός σώματος F τάξης p^d ($\beta\lambda$. Θεώρημα 2.38). Το σώμα F περιέχει το στοιχείο α και συνεπώς όλο το $\mathbb{F}_{p^n}$. Άρα ισχύει $d \geq n$, και από την Ιδιότητα 2.46 λαμβάνουμε $d = n$. □

Ιδιότητα 2.48. Τα στοιχεία $\alpha, \alpha^p \in \mathbb{F}_{p^n}$ έχουν το ίδιο ελάχιστο πολυώνυμο.

Απόδειξη. Ας υποθέσουμε ότι $m_\alpha(z) = \sum a_i z^i$ και $m_{\alpha^p}(z) = \sum b_i z^i$ είναι τα ελάχιστα πολυώνυμα των στοιχείων α και α^p αντίστοιχα στο $\mathbb{F}_p$. Από την ταυτότητα $a_i = a_i^p$, και το Λήμμα 2.36, έχουμε

$$m_\alpha(\alpha^p) = \sum a_i(\alpha^p)^i = \sum a_i^p(\alpha^i)^p = \Big(\sum a_i\alpha^i\Big)^p = m_\alpha(\alpha)^p = 0.$$

Σύμφωνα με την Ιδιότητα 2.44, το ελάχιστο πολυώνυμο $m_{\alpha^p}(z)$ διαιρεί το $m_\alpha(z)$. Από την Ιδιότητα 2.43, το πολυώνυμο $m_\alpha(z)$ είναι ανάγωγο, και συνεπώς ισχύει $m_\alpha(z) = m_{\alpha^p}(z)$. □

Ορισμός 2.49. Έστω $\alpha \in \mathbb{F}_{p^n}$. Τότε, τα στοιχεία $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ ονομάζονται *συζυγή στοιχεία* του α στο $\mathbb{F}_p$.

είσοδος: ένα πρωταρχικό πολυώνυμο $f(x)$ στο $\mathbb{F}_p$ βαθμού n

βήμα 1: κατασκευή του πεπερασμένου σώματος $\mathbb{F}_{p^n}$ βάσει της εξίσωσης $f(\alpha) = 0$

βήμα 2: υπολογισμός των κυκλοτομικών κλάσεων $C_1, \ldots, C_r \bmod p^n - 1$, και του συνόλου I των επικεφαλείς κλάσεων $\bmod p^n - 1$

βήμα 3: $\forall\, s \in I$, υπολογισμός του πολυωνύμου $m_s(x) = \prod_{i \in C_s} (x - \alpha^i)$

έξοδος: όλα τα ανάγωγα πολυώνυμα στο $\mathbb{F}_p$, των οποίων ο βαθμός διαιρεί το n

Σχήμα 2.1. Αλγόριθμος εύρεσης ελαχίστων πολυωνύμων

Από την Ιδιότητα 2.48, συμπεραίνουμε ότι όλα τα συζυγή στοιχεία του α έχουν το ίδιο ελάχιστο πολυώνυμο. Ο πολλαπλασιασμός των εκθετών του α με p διαιρεί τους ακέραιους $\bmod p^n - 1$ σε σύνολα που ονομάζονται *κυκλοτομικές κλάσεις* $\bmod p^n - 1$. Γενικά, η κυκλοτομική κλάση του s, συμβολίζεται με C_s, και περιέχει τους ακεραίους [33]

$$C_s = \{s, sp, \ldots, sp^{n_s - 1}\}$$

όπου n_s είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $sp^{n_s} \equiv s \pmod{p^n - 1}$.

Παράδειγμα 2.50. Έστω $p = 2$ και $n = 4$. Οι κυκλοτομικές κλάσεις $\bmod 15$ είναι οι

$$C_1 = \{1, 2, 4, 8\} \qquad C_5 = \{5, 10\}$$
$$C_3 = \{3, 6, 12, 9\} \qquad C_7 = \{7, 14, 13, 11\}$$

όπου πάντα έχουμε και την κυκλοτομική κλάση $C_0 = \{0\}$. □

Συνήθως συμβολίζουμε με s τον ελάχιστο ακέραιο της κυκλοτομικής κλάσης C_s, ο οποίος ονομάζεται *επικεφαλής κλάσης* $\bmod p^n - 1$, και με I το σύνολο των επικεφαλείς κλάσεων $\bmod p^n - 1$. Έαν περιοριστούμε σε πεπερασμένα σώματα

$\mathbb{F}_{2^n}$, τότε το πλήθος των κυκλοτομικών κλάσεων του $\mathbb{F}_{2^n}$ δίνεται από τη σχέση [33]

$$|I| = \frac{1}{n}\sum_{d|n}\varphi(n/d)2^d - 1 \tag{2.6}$$

όπου $\varphi()$ είναι η συνάρτηση του Euler.

Έαν ο ακέραιος i διατρέχει τα στοιχεία μιας κυκλοτομικής κλάσης, τότε όλα τα α^i έχουν το ίδιο ελάχιστο πολυώνυμο. Στο Σχ. 2.1 παρουσιάζουμε έναν αλγόριθμο εύρεσης ελαχίστων πολυωνύμων του $\mathbb{F}_{p^n}$. Το πολυώνυμο $m_s(z)$, που κατασκευάζεται από τον αλγόριθμο του Σχ. 2.1, είναι το ελάχιστο πολυώνυμο του α^s και των συζυγών του στοιχείων.

Σύμφωνα με το Γεγονός 2.31, έαν οι ακέραιοι s και p^n-1 είναι πρώτοι μεταξύ τους, τότε ισχύει

$$\mathrm{ord}(\alpha^s) = \mathrm{ord}(\alpha) = p^n - 1$$

και το α^s αποτελεί επίσης πρωταρχικό στοιχείο του $\mathbb{F}_{p^n}$. Συνεπώς το $m_s(z)$ είναι πρωταρχικό πολυώνυμο στο $\mathbb{F}_p$ βαθμού n. Το γινόμενο όλων των ανάγωγων πολυωνύμων στο $\mathbb{F}_p$, των οποίων ο βαθμός διαιρεί το n, είναι ίσο με [72]

$$z^{p^n} - z = z\prod_{s\in I} m_s(z).$$

Το πλήθος των ανάγωγων πολυωνύμων βαθμού n του πεπερασμένου σώματος $\mathbb{F}_{p^n}$ είναι [33]

$$\frac{1}{n}\sum_{d|n}\mu(n/d)p^d \tag{2.7}$$

όπου $\mu()$ είναι η συνάρτηση του Möbius. Επιπλέον, το πλήθος των πρωταρχικών πολυωνύμων βαθμού n είναι $\varphi(p^n-1)/n$ [50].

Παράδειγμα 2.51. Ας θεωρήσουμε το πεπερασμένο σώμα $\mathbb{F}_{2^4}$ το οποίο ορίζεται από τη σχέση $\alpha^4 + \alpha + 1 = 0$. Οι κυκλοτομικές κλάσεις και τα αντίστοιχα ελάχιστα πολυώνυμα του $\mathbb{F}_{2^4}$ παρατίθενται στον Πίνακα 2.5. Επιπλέον ισχύει

$$\begin{aligned} z^{2^4} + z &= z\, m_0(z)\, m_1(z)\, m_3(z)\, m_5(z)\, m_7(z) \\ &= z(1+z)(1+z+z^4)(1+z+z^2+z^3+z^4)(1+z+z^2) \\ &\quad \times (1+z^3+z^4) \end{aligned}$$

όπου οι επικεφαλείς κλάσεων του $\mathbb{F}_{2^4}$ είναι οι $I = \{0,1,3,5,7\}$. □

Πίνακας 2.5. Ελάχιστα πολυώνυμα και κυκλοτομικές κλάσεις του πεπερασμένου σώματος $\mathbb{F}_{2^4}$

κυκλοτομική κλάση	στοιχείο	ελάχιστο πολυώνυμο
$C_0 = \{0\}$	1	$m_0(z) = 1 + z$
$C_1 = \{1, 2, 4, 8\}$	$\alpha, \alpha^2, \alpha^4, \alpha^8$	$m_1(z) = 1 + z + z^4$
$C_3 = \{3, 6, 12, 9\}$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$m_3(z) = 1 + z + z^2 + z^3 + z^4$
$C_5 = \{5, 10\}$	α^5, α^{10}	$m_5(z) = 1 + z + z^2$
$C_7 = \{7, 14, 13, 11\}$	$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$m_7(z) = 1 + z^3 + z^4$

Από τον Πίνακα 2.5 παρατηρούμε ότι για τα ελάχιστα πολυώνυμα $m_1(z)$ και $m_7(z)$ των στοιχείων α και $\alpha^{14} = \alpha^{-1}$ αντίστοιχα, ισχύει η σχέση

$$m_7(z) = z^4 m_1(1/z).$$

Τα $m_1(z)$ και $m_7(z)$ ονομάζονται *ανάστροφα πολυώνυμα*. Τα ανάστροφα πολυώνυμα χρησιμοποιούνται ιδιαίτερα συχνά στην ανάλυση ακολουθιών λόγω της συγκεκριμένης ιδιότητας που τα διέπει. Γενικά, το ανάστροφο πολυώνυμο του

$$f(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} + a_n z^n \in \mathbb{F}_p[z] \tag{2.8}$$

είναι το

$$f^*(z) = a_n + a_{n-1} z + \cdots + a_1 z^{n-1} + a_0 z^n \in \mathbb{F}_p[z] \tag{2.9}$$

το οποίο λαμβάνεται αντιστρέφοντας τη διάταξη των συντελεστών. Επιπρόσθετα, οι ρίζες του πολυωνύμου $f^*(z)$ είναι οι αντίστροφες των ριζών του $f(z)$, στην επέκταση $\mathbb{F}_{p^n}$ του $\mathbb{F}_p$. Είναι προφανές ότι έαν το πολυώνυμο $f(z)$ είναι πρωταρχικό, τότε και το $f^*(z)$ είναι πρωταρχικό, και αντιστρόφως [56].

2.5 Υποσώματα

Στην παρούσα ενότητα αναλύουμε τις σχέσεις που διέπουν τα σώματα και τα υποσώματα αυτών. Η γνώση των σχέσεων αυτών είναι απαραίτητη σε πολλά προβλήματα της θεωρίας πεπερασμένων σωμάτων, καθώς και στο σχεδιασμό και χαρακτηρισμό ακολουθιών που παράγονται από καταχωρητές ολίσθησης γραμμικής ανάδρασης [33].

Γεγονός 2.52. Έστω F επέκταση του σώματος $\mathbb{F}_p$, το οποίο περιέχει όλες τις ρίζες του πολυωνύμου $z^{p^n} - z$. Τότε, το σύνολο αυτό των ριζών αποτελεί πεπερασμένο σώμα τάξης p^n.

Προκειμένου να αποδείξουμε το βασικό θεώρημα της παρούσας ενότητας, θα χρειαστεί πρώτα να δείξουμε το ακόλουθο Λήμμα [64], [65].

Λήμμα 2.53. *Έστω n_1, n_2, και a ακέραιοι τέτοιοι ώστε $n_1, n_2 \geq 1$ και $a \geq 2$. Τότε*

$$\gcd(a^{n_1} - 1, a^{n_2} - 1) = a^{\gcd(n_1, n_2)} - 1. \tag{2.10}$$

Απόδειξη. Δίχως βλάβη της γενικότητας υποθέτουμε ότι $n_2 \leq n_1$. Εαν ο ακέραιος n_2 διαιρεί τον n_1, τότε υπάρχει ακέραιος q τέτοιος ώστε $n_1 = qn_2$. Αντίστοιχα ο ακέραιος $a^{n_2} - 1$ θα διαιρεί τον $a^{n_1} - 1$ αφού

$$a^{n_1} - 1 = \left(a^{n_2(q-1)} + \cdots + a^{n_2} + 1\right)(a^{n_2} - 1)$$

και συνεπώς η (2.10) ισχύει. Έστω ότι ο ακέραιος n_2 δεν διαιρεί τον n_1. Τότε, από τον αλγόριθμο του Ευκλείδη λαμβάνουμε ότι ισχύει $n_1 = q_1 n_2 + n_3$, με $0 < n_3 < n_2$. Συνεπώς

$$\begin{aligned} a^{n_1} - 1 &= a^{q_1 n_2 + n_3} - 1 = a^{n_3}(a^{q_1 n_2} - 1) + (a^{n_3} - 1) \\ &= Q_1(a^{n_2} - 1) + (a^{n_3} - 1) \end{aligned}$$

όπου

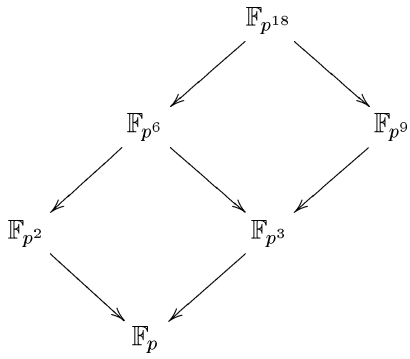
$$Q_1 = a^{n_3}\left(a^{n_2(q_1 - 1)} + \cdots + a^{n_2} + 1\right)$$

και $0 < a^{n_3} - 1 < a^{n_2} - 1$. Παρατηρούμε ότι το υπόλοιπο της διαίρεσης του ακεραίου $a^{n_1} - 1$ με τον $a^{n_2} - 1$ εκφράζεται συναρτήσει του υπολοίπου n_3 της διαίρεσης του ακεραίου n_1 με τον n_2.

Εφαρμόζοντας κατ΄ επανάληψη τον αλγόριθμο του Ευκλείδη, η ανωτέρω διαδικασία θα τερματίσει μετά από έναν πεπερασμένο αριθμό βημάτων δίνοντας $n_{s-1} = q_{s-1} n_s + n_{s+1}$, με $n_{s+1} = 0$, για έναν συγκεκριμένο ακέραιο s, και επιπλέον

$$a^{n_{s-1}} - 1 = Q_{s-1}(a^{n_s} - 1) + (a^{n_{s+1}} - 1)$$

με $a^{n_{s+1}} - 1 = 0$. Τότε, είναι φανερό ότι ο ακέραιος $a^{n_s} - 1$ είναι ο μέγιστος κοινός διαιρέτης των $a^{n_1} - 1$ και $a^{n_2} - 1$, ενώ αντίστοιχα ο ακέραιος n_s είναι ο μέγιστος κοινός διαιρέτης των n_1 και n_2. □



Σχήμα 2.2. Τα υποσώματα του $\mathbb{F}_{p^{18}}$ και οι μεταξύ τους σχέσεις

Πόρισμα 2.54. *Οι ακέραιοι $N_1 = 2^{n_1} - 1$ και $N_2 = 2^{n_2} - 1$ είναι πρώτοι μεταξύ τους εάν και μόνον εάν οι ακέραιοι n_1 και n_2 είναι πρώτοι μεταξύ τους.*

Θεώρημα 2.55. *Έστω $F = \mathbb{F}_{p^n}$ και $K = \mathbb{F}_{p^m}$ είναι πεπερασμένα σώματα με p^n και p^m στοιχεία αντίστοιχα, όπου p πρώτος αριθμός. Τότε [72]*

i. Το F περιέχει το K ως υπόσωμα εάν και μόνον εάν $m|n$.

ii. Εαν $\alpha \in F$, τότε το $\alpha \in K$ εάν και μόνον εάν $\alpha^{p^m} = \alpha$.

Απόδειξη. Για την απόδειξη της πρώτης ιδιότητας, ας υποθέσουμε ότι $m|n$. Τότε, από το Γεγονός 2.52 συμπεραίνουμε ότι το F περιέχει το K ως υπόσωμα. Αντιστρόφως, έστω ότι $\alpha \in K$ είναι πρωταρχικό στοιχείο του K. Τότε, ισχύει

$$\alpha^{p^m-1} = 1 \quad \text{και} \quad \alpha^{p^n-1} = 1.$$

Συνεπώς ο ακέραιος $p^m - 1$ διαιρεί τον $p^n - 1$, και από το Λήμμα 2.53 λαμβάνουμε ότι $m|n$. Η δεύτερη ιδιότητα είναι άμεση απόρροια του Πορίσματος 2.35. □

Παράδειγμα 2.56. Τα υποσώματα του $\mathbb{F}_{p^{18}}$ καθορίζονται από τους διαιρέτες του ακεραίου 18. Βάσει του Θεωρήματος 2.55, οι σχέσεις μεταξύ των διαφόρων υποσωμάτων επεξηγούνται στο Σχ. 2.2. □

Άμεση συνέπεια των Ιδιοτήτων 2.45, 2.46, και 2.47, του Λήμματος 2.53, και του Θεωρήματος 2.55 είναι το ακόλουθο Πόρισμα.

Πόρισμα 2.57. *Έστω $F = \mathbb{F}_{p^n}$. Επιπλέον, έστω $\alpha \in F$ με ελάχιστο πολυώνυμο $m_\alpha(z)$. Τότε*

i. Η τάξη r του α διαιρεί το $p^n - 1$.

ii. Το $m_\alpha(z)$ διαιρεί το $z^r - 1$, το οποίο είναι το διώνυμο ελαχίστου βαθμού με αυτή την ιδιότητα.

iii. Ο βαθμός του $m_\alpha(z)$ διαιρεί το n.

Είναι προφανές από το Πόρισμα 2.57 ότι έαν ο ακέραιος n είναι πρώτος αριθμός, τότε ο βαθμός του ελαχίστου πολυωνύμου οποιουδήποτε στοιχείου του $\mathbb{F}_{p^n}$ είναι ίσος με n. Επιπλέον, ο ακέραιος r ονομάζεται και *τάξη* του $m_\alpha(z)$.

2.6 Απεικονίσεις σε πεπερασμένα σώματα

Στην παρούσα ενότητα αναφέρουμε ιδιότητες πεπερασμένων σωμάτων που σχετίζονται με τον ορισμό απεικονίσεων, συναρτήσεων ίχνους και νόρμας, και συνοψίζονται οι ιδιότητες [72].

2.6.1 Συναρτήσεις ίχνους

Ορισμός 2.58. Έστω $F = \mathbb{F}_{q^n}$ και $K = \mathbb{F}_q$ είναι πεπερασμένα σώματα με q^n και q στοιχεία αντίστοιχα, όπου q είναι πρώτος ή δύναμη πρώτου αριθμού. Η *συνάρτηση ίχνους* $\mathrm{tr}_{F/K}(z)$, όπου $z \in F$, ορίζεται από τη σχέση

$$\mathrm{tr}_{F/K}(z) = z + z^q + \cdots + z^{q^{n-1}}.$$

Έαν $\alpha \in F$, τότε το $\mathrm{tr}_{F/K}(\alpha)$ ονομάζεται *ίχνος* του στοιχείου α στο K.

Από τον Ορισμό 2.58 της συνάρτησης ίχνους, έαν $q = p$ πρώτος, τότε απλά γράφουμε $\mathrm{tr}_F(\alpha)$ ή $\mathrm{tr}(\alpha)$. Επιπρόσθετα, έαν $q = 2$, τότε το $\mathrm{tr}_{F/K}(z) \triangleq \mathrm{tr}_1^n(z)$ είναι 0 ή 1 για κάθε $z \in \mathbb{F}_{2^n}$. Από την ισχύ της ταυτότητας

$$\mathrm{tr}_{F/K}(z)^q = \sum_{i=0}^{n-1} z^{q^{i+1}} = \mathrm{tr}_{F/K}(z)$$

από το Θεώρημα 2.55 συμπεραίνουμε ότι $\mathrm{tr}_{F/K}(z) \in K$. Συνεπώς, η συνάρτηση ίχνους είναι απεικόνιση από το σώμα F στο υπόσωμα K.

Θεώρημα 2.59. *Έστω $F = \mathbb{F}_{q^n}$ και $K = \mathbb{F}_q$ είναι πεπερασμένα σώματα με q^n και q στοιχεία αντίστοιχα. Η συνάρτηση ίχνους ικανοποιεί τις ακόλουθες ιδιότητες*

i. $\mathrm{tr}_{F/K}(\alpha + \beta) = \mathrm{tr}_{F/K}(\alpha) + \mathrm{tr}_{F/K}(\beta)$, *για κάθε* $\alpha, \beta \in F$.

ii. $\mathrm{tr}_{F/K}(c\,\alpha) = c\,\mathrm{tr}_{F/K}(\alpha)$, *για κάθε* $c \in K$ *και* $\alpha \in F$.

iii. $\mathrm{tr}_{F/K}$ *είναι γραμμικός μετασχηματισμός από το σώμα* F *επί το υπόσωμα* K, *όπου τα* F *και* K *λαμβάνονται ως διανυσματικοί χώροι στο* K.

iv. $\mathrm{tr}_{F/K}(c) = n\,c$, *για κάθε* $c \in K$.

v. $\mathrm{tr}_{F/K}(\alpha^q) = \mathrm{tr}_{F/K}(\alpha)$, *για κάθε* $\alpha \in F$.

Απόδειξη. (i) Για κάθε $\alpha, \beta \in F$ χρησιμοποιούμε το Πόρισμα 2.37 για να πάρουμε

$$\begin{aligned}\mathrm{tr}_{F/K}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{n-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{n-1}} + \beta^{q^{n-1}} \\ &= \mathrm{tr}_{F/K}(\alpha) + \mathrm{tr}_{F/K}(\beta).\end{aligned}$$

(ii) Για κάθε $c \in K$ και $j \geq 0$ ισχύει $c^{q^j} = c$ λόγω του Θεωρήματος 2.55(ii). Συνεπώς

$$\mathrm{tr}_{F/K}(c\,\alpha) = c\,\alpha + c^q\,\alpha^q + \cdots + c^{q^{n-1}}\,\alpha^{q^{n-1}} = c\,\mathrm{tr}_{F/K}(\alpha).$$

(iii) Οι Ιδιότητες (i) και (ii), μαζί με το γεγονός ότι $\mathrm{tr}_{F/K}(\alpha) \in K$ για κάθε $\alpha \in F$, δείχνουν ότι η απεικόνιση $\mathrm{tr}_{F/K}$ είναι γραμμικός μετασχηματισμός από το F στο K. Για να αποδείξουμε ότι η συγκεκριμένη απεικόνιση είναι και επί, αρκεί να δείξουμε την ύπαρξη στοιχείου $\alpha \in F$ τέτοιου ώστε $\mathrm{tr}_{F/K}(\alpha) \neq 0$. Όμως $\mathrm{tr}_{F/K}(\alpha) = 0$ έαν και μόνον έαν το στοιχείο α είναι ρίζα του πολυωνύμου

$$z + z^q + \cdots + z^{q^{n-1}} \in K[z] \tag{2.11}$$

στο F. Επειδή το πολυώνυμο της (2.11) έχει το πολύ q^{n-1} ρίζες στο F, ενώ το F έχει q^n στοιχεία, υπάρχει $\alpha \in F$ με $\mathrm{tr}_{F/K}(\alpha) \neq 0$.

(iv) Η συγκεκριμένη ιδιότητα είναι άμεση απόρροια του Ορισμού 2.58 και του Θεωρήματος 2.55(ii).

(v) Για κάθε $\alpha \in F$ έχουμε ότι $\alpha^{q^n} = \alpha$ από το Πόρισμα 2.35, και συνεπώς

$$\mathrm{tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^n} = \mathrm{tr}_{F/K}(\alpha). \qquad \square$$

Θεώρημα 2.60 (Ιδιότητα μεταβατικότητας). *Έστω το πεπερασμένο σώμα K, η πεπερασμένη επέκταση F του K, και η πεπερασμένη επέκταση E του F, δηλ. $K \subset F \subset E$. Τότε, ισχύει η ακόλουθη σχέση*

$$\mathrm{tr}_{E/K}(\alpha) = \mathrm{tr}_{F/K}\left(\mathrm{tr}_{E/F}(\alpha)\right)$$

για κάθε $\alpha \in E$.

Απόδειξη. Ας θεωρήσουμε ότι $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$, και $E = \mathbb{F}_{q^{nm}}$. Τότε, ισχύει

$$\begin{aligned}\mathrm{tr}_{F/K}\left(\mathrm{tr}_{E/F}(\alpha)\right) &= \sum_{i=0}^{n-1} \mathrm{tr}_{E/F}(\alpha)^{q^i} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} \alpha^{q^{nj}}\right)^{q^i} \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} \alpha^{q^{nj+i}} = \sum_{k=0}^{nm-1} \alpha^{q^k} = \mathrm{tr}_{E/K}(\alpha)\end{aligned}$$

για κάθε $\alpha \in E$. □

2.6.2 Νόρμες

Μία άλλη απεικόνιση από ένα πεπερασμένο σώμα σε ένα υπόσωμα ορίζεται από το γινόμενο όλων των συζυγών, σε σχέση με το υπόσωμα, ενός στοιχείου του πεπερασμένου σώματος.

Ορισμός 2.61. Έστω $F = \mathbb{F}_{q^n}$ και $K = \mathbb{F}_q$ είναι πεπερασμένα σώματα με q^n και q στοιχεία αντίστοιχα. Έαν $\alpha \in F$, τότε η *νόρμα* $\mathrm{N}_{F/K}(\alpha)$ του στοιχείου α στο K ορίζεται ως εξής

$$\mathrm{N}_{F/K}(\alpha) = \alpha\,\alpha^q \cdots \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}.$$

2.7 Δυϊκές βάσεις

Εκτός από την πολυωνυμική και την κανονική βάση που ορίστηκαν στην ενότητα 2.2.3, ιδιαίτερο σημαντική είναι η έννοια της δυϊκής βάσης που ορίζεται στη συνέχεια.

Ορισμός 2.62. Έστω $F = \mathbb{F}_{q^n}$ και $K = \mathbb{F}_q$ είναι πεπερασμένα σώματα με q^n και q στοιχεία αντίστοιχα. Τότε οι βάσεις $\{\alpha_1, \ldots, \alpha_n\}$ και $\{\beta_1, \ldots, \beta_n\}$ του F στο K ονομάζονται *δυϊκές* έαν ισχύει [72]

$$\mathrm{tr}_{F/K}(\alpha_i \beta_j) = \begin{cases} 0 & \text{έαν } i \neq j, \\ 1 & \text{έαν } i = j, \end{cases}$$

για κάθε $1 \leq i, j \leq n$.

Θεώρημα 2.63. *Έστω $F = \mathbb{F}_{q^n}$ και $K = \mathbb{F}_q$ είναι πεπερασμένα σώματα με q^n και q στοιχεία αντίστοιχα. Επιπλέον, θεωρούμε τις δυϊκές βάσεις $\{\alpha_1, \ldots, \alpha_n\}$ και $\{\beta_1, \ldots, \beta_n\}$ του F στο K. Έαν*

$$z = z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n \in F \tag{2.12}$$

όπου $z_j \in K$, $1 \leq j \leq n$, τότε $z_j = \mathrm{tr}_{F/K}(\beta_j z)$.

Απόδειξη. Το αποτέλεσμα αποδεικνύεται πολλαπλασιάζοντας με β_j και τα δύο μέλη της (2.12), και εφαρμόζοντας στη συνέχεια τον Ορισμό 2.62. □

Κεφάλαιο 3

Ακολουθίες με στοιχεία σε πεπερασμένο σώμα

Ακολουθίες με στοιχεία σε ένα πεπερασμένο σώμα, των οποίων οι όροι εξαρτώνται με απλό τρόπο από προγενέστερους όρους, είναι ιδιαίτερα σημαντικές για ένα μεγάλο πλήθος εφαρμογών. Οι ακολουθίες αυτές παράγονται εύκολα από αναδρομικές σχέσεις, έχουν χαμηλή υπολογιστική πολυπλοκότητα, και χαρακτηρίζονται από ένα σύνολο χρήσιμων ιδιοτήτων. Ιδιαίτερο ενδιαφέρον έχουν οι *γραμμικά αναδρομικές ακολουθίες* των οποίων οι όροι εξαρτώνται από σταθερό αριθμό προγενέστερων όρων.

Ο πιο διαδεδομένος τρόπος παραγωγής των γραμμικά αναδρομικών ακολουθιών είναι οι *καταχωρητές ολίσθησης γραμμικής ανάδρασης*, οι ιδιότητες των οποίων μελετήθηκαν σε μεγάλο βαθμό στο κλασικό βιβλίο του Golomb [33]. Λόγω της ευκολίας υλοποίησής τους έχουν ευρύ φάσμα εφαρμογών, συμπεριλαμβανομένων της κρυπτογραφίας [15], [16], [19], [84], [102], κωδίκων ελέγχου σφαλμάτων [9], [73], [76], επεξεργασίας σήματος [10], [49], [50], και συστημάτων επικοινωνιών ευρέως φάσματος [96], [114].

Στις περισσότερες από τις ανωτέρω εφαρμογές τα στοιχεία των ακολουθιών λαμβάνονται από το σώμα $\mathbb{F}_2$, αλλά η θεωρία ανάλυσης γενικεύεται εύκολα για οποιοδήποτε πεπερασμένο σώμα (βλ. Κεφάλαιο 2). Αναλόγως της εφαρμογής, απαιτείται η χρήση ακολουθιών με συγκεκριμένες ιδιοτήτες, όπως μεγάλη περίοδο και γραμμική πολυπλοκότητα [42], [56], ισοκατανομή άσσων και μηδενικών, δίτιμη συνάρτηση αυτοσυσχέτισης, χαρακτηριστικά λευκού θορύβου, κ.λπ. Ιδιαίτερη

κατηγορία ακολουθιών που παράγονται από καταχωρητές ολίσθησης γραμμικής ανάδρασης αποτελούν οι *ακολουθίες μεγίστου μήκους*.

Σκοπός του παρόντος κεφαλαίου είναι να εισάγει τις βασικές έννοιες που απαιτούνται για την κατανόηση των επόμενων κεφαλαίων.

3.1 Γραμμικά αναδρομικές ακολουθίες

Ας θεωρήσουμε το θετικό ακέραιο n, και τους συντελεστές $f_1, \ldots, f_{n-1}$ που λαμβάνουν τιμές στο πεπερασμένο σώμα $\mathbb{F}_2$. Η άπειρη ακολουθία $x = x_0, x_1, x_2, \ldots$ στοιχείων του $\mathbb{F}_2$ που ικανοποιεί την ομογενή σχέση

$$x_{j+n} = f_{n-1}x_{j+n-1} + \cdots + f_1 x_{j+1} + x_j \qquad j \geq 0 \tag{3.1α′}$$

ή ισοδύναμα την

$$x_j = f_{n-1}x_{j-1} + \cdots + f_1 x_{j-n+1} + x_{j-n} \qquad j \geq n \tag{3.1β′}$$

ονομάζεται *γραμμικά αναδρομική ακολουθία τάξης* n. Οι πρώτοι n όροι της ακολουθίας x, δηλ. οι $x_0, x_1, \ldots, x_{n-1}$, προσδιορίζουν με μοναδικό τρόπο τους υπόλοιπους όρους της ακολουθίας.

Είναι γνωστό [33], [72], [102], ότι έαν η ακολουθία x ικανοποιεί τη σχέση (3.1), τότε η x έχει *ελάχιστο πολυώνυμο* το

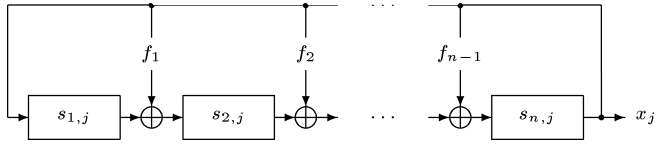
$$f(z) = z^n + f_{n-1}z^{n-1} + \cdots + f_1 z + 1. \tag{3.2}$$

Το $f(z)$ ονομάζεται *χαρακτηριστικό πολυώνυμο* της ακολουθίας x. Πολλές ιδιότητες της ακολουθίας x, όπως η περίοδος της x (βλ. Κεφάλαιο 2), καθορίζονται από τα χαρακτηριστικά του πολυωνύμου $f(z)$. Στη συνέχεια, θεωρούμε ότι οι ρίζες του πολυωνύμου $f(z)$ βρίσκονται στην επέκταση $\mathbb{F}_{2^m}$ του πεπερασμένου σώματος $\mathbb{F}_2$.

Η x είναι ακολουθία μεγίστου μήκους έαν και μόνον έαν το $f(z)$ είναι πρωταρχικό πολυώνυμο, οπότε ισχύει $m = n$. Οι ιδιότητες των ακολουθιών μεγίστου μήκους περιγράφονται στην Ενότητα 3.6.

3.2 Κυκλώματα κατασκευής ακολουθιών

Οι *καταχωρητές ολίσθησης με ανάδραση*, και ειδικότερα οι καταχωρητές ολίσθησης γραμμικής ανάδρασης, αποτελούν τον κυριότερο τρόπο κατασκευής των



Σχήμα 3.1. Το μοντέλο Galois ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης n βαθμίδων με γραμμική έξοδο

γραμμικά αναδρομικών ακολουθιών. Στη συνέχεια, περιγράφονται τα μοντέλα κυκλωμάτων τύπου Galois και Fibonacci των καταχωρητών ολίσθησης γραμμικής ανάδρασης [109].

3.2.1 Κυκλώματα Galois

Ο πρώτος τύπος καταχωρητών ολίσθησης γραμμικής ανάδρασης που παράγουν την ακολουθία x της σχέσης (3.1) ακολουθεί το *μοντέλο Galois* και απεικονίζεται στο Σχ. 3.1.

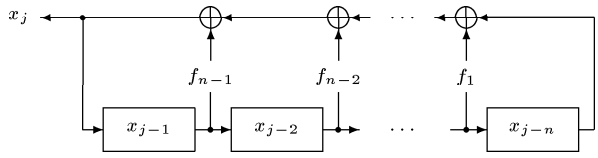
Στο συγκεκριμένο τύπο, ο αθροιστής βρίσκεται μεταξύ των βαθμίδων του καταχωρητή. Παρατηρούμε ότι το *πολυώνυμο ανάδρασης* του καταχωρητή στο Σχ. 3.1 είναι το $f(z)$, δηλ. ταυτίζεται με το ελάχιστο πολυώνυμο της ακολουθίας x. Η *κατάσταση* του καταχωρητή ολίσθησης γραμμικής ανάδρασης τη χρονική στιγμή j είναι το $1 \times n$ διάνυσμα

$$\boldsymbol{s}_j = \begin{pmatrix} s_{1,j} & s_{2,j} & \cdots & s_{n,j} \end{pmatrix}$$

που αποτελείται από τα περιεχόμενα του καταχωρητή τη συγκεκριμένη χρονική στιγμή. Στη συνέχεια αποδεικνύουμε ότι η ακολουθία που παράγεται από το κύκλωμα του Σχ. 3.1 ικανοποιεί τη σχέση (3.1).

Η έξοδος x_j, κατά τη χρονική στιγμή j, και η επόμενη κατάσταση $\boldsymbol{s}_{j+1}$ του καταχωρητή ολίσθησης γραμμικής ανάδρασης δίνονται από τις σχέσεις [33]

$$\boldsymbol{s}_{j+1} = \boldsymbol{s}_j \cdot \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & f_1 & \cdots & f_{n-1} \end{pmatrix} = \boldsymbol{s}_j \cdot \boldsymbol{\Delta} \qquad (3.3\alpha')$$



Σχήμα 3.2. Το μοντέλο Fibonacci ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης n βαθμίδων με γραμμική έξοδο

και

$$x_j = s_{n,j} \tag{3.3β′}$$

αντίστοιχα, όπου ο $n \times n$ πίνακας $\boldsymbol{\Delta}$ καθορίζεται από το πολυώνυμο $f(z)$. Η σχέση (3.3) περιγράφει τη λειτουργία του καταχωρητή του Σχ. 3.1 στο χώρο των καταστάσεων και αποκαλείται *αναπαράσταση πινάκων* της ακολουθίας x [37].

Έστω $\boldsymbol{I}_n$ και $\mathbf{0}$ ο μοναδιαίος και ο μηδενικός πίνακας τάξης n αντίστοιχα. Το χαρακτηριστικό πολυώνυμο του πίνακα $\boldsymbol{\Delta}$, το οποίο υπολογίζεται από την ορίζουσα $\det(z\boldsymbol{I}_n + \boldsymbol{\Delta})$, ταυτίζεται με το $f(z)$. Λόγω του θεωρήματος των Cayley–Hamilton, ο πίνακας $\boldsymbol{\Delta}$ ικανοποιεί τη σχέση

$$f(\boldsymbol{\Delta}) = \mathbf{0} \quad \Leftrightarrow \quad \boldsymbol{\Delta}^n + f_{n-1}\boldsymbol{\Delta}^{n-1} + \cdots + f_1\boldsymbol{\Delta} + \boldsymbol{I}_n = \mathbf{0}$$

η οποία για κάθε $j \geq 0$ γράφεται ως εξής

$$\begin{aligned} \boldsymbol{s}_0\boldsymbol{\Delta}^{j+n} + f_{n-1}\boldsymbol{s}_0\boldsymbol{\Delta}^{j+n-1} + \cdots + f_1\boldsymbol{s}_0\boldsymbol{\Delta}^{j+1} + \boldsymbol{s}_0\boldsymbol{\Delta}^j = \mathbf{0} \quad &\Leftrightarrow \\ \boldsymbol{s}_{j+n} + f_{n-1}\boldsymbol{s}_{j+n-1} + \cdots + f_1\boldsymbol{s}_{j+1} + \boldsymbol{s}_j = \mathbf{0}. \end{aligned}$$

Από την (3.3) και τον ορισμό του διανύσματος $\boldsymbol{s}_j$, καταλήγουμε στο συμπέρασμα ότι για κάθε $j \geq 0$, η ακολουθία x ικανοποιεί τη σχέση (3.1).

3.2.2 Κυκλώματα Fibonacci

Ο δεύτερος τύπος καταχωρητών ολίσθησης γραμμικής ανάδρασης που παράγουν την ακολουθία x της σχέσης (3.1) ακολουθεί το *μοντέλο Fibonacci* και απεικονίζεται στο Σχ. 3.2.

Στο συγκεκριμένο τύπο, ο αθροιστής δε βρίσκεται μεταξύ των βαθμίδων του καταχωρητή. Παρατηρούμε ότι το πολυώνυμο ανάδρασης του καταχωρητή στο

Σχ. 3.2 είναι το $f^*(z) = z^n f(1/z)$, δηλ. είναι το ανάστροφο του ελαχίστου πολυωνύμου της ακολουθίας x. Το πολυώνυμο $f^*(z)$ είναι πρωταρχικό έαν και μόνον έαν το $f(z)$ είναι πρωταρχικό (βλ. Κεφάλαιο 2). Επιπρόσθετα, οι ρίζες του $f^*(z)$ είναι οι αντίστροφες των ριζών του $f(z)$ στο $\mathbb{F}_{2^m}$.

Η κατάσταση του καταχωρητή ολίσθησης γραμμικής ανάδρασης τη χρονική στιγμή j είναι το $1 \times n$ διάνυσμα

$$\boldsymbol{x}_j = \begin{pmatrix} x_{j-1} & x_{j-2} & \cdots & x_{j-n} \end{pmatrix}$$

που αποτελείται από τα περιεχόμενα του καταχωρητή τη συγκεκριμένη χρονική στιγμή. Το διάνυσμα $\boldsymbol{x}_n$ ονομάζεται *αρχική κατάσταση* του καταχωρητή ολίσθησης γραμμικής ανάδρασης. Συχνά, στο διάνυσμα της αρχικής κατάστασης $\boldsymbol{x}_n$ αντιστοιχίζεται το πολυώνυμο

$$x^n(z) = x_{n-1} z^{n-1} + \cdots + x_1 z + x_0 \tag{3.4}$$

βαθμού $n-1$. Η απόδειξη ότι η ακολουθία που παράγεται από το κύκλωμα του Σχ. 3.2 ικανοποιεί τη σχέση (3.1) είναι τετριμμένη

Από τη σχέση (3.1), το μοντέλο Fibonacci του καταχωρητή ολίσθησης γραμμικής ανάδρασης στο Σχ. 3.2 περιγράφεται στο χώρο των καταστάσεων ως εξής

$$\boldsymbol{x}_{j+1} = \boldsymbol{x}_j \cdot \begin{pmatrix} f_{n-1} & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ f_1 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix} = \boldsymbol{x}_j \cdot \widetilde{\boldsymbol{\Delta}}. \tag{3.5}$$

όπου ο $n \times n$ πίνακας $\widetilde{\boldsymbol{\Delta}}$ καθορίζεται από το πολυώνυμο $f(z)$. Η σχέση που συνδέει τους πίνακες $\boldsymbol{\Delta}$ και $\widetilde{\boldsymbol{\Delta}}$ είναι η

$$\widetilde{\boldsymbol{\Delta}} = \boldsymbol{J}_n \boldsymbol{\Delta}^T \boldsymbol{J}_n \tag{3.6}$$

όπου $\boldsymbol{J}_n$ είναι ο $n \times n$ πίνακας αντιστροφής διάταξης

$$\boldsymbol{J}_n = \begin{pmatrix} & & & 1 & 1 \\ & & \cdot^{\cdot^{\cdot}} & & \\ & \cdot & & & \\ 1 & & & & \end{pmatrix}.$$

Αποδεικνύεται εύκολα ότι οι πίνακες $\boldsymbol{\Delta}$ και $\widetilde{\boldsymbol{\Delta}}$ έχουν το ίδιο χαρακτηριστικό πολυώνυμο [79].

3.3 Αναπαράσταση ακολουθιών

Εκτός της αναπαράστασης πινάκων που περιγράφηκε στην Ενότητα 3.2, η άπειρη ακολουθία x χαρακτηρίζεται από πλήθος άλλων αναπαραστάσεων, όπως η *τυπική αναπαράσταση δυναμοσειράς*, η *ρητή αναπαράσταση*, και η *αναπαράσταση ίχνους*. Οι περιγραφές τους δίνονται στις επόμενες ενότητες.

3.3.1 Τυπική αναπαράσταση δυναμοσειράς

Σε κάθε ακολουθία $x = x_0, x_1, x_2, \ldots$ στοιχείων του $\mathbb{F}_2$ αντιστοιχίζεται η *συνάρτηση γεννήτορας* $F(z)$, με

$$F(z) = x_0 + x_1 z + x_2 z^2 + \cdots = \sum_{j=0}^{\infty} x_j z^j. \tag{3.7}$$

Η έκφραση (3.7) έχει ως συντελεστές τους όρους της ακολουθίας και ονομάζεται επίσης τυπική αναπαράσταση δυναμοσειράς της ακολουθίας x.

Ας θεωρήσουμε επιπλέον τη συνάρτηση γεννήτορα $G(z) = \sum_{j=0}^{\infty} y_j z^j$ και ας ορίσουμε τις συνήθεις πράξεις της πρόσθεσης

$$F(z) + G(z) = \sum_{j=0}^{\infty} (x_j + y_j) z^j \tag{3.8}$$

και του πολλαπλασιασμού

$$F(z)G(z) = \sum_{j=0}^{\infty} \Big(\sum_{i=0}^{j} x_i y_{j-i} \Big) z^j. \tag{3.9}$$

Αποδεικνύεται ότι το σύνολο όλων των τυπικών αναπαραστάσεων δυναμοσειράς με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, όπως ορίστηκαν στις σχέσεις (3.8) και (3.9), αποτελεί ακέραια περιοχή (βλ. Κεφάλαιο 2), και συμβολίζεται με $\mathbb{F}_2[[z]]$. Επιπλέον, αποδεικνύεται ότι η συνάρτηση γεννήτορας $F(z)$ έχει αντίστροφο στο $\mathbb{F}_2[[z]]$ έαν και μόνον έαν $x_0 \neq 0$ [72].

Επειδή η ακολουθία x έχει χαρακτηριστικό πολυώνυμο το $f(z)$, έαν θέσουμε $f_0 = f_n = 1$ λαμβάνουμε από τη σχέση (3.1)

$$f^*(z)F(z) = \Big(\sum_{i=0}^{n} f_{n-i} z^i \Big) \Big(\sum_{j=0}^{\infty} x_j z^j \Big)$$

$$= \sum_{j=0}^{n-1} \Big(\sum_{i=0}^{j} f_{n-j+i} x_i \Big) z^j + \sum_{j=n}^{\infty} \Big(\sum_{i=j-n}^{j} f_{n-j+i} x_i \Big) z^j$$
$$= \sum_{j=0}^{n-1} \Big(\sum_{i=0}^{j} f_{n-j+i} x_i \Big) z^j .$$

Συνεπώς, η συνάρτηση γεννήτορας $F(z)$ της ακολουθίας x δίνεται από τη σχέση

$$F(z) = \frac{r(z)}{f^*(z)} \qquad \text{όπου} \qquad r(z) = \sum_{j=0}^{n-1} \Big(\sum_{i=0}^{j} f_{n-j+i} x_i \Big) z^j \tag{3.10}$$

με $\deg(r) < \deg(f^*)$. Η έκφραση της σχέσης (3.10) ονομάζεται *ρητή αναπαράσταση* της ακολουθίας x [50], [102]. Τα πολυώνυμα $r(z)$ και $f(z)$ είναι πρώτα μεταξύ τους.

Παρατήρηση 3.1. Ισοδύναμα, το πολυώνυμο $r(z)$ δύναται να υπολογιστεί επίσης από τη σχέση

$$\boldsymbol{r} = \boldsymbol{x}_n \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ f_{n-1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ f_2 & f_3 & \cdots & 1 & 0 \\ f_1 & f_2 & \cdots & f_{n-1} & 1 \end{pmatrix}$$

όπου $\boldsymbol{r} = \begin{pmatrix} r_{n-1} & r_{n-2} & \cdots & r_0 \end{pmatrix}$ περιέχει τους συντελεστές του πολυωνύμου $r(z)$.

Παρατήρηση 3.2. Εναλλακτικός τρόπος υπολογισμού του πολυωνύμου $r(z)$ είναι επίσης ο ακόλουθος

$$r(z) = f^*(z) x^n(z) \bmod z^n$$

και αντιστοιχεί στα περιεχόμενα του καταχωρητή στο Σχ. 3.1 τη χρονική στιγμή $j = 0$.

Η ακολουθία x, της οποίας κυκλώματα παραγωγής περιγράφηκαν στην Ενότητα 3.2, είναι περιοδική με περίοδο $M = 2^m - 1$, όχι κατ' ανάγκη ελάχιστη. Στη γενική περίπτωση, η ελάχιστη περίοδος της x είναι διαιρέτης του M. Επειδή $f^*(z) | z^M + 1$ (βλ. Κεφάλαιο 2), η σχέση (3.10) γράφεται

$$F(z) = \frac{r(z) h^*(z)}{z^M + 1} = \frac{x^M(z)}{z^M + 1} \qquad \text{όπου} \qquad f^*(z) h^*(z) = z^M + 1. \tag{3.11}$$

Το πολυώνυμο $x^M(z)$ συμβολίζεται συχνά ως $x(z)$, και αποδεικνύεται εύκολα ότι ισχύει $x(z) = x_{M-1}z^{M-1} + \cdots + x_1 z + x_0$, δηλ. περιλαμβάνει τους όρους μίας περιόδου της ακολουθίας x. Στο πολυώνυμο $x(z)$ αντιστοιχεί το διάνυσμα $\boldsymbol{x} = \begin{pmatrix} x_{M-1} & \cdots & x_1 & x_0 \end{pmatrix}$.

Αθροίσματα ακολουθιών

Ας θεωρήσουμε ότι το ελάχιστο πολυώνυμο $f(z)$ της άπειρης ακολουθίας x δεν είναι ανάγωγο, και έστω k θετικός ακέραιος. Τότε, το πολυώνυμο $f(z)$ παραγοντοποιείται με μοναδικό τρόπο (βλ. Κεφάλαιο 2) ως εξής

$$f(z) = f_1(z)f_2(z)\cdots f_k(z)$$

όπου ο βαθμός του πολυωνύμου $f_i(z)$ είναι m_i, ο ακέραιος m_i διαιρεί τον m, και $n = m_1 + m_2 + \cdots + m_k$. Η σχέση (3.10) λαμβάνει την ακόλουθη μορφή

$$F(z) = \frac{r_1(z)}{f_1^*(z)} + \frac{r_2(z)}{f_2^*(z)} + \cdots + \frac{r_k(z)}{f_k^*(z)} \tag{3.12}$$

με $\deg(r_i) < \deg(f_i^*)$. Συνεπώς, η x γράφεται ως άθροισμα (modulo 2) των k ακολουθιών

$$x = x^1 + x^2 + \cdots + x^k$$

οι οποίες ονομάζονται *συνιστώσες ακολουθίες* της x. Οι ακολουθίες x^i, $1 \leq i \leq k$, υλοποιούνται από κυκλώματα του Σχ. 3.1 ή 3.2.

Είναι γνωστό [33], [37], [102], ότι το ελάχιστο πολυώνυμο του αθροίσματος (modulo 2) δύο ή περισσοτέρων ακολουθιών είναι ίσο με το ελάχιστο κοινό πολλαπλάσιο αυτών.

3.3.2 Αναπαράσταση ίχνους

Ας υποθέσουμε αρχικά ότι το ελάχιστο πολυώνυμο $f(z)$ της άπειρης ακολουθίας x είναι ανάγωγο. Τότε, $m = n$, και οι ρίζες του $f(z)$ βρίσκονται στην επέκταση $\mathbb{F}_{2^n}$ του πεπερασμένου σώματος $\mathbb{F}_2$.

Έστω $\alpha, \beta \in \mathbb{F}_{2^n}$ είναι στοιχεία του πεπερασμένου σώματος $\mathbb{F}_{2^n}$,όπου α είναι ρίζα του πολυωνύμου $f(z)$. Τότε, ισχύει

$$f(\alpha) = 0 \quad \Leftrightarrow \quad \alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_1\alpha + 1 = 0 \tag{3.13}$$

και για κάθε $j \geq 0$

$$\begin{aligned}\mathrm{tr}_1^n(\beta\alpha^{j+n}) + f_{n-1}\,\mathrm{tr}_1^n(\beta\alpha^{j+n-1}) + \cdots + f_1\,\mathrm{tr}_1^n(\beta\alpha^{j+1}) + \mathrm{tr}_1^n(\beta\alpha^j) \\ = \mathrm{tr}_1^n\big(\beta(\alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_1\alpha + 1)\alpha^j\big) \\ = \mathrm{tr}_1^n\big(\beta f(\alpha)\alpha^j\big) = 0.\end{aligned}$$

Συνεπώς, η συνάρτηση ίχνους $\mathrm{tr}_1^n(\beta\alpha)$ είναι λύση της γραμμικής αναδρομικής σχέσης (3.1), και ισχύει

$$x_j = \mathrm{tr}_1^n(\beta\alpha^j) \qquad \text{για κάθε } j \geq 0. \tag{3.14}$$

Η έκφραση (3.14) ονομάζεται αναπαράσταση ίχνους της δυαδικής ακολουθίας x. Έστω $\boldsymbol{\beta} = \begin{pmatrix}\beta^{2^{n-1}} & \cdots & \beta^2 & \beta\end{pmatrix}$. Ο συντελεστής $\beta \in \mathbb{F}_{2^n}$ βρίσκεται επιλύοντας το σύστημα

$$\boldsymbol{\beta}\begin{pmatrix}\alpha^{n-1} & \cdots & \alpha & 1 \\ \alpha^{(n-1)2} & \cdots & \alpha^2 & 1 \\ \vdots & & \vdots & \vdots \\ \alpha^{(n-1)2^{n-1}} & \cdots & \alpha^{2^{n-1}} & 1\end{pmatrix} = \boldsymbol{x}_n \;\Leftrightarrow\; \boldsymbol{\beta}\,\boldsymbol{V} = \boldsymbol{x}_n.$$

Ο πίνακας συντελεστών του ανωτέρω συστήματος είναι αντιστρέψιμος πίνακας Vandermonde, αφού τα στοιχεία $1, \alpha, \ldots, \alpha^{n-1}$ αποτελούν πολυωνυμική βάση του $\mathbb{F}_{2^n}$ (βλ. Κεφάλαιο 2). Η λύση του συστήματος δίνεται από τη σχέση [1]

$$\boldsymbol{\beta} = \boldsymbol{x}_n\,\boldsymbol{V}^{-1} \;\Leftrightarrow\; \boldsymbol{\beta} = \boldsymbol{x}_n\begin{pmatrix}\alpha^{-(n-1)} & \alpha^{-(n-1)2} & \cdots & \alpha^{-(n-1)2^{n-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-2^{n-1}} \\ 1 & 1 & \cdots & 1\end{pmatrix}. \tag{3.15}$$

Στην περίπτωση που η λύση (3.15) του συστήματος εξισώσεων είναι $\beta = 1$, τότε η ακολουθία x βρίσκεται στη *χαρακτηριστική φάση* [33], [71]. Οι όροι μίας ακολουθίας που βρίσκεται στη χαρακτηριστική της φάση, των οποίων οι θέσεις ανήκουν στην ίδια κυκλοτομική κλάση, έχουν σταθερή τιμή. Οι συγκεκριμένες ακολουθίες αντιστοιχούν σε *ταυτοδύναμα πολυώνυμα* της θεωρίας κωδίκων ελέγχου σφαλμάτων [2], [76, Κεφ. 8], [93], [94].

Έστω $y = y_0, y_1, y_2, \ldots$ μία άπειρη ακολουθία στοιχείων του $\mathbb{F}_2$ της ιδίας περιόδου με τη x. Οι ακολουθίες x και y ονομάζονται *κυκλικά ισοδύναμες* έαν

και μόνον έαν τα διανύσματα $\boldsymbol{x}$ και $\boldsymbol{y}$ σχετίζονται με κατάλληλο αριθμό δεξιών (ή αριστερών) κυκλικών ολισθήσεων. Έαν οι x και y είναι κυκλικά ισοδύναμες γράφουμε $x \sim y$.

Στη γενική περίπτωση, ακολουθίες παραγόμενες από τον ίδιο καταχωρητή ολίσθησης γραμμικής ανάδρασης δεν είναι κυκλικά ισοδύναμες. Έαν το ελάχιστο πολυώνυμο $f(z)$ είναι πρωταρχικό, τότε όλες οι παραγόμενες μη–μηδενικές ακολουθίες είναι κυκλικά ισοδύναμες, και προκύπτουν για διαφορετικές τιμές του $\beta \in \mathbb{F}_{2^n}$ στη σχέση (3.14).

Αθροίσματα ακολουθιών

Σε αντιστοιχία με την Ενότητα 3.3.1, υποθέτουμε ότι η άπειρη ακολουθία x γράφεται ως άθροισμα (modulo 2) k συνιστωσών ακολουθιών σύμφωνα με τον τύπο

$$x = x^1 + x^2 + \cdots + x^k.$$

Επιπλέον, υποθέτουμε ότι το στοιχείο $\alpha^{t_i} \in \mathbb{F}_{2^{m_i}}$, $m_i | m$, αποτελεί ρίζα του ελαχίστου πολυωνύμου $f_i(z)$ της ακολουθίας x^i με βαθμό m_i. Επιπλέον, ισχύει ότι $n = m_1 + m_2 + \cdots + m_k$. Τότε, η σχέση (3.14) λαμβάνει την ακόλουθη μορφή [102]

$$x_j = \mathrm{tr}_1^{m_1}(\beta_1 \alpha^{t_1 j}) + \mathrm{tr}_1^{m_2}(\beta_2 \alpha^{t_2 j}) + \cdots + \mathrm{tr}_1^{m_k}(\beta_k \alpha^{t_k j}) \tag{3.16}$$

για κάθε $j \geq 0$, όπου $\beta_i \in \mathbb{F}_{2^{m_i}}$ και ο ακέραιος t_i είναι ο επικεφαλής της κυκλοτομικής κλάσης C_{t_i} (βλ. Κεφάλαιο 2).

Παρατήρηση 3.3. Η άπειρη ακολουθία x που ορίζεται από τη σχέση (3.16) βρίσκεται στη χαρακτηριστική της φάση έαν και μόνον έαν $\beta_1 = \cdots = \beta_k = 1$.

3.4 Διακριτός μετασχηματισμός Fourier

Στην παρούσα ενότητα αναλύουμε τις βασικές ιδιότητες του *διακριτού μετασχηματισμού Fourier (DFT)* της άπειρης ακολουθίας $x = x_0, x_1, x_2, \ldots$ στοιχείων του $\mathbb{F}_2$. Επιπλέον, εξάγονται σχέσεις που συνδέουν το διακριτό μετασχηματισμό Fourier με την αναπαράσταση ίχνους της ακολουθίας x.

Κάνοντας χρήση του συμβολισμού της Ενότητας 3.3.1, υποθέτουμε ότι η ακολουθία x έχει ελάχιστη περίοδο $M = 2^m - 1$, και γράφεται ως άθροισμα

(modulo 2) k συνιστωσών ακολουθιών σύμφωνα με τον τύπο

$$x = x^1 + x^2 + \cdots + x^k.$$

Έστω $\alpha \in \mathbb{F}_{2^m}$ πρωταρχικό στοιχείο του $\mathbb{F}_{2^m}$. Τότε, από την ανάλυση της προηγούμενης ενότητας, ο j–στός όρος της ακολουθίας x δίνεται από τη σχέση (3.16).

Ας θεωρήσουμε ότι ο διακριτός μετασχηματισμός Fourier της x είναι η άπειρη ακολουθία $X = X_0, X_1, X_2, \ldots$ στοιχείων του $\mathbb{F}_{2^m}$, με ελάχιστη περίοδο M. Τότε, ο k–στός όρος της ακολουθίας X υπολογίζεται ως εξής [9], [50]

$$X_i = \sum_{j=0}^{M-1} x_j \alpha^{ij} = x(\alpha^i) \qquad i \geq 0. \tag{3.17}$$

Στη συνέχεια, αποδεικνύουμε ένα αποτέλεσμα που είναι απαραίτητο για την εύρεση του αντίστροφου διακριτού μετασχηματισμού Fourier.

Λήμμα 3.4. *Έστω $\alpha \in \mathbb{F}_{2^m}$ πρωταρχικό στοιχείο και d μη–αρνητικός ακέραιος. Τότε, ισχύει*

$$\sum_{i=0}^{M-1} \alpha^{di} = \begin{cases} 1 & \text{εάν } d \equiv 0 \pmod{M}, \\ 0 & \text{διαφορετικά.} \end{cases}$$

Απόδειξη. Εαν $d \equiv 0 \pmod{M}$, τότε είναι προφανές ότι ισχύει $\sum_{i=0}^{M-1} \alpha^0 = 1$ επειδή ο M είναι περιττός ακέραιος. Στην αντίθετη περίπτωση, ισχύει

$$1 + \alpha^d + \alpha^{d2} + \cdots + \alpha^{d(M-1)} = (1 + \alpha^{dM})(1 + \alpha^d)^{-1}. \tag{3.18}$$

Εξ' υποθέσεως, το α είναι πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^m}$. Αφού $d \not\equiv 0 \pmod{M}$, η τάξη του στοιχείου α^d ικανοποιεί την ανισότητα

$$1 < \operatorname{ord}(\alpha^d) = M/\gcd(M, d) \leq M.$$

Συνεπώς, ο αντίστροφος του στοιχείου $1 + \alpha^d$ είναι καλά ορισμένος. Από τη σχέση $\operatorname{ord}(\alpha^{dM}) = M/\gcd(M, dM) = 1$, συμπεραίνουμε ότι $1 + \alpha^{dM} = 0$ και η σχέση (3.18) μηδενίζεται. □

Ο αντίστροφος του διακριτού μετασχηματισμού Fourier που ορίστηκε στη σχέση (3.17), υπολογίζεται από την έκφραση

$$x_j = \sum_{i=0}^{M-1} X_i \alpha^{-ji} = X(\alpha^{-j}) \qquad j \geq 0 \tag{3.19}$$

όπου $X(z) \in \mathbb{F}_{2^m}[z]$ είναι το πολυώνυμο βαθμού μικρότερου ή ίσου του $M-1$ που αντιστοιχεί στο διάνυσμα $\boldsymbol{X} = \begin{pmatrix} X_{M-1} & \cdots & X_1 & X_0 \end{pmatrix}$. Πράγματι, έαν αντικαταστήσουμε τη σχέση (3.17) στην (3.19), λαμβάνουμε

$$\sum_{i=0}^{M-1} X_i \alpha^{-ji} = \sum_{i=0}^{M-1} \Big(\sum_{k=0}^{M-1} x_k \alpha^{ik} \Big) \alpha^{-ji} = \sum_{k=0}^{M-1} \Big(\sum_{i=0}^{M-1} \alpha^{(k-j)i} \Big) x_k = x_j$$

αφού το εσωτερικό άθροισμα της ανωτέρω έκφρασης μηδενίζεται για όλες τις τιμές του k εκτός της $k = j$, από το Λήμμα 3.4. Ο διακριτός μετασχηματισμός Fourier της άπειρης δυαδικής ακολουθίας x, περιόδου M, και ο αντίστροφός του πραγματοποιούνται ισοδύναμα μέσω πολλαπλασιασμού πινάκων από τις ακόλουθες σχέσεις

$$\boldsymbol{X} = \boldsymbol{x}\,\boldsymbol{A} \;\Leftrightarrow\; \boldsymbol{X} = \boldsymbol{x} \begin{pmatrix} \alpha^{(M-1)(M-1)} & \cdots & \alpha^{M-1} & 1 \\ \vdots & & \vdots & \vdots \\ \alpha^{M-1} & \cdots & \alpha & 1 \\ 1 & \cdots & 1 & 1 \end{pmatrix} \tag{3.20}$$

και

$$\boldsymbol{x} = \boldsymbol{X}\,\boldsymbol{A}^{-1} \;\Leftrightarrow\; \boldsymbol{x} = \boldsymbol{X} \begin{pmatrix} \alpha^{-(M-1)(M-1)} & \cdots & \alpha^{-(M-1)} & 1 \\ \vdots & & \vdots & \vdots \\ \alpha^{-(M-1)} & \cdots & \alpha^{-1} & 1 \\ 1 & \cdots & 1 & 1 \end{pmatrix} \tag{3.21}$$

αντίστοιχα.

Ο γρήγορος αλγόριθμος των Cooley–Tukey είναι ένας από τους αποτελεσματικούς αλγορίθμους που υλοποιούν το διακριτό μετασχηματισμό Fourier, και εφαρμόζεται στην ακολουθία που προκύπτει από την x με την προσάρτιση ενός μηδενικού [10], [50].

Εναλλακτικά, είναι δυνατό να χρησιμοποιηθεί ο αλγόριθμος του Rader ο οποίος μετατρέπει με αποτελεσματικό τρόπο τον υπολογισμό του διακριτού μετασχηματισμού Fourier σε υπολογισμό κυκλικής συνέλιξης (έαν ο ακέραιος M είναι πρώτος αριθμός Mersenne). Στη συνέχεια, η κυκλική συνέλιξη υπολογίζεται με γρήγορους αλγορίθμους, όπως ο αλγόριθμος του Winograd [50].

Στην ανάλυση και σχεδίαση περιοδικών ακολουθιών με επιθυμητά χαρακτηριστικά, εκτός του διακριτού μετασχηματισμού Fourier, χρησιμοποιείται ευρέως και ο μετασχηματισμός Walsh–Hadamard [14], [122].

3.4.1 DFT και αναπαράσταση ίχνους

Ο διακριτός μετασχηματισμός Fourier της δυαδικής ακολουθίας x, περιόδου M, που δίνεται από τη σχέση (3.16) υπολογίζεται εύκολα από την αναπαράσταση ίχνους της x, και αντιστρόφως.

Πράγματι, αντικαθιστώντας τη σχέση (3.16) στην (3.17) λαμβάνουμε την ακόλουθη έκφραση

$$\begin{aligned} X_i &= \sum_{j=0}^{M-1} \Big(\sum_{r=1}^{k} \mathrm{tr}_1^{m_r}(\beta_r \alpha^{t_r j}) \Big) \alpha^{ij} = \sum_{j=0}^{M-1} \Big(\sum_{r=1}^{k} \sum_{s=0}^{m_r-1} (\beta_r \alpha^{t_r j})^{2^s} \Big) \alpha^{ij} \\ &= \sum_{r=1}^{k} \sum_{s=0}^{m_r-1} \beta_r^{2^s} \Big(\sum_{j=0}^{M-1} \alpha^{(2^s t_r + i)j} \Big). \end{aligned} \tag{3.22}$$

Από το Λήμμα 3.4, ο συντελεστής Fourier X_i είναι μη–μηδενικός μόνο στην περίπτωση όπου ο δείκτης i, με $0 \le i < M$, είναι τέτοιος ώστε να ισχύει

$$i \equiv -2^s t_r \pmod{M}$$

για συγκεκριμένο ζεύγος ακεραίων (r, s), με $1 \le r \le k$ και $0 \le s < m_r$. Τότε καταλήγουμε στη σχέση

$$X_{-2^s t_r} = x(\alpha^{-2^s t_r}) = \beta_r^{2^s}. \tag{3.23}$$

Από τη σχέση (3.23) καθίσταται φανερό ότι οι συντελεστές Fourier $X_i \in \mathbb{F}_{2^m}$ ανήκουν στο υπόσωμα $\mathbb{F}_2$ έαν και μόνον έαν η ακολουθία x βρίσκεται στη χαρακτηριστική της φάση.

Παρατήρηση 3.5. Οι όροι της ακολουθίας Fourier X είναι μη–μηδενικοί μόνο σε θέσεις που ανήκουν στις κυκλοτομικές κλάσεις $C_{-t_1}, C_{-t_2}, \ldots, C_{-t_k}$.

Παρατήρηση 3.6. Το πολυώνυμο $X(z) \in \mathbb{F}_{2^m}[z]$ βαθμού μικρότερου ή ίσου του $M-1$ είναι το ανάστροφο του Mattson–Solomon πολυωνύμου $E(z) = X^*(z)$ της θεωρίας κωδίκων ελέγχου σφαλμάτων [55], [76, Κεφ. 8], [93], [94].

3.5 Αυτο– και ετερο– συσχέτιση ακολουθιών

Ας θεωρήσουμε την άπειρη ακολουθία x, περιόδου N, με στοιχεία στο $\mathbb{F}_2$. Επιπλέον, έστω D ο τελεστής καθυστέρησης ο οποίος ολισθαίνει ένα διάνυσμα κυκ-

λικά προς τα αριστερά κατά μία θέση. Προφανώς, ισχύει

$$D^j \boldsymbol{x} = \begin{pmatrix} x_{N-j-1} & \cdots & x_0 & x_{N-1} & \cdots & x_{N-j} \end{pmatrix}.$$

Επειδή η ακολουθία x έχει περίοδο N, $D^{j+N}\boldsymbol{x} = D^j \boldsymbol{x}$.

Έαν ο τελεστής D εφαρμοστεί στην ακολουθία x, τότε καθίσταται ο συνήθης τελεστής καθυστέρησης, ή προς τα εμπρός ολίσθησης, αφού η ακολουθία $D^j x$ είναι η περιοδική επέκταση του διανύσματος $D^j \boldsymbol{x}$. Όμοια, ο αντίστροφος του τελεστή καθυστέρησης, ο οποίος συμβολίζεται με D^{-1}, ολισθαίνει ένα διάνυσμα κυκλικά προς τα δεξιά κατά μία θέση, και ισχύει $D^{-j}\boldsymbol{x} = D^{N-j}\boldsymbol{x}$.

Η συνάρτηση περιοδικής αυτοσυσχέτισης AC_x της ακολουθίας x είναι η συνάρτηση πραγματικών τιμών που δίνεται από τη σχέση [33], [44]

$$\mathrm{AC}_x(t) = \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{x_j + x_{j-t}} = 1 - \frac{2}{N}\,\mathrm{wt}(\boldsymbol{x} + D^t\boldsymbol{x}) \tag{3.24}$$

όπου $t \in \mathbb{Z}_N$, και $\mathrm{wt}(\boldsymbol{x})$ το βάρος Hamming, δηλ. ο αριθμός των μη–μηδενικών στοιχείων του διανύσματος $\boldsymbol{x}$. Επειδή η x είναι περιοδική, η ακολουθία αυτοσυσχέτισης $\{\mathrm{AC}_x(t)\}_{t\geq 0}$ είναι επίσης περιοδική, με ελάχιστη περίοδο N.

Ας θεωρήσουμε επίσης την άπειρη ακολουθία y, ιδίας περιόδου με την x, με στοιχεία στο $\mathbb{F}_2$. Η συνάρτηση περιοδικής ετεροσυσχέτισης $\mathrm{CC}_{x,y}$ των ακολουθιών x και y είναι η συνάρτηση πραγματικών τιμών που δίνεται από τη σχέση [33], [44]

$$\mathrm{CC}_{x,y}(t) = \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{x_j + y_{j-t}} = 1 - \frac{2}{N}\,\mathrm{wt}(\boldsymbol{x} + D^t\boldsymbol{y}) \tag{3.25}$$

όπου $t \in \mathbb{Z}_N$. Σε αντιστοιχία με τη συνάρτηση αυτοσυσχέτισης, η ακολουθία ετεροσυσχέτισης $\{\mathrm{CC}_{x,y}(t)\}_{t\geq 0}$ είναι περιοδική, με ελάχιστη περίοδο N.

Στην ειδική περίπτωση που οι x και y είναι ακολουθίες μεγίστου μήκους, η συνάρτηση περιοδικής ετεροσυσχέτισης $\mathrm{CC}_{x,y}$ λαμβάνει τουλάχιστον τρεις τιμές [43]. Έαν οι τιμές που λαμβάνονται είναι ακριβώς τρεις, τότε το ζεύγος των ακολουθιών μεγίστου μήκους x και y ονομάζεται *προτιμητέο ζεύγος*.

Είναι σύνηθες να χρησιμοποιούνται οι $\{+1, -1\}$, αντί των $\{0, 1\}$, εκδοχές των ακολουθιών x και y για τον υπολογισμό των συναρτήσεων αυτοσυσχέτισης και ετεροσυσχέτισης [107].

Οι συναρτήσεις αυτοσυσχέτισης και ετεροσυσχέτισης είναι ιδιαίτερα σημαντικές για την ασφάλεια κρυπτοσυστημάτων και τη σχεδίαση μεγάλων οικογενειών ακολουθιών με επιθυμητά στατιστικά χαρακτηριστικά [11]. Έστω η ακόλουθη οικογένεια k άπειρων ακολουθιών, ιδίας περιόδου N, με στοιχεία από το $\mathbb{F}_2$

$$\mathcal{F} = \Big\{ x^i : \ 1 \leq i \leq k \Big\}.$$

Από τις σχέσεις (3.24) και (3.25) ορίζονται οι ποσότητες

$$\mathrm{PAC}_{\mathcal{F}} = \max_{0<t<N} \Big\{ |\, \mathrm{AC}_x(t)| : \ x \in \mathcal{F} \Big\} \tag{3.26}$$

και

$$\mathrm{PCC}_{\mathcal{F}} = \max_{0\leq t<N} \Big\{ |\, \mathrm{CC}_{x,y}(t)| : \ x, y \in \mathcal{F}, \ \text{και } x \neq y \Big\} \tag{3.27}$$

οι οποίες ονομάζονται *μέγιστη εκτός–φάσης αυτοσυσχέτιση* και *μέγιστη ετεροσυσχέτιση* αντίστοιχα. Κατά τη σχεδίαση οικογενειών ακολουθιών $\mathcal{F}$ γίνεται προσπάθεια ελαχιστοποίησης της *μέγιστης συσχέτισης*

$$\mathrm{PC}_{\mathcal{F}} = \max\Big\{ \mathrm{PAC}_{\mathcal{F}}, \mathrm{PCC}_{\mathcal{F}} \Big\} \tag{3.28}$$

με παράλληλη μεγιστοποίηση του πλήθους k των ακολουθιών που ανήκουν στην οικογένεια $\mathcal{F}$. Η οικογένεια ακολουθιών $\mathcal{F}$ έχει χαμηλή μέγιστη συσχέτιση έαν $\mathrm{PC}_{\mathcal{F}} \leq c\sqrt{N}$, όπου c σταθερός ακέραιος [120].

3.6 Ιδιότητες ακολουθιών μεγίστου μήκους

Ας θεωρήσουμε την άπειρη ακολουθία x περιόδου $N = 2^n - 1$, όχι κατ' ανάγκη ελάχιστης, με στοιχεία στο $\mathbb{F}_2$. Στη συνέχεια, παραθέτουμε πλήθος βασικών ιδιοτήτων της x, στην περίπτωση όπου η x είναι ακολουθία μεγίστου μήκους [33], [72], [76]. Οι ακολουθίες μεγίστου μήκους ονομάζονται και ψευδο–τυχαίες ακολουθίες.

Ιδιότητα 3.7. Η ελάχιστη περίοδος της ακολουθίας μεγίστου μήκους x είναι $N = 2^n - 1$.

Ιδιότητα 3.8. Υπάρχουν N μη–μηδενικές ακολουθίες μεγίστου μήκους με ελάχιστο πολυώνυμο $f(z)$.

Οι συγκεκριμένες ακολουθίες παράγονται από τους καταχωρητές ολίσθησης γραμμικής ανάδρασης των Σχ. 3.1 και 3.2 με πολυώνυμα ανάδρασης $f(z)$ και $f^*(z)$ αντίστοιχα. Επιπλέον, οι ακολουθίες αυτές αντιστοιχούν στις περιοδικές επεκτάσεις των N διακριτών διανυσμάτων

$$\boldsymbol{x}, D\boldsymbol{x}, \ldots, D^{N-1}\boldsymbol{x}$$

που ονομάζονται *φάσεις* της ακολουθίας x.

Ιδιότητα 3.9. Από την πρόσθεση δύο διακριτών φάσεων της ακολουθίας μεγίστου μήκους x προκύπτει μία νέα φάση της x.

Η Ιδιότητα 3.9 είναι γνωστή ως ιδιότητα *ολίσθησης–και–πρόσθεσης*, όπου ισχύει

$$D^{j_1}\boldsymbol{x} + D^{j_2}\boldsymbol{x} = D^{j_3}\boldsymbol{x}. \tag{3.29}$$

Οι ακέραιοι j_i είναι διαφορετικοί μεταξύ τους και ανήκουν στο σύνολο $\mathbb{Z}_N$.

Ιδιότητα 3.10. Η ακολουθία μεγίστου μήκους x ικανοποιεί κάθε γραμμική επαναληπτική σχέση που αντιστοιχεί σε πολλαπλάσιο του πολυωνύμου $f^*(z)$ βαθμού μικροτέρου ή ίσου του N.

Γενικότερα, η Ιδιότητα 3.10 ισχύει για κάθε περιοδική δυαδική ακολουθία x, και βάσει αυτής πραγματοποιείται η ανάλυση της τυχαιότητας ακολουθιών στο Κεφάλαιο 6.

Ιδιότητα 3.11. Η ακολουθία μεγίστου μήκους x είναι *ισοβαρής* ακολουθία πρώτης τάξης.

Ο αριθμός των άσσων και των μηδενικών στο διάνυσμα $\boldsymbol{x}$ είναι ίσος με 2^{n-1} και $2^{n-1} - 1$ αντίστοιχα [33]. Γενικότερα, ισοβαρείς ονομάζονται οι ακολουθίες των οποίων το πλήθος των άσσων και μηδενικών, σε μία περίοδο, διαφέρουν το πολύ κατά ένα.

Ιδιότητα 3.12. Η ακολουθία μεγίστου μήκους x είναι *ισοβαρής* ακολουθία τάξης n, όπου n είναι ο βαθμός του ελαχίστου πολυωνύμου $f(z)$ της x.

Ας θεωρήσουμε τον ακέραιο k ο οποίος είναι μικρότερος ή ίσος του n. Ορίζουμε μία *συμβολοσειρά μήκους* k ως τη σειρά k συνεχόμενων ψηφίων της x (για δυαδικές ακολουθίες τα ψηφία είναι τα 0 και 1). Υπάρχουν 2^k διαφορετικές συμβολοσειρές μήκους k, ιδιαίτερες περιπτώσεις των οποίων αποτελούν η μοναδιαία και η μηδενική συμβολοσειρά. Ο αριθμός εμφάνισης κάθε μη–μηδενικής

συμβολοσειράς μήκους k είναι ίσος με 2^{n-k}, ενώ της μηδενικής συμβολοσειράς $2^{n-k}-1$ [33], [84].

Ιδιότητα 3.13. Η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας μεγίστου μήκους x παράγει μία ακολουθία πραγματικών αριθμών που προσομοιάζει τον παλμό Dirac.

Από τις Ιδιότητες 3.9 και 3.11 συμπεραίνουμε ότι οι ακολουθίες μεγίστου μήκους χαρακτηρίζονται από τη σχέση

$$\mathrm{AC}_x(t) = \begin{cases} 1 & \text{εαν } t \equiv 0 \pmod N, \\ -1/N & \text{διαφορετικά.} \end{cases} \tag{3.30}$$

Η Ιδιότητα 3.13 των ακολουθιών μεγίστου μήκους είναι γνωστή ως ιδιότητα *ιδανικής αυτοσυσχέτισης*. Είναι γνωστή στη βιβλιογραφία η αντιστοιχία μεταξύ των ακολουθιών με ιδανική αυτοσυσχέτιση και των *κυκλικών συνόλων διαφορών Hadamard* [36].

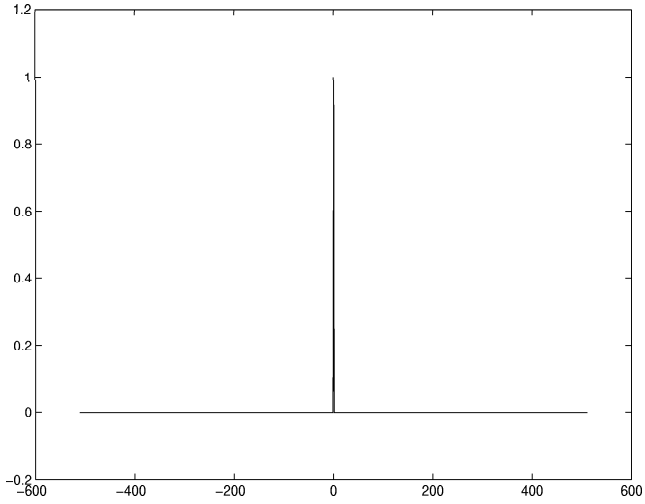
Παράδειγμα 3.14. Η ακολουθία αυτοσυσχέτισης της ακολουθίας μεγίστου μήκους με ελάχιστη περίοδο 1023 και ελάχιστο πολυώνυμο $f(z) = 1 + z^3 + z^{10}$ δίνεται στο Σχ. 3.3, όπου έγινε χρήση της ιδιότητας $\mathrm{AC}_x(-t) = \mathrm{AC}_x(N-t)$. □

Οι Ιδιότητες 3.11–3.13 είναι γνωστές ως *αξιώματα τυχαιότητας* του Golomb [33]. Άλλες ιδιότητες τυχαιότητας ακολουθιών παραγόμενων από καταχωρητές ολίσθησης γραμμικής ανάδρασης αφορούν τις κατανομές συμβολοσειρών μήκους μεγαλυτέρου του βαθμού του ελαχίστου πολυωνύμου [26], [74], τις ροπές μερικής περιόδου ακολουθιών αυτοσυσχέτισης [69], [92], τη δειγματοληψία [106], [107], και τη γραμμική πολυπλοκότητα (*βλ.* Κεφάλαιο 4) [5], [64], [80].

3.6.1 Δειγματοληψία ακολουθιών

Ας θεωρήσουμε το θετικό ακέραιο d και έστω $y = x[d]$ είναι η περιοδική δυαδική ακολουθία που παράγεται από τη δειγματοληψία με παράγοντα d της ακολουθίας μεγίστου μήκους x, ελαχίστης περιόδου N, και με ελάχιστο πολυώνυμο $f(z)$.

Έστω $g(z)$ είναι το ελάχιστο πολυώνυμο της ακολουθίας y. Τότε, οι ρίζες του $g(z)$ είναι η d–στή δύναμη των ριζών του πολυωνύμου $f(z)$. Επιπλέον, η ακολουθία y έχει ελάχιστη περίοδο $N/\gcd(N,d)$. Έαν οι ακέραιοι d και N είναι σχετικά πρώτοι μεταξύ τους, τότε η y είναι επίσης ακολουθία μεγίστου μήκους



Σχήμα 3.3. Η συνάρτηση αυτοσυσχέτισης της ακολουθίας x με ελάχιστο πολυώνυμο $f(z) = 1 + z^3 + z^{10}$

και ο ακέραιος d ονομάζεται *γνήσιος παράγοντας δειγματοληψίας* της ακολουθίας x [33], [72]. Στη συγκεκριμένη περίπτωση, λόγω της Ιδιότητας 3.8, συμπεραίνουμε ότι σε όποια φάση της ακολουθίας x κι αν εφαρμόσουμε δειγματοληψία το αποτέλεσμα είναι πάντα μία διαφορετική φάση της y.

Παράδειγμα 3.15. Έστω $\alpha, \alpha^3 \in \mathbb{F}_{2^n}$ είναι οι ρίζες των πολυωνύμων $f(z)$ και $g(z)$ αντίστοιχα. Τότε, η ακολουθία y λαμβάνεται από την x εφαρμόζοντας δειγματοληψία με παράγοντα 3.

Η y έχει ελάχιστη περίοδο N, δηλ. είναι ακολουθία μεγίστου μήκους, έαν ο ακέραιος n είναι περιττός, ενώ έχει ελάχιστη περίοδο $N/3$ έαν ο ακέραιος n είναι άρτιος. Και στις δύο περιπτώσεις ο βαθμός του ελαχίστου πολυωνύμου $g(z)$ της ακολουθίας y είναι ίσος με n. □

3.7 Γραμμική πολυπλοκότητα ακολουθιών

Ο χαρακτηρισμός μίας δοθείσας ακολουθίας x στοιχείων του $\mathbb{F}_2$ ως γραμμικά αναδρομικής είναι σημαντικό πρόβλημα. Επιτυγχάνεται κυρίως μέσω εύρεσης

του ελαχίστου πολυωνύμου $f(z)$ της ακολουθίας x ή ισοδύναμα της αναδρομικής σχέσης που ικανοποιείται από αυτή. Ένα από τα βασικά χαρακτηριστικά μίας ακολουθίας είναι η *γραμμική πολυπλοκότητα*, η οποία αποτελεί επίσης μέτρο ανθεκτικότητας της ακολουθίας σε επιθέσεις κρυπτανάλυσης [19], [23], [104], όπως ο αλγόριθμος των Berlekamp–Massey.

Ορισμός 3.16. Η γραμμική πολυπλοκότητα L_x της ακολουθίας x ορίζεται ως η τάξη της ελαχίστου βαθμού ομογενούς γραμμικά αναδρομικής σχέσης που ικανοποιεί η x.

Συνεπώς, η γραμμική πολυπλοκότητα L_x της ακολουθίας x είναι ίση με τον ελάχιστο αριθμό διαδοχικών όρων της x που απαιτούνται για το γραμμικό προσδιορισμό όλων των όρων της ακολουθίας [91]. Στη συνέχεια, παρέχουμε πλήθος ιδιοτήτων οι οποίες συνδέουν τη γραμμική πολυπλοκότητα με τις αναπαραστάσεις ακολουθιών των προηγούμενων ενοτήτων [80], [84].

Ιδιότητα 3.17. Έστω x και y *πεπερασμένες* δυαδικές ακολουθίες μήκους N. Τότε, ισχύουν τα ακόλουθα:

i. Για κάθε $N \geq 1$, η γραμμική πολυπλοκότητα της ακολουθίας x ικανοποιεί την ανισότητα $0 \leq L_x \leq N$.

ii. $L_x = 0$ έαν και μόνον έαν η x είναι η μηδενική ακολουθία.

iii. $L_x = N$ έαν και μόνον έαν η x είναι η ακολουθία $0, \ldots, 0, 1$.

iv. Έαν η ακολουθία x είναι περιοδική με περίοδο N, τότε $L_x \leq N$.

v. $L_{x+y} \leq L_x + L_y$, όπου $x + y$ η πρόσθεση (modulo 2) των ακολουθιών x και y.

Ιδιότητα 3.18. Η γραμμική πολυπλοκότητα L_x της ακολουθίας x είναι ίση με το βαθμό του ελαχίστου πολυωνύμου $f(z)$, δηλ. $L_x = \deg(f(z))$.

Ιδιότητα 3.19. Οι ακολουθίες που παράγονται από έναν καταχωρητή ολίσθησης γραμμικής ανάδρασης, με πρωταρχικό πολυώνυμο ανάδρασης βαθμού n, έχουν γραμμική πολυπλοκότητα n.

Ιδιότητα 3.20. Η γραμμική πολυπλοκότητα L_x της δυαδικής ακολουθίας x είναι ίση με τον αριθμό των μη–μηδενικών στοιχείων του διακριτού μετασχηματισμού Fourier X της x [8], [9], [81], [104].

Έστω ότι η ακολουθία x επιλέγεται *τυχαία* από το σύνολο όλων των πεπερασμένων δυαδικών ακολουθιών μήκους N. Επιπλέον, ας θεωρήσουμε τη συνάρτηση $p(n) = n \bmod 2$. Οι παρακάτω ιδιότητες παρέχουν χρήσιμες πληροφορίες ως προς τη γραμμική πολυπλοκότητα τυχαίων ακολουθιών.

Ιδιότητα 3.21. Η αναμενόμενη γραμμική πολυπλοκότητα της τυχαίας πεπερασμένης δυαδικής ακολουθίας x μήκους N είναι [84], [102]

$$\mathrm{E}(L_x) = \frac{N}{2} + \frac{4 + p(N)}{18} - \frac{1}{2^N}\Big(\frac{N}{3} + \frac{2}{9}\Big). \tag{3.31}$$

Για μεγάλα μήκη N, ισχύει $\mathrm{E}(L_x) \approx (9N+4)/18$, έαν το N είναι άρτιος ακέραιος, και $\mathrm{E}(L_x) \approx (9N+5)/18$, έαν το N είναι περιττός ακέραιος.

Ιδιότητα 3.22. Η διακύμανση στη γραμμική πολυπλοκότητα της τυχαίας πεπερασμένης δυαδικής ακολουθίας x μήκους N είναι [84], [102]

$$\mathrm{Var}(L_x) = \frac{86}{81} - \frac{1}{2^N}\Big(\frac{14 - p(N)}{27}N + \frac{82 - 2p(N)}{81}\Big) - \frac{1}{2^{2N}}\Big(\frac{1}{9}N^2 + \frac{4}{27}N + \frac{4}{81}\Big). \tag{3.32}$$

Για μεγάλα μήκη N, ισχύει $\mathrm{Var}(L_x) \approx 86/81$.

Διάφορες μέθοδοι είναι γνωστές στη βιβλιογραφία, και οι οποίες χρησιμοποιούν τεχνικές από τη γραμμική Άλγεβρα, για τον υπολογισμό της γραμμικής πολυπλοκότητας. Παράδειγμα αποτελούν οι ορίζουσες Hankel, που δίνονται από τη σχέση

$$\boldsymbol{H}_j^{(n)} = \begin{vmatrix} x_j & x_{j+1} & \cdots & x_{j+n-1} \\ x_{j+1} & x_{j+2} & \cdots & x_{j+n} \\ \vdots & \vdots & & \vdots \\ x_{j+n-1} & x_{j+n} & \cdots & x_{j+2n-2} \end{vmatrix}. \tag{3.33}$$

Βασικό χαρακτηριστικό των συγκεκριμένων μεθόδων είναι ο μηδενισμός ενός αριθμού οριζουσών Hankel, για διάφορες τιμές των j και n [46], [72].

Μεταξύ αυτών των μεθόδων είναι και ο αλγόριθμος των Berlekamp–Massey [50], ο οποίος απεικονίζεται στο Σχ. 3.4. Ο αλγόριθμος πραγματοποιεί N επαναλήψεις, και στην επανάληψη j υπολογίζει τον καταχωρητή ολίσθησης γραμμικής ανάδρασης που παράγει την υπο–ακολουθία $x_0, x_1, \ldots, x_j$. Ο ακέραιος n είναι το τρέχον μήκος του καταχωρητή, και $g(z)$ το αντίστοιχο πολυώνυμο

set $n = 0$
set $g(z) = 1$
set $h(z) = 1$

for $j = 0, \ldots, N-1$ **do**
    set $d = x_j + g_1 x_{j-1} + \cdots + g_n x_{j-n}$

    if $d = 1$ **and** $2n \leq j$ **then**
        set $\delta = 1$
    else
        set $\delta = 0$
    endif

    set $\begin{pmatrix} g(z) \\ h(z) \end{pmatrix} = \begin{pmatrix} 1 & dz \\ d\delta & (1-\delta)z \end{pmatrix} \begin{pmatrix} g(z) \\ h(z) \end{pmatrix}$

    set $n = \delta(j-n) + (1-\delta)n$
endfor

Σχήμα 3.4. Ο αλγόριθμος των Berlekamp–Massey για δυαδικές ακολουθίες

ανάδρασης, δηλ. $f(z) = g^*(z)$. Η υπολογιστική πολυπλοκότητα του αλγορίθμου Berlekamp–Massey είναι $O(N^2)$.

Ο αλγόριθμος Berlekamp–Massey [5], [80], είναι ίσως η πιο γνωστή επίθεση κρυπτανάλυσης μέχρι σήμερα. Χρειάζεται $2N$ στοιχεία από την ακολουθία για τον καθορισμό του L_x και του καταχωρητή ολίσθησης γραμμικής ανάδρασης που αντιστοιχεί στην ελαχίστου βαθμού ομογενή γραμμική επαναληπτική σχέση [80].

Η γραμμική πολυπλοκότητα L_x και ο καταχωρητής ολίσθησης γραμμικής ανάδρασης που παράγει μία πεπερασμένη ακολουθία x μήκους N, είναι δυνατό να υπολογιστούν και με άλλους αλγορίθμους, όπως ο αλγόριθμος του Ευκλείδη, η επέκταση συνεχών κλασμάτων, κ.λπ. Η ισοδυναμία των συγκεκριμένων αλγορίθμων με τον αλγόριθμο των Berlekamp–Massey έχει μελετηθεί στις αναφορές [13], [21], [121].

Εκτός των εφαρμογών που βρίσκει στην κρυπτογραφία, ο αλγόριθμος των Berlekamp–Massey χρησιμοποιείται ευρέως στους κώδικες ελέγχου σφαλμάτων [24], [93], [94], [123].

Κεφάλαιο 4

Ακολουθίες με μη–γραμμικά χαρακτηριστικά

Τα χαρακτηριστικά τυχαίου θορύβου που επιδεικνύουν οι ακολουθίες που παράγονται από καταχωρητές ολίσθησης γραμμικής ανάδρασης, δεν αρκούν για να εξασφαλίσουν υψηλή μη–γραμμικότητα, εκτός έαν γίνει χρήση καταχωρητών μεγάλου μήκους. Για τη βελτίωση της γραμμικής πολυπλοκότητας των παραγόμενων ακολουθιών είναι αναγκαία η χρήση μη–γραμμικών δομών. Αυτή η ανάγκη έγινε αντιληπτή από μεγάλο πλήθος ερευνητών, μεταξύ των οποίων ο Groth [42], και ο Key [56].

Ο Key μελέτησε το γινόμενο (όρο–προς–όρο) ακολουθιών που λαμβάνονται από διαφορετικές βαθμίδες ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης, δίνοντας ιδιαίτερη βαρύτητα σε γινόμενα δευτέρου βαθμού. Ο καθορισμός του ελαχίστου πολυωνύμου μιας ακολουθίας είναι ισοδύναμος με την εύρεση της γραμμικής της πολυπλοκότητας. Αυτό το πρόβλημα έχει διερευνηθεί στα πλαίσια ενός πεπερασμένου σώματος από [40], [41], [82], και [126]. Τεχνικές βασιζόμενες στο *διακριτό μετασχηματισμό Fourier* εφαρμόστηκαν στο [81], σε δευτέρου βαθμού γινόμενα ακολουθιών παραγόμενων από τον ίδιο καταχωρητή ολίσθησης γραμμικής ανάδρασης.

Συναρτήσεις που δέχονται σαν είσοδο στοιχεία ακολουθιών λαμβανόμενα από διαφορετικές βαθμίδες ενός καταχωρητή ολίσθησης, ονομάζονται *μη–γραμμικά φίλτρα*. Παρομοίως, συναρτήσεις που δέχονται σαν είσοδο στοιχεία ακολουθιών λαμβανόμενα από διαφορετικούς καταχωρητές ολίσθησης, ονομάζονται *μη–*

γραμμικοί συνδυαστές. Τεχνικές υπολογισμού της γραμμικής πολυπλοκότητας ακολουθιών που παράγονται από τη δεύτερη κλάση συναρτήσεων αναπτύχθηκαν στα [32], [103]. Ιδιότητες της πρώτης κατηγορίας συναρτήσεων μελετήθηκαν σε βάθος από τον Rueppel στο [102], ο οποίος εξήγαγε κάτω φράγματα σχετικά με τη γραμμική πολυπλοκότητα ακολουθιών που παράγονται από τέτοιες δομές. Επιπρόσθετα, υπολογίζονται οι συντελεστές Fourier που αντιστοιχούν σε στοιχεία πεπερασμένου σώματος των οποίων ο εκθέτης έχει δυαδικό βάρος k, όταν το μη–γραμμικό φίλτρο αποτελείται από ένα μόνο γινόμενο βαθμού k, ή είναι το άθροισμα γινομένων βαθμού k.

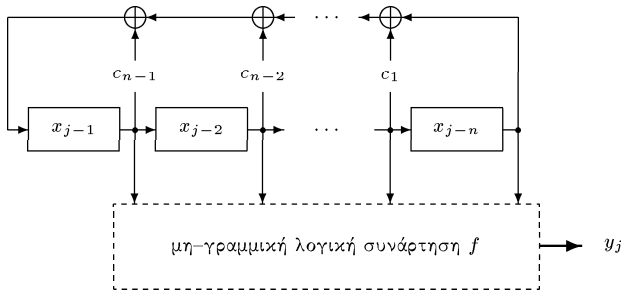
Στο παρόν κεφάλαιο, επεκτείνονται οι τεχνικές που χρησιμοποιήθηκαν στις αναφορές [56] και [102] για την ανάλυση της γραμμικής πολυπλοκότητας ακολουθιών που παράγονται από το μη–γραμμικό φιλτράρισμα *ακολουθιών μεγίστου μήκους*. Δίνονται κλειστοί τύποι υπολογισμού των συντελεστών Fourier όλων των στοιχείων ενός πεπερασμένου σώματος, και για οποιοδήποτε μη–γραμμικό φίλτρο. Σαν αποτέλεσμα, καθίσταται δυνατός ο πλήρης προσδιορισμός της *αναπαράστασης ίχνους* της ακολουθίας εξόδου σε σχέση με το μη–γραμμικό φίλτρο. Επιπρόσθετα, εισάγεται ένας νέος τρόπος επιλογής γινομένων ακολουθιών που λαμβάνονται από διαφορετικές βαθμίδες ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης, έτσι ώστε να εξασφαλίζεται ότι η γραμμική πολυπλοκότητα των γινομένων είναι κάτω φραγμένη από μία συγκεκριμένη ποσότητα. Τέλος, περιγράφονται μέθοδοι για την εύρεση μη–γραμμικών φίλτρων που παράγουν ακολουθίες καθορισμένης γραμμικής πολυπλοκότητας.

4.1 Μη–γραμμικά φίλτρα

Ας θεωρήσουμε τη δυαδική ακολουθία $x = \{x_j\}_{j \geq 0}$ που παράγεται από το μοντέλο Fibonacci (Σχ. 3.2) ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης n βαθμίδων, με πρωταρχικό ελάχιστο πολυώνυμο $c(z)$. Συνεπώς, η ακολουθία x είναι περιοδική, έχοντας τη μέγιστη δυνατή περίοδο $N = 2^n - 1$, και στατιστικά τυχαίου θορύβου [71]. Έστω ότι ο j–στός όρος της x δίνεται από τη σχέση

$$x_j = \sum_{m=0}^{n-1} (\beta \alpha^{-j})^{2^m} = \mathrm{tr}_1^n(\beta \alpha^{-j}). \tag{4.1}$$

Οι ακολουθίες που παράγονται από έναν καταχωρητή ολίσθησης γραμμικής ανάδρασης, με πρωταρχικό πολυώνυμο ανάδρασης βαθμού n, έχουν γραμμική πολυ-



Σχήμα 4.1. Το μοντέλο Fibonacci ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης με μη–γραμμική έξοδο

πλοκότητα n. Η γραμμική πολυπλοκότητα των παραγόμενων ακολουθιών μπορεί να ενισχυθεί εφαρμόζοντας μία μη–γραμμική συνάρτηση f, χωρίς μνήμη, στις βαθμίδες ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης [48], όπως φαίνεται στο Σχ. 4.1.

Το μη–γραμμικό φίλτρο f επηρεάζει τόσο τις στατιστικές ιδιότητες και γραμμική πολυπλοκότητα των παραγόμενων ακολουθιών, όσο και την περίοδό τους. Η περίοδος της ακολουθίας εξόδου y είναι διαιρέτης της περιόδου της ακολουθίας x, η οποία καθορίζει τη σειρά διαδοχής των καταστάσεων του καταχωρητή ολίσθησης. Κάθε συνάρτηση που ορίζεται στο χώρο των δυαδικών διανυσμάτων πεπερασμένου μήκους είναι δυνατό να γραφεί σε πολυωνυμική μορφή.

Ορισμός 4.1. Έστω f λογική συνάρτηση n μεταβλητών, με $f(0,\ldots,0)=0$, και ας υποθέσουμε ότι $t \in \mathbb{Z}_{2^n}^*$. Η *κανονική αλγεβρική μορφή* της f ορίζεται ως εξής [4]

$$f(z_1,\ldots,z_n) = \sum_{k=1}^{n} \sum_{\mathrm{wt}(t)=k} r_t z_{t_1} \cdots z_{t_k}, \qquad r_t \in \mathbb{F}_2$$

όπου

$$t = 2^{t_1-1} + \cdots + 2^{t_k-1}, \qquad 1 \le t_1 < \cdots < t_k \le n$$

και $\mathrm{wt}(\cdot)$ συμβολίζει το δυαδικό βάρος. Ο συντελεστής r_t ονομάζεται *δείκτης* του γινομένου $z_{t_1} \cdots z_{t_k}$. Η ακολουθία εξόδου y υπολογίζεται από την x με τη βοήθεια της σχέσης $y_j = f(x_{j-1},\ldots,x_{j-n})$.

Ένα γινόμενο k όρων λέμε ότι είναι γινόμενο βαθμού k. Ο βαθμός της

συνάρτησης f είναι ίσος με το μέγιστο των βαθμών των γινομένων που εμφανίζονται στην κανονική αλγεβρική μορφή της f με μη–μηδενικούς δείκτες. Εάν ο βαθμός της f είναι ίσος με m, τότε η γραμμική πολυπλοκότητα της ακολουθίας y είναι άνω φραγμένη από την ποσότητα [56]

$$L_y \leq \sum_{k=1}^{m} \binom{n}{k}.$$

Στις ακόλουθες ενότητες, δίνουμε ιδιαίτερη έμφαση στην κατασκευή καταχωρητών ολίσθησης γραμμικής ανάδρασης με μη–γραμμικές συναρτήσεις εξόδου που παράγουν ακολουθίες με καθορισμένη γραμμική πολυπλοκότητα.

4.2 Ανάλυση γινομένων ακολουθιών μεγίστου μήκους

Ας θεωρήσουμε την ακολουθία μεγίστου μήκους x η οποία δίνεται από τη σχέση (4.1). Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι η x βρίσκεται στη *χαρακτηριστική της φάση* [33], [71], δηλ. $\beta = 1$. Για την εύρεση μιας συμπαγούς αναπαράστασης της ακολουθίας y, που προκύπτει από την x εφαρμόζοντας το μη–γραμμικό φίλτρο f, θα διερευνήσουμε πρώτα τη συμπεριφορά γινομένων διακριτών φάσεων της x.

Στη συνέχεια, θεωρούμε ότι οι εκθέτες της ρίζας α είναι ισοδύναμοι με το υπόλοιπο της διαίρεσής τους με το N. Συνεπώς, χρησιμοποιούμε α^m και $\alpha^{2^{-m}}$ αντί του $\alpha^{m \bmod N}$, και $\alpha^{2^{n-m}}$ αντίστοιχα. Για τη μελέτη του γινομένου $x_{j-t_1} \cdots x_{j-t_k}$, βαθμού k, ορίζουμε $t = 2^{t_1-1} + \cdots + 2^{t_k-1}$ και $t' = t - 2^{t_k-1}$.

Έστω ότι οι ακέραιοι $i \in \mathbb{Z}_{2^n}^*$ και t έχουν δυαδικό βάρος ένα. Η ακολουθία που ορίζεται από τη σχέση $\{2^m \bmod N\}_{m\geq 0}$ διατρέχει όλα τα στοιχεία της κυκλοτομικής κλάσης C_1, δηλ. όλους τους ακέραιους με δυαδικό βάρος ένα. Συνεπώς, από τη σχέση (4.1) λαμβάνουμε ότι οι γραμμικοί όροι του μη–γραμμικού φίλτρου f έχουν την ακόλουθη μορφή

$$x_{j-t_1} = \sum_{\mathrm{wt}(i)=1} A_1(t,i)\alpha^{-ji} \tag{4.2}$$

όπου $A_1(t,i) = \alpha^{t_1 i}$.

Πίνακας 4.1. Τα ζεύγη (i_1, i_2) που ικανοποιούν τη σχέση $0 \le i_1 < i_2 < n$, ή ισοδύναμα την $\mathrm{wt}(2^{i_1} + 2^{i_2}) = \mathrm{wt}(i) = 2$

$(0,1)$	$(0,2)$	$(0,3)$	$\cdots$	$(0,n-2)$	$(0,n-1)$
	$(1,2)$	$(1,3)$	$\cdots$	$(1,n-2)$	$(1,n-1)$
		$(2,3)$	$\cdots$	$(2,n-2)$	$(2,n-1)$
				$\vdots$	$\vdots$
				$(n-3,n-2)$	$(n-3,n-1)$
					$(n-2,n-1)$

Στη συνέχεια, θα μελετήσουμε τις ιδιότητες των όρων δευτέρου βαθμού του μη–γραμμικού φίλτρου f. Από τη σχέση

$$\begin{aligned} x_{j-t_1}x_{j-t_2} &= \sum_{\mathrm{wt}(i)=1} A_1(t',i)\alpha^{-ji}\sum_{i_2=0}^{n-1}\alpha^{(t_2-j)2^{i_2}} \\ &= \sum_{i_1=0}^{n-1}\sum_{i_2=0}^{n-1}\alpha^{t_1 2^{i_1}+t_2 2^{i_2}}\alpha^{-j(2^{i_1}+2^{i_2})} \end{aligned} \tag{4.3}$$

διαχωρίζοντας τις περιπτώσεις $i_1 \neq i_2$ και $i_1 = i_2$, λαμβάνουμε

$$x_{j-t_1}x_{j-t_2} = \sum_{i_1=0}^{n-2}\sum_{i_2=i_1+1}^{n-1} A_2(t,i)\alpha^{-j(2^{i_1}+2^{i_2})} + \sum_{i_1=0}^{n-1} A_1(t,i)\alpha^{-j2^{i_1+1}}$$

όπου

$$A_2(t,i) = \alpha^{t_1 2^{i_2}+t_2 2^{i_1}} + \alpha^{t_1 2^{i_1}+t_2 2^{i_2}}, \tag{4.4α′}$$

$$A_1(t,i) = \alpha^{(t_1+t_2)2^{i_1}}. \tag{4.4β′}$$

Ως αποτέλεσμα του περιορισμού $0 \le i_1 < i_2 < n$, οι ακέραιοι $i = 2^{i_1} + 2^{i_2}$ διατρέχουν όλα τα στοιχεία του $\mathbb{Z}^*_{2^n}$ με δυαδικό βάρος δύο ($\beta\lambda$. Πίνακα 4.1). Οι όροι δευτέρου βαθμού είναι δυνατό να γραφούν στην ακόλουθη απλούστερη μορφή

$$x_{j-t_1}x_{j-t_2} = \sum_{l=1}^{2}\sum_{\mathrm{wt}(i)=l} A_l(t,i)\alpha^{-j2^{2-l}i}. \tag{4.5}$$

Από τον ορισμό των t, t', οι συντελεστές $A_l(t,i)$ γράφονται συναρτήσει των $A_l(t',i)$ ως εξής

$$A_2(t,i) = A_1(t', i-2^{i_1})\alpha^{t_2 2^{i_1}} + A_1(t', i-2^{i_2})\alpha^{t_2 2^{i_2}}, \tag{4.6α'}$$

$$A_1(t,i) = A_1(t', 2i-2^{i_1})\alpha^{t_2 2^{i_1}}, \tag{4.6β'}$$

επειδή $\mathrm{wt}(i) = 1$. Συνεπώς $i = 2i - i = 2i - 2^{i_1}$.

Παρατήρηση 4.2. Ο δείκτης l του συντελεστή $A_l(t,i)$ είναι μικρότερος ή ίσος από το δυαδικό βάρος του t και συμβολίζει το αναμενόμενο πραγματικό δυαδικό βάρος του ακεραίου i, βάσει του οποίου θα υπολογιστεί ο $A_l(t,i)$.

Παρατήρηση 4.3. Στην περίπτωση που το δυαδικό βάρος του ακέραιου i είναι δύο, τότε οι συντελεστές $A_2(t,i)$, που δίνονται από τη σχέση (4.4α'), είναι καλά ορισμένοι. Αντιθέτως, όταν το δυαδικό βάρος του ακέραιου $i' \in \mathbb{Z}_{2^n}^*$ είναι ένα, με $i' = 2^{i_1} + 2^{i_2}$ και $i_2 = i_1$, τότε έχουμε $A_2(t,i') = 0$.

Παρατήρηση 4.4. Στη συνέχεια της ενότητας, θα θεωρούμε ότι $A_0(t,0) = 0$, για κάθε $t \in \mathbb{Z}_{2^n}^*$, ενώ $A_0(0,0) = 1$.

Για να αναδείξουμε τις ιδιότητες που χαρακτηρίζουν τους συντελεστές $A_l(t,i)$ θα πρέπει να αποδείξουμε πρώτα το ακόλουθο Λήμμα.

Λήμμα 4.5. *Έστω οι θετικοί ακέραιοι k και n, τέτοιοι ώστε $k < n$. Για κάθε $n \geq 2$ ισχύει η σχέση*

$$\frac{2^n - 1}{2^{\gcd(k,n)} - 1} > n.$$

Απόδειξη. Από την υπόθεση έχουμε ότι ο μέγιστος κοινός διαιρέτης των k και n είναι μικρότερος ή ίσος με n/p, όπου $p > 1$ είναι ο μικρότερος πρώτος παράγοντας του n. Σαν αποτέλεσμα έχουμε

$$\frac{2^n - 1}{2^{\gcd(k,n)} - 1} \geq \frac{2^n - 1}{2^{n/p} - 1} = 1 + \sum_{i=1}^{p-1} 2^{(n/p)i}. \tag{4.7}$$

Όμως, είναι γνωστό ότι ισχύει $2^m \geq 2m$ για όλους τους ακέραιους $m \in \mathbb{N}$. Συνεπώς, η σχέση (4.7) οδηγεί στο αποτέλεσμα

$$\frac{2^n - 1}{2^{n/p} - 1} \geq 1 + 2\frac{n}{p}\sum_{i=1}^{p-1} i = 1 + n(p-1). \qquad \square$$

Θεώρημα 4.6. *Ας θεωρήσουμε τους ακέραιους $i \in \mathbb{Z}_{2^n}^*$ των οποίων το δυαδικό βάρος ισούται με l, όπου $1 \leq l \leq 2$. Επιπρόσθετα, θεωρούμε ότι* $\mathrm{wt}(t) = 2$. *Τότε ισχύουν τα ακόλουθα:*

1. $A_l(t,i)^{2^m} = A_l(t, 2^m i \bmod N)$ *για κάθε* $m \geq 0$,
2. $A_l(t,i) \neq 0$ *έαν* $t \in \mathbb{Z}_{2^n}^*$.

Απόδειξη. Η απόδειξη δίνεται στην περίπτωση όπου $l = 2$, αφού όμοια επιχειρήματα ισχύουν και στην περίπτωση όπου $l = 1$.

Καθώς ο ακέραιος $i \in \mathbb{Z}_{2^n}^*$ έχει δυαδικό βάρος δύο, γράφεται ως $i = 2^{i_1} + 2^{i_2}$ με $0 \leq i_1 < i_2 < n$. Είναι σημαντικό ότι η πράξη της ολίσθησης και λήψης του υπολοίπου $i \leftarrow 2^m i \bmod N$ δε μεταβάλλει το δυαδικό βάρος του ακεραίου i. Από τη σχέση (4.4α′) λαμβάνουμε

$$\begin{aligned} A_2(t,i)^{2^m} &= \alpha^{t_1 2^{i_2+m \bmod n} + t_2 2^{i_1+m \bmod n}} + \alpha^{t_1 2^{i_1+m \bmod n} + t_2 2^{i_2+m \bmod n}} \\ &= A_2(t, 2^m i \bmod N). \end{aligned}$$

Για την απόδειξη της Ιδιότητας 1 θεωρήσαμε ότι $i < N$. Στην περίπτωση όπου $i > N$, π.χ. έαν $0 \leq i_1 < n < i_2$, η Ιδιότητα 1 εξακολουθεί να ισχύει χρησιμοποιώντας το $i_2 - n$ αντί του i_2.

Τέλος, έστω $A_2(t,i) = 0$. Από τον περιορισμό $0 < i_2 - i_1 < n$, λαμβάνουμε τη γραμμική ισοδυναμία

$$(t_2 - t_1)(2^{i_2 - i_1} - 1) \equiv 0 \pmod{N}.$$

Από το Λήμμα 2.53, ο μέγιστος κοινός διαιρέτης των $2^{i_2-i_1} - 1$ και N είναι ίσος με $2^{\gcd(i_2-i_1,n)} - 1$. Συνεπώς, η ανωτέρω γραμμική ισοδυναμία οδηγεί στη σχέση

$$N' = \frac{N}{2^{\gcd(i_2-i_1,n)} - 1} \mid t_2 - t_1. \tag{4.8}$$

Όμως από την υπόθεση έχουμε ότι $1 \leq t_1 < t_2 \leq n$, απ′ όπου παίρνουμε τον περιορισμό $t_2 - t_1 < n$. Από το Λήμμα 4.5 ισχύει $N' > n > t_2 - t_1$, και τελικώς η σχέση (4.8) οδηγεί σε άτοπο. Συνεπώς ισχύει $A_2(t,i) \neq 0$. □

Στο Κεφάλαιο 3 σημειώθηκε ότι η γραμμική πολυπλοκότητα της περιοδικής ακολουθίας y είναι ίση με το βάρος Hamming του διακριτού μετασχηματισμού

Fourier Y της y. Έαν η ακολουθία y δίνεται από τη σχέση $y_j = x_{j-t_1}x_{j-t_2}$, τότε από την (4.5) λαμβάνουμε ότι ο m–στός όρος της Y δίνεται από

$$Y_m = \begin{cases} A_{\mathrm{wt}(m)}(t,m)^{2^{\mathrm{wt}(m)-2}} & \text{έαν } 1 \le \mathrm{wt}(m) \le 2, \\ 0 & \text{διαφορετικά.} \end{cases} \tag{4.9}$$

Το σύνολο $\mathbb{Z}_N$ περιέχει $\binom{n}{1}$ και $\binom{n}{2}$ ακεραίους με δυαδικό βάρος ένα και δύο αντίστοιχα. Από το Θεώρημα 4.6 και τη σχέση (4.9) λαμβάνουμε το ακόλουθο αποτέλεσμα, το οποίο διατύπωσε και απέδειξε πρώτος ο Key [56].

Πόρισμα 4.7. *Ας θεωρήσουμε την ακολουθία μεγίστου μήκους $x = \{x_j\}_{j\ge 0}$ περιόδου $2^n - 1$, και τους ακέραιους t_1, t_2, τέτοιοι ώστε $1 \le t_1 < t_2 \le n$. Το γινόμενο δευτέρου βαθμού $x_{j-t_1}x_{j-t_2}$ έχει τη μέγιστη δυνατή τιμή $\binom{n}{1} + \binom{n}{2}$ της γραμμικής πολυπλοκότητας.*

Στο Θεώρημα 4.6, η υπόθεση ότι οι ακέραιοι t_1, t_2 λαμβάνουν τιμές στο σύνολο $\{1, \ldots, n\}$, έπαιξε καθοριστικό ρόλο ώστε να αποδειχθεί ότι οι συντελεστές $A_l(t,i)$, με $1 \le l \le 2$, δε μηδενίζονται. Έαν εξαλειφθεί αυτός ο περιορισμός, τότε είναι δυνατό να συμβούν εκφυλισμοί, όπως φαίνεται στο ακόλουθο παράδειγμα [102, Κεφ. 5].

Παράδειγμα 4.8. Έστω ότι η ακολουθία μεγίστου μήκους x δίνεται από τη σχέση $x_j = \mathrm{tr}_1^4(\alpha^{-j})$, όπου το $\alpha \in \mathbb{F}_{2^4}$ είναι πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^4}$ και ικανοποιεί τη σχέση $\alpha^4 = \alpha + 1$. Ας θεωρήσουμε το γινόμενο

$$y_j = x_j x_{j-5}.$$

Τότε, με τη βοήθεια του αλγορίθμου Berlekamp–Massey βρίσκουμε ότι η γραμμική πολυπλοκότητα της ακολουθίας y είναι ίση με $L_y = 8 < 10$. □

Σε αντίθεση με τα δευτέρου βαθμού γινόμενα διακριτών φάσεων της μεγίστου μήκους ακολουθίας x, δεν είναι δυνατό να διασφαλιστεί ότι τα γινόμενα τρίτου βαθμού $x_{j-t_1}x_{j-t_2}x_{j-t_3}$ θα έχουν τη μέγιστη δυνατή γραμμική πολυπλοκότητα $\binom{n}{1}+\binom{n}{2}+\binom{n}{3}$ έαν οι ακέραιοι t_1, t_2, t_3 λαμβάνουν τιμές από το σύνολο $\{1, \ldots, n\}$. Για το λόγο αυτό παραθέτουμε το ακόλουθο Παράδειγμα.

Παράδειγμα 4.9. Έστω ότι η ακολουθία μεγίστου μήκους x δίνεται από τη σχέση $x_j = \mathrm{tr}_1^4(\alpha^{-j})$, όπου το $\alpha \in \mathbb{F}_{2^4}$ είναι πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^4}$ και ικανοποιεί τη σχέση $\alpha^4 = \alpha + 1$. Ας θεωρήσουμε το

γινόμενο

$$y_j = x_{j-1}x_{j-2}x_{j-4}.$$

Τότε, με τη βοήθεια του αλγορίθμου Berlekamp–Massey βρίσκουμε ότι η γραμμική πολυπλοκότητα της ακολουθίας y είναι ίση με $L_y = 10 < 14$. □

Στη συνέχεια, γενικεύουμε τα ανωτέρω αποτελέσματα σε γινόμενα οποιασδήποτε τάξης $k \leq n$.

Θεώρημα 4.10. *Ας θεωρήσουμε τους ακεραίους $i, t' \in \mathbb{Z}_{2^n}^*$ και έστω ότι ο ακέραιος l ορίζεται έτσι ώστε να ισχύει $1 \leq \mathrm{wt}(i) \leq l \leq \mathrm{wt}(t') = r$. Εαν οι συντελεστές $A_l(t', i)$ ικανοποιούν τις συνθήκες*

1. *$A_l(t', i)^{2^m} = A_l(t', 2^m i \bmod N)$ για κάθε $m \geq 0$,*
2. *$A_l(t', i) = 0$ έαν $\mathrm{wt}(i) < l$,*

τότε, για κάθε $1 \leq l \leq r$, η παράσταση

$$D_r(l,t) = \left(\sum_{\mathrm{wt}(i)=l} A_l(t', i)^{2^{l-r}} \alpha^{-ji} \right) \left(\sum_{i_{l+1}=0}^{n-1} \alpha^{(t_{r+1}-j)2^{i_l+1}} \right)$$

υπολογίζεται από τη σχέση

$$D_r(l,t) = \sum_{s=1}^{l+1} \sum_{\mathrm{wt}(i)=s} \left(\sum_{e=1}^{s} A_l(t', 2^{l+1-s}i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-j2^{l+1-s}i}.$$

Απόδειξη. Θα χειριστούμε τις περιπτώσεις $i_{l+1} \neq i_1, \ldots, i_l$ και $i_{l+1} = i_1, \ldots, i_l$ ανεξάρτητα. Από την υπόθεση, η παράσταση $D_r(l,t)$ είναι δυνατό να γραφεί στην ακόλουθη μορφή

$$\begin{aligned} D_r(l,t) = &\sum_{\mathrm{wt}(i)=l} \sum_{i_{l+1} \neq i_1, \ldots, i_l} A_l(t', i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_l+1}} \alpha^{-j(i+2^{i_l+1})} \\ &+ \sum_{e=1}^{l} \sum_{\mathrm{wt}(i)=l} A_l(t', i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \alpha^{-j(i+2^{i_e})}. \end{aligned}$$

Πρώτα θα μελετήσουμε την περίπτωση όπου ισχύει $i_{l+1} \neq i_1, \ldots, i_l$. Ως αποτέλεσμα, το δυαδικό βάρος του ακέραιου $i + 2^{i_l+1}$ είναι ίσο με $l+1$. Στην περίπτωση αυτή, είναι δυνατές οι εξής $l+1$ διατάξεις

$$0 \leq i_1 < \cdots < i_l < i_{l+1} < n,$$

$$
\begin{gathered}
0 \le i_1 < \cdots < i_{l+1} < i_l < n, \\
\vdots \\
0 \le i_1 < i_{l+1} < \cdots < i_l < n, \\
0 \le i_{l+1} < i_1 < \cdots < i_l < n.
\end{gathered}
$$

Όλες οι διατάξεις, εκτός από την πρώτη, υποβάλλονται στις αντίστοιχες αλλαγές μεταβλητών

$$
\begin{gathered}
i_l \leftarrow i_{l+1}, i_{l+1} \leftarrow i_l, \\
\vdots \\
i_2 \leftarrow i_3, \ldots, i_l \leftarrow i_{l+1}, i_{l+1} \leftarrow i_2, \\
i_1 \leftarrow i_2, \ldots, i_l \leftarrow i_{l+1}, i_{l+1} \leftarrow i_1,
\end{gathered}
$$

όπου $a \leftarrow b$ συμβολίζει ότι αντικαθίσταται κάθε εκδοχή του a με το b. Αυτό μας επιτρέπει να φέρουμε την παράσταση $D_r(l,t)$ στη μορφή

$$
\begin{aligned}
D_r(l,t) = & \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \right) \alpha^{-ji} \\
& + \sum_{e=1}^{l} \sum_{\mathrm{wt}(i)=l} A_l(t', i)^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \alpha^{-j(i+2^{i_e})}. \qquad (4.10)
\end{aligned}
$$

Ανάλογα με την τιμή της μεταβλητής e, είναι δυνατόν ο ακέραιος $i + 2^{i_e}$ να έχει δυαδικό βάρος ίσο ή μικρότερο του $l-1$ έαν ο ακέραιος $i \in \mathbb{Z}_{2^n}^*$, με δυαδικό βάρος l, έχει δύο ή περισσότερους αντίστοιχα συνεχόμενους άσσους $(\mathrm{mod}\ N)$ στη δυαδική του αναπαράσταση.

Στη συνέχεια, θα ακολουθήσουμε μία σειρά από βήματα, τα οποία θα περιλαμβάνουν κατάλληλες ανταλλαγές όρων μεταξύ των αθροισμάτων που εμπλέκονται στη δεύτερη παράσταση από το δεξιό μέρος της σχέσης (4.10), ώστε να υπερνικήσουμε αυτό το εμπόδιο. Ας ορίσουμε το σύνολο J^0, το οποίο περιέχει ακεραίους $i \in \mathbb{Z}_{2^n}^*$ με δυαδικό βάρος l, ως εξής

$$
\begin{aligned}
J^0 &= \{2^{i_1} + \cdots + 2^{i_l} |\ 0 \le i_1 < \cdots < i_l < n\} \qquad (4.11\alpha') \\
&= \{0 \le i_1 < \cdots < i_l < n\}. \qquad (4.11\beta')
\end{aligned}
$$

Η σχέση (4.11β′) θα χρησιμοποιείται αντί της (4.11α′) έαν είναι εμφανές από τα συμφραζόμενα ότι πραγματεύονται ακέραιοι με δυαδικό βάρος l. Παρομοίως, η (4.11β′) θα χρησιμοποιείται όταν πραγματεύονται ακέραιοι με δυαδικό βάρος μικρότερο του l, τους οποίους όμως γράφουμε ως άθροισμα l δυνάμεων του 2. Συνεπώς, η σχέση (4.10) γράφεται ως εξής

$$D_r(l,t) = \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i-2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-ji} + \sum_{e=1}^{l} \sum_{i \in J^0} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \alpha^{-j(i+2^{i_e})}. \tag{4.12}$$

Ορίζουμε τα σύνολα

$$\begin{aligned} J_2^1 &= \{0 \le i_1 \le i_2 < \cdots < i_l < n\} \\ &= \{0 < i_1 \le i_2 < \cdots < i_l < n\} \cup \{i_1 = 0, 0 \le i_2 < \cdots < i_l < n\} \\ &= J_{2,a}^1 \cup J_{2,b}^1, \\ &\vdots \\ J_l^1 &= \{0 \le i_1 < \cdots < i_{l-1} \le i_l < n\} \\ &= \{0 < i_1 < \cdots < i_{l-1} \le i_l < n\} \cup \{i_1 = 0, 0 < i_2 < \cdots < i_{l-1} \le i_l < n\} \\ &= J_{l,a}^1 \cup J_{l,b}^1. \end{aligned}$$

Τα σύνολα $J_2^1, \ldots, J_l^1$ περιέχουν ακεραίους με δυαδικό βάρος ίσο ή μικρότερο του l. Επειδή για τους ακεραίους με δυαδικό βάρος μικρότερο του l ισχύει $A_l(t',i) = 0$ εξ′ υποθέσεως, η (4.12) οδηγεί στο εξής αποτέλεσμα

$$\begin{aligned} D_r(l,t) &= \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i-2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-ji} \\ &\quad + \sum_{e=2}^{l} \sum_{i \in J_e^1} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \alpha^{-j(i+2^{i_e})} \\ &\quad + \sum_{i \in J^0} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_1}} \alpha^{-j(i+2^{i_1})} \\ &= \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i-2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-ji} \end{aligned}$$

$$+\sum_{e=2}^{l}\sum_{i\in J^1_{e,a}} A_l(t',i)^{2^{l-r}}\alpha^{t_{r+1}2^{i_e}}\alpha^{-j(i+2^{i_e})}$$
$$+\sum_{e=2}^{l}\sum_{i\in J^1_{e,b}} A_l(t',i)^{2^{l-r}}\alpha^{t_{r+1}2^{i_e}}\alpha^{-j(i+2^{i_e})}$$
$$+\sum_{i\in J^0} A_l(t',i)^{2^{l-r}}\alpha^{t_{r+1}2^{i_1}}\alpha^{-j(i+2^{i_1})}.$$

Εφαρμόζουμε τις αλλαγές μεταβλητών

$$i_1 \leftarrow i_2,\ldots,i_{l-1}\leftarrow i_l, i_l \leftarrow i_1+n \tag{4.13}$$

στην τρίτη παράσταση από το δεξιό μέρος του $D_r(l,t)$. Οι ανωτέρω αλλαγές μεταβλητών επηρεάζουν και τον τρόπο με τον οποίο ορίζονται τα σύνολα $J^1_{e,b}$, όπου $e=2,\ldots,l$. Έστω ότι ορίζουμε ως $J^2_{e-1,b}$ το αποτέλεσμα εφαρμογής της (4.13) στα σύνολα $J^1_{e,b}$, δηλαδή

$$J^2_{1,b} = \{0\le i_1<\cdots<i_{l-1}<n, i_l=n\},$$
$$\vdots$$
$$J^2_{l-1,b} = \{0< i_1<\cdots<i_{l-2}\le i_{l-1}<n, i_l=n\}.$$

Εξ' υποθέσεως, ισχύει $A_l(t',i)=A_l(t',i \bmod N)$ αφού $\mathrm{wt}(t')=r$. Συνεπώς

$$\sum_{i\in J^2_{e-1,b}} A_l(t',i)^{2^{l-r}}\alpha^{t_{r+1}2^{i_e-1}}\alpha^{-j(i+2^{i_e-1})}$$
$$=\sum_{i\in J^1_{e,b}} A_l(t',i)^{2^{l-r}}\alpha^{t_{r+1}2^{i_e}}\alpha^{-j(i+2^{i_e})}$$

για όλες τις τιμές $e=2,\ldots,l$. Σαν αποτέλεσμα, το $D_r(l,t)$ γράφεται ως εξής

$$D_r(l,t)=\sum_{\mathrm{wt}(i)=l+1}\left(\sum_{e=1}^{l+1} A_l(t',i-2^{i_e})^{2^{l-r}}\alpha^{t_{r+1}2^{i_e}}\right)\alpha^{-ji}$$
$$+\sum_{e=2}^{l}\sum_{i\in J^1_{e,a}} A_l(t',i)^{2^{l-r}}\alpha^{t_{r+1}2^{i_e}}\alpha^{-j(i+2^{i_e})}$$
$$+\sum_{e=1}^{l-1}\sum_{i\in J^2_{e,b}} A_l(t',i)^{2^{l-r}}\alpha^{t_{r+1}2^{i_e}}\alpha^{-j(i+2^{i_e})}$$

$$
\begin{aligned}
&+ \sum_{i\in J^0} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_1}} \alpha^{-j(i+2^{i_1})} \\
&= \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i-2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-ji} \\
&+ \sum_{i\in J^1_{l,a}} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_l}} \alpha^{-j(i+2^{i_l})} \\
&+ \sum_{e=2}^{l-1} \sum_{i\in J^1_{e,a}\cup J^2_{e,b}} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \alpha^{-j(i+2^{i_e})} \\
&+ \sum_{i\in J^0\cup J^2_{1,b}} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_1}} \alpha^{-j(i+2^{i_1})} \\
&= \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i-2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-ji} \\
&+ \sum_{i\in J^1_{l,a}} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_l}} \alpha^{-j(i+2^{i_l})} \\
&+ \sum_{e=1}^{l-1} \sum_{i\in J^3_e} A_l(t',i)^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \alpha^{-j(i+2^{i_e})}
\end{aligned}
$$

όπου $J^3_1 = J^0 \cup J^2_{1,b}$, και $J^3_e = J^1_{e,a} \cup J^2_{e,b}$ για όλες τις τιμές $e = 2, \ldots, l-1$. Πιο συγκεκριμένα, έχουμε ότι

$$
\begin{aligned}
J^3_1 &= \{0 \le i_1 < \cdots < i_l \le n\}, \\
&\vdots \\
J^3_{l-1} &= \{0 < i_1 < \cdots < i_{l-2} \le i_{l-1} < i_l \le n\}.
\end{aligned}
$$

Για όλες τις τιμές $e = 1, \ldots, l-1$, οι ακέραιοι που περιέχονται στο σύνολο J^3_e ικανοποιούν τη σχέση $i_e < i_{e+1}$, ή ισοδύναμα την $i_e + 1 \le i_{e+1}$. Κατά συνέπεια, έαν ο ακέραιος $i \in J^3_e$ είναι τέτοιος ώστε να ισχύει $i_{e+1} = i_e + 1$, τότε ο ακέραιος $i + 2^{i_e}$ έχει δυαδικό βάρος μικρότερο του l. Έαν χειριστούμε ανεξάρτητα τις προαναφερθείσες περιπτώσεις, τότε τα σύνολα $J^3_1, \ldots, J^3_{l-1}$ γράφονται στην ακόλουθη μορφή

$$
J^3_1 = \{0 < i_1 + 1 < i_2 < \cdots < i_l \le n\}
$$

$$
\begin{aligned}
&\cup \{0 < i_1 + 1 < i_3 < \cdots < i_l \leq n, i_2 = i_1 + 1\} \\
&= J^3_{1,a} \cup J^3_{1,b}, \\
&\quad \vdots \\
J^3_{l-1} &= \{0 < i_1 < \cdots < i_{l-2} < i_{l-1} + 1 < i_l \leq n\} \\
&\quad \cup \{0 < i_1 < \cdots < i_{l-2} < i_{l-1} + 1 \leq n, i_l = i_{l-1} + 1\} \\
&\quad = J^3_{l-1,a} \cup J^3_{l-1,b}.
\end{aligned}
$$

Από την παρατήρηση ότι ισχύει

$$J^1_{l,a} = \{0 < i_1 < \cdots < i_{l-1} \leq i_l < n\} = \{0 < i_1 < \cdots < i_{l-1} < i_l + 1 \leq n\}$$

θέτουμε $J^3_{l,a} \triangleq J^1_{l,a}$. Επιπρόσθετα, παρατηρούμε ότι το σύνολο $J^3_{e,a}$ περιέχει όλους τους ακεραίους $i = 2^{i_1} + \cdots + 2^{i_{e-1}} + 2^{i_e} + 2^{i_{e+1}} + \cdots + 2^{i_l}$ που ικανοποιούν τη σχέση

$$0 < i_1 < \cdots < i_{e-1} < i_e + 1 < i_{e+1} < \cdots < i_l \leq n. \tag{4.14}$$

Ας θεωρήσουμε ότι ο ακέραιος $i' = 2^{i'_1} + \cdots + 2^{i'_{e-1}} + 2^{i'_e} + 2^{i'_{e+1}} + \cdots + 2^{i'_l}$ δίνεται από τη σχέση

$$
\begin{aligned}
i' &= 2^{i_1 - 1} + \cdots + 2^{i_{e-1} - 1} + 2^{i_e} + 2^{i_{e+1} - 1} + \cdots + 2^{i_l - 1} \\
&= (i + 2^e)/2.
\end{aligned}
$$

Τότε, είναι εμφανές ότι ο i' έχει δυαδικό βάρος l και ανήκει στο σύνολο $\mathbb{Z}^*_{2^n}$, αφού από την (4.14) λαμβάνουμε πως ο ακέραιος i' ικανοποιεί την ανισότητα $0 \leq i'_1 < \cdots < i'_l < n$.

Παρομοίως, το σύνολο $J^3_{e,b}$ περιέχει όλους τους ακεραίους $i = 2^{i_1} + \cdots + 2^{i_{e-1}} + 3 \cdot 2^{i_e} + 2^{i_{e+2}} + \cdots + 2^{i_l}$ που ικανοποιούν τη σχέση

$$0 < i_1 < \cdots < i_{e-1} < i_e + 1 < i_{e+2} < \cdots < i_l \leq n. \tag{4.15}$$

Ας θεωρήσουμε ότι ο ακέραιος $i' = 2^{i'_1} + \cdots + 2^{i'_{e-1}} + 2^{i'_e} + 2^{i'_{e+1}} + \cdots + 2^{i'_{l-1}}$ δίνεται από τη σχέση

$$
\begin{aligned}
i' &= 2^{i_1 - 1} + \cdots + 2^{i_{e-1} - 1} + 2^{i_e} + 2^{i_{e+2} - 1} + \cdots + 2^{i_l - 1} \\
&= (i - 2^e)/2.
\end{aligned}
$$

Τότε, είναι εμφανές ότι ο i' έχει δυαδικό βάρος $l-1$ και ανήκει στο σύνολο $\mathbb{Z}_{2^n}^*$, αφού από την (4.15) λαμβάνουμε πως ο ακέραιος i' ικανοποιεί την ανισότητα $0 \leq i'_1 < \cdots < i'_{l-1} < n$.

Απ' όλα τα παραπάνω, και επειδή και στις δύο περιπτώσεις ισχύει $i'_e = i_e$, το $D_r(l,t)$ λαμβάνει τη μορφή

$$\begin{aligned}
D_r(l,t) &= \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \right) \alpha^{-ji} \\
&\quad + \sum_{e=1}^{l} \sum_{i \in J^3_{e,a}} A_l(t', i)^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \alpha^{-j(i+2^{i_e})} \\
&\quad + \sum_{e=1}^{l-1} \sum_{i \in J^3_{e,b}} A_l(t', i)^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \alpha^{-j(i+2^{i_e})} \\
&= \sum_{\mathrm{wt}(i)=l+1} \left(\sum_{e=1}^{l+1} A_l(t', i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \right) \alpha^{-ji} \\
&\quad + \sum_{\mathrm{wt}(i')=l} \left(\sum_{e=1}^{l} A_l(t', 2i' - 2^{i'_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i'_e}} \right) \alpha^{-j2i'} \\
&\quad + \sum_{e=1}^{l-1} \sum_{\mathrm{wt}(i')=l-1} A_l(t', 2i' + 2^{i'_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i'_e}} \alpha^{-j2(i'+2^{i'_e})}
\end{aligned}$$

ή σε πιο συμπαγής γραφή

$$\begin{aligned}
D_r(l,t) &= \sum_{s=l}^{l+1} \sum_{\mathrm{wt}(i)=s} \left(\sum_{e=1}^{s} A_l(t', 2^{l+1-s} i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \right) \alpha^{-j 2^{l+1-s} i} \\
&\quad + \sum_{e=1}^{l-1} \sum_{\mathrm{wt}(i)=l-1} A_l(t', 2i + 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \alpha^{-j\,((2i+2^{i_e})+2^{i_e})}. \qquad (4.16)
\end{aligned}$$

Παρατηρούμε πως η (4.10) γράφεται ισοδύναμα ως εξής

$$\begin{aligned}
D_r(l,t) &= \sum_{s=l+1}^{l+1} \sum_{\mathrm{wt}(i)=s} \left(\sum_{e=1}^{s} A_l(t', 2^{l+1-s} i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \right) \alpha^{-j 2^{l+1-s} i} \\
&\quad + \sum_{e=1}^{l} \sum_{\mathrm{wt}(i)=l} A_l(t', i)^{2^{l-r}} \alpha^{t_{r+1} 2^{i_e}} \alpha^{-j\,(i+2^{i_e})}. \qquad (4.17)
\end{aligned}$$

Η σύγκριση των (4.16) και (4.17), υποδεικνύει τα αποτελέσματα εφαρμογής των προηγούμενων βημάτων.

Στην πρώτη παράσταση από το δεξιό μέρος της (4.17):

- η αρχική τιμή του s $(= l+1)$ μειώνεται κατά 1.

Στη δεύτερη παράσταση από το δεξιό μέρος της (4.17):

- η τελική τιμή του e $(= l)$ και το δυαδικό βάρος του ακεραίου i $(= l)$ μειώνονται κατά 1,
- το νέο δεύτερο όρισμα $(= 2i + 2^{i_e})$ του συντελεστή A_l είναι ίσο με το διπλάσιο του παλαιού του ορίσματος $(= i)$ συν τον όρο 2^{i_e}, και
- ο νέος εκθέτης του δεξιότερου όρου, δηλ. του όρου $\alpha^{-j\,((2i+2^{i_e})+2^{i_e})}$, είναι ίσος με το νέο δεύτερο όρισμα του συντελεστή A_l συν τον όρο 2^{i_e}, πολλαπλασιασμένος με $-j$.

Εφαρμόζοντας τα ανωτέρω βήματα επιπλέον $l-2$ φορές, λαμβάνουμε τελικά

$$\begin{aligned} D_r(l,t) &= \sum_{s=2}^{l+1} \sum_{\mathrm{wt}(i)=s} \left(\sum_{e=1}^{s} A_l(t', 2^{l+1-s}i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-j2^{l+1-s}i} \\ &\quad + \sum_{\mathrm{wt}(i)=1} A_l(t', 2^{l-1}i + 2^{i_1+l-2} + \cdots + 2^{i_1})^{2^{l-r}} \alpha^{t_{r+1}2^{i_1}} \\ &\quad \times \alpha^{-j\,((2^{l-1}i+2^{i_1+l-2}+\cdots+2^{i_1})+2^{i_1})} \\ &= \sum_{s=1}^{l+1} \sum_{\mathrm{wt}(i)=s} \left(\sum_{e=1}^{s} A_l(t', 2^{l+1-s}i - 2^{i_e})^{2^{l-r}} \alpha^{t_{r+1}2^{i_e}} \right) \alpha^{-j2^{l+1-s}i} \end{aligned}$$

αφού στην περίπτωση που το δυαδικό βάρος του ακεραίου i είναι ίσο με 1, τότε έχουμε $i = 2^{i_1}$ και συνεπώς ισχύει $2^{l-1}i + 2^{i_1+l-2} + \cdots + 2^{i_1} = 2^l i - 2^{i_1}$. □

Θεώρημα 4.11. *Ας θεωρήσουμε τον ακέραιο $i \in \mathbb{Z}_{2^n}^*$, και τις διακριτές φάσεις $x_{j-t_1}, \ldots, x_{j-t_k}$ της ακολουθίας μεγίστου μήκους x. Τότε ισχύει η σχέση*

$$x_{j-t_1} \cdots x_{j-t_k} = \sum_{l=1}^{k} \sum_{\mathrm{wt}(i)=l} A_l(t,i) \alpha^{-j2^{k-l}i} \tag{4.18}$$

όπου $\mathrm{wt}(t) = k$ *και*

$$A_l(t,i) = \sum_{d=l}^{k} \sum_{e=1}^{l} A_{d-1}(t', 2^{d-l}i - 2^{i_e})\alpha^{t_k 2^{i_e+k-d}}. \tag{4.19}$$

Επιπλέον, οι συντελεστές $A_l(t,i)$ *ικανοποιούν τα ακόλουθα:*

1. $A_l(t,i)^{2^m} = A_l(t, 2^m i \bmod N)$ *για κάθε* $m \geq 0$,
2. $A_l(t,i) = 0$ *έαν* $\mathrm{wt}(i) < l$.

Απόδειξη. Η απόδειξη θα βασιστεί στη μέθοδο της επαγωγής ως προς το βαθμό k των γινομένων, δηλ. το δυαδικό βάρος του ακεραίου t. Οι σχέσεις (4.18) και (4.19), καθώς και οι Ιδιότητες 1–2 έχουν αποδειχθεί για γινόμενα δευτέρου βαθμού. Στη συνέχεια, υποθέτουμε πως οι σχέσεις (4.18) και (4.19), καθώς και οι Ιδιότητες 1–2 ισχύουν για γινόμενα βαθμού $k-1$, δηλ. έχουμε ότι

$$x_{j-t_1} \cdots x_{j-t_{k-1}} = \sum_{l=1}^{k-1} \sum_{\mathrm{wt}(i)=l} A_l(t', i)\alpha^{-j2^{k-1-l}i}. \tag{4.20}$$

Από την (4.20) λαμβάνουμε ότι το γινόμενο $(x_{j-t_1} \cdots x_{j-t_{k-1}})x_{j-t_k}$ γράφεται ως εξής

$$\begin{aligned}
x_{j-t_1} \cdots x_{j-t_k} &= \\
&= \left(\sum_{l=1}^{k-1} \sum_{\mathrm{wt}(i)=l} A_l(t', i)\alpha^{-j2^{k-1-l}i} \right) \left(\sum_{m=0}^{n-1} \alpha^{(t_k-j)2^m} \right) \\
&= \sum_{l=1}^{k-1} \left(\sum_{\mathrm{wt}(i)=l} A_l(t', i)^{2^{l+1-k}} \alpha^{-ji} \right)^{2^{k-1-l}} \left(\sum_{i_{l+1}=0}^{n-1} \alpha^{(t_k-j)2^{i_l+1}} \right)^{2^{k-1-l}} \\
&= \sum_{l=1}^{k-1} D_{k-1}(l,t)^{2^{k-1-l}} \\
&= \sum_{l=1}^{k-1} \sum_{s=1}^{l+1} \sum_{\mathrm{wt}(i)=s} \left(\sum_{e=1}^{s} A_l(t', 2^{l+1-s}i - 2^{i_e})\alpha^{t_k 2^{i_e+k-1-l}} \right) \alpha^{-j2^{k-s}i}
\end{aligned}$$

από το Θεώρημα 4.10. Θέτοντας $s \leftarrow l$ και $l \leftarrow d-1$ λαμβάνουμε ότι

$$x_{j-t_1} \cdots x_{j-t_k} =$$

$$= \sum_{d=2}^{k} \sum_{l=1}^{d} \sum_{\mathrm{wt}(i)=l} \left(\sum_{e=1}^{l} A_{d-1}(t', 2^{d-l}i - 2^{i_e}) \alpha^{t_k 2^{i_e+k-d}} \right) \alpha^{-j2^{k-l}i}$$

$$= \sum_{d=1}^{k} \sum_{l=1}^{d} \sum_{\mathrm{wt}(i)=l} \left(\sum_{e=1}^{l} A_{d-1}(t', 2^{d-l}i - 2^{i_e}) \alpha^{t_k 2^{i_e+k-d}} \right) \alpha^{-j2^{k-l}i} \quad (4.21)$$

αφού για $d = 1$ αναγκαστικά έχουμε $l = 1$, $e = 1$, και οι μοναδικοί όροι που προστίθενται είναι ίσοι με

$$\sum_{\mathrm{wt}(i)=1} \left(A_0(t', i - 2^{i_1}) \alpha^{t_k 2^{i_1+k-1}} \right) \alpha^{-j2^{k-1}i} = \sum_{\mathrm{wt}(i)=1} A_0(t', 0) \alpha^{(t_k-j)2^{k-1}i}$$

$$= A_0(t', 0) \left(\sum_{\mathrm{wt}(i)=1} \alpha^{(t_k-j)i} \right)^{2^{k-1}}$$

$$= 0$$

από την Παρατήρηση 4.4. Οι δύο πρώτοι τελεστές αθροισμάτων στην (4.21) είναι δυνατό να αντιμετατεθούν ώστε να λάβουμε

$$x_{j-t_1} \cdots x_{j-t_k} =$$

$$= \sum_{l=1}^{k} \sum_{d=l}^{k} \sum_{\mathrm{wt}(i)=l} \left(\sum_{e=1}^{l} A_{d-1}(t', 2^{d-l}i - 2^{i_e}) \alpha^{t_k 2^{i_e+k-d}} \right) \alpha^{-j2^{k-l}i}$$

$$= \sum_{l=1}^{k} \sum_{\mathrm{wt}(i)=l} \left(\sum_{d=l}^{k} \sum_{e=1}^{l} A_{d-1}(t', 2^{d-l}i - 2^{i_e}) \alpha^{t_k 2^{i_e+k-d}} \right) \alpha^{-j2^{k-l}i}$$

όπου οι όροι στο εσωτερικό των παρενθέσεων συμβολίζονται με το συντελεστή $A_l(t, i)$, ολοκληρώνοντας το πρώτο μέρος της απόδειξης.

Στη συνέχεια, αποδεικνύουμε ότι για όλους τους ακεραίους $1 \leq l \leq k$, οι νέοι συντελεστές $A_l(t, i)$, που ορίζονται από την (4.19), ικανοποιούν τις Ιδιότητες 1–2. Για κάθε $m \geq 0$, ισχύει

$$A_l(t, i)^{2^m} = \sum_{d=l}^{k} \sum_{e=1}^{l} A_{d-1}(t', 2^{d-l}i - 2^{i_e})^{2^m} \alpha^{t_k 2^{i_e+k-d+m}}$$

$$= \sum_{d=l}^{k} \sum_{e=1}^{l} A_{d-1}(t', 2^m(2^{d-l}i - 2^{i_e}) \bmod N) \alpha^{t_k 2^{i_e+k-d+m}}$$

$$
\begin{aligned}
&= \sum_{d=l}^{k} \sum_{e=1}^{l} A_{d-1}(t', 2^{d-l}(2^m i \bmod N) - 2^{i_e + m \bmod n}) \\
&\quad \times \alpha^{t_k 2^{(i_e + m \bmod n) + k - d}} \\
&= A_l(t, 2^m i \bmod N)
\end{aligned}
$$

αφού $\mathrm{wt}(t') = \mathrm{wt}(t) - 1 = k - 1$, και συνεπώς λόγω της επαγωγής έχουμε ότι για κάθε $l \leq d \leq k$ ισχύει

$$A_{d-1}(t', 2^{d-l} i - 2^{i_e})^{2^m} = A_{d-1}(t', 2^m (2^{d-l} i - 2^{i_e}) \bmod N).$$

Για την απόδειξη της Ιδιότητας 1 θεωρήσαμε ότι $i < N$. Στην περίπτωση όπου $i > N$, π.χ. έαν $0 \leq i_1 < \cdots < i_{l-1} < n < i_l$, $1 \leq l \leq k$, η Ιδιότητα 1 εξακολουθεί να ισχύει χρησιμοποιώντας το $i_l - n$ αντί του i_l.

Ας υποθέσουμε ότι $\mathrm{wt}(i) = l - 1 < l$. Χωρίς βλάβη της γενικότητας θεωρούμε την περίπτωση $i = 2^{i_1} + \cdots + 2^{i_{l-1}} + 2^{i_l}$, όπου $i_{l-1} = i_l$. Για κάθε τιμή του ακεραίου e διαφορετική των $l-1, l$, και για κάθε $l \leq d \leq k$, ο ακέραιος $2^{d-l} i - 2^{i_e}$ έχει δυαδικό βάρος μικρότερο του $d - 1$. Επειδή $\mathrm{wt}(t') = \mathrm{wt}(t) - 1 = k - 1$, από την επαγωγή λαμβάνουμε ότι ο συντελεστής $A_{d-1}(t', 2^{d-l} i - 2^{i_e})$ μηδενίζεται. Ως αποτέλεσμα

$$
\begin{aligned}
A_l(t, i) = &\sum_{d=l}^{k} A_{d-1}(t', 2^{d-l} i - 2^{i_{l-1}}) \alpha^{t_k 2^{i_{l-1} + k - d}} \\
&+ \sum_{d=l}^{k} A_{d-1}(t', 2^{d-l} i - 2^{i_l}) \alpha^{t_k 2^{i_l + k - d}}
\end{aligned}
$$

και από την $i_{l-1} = i_l$, καταλήγουμε πως ισχύει $A_l(t, i) = 0$. □

Παρατήρηση 4.12. Η Ιδιότητα 1 του Θεωρήματος 4.11 παρέχει έναν εύκολο τρόπο υπολογισμού της τιμής του συντελεστή $A_l(t, i)$ σε ακέραιους της ίδιας κυκλοτομικής κλάσης (modulo N).

Έστω ότι το δυαδικό βάρος του ακέραιου i είναι ίσο με l, όπου $i \in \mathbb{Z}_{2^n}^*$. Ορισμένοι από τους όρους που συμμετέχουν στον υπολογισμό της τιμής του συντελεστή $A_l(t, i)$, στο δεξιό μέρος της (4.19), είναι ίσοι με μηδέν λόγω της δεύτερης Ιδιότητας του Θεωρήματος 4.11. Είναι δυνατό να προβλέψουμε αυτές τις περιπτώσεις, μειώνοντας έτσι την υπολογιστική πολυπλοκότητα υπολογισμού

της τιμής του $A_l(t,i)$. Ας ορίσουμε τον ακέραιο $\delta_{d,l}$, που ικανοποιεί τον περιορισμό $0 \leq \delta_{d,l} < n$, ως εξής

$$\delta_{d,l} \triangleq \min_{1 \leq m \leq l} \{i_m - i_e + d - l \bmod N\}. \tag{4.22}$$

Παρατηρούμε ότι $\delta_{d,l} \leq d - l$, όπου η ισότητα ισχύει στην περίπτωση όπου $m = e$. Από τις (4.19) και (4.22), συμπεραίνουμε πως το δυαδικό βάρος του ακεραίου $2^{d-l}i - 2^{i_e}$ είναι ίσο με $l + \delta_{d,l} - 1$. Η Ιδιότητα 2 του Θεωρήματος 4.11, συνεπάγεται ότι ο συντελεστής $A_{d-1}(t', 2^{d-l}i - 2^{i_e})$ μηδενίζεται έαν

$$\mathrm{wt}(2^{d-l}i - 2^{i_e}) < d - 1 \Leftrightarrow \delta_{d,l} < d - l.$$

Όπως και στην περίπτωση γινομένων δευτέρου βαθμού, η γραμμική πολυπλοκότητα ενός γινομένου $x_{j-t_1} \cdots x_{j-t_k}$ βαθμού k είναι ίση με τον αριθμό των μη–μηδενικών συντελεστών $A_l(t,i)$, στο δεξιό μέρος της (4.18). Στη μελέτη που πραγματοποίησε ο Herlestam [45], είναι απαραίτητο να λυθεί το ακόλουθο σύστημα εξισώσεων

$$\begin{aligned} c_0 + 2c_1 + \cdots + 2^{n-1}c_{n-1} &\equiv i \pmod N \\ c_0 + c_1 + \cdots + c_{n-1} &= k \end{aligned}$$

ώστε να υπολογίσουμε τους συγκεκριμένους συντελεστές, όπου $c_m \geq 0$ και $i \in \mathbb{Z}_{2^n}^*$. Το πλεονέκτημα της αναδρομικής σχέσης (4.19) είναι πως αποφεύγουμε την απ' ευθείας λύση των ανωτέρω εξισώσεων.

4.3 Εύρεση ισοδύναμων παραστάσεων

Η αναδρομική φύση της (4.19) καθιστά δυνατό τον υπολογισμό των συντελεστών $A_l(t,i)$ από τους $A_{l'}(t',i')$, όπου ισχύει $\mathrm{wt}(t) = \mathrm{wt}(t') + 1$. Στη συνέχεια της ενότητας, θα παράγουμε ισοδύναμες παραστάσεις για τον υπολογισμό της τιμής συγκεκριμένων συντελεστών $A_l(t,i)$, των οποίων η κατανόηση είναι πιο εύκολη. Στο εξής, συμβολίζουμε με P_j το σύνολο όλων των αντιμεταθέσεων του συνόλου $I_j = \{i_1, \ldots, i_j\}$, και με S_j το σύνολο

$$S_j = \left\{ \begin{pmatrix} c_1 & \cdots & c_j \end{pmatrix} \mid 1 \leq c_1 < \cdots < c_j \leq k \right\}.$$

Πόρισμα 4.13. *Ας θεωρήσουμε το γινόμενο $x_{j-t_1}\cdots x_{j-t_k}$ διακριτών φάσεων της ακολουθίας μεγίστου μήκους x, και έστω ότι $i \in \mathbb{Z}_{2^n}^*$ με $\mathrm{wt}(i) = k$. Τότε ισχύει*

$$A_k(t,i) = \begin{vmatrix} \alpha^{t_1 2^{i_1}} & \alpha^{t_1 2^{i_2}} & \cdots & \alpha^{t_1 2^{i_k}} \\ \alpha^{t_2 2^{i_1}} & \alpha^{t_2 2^{i_2}} & \cdots & \alpha^{t_2 2^{i_k}} \\ \vdots & \vdots & & \vdots \\ \alpha^{t_k 2^{i_1}} & \alpha^{t_k 2^{i_2}} & \cdots & \alpha^{t_k 2^{i_k}} \end{vmatrix} \tag{4.23}$$

όπου $i = 2^{i_1} + \cdots + 2^{i_k}$ και $t = 2^{t_1 - 1} + \cdots + 2^{t_k - 1}$.

Απόδειξη. Ορίζουμε το διάνυσμα $\boldsymbol{e} = \begin{pmatrix} e_1 & \cdots & e_k \end{pmatrix}$, όπου οι τιμές των μεταβλητών $e_1, \ldots, e_k$ είναι διαφορετικές μεταξύ τους και ανήκουν στο σύνολο I_k. Επιπρόσθετα, ορίζουμε τον ακέραιο $t^m = 2^{t_1 - 1} + \cdots + 2^{t_m - 1}$, για κάθε $1 \le m \le k$. Τότε, από το Θεώρημα 4.11 και την σχέση (4.19) λαμβάνουμε

$$\begin{aligned} A_k(t,i) &= \sum_{e_k} A_{k-1}(t^{k-1}, i - 2^{e_k}) \alpha^{t_k 2^{e_k}} \\ &= \sum_{e_k} \sum_{e_{k-1} \neq e_k} A_{k-2}(t^{k-2}, i - 2^{e_{k-1}} - 2^{e_k}) \alpha^{t_{k-1} 2^{e_{k-1}}} \alpha^{t_k 2^{e_k}} \\ &\vdots \\ &= \sum_{e_k} \cdots \sum_{e_1 \neq e_2, \ldots, e_k} A_0(t^0, i - 2^{e_1} - \cdots - 2^{e_k}) \alpha^{t_1 2^{e_1}} \cdots \alpha^{t_k 2^{e_k}}. \end{aligned}$$

Εξ' ορισμού ισχύει ότι $t^0 = 0$ και $i - 2^{e_1} - \cdots - 2^{e_k} = 0$. Συνεπώς, από την Παρατήρηση 4.4 συνεπάγεται ότι $A_0(t^0, i - 2^{e_1} - \cdots - 2^{e_k}) = 1$. Κατά συνέπεια θα ισχύει

$$A_k(t,i) = \sum_{\boldsymbol{e} \in P_k} \alpha^{t_1 2^{e_1}} \cdots \alpha^{t_k 2^{e_k}}$$

που είναι ισοδύναμη με την (4.23). □

Πόρισμα 4.14. *Ας θεωρήσουμε το γινόμενο $x_{j-t_1}\cdots x_{j-t_k}$ διακριτών φάσεων της ακολουθίας μεγίστου μήκους x, και έστω ότι $i \in \mathbb{Z}_{2^n}^*$ με $\mathrm{wt}(i) = k-1$. Τότε ισχύει*

$$A_{k-1}(t,i) = \sum_{\boldsymbol{c} \in S_2} \begin{vmatrix} \alpha^{t_1 2^{i_1}} & \alpha^{t_1 2^{i_2}} & \cdots & \alpha^{t_1 2^{i_{k-1}}} \\ \vdots & \vdots & & \vdots \\ \alpha^{t_k 2^{i_1}} & \alpha^{t_k 2^{i_2}} & \cdots & \alpha^{t_k 2^{i_{k-1}}} \\ \alpha^{\tau_{\boldsymbol{c}} 2^{i_1}} & \alpha^{\tau_{\boldsymbol{c}} 2^{i_2}} & \cdots & \alpha^{\tau_{\boldsymbol{c}} 2^{i_{k-1}}} \end{vmatrix}^2 \tag{4.24}$$

όπου $i = 2^{i_1} + \cdots + 2^{i_{k-1}}$, $t = 2^{t_1 - 1} + \cdots + 2^{t_k - 1}$, *και* $\tau_{\boldsymbol{c}} = (t_{c_1} + t_{c_2})/2$. *Από την ορίζουσα στο δεξιό μέρος της* (4.24) *δεν περιλαμβάνονται οι γραμμές που αντιστοιχούν στους εκθέτες* t_{c_1} *και* t_{c_2}.

Απόδειξη. Ακολουθώντας τον ίδιο συμβολισμό με το Πόρισμα 4.13, ορίζουμε το διάνυσμα $\boldsymbol{e} = \begin{pmatrix} e_1 & \cdots & e_{k-1} \end{pmatrix}$, όπου οι τιμές των μεταβλητών $e_1, \ldots, e_{k-1}$ είναι διαφορετικές μεταξύ τους και ανήκουν στο σύνολο I_{k-1}. Θέτοντας $l = k - 1$ στην (4.19), λαμβάνουμε

$$\begin{aligned} A_{k-1}(t, i) = &\sum_{e_{k-1}} A_{k-2}(t^{k-1}, i - 2^{e_{k-1}}) \alpha^{t_k 2^{e_{k-1}+1}} \\ &+ \sum_{e_{k-1}} A_{k-1}(t^{k-1}, 2i - 2^{e_{k-1}}) \alpha^{t_k 2^{e_{k-1}}}. \end{aligned}$$

Σύμφωνα με το Πόρισμα 4.13, οι συντελεστές $A_{k-1}(t^{k-1}, 2i - 2^{e_{k-1}})$ είναι ορίζουσες τάξης $k - 1$. Συνεπώς, εφαρμόζοντας την (4.19) για τους συντελεστές $A_{k-2}(t^{k-1}, i - 2^{e_{k-1}})$ έχουμε

$$\begin{aligned} A_{k-1}(t, i) = &\sum_{e_{k-1}} \sum_{e_{k-2} \neq e_{k-1}} A_{k-3}(t^{k-2}, i - 2^{e_{k-2}} - 2^{e_{k-1}}) \\ &\times \alpha^{t_{k-1} 2^{e_{k-2}+1}} \alpha^{t_k 2^{e_{k-1}+1}} \\ &+ \sum_{e_{k-1}} \sum_{e_{k-2} \neq e_{k-1}} A_{k-2}(t^{k-2}, 2i - 2^{e_{k-2}} - 2^{e_{k-1}+1}) \\ &\times \alpha^{t_{k-1} 2^{e_{k-2}}} \alpha^{t_k 2^{e_{k-1}+1}} \\ &+ \sum_{e_{k-1}} A_{k-1}(t^{k-1}, 2i - 2^{e_{k-1}}) \alpha^{t_k 2^{e_{k-1}}} \\ &\vdots \\ = &\sum_{e_{k-1}} \cdots \sum_{e_1 \neq e_2, \ldots, e_{k-1}} A_0(t^1, i - 2^{e_1} - \cdots - 2^{e_{k-1}}) \\ &\times \alpha^{t_2 2^{e_1+1}} \cdots \alpha^{t_k 2^{e_{k-1}+1}} \\ &+ \sum_{j=1}^{k-1} \sum_{e_{k-1}} \cdots \sum_{e_{k-j} \neq e_{k-j+1}, \ldots, e_{k-1}} A_{k-j}(t^{k-j}, 2i - 2^{e_{k-j}} \\ &- \sum_{m=k-j+1}^{k-1} 2^{e_m + 1}) \alpha^{t_{k-j+1} 2^{e_{k-j}}} \prod_{m=k-j+1}^{k-1} \alpha^{t_{m+1} 2^{e_m+1}}. \end{aligned}$$

Επειδή $t^1 = 2^{t_1-1}$ και $i - 2^{e_1} - \cdots - 2^{e_{k-1}} = 0$, η Παρατήρηση 4.4 μας δίνει $A_0(t^1, i - 2^{e_1} - \cdots - 2^{e_{k-1}}) = 0$. Επιπλέον, θα πρέπει να παρατηρήσουμε ότι ισχύει

$$2i - 2^{e_{k-j}} - \sum_{m=k-j+1}^{k-1} 2^{e_m+1} = 2\left(i - \sum_{m=k-j}^{k-1} 2^{e_m}\right) + 2^{e_{k-j}}$$

για κάθε $1 \leq j \leq k-1$. Αναλύοντας την ορίζουσα $A_{k-j}(t^{k-j}, 2i - 2^{e_{k-j}} - 2^{e_{k-j+1}+1} - \cdots - 2^{e_{k-1}+1})$ τάξης $k-j$ κατά μήκος της στήλης που περιέχει τη μεταβλητή e_{k-j}, λαμβάνουμε

$$\begin{aligned} A_{k-1}(t,i) = \sum_{j=1}^{k-1}\sum_{l=1}^{k-j}\sum_{e_{k-1}} \cdots \sum_{e_{k-j} \neq e_{k-j+1},\ldots,e_{k-1}} & A_{k-j-1}(t^{k-j} - 2^{t_l-1}, 2i \\ - \sum_{m=k-j}^{k-1} 2^{e_m+1})\alpha^{\frac{t_l+t_{k-j+1}}{2}2^{e_{k-j}+1}} & \prod_{m=k-j+1}^{k-1} \alpha^{t_{m+1}2^{e_m+1}}. \end{aligned}$$

Στη συνέχεια, συνθέτουμε ορίζουσες της ίδιας τάξης $k-1$ από τις υπο–ορίζουσες $A_{k-j-1}(t^{k-j} - 2^{t_l-1}, 2i - 2^{e_{k-j}+1} - \cdots - 2^{e_{k-1}+1})$ για να λάβουμε τη σχέση

$$A_{k-1}(t,i) = \sum_{j=1}^{k-1}\sum_{l=1}^{k-j} A_{k-1}(\bar{t}(l, k-j+1), i)^2$$

όπου

$$\bar{t}(l, k-j+1) = t - 2^{t_l-1} - 2^{t_{k-j+1}-1} + 2^{\frac{t_l+t_{k-j+1}}{2}-1}.$$

Τέλος, οι αλλαγές μεταβλητών $c_1 \leftarrow l$ και $c_2 \leftarrow k-j+1$ οδηγούν στο επιθυμητό αποτέλεσμα. □

Ο τρόπος με τον οποίο πραγματοποιήθηκε η απόδειξη του Πορίσματος 4.14 είναι δυνατό να χρησιμοποιηθεί για την εύρεση ισοδύναμων παραστάσεων για όλους τους συντελεστές $A_l(t,i)$. Στη συνέχεια, παρέχουμε το ακόλουθο Πόρισμα χωρίς απόδειξη.

Πόρισμα 4.15. *Ας θεωρήσουμε το γινόμενο $x_{j-t_1} \cdots x_{j-t_k}$ διακριτών φάσεων της ακολουθίας μεγίστου μήκους x, και έστω ότι $i \in \mathbb{Z}_{2^n}^*$ με $\mathrm{wt}(i) = k-2$. Τότε ισχύει*

$$A_{k-2}(t,i) = \sum_{\mathbf{c}\in S_3} \begin{vmatrix} \alpha^{t_1 2^{i_1}} & \alpha^{t_1 2^{i_2}} & \cdots & \alpha^{t_1 2^{i_{k-2}}} \\ \vdots & \vdots & & \vdots \\ \alpha^{t_k 2^{i_1}} & \alpha^{t_k 2^{i_2}} & \cdots & \alpha^{t_k 2^{i_{k-2}}} \\ \alpha^{\tau_{\mathbf{c}} 2^{i_1}} & \alpha^{\tau_{\mathbf{c}} 2^{i_2}} & \cdots & \alpha^{\tau_{\mathbf{c}} 2^{i_{k-2}}} \end{vmatrix}^4$$

$$+ \sum_{\mathbf{c}\in S_4} \sum_{(\varepsilon_1,\varepsilon_2)\in T_{\mathbf{c}}} \begin{vmatrix} \alpha^{t_1 2^{i_1}} & \alpha^{t_1 2^{i_2}} & \cdots & \alpha^{t_1 2^{i_{k-2}}} \\ \vdots & \vdots & & \vdots \\ \alpha^{t_k 2^{i_1}} & \alpha^{t_k 2^{i_2}} & \cdots & \alpha^{t_k 2^{i_{k-2}}} \\ \alpha^{\varepsilon_1 2^{i_1}} & \alpha^{\varepsilon_1 2^{i_2}} & \cdots & \alpha^{\varepsilon_1 2^{i_{k-2}}} \\ \alpha^{\varepsilon_2 2^{i_1}} & \alpha^{\varepsilon_2 2^{i_2}} & \cdots & \alpha^{\varepsilon_2 2^{i_{k-2}}} \end{vmatrix}^4 \qquad (4.25)$$

όπου $i = 2^{i_1} + \cdots + 2^{i_{k-2}}$, $t = 2^{t_1-1} + \cdots + 2^{t_k-1}$, *και*

$$\alpha^{4\tau_{\mathbf{c}}} = \alpha^{t_{c_1}+t_{c_2}+t_{c_3}}(\alpha^{t_{c_1}} + \alpha^{t_{c_2}} + \alpha^{t_{c_3}}),$$

$$T_{\mathbf{c}} = \left\{ (\frac{t_{c_1}+t_{c_2}}{2}, \frac{t_{c_3}+t_{c_4}}{2}),\ (\frac{t_{c_1}+t_{c_3}}{2}, \frac{t_{c_2}+t_{c_4}}{2}),\ (\frac{t_{c_1}+t_{c_4}}{2}, \frac{t_{c_2}+t_{c_3}}{2}) \right\}.$$

Από τις ορίζουσες στο δεξιό μέρος της (4.25) *δεν περιλαμβάνονται οι γραμμές που αντιστοιχούν στους εκθέτες* t_{c_1}, t_{c_2} *και* t_{c_3}, *ενώ επιπρόσθετα δεν περιλαμβάνεται η γραμμή που αντιστοιχεί στον εκθέτη* t_{c_4} *από τη δεύτερη ορίζουσα.*

Η σχέση (4.23) εμφανίζεται και στο κλασσικό βιβλίο του Rueppel [102], όπου ο συντελεστής $A_k(t,i)$ χρησιμοποιήθηκε για την πραγματοποίηση ενός *τεστ ύπαρξης των ριζών* α^i, με $\mathrm{wt}(i) = k$. Στο συγκεκριμένο βιβλίο δε δόθηκαν σχέσεις για την εύρεση των υπολοίπων συντελεστών του α^i, με $\mathrm{wt}(i) < k$. Εκτός από τον απ' ευθείας υπολογισμό των $A_{\mathrm{wt}(i)}(t,i)$, για $\mathrm{wt}(i) = k, k-1, k-2$, μέσω των σχέσεων (4.23), (4.24), και (4.25) αντίστοιχα, είναι δυνατός ο αναδρομικός υπολογισμός όλων των συντελεστών μέσω του Θεωρήματος 4.11.

4.4 Νέα αποτελέσματα μη–γραμμικών φίλτρων

Θεωρούμε το σύνολο I των επικεφαλείς κλάσεων των κυκλοτομικών κλάσεων modulo N ($\beta\lambda$. Κεφάλαιο 2), και έστω ότι e_i είναι η τάξη του στοιχείου α^i, όπου $i \in I$, του πεπερασμένου σώματος $\mathbb{F}_{2^n}$. Συμβολίζουμε με n_i την πολλαπλασιαστική τάξη του 2 modulo e_i. Στη συνέχεια παραθέτουμε το ακόλουθο Λήμμα από το [72, Κεφ. 3].

Λήμμα 4.16. *Ας θεωρήσουμε τα στοιχεία $\beta_1, \ldots, \beta_k$, με $k \leq n$, του πεπερασμένου σώματος $\mathbb{F}_{2^n}$, και έστω ότι*

$$E = \begin{vmatrix} \beta_1 & \beta_1^2 & \cdots & \beta_1^{2^{k-1}} \\ \beta_2 & \beta_2^2 & \cdots & \beta_2^{2^{k-1}} \\ \vdots & \vdots & & \vdots \\ \beta_k & \beta_k^2 & \cdots & \beta_k^{2^{k-1}} \end{vmatrix}.$$

Τότε ισχύει

$$E = \prod_{l=1}^{k} \prod_{c_1,\ldots,c_{l-1} \in \mathbb{F}_2} (c_1\beta_1 + \cdots + c_{l-1}\beta_{l-1} + \beta_l)$$

και συνεπώς η ορίζουσα είναι μηδέν έαν και μόνο έαν τα στοιχεία $\beta_1, \ldots, \beta_k$ είναι γραμμικώς εξαρτημένα στο $\mathbb{F}_2$.

Παρατήρηση 4.17. Ας θεωρήσουμε το διάνυσμα $\boldsymbol{c} = \begin{pmatrix} c_1 & \cdots & c_k \end{pmatrix}$, του οποίου τα στοιχεία ανήκουν στο $\mathbb{F}_2$, και έστω ότι $\mathbf{0}$ είναι το $1 \times k$ μηδενικό διάνυσμα. Τότε, η σχέση υπολογισμού της ορίζουσας του Λήμματος 4.16 γράφεται ως εξής

$$E = \prod_{\boldsymbol{c} \in \mathbb{F}_2^k \setminus \{\mathbf{0}\}} (c_1\beta_1 + \cdots + c_k\beta_k).$$

Λήμμα 4.18. *Ας θεωρήσουμε ένα οποιοδήποτε πρωταρχικό στοιχείο $\alpha \in \mathbb{F}_{2^n}$ του πεπερασμένου σώματος $\mathbb{F}_{2^n}$, και έστω ότι*

$$E = \begin{vmatrix} \alpha^1 & \alpha^{1\cdot 2} & \cdots & \alpha^{1\cdot 2^{n-1}} \\ \alpha^2 & \alpha^{2\cdot 2} & \cdots & \alpha^{2\cdot 2^{n-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^n & \alpha^{n\cdot 2} & \cdots & \alpha^{n\cdot 2^{n-1}} \end{vmatrix}.$$

Τότε ισχύει $E = 1$.

Απόδειξη. Στην ορίζουσα E του Λήμματος 4.16 θέτουμε $k = n$ και $\beta_i = \alpha^i$, για κάθε $1 \leq i \leq n$. Τότε, από την Παρατήρηση 4.17 ισχύει ότι

$$E = \prod_{\boldsymbol{c} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}} (c_1\alpha + \cdots + c_n\alpha^n) = \alpha^N \prod_{i \in \mathbb{Z}_N} \alpha^i.$$

Σαν αποτέλεσμα, λαμβάνουμε $E = \alpha^{N\frac{N+1}{2}} = 1$. □

Παρατήρηση 4.19. Το Πόρισμα 4.13 μαζί με το Λήμμα 4.18, οδηγούν στη σχέση $E = A_n(N, N) = 1$.

Θεώρημα 4.20. *Ας θεωρήσουμε ότι η ακολουθία y παράγεται από τη δομή του Σχ. 4.1. Τότε ισχύει*

$$y_j = \sum_{i \in I^*} \mathrm{tr}_1^{n_i}(b_i \alpha^{-ji}) + r_N \tag{4.26}$$

όπου οι συντελεστές $b_i \in \mathbb{F}_{2^n}$ δίνονται από τη σχέση

$$b_i = \sum_{\mathrm{wt}(t) \geq \mathrm{wt}(i)} r_t A_{\mathrm{wt}(i)}(t, i)^{2^{\mathrm{wt}(i)-\mathrm{wt}(t)}}. \tag{4.27}$$

Απόδειξη. Πραγματοποιώντας την αλλαγή μεταβλητών $i \leftarrow 2^{l-k} i \bmod N$ στην (4.18) λαμβάνουμε ότι το γινόμενο βαθμού k γράφεται ως εξής

$$\begin{aligned} x_{j-t_1} \cdots x_{j-t_k} &= \sum_{l=1}^{k} \sum_{\mathrm{wt}(2^{l-k} i \bmod N) = l} A_l(t, 2^{l-k} i \bmod N) \alpha^{-ji} \\ &= \sum_{l=1}^{k} \sum_{\mathrm{wt}(i)=l} A_l(t, i)^{2^{l-k}} \alpha^{-ji} \end{aligned} \tag{4.28}$$

αφού έαν το $2^m i \bmod N$, για κάθε m, διατρέχει όλους τους ακεραίους του συνόλου $\mathbb{Z}_N^*$ με δυαδικό βάρος l, τότε και το ίδιο συμβαίνει και με το i. Από την (4.28) και τον Ορισμό 4.1, λαμβάνουμε

$$\begin{aligned} y_j &= \sum_{k=1}^{n} \sum_{\mathrm{wt}(t)=k} r_t x_{j-t_1} \cdots x_{j-t_k} \\ &= \sum_{k=1}^{n} \sum_{\mathrm{wt}(t)=k} r_t \left(\sum_{l=1}^{k} \sum_{\mathrm{wt}(i)=l} A_l(t, i)^{2^{l-k}} \alpha^{-ji} \right) \\ &= \sum_{l=1}^{n} \sum_{\mathrm{wt}(i)=l} \left(\sum_{k=l}^{n} \sum_{\mathrm{wt}(t)=k} r_t A_l(t, i)^{2^{l-k}} \right) \alpha^{-ji} \\ &= \sum_{l=1}^{n-1} \sum_{\mathrm{wt}(i)=l} b_i \alpha^{-ji} + b_N \alpha^{-jN} \end{aligned}$$

όπου

$$b_i = \sum_{k=\mathrm{wt}(i)}^{n} \sum_{\mathrm{wt}(t)=k} r_t A_{\mathrm{wt}(i)}(t, i)^{2^{\mathrm{wt}(i)-k}}. \tag{4.29}$$

Επειδή ισχύει $b_N = r_N A_n(N,N)$, η Παρατήρηση 4.19 οδηγεί στο αποτέλεσμα $b_N = r_N$. Ταξινομώντας τους $\binom{n}{l}$ ακεραίους $i \in \mathbb{Z}_N$, με δυαδικό βάρος l, σε κυκλοτομικές κλάσεις λαμβάνουμε

$$y_j = \sum_{l=1}^{n-1} \sum_{\substack{i \in I^* \\ \mathrm{wt}(i)=l}} \sum_{m=0}^{n_i-1} (b_i \alpha^{-ji})^{2^m} + r_N = \sum_{l=1}^{n-1} \sum_{\substack{i \in I^* \\ \mathrm{wt}(i)=l}} \mathrm{tr}_1^{n_i}(b_i \alpha^{-ji}) + r_N.$$

Στην ανωτέρω σχέση κάναμε χρήση της Παρατήρησης 4.12 και της (4.29), για να γράψουμε ότι $b_i^{2^m} = b_{2^m i \bmod N}$. □

Πόρισμα 4.21. *Έστω y είναι η δυαδική ακολουθία που ορίστηκε στο Θεώρημα 4.20, και Y είναι η ακολουθία που αντιστοιχεί στο διακριτό μετασχηματισμό Fourier της y. Τότε, ο m–στός όρος της Y δίνεται από την ακόλουθη σχέση*

$$Y_m = \begin{cases} r_N & \text{έαν } m = 0, \\ b_m & \text{διαφορετικά.} \end{cases} \tag{4.30}$$

Απόδειξη. Η απόδειξη είναι άμεση απόρροια της (4.26). □

Ας υποθέσουμε ότι ο βαθμός k του μη–γραμμικού φίλτρου f είναι μικρότερος του n. Τότε, από την (4.27), συμπεραίνουμε ότι ισχύει $b_i = 0$ για όλους τους ακεραίους $i \in I^*$ με δυαδικό βάρος μεγαλύτερο από k. Κατά συνέπεια, η γραμμική πολυπλοκότητα της ακολουθίας y είναι ίση με

$$L_y = \sum_{\substack{i \in I^* \\ \mathrm{wt}(i) \le k}} c_i n_i + c_N \tag{4.31}$$

όπου $c_i = 0$ έαν $b_i = 0$, και $c_i = 1$ διαφορετικά. Έαν ο συντελεστής b_i είναι διάφορος του μηδενός, τότε ο b_i καθορίζει και τη φάση της δυαδικής ακολουθίας που παράγεται από τον καταχωρητή ολίσθησης γραμμικής ανάδρασης με πολυώνυμο ανάδρασης το ελάχιστο πολυώνυμο του α^i.

Ορισμός 4.22. Τα γινόμενα $x_{j-t_1} \cdots x_{j-t_k}$ και $x_{j-t_1^*} \cdots x_{j-t_k^*}$, βαθμού k, ονομάζονται *ισοδύναμα* έαν υπάρχει ακέραιος $d \ge 0$, τέτοιος ώστε να ισχύει $t_i^* = t_i + d$ για κάθε $1 \le i \le k$.

Πόρισμα 4.23. *Έστω ότι τα γινόμενα* $x_{j-t_1}\cdots x_{j-t_k}$ *και* $x_{j-t_1^*}\cdots x_{j-t_k^*}$ *ανήκουν στην ίδια κλάση ισοδυναμίας. Τότε, υπάρχει ακέραιος* $d \geq 0$*, τέτοιος ώστε να ισχύει*

$$A_{\mathrm{wt}(i)}(t^*, i) = A_{\mathrm{wt}(i)}(t, i)\alpha^{d2^{\mathrm{wt}(t)-\mathrm{wt}(i)}i}$$

όπου $t = 2^{t_1-1} + \cdots + 2^{t_k-1}$ *και* $t^* = 2^{t_1^*-1} + \cdots + 2^{t_k^*-1}$.

Απόδειξη. Βάσει του Ορισμού 4.22, υπάρχει ακέραιος $d \geq 0$, τέτοιος ώστε να ισχύει

$$\begin{aligned} x_{j-t_1^*}\cdots x_{j-t_k^*} &= x_{(j-d)-t_1}\cdots x_{(j-d)-t_k} \\ &= \sum_{l=1}^{k}\sum_{\mathrm{wt}(i)=l} A_l(t,i)\alpha^{-(j-d)2^{k-l}i} \\ &= \sum_{l=1}^{k}\sum_{\mathrm{wt}(i)=l} \left(A_l(t,i)\alpha^{d2^{k-l}i}\right)\alpha^{-j2^{k-l}i} \end{aligned}$$

το οποίο οδηγεί στη σχέση $A_l(t^*, i) = A_l(t, i)\alpha^{d2^{k-l}i}$. □

Έαν τα γινόμενα $x_{j-t_1}\cdots x_{j-t_k}$ και $x_{j-t_1^*}\cdots x_{j-t_k^*}$ είναι ισοδύναμα, τότε βάσει του Ορισμού 4.22 υπάρχει $d \geq 0$, τέτοιος ώστε ο ακέραιος $t^* \in \mathbb{Z}_{2^n}^*$ να γράφεται ως εξής $t^* = 2^d t$. Μεταξύ όλων των γινομένων που ανήκουν στην ίδια κλάση ισοδυναμίας, το γινόμενο που αντιστοιχεί σε περιττό ακέραιο t είναι μοναδικό και ονομάζεται *γινόμενο–επικεφαλής* της κλάσης. Συνεπώς, το Πόρισμα 4.23 οδηγεί στη σχέση

$$A_{\mathrm{wt}(i)}(2^d t, i) = A_{\mathrm{wt}(i)}(t, i)\alpha^{d2^{\mathrm{wt}(t)-\mathrm{wt}(i)}i}. \tag{4.32}$$

Ακόμη και στην απλούστερη περίπτωση μη–γραμμικού φίλτρου f, δηλ. το f να αποτελείται από ένα μόνο γινόμενο, δεν είναι δυνατό να εξασφαλίσουμε ότι η παραγόμενη ακολουθία επιτυγχάνει τη μέγιστη δυνατή τιμή της γραμμικής πολυπλοκότητας. Έχουν πραγματοποιηθεί εξαντλητικές αναζητήσεις, μεταξύ $2 \leq n \leq 9$, για την εύρεση των γινομένων που δεν καταφέρνουν να επιτύχουν τη μέγιστη δυνατή τιμή της γραμμικής πολυπλοκότητας. Τα αποτελέσματα της αναζήτησης εμφανίζονται στον Πίνακα 4.2. Μόνο τα γινόμενα–επικεφαλείς έχουν περιληφθεί, από το Πόρισμα 4.23. Ως παράδειγμα αναφέρουμε την περίπτωση $n = 6$ όπου έχουμε

$$A_2(15, 9) = A_2(30, 9) = A_2(60, 9) = 0$$

Πίνακας 4.2. Οι συντελεστές $A_{\mathrm{wt}(i)}(t,i)$ που μηδενίζονται στο πεπερασμένο σώμα $\mathbb{F}_{2^n}$, για $2 \leq n \leq 9$

n	i	t
4	3	11
6	7	59
	9	15, 19, 53
	21	25, 27, 39, 43, 55, 59
7	11	39
	13	11, 69
	23	23, 57
	43	91
8	3	41, 173
	9	41, 173
	15	173
	17	15, 23, 85, 135, 139, 201, 211, 227, 251
	21	41, 173
	25	45
	27	173
	39	173
	45	173
	51	45, 51, 173, 185, 195, 211, 243, 251
	85	43, 45, 57, 61, 83, 93, 105, 111, 141, 151, 165, 169, 179, 181, 191, 199, 211, 213, 215, 219, 235, 237, 251
	87	173
	119	245, 251
9	3	359
	9	161
	11	407
	17	149, 305
	35	327, 497
	37	415, 501
	39	117, 143
	53	335
	73	41, 57, 99, 105, 113, 141, 145, 149, 181, 229, 241, 287, 305, 307, 345, 363, 367, 441, 443, 457, 469, 487, 491, 495, 505
	77	237
	83	63
	117	187
	219	187, 215, 349, 363, 367, 487, 491, 495, 505

αλλά μόνο ο ακέραιος $t = 15$ περιέχεται στον Πίνακα 4.2, ο οποίος αντιστοιχεί στο γινόμενο $x_{j-1}x_{j-2}x_{j-3}x_{j-4}$.

Για το λόγο αυτό, στις επόμενες υπο–ενότητες πραγματοποιείται λεπτομερής μελέτη ορισμένων ειδικών περιπτώσεων μη–γραμμικών φίλτρων.

4.4.1 Ισαπέχουσες φάσεις

Ας θεωρήσουμε πρώτα την περίπτωση όπου το μη–γραμμικό φίλτρο αποτελείται από ένα μόνο γινόμενο βαθμού k. Επιπρόσθετα, υποθέτουμε ότι το γινόμενο είναι το ακόλουθο

$$y_j = x_{j-t_1} x_{j-t_1-d} \cdots x_{j-t_1-(k-1)d} \tag{4.33}$$

όπου ο ακέραιος d αναγκαστικά πρέπει να ικανοποιεί τον περιορισμό $1 \leq d \leq \lfloor \frac{n-1}{k-1} \rfloor$. Ένα γινόμενο διακριτών φάσεων της ακολουθίας μεγίστου μήκους x που κατασκευάζεται με αυτόν τον τρόπο ονομάζεται *γινόμενο ισαπεχουσών φάσεων*. Κατά συνέπεια, το δεξιό μέρος της (4.23) καθίσταται μία ορίζουσα Vandermonde της οποίας η τιμή δίνεται από τη σχέση [50], [102]

$$A_k(t,i) = \alpha^{it_1} \prod_{1 \leq p < q \leq k} \left(\alpha^{d2^{i_p}} + \alpha^{d2^{i_q}} \right) \tag{4.34}$$

όπου $\mathrm{wt}(i) = k$. Αυτό συνεπάγεται ότι ισχύει $b_i = A_k(t,i) = 0$ έαν και μόνον έαν υπάρχουν ακέραιοι i_p και i_q, με $i_p < i_q$, τέτοιοι ώστε

$$\alpha^{d(2^{i_q - i_p} - 1)} = 1 \Leftrightarrow N \mid d(2^{i_q - i_p} - 1) \Leftrightarrow \frac{N}{2^{\gcd(i_q - i_p, n)} - 1} \mid d.$$

Επειδή ισχύει $0 < i_q - i_p < n$, το Λήμμα 4.5 οδηγεί στη σχέση

$$\frac{N}{2^{\gcd(i_q - i_p, n)} - 1} > d$$

ή ισοδύναμα στην $A_k(t,i) \neq 0$. Συνεπώς, για όλους τους ακεραίους $i \in I$ με δυαδικό βάρος k, ισχύει ότι $b_i \neq 0$ και τελικά η γραμμική πολυπλοκότητα της ακολουθίας y ικανοποιεί την ανισότητα

$$L_y \geq \binom{n}{k}. \tag{4.35}$$

Στη συνέχεια, θα εξετάσουμε την περίπτωση όπου το μη–γραμμικό φίλτρο f είναι το άθροισμα ολισθήσεων ενός γινομένου ισαπεχουσών φάσεων βαθμού k. Επειδή τα συγκεκριμένα γινόμενα ανήκουν στην ίδια κλάση ισοδυναμίας, από την (4.32) και το Θεώρημα 4.20 λαμβάνουμε

$$b_i = \left(r_t A_l(t,i) + r_{2t} A_l(2t,i) + \cdots + r_{2^m t} A_l(2^m t, i) \right)^{2^{l-k}}$$

$$= (r_t + r_{2t}\alpha^i + \cdots + r_{2^m t}\alpha^{mi}) A_l(t,i)^{2^{l-k}} \tag{4.36}$$

για κάθε $1 \leq l \leq k$, όπου $l = \mathrm{wt}(i)$ και $m = n - t_k$. Στην περίπτωση όπου $l = k$, παρατηρήσαμε ότι ο συντελεστής $A_k(t,i)$ είναι διάφορος του μηδενός. Συνεπώς, απομένει να εξασφαλίσουμε ότι για κάθε $i \in I$ με $\mathrm{wt}(i) = k$, το στοιχείο α^i δεν είναι ρίζα του πολυωνύμου

$$g(z) = r_t + r_{2t}z + \cdots + r_{2^m t}z^m. \tag{4.37}$$

Η συγκεκριμένη περίπτωση μελετήθηκε και από τον Rueppel [102], ο οποίος κατέληξε στο ακόλουθο γενικό φράγμα

$$L_y \geq \binom{n}{k} - m. \tag{4.38}$$

Σύμφωνα με το Πόρισμα 2.57, έαν ο ακέραιος n είναι πρώτος αριθμός, τότε ο βαθμός του ελαχίστου πολυωνύμου ενός οποιουδήποτε στοιχείου του πεπερασμένου σώματος $\mathbb{F}_{2^n}$ είναι ίσος με n. Επειδή $\deg(g) < n$, η γραμμική πολυπλοκότητα της ακολουθίας y ικανοποιεί την (4.35).

Στις περιπτώσεις που μελετήθηκαν στις εργασίες [6], [102], οι διακριτές φάσεις $t_1, \ldots, t_k$, των γινομένων που βασίζονται στην ακολουθία μεγίστου μήκους x, ήταν δυνατό να λαμβάνουν τιμές μεγαλύτερες του n. Επιπρόσθετα, κατά τη μελέτη γινομένων ισαπεχουσών φάσεων, ο ακέραιος d ήταν απαραίτητο να ικανοποιεί τον περιορισμό $\gcd(d, N) = 1$. Στη δική μας κατασκευή, ο ακέραιος d είναι δυνατό να είναι οποιοσδήποτε ακέραιος στο διάστημα $1 \leq d \leq \lfloor \frac{n-1}{k-1} \rfloor$.

4.4.2 Κανονικές φάσεις

Στην τρέχουσα ενότητα παραθέτουμε ένα νέο τρόπο επιλογής των φάσεων ενός γινομένου διακριτών φάσεων της ακολουθίας μεγίστου μήκους x. Ας θεωρήσουμε την κανονική βάση $\{\alpha^e, \alpha^{2e}, \ldots, \alpha^{2^{n-1}e}\}$ του πεπερασμένου σώματος $\mathbb{F}_{2^n}$ στο $\mathbb{F}_2$, και ας ορίσουμε το σύνολο των $k \leq n$ στοιχείων

$$W_{s,k} = \left\{2^s e \bmod N, \ldots, 2^{s+k-1} e \bmod N\right\}.$$

Συμβολίζουμε με $W_{s,k}(1)$ το μικρότερο στοιχείο του $W_{s,k}$, με $W_{s,k}(2)$ το μικρότερο στοιχείο του $W_{s,k}$ το οποίο είναι μεγαλύτερο του $W_{s,k}(1)$, κ.λπ. Συνεπώς, έχουμε τη διάταξη

$$W_{s,k}(1) < W_{s,k}(2) < \cdots < W_{s,k}(k). \tag{4.39}$$

Υποθέτουμε ότι οι παράμετροι s και k είναι τέτοιες ώστε να ισχύει

$$W_{s,k}(k) - W_{s,k}(1) < n. \tag{4.40}$$

Τότε, οι φάσεις που απαιτούνται για την κατασκευή ενός γινομένου βαθμού k υπολογίζονται από τη σχέση

$$t_m = W_{s,k}(m) - W_{s,k}(1) + 1 \tag{4.41}$$

για κάθε $1 \leq m \leq k$. Επιπλέον, από τις (4.39) και (4.41), ισχύει η διάταξη $1 \leq t_1 < \cdots < t_k \leq n$.

Ας ορίσουμε το γινόμενο $y_j = x_{j-t_1} \cdots x_{j-t_k}$. Ένα γινόμενο διακριτών φάσεων της ακολουθίας μεγίστου μήκους x που κατασκευάζεται με το συγκεκριμένο τρόπο ονομάζεται *γινόμενο κανονικών φάσεων*. Αντικαθιστώντας τις φάσεις στην (4.23), λαμβάνουμε

$$\begin{aligned} A_k(t,i) &= \alpha^{-i\tau} \begin{vmatrix} \alpha^{e2^{i_1}} & \cdots & \alpha^{e2^{i_k}} \\ \vdots & & \vdots \\ \alpha^{e2^{i_1+k-1}} & \cdots & \alpha^{e2^{i_k+k-1}} \end{vmatrix}^{2^s} \\ &= \alpha^{-i\tau} \prod_{\boldsymbol{c} \in \mathbb{F}_2^k \setminus \{\mathbf{0}\}} \left(c_1 \alpha^{e2^{i_1}} + \cdots + c_k \alpha^{e2^{i_k}} \right)^{2^s} \end{aligned} \tag{4.42}$$

λόγω του Λήμματος 4.16 και της Παρατήρησης 4.17, όπου $\tau = W_{s,k}(1) - 1$. Επειδή τα στοιχεία $\alpha^{2^{i_1}e}, \ldots, \alpha^{2^{i_k}e}$ είναι k διαφορετικά στοιχεία από κανονική βάση, από την (4.42) λαμβάνουμε ότι ο συντελεστής $b_i = A_k(t,i)$ είναι διάφορος του μηδενός για κάθε ακέραιο $i \in I$ με $\mathrm{wt}(i) = k$. Συνεπώς, η γραμμική πολυπλοκότητα της ακολουθίας y ικανοποιεί την (4.35).

Παράδειγμα 4.24. Έστω ότι η ακολουθία μεγίστου μήκους x δίνεται από τη σχέση $x_j = \mathrm{tr}_1^4(\alpha^{-j})$, όπου το $\alpha \in \mathbb{F}_{2^4}$ είναι πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^4}$ και ικανοποιεί τη σχέση $\alpha^4 = \alpha + 1$. Τα στοιχεία $\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$ αποτελούν κανονική βάση του $\mathbb{F}_{2^4}$ στο $\mathbb{F}_2$. Το σύνολο

$$W_{1,3} = \{14, 13, 11\}$$

ικανοποιεί την (4.40), όπου $W_{1,3}(1) = 11$, $W_{1,3}(2) = 13$ και $W_{1,3}(3) = 14$. Από την (4.41) λαμβάνουμε τις φάσεις $t_1 = 1$, $t_2 = 3$, $t_3 = 4$, και το γινόμενο

$$y_j = x_{j-1} x_{j-3} x_{j-4}.$$

Ο ακέραιος 7 είναι ο μοναδικός επικεφαλής κλάσης του συνόλου $\mathbb{Z}_{15}$ του οποίου το δυαδικό βάρος είναι ίσο με 3. Επειδή ισχύει $A_3(13,7) = \alpha^8$, η γραμμική πολυπλοκότητα της ακολουθίας y είναι μεγαλύτερη ή ίση με 4. Πιο συγκεκριμένα, η γραμμική πολυπλοκότητα της y είναι ίση με 14. □

Στη συνέχεια, θα εξετάσουμε την περίπτωση όπου το μη–γραμμικό φίλτρο f είναι το άθροισμα ολισθήσεων ενός γινομένου κανονικών φάσεων βαθμού k. Ο συντελεστής b_i εξακολουθεί να δίνεται από την (4.36), αφού τα συγκεκριμένα γινόμενα ανήκουν στην ίδια κλάση ισοδυναμίας. Αρκεί να εξετάσουμε έαν ισχύει $g(\alpha^i) \neq 0$, για κάθε $i \in I$ με $\mathrm{wt}(i) = k$, όπου το πολυώνυμο $g(z)$ δίνεται από την (4.37), αφού ένα γινόμενο κανονικών φάσεων βαθμού k εξασφαλίζει ότι $A_k(t,i) \neq 0$, για κάθε $i \in I$ με $\mathrm{wt}(i) = k$.

Παράδειγμα 4.25. Έστω ότι η ακολουθία μεγίστου μήκους x δίνεται από τη σχέση $x_j = \mathrm{tr}_1^6(\alpha^{-j})$, όπου το $\alpha \in \mathbb{F}_{2^6}$ είναι πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^6}$ και ικανοποιεί τη σχέση $\alpha^6 = \alpha + 1$. Τα στοιχεία $\{\alpha^{31}, \alpha^{62}, \alpha^{61}, \alpha^{59}, \alpha^{55}, \alpha^{47}\}$ αποτελούν κανονική βάση του $\mathbb{F}_{2^6}$ στο $\mathbb{F}_2$. Το σύνολο

$$W_{1,3} = \{62, 61, 59\}$$

ικανοποιεί την (4.40), όπου $W_{1,3}(1) = 59$, $W_{1,3}(2) = 61$ και $W_{1,3}(3) = 62$. Από την (4.41) λαμβάνουμε τις φάσεις $t_1 = 1$, $t_2 = 3$, $t_3 = 4$, το γινόμενο

$$y_j = r_{13} x_{j-1} x_{j-3} x_{j-4} + r_{26} x_{j-2} x_{j-4} x_{j-5} + r_{52} x_{j-3} x_{j-5} x_{j-6}$$

και το πολυώνυμο $g(z) = r_{13} + r_{26} z + r_{52} z^2$. Τα ελάχιστα πολυώνυμα των επικεφαλείς κλάσεων με δυαδικό βάρος 3 είναι τα ακόλουθα

$$\mu_7(z) = 1 + z^3 + z^6, \qquad \mu_{11}(z) = 1 + z^2 + z^3 + z^5 + z^6,$$
$$\mu_{21}(z) = 1 + z + z^2, \qquad \mu_{13}(z) = 1 + z + z^3 + z^4 + z^6.$$

Συνεπώς, θα πρέπει να διαλέξουμε $g(z) \neq \mu_{21}(z)$. □

4.5 Αποτελεσματικός υπολογισμός της γραμμικής πολυπλοκότητας

Η σχέση (4.19) και το Θεώρημα 4.20 παρέχουν τον τρόπο για τον υπολογισμό της αναπαράστασης ίχνους, και τελικά της γραμμικής πολυπλοκότητας, ακολουθιών μεγίστου μήκους x στις οποίες επιδρούν μη–γραμμικά φίλτρα. Όλοι οι

συντελεστές $b_i \in \mathbb{F}_{2^n}$, εκτός του $b_0 = r_N \in \mathbb{F}_2$, δίνονται στον Πίνακα 4.3, για $2 \leq n \leq 5$. Οι συντελεστές έχουν εκφραστεί βάσει των δεικτών των γινομένων του μη–γραμμικού φίλτρου και της πολυωνυμικής βάσης $\{1, \alpha, \ldots, \alpha^{n-1}\}$ του $\mathbb{F}_{2^n}$ στο $\mathbb{F}_2$ (βλ. Κεφάλαιο 2).

Παράδειγμα 4.26. Έστω ότι η ακολουθία μεγίστου μήκους x δίνεται από τη σχέση $x_j = \mathrm{tr}_1^4(\alpha^{-j})$, όπου το $\alpha \in \mathbb{F}_{2^4}$ είναι πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^4}$ και ικανοποιεί τη σχέση $\alpha^4 = \alpha + 1$. Έστω το μη–γραμμικό φίλτρο

$$y_j = x_{j-4} + x_{j-2}x_{j-3} + x_{j-1}x_{j-2}x_{j-3} + x_{j-1}x_{j-2}x_{j-4}$$

όπου ισχύει $r_6 = r_7 = r_8 = r_{11} = 1$. Από τον Πίνακα 4.3 λαμβάνουμε ότι

$$\begin{aligned} b_1 &= 0, & b_5 &= 1 + \alpha + \alpha^2 = \alpha^{10}, \\ b_3 &= 0, & b_7 &= \alpha + \alpha^3 = \alpha^9. \end{aligned}$$

Από το Θεώρημα 4.20, η ακολουθία y έχει την ακόλουθη αναπαράσταση

$$y_j = \mathrm{tr}_1^2(\alpha^{10}\alpha^{-5j}) + \mathrm{tr}_1^4(\alpha^9\alpha^{-7j}).$$

Η γραμμική πολυπλοκότητα της y είναι 6, μικρότερη της μέγιστης τιμής 14. □

Το μη–γραμμικό φίλτρο f, το οποίο δίνεται από τον Ορισμό 4.1, είναι δυνατό να γραφεί ως ένα $1 \times N$ διάνυσμα

$$\boldsymbol{f} = \begin{pmatrix} r_1 \cdots r_{2^{n-1}} & \cdots & r_{2^{n-1}-1} \cdots r_{2^{n-1}(2^{n-1}-1)} & r_N \end{pmatrix}$$

όπου όλοι οι δείκτες υπολογίζονται modulo N, εκτός του τελευταίου. Οι δείκτες γινομένων r_t κατηγοριοποιούνται σύμφωνα με την κυκλοτομική κλάση στην οποία ανήκει ο ακέραιος $t \in \mathbb{Z}_{2^n}^*$, και στη συνέχεια ταξινομούνται σύμφωνα με την τάξη μεγέθους των επικεφαλείς κλάσεων. Αντίστοιχα, ορίζουμε το $1 \times (n|I^*|+1)$ διάνυσμα

$$\boldsymbol{b} = \begin{pmatrix} b_{1,0} \cdots b_{1,n-1} & \cdots & b_{2^{n-1}-1,0} \cdots b_{2^{n-1}-1,n-1} & b_0 \end{pmatrix}.$$

Έαν ο ακέραιος n είναι πρώτος αριθμός, τότε όλες οι κυκλοτομικές κλάσεις modulo N περιέχουν n στοιχεία, και συνεπώς τα διανύσματα $\boldsymbol{f}$ και $\boldsymbol{b}$ έχουν το ίδιο μέγεθος. Ας ορίσουμε τον $N \times (n|I^*|+1)$ πίνακα $\boldsymbol{R}$ ο οποίος κατασκευάζεται βάσει του Πίνακα 4.3, και είναι τέτοιος ώστε να ισχύει

$$\boldsymbol{b} = \boldsymbol{f} \cdot \boldsymbol{R}. \tag{4.43}$$

Πίνακας 4.3. Οι συντελεστές $b_i = b_{i,0} + b_{i,1}\alpha + \cdots + b_{i,n-1}\alpha^{n-1}$, για $2 \le n \le 5$. Η κυκλοτομική κλάση του 0 περιέχει μόνο το r_N

$\mathbb{F}_{2^2}$: $\alpha^2 + \alpha + 1 = 0$		
1	$b_{1,0}$	$r_{02} + r_{03}$
	$b_{1,1}$	$r_{01} + r_{02}$
$\mathbb{F}_{2^3}$: $\alpha^3 + \alpha + 1 = 0$		
1	$b_{1,0}$	$r_{03} + r_{04} + r_{06} + r_{07}$
	$b_{1,1}$	$r_{01} + r_{03} + r_{04} + r_{07}$
	$b_{1,2}$	$r_{02} + r_{03} + r_{05} + r_{06}$
3	$b_{3,0}$	$r_{03} + r_{06}$
	$b_{3,1}$	$r_{05} + r_{06}$
	$b_{3,2}$	$r_{05} + r_{07}$
$\mathbb{F}_{2^4}$: $\alpha^4 + \alpha + 1 = 0$		
1	$b_{1,0}$	$r_{06} + r_{07} + r_{08} + r_{09} + r_{11} + r_{13}$
	$b_{1,1}$	$r_{01} + r_{03} + r_{06} + r_{08} + r_{09} + r_{12} + r_{14} + r_{15}$
	$b_{1,2}$	$r_{02} + r_{05} + r_{06} + r_{07} + r_{09} + r_{12} + r_{13} + r_{15}$
	$b_{1,3}$	$r_{03} + r_{04} + r_{10} + r_{12} + r_{13} + r_{14}$
3	$b_{3,0}$	$r_{03} + r_{05} + r_{12} + r_{13} + r_{14} + r_{15}$
	$b_{3,1}$	$r_{06} + r_{07} + r_{09} + r_{10}$
	$b_{3,2}$	$r_{03} + r_{05} + r_{06} + r_{07} + r_{09} + r_{13}$
	$b_{3,3}$	$r_{05} + r_{06} + r_{07} + r_{12} + r_{13} + r_{14}$
5	$b_{5,0}$	$r_{06} + r_{07} + r_{09} + r_{10} + r_{11} + r_{12} + r_{13} + r_{15}$
	$b_{5,1}$	$r_{03} + r_{05} + r_{06} + r_{10} + r_{14} + r_{15}$
	$b_{5,2}$	$r_{03} + r_{05} + r_{06} + r_{10} + r_{14} + r_{15}$
	$b_{5,3}$	0
7	$b_{7,0}$	$r_{07} + r_{11} + r_{13} + r_{14}$
	$b_{7,1}$	$r_{07} + r_{15}$
	$b_{7,2}$	$r_{13} + r_{15}$
	$b_{7,3}$	$r_{07} + r_{14}$
$\mathbb{F}_{2^5}$: $\alpha^5 + \alpha^2 + 1 = 0$		
1	$b_{1,0}$	$r_{03} + r_{06} + r_{09} + r_{16} + r_{19} + r_{21} + r_{23} + r_{28} + r_{30} + r_{31}$
	$b_{1,1}$	$r_{01} + r_{03} + r_{06} + r_{09} + r_{11} + r_{12} + r_{13} + r_{15} + r_{18} + r_{25} + r_{29} + r_{31}$
	$b_{1,2}$	$r_{02} + r_{05} + r_{07} + r_{12} + r_{13} + r_{16} + r_{18} + r_{19} + r_{21} + r_{22} + r_{24} + r_{26} + r_{28} + r_{31}$
	$b_{1,3}$	$r_{04} + r_{07} + r_{10} + r_{13} + r_{14} + r_{15} + r_{17} + r_{21} + r_{24} + r_{25} + r_{26} + r_{31}$
	$b_{1,4}$	$r_{03} + r_{08} + r_{14} + r_{15} + r_{19} + r_{20} + r_{25} + r_{26} + r_{27} + r_{28} + r_{29} + r_{30}$
3	$b_{3,0}$	$r_{03} + r_{05} + r_{06} + r_{07} + r_{11} + r_{17} + r_{20} + r_{22} + r_{23} + r_{24} + r_{25} + r_{27} + r_{29} + r_{30}$
	$b_{3,1}$	$r_{07} + r_{12} + r_{13} + r_{17} + r_{19} + r_{20} + r_{22} + r_{26} + r_{28} + r_{29}$
	$b_{3,2}$	$r_{03} + r_{10} + r_{11} + r_{12} + r_{15} + r_{18} + r_{21} + r_{25} + r_{26} + r_{28} + r_{30} + r_{31}$
	$b_{3,3}$	$r_{06} + r_{10} + r_{11} + r_{13} + r_{14} + r_{19} + r_{20} + r_{26} + r_{27} + r_{28}$
	$b_{3,4}$	$r_{03} + r_{05} + r_{06} + r_{09} + r_{10} + r_{11} + r_{12} + r_{13} + r_{14} + r_{17} + r_{18} + r_{20} + r_{22} + r_{23} + r_{25} + r_{28} + r_{29} + r_{31}$

συνεχίζεται στην επόμενη σελίδα...

...συνέχεια από την προηγούμενη σελίδα

5	$b_{5,0}$	$r_{07}+r_{10}+r_{12}+r_{13}+r_{14}+r_{18}+r_{19}+r_{21}+r_{26}+r_{27}+r_{28}+r_{31}$
	$b_{5,1}$	$r_{06}+r_{09}+r_{13}+r_{15}+r_{17}+r_{19}+r_{21}+r_{24}+r_{25}+r_{30}$
	$b_{5,2}$	$r_{09}+r_{10}+r_{11}+r_{12}+r_{14}+r_{15}+r_{19}+r_{20}+r_{21}+r_{22}+r_{23}+r_{24}+$ $r_{25}+r_{26}+r_{30}+r_{31}$
	$b_{5,3}$	$r_{05}+r_{06}+r_{09}+r_{10}+r_{12}+r_{18}+r_{20}+r_{23}+r_{25}+r_{27}+r_{29}+r_{30}$
	$b_{5,4}$	$r_{03}+r_{06}+r_{09}+r_{12}+r_{13}+r_{20}+r_{21}+r_{22}+r_{23}+r_{26}+r_{28}+r_{29}+$ $r_{30}+r_{31}$
7	$b_{7,0}$	$r_{11}+r_{14}+r_{19}+r_{21}+r_{22}+r_{23}+r_{28}+r_{29}$
	$b_{7,1}$	$r_{07}+r_{13}+r_{21}+r_{23}+r_{25}+r_{26}+r_{28}+r_{29}+r_{30}+r_{31}$
	$b_{7,2}$	$r_{13}+r_{14}+r_{21}+r_{22}+r_{23}+r_{26}+r_{27}+r_{28}+r_{29}+r_{30}$
	$b_{7,3}$	$r_{11}+r_{13}+r_{14}+r_{15}+r_{19}+r_{23}+r_{25}+r_{28}+r_{29}+r_{31}$
	$b_{7,4}$	$r_{15}+r_{19}+r_{21}+r_{23}+r_{28}+r_{30}$
11	$b_{11,0}$	$r_{11}+r_{14}+r_{21}+r_{22}+r_{26}+r_{28}+r_{29}+r_{31}$
	$b_{11,1}$	$r_{11}+r_{19}+r_{22}+r_{25}+r_{26}+r_{28}+r_{29}+r_{30}$
	$b_{11,2}$	$r_{07}+r_{13}+r_{15}+r_{27}+r_{28}+r_{29}+r_{30}+r_{31}$
	$b_{11,3}$	$r_{07}+r_{11}+r_{15}+r_{19}+r_{21}+r_{22}+r_{23}+r_{30}$
	$b_{11,4}$	$r_{11}+r_{13}+r_{15}+r_{19}+r_{25}+r_{27}+r_{29}+r_{30}$
15	$b_{15,0}$	$r_{23}+r_{27}$
	$b_{15,1}$	$r_{29}+r_{30}$
	$b_{15,2}$	$r_{15}+r_{27}+r_{29}+r_{30}$
	$b_{15,3}$	$r_{15}+r_{23}+r_{27}+r_{29}$
	$b_{15,4}$	$r_{15}+r_{27}+r_{30}+r_{31}$

Έαν ο ακέραιος n είναι πρώτος αριθμός, τότε ο πίνακας $\boldsymbol{R}$ είναι τετραγωνικός. Όλοι οι πίνακες θεωρούμε ότι είναι block πίνακες. Το διάνυσμα $\boldsymbol{b}$ έχει $|I^*|$ blocks μεγέθους n και ένα block μεγέθους 1, ενώ τα μεγέθη των blocks στο διάνυσμα $\boldsymbol{f}$ καθορίζονται από τον αριθμό των στοιχείων n_i που περιλαμβάνονται στην κυκλοτομική κλάση του $i \in I$.

Έστω ότι ο αριθμός των μηδενικών blocks, μεγέθους n, στο διάνυσμα $\boldsymbol{b}$ είναι ίσος με K. Τότε, έαν ο ακέραιος n είναι πρώτος αριθμός, η γραμμική πολυπλοκότητα της ακολουθίας y, η οποία καθορίζεται μοναδικά από το διάνυσμα $\boldsymbol{f}$, δίνεται από τη σχέση

$$L_y = n(|I^*| - K) + b_0. \tag{4.44}$$

Παράδειγμα 4.27. Έστω ότι η ακολουθία μεγίστου μήκους x δίνεται από τη σχέση $x_j = \mathrm{tr}_1^3(\alpha^{-j})$, όπου το $\alpha \in \mathbb{F}_{2^3}$ είναι πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^3}$ και ικανοποιεί τη σχέση $\alpha^3 = \alpha + 1$. Τότε, έχουμε ότι

$$\boldsymbol{f} = \begin{pmatrix} r_1 & r_2 & r_4 & r_3 & r_6 & r_5 & r_7 \end{pmatrix}$$

και

$$\boldsymbol{b} = \begin{pmatrix} b_{1,0} & b_{1,1} & b_{1,2} & b_{3,0} & b_{3,1} & b_{3,2} & b_0 \end{pmatrix}.$$

Επιπρόσθετα, από τον Πίνακα 4.3, λαμβάνουμε

$$\boldsymbol{R} = \begin{pmatrix} 0\,1\,0 & 0\,0\,0 & 0 \\ 0\,0\,1 & 0\,0\,0 & 0 \\ 1\,1\,0 & 0\,0\,0 & 0 \\ 1\,1\,1 & 1\,0\,0 & 0 \\ 1\,0\,1 & 1\,1\,0 & 0 \\ 0\,0\,1 & 0\,1\,1 & 0 \\ 1\,1\,0 & 0\,0\,1 & 1 \end{pmatrix}.$$

Ο πίνακας $\boldsymbol{R}$ είναι τετραγωνικός, αφού το 3 είναι πρώτος αριθμός. □

Ο πίνακας $\boldsymbol{R}$ παρουσιάζει ορισμένες πολύ ενδιαφέρουσες ιδιότητες. Πράγματι, ισχύουν τα ακόλουθα:

- ο $\boldsymbol{R}$ είναι ένας block κάτω τριγωνικός πίνακας, του οποίου το μέγεθος του κάθε block καθορίζεται από τα μεγέθη των blocks των διανυσμάτων $\boldsymbol{f}$ και $\boldsymbol{b}$ αντίστοιχα,
- το άνω αριστερό $n \times n$ block είναι ίσο με τον πίνακα $\boldsymbol{\Delta}$ που καθορίζεται από το πολυώνυμο ανάδρασης του καταχωρητή ολίσθησης (βλ. Κεφάλαιο 3),
- το άθροισμα των στοιχείων κάθε στήλης του $\boldsymbol{R}$, εκτός της τελευταίας, είναι άρτιος αριθμός, και
- η ακόλουθη εικασία έχει επιβεβαιωθεί για μικρές πρώτες τιμές του n.

Εικασία 4.28. Εαν ο ακέραιος n είναι πρώτος αριθμός, τότε ο πίνακας $\boldsymbol{R}$ είναι αντιστρέψιμος.

Έαν η Εικασία 4.28 είναι αληθής, τότε είναι δυνατό να βρούμε ένα μη–γραμμικό φίλτρο f, το οποίο αντιστοιχεί στο διάνυσμα $\boldsymbol{f} = \boldsymbol{b} \cdot \boldsymbol{R}^{-1}$ και παράγει την ακολουθία y φιλτράροντας την $x_j = \mathrm{tr}_1^n(\alpha^{-j})$, απλά επιλέγοντας το διάνυσμα $\boldsymbol{b}$ ή ισοδύναμα θέτοντας την γραμμική πολυπλοκότητα της παραγόμενης ακολουθίας y σε μία επιθυμητή τιμή.

Σε μία τέτοια περίπτωση, από τον ορισμό του διανύσματος $\boldsymbol{b}$, υπάρχουν $N^{|I|}$ λογικές συναρτήσεις f με n μεταβλητές, τέτοιες ώστε $f(0,\ldots,0) = 0$, οι οποίες παράγουν ακολουθίες γραμμικής πολυπλοκότητας $N = 2^n - 1$, όπου ο ακέραιος n είναι πρώτος αριθμός.

Κεφάλαιο 5

Ελάχιστη προσέγγιση ακολουθιών

Ανάλογα με το πεδίο εφαρμογής των δυαδικών ακολουθιών, σχηματίζονται και οι αντίστοιχες απαιτήσεις ύπαρξης συγκεκριμένων ιδιοτήτων, όπως μεγάλη περίοδο, ισοκατανομή άσσων και μηδενικών, δίτιμη συνάρτηση αυτοσυσχέτισης, και μεγάλη γραμμική πολυπλοκότητα [42], [56]. Η χρήση ακολουθιών με μεγάλη γραμμική πολυπλοκότητα δεν είναι πάντα αρκετή για να εξασφαλίσει ότι οι συγκεκριμένες ακολουθίες είναι ασφαλείς. Χαρακτηριστικό είναι το παράδειγμα της ακολουθίας που αντιστοιχεί στο διάνυσμα

$$\begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix}$$

μήκους N. Η γραμμική πολυπλοκότητα της ακολουθίας είναι η μέγιστη δυνατή, δηλ. ίση με N, αλλά παρατηρούμε ότι η συγκεκριμένη ακολουθία μπορεί να προσεγγιστεί από τη μηδενική ακολουθία της οποίας η γραμμική πολυπλοκότητα είναι μηδέν.

Στην πράξη, μικρές αποκλίσεις από μία δοθείσα ακολουθία είναι αποδεκτές από πολλές εφαρμογές έαν αυτή η απόκλιση αποφέρει σημαντικό όφελος όσον αφορά τη γραμμική πολυπλοκότητα της ακολουθίας. Το πρόβλημα της παραγωγής κατά προσέγγιση ταιριάζει απόλυτα στο συγκεκριμένο πεδίο εφαρμογών. Ας θεωρήσουμε ότι το διάνυσμα

$$\boldsymbol{x} = \begin{pmatrix} x_0 & \cdots & x_{N-1} \end{pmatrix}$$

περιέχει τα πρώτα N στοιχεία της ακολουθίας x και έστω $\boldsymbol{e}_m$ είναι ένα δυαδικό διάνυσμα βάρους 1, όπου ο μοναδικός άσσος βρίσκεται στη θέση m, με $m \in \mathbb{Z}_N$.

Ορίζουμε την ακολουθία $y_m = x + e_m$, η οποία είναι το άθροισμα (modulo 2) των ακολουθιών x και e_m. Το πρόβλημα της παραγωγής κατά προσέγγιση είναι ισοδύναμο με το ακόλουθο πρόβλημα ελαχιστοποίησης

$$\mathrm{wc}_1(x) \triangleq \min_{m \in \mathbb{Z}_N} L_{y_m}. \tag{5.1}$$

Η ποσότητα $\mathrm{wc}_1(x)$ είναι γνωστή στη βιβλιογραφία ως η *πολυπλοκότητα βάρους* της ακολουθίας x [15], [18]. Είναι προφανές ότι το πρόβλημα προσέγγισης ακολουθιών παρέχει χρήσιμα αποτελέσματα έαν η πολυπλοκότητα βάρους $\mathrm{wc}_1(x)$ είναι μικρότερη της γραμμικής πολυπλοκότητας L_x της αρχικής ακολουθίας. Στις ακόλουθες ενότητες διερευνούμε για την ύπαρξη αναγκαίων συνθηκών ώστε να ισχύει $\mathrm{wc}_1(x) < L_x$.

Η βέλτιστη θέση $m = m^{\mathrm{opt}}$ στην οποία πρέπει να πραγματοποιηθεί το λάθος, δεν είναι πάντα μοναδικά ορισμένη, αναφέρεται ως η *βέλτιστη φάση*. Κατ΄ αντιστοιχία, η λαμβανόμενη ακολουθία $y_{m^{\mathrm{opt}}}$ ονομάζεται *βέλτιστη προσέγγιση πρώτης τάξης* της ακολουθίας x, και συμβολίζεται με $x^{(1)}$. Ο καταχωρητής ολίσθησης γραμμικής ανάδρασης, με πολυώνυμο ανάδρασης $f^{(1)}(z)$, που παράγει την $x^{(1)}$ αναφέρεται ως *γραμμικό κύκλωμα προσέγγισης πρώτης τάξης* της ακολουθίας x. Η έννοια του *προφίλ της γραμμικής πολυπλοκότητας με πραγματοποίηση ενός λάθους* είναι άμεσα συνδεδεμένη με τους προηγούμενους ορισμούς, και αναπαριστά το μέγεθος μεταβολής της γραμμικής πολυπλοκότητας σε σχέση με τη θέση που πραγματοποιείται το ένα λάθος.

Η επίλυση του προβλήματος παραγωγής ακολουθιών κατά προσέγγιση αποτελεί αντικείμενο μελέτης του παρόντος κεφαλαίου. Πρόκειται να παρουσιάσουμε τρεις μεθόδους εύρεσης της βέλτιστης φάσης, πιο συγκεκριμένα τις μεθόδους διαδοχικών διαιρέσεων, εξισώσεων ισοδυναμίας, και συγχρονισμού φάσεων. Η πρώτη μέθοδος βασίζεται στη διαδοχική εφαρμογή του αλγορίθμου του Ευκλείδη χρησιμοποιώντας παράγοντες του ελαχίστου πολυωνύμου της ακολουθίας x. Η δεύτερη μέθοδος λειτουργεί στο χώρο των συχνοτήτων και προσδιορίζει τη βέλτιστη φάση επιλύωντας ένα σύνολο εξισώσεων ισοδυναμίας. Επιπλέον, αναλύεται η επιλυσιμότητα των εξισώσεων και παράγεται ένα σύνολο κλειστών τύπων. Τέλος, η τρίτη μέθοδος βασίζεται στην αναπαράσταση ίχνους της ακολουθίας και στην έννοια της κυκλικής ισοδυναμίας ώστε να προσδιορίσει τη θέση m^{opt} [60], [63].

Έννοιες όπως η υλοποίηση αλγορίθμων για την εύρεση της βέλτιστης φάσης, σχεδίασης και χαρακτηρισμού ακολουθιών σχετίζονται με το πρόβλημα παραγωγής ακολουθιών κατά προσέγγιση. Η υλοποίηση αλγορίθμων αφορά κυρίως το σχεδιασμό αποτελεσματικών αλγορίθμων για τον καθορισμό των αγνώστων

$$\mathrm{wc}_1(x),\ m^{\mathrm{opt}},\ x^{(1)},\ \text{και}\ f^{(1)}(z).$$

Στο κλασσικό βιβλίο των Cusick, Ding, και Renvall [15] δίνεται ένας αλγόριθμος, που ακολουθεί μία προσέγγιση αποκωδικοποίησης, για τον προσδιορισμό της βέλτιστης φάσης του οποίου όμως η υπολογιστική πολυπλοκότητα είναι υψηλή. Επιπλέον, δεν παρέχει γνώση όσον αφορά το σχεδιασμό ακολουθιών ανθεκτικών σε επιθέσεις προσέγγισης. Κατά τη μελέτη κάθε μίας από τις προτεινόμενες μεθόδους, δίνονται και αλγόριθμοι υλοποίησης των συγκρκριμένων σχημάτων.

Ο σχεδιασμός ακολουθιών αφορά κυρίως τη διερεύνηση τρόπων παραγωγής ακολουθιών οι οποίες, εκτός άλλων ιδιοτήτων, θα χαρακτηρίζονται από ιδιαίτερα υψηλές τιμές γραμμικής πολυπλοκότητας. Δίνεται στο τέλος του κεφαλαίου ένα σύνολο κατευθύνσεων.

Ο χαρακτηρισμός ακολουθιών αφορά την κατάλληλη περιγραφή ακολουθιών x των οποίων οι προσεγγίσεις πρώτης τάξης έχουν δοθείσα γραμμική πολυπλοκότητα. Ιδιαίτερα μεγάλης σημασίας είναι οι ακολουθίες εκείνες για τις οποίες ισχύει $\mathrm{wc}_1(x) \geq L_x$. Τέτοιες ακολουθίες ονομάζονται *ανθεκτικές* καθώς προσεγγίσεις πρώτης τάξης δε μειώνουν τη γραμμική τους πολυπλοκότητα. Μελέτες, όπως οι [15], [19] και [70], που διερευνούν το προφίλ της γραμμικής πολυπλοκότητας ακολουθιών μετά τη προσέγγισή τους πραγματοποιώντας ένα λάθος, πραγματεύονται άμεσα ή έμμεσα θέματα χαρακτηρισμού ακολουθιών.

Σε αντίθεση με τις ανωτέρω μελέτες, διερευνούμε την πιο ενδιαφέρουσα περίπτωση δυαδικών ακολουθιών περιόδου $N = 2^n - 1$. Οι συγκεκριμένες ακολουθίες παράγονται από τυπικά μη–γραμμικά κυκλώματα (βλ. Κεφάλαιο 4). Επιπλέον, δεν προσδιορίζουμε μόνο την πολυπλοκότητα βάρους $\mathrm{wc}_1(x)$, αλλά και θέση λάθους m^{opt} και κατά συνέπεια τη βέλτιστη ακολουθία προσέγγισης $x^{(1)}$ πρώτης τάξης.

5.1 Κυκλική ισοδυναμία ακολουθιών

Ας θεωρήσουμε τη δυαδική ακολουθία $x = \{x_j\}_{j\geq 0}$, περιόδου $N = 2^n - 1$, η οποία παράγεται από το μοντέλο Fibonacci (Σχ. 3.2) ενός καταχωρητή ολίσθησης

γραμμικής ανάδρασης, με πολυώνυμο ανάδρασης

$$f^*(z) = f_0^*(z) \cdots f_{K-1}^*(z). \tag{5.2}$$

Τα πολυώνυμα $f_i(z)$, με $i \in \mathbb{Z}_K$, είναι ανάγωγα βαθμού n_i, όπου ο ακέραιος n_i διαιρεί το n (βλ. Κεφάλαιο 2). Το πολυώνυμο $f(z)$ είναι το ελάχιστο πολυώνυμο της ακολουθίας x, η οποία έχει γραμμική πολυπλοκότητα

$$L_x = n_0 + \cdots + n_{K-1}.$$

Έστω το στοιχείο α είναι ένα πρωταρχικό στοιχείο του πεπερασμένου σώματος $\mathbb{F}_{2^n}$ και έστω ότι το $\alpha^{s_i} \in \mathbb{F}_{2^{n_i}}^*$ αποτελεί ρίζα του πολυωνύμου $f_i^*(z)$. Θεωρούμε ότι ο ακέραιος s_i είναι ο επικεφαλής της κυκλοτομικής κλάσης C_{s_i}. Σύμφωνα με το Κεφάλαιο 3, η ακολουθία x γράφεται ως εξής

$$x_j = \sum_{i=0}^{K-1} x_j^i = \sum_{i=0}^{K-1} \mathrm{tr}_1^{n_i}(\gamma_i \alpha^{t_i j}) \tag{5.3}$$

όπου ο ακέραιος t_i είναι ο επικεφαλής της κυκλοτομικής κλάσης C_{-s_i} και ο συντελεστής γ_i ανήκει στο σύνολο $\mathbb{F}_{2^{n_i}}^*$.

Ας θεωρήσουμε την ακολουθία $\{X_k\}_{k\geq 0}$ που αντιστοιχεί στο διακριτό μετασχηματισμό Fourier της x. Στο Κεφάλαιο 3 αποδείχθηκε ότι για κάθε $k \in C_{s_i}$ υπάρχουν ακέραιοι t_i, b, με $0 \leq b < n_i$, τέτοιοι ώστε

$$X_{-2^b t_i} = \gamma_i^{2^b}. \tag{5.4}$$

Το αποτέλεσμα που αποδεικνύουμε στη συνέχεια αφορά κλάσεις ισοδυναμίας ακολουθιών που παράγονται από τον ίδιο καταχωρητή ολίσθησης γραμμικής ανάδρασης.

Λήμμα 5.1. *Ας θεωρήσουμε τη συνάρτηση $g_\gamma(z) = \mathrm{tr}_1^n(\gamma z^t)$, όπου $\gamma \in \mathbb{F}_{2^n}^*$, $t \in \mathbb{Z}_N$, και έστω ότι ο ακέραιος d είναι ο μέγιστος κοινός διαιρέτης των t και N. Ορίζουμε το σύνολο*

$$S = \left\{ x_c : x_c = \{g_{\alpha^c}(\alpha^j)\}_{j\geq 0},\ 0 \leq c < d \right\}.$$

Τότε, για κάθε ακολουθία $x = \{g_\gamma(\alpha^j)\}_{j\geq 0}$, υπάρχει ακέραιος c, με $0 \leq c < d$, τέτοιος ώστε $x \sim x_c$.

Απόδειξη. Έστω ο ακέραιος $q \in \mathbb{Z}_N$ είναι τέτοιος ώστε να ισχύει $\gamma = \alpha^q$. Το σύνολο των ακολουθιών της μορφής $x = \{g_\gamma(\alpha^j)\}_{j\geq 0}$ διαμερίζεται σε d κλάσεις ισοδυναμίας αφού οι τάξεις και των δύο στοιχείων α^t και α^d είναι ίσες με N/d. Εφαρμογή του αλγορίθμου του Ευκλείδη δίνει το ακόλουθο αποτέλεσμα

$$q = ud + c, \qquad 0 \leq c < d.$$

Συνεπώς ισχύει

$$\gamma = \alpha^{c+ud} = \alpha^{c-t\nu} \tag{5.5}$$

όπου

$$\nu = -u(\frac{t}{d})^{\varphi(\frac{N}{d})-1} \bmod \frac{N}{d}$$

και $\varphi(\cdot)$ είναι η συνάρτηση του Euler. Εύκολα διακρίνουμε από την (5.5) ότι η ακολουθία x είναι ισοδύναμη με την x_c, και ότι ο ακέραιος ν είναι ίσος με τον αριθμό των δεξιών κυκλικών ολισθήσεων που απαιτούνται ώστε να λάβουμε την x από την x_c. □

Οι ακολουθίες που περιλαμβάνονται στο σύνολο S δεν είναι κυκλικά ισοδύναμες μεταξύ τους και ονομάζονται *επικεφαλείς κλάσεων*. Επιπλέον, μόνον η ακολουθία x_0 χαρακτηρίζεται από την ιδιότητα ότι έχει σταθερή τιμή σε θέσεις που αντιστοιχούν στην ίδια κυκλοτομική κλάση.

Όλες οι μη–μηδενικές ακολουθίες που παράγονται από το ίδιο πρωταρχικό ελάχιστο πολυώνυμο είναι κυκλικά ισοδύναμες μεταξύ τους. Στη συγκεκριμένη περίπτωση ισχύει $d = 1$, και η ακολουθία x_0 αντιστοιχεί στη χαρακτηριστική φάση της x [33], [34].

5.2 Η μέθοδος των διαδοχικών διαιρέσεων

Σύμφωνα με το Κεφάλαιο 3, η τυπική αναπαράσταση δυναμοσειράς της ακολουθίας x γράφεται στην ακόλουθη μορφή

$$\sum_{j=0}^{\infty} x_j z^j = \frac{x(z)}{1+z^N} = \frac{r(z)}{f^*(z)}, \qquad \deg(r) < \deg(f^*)$$

όπου τα πολυώνυμα $r(z)$ και $f^*(z)$ είναι πρώτα μεταξύ τους, και το $f^*(z)$ αναλύεται σε γινόμενο πρώτων παραγόντων σύμφωνα με την (5.2). Από την ανωτέρω

σχέση συνεπάγεται ότι

$$x(z) = r(z)\frac{1+z^N}{f^*(z)} = r(z)h^*(z) \tag{5.6}$$

όπου τα πολυώνυμα $h^*(z) = (1+z^N)/f^*(z)$ και $f^*(z)$ είναι επίσης πρώτα μεταξύ τους. Έστω οι ακολουθίες y_m και e_m είναι οι περιοδικές επεκτάσεις των διανυσμάτων $\boldsymbol{y}_m$ και $\boldsymbol{e}_m$ αντίστοιχα. Προφανώς ισχύει $y_m = x + e_m$ και

$$\sum_{j=0}^{\infty} y_{m,j} z^j = \frac{x(z) + z^m}{1+z^N} = \frac{y_m(z)}{1+z^N}. \tag{5.7}$$

Από την (5.7), η γραμμική πολυπλοκότητα της ακολουθίας προσέγγισης y_m δίνεται από τη σχέση

$$L_{y_m} = N - \deg \gcd(y_m(z), 1+z^N).$$

Κατά συνέπεια, το πρόβλημα ελαχιστοποίησης, όπως εκφράζεται από την (5.1), καταλήγει στη μεγιστοποίηση της

$$\mathrm{wc}_1(x) = N - \max_{m \in \mathbb{Z}_N} \deg \gcd(y_m(z), 1+z^N). \tag{5.8}$$

Λήμμα 5.2. *Ο μέγιστος κοινός διαιρέτης των πολυωνύμων $y_m(z)$ και $1+z^N$ διαιρεί το $f^*(z)$.*

Απόδειξη. Ας υποθέσουμε ότι το πολυώνυμο $g(z)$ είναι πρώτος παράγοντας του μέγιστου κοινού διαιρέτη των $y_m(z)$ και $1+z^N$. Τότε, το $g(z)$ διαιρεί ταυτόχρονα το $y_m(z)$ και $1+z^N$ αντίστοιχα. Επειδή

$$1 + z^N = h(z)f(z)$$

τα πολυώνυμα $h(z)$ και $f(z)$ είναι πρώτα μεταξύ τους, και συνεπώς το $g(z)$ διαιρεί ένα από τα $h^*(z)$ και $f^*(z)$, αλλά όχι και τα δύο ταυτόχρονα.

Έστω ότι το πολυώνυμο $g(z)$ διαιρεί το $h^*(z)$. Τότε, από την (5.7) λαμβάνουμε ότι το $g(z)$ αναγκαστικά διαιρεί το μονόνυμο z^m, λόγω της αρχικής υπόθεσης ότι το $g(z)$ διαιρεί το πολυώνυμο

$$y_m(z) = x(z) + z^m = r(z)h^*(z) + z^m.$$

Συνεπώς, καταλήγουμε σε άτοπο και αναγκαστικά θα πρέπει το πολυώνυμο $g(z)$ να είναι παράγοντας του $f^*(z)$. □

Καθώς ο ακέραιος m διατρέχει τις τιμές του συνόλου $\mathbb{Z}_N$, καταλήγουμε στο συμπέρασμα ότι η κωδική λέξη που αντιστοιχεί στο πολυώνυμο $y_m(z)$ είτε ανήκει στο γραμμικό κυκλικό κώδικα που παράγεται από ένα υποσύνολο παραγόντων του $f^*(z)$, είτε είναι πρώτο προς αυτό, λόγω του Λήμματος 5.2.

Πόρισμα 5.3. *Ο ακέραιος $m = m^{opt}$ για τον οποίο το πολυώνυμο $y_{m^{opt}}(z)$ διαιρείται από το μεγίστου δυνατού βαθμού παράγοντα του $f^*(z)$ αποτελεί βέλτιστη φάση της ακολουθίας x.*

Από την υπόθεση του Πορίσματος 5.3 συνεπάγεται ότι πρέπει ο βαθμός του μέγιστου κοινού διαιρέτη των πολυωνύμων $y_m(z)$ και $1 + z^N$ να είναι μικρότερος ή ίσος της γραμμικής πολυπλοκότητας της ακολουθίας x. Έαν συνδυάσουμε το αποτέλεσμα αυτό με την (5.8) λαμβάνουμε

$$N - L_x \leq \mathrm{wc}_1(x). \tag{5.9}$$

Προφανώς, έχει νόημα η χρήση του αποτελέσματος της προσέγγισης έαν η πολυπλοκότητα βάρους της ακολουθίας x είναι μικρότερη της γραμμικής της πολυπλοκότητας. Συνεπώς, λόγω της σχέσης (5.9) λαμβάνουμε την ανισότητα

$$N - L_x \leq \mathrm{wc}_1(x) < L_x$$

η οποία με τη σειρά της οδηγεί στην ακόλουθη αναγκαία αλλά όχι ικανή συνθήκη $N < 2L_x$.

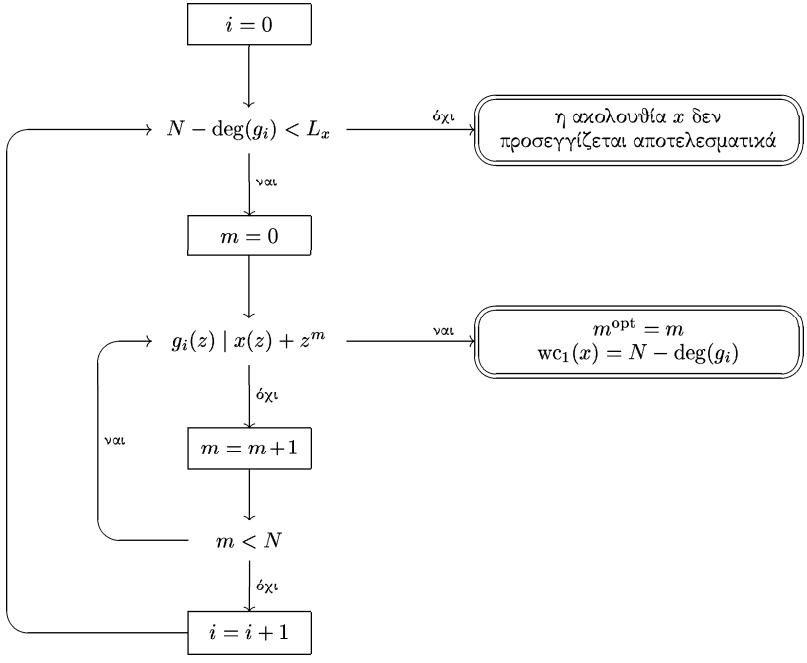
Η βέλτιστη φάση της ακολουθίας x υπολογίζεται βάσει του Πορίσματος 5.3 και ο αντίστοιχος αλγόριθμος δίνεται στο Σχ. 5.1. Η λογική του αλγορίθμου βασίζεται στη διαδοχική εφαρμογή διαιρέσεων με κάποιο παράγοντα του πολυωνύμου $f^*(z)$. Έστω ότι το σύνολο

$$G = \{g_0(z), \ldots, g_{2^K-1}(z)\}$$

περιλαμβάνει όλους τους δυνατούς παράγοντες του πολυωνύμου $f^*(z)$ διατεταγμένους με φθίνουσα σειρά των βαθμών τους, δηλ.

$$\forall\, i < j \;\Rightarrow \deg(g_i(z)) \geq \deg(g_j(z)).$$

Στη συνέχεια, ελέγχεται έαν το πολυώνυμο $g_i(z)$ διαιρεί το $y_m(z)$, για όλες τις δυνατές τιμές του m, αρχίζοντας με την $g_0(z) = f^*(z)$. Ο αλγόριθμος επιστρέφει



Σχήμα 5.1. Ο αλγόριθμος διαδοχικών διαιρέσεων. Εξάγει τη θέση m του λάθους και τη γραμμική πολυπλοκότητα της ακολουθίας προσέγγισης

τη βέλτιστη φάση m^{opt} και την πολυπλοκότητα βάρους $\text{wc}_1(x)$ που αντιστοιχεί στη συγκεκριμένη θέση.

Η πολυπλοκότητα του αλγορίθμου των διαδοχικών διαιρέσεων οφείλεται κυρίως στον υπολογισμό του υπολοίπου της διαίρεσης του πολυωνύμου $y_m(z)$ με το $g_i(z)$ για κάθε $m \in \mathbb{Z}_N$. Το πλήθος των αριθμητικών πράξεων που απαιτούνται για τη διαίρεση είναι ανάλογο με [58]

$$\deg(g_i(z))\Big(\deg(y_m(z)) - \deg(g_i(z)) + 1\Big)$$

όπου

$$N - L_x < \deg(g_i(z)) \leq L_x \qquad \text{και} \qquad \deg(y_m(z)) \in \mathbb{Z}_N.$$

Η διαίρεση είναι δυνατό να υλοποιηθεί σε υλικό μέσω ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης με πολυώνυμο ανάδρασης το $g_i(z)$ [73]. Συνεπώς, γίνεται χρήση το πολύ L_x βαθμίδων μνήμης.

Η κυρίως διαδικασία επαναλαμβάνεται το πολύ $|G'|$ φορές, όπου G' είναι το υποσύνολο του G που αποτελείται από τα πολυώνυμα με βαθμό μεγαλύτερο από $N - L_x$. Ο αλγόριθμος του Σχ. 5.1 θεωρεί την παραγοντοποίηση του πολυωνύμου $f(z)$ ως στάδιο προ–υπολογισμού. Η παραγοντοποίηση είναι δυνατό να υλοποιηθεί με τον αλγορίθμο του Berlekamp [58], ο οποίος απαιτεί

$$O(L_x^3 + 2KL_x^2)$$

βήματα. Το πλήθος K των παραγόντων του πολυωνύμου $f(z)$ παίρνει τιμές από 1 έως τον αριθμό των κυκλοτομικών κλάσεων (modulo N) και προσεγγίζεται από την ποσότητα $\ln L_x$ (βλ. Κεφάλαιο 2). Σημαντική μείωση του πλήθους των αριθμητικών πράξεων που απαιτούνται επιτυγχάνεται με τη μέθοδο που περιγράφεται στη συνέχεια.

Ορισμός 5.4. Ας θεωρήσουμε τον πίνακα γεννήτορα $\boldsymbol{F}$, σε μη–συστηματική μορφή [9], του γραμμικού κυκλικού κώδικα $\mathcal{F}$ και έστω ότι $n > 0$. Ο πίνακας που λαμβάνεται προσθέτοντας στο τέλος n γραμμές και στήλες ονομάζεται *επεκτεταμένος πίνακας γεννήτορας* και συμβολίζεται με $\boldsymbol{F}^{[n]}$.

Παρατήρηση 5.5. Αντίστοιχα ορίζεται και ο *συρρικνωμένος πίνακας γεννήτορας* $\boldsymbol{F}^{[-n]}$ ο οποίος λαμβάνεται από τον $\boldsymbol{F}$ διαγράφοντας από το τέλος n γραμμές και στήλες.

Έστω $\boldsymbol{F}$ και $\widehat{\boldsymbol{F}}$ είναι οι πίνακες γεννήτορες των $(N, N-k)$ γραμμικών κυκλικών κωδίκων που παράγονται από τα πολυώνυμα $f(z)$ και $f^*(z)$ αντίστοιχα. Τότε, οι πίνακες $\boldsymbol{F}$ και $\widehat{\boldsymbol{F}}$ συνδέονται με τη σχέση

$$\widehat{\boldsymbol{F}} = \boldsymbol{J}_{N-k}\, \boldsymbol{F}\, \boldsymbol{J}_N \tag{5.10}$$

όπου $\boldsymbol{J}_n$ είναι ο $n \times n$ πίνακας αντιστροφής διάταξης (βλ. Κεφάλαιο 3). Ας υποθέσουμε ότι το πολυώνυμο $f^*(z)$ γράφεται ως

$$f^*(z) = g_i(z) g_j(z) \tag{5.11}$$

όπου τα $g_i(z)$ και $g_j(z)$ είναι πρώτα μεταξύ τους και ανήκουν στο σύνολο G. Έστω $\boldsymbol{G}_i$ και $\boldsymbol{G}_j$ είναι οι πίνακες γεννήτορες των $(N, N-k_i)$ και $(N, N-k_j)$ γραμμικών κυκλικών κωδίκων που παράγονται από τα πολυώνυμα $g_i(z)$ και $g_j(z)$ αντίστοιχα. Προφανώς, ισχύει $k = k_i + k_j$ και ο πίνακας $\widehat{\boldsymbol{F}}$ γράφεται

$$\widehat{\boldsymbol{F}} = \boldsymbol{G}_j^{[-k_i]}\, \boldsymbol{G}_i = \boldsymbol{G}_i^{[-k_j]}\, \boldsymbol{G}_j. \tag{5.12}$$

Θεώρημα 5.6. *Ας θεωρήσουμε ότι το ανάστροφο του ελαχίστου πολυωνύμου $f(z)$ της ακολουθίας x παραγοντοποιείται όπως στην (5.11) και έστω ο ακέραιος $m \in \mathbb{Z}_N$ αντιστοιχεί σε θέση λάθους τέτοια ώστε*

$$g_i(z) \mid y_m(z). \tag{5.13}$$

Τότε, ισχύει η σχέση

$$\boldsymbol{y}_m \, \boldsymbol{G}_j^{[k_j]} \, \boldsymbol{J}_{N+k_j} \, (\boldsymbol{x}^{[k_j]})^T = 0 \tag{5.14}$$

όπου το $1 \times (N + k_j)$ διάνυσμα $\boldsymbol{x}^{[k_j]}$ είναι η περιοδική επέκταση του $\boldsymbol{x}$ κατά k_j στοιχεία.

Απόδειξη. Από την (5.6) συμπεραίνουμε ότι το πολυώνυμο $x(z)$ ανήκει στο γραμμικό κυκλικό κώδικα $\mathcal{H}$ που παράγεται από το $h(z)$. Έστω $\boldsymbol{r}$ και $\widehat{\boldsymbol{H}}$ είναι το διάνυσμα και ο πίνακας γεννήτορας που αντιστοιχούν στα πολυώνυμα $r(z)$ και $h^*(z)$ της σχέσης (5.6). Τότε ισχύει

$$\boldsymbol{x} = \boldsymbol{r} \, \widehat{\boldsymbol{H}}.$$

Ο πίνακας γεννήτορας $\boldsymbol{F}$ του δυϊκού κυκλικού κώδικα $\mathcal{H}^\perp$ παράγεται από το πολυώνυμο $f(z)$. Συνεπώς $\boldsymbol{F}\,\boldsymbol{x}^T = \boldsymbol{0}$, όπου το $\boldsymbol{x}^T$ είναι το ανάστροφο του διανύσματος $\boldsymbol{x}$. Από τις (5.10) και (5.12) η τελευταία σχέση οδηγεί στο ακόλουθο αποτέλεσμα

$$\boldsymbol{G}_i^{[-k_j]} \, \boldsymbol{G}_j \, \boldsymbol{J}_N \, \boldsymbol{x}^T = \boldsymbol{0}. \tag{5.15}$$

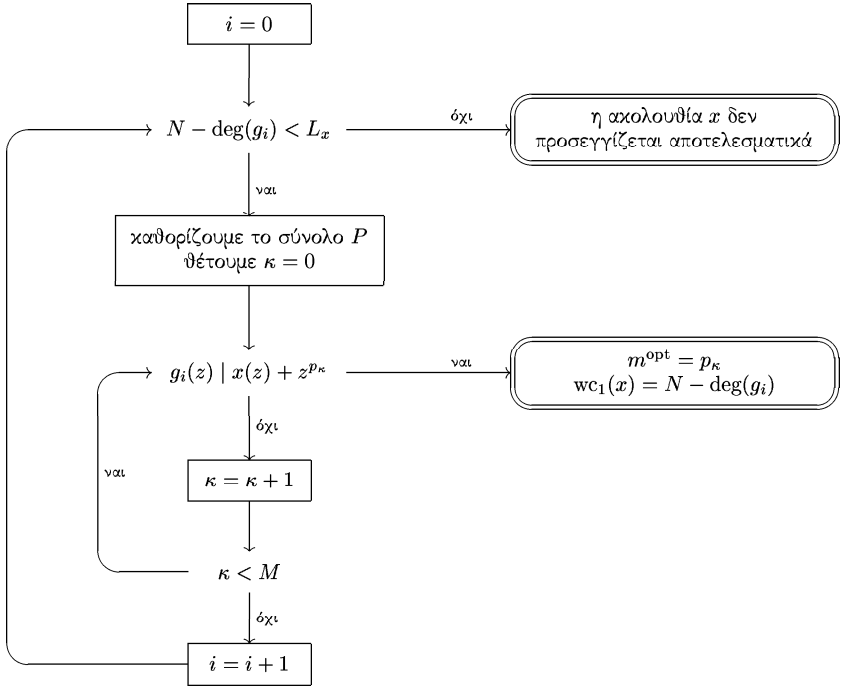
Επειδή ο γραμμικός κώδικας είναι κυκλικός, η περιοδική επέκταση της κωδικής λέξης $\boldsymbol{x}$ ικανοποιεί την ίδια εξίσωση ελέγχου ισοτιμίας με την $\boldsymbol{x}$, με τη διαφορά ότι εφαρμόζεται σε κυκλική ολίσθηση της $\boldsymbol{x}$. Επομένως, από την (5.15) λαμβάνουμε

$$\boldsymbol{G}_i \, \boldsymbol{G}_j^{[k_j]} \, \boldsymbol{J}_{N+k_j} \, (\boldsymbol{x}^{[k_j]})^T = \boldsymbol{0}. \tag{5.16}$$

Εξ' υποθέσεως, η κωδική λέξη $\boldsymbol{y}_m$ ανήκει στο γραμμικό κυκλικό κώδικα που παράγεται από τον πίνακα $\boldsymbol{G}_i$. Κατά συνέπεια, υπάρχει διάνυσμα $\boldsymbol{u}$ τέτοιο ώστε να ισχύει

$$\boldsymbol{y}_m = \boldsymbol{u} \, \boldsymbol{G}_i.$$

Πολλαπλασιάζοντας από τα αριστερά και τα δύο μέλη της (5.16) με $\boldsymbol{u}$, λόγω της ανωτέρω σχέσης, λαμβάνουμε την (5.14). □



Σχήμα 5.2. Η βελτιωμένη έκδοση του αλγορίθμου διαδοχικών διαιρέσεων. Για κάθε $g_i \in G$ υπολογίζεται το σύνολο $P = \{p_0, \ldots, p_{M-1}\}$ των δυνατών θέσεων λάθους

Παρατήρηση 5.7. Ορίζουμε το διάνυσμα $\boldsymbol{b}_j^T = \boldsymbol{G}_j^{[k_j]} \boldsymbol{J}_{N+k_j} (\boldsymbol{x}^{[k_j]})^T$ και τον ακέραιο $c_j = \boldsymbol{x}\, \boldsymbol{b}_j^T$. Τότε, η (5.14) γράφεται ως

$$\boldsymbol{y}_m\, \boldsymbol{b}_j^T = 0 \Leftrightarrow \boldsymbol{e}_m\, \boldsymbol{b}_j^T = \boldsymbol{x}\, \boldsymbol{b}_j^T \Leftrightarrow \boldsymbol{b}_{j,m} = c_j \tag{5.17}$$

αφού $\boldsymbol{y}_m = \boldsymbol{x} + \boldsymbol{e}_m$ και το δυαδικό βάρος του $\boldsymbol{e}_m$ είναι 1. Συμβολίζουμε με $\boldsymbol{b}_{j,m}$ το m–στό στοιχείο του διανύσματος $\boldsymbol{b}_j$. Παρατηρούμε ότι το αριστερό μέλος της (5.17) εξαρτάται ουσιαστικά από τη θέση λάθους, ενώ το δεξιό της μέλος αποτελεί γνωστή ποσότητα.

Παράδειγμα 5.8. Κατά την πρώτη επανάληψη του αλγορίθμου διαδοχικών διαιρέσεων, όπου έχουμε $g_i(z) = f^*(z)$ και $g_j(z) = 1$, οι σχέσεις (5.13) και (5.17)

λαμβάνουν τη μορφή

$$f^*(z) \mid y_m(z) \tag{5.18}$$

και $x_{N-1-m} = x_{(N-1)/2}$ αντίστοιχα. □

Όπως γίνεται φανερό από το ανωτέρω παράδειγμα, η χρήση της σχέσης (5.17) απλοποιεί σημαντικά τον αλγόριθμο διαδοχικών διαιρέσεων. Η νέα έκδοση του αλγόριθμου που απορρέει από το Θεώρημα 5.6 παρατίθεται στο Σχ. 5.2. Ωστόσο, η μείωση της πολυπλοκότητας του αλγορίθμου επιφέρει το κόστος εύρεσης του συνόλου θέσεων $P = \{p_0, \ldots, p_{M-1}\}$ της ακολουθίας οι οποίες ικανοποιούν την (5.17). Το αναμενόμενο ποσοστό θέσεων που αποκλείονται είναι 50%.

Το σύνολο θέσεων που απομένουν μετά την εφαρμογή της (5.17) είναι δυνατό να υποστεί επιπλέον μείωση έαν θεωρήσουμε την ακολουθία $x^* \sim x$ η οποία λαμβάνεται από την x με ολίσθηση προς τα δεξιά κατά τ θέσεις. Έστω $c_j^* \in \mathbb{F}_2$ και $P^* = \{p_0^*, \ldots, p_{R-1}^*\}$ είναι ο ακέραιος και το σύνολο θέσεων που αντιστοιχούν στην ακολουθία x^*. Έαν ο ακέραιος τ επιλεγεί έτσι ώστε να ισχύει $c_j^* \neq c_j$, τότε η βέλτιστη φάση ανήκει στο σύνολο $P \cap (P^* - \tau)$.

5.3 Η μέθοδος των εξισώσεων ισοδυναμίας

Στην τρέχουσα ενότητα παρουσιάζουμε έναν εναλλακτικό τρόπο επίλυσης του προβλήματος ελαχιστοποίησης (5.1) μέσω ενός συστήματος εξισώσεων ισοδυναμίας. Αρχικά, διερευνούμε την ύπαρξη ικανών και αναγκαίων συνθηκών για την επιλυσιμότητα του συστήματος εξισώσεων στην περίπτωση όπου το ελάχιστο πολυώνυμο $f(z)$ της ακολουθίας x γράφεται ως γινόμενο δύο ανάγωγων πολυωνύμων. Στη συνέχεια, παραθέτουμε τις αντίστοιχες συνθήκες που ισχύουν στη γενικότερη περίπτωση παραγοντοποίησης του $f(z)$ σε μεγαλύτερο αριθμό ανάγωγων πολυωνύμων.

Λήμμα 5.9. *Ας θεωρήσουμε τον ακέραιο r_i που ικανοποιεί τη σχέση $\alpha^{r_i} = x(\alpha^{s_i})$, όπου α^{s_i} είναι ρίζα του πολυωνύμου $f_i^*(z)$. Τότε, η βέλτιστη φάση m^{opt} ικανοποιεί ένα υποσύνολο των ακολούθων εξισώσεων ισοδυναμίας*

$$s_i m \equiv r_i \pmod{N}, \qquad i \in \mathbb{Z}_K. \tag{5.19}$$

Απόδειξη. Από την (5.18), εξάγουμε το συμπέρασμα ότι οι ρίζες του πολυωνύμου $f^*(z)$ είναι επιπλέον και ρίζες του $y_m(z)$. Συνεπώς, υπολογίζοντας την (5.18)

στις ρίζες του πολυωνύμου $f^*(z)$ λαμβάνουμε τις ακόλουθες K εξισώσεις

$$\alpha^{r_i} + \alpha^{s_i m} \equiv 0 \pmod{\alpha^N + 1}, \qquad i \in \mathbb{Z}_K$$

οι οποίες οδηγούν ευθέως στην (5.19). Προφανώς, η πολυπλοκότητα βάρους $\mathrm{wc}_1(x)$ της ακολουθίας x ικανοποιεί την (5.9) με ισότητα έαν και μόνον έαν η (5.19) έχει ως λύση την $m = m^{\mathrm{opt}}$. Διαφορετικά, ισχύει

$$N - L_x < \mathrm{wc}_1(x)$$

και συνεπώς η βέλτιστη φάση m^{opt} ικανοποιεί ένα υποσύνολο των εξισώσεων ισοδυναμίας της (5.19). □

Από τον Ορισμό 5.1, το υποσύνολο των εξισώσεων ισοδυναμίας που ικανοποιεί η βέλτιστη φάση m^{opt} μεγιστοποιεί το άθροισμα βαθμών των ελαχίστων πολυωνύμων που αντιστοιχούν στα στοιχεία α^{s_i}, για τα οποία ισχύει

$$s_i m^{\mathrm{opt}} \equiv r_i \pmod{N}.$$

Οι ακέραιοι αριθμοί r_i και s_i είναι δυνατό να υπολογιστούν μέσω του διακριτού μετασχηματισμού Fourier της ακολουθίας x, σύμφωνα με την (5.4). Σύμφωνα με το Κεφάλαιο 3, οι αλγόριθμοι των Cooley–Tukey, ή του Rader ακολουθούμενου από τον αλγόριθμο του Winograd, είναι από τους αποτελεσματικούς αλγορίθμους που υλοποιούν το διακριτό μετασχηματισμό Fourier.

Οι λύσεις κάθε εξίσωσης ισοδυναμίας αναφέρονται ως *τοπικές λύσεις*, ενώ η λύση του συστήματος εξισώσεων ονομάζεται *ολική λύση*. Στη συνέχεια, διερευνούμε την εξαγωγή συνθηκών ύπαρξης και μοναδικότητας της ολικής λύσης. Για λόγους απλοποίησης των αποδείξεων, πραγματοποιούμε αρχικά λεπτομερή μελέτη της περίπτωσης $K = 2$.

Ας θεωρήσουμε ότι το ελάχιστο πολυώνυμο της ακολουθίας x αναλύεται σε γινόμενο δύο πρωταρχικών παραγόντων ως εξής

$$f(z) = f_0(z) f_1(z).$$

Τότε, κάθε εξίσωση ισοδυναμίας της (5.19) έχει μία μοναδική τοπική λύση έαν και μόνον έαν ο ακέραιος $d_i = \gcd(s_i, N)$ διαιρεί τον r_i. Από την υπόθεση, ισχύει ότι $d_i = 1$ και συνεπώς κάθε εξίσωση ισοδυναμίας έχει ως μοναδική τοπική λύση την

$$m_i = r_i s_i^{\varphi(N)-1} \bmod N, \qquad i = 0, 1.$$

Επομένως, για το σύστημα των δύο εξισώσεων ισοδυναμίας θα υπάρχει ολική λύση $m^{\text{opt}} = m_0 = m_1$ έαν και μόνον έαν ισχύει

$$r_0 s_1 \equiv r_1 s_0 \pmod{N}.$$

Στη συνέχεια, θεωρούμε ότι τα πολυώνυμα $f_0(z)$ και $f_1(z)$ είναι ανάγωγα αλλά όχι απαραίτητα πρωταρχικά. Τότε, η εξίσωση ισοδυναμίας που αντιστοιχεί στο πολυώνυμο $f_i^*(z)$ έχει d_i τοπικές λύσεις, οι οποίες δίνονται από την ακόλουθη σχέση

$$m_{i,c_i} = \frac{r_i}{d_i}\left(\frac{s_i}{d_i}\right)^{\varphi(\frac{N}{d_i})-1} + \frac{N}{d_i}c_i \bmod N, \qquad i = 0, 1$$

όπου οι ακέραιοι c_i παίρνουν τιμές μεταξύ 0 και $d_i - 1$. Το σύστημα εξισώσεων ισοδυναμίας έχει λύση, δηλ. υπάρχει ζεύγος (c_0, c_1) τέτοιο ώστε $m^{\text{opt}} = m_{0,c_0} = m_{1,c_1}$, έαν και μόνον έαν ισχύει

$$\frac{N}{d_0}c_0 - \frac{N}{d_1}c_1 \equiv \left(\frac{s_0}{d_0}\right)^{\varphi(\frac{N}{d_0})-1}\left(\frac{s_1}{d_1}\right)^{\varphi(\frac{N}{d_1})-1}\left(\frac{r_1}{d_1}\frac{s_0}{d_0} - \frac{r_0}{d_0}\frac{s_1}{d_1}\right) \pmod{N}.$$

Η ανωτέρω διοφαντική εξίσωση, με αγνώστους τους ακεραίους c_0 και c_1, έχει λύση έαν και μόνον έαν

$$\gcd\left(\frac{N}{d_0}, \frac{N}{d_1}, N\right) \mid \left(\frac{s_0}{d_0}\right)^{\varphi(\frac{N}{d_0})-1}\left(\frac{s_1}{d_1}\right)^{\varphi(\frac{N}{d_1})-1}\left(\frac{r_1}{d_1}\frac{s_0}{d_0} - \frac{r_0}{d_0}\frac{s_1}{d_1}\right)$$

ή ισοδύναμα

$$\frac{N}{\operatorname{lcm}(d_0, d_1)} \mid \left(\frac{s_0}{d_0}\right)^{\varphi(\frac{N}{d_0})-1}\left(\frac{s_1}{d_1}\right)^{\varphi(\frac{N}{d_1})-1}\left(\frac{r_1}{d_1}\frac{s_0}{d_0} - \frac{r_0}{d_0}\frac{s_1}{d_1}\right). \tag{5.20}$$

Επειδή ο μέγιστος κοινός διαιρέτης των ακεραίων s_i και N είναι ίσος με d_i, καταλήγουμε στο συμπέρασμα ότι τα N/d_i και s_i/d_i είναι πρώτα μεταξύ τους. Με παρόμοιο τρόπο είναι δυνατό να δείξουμε ότι οι ακέραιοι N/d_i και s_{1-i}/d_{1-i} δεν έχουν μεταξύ τους κοινούς παράγοντες. Η συνθήκη (5.20) δίνει

$$\frac{N}{\operatorname{lcm}(d_0, d_1)} \mid \frac{r_1}{d_1}\frac{s_0}{d_0} - \frac{r_0}{d_0}\frac{s_1}{d_1} \Leftrightarrow N \mid \frac{r_1 s_0 - r_0 s_1}{\gcd(d_0, d_1)}.$$

Συνεπώς, αποδείξαμε το ακόλουθο Θεώρημα.

Θεώρημα 5.10. *Το σύστημα εξισώσεων ισοδυναμίας*

$$s_0 m \equiv r_0 \pmod{N}$$

$$s_1 m \equiv r_1 \pmod{N}$$

έχει ολική λύση έαν και μόνον έαν ο ακέραιος $d_i = \gcd(s_i, N)$ *διαιρεί τον* r_i *για* $i = 0, 1$, *και επιπλέον ισχύει*

$$\frac{1}{\gcd(d_0, d_1)} \begin{vmatrix} s_0 & r_0 \\ s_1 & r_1 \end{vmatrix} \equiv 0 \pmod{N}. \tag{5.21}$$

Η συνθήκη (5.21) είναι εξαιρετικά χρήσιμη για τον έλεγχο επιλυσιμότητας του συστήματος εξισώσεων ισοδυναμίας σε μεγάλα πεπερασμένα σώματα, αφού σε αυτήν την περίπτωση ο υπολογισμός της συνάρτησης του Euler είναι ιδιαίτερα δύσκολος. Στο Πόρισμα που ακολουθεί γενικεύουμε τη συνθήκη (5.21) σε συστήματα εξισώσεων ισοδυναμιών με $K > 2$ εξισώσεις.

Πόρισμα 5.11. *Το σύστημα εξισώσεων ισοδυναμίας* (5.19) *έχει ολική λύση έαν και μόνον έαν ο ακέραιος* $d_i = \gcd(s_i, N)$ *διαιρεί τον* r_i *για όλα τα* $i \in \mathbb{Z}_K$, *και επιπλέον υπάρχει ακέραιος* $m \in \mathbb{Z}_N$ *τέτοιος ώστε να ισχύει*

$$\boldsymbol{r} - m\boldsymbol{s} = \boldsymbol{0} \bmod N \tag{5.22}$$

όπου $\boldsymbol{r} = \begin{pmatrix} r_0 & \cdots & r_{K-1} \end{pmatrix}$ *και* $\boldsymbol{s} = \begin{pmatrix} s_0 & \cdots & s_{K-1} \end{pmatrix}$. *Τότε, η βέλτιστη φάση δίνεται από τη σχέση* $m^{opt} = m$.

Η μεθοδολογία των εξισώσεων ισοδυναμίας συνδέεται άμεσα με τη μέθοδο των διαδοχικών διαιρέσεων. Έαν τα διανύσματα $\boldsymbol{r}$ και $\boldsymbol{s}$ είναι γραμμικώς εξαρτημένα, τότε βάσει του Λήμματος 5.9 και της (5.22) όλες οι ρίζες του πολυωνύμου $f^*(z)$ είναι και ρίζες του $y_{m^{\text{opt}}}(z)$. Κατά συνέπεια, το πολυώνυμο $f^*(z)$ διαιρεί το $y_{m^{\text{opt}}}(z)$, σε αντιστοιχία με το πρώτο βήμα του αλγορίθμου διαδοχικών διαιρέσεων.

Στην περίπτωση που τα διανύσματα $\boldsymbol{r}$ και $\boldsymbol{s}$ είναι γραμμικώς ανεξάρτητα, τότε η βέλτιστη φάση m^{opt} ικανοποιεί ένα υποσύνολο των εξισώσεων της (5.19). Συνεπώς, υπάρχει πολυώνυμο $g_i(z) \in G$ τέτοιο ώστε το $g_i(z)$ να διαιρεί το $y_{m^{\text{opt}}}(z)$, όπου το πολυώνυμο $g_i(z)$ είναι ο παράγοντας μεγαλυτέρου βαθμού του $f^*(z)$ με αυτήν την ιδιότητα.

5.4 Η μέθοδος του συγχρονισμού φάσεων

Σε αντιστοιχία με τις δύο προηγούμενες ενότητες, η μέθοδος συγχρονισμού φάσεων της ακολουθίας x αποτελεί εναλλακτικό τρόπο επίλυσης του προβλή-

ματος ελαχιστοποίησης (5.1). Η συγκεκριμένη μέθοδος παρουσιάζει πολλαπλά πλεονεκτήματα έναντι των άλλων τεχνικών, το πιο σημαντικό από τα οποία είναι η απλότητα ελέγχου ύπαρξης και εύρεσης της βέλτιστης φάσης. Ως αποτέλεσμα, η μέθοδος συγχρονισμού φάσεων αποτελεί μοναδικό εργαλείο για το σχεδιασμό ακολουθιών ανθεκτικών σε επιθέσεις προσέγγισης.

Ας υποθέσουμε ότι το σύνολο I των επικεφαλείς κλάσεων των κυκλοτομικών κλάσεων (modulo N) περιέχει $|I| = V$ στοιχεία. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι οι ακέραιοι $t_0, \ldots, t_{K-1}$ είναι τα πρώτα K στοιχεία του I, και ότι ο συντελεστής γ_i όπως ορίστηκε στην (5.3) γράφεται ως $\gamma_i = \alpha^{q_i}$, $i \in \mathbb{Z}_K$. Από την (5.3) λαμβάνουμε

$$x_j = \sum_{i=0}^{K-1} \mathrm{tr}_1^{n_i}(\alpha^{q_i + t_i j}). \tag{5.23}$$

Επειδή η ακολουθία λάθους e_m έχει ένα μοναδικό άσσο, στη θέση m, έχει γραμμική πολυπλοκότητα ίση με N, και συνεπώς περιλαμβάνει όλους τους επικεφαλείς κλάσεων στην αναπαράσταση ίχνους της. Πιο συγκεκριμένα, η ακολουθία e_m δίνεται από τη σχέση

$$e_{m,j} = \sum_{i=0}^{V-1} \mathrm{tr}_1^{n_i}(\alpha^{t_i(j-m)}).$$

Προσθέτοντας την ακολουθία λάθους στην x λαμβάνουμε

$$y_{m,j} = \sum_{i=0}^{K-1} \mathrm{tr}_1^{n_i}((\alpha^{q_i} + \alpha^{-mt_i})\alpha^{t_i j}) + \sum_{i=K}^{V-1} \mathrm{tr}_1^{n_i}(\alpha^{t_i(j-m)}). \tag{5.24}$$

Από την (5.24), το πρόβλημα της παραγωγής ακολουθιών κατά προσέγγιση είναι ισοδύναμο με

$$\mathrm{wc}_1(x) = N - \max_{m \in \mathbb{Z}_N} \sum_{i=0}^{K-1} w_{m,i} n_i \tag{5.25}$$

όπου ο συντελεστής $w_{m,i}$ είναι ίσος με $w_{m,i} = 1$ εάν $q_i = -mt_i \bmod N$ και $w_{m,i} = 0$ στην αντίθετη περίπτωση.

Είναι προφανές ότι η μέγιστη δυνατή μείωση στη γραμμική πολυπλοκότητα της ακολουθίας x συμβαίνει εάν ισχύει $q_i = -m^{\mathrm{opt}} t_i \bmod N$ για κάθε $i \in \mathbb{Z}_K$. Σύμφωνα με το Λήμμα 5.1, όλες οι συνιστώσες ακολουθίες της x πρέπει να ικανοποιούν τη σχέση ισοδυναμίας $x^i \sim x_0^i$ και να λαμβάνονται από την x_0^i

εφαρμόζοντας m^{opt} ολισθήσεις προς τα δεξιά. Στην περίπτωση αυτή, η πολυπλοκότητα βάρους $\mathrm{wc}_1(x)$ ικανοποιεί την (5.9) με ισότητα, ενώ από την (5.24) λαμβάνουμε

$$x_j^{(1)} = \sum_{i=K}^{V-1} \mathrm{tr}_1^{n_i}(\alpha^{t_i(j-m^{\mathrm{opt}})}).$$

Σε μια τέτοια περίπτωση, θα αναφέρουμε ότι οι συνιστώσες ακολουθίες της x είναι *συγχρονισμένες*. Συνεπώς, αποδείξαμε το ακολουθο Θεώρημα.

Θεώρημα 5.12. *Ας θεωρήσουμε τη δυαδική ακολουθία $x = \{g(\alpha^j)\}_{j\geq 0}$, όπου το πολυώνυμο $g(z)$ δίνεται από τη σχέση*

$$g(z) = \sum_{i=0}^{K-1} \mathrm{tr}_1^{n_i}(\alpha^{q_i} z^{t_i}).$$

Έστω ότι ο ακέραιος $m \in \mathbb{Z}_N$ είναι τέτοιος ώστε να ισχύει

$$\boldsymbol{q} + m\boldsymbol{t} = \boldsymbol{0} \bmod N \tag{5.26}$$

όπου $\boldsymbol{q} = \begin{pmatrix} q_0 & \cdots & q_{K-1} \end{pmatrix}$ και $\boldsymbol{t} = \begin{pmatrix} t_0 & \cdots & t_{K-1} \end{pmatrix}$. Τότε, η βέλτιστη φάση δίνεται από τη σχέση $m^{opt} = m$.

Οι σχέσεις (5.22) και (5.26) συνδέονται μεταξύ τους. Πιο συγκεκριμένα, είναι δυνατό να αποδείξουμε την ισχύ της (5.26) από την (5.22) και αντιστρόφως. Πράγματι, για κάθε $i \in \mathbb{Z}_K$ υπάρχει ακέραιος b_i τέτοιος ώστε

$$s_i + 2^{b_i} t_i \equiv 0 \pmod N$$

όπου ο ακέραιος b_i λαμβάνει τιμές μεταξύ 0 και $n_i - 1$. Ας θεωρήσουμε το διάνυσμα $\boldsymbol{b} = \begin{pmatrix} 2^{b_0} & \cdots & 2^{b_{K-1}} \end{pmatrix}$. Τότε ισχύει η σχέση

$$-\boldsymbol{s} = \boldsymbol{b} \odot \boldsymbol{t} \bmod N \tag{5.27}$$

όπου συμβολίζουμε με $\odot$ το γινόμενο Schur–Hadamard. Από το Λήμμα 5.9 και την (5.4), λαμβάνουμε ότι $\alpha^{r_i} = \gamma_i^{2^{b_i}}$, το οποίο με τη σειρά του οδηγεί στο ακόλουθο αποτέλεσμα

$$\boldsymbol{r} = \boldsymbol{b} \odot \boldsymbol{q} \bmod N. \tag{5.28}$$

Συνδυάζοντας τις (5.27) και (5.28), η σχέση (5.22) δίνει

$$\boldsymbol{r} - m\boldsymbol{s} = \boldsymbol{0} \bmod N \Leftrightarrow \boldsymbol{b} \odot \{\boldsymbol{q} + m\boldsymbol{t}\} = \boldsymbol{0} \bmod N$$

```
for m = 0, ..., N − 1 do
    set L_m = N

    for i = 0, ..., K − 1 do
        set c_i = q_i + m t_i mod N

        if c_i > 0 then
            set w_i = 0
        else
            set w_i = 1
        endif

        set L_m = L_m − w_i n_i
    endfor

endfor
```

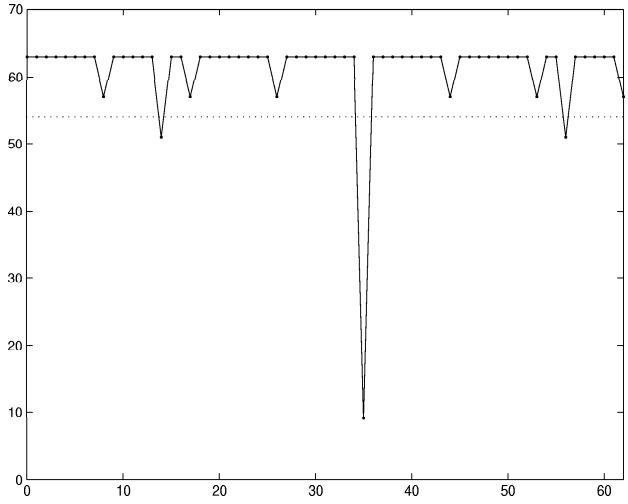
Σχήμα 5.3. Ο αλγόριθμος υπολογισμού του προφίλ της γραμμικής πολυπλοκότητας μετά την προσέγγιση με πραγματοποίηση ενός λάθους

$$\Leftrightarrow \boldsymbol{q} + m\boldsymbol{t} = \boldsymbol{0} \bmod N$$

αφού οι ακέραιοι 2^{b_i} και N είναι πρώτοι μεταξύ τους για κάθε $i \in \mathbb{Z}_K$. Συνεπώς, το σύστημα εξισώσεων ισοδυναμίας που αντιστοιχεί στην (5.26) είναι δυνατό να επιλυθεί εφαρμόζοντας τη μεθοδολογία της Ενότητας 5.3.

Ως αποτέλεσμα της (5.25), είναι δυνατό να υλοποιήσουμε ένα γρήγορο αλγόριθμο εύρεσης του προφίλ της γραμμικής πολυπλοκότητας της ακολουθίας x μετά την προσέγγισή της με πραγματοποίηση ενός λάθους. Ο αλγόριθμος δίνεται στο Σχ. 5.3, όπου $\boldsymbol{n} = \begin{pmatrix} n_0 & \cdots & n_{K-1} \end{pmatrix}$ ενώ το $\boldsymbol{L} = \begin{pmatrix} L_0 & \cdots & L_{N-1} \end{pmatrix}$ δείχνει τη μεταβολή της γραμμικής πολυπλοκότητας της ακολουθίας x σε σχέση με τη θέση m του λάθους.

Η πολυπλοκότητα του αλγορίθμου του Σχ. 5.3 είναι $O(N)$, αλλά ο χρόνος εκτέλεσής του είναι ιδιαίτερα χαμηλός αφού δεν χρησιμοποιεί τον αλγόριθμο των Berlekamp–Massey [15]. Ο αλγόριθμος απαιτεί τη χρήση $3NK$ πολλαπλασιασμών και $2NK$ προσθέσεων/αφαιρέσεων.



Σχήμα 5.4. Το προφίλ της γραμμικής πολυπλοκότητας της ακολουθίας x, στο Παράδειγμα 5.13, μετά την προσέγγισή της με πραγματοποίηση ενός λάθους. Η διακεκομμένη γραμμή αντιστοιχεί στην τρέχουσα τιμή $L_x = 54$ της γραμμικής πολυπλοκότητας της x

Παράδειγμα 5.13. Ας θεωρήσουμε τη δυαδική ακολουθία $x = \{g(\alpha^j)\}_{j\geq 0}$, περιόδου 63 και γραμμικής πολυπλοκότητας $L_x = 54$, όπου

$$g(z) = \mathrm{tr}_1^6(\alpha^{28}z^{01}) + \mathrm{tr}_1^6(\alpha^{21}z^{03}) + \mathrm{tr}_1^6(\alpha^{14}z^{05}) + \mathrm{tr}_1^6(\alpha^{07}z^{07}) + \mathrm{tr}_1^6(\alpha^{56}z^{11}) + \mathrm{tr}_1^6(\alpha^{49}z^{13}) + \mathrm{tr}_1^6(\alpha^{42}z^{15}) + \mathrm{tr}_1^6(\alpha^{14}z^{23}) + \mathrm{tr}_1^6(\alpha^{49}z^{31}).$$

Τα διανύσματα

$$\boldsymbol{q} = \begin{pmatrix} 28 & 21 & 14 & 07 & 56 & 49 & 42 & 14 & 49 \end{pmatrix}$$
$$\boldsymbol{t} = \begin{pmatrix} 01 & 03 & 05 & 07 & 11 & 13 & 15 & 23 & 31 \end{pmatrix}$$

είναι γραμμικώς εξαρτημένα, και συνεπώς η πολυπλοκότητα βάρους της ακολουθίας x είναι ίση με $\mathrm{wc}_1(x) = 63 - 54 = 9$. Όπως φαίνεται στο Σχ. 5.4 το συγκεκριμένο κάτω φράγμα επιτυγχάνεται στη θέση $m^{\mathrm{opt}} = 35$. □

5.5 Θέματα σχεδιασμού ακολουθιών

Κατά το σχεδιασμό κυκλωμάτων για χρήση ως *γεννητόρων σειριακών κλειδιών* (βλ. Κεφάλαια 1 και 7), ο στόχος δεν είναι μόνο να εξασφαλίσουμε ότι το σειριακό κλειδί χαρακτηρίζεται από μεγάλη γραμμική πολυπλοκότητα, αλλά επιπλέον ότι μικρές αλλαγές στα ψηφία που το απαρτίζουν δε μειώνουν τη γραμμική του πολυπλοκότητα. Στην αντίθετη περίπτωση, μία επίθεση προσέγγισης θα είναι δυνατό να εξάγει πολύτιμη πληροφορία.

Ορισμός 5.14. Μία δυαδική ακολουθία x, περιόδου $N = 2^n - 1$, ονομάζεται ανθεκτική σε προσεγγίσεις πραγματοποίησης ενός λάθους έαν $\mathrm{wc}_1(x) \geq L_x$.

Θεώρημα 5.15. *Ας θεωρήσουμε ότι η δυαδική ακολουθία x είναι το αποτέλεσμα αθροίσματος συνιστωσών ακολουθιών και ότι η γραμμική της πολυπλοκότητα ικανοποιεί τη σχέση $L_x \leq N - n$. Τότε, οι ακόλουθες προτάσεις είναι ισοδύναμες:*

1. *Η ακολουθία x είναι ανθεκτική σε προσεγγίσεις πραγματοποίησης ενός λάθους και ισχύει $\mathrm{wc}_1(x) \geq N - n$.*

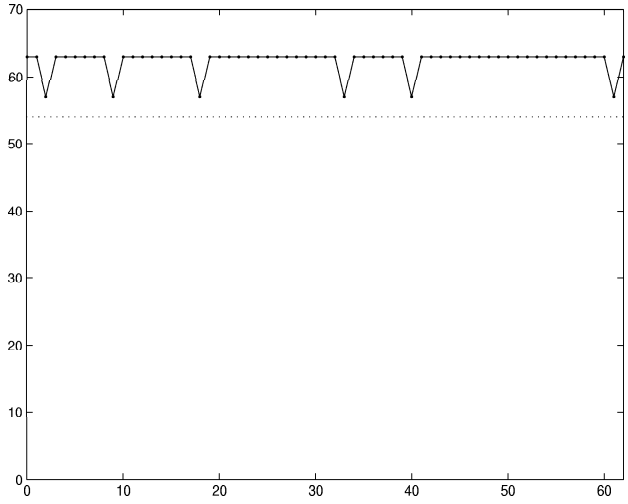
2. *Για κάθε ζεύγος x^i και x^j συνιστωσών ακολουθιών της x τέτοιες ώστε $x^i \sim x_0^i$ και $x^j \sim x_0^j$ ισχύει*

$$(\nu_i - \nu_j) \cdot \mathrm{lcm}(d_i, d_j) \not\equiv 0 \pmod{N}$$

   όπου ν_i και ν_j είναι οι αριθμοί των δεξιών ολισθήσεων που πρέπει να εφαρμόσουμε ώστε να λάβουμε τις ακολουθίες x^i και x^j από τις x_0^i και x_0^j αντίστοιχα.

3. *Δεν υπάρχει αναγώγιμος παράγοντας $g_i(z) \in G$ του πολυωνύμου $f^*(z)$ ο οποίος να διαιρεί το $y_m(z)$ για κάποια τιμή του ακεραίου $m \in \mathbb{Z}_N$.*

Από το Θεώρημα 5.15, δύναται να διασφαλιστεί η ανθεκτικότητα έαν αποφεύγεται η χρήση ακολουθιών μεγίστου μήκους ως συνιστωσών ακολουθιών. Αντιθέτως, συνίσταται η χρήση ακολουθιών x^i οι οποίες δεν ανήκουν στην ίδια κλάση ισοδυναμίας με τις x_0^i, και παράγονται από τους ίδιους καταχωρητές ολίσθησης γραμμικής ανάδρασης βάσει διαφορετικών αρχικών καταστάσεων. Η συγκεκριμένη τεχνική εξασφαλίζει ότι το σύστημα εξισώσεων ισοδυναμίας (5.19) δεν παραδέχεται τοπικές λύσεις, οδηγώντας στο ακόλουθο Πόρισμα.



Σχήμα 5.5. Το προφίλ της γραμμικής πολυπλοκότητας της ακολουθίας x, στο Παράδειγμα 5.17, μετά την προσέγγισή της με πραγματοποίηση ενός λάθους. Η διακεκομμένη γραμμή αντιστοιχεί στην τρέχουσα τιμή $L_x = 54$ της γραμμικής πολυπλοκότητας της x

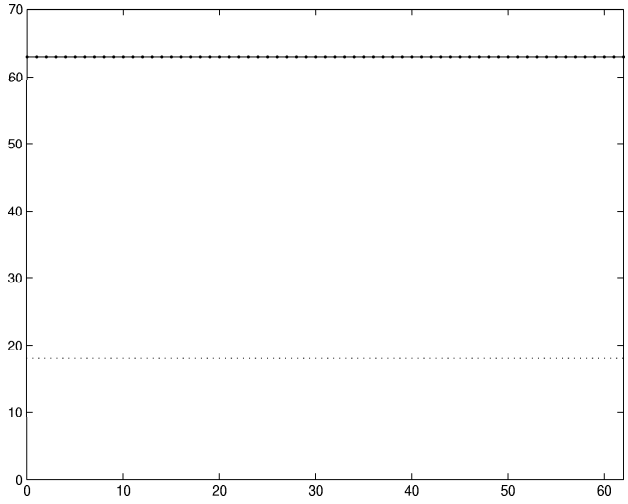
Πόρισμα 5.16. *Ας θεωρήσουμε ότι η δυαδική ακολουθία x είναι το αποτέλεσμα αθροίσματος συνιστωσών ακολουθιών x^i οι οποίες δεν ανήκουν στην ίδια κλάση ισοδυναμίας με τις x_0^i. Τότε, ισχύει $\mathrm{wc}_1(x) = N$ και η ακολουθία x είναι ανθεκτική σε προσεγγίσεις πραγματοποίησης ενός λάθους.*

Το Θεώρημα 5.15 επιτρέπει τον εμπλουτισμό των χαρακτηριστικών γραμμικής πολυπλοκότητας μίας ακολουθίας με κατάλληλη τροποποίηση των φάσεων των συνιστωσών ακολουθιών που την απαρτίζουν, όπως φαίνεται και στη συνέχεια.

Παράδειγμα 5.17. Ας θεωρήσουμε τη δυαδική ακολουθία x που παράγεται από το πολυώνυμο $g(z)$ του Παραδείγματος 5.13. Οδηγούμενοι από το Θεώρημα 5.15, τροποποιούμε το πολυώνυμο $g(z)$ ώστε να λάβουμε

$$g'(z) = \mathrm{tr}_1^6(\alpha^{23}z^{01}) + \mathrm{tr}_1^6(\alpha^{34}z^{03}) + \mathrm{tr}_1^6(\alpha^{10}z^{05}) + \mathrm{tr}_1^6(\alpha^{45}z^{07}) + \mathrm{tr}_1^6(\alpha^{41}z^{11}) + \mathrm{tr}_1^6(\alpha^{18}z^{13}) + \mathrm{tr}_1^6(\alpha^{62}z^{15}) + \mathrm{tr}_1^6(\alpha^{45}z^{23}) + \mathrm{tr}_1^6(\alpha^{48}z^{31}).$$

Η ελάχιστη τιμή της γραμμικής πολυπλοκότητας που λαμβάνουμε με προσέγγιση



Σχήμα 5.6. Το προφίλ της γραμμικής πολυπλοκότητας της ακολουθίας x, στο Παράδειγμα 5.18, μετά την προσέγγισή της με πραγματοποίηση ενός λάθους. Η διακεκομμένη γραμμή αντιστοιχεί στην τρέχουσα τιμή $L_x = 18$ της γραμμικής πολυπλοκότητας της x

της ακολουθίας x πραγματοποίησης ενός λάθους είναι $\mathrm{wc}_1(x) = 63 - 6 = 57$, όπως φαίνεται στο Σχ. 5.5. □

Παράδειγμα 5.18. Ας θεωρήσουμε τη δυαδική ακολουθία x που παράγεται από το δεύτερο, τέταρτο, και έβδομο όρο του πολυωνύμου $g'(z)$ του Παραδείγματος 5.17

$$g''(z) = \mathrm{tr}_1^6(\alpha^{34} z^{03}) + \mathrm{tr}_1^6(\alpha^{45} z^{07}) + \mathrm{tr}_1^6(\alpha^{62} z^{15}).$$

Η συγκεκριμένη ακολουθία έχει σταθερό προφίλ γραμμικής πολυπλοκότητας μετά από προσέγγιση με πραγματοποίηση ενός λάθους, δηλ. $\mathrm{wc}_1(x) = N$, όπως φαίνεται στο Σχ. 5.6. □

Θέματα σχεδιασμού ακολουθιών, όπως αυτά που μελετήθηκαν στην παρούσα ενότητα, έχουν ιδιαίτερη βαρύτητα στο χώρο της κρυπτογραφίας [27], [70], [116].

Κεφάλαιο 6

Ακολουθίες με χαρακτηριστικά λευκού θορύβου

Ψευδοτυχαίες δυαδικές ακολουθίες παραγόμενες από καταχωρητές ολίσθησης γραμμικής ανάδρασης έχουν χρησιμοποιηθεί εκτενώς σε εφαρμογές όπου απαιτείται η χρήση ακολουθιών που προσομοιάζουν αποτελεσματικά λευκό θόρυβο. Παραδείγματα εφαρμογών αποτελούν η κρυπτογραφία (βλ. Κεφάλαια 1 και 7), συστήματα επικοινωνιών ευρέως φάσματος [96], [114], και η επεξεργασία σήματος [50]. Οι ακολουθίες μεγίστου μήκους αποτελούν ιδιαίτερη κατηγορία ψευδοτυχαίων ακολουθιών και μπορούν να προσεγγίσουν πολύ καλά λευκό θόρυβο δεύτερης τάξης.

Οι ιδιότητες των συγκεκριμένων ακολουθιών έχουν μελετηθεί διεξοδικά στα πλαίσια ταυτοποίησης γραμμικών [22], [39], [115], και μη–γραμμικών συστημάτων [78], [105], [118]. Επιπλέον, μη–δυαδικές ακολουθίες μεγίστου μήκους έχουν επίσης χρησιμοποιηθεί για την ταυτοποίηση μη–γραμμικών συστημάτων ώστε να ικανοποιούνται συνθήκες επίμονης διέγερσης [38], [89], [113].

Ωστόσο, οι ακολουθίες μεγίστου μήκους έχουν το μειονέκτημα ότι δεν είναι δυνατό να χρησιμοποιηθούν για την προσέγγιση σημάτων λευκού θορύβου ανωτέρας τάξης λόγω της ύπαρξης τοπικών μεγίστων στις στατιστικές (ροπές και αθροιστικές) ανωτέρας τάξης. Σημαντικές εφαρμογές επεξεργασίας σήματος απαιτούν εφαρμογή της διαδικασίας ταυτοποίησης με διέγερση του αγνώστου συστήματος μέσω λευκού θορύβου ανωτέρας τάξης ως σήμα εισόδου. Μεταξύ άλλων, παραδείγματα τέτοιων εφαρμογών αποτελούν τα ακόλουθα:

- τυφλή ταυτοποίηση γραμμικών παραμετρικών (ARMA) ή μη–παραμετρικών μοντέλων [50], [83],
- ταυτοποίηση πεπερασμένων μη–παραμετρικών σειρών Volterra βασιζόμενη σε στατιστικές των δεδομένων εισόδου–εξόδου [57], [66], [67], [68], [78], [105], [108],
- ταυτοποίηση παραμετρικών αναπαραστάσεων συστημάτων Volterra, όπως διγραμμικά μοντέλα εισόδου–εξόδου [119], και συστήματα αφινικών καταστάσεων [28],
- τυφλή εξίσωση καναλιών και η τυφλή αποκατάσταση εικόνας με πεπερασμένα πολυωνυμικά (FIR) συστήματα Volterra μεγάλου αριθμού παραμέτρων [49], και
- ταυτοποίηση επαναληπτικών ελαχίστων τετραγώνων [49], [50], [115].

Στο παρόν κεφάλαιο διερευνούμε τη δημιουργία δυαδικών ακολουθιών που επιδεικνύουν τα χαρακτηρηστικά σημάτων λευκού θορύβου ανωτέρας τάξης και παράγονται από καταλλήλως επιλεγμένα ζεύγη ακολουθιών μεγίστου μήκους της ιδίας ή διαφορετικών ελαχίστων περιόδων.

Ειδικότερα, αποδείκνύεται ότι η συνάρτηση αυτοσυσχέτισης και οι ροπές ανωτέρας τάξης δυαδικών ακολουθιών παραγόμενων από την πρόσθεση (modulo 2) δύο ακολουθιών μεγίστου μήκους αυθαιρέτων ελαχίστων περιόδων, εξαρτώνται από τη συνάρτηση ετεροσυσχέτισης των συγκεκριμένων ακολουθιών. Έαν οι δύο ακολουθίες μεγίστου μήκους έχουν την ίδια ελάχιστη περίοδο, τότε οι ροπές ανωτέρας τάξης των παραγόμενων ακολουθιών λαμβάνουν τιμές από ένα προκαθορισμένο σύνολο, και έαν υπάρχουν, τα τοπικά τους μέγιστα είναι ελάχιστα και ελεγχόμενα εκ των προτέρων με κατάλληλη επιλογή των αρχικών ακολουθιών μεγίστου μήκους. Τα ανωτέρω αποτελέσματα εφαρμόζονται στις ακολουθίες Gold [20], [29], [30], [53], όπου και καθίσταται δυνατός ο έλεγχος των τιμών της συνάρτησης ετεροσυσχέτισης καθώς και της συχνότητα εμφάνισής τους σε μια περίοδο.

Ειδική περίπτωση αποτελούν οι δυϊκές BCH ακολουθίες, οι οποίες παράγονται από το πολυώνυμο γεννήτορα ενός BCH κώδικα διόρθωσης δύο σφαλμάτων [107]. Επιπλέον, αποδείκνύεται ότι έαν το χαρακτηριστικό πολυώνυμο ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης είναι το ανάστροφο του πολυωνύμου γεννήτορα ενός δυαδικού BCH κώδικα διόρθωσης t–σφαλμάτων [5], [9], [73],

[76], τότε η προκύπτουσα δυαδική ακολουθία δεν έχει τοπικά μέγιστα σε όλες τις ροπές μέχρι τάξεως $2t$. Ιδιαίτερα λεπτομερής ανάλυση δίνεται στην περίπτωση συνιστωσών ακολουθιών μεγίστου μήκους διαφορετικών ελαχίστων περιόδων.

Ειδική περίπτωση αποτελεί η κατασκευή των νέων ακολουθιών KRG [62], [97], των οποίων οι συνιστώσες έχουν σχετικά πρώτες περιόδους. Η συνάρτηση ετεροσυσχέτισης των συνιστωσών ακολουθιών είναι σταθερή και ίση με τον αντίστροφο του γινομένου των περιόδων τους. Επιπρόσθετα, η συνάρτηση αυτοσυσχέτισης και οι ροπές ανωτέρας τάξης των ακολουθιών KRG συμπεριφέρονται όπως στην περίπτωση ακολουθιών Gold με τη διαφορά ότι επιτρέπουν καλύτερο έλεγχο των θέσεων εμφάνισης των τοπικών μεγίστων καθώς και του μεγέθους των τιμών τους. Συγκεκριμένα, η απόσταση των τοπικών μεγίστων από την αρχή των αξόνων είναι ιδιαίτερα μεγάλη καθιστώντας τις ακολουθίες αυτές σχεδόν ιδανικές για την προσομοίωση λευκού θορύβου ανωτέρας τάξεως σε ορισμένα προβλήματα ταυτοποίησης.

Η ποιότητα των παραπάνω δυαδικών ακολουθιών στην προσομοίωση λευκού θορύβου ανωτέρας τάξης αποδείκνύεται με πειράματα ταυτοποίησης διγραμμικών συστημάτων, όπου οι ακολουθίες μεγίστου μήκους αποτυγχάνουν να δώσουν αμερόληπτες εκτιμήσεις των παραμέτρων του συστήματος.

6.1 Ακολουθίες μεγίστου μήκους

Στην παρούσα ενότητα εισάγουμε την έννοια του *τριωνύμου* μίας ακολουθίας και αποδεικνύουμε ότι τα σύνολα τριωνύμων των ακολουθιών μεγίστου μήκους τις χαρακτηρίζουν ως ακατάλληλες για την προσομοίωση σημάτων λευκού θορύβου ανωτέρας τάξης. Επιπρόσθετα, παρουσιάζουμε αποτελέσματα σχετικά με τον υπολογισμό των τριωνύμων που αντιστοιχούν σε μία ακολουθία.

Ας θεωρήσουμε την άπειρη περιοδική δυαδική ακολουθία $x = \{x_j\}_{j\geq 0}$, με ελάχιστη περίοδο N, που παράγεται από το μοντέλο Galois (Σχ. 3.1) ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης με n βαθμίδες. Σύμφωνα με το Κεφάλαιο 3, η ακολουθία x έχει ελάχιστο πολυώνυμο $f(z)$, ενώ $\boldsymbol{x}$ και D είναι το διάνυσμα που περιέχει τα πρώτα N στοιχεία της x και ο τελεστής καθυστέρησης αντίστοιχα.

Ακολούθως, δίνουμε έναν πρώτο ορισμό των ακολουθιών που προσομοιάζουν λευκό θόρυβο δευτέρας τάξης.

Ορισμός 6.1. Η περιοδική δυαδική ακολουθία x αποτελεί λευκό θόρυβο δευτέρας τάξης έαν και μόνον έαν ικανοποιούνται οι ακόλουθες συνθήκες [50]

i. Οι πιθανότητες εμφάνισης των συμβόλων 0 και 1 στο διάνυσμα $\boldsymbol{x}$ είναι ίσες, δηλ. $\Pr(x_j = 0) = \Pr(x_j = 1)$.

ii. Δύο τυχαίες διαφορετικές φάσεις της ακολουθίας x, που αντιστοιχούν στα διανύσματα $D^i\boldsymbol{x}$ και $D^j\boldsymbol{x}$, είναι ασυσχέτιστες, δηλ. η ροπή δεύτερης τάξης $\mathrm{AC}_x(j-i)$ είναι ίση με μηδέν.

Ως αποτέλεσμα του ορισμού και των Ιδιοτήτων 3.11 και 3.13, λαμβάνουμε ότι οι ακολουθίες μεγίστου μήκους προσομοιάζουν αποτελεσματικά λευκό θόρυβο δευτέρας τάξης έαν έχουν επαρκώς μεγάλη ελάχιστη περίοδο N.

6.1.1 Τριώνυμα ακολουθιών μεγίστου μήκους

Στη συνέχεια, μελετάμε την αποτελεσματικότητα ακολουθιών μεγίστου μήκους στην προσομοίωση σημάτων λευκού θορύβου τρίτης τάξης. Ιδιαίτερα χρήσιμος προς αυτήν την κατεύθυνση είναι ο υπολογισμός των τριωνύμων των ακολουθιών μεγίστου μήκους [31], [35], [74], [124], [125].

Ορισμός 6.2. Το πολυώνυμο $h(z) = 1 + z^{t_1} + z^{t_2}$ ονομάζεται *τριώνυμο* της ακολουθίας x έαν και μόνον έαν διαιρείται από το ανάστροφο του ελαχίστου πολυωνύμου της x.

Στο υπόλοιπο του κεφαλαίου, θεωρούμε ότι το βάρος ενός πολυωνύμου είναι ίσο με το πλήθος των μονονύμων του. Συχνά, αντί του πολυωνύμου $h(z)$, χρησιμοποιούμε το ζεύγος ακεραίων (t_1, t_2) που αντιστοιχεί στις δυνάμεις της μεταβλητής z. Το σύνολο των τριωνύμων της ακολουθίας x, με ελάχιστο πολυώνυμο το $f(z)$, συμβολίζεται με T_f.

Στη συνέχεια παραθέτουμε ορισμένες από τις μεθόδους που χρησιμοποιούνται ευρέως για την εύρεση τριωνύμων του συνόλου T_f.

Θεώρημα 6.3 (Lindholm [74]). *Έστω (t_1, t_2) είναι τριώνυμο της ακολουθίας x που αντιστοιχεί στο πολυώνυμο $h(z)$. Τότε, τα πολυώνυμα*

$$h_{ij}(z) = z^{i2^j} h(z)^{2^j} \pmod{1 + z^N} \tag{6.1}$$

με $i = 0, N - t_2, N - t_1$ και $j \geq 0$, είναι επίσης τριώνυμα της ακολουθίας x.

Απόδειξη. Για να αποδείξουμε ότι το πολυώνυμο $h_{ij}(z)$ ανήκει στο σύνολο T_f πρέπει να δείξουμε ότι **(α)** το $f^*(z)$ διαιρεί το $h_{ij}(z)$, **(β)** το βάρος του $h_{ij}(z)$ είναι 3, και **(γ)** ο σταθερός όρος του $h_{ij}(z)$ είναι η μονάδα.

Εξ' υποθέσεως, το ανάστροφο $f^*(z)$ του ελαχίστου πολυωνύμου της ακολουθίας x διαιρεί το πολυώνυμο $h(z)$. Από την (6.1), το $f^*(z)$ διαιρεί το πολυώνυμο $z^{i2^j}h(z)^{2^j}$, και κατά συνέπεια διαιρεί και το $h_{ij}(z)$.

Από την (6.1), λαμβάνουμε ότι το πολυώνυμο $h_{ij}(z)$ γράφεται ως άθροισμα των τριών μονονύμων

$$h_{ij}(z) = z^{i2^j \bmod N} + z^{(i+t_1)2^j \bmod N} + z^{(i+t_2)2^j \bmod N} \tag{6.2}$$

αφού η λήψη του υπολοίπου της διαίρεσης ενός πολυωνύμου με το $1+z^N$ διατηρεί το βάρος του. Τέλος, από την (6.2) παρατηρούμε ότι η επιλογή των τιμών του ακεραίου i εξασφαλίζει ότι ο σταθερός όρος του $h_{ij}(z)$ είναι ίσος με 1. □

Θεώρημα 6.4 (Golomb και Gong [35]). *Έστω ο ακέραιος m είναι διαιρέτης του n, και έστω $M = 2^m - 1$. Έαν $K = N/M$, τότε για κάθε $t_1 = 1, 2, \ldots, M$ το ζέυγος ακεραίων*

$$(t_1 K \bmod N, t_2 K \bmod N)$$

αντιστοιχεί σε τριώνυμο της ακολουθίας x. Επιπλέον, ο ακέραιος t_2 δίνεται από τη σχέση $\alpha^{t_2 K} = \alpha^{t_1 K} + 1$, όπου το στοιχείο $\alpha \in \mathbb{F}_{2^n}$ είναι ρίζα του πολυωνύμου $f^*(z)$ στην επέκταση $\mathbb{F}_{2^n}$ του πρωταρχικού σώματος $\mathbb{F}_2$.

Εφαρμόζοντας το Θεώρημα 6.4 σε μικρά πεπερασμένα σώματα $\mathbb{F}_{2^n}$, δηλ. για $n \leq 10$, για όλους τους διαιρέτες m του ακεραίου n λαμβάνουμε ακριβώς το σύνολο των τριωνύμων T_f της ακολουθίας x. Στον Πίνακα 6.1 παρουσιάζουμε το αποτέλεσμα εφαρμογής του Θεωρήματος 6.4 σε δυαδικές ακολουθίες μήκους 63. Επειδή η επέκταση $\mathbb{F}_{2^n}$ του πρωταρχικού σώματος $\mathbb{F}_2$ είναι δυνατό να κατασκευαστεί από ρίζες ενός οποιουδήποτε πρωταρχικού πολυωνύμου βαθμού n με συντελεστές στο $\mathbb{F}_2$ ($\beta\lambda$. Κεφάλαιο 2), λαμβάνουμε το ακόλουθο αποτέλεσμα.

Πόρισμα 6.5. *Έστω x και y είναι δύο τυχαίες ακολουθίες μεγίστου μήκους, της ιδίας ελαχίστης περιόδου, με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Τότε ισχύει*

$$|T_f| = |T_g| .$$

Πίνακας 6.1. Τριώνυμα ακολουθιών που παράγονται από τα ανάστροφα των ελαχίστων πολυωνύμων του πεπερασμένου σώματος $\mathbb{F}_{2^6}$

πρωταρχικά στοιχεία

α^1	α^5	α^{11}	α^{13}	α^{23}	α^{31}
$(01, 06)$	$(01, 25)$	$(01, 08)$	$(01, 56)$	$(01, 39)$	$(01, 58)$
$(02, 12)$	$(02, 50)$	$(02, 16)$	$(02, 49)$	$(02, 15)$	$(02, 53)$
$(03, 32)$	$(03, 55)$	$(03, 53)$	$(03, 13)$	$(03, 11)$	$(03, 34)$
$(04, 24)$	$(04, 37)$	$(04, 32)$	$(04, 35)$	$(04, 30)$	$(04, 43)$
$(05, 62)$	$(05, 40)$	$(05, 38)$	$(05, 30)$	$(05, 28)$	$(05, 06)$
$(07, 26)$	$(06, 47)$	$(06, 43)$	$(06, 26)$	$(06, 22)$	$(07, 44)$
$(08, 48)$	$(07, 53)$	$(07, 62)$	$(07, 08)$	$(07, 17)$	$(08, 23)$
$(09, 45)$	$(08, 11)$	$(09, 45)$	$(09, 27)$	$(08, 60)$	$(09, 27)$
$(10, 61)$	$(09, 27)$	$(10, 13)$	$(10, 60)$	$(09, 45)$	$(10, 12)$
$(11, 25)$	$(10, 17)$	$(11, 51)$	$(11, 23)$	$(10, 56)$	$(11, 49)$
$(13, 35)$	$(12, 31)$	$(12, 23)$	$(12, 52)$	$(12, 44)$	$(13, 41)$
$(14, 52)$	$(13, 15)$	$(14, 61)$	$(14, 16)$	$(13, 61)$	$(14, 25)$
$(15, 23)$	$(14, 43)$	$(15, 44)$	$(15, 34)$	$(14, 34)$	$(15, 55)$
$(16, 33)$	$(16, 22)$	$(17, 41)$	$(17, 39)$	$(16, 57)$	$(16, 46)$
$(17, 47)$	$(18, 54)$	$(18, 27)$	$(18, 54)$	$(18, 27)$	$(17, 33)$
$(18, 27)$	$(19, 51)$	$(19, 34)$	$(19, 48)$	$(19, 31)$	$(18, 54)$
$(19, 56)$	$(20, 34)$	$(20, 26)$	$(20, 57)$	$(20, 49)$	$(19, 26)$
$(20, 59)$	$(21, 42)$	$(21, 42)$	$(21, 42)$	$(21, 42)$	$(20, 24)$
$(21, 42)$	$(23, 28)$	$(22, 39)$	$(22, 46)$	$(23, 58)$	$(21, 42)$
$(22, 50)$	$(24, 62)$	$(24, 46)$	$(24, 41)$	$(24, 25)$	$(22, 35)$
$(28, 41)$	$(26, 30)$	$(25, 30)$	$(25, 58)$	$(26, 59)$	$(28, 50)$
$(29, 60)$	$(29, 49)$	$(28, 59)$	$(28, 32)$	$(29, 43)$	$(29, 32)$
$(30, 46)$	$(32, 44)$	$(29, 48)$	$(29, 44)$	$(32, 51)$	$(30, 47)$
$(31, 34)$	$(33, 59)$	$(31, 35)$	$(31, 59)$	$(33, 37)$	$(31, 60)$
$(36, 54)$	$(35, 58)$	$(33, 58)$	$(33, 38)$	$(35, 40)$	$(36, 45)$
$(37, 44)$	$(36, 45)$	$(36, 54)$	$(36, 45)$	$(36, 54)$	$(37, 56)$
$(38, 49)$	$(38, 39)$	$(37, 57)$	$(37, 43)$	$(38, 62)$	$(38, 52)$
$(39, 43)$	$(41, 57)$	$(40, 52)$	$(40, 51)$	$(41, 47)$	$(39, 59)$
$(40, 55)$	$(46, 56)$	$(47, 49)$	$(47, 61)$	$(46, 53)$	$(40, 48)$
$(51, 53)$	$(48, 61)$	$(50, 60)$	$(50, 53)$	$(48, 50)$	$(51, 61)$
$(57, 58)$	$(52, 60)$	$(55, 56)$	$(55, 62)$	$(52, 55)$	$(57, 62)$

μη–πρωταρχικά στοιχεία

α^3	α^7	α^9	α^{15}	α^{21}	α^{27}
$(03, 15)$	$(03, 06)$	$(01, 05)$	$(03, 09)$	$(01, 02)$	$(01, 03)$
$(06, 09)$		$(02, 03)$	$(06, 18)$		$(02, 06)$
$(07, 14)$		$(04, 06)$	$(07, 14)$		$(04, 05)$
$(12, 18)$			$(12, 15)$		

Σε μεγαλύτερα πεπερασμένα σώματα, η μέθοδος των Golomb και Gong αποτυγχάνει να παράγει ακριβώς το σύνολο T_f. Σε κάθε περίπτωση, ο ακριβής υπολογισμός των τριωνύμων της ακολουθίας x επιτυγχάνεται από την εύρεση

των τοπικών μεγίστων της ροπής τρίτης τάξης της x, η οποία σε αντιστοιχία με την (3.24) ορίζεται ως εξής

$$\begin{aligned} \mathrm{AC}_x(t_1,t_2) &= \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{x_j+x_{j-t_1}+x_{j-t_2}} \\ &= 1-\frac{2}{N}\,\mathrm{wt}(\boldsymbol{x}+D^{t_1}\boldsymbol{x}+D^{t_2}\boldsymbol{x}) \end{aligned} \tag{6.3}$$

όπου $t_i \in \mathbb{Z}_N$. Η ακολουθία $\{\mathrm{AC}_x(t_1,t_2)\}_{t_1,t_2\geq 0}$ είναι δισδιάστατη περιοδική ακολουθία, με ελάχιστη περίοδο N προς κάθε κατεύθυνση. Επιπρόσθετα, η ροπή τρίτης τάξης είναι συμμετρική συνάρτηση, δηλ. $\mathrm{AC}_x(t_1,t_2)=\mathrm{AC}_x(t_2,t_1)$, επιτρέποντας τον ακριβή υπολογισμό του συνόλου T_f εξετάζοντας μόνον την περίπτωση όπου $t_1<t_2$.

Ο αποτελεσματικός υπολογισμός των ροπών τρίτης τάξης γίνεται μέσω του δισδιάστατου γρήγορου μετασχηματισμού Fourier (FFT), ακολουθούμενου από ένα σχήμα διάταξης. Η υπολογιστική πολυπλοκότητα του γρήγορου μετασχηματισμού Fourier κυμαίνεται από $\frac{3}{4}N^2\log_2 N$ έως $N^2\log_2 N$, αναλόγως έαν χρησιμοποιηθεί δισδιάστατος ή μονοδιάστατος FFT αντίστοιχα [50]. Η συγκεκριμένη μέθοδος υπολογισμού των τριωνύμων απαιτεί γνώση ολόκληρης της περιόδου $\boldsymbol{x}$ της ακολουθίας x.

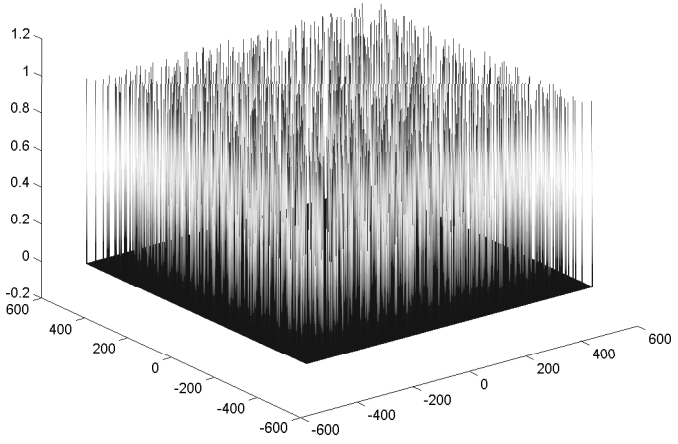
Από τις Ιδιότητες 3.9 και 3.11, η (6.3) οδηγεί στο συμπέρασμα ότι η ροπή τρίτης τάξης των ακολουθιών μεγίστου μήκους λαμβάνει την τιμή $-1/N$ σε όλο το φάσμα του συνόλου ορισμού $\mathbb{Z}_N^2$ εκτός από τα ζεύγη των ακεραίων $(t_1,t_2)\in\mathbb{Z}_N^2$ τα οποία είναι τέτοια ώστε

$$\boldsymbol{x}=D^{t_1}\boldsymbol{x}+D^{t_2}\boldsymbol{x}.$$

Τότε, η συνάρτηση $\mathrm{AC}_x(t_1,t_2)$ λαμβάνει την τιμή 1, και το ζεύγος ακεραίων (t_1,t_2) αντιστοιχεί σε τριώνυμο της ακολουθίας μεγίστου μήκους x.

Παράδειγμα 6.6. Οι ροπές τρίτης τάξης της ακολουθίας μεγίστου μήκους x με ελάχιστο πολυώνυμο $f(z)=1+z^3+z^{10}$ και ελάχιστη περίοδο 1023 επιδεικνύονται στο Σχ. 6.1. Έαν $(t_1,t_2)\notin T_f$, τότε η ροπή τρίτης τάξης $\mathrm{AC}_x(t_1,t_2)$ λαμβάνει την τιμή -0.001. Όπως ήταν αναμενόμενο, τα ζεύγη ακεραίων $(7,10)$ και $(10,7)$ είναι τριώνυμα της x αφού $f^*(z)=1+z^7+z^{10}$, ενώ $|T_f|=511$. □

Όπως φαίνεται στο Σχ. 6.1, έαν η x είναι ακολουθία μεγίστου μήκους, τότε για κάθε $t_1\in\mathbb{Z}_N^*$, λόγω της Ιδιότητας 3.9 υπάρχει μοναδικός ακέραιος $t_2\in\mathbb{Z}_N^*$



Σχήμα 6.1. Οι ροπές τρίτης τάξης της ακολουθίας x με ελάχιστο πολυώνυμο $f(z) = 1 + z^3 + z^{10}$

τέτοιος ώστε το ζεύγος ακεραίων (t_1, t_2) να αντιστοιχεί σε τριώνυμο της x. Συνεπώς, η μεταβλητή t_2 διατρέχει όλα τα στοιχεία του $\mathbb{Z}_N^*$ ακριβώς από μία φορά.

Ορισμός 6.7. Η περιοδική δυαδική ακολουθία x αποτελεί λευκό θόρυβο τρίτης τάξης έαν και μόνον έαν, επιπρόσθετα με τις συνθήκες του Ορισμού 6.1, ικανοποιείται η ακόλουθη συνθήκη [50]

iii. Τρεις τυχαίες διαφορετικές φάσεις της ακολουθίας x, που αντιστοιχούν στα διανύσματα $D^i\boldsymbol{x}$, $D^j\boldsymbol{x}$, και $D^k\boldsymbol{x}$, είναι ασυσχέτιστες, δηλ. η ροπή τρίτης τάξης $\mathrm{AC}_x(j-i, k-i)$ είναι ίση με μηδέν.

Σύμφωνα με τον Ορισμό 6.7, και την ανάλυση που προηγήθηκε, τα τριώνυμα ακολουθιών καταστρέφουν τα χαρακτηριστικά λευκού θορύβου τρίτης τάξης. Η κατάσταση αυτή είναι ενδεικτική για τις ακολουθίες μεγίστου μήκους αφού η συνάρτηση $\mathrm{AC}_x(t_1, t_2)$ λαμβάνει $N-1$ τοπικά μέγιστα στο χώρο $\mathbb{Z}_N^2$. Συνεπώς, οι ακολουθίες μεγίστου μήκους είναι ακατάλληλες για την προσομοίωση σημάτων λευκού θορύβου τρίτης (και γενικότερα ανωτέρας) τάξης.

6.1.2 Κανονικά πολυώνυμα ακολουθιών μεγίστου μήκους

Η εύρεση δυαδικών ακολουθιών, που προσομοιάζουν αποτελεσματικά σήματα λευκού θορύβου ανωτέρας τάξης, απαιτεί τη γενίκευση των αποτελεσμάτων της ενότητας 6.1.1. Η γενίκευση των ορισμών των τριωνύμων και των ροπών σε τάξεις μεγαλύτερες του τρία είναι άμεση και παρατίθεται στη συνέχεια.

Ορισμός 6.8. Το πολυώνυμο $h(z) = 1 + z^{t_1} + \cdots + z^{t_{k-1}}$, $t_i \in \mathbb{Z}_N$, ονομάζεται *κανονικό πολυώνυμο* της ακολουθίας x έαν και μόνον έαν όλες οι δυνάμεις t_i της μεταβλητής z είναι διαφορετικές μεταξύ τους, και το $h(z)$ διαιρείται από το ανάστροφο του ελαχίστου πολυωνύμου της x.

Στην περίπτωση όπου οι δυνάμεις t_i της μεταβλητής z δεν είναι όλες διαφορετικές μεταξύ τους, και το $h(z)$ διαιρείται από το ανάστροφο του ελαχίστου πολυωνύμου της x, τότε το $h(z)$ ονομάζεται *μη–κανονικό πολυώνυμο* της ακολουθίας x. Το πολυώνυμο $h(z)$ συμβολίζεται ισοδύναμα με το $1 \times k-1$ διάνυσμα $\boldsymbol{t} = (t_1, \ldots, t_{k-1})$.

Έαν το διάνυσμα $\boldsymbol{t}$ αντιστοιχεί σε κανονικό πολυώνυμο της ακολουθίας x, τότε προφανώς ισχύει η σχέση

$$\boldsymbol{x} + D^{t_1}\boldsymbol{x} + \cdots + D^{t_{k-1}}\boldsymbol{x} = \boldsymbol{0}$$

και κατά συνέπεια η ακολουθία x ικανοποιεί τη γραμμική επαναληπτική σχέση

$$x_j = x_{j-t_1} + \cdots + x_{j-t_{k-1}}$$

για κάθε $j \geq t_{k-1}$. Στην περίπτωση όπου το διάνυσμα $\boldsymbol{t}$ αντιστοιχεί σε μη–κανονικό πολυώνυμο της ακολουθίας x, τότε υπάρχει ακέραιος m τέτοιος ώστε η ακολουθία x να ικανοποιεί γραμμική επαναληπτική σχέση τάξης $m < k$.

Όμοια με την περίπτωση των τριωνύμων, η τιμή των ροπών τάξης k σε διανύσματα $\boldsymbol{t}$ που αντιστοιχούν σε κανονικά και μη–κανονικά πολυώνυμα $h(z)$ της ακολουθίας x είναι ίση με τη μονάδα. Προφανώς, διανύσματα με αυτήν την ιδιότητα αντιστοιχούν σε τοπικά μέγιστα ροπών τάξης k. Ωστόσο, η εύρεση των κανονικών και μη–κανονικών πολυωνύμων της ακολουθίας x, σε τάξεις μεγαλύτερες του τρία, γίνεται πιο αποτελεσματικά κάνοντας χρήση *αθροιστικών*.

Οι αθροιστικές, όπως και οι ροπές, ενός σήματος παρέχουν πληροφορία ανωτέρας τάξης στο πεδίο του χρόνου και των συχνοτήτων αντίστοιχα. Παρ' ότι οι αθροιστικές και οι ροπές παρέχουν ισοδύναμη πληροφορία, οι αθροιστικές

προτιμούνται λόγω των ελκυστικών ιδιοτήτων που επιδεικνύουν [50]. Η σχέση μεταξύ αθροιστικών και ροπών αναλύεται στο Παράρτημα Β. Έαν η ακολουθία x είναι ισοβαρής, όπως ισχύει για τις ακολουθίες μεγίστου μήκους, τότε οι αθροιστικές μέχρι τρίτης τάξης είναι ίσες με τις αντίστοιχες ροπές ιδίας τάξης. Στη συνέχεια δίνεται ο γενικός ορισμός σημάτων λευκού θορύβου ανωτέρας τάξης βάσει αθροιστικών.

Ορισμός 6.9. Η περιοδική ακολουθία x αποτελεί σήμα λευκού θορύβου τάξης k έαν οι αθροιστικές της μέχρι τάξης k είναι πολυδιάστατες συναρτήσεις παλμών Dirac, δηλ.

$$\mathrm{cum}(\boldsymbol{x}, D^{t_1}\boldsymbol{x}, \ldots, D^{t_{s-1}}\boldsymbol{x}) = \gamma_s \delta(t_1) \cdots \delta(t_{s-1})$$

για κάθε $s = 2, \ldots, k$, όπου $\mathrm{cum}(\cdot)$ συμβολίζει την αθροιστική τάξης s, $\delta(\cdot)$ είναι η μονοδιάστατη συνάρτηση παλμού Dirac, και γ_s είναι η *ένταση* τάξης s της ακολουθίας x.

Καθίσταται φανερό από την ανωτέρω ανάλυση ότι ακολουθίες παραγόμενες από σύνθετες δομές είναι αναγκαίες ώστε να εξασφαλιστεί η απώλεια (ή ύπαρξη ελαχίστου πλήθους) τοπικών μεγίστων στις ροπές και αθροιστικές ανωτέρας τάξης. Επιπρόσθετα, είναι απαραίτητη η διατήρηση του υπολοίπου φάσματος τιμών των ροπών και αθροιστικών σε χαμηλά επίπεδα, ώστε να χαρακτηριστούν οι παραγόμενες ακολουθίες κατάλληλες για την προσομοίωση σημάτων λευκού θορύβου ανωτέρας τάξης.

6.2 Δυϊκές BCH και Gold ακολουθίες

Στην παρούσα ενότητα εξετάζεται η περίπτωση των δυαδικών ακολουθιών που προκύπτουν από την όρο–προς–όρο (modulo 2) πρόσθεση ακολουθιών μεγίστου μήκους ιδίας ελαχίστης περιόδου.

Αρχικά δείχνουμε ότι τα στατιστικά (ροπές και αθροιστικές) των παραγόμενων ακολουθιών καθορίζονται σε μεγάλο βαθμό από τη συνάρτηση περιοδικής ετεροσυσχέτισης των συνιστωσών ακολουθιών μεγίστου μήκους. Όταν οι ρίζες των ελαχίστων πολυωνύμων των συνιστωσών ακολουθιών σχετίζονται με συγκεκριμένο τρόπο, τότε η συνάρτηση ετεροσυσχέτισης λαμβάνει ένα καθορισμένο σύνολο τιμών καθιστώντας δυνατό τον έλεγχό τους επιλέγοντας κατάλληλα τις τιμές σχετικών παραμέτρων.

Επιπρόσθετα, το πλήθος των τοπικών μεγίστων των ροπές ανωτέρας τάξης μειώνεται δραστικά ή μηδενίζεται. Τέλος, δείχνουμε ότι στην περίπτωση δυϊκών BCH ακολουθιών διόρθωσης t σφαλμάτων οι ροπές τάξης έως $2t$ δεν παρουσιάζουν τοπικά μέγιστα.

6.2.1 Τριώνυμα αθροίσματος ακολουθιών ιδίας περιόδου

Στο Κεφάλαιο 3 σημειώθηκε ότι έαν $f(z)$ και $g(z)$ είναι τα ελάχιστα πολυώνυμα δύο τυχαίων δυαδικών ακολουθιών x και y, τότε το ελάχιστο πολυώνυμο της ακολουθίας $w = x + y$ είναι ίσο με το ελάχιστο κοινό πολλαπλάσιο των $f(z)$ και $g(z)$ [126]. Ως αποτέλεσμα, έαν τα πολυώνυμα $f(z)$ και $g(z)$ είναι πρώτα μεταξύ τους, όπως ισχύει στην περίπτωση που οι x και y είναι διαφορετικές ακολουθίες μεγίστου μήκους, τότε το ελάχιστο πολυώνυμο της w είναι ίσο με το γινόμενο των $f(z)$ και $g(z)$.

Ακολουθίες αυτής της κλάσης παρουσιάζουν ιδιαίτερο ενδιαφέρον αφού επιτρέπουν την απαλοιφή των τοπικών μεγίστων των ροπών τρίτης (και ανωτέρας) τάξης των ακολουθιών μεγίστου μήκους.

Λήμμα 6.10. *Έστω $f(z)$ και $g(z)$, με $f(0) = g(0) = 1$, είναι τυχαία πολυώνυμα του δακτυλίου $\mathbb{F}_2[z]/(1 + z^N)$. Τότε*

i. $(fg)^* = f^* g^*$,

ii. $\gcd(f^*, g^*) = \gcd(f, g)^*$, *και*

iii. $\mathrm{lcm}(f^*, g^*) = \mathrm{lcm}(f, g)^*$.

Απόδειξη. Έστω k και l είναι οι βαθμοί των πολυωνύμων $f(z)$ και $g(z)$ αντίστοιχα. Τότε, ο βαθμός του πολυωνύμου $(fg)(z)$ είναι ίσος με $k + l$, και ισχύει ότι

$$\begin{aligned}(fg)^*(z) &= z^{k+l}(fg)(1/z) = z^k f(1/z) z^l g(1/z) \\ &= f^*(z) g^*(z).\end{aligned}$$

Επιπρόσθετα, παρατηρούμε ότι λόγω της υπόθεσης $f(0) = g(0) = 1$, λαμβάνουμε $\deg(f^* g^*) = \deg(fg)$ και συνεπώς ισχύει η σχέση $(f^* g^*)^* = fg$.

Έαν συμβολίσουμε με $r(z)$ το μέγιστο κοινό διαιρέτη των πολυωνύμων $f(z)$ και $g(z)$, τότε υπάρχουν πολυώνυμα $p(z)$ και $q(z)$ τέτοια ώστε

$$f(z) = p(z) r(z) \quad \text{και} \quad g(z) = q(z) r(z).$$

Λόγω του πρώτου μέρους της απόδειξης, οι ανωτέρω σχέσεις οδηγούν στις ακόλουθες ισοδύναμες

$$f^*(z) = p^*(z)r^*(z) \qquad \text{και} \qquad g^*(z) = q^*(z)r^*(z).$$

Συνεπώς, το πολυώνυμο $r^*(z)$ είναι κοινός διαιρέτης των $f^*(z)$ και $g^*(z)$. Το αποτέλεσμα ότι το πολυώνυμο $r^*(z)$ είναι ο μέγιστος κοινός διαιρέτης των $f^*(z)$ και $g^*(z)$ απορρέει από το μέγιστο του βαθμού του πολυωνύμου $r(z)$ και την ιδιότητα $\deg(r) = \deg(r^*)$.

Η τελευταία ιδιότητα του λήμματος αποδεικνύεται με όμοιο τρόπο. □

Το ακόλουθο θεώρημα εκφράζει το σύνολο τριωνύμων της ακολουθίας $w = x + y$ συναρτήσει των συνόλων τριωνύμων των συνιστωσών ακολουθιών x και y.

Θεώρημα 6.11. *Έστω x και y είναι διαφορετικές δυαδικές ακολουθίες της ιδίας ελαχίστης περιόδου με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Τότε, το σύνολο τριωνύμων της ακολουθίας $w = x + y$ δίνεται από τη σχέση*

$$T_{\mathrm{lcm}(f,g)} = T_f \cap T_g.$$

Απόδειξη. Ας υποθέσουμε ότι το ζεύγος ακεραίων (t_1, t_2) αντιστοιχεί στο τριώνυμο $h(z)$ της ακολουθίας w. Σύμφωνα με τον Ορισμό 6.2 και το Λήμμα 6.10, το πολυώνυμο $\mathrm{lcm}(f^*(z), g^*(z))$ αποτελεί διαιρέτη του $h(z)$, και συνεπώς το $h(z)$ διαιρείται και από τα δύο πολυώνυμα $f^*(z)$ και $g^*(z)$. Ισοδύναμα, το (t_1, t_2) είναι τριώνυμο και των δύο συνιστωσών ακολουθιών x και y, δηλ.

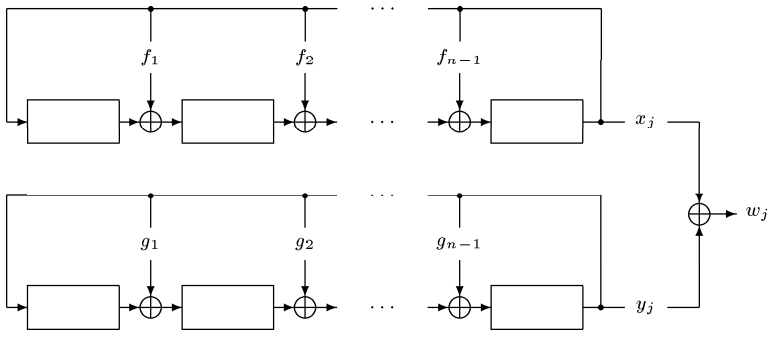
$$T_{\mathrm{lcm}(f,g)} \subseteq T_f \cap T_g. \tag{6.4}$$

Αντιστρόφως, έαν το (t_1, t_2) είναι τριώνυμο και των δύο συνιστωσών ακολουθιών x και y, τότε το $h(z)$ διαιρείται και από τα δύο πολυώνυμα $f^*(z)$ και $g^*(z)$. Συνεπώς, το πολυώνυμο $\mathrm{lcm}(f^*(z), g^*(z))$ επίσης διαιρεί το $h(z)$, και έχουμε

$$T_f \cap T_g \subseteq T_{\mathrm{lcm}(f,g)}. \tag{6.5}$$

Η ισχύς της υπόθεσης αποδεικνύεται από τις σχέσεις (6.4) και (6.5). □

Αν και, σύμφωνα με το Θεώρημα 6.11, το πλήθος των τριωνύμων (ισοδύναμα των τοπικών μεγίστων που παρουσιάζονται στις ροπές τρίτης τάξης) των ακολουθιών της μορφής $x + y$, μειώνεται ή μηδενίζεται, εξαρτάται από την επιλογή των



Σχήμα 6.2. Κύκλωμα παραγωγής ακολουθιών που ανήκουν στο δυϊκό κώδικα ενός διπλού διορθωτικού BCH κώδικα με πολυώνυμο γεννήτορα $f^*(z)g^*(z)$

συγκεκριμένων περιοδικών ακολουθιών ιδίας περιόδου x και y. Στις ενότητες 6.2.2 και 6.2.3 δίνονται τρόποι επιλογής κατάλληλων ζευγών ακολουθιών ώστε να μειώνεται το πλήθος των τριωνύμων της $x + y$ στο ελάχιστο δυνατό.

6.2.2 Δυϊκές BCH ακολουθίες

Έστω η δυαδική ακολουθία μεγίστου μήκους x, ελαχίστης περιόδου $N = 2^n - 1$, και με ελάχιστο πολυώνυμο $f(z)$. Επιπλέον, ας θεωρήσουμε την ακολουθία $y = x[3]$, με ελάχιστο πολυώνυμο $g(z)$, που παράγεται από τη δειγματοληψία της x με παράγοντα 3.

Από το Κεφάλαιο 3, η y έχει ελάχιστη περίοδο N, δηλ. είναι ακολουθία μεγίστου μήκους, έαν ο ακέραιος n είναι περιττός, ενώ έχει ελάχιστη περίοδο $N/3$ έαν ο ακέραιος n είναι άρτιος. Και στις δύο περιπτώσεις ο βαθμός του ελαχίστου πολυωνύμου $g(z)$ της ακολουθίας y είναι ίσος με n. Επιπλέον, οι ρίζες των πολυωνύμων $f(z)$ και $g(z)$ είναι οι $\alpha, \alpha^3 \in \mathbb{F}_{2^n}$ αντίστοιχα.

Η ακολουθία $w = x + y$ παράγεται από το κύκλωμα του Σχ. 6.2, έχει ελάχιστο πολυώνυμο το $f(z)g(z)$, και ανήκει στο δυϊκό κώδικα του BCH κώδικα διόρθωσης δύο σφαλμάτων $\mathcal{C}$ με πολυώνυμο γεννήτορα το $f^*(z)g^*(z)$ [5], [9], [76]. Σύμφωνα με τον Ορισμό 6.2, τα τριώνυμα της ακολουθίας w ταυτοποιούνται με τα πολλαπλάσια του πολυωνύμου $f^*(z)g^*(z)$ βάρους 3.

Επειδή ο $\mathcal{C}$ είναι κώδικας διόρθωσης δύο σφαλμάτων, όλες οι κωδικές λέξεις, ή ισοδύναμα όλα τα πολλαπλάσια του πολυωνύμου $f^*(z)g^*(z)$ έχουν βάρος

μεγαλύτερο του 4 [50]. Συνεπώς, διασφαλίζεται ότι στις ροπές τρίτης και τέταρτης τάξης της ακολουθίας w δεν παρουσιάζονται τοπικά μέγιστα, δηλ. ζεύγη ακεραίων (t_1, t_2) τέτοια ώστε $\mathrm{AC}_w(t_1, t_2) = 1$.

Παράδειγμα 6.12. Έστω x και y είναι δυαδικές ακολουθίες με ελάχιστα πολυώνυμα

$$f(z) = 1 + z^3 + z^{10} \quad \text{και} \quad g(z) = 1 + z + z^2 + z^3 + z^{10}$$

αντίστοιχα, όπου οι ρίζες του $g(z)$ είναι οι κύβοι των ριζών του $f(z)$ στο πεπερασμένο σώμα $\mathbb{F}_{2^{10}}$. Επειδή ο ακέραιος n είναι άρτιος, το πολυώνυμο $g(z)$ δεν είναι πρωταρχικό και η ακολουθία y έχει ελάχιστη περίοδο $N/3$. Το διάνυσμα $\boldsymbol{w}$, το οποίο περιλαμβάνει τα στοιχεία μιας περιόδου της ακολουθίας w, προκύπτει από το άθροισμα (modulo 2) των διανυσμάτων

$$\boldsymbol{x} \quad \text{και} \quad \boldsymbol{y}' = \begin{pmatrix} \boldsymbol{y} & \boldsymbol{y} & \boldsymbol{y} \end{pmatrix}.$$

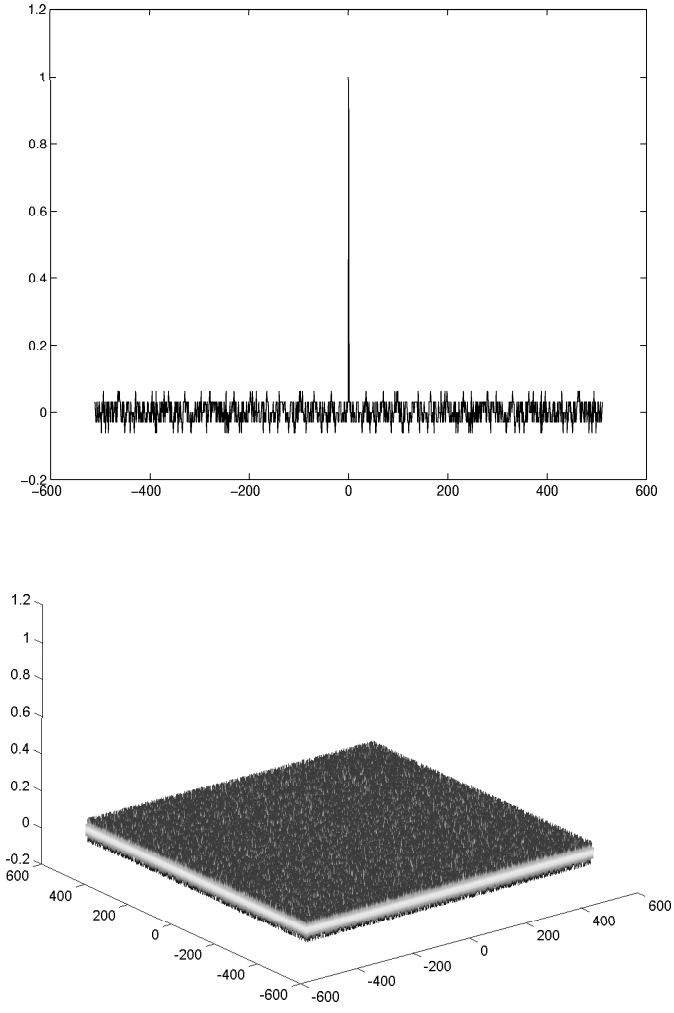
Παραθέτουμε στο Σχ. 6.3 τις συναρτήσεις περιοδικής αυτοσυσχέτισης δεύτερης και τρίτης τάξης της ακολουθίας $w = x + y$ για σύγκριση με τις αντίστοιχες των Σχ. 3.3 και 6.1. Οι τιμές της συνάρτησης $\mathrm{AC}_w(t_1, t_2)$ είναι μεταξύ των ακεραίων -0.0635 και 0.0616. □

Στην περίπτωση του Παραδείγματος 6.12, το Θεώρημα 6.11 εφαρμόζεται θεωρώντας ότι η ακολουθία y έχει περίοδο N και χρησιμοποιώντας την περιοδική επέκταση $\boldsymbol{y}'$ του διανύσματος $\boldsymbol{y}$. Επιπλέον, για την εύρεση των τριωνύμων της ακολουθίας w αντικαθιστούμε το σύνολο T_g που αντιστοιχεί στην y με το T'_g, το οποίο ορίζεται στο ακόλουθο Λήμμα.

Λήμμα 6.13. *Ας θεωρήσουμε τη δυαδική ακολουθία x ελαχίστης περιόδου M, όπου ο ακέραιος M είναι διαιρέτης του N. Έστω $f(z)$ και T_f είναι το ελάχιστο πολυώνυμο και το σύνολο τριωνύμων της ακολουθίας x αντίστοιχα. Θεωρώντας την x ως ακολουθία περιόδου N, τότε το σύνολο τριωνύμων T'_f της x στο σύνολο $\mathbb{Z}_N^2$ δίνεται από τη σχέση*

$$T'_f = \Big\{(t_1, t_2) \in \mathbb{Z}_N^2 : (t_1 \bmod M, t_2 \bmod M) \in T_f\Big\}.$$

Απόδειξη. Σύμφωνα με την ανάλυση που πραγματοποιήθηκε στην ενότητα 6.1, η τάξη του πολυωνύμου $f(z)$ είναι M, δηλ. το $f(z)$ ανήκει στο σύνολο $\mathbb{F}_2[z]/$



Σχήμα 6.3. Η αυτοσυσχέτιση και οι ροπές τρίτης τάξης της ακολουθίας $w = x+y$ με ελάχιστο πολυώνυμο $f(z)g(z) = 1+z+z^2+z^4+z^5+z^6+z^{11}+z^{12}+z^{20}$

$(1+z^M)$. Έστω $h(z)$ είναι τυχαίο πολυώνυμο του συνόλου $\mathbb{F}_2[z]/(1+z^M)$. Έαν $t_1, t_2 \in \mathbb{Z}_N$, τα πολυώνυμα $h'(z) = 1 + z^{t_1} + z^{t_2}$ και

$$h(z) = h'(z) \bmod 1 + z^M \Leftrightarrow h(z) = 1 + z^{t_1 \bmod M} + z^{t_2 \bmod M}$$

ταυτίζονται [72]. Το αποτέλεσμα αποδεικνύεται εύκολα λαμβάνοντας υπόψη ότι το $f^*(z)$ διαιρεί το $h'(z)$ έαν και μόνον έαν το $f^*(z)$ διαιρεί το $h(z)$. □

Όπως αποδεικνύεται στη συνέχεια, οι ροπές τρίτης (και ανωτέρας) τάξης της ακολουθίας $w = x + y$ καθορίζονται πλήρως από τις τιμές της συνάρτησης περιοδικής ετεροσυσχέτισης των x και y, ελαχίστης περιόδου N. Έαν οι ακολουθίες x και y έχουν διαφορετικές ελάχιστες περιόδους, έστω N_1 και N_2 αντίστοιχα, τότε στην (3.25) χρησιμοποιούμε όπου N το ελάχιστο κοινό πολλαπλάσιο των ακεραίων N_1 και N_2. Το ακόλουθο θεώρημα αποδεικνύεται στη γενική περίπτωση όπου οι ακολουθίες μεγίστου μήκους έχουν διαφορετικές ελάχιστες περιόδους.

Θεώρημα 6.14. *Έστω x και y είναι ακολουθίες μεγίστου μήκους, ελαχίστων περιόδων N_1 και N_2, με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Τότε, οι ροπές τρίτης τάξης της ακολουθίας $w = x + y$, ελαχίστης περιόδου $N = \mathrm{lcm}(N_1, N_2)$, δίνονται από τη σχέση*

$$\mathrm{AC}_w(t_1, t_2) = \begin{cases} 1 & \text{έαν } (t_1, t_2) \in T'_f \cap T'_g, \\ -1/N_1 & \text{έαν } (t_1, t_2) \in T'_g \setminus T'_f, \\ -1/N_2 & \text{έαν } (t_1, t_2) \in T'_f \setminus T'_g, \\ \mathrm{CC}_{x',y'}(t) & \text{διαφορετικά}, \end{cases}$$

όπου $t \in \mathbb{Z}_N$.

Απόδειξη. Σύμφωνα με την (6.3), η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας w δίνεται από τη σχέση

$$\mathrm{AC}_w(t_1, t_2) = \frac{1}{N} \sum_{j=0}^{N-1} (-1)^{(x_j + x_{j-t_1} + x_{j-t_2}) + (y_j + y_{j-t_1} + y_{j-t_2})}.$$

Έαν το ζεύγος ακεραίων (t_1, t_2) αντιστοιχεί σε τριώνυμο και των δύο ακολουθιών x και y στο σύνολο $\mathbb{Z}_N^2$, τότε προφανώς ισχύει $\mathrm{AC}_w(t_1, t_2) = 1$.

Στην περίπτωση που το ζεύγος ακεραίων (t_1, t_2) είναι τριώνυμο της ακολουθίας y αλλά όχι και της x, οι ροπές τρίτης τάξης γράφονται ως εξής

$$\mathrm{AC}_w(t_1, t_2) = \frac{1}{N} \sum_{j=0}^{N-1} (-1)^{x_{j-t_3}} = \frac{1}{N_1} \sum_{j=0}^{N_1-1} (-1)^{x_{j-t_3}}$$

λόγω της Ιδιότητας 3.9 των ακολουθιών μεγίστου μήκους, και ότι η ελάχιστη περίοδος της x είναι ίση με N_1. Από την Ιδιότητα 3.11 των ακολουθιών μεγίστου μήκους λαμβάνουμε ότι $\mathrm{AC}_w(t_1, t_2) = -1/N_1$. Η περίπτωση που το ζεύγος ακεραίων (t_1, t_2) είναι τριώνυμο της ακολουθίας x αλλά όχι και της y αποδεικνύεται με όμοιο τρόπο.

Τέλος, έαν το ζεύγος ακεραίων (t_1, t_2) δεν αποτελεί τριώνυμο των ακολουθιών x και y στο σύνολο $\mathbb{Z}_N^2$, τότε λόγω της Ιδιότητας 3.9 των ακολουθιών μεγίστου μήκους υπάρχουν ακέραιοι t_3 και t_4 τέτοιοι ώστε

$$\boldsymbol{x} + D^{t_1}\boldsymbol{x} + D^{t_2}\boldsymbol{x} = D^{t_3}\boldsymbol{x} \quad \text{και} \quad \boldsymbol{y} + D^{t_1}\boldsymbol{y} + D^{t_2}\boldsymbol{y} = D^{t_4}\boldsymbol{y}.$$

Συνεπώς, οι ροπές τρίτης τάξης γράφονται ως εξής

$$\mathrm{AC}_w(t_1, t_2) = \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{x_{j-t_3}+y_{j-t_4}} = \mathrm{CC}_{x',y'}(t_4 - t_3)$$

ολοκληρώνοντας την απόδειξη. □

Θεώρημα 6.15. *Έστω x και y είναι ακολουθίες μεγίστου μήκους, ελαχίστων περιόδων N_1 και N_2, με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Τότε, η συνάρτηση αυτοσυσχέτισης της ακολουθίας $w = x + y$, ελαχίστης περιόδου $N = \mathrm{lcm}(N_1, N_2)$, δίνεται από τη σχέση*

$$\mathrm{AC}_w(t) = \begin{cases} 1 & \text{εαν } t \equiv 0 \pmod{N}, \\ -1/N_1 & \text{εαν } t \equiv 0 \pmod{N_2}, \\ -1/N_2 & \text{εαν } t \equiv 0 \pmod{N_1}, \\ \mathrm{CC}_{x',y'}(t') & \text{διαφορετικά}, \end{cases}$$

όπου $t' \in \mathbb{Z}_N$.

Απόδειξη. Όμοια με την προηγούμενη απόδειξη. □

Επειδή οι x και y είναι ακολουθίες μεγίστου μήκους, είναι προφανές ότι ισχύει $\mathrm{CC}_{x,y}(t) < 1$ για κάθε $t \in \mathbb{Z}_N$. Συνεπώς, το Θεώρημα 6.14 είναι σε συμφωνία με το Θεώρημα 6.11 σχετικά με το σύνολο τριωνύμων της ακολουθίας w. Στη συνέχεια, παραθέτουμε τις περιπτώσεις όπου οι ακολουθίες μεγίστου μήκους x και y έχουν την ίδια ελάχιστη περίοδο.

Πόρισμα 6.16. *Έστω x, y είναι ακολουθίες μεγίστου μήκους, ιδίας ελαχίστης περιόδου N, με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Τότε, οι ροπές τρίτης τάξης της ακολουθίας $w = x + y$ δίνονται από τη σχέση*

$$\mathrm{AC}_w(t_1, t_2) = \begin{cases} 1 & \text{έαν } (t_1, t_2) \in T_f \cap T_g, \\ -1/N & \text{έαν } (t_1, t_2) \in (T_f \cup T_g) \setminus (T_f \cap T_g), \\ \mathrm{CC}_{x,y}(t) & \text{διαφορετικά}, \end{cases}$$

όπου $t \in \mathbb{Z}_N$.

Πόρισμα 6.17. *Έστω x και y ακολουθίες μεγίστου μήκους, ιδίας ελαχίστης περιόδου N, με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Τότε, η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας $w = x + y$ δίνεται από τη σχέση*

$$\mathrm{AC}_w(t) = \begin{cases} 1 & \text{έαν } t \equiv 0 \pmod N, \\ \mathrm{CC}_{x,y}(t') & \text{διαφορετικά}, \end{cases}$$

όπου $t' \in \mathbb{Z}_N$.

Οι ροπές k τάξης $\mathrm{AC}_w(t_1, \ldots, t_{k-1})$ της ακολουθίας w υπολογίζονται όμοια με τις ροπές τρίτης τάξης, μέσω του Θεωρήματος 6.14 ή του Πορίσματος 6.16. Στη συγκεκριμένη περίπτωση, τα σύνολα T_f και T_g περιλαμβάνουν όλα τα κανονικά και μη–κανονικά πολυώνυμα βάρους k των ακολουθιών x και y αντίστοιχα. Η απουσία τοπικών μεγίστων στις ροπές τρίτης και τέταρτης τάξης των δυϊκών BCH ακολουθιών διόρθωσης δύο σφαλμάτων γενικεύεται με το ακόλουθο θεώρημα.

Θεώρημα 6.18. *Έστω $f^*(z)$ είναι το πολυώνυμο γεννήτορας ενός δυαδικού BCH κώδικα διόρθωσης k σφαλμάτων. Τότε, οι ροπές s τάξης της δυαδικής ακολουθίας w, περιόδου N, με ελάχιστο πολυώνυμο $f(z)$ δεν παρουσιάζουν τοπικά μέγιστα, για κάθε ακέραιο $s \leq 2k$.*

Απόδειξη. Έστω $\{A_0, A_1, \ldots, A_N\}$ είναι οι τιμές της συνάρτησης κατανομής βάρους του $(N, N - \deg(f^*))$ γραμμικού κυκλικού κώδικα $\mathcal{C}$ με πολυώνυμο γεννήτορα $f^*(z)$. Ως γνωστό, ο ακέραιος A_i είναι ίσος με το πλήθος των κωδικών λέξεων του $\mathcal{C}$, ή ισοδύναμα των πολλαπλασίων του πολυωνύμου $f^*(z)$, βάρους i [50].

Τότε, η ακολουθία w με ελάχιστο πολυώνυμο $f(z)$ ανήκει στο δυϊκό κώδικα του $\mathcal{C}$, και σύμφωνα με τον Ορισμό 6.8 το πλήθος των κανονικών πολυωνύμων

βάρους s, που αντιστοιχούν σε τοπικά μέγιστα ροπών τάξης s, δίνεται από τον ακέραιο A_s. Συνεπώς, η συνθήκη

$$A_1 = A_2 = \cdots = A_{2k} = 0$$

είναι αναγκαία αλλά όχι και ικανή για κατασκευή ακολουθιών w που προσομοιάζουν σήματα λευκού θορύβου τάξης k. Η συγκεκριμένη συνθήκη είναι χαρακτηριστική για τους (μεταξύ άλλων) BCH κώδικες διόρθωσης k σφαλμάτων [5], [9], [76]. □

Επιπρόσθετα με την ισχύ του Θεωρήματος 6.18 πρέπει η ακολουθία w να είναι ισοβαρής, ώστε να ικανοποιούνται όλες οι συνθήκες του Ορισμού 6.9. Η κατάλληλη επιλογή των αρχικών καταστάσεων των καταχωρητών ολίσθησης γραμμικής ανάδρασης που παράγουν τις δυϊκές BCH ακολουθίες, είναι δυνατό να οδηγήσει στην παραγωγή ισοβαρών ακολουθιών w.

6.2.3 Ακολουθίες Gold

Ιδιότητες όμοιες με εκείνες των δυϊκών BCH ακολουθιών παρουσιάζουν και οι *ακολουθίες Gold*, οι οποίες κατασκευάζονται προσθέτοντας (modulo 2) δύο ακολουθίες μεγίστου μήκους ιδίας περιόδου [29], [30], [107]. Το πλεονέκτημα των ακολουθιών Gold είναι ότι επιτρέπουν μεγαλύτερο έλεγχο του μεγέθους των τιμών που λαμβάνει η συνάρτηση περιοδικής αυτοσυσχέτισης μέσω του ακόλουθου θεωρήματος [30], [53].

Θεώρημα 6.19 (Gold και Kasami). *Έστω $w = x + y$ είναι ακολουθία Gold ελαχίστης περιόδου $N = 2^n - 1$, όπου x και y είναι ακολουθίες μεγίστου μήκους με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Εαν οι ρίζες του πολυωνύμου $g(z)$ είναι η d–στή δύναμη των ριζών του $f(z)$, όπου*

$$d = 2^k + 1 \quad \text{ή} \quad d = 2^{2k} - 2^k + 1$$

και ο ακέραιος $e = \gcd(k, n)$ είναι τέτοιος ώστε το κλάσμα n/e είναι περιττός ακέραιος, τότε η συνάρτηση περιοδικής ετεροσυσχέτισης των ακολουθιών x και y λαμβάνει τις ακόλουθες τρεις τιμές

$$\begin{aligned} -1/N \quad & \text{με συχνότητα} \quad 2^n - 2^{n-e} - 1, \\ (-1 - 2^{\frac{n+e}{2}})/N \quad & \text{με συχνότητα} \quad 2^{n-e-1} - 2^{\frac{n-e-2}{2}}, \text{ και} \end{aligned}$$

Πίνακας 6.2. Εφαρμογή του Θεωρήματος 6.19 για $n = 9, 15$. Δίνονται οι τιμές που λαμβάνει η συνάρτηση ετεροσυσχέτισης και η συχνότητα εμφάνισής τους

n	e	k	τιμές	συχνότητα
9	1	$1, 2, 4, 5, 7, 8$	-0.00196	255
			-0.06458	120
			0.06067	136
	3	$3, 6$	-0.00196	447
			-0.12720	28
			0.12329	36
15	1	$1, 2, 4, 7, 8, 11, 13, 14$	-0.00003	16383
			-0.00784	8128
			0.00778	8256
	3	$3, 6, 9, 12$	-0.00003	28671
			-0.01566	2016
			0.01559	2080
	5	$5, 10$	-0.00003	31743
			-0.03128	496
			0.03122	528

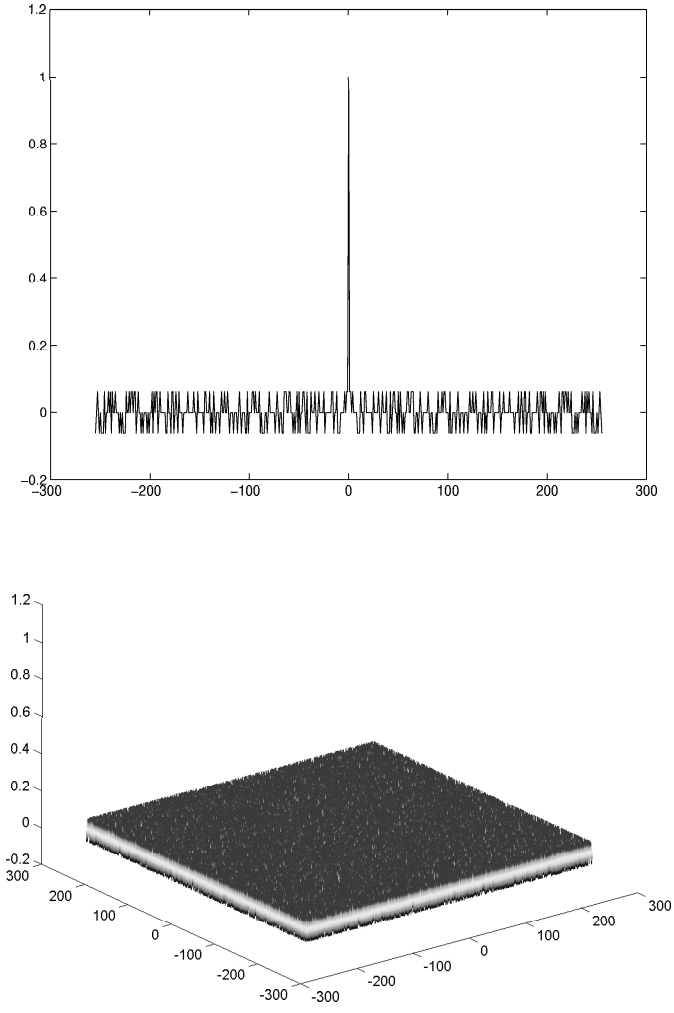
$$(-1 + 2^{\frac{n+e}{2}})/N \quad \mu\epsilon\ \sigma\upsilon\chi\nu\acute{o}\tau\eta\tau\alpha \quad 2^{n-e-1} + 2^{\frac{n-e-2}{2}},$$

αντίστοιχα.

Έαν ο ακέραιος n είναι περιττός και $k = 1$ (δηλ. $e = 1$ και $d = 3$), τότε οι ακολουθίες που κατασκευάζονται ταυτίζονται με την κλάση των δυϊκών BCH ακολουθιών διόρθωσης δύο σφαλμάτων, όπου και οι δύο συνιστώσες x και y είναι ακολουθίες μεγίστου μήκους. Αντιθέτως, έαν ο ακέραιος n είναι άρτιος και $k = 1$ (δηλ. $e = 1$ και $d = 3$), τότε το Θεώρημα 6.19 δεν είναι δυνατό να εφαρμοστεί, ενώ επιπλέον, η y δεν είναι ακολουθία μεγίστου μήκους ($\beta\lambda$. ενότητα 6.2.2). Τότε, η συνάρτηση περιοδικής ετεροσυσχέτισης των ακολουθιών x και y λαμβάνει τις τιμές $-1/N$, $(-1 \pm 2^{n/2})/N$, και $(-1 \pm 2^{(n+2)/2})/N$ [107].

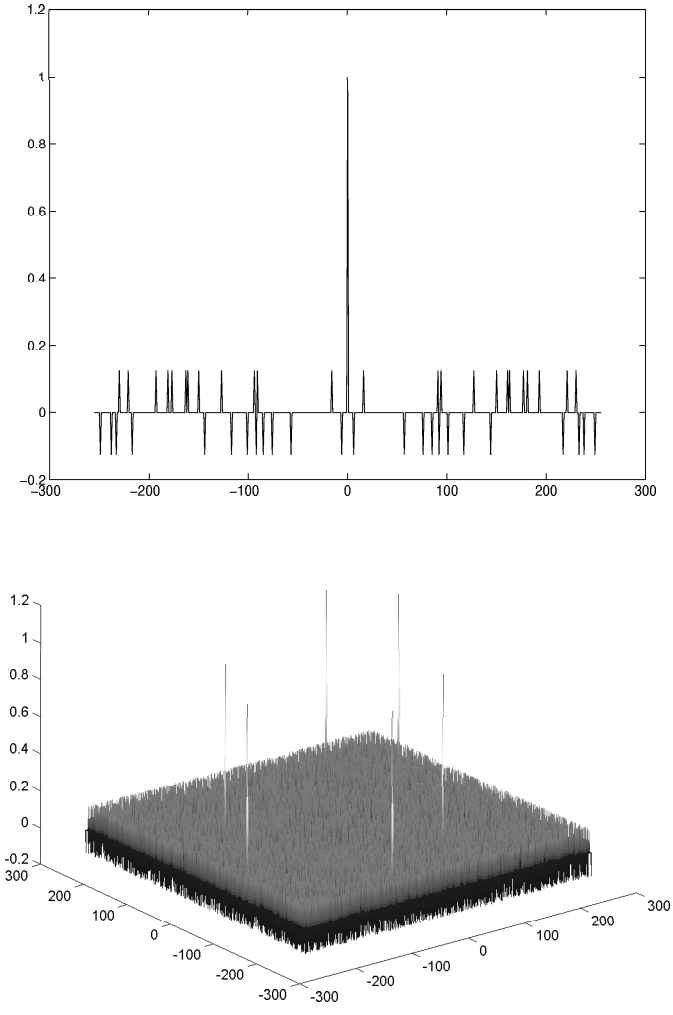
Η παράμετρος e επηρεάζει το μέγεθος των τιμών που λαμβάνει η συνάρτηση ετεροσυσχέτισης των ακολουθιών μεγίστου μήκους x και y. Πιο συγκεκριμένα, έαν ο ακέραιος e είναι μεγάλος, η συνάρτηση ετεροσυσχέτισης λαμβάνει μεγαλύτερες τιμές με μικρότερη συχνότητα. Αντιθέτως, έαν ο ακέραιος e είναι μικρός, η συνάρτηση ετεροσυσχέτισης λαμβάνει μικρότερες τιμές με μεγαλύτερη συχνότητα. Συνεπώς, η τιμή της παραμέτρου e πρέπει να επιλέγεται αναλόγως του πεδίου εφαρμογής.

Στον Πίνακα 6.2 παραθέτουμε τις τιμές που λαμβάνει η συνάρτηση περιοδικής



Σχήμα 6.4. Η αυτοσυσχέτιση και οι ροπές τρίτης τάξης της ακολουθίας $w = x + y$, όπου η y λαμβάνεται από την ακολουθία μεγίστου μήκους x, με ελάχιστο πολυώνυμο $f(z) = 1 + z^4 + z^9$, εφαρμόζοντας δειγματοληψία με παράγοντα 5

ετεροσυσχέτισης, και τη συχνότητα εμφάνισής τους, για $n = 9$ και $n = 15$ αντίστοιχα. Παρατηρούμε ότι έαν $n = 9$, οι δυνατές επιλογές του ακεραίου e είναι 1 και 3, ενώ έαν $n = 15$, είναι 1, 3, και 5. Επιπρόσθετα, παραθέτουμε στα



Σχήμα 6.5. Η αυτοσυσχέτιση και οι ροπές τρίτης τάξης της ακολουθίας $w = x + y$, όπου η y λαμβάνεται από την ακολουθία μεγίστου μήκους x, με ελάχιστο πολυώνυμο $f(z) = 1 + z^4 + z^9$, εφαρμόζοντας δειγματοληψία με παράγοντα 9

Σχ. 6.4 και 6.5 τις συναρτήσεις περιοδικής αυτοσυσχέτισης και τις ροπές τρίτης τάξης ακολουθιών Gold $w = x+y$. Η y λαμβάνεται από την ακολουθία μεγίστου μήκους x εφαρμόζοντας δειγματοληψία με παράγοντα 5 ($k = 2$ και $e = 1$) και 9

($k = 3$ και $e = 3$) αντίστοιχα.

Χρησιμοποιώντας τα Πορίσματα 6.16 και 6.17, και το Θεώρημα 6.19, είναι δυνατό να κατασκευάσουμε ακολουθίες των οποίων η συνάρτηση περιοδικής αυτοσυσχέτισης και οι ροπές ανωτέρας τάξης ελέγχονται πλήρως επιλέγοντας κατάλληλα συγκεκριμένες παραμέτρους. Επιπρόσθετα, εξασφαλίζεται ότι το πλήθος των τοπικών μεγίστων στις ροπές ανωτέρας τάξης μειώνεται δραστικά ή μηδενίζεται. Τέλος, από την σχέση

$$\sum_{j=0}^{N-1} (-1)^{w_j} = N\,\mathrm{CC}_{x,y}(0) = -1$$

συμπεραίνουμε ότι ο τρόπος κατασκευής των ακολουθιών Gold οδηγεί σε ισοβαρείς ακολουθίες.

6.3 Ακολουθίες KRG

Στην παρούσα ενότητα εισάγονται και διερευνούνται οι νέες δυαδικές ακολουθίες KRG [62], [97], οι οποίες παράγονται από την πρόσθεση (modulo 2) δύο δυαδικών ακολουθιών μεγίστου μήκους σχετικά πρώτων ελαχίστων περιόδων. Οι KRG ανήκουν στην κλάση ακολουθιών που παράγονται από μη–γραμμικούς συνδυαστές. Οι βαθμοί των ελαχίστων πολυωνύμων των συνιστωσών ακολουθιών είναι πρώτοι μεταξύ τους και αποδεικνύεται ότι η συνάρτηση ετεροσυσχέτισής τους είναι σταθερή και ίση με $1/N$. Κατά συνέπεια, η συνάρτηση αυτοσυσχέτισης και οι ροπές ανωτέρας τάξης των ακολουθιών KRG λαμβάνουν τιμές από ένα προκαθορισμένο σύνολο τιμών, οι οποίες εμφανίζονται με συγκεκριμένη συχνότητα και σε συγκεκριμένες θέσεις.

Επιπλέον, εξάγεται σαφής έκφραση για την εύρεση του συνόλου τριωνύμων των ακολουθιών KRG. Αποδεικνύεται ότι το πλήθος των τοπικών μεγίστων που εμφανίζονται στις ροπές ανωτέρας τάξης μειώνεται δραστικά ή μηδενίζεται έαν η μία ή και οι δύο εκ των συνιστωσών ακολουθιών αντικατασταθεί από μία ακολουθία Gold. Στη συγκεκριμένη περίπτωση, οι ροπές της παραγόμενης δυαδικής ακολουθίας εξαρτώνται από τις συναρτήσεις ετεροσυσχέτισης των συνιστωσών ακολουθιών των ακολουθιών Gold.

Ας συμβολίσουμε με $w = x + y$ το άθροισμα των ακολουθιών μεγίστου μήκους x και y, με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα, των οποίων

οι βαθμοί $n_1 = \deg(f)$ και $n_2 = \deg(g)$ είναι πρώτοι μεταξύ τους. Τότε, οι ελάχιστες περίοδοι N_1 και N_2, των ακολουθιών x και y αντίστοιχα, είναι πρώτες μεταξύ τους, και συνεπώς η ελάχιστη περίοδος της w είναι ίση με $N = N_1 N_2$. Η συνάρτηση περιοδικής ετεροσυσχέτισης των ακολουθιών x και y παρουσιάζει ενδιαφέρουσες ιδιότητες, όπως αποδεικνύεται στη συνέχεια.

Θεώρημα 6.20. *Η συνάρτηση περιοδικής ετεροσυσχέτισης* $\mathrm{CC}_{x,y}(t)$ *των ακολουθιών μεγίστου μήκους* x *και* y*, όπως ορίστηκαν παραπάνω, είναι ίση με* $1/N$ *για κάθε* $t \in \mathbb{Z}_N$*.*

Απόδειξη. Γνωρίζουμε από τον αλγόριθμο του Ευκλείδη ότι για κάθε ακέραιο $t \in \mathbb{Z}_N$ υπάρχει μοναδικό ζεύγος ακεραίων $(t_1, t_2) \in \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$ τέτοιο ώστε $t = t_1 N_2 + t_2$. Συνεπώς, η συνάρτηση περιοδικής ετεροσυσχέτισης των ακολουθιών μεγίστου μήκους x και y γράφεται ως εξής

$$\begin{aligned}\mathrm{CC}_{x,y}(t) &= \frac{1}{N} \sum_{j_2=0}^{N_2-1} \sum_{j_1=0}^{N_1-1} (-1)^{x_{j_1 N_2 + j_2} + y_{j_1 N_2 + j_2 - t}} \\ &= \frac{1}{N} \sum_{j_2=0}^{N_2-1} (-1)^{y_{j_2 - t}} \sum_{j_1=0}^{N_1-1} (-1)^{x_{j_1 N_2 + j_2}}.\end{aligned}$$

Ας συμβολίσουμε με $\widehat{x}^{j_2}$ την ακολουθία που παράγεται έαν ολισθήσουμε πρώτα την x προς τ΄ αριστερά κατά j_2 χρονικές στιγμές και στη συνέχεια πραγματοποιήσουμε δειγματοληψία με παράγοντα N_2. Επειδή $\gcd(N_1, N_2) = 1$, η δειγματοληψία είναι γνήσια και συνεπώς η $\widehat{x}^{j_2}$ είναι επίσης ακολουθία μεγίστου μήκους της ιδίας ελαχίστης περιόδου. Ως αποτέλεσμα, παίρνουμε τη σχέση

$$\mathrm{CC}_{x,y}(t) = \frac{1}{N} \sum_{j_2=0}^{N_2-1} (-1)^{y_{j_2 - t}} \sum_{j_1=0}^{N_1-1} (-1)^{\widehat{x}^{j_2}_{j_1}}.$$

Για κάθε ακέραιο j_2, το δεύτερο άθροισμα στο δεξιό μέρος της ανωτέρω παράστασης προσθέτει όλα τα στοιχεία της $\{+1, -1\}$ εκδοχής της ακολουθίας $\widehat{x}^{j_2}$, και είναι ίσο με -1 ανεξάρτητα της τιμής του ακεραίου j_2. Τελικά, η συνάρτηση περιοδικής ετεροσυσχέτισης λαμβάνει τη μορφή

$$\mathrm{CC}_{x,y}(t) = -\frac{1}{N} \sum_{j_2=0}^{N_2-1} (-1)^{y_{j_2 - t}} = \frac{1}{N}. \qquad \square$$

Η οικογένεια δυαδικών ακολουθιών KRG είναι μεγάλη σε μέγεθος και χαρακτηρίζεται από πλήθος ιδιοτήτων. Κατ΄ αρχήν, δεν τέθηκε κανένας περιορισμός ως προς τη φύση των συνιστωσών ακολουθιών x και y, και συνεπώς δύναται η χρήση δύο οποιωνδήποτε τυχαίων ακολουθιών μεγίστου μήκους σχετικά πρώτων περιόδων N_1 και N_2. Επιπρόσθετα, η ακολουθία w είναι πάντοτε ισοβαρής και η συνάρτηση περιοδικής αυτοσυσχέτισης λαμβάνει τέσσερις τιμές, όπως αποδεικνύεται στα ακόλουθα Λήμματα.

Λήμμα 6.21. *Οι ακολουθίες KRG είναι ισοβαρείς ακολουθίες.*

Απόδειξη. Έστω $w = x + y$ είναι ακολουθία KRG περιόδου $N = N_1 N_2$. Η ακολουθία w είναι ισοβαρής έαν και μόνον έαν

$$\sum_{j=0}^{N-1} (-1)^{w_j} = \pm 1 \Leftrightarrow N\,\mathrm{CC}_{x,y}(0) = \pm 1.$$

Πράγματι, από το Θεώρημα 6.20 λαμβάνουμε $N\,\mathrm{CC}_{x,y}(0) = 1$, το οποίο οδηγεί στο συμπέρασμα ότι το πλήθος των άσσων και των μηδενικών στο διάνυσμα $\boldsymbol{w}$ είναι $(N-1)/2$ και $(N+1)/2$ αντίστοιχα. □

Λήμμα 6.22. *Το φάσμα της συνάρτησης περιοδικής αυτοσυσχέτισης της KRG ακολουθίας $w = x + y$, λαμβάνει τέσσερις τιμές και δίνεται από τη σχέση*

$$\mathrm{AC}_w(t) = \begin{cases} 1 & \text{έαν } t \equiv 0 \pmod{N}, \\ -1/N_1 & \text{έαν } t \equiv 0 \pmod{N_2}, \\ -1/N_2 & \text{έαν } t \equiv 0 \pmod{N_1}, \\ 1/N & \text{διαφορετικά.} \end{cases}$$

Το πλήθος εμφανίσεων των ανωτέρω τιμών σε μία περίοδο της ακολουθίας w είναι 1, $N_1 - 1$, $N_2 - 1$, *και* $N - N_1 - N_2 + 1$ *αντίστοιχα.*

Απόδειξη. Η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας w δίνεται από τη σχέση

$$\mathrm{AC}_w(t) = \frac{1}{N} \sum_{j=0}^{N-1} (-1)^{(x_j + x_{j-t}) + (y_j + y_{j-t})}.$$

Προφανώς, έαν ο ακέραιος t είναι ίσος με το μηδέν, η συνάρτηση αυτοσυσχέτισης λαμβάνει την τιμή 1. Έαν ο ακέραιος t είναι πολλαπλάσιο του N_2, δηλ. $t = kN_2$

με $k = 1, \ldots, N_1 - 1$, τότε η συνάρτηση αυτοσυσχέτισης γράφεται ως εξής

$$\mathrm{AC}_w(t) = \frac{1}{N} \sum_{j=0}^{N-1} (-1)^{x_j + x_{j-t}} = \frac{1}{N}(-N_2) = -\frac{1}{N_1}$$

αφού το διάνυσμα $\boldsymbol{x}$ επαναλαμβάνεται N_2 φορές εντός του $\boldsymbol{w}$. Όμοια αποτελέσματα λαμβάνουμε και στην περίπτωση όπου ο ακέραιος t είναι πολλαπλάσιο του N_1. Τέλος, σε κάθε άλλη περίπτωση η συνάρτηση περιοδικής αυτοσυσχέτισης θα δίνεται από τη σχέση

$$\mathrm{AC}_w(t) = \frac{1}{N} \sum_{j=0}^{N-1} (-1)^{x_{j-t_1} + y_{j-t_2}} = \mathrm{CC}_{x,y}(t_2 - t_1)$$

όπου

$$x_j + x_{j-t} = x_{j-t_1} \qquad \text{και} \qquad y_j + y_{j-t} = y_{j-t_2}$$

λόγω της Ιδιότητας 3.9 των ακολουθιών μεγίστου μήκους. Η ισχύς της υπόθεσης επιβεβαιώνεται από το Θεώρημα 6.20. □

Σημείωση 6.23. Ο συμβολισμός $t \equiv 0 \pmod{N_i}$ του Λήμματος 6.22 δηλώνει ότι ο ακέραιος t είναι μη–μηδενικό πολλαπλάσιο του N_i αλλά όχι και του N. Ο συμβολισμός αυτός χρησιμοποιείται και στο υπόλοιπο της παρούσας ενότητας.

Από το Λήμμα 6.22 συμπεραίνουμε ότι οι τιμές της συνάρτησης αυτοσυσχέτισης των ακολουθιών KRG διακρίνονται από τη συγκεκριμένη συχνότητα εμφάνισης στο διάνυσμα $\boldsymbol{w}$ και τη σταθερότητα των σημείων στα οποία λαμβάνονται οι τιμές αυτές. Πιο συγκεκριμένα, τα σημεία αυτά καθορίζονται πλήρως από τις ελάχιστες περιόδους των συνιστωσών ακολουθιών μεγίστου μήκους.

Παρόμοια αποτελέσματα ισχύουν και στην περίπτωση των ροπών τρίτης ή υψηλότερης τάξης της ακολουθίας w, τα οποία δίνονται από το Θεώρημα 6.14 αντικαθιστώντας τη συνάρτηση ετεροσυσχέτισης $\mathrm{CC}_{x,y}$ με το $1/N$. Οι συγκεκριμένες θέσεις όπου εμφανίζονται τοπικά μέγιστα στις ροπές ανωτέρας τάξης των ακολουθιών KRG καθορίζονται εκ΄ των προτέρων βάσει των περιόδων των συνιστωσών ακολουθιών.

Τα τριώνυμα των ακολουθιών KRG είναι δυνατό να υπολογιστούν μέσω του Λήμματος 6.13 και του Θεωρήματος 6.11. Το ακόλουθο Θεώρημα παρέχει σαφείς εκφράσεις υπολογισμού των τριωνύμων της KRG ακολουθίας w βάσει των τριωνύμων των συνιστωσών ακολουθιών μεγίστου μήκους x και y αντίστοιχα.

Θεώρημα 6.24. *Έστω x και y είναι ακολουθίες μεγίστου μήκους, σχετικά πρώτων ελαχίστων περιόδων N_1 και N_2, με ελάχιστα πολυώνυμα $f(z)$ και $g(z)$ αντίστοιχα. Τότε, το σύνολο τριωνύμων T_{fg} της KRG ακολουθίας $w = x + y$, ελαχίστης περιόδου $N = N_1 N_2$, δίνεται από*

$$T_{fg} = \Big\{(t_1^w, t_2^w) \in \mathbb{Z}_N^2 :\ t_i^w = t_i^x N_2^{\varphi(N_1)} + t_i^y N_1^{\varphi(N_2)} \bmod N,$$
$$i = 1, 2,\ \text{όπου } (t_1^x, t_2^x) \in T_f \text{ και } (t_1^y, t_2^y) \in T_g\Big\}.$$

Επιπρόσθετα ισχύει $|T_{fg}| = |T_f||T_g|$.

Απόδειξη. Ας θεωρήσουμε τα τυχαία τριώνυμα $(t_1^x, t_2^x) \in T_f$ και $(t_1^y, t_2^y) \in T_g$ των ακολουθιών μεγίστου μήκους x και y αντίστοιχα.

Έαν υπάρχει ζεύγος ακεραίων $(t_1^w, t_2^w) \in \mathbb{Z}_N^2$ το οποίο να αντιστοιχεί σε τριώνυμο της ακολουθίας w και να προκύπτει από τα τριώνυμα των ακολουθιών x και y σύμφωνα με το Θεώρημα 6.11 και Λήμμα 6.13, τότε θα ικανοποιεί τις ακόλουθες εξισώσεις

$$\begin{aligned} t_1^w &\equiv t_1^x \pmod{N_1} \quad \text{και} \quad t_2^w \equiv t_2^x \pmod{N_1}, \\ t_1^w &\equiv t_1^y \pmod{N_2} \quad \text{και} \quad t_2^w \equiv t_2^y \pmod{N_2}. \end{aligned}$$

Οι ακέραιοι N_1, N_2 είναι πρώτοι μεταξύ τους, και σύμφωνα με το *Θεώρημα Υπολοίπων του Κινέζου* [50], [72], οι ανωτέρω εξισώσεις παραδέχονται τις ακόλουθες μοναδικές λύσεις t_1^w και t_2^w στο σύνολο $\mathbb{Z}_N$

$$t_1^w = t_1^x N_2^{\varphi(N_1)} + t_1^y N_1^{\varphi(N_2)} \bmod N, \tag{6.6α′}$$
$$t_2^w = t_2^x N_2^{\varphi(N_1)} + t_2^y N_1^{\varphi(N_2)} \bmod N. \tag{6.6β′}$$

Αντιστρόφως, δοθέντος του τριωνύμου $(t_1^w, t_2^w) \in T_{fg}$, είναι δυνατό να υπολογίσουμε τα αντίστοιχα τριώνυμα των συνόλων T_f και T_g από

$$(t_1^x, t_2^x) = (t_1^w \bmod N_1, t_2^w \bmod N_1) \in T_f$$
$$(t_1^y, t_2^y) = (t_1^w \bmod N_2, t_2^w \bmod N_2) \in T_g$$

βάσει του Θεωρήματος 6.11 και του Λήμματος 6.13.

Επειδή οι ακέραιοι N_1 και N_2 είναι πρώτοι μεταξύ τους, οι εξισώσεις (6.6α′) και (6.6β′) αποτελούν *πλήρη συστήματα υπολοίπων* [72], και συνεπώς το ζεύγος ακεραίων (t_i^x, t_i^y) αντιστοιχίζεται με μοναδικό τρόπο στον t_i^w και αντιστρόφως.

Επιπρόσθετα, οι ακέραιοι t_i^x και t_i^y διατρέχουν όλα τα μη–μηδενικά στοιχεία των συνόλων $\mathbb{Z}_{N_1}$ και $\mathbb{Z}_{N_2}$ αντίστοιχα ακριβώς μία φορά, αφού οι x και y είναι ακολουθίες μεγίστου μήκους.

Συνεπώς, ο ακέραιος t_i^w δε δύναται να είναι μηδέν ή πολλαπλάσιο των N_1, N_2, και λαμβάνει $(N_1-1)(N_2-1)$ διακριτές τιμές ακριβώς από μία φορά. Αυτός είναι και ο αριθμός $N-1-(N_1-1)-(N_2-1)$ των στοιχείων του συνόλου $\mathbb{Z}_N$ τα οποία δεν είναι μηδέν ή πολλαπλάσιο των N_i, αποδεικνύοντας ότι η τάξη του T_{fg} είναι ίση με το γινόμενο των τάξεων των συνόλων T_f και T_g. □

Πόρισμα 6.25. *Η KRG ακολουθία w έχει τριώνυμα στο σύνολο $\mathbb{Z}^2_{\min\{N_1,N_2\}}$ έαν και μόνον έαν οι συνιστώσες ακολουθίες x και y έχουν κοινά τριώνυμα εντός του συνόλου.*

Απόδειξη. Δίχως βλάβη της γενικότητας υποθέτουμε ότι $N_1 < N_2$. Το ζεύγος ακεραίων $(t_1,t_2) \in \mathbb{Z}^2_{N_1}$ είναι κοινό τριώνυμο των ακολουθιών x και y, έαν και μόνον έαν

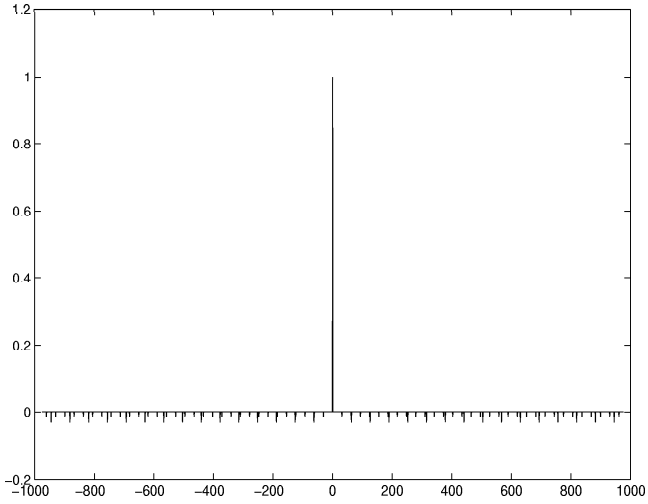
$$\left.\begin{aligned} x &= D^{t_1}x + D^{t_2}x \\ y &= D^{t_1}y + D^{t_2}y \end{aligned}\right\} \Leftrightarrow (x+y) = D^{t_1}(x+y) + D^{t_2}(x+y)$$
$$\Leftrightarrow w = D^{t_1}w + D^{t_2}w$$

δηλ. το $(t_1,t_2) \in \mathbb{Z}^2_{N_1}$ είναι τριώνυμο της ακολουθίας w. □

Έαν υποθέσουμε ότι $N_1 < N_2$ και επιπρόσθετα ότι τα ζεύγη ακεραίων (t_1+N_1,t_2), (t_1,t_2+N_1), και (t_1+N_1,t_2+N_1) δεν αποτελούν τριώνυμα της y, τότε η ακολουθία w δεν έχει τριώνυμα εντός του συνόλου $\mathbb{Z}^2_{\max\{N_1,N_2\}}$. Συνήθως, το αποτέλεσμα αυτό ισχύει στην πράξη και συνεπώς τα τριώνυμα της ακολουθίας w είναι αρκετά απομακρυσμένα από την αρχή των αξόνων.

Επειδή η προαναφερθείσα ιδιότητα γενικεύεται εύκολα σε πολυώνυμα της ακολουθίας w, συμπεραίνουμε ότι οι ακολουθίες KRG είναι σχεδόν ιδανικές για την προσομοίωση σημάτων λευκού θορύβου ανωτέρας τάξης σε προβλήματα ταυτοποίησης όπου τοπικά μέγιστα απομακρυσμένα από την αρχή των αξόνων δεν επηρεάζουν τη διαδικασία ταυτοποίησης. Το συμπέρασμα αυτό επιβεβαιώνεται από τα συγκριτικά πειραματικά αποτελέσματα, μεταξύ ακολουθιών KRG και μεγίστου μήκους, της επόμενης ενότητας.

Παράδειγμα 6.26. Ας θεωρήσουμε τη συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας $w = x + y$, όπου οι συνιστώσες ακολουθίες μεγίστου μήκους x



Σχήμα 6.6. Η αυτοσυσχέτιση της ακολουθίας $w = x + y$, όπου x και y έχουν ελάχιστα πολυώνυμα $f(z) = 1 + z^2 + z^5$ και $g(z) = 1 + z + z^6$ αντίστοιχα

και y, περιόδου 31 και 63, έχουν ελάχιστα πολυώνυμα

$$f(z) = 1 + z^2 + z^5 \qquad \text{και} \qquad g(z) = 1 + z + z^6$$

αντίστοιχα. Η ελάχιστη περίοδος της ακολουθίας w είναι 1953, ενώ οι εκτός–φάσης τιμές που λαμβάνει η συνάρτηση περιοδικής αυτοσυσχέτισης είναι οι εξής

$$\begin{aligned} 0.0005, &\quad \text{εμφανίζεται 1860 φορές,} \\ -0.0159, &\quad \text{εμφανίζεται 62 φορές, και} \\ -0.0323, &\quad \text{εμφανίζεται 30 φορές} \end{aligned}$$

όπως φαίνεται στο Σχ. 6.6. □

Η ίδια συνάρτηση περιοδικής αυτοσυσχέτισης λαμβάνεται για κάθε πιθανή επιλογή συνιστωσών ακολουθιών μεγίστου μήκους ιδίων ελαχίστων περιόδων N_1 και N_2, αφού οι τιμές και οι θέσεις του εκτός–φάσης φάσματος εξαρτώνται μόνον από τις περιόδους N_1 και N_2 [65], [110]. Χρησιμοποιώντας συνιστώσες ακολουθίες μεγίστου μήκους διαφορετικών περιόδων, κρατώντας κατά προσέγγιση σταθερή

την περίοδο της παραγόμενης ακολουθίας KRG, είναι δυνατό να ορίσουμε το επιθυμητό μέγεθος και συχνότητα εμφάνισης των τιμών της συνάρτησης περιοδικής αυτοσυσχέτισης.

Παράδειγμα 6.27. Ας θεωρήσουμε τη συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας $w = x + y$, όπου οι συνιστώσες ακολουθίες μεγίστου μήκους x και y, περιόδου 15 και 127, έχουν ελάχιστα πολυώνυμα

$$f(z) = 1 + z + z^4 \quad \text{και} \quad g(z) = 1 + z^3 + z^7$$

αντίστοιχα. Η ελάχιστη περίοδος της ακολουθίας w είναι 1905, ενώ οι εκτός–φάσης τιμές που λαμβάνει η συνάρτηση περιοδικής αυτοσυσχέτισης είναι οι εξής

$$\begin{aligned} 0.0005, &\quad \text{εμφανίζεται 1764 φορές,} \\ -0.0079, &\quad \text{εμφανίζεται 126 φορές, και} \\ -0.0667, &\quad \text{εμφανίζεται 14 φορές} \end{aligned}$$

αντί αυτών του προηγούμενου παραδείγματος. □

Το πλεονέκτημα επιλογής των ανωτέρω ελαχίστων πολυωνύμων είναι ότι η μέγιστη κατ΄ απόλυτη τιμή της συνάρτησης περιοδικής αυτοσυσχέτισης εμφανίζεται λιγότερες φορές έχοντας όμως μεγαλύτερο μέγεθος. Επειδή στην κατασκευή ψευδο–τυχαίων ακολουθιών μας ενδιαφέρει και η γραμμική τους πολυπλοκότητα, παραθέτουμε το ακόλουθο Λήμμα [97].

Λήμμα 6.28. *Η γραμμική πολυπλοκότητα της KRG ακολουθίας w είναι ίση με το άθροισμα των γραμμικών πολυπλοκοτήτων των συνιστωσών ακολουθιών x και y.*

Απόδειξη. Εφαρμόζοντας το διακριτό μετασχηματισμό Fourier, οι ακολουθίες x και y γράφονται στην ακόλουθη μορφή

$$x_j = \sum_{i=0}^{N_1-1} X_i \alpha^{ji} \quad \text{και} \quad y_j = \sum_{i=0}^{N_2-1} Y_i \beta^{ji}$$

όπου α και β είναι πρωταρχικά στοιχεία των πεπερασμένων σωμάτων $\mathbb{F}_{2^{n_1}}$ και $\mathbb{F}_{2^{n_2}}$ αντίστοιχα. Η γραμμική πολυπλοκότητα των ακολουθιών x και y είναι ίση με

το πλήθος των μη–μηδενικών συντελεστών X_i και Y_i της ανωτέρω παράστασης [56]. Συνεπώς, η ακολουθία w γράφεται ως εξής

$$w_j = x_j + y_j = \sum_{i=0}^{N_1-1} X_i \alpha^{ji} + \sum_{i=0}^{N_2-1} Y_i \beta^{ji}.$$

Επειδή $\gcd(N_1, N_2) = 1$, το Λήμμα 2.53 δίνει ότι $\gcd(n_1, n_2) = 1$, δηλ. τα στοιχεία α και β ανήκουν σε πεπερασμένα σώματα των οποίων η τομή είναι το πρωταρχικό σώμα $\mathbb{F}_2$. Κατά συνέπεια, κανένας συντελεστής του αθροίσματος δεν απαλοίφεται, και η γραμμική πολυπλοκότητα L_w της ακολουθίας w είναι ίση με $L_x + L_y$ [72]. □

6.3.1 Σύνθετες ακολουθίες KRG

Στη συνέχεια εξετάζουμε την περίπτωση αντικατάστασης μίας εκ' των δύο συνιστωσών ακολουθιών μεγίστου μήκους από μία ακολουθία Gold. Οι παραγόμενες ακολουθίες ονομάζονται *σύνθετες ακολουθίες KRG*.

Δίχως βλάβη της γενικότητας, υποθέτουμε ότι η ακολουθία y γράφεται ως άθροισμα των ακολουθιών μεγίστου μήκους y^1 και y^2, ελαχίστης περιόδου N_2, με ελάχιστα πολυώνυμα $g_1(z)$ και $g_2(z)$ αντίστοιχα που ικανοποιούν τις υποθέσεις του Θεωρήματος 6.19. Είναι δυνατό να αποδείξουμε, με τρόπο παρόμοιο με αυτόν του Θεωρήματος 6.20, ότι

$$\mathrm{CC}_{x,y}(t) = -\frac{1}{N_1} \mathrm{CC}_{y^1,y^2}(0) \tag{6.7}$$

για κάθε $t \in \mathbb{Z}_N$. Συνεπώς, η συνάρτηση περιοδικής ετεροσυσχέτισης των ακολουθιών x και y είναι σταθερή, και η τιμή της είναι ίση με $1/N$ έαν και μόνον έαν η y είναι ισοβαρής. Στη συγκεκριμένη περίπτωση, δεν εφαρμόζονται το Θεώρημα 6.14 και το Λήμμα 6.22 αφού η y δεν είναι πλέον ακολουθία μεγίστου μήκους. Η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας $w = x + y$ δίνεται από το ακόλουθο Λήμμα.

Λήμμα 6.29. *Έστω x και y είναι ακολουθίες μεγίστου μήκους και Gold αντίστοιχα, σχετικά πρώτων ελαχίστων περιόδων N_1 και N_2, με ελάχιστα πολυώνυμα $f(z)$ και $g(z) = g_1(z)g_2(z)$ αντίστοιχα. Τότε, η συνάρτηση περιοδικής αυτο-*

συσχέτισης της ακολουθίας $w = x + y$ *δίνεται από τη σχέση*

$$\mathrm{AC}_w(t) = \begin{cases} 1 & \text{εάν } t \equiv 0 \pmod{N}, \\ -1/N_1 & \text{εάν } t \equiv 0 \pmod{N_2}, \\ \mathrm{CC}_{y^1,y^2}(t') & \text{εάν } t \equiv 0 \pmod{N_1}, \\ -\frac{1}{N_1}\,\mathrm{CC}_{y^1,y^2}(t') & \text{διαφορετικά}, \end{cases}$$

όπου $t' \in \mathbb{Z}_{N_2}$.

Απόδειξη. Η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας w δίνεται από τη σχέση

$$\mathrm{AC}_w(t) = \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{(x_j+x_{j-t})+(y_j+y_{j-t})}.$$

Οι δύο πρώτες περιπτώσεις αποδεικνύονται όπως στο Λήμμα 6.22. Αν ο ακέραιος t είναι πολλαπλάσιο του N_1, δηλ. $t = kN_1$ με $k = 1, \ldots, N_2-1$, τότε η συνάρτηση αυτοσυσχέτισης γράφεται ως εξής

$$\mathrm{AC}_w(t) = \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{y_j+y_{j-t}} = \frac{1}{N_2}\sum_{j=0}^{N_2-1}(-1)^{y_j+y_{j-t}} = \mathrm{AC}_y(t).$$

Από το Πόρισμα 6.17, συμπεραίνουμε ότι στη συγκεκριμένη περίπτωση ισχύει $\mathrm{AC}_w(t) = \mathrm{CC}_{y^1,y^2}(t')$. Τέλος, σε κάθε άλλη περίπτωση η συνάρτηση περιοδικής αυτοσυσχέτισης θα δίνεται από τη σχέση

$$\begin{aligned}\mathrm{AC}_w(t) &= \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{(x_j+x_{j-t})+(y^1_j+y^1_{j-t})+(y^2_j+y^2_{j-t})} \\ &= \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{x_{j-t_1}+(y^1_{j-t_2}+y^2_{j-t_3})}\end{aligned}$$

όπου, λόγω της Ιδιότητας 3.9 των ακολουθιών μεγίστου μήκους, έχουμε

$$x_j + x_{j-t} = x_{j-t_1}, \qquad y^1_j + y^1_{j-t} = y^1_{j-t_2}, \qquad \text{και} \qquad y^2_j + y^2_{j-t} = y^2_{j-t_3}$$

με $t_1 \in \mathbb{Z}_{N_1}$ και $t_2, t_3 \in \mathbb{Z}_{N_2}$. Η ισχύς της υπόθεσης επιβεβαιώνεται από το Θεώρημα 6.20. □

Σύμφωνα με το Θεώρημα 6.19, η συνάρτηση ετεροσυσχέτισης των ακολουθιών y^1 και y^2 λαμβάνει τρεις τιμές, με αποτέλεσμα η συνάρτηση περιοδικής αυτοσυσχέτισης της ακολουθίας w λαμβάνει οκτώ τιμές. Το μέγεθος των τιμών εξαρτάται από τις ελάχιστες περιόδους των συνιστωσών ακολουθιών και την τιμή της παραμέτρου e του Θεωρήματος 6.19.

Οι ροπές τρίτης (και ανωτέρας) τάξης της σύνθετης KRG ακολουθίας w υπολογίζονται από το ακόλουθο θεώρημα, η απόδειξη του οποίου βασίζεται στα Θεωρήματα 6.14 και 6.20, και επιπλέον στο Πόρισμα 6.16 και Λήμμα 6.29.

Θεώρημα 6.30. *Οι ροπές τρίτης τάξης της ακολουθίας $w = x + y$, όπου x και y είναι ακολουθίες μεγίστου μήκους και Gold αντίστοιχα, δίνεται από τη σχέση*

$$\mathrm{AC}_w(t_1,t_2) = \begin{cases} 1 & \text{έαν } (t_1,t_2) \in T'_f \cap T'_g, \\ -1/N_1 & \text{έαν } (t_1,t_2) \in T'_g \setminus T'_f, \\ -1/N_2 & \text{έαν } (t_1,t_2) \in T'_f \cap ((T'_{g_1} \cup T'_{g_2}) \setminus T'_g), \\ 1/N & \text{έαν } (t_1,t_2) \in (T'_{g_1} \cup T'_{g_2}) \setminus (T'_f \cup T'_g), \\ \mathrm{CC}_{y^1,y^2}(l) & \text{έαν } (l_1,l_2) \in T'_f \setminus (T'_{g_1} \cup T'_{g_2}), \\ -\frac{1}{N_1}\mathrm{CC}_{y^1,y^2}(t) & \text{διαφορετικά}, \end{cases}$$

όπου $t \in \mathbb{Z}_{N_2}$.

Το σύνολο των τριωνύμων της ακολουθίας w είναι ίσο με $T_{fg} = T'_f \cap T'_g = T'_f \cap T'_{g_1} \cap T'_{g_2}$. Οι ακολουθίες Gold έχουν ελάχιστο πλήθος τοπικών μεγίστων στις ροπές ανωτέρας τάξης, και συνεπώς το πλήθος τοπικών μεγίστων που παρουσιάζονται στις ροπές ανωτέρας τάξης της σύνθετης KRG ακολουθίας w μειώνεται δραστικά ή μηδενίζεται.

Η τελευταία περίπτωση επιτυγχάνεται και με την ειδική κλάση των δυϊκών BCH ακολουθιών διόρθωσης δύο σφαλμάτων, όταν ο βαθμός του πολυωνύμου g_1 είναι περιττός ακέραιος. Τότε, τα σύνολα τριωνύμων T_g και T'_g είναι κενά, και συνεπώς οι ροπές τρίτης τάξης της σύνθετης KRG ακολουθίας w δίνονται από το Θεώρημα 6.30 αφαιρώντας την πρώτη και δεύτερη περίπτωση. Παρόμοια αποτελέσματα λαμβάνουμε έαν η x είναι επίσης ακολουθία Gold.

6.4 Πειραματικά αποτελέσματα

Στην παρούσα ενότητα επιδεικνύουμε την ποιότητα και αποτελεσματικότητα των προτεινόμενων δυαδικών ακολουθιών στην προσομοίωση σημάτων λευκού θορύβου ανωτέρας τάξης, παρέχοντας συγκριτικά αποτελέσματα πειραμάτων προσομοίωσης, έναντι των ακολουθιών μεγίστου μήκους, για την ταυτοποίηση δύο διγραμμικών μοντέλων εισόδου–εξόδου. Στα πειράματα προσομοίωσης χρησιμοποιούμε τον αλγόριθμο αθροιστικών που αναπτύχθηκε στην [119].

Ειδικότερα, θα ασχοληθούμε με την ταυτοποίηση δύο διακριτών άνω τριγωνικών διγραμμικών μοντέλων εισόδου–εξόδου της μορφής

$$y(n) = z(n) + \eta(n) \tag{6.8}$$

και

$$z(n) = \sum_{i=1}^{k_1} a_i z(n-i) + \sum_{i=1}^{k_2} \sum_{j=i}^{k_3} c_{ij} z(n-i)u(n-j) + \sum_{i=0}^{k_4} b_i u(n-i) \tag{6.9}$$

όπου $y(n)$ είναι η μετρούμενη έξοδος του μοντέλου, ενώ η είσοδος $u(n)$ είναι λευκός θόρυβος ανωτέρας τάξης. Για το θόρυβο μέτρησης $\eta(n)$, επειδή εξ΄ υποθέσεως είναι στοχαστική διαδικασία μηδενικής μέσης τιμής ανεξάρτητη της εισόδου, χρησιμοποιήθηκε σε σε όλα τα πειράματα προσομοίωσης μία Gaussian IID στοχαστική διαδικασία.

Η σειρά Volterra που αντιστοιχεί στο παραπάνω διγραμμικό μοντέλο είναι άπειρη. Πιο συγκεκριμένα, η (6.8) είναι δυνατό να γραφεί ως εξής

$$\begin{aligned} y(n) = &\sum_{k_1=0}^{\infty} h_1(k_1)u(n-k_1) + \sum_{k_1,k_2=1}^{\infty} h_2(k_1,k_2)u(n-k_1)u(n-k_2) \\ &+ \sum_{k_1,k_2,k_3=2}^{\infty} h_3(k_1,k_2,k_3)u(n-k_1)u(n-k_2)u(n-k_3) + \cdots + \eta(n) \end{aligned} \tag{6.10}$$

όπου h_m παριστάνει τον πυρήνα Volterra τάξης m. Έαν $p_1, p_2, \ldots, p_{k_1}$ είναι οι ρίζες του πολυωνύμου

$$z^{k_1}\left(1 - \sum_{i=1}^{k_1} a_i z^{-i}\right) \tag{6.11}$$

τότε προϋπόθεση για τη στατικότητα του $z(n)$ είναι όλες οι ρίζες p_i να βρίσκονται εντός του μοναδιαίου κύκλου.

Πίνακας 6.3. Συγκριτικά αποτελέσματα ακολουθιών μεγίστου μήκους με τις ακολουθίες Gold για 40 επαναλήψεις, 20dB SNR, και με περίοδο 4095

πραγμ. μοντέλο		μεγίστου μήκους		Gold	
παράμετροι	τιμή	μέση τιμή	διακύμανση	μέση τιμή	διακύμανση
a_1	1.40	1.7551	5.32	1.3965	6.78×10^{-1}
a_2	-0.48	-3.7441	$3.43 \times 10^{+2}$	-0.5984	7.93
b_0	1.00	0.9785	1.00×10^{-4}	1.0104	2.00×10^{-4}
b_1	0.50	0.1752	5.14	0.4450	7.18×10^{-1}
c_{11}	0.05	0.0288	2.00×10^{-4}	0.1128	2.00×10^{-4}
c_{12}	0.10	0.1026	2.40×10^{-3}	0.1147	1.70×10^{-3}
c_{22}	0.20	0.1903	1.20×10^{-2}	0.1527	6.40×10^{-3}

Επιπλέον, οι πυρήνες Volterra είναι πολυωνυμικές συναρτήσεις των παραμέτρων a_i, b_i, και c_{ij} του διγραμμικού μοντέλου και εξαρτώνται εκθετικά από κάθε p_i, όπως στην περίπτωση των γραμμικών μοντέλων ARMA. Κατά συνέπεια, το εύρος στο πεδίο του χρόνου για το οποίο κάθε πυρήνας Volterra παραμένει πρακτικά μη–μηδενικός εξαρτάται κυρίως από την ακριβή θέση των p_i εντός του μοναδιαίου κύκλου. Όσο πιο κοντά στο μοναδιαίο κύκλο βρίσκονται τα p_i, τόσο μεγαλύτερο είναι το εύρος στο πεδίο του χρόνου για το οποίο κάθε πυρήνας Volterra είναι πρακτικά μη–μηδενικός.

Προφανώς, σε αυτήν την περίπτωση οι ετεροαθροιστικές της εξόδου $y(n)$ με την είσοδο $u(n)$ που χρησιμοποιούνται στον αλγόριθμο ταυτοποίησης στην [119], επηρεάζονται από τοπικά μέγιστα στις ροπές ή αθροιστικές ανωτέρας τάξης του $u(n)$. Παρόμοια συμπεριφορά παρατηρείται ακόμα κι αν τα συγκεκριμένα τοπικά μέγιστα εμφανίζονται σε υψηλές χρονικές τιμές, όπως είναι δυνατό να συμπεραίνουμε από την (6.10). Αυτό φαίνεται καθαρά στα επόμενα δύο παραδείγματα, όπου από όλες τις ακολουθίες μεγίστου μήκους ιδίας περιόδου χρησιμοποιήθηκαν εκείνες των οποίων η Ευκλείδεια απόσταση του πλησιέστερου στην αρχή των αξόνων ζεύγους ακεραίων (a, b), που αντιστοιχεί σε τριώνυμο $1 + z^a + z^b$ της ακολουθίας, ήταν η μεγαλύτερη δυνατή. Οι συγκεκριμένες ακολουθίες μεγίστου μήκους είναι οι *βέλτιστες* για χρήση σε πειράματα ταυτοποίησης.

Παράδειγμα 6.31. Ας θεωρήσουμε το διγραμμικό μοντέλο της (6.9), με παραμέτρους $k_1 = k_2 = k_3 = 2$ και $k_4 = 1$, του οποίου οι ρίζες του πολυωνύμου (6.11) είναι ίσες με 0.6 και 0.8 αντίστοιχα. Τα πειραματικά αποτελέσματα παρουσιάζονται στον Πίνακα 6.3 συγκρίνοντας τις βέλτιστες ακολουθίες μεγίστου μήκους,

Πίνακας 6.4. Συγκριτικά αποτελέσματα ακολουθιών μεγίστου μήκους με τις ακολουθίες KRG για 40 επαναλήψεις, 20dB SNR, και με περίοδο 8191 και 7905 αντίστοιχα

πραγμ. μοντέλο		μεγίστου μήκους		KRG	
παράμετροι	τιμή	μέση τιμή	διακύμανση	μέση τιμή	διακύμανση
a_1	1.30	1.5647	8.01×10^{-1}	1.2362	2.10×10^{-1}
a_2	-0.36	-1.7143	$1.20 \times 10^{+1}$	-0.2963	7.14×10^{-1}
b_0	1.00	0.9840	1.00×10^{-4}	0.9970	1.00×10^{-4}
b_1	0.50	0.2584	7.84×10^{-1}	0.5745	2.16×10^{-1}
c_{11}	0.05	0.0250	6.00×10^{-4}	0.0177	8.00×10^{-4}
c_{12}	0.10	0.1279	4.20×10^{-3}	0.1278	8.40×10^{-3}
c_{13}	0.20	0.2189	5.90×10^{-3}	0.2636	7.20×10^{-3}
c_{22}	-0.15	-0.1894	4.50×10^{-3}	-0.1765	5.00×10^{-3}
c_{23}	0.07	0.0015	2.79×10^{-2}	-0.0156	3.92×10^{-2}
c_{33}	0.30	0.4323	4.54×10^{-2}	0.3331	1.76×10^{-2}

περιόδου 4095, με τις ακολουθίες Gold, ιδίας περιόδου, με παραμέτρους $e = 4$, $k = 8$, και $d = 2^{2k} - 2^k + 1 = 3856$, από το Θεώρημα 6.19.

Παρατηρούμε ότι οι περισσότερες από τις εκτιμήσεις των παραμέτρων, κυρίως του a_2, που λαμβάνονται με ακολουθίες μεγίστου μήκους δεν είναι αμερόληπτες, σε αντίθεση με τις εκτιμήσεις που λαμβάνονται από τις ακολουθίες Gold. Επιπλέον, οι διακυμάνσεις των εκτιμήσεων στην πρώτη περίπτωση είναι κατά πολύ μεγαλύτερες από τις αντίστοιχες που λαμβάνονται στη δεύτερη. □

Παράδειγμα 6.32. Ας θεωρήσουμε το διγραμμικό μοντέλο της (6.9), με παραμέτρους $k_1 = 2$, $k_2 = k_3 = 3$, και $k_4 = 1$, του οποίου οι ρίζες του πολυωνύμου (6.11) είναι ίσες με 0.4 και 0.9 αντίστοιχα. Τα πειραματικά αποτελέσματα παρουσιάζονται στους Πίνακες 6.4 και 6.5 συγκρίνοντας τις βέλτιστες ακολουθίες μεγίστου μήκους, περιόδων 8191 και 16383 αντίστοιχα, με τις ακολουθίες KRG, περιόδων 7905 και 15841 αντίστοιχα. Στην πρώτη περίπτωση οι συνιστώσες ακολουθίες της ακολουθίας KRG είχαν περιόδους 31 και 255, ενώ στη δεύτερη περίπτωση 31 και 511.

Παρατηρούμε ότι οι περισσότερες από τις εκτιμήσεις των παραμέτρων, κυρίως του a_2, που λαμβάνονται με ακολουθίες μεγίστου μήκους δεν είναι αμερόληπτες, σε αντίθεση με τις εκτιμήσεις που λαμβάνονται από τις ακολουθίες KRG. Επιπλέον, οι διακυμάνσεις των εκτιμήσεων στην πρώτη περίπτωση είναι κατά πολύ μεγαλύτερες από τις αντίστοιχες που λαμβάνονται στη δεύτερη. □

Πίνακας 6.5. Συγκριτικά αποτελέσματα ακολουθιών μεγίστου μήκους με τις ακολουθίες KRG για 40 επαναλήψεις, 20dB SNR, και με περίοδο 16383 και 15841 αντίστοιχα

πραγμ. μοντέλο		μεγίστου μήκους		KRG	
παράμετροι	τιμή	μέση τιμή	διακύμανση	μέση τιμή	διακύμανση
a_1	1.30	1.3953	5.14×10^{-1}	1.2969	1.35×10^{-1}
a_2	-0.36	-1.0572	6.80	-0.4261	8.09×10^{-1}
b_0	1.00	0.9975	1.86×10^{-5}	0.9983	2.31×10^{-5}
b_1	0.50	0.4091	5.21×10^{-1}	0.5050	1.37×10^{-1}
c_{11}	0.05	0.0425	3.00×10^{-4}	0.0467	2.00×10^{-4}
c_{12}	0.10	0.1510	2.10×10^{-3}	0.0915	1.40×10^{-3}
c_{13}	0.20	0.1809	2.80×10^{-3}	0.1881	1.40×10^{-3}
c_{22}	-0.15	-0.2005	2.50×10^{-3}	-0.1361	1.90×10^{-3}
c_{23}	0.07	0.0472	9.10×10^{-3}	0.0760	9.70×10^{-3}
c_{33}	0.30	0.3867	3.04×10^{-2}	0.3176	9.40×10^{-3}

Τα αποτελέσματα των ανωτέρω παραδειγμάτων αποδεικνύουν ότι οι ακολουθίες Gold και ιδιαίτερα οι ακολουθίες KRG είναι σχεδόν ιδανικές για την προσομοίωση σημάτων λευκού θορύβου ανωτέρας τάξης.

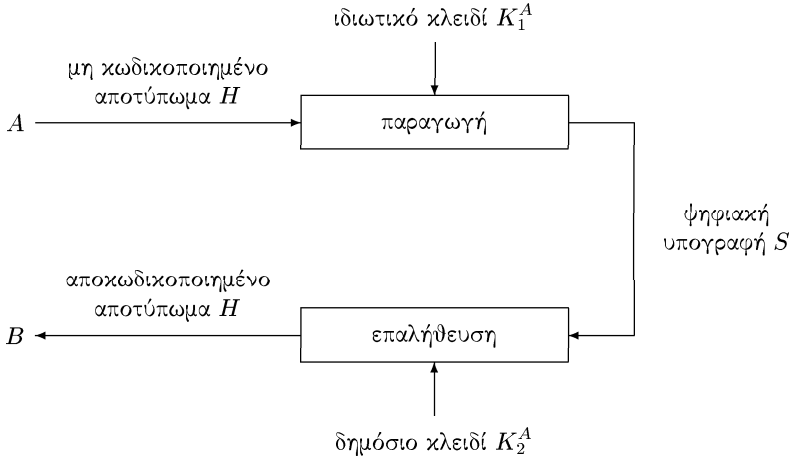
Κεφάλαιο 7

Εφαρμογές της κρυπτογραφίας

Η ανάπτυξη εφαρμογών που χρησιμοποιούνται για την ηλεκτρονική ανταλλαγή δεδομένων και διεκπεραίωση συναλλαγών πραγματοποιείται με αλματώδεις ρυθμούς. Σημαντικά παραδείγματα αποτελούν εφαρμογές ηλεκτρονικού εμπορίου, μάθησης, και διακυβέρνησης, καθώς και εφαρμογές ηλεκτρονικών προσφορών, προμηθειών, πληρωμών, και δημοπρασιών. Βασικό κίνητρο αποτέλεσε η γρήγορη εξάπλωση του Διαδικτύου ως μέσου επικοινωνίας, λόγω του χαμηλού κόστους χρήσης, ευκολίας πρόσβασης και χρήσης, καθώς και δυνατότητας διασύνδεσης ετερογενών συστημάτων. Ως αποτέλεσμα, παρατηρείται σημαντική αύξηση του όγκου διακίνησης ευαίσθητων δεδομένων μέσω του Διαδικτύου.

Βασικές προϋποθέσεις επιτυχίας των αναπτυσσόμενων εφαρμογών είναι η διαφύλαξη της ασφάλειας των επικοινωνιών και ευαίσθητων προσωπικών δεδομένων (εμπιστευτικότητα και ακεραιότητα), η πιστοποίηση της ταυτότητας των συναλλασσόμενων μερών (αυθεντικότητα), και η δυνατότητα επιβεβαίωσης πραγματοποίησης συναλλαγών (μη–αποποίηση). Οι συγκεκριμένες προϋποθέσεις αποτελούν αντικείμενο της κρυπτογραφίας, και ικανοποιούνται κάνοντας χρήση τεχνικών που προσφέρει [88], [95], [109].

Μέθοδοι που στοχεύουν στην επίτευξη της εμπιστευτικότητας περιγράφηκαν στο Κεφάλαιο 1. Το παρόν κεφάλαιο παρουσιάζει τρόπους εφαρμογής μεθόδων κρυπτογραφίας στην ανάπτυξη τεχνικών διαφύλαξης της ασφάλειας ανοικτών δικτύων επικοινωνιών. Συγκεκριμένα, εισάγονται οι έννοιες των *ψηφιακών υπογραφών*, *πιστοποιητικών δημοσίου κλειδιού*, *αρχών πιστοποίησης*, και *υποδομών δημοσίου κλειδιού*. Τέλος, περιγράφονται τα βασικά πρωτόκολλα και τεχνικές



Σχήμα 7.1. Παραγωγή/επαλήθευση ψηφιακής υπογραφής με κρυπτογραφία δημοσίου κλειδιού

που υποβοηθούν την ανάπτυξη ασφαλών εφαρμογών Διαδικτύου [25], [54].

7.1 Τεχνολογίες: ψηφιακές υπογραφές

Η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιείται για την επίτευξη της εμπιστευτικότητας (Κεφάλαιο 1) και ακεραιότητας. Η τελευταία επιτυγχάνεται με τη χρήση *ψηφιακών υπογραφών* σε αντιστοιχία με τις ιδιόχειρες υπογραφές. Για την παραγωγή των ψηφιακών υπογραφών ο αποστολέας A χρησιμοποιεί το ιδιωτικό του κλειδί K_1^A, ενώ για την επαλήθευση ο παραλήπτης B χρησιμοποιεί το δημόσιο κλειδί K_2^A του αποστολέα A.

Η διαδικασία παραγωγής και επαλήθευσης της ψηφιακής υπογραφής απεικονίζεται στο Σχ. 7.1 και βασίζεται στη *συνάρτηση κατακερματισμού*. Η συνάρτηση κατακερματισμού είναι μονόδρομη και για κάθε μήνυμα δημιουργεί ένα μοναδικό *αποτύπωμα* συγκεκριμένου μεγέθους (συνήθως 128 ή 160 bits). Η πιθανότητα δύο μηνύματα να έχουν το ίδιο αποτύπωμα είναι εξαιρετικά μικρή, με αποτέλεσμα κάθε αλλοίωση του αρχικού μηνύματος γίνεται αντιληπτή. Η ψηφιακή υπογραφή είναι η κρυπτογράφηση του αποτυπώματος.

7.1.1 Παραγωγή και επαλήθευση

Τα βήματα που πρέπει να ακολουθήσει ο αποστολέας για την παραγωγή της ψηφιακής υπογραφής που αντιστοιχεί στο απλό κείμενο M είναι τα ακόλουθα:

- Χρήση μίας συνάρτησης κατακερματισμού για τη δημιουργία του αποτυπώματος H.
- Κρυπτογράφηση του αποτυπώματος H με το ιδιωτικό κλειδί K_1^A ώστε να παραχθεί η ψηφιακή υπογραφή S, δηλ. $S = E_{K_1^A}(H)$.
- Μετάδοση του ζεύγους (M, S) μέσω του Διαδικτύου.

Υποθέτοντας χρήση καναλιού επικοινωνίας απαλλαγμένου από λάθη, τα βήματα που πρέπει να ακολουθήσει ο παραλήπτης για την επαλήθευση της ψηφιακής υπογραφής που αντιστοιχεί στο απλό κείμενο M είναι τα εξής:

- Λήψη του ζεύγους (M', S) μέσω του Διαδικτύου.
- Χρήση της ίδιας συνάρτησης κατακερματισμού για τη δημιουργία του αποτυπώματος H'.
- Αποκρυπτογράφηση της ψηφιακής υπογραφής S με το δημόσιο κλειδί K_2^A ώστε να ληφθεί το αποτύπωμα H, δηλ. $H = D_{K_2^A}(S) = D_{K_2^A}(E_{K_1^A}(H))$.
- Σύγκριση των αποτυπωμάτων H' και H.

Έαν η σύγκριση των αποτυπωμάτων είναι επιτυχής, τότε το μήνυμα M' που έλαβε ο παραλήπτης είναι ακέραιο, δηλ. $M' = M$. Στην περίπτωση όπου το μήνυμα έχει αλλοιωθεί, το αποτύπωμα H' που θα παράγει ο παραλήπτης θα είναι διαφορετικό από το αποτύπωμα H που κρυπτογραφήθηκε.

7.1.2 Χρήση ψηφιακού φακέλου

Η διαδικασία που περιγράφηκε στην προηγούμενη υπο–ενότητα διασφαλίζει την ακεραιότητα του μηνύματος M, αλλά όχι την εμπιστευτικότητα. Ένας τρόπος για την επίτευξη και των δύο στόχων είναι η δημιουργία *ψηφιακών φακέλων*.

Οι ψηφιακοί φάκελοι χρησιμοποιούνται για την εγκαθίδρυση ενός ιδιωτικού συμμετρικού κλειδιού L κρυπτογράφησης. Η δημιουργία τους προϋποθέτει χρήση διαφορετικού ζεύγους κλειδιών (X_1^A, X_2^A) και (X_1^B, X_2^B) ανταλλαγής κλειδιών

για τον αποστολέα και παραλήπτη αντίστοιχα. Μετά την παραγωγή της ψηφιακής υπογραφής S, απαιτούνται επιπλέον τα ακόλουθα βήματα:

- Κρυπτογράφηση του ζεύγους (M, S) με το ιδιωτικό συμμετρικό κλειδί L, δηλ. $V = E_L(M, S)$.
- Κρυπτογράφηση του L με το δημόσιο κλειδί ανταλλαγής κλειδιών X_2^B του παραλήπτη ώστε να παραχθεί ο ψηφιακός φάκελος W, δηλ. $W = E_{X_2^B}(L)$.
- Μετάδοση του ζεύγους (V, W) μέσω του Διαδικτύου.

Τα επιπλέον βήματα που πρέπει να διεξαχθούν πριν την επαλήθευση της ψηφιακής υπογραφής από τον παραλήπτη είναι αντίστοιχα:

- Λήψη του ζεύγους (V, W) μέσω του Διαδικτύου.
- Αποκρυπτογράφηση του ψηφιακού φακέλου W με το ιδιωτικό κλειδί ανταλλαγής κλειδιών X_1^B ώστε να ληφθεί το L, δηλ.

$$L = D_{X_1^B}(W) = D_{X_1^B}(E_{X_2^B}(L)).$$

- Αποκρυπτογράφηση του V με το ιδιωτικό συμμετρικό κλειδί L ώστε να ληφθεί το ζεύγος (M, S), δηλ. $(M, S) = D_L(V) = D_L(E_L(M, S))$.

Το πλεονέκτημα του ψηφιακού φακέλου είναι ότι ο αποστολέας A και ο παραλήπτης B μπορούν να αλλάζουν συχνά το ιδιωτικό συμμετρικό κλειδί L αυξάνοντας κατακόρυφα την ασφάλεια της μεταξύ τους επικοινωνίας. Επιπλέον, οι ψηφιακοί φάκελοι βελτιώνουν σημαντικά την απόδοση του συστήματος αφού η συμμετρική κρυπτογράφηση είναι ταχύτερη της ασύμμετρης [109].

7.2 Πιστοποιητικά δημοσίου κλειδιού

Οι μεθοδολογίες που περιγράφηκαν στην Ενότητα 7.1 εξασφαλίζουν την εμπιστευτικότητα και ακεραιότητα των μεταδιδόμενων μηνυμάτων. Η αυθεντικότητα επιτυγχάνεται μόνον έαν ο παραλήπτης B είναι απόλυτα βέβαιος ότι το δημόσιο κλειδί K_2^A, το οποίο αντιστοιχεί με μοναδικό τρόπο στο ιδιωτικό κλειδί K_1^A, πράγματι ανήκει στον αποστολέα A (υποθέτοντας ότι το απόρρητο του ιδιωτικού κλειδιού K_1^A δεν έχει παραβιαστεί) [54].

Αυτή η λειτουργία πραγματοποιείται με τη χρήση *πιστοποιητικών δημοσίου κλειδιού*. Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Η ισχυρή σύνδεση μεταξύ δικαιούχου του πιστοποιητικού και του δημοσίου κλειδιού επιτυγχάνεται μέσω της ψηφιακής υπογραφής του εκδότη, η οποία επιβεβαιώνει την ακρίβεια των στοιχείων. Ταυτόχρονα με την επίτευξη της αυθεντικότητας πραγματοποιείται η λειτουργία της μη–αποποίησης. Ο αποστολέας A ενός μηνύματος ψηφιακά υπογεγραμμένου με το ιδιωτικό κλειδί K_1^A δε μπορεί εκ΄ των υστέρων να ισχυριστεί ότι δεν έστειλε το μήνυμα [25].

Τα πρωτόκολλα υλοποίησης ψηφιακών υπογραφών προσαρτούν το πιστοποιητικό δημοσίου κλειδιού στο κυρίως μέρος του μηνύματος, μαζί με τη ψηφιακή υπογραφή. Συνεπώς, σε μία βελτιωμένη έκδοση της διαδικασίας που περιγράφηκε στην Ενότητα 7.1.2, ο αποστολέας A κρυπτογραφεί με το ιδιωτικό συμμετρικό κλειδί L το (M, S, C_A) αντί του (M, S), όπου C_A είναι το πιστοποιητικό δημοσίου κλειδιού του A.

Τα πιστοποιητικά δημοσίου κλειδιού περιλαμβάνουν πλήθος πληροφοριών που επιτρέπουν την ακριβή ταυτοποίηση του δικαιούχου. Επιπρόσθετα, δύναται να περιληφθούν πληροφορίες που περιορίζουν τη χρήση του δημοσίου κλειδιού ενός πιστοποιητικού. Παραδείγματα αποτελούν ο διαχωρισμός ζευγών ασύμμετρων κλειδιών σε [84]

- *διαφύλαξης εμπιστευτικότητας*,
- *διαχείρισης ψηφιακών υπογραφών*, και
- *ανταλλαγής κλειδιών*.

Ο πλέον αναγνωρισμένος τύπος πιστοποιητικών δημοσίου κλειδιού ορίζεται στο πρότυπο ISO/IEC/ITU X.509 [47], η βασική δομή του οποίου περιλαμβάνεται στον Πίνακα 7.1. Άλλοι τύποι πιστοποιητικών δημοσίων κλειδιών περιλαμβάνουν τα πρότυπα PKCS #6 [100] και PKCS #9 [101].

7.2.1 Αρχές πιστοποίησης

Η ευρεία εφαρμογή της κρυπτογραφίας δημοσίου κλειδιού απαιτεί εύρεση λύσης στα προβλήματα της ορθότητας των αναγραφόμενων στοιχείων σε πιστοποιητικά δημοσίου κλειδιού και της αξιόπιστης διανομής τους. Οι *αρχές πιστοποίησης* είναι

Πίνακας 7.1. Πεδία πιστοποιητικών δημοσίου κλειδιού τύπου X.509

πεδίο	**περιγραφή**
έκδοση	έκδοση του τύπου X.509 στον οποίο βασίζεται το πιστοποιητικό
κωδικός σειράς	μοναδικός κωδικός αριθμός του πιστοποιητικού ο οποίος καθορίζεται από τον εκδότη
περίοδος ισχύος	χρονική περίοδος εγκυρότητας του πιστοποιητικού
επεκτάσεις	σύνολο πεδίων που καθορίζουν επιπλέον ιδιότητες του πιστοποιητικού
δικαιούχος	μοναδικό όνομα (ονοματολογίας τύπου X.500) της οντότητας της οποίας πιστοποιείται το δημόσιο κλειδί
κωδικός δικαιούχου	προαιρετικό πεδίο που διασφαλίζει τη μοναδικότητα ταυτοποίησης του δικαιούχου
αλγόριθμος δικαιούχου	μοναδικός κωδικός αριθμός του ασύμμετρου αλγορίθμου που χρησιμοποιείται από το δικαιούχο για την παραγωγή ψηφιακών υπογραφών
κλειδί δικαιούχου	το δημόσιο κλειδί του δικαιούχου που πιστοποιείται (αντιστοιχεί στον *αλγόριθμο δικαιούχου*)
εκδότης	μοναδικό όνομα (ονοματολογίας τύπου X.500) της αρχής έκδοσης του πιστοποιητικού
κωδικός εκδότη	προαιρετικό πεδίο που διασφαλίζει τη μοναδικότητα ταυτοποίησης του εκδότη
αλγόριθμος εκδότη	μοναδικός κωδικός αριθμός του ασύμμετρου αλγορίθμου που χρησιμοποιήθηκε από τον εκδότη για την παραγωγή της ψηφιακής υπογραφής
υπογραφή εκδότη	ψηφιακή υπογραφή του εκδότη η οποία πιστοποιεί την ακρίβεια των ανωτέρω στοιχείων

έμπιστοι οργανισμοί οι οποίοι επιλύουν τα ανωτέρω προβλήματα ακολουθώντας ασφαλείς διαδικασίες έκδοσης και διανομής πιστοποιητικών δημοσίου κλειδιού. Ο παραλήπτης ενός ψηφιακά υπογεγραμμένου μηνύματος πιστοποιεί την αυθεντικότητα του μηνύματος έαν εμπιστεύεται την αρχή πιστοποίησης που εξέδωσε το πιστοποιητικό δημοσίου κλειδιού του αποστολέα [88].

Έαν τα δημόσια κλειδιά του αποστολέα A και του παραλήπτη B πιστοποιούνται από την ίδια αρχή πιστοποίησης, τότε η μεταξύ τους σχέση εμπιστοσύνης είναι άμεση (Σχ. 7.2). Επιπλέον, η σχέση εμπιστοσύνης βασίζεται στις αξιόπιστες διαδικασίες έκδοσης και διαχείρισης πιστοποιητικών δημοσίου κλειδιού που ακολουθεί η αρχή πιστοποίησης και τις οποίες αποδέχονται τα υποκείμενα πιστοποίησης. Οι διαδικασίες αυτές καθορίζονται από την *αρχή πολιτικών πιστοποίησης* [25].

Βασικό μέρος των διαδικασιών που καθορίζει η αρχή πολιτικών πιστοποίησης

Σχήμα 7.2. Μονοπάτι πιστοποίησης της εγκυρότητας πιστοποιητικών που εκδόθηκαν από την ίδια αρχή πιστοποίησης

αφορά την εξακρίβωση των στοιχείων του υποκειμένου που αναγράφονται στο πιστοποιητικό δημοσίου κλειδιού. Αναλόγως του βαθμού ασφάλειας που απαιτείται στις εφαρμογές όπου θα χρησιμοποιηθεί το πιστοποιητικό δημοσίου κλειδιού, καθορίζονται διαφορετικές διαδικασίες εξακρίβωσης στοιχείων. Οι διαδικασίες αυτές πραγματοποιούνται από την *αρχή εγγραφής* [25].

Κάθε πιστοποιητικό δημοσίου κλειδιού αναγράφει το χρονικό διάστημα κατά το οποίο το πιστοποιητικό θεωρείται έγκυρο. Το πιστοποιητικό δημοσίου κλειδιού ανακαλείται από την αρχή πιστοποίησης μετά τη λήξη της περιόδου ισχύος. Άλλα αίτια ανάκλησης πιστοποιητικών περιλαμβάνουν την άρση του απορρήτου του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί του πιστοποιητικού. Συνεπώς, είναι απαραίτητο η αρχή πιστοποίησης να γνωστοποιεί τους κωδικούς σειράς όλων των πιστοποιητικών δημοσίου κλειδιού που έχουν ανακληθεί. Η δημοσίευση των ανακληθέντων κωδικών σειράς γίνεται στη *λίστα ανάκλησης πιστοποιητικών* της οποίας η ενημέρωση γίνεται σε τακτά χρονικά διαστήματα [88].

Τα γενικά χαρακτηριστικά που απαιτούνται από τις αρχές πιστοποίησης περιλαμβάνουν την ανεξαρτησία, ουδετερότητα, αξιοπιστία, και την κοινή αποδοχή από τους συμμετέχοντες του πλαισίου πιστοποίησης.

7.3 Υποδομές δημοσίου κλειδιού

Οι υπηρεσίες που προσφέρονται από μία αρχή πιστοποίησης πραγματοποιούνται σε διαφορετικά οργανωτικά επίπεδα (εταιρικό, εθνικό, πολυεθνικό). Στην περίπτωση όπου ο αποστολέας A και ο παραλήπτης B ενός μηνύματος είναι εγγεγραμμένοι σε διαφορετικές αρχές πιστοποίησης (π.χ. έαν οι αρχές πιστοποίησης των A και B λειτουργούν σε εταιρικό επίπεδο), τότε πρέπει να βρεθούν τρόποι

επίλυσης του προβλήματος διατήρησης εμπιστοσύνης μεταξύ των A και B [25], [54].

Οι *υποδομές δημοσίου κλειδιού* προσφέρουν λύση στο πρόβλημα ασφαλούς επικοινωνίας μεταξύ δύο οντοτήτων, των οποίων το δημόσιο κλειδί πιστοποιείται από διαφορετικές αρχές πιστοποίησης, επεκτείνοντας το *άμεσο μονοπάτι πιστοποίησης* του Σχ. 7.2.

7.3.1 Αρχιτεκτονικές

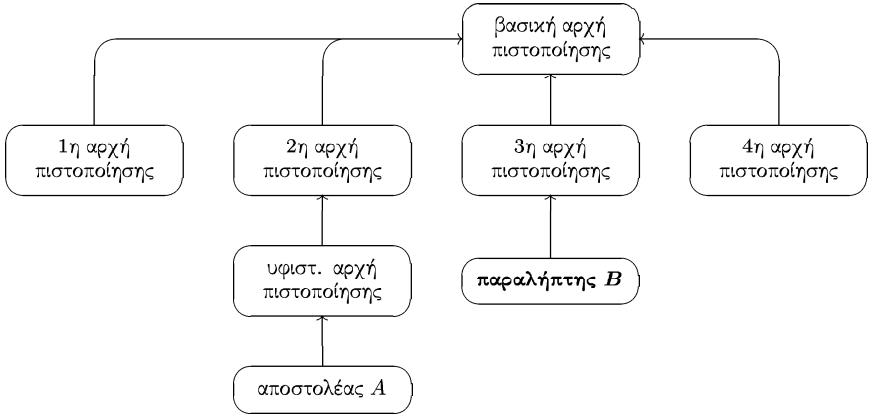
Κατά τη διαδικασία επαλήθευσης της ψηφιακής υπογραφής S ο παραλήπτης B ελέγχει την εγκυρότητα του πιστοποιητικού δημοσίου κλειδιού C_A επαληθεύοντας και τη ψηφιακή υπογραφή της αρχής πιστοποίησης που εξέδωσε το πιστοποιητικό. Το συγκεκριμένο βήμα απαιτεί η αρχή πιστοποίησης να έχει εκδόσει πιστοποιητικό για το δημόσιο κλειδί που αντιστοιχεί μοναδικά στο ιδιωτικό της κλειδί δημιουργίας ψηφιακών υπογραφών [88], [95], [109].

Έαν ο παραλήπτης B δεν εμπιστεύεται την αρχή πιστοποίησης που εξέδωσε το πιστοποιητικό του αποστολέα A, συνεχίζει την ανωτέρω διαδικασία επαλήθευσης ψηφιακών υπογραφών έως ότου καταλήξει σε μία αρχή πιστοποίησης την οποία εμπιστεύεται. Με τη συγκεκριμένη διαδικασία σχηματίζονται *σύνθετα μονοπάτια πιστοποίησης*. Μία από τις λειτουργίες που είναι απαραίτητες για την ανάπτυξη επεκτάσιμων υποδομών είναι η κατασκευή μονοπατιών τα οποία θα διευκολύνουν την πιστοποίηση των δημοσίων κλειδιών.

Ένα σύνολο από μονοπάτια πιστοποίησης ονομάζεται *μοντέλο εμπιστοσύνης* το οποίο απεικονίζει την αρχιτεκτονική της υποδομής δημοσίου κλειδιού. Μεταξύ άλλων, τα κυριότερα μοντέλα εμπιστοσύνης είναι το *ιεραρχικό* και *σύνθετο ιεραρχικό* [25].

Ιεραρχικό μοντέλο

Στη συγκεκριμένη δομή κάθε υποκείμενο συσχετίζεται μόνο με την αρχή πιστοποίησης του αμέσως υψηλότερου επιπέδου. Για να πιστοποιήσει ο παραλήπτης B την εγκυρότητα του δημοσίου κλειδιού του αποστολέα A πρέπει να καταφύγει στη *βασική αρχή πιστοποίησης* που είναι έμπιστη κι από τους δύο. Χωρίς την ύπαρξη αυτής, θα ήταν αδύνατο ο παραλήπτης B να εμπιστευτεί τον αποστολέα A (Σχ. 7.3).



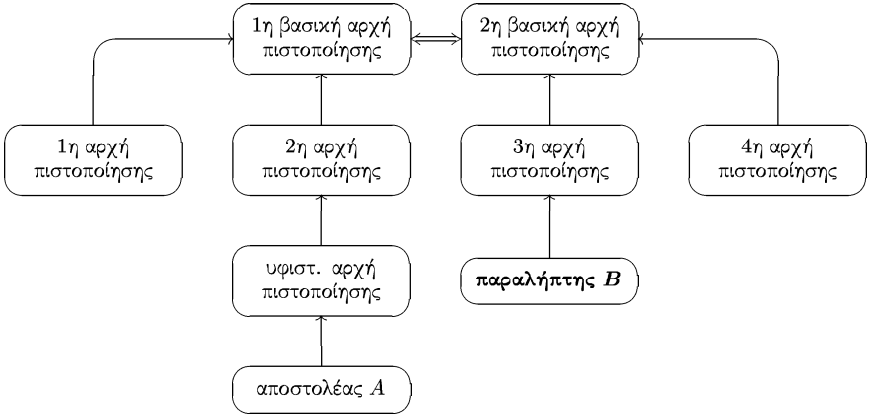
Σχήμα 7.3. Ιεραρχικό μοντέλο υποδομής δημοσίου κλειδιού

Πιθανή αποκάλυψη του ιδιωτικού κλειδιού της βασικής αρχής πιστοποίησης καθιστά τα πιστοποιητικά όλων των υφιστάμενων αρχών πιστοποίησης άκυρα. Το κόστος μίας τέτοιας αποκάλυψης είναι μεγάλο, και οδηγεί στην ανάπτυξη πιο σύνθετων αρχιτεκτονικών υποδομών δημοσίου κλειδιού. Επιπρόσθετο πρόβλημα του συγκεκριμένου μοντέλου είναι η δυσκολία ύπαρξης μίας ευρέως αποδεκτής αρχής πιστοποίησης [25].

Σύνθετο ιεραρχικό μοντέλο

Το σύνθετο ιεραρχικό μοντέλο επιλύει τα προβλήματα του απλού ιεραρχικού μοντέλου. Στην πράξη, οι υπάρχουσες υποδομές δημοσίου κλειδιού διαφέρουν ως προς τα τεχνικά χαρακτηριστικά και τις υπηρεσίες που προσφέρουν. Η δημιουργία μίας υποδομής δημοσίου κλειδιού ευρείας κλίμακας που θα επιτρέπει την ασφαλή επικοινωνία μεταξύ δύο υποκειμένων απαιτεί τη συνεργασία μεγάλου πλήθους υποδομών δημοσίου κλειδιού (Σχ. 7.4).

Το σύνθετο ιεραρχικό μοντέλο διευκολύνει την επικοινωνία μεταξύ ετερογενών υποδομών δημοσίου κλειδιού. Η πιστοποίηση της αμοιβαίας εμπιστοσύνης μεταξύ δύο βασικών αρχών πιστοποίησης συνήθως εκφράζεται με την υπογραφή επισήμων εγγράφων. Το μειονέκτημα της συγκεκριμένης αρχιτεκτονικής είναι η δυσκολία γνώσης, ενός υποκειμένου, των αρχών πιστοποίησης με τις οποίες διατηρείται συνεργασία, δεδομένου του πλήθους οργανισμών που διατηρούν δική



Σχήμα 7.4. Σύνθετο ιεραρχικό μοντέλο υποδομής δημοσίου κλειδιού

τους υποδομή δημοσίου κλειδιού [25].

7.3.2 Στόχοι και υπηρεσίες

Οι υποδομές δημοσίου κλειδιού προσφέρουν ένα σύνολο υπηρεσιών απαραίτητες για την ευρεία χρήση τεχνολογιών βασισμένων στην κρυπτογραφία δημοσίου κλειδιού. Μεταξύ άλλων, περιλαμβάνονται τα ακόλουθα [25], [88].

- **παροχή χρονο–σφραγίδων:** είναι πιστοποιητικά που βεβαιώνουν την πραγματοποίηση μίας διαδικασίας (αποστολή μηνυμάτων και διεκπεραίωση συναλλαγών) σε συγκεκριμένη χρονική στιγμή. Απαραίτητη προϋπόθεση είναι η κατοχή αξιόπιστης συσκευής μέτρησης του χρόνου. Αποτελούν το κύριο μέσο επίλυσης διαφορών που σχετίζονται με το χρόνο αποδοχής ή ανάκλησης συμφωνιών.

- **διατήρηση αποδεικτικών στοιχείων:** επιβεβαιώνουν την ύπαρξη επικοινωνίας μεταξύ δύο υποκειμένων. Η διατήρησή τους καθιστά δυνατή τη μεταγενέστερη χρήση τους σε περιπτώσεις αποποίησης αποστολής ή παραλαβής μηνυμάτων και διεκπεραίωσης συναλλαγών. Η διατήρηση των αποδεικτικών στοιχείων για μεγάλες χρονικές περιόδους απαιτεί την ύπαρξη κατάλληλων υποδομών ασφαλείας.

- **μεσολάβηση διανομών:** περιλαμβάνουν την παροχή υπηρεσιών, σε περιπτώσεις στέρησης κατάλληλων υποδομών στα πληροφοριακά συστήματα των συναλλασσόμενων μερών, που εξασφαλίζουν αξιόπιστη επικοινωνία. Μεταξύ άλλων, παραδείγματα υπηρεσιών περιλαμβάνονται σε συστήματα ηλεκτρονικού εμπορίου και ηλεκτρονικής πληρωμής λογαριασμών [61], [77].

7.4 Ασφάλεια Διαδικτύου

Το χαμηλό κόστος χρήσης, ευκολία πρόσβασης, και δυνατότητα διασύνδεσης ετερογενών συστημάτων καθιστούν το Διαδίκτυο βασικό μέσο επικοινωνίας μεταξύ οργανισμών, εταιρειών, ερευνητικών φορέων, και μεμονωμένων χρηστών. Η ανάπτυξη εφαρμογών ηλεκτρονικής ανταλλαγής δεδομένων και διεκπεραίωσης συναλλαγών πραγματοποιείται με αλματώδη ρυθμό. Παραδείγματα αποτελούν εφαρμογές ηλεκτρονικού εμπορίου, μάθησης, διακυβέρνησης, καθώς και εφαρμογές ηλεκτρονικών προσφορών, προμηθειών, πληρωμών, δημοπρασιών.

Τα βασικότερα εμπόδια στην απρόσκοπτη χρήση του Διαδικτύου ως μέσου επικοινωνίας αφορούν θέματα ασφάλειας των πληροφοριακών συστημάτων και των ευαίσθητων δεδομένων που διατηρούν. Βασικός τρόπος αντιμετώπισης των ανωτέρω θεμάτων είναι η θεώρηση μίας ακολουθίας βημάτων για την ανάπτυξη στρατηγικών ασφάλειας. Μεταξύ των βημάτων είναι η διερεύνηση μηχανισμών επιβολής της στρατηγικής ασφάλειας σε ευαίσθητα δεδομένα κατά [61], [77]

- την αποθήκευσή τους σε κεντρικά αποθηκευτικά συστήματα, και
- τη μετάδοσή τους μέσω ανοικτών δικτύων, όπως το Διαδίκτυο.

Η ασφάλεια των δεδομένων κατά την αποθήκευσή τους σε κεντρικά αποθηκευτικά συστήματα εξαρτάται σε μεγάλο βαθμό από την ασφάλεια που παρέχεται από τα λειτουργικά συστήματα και τα συστήματα διαχείρισης βάσεων δεδομένων ενός οργανισμού. Η επιτυχής αντιμετώπιση πιθανών απειλών βασίζεται σε διαδικασίες ταυτοποίησης της ταυτότητας των χρηστών και *ελέγχου δικαιωμάτων πρόσβασης* [17].

7.4.1 Πρωτόκολλα ασφάλειας

Η ασφάλεια των δεδομένων κατά τη μετάδοσή τους μέσω ανοικτών δικτύων βασίζεται στην εφαρμογή πρότυπων πρωτοκόλλων ασφάλειας. Ανάλογα με το

Πίνακας 7.2. Μηχανισμοί επίτευξης ασφάλειας κατά τη μετάδοση δεδομένων

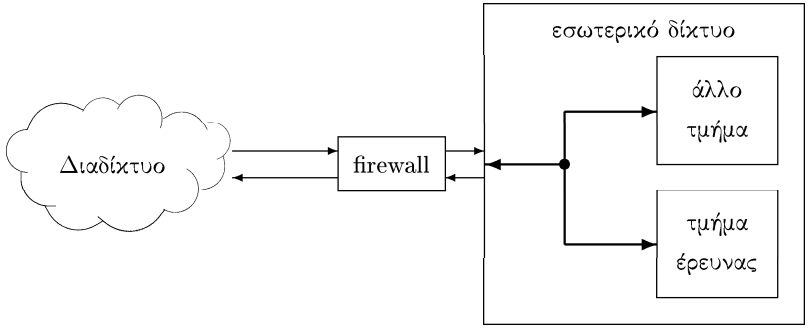
επίπεδο	ασφάλεια	μηχανισμός
δικτύου	μεταξύ ξενιστών	IP security protocol network layer security protocol point–to–point tunneling protocol
μεταφοράς/ συνόδου	μεταξύ διαδικασιών	secure sockets layer transport layer security
εφαρμογής	αναλόγως δομής δεδομένων	secure hypertext transfer protocol pretty good privacy privacy enhanced mail secure multipurpose Internet mail extensions
	αναλόγως φύσης δεδομένων	secure electronic transactions open financial exchange

επίπεδο του μοντέλου OSI όπου λειτουγούν, διαχωρίζονται σε τρεις βασικές κατηγορίες [61]: δικτύου, μεταφοράς/συνόδου, και εφαρμογής (βλ. Πίνακα 7.2). Επιπλέον, τα πρωτόκολλα του επιπέδου εφαρμογής υποδιαιρούνται σε εκείνα που εξειδικεύονται σε δεδομένα συγκεκριμένης δομής κι εκείνα που εξειδικεύονται σε δεδομένα συγκεκριμένης φύσης (π.χ. οικονομικά στοιχεία).

Κάθε πρωτόκολλο χαρακτηρίζεται από πλεονεκτήματα και μειονεκτήματα, π.χ. τα πρωτόκολλα δικτύου πραγματοποιούν πιστοποίηση ταυτότητας σε επίπεδο ξενιστών έναντι πρωτοκόλλων μεταφοράς/συνόδου που πραγματοποιούν πιστοποίηση ταυτότητας σε επίπεδο διαδικασιών. Πάντως, ορισμένα πρωτόκολλα (όπως το SSL) έχουν τη δυνατότητα να πιστοποιήσουν την ταυτότητα των χρηστών έαν γίνει χρήση πιστοποιητικών δημοσίου κλειδιού κατά τη διάρκεια της φάσης έναρξης.

Το SSL είναι το πιο ευρέως διαδεδομένο πρωτόκολλο ασφάλειας. Οι αλγόριθμοι κρυπτογράφησης που υποστηρίζει είναι οι RC2, RC4, DES, τριπλός DES, IDEA, και Fortezza. Η λειτουργία του διακρίνεται στη *φάση χειραψίας* και στη *φάση καταγραφής*. Κατά τη φάση χειραψίας, το πρωτόκολλο SSL διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση ταυτότητας των συναλλασσόμενων μερών. Κατά τη φάση καταγραφής, το πρωτόκολλο SSL κρυπτογραφεί τα προς αποστολή πακέτα και αποκρυπτογραφεί τα παραληφθέντα πακέτα. Η πιο κοινή χρήση του πρωτοκόλλου SSL είναι η διασφάλιση των επικοινωνιών τύπου HTTP [111].

Μεταξύ των πρωτοκόλλων που χρησιμοποιούνται ευρέως είναι επίσης το PGP



Σχήμα 7.5. Περίμετρος ασφάλειας εσωτερικού δικτύου

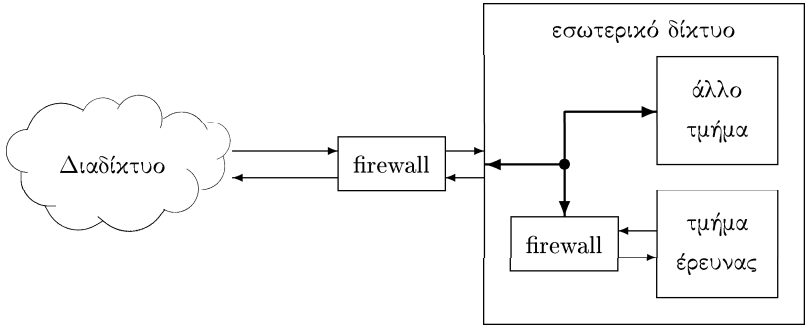
στην ανταλλαγή ηλεκτρονικού ταχυδρομείου, το SET στη διεκπεραίωση οικονομικών συναλλαγών, και το IPsec στην υλοποίηση *ιδεατών ιδιωτικών δικτύων*.

7.4.2 Πύλες ασφάλειας

Εκτός των πρωτοκόλλων που αναφέρθηκαν στην προηγούμενη ενότητα, οι *πύλες ασφάλειας* αποτελούν βασικό μηχανισμό προστασίας ενός εσωτερικού δικτύου από εξωτερικές επιθέσεις. Μία πύλη ασφάλειας αποτρέπει την ανεπιθύμητη και μη–εξουσιοδοτημένη επικοινωνία προς ένα δίκτυο ελέγχοντας τη ροή των εισερχόμενων πακέτων του Διαδικτύου. Το βασικό πλεονέκτημα χρήσης των πυλών ασφάλειας είναι ότι αποτελούν το μοναδικό σημείο που πρέπει να διαμορφωθεί προσεκτικά για την παρεμπόδιση εξωτερικών απειλών.

Η πύλη ασφάλειας του Σχ. 7.5 καθορίζει την *περίμετρο ασφάλειας* του εσωτερικού δικτύου. Το συγκεκριμένο μοντέλο ονομάζεται *μονοδιάστατο* λόγω έλλειψης εναλλακτικών μεθόδων ασφάλειας για την περαιτέρω παρεμπόδιση των επιτυχών επιθέσεων [90]. Στην πράξη, υλοποιούνται πολλαπλές περίμετροι ασφάλειας για την προστασία των ευαίσθητων δεδομένων του εσωτερικού δικτύου. Σε ένα *πολυδιάστατο* μοντέλο ασφάλειας, τοποθετούνται επιπλέον πύλες ασφάλειας που ελέγχουν την πρόσβαση προς συγκεκριμένα υποδίκτυα (Σχ. 7.6). Συνήθως, τα τελευταία μοντέλα συνδυάζονται με άλλους μηχανισμούς ελέγχου πρόσβασης για να δημιουργήσουν ένα συμπαγές σύστημα ασφάλειας [111].

Οι λειτουργίες των πυλών ασφάλειας συνδυάζονται συχνά με μεθόδους κρυπτογραφίας. Αυτό αποδεικνύεται ιδιαίτερα χρήσιμο σε περιπτώσεις όπου τμήμα-



Σχήμα 7.6. Ενισχυμένη περίμετρος ασφάλειας εσωτερικού δικτύου

τα ενός οργανισμού βρίσκονται σε γεωγραφικά απομακρυσμένες περιοχές. Στη συγκεκριμένη περίπτωση, η δημιουργία ενός *ιδεατού ιδιωτικού δικτύου* θεωρείται ο καταλληλότερος τρόπος επίτευξης της εμπιστευτικότητας των μεταδιδόμενων πληροφοριών.

Κεφάλαιο 8

Σύνοψη και περαιτέρω έρευνα

Η παρούσα διατριβή επικεντρώθηκε στη μελέτη σύγχρονων σειριακών αλγορίθμων κρυπτογράφησης που στοχεύουν στην επίτευξη της εμπιστευτικότητας σημάτων ή δεδομένων προς αποθήκευση ή μετάδοση μέσω ανοικτών δικτύων. Αναπτύχθηκαν τεχνικές επεξεργασίας σήματος για την ακριβή αποτίμηση και βελτίωση των χαρακτηριστικών τα οποία καθορίζουν το βαθμό ασφάλειας που αποδίδεται σε κρυπτογραφήματα.

Δόθηκε ιδιαίτερη έμφαση σε γεννήτορες παραγωγής ψευδοτυχαίων ακολουθιών κλειδιών, και στην υλοποίηση αυτών μέσω μη–γραμμικών συνδυαστών και μη–γραμμικών φίλτρων. Η ασφάλεια σειριακών αλγορίθμων κρυπτογράφησης εξαρτάται με αποφασιστικό τρόπο από το βαθμό τυχαιότητας των ψευδοτυχαίων ακολουθιών κλειδιών.

Προς αυτήν την κατεύθυνση, η έρευνα συνέβαλε στην ανάλυση και παραγωγή ψευδοτυχαίων ακολουθιών που προσομοιάζουν πραγματικά τυχαίες ακολουθίες, μελετώντας έννοιες, όπως η γραμμική πολυπλοκότητα και συνάρτηση αυτοσυσχέτισης, και εισάγοντας νέες, όπως η προσέγγιση ακολουθιών και στατιστικές υψηλότερων τάξεων.

8.1 Σύνοψη ερευνητικών αποτελεσμάτων

Η γραμμική πολυπλοκότητα αποτελεί σημαντικό κριτήριο ανθεκτικότητας σε αλγορίθμους κρυπτανάλυσης, όπως ο αλγόριθμος των Berlekamp–Massey (βλ. Κεφάλαιο 4). Για την ακρίβεια, επεκτάθηκαν οι τεχνικές ανάλυσης της γραμμικής

πολυπλοκότητας ακολουθιών παραγόμενων από μη–γραμμικά φίλτρα. Δόθηκαν κλειστοί τύποι υπολογισμού των συντελεστών Fourier όλων των στοιχείων ενός πεπερασμένου σώματος, και για οποιοδήποτε μη–γραμμικό φίλτρο, ώστε να προσδιοριστεί πλήρως η αναπαράσταση ίχνους της ακολουθίας εξόδου σε σχέση με το μη–γραμμικό φίλτρο.

Επίσης, καθορίστηκαν νέοι τρόποι επιλογής γινομένων ακολουθιών που λαμβάνονται από διαφορετικές βαθμίδες ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης, ώστε να εξασφαλιστεί ότι η γραμμική πολυπλοκότητα των γινομένων είναι μεγαλύτερη από μία συγκεκριμένη τιμή. Ως αποτέλεσμα, αναπτύχθηκαν μέθοδοι προσδιορισμού μη–γραμμικών φίλτρων τα οποία παράγουν ακολουθίες καθορισμένης γραμμικής πολυπλοκότητας.

Η παραγωγή και εύρεση ακολουθιών που προσεγγίζουν αποτελεσματικά μία δοθείσα ακολουθία αποτελεί σημαντικό παράγοντα για το χαρακτηρισμό της ως ψευδοτυχαίας και ανθεκτικής σε κρυπταναλυτικές τεχνικές (βλ. Κεφάλαιο 5). Στη διατριβή μελετήθηκε το πρόβλημα της προσέγγισης με απόκλιση ενός σφάλματος. Η θέση του σφάλματος που παράγει τη βέλτιστη προσέγγιση ονομάστηκε βέλτιστη φάση. Παρουσιάστηκαν τρεις μέθοδοι εύρεσης της βέλτιστης φάσης, η μέθοδος των διαδοχικών διαιρέσεων, η μέθοδος των εξισώσεων ισοδυναμίας, και η μέθοδος του συγχρονισμού φάσεων.

Η πρώτη μέθοδος βασίζεται στη διαδοχική εφαρμογή του αλγορίθμου του Ευκλείδη χρησιμοποιώντας παράγοντες του ελαχίστου πολυωνύμου της δοθείσας ακολουθίας. Η δεύτερη μέθοδος λειτουργεί στο χώρο των συχνοτήτων και προσδιορίζει τη βέλτιστη φάση επιλύοντας ένα σύνολο από εξισώσεις ισοδυναμίας. Επιπρόσθετα, αναλύθηκε η επιλυσιμότητα των εξισώσεων και παράχθηκε ένα σύνολο κλειστών τύπων. Τέλος, η τρίτη μέθοδος υπολογίζει τη βέλτιστη φάση με την αναπαράσταση ίχνους και την έννοια της κυκλικής ισοδυναμίας.

Η αλγοριθμική υλοποίηση των μεθόδων και η ανάλυση της υπολογιστικής πολυπλοκότητας αντιμετωπίστηκε με επάρκεια. Επιπλέον, καθορίστηκαν ακολουθίες των οποίων οι προσεγγίσεις πρώτης τάξεως έχουν προκαθορισμένη γραμμική πολυπλοκότητα. Ιδιαίτερα μεγάλης σημασίας είναι οι ακολουθίες εκείνες των οποίων η βέλτιστη προσέγγιση έχει μεγαλύτερη γραμμική πολυπλοκότητα από εκείνη της αρχικής ακολουθίας. Οι ακολουθίες αυτές ονομάστηκαν ανθεκτικές ακολουθίες.

Η παραγωγή κατάλληλων ψευδοτυχαίων ακολουθιών είναι από τα βασικά προβλήματα τόσο της κρυπτογραφίας όσο και της επεξεργασίας σήματος. Στη

διατριβή, διερευνήθηκε η δημιουργία δυαδικών ακολουθιών οι οποίες επιδεικνύουν τα χαρακτηριστικά λευκού θορύβου ανωτέρας τάξεως (βλ. Κεφάλαιο 6) και παράγονται από καταλλήλως επιλεγμένα ζεύγη ακολουθιών της ιδίας ή διαφορετικών ελαχίστων περιόδων. Αποδείχθηκε η ακαταλληλότητα χρήσης ακολουθιών μεγίστου μήκους ως λευκού θορύβου ανωτέρας τάξεως. Η έρευνα επικεντρώθηκε στις ακολουθίες Gold, δυϊκές BCH και παράγωγα αυτών, ενώ κατασκευάστηκε μία νέα κλάση ακολουθιών, οι KRG, των οποίων η καταλληλότητα αποδείχθηκε σε πειράματα ταυτοποίησης συστημάτων διγραμμικών μοντέλων.

Συγκεκριμένα, αποδείχθηκε ότι η συνάρτηση αυτοσυσχέτισης και οι ροπές ανωτέρας τάξεως δυαδικών ακολουθιών παραγόμενων από την πρόσθεση δύο ακολουθιών μεγίστου μήκους αυθαιρέτων ελαχίστων περιόδων, εξαρτώνται από τη συνάρτηση ετεροσυσχέτισης των συγκεκριμένων ακολουθιών. Έαν οι δύο ακολουθίες μεγίστου μήκους έχουν την ίδια ελάχιστη περίοδο, τότε οι ροπές ανωτέρας τάξεως των παραγόμενων ακολουθιών λαμβάνουν τιμές από ένα προκαθορισμένο σύνολο, και έαν υπάρχουν, τα τοπικά τους μέγιστα είναι ελάχιστα και ελεγχόμενα εκ΄ των προτέρων με κατάλληλη επιλογή των αρχικών ακολουθιών μεγίστου μήκους. Τα ανωτέρω αποτελέσματα εφαρμόστηκαν στις ακολουθίες Gold, όπου και κατέστη δυνατός ο έλεγχος των τιμών της συνάρτησης ετεροσυσχέτισης καθώς και της συχνότητα εμφάνισής τους σε μια περίοδο.

Ειδική περίπτωση αποτέλεσαν οι δυϊκές BCH ακολουθίες που παράγονται από το πολυώνυμο γεννήτορα ενός BCH κώδικα διόρθωσης δύο σφαλμάτων. Επιπλέον, αποδείχθηκε ότι έαν το χαρακτηριστικό πολυώνυμο ενός καταχωρητή ολίσθησης γραμμικής ανάδρασης είναι το ανάστροφο του πολυωνύμου γεννήτορα ενός δυαδικού BCH κώδικα διόρθωσης t–σφαλμάτων, τότε η προκύπτουσα δυαδική ακολουθία δεν έχει τοπικά μέγιστα σε όλες τις ροπές μέχρι τάξεως $2t$. Ιδιαίτερα λεπτομερής ανάλυση δόθηκε στην περίπτωση συνιστωσών ακολουθιών μεγίστου μήκους διαφορετικών ελαχίστων περιόδων.

Ειδική περίπτωση αποτέλεσε η κατασκευή των νέων ακολουθιών KRG, των οποίων οι συνιστώσες ακολουθίες έχουν σχετικά πρώτες περιόδους. Η συνάρτηση ετεροσυσχέτισης των συνιστωσών ακολουθιών είναι σταθερή και ίση με τον αντίστροφο του γινομένου των περιόδων τους. Επιπρόσθετα, η συνάρτηση αυτοσυσχέτισης και οι ροπές ανωτέρας τάξεως των ακολουθιών KRG συμπεριφέρονται όπως στην περίπτωση ακολουθιών Gold με τη διαφορά ότι επιτρέπουν καλύτερο έλεγχο των θέσεων εμφάνισης των τοπικών μεγίστων καθώς και του μεγέθους των τιμών τους. Συγκεκριμένα, η απόσταση των τοπικών μεγίστων

από την αρχή των αξόνων είναι ιδιαίτερα μεγάλη καθιστώντας τις ακολουθίες αυτές σχεδόν ιδανικές για την προσομοίωση λευκού θορύβου ανωτέρας τάξεως σε ορισμένα προβλήματα ταυτοποίησης.

Η ποιότητα των παραπάνω δυαδικών ακολουθιών στην προσομοίωση λευκού θορύβου ανωτέρας τάξεως αποδείχθηκε με πειράματα ταυτοποίησης διγραμμικών συστημάτων, όπου οι ακολουθίες μεγίστου μήκους απέτυχαν να δώσουν αμερόληπτες εκτιμήσεις των παραμέτρων του συστήματος.

Η αξία των ερευνητικών αποτελεσμάτων δεν περιορίζεται μόνο στο σχεδιασμό σειριακών κρυπτοσυστημάτων καθώς ο βαθμός ασφάλειας πλήθους άλλων κρυπτοσυστημάτων βασίζεται στη χρήση τυχαίων ακολουθιών (βλ. Κεφάλαια 1 και 7). Επιπλέον, τα ερευνητικά αποτελέσματα δύναται να χρησιμοποιηθούν στην ευρύτερη περιοχή της επεξεργασίας σήματος, και ειδικότερα στην ταυτοποίηση μη–γραμμικών συστημάτων όπου η ποιότητα και η ακρίβεια των εκτιμήσεων των παραμέτρων του άγνωστου συστήματος εξαρτάται από τον τύπο των σημάτων εισόδου που χρησιμοποιούνται για τη διέγερση του συστήματος.

8.2 Μελλοντικές ερευνητικές κατευθύνσεις

Πολλά είναι τα ερευνητικά προβλήματα στο χώρο της κρυπτογραφίας που παραμένουν ανοικτά, τα σημαντικότερα εκ΄ των οποίων αφορούν το σχεδιασμό λογικών συναρτήσεων και ψευδο–τυχαίων ακολουθιών, και το σχεδιασμό πολυπληθών οικογενειών ακολουθιών με επιθυμητές ιδιότητες αυτο– και ετερο– συσχέτισης.

Στις ακόλουθες ενότητες αναλύουμε μελλοντικές ερευνητικές δραστηριότητες που σχετίζονται με το αντικείμενο της παρούσας διατριβής.

Μη–γραμμική πολυπλοκότητα

Η γραμμική πολυπλοκότητα ορίζεται ως το μήκος του ελαχίστου καταχωρητή ολίσθησης γραμμικής ανάδρασης που παράγει μία δοθείσα ακολουθία. Γενίκευση αυτής είναι η *μη–γραμμική πολυπλοκότητα τάξης* k, $k \geq 1$, που ορίζεται ως το μήκος του ελαχίστου καταχωρητή ολίσθησης μη–γραμμικής ανάδρασης τάξης μικρότερης ή ίσης με k που παράγει μία δοθείσα ακολουθία.

Διεξάγεται έρευνα για την επίλυση του προβλήματος αναθεωρώντας την προσέγγιση που δίνεται στα [12] και [46]. Στόχος είναι η κατασκευή αποδοτικών αλγορίθμων για την εύρεση της μη–γραμμικής πολυπλοκότητας, και η θεωρητική

τους θεμελίωση. Έαν η δοθείσα ακολουθία έχει n στοιχεία και γνωρίζαμε ότι το ελάχιστο μήκος του καταχωρητή ολίσθησης είναι 3, τότε το πρόβλημα δύναται να περιγραφεί (για $k = 2$) ως ένα σύνολο εξισώσεων της μορφής

$$\begin{pmatrix} x_1 & x_2 & x_1x_2 & x_3 & x_2x_3 & x_1x_3 \\ x_2 & x_3 & x_2x_3 & x_4 & x_3x_4 & x_2x_4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n-3} & x_{n-2} & x_{n-3}x_{n-2} & x_{n-1} & x_{n-2}x_{n-1} & x_{n-3}x_{n-1} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_{1,2} \\ r_3 \\ r_{2,3} \\ r_{1,3} \end{pmatrix} = \begin{pmatrix} x_4 \\ x_5 \\ \vdots \\ x_n \end{pmatrix}.$$

Προκαταρκτικά αποτελέσματα έχουν ήδη ληφθεί στην περίπτωση μη–γραμμικής ανάδρασης δεύτερης τάξης [98], ενώ συνεχίζεται η έρευνα για τη λύση του γενικού προβλήματος.

Αλγόριθμοι σχεδιασμού λογικών συναρτήσεων

Η θεματική περιοχή εύρεσης και σχεδιασμού λογικών συναρτήσεων παρουσιάζει εξαιρετικό ενδιαφέρον. Αναλόγως του πεδίου εφαρμογής, οι λογικές συναρτήσεις πρέπει να ενσωματώνουν διαφορετικά χαρακτηριστικά. Μελλοντικές ερευνητικές κατευθύνσεις περιλαμβάνουν το σχεδιασμό αλγορίθμων κατασκευής λογικών συναρτήσεων που παράγουν ακολουθίες με συγκεκριμένο προφίλ συνάρτησης αυτοσυσχέτισης, είναι ανθεκτικές σε επιθέσεις κρυπτανάλυσης, είναι ισοβαρείς, κλπ.

Η συγκεκριμένη ερευνητική δραστηριότητα αναμένεται να βασιστεί στις σχέσεις του Κεφαλαίου 4 που συνδέουν την κανονική αλγεβρική μορφή της συνάρτησης φίλτρου f με την αναπαράσταση ίχνους των παραγόμενων ψευδο–τυχαίων ακολουθιών (δηλ. $\boldsymbol{b} = \boldsymbol{f} \cdot \boldsymbol{R}$).

Ελάχιστη προσέγγιση ανωτέρας τάξης

Διεξάγεται έρευνα για την επέκταση της προσέγγισης δυαδικών ακολουθιών περιόδου $2^n - 1$ σε περισσότερα του ενός λάθη, με ταυτόχρονη επέκταση και των τριών μεθοδολογιών που αναπτύχθηκαν. Στην γενική περίπτωση k λαθών, η μέθοδος των διαδοχικών διαιρέσεων απαιτεί επιπρόσθετα τον υπολογισμό του μέγιστου κοινού διαιρέτη των

$$e(z) = 1 + z^{i_1} + \cdots + z^{i_{k-1}} \quad \text{και} \quad 1 + z^N$$

όπου $i_1, \ldots, i_{k-1}$ είναι η απόσταση μεταξύ διαδοχικών θέσεων λαθών. Ομοίως, η μέθοδος του συγχρονισμού φάσεων εξαρτάται από την εύρεση κανονικών και μη–κανονικών πολυωνύμων ακολουθιών βάρους k. Ταυτόχρονα, ερευνάται η περίπτωση χρήσης τεχνικών αποκωδικοποίησης (π.χ. αλγόριθμος Berlekamp–Massey) της θεωρίας *κωδίκων ελέγχου σφαλμάτων* για την εύρεση των θέσεων λάθους. Τα αποτελέσματα του Κεφαλαίου 5 δύναται να γενικευτούν σε μη–δυαδικές ακολουθίες.

Μη–δυαδικές ακολουθίες λευκού θορύβου

Διεξάγεται έρευνα για την κατασκευή επιπλέον ακολουθιών με χαρακτηριστικά σημάτων λευκού θορύβου ανωτέρας τάξης. Ο στόχος είναι

- η διατήρηση των χαρακτηριστικών των ακολουθιών KRG, δηλ. πλήρης έλεγχος του μεγέθους, θέσης, και συχνότητας εμφάνισης των τιμών της συνάρτησης αυτοσυσχέτισης, και
- η ταυτόχρονη αύξηση της γραμμικής πολυπλοκότητας των συνιστωσών ακολουθιών θεωρώντας οποιεσδήποτε ακολουθίες με ιδανική συνάρτηση αυτοσυσχέτισης.

Επιπλέον, εξετάζονται τεχνικές της θεωρίας *πιθανοτήτων* για την παραγωγή πραγματικών σημάτων που ακολουθούν την *κανονική κατανομή* και εφαρμογή τους σε ακολουθίες μεγίστου μήκους. Εικάζεται ότι το βήμα αυτό απαιτεί τη γενίκευση των αποτελεσμάτων του Κεφαλαίου 6 σε μη–δυαδικές ακολουθίες.

Παραρτήματα

Α Πρωταρχικά πολυώνυμα

Στον ακόλουθο πίνακα παραθέτουμε πρωταρχικά πολυώνυμα στο $\mathbb{F}_2$ βαθμού n, με $2 \leq n \leq 31$, όπως αναφέρονται στο [72]. Στη δεύτερη στήλη αναπαριστούμε το πρωταρχικό πολυώνυμο

$$f(z) = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1} + c_n z^n, \qquad \text{με } c_n = 1$$

με το διάνυσμα $\begin{pmatrix} c_0 & c_1 & \cdots & c_n \end{pmatrix}$. Π.χ. για $n = 3$, έχουμε το πρωταρχικό πολυώνυμο $f(z) = 1 + z + z^3$.

Πίνακας Α.1. Πρωταρχικά πολυώνυμα στο $\mathbb{F}_2$ βαθμού n, όπου $2 \leq n \leq 31$

n	$c_0\, c_1 \cdots c_n$	n	$c_0\, c_1 \cdots c_n$
2	111	17	100100000000000001
3	1101	18	110010000000000001
4	11001	19	110010000000000001
5	100101	20	100100000000000000001
6	1100001	21	101000000000000000001
7	11000001	22	110000000000000000001
8	101110001	23	100001000000000000000001
9	1000100001	24	110110000000000000000001
10	10010000001	25	100100000000000000000000001
11	101000000001	26	111000100000000000000000001
12	1100101000001	27	111001000000000000000000001
13	11011000000001	28	100100000000000000000000000001
14	110101000000001	29	101000000000000000000000000001
15	1100000000000001	30	110010100000000000000000000001
16	10110100000000001	31	100100000000000000000000000000001

Β Αθροιστικές

Οι αθροιστικές, όπως και οι ροπές, ενός σήματος παρέχουν πληροφορία ανωτέρας τάξης στο πεδίο του χρόνου και των συχνοτήτων αντίστοιχα. Είναι χρήσιμες στην ανάλυση και επεξεργασία σημάτων (ή ακολουθιών) που παράγονται από μη–γραμμικά συστήματα. Παρ΄ ότι οι αθροιστικές και οι ροπές παρέχουν ισοδύναμη πληροφορία, οι αθροιστικές προτιμούνται λόγω των ελκυστικών ιδιοτήτων που επιδεικνύουν [50].

Οι αθροιστικές είναι δυνατό να υπολογιστούν από τις ροπές και αντιστρόφως. Η *διαμέριση* ενός συνόλου είναι μία συλλογή από μη–κενά υποσύνολα του συνόλου, ξένα μεταξύ τους, των οποίων η ένωση δίνει το αρχικό σύνολο και ο αριθμός τους καθορίζει την τάξη της διαμέρισης.

Ας συμβολίσουμε με R_k^j το σύνολο όλων των διαμερίσεων του $\{1, 2, \ldots, k\}$ τάξης j. Η αθροιστική τάξης k υπολογίζεται από τις ροπές τάξης μικρότερης ή ίσης με k, σύμφωνα με τον ακόλουθο τύπο

$$\operatorname{cum}(z_1, \ldots, z_k) = \sum_{j=1}^{k} (-1)^{j-1} (j-1)! \sum_{R \in R_k^j} \prod_{Q \in R} \operatorname{E}(z_{i_1} \cdots z_{i_s}) \tag{B.1}$$

όπου cum και E συμβολίζουν την αθροιστική και αναμενόμενη τιμή αντίστοιχα των τυχαίων μεταβλητών. Ο ακέραιος s είναι ίσος με το πλήθος των στοιχείων του συνόλου Q και εξαρτάται τόσο από το σύνολο Q όσο και από το διαμέρισμα R. Όμοια, οι ροπές είναι δυνατό να υπολογιστούν από τις αθροιστικές ως εξής

$$\operatorname{E}(z_1 \cdots z_k) = \sum_{j=1}^{k} \sum_{R \in R_k^j} \prod_{Q \in R} \operatorname{cum}(z_{i_1}, \ldots, z_{i_s}). \tag{B.2}$$

Οι σχέσεις (B.1) και (B.2) είναι δυνατό να αποδειχτούν με τη χρήση επαγωγής. Στη συνέχεια παραθέτουμε τις αθροιστικές τάξης μικρότερης ή ίσης με τρία

$$\begin{aligned}
\operatorname{cum}(z_1) &= \operatorname{E}(z_1) \\
\operatorname{cum}(z_1, z_2) &= \operatorname{E}(z_1 z_2) - \operatorname{E}(z_1) \operatorname{E}(z_2) \\
\operatorname{cum}(z_1, z_2, z_3) &= \operatorname{E}(z_1 z_2 z_3) - \operatorname{E}(z_1) \operatorname{E}(z_2 z_3) - \operatorname{E}(z_2) \operatorname{E}(z_1 z_3) \\
&\quad - \operatorname{E}(z_3) \operatorname{E}(z_1 z_2) + 2 \operatorname{E}(z_1) \operatorname{E}(z_2) \operatorname{E}(z_3).
\end{aligned}$$

Είναι προφανές ότι έαν οι τυχαίες μεταβλητές z_1, z_2, και z_3 έχουν μέσον όρο μηδέν, τότε οι αθροιστικές μέχρι τρίτης τάξης είναι ίσες με τις αντίστοιχες

ροπές ιδίας τάξης. Η ανωτέρω παρατήρηση δεν ισχύει για τις αθροιστικές τάξης μεγαλύτερης του τρία. Πράγματι, έαν ορίσουμε

$$\operatorname{cum}^*(z_1, z_2, z_3) = \operatorname{cum}(z_1, z_2, z_3) - \frac{1}{2}\operatorname{E}(z_1)\operatorname{E}(z_2)\operatorname{E}(z_3)$$

τότε η αθροιστική τετάρτης τάξης δίνεται από τη σχέση

$$\begin{aligned}\operatorname{cum}(z_1, z_2, z_3, z_4) = {} & \operatorname{E}(z_1 z_2 z_3 z_4) - \operatorname{E}(z_1 z_2)\operatorname{E}(z_3 z_4) - \operatorname{E}(z_1 z_3)\operatorname{E}(z_2 z_4) \\ & - \operatorname{E}(z_1 z_4)\operatorname{E}(z_2 z_3) - \operatorname{E}(z_1)\operatorname{cum}^*(z_2, z_3, z_4) \\ & - \operatorname{E}(z_2)\operatorname{cum}^*(z_1, z_3, z_4) - \operatorname{E}(z_3)\operatorname{cum}^*(z_1, z_2, z_4) \\ & - \operatorname{E}(z_4)\operatorname{cum}^*(z_1, z_2, z_3)\end{aligned}$$

και έαν οι τυχαίες μεταβλητές z_1, z_2, z_3, και z_4 έχουν μέσον όρο μηδέν, τότε μόνον οι τελευταίοι τέσσερις όροι μηδενίζονται.

Βιβλιογραφία

[1] H. L. Althaus and R. J. Leake, "Inverse of a finite–field Vandermonde matrix," *IEEE Transactions on Information Theory*, vol. IT-15, pp. 173, Jan. 1969.

[2] D. Augot and N. Sendrier, "Idempotents and the BCH bound," *IEEE Transactions on Information Theory*, vol. IT-40, pp. 204–207, Jan. 1994.

[3] F. L. Bauer, *Decrypted secrets*. Berlin, Germany: Springer–Verlag, 1997.

[4] B. Benjauthrit and I. S. Reed, "Galois switching functions and their applications," *IEEE Transactions on Computers*, vol. C-25, pp. 78–86, Jan. 1976.

[5] E. R. Berlekamp, *Algebraic coding theory*. New York: McGraw–Hill, 1968.

[6] J. Bernasconi and C. G. Günther, "Analysis of a nonlinear feedforward logic for binary sequence generators," *Advances in Cryptology–EUROCRYPT '85*, pp. 161–166. Berlin, Germany: Springer–Verlag, 1985.

[7] A. Beutelspacher and U. Rosenbaum, *Projective geometry*. Cambridge, U.K.: Cambridge University Press, 1998.

[8] S. R. Blackburn, "A generalization of the discrete Fourier transform: determining the minimal polynomial of a periodic sequence," *IEEE Transactions on Information Theory*, vol. IT-40, pp. 1702–1704, Sep. 1994.

[9] R. E. Blahut, *Theory and practice of error control codes*. Reading, MA: Addison–Wesley, 1983.

[10] R. E. Blahut, *Fast algorithms for digital signal processing.* Reading, MA: Addison–Wesley, 1985.

[11] K. Brincat, F. C. Piper, and P. R. Wild, "Stream ciphers and correlation," *Difference sets, sequences, and their correlation properties* (A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, ed.), pp. 17–44. NATO Science Series, Series C: Mathematical and Physical Sciences, vol. 542. The Netherlands: Kluwer Academic Publishers, 1999.

[12] A. H. Chan and R. A. Games, "On the quadratic spans of de Bruijn sequences," *IEEE Transactions on Information Theory*, vol. IT-36, pp. 822–829, Jul. 1990.

[13] U. Cheng, "On the continued fractions and Berlekamp's algorithm," *IEEE Transactions on Information Theory*, vol. IT-30, pp. 541–544, May 1984.

[14] M. Cohn and A. Lempel, "On fast m–sequence transforms," *IEEE Transactions on Information Theory*, vol. IT-23, pp. 135–137, Jan. 1977.

[15] T. W. Cusick, C. Ding, and A. Renvall, *Stream ciphers and number theory.* North–Holland Mathematical Library, vol. 55. Amsterdam, Netherlands: Elsevier Science, 1998.

[16] J. Daemen, *Cipher and hash function design strategies based on linear and differential cryptanalysis.* Ph.D. Thesis. Leuven, Belgium: Department of Electrical Engineering, Katholieke Universiteit Leuven, 1995.

[17] D. E. Denning, *Cryptography and data security.* Reading, MA: Addison–Wesley, 1982.

[18] C. Ding, "Lower bounds on the weight complexity of cascaded binary sequences," *Advances in Cryptology–AUSCRYPT '90*, pp. 39–43. Berlin, Germany: Springer–Verlag, 1991.

[19] C. Ding, G. Xiao, and W. Shan, *The stability theory of stream ciphers.* Lecture Notes in Computer Science, vol. 561. Berlin, Germany: Springer–Verlag, 1991.

[20] H. Dobbertin, "Another proof of Kasami's theorem," *Designs, Codes, and Cryptography*, vol. 17, pp. 177–180, 1999.

[21] J. L. Dornstetter, "On the equivalence between Berlekamp's and Euclid's algorithms," *IEEE Transactions on Information Theory*, vol. IT-33, pp. 428–431, May 1987.

[22] P. Eyekoff, *System identification, parameter and state estimation.* New York: Wiley, 1974.

[23] H. J. Fell, "Linear complexity of transformed sequences," *International Symposium on Coding Theory and Applications – EUROCODE '90*, pp. 205–214. Berlin, Germany: Springer–Verlag, 1990.

[24] G. L. Feng and K. K. Tzeng, "A generalization of the Berlekamp–Massey algorithm for multisequence shift register synthesis with applications to decoding cyclic codes," *IEEE Transactions on Information Theory*, vol. IT-37, pp. 1274–1287, Sep. 1991.

[25] W. Ford and M. S. Baum, *Secure electronic commerce: building the infrastructure for digital signatures and encryption.* Cambridge, U.K.: Prentice–Hall, 1997.

[26] S. A. Fredricsson, "Pseudo–randomness properties of binary shift register sequences," *IEEE Transactions on Information Theory*, vol. IT-21, pp. 115–120, Jan. 1975.

[27] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Transactions on Information Theory*, vol. IT-29, pp. 144–146, Jan. 1983.

[28] G. Gatt and N. Kalouptsidis, "Identification of discrete–time state affine state space models using cumulants," *Automatica*, vol. 38, no. 10, pp. 1663–1681, Oct. 2002.

[29] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Transactions on Information Theory*, vol. IT-13, pp. 619–621, 1967.

[30] R. Gold, "Maximal recursive sequences with 3–valued recursive cross-correlation functions," *IEEE Transactions on Information Theory*, vol. IT-14, pp. 154–156, Jan. 1968.

[31] R. M. Goldstein and N. Zierler, "On trinomial recurrences," *IEEE Transactions on Information Theory*, vol. IT-14, pp. 150–151, Jan. 1968.

[32] J. D. Golić, "On the linear complexity of functions of periodic GF(q) sequences," *IEEE Transactions on Information Theory*, vol. IT-35, pp. 69–75, Jan. 1989.

[33] S. W. Golomb, *Shift register sequences*. San Francisco, CA: Holden–Day, 1967.

[34] S. W. Golomb, "On the classification of balanced binary sequences of period $2^n - 1$," *IEEE Transactions on Information Theory*, vol. IT-26, pp. 730–732, Nov. 1980.

[35] S. W. Golomb and G. Gong, "Periodic binary sequences with the trinomial property," *IEEE Transactions on Information Theory*, vol. IT-45, pp. 1276–1279, May 1999.

[36] S. W. Golomb, "Cyclic Hadamard difference sets – constructions and applications," *Sequences and Their Applications Conference Proceedings* (C. Ding, T. Helleseth, and H. Niederreiter, ed.), pp. 39–48. Series in Discrete Mathematics and Theoretical Computer Science. Berlin, Germany: Springer–Verlag, May 1999.

[37] G. Gong, *Sequence analysis*. Lecture Notes for CO739x. Waterloo, Canada: Department of Combinatorics and Optimization, University of Waterloo, 1999.

[38] G. C. Goodwin, "Optimal input signals for nonlinear system identification," *Proceedings of the IEE*, vol. 118, no. 7, pp. 922–926, 1971.

[39] G. C. Goodwin and R. L. Payne, *Dynamic system identification: experiment design and data analysis*. New York: Academic Press, 1977.

[40] R. Göttfert and H. Niederreiter, "On the linear complexity of products of shift–register sequences," *Advances in Cryptology–EUROCRYPT '93*, pp. 151–158. Berlin, Germany: Springer–Verlag, 1993.

[41] R. Göttfert and H. Niederreiter, "On the minimal polynomial of the product of linear recurring sequences," *Finite Fields and their Applications*, vol. 1, pp. 204–218, Apr. 1995.

[42] E. J. Groth, "Generation of binary sequences with controllable complexity," *IEEE Transactions on Information Theory*, vol. IT-17, pp. 288–296, May 1971.

[43] T. Helleseth, "Some results about the crosscorrelation function between two maximal linear sequences," *Discrete Mathematics*, vol. 16, pp. 209–232, 1976.

[44] T. Helleseth, "On the crosscorrelation of m–sequences and related sequences with ideal autocorrelation," *Sequences and Their Applications Conference Proceedings* (T. Helleseth, P. V. Kumar, and K. Yang, ed.), pp. 34–45. Series in Discrete Mathematics and Theoretical Computer Science. Berlin, Germany: Springer–Verlag, May 2001.

[45] T. Herlestam, "On functions of linear shift register sequences," *Advances in Cryptology–EUROCRYPT '85*, pp. 119–129. Berlin, Germany: Springer–Verlag, 1985.

[46] K. Imamura and W. Yoshida, "A simple derivation of the Berlekamp–Massey algorithm and some applications," *IEEE Transactions on Information Theory*, vol. IT-33, pp. 146–150, Jan. 1987.

[47] International Telecommunication Union, *Public key and attribute certificate frameworks*. Series X: Data Networks and Open System Communications – Directory, Recommendation, Mar. 2000.

[48] N. Kalouptsidis and M. Manolarakis, "Sequences of linear feedback shift registers with nonlinear feedforward logic," *Proceedings of the IEE*, vol. 130, pp. 174–176, Sep. 1983.

[49] N. Kalouptsidis and S. Theodoridis, *Adaptive system identification and signal processing algorithms.* Series in Accoustics, Speech and Signal Processing. Cambridge, U.K.: Prentice–Hall, 1993.

[50] N. Kalouptsidis, *Signal processing systems.* Series in Telecommunications and Signal Processing. New York: Wiley, 1996.

[51] N. Kalouptsidis, N. Kolokotronis, and P. Rizomiliotis, "Analysis and design of symmetric cryptographic algorithms," presented at the *1st Conference on Cyberspace Security and Hacking*, Oct. 8–9, 2001, Athens, Greece.

[52] J. B. Kam and G. I. Davida, "Structured design of substitution–permutation encryption networks," *IEEE Transactions on Computers*, vol. C-28, pp. 747–753, Oct. 1979.

[53] T. Kasami, "Weight distribution of Bose–Chaudhuri–Hocquenghem codes," *Key papers in the development of coding theory* (E. R. Berlekamp, ed.), New York: IEEE Press, 1974.

[54] C. Kaufman, R. Perlman and M. Speciner, *Network security: private communication in a public world.* Series in Computer Networking and Distributed Systems. Cambridge, U.K.: Prentice–Hall, 1995.

[55] A. M. Kerdock, F. J. MacWilliams, and A. M. Odlyzko, "A new theorem about the Mattson–Solomon polynomial and some applications," *IEEE Transactions on Information Theory*, vol. IT-20, pp. 85–89, Jan. 1974.

[56] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 732–736, Nov. 1976.

[57] S. Klein and S. Yasui, "Nonlinear systems analysis with non–Gaussian white stimuli: general basis functionals and kernels," *IEEE Transactions on Information Theory*, vol. IT-25, pp. 495–500, Jul. 1979.

[58] D. E. Knuth, *The art of computer programming, vol. 2.* Reading, MA: Addison–Wesley, 1998.

[59] N. Koblitz, *Algebraic aspects of cryptography.* Series in Algorithms and Computation in Mathematics, vol. 3. Berlin, Germany: Springer–Verlag, 1998.

[60] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "First–order optimal approximation of binary sequences," *Sequences and Their Applications Conference Proceedings* (T. Helleseth, P. V. Kumar, and K. Yang, ed.), pp. 242–256. Series in Discrete Mathematics and Theoretical Computer Science. Berlin, Germany: Springer–Verlag, May 2001.

[61] N. Kolokotronis, C. Margaritis, P. Papadopoulou, P. Kanellis, and D. Martakos, "An integrated approach for securing electronic transactions over the Web," *Benchmarking International Journal*, vol. 9, no. 2, pp. 166–181. Bradford, U.K.: MCB University Press, 2002.

[62] N. Kolokotronis, G. Gatt, and N. Kalouptsidis, "On the generation of sequences simulating higher order white noise for system identification," presented at the *11th European Signal Processing Conference*, Sep. 3–6, 2002, Toulouse, France.

[63] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Transactions on Information Theory*, vol. IT-48, pp. 2758–2764, Oct. 2002.

[64] N. Kolokotronis and N. Kalouptsidis, "On the linear complexity of nonlinearly filtered PN–sequences," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 3047–3059, Nov. 2003.

[65] N. Kolokotronis, G. Gatt, and N. Kalouptsidis, "On the generation of sequences simulating higher order white noise for system identification," accepted for publication in *Signal Processing.* Amsterdam, Netherlands: Elsevier Science.

[66] P. Koukoulas, *Identification of Volterra systems using higher order statistics.* Ph.D. Thesis. Athens, Greece: Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, 1997.

[67] P. Koukoulas and N. Kalouptsidis, "Third order Volterra system identification," *ICASSP Proceedings*, pp. 2405–2408, Munich, Germany, 1997.

[68] P. Koukoulas and N. Kalouptsidis, "Second order Volterra system identification," *IEEE Transactions on Signal Processing*, vol. 48, pp. 3574–3577, Dec. 2000.

[69] P. V. Kumar, "The partial–period correlation moments of arbitrary binary sequences," *IEEE Global Telecommunications Conference Proceedings*, pp. 499–503, Dec. 1985.

[70] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k–error linear complexity," *IEEE Transactions on Information Theory*, vol. IT-46, pp. 694–698, Mar. 2000.

[71] A. Lempel, "Analysis and synthesis of polynomials and sequences over GF(2)," *IEEE Transactions on Information Theory*, vol. IT-17, pp. 297–303, May 1971.

[72] R. Lidl and H. Niederreiter, *Finite fields*. Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge, U.K.: Cambridge University Press, 1996, 2nd ed.

[73] S. Lin and D. J. Costello, *Error control coding: fundamentals and applications*. Series in Computer Applications in Electrical Engineering. Cambridge, U.K.: Prentice–Hall, 1982.

[74] J. H. Lindholm, "An analysis of the pseudo–randomness properties of subsequences of long m–sequences," *IEEE Transactions on Information Theory*, vol. IT–14, pp. 569–576, Jul. 1968.

[75] I. G. MacDonald, *Symmetric functions and Hall polynomials*. New York: Oxford University Press, 2nd ed., 1995.

[76] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*. North–Holland Mathematical Library. Amsterdam, Netherlands: Elsevier Science, 1978.

[77] C. Margaritis, N. Kolokotronis, P. Papadopoulou, P. Kanellis, and D. Martakos, "A model and implementation guidelines for information security strategies in Web environments," *Advances in Information Security Management & Small Systems Security* (J. Eloff, L. Labuschagne, R. Solms, and G. Dhillon, ed.), pp. 13–34. Series in International Federation for Information Processing, vol. 200. Boston: Kluwer Academic Publishers, 2001.

[78] P. Z. Marmarelis and V. Z. Marmarelis, *Analysis of physiological systems: The White Noise Approach.* New York: Plenum Press, 1978.

[79] J. L. Massey and R. W. Liu, "Equivalence of nonlinear shift–registers," *IEEE Transactions on Information Theory*, vol. IT-10, pp. 378–379, Oct. 1964.

[80] J. L. Massey, "Shift–register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. IT-15, pp. 122–127, Jan. 1969.

[81] J. L. Massey and S. Serconek, "A Fourier transform approach to the linear complexity of nonlinearly filtered sequences," *Advances in Cryptology–CRYPTO '94*, pp. 332–340. Berlin, Germany: Springer–Verlag, 1994.

[82] J. L. Massey and S. Serconek, "Linear complexity of periodic sequences: a general theory," *Advances in Cryptology–CRYPTO '96*, pp. 358–371. Berlin, Germany: Springer–Verlag, 1996.

[83] J. Mendel, "Tutorial on higher–order statistics (spectra) in signal processing and system theory: theoretical results and some applications," *Proceedings of the IEEE*, vol. 79, no 3, pp. 278–305, Mar. 1991.

[84] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography.* New York: CRC Press, 1997.

[85] National Institute of Standards and Technology, "Data encryption standard," *Federal Information Processing Standards*, Publication 46–2, U.S. Department of Commerce, Dec 1993.

[86] National Institute of Standards and Technology, "DES modes of operation," *Federal Information Processing Standards*, Publication 81, U.S. Department of Commerce, Dec 1980.

[87] J. Nechvatal, "Public key cryptography," *Contemporary cryptology: the science of information integrity* (G. J. Simmons, ed.), pp. 177–288. New York: IEEE Press, 1992.

[88] R. K. Nichols, *ICSA guide to cryptography.* New York: McGraw–Hill, 1999.

[89] R. D. Nowak and B. D. van Veen, "Random and pseudorandom inputs for Volterra filter identification," *IEEE Transactions on Signal Processing*, vol. 42, pp. 2124–2135, Aug. 1994.

[90] R. Oppliger, "Internet security: firewalls and beyond," *Communications of the ACM*, vol. 40, pp. 92–102, May 1997.

[91] V. Y. Pan, "New techniques for the computation of linear recurrence coefficients," *Finite Fields and their Applications*, vol. 6, pp. 93–118, Jan. 2000.

[92] K. G. Paterson and P. J. G. Lothian, "Bounds on partial correlations of sequences," *IEEE Transactions on Information Theory*, vol. IT-44, pp. 1164–1175, May 1998.

[93] V. S. Pless and W. C. Huffman, *Handbook of coding theory*, vol. I. Amsterdam, Netherlands: Elsevier Science, 1998.

[94] V. S. Pless and W. C. Huffman, *Handbook of coding theory*, vol. II. Amsterdam, Netherlands: Elsevier Science, 1998.

[95] M. Y. Rhee, *Cryptography and secure communications.* New York: McGraw–Hill, 1994.

[96] M. Y. Rhee, *CDMA cellular mobile communications & network security.* Cambridge, U.K.: Prentice–Hall, 1998.

[97] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "Construction of sequences with four–valued autocorrelation from GMW sequences,"

IEEE International Symposium on Information Theory Proceedings, pp. 183, Jul. 2002.

[98] P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "On the quadratic span of binary sequences," presented at the *IEEE International Symposium on Information Theory*, Jun. 29–Jul. 4, 2003, Yokohama, Japan.

[99] M. J. B. Robshaw, "Stream ciphers," *Technical Report TR–701*, ver. 2.0. RSA Laboratories, 1995.

[100] RSA Data Security Inc., *PKCS #6: extended–certificate syntax standard.* Technical Note, ver. 1.5, Nov. 1993.

[101] RSA Data Security Inc., *PKCS #9: selected attribute types.* Technical Note, ver. 1.1, Nov. 1993.

[102] R. A. Rueppel, *Analysis and design of stream ciphers.* Series in Communications and Control Engineering. Berlin, Germany: Springer–Verlag, 1986.

[103] R. A. Rueppel and O. J. Staffelbach, "Products of linear recurring sequences with maximum complexity," *IEEE Transactions on Information Theory*, vol. IT-33, pp. 124–131, Jan. 1987.

[104] R. A. Rueppel, "Stream ciphers," *Contemporary cryptology: the science of information integrity* (G. J. Simmons, ed.), pp. 65–134. New York: IEEE Press, 1992.

[105] W. J. Rugh, *Nonlinear system theory: the Volterra/Wiener approach.* Baltimore, MD: Johns Hopkins University Press, 1981.

[106] D. V. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences," *IEEE Transactions on Information Theory*, vol. IT-25, pp. 720–724, Nov. 1979.

[107] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proceedings of the IEEE*, vol. 68, pp. 593–619, May 1980.

[108] M. Schetzen, *The Volterra and Wiener theories of nonlinear systems.* New York: Wiley, 1980.

[109] B. Schneier, *Applied cryptography: protocols, algorithms and source code in C*. New York: Wiley, 2nd ed., 1996.

[110] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Transactions on Information Theory*, vol. IT-30, pp. 548–553, May 1984.

[111] A. Segev, J. Porra, and M. Roldan, "Internet security and the case of bank of america," *Communications of the ACM*, vol. 41, pp. 81–87, Oct. 1998.

[112] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[113] Y. Shi, *System identification with maximum length sequences and applications in brainstem auditory evoked responses*. Ph.D. Thesis. University of Wisconsin–Madison, 1990.

[114] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread spectrum communications handbook*. New York: McGraw–Hill, Revised ed., 1994.

[115] T. Soderstrom and P. Stoica, *System identification*. Cambridge, U.K.: Prentice–Hall, 1989.

[116] M. Stamp and C. F. Martin, "An algorithm for the k–error linear complexity of binary sequences with period 2^n," *IEEE Transactions on Information Theory*, vol. IT-39, pp. 1398–1401, Jul. 1993.

[117] H. Stichtenoth, *Algebraic function fields and codes*. Berlin, Germany: Springer–Verlag, 1993.

[118] E. E. Sutter, "A practical nonstochastic approach to nonlinear time–domain analysis," *Advanced methods of physiological system modeling* (V. Z. Marmarelis, ed.), University of Southern California, Los Angeles, 1987.

[119] V. Tsoulkas, P. Koukoulas, and N. Kalouptsidis, "Identification of input–output bilinear systems using cumulants," *IEEE Transactions on Signal Processing*, vol. 49, no. 11, pp. 2753–2761, Nov. 2001.

[120] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Transactions on Information Theory*, vol. IT-20, pp. 397–399, May 1974.

[121] L. R. Welch and R. A. Scholtz, "Continued fractions and Berlekamp's algorithm," *IEEE Transactions on Information Theory*, vol. IT-25, pp. 19–27, Jan. 1979.

[122] L. J. Weng, "Decomposition of m–sequences and its applications," *IEEE Transactions on Information Theory*, vol. IT-17, pp. 457–463, Jul. 1971.

[123] S. B. Wicker and V. K. Bhargava, *Reed–Solomon codes and their applications*. New York: IEEE Press, 1998.

[124] N. Zierler and J. Brillhart, "On primitive trinomials (mod 2)," *Information and Control*, vol. 13, pp. 541–554, 1968.

[125] N. Zierler, "Primitive trinomials whose degree is a Mersenne exponent," *Information and Control*, vol. 15, pp. 67–69, 1969.

[126] N. Zierler and W. H. Mills, "Products of linear recurring sequences," *Journal of Algebra*, vol. 27, pp. 147–157, 1973.

Ευρετήριο

Β

Γ

Δ

Ψ

Ορολογία

A

Αβελιανή ομάδα	Abelian group
Αθροιστική	Cumulant
Ακέραια περιοχή	Integral domain
Ακεραιότητα	Integrity
Ακολουθία μεγίστου μήκους	Maximal length sequence
Αλγεβρική δομή	Algebraic structure
Αμερόληπτος	Unbiased
Αναγκαία συνθήκη	Necessary condition
Αναγώγιμο πολυώνυμο	Reducible polynomial
Ανάγωγο πολυώνυμο	Irreducible polynomial
Ανάδραση	Feedback
Αναδρομική σχέση	Recursive relation
Αναπαράσταση ίχνους	Trace representation
Ανάστροφο πολυώνυμο	Reciprocal polynomial
Ανάστροφος πίνακας	Transpose matrix
Ανθεκτική ακολουθία	Robust sequence
Αντιμετάθεση	Permutation
Αντιμεταθετική ομάδα	Commutative group
Αντιστρέψιμος πίνακας	Non–singular matrix
Αντίστροφο στοιχείο	Inverse element
Απεικόνιση	Mapping
Απλό κείμενο	Plaintext
Αποκωδικοποίηση	Decoding
Αποτύπωμα	Hash value

Άρτιος αριθμός	Even number
Αρχή εγγραφής	Registration authority
Αρχή πιστοποίησης	Certification authority
Αρχή πολιτικών πιστοποίησης	Policy certification authority
Ασύμμετρος αλγόριθμος	Asymmetric algorithm
Αυθεντικότητα	Authentication
Αυτοσυσχέτιση	Autocorrelation
Αφινικός	Affine

Β

Βαθμίδα καταχωρητή	Register stage
Βάρος	Weight
Βασική αρχή πιστοποίησης	Root certification authority
Βέλτιστη φάση	Optimal shift

Γ

Γεννήτορας τρέχοντος κλειδιού	Running key generator
Γεννήτορας σειριακού κλειδιού	Key–stream generator
Γραμμικά αναδρομική ακολουθία	Linear recurring sequence
Γραμμική εξάρτηση	Linear dependence
Γραμμική πολυπλοκότητα	Linear complexity
Γραμμικό κύκλωμα προσέγγισης	Approximate linear synthesizer
Γνήσια δειγματοληψία	Proper decimation/down–sampling

Δ

Δείκτης γινομένου	Product indicator
Διαδίκτυο	Internet
Διακριτός μετασχηματισμός Fourier	Discrete Fourier transform
Διαμέρισμα	Partition
Διάνυσμα	Vector
Διγραμμικό μοντέλο	Bilinear model
Διοφαντική εξίσωση	Diophantine equation
Διώνυμο	Binomial
Δυϊκός κώδικας	Dual code

E

Εκθέτης	Exponent
Ελάχιστο πολυώνυμο	Minimal polynomial
Έλεγχος δικαιωμάτων πρόσβασης	Access rights control
Εμπιστευτικότητα	Confidentiality
Εν τέλει περιοδικός	Ultimately periodic
Ενδιάμεση μνήμη	Buffer
Ένταση	Intensity
Επέκταση μερικών κλασμάτων	Partial fractions expansion
Επεκτεταμένος πίνακας	Extended matrix
Επικεφαλής κλάσης	Coset leader
Επιμεριστική ιδιότητα	Distributive property
Ετεροαθροιστική	Crosscumulant
Ετεροσυσχέτιση	Crosscorrelation

I

Ιδεατό ιδιωτικό δίκτυο	Virtual private network
Ικανή συνθήκη	Sufficient condition
Ισαπέχουσες φάσεις	Equidistant phases
Ισόβαρος	Balanced
Ισοδυναμία	Congruential equation
Ισοτιμία	Parity

K

Κανονική αλγεβρική μορφή	Algebraic normal form
Κανονική βάση	Normal basis
Κανονική κατανομή	Normal distribution
Κατάσταση	State
Καταχωρητής ολίσθησης γραμμικής ανάδρασης	Linear feedback shift register
Καταχωρητής ολίσθησης με ανάδραση	Feedback shift register
Κάτω τριγωνικός	Lower triangular
Κρυπτανάλυση	Cryptanalysis
Κρυπτογράφημα	Ciphertext
Κρυπτογραφία	Cryptography

Κυκλικά ισοδύναμος	Cyclically equivalent
Κυκλικό σύνολο διαφορών Hadamard	Cyclic Hadamard difference set
Κυκλοτομική κλάση	Cyclotomic coset
Κώδικας ελέγχου σφαλμάτων	Error control code
Κωδική λέξη	Codeword
Κωδικοποίηση	Encoding

Λ

Λίστα ανάκλησης πιστοποιητικών	Certificate revocation list
Λογική συνάρτηση	Boolean function

Μ

Μέγιστη εκτός–φάσης αυτοσυσχέτιση	Peak out–of–phase autocorrelation
Μέγιστη ετεροσυσχέτιση	Peak crosscorrelation
Μέγιστη συσχέτιση	Peak correlation
Μέγιστος κοινός διαιρέτης	Greatest common divisor
Μεταβατικότητα	Transitivity
Μεταβλητή	Variable
Μετασχηματισμός	Transform
Μη–αποποίηση	Non–repudiation
Μη–γραμμικός συνδυαστής	Nonlinear combining function
Μη–γραμμικό φίλτρο	Nonlinear filter function
Μονικό πολυώνυμο	Monic polynomial
Μονόνυμο	Monomial
Μονοπάτι πιστοποίησης	Certification path
Μοντέλο εμπιστοσύνης	Trust model

Ξ

Ξενιστής	Host

Ο

Ομάδα	Group
Ορίζουσα	Determinant
Ορίζων πολυώνυμο	Defining polynomial
Ορίζων στοιχείο	Defining element

Π

Παράγοντας	Factor
Παραγοντοποίηση	Factorization
Πεπερασμένο σώμα	Finite field
Περίμετρος ασφάλειας	Security perimeter
Περιττός αριθμός	Odd number
Πίνακας	Matrix
Πιστοποιητικό δημοσίου κλειδιού	Public key certificate
Πλήρες σύστημα υπολοίπων	Complete residue system
Πολυώνυμο ανάδρασης	Feedback polynomial
Πολυώνυμο γεννήτορας	Generating polynomial
Προ–υπολογισμός	Precomputation
Πρόκληση–απόκριση	Challenge–response
Προσεταιριστική ιδιότητα	Associative property
Προτιμητέο ζεύγος ακολουθιών	Preferred pair of sequences
Πρωταρχικό στοιχείο	Primitive element
Πρωταρχικό σώμα	Prime field
Πρώτος αριθμός	Prime number
Πύλη ασφάλειας	Firewall
Πυρήνας	Kernel

Ρ

Ροπή	Moment
Ρητή αναπαράσταση	Rational representation

Σ

Σειριακός αλγόριθμος	Stream cipher
Σημειογραφία	Notation
Συζυγείς ρίζες	Conjugate roots
Συμβολοσειρά	Run
Συμμετρικός αλγόριθμος	Symmetric algorithm
Συνάρτηση επόμενης κατάστασης	Next state function
Συνάρτηση κατακερματισμού	Hash function
Συνδυαστική	Combinatorics
Συνέλιξη	Convolution

Συνιστώσα ακολουθία	Component sequence
Συντελεστής	Coefficient
Συρρικνωμένος πίνακας	Shortened matrix
Σύστημα επικοινωνιών ευρέως φάσματος	Spread spectrum communications system

Τ

Ταξινόμηση	Classification
Ταυτοδύναμο πολυώνυμο	Idempotent polynomial
Ταυτοποίηση	Identification
Τελεστής	Operator
Τεστ καθολικότητας	Universality test
Τετραγωνικός πίνακας	Square matrix
Τμηματικός αλγόριθμος	Block cipher
Τοπικό μέγιστο	Peak
Τριώνυμο	Trinomial
Τυπική αναπαράσταση δυναμοσειράς	Formal power series representation
Τυχαίος θόρυβος	Pseudo–noise

Υ

Υποδομή δημοσίου κλειδιού	Public key infrastructure

Φ

Φάση καταγραφής	SSL record subprotocol
Φάση χειραψίας	SSL handshake subprotocol
Φράγμα	Bound

Χ

Χαρακτηριστική φάση	Characteristic phase
Χρονικά ελεγχόμενος γεννήτορας	Clock–controlled generator
Χρονο–σφραγίδα	Timestamp
Χώρος καταστάσεων	State space
Χώρος συχνοτήτων	Frequency domain

Ψ

Ψευδοτυχαία ακολουθία	Pseudorandom sequence
Ψηφιακή υπογραφή	Digital signature
Ψηφιακός φάκελος	Digital envelope