ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Τεχνικές Επεξεργασίας Σήματος στην Κρυπτογραφία

Κωνσταντίνος Α. Λιμνιώτης

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2007

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Τεχνικές Επεξεργασίας Σήματος στην Κρυπτογραφία

Κωνσταντίνος Α. Λιμνιώτης

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Νικόλαος Καλουπτσίδης, Καθηγητής ΕΚΠΑ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:

Νικόλαος Καλουπτσίδης, Καθηγητής ΕΚΠΑ
Αγγελική Αραπογιάννη, Αν. Καθηγήτρια ΕΚΠΑ
Λάζαρος Μεράκος, Καθηγητής ΕΚΠΑ

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Νικόλαος Καλουπτσίδης,
Καθηγητής ΕΚΠΑ

Αγγελική Αραπογιάννη,
Αν. Καθηγήτρια ΕΚΠΑ

Λάζαρος Μεράκος,
Καθηγητής ΕΚΠΑ

Ιωάννης Εμίρης,
Καθηγητής ΕΚΠΑ

Ευστάθιος Ζάχος,
Καθηγητής ΕΜΠ

Σέργιος Θεοδωρίδης,
Καθηγητής ΕΚΠΑ

Ηλίας Κουτσουπιάς,
Καθηγητής ΕΚΠΑ

Ημερομηνία εξέτασης 19/10/2007

Περίληψη

Η κρυπτογραφία αποτελεί τον κύριο επιστημονικό κλάδο για τη μελέτη της ασφάλειας των τηλεπικοινωνιών. Οι αλγόριθμοι ροής αποτελούν μία σημαντική κατηγορία κρυπτογραφικών αλγορίθμων, οι οποίοι χρησιμοποιούνται κυρίως σε εφαρμογές υψηλών απαιτήσεων σε ταχύτητα κρυπτογράφησης, καθώς επίσης και όταν η διαθέσιμη υπολογιστική ισχύς είναι περιορισμένη. Βασικό δομικό στοιχείο των αλγορίθμων ροής αποτελούν οι καταχωρητές ολίσθησης, με γραμμική (LFSR) ή μη γραμμική (FSR) συνάρτηση ανάδρασης. Η ασφάλεια αυτών των αλγορίθμων έγκειται σε μεγάλο βαθμό στα χαρακτηριστικά τυχαιότητας που εμφανίζει η ακολουθία του κλειδιού. Μεταξύ των διαφόρων κρυπτογραφικών κριτηρίων που χρησιμοποιούνται για τον χαρακτηρισμό μίας ακολουθίας ως ψευδοτυχαία είναι η *πολυπλοκότητα*, η οποία ορίζεται ως το μήκος του μικρότερου FSR που παράγει την ακολουθία. Ιδιαίτερα η γραμμική πολυπλοκότητα είναι πολύ σημαντική: μία κρυπτογραφική ακολουθία πρέπει να έχει υψηλή γραμμική πολυπλοκότητα προκειμένου το σύστημα να είναι ασφαλές απέναντι σε διάφορες κρυπταναλυτικές επιθέσεις, όπως ο αλγόριθμος Berlekamp-Massey (BMA). Για την παραγωγή ακολουθιών υψηλής γραμμικής πολυπλοκότητας χρησιμοποιούνται μη γραμμικές λογικές συναρτήσεις, οι οποίες εφαρμόζονται ως φίλτρα ή συνδυαστές σε έναν ή περισσότερους FSRs αντίστοιχα. Ωστόσο, η ασφάλεια του συστήματος εξαρτάται επίσης και από επί μέρους ιδιότητες αυτών των λογικών συναρτήσεων. Επιπλέον, υπάρχουν πολλά αναπάντητα ερωτήματα όσον αφορά τις σχέσεις μεταξύ των διαφόρων κρυπτογραφικών κριτηρίων μίας ακολουθίας.

Στην παρούσα διατριβή μελετώνται χαρακτηριστικά τυχαιότητας των ακολουθιών, χρησιμοποιώντας εργαλεία της θεωρίας συστημάτων. Έμφαση δίνεται στη γραμμική πολυπλοκότητα, η οποία μελετάται με χρήση των εννοιών της ελεγξιμότητας και παρατηρησιμότητας των συστημάτων παραγωγής ακολουθιών. Αναπτύσσεται μία νέα αναπαράσταση ίχνους των ακολουθιών, απόρροια της οποίας είναι ένας γενικευμένος μετασχηματισμός Fourier που περιγράφει όλες τις ακολουθίες ανεξαρτήτως περιόδου και επιτρέπει την κατασκευή ακολουθιών με οποιαδήποτε επιθυμητή τιμή για τη γραμμική πολυπλοκότητα. Επίσης, κατασκευάζεται μία νέα οικογένεια μη γραμμικών φίλτρων, η οποία γενικεύει άλλες γνωστές οικογένειες φίλτρων και παράγει ακολουθίες υψηλής γραμμικής πολυπλοκότητας.

Η διατριβή μελετά επίσης τη μη γραμμική πολυπλοκότητα, καθώς και τη σχέση της με άλλα κρυπτογραφικά κριτήρια. Αναπτύσσεται ένας νέος αναδρομικός αλγόριθμος για την εύρεση του ελάχιστου FSR που παράγει μία ακολουθία, γενικεύοντας κατά αυτόν τον τρόπο τον BMA στη μη γραμμική περίπτωση. Επιπλέον, αναδεικνύεται η σχέση της μη γραμμικής πολυπλοκότητας με την πολυπλοκότητα Lempel-Ziv. Αποδεικνύεται επίσης ένα κάτω φράγμα του λόγου συμπίεσης μίας ακολουθίας, το οποίο εξαρτάται από τη μη γραμμική πολυπλοκότητά της.

Τέλος, με δεδομένο ότι οι κρυπτογραφικές λογικές συναρτήσεις δεν πρέπει να μπορούν να προσεγγιστούν ικανοποιητικά από συναρτήσεις χαμηλού βαθμού, η εργασία μελετά το πρόβλημα εύρεσης βέλτιστων προσεγγίσεων δευτέρου βαθμού. Αναπτύσσονται αποδοτικές τεχνικές για την εύρεση αυτών των προσεγγίσεων για κατηγορία συναρτήσεων βαθμού 3 και 4, οι οποίες δεν εξαρτώνται από το πλήθος των μεταβλητών. Οι τεχνικές αυτές καθορίζουν νέες σχεδιαστικές αρχές που πρέπει να τηρούνται στην κατασκευή κρυπτογραφικών συναρτήσεων. Μελέτη γνωστών κατασκευών συναρτήσεων καταδεικνύει ύπαρξη αδυναμιών σε αυτές, λόγω μη τήρησης των παραπάνω αρχών σχεδίασης.

Θεματική περιοχή: *Κρυπτογραφία*

Λέξεις-κλειδιά: *Ακολουθίες, Αλγόριθμοι ροής, Καταχωρητής ολίσθησης με ανάδραση, Λογικές συναρτήσεις, Πολυπλοκότητα.*

Abstract

Cryptography is the study of mathematical techniques concerning aspects of telecommunication security. There exist several types of cryptographic algorithms; amongst them, stream ciphers are widely used to provide confidentiality in environments characterized by a limited computing power or memory capacity, and the need to encrypt at high speed. Shift registers with linear (LFSR) or nonlinear (NFSR) feedback are basic building blocks in stream ciphers. The security of these systems is mainly attributed to pseudorandom characteristics of the keystreams. Amongst the measures used to characterize a sequence as pseudorandom is its *complexity*, defined as the length of the shortest FSR that generates the sequence. Especially the *linear complexity* is important for assessing resistance to cryptanalytic attacks, like the Berlekamp–Massey algorithm (BMA). Hence, sequences achieving high linear complexity are required for cryptographic systems. Such keystreams are generated by applying nonlinear Boolean functions either as filters or combiners to one or several FSRs respectively. However, resistance of cryptosystems to various attacks is also associated with properties of the Boolean functions used. Determining the connections between several cryptographic criteria of sequences remains an open problem.

In this thesis, pseudorandom properties of sequences are studied, by using system theoretic concepts. A new unified approach for analyzing the linear complexity is developed, via controllability and observability conditions applied to sequence generators. A vectorial trace representation of sequences with arbitrary period is provided, which leads to a new generalized discrete Fourier transform allowing the generation of sequences with prescribed linear complexity. Moreover, new classes of nonlinear filters are constructed, which generalize existing results and guarantee the same lower bound on the linear complexity.

Furthermore, the nonlinear complexity of binary sequences and its connections to other cryptographic criteria is studied. A new efficient recursive algorithm is presented, which produces the minimal nonlinear feedback shift register of a given sequence, thus generalizing the BMA to the nonlinear case. Connections between Lempel-Ziv complexity and nonlinear complexity are also established. Moreover, a lower bound for the Lempel-Ziv compression ratio of a given sequence is proved, which depends on its nonlinear complexity.

Finally, the well-known problem of computing best quadratic approximations of Boolean functions is studied. Efficient formulas for computing such approximations for a class of functions with degree 3 and 4 are proved. The methodology is developed upon Shannon's expansion formula. The derived method reveals new design principles for cryptographic functions. An analysis of recently proposed constructions of cryptographic functions is carried out, indicating potential weaknesses if construction parameters are not properly chosen.

Subject area: *Cryptography*

Keywords: *Boolean functions, complexity, feedback shift registers, sequences, stream ciphers.*

Στην οικογένειά μου

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κατάλογος Συμβολισμών

$\otimes$:	Γινόμενο Kronecker
$\langle a, b \rangle$:	Εσωτερικό γινόμενο των διανυσμάτων a, b
$\mathcal{A}_f$:	Σύνολο όλων των βέλτιστων γραμμικών προσεγγίσεων της συνάρτησης f
$\boldsymbol{A}^T$:	Ανάστροφος πίνακας του $\boldsymbol{A}$
$\mathbb{B}_n$:	Σύνολο λογικών συναρτήσεων n μεταβλητών
$\boldsymbol{C}$:	Πίνακας ελεγξιμότητας
$C_f(y)$:	Πολυπλοκότητα σώματος της ακολουθίας y
$C_s(y)$:	Πολυπλοκότητα συνόλου της ακολουθίας y
$c(y)$:	Μη γραμμική πολυπλοκότητα της ακολουθίας y
$\deg(f)$:	Βαθμός της λογικής συνάρτησης f
$\mathbb{F}_q$:	Πεπερασμένο σώμα q στοιχείων
$k(y)$:	Ιδιοτιμή της ακολουθίας y
$lc(y)$:	Γραμμική πολυπλοκότητα της ακολουθίας y
$LZ(y^N)$:	Πολυπλοκότητα Lempel-Ziv της ακολουθίας y
$\mathcal{NL}_f$:	Μη γραμμικότητα λογικής συνάρτησης f
$\mathcal{NL}_f^r$:	Μη γραμμικότητα βαθμού r λογικής συνάρτησης f
$\mathcal{NQ}_f$:	Μη γραμμικότητα δευτέρου βαθμού της λογικής συνάρτησης f
$\mathrm{ord}(f)$:	Τάξη του πολυωνύμου f
$\boldsymbol{J}_\alpha$	Jordan μπλοκ, με διαγώνιο στοιχείο το α
$\boldsymbol{O}$:	Πίνακας παρατηρησιμότητας
$\mathcal{Q}_f$:	Σύνολο όλων των βέλτιστων προσεγγίσεων δευτέρου βαθμού της συνάρτησης f
$\mathfrak{R}(r, n)$:	Δυαδικός Reed-Muller κώδικας τάξης r

$\mathrm{rank}(\boldsymbol{A})$:	Βαθμός του πίνακα $\boldsymbol{A}$
tr :	Συνάρτηση ίχνους
$\mathrm{wt}(e)$:	Βάρος Hamming της δυαδικής αναπαράστασης του ακεραίου e
$\mathrm{wt}(f)$:	Βάρος Hamming της λογικής συνάρτησης f
y_i^j :	Υπακολουθία $y_i y_{i+1} \dots y_j$ της y
y^N :	Ακολουθία $y_0 y_1 \dots y_{N-1}$ πεπερασμένου μήκους N
y_{opt}^s :	$s-$βέλτιστη ακολουθία
λ_f :	Βέλτιστη γραμμική προσέγγιση της συνάρτησης f
ξ_f :	Βέλτιστη τετραγωνική προσέγγιση της συνάρτησης f
ρ_{opt}^s :	Λόγος συμπίεσης μίας $s-$βέλτιστης ακολουθίας
ρ_y :	Λόγος συμπίεσης της ακολουθίας y
$\widehat{\chi}_f(a)$:	Τιμή του μετασχηματισμού Walsh της συνάρτησης f στη θέση a

Ακρωνύμια

AES	Advanced Encryption Standard
ANF	Algebraic Normal Form
BMA	Berlekamp-Massey Algorithm
DAWG	Directed Acyclic Word Graph
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DNF	Disjunctive Normal Form
ESOP	Exclusive-or Sum Of Products
FSR	Feedback Shift Register
GDFT	Generalized Discrete Fourier Transform
KMP	Knuth-Morris-Pratt algorithm
LFSR	Linear Feedback Shift Register
LZ78	Lempel-Ziv compression algorithm - version 1978
NIST	National Institute of Standards and Technology
SPN	Substitution-Permutation Network

Πρόλογος

Θα ήθελα να εκφράσω τις πιο θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή μου κ. Ν. Καλουπτσίδη, Καθηγητή του Πανεπιστημίου Αθηνών, για τη συνεχή καθοδήγησή του, την αδιάκοπη ενθάρρυνσή του και τον ενθουσιασμό που μου ενέπνεε. Χάρη στην επιστημονική του κατάρτιση και στον ερευνητικό του ζήλο γνώριζα πάντα ότι κάθε συζήτηση μαζί του θα μου άνοιγε νέους δρόμους και θα μου ενίσχυε τον ενθουσιασμό. Για την επιστημονική στήριξη και τις γνώσεις που μου μετέδωσε όλα αυτά τα χρόνια, για τις εποικοδομητικές επιστημονικές μας συζητήσεις και τις παροτρύνσεις του να προσπαθώ για το καλύτερο, αλλά και για το ότι δίπλα του απέκτησα πιο δημιουργικό τρόπο σκέψης, του οφείλω τα μέγιστα.

Ευχαριστώ επίσης ολόθερμα την κ. Α. Αραπογιάννη, Αν. Καθηγήτρια του Πανεπιστημίου Αθηνών, μέλος της τριμελούς συμβουλευτικής επιτροπής, για την ερευνητική συνεργασία που είχαμε σε όλη τη διάρκεια των μεταπτυχιακών μου σπουδών, για τη συνεχή στήριξη και ηθική συμπαράσταση που μου παρείχε, αλλά και για την ανιδιοτελή καλοσύνη της. Ευχαριστώ επίσης θερμά τον κ. Λ. Μεράκο, Καθηγητή του Πανεπιστημίου Αθηνών, που δέχτηκε να αποτελέσει μέλος της τριμελούς συμβουλευτικής επιτροπής και να αξιολογήσει την υποβαλλόμενη εργασία.

Ευχαριστώ θερμά τους κ. Ι. Εμίρη, Καθηγητή του Πανεπιστημίου Αθηνών, Ε. Ζάχο, Καθηγητή του Εθνικού Μετσόβιου Πολυτεχνείου, Σ. Θεοδωρίδη, Καθηγητή του Πανεπιστημίου Αθηνών, και Η. Κουτσουπιά, Καθηγητή του Πανεπιστημίου Αθηνών, που δέχτηκαν να συμμετάσχουν στην επταμελή μου εξεταστική επιτροπή.

Θα ήθελα να εκφράσω ένα πολύ μεγάλο ευχαριστώ στον Δρ. Ν. Κολοκοτρώνη για την άψογη συνεργασία που είχαμε και την πολύ σημαντική βοήθεια που μου προσέφερε απλόχερα, η οποία σε πολλές στιγμές υπήρξε καταλυτική. Έμαθα πολλά από τη συνεργασία μαζί του, την εργατικότητα και μεθοδικότητά του, καθώς και από τις πολύωρες γόνιμες συζητήσεις μας. Τον ευχαριστώ ιδιαίτερα για το ενδιαφέρον και τη θέρμη που επέδειξε. Ευχαριστώ επίσης θερμά τον Δρ. Π. Ριζομιλιώτη για τη βοήθειά του και για τις πολλές ανταλλαγές απόψεων που είχαμε πάνω σε ερευνητικά θέματα. Είμαι ιδιαίτερα χαρούμενος που είχα την τύχη να

συνεργαστώ μαζί τους.

Ευχαριστώ θερμά όλους τους φίλους συνεργάτες και υποψήφιους διδάκτορες στο εργαστήριο Επεξεργασίας Σήματος και στο εργαστήριο Μικροηλεκτρονικής όπου και φιλοξενήθηκα, οι οποίοι δημιούργησαν ένα ιδανικό κλίμα εργασίας και ένα πολύ ευχάριστο κλίμα παρέας.

Ένα μεγάλο ευχαριστώ οφείλω σε όλους τους φίλους μου οι οποίοι με ενθάρρυναν διαρκώς σε αυτή την προσπάθεια. Ένα ιδιαίτερο ευχαριστώ θα ήθελα να απευθύνω στους φίλους μου Δρ. Σ. Στεργίου και υπ. διδάκτορα Ν. Φραγκιαδάκη για την αδιάκοπη στήριξή τους όλα τα χρόνια και για τις αμέτρητες συζητήσεις μας, πολλές εκ των οποίων υπερατλαντικές, που πάντα μου αναπτέρωναν το ηθικό.

Τέλος, θα ήθελα να εκφράσω ένα πολύ μεγάλο ευχαριστώ αλλά και την ευγνωμοσύνη μου σε όλη την οικογένειά μου για την ηθική και υλική συμπαράσταση που μου προσέφεραν όλα τα χρόνια των σπουδών μου.

Η παρούσα διδακτορική διατριβή αποτελεί υποέργο του προγράμματος: "Ηράκλειτος: Υποτροφίες έρευνας με προτεραιότητα στην βασική έρευνα". Το Πρόγραμμα "ΗΡΑΚΛΕΙΤΟΣ" συγχρηματοδοτείται από το Ευρωπαϊκό Κοινοτικό Ταμείο (75%) και από Εθνικούς Πόρους (25%). The Project "HRAKLEITOS" is co-funded by the European Social Fund (75%) and National Resources (25%).

Κεφάλαιο 1

Εισαγωγή

> The last thing one knows when writing a book is what to put first.
>
> *Blaise Pascal*

Η κρυπτογραφία, ως ο κλάδος που άπτεται ζητημάτων ασφάλειας των επικοινωνιών, έχει μία πλούσια ιστορία πολλών ετών: ξεκινάει με την εμφάνιση πρωτόλειων μορφών κρυπτογράφησης, που βασίζονται σε απλές αντικαταστάσεις των συμβόλων του μεταδιδόμενου μηνύματος, και συνεχίζεται μέχρι σήμερα όπου υπάρχει πληθώρα σύνθετων, διαρκώς εξελισσόμενων, αλγορίθμων κρυπτογράφησης. Ιδιαίτερα στις τελευταίες δεκαετίες, η ραγδαία άνθηση των τηλεπικοινωνιών (με κυριότερο εκφραστή αυτής το διαδίκτυο) έχει γιγαντώσει την ανάγκη για τη διασφάλιση του απορρήτου των επικοινωνιών, κάτι το οποίο καθιστά την κρυπτογραφία αντικείμενο έντονης ερευνητικής δραστηριότητας.

Η σημερινή μορφή των κρυπτογραφικών συστημάτων έχει καθοριστεί σε πολύ μεγάλο βαθμό από δύο, κεφαλαιώδους σημασίας για την κρυπτογραφία και τις επικοινωνίες γενικότερα, επιστημονικές εργασίες [72, 126], που δημοσιεύτηκαν στα 1883 και 1949 αντίστοιχα. Στην πρώτη, ο Kerchoffs έθεσε τη βασική σχεδιαστική αρχή που έκτοτε διέπει κάθε κρυπτογραφικό σύστημα, σύμφωνα με την οποία η ασφάλεια ενός συστήματος πρέπει να έγκειται *μόνο* στη μυστικότητα του κλειδιού και να μην εξαρτάται από τη μυστικότητα του αλγορίθμου κρυπτογράφησης. Η δεύτερη εργασία ανήκει στο θεμελιωτή της Θεωρίας Πληροφορίας Claude Shannon. Στην εργασία αυτή η κρυπτογραφία μετατρέπεται σε αυστηρό επιστημονικό πεδίο, όπου ορίζεται η έννοια του κρυπτοσυστήματος και η απόλυτη ασφάλεια. Η εργασία αυτή του Shannon αποτέλεσε ισχυρή κινητήρια δύναμη για την ταχεία εξέλιξη της έρευνας στο χώρο της κρυπτογραφίας, η οποία έλαβε χώρα στο δεύτερο μισό του εικοστού αιώνα και συνεχίζεται μέχρι σήμερα. Όλοι οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται υπό το πρίσμα

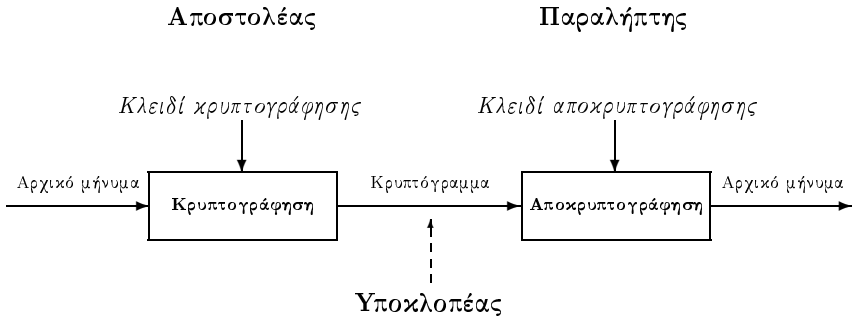
των εννοιών που εισήγαγε ο Shannon. Σημαντική τομή επίσης στο χώρο της κρυπτογραφίας αποτέλεσε η εργασία των Diffie-Hellman το 1976 [29], όπου προτάθηκε μία διαφορετική τεχνική κρυπτογράφησης που καλείται *κρυπτογραφία δημοσίου κλειδιού*, η οποία επιλύει προβλήματα που σχετίζονται τόσο με την ασφαλή ανταλλαγή του κλειδιού όσο και με την πιστοποίηση της ταυτότητας των χρηστών.

Στην παρούσα διατριβή μελετώνται βασικά δομικά συστατικά σύγχρονων κρυπτογραφικών συστημάτων, με απώτερο στόχο τόσο την παραγωγή νέων μεθόδων για τον ποιοτικό χαρακτηρισμό τους όσο και την κατασκευή συστημάτων με καλά κρυπτογραφικά χαρακτηριστικά. Έμφαση δίνεται στη μελέτη, ανάλυση και κατασκευή κρυπτογραφικών ακολουθιών οι οποίες, εφόσον αποτελούν το μυστικό κλειδί στους αλγορίθμους κρυπτογράφησης, πρέπει να εμφανίζουν υψηλή *τυχαιότητα*. Μελετώνται επίσης ιδιότητες λογικών συναρτήσεων που χρησιμοποιούνται σε κρυπτογραφικούς αλγορίθμους, αναδεικνύοντας νέα κριτήρια που πρέπει να λαμβάνονται υπ' όψιν στη σχεδίαση ενός τέτοιου αλγορίθμου. Τόσο η τυχαιότητα των ακολουθιών, όσο και τα καλά χαρακτηριστικά των κρυπτογραφικών λογικών συναρτήσεων, υπάγονται στις γενικότερες ιδιότητες που όρισε ο Shannon ως αναγκαίες για την ασφάλεια ενός συστήματος: κατά συνέπεια, η μελέτη αυτών είναι ιδιαίτερης σημασίας. Το ακριβές πλαίσιο στο οποίο εντάσσονται τα αποτελέσματα της διατριβής παρουσιάζεται στην ενότητα 1.4.

Για την εξαγωγή των αποτελεσμάτων της παρούσας διατριβής χρησιμοποιούνται έννοιες και μαθηματικά εργαλεία από τη θεωρία σημάτων και συστημάτων. Συγκεκριμένα, κρυπτογραφικές ιδιότητες των ακολουθιών μελετώνται μέσω του μετασχηματισμού Fourier, ενώ επίσης χρησιμοποιείται ο μετασχηματισμός Walsh για τη μελέτη κρυπτογραφικών λογικών συναρτήσεων. Τα συστήματα παραγωγής ακολουθιών περιγράφονται με χρήση εννοιών γνωστών από τη θεωρία συστημάτων, όπως η ελεγξιμότητα και η παρατηρησιμότητα. Αυτή η νέα θεώρηση παρέχει περισσότερες δυνατότητες για τη μελέτη των κρυπτογραφικών συστημάτων, καταδεικνύοντας για μία ακόμη φορά πως ο συνδυασμός πολλών ερευνητικών πεδίων είναι μία εξαιρετικά γόνιμη και αποδοτική διαδικασία.

1.1 Βασικές αρχές της κρυπτογραφίας

Με τον όρο *κρυπτογράφηση (encryption)* εννοούμε τη διαδικασία μετασχηματισμού ενός *αρχικού μηνύματος (plaintext)* σε μία νέα, ακατάληπτη μορφή που αποκαλείται *κρυπτόγραμμα (ciphertext)*, προκειμένου να μεταδοθεί μέσα από ένα δημόσιο κανάλι μετάδοσης χωρίς να μπο-



Σχήμα 1.1. Διάγραμμα ενός κρυπτογραφικού συστήματος

ρεί να το διαβάσει κανείς πλην του εξουσιοδοτημένου παραλήπτη. Η κρυπτογράφηση πρέπει να γίνεται με τρόπο τέτοιο ώστε ο παραλήπτης να μπορεί να ανασκευάσει το αρχικό μήνυμα από το λαμβανόμενο κρυπτόγραμμα - αυτή η αντίστροφη διαδικασία καλείται *αποκρυπτογράφηση (decryption)*. Στις διαδικασίες κρυπτογράφησης E και αποκρυπτογράφησης D υπεισέρχεται και μία άλλη ποσότητα, το *κλειδί (key)* K, το οποίο το γνωρίζουν μόνο οι δύο συνδιαλεγόμενοι - εν αντιθέσει με τις διαδικασίες κρυπτογράφησης/αποκρυπτογράφησης, οι οποίες είναι πλήρως γνωστές σε όλους (*Αρχή του Kerchoffs (Kerchoffs Principle)*). Το βασικό διάγραμμα ενός κρυπτογραφικού συστήματος απεικονίζεται στο Σχήμα 1.1. Αν M, C συμβολίζουν το αρχικό μήνυμα και το κρυπτόγραμμα αντίστοιχα, ενώ K_e, K_d είναι τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης, τότε ισχύουν οι ακόλουθες σχέσεις:

$$C = E_{K_e}(M), \qquad D_{K_d}(C) = M\ .$$

Από τα μέσα του 1970, η έννοια της κρυπτογραφίας έχει διευρυνθεί, έτσι ώστε μέσω της διαδικασίας της κρυπτογράφησης να επιτυγχάνονται και άλλοι στόχοι. Πιο συγκεκριμένα, έχει διατυπωθεί ο ακόλουθος ορισμός [105]:

Ορισμός 1.1. Κρυπτογραφία είναι η μελέτη των μαθηματικών τεχνικών που χρησιμοποιούνται για την εξασφάλιση, κατά τη μετάδοση ενός μηνύματος, των ακόλουθων:

- εμπιστευτικότητα (confidentiality): κανείς μη εξουσιοδοτημένος χρήστης δεν πρέπει να έχει πρόσβαση στο μεταδιδόμενο μήνυμα,
- έλεγχος ακεραιότητας των δεδομένων (data integrity): αλλοίωση των δεδομένων κατά τη μετάδοση πρέπει να γίνεται αντιληπτή στον παραλήπτη,
- πιστοποίηση ταυτότητας (authentication): ο παραλήπτης πρέπει να είναι σίγουρος για την ταυτότητα του αποστολέα ή για την προέλευση των δεδομένων που λαμβάνει.

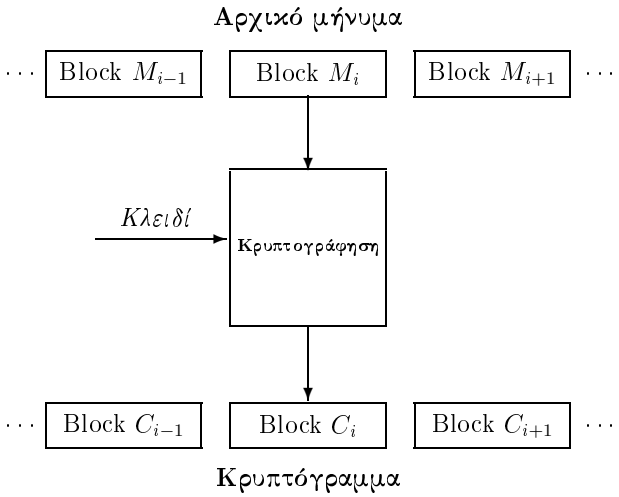
Από την άλλη πλευρά, η *κρυπτανάλυση (cryptanalysis)* ορίζεται ως η μελέτη των μαθηματικών τεχνικών που αποσκοπούν στην παραβίαση, σε ένα κρυπτογραφικό σύστημα, των παραπάνω χαρακτηριστικών. Το κρυπτόγραμμα, εφόσον μεταδίδεται μέσα από δημόσιο τηλεπικοινωνιακό κανάλι, είναι διαθέσιμο στον οποιονδήποτε, ακόμα και στον επίδοξο υποκλοπέα (Σχήμα 1.1). Η εμπιστευτικότητα σε ένα κρυπτογραφικό σύστημα παραβιάζεται αν κάποιος υποκλοπέας καταφέρει τελικά, χωρίς τη γνώση του κλειδιού, να διαβάσει το αρχικό μήνυμα (ή, ισοδύναμα, να ανακαλύψει το κλειδί αποκρυπτογράφησης). Έχουν αναπτυχθεί πολλές κρυπταναλυτικές τεχνικές για όλα τα είδη κρυπτογραφικών αλγορίθμων. Η εμφάνιση κάθε κρυπταναλυτικής τεχνικής έχει εν τέλει ως αποτέλεσμα το να καθορίζονται νέες σχεδιαστικές αρχές που πρέπει να λαμβάνονται υπ' όψιν κατά την κατασκευή κρυπτογραφικών αλγορίθμων. Κατά συνέπεια, η κρυπτογραφία και η κρυπτανάλυση συμβαδίζουν ως προς την εξέλιξή τους. Ο όρος *κρυπτολογία (cryptology)* έχει παγιωθεί, προκειμένου να συμπεριλαμβάνει ταυτόχρονα τόσο την κρυπτογραφία όσο και την κρυπτανάλυση.

Οι κρυπτογραφικοί αλγόριθμοι χωρίζονται σε δύο βασικές κατηγορίες: η πρώτη περιγράφεται με τον γενικό όρο *συμμετρική κρυπτογραφία (symmetric cryptography)*, ενώ η δεύτερη κατηγορία αλγορίθμων εντάσσεται στο γενικότερο χώρο που καλείται *κρυπτογραφία δημοσίου κλειδιού (public-key cryptography) ή ασύμμετρη κρυπτογραφία (asymmetric cryptography)*. Τα γενικά χαρακτηριστικά των αλγορίθμων κάθε κατηγορίας παρουσιάζονται στη συνέχεια.

1.2 Συμμετρικοί αλγόριθμοι κρυπτογράφησης

Στους αλγόριθμους αυτής της κατηγορίας χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση, δηλαδή $K_e = K_d$. Το κοινό αυτό κλειδί το γνωρίζουν μόνο οι συνδιαλεγόμενοι, για αυτό η εν λόγω κατηγορία αλγορίθμων συναντάται επίσης στη βιβλιογραφία με το όνομα *κρυπτογραφία ιδιωτικού κλειδιού (private key cryptography)*. Σε έναν αλγόριθμο συμμετρικού κλειδιού, οι συνδιαλεγόμενοι πρέπει να ανταλλάξουν, πριν την έναρξη της επικοινωνίας τους, το κοινό κλειδί κρυπτογράφησης/αποκρυπτογράφησης με ασφαλή τρόπο (για αυτόν το λόγο επιστρατεύονται, όπως θα δούμε στη συνέχεια, οι αλγόριθμοι δημοσίου κλειδιού).

Οι αλγόριθμοι συμμετρικού κλειδιού χωρίζονται με τη σειρά τους σε δύο σημαντικές υποκατηγορίες, στους *αλγόριθμους τμήματος (block ciphers)* και στους *αλγόριθμους ροής (stream ciphers)*.



Σχήμα 1.2. Διάγραμμα βασικής λειτουργίας ενός αλγορίθμου τμήματος

1.2.1 Αλγόριθμοι τμήματος

Σε έναν αλγόριθμο τμήματος, το αρχικό μήνυμα M χωρίζεται σε διαδοχικά τμήματα $M_1, M_2, \ldots$ ίσου μεγέθους. Κάθε τμήμα M_i κρυπτογραφείται ξεχωριστά, δίνοντας ως αποτέλεσμα ένα τμήμα του κρυπτογράμματος C_i, δηλαδή $C_i = E_K(M_i)$ για $i = 1, 2, \ldots$. Η αποκρυπτογράφηση στον παραλήπτη γίνεται επίσης κατά τμήματα, δηλαδή $M_i = D_K(C_i)$ για κάθε i. Αυτή η διαδικασία κρυπτογράφησης απεικονίζεται στο Σχήμα 1.2. Μία τυπική τιμή σήμερα για το μέγεθος του τμήματος σε αλγορίθμους αυτής της κατηγορίας είναι 128 bits. Η λειτουργία αυτών των αλγορίθμων είναι επαναληπτική, υπό την έννοια ότι το αρχικό τμήμα μηνύματος M_i κρυπτογραφείται μέσα από διάφορα διαδοχικά *στάδια (rounds)*, όπου σε κάθε στάδιο συντελείται ακριβώς ο ίδιος κρυπτογραφικός μετασχηματισμός, προκειμένου να σχηματιστεί το τελικό τμήμα κρυπτογράμματος C_i· για κάθε στάδιο, χρησιμοποιείται διαφορετικό τμήμα του κλειδιού. Η παραπάνω βασική λειτουργία των αλγορίθμων τμήματος, όπως απεικονίζεται στο Σχήμα 1.2, καλείται *λειτουργία ηλεκτρονικού κωδικοβιβλίου (Electronic CodeBook - ECB)*. Υπάρχουν και άλλοι τρόποι λειτουργίας για αυτούς τους αλγόριθμους - σημαντικός εκ των οποίων είναι *τρόπος λειτουργίας αλυσιδωτού τμήματος (Cipher Block Chaining mode - CBC)*, όπου σε κάθε τμήμα M_i του μηνύματος, πριν κρυπτογραφηθεί, προστίθεται modulo 2 το τμήμα C_{i-1}.

Σε όλους τους αλγόριθμους τμήματος υπεισέρχεται στη λειτουργία τους μία δομική μονάδα που καλείται *μονάδα αντικατάστασης (Substitution Box ή S-Box)*, η οποία πραγματοποιεί αντικαταστάσεις bits με μη γραμμικό τρόπο. Αποτέλεσμα αυτής της λειτουργίας κατά την κρυ-

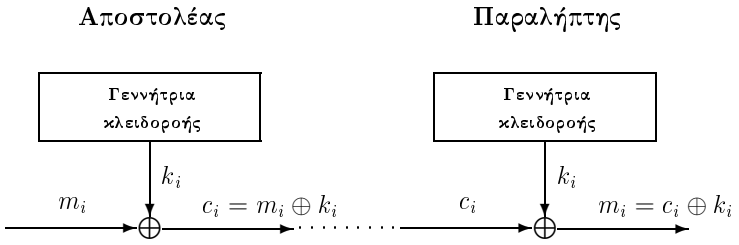
πτογράφηση είναι το να υπάρχει εν τέλει μία σύνθετη σχέση μεταξύ των bits του κλειδιού και των bits του κρυπτογράμματος. Αυτή η ιδιότητα καλείται *σύγχυση (confusion)* και έχει οριστεί από τον Shannon στο [126] ως αναγκαία συνθήκη για τον χαρακτηρισμό ενός συστήματος ως ασφαλές. Κατά συνέπεια, οι ιδιότητες του S-Box είναι πολύ σημαντικές για την ασφάλεια του αλγορίθμου στο σύνολό του. Από μαθηματική άποψη, κάθε S-box με m εισόδους και n εξόδους μπορεί να θεωρηθεί ως συνάρτηση $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ ή, ισοδύναμα, ως συλλογή n λογικών συναρτήσεων $f_i : \mathbb{F}_2^m \to \mathbb{F}_2$, $i = 1, 2, \ldots, n$ (όπου $\mathbb{F}_2 = \{0, 1\}$).

Μία άλλη σημαντική ιδιότητα που όρισε ο Shannon ως απαραίτητη για ένα κρυπτογραφικό σύστημα είναι η *διάχυση (diffusion)*, η οποία υποδηλώνει ότι ένα bit του μηνύματος πρέπει να επηρεάζει πολλά bits του κρυπτογράμματος. Για την ικανοποίηση αυτής της ιδιότητας, οι σύγχρονοι αλγόριθμοι τμήματος περιέχουν δομικές μονάδες που επιτελούν αντιμεταθέσεις bits (*μονάδες αντιμετάθεσης (Permutation-Box ή P-Box)*) ή γραμμικούς μετασχηματισμούς. Πολλοί αλγόριθμοι τμήματος βασίζονται σε αλληλουχία ενεργειών αντικατάστασης και αντιμετάθεσης, βασισμένοι ακριβώς στις θεωρητικές αρχές του Shannon: αυτοί οι αλγόριθμοι καλούνται *δίκτυα αντικατάστασης/αντιμετάθεσης (Substitution-Permutation Networks (SPN))*.

Ο πιο γνωστός και περισσότερο διαδεδομένος αλγόριθμος τμήματος είναι ο Advanced Encryption Standard (AES), γνωστός επίσης ως Rijndael [107], ο οποίος επελέγη από τον οργανισμό NIST (National Institute of Standards and Technology) ως καθολικό πρότυπο κρυπτογράφησης το 2001, αντικαθιστώντας τον προκάτοχό του DES (Data Encryption Standard) [108]. Ο AES είναι αλγόριθμος της μορφής SPN και συναντάται σε μεγάλο εύρος εφαρμογών, όπως για παράδειγμα σε συναλλαγές ηλεκτρονικού εμπορίου, σε Εικονικά Ιδιωτικά Δίκτυα και σε ασύρματες επικοινωνίες. Άλλοι γνωστοί αλγόριθμοι τμήματος είναι οι FEAL [127], IDEA [85], RC6 [119], SERPENT [4], και TWOFISH [128].

1.2.2 Αλγόριθμοι ροής

Οι αλγόριθμοι ροής κρυπτογραφούν, στη γενική περίπτωση, ξεχωριστά το κάθε bit του μηνύματος. Το πιο γνωστό μοντέλο αλγόριθμου ροής είναι το λεγόμενο *σημειωματάριο μιας χρήσης (one-time pad) ή αλγόριθμος Vernam (Vernam cipher)* [135], στον οποίο χρησιμοποιείται μία τυχαία ακολουθία bits που καλείται *κλειδοροή (keystream)* η οποία προστίθεται modulo 2 (XOR) στα bits του μηνύματος. Βασικές προϋποθέσεις για τον αλγόριθμο Vernam είναι η απόλυτη τυχαιότητα της κλειδοροής, καθώς επίσης και ότι το μέγεθός της πρέπει να είναι όσο και το μέγεθος του μηνύματος. Ο Shannon στο [126] αποδεικνύει ότι ο αλγόριθμος



Σχήμα 1.3. Διάγραμμα ενός δυαδικού προσθετικού αλγόριθμου

Vernam επιτυγχάνει *απεριόριστη ασφάλεια (perfect secrecy)*, η οποία ορίζεται με χρήση των εννοιών της εντροπίας του μηνύματος και του κρυπτογράμματος: συγκεκριμένα, *ένα σύστημα ορίζεται ως απεριόριστα ασφαλές εάν γνώση του κρυπτογράμματος δεν παρέχει καμία πληροφορία για το αρχικό μήνυμα.* Ωστόσο, παρόλα τα ιδανικά κρυπτογραφικά χαρακτηριστικά του αλγόριθμου Vernam, είναι ουσιαστικά μη πρακτικό σύστημα, αφενός λόγω του πολύ μεγάλου μήκους κλειδιού που απαιτεί (ίσου με το μέγεθος του μηνύματος, καθιστώντας την ασφαλή ανταλλαγή του πρόβλημα ίδιας δυσκολίας με αυτή της ασφαλούς ανταλλαγής του ίδιου του μηνύματος) και, αφετέρου, λόγω του ότι δεν μπορούν να υπάρξουν απόλυτα τυχαίες ακολουθίες. Παρόλα αυτά, οι αλγόριθμοι ροής σχεδιάζονται με τρόπο τέτοιο ώστε να προσομοιάζουν, κατά το δυνατόν περισσότερο, τον αλγόριθμο Vernam.

Μία μεγάλη κατηγορία αλγορίθμων ροής είναι οι *δυαδικοί προσθετικοί αλγόριθμοι (binary additive stream ciphers)*, οι οποίοι αποτελούνται από μία γεννήτρια κλειδοροής, όπου κάθε bit k_i αυτής προστίθεται στο αντίστοιχο bit m_i του αρχικού μηνύματος προκειμένου να δημιουργηθεί το bit c_i του κρυπτογράμματος. Το βασικό διάγραμμα ενός δυαδικού προσθετικού αλγόριθμου απεικονίζεται στο Σχήμα 1.3. Η γεννήτρια κλειδοροής έχει μία αρχική κατάσταση, η οποία αποτελεί το μυστικό κλειδί του αλγορίθμου: από αυτήν την αρχική κατάσταση ξεκινά τη λειτουργία της και, εν συνεχεία, περνάει σε διαδοχικές καταστάσεις, παράγοντας ένα bit της κλειδοροής σε κάθε κατάσταση. Με άλλα λόγια, κάθε γεννήτρια κλειδοροής είναι μία *μηχανή πεπερασμένων καταστάσεων (finite-state machine)* με έξοδο. Από την περιγραφή του αλγορίθμου Vernam γίνεται φανερό ότι η ασφάλεια αυτών των συστημάτων εξαρτάται από τα χαρακτηριστικά τυχαιότητας της κλειδοροής, καθώς και από την περίοδό της. Κατά συνέπεια, η σχεδίαση αυτών των συστημάτων επικεντρώνεται ουσιαστικά στην κατασκευή κατάλληλων γεννητριών κλειδοροής ώστε να παράγουν ποιοτικές κρυπτογραφικά ακολουθίες στην έξοδό τους. Γεννήτριες αυτής της μορφής βασίζονται κυρίως σε καταχωρητές ολίσθησης με ανάδραση, στους οποίους υπεισέρχονται μη γραμμικές λειτουργίες (μη γραμμικές λογικές συναρτήσεις). Αναλυτική περιγραφή τους παρατίθεται στο Κεφάλαιο 2.

Εκτός από τον δυαδικό προσθετικό αλγόριθμο, υπάρχουν και άλλες οικογένειες αλγορίθμων ροής: μία σημαντική οικογένεια αποτελούν οι λεγόμενοι *ασύγχρονοι αλγόριθμοι ροής (asynhronous stream ciphers)*, στους οποίους το κάθε bit κλειδοροής εξαρτάται επίσης, εκτός από την τρέχουσα κατάσταση της γεννήτριας, και από προηγούμενα bits του κρυπτογράμματος. Επίσης, υπάρχουν αλγόριθμοι ροής οι οποίοι κρυπτογραφούν όχι ανά bit αλλά ανά byte ή, γενικότερα, ανά λέξη (word). Σε όλες τις περιπτώσεις, τόσο τα στατιστικά χαρακτηριστικά της κλειδοροής όσο και η μαθηματική μορφή της γεννήτριας αποτελούν κρίσιμους παράγοντες για την ασφάλεια του αλγορίθμου.

Οι αλγόριθμοι ροής παρουσιάζουν πολύ μεγαλύτερη ταχύτητα από ό,τι οι αλγόριθμοι τμήματος και, ως εκ τούτου, προτιμώνται σε εφαρμογές πραγματικού χρόνου, όπως για μετάδοση ομιλίας ή video. Γενικότερα, εμφανίζονται σε ένα πολύ ευρύτερο φάσμα εφαρμογών [105]. Χαρακτηριστικά παραδείγματα αλγορίθμων ροής που χρησιμοποιούνται ευρέως είναι ο αλγόριθμος E0 στο πρωτόκολλο Bluetooth [8] για ασύρματες επικοινωνίες, ο A5/1 που χρησιμοποιείται για κρυπτογράφηση κινητών επικοινωνιών στο GSM (Global System for Mobile communications) [1], καθώς επίσης και ο RC4 που χρησιμοποιείται στα πρωτόκολλα SSH (Secure SHell) και HTTPS (HyperText Transfer Protocol Secure) [118]. Ωστόσο, δεν υπάρχει μέχρι τώρα κάποιο καθολικό πρότυπο αλγορίθμου ροής, όπως συμβαίνει για τους αλγόριθμους τμήματος. Τα τελευταία χρόνια υπάρχει έντονο ερευνητικό ενδιαφέρον για την κατασκευή ενός καθολικά αποδεκτού αλγορίθμου ροής (σε εξέλιξη βρίσκεται το σχετικό ευρωπαϊκό ερευνητικό πρόγραμμα eSTREAM [34]), λόγω της κοινής πεποίθησης ότι ένας τέτοιος αλγόριθμος μπορεί να υπερτερεί σε σχέση με τους αλγορίθμους τμήματος τόσο σε ταχύτητα στο λογισμικό (software), όσο και σε ευκολία υλοποίησης στο υλικό (hardware).

1.3 Αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού

Οι αλγόριθμοι συμμετρικού κλειδιού που παρουσιάστηκαν ανωτέρω παρουσιάζουν το σημαντικό μειονέκτημα του ότι απαιτείται η εκ των προτέρων ασφαλής ανταλλαγή του κλειδιού μεταξύ των δύο συνδιαλεγομένων. Στα πλαίσια αντιμετώπισης αυτού του προβλήματος, προτάθηκε από τους W. Diffie και M. Hellman το 1976 ένα διαφορετικό μοντέλο κρυπτογράφησης που καλείται *κρυπτογραφία δημοσίου κλειδιού ή κρυπτογραφία ασύμμετρου κλειδιού (asymmetric key cryptography)* [29]. Σε αυτή τη νέα κατηγορία αλγορίθμων, κάθε χρήστης έχει στην κατοχή του δύο κλειδιά: το ένα χρησιμοποιείται για κρυπτογράφηση και είναι ευρέως γνωστό σε όλους (δημόσιο κλειδί), ενώ το δεύτερο χρησιμοποιείται για αποκρυπτογράφηση

και δεν το γνωρίζει κανείς άλλος παρά μόνο ο κάτοχός του (ιδιωτικό κλειδί). Αν ένα μήνυμα κρυπτογραφηθεί με το δημόσιο κλειδί ενός χρήστη, τότε αποκρυπτογραφείται σωστά με χρήση του ιδιωτικού του κλειδιού. Απαραίτητη προϋπόθεση για την ασφάλεια ενός κρυπτοσυστήματος αυτής της κατηγορίας είναι ότι η γνώση του δημοσίου κλειδιού δεν πρέπει να επιτρέπει τον προσδιορισμό του ιδιωτικού κλειδιού.

Η ακριβής λειτουργία αυτών των αλγορίθμων είναι η εξής: έστω Α, Β δύο χρήστες, με δημόσιο και ιδιωτικό κλειδί του Β τα e_B, d_B αντιστοίχως. Για να στείλει ο Α το μήνυμα M στον Β, χρησιμοποιεί το δημόσιο κλειδί e_B (στο οποίο έχει πρόσβαση), οπότε παράγεται το κρυπτόγραμμα $C = E_{e_B}(M)$. Ο παραλήπτης Β με τη σειρά του αποκρυπτογραφεί το κρυπτόγραμμα C μέσω της πράξης $D_{d_B}(C) = M$. Επειδή μόνο ο Β γνωρίζει το κλειδί d_B, είναι ο μόνος ο οποίος μπορεί να αποκρυπτογραφήσει σωστά το C.

Οι αλγόριθμοι δημοσίου κλειδιού επιτρέπουν την ασφαλή ανταλλαγή μηνυμάτων, χωρίς να απαιτείται κάποια εκ των προτέρων ασφαλής ανταλλαγή του κλειδιού. Ωστόσο είναι εξαιρετικά αργοί αλγόριθμοι, γεγονός που τους καθιστά, στη γενική περίπτωση, μη κατάλληλους για κρυπτογράφηση μεγάλων μηνυμάτων. Η βασική τους λειτουργία είναι η ανταλλαγή των κλειδιών για τους συμμετρικούς αλγόριθμους κρυπτογράφησης, ενώ επίσης εφαρμόζονται για τη δημιουργία *ψηφιακών υπογραφών (digital signatures)*, οι οποίες επισυνάπτονται στα μεταδιδόμενα μηνύματα προκειμένου ο παραλήπτης να πιστοποιεί την ταυτότητα του αποστολέα. Ο πιο σημαντικός και ευρέως χρησιμοποιούμενος αλγόριθμος δημοσίου κλειδιού είναι ο RSA (Rivest-Shamir-Adleman) [120].

1.4 Αντικείμενο και δομή της διατριβής

Η παρούσα διατριβή εντάσσεται στο χώρο της συμμετρικής κρυπτογραφίας και επικεντρώνεται κυρίως στους αλγορίθμους ροής. Όπως έχει ήδη αναφερθεί νωρίτερα, οι ιδιότητες της ακολουθίας που χρησιμοποιείται ως κλειδοροή αποτελούν κρίσιμο παράγοντα για την ασφάλεια ενός συστήματος αυτής της κατηγορίας. Ως εκ τούτου, βασικός στόχος κατά τη σχεδίαση αλγορίθμων ροής είναι η παραγωγή *ψευδοτυχαίων* ακολουθιών, δηλαδή ακολουθιών των οποίων τα χαρακτηριστικά προσομοιάζουν εκείνα των πραγματικά τυχαίων ακολουθιών που λαμβάνονται από φυσικές πηγές. Υπάρχουν διάφορα μέτρα αποτίμησης της ψευδοτυχαιότητας μίας ακολουθίας: ένα από τα πλέον σημαντικά είναι η (γραμμική/μη γραμμική) *πολυπλοκότητα* της ακολουθίας, η οποία περιγράφει το μήκος του μικρότερου (γραμμικού/μη γραμμικού) καταχωρητή ολίσθησης με ανάδραση ο οποίος απαιτείται για την παραγωγή της ακολουθίας. Οι

κρυπτογραφικές ακολουθίες πρέπει να έχουν υψηλή πολυπλοκότητα (ενότητα 2.4). Ιδιαίτερα η γραμμική πολυπλοκότητα έχει μελετηθεί εκτενώς στη βιβλιογραφία· βασικό παράγοντα για αυτό αποτέλεσε ο πολύ γνωστός αναδρομικός αλγόριθμος των Berlekamp-Massey [3, 97] ο οποίος υπολογίζει αποδοτικά τον ελάχιστο γραμμικό καταχωρητή ο οποίος παράγει μία ακολουθία, ενώ χρήση του αλγορίθμου αυτού παρέχει τη δυνατότητα *πρόβλεψης ολόκληρης της ακολουθίας* από ένα μικρό γνωστό τμήμα της, εφόσον η γραμμική της πολυπλοκότητα είναι μικρή (ενότητα 2.4). Επίσης, υπάρχει μία άμεση συσχέτιση του μετασχηματισμού Fourier μίας περιοδικής ακολουθίας με τη γραμμική της πολυπλοκότητα (εφ' όσον ο μετασχηματισμός αυτός ορίζεται) [98], κάτι το οποίο αναδεικνύει διάφορες μεθόδους αντιμετώπισης ζητημάτων πολυπλοκότητας (ενότητες 2.3-2.4). Συνεπώς, ως απόρροια της μεγάλης κρυπτογραφικής της αξίας, έχουν προταθεί και χρησιμοποιούνται διάφορες μέθοδοι παραγωγής ακολουθιών υψηλής γραμμικής πολυπλοκότητας. Η πλειοψηφία αυτών των τεχνικών βασίζεται στην εφαρμογή μη γραμμικών λογικών συναρτήσεων σε έναν ή περισσότερους γραμμικούς καταχωρητές ολίσθησης με ανάδραση. Οι δύο σημαντικότερες κατηγορίες αυτών των συστημάτων είναι τα *μη γραμμικά φίλτρα* και οι *μη γραμμικοί συνδυαστές* (ενότητες 2.5.2-2.5.3). Ωστόσο, και για τις δύο περιπτώσεις, η επιλογή των λογικών συναρτήσεων είναι κρίσιμη όσον αφορά την ασφάλεια που εν τέλει θα παρέχει το σύστημα, γιατί έχουν αναπτυχθεί πολλές κρυπταναλυτικές τεχνικές που εκμεταλλεύονται συγκεκριμένες ιδιότητες στις συναρτήσεις αυτές - και, ως εκ τούτου, πρέπει να εξασφαλίζεται ότι αυτές οι ιδιότητες δεν θα υπάρχουν σε μία κρυπτογραφική λογική συνάρτηση.

Βασικός άξονας της παρούσας διατριβής είναι η πολυπλοκότητα των ακολουθιών. Σε αυτό το πλαίσιο, κατασκευάζεται μία νέα οικογένεια μη γραμμικών φίλτρων, η οποία εξασφαλίζει την παραγωγή ακολουθιών υψηλής γραμμικής πολυπλοκότητας. Η νέα αυτή μεθοδολογία σχεδίασης φίλτρων γενικεύει άλλες σημαντικές οικογένειες φίλτρων που έχουν προταθεί στη βιβλιογραφία [79, 124], ενώ επίσης δύναται να εφαρμοστεί και σε άλλες κατασκευές φίλτρων που ενδεχομένως εμφανιστούν στο μέλλον. Επιπλέον, αναλύονται πλήρως οι ιδιότητες των περιοδικών ακολουθιών για τις οποίες δεν ορίζεται ο μετασχηματισμός Fourier. Αποτέλεσμα αυτής της ανάλυσης είναι ο ορισμός ενός νέου *γενικευμένου Διακριτού Μετασχηματισμού Fourier*, ο οποίος αποτελεί άμεση γενίκευση του κλασικού μετασχηματισμού Fourier και, επίσης, περιγράφει την γραμμική πολυπλοκότητα των ακολουθιών κατά πλήρη αντιστοιχία με τον κλασικό μετασχηματισμό. Ο νέος μετασχηματισμός Fourier που προτείνεται εδώ συγκεντρώνει περισσότερα πλεονεκτήματα από ό,τι ο γενικευμένος μετασχηματισμός Fourier που προτείνεται στο [99], λόγω του ότι παρέχει έναν ενιαίο τρόπο μαθηματικής περιγραφής όλων

των περιοδικών ακολουθιών, ανεξαρτήτως περιόδου.

Η παρούσα διατριβή εξετάζει επίσης τη μη γραμμική πολυπλοκότητα των ακολουθιών - η οποία, στην ευρύτερη βιβλιογραφία, έχει μελετηθεί σε σημαντικά μικρότερο βαθμό από ό,τι η γραμμική. Αναπτύσσεται καινούριος αναδρομικός αλγόριθμος για τον υπολογισμό της μη γραμμικής πολυπλοκότητας δυαδικών ακολουθιών, γενικεύοντας έτσι τον αλγόριθμο των Berlekamp-Massey για τη μη γραμμική περίπτωση. Ο αλγόριθμος που προτείνεται εδώ αποτελεί τον πρώτο αναδρομικό αλγόριθμο στη βιβλιογραφία για τον υπολογισμό του ελάχιστου καταχωρητή που παράγει μία ακολουθία και έχει την ίδια υπολογιστική πολυπλοκότητα (πολυωνυμική) με τον μη αναδρομικό αλγόριθμο που περιγράφεται στο [58]. Η αναδρομική φύση του αλγορίθμου είναι ιδιαίτερης σημασίας, αφού δεν απαιτείται εξ αρχής γνώση ολόκληρης της ακολουθίας για τον υπολογισμό της πολυπλοκότητάς της. Επιπρόσθετα, μελετώνται συσχετίσεις της πολυπλοκότητας με άλλα γνωστά κρυπτογραφικά κριτήρια ακολουθιών, όπως η πολυπλοκότητα Lempel-Ziv και ο λόγος συμπίεσης μίας ακολουθίας: η διερεύνηση αυτών των συσχετίσεων έχει διατυπωθεί ως ανοιχτό ερευνητικό πρόβλημα [110]. Σε αυτό το πλαίσιο αποδεικνύεται ένα κάτω φράγμα του λόγου συμπίεσης κάθε περιοδικής ακολουθίας, το οποίο εξαρτάται από την πολυπλοκότητά της. Επίσης, αποδεικνύεται ότι το προφίλ ιδιοτιμής μίας ακολουθίας, το οποίο ορίζεται στο [88] ως κρυπτογραφικό μέτρο που καθορίζει την πολυπλοκότητα Lempel-Ziv, καθορίζει επίσης μονοσήμαντα το προφίλ της μη γραμμικής πολυπλοκότητας της ακολουθίας.

Τέλος, η διατριβή μελετά τις λογικές συναρτήσεις οι οποίες χρησιμοποιούνται σε αλγορίθμους ροής ως μη γραμμικοί συνδυαστές για την παραγωγή ακολουθιών υψηλής γραμμικής πολυπλοκότητας. Μεταξύ των ιδιοτήτων που πρέπει να πληρούν αυτές οι συναρτήσεις, όπως αυτές αναδεικνύονται από διάφορες γνωστές κρυπταναλυτικές επιθέσεις, είναι η μη δυνατότητα ικανοποιητικής προσέγγισής τους από άλλη συνάρτηση χαμηλού βαθμού. Ωστόσο, με εξαίρεση τις προσεγγίσεις από συναρτήσεις πρώτου βαθμού (οι οποίες υπολογίζονται με το μετασχηματισμό Walsh), ελάχιστα αποτελέσματα είναι γνωστά στη βιβλιογραφία μέχρι σήμερα όσον αφορά στην εύρεση βέλτιστων προσεγγίσεων χαμηλού βαθμού r μίας συνάρτησης, ακόμα και για $r = 2$ (τετραγωνικές προσεγγίσεις). Οι μέχρι τώρα τεχνικές είτε δεν υπολογίζουν τις καλύτερες δυνατές προσεγγίσεις είτε περιορίζονται σε συναρτήσεις μικρού πλήθους μεταβλητών [65, 106]. Η συνεισφορά της διατριβής σε αυτή την κατεύθυνση είναι μία νέα αποδοτική τεχνική για τον προσδιορισμό όλων των βέλτιστων τετραγωνικών προσεγγίσεων για συγκεκριμένες οικογένειες συναρτήσεων βαθμού 3 και 4. Η τεχνική αυτή ανάγει το πρόβλημα εύρεσης βέλτιστων τετραγωνικών προσεγγίσεων για μία συνάρτηση n μεταβλητών βαθμού 3 στο απλούστερο

πρόβλημα εύρεσης βέλτιστων γραμμικών προσεγγίσεων για τετραγωνική συνάρτηση $n-1$ μεταβλητών: για τις γραμμικές αυτές προσεγγίσεις αποδίδεται ακριβής μαθηματικός τύπος που τις περιγράφει, με αποτέλεσμα ο υπολογισμός αυτών να γίνεται άμεσα και χωρίς τη χρήση του μετασχηματισμού Walsh. Το πολύ σημαντικό πλεονέκτημα της αλγοριθμικής αυτής τεχνικής είναι το ότι μπορεί να εφαρμοστεί σε συναρτήσεις οποιουδήποτε πλήθους μεταβλητών. Άμεση απόρροια της ανάλυσης που ακολουθείται είναι η ανάδειξη συγκεκριμένων χαρακτηριστικών που πρέπει να αποφεύγονται κατά τη σχεδίαση κρυπτογραφικών συναρτήσεων, προκειμένου να μην μπορούν να προσεγγιστούν ικανοποιητικά από συναρτήσεις βαθμού 2. Ωστόσο, αποδεικνύεται ότι υπάρχουν κατασκευές κρυπτογραφικών συναρτήσεων που έχουν προταθεί στη βιβλιογραφία, οι οποίες ενσωματώνουν αυτά τα αρνητικά χαρακτηριστικά (μεταξύ των οποίων και σύγχρονα κρυπτογραφικά συστήματα). Κατά συνέπεια, τα αποτελέσματα της διατριβής μπορούν να αποτελέσουν εργαλεία κρυπτανάλυσης σε πραγματικά συστήματα. Αξίζει, εν κατακλείδι, να σημειωθεί ότι και στους αλγορίθμους τμήματος υπάρχουν τεχνικές κρυπτανάλυσης που στηρίζονται σε βέλτιστες χαμηλού βαθμού προσεγγίσεις των S-boxes [57, 101], γεγονός το οποίο διευρύνει το πλαίσιο στο οποίο υπάγονται τα αποτελέσματα της διατριβής.

Η δομή της διατριβής, όπως αυτή διαρθρώνεται ανά κεφάλαιο, είναι η ακόλουθη:

Στο **Κεφάλαιο 2** παρουσιάζονται οι βασικές έννοιες που χρησιμοποιούνται για την ανάλυση ακολουθιών, όπως η αναπαράσταση ίχνους, η ρητή αναπαράσταση και ο μετασχηματισμός Fourier. Περιγράφονται επίσης οι καταχωρητές ολίσθησης με ανάδραση, ως στοιχειώδη συστήματα παραγωγής ακολουθιών. Ορίζεται η έννοια της πολυπλοκότητας ακολουθιών ως σημαντικό κρυπτογραφικό κριτήριο και περιγράφονται τα συστήματα μη γραμμικών φίλτρων και μη γραμμικών συνδυαστών, τα οποία βασίζονται σε μη γραμμικές συναρτήσεις και σε γραμμικούς καταχωρητές ολίσθησης με ανάδραση προκειμένου να παράγουν ακολουθίες υψηλής γραμμικής πολυπλοκότητας. Αναλύεται επίσης ένα σημαντικό εύρος κρυπταναλυτικών επιθέσεων που μπορούν να εφαρμοστούν σε αυτά τα συστήματα, αναδεικνύοντας συγκεκριμένες ιδιότητες που πρέπει να πληρούν οι κρυπτογραφικές λογικές συναρτήσεις έτσι ώστε τα αντίστοιχα συστήματα να είναι ανθεκτικά σε αυτές τις επιθέσεις.

Στο **Κεφάλαιο 3** εισάγονται τα εργαλεία της θεωρίας συστημάτων με τα οποία θα μελετηθούν τα συστήματα παραγωγής ακολουθιών. Ορίζεται η ελεγξιμότητα και η παρατηρησιμότητα συστημάτων, ενώ προσδιορίζονται διάφορα είδη συστημάτων παραγωγής ακολουθιών, όπου η δομή καθενός από αυτά οδηγεί στον ορισμό νέων μέτρων πολυπλοκότητας για αυτές.

Στο **Κεφάλαιο 4** εφαρμόζονται οι έννοιες της ελεγξιμότητας και παρατηρησιμότητας σε γραμμικά συστήματα για τον προσδιορισμό μίας νέας διανυσματικής αναπαράστασης ίχνους

και ενός Γενικευμένου Διακριτού Μετασχηματισμού Fourier ο οποίος περιγράφει όλες ανεξαιρέτως τις περιοδικές ακολουθίες. Επίσης, αναλύονται υπό το ίδιο πρίσμα συστήματα μη γραμμικών φίλτρων, κάτι που οδηγεί σε γενίκευση των αποτελεσμάτων του Rueppel ως προς τις κατασκευές φίλτρων με καλά χαρακτηριστικά. Προτείνεται μία νέα μεθοδολογία κατασκευής μη γραμμικών φίλτρων, κάνοντας χρήση ιδιοτήτων των γινομένων Kronecker, η οποία εξασφαλίζει την παραγωγή ακολουθιών υψηλής γραμμικής πολυπλοκότητας.

Στο **Κεφάλαιο 5** αποδεικνύονται συσχετίσεις της μη γραμμικής πολυπλοκότητας μίας ακολουθίας τόσο με τη Lempel-Ziv πολυπλοκότητα όσο και με την ικανότητα συμπίεσης αυτής, με βάση τον γνωστό αλγόριθμο συμπίεσης των Lempel-Ziv. Αναπτύσσεται επίσης νέος αναδρομικός αλγόριθμος για τον υπολογισμό του ελάχιστου καταχωρητή με ανάδρασης ο οποίος παράγει μία ακολουθία, γενικεύοντας έτσι τον πολύ γνωστό αλγόριθμο Berlekamp-Massey για τη μη γραμμική περίπτωση.

Στο **Κεφάλαιο 6** αναπτύσσονται αποδοτικές αλγοριθμικές τεχνικές για τον προσδιορισμό των βέλτιστων τετραγωνικών προσεγγίσεων συναρτήσεων βαθμού 3 και 4, με οποιοδήποτε πλήθος μεταβλητών. Οι τεχνικές αυτές βασίζονται στο ανάπτυγμα κατά Shannon των λογικών συναρτήσεων, καθώς επίσης και στην αναπαράσταση των τετραγωνικών συναρτήσεων βάσει του Θεωρήματος του Dickson [95]. Επίσης, μελετώνται συγκεκριμένες κατασκευές συναρτήσεων που έχουν προταθεί στη βιβλιογραφία, αναδεικνύοντας την πρακτική εφαρμογή και την κρυπτογραφική αξία των παραπάνω αποτελεσμάτων.

Τέλος, στο **Κεφάλαιο 7** γίνεται μία σύνοψη των αποτελεσμάτων, ενώ επίσης παρουσιάζονται μελλοντικές ερευνητικές κατευθύνσεις.

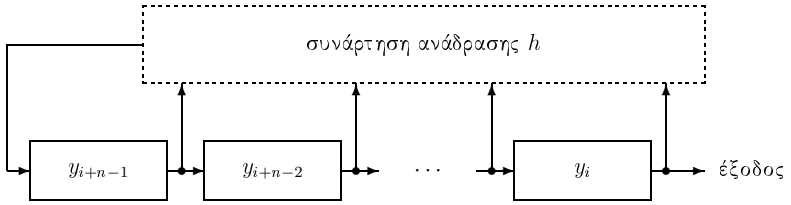
Κεφάλαιο 2

Κρυπτογραφικές ιδιότητες ακολουθιών

> Any one who considers automatical methods of producing random digits is, of course, in a state of sin
>
> *J. V. Neumann*

Ακολουθίες με τιμές σε ένα πεπερασμένο σώμα χρησιμοποιούνται σε ένα ευρύ φάσμα εφαρμογών, μεταξύ των οποίων η κρυπτογραφία, οι κώδικες ελέγχου σφάλματος και τα συστήματα επικοινωνιών ευρέου φάσματος [43, 67, 105]. Σε κρυπτογραφικές εφαρμογές, όπου κύριος στόχος είναι η διασφάλιση του ότι η μεταδιδόμενη πληροφορία δεν μπορεί να υποκλαπεί από τρίτους, η μυστικότητα της ακολουθίας του κλειδιού είναι απολύτως απαραίτητη. Συνεπώς, μία βασική ιδιότητα που πρέπει να διέπει τις κρυπτογραφικές ακολουθίες είναι η μη προβλεψιμότητα ή η τυχαιότητα. Στην πράξη όμως κάθε ακολουθία παράγεται από κάποιο πεπερασμένο αυτόματο και, ως εκ τούτου, η τιμή του κάθε στοιχείου της εξαρτάται από τιμές προηγούμενων στοιχείων. Κατ' επέκταση, δεν μπορούν να υπάρξουν απόλυτα τυχαίες ακολουθίες από αυτά τα συστήματα, αλλά μόνο *ψευδοτυχαίες (pseudorandom)* - δηλαδή, ακολουθίες των οποίων τα χαρακτηριστικά προσομοιάζουν αυτά μίας εντελώς τυχαίας ακολουθίας. Υπάρχουν διάφορα κριτήρια ψευδοτυχαιότητας για μία ακολουθία· ένα από τα πλέον σημαντικά είναι η πολυπλοκότητα αυτής, η οποία υποδηλώνει το μήκος του μικρότερου καταχωρητή ολίσθησης με ανάδραση ο οποίος μπορεί να παράγει την ακολουθία.

Αντικείμενο αυτού του κεφαλαίου αποτελεί η μελέτη κρυπτογραφικών ιδιοτήτων των ακολουθιών, καθώς επίσης και των συστημάτων παραγωγής αυτών. Έμφαση θα δοθεί στις ακολουθίες που παράγονται από καταχωρητές ολίσθησης των οποίων η συνάρτηση ανάδρασης είναι γραμμική: οι γραμμικοί καταχωρητές έχουν μελετηθεί σε μεγάλο βαθμό στη βιβλιογραφία, αφενός λόγω των πολύ καλών μαθηματικών ιδιοτήτων που τους διέπουν και, αφετέρου,



Σχήμα 2.1. Διάγραμμα ενός καταχωρητή ολίσθησης με ανάδραση (FSR)

λόγω της ευκολίας υλοποίησής τους. Αξίζει να σημειωθεί ότι στην πλειοψηφία των σύγχρονων αλγορίθμων ροής χρησιμοποιούνται γραμμικοί καταχωρητές ολίσθησης με ανάδραση για την παραγωγή της κλειδοροής, σε συνδυασμό πάντα με διάφορους μη γραμμικούς τελεστές, όπως θα περιγραφεί παρακάτω. Για τις περιοδικές ακολουθίες που παράγονται από καταχωρητές ολίσθησης δίνονται διάφοροι τρόποι αναπαράστασής τους, συγκεκριμένα η ρητή αναπαράσταση, ο μετασχηματισμός Fourier και η συνάρτηση ίχνους. Εισάγεται επίσης η έννοια της (γραμμικής/μη γραμμικής) πολυπλοκότητας ως σημαντικό κρυπτογραφικό κριτήριο για μία ακολουθία και περιγράφονται τεχνικές οι οποίες, κάνοντας χρήση μη γραμμικών λογικών συναρτήσεων, οδηγούν στη δημιουργία ακολουθιών μεγάλης γραμμικής πολυπλοκότητας. Αυτές οι τεχνικές στηρίζονται σε μη γραμμικά φίλτρα (ενότητα 2.5.2) και σε μη γραμμικούς συνδυαστές (ενότητα 2.5.3), τα οποία εφαρμόζονται κατάλληλα σε γραμμικούς καταχωρητές. Τέλος, περιγράφονται κάποιες από τις βασικές επιθέσεις κρυπτανάλυσης που έχουν εφαρμοστεί σε συστήματα αυτής της μορφής. Κάθε τέτοια επίθεση έχει ως αποτέλεσμα το να καθορίζονται συγκεκριμένες ιδιότητες που πρέπει να πληρούνται από τις λογικές συναρτήσεις, έτσι ώστε τα συστήματα να είναι ανθεκτικά σε αυτές.

Οι έννοιες που εισάγονται στο παρόν κεφάλαιο χρησιμοποιούνται ευρέως στα μετέπειτα κεφάλαια.

2.1 Καταχωρητές ολίσθησης με ανάδραση

Ας θεωρήσουμε το πεπερασμένο σώμα $\mathbb{F}_q$ που αποτελείται από q στοιχεία.

Ορισμός 2.1. Μία ακολουθία $y = \{y_i\}_{i\geq 0}$ με στοιχεία στο σώμα $\mathbb{F}_q$ ονομάζεται τελικά περιοδική (ultimately periodic) εάν υπάρχουν ακέραιοι $T > 0$ και $t_0 \geq 0$ τέτοιοι ώστε $y_{i+T} = y_i \ \forall \ i \geq t_0$. Ο μικρότερος ακέραιος T με την παραπάνω ιδιότητα ονομάζεται πρωταρχική περίοδος (fundamental period) της ακολουθίας y ή απλά περίοδος, και ο ακέραιος t_0 εκφράζει την προ-περίοδο (preperiod) της y. Αν $t_0 = 0$, τότε η ακολουθία y καλείται περιοδική (periodic).

Αν μία ακολουθία παίρνει τιμές στο $\mathbb{F}_2 = \{0, 1\}$, τότε καλείται *δυαδική ακολουθία* - αυτή είναι και η συνηθέστερη περίπτωση για κρυπτογραφικές εφαρμογές. Όταν αναφερόμαστε σε μία ακολουθία πεπερασμένου μήκους με N στοιχεία, θα τη συμβολίζουμε με y^N. Για κάθε τέτοια πεπερασμένη ακολουθία $y^N = y_0 y_1 \dots y_{N-1}$ και για κάθε $j \leq N$, συμβολίζουμε με y^j την υπακολουθία $y_0 y_1 \dots y_{j-1}$ που απαρτίζεται από τα πρώτα j στοιχεία της y. Κάθε τέτοια υπακολουθία καλείται *πρόθεμα (prefix)* της y^N. Στην περίπτωση όπου $j < N$, η υπακολουθία y^j καλείται *γνήσιο πρόθεμα (proper prefix)* της y^N. Ορίζουμε επίσης $y_i^j \triangleq y_i y_{i+1} \dots y_j$ για κάθε $i \leq j$ - συνεπώς, $y^j = y_0^{j-1}$. Αν $j = N - 1$, τότε κάθε υπακολουθία y_i^j καλείται *επίθεμα (suffix)* της y^N. Αντίστοιχα, αν για ένα επίθεμα ισχύει $i > 0$, τότε ονομάζεται *γνήσιο επίθεμα (proper suffix)*.

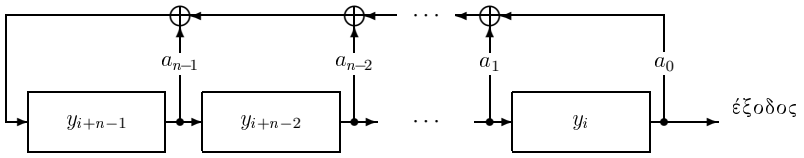
Περιοδικές ή τελικά περιοδικές ακολουθίες παράγονται από *καταχωρητές ολίσθησης με ανάδραση* (*feedback shift registers - FSRs*) (Σχήμα 2.1). Ένας καταχωρητής μήκους n στο σώμα $\mathbb{F}_q$ αποτελείται από n θέσεις μνήμης ή βαθμίδες, κάθε μία εκ των οποίων μπορεί να περιέχει ένα στοιχείο του σώματος $\mathbb{F}_q$. Σε κάθε παλμό του ρολογιού, το περιεχόμενο της κάθε θέσης μνήμης μετατοπίζεται κατά μία θέση δεξιά, ενώ η τιμή της αριστερότερης βαθμίδας καθορίζεται από την πράξη ανάδρασης h. Συνεπώς, κάθε ακολουθία που παράγεται από έναν τέτοιο καταχωρητή ικανοποιεί την ακόλουθη αναδρομική σχέση

$$y_{i+n} = h(y_{i+n-1}, \dots, y_i), \qquad i \geq 0, \tag{2.1}$$

όπου η συνάρτηση $h : \mathbb{F}_q^n \to \mathbb{F}_q$ είναι στη γενική περίπτωση μη γραμμική· στις περισσότερες περιπτώσεις, ο σταθερός όρος της συνάρτησης h ισούται με 0.

Για κάθε χρονική στιγμή, τα περιεχόμενα των θέσεων μνήμης ορίζουν την *κατάσταση (state)* του FSR. Με άλλα λόγια, αν y είναι η παραγόμενη ακολουθία από έναν FSR, τότε η κατάστασή του για κάθε χρονική στιγμή $i \geq 0$ δίνεται από το διάνυσμα $(y_{i+n-1}\ y_{i+n-2}\ \dots\ y_i)$. Προφανώς, ένας FSR μήκους n μπορεί να περάσει από q^n διαφορετικές καταστάσεις. Συνεπώς, η μέγιστη περίοδος που μπορεί να έχει μία ακολουθία που παράγεται από έναν FSR n βαθμίδων είναι q^n. Μία περιοδική ακολουθία στο $\mathbb{F}_q$ περιόδου q^n, όπου η περίοδός της περιέχει όλες τις πιθανές n-άδες στο $\mathbb{F}_q$, ονομάζεται *ακολουθία De Brujin*. Οι ακολουθίες De Brujin παρουσιάζουν σημαντικό ερευνητικό ενδιαφέρον.

Αν περιοριστούμε στους FSRs των οποίων η συνάρτηση ανάδρασης έχει μηδενικό σταθερό όρο, τότε η μέγιστη δυνατή περίοδος της ακολουθίας εξόδου είναι $q^n - 1$, λόγω του ότι αν ο FSR περάσει από τη μηδενική κατάσταση θα παραμείνει για πάντα σε αυτή. Στο υπόλοιπο τμήμα αυτού του κεφαλαίου θα θεωρούμε ότι ο σταθερός όρος της συνάρτησης ανάδρασης



Σχήμα 2.2. Διάγραμμα ενός γραμμικού καταχωρητή ολίσθησης με ανάδραση (LFSR)

είναι 0.

Για την ειδική περίπτωση των δυαδικών ακολουθιών, το διάγραμμα ενός καταχωρητή όπως αυτό του Σχήματος 2.1 αντικατοπτρίζει άμεσα και την υλοποίησή του σε επίπεδο λογικών πυλών· συγκεκριμένα, κάθε θέση μνήμης του καταχωρητή αντιστοιχεί σε ένα flip-flop, ενώ επιπλέον οι προσθέσεις και οι πολλαπλασιασμοί που υπεισέρχονται στη συνάρτηση ανάδρασης h υλοποιούνται ως κλασικοί αθροιστές και πολλαπλασιαστές αντίστοιχα σε επίπεδο bit (στη γενική περίπτωση όπου οι πράξεις γίνονται πάνω σε κάποιο πεπερασμένο σώμα $\mathbb{F}_q$, τότε οι προσθέσεις και οι πολλαπλασιασμοί πάνω στο σώμα έχουν πιο σύνθετη υλοποίηση). Επιπρόσθετα, όταν η παραγόμενη ακολουθία είναι δυαδική, τότε η συνάρτηση ανάδρασης h είναι μία *λογική συνάρτηση (Boolean function)* με n μεταβλητές. Οι λογικές συναρτήσεις περιγράφονται αναλυτικά στην υπο-ενότητα 2.5.1.

2.1.1 Γραμμικοί καταχωρητές ολίσθησης με ανάδραση - Ακολουθίες μεγίστου μήκους

Γραμμικοί καταχωρητές ολίσθησης με ανάδραση (Linear Feedback Shift Registers - LFSRs) ονομάζονται εκείνοι οι καταχωρητές των οποίων η συνάρτηση ανάδρασης είναι γραμμική, δηλαδή της μορφής

$$y_{i+n} = a_{n-1}y_{i+n-1} + \cdots + a_1 y_{i+1} + a_0 y_i,\ a_j \in \mathbb{F}_q,\ \forall\ j = 1, 2, \ldots, n. \tag{2.2}$$

Ένας LFSR με n βαθμίδες απεικονίζεται στο Σχήμα 2.2. Βασικές ιδιότητες των συστημάτων αυτών έχουν μελετηθεί διεξοδικά στο κλασικό βιβλίο του Golomb [42], αλλά και στο κεφάλαιο 8 του βιβλίου των Lidl-Niederreiter [89]. Το *χαρακτηριστικό πολυώνυμο (characteristic polynomial)* ενός LFSR που δίνεται από το σχήμα 2.2 είναι το πολυώνυμο

$$f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathbb{F}_q[x]. \tag{2.3}$$

Στη βιβλιογραφία συχνά χρησιμοποιείται, για την περιγραφή ενός LFSR όπως αυτού του σχήματος 2.2, το πολυώνυμο $f'(x) = 1 - a_{n-1}x - a_{n-2}x^2 - \ldots - a_0 x^n$. Αυτό το πολυώνυμο,

που επίσης προσδιορίζει μονοσήμαντα έναν LFSR, καλείται *πολυώνυμο ανάδρασης (feedback polynomial)*[52]. Αντίστροφα, αν για μία δοθείσα ακολουθία όλοι οι όροι της ικανοποιούν μία αναδρομική σχέση της μορφής (2.2), τότε το πολυώνυμο f που περιγράφεται στην (2.3) καλείται *χαρακτηριστικό πολυώνυμο της ακολουθίας*. Στη γενική περίπτωση, μία ακολουθία έχει πολλά χαρακτηριστικά πολυώνυμα (ισοδύναμα, υπάρχουν πολλοί διαφορετικοί LFSRs που παράγουν την ακολουθία).

Ένας LFSR παράγει περιοδική ακολουθία αν και μόνο αν ο σταθερός όρος a_0 του χαρακτηριστικού του πολυωνύμου είναι μη μηδενικός - δηλαδή, αν $f(0) \neq 0$. Στο υπόλοιπο της ενότητας περιοριζόμαστε σε αυτούς τους LFSRs. Για οποιονδήποτε LFSR μήκους n με χαρακτηριστικό πολυώνυμο f, αν η αρχική του κατάσταση είναι η $100\ldots0$ τότε η παραγόμενη ακολουθία έχει τη μέγιστη δυνατή περίοδο που μπορεί να έχει οποιαδήποτε ακολουθία παράγεται από αυτόν τον LFSR. Η συγκεκριμένη περιοδική ακολουθία που προκύπτει καλείται *ακολουθία κρουστικής απόκρισης (impulse response sequence)*. Οποιαδήποτε άλλη ακολουθία παράγεται από αυτόν τον LFSR έχει περίοδο που είναι διαιρέτης της περιόδου της κρουστικής απόκρισης ή ίση με αυτή. Με τη σειρά της, η περίοδος της ακολουθίας κρουστικής απόκρισης του LFSR ισούται με την τάξη $\mathrm{ord}(f)$ του χαρακτηριστικού πολυωνύμου f - δηλαδή, είναι ίση με τον μικρότερο ακέραιο k τέτοιον ώστε το f να διαιρεί το $x^k - 1$. Αν το πολυώνυμο f είναι *ανάγωγο (irreducible)* στο $\mathbb{F}_q$ και έχει βαθμό n, τότε $\mathrm{ord}(f) \mid q^n - 1$. Ισχύει $\mathrm{ord}(f) = q^n - 1$ αν και μόνο αν το f είναι *πρωταρχικό πολυώνυμο (primitive polynomial)* στο $\mathbb{F}_q$ [89, pp. 89].

Αν μία ακολουθία $y \in \mathbb{F}_q$ που περιγράφεται από την (2.2) έχει χαρακτηριστικό πολυώνυμο f του οποίου οι ρίζες $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι ανά δύο διαφορετικές μεταξύ τους (ή, ισοδύναμα, η πολλαπλότητα κάθε ρίζας του f είναι 1), τότε υπάρχουν στοιχεία $\beta_1, \beta_2, \ldots, \beta_n$, που εξαρτώνται από τις πρώτες n τιμές της ακολουθίας, τέτοια ώστε

$$y_i = \sum_{j=1}^{n} \beta_j \alpha_j^i, \qquad i = 0, 1, \ldots \tag{2.4}$$

Οι ακριβείς τιμές των $\beta_1, \ldots, \beta_n$ προσδιορίζονται από την επίλυση γραμμικού συστήματος [89]. Ουσιαστικά, καθορίζονται πλήρως από την αρχική κατάσταση εκείνου του LFSR με χαρακτηριστικό πολυώνυμο f που παράγει την ακολουθία. Μπορεί εύκολα να αποδειχτεί πως για την ειδική περίπτωση όπου το χαρακτηριστικό πολυώνυμο f του LFSR είναι ανάγωγο με ρίζες $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$, τότε οι συντελεστές $\beta_1, \ldots, \beta_n$ παίρνουν τέτοια μορφή ώστε η (2.4) να γράφεται ισοδύναμα ως

$$y_i = \beta\alpha^i + \beta^q\alpha^{qi} + \beta^{q^2}\alpha^{q^2 i} + \ldots + \beta^{q^{n-1}}\alpha^{q^{n-1} i}, \qquad i = 0, 1, \ldots \tag{2.5}$$

Έστω ακολουθία $y \in \mathbb{F}_q$ που ικανοποιεί τη σχέση (2.2) για κάθε χρονική στιγμή i. Τότε υπάρχει ένα μοναδικό *μονικό (monic)* πολυώνυμο $m(x) \in \mathbb{F}_q[x]$ (όπου ως μονικό ορίζεται ένα πολυώνυμο του οποίου ο συντελεστής του μεγιστοβάθμιου όρου είναι μονάδα) με την ακόλουθη ιδιότητα: ένα μονικό πολυώνυμο $f(x) \in \mathbb{F}_q[x]$ είναι χαρακτηριστικό πολυώνυμο της ακολουθίας y αν και μόνο αν το πολυώνυμο $m(x)$ διαιρεί το $f(x)$. Το πολυώνυμο $m(x)$ ονομάζεται *ελάχιστο πολυώνυμο (minimal polynomial)* της ακολουθίας y. Με άλλα λόγια, το ελάχιστο πολυώνυμο μίας ακολουθίας περιγράφει τη συνάρτηση ανάδρασης του LFSR με το μικρότερο μήκος που μπορεί να παράγει την ακολουθία. Η περίοδος μίας ακολουθίας με ελάχιστο πολυώνυμο $m(x)$ ισούται με $\mathrm{ord}(m(x))$. Από την προηγούμενη ανάλυση γίνεται σαφές ότι ένας LFSR παράγει πάντα ακολουθίες με τη μέγιστη δυνατή περίοδο $q^n - 1$, ανεξαρτήτως της αρχικής του κατάστασης (πλην της μηδενικής), *αν και μόνο αν* το χαρακτηριστικό του πολυώνυμο είναι πρωταρχικό πολυώνυμο στο σώμα $\mathbb{F}_q$. Σε αυτήν την περίπτωση, το χαρακτηριστικό πολυώνυμο του LFSR είναι προφανώς και το ελάχιστο πολυώνυμο της παραγόμενης ακολουθίας. Αυτοί οι LFSRs καλούνται *πρωταρχικοί LFSRs*, ενώ οι ακολουθίες που παράγονται από πρωταρχικούς LFSRs ονομάζονται *ακολουθίες μεγίστου μήκους (maximal-length sequences ή m-sequences)*, λόγω της μέγιστης περιόδου που έχουν. Οι ακολουθίες μεγίστου μήκους ικανοποιούν πολλές σημαντικές ιδιότητες. Χαρακτηριστική είναι η *ιδιότητα ολίσθησης-πρόσθεσης (shift-and-add property)*: αν σε μία οποιαδήποτε ακολουθία μεγίστου μήκους y προσθέσουμε μία αυθαίρετη κυκλική ολίσθησή της, τότε η προκύπτουσα ακολουθία είναι επίσης κυκλική ολίσθηση της y. Άλλες σημαντικές ιδιότητες των ακολουθιών αυτών, με κρυπτογραφική χροιά, θα αναλυθούν στην Ενότητα 2.4.

Από τους παραπάνω ορισμούς γίνεται φανερό ότι υπάρχει άμεσος τρόπος κατασκευής δυαδικών ακολουθιών De Brujin μέσω των ακολουθιών μεγίστου μήκους. Αν y είναι μία δυαδική ακολουθία μεγίστου μήκους με περίοδο $2^n - 1$, τότε όλες οι πιθανές n-άδες στο $\mathbb{F}_2$ εμφανίζονται σε μία περίοδο της ακολουθίας, πλην της n-άδας που αποτελείται μόνο από μηδενικά· συνεπώς, αν σε μία περίοδο της y εισάγουμε ένα 0 αμέσως μετά την εμφάνιση $n-1$ διαδοχικών 0, τότε η νέα ακολουθία περιόδου 2^n που θα προκύψει θα είναι De Brujin. Ωστόσο, πρέπει να σημειωθεί ότι δεν παράγονται όλες οι δυαδικές ακολουθίες De Brujin με αυτόν τον τρόπο.

2.2 Ρητή αναπαράσταση περιοδικής ακολουθίας

Σημαντικές ιδιότητες των περιοδικών ακολουθιών αναδεικνύονται μέσω της αναπαράστασης σε *δυναμοσειρά (formal power series)*. Έστω $y \in \mathbb{F}_q$ περιοδική ακολουθία με περίοδο N.

Τότε, η δυναμοσειρά της

$$Y(z) = \sum_{i=0}^{\infty} y_i z^i = y_0 + y_1 z + y_2 z^2 + \dots$$

μπορεί να γραφεί ως

$$Y(z) = y^N(z)(1 + z^N + z^{2N} + \dots)$$

όπου $y^N(z) = y_0 + y_1 z + \dots + y_{N-1} z^{N-1}$ (πλήρως ορισμένο από μία περίοδο της ακολουθίας). Συνεπώς, προκύπτει η ακόλουθη σχέση

$$Y(z) = \frac{y^N(z)}{1 - z^N}\,, \tag{2.6}$$

η οποία καλείται *ρητή αναπαράσταση της ακολουθίας*. Από την ρητή αναπαράσταση (2.6) προκύπτει πως αν $\gcd(y^N(z), 1 - z^N) = g(z)$, τότε η δυναμοσειρά της ακολουθίας μπορεί να γραφεί στην ισοδύναμη ρητή παράσταση

$$Y(z) = \frac{p(z)}{c(z)}\,, \qquad \deg(p(z)) < \deg(c(z)),\ \gcd(p(z), c(z)) = 1 \tag{2.7}$$

όπου $y^N(z) = p(z)g(z)$ και $1 - z^N = c(z)g(z)$. *Το πολυώνυμο $c(z)$ είναι το ελάχιστο πολυώνυμο της ακολουθίας*. Αντίστροφα, μία άπειρη ακολουθία είναι περιοδική αν και μόνο αν η δυναμοσειρά της μπορεί να γραφεί στη μορφή (2.7).

2.3 Μετασχηματισμός Fourier - Αναπαράσταση ίχνους

Ο *Διακριτός Μετασχηματισμός Fourier (Discrete Fourier Transform - DFT)* είναι ένα σημαντικό εργαλείο στην επεξεργασία σήματος. Για μία περιοδική ακολουθία $y \in \mathbb{F}_q$ με περίοδο N τέτοια ώστε $N|q^n - 1$ για κάποιο $n \geq 1$, ο μετασχηματισμός Fourier $\boldsymbol{Y} \in \mathbb{F}_{q^n}$ δίνεται από τη σχέση

$$\boldsymbol{Y}_i = \sum_{j=0}^{N-1} y_j \alpha^{ij}, \qquad i = 0, 1, \dots, N-1, \tag{2.8}$$

όπου το α είναι στοιχείο του σώματος $\mathbb{F}_{q^n}$ με τάξη N. Ο αντίστροφος μετασχηματισμός Fourier δίνεται από τη σχέση

$$y_i = \frac{1}{N} \sum_{j=0}^{N-1} \boldsymbol{Y}_j \alpha^{-ij}, \qquad i = 0, 1, \dots, N-1, \tag{2.9}$$

Από τον ορισμό του πολυωνύμου $y^N(x) \in \mathbb{F}_q[x]$ στην ενότητα 2.2 και από την (2.8) προκύπτει ότι ο μετασχηματισμός Fourier της ακολουθίας y δίνεται ισοδύναμα από τη σχέση

$$\boldsymbol{Y} = (y^N(1)\ y^N(\alpha)\ y^N(\alpha^2)\ \ldots\ y^N(\alpha^{N-1})) \tag{2.10}$$

Η απαίτηση $N|q^n - 1$ εξασφαλίζει το ότι υπάρχει στοιχείο του σώματος $\mathbb{F}_{q^n}$ με τάξη N ή, ισοδύναμα, ότι υπάρχει στοιχείο που είναι ρίζα N-ιοστής τάξης της μονάδας - κάτι το οποίο είναι αναγκαία προϋπόθεση για να ορίζεται ο αντίστροφος DFT της σχέσης (2.9). Οι συντελεστές $\boldsymbol{Y}_i,\ i = 0, 1, \ldots, N-1$, καλούνται και *φάσμα (spectrum)* της ακολουθίας και ικανοποιούν την ακόλουθη σχέση συζυγίας για κάθε $1 \leq i \leq N-1$:

$$\boldsymbol{Y}_{iq^j} = \boldsymbol{Y}_i^{q^j}, \qquad 0 \leq j < n. \tag{2.11}$$

Παρατήρηση 2.2. Αν $q = p^r$ για κάποιον πρώτο αριθμό p και ακέραιο $r \geq 1$, τότε ικανή και αναγκαία συνθήκη για να υπάρχει ρίζα N-ιοστής τάξης της μονάδας σε κάποιο ευρύτερο σώμα, το οποίο περιέχει ως υπόσωμα το $\mathbb{F}_q$, είναι $\gcd(N, p) = 1$. Συνεπώς, για δυαδικές ακολουθίες, ο μετασχηματισμός Fourier ορίζεται αν και μόνο αν η περίοδος της ακολουθίας είναι περιττός αριθμός. Επίσης στις δυαδικές ακολουθίες, επειδή $N \equiv 1 \pmod 2$, ισχύει $N^{-1} \equiv 1$ και, συνεπώς, στη σχέση (2.9) ο συντελεστής $1/N$ μπορεί να παραλειφθεί.

Συγκρίνοντας τη σχέση (2.9) με την (2.4), γίνεται φανερό ότι υπάρχει μία σχέση μεταξύ της γραμμικής αναδρομικής υλοποίησης μιας ακολουθίας και του μετασχηματισμού Fourier αυτής. Αυτή η συσχέτιση, η οποία εν τέλει υποδηλώνει τα κρυπτογραφικά χαρακτηριστικά της ακολουθίας που αναδεικνύει ο μετασχηματισμός Fourier, θα αποσαφηνιστεί στην ενότητα 2.4.

Ορισμός 2.3. Έστω ακέραιοι s, N με $0 \leq s < N$ και $N|q^n - 1$ για κάποιο n (όπου το q είναι πρώτος αριθμός ή δύναμη κάποιου πρώτου αριθμού). Το σύνολο

$$C_s = \{s, sq, sq^2, \ldots, sq^{n_s - 1}\} \tag{2.12}$$

ονομάζεται κυκλοτομική κλάση (cyclotomic class) modulo N του s ως προς το q, όπου n_s είναι ο μικρότερος ακέραιος με την ιδιότητα $sq^{n_s} \equiv s \pmod N$. Ο μικρότερος ακέραιος στο C_s καλείται στοιχείο-οδηγός (coset leader) modulo N ως προς το q. Ο ακέραιος n_s αποτελεί την τάξη (order) του C_s και συμβολίζεται επίσης με $n_s = \mathrm{ord}(s)$.

Αποδεικνύεται εύκολα ότι $n_s | n$ [89]. Επίσης, από τον παραπάνω ορισμό γίνεται φανερό ότι το σύνολο $\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$ ισούται με την ένωση $\cup_{j \in I} C_j$, όπου I είναι το σύνολο εκείνο που αποτελείται από όλα τα στοιχεία-οδηγούς των κυκλοτομικών κλάσεων modulo

N ως προς q. Από τον ορισμό του συνόλου I, τη σχέση (2.9) και την ιδιότητα συζυγίας που περιγράφεται στη σχέση (2.11), προκύπτει η ακόλουθη αναπαράσταση μιας περιοδικής ακολουθίας $y \in \mathbb{F}_q$ με περίοδο N διαιρέτη του $q^n - 1$ για κάποιο n:

$$y_i = \frac{1}{N} \sum_{j \in I} \mathrm{tr}_1^{n_j}(\boldsymbol{Y}_j \alpha^{-ij}), \qquad i = 0, 1, \ldots, N-1, \tag{2.13}$$

όπου $n_j = \mathrm{ord}(j)$ και $\mathrm{tr}_1^{n_j} : \mathbb{F}_{q^{n_j}} \to \mathbb{F}_q$ είναι η *συνάρτηση ίχνους (trace function)* που δίνεται από τη σχέση

$$\mathrm{tr}_1^{n_j}(x) = x + x^q + x^{q^2} + \ldots + x^{q^{n_j - 1}} . \tag{2.14}$$

Η σχέση (2.13) καλείται *αναπαράσταση ίχνους (trace representation)* της ακολουθίας y και είναι ισοδύναμη της αναπαράστασης Fourier της ακολουθίας, όπως αυτή δίνεται από την (2.9).

Ας θεωρήσουμε μία περιοδική ακολουθία $y \in \mathbb{F}_q$ με περίοδο N η οποία παράγεται από έναν LFSR του οποίου το χαρακτηριστικό πολυώνυμο είναι ανάγωγο. Τότε, η αναπαράσταση ίχνους της δίνεται από την σχέση

$$y_i = \mathrm{tr}_1^{n_j}(\beta \alpha^i), \qquad i = 0, 1, \ldots, N-1 \tag{2.15}$$

η οποία μπορεί επίσης να προκύψει άμεσα από την (2.5). Αν στην (2.15) ισχύει $\beta = 1$, τότε λέμε πως η ακολουθία y είναι στη *χαρακτηριστική της φάση*.

2.3.1 Γενικευμένος Διακριτός Μετασχηματισμός Fourier

Όπως αναφέρθηκε παραπάνω, ο μετασχηματισμός Fourier για μία ακολουθία δεν ορίζεται όταν $\gcd(N, p) \neq 1$, όπου N η περίοδος της ακολουθίας και p η χαρακτηριστική του σώματος. Στη βιβλιογραφία έχουν προταθεί διάφορες γενικεύσεις του μετασχηματισμού Fourier, υπό την έννοια ότι ορίζονται για όλες τις ακολουθίες ανεξαρτήτως περιόδου και, επίσης, παρουσιάζουν πολλά κοινά χαρακτηριστικά με τον κλασικό μετασχηματισμό Fourier [5, 48, 100, 99]. Ο πιο συχνά χρησιμοποιούμενος μέχρι σήμερα *Γενικευμένος Διακριτός Μετασχηματισμός Fourier (Generalized Discrete Fourier Transform - GDFT)* είναι αυτός που προτάθηκε από τους Massey και Serconek [99]. Ο μετασχηματισμός αυτός βασίζεται στην έννοια της παραγώγου Hasse: συγκεκριμένα, για ένα πολυώνυμο $s(x) \in \mathbb{F}_q[x]$ όπου $s(x) = \sum_i s_i x^i$, η *παράγωγος Hasse j τάξης* $s^{[j]}(x)$ του πολυωνύμου s δίνεται από τη σχέση

$$s^{[j]}(x) = \sum_i \binom{i}{j} s_i x^{i-j} .$$

Βάσει του παραπάνω ορισμού, για μία ακολουθία $y \in \mathbb{F}_q$ περιόδου $N = mp^e$, όπου p η χαρακτηριστική του $\mathbb{F}_q$ και $\gcd(m,p) = 1$, ο GDFT ορίζεται ως

$$\boldsymbol{Y}_{GDFT} = \begin{pmatrix} y^N(1) & y^N(\alpha) & \dots & y^N(\alpha^{m-1}) \\ y^{N[1]}(1) & y^{N[1]}(\alpha) & \dots & y^{N[1]}(\alpha^{m-1}) \\ \vdots & \vdots & & \vdots \\ y^{N[p^e-1]}(1) & y^{N[p^e-1]}(\alpha) & \dots & y^{N[p^e-1]}(\alpha^{m-1}) \end{pmatrix}, \tag{2.16}$$

όπου α είναι στοιχείο με τάξη m. Γίνεται φανερό ότι για $e = 0$ (δηλαδή $\gcd(N,p) = 1$), ο GDFT της σχέσης (2.16) μετατρέπεται στον κλασικό DFT της σχέσης (2.10). Το *βάρος Günther (Günther weight) ενός πίνακα δίνεται από το πλήθος των ψηφίων του που είτε είναι μη μηδενικά είτε βρίσκονται κάτω από έναν μη μηδενικό αριθμό.* Ο ορισμός αυτός θα χρησιμοποιηθεί στην ενότητα 2.4, όπου επίσης θα αποσαφηνιστεί και ο λόγος που οι συντελεστές του GDFT διευθετούνται σε μορφή πίνακα διαστάσεων $p^e \times m$ στη σχέση (2.16) και όχι σαν μονοδιάστατο διάνυσμα διάστασης $N = mp^e$.

2.4 Πολυπλοκότητα ακολουθιών

Όπως αναφέρθηκε στο κεφάλαιο 1, η ψευδοτυχαιότητα μιας ακολουθίας είναι αναγκαία προϋπόθεση για την κατασκευή ενός ασφαλούς κρυπτογραφικού συστήματος. Το πότε μια ακολουθία μπορεί να χαρακτηριστεί ως ψευδοτυχαία δεν είναι εύκολο ερώτημα. Ένα αυτονόητο κριτήριο που πρέπει να ικανοποιεί μια ψευδοτυχαία ακολουθία είναι το να έχει μεγάλη περίοδο. Εκτός της μεγάλης περιόδου, ο Golomb στο [42] πρότεινε τα ακόλουθα τρία κριτήρια ψευδοτυχαιότητας περιοδικών *δυαδικών* ακολουθιών, τα οποία είναι γνωστά ως *κριτήρια ψευδοτυχαιότητας του Golomb (Golomb's randomness postulates)*:

1. Σε μία περίοδο της ακολουθίας, το πλήθος των 0 είναι ίσο ή διαφέρει κατά ένα με το πλήθος των 1. Αυτή η ιδιότητα ονομάζεται *ιδιότητα ισοβαρούς ακολουθίας (balance property).*

2. Ως *διαδρομή (run)* σε μία δυαδική ακολουθία θεωρούμε ένα τμήμα της $\tilde{y} = xx\dots x$ που αποτελείται από όμοια στοιχεία x ($x = 0$ ή 1), όπου όμως τόσο το στοιχείο που προηγείται του $\tilde{y}$ όσο και αυτό που έπεται του $\tilde{y}$ είναι διαφορετικά από το x. Το κριτήριο ψευδοτυχαιότητας έχει ως εξής: σε μία περίοδο, το $1/2$ των διαδρομών έχουν μήκος 1, το $1/4 = 1/2^2$ αυτών έχουν μήκος 2, το $1/8 = 1/2^3$ αυτών μήκος 3 κ.ο.κ. μέχρις

ώτου το $1/2^k$ του πλήθους των διαδρομών είναι μικρότερο της μονάδας. Αυτή η ιδιότητα καλείται *ιδιότητα διαδρομής (run property)*.

3. Η συνάρτηση αυτοσυσχέτισης $c(\tau) = \sum_{i=0}^{N-1}(-1)^{y_i+y_{i+\tau}}$ της δυαδικής ακολουθίας y, όπου N η περίοδός της, παίρνει δύο τιμές, συγκεκριμένα

$$c(\tau) = \begin{cases} N, & \text{αν } \tau \equiv 0(\text{mod } N) \\ K, & \text{αν } \tau \neq 0(\text{mod } N) \end{cases}$$

όπου K σταθερός ακέραιος. Αυτή η ιδιότητα καλείται *ιδιότητα αυτοσυσχέτισης (autocorrelation property)*.

Οι ακολουθίες μεγίστου μήκους ικανοποιούν και τα τρία κριτήρια ψευδοτυχαιότητας του Golomb [42]. Το γεγονός αυτό, σε συνδυασμό με το ότι οι ακολουθίες μεγίστου μήκους έχουν τη μέγιστη δυνατή περίοδο ως προς το μήκος του καταχωρητή από τον οποίο παράγονται, τις κατέστησε βασικές κρυπτογραφικές ακολουθίες στα πρώτα χρόνια εμφάνισης κρυπτογραφικών εφαρμογών. Μία σημαντική αδυναμία τους όμως είχε σαν αποτέλεσμα να χαρακτηριστούν, αν και διαθέτουν πολύ καλές ιδιότητες, κρυπτογραφικά ακατάλληλες: η αδυναμία τους αυτή είναι η χαμηλή *γραμμική πολυπλοκότητα* που έχουν, η οποία ορίζεται στη συνέχεια.

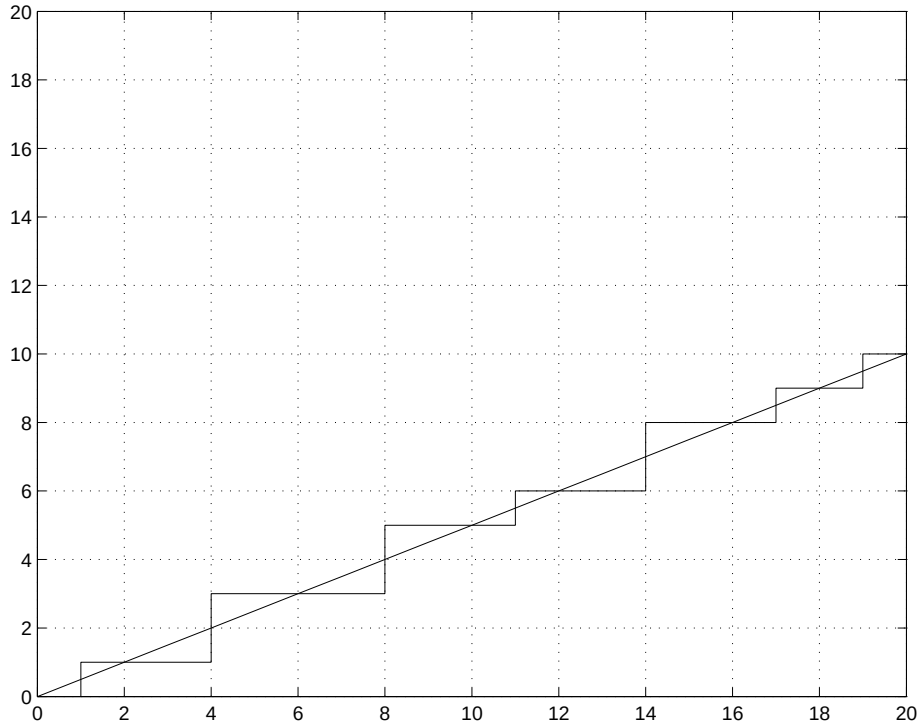
Ορισμός 2.4. Μη γραμμική πολυπλοκότητα (nonlinear complexity ή nonlinear span) ή απλά πολυπλοκότητα μιας ακολουθίας ορίζεται ως το μήκος του μικρότερου FSR ο οποίος παράγει την ακολουθία. Κάθε FSR ο οποίος παράγει μία ακολουθία και έχει μήκος όσο η πολυπλοκότητά της καλείται ελάχιστος FSR της ακολουθίας. Αντίστοιχα, γραμμική πολυπλοκότητα μιας ακολουθίας (linear complexity ή linear span) ορίζεται ως το μήκος του μικρότερου LFSR ο οποίος παράγει την ακολουθία. Ο ελάχιστος LFSR για μία ακολουθία ορίζεται με όμοιο τρόπο.

Από τον παραπάνω ορισμό γίνεται προφανές ότι αν τα $c(y), \text{lc}(y)$ υποδηλώνουν αντίστοιχα τη μη γραμμική και τη γραμμική πολυπλοκότητα της ακολουθίας y, τότε $c(y) \leq \text{lc}(y)$.

Ορισμός 2.5. Για μία ακολουθία $y^N = y_0y_1 \dots y_{N-1}$ πεπερασμένου μήκους, το προφίλ πολυπλοκότητας (complexity profile) ορίζεται ως η ακολουθία των ακεραίων αριθμών

$$c(y^1), c(y^2) \dots, c(y^N).$$

Με ανάλογο τρόπο ορίζεται το προφίλ γραμμικής πολυπλοκότητας (linear complexity profile).



Σχήμα 2.3. Το προφίλ της γραμμικής πολυπλοκότητας για τη δυαδική ακολουθία $y^{20} = 10010011110001001110$

Γραμμική πολυπλοκότητα

Η γραμμική πολυπλοκότητα ακολουθιών έχει μελετηθεί σε πολύ μεγάλο βαθμό στη βιβλιογραφία [21, 47, 73, 56, 97, 98, 99, 124, 125]. Σημαντικές ιδιότητες που χαρακτηρίζουν το προφίλ γραμμικής πολυπλοκότητας ακολουθιών πεπερασμένου μήκους είναι οι ακόλουθες:

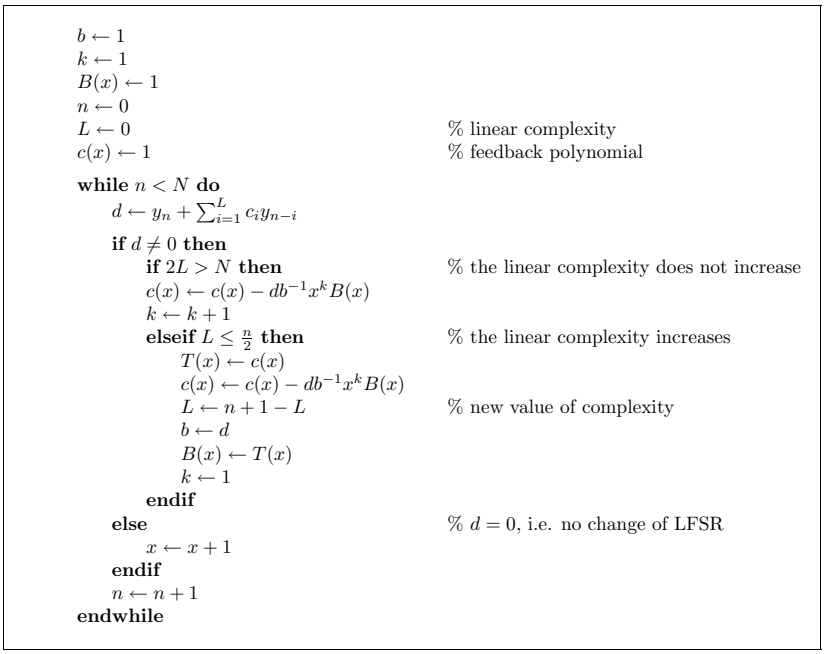
1. Αν $j > i$, τότε $\mathrm{lc}(y^j) \geq \mathrm{lc}(y^i)$.
2. Αν $\mathrm{lc}(y^{i+1}) > \mathrm{lc}(y^i)$, τότε $\mathrm{lc}(y^i) \leq \frac{i}{2}$.
3. Αν $\mathrm{lc}(y^{i+1}) > \mathrm{lc}(y^i)$, τότε $\mathrm{lc}(y^{i+1}) + \mathrm{lc}(y^i) = i + 1$.

Από τις παραπάνω ιδιότητες προκύπτει πως, οποτεδήποτε έχουμε αύξηση στην τιμή της γραμμικής πολυπλοκότητας μίας ακολουθίας, τότε η νέα τιμή της γραμμικής πολυπλοκότητας είναι συμμετρική της παλιάς ως προς τη γραμμή $f(N) = \frac{N}{2}$, $N = 1, 2, \ldots$. Αυτό αναδεικνύεται στο Σχήμα 2.3 όπου απεικονίζεται το προφίλ γραμμικής πολυπλοκότητας της ακολουθίας πεπερασμένου μήκους $y^{20} = 10010011110001001110$. Η τιμή $\frac{N}{2}$ ισούται επίσης (κατά προσέγγιση) με την αναμενόμενη τιμή $E(\mathrm{lc}(y^N))$ της γραμμικής πολυπλοκότητας για μια τυχαία ακολουθία y^N, όπως αυτή έχει υπολογιστεί από τον Rueppel στο [124]: με άλλα λόγια, ισχύει

$E(\mathrm{lc}(y^N)) \approx \frac{N}{2}$ για μεγάλες τιμές του N. Επίσης, η διασπορά $\mathrm{Var}(\mathrm{lc}(y^N))$ ικανοποιεί τη σχέση $\mathrm{Var}(\mathrm{lc}(y^N)) \approx \frac{86}{81}$ [124].

Η εύρεση του ελάχιστου LFSR που παράγει μία ακολουθία πραγματοποιείται με τον *αλγόριθμο Berlekamp-Massey* (BMA) [3, 97] (σχήμα 2.4). Είναι ένας διαδεδομένος αλγόριθμος που πρωτοεισήχθη για την αποκωδικοποίηση BCH κωδίκων από τον Berlekamp το 1967 [3], ενώ δύο χρόνια αργότερα ο Massey χρησιμοποίησε τον ίδιο αλγόριθμο για την εύρεση του ελάχιστου LFSR που απαιτείται για την παραγωγή μίας ακολουθίας y^N [97]. Ο αλγόριθμος είναι αναδρομικός και υπολογίζει το πολυώνυμο ανάδρασης του ελάχιστου LFSR για κάθε υπακολουθία y^i, $1 \leq i \leq N$. Για κάθε χρονική στιγμή n, $0 \leq n < N$, γίνεται έλεγχος αν ο τρέχων ελάχιστος LFSR της υπακολουθίας y^n παράγει την υπακολουθία y^{n+1}. Αν ναι, τότε προφανώς ο τρέχων LFSR είναι ο ελάχιστος για την υπακολουθία y^{n+1} και μένει αμετάβλητος (η περίπτωση όπου $d = 0$): διαφορετικά, γίνεται έλεγχος για το αν η γραμμική πολυπλοκότητα της y^{n+1} είναι μεγαλύτερη ή ίση της αντίστοιχης για την y^n. Αν η γραμμική πολυπλοκότητα παραμένει ίση (ισοδύναμα, $2\,\mathrm{lc}(y^n) > n$) ή αυξάνει ($2\,\mathrm{lc}(y^n) \leq n$), τότε μία διορθωτική συνάρτηση προστίθεται στο πολυώνυμο ανάδρασης του ελάχιστου LFSR της y^n προκειμένου να προσδιοριστεί το πολυώνυμο ανάδρασης του ελάχιστου LFSR της y^{n+1}. Αυτή η διορθωτική συνάρτηση είναι πλήρως ορισμένη και εξαρτάται από το πολυώνυμο ανάδρασης του ελάχιστου LFSR της y^j, όπου $j < n$ η πιο πρόσφατη χρονική στιγμή κατά την οποία υπήρξε αύξηση στην γραμμική πολυπλοκότητα. Ο αλγόριθμος Berlekamp-Massey έχει ακόμα πιο απλή μορφή όταν εξετάζουμε δυαδικές ακολουθίες, γιατί σε αυτήν την περίπτωση οι υπεισερχόμενες προσθέσεις πάνω στο σώμα είναι πράξεις XOR. Για μία δυαδική ακολουθία μήκους N, ο BMA έχει υπολογιστική πολυπλοκότητα $O(N^2)$. Μία ισοδύναμη αλλά διαφορετική περιγραφή του BMA, βασισμένη σε ιδιότητες πινάκων που προκύπτουν από την επίλυση ενός κατάλληλου γραμμικού συστήματος, παρουσιάζεται στο [56]. Επίσης, η ισοδυναμία του BMA με τον κλασικό αλγόριθμο του Ευκλείδη που χρησιμοποιείται για αποκωδικοποίηση BCH κωδίκων αποσαφηνίζεται στο [54].

Μία σημαντική ιδιότητα του προφίλ γραμμικής πολυπλοκότητας, που καθιστά τον αλγόριθμο Berlekamp-Massey ισχυρό εργαλείο κρυπτανάλυσης, είναι η ακόλουθη: *ο ελάχιστος LFSR μίας ακολουθίας y^N είναι μοναδικός αν και μόνο αν $\mathrm{lc}(y^N) \leq \frac{N}{2}$.* Με άλλα λόγια, *αν η γραμμική πολυπλοκότητα μίας ακολουθίας είναι L, τότε γνωρίζοντας μόνο $2L$ διαδοχικά στοιχεία της ακολουθίας μας επιτρέπουν, μέσω του BMA, να υπολογίσουμε ολόκληρη την ακολουθία.* Συνεπώς, ο Berlekamp-Massey αλγόριθμος κατέστησε τη γραμμική πολυπλοκότητα ως σημαντικό κρυπτογραφικό κριτήριο: *μία ακολουθία που χρησιμοποιείται ως*



```
b ← 1
k ← 1
B(x) ← 1
n ← 0
L ← 0                                   % linear complexity
c(x) ← 1                                % feedback polynomial
while n < N do
    d ← y_n + Σ_{i=1}^{L} c_i y_{n−i}
    if d ≠ 0 then
        if 2L > N then                  % the linear complexity does not increase
        c(x) ← c(x) − db^{−1} x^k B(x)
        k ← k + 1
        elseif L ≤ n/2 then             % the linear complexity increases
            T(x) ← c(x)
            c(x) ← c(x) − db^{−1} x^k B(x)
            L ← n + 1 − L               % new value of complexity
            b ← d
            B(x) ← T(x)
            k ← 1
        endif
    else                                % d = 0, i.e. no change of LFSR
        x ← x + 1
    endif
    n ← n + 1
endwhile
```

Σχήμα 2.4. Ο αλγόριθμος Berlekamp-Massey

κλειδοροή σε έναν αλγόριθμο ροής πρέπει να έχει υψηλή γραμμική πολυπλοκότητα. Γίνεται φανερό λοιπόν πια ότι οι ακολουθίες μεγίστου μήκους, παρόλο που πληρούν τα κριτήρια ψευδοτυχαιότητας του Golomb, είναι ακατάλληλες για κρυπτογραφικές εφαρμογές: μία ακολουθία μεγίστου μήκους με περίοδο $2^N - 1$ έχει, προφανώς, γραμμική πολυπλοκότητα ίση με N και, συνεπώς, γνώση μόνο $2N$ διαδοχικών bits της ακολουθίας επιτρέπει τον πλήρη προσδιορισμό όλης της ακολουθίας!

Για περιοδικές ακολουθίες υπάρχουν επίσης πολλά σημαντικά αποτελέσματα που σχετίζονται με τη γραμμική πολυπλοκότητα. Από την ανάλυση της Ενότητας 2.1.1 προκύπτει άμεσα ότι *για περιοδική ακολουθία, η γραμμική της πολυπλοκότητα ισούται με το βαθμό του ελάχιστου πολυωνύμου της.* Συνεπώς, ανακαλώντας τους ορισμούς και συμβολισμούς της ενότητας 2.2, ισχύει $\mathrm{lc}(y) = N - \deg(gcd(y^N(z), 1 - z^N))$. Επίσης η γραμμική πολυπλοκότητα μίας περιοδικής ακολουθίας μπορεί να προσδιοριστεί από το φάσμα της μέσω της ακόλουθης Πρότασης, γνωστή ως *Θεώρημα Blahut* [7]:

Πρόταση 2.6. *Η γραμμική πολυπλοκότητα μιας περιοδικής ακολουθίας $y \in \mathbb{F}_q$ ισούται με το πλήθος των μη μηδενικών στοιχείων του Διακριτού Μετασχηματισμού Fourier (εφόσον ο Μετασχηματισμός Fourier ορίζεται), δηλαδή με το βάρος Hamming του μετασχηματισμού Fourier της y.*

Ένα αντίστοιχο αποτέλεσμα ισχύει και για την περίπτωση όπου ο μετασχηματισμός Fourier της ακολουθίας δεν ορίζεται. Συγκεκριμένα, αποδεικνύεται στο [99] ότι για κάθε περιοδική ακολουθία στο σώμα $\mathbb{F}_{p^r}$, p πρώτος, με περίοδο $N = mp^e$, $\gcd(m,p) \neq 1$, η γραμμική της πολυπλοκότητα ισούται με το βάρος Günther του Γενικευμένου Διακριτού Μετασχηματισμού Fourier, όπως αυτός δίνεται στην (2.16). Αυτό είναι και το βασικό πλεονέκτημα του GDFT που προτείνεται στο [99]. Γίνεται φανερό λοιπόν από τα παραπάνω ότι η κρυπτογραφική πληροφορία που αναδεικνύεται από το φάσμα μίας ακολουθίας είναι η γραμμική της πολυπλοκότητα.

Αξίζει τέλος να αναφερθεί πως η γραμμική πολυπλοκότητα περιοδικών δυαδικών ακολουθιών, με περίοδο $N = 2^n$ για κάποιον θετικό ακέραιο n, υπολογίζεται πολύ αποδοτικά από τον αλγόριθμο των Games-Chan [38]. Ο αλγόριθμος αυτός είναι γραμμικός ως προς την περίοδο της ακολουθίας. Μειονέκτημά του, εκτός του ότι μπορεί να εφαρμοστεί μόνο σε ακολουθίες συγκεκριμένης περιόδου, είναι το ότι ολόκληρη η περίοδος της ακολουθίας πρέπει να είναι εκ των προτέρων γνωστή: δεν έχει δηλαδή τη "βήμα-προς-βήμα" δομή του BMA. Επίσης, ο αλγόριθμος των Games-Chan δεν είναι κατάλληλος για ακολουθίες με πολύ μεγάλες περιόδους λόγω του ότι απαιτεί την αποθήκευση ολόκληρης της περιόδου προκειμένου να αρχίσει την επεξεργασία της. Ωστόσο παραμένει πολύ σημαντικός αλγόριθμος επειδή αναδεικνύει ξεχωριστές ιδιότητες που διέπουν τις ακολουθίες με περίοδο κάποια δύναμη του 2. Τέτοιες ακολουθίες έχουν προταθεί για εφαρμογή σε κρυπτογραφικές εφαρμογές: για παράδειγμα, οι T-συναρτήσεις (T-functions) [75], κρυπτογραφικές αδυναμίες των οποίων έχουν μελετηθεί στο [78], εμπίπτουν σε αυτήν την περίπτωση.

Μη γραμμική πολυπλοκότητα

Η μη γραμμική πολυπλοκότητα έχει μελετηθεί σε σημαντικά μικρότερο βαθμό στη βιβλιογραφία από ό,τι η γραμμική. Η τιμή της $c(y)$ για μία ακολουθία y υπολογίζεται από την ακόλουθη Πρόταση [58]:

Πρόταση 2.7. *Για μία ακολουθία y, έστω L ο μεγαλύτερος ακέραιος αριθμός που ικανοποιεί την ακόλουθη ιδιότητα: υπάρχουν $0 \leq i < j \leq N-1-L$ τέτοια ώστε $y_i^{i+L-1} = y_j^{j+L-1}$ και $y_{i+L} \neq y_{j+L}$. Τότε, ισχύει $c(y) = L+1$.*

Κατά αναλογία με το ελάχιστο πολυώνυμο μίας ακολουθίας, ορίζουμε ως *ελάχιστο μη γραμμικό πολυώνυμο (nonlinear minimal polynomial)* μίας ακολουθίας y τη συνάρτηση ανάδρασης οποιουδήποτε FSR μήκους $m = c(y)$ που παράγει την y. Στο [59] αποδεικνύεται πως, για μία ακολουθία y με τιμές σε οποιοδήποτε πεπερασμένο σώμα, ένας κατευθυνόμενος

ακυκλικός γράφος λέξεων (directed acyclic word graph - DAWG) μπορεί να χρησιμοποιηθεί έτσι ώστε να προσδιοριστεί το προφίλ μη γραμμικής πολυπλοκότητας της $y^{\cdot}$ οι κόμβοι-λέξεις του γράφου είναι κατάλληλα επιλεγμένες υπακολουθίες της y. Στο [33] δίνεται μία κατανομή (κατά προσέγγιση) της τιμής της μη γραμμικής πολυπλοκότητας για τυχαίες δυαδικές ακολουθίες, έτσι ώστε να μπορεί να χρησιμοποιηθεί ως μέτρο εκτίμησης της ψευδοτυχαιότητάς τους. Στο [116] παρουσιάζεται μία αλγοριθμική τεχνική για τον υπολογισμό ενός ελάχιστου μη γραμμικού FSR που παράγει μία οποιαδήποτε ακολουθία στο $\mathbb{F}_2$. Η τεχνική αυτή βασίζεται σε ιδιότητες που ενυπάρχουν στον πίνακα του ισοδύναμου γραμμικού συστήματος εξισώσεων, η λύση του οποίου προσδιορίζει τη συνάρτηση ανάδρασης του ελάχιστου FSR. Στο [117] μελετάται η ειδική περίπτωση όπου η συνάρτηση ανάδρασης του FSR είναι πολυώνυμο βαθμού το πολύ 2 (δηλαδή, σε κάθε πολλαπλασιαστή υπεισέρχονται το πολύ 2 βαθμίδες) και παρουσιάζεται αλγόριθμος για τον υπολογισμό του ελάχιστου FSR αυτής της μορφής ο οποίος παράγει δοθείσα δυαδική ακολουθία. Τέλος, στο [115] παρουσιάζεται μέθοδος με την οποία, για κάθε επιθυμητή τιμή γραμμικής πολυπλοκότητας, κατασκευάζονται ακολουθίες με τη μέγιστη δυνατή τιμή για τη μη γραμμική πολυπλοκότητα.

2.5 Παραγωγή ακολουθιών υψηλής πολυπλοκότητας

Από την προηγούμενη ενότητα κατέστη σαφές πως, λόγω του αλγορίθμου Berlekamp-Massey, υψηλή γραμμική πολυπλοκότητα είναι αναγκαία προϋπόθεση για κρυπτογραφικές ακολουθίες. Είδαμε επίσης πως LFSRs με πρωταρχικό χαρακτηριστικό πολυώνυμο παράγουν ακολουθίες με τη μικρότερη δυνατή γραμμική πολυπλοκότητα - τις λεγόμενες ακολουθίες μεγίστου μήκους. Εν τούτοις, οι πολύ καλές λοιπές ιδιότητες αυτών των LFSRs, με κύρια τη μεγάλη περίοδο των παραγομένων ακολουθιών, είχαν σαν αποτέλεσμα να μην τεθούν στο περιθώριο. Η πλειοψηφία των αλγορίθμων ροής εξακολουθούν να χρησιμοποιούν LFSRs ως δομικά συστατικά της γεννήτριας της κλειδοροής (LFSR-based stream ciphers). Προκειμένου όμως να αυξηθεί η γραμμική πολυπλοκότητα των παραγομένων ακολουθιών, υπεισέρχονται και μη γραμμικές πράξεις οι οποίες επιδρούν με κάποιο τρόπο στην κανονική γραμμική λειτουργία των LFSRs. Αυτές οι μη γραμμικές πράξεις κατηγοριοποιούνται ως εξής [105]:

- *Μη γραμμικά φίλτρα (nonlinear filter generators).* Σε αυτήν την περίπτωση, μία μη γραμμική λογική συνάρτηση δρα στις βαθμίδες ενός LFSR - η παραγόμενη κλειδοροή είναι πια η έξοδος αυτής της συνάρτησης.

- *Μη γραμμικοί συνδυαστές (nonlinear combination generators).* Σε αυτήν την περίπτωση, οι έξοδοι πολλών LFSRs "τροφοδοτούν" μία μη γραμμική λογική συνάρτηση - η παραγόμενη κλειδοροή προκύπτει από την έξοδο αυτής της συνάρτησης.

- *Γεννήτριες ελεγχόμενες από ρολόι (Clock-controlled generators).* Αυτή είναι η περίπτωση κατά την οποία ο χρονισμός ενός LFSR (δηλαδή το κάθε πότε αλλάζει κατάσταση) καθορίζεται από την έξοδο ενός άλλου LFSR.

Με άλλα λόγια, οι λογικές συναρτήσεις παίζουν σημαντικό ρόλο στην κατασκευή δυαδικών ακολουθιών μεγάλης γραμμικής πολυπλοκότητας. Στην επόμενη υπο-ενότητα μελετούνται βασικές κρυπτογραφικές ιδιότητες των λογικών συναρτήσεων, ενώ ακολουθεί η ανάλυση των συστημάτων που βασίζονται σε λογικές συναρτήσεις.

2.5.1 Κρυπτογραφικές ιδιότητες λογικών συναρτήσεων

Έστω $\mathbb{F}_2 = \{0, 1\}$ το πεπερασμένο σώμα που αποτελείται από δύο στοιχεία. Κάθε συνάρτηση $f : \mathbb{F}_2^n \to \mathbb{F}_2$ καλείται *λογική συνάρτηση (boolean function)* με n μεταβλητές. Το σύνολο όλων των λογικών συναρτήσεων με n μεταβλητές συμβολίζεται με $\mathbb{B}_n$. Το *συμπλήρωμα (complement)* μιας δυαδικής μεταβλητής x συμβολίζεται ως x', δηλαδή $x' = x + 1$ (όπου η πρόσθεση "+" γίνεται πάνω στο σώμα $\mathbb{F}_2$, με άλλα λόγια είναι πρόσθεση modulo 2 ή, ισοδύναμα, πρόσθεση XOR). Για κάθε λογική συνάρτηση $f(x_1, \ldots, x_n)$ ένας *ελαχιστόρος (minterm)* $\underline{x}_c$ ορίζεται ως $\underline{x}_c = x_1^{c_1} \cdots x_n^{c_n}$, όπου $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$, $x_i^0 = x_i'$ και $x_i^1 = x_i$ [77]. Με άλλα λόγια, ελαχιστόρος είναι ένα γινόμενο στο οποίο εμφανίζονται όλες οι μεταβλητές της συνάρτησης, είτε στην κανονική τους μορφή είτε στη συμπληρωματική τους. Συνεπώς, υπάρχουν 2^n ελαχιστόροι, όπου ο καθένας αντιστοιχεί κατά μονοσήμαντο τρόπο με κάποιο διάνυσμα $c \in \mathbb{F}_2^n$ ή, ισοδύναμα, με κάποια n-άδα $c_1 \ldots c_n$. Υπάρχει λοιπόν μία $'1-1'$ αντιστοιχία μεταξύ του συνόλου των ελαχιστόρων και του συνόλου των διανυσμάτων που ανήκουν στο $\mathbb{F}_2^n$. Για παράδειγμα, ο ελαχιστόρος της 5-άδας 00101 είναι ο $x_1' x_2' x_3 x_4' x_5$.

Παρατήρηση 2.8. Κάθε ελαχιστόρος $\underline{x}_c$, $c = (c_1, \ldots, c_n)$, προσδιορίζεται μονοσήμαντα από την ιδιότητα ότι η τιμή που δίνει είναι 1 αν η i-οστή μεταβλητή του αντικατασταθεί από την τιμή του c_i. Για οποιαδήποτε άλλη ανάθεση τιμών στις μεταβλητές του, ο ελαχιστόρος δίνει τιμή 0.

Μία λογική συνάρτηση μπορεί να αναπαρασταθεί με πολλούς τρόπους. Μία διαδεδομένη αναπαράσταση για συναρτήσεις που χρησιμοποιούνται σε κρυπτογραφικές εφαρμογές είναι η

Αλγεβρική Κανονική Μορφή (Algebraic Normal Form - ANF) που ορίζεται ως

$$f(x_1, \dots x_n) = \sum_{c \in \mathbb{F}_2^n} a_c \, x_1^{c_1} \cdots x_n^{c_n}, \qquad a_c \in \mathbb{F}_2 \tag{2.17}$$

όπου η άθροιση είναι modulo 2, $c = (c_1, \dots, c_n)$, και επίσης $x_i^1 = x_i$, $x_i^0 = 1$. Ο *αλγεβρικός βαθμός (algebraic degree)* ή απλά *βαθμός* μίας συνάρτησης f ορίζεται ως $\deg(f) = \max\{\mathrm{wt}(c) : a_c = 1\}$, όπου με $\mathrm{wt}(c)$ συμβολίζουμε το πλήθος των $'1'$ στο διάνυσμα c - δηλαδή, το *βάρος Hamming (Hamming weight)* του c. Όταν $\deg(f) = 1, 2, \text{or } 3$, η f καλείται *γραμμική (affine)*, *τετραγωνική (quadratic)*, ή *κυβική (cubic)* αντίστοιχα. Το άθροισμα όλων των όρων $x_1^{c_1} \cdots x_n^{c_n}$ στην (2.17) με $\mathrm{wt}(c) = 1, 2$ ή 3 αποτελεί το *γραμμικό (linear)* (*τετραγωνικό (quadratic)*) ή *κυβικό (cubic)* τμήμα της f αντιστοίχως. Αν k είναι ο βαθμός της f, τότε κάθε όρος $x_1^{c_1} \cdots x_n^{c_n}$ που είναι παρών στην (2.17) με $\mathrm{wt}(c) = k$ ονομάζεται *μεγιστοβάθμιος όρος* της f.

Μία άλλη αναπαράσταση των λογικών συναρτήσεων είναι η *Κανονική Μορφή Διάζευξης (Disjunctive Normal Form - DNF)*, όπου εκφράζεται ως το άθροισμα εκείνων των ελαχιστόρων που αντιστοιχούν στα διανύσματα του συνόλου $\{c \in \mathbb{F}_2^n : f(c) = 1\}$: με άλλα λόγια, η DNF δίνεται από τον τύπο

$$f(x_1, \dots x_n) = \sum_{c \in \mathbb{F}_2^n} f(c) \, x_1^{c_1} \cdots x_n^{c_n} \ , \tag{2.18}$$

όπου $x_i^1 = x_i$, $x_i^0 = x_i'$. Η άθροιση στην (2.18) είναι η λογική πρόσθεση (λογική πράξη OR), αλλά ισοδύναμα για τη DNF μπορούμε να θεωρούμε ότι η πρόσθεση είναι modulo 2 (λογικό XOR), λόγω της ιδιότητας των ελαχιστόρων που αναφέρεται στην Παρατήρηση 2.8.

Μία αναπαράσταση των λογικών συναρτήσεων, που προσομοιάζει τόσο την (2.17) όσο και την (2.18), είναι το *XOR Άθροισμα Γινομένων (Exclusive-or Sum-Of-Products - ESOP)*. Αυτή η αναπαράσταση γενικεύει την (2.17) γιατί επιτρέπει σε μία μεταβλητή να είναι παρούσα σε ένα γινόμενο είτε στην κανονική της μορφή είτε στη συμπληρωματική [132]. Στη γενική περίπτωση, η ESOP αναπαράσταση δεν είναι μοναδική για μία λογική συνάρτηση (εν αντιθέσει με την ANF και την DNF).

Για παράδειγμα, ας θεωρήσουμε τη λογική συνάρτηση f με 3 μεταβλητές της οποίας η ANF δίνεται από τη σχέση $f(x_1, x_2, x_3) = x_2 + x_1 x_2$. Τότε η DNF είναι η $x_1' x_2 x_3 + x_1' x_2 x_3'$, ενώ μία ESOP αναπαράσταση της f είναι η $x_1' x_2$.

Ο *πίνακας αληθείας (truth table)* της $f \in \mathbb{B}_n$ είναι το διάνυσμα

$$f = \big(f(0, 0, \dots, 0), f(1, 0, \dots, 0), \dots, f(1, 1, \dots, 1)\big) \tag{2.19}$$

μήκους 2^n. Για απλοποίηση στο συμβολισμό, με το γράμμα f θα υποδηλώνουμε επίσης και το διάνυσμα της (2.19). Αξίζει να σημειωθεί ότι οι κωδικές λέξεις του δυαδικού *Reed-Muller κώδικα* τάξης r, ο οποίος συμβολίζεται ως $\mathfrak{R}(r,n)$, συμπίπτουν με τους πίνακες αληθείας των λογικών συναρτήσεων f για τις οποίες ισχύει $\deg(f) \leq r$. [95].

Παρατήρηση 2.9. Οι Reed-Muller κώδικες διόρθωσης σφάλματος, που προτάθηκαν από τους D. E. Muller και L.S. Reed το 1954, είναι κώδικες με πλούσιο μαθηματικό υπόβαθρο και αποτελούν αντικείμενο έντονης ερευνητικής δραστηριότητας, παρόλο που η ελάχιστη απόστασή τους είναι μικρότερη από αυτή των BCH κωδίκων· η αξία τους βασίζεται κυρίως στο ότι έχουν πολύ αποδοτικούς αλγορίθμους αποκωδικοποίησης [94]. Από κρυπτογραφική άποψη, η μελέτη των Reed-Muller κωδίκων ισοδυναμεί με μελέτη κρυπτογραφικών λογικών συναρτήσεων, αποτυπώνοντας κατ' αυτόν τον τρόπο μία ακόμα συσχέτιση μεταξύ της θεωρίας κωδίκων και της κρυπτογραφίας.

Το *βάρος Hamming (Hamming weight)* της f ισούται με το πλήθος των μονάδων στον πίνακα αληθείας της και συμβολίζεται ως $\mathrm{wt}(f)$. Η f καλείται *ισοβαρής (balanced)* αν $\mathrm{wt}(f) = 2^{n-1}$, όταν δηλαδή το πλήθος των μονάδων ισούται με το πλήθος των μηδενικών στον πίνακα αληθείας της. Η *απόσταση Hamming (Hamming distance)* μεταξύ δύο συναρτήσεων $f, g \in \mathbb{B}_n$ ορίζεται ως $\mathrm{wt}(f+g)$.

Ορισμός 2.10. Έστω $j_1, \ldots, j_k$ ακέραιοι αριθμοί τέτοιοι ώστε $1 \leq j_1 < \cdots < j_k \leq n$ και $k < n$. Έστω επίσης $r = r_1 + 2r_2 + \cdots + 2^{k-1}r_k$ η δυαδική αναπαράσταση του ακεραίου $0 \leq r < 2^k$. Η έκφραση

$$f(x_1, \ldots, x_n) = \sum_{r=0}^{2^k-1} \left(\prod_{i=1}^{k} (x_{j_i} + r_i') \right) f_r \tag{2.20}$$

καλείται ανάπτυγμα k τάξης κατά Shannon (kth order Shannon's expansion formula) της συνάρτησης f ως προς τις μεταβλητές $x_{j_1}, \ldots, x_{j_k}$ (όπου r_i' το συμπλήρωμα του r_i και κάθε συνάρτηση $f_r \in \mathbb{B}_{n-k}$ δεν εξαρτάται από τις μεταβλητές $x_{j_1}, \ldots, x_{j_k}$).

Από τον παραπάνω ορισμό γίνεται φανερό πως, για κάθε $x_{j_1}, \ldots, x_{j_k}$, οι υπο-συναρτήσεις $f_0, \ldots, f_{2^k-1}$ ορίζονται μονοσήμαντα, καθώς η f_r μπορεί να προσδιοριστεί από την f θέτοντας $x_{j_i} = r_i$, $1 \leq i \leq k$. Αν $\mathcal{J} = \{j_1, \ldots, j_k\}$, τότε το ανάπτυγμα k τάξης κατά Shannon ως προς τις μεταβλητές του συνόλου $\mathcal{J}$ θα συμβολίζεται ως $f = f_0 \parallel_{\mathcal{J}} \cdots \parallel_{\mathcal{J}} f_{2^k-1}$. Στην ειδική περίπτωση όπου $\mathcal{J} = \{j\}$, τότε το ανάπτυγμα γράφεται $f = f_0 \parallel_j f_1$. Αν $\mathcal{J} = \{n-k+1, \ldots, n\}$, τότε ο πίνακας αληθείας της $f(x_1, \ldots, x_n)$ ισούται με το διάνυσμα που

προκύπτει από τη *συνένωση (concatenation)* των πινάκων αληθείας των υπο-συναρτήσεων $f_r(x_1, \ldots, x_{n-k})$, $0 \leq r < 2^k$ [106].

Ορισμός 2.11. Ο μετασχηματισμός Walsh ή Hadamard μίας λογικής συνάρτησης $f \in \mathbb{B}_n$ στο σημείο $a \in \mathbb{F}_2^n$ δίνεται από τη σχέση [95]

$$\widehat{\chi}_f(a) = \sum_{x \in \mathbb{F}_2^n} \chi_f(x)(-1)^{\langle a,x \rangle} = 2^n - 2\,\mathrm{wt}(f \oplus \phi_a) \tag{2.21}$$

όπου $\chi_f(x) = (-1)^{f(x)}$ και ϕ_a είναι η γραμμική συνάρτηση $\phi_a(x) = \langle a, x \rangle = a_1x_1 + \cdots + a_nx_n$ (η άθροιση στην (2.21) είναι πάνω στους πραγματικούς αριθμούς).

Από τη (2.21) προκύπτει πως η f είναι ισοβαρής αν και μόνο αν $\widehat{\chi}_f(0) = 0$.

Ορισμός 2.12. Η ελάχιστη απόσταση Hamming μεταξύ της f και όλων των γραμμικών συναρτήσεων ονομάζεται *μη γραμμικότητα (nonlinearity)* της f και συμβολίζεται με $\mathcal{NL}_f$.

Η μη γραμμικότητα της f υπολογίζεται από το μετασχηματισμό Walsh μέσω της ακόλουθης σχέσης [104]

$$\mathcal{NL}_f = \min_{g \in \mathfrak{R}(1,n)} \big\{\mathrm{wt}(f+g)\big\} = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\widehat{\chi}_f(a)| \,. \tag{2.22}$$

Ορισμός 2.13. Κάθε γραμμική συνάρτηση g τέτοια ώστε $\mathrm{wt}(f+g) = \mathcal{NL}_f$ είναι *βέλτιστη γραμμική προσέγγιση (best affine approximation)* της f και συμβολίζεται με λ_f. Το σύνολο όλων των βέλτιστων γραμμικών προσεγγίσεων της f συμβολίζεται ως $\mathcal{A}_f \subseteq \mathfrak{R}(1,n)$.

Ο μετασχηματισμός Walsh μίας συνάρτησης $f \in \mathbb{B}_n$ ικανοποιεί την ακόλουθη σχέση, γνωστή ως *εξίσωση Parseval (Parseval's equation)* [95]:

$$\sum_{a \in \mathbb{F}_2^n} \widehat{\chi}_f(a)^2 = 2^{2n} \,. \tag{2.23}$$

Συνδυάζοντας τις (2.22) και (2.23) συμπεραίνουμε ότι η μέγιστη δυνατή μη γραμμικότητα για την f είναι $2^{n-1} - 2^{n/2-1}$, και για κάθε τέτοια f ισχύει $\widehat{\chi}_f(a) = \pm 2^{n/2}$ $\forall$ $a \in \mathbb{F}_2^n$. Οι συναρτήσεις αυτές έχουν άρτιο πλήθος μεταβλητών και ονομάζονται *συναρτήσεις bent*. Οι συναρτήσεις bent ορίστηκαν για πρώτη φορά στο [123] και παρουσιάζουν σημαντικό κρυπτογραφικό ενδιαφέρον γιατί είναι υψηλά μη γραμμικές - ένα χαρακτηριστικό που είναι απαραίτητο για κρυπτογραφικές συναρτήσεις, όπως θα αποσαφηνιστεί στις υπο-ενότητες 2.5.2 και 2.5.3. Για κάθε συνάρτηση bent n μεταβλητών, ο βαθμός της είναι το πολύ $\frac{n}{2}$ [123]. Οι συναρτήσεις bent έχουν επίσης άμεση εφαρμογή, εκτός της κρυπτογραφίας, τόσο στη θεωρία κωδίκων

(για παράδειγμα, στη σχεδίαση κωδίκων Kerdock [95]) όσο και στις επικοινωνίες (για παράδειγμα, στη σχεδίαση ακολουθιών για CDMA (Code Division Multiple Access) συστήματα [43]). Λόγω της σπουδαιότητάς τους, έχουν προταθεί πολλές μεθοδολογίες κατασκευής συναρτήσεων bent [15, 22, 30, 32, 55, 123]. Ωστόσο, οι συναρτήσεις bent δεν είναι ισοβαρείς, γεγονός που τις καθιστά μη κατάλληλες για άμεση χρήση σε κρυπτογραφικές εφαρμογές (στις αμέσως επόμενες ενότητες 2.5.2-2.5.3 θα γίνει σαφής η αναγκαιότητα για τις κρυπτογραφικές συναρτήσεις να έχουν ισομοιρασμένα 1 και 0 στον πίνακα αληθείας τους). Συνεπώς, έχουν προταθεί πολλές κατασκευές συναρτήσεων που επιτυγχάνουν υψηλή (όχι απαραίτητα τη μέγιστη δυνατή) μη γραμμικότητα, ενώ επίσης μπορούν να είναι και ισοβαρείς. Προς αυτήν την κατεύθυνση έχουν προταθεί οι *συναρτήσεις partially bent* [14], που είναι υπερ-σύνολο των συναρτήσεων bent. Οι συναρτήσεις partially bent αποτελούν με τη σειρά τους υποσύνολο των *συναρτήσεων plateaued* που ορίζονται στο [138] ως οι συναρτήσεις εκείνες των οποίων ο μετασχηματισμός Walsh παίρνει το πολύ 3 τιμές, τις 0 και $\pm\lambda$, όπου το λ είναι αριθμός της μορφής 2^r για κάποιο $r \geq \frac{n}{2}$. Έτσι, για μία συνάρτηση plateaued οι τιμές του μετασχηματισμού Walsh διαιρούνται από το $2^{\frac{n}{2}}$ ($2^{\frac{n+1}{2}}$) αν το n είναι άρτιος (περιττός). Τα παραπάνω οδηγούν στον ακόλουθο ορισμό των *συναρτήσεων semi-bent functions*, που αποτελούν γενίκευση των συναρτήσεων bent για την περίπτωση περιττού πλήθους μεταβλητών:

Ορισμός 2.14 ([74]). Μία συνάρτηση $f \in \mathbb{B}_n$ είναι συνάρτηση bent, για n άρτιο αριθμό, αν και μόνο αν $\widehat{\chi}_f(a) = \pm 2^{n/2}$ για κάθε $a \in \mathbb{F}_2^n$. Μία συνάρτηση $g \in \mathbb{B}_n$ είναι semi-bent, για n περιττό αριθμό, αν και μόνο αν $\widehat{\chi}_g(a) \in \left\{0, \pm 2^{(n+1)/2}\right\}$ για κάθε $a \in \mathbb{F}_2^n$.

Η μη γραμμικότητα των συναρτήσεων semi-bent είναι $2^{n-1} - 2^{(n-1)/2}$. Ωστόσο, παραμένει ανοιχτό ερευνητικό πρόβλημα για το ποια είναι η μέγιστη δυνατή τιμή της μη γραμμικότητας που μπορεί να έχει μία συνάρτηση περιττού πλήθους μεταβλητών (εν αντιθέσει με την περίπτωση του άρτιου πλήθους μεταβλητών, όπου η μέγιστη μη γραμμικότητα εξασφαλίζεται από τις συναρτήσεις bent). Πρόσφατα αποδείχτηκε ότι υπάρχουν συναρτήσεις που έχουν μη γραμμικότητα μεγαλύτερη από $2^{n-1} - 2^{(n-1)/2}$ για περιττό $n \geq 9$ [71].

Ορισμός 2.15. Έστω $X_1, X_2, \ldots, X_n$ ανεξάρτητες δυαδικές τυχαίες μεταβλητές, όπου η κάθε μία παίρνει την τιμή 1 με πιθανότητα $\frac{1}{2}$. Μία λογική συνάρτηση $f(x_1, x_2, \ldots, x_n)$ καλείται *ανθεκτική σε συσχετίσεις τάξης m (mth-order correlation-immune)* εάν για κάθε υποσύνολο $(X_{i_1}, X_{i_2}, \ldots, X_{i_m})$ m τυχαίων μεταβλητών, $1 \leq i_1 < i_2 < \ldots < i_m \leq n$, η τυχαία μεταβλητή $Z = f(X_1, X_2, \ldots, X_n)$ είναι στατιστικά ανεξάρτητη από το διάνυσμα τυχαίων μεταβλητών $(X_{i_1}, X_{i_2}, \ldots, X_{i_m})$.

Αν μία συνάρτηση ανθεκτική σε συσχετίσεις τάξης m είναι επιπλέον και ισοβαρής, τότε καλείται με τον πιο γενικό όρο *ανθεκτική τάξης m(m-th order resilient)*. Αυτές οι συναρτήσεις μπορούν να περιγραφούν με απλά λόγια από την ακόλουθη ιδιότητα: αν αναθέσουμε οποιεσδήποτε συγκεκριμένες τιμές σε οποιεσδήποτε m μεταβλητές, τότε η προκύπτουσα συνάρτηση $n-m$ μεταβλητών είναι ισοβαρής (και, προφανώς, το ίδιο ισχύει αν ανατεθούν συγκεκριμένες τιμές σε οποιεσδήποτε r μεταβλητές, $0 \leq r \leq m$) [137]. Η ανθεκτικότητα σε συσχετίσεις μίας συνάρτησης συνδέεται με το μετασχηματισμό Walsh αυτής μέσω της ακόλουθης Πρότασης [49].

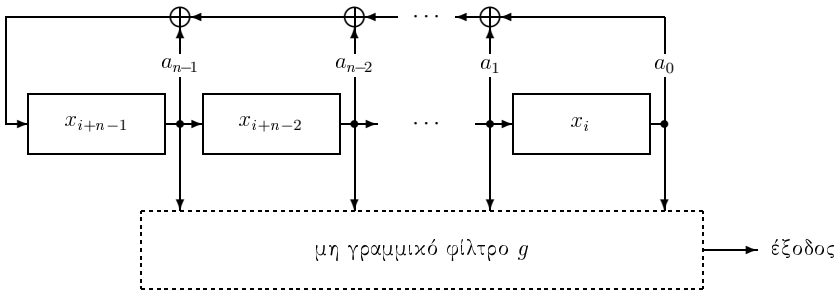
Πρόταση 2.16. *Μία λογική συνάρτηση $f \in \mathbb{B}_n$ είναι ανθεκτική σε συσχετίσεις τάξης m αν και μόνο αν $\widehat{\chi}_f(a) = 0$ για κάθε $a \in \mathbb{F}_2^n$ με $1 \leq \mathrm{wt}(a) \leq m < n$.*

Όπως θα διαφανεί στη συνέχεια, είναι σημαντικό για τις κρυπτογραφικές συναρτήσεις να έχουν μεγάλης τάξης ανθεκτικότητα σε συσχετίσεις. Έχουν προταθεί διάφορες τεχνικές για την κατασκευή τέτοιων συναρτήσεων [12, 96, 129, 134]. Μία σημαντική ιδιότητα που τις χαρακτηρίζει είναι η ακόλουθη: αν μία συνάρτηση με n μεταβλητές είναι ανθεκτική σε συσχετίσεις τάξης m, τότε ο βαθμός της είναι το πολύ $n-m$, ενώ αν επιπρόσθετα είναι και ισοβαρής, τότε ο βαθμός της είναι το πολύ $n-m-1$ όταν $1 \leq m \leq n-m-2$ [129]. Επίσης, για μία ισοβαρή λογική συνάρτηση n μεταβλητών η οποία είναι ανθεκτική σε συσχετίσεις τάξης m, η μέγιστη δυνατή τιμή της μη γραμμικότητάς της ισούται με $2^{n-1} - 2^{m+1}$ για $(2n-7)/3 \leq m \leq n-2$ [133].

Εκτός από την υψηλή μη γραμμικότητα και την ανθεκτικότητα σε συσχετίσεις, υπάρχουν και άλλα κριτήρια που πρέπει κατά το δυνατόν να πληρούνται από μία κρυπτογραφική συνάρτηση (όπως ο μεγάλος βαθμός, το να είναι ισοβαρής κ.α.). Πολλά από αυτά είναι αντικρουόμενα (όπως για παράδειγμα η τάξη ανθεκτικότητας σε συσχετίσεις και ο βαθμός μίας συνάρτησης), οπότε απώτερος στόχος είναι η κατασκευή λογικών συναρτήσεων που να επιτυγχάνουν όσο το δυνατόν καλύτερα την ταυτόχρονη ικανοποίηση όλων αυτών των κριτηρίων, με μία κατά κάποιο τρόπο εξισορρόπησή τους. Μία συγκεντρωτική περιγραφή όλων των κρυπτογραφικών ιδιοτήτων λογικών συναρτήσεων, καθώς και όλων των σημαντικών κατασκευών συναρτήσεων που έχουν προταθεί στη βιβλιογραφία, παρουσιάζεται στο [16].

2.5.2 Μη γραμμικά φίλτρα

Μία τεχνική που οδηγεί σε δυαδικές ακολουθίες μεγάλης γραμμικής πολυπλοκότητας είναι η εφαρμογή μίας μη γραμμικής λογικής συνάρτησης στις βαθμίδες ενός πρωταρχικού LFSR,



Σχήμα 2.5. Εφαρμογή μη γραμμικού φίλτρου σε έναν LFSR

όπως απεικονίζεται στο Σχήμα 2.5. Η συνάρτηση g καλείται *μη γραμμικό φίλτρο (nonlinear filter function)*. Ιδανικά, το μη γραμμικό φίλτρο θα πρέπει να είναι ισοβαρής συνάρτηση, έτσι ώστε να εξασφαλίζεται ομοιόμορφη κατανομή των bits 0 ή 1 στην παραγόμενη κλειδοροή. Στη γενική περίπτωση, οι παραγόμενες ακολουθίες έχουν μεγάλη περίοδο και υψηλή γραμμική πολυπλοκότητα [47]. Ωστόσο, ανοιχτό ερευνητικό πρόβλημα παραμένει ο ακριβής προσδιορισμός της τιμής της γραμμικής πολυπλοκότητας των ακολουθιών που παράγονται από συστήματα αυτής της κατηγορίας. Ένα άνω φράγμα για τη γραμμική πολυπλοκότητα δίνεται από τον Key στο [73]: συγκεκριμένα, αν n είναι το μήκος του LFSR και k ο βαθμός του μη γραμμικού φίλτρου, τότε η γραμμική πολυπλοκότητα της ακολουθίας που παράγεται είναι το πολύ ίση με $L_k = \sum_{i=1}^{k} \binom{n}{i}$. Το ίδιο αποτέλεσμα δίνουν και οι Massey και Serconek στο [98], κάνοντας χρήση του μετασχηματισμού Fourier της παραγομένης ακολουθίας. Η ισοδυναμία των δύο αυτών προσεγγίσεων αποδεικνύεται στο [112]. Το άνω φράγμα L_k είναι απόρροια του γεγονότος ότι το ελάχιστο πολυώνυμο της παραγομένης ακολουθίας έχει διακριτές ρίζες της μορφής α^e, με $\mathrm{wt}(e) \leq k$ όπου $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$ οι ρίζες του χαρακτηριστικού πολυωνύμου του LFSR και $\mathrm{wt}(e)$ το πλήθος των $'1'$ (*βάρος Hamming*) στη δυαδική αναπαράσταση του ακέραιου e. Ο Rueppel στο [124] αποδεικνύει πως, αν το μήκος n του LFSR είναι πρώτος αριθμός, τότε το ποσοστό των λογικών συναρτήσεων που οδηγούν σε ακολουθίες με τη μέγιστη δυνατή γραμμική πολυπλοκότητα L_k προσεγγίζει την τιμή $e^{-\frac{L_k}{n \cdot 2^n}} > e^{-\frac{1}{n}}$. Με άλλα λόγια, για μεγάλες τιμές του n, η πλειοψηφία των μη γραμμικών συναρτήσεων επιτυγχάνουν τη μέγιστη δυνατή τιμή γραμμικής πολυπλοκότητας για τις ακολουθίες που παράγουν. Για ειδικές περιπτώσεις των n και k, μία βελτίωση στο άνω φράγμα L_k αποδεικνύεται στο [10], όπου λαμβάνεται υπ' όψιν το γεγονός ότι υπάρχουν ακέραιοι n τέτοιοι ώστε κάποιες κυκλοτομικές κλάσεις modulo $2^n - 1$ να έχουν πλήθος στοιχείων μικρότερο από n - οι λεγόμενες *ελλιπείς κυκλοτομικές κλάσεις (regular cosets)*.

Στη γενική περίπτωση, δεν μπορούν να προσδιοριστούν πλήρως τα στοιχεία του $\mathbb{F}_{2^n}$ που

είναι ρίζες του ελάχιστου πολυωνύμου της παραγόμενης ακολουθίας· κατά συνέπεια δεν μπορεί να υπολογιστεί η γραμμική της πολυπλοκότητα, η οποία ισούται με το πλήθος των στοιχείων αυτών. Σε αυτήν την κατεύθυνση, ο Rueppel στο [124] αποδεικνύει την ακόλουθη συνθήκη:

Πρόταση 2.17. *Έστω ένας πρωταρχικός LFSR με n βαθμίδες, του οποίου το χαρακτηριστικό πολυώνυμο έχει ρίζες $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$ (όπου α είναι πρωταρχικό στοιχείο του σώματος $\mathbb{F}_{2^n}$). Έστω επίσης ότι εφαρμόζεται στον LFSR ένα μη γραμμικό φίλτρο $g : \mathbb{F}_2^n \to \mathbb{F}_2$ βαθμού $k \leq n$, της μορφής $g(x_1, x_2, \ldots, x_n) = x_{t_1} x_{t_2} \ldots x_{t_k}$, όπου $1 \leq t_1 < t_2 < \ldots < t_k \leq x_n$. Τότε, για κάθε ακέραιο e με $\mathrm{wt}(e) = k$, το στοιχείο α^e είναι ρίζα του ελάχιστου πολυωνύμου της ακολουθίας αν και μόνο αν η ακόλουθη ορίζουσα είναι μη μηδενική*

$$T_e = \begin{vmatrix} \alpha^{t_1 2^{e_1}} & \ldots & \alpha^{t_k 2^{e_1}} \\ \alpha^{t_1 2^{e_2}} & \ldots & \alpha^{t_k 2^{e_2}} \\ \vdots & & \vdots \\ \alpha^{t_1 2^{e_k}} & \ldots & \alpha^{t_k 2^{e_k}} \end{vmatrix}, \tag{2.24}$$

όπου $e = 2^{e_1} + 2^{e_2} + \ldots + 2^{e_k}$, $0 \leq e_1 < e_2 < \ldots < e_k < n$.

Παρατήρηση 2.18. Στην παραπάνω σχέση, οι δείκτες t_i αναφέρονται σε συγκεκριμένες βαθμίδες του LFSR οι οποίες υπεισέρχονται στο φίλτρο ή, ισοδύναμα, σε ολισθήσεις της αρχικής ακολουθίας εξόδου του LFSR (οπότε η έξοδος του φίλτρου αντιστοιχεί σε γινόμενο των διαφόρων ολισθήσεων της αρχικής ακολουθίας εξόδου του LFSR, όπως αυτές καθορίζονται από την Αλγεβρική Κανονική Μορφή του φίλτρου). Πρέπει να σημειωθεί ότι η αρίθμηση στις βαθμίδες, αν αναλογιστούμε το Σχήμα 2.5, γίνεται από δεξιά προς τα αριστερά: για παράδειγμα, αν $g(x_1, \ldots, x_n) = x_1 x_2$, τότε το φίλτρο αυτό αντιστοιχεί στο γινόμενο των δύο δεξιότερων βαθμίδων του LFSR στο Σχήμα 2.5.

Η σχέση (2.24) είναι γνωστή ως *κριτήριο ύπαρξης ριζών (root presence test)* και αποτελεί βασικό μαθηματικό εργαλείο για την κατασκευή κατάλληλων φίλτρων που να επιτυγχάνουν την παραγωγή ακολουθιών με εγγυημένη ελάχιστη τιμή της γραμμικής πολυπλοκότητας. Μία τυπική και σημαντική κατηγορία φίλτρων είναι τα *ισαπέχοντα φίλτρα (equidistant filters)* [124], τα οποία έχουν έναν μόνο μεγιστοβάθμιο όρο της μορφής

$$x_{t_1} x_{t_1+\delta} x_{t_1+2\delta} \ldots x_{t_1+(k-1)\delta}, \qquad \gcd(\delta, 2^n - 1) = 1.$$

Τα ισαπέχοντα φίλτρα έχουν την ιδιότητα ότι εξασφαλίζουν τον μη μηδενισμό της ορίζουσας T_e για κάθε στοιχείο α^e με $\mathrm{wt}(e) = k$, γιατί σε αυτήν την περίπτωση η T_e ισούται με την ορίζουσα ενός Vandermonde πίνακα και, κατά συνέπεια, μηδενίζεται αν και μόνο αν $\alpha^{\delta 2^{e_i}} = \alpha^{\delta 2^{e_j}}$ για

κάποιο ζευγάρι $e_i \neq e_j$· όμως ο ακέραιος δ είναι πρώτος ως προς την τάξη 2^n-1 του στοιχείου α, οπότε εξασφαλίζεται η σχέση $T_e \neq 0$. Με άλλα λόγια, *κάθε ισαπέχον φίλτρο βαθμού k παράγει ακολουθίες με γραμμική πολυπλοκότητα εγγυημένα μεγαλύτερη ή ίση από* $\binom{n}{k}$ (αφού όλα τα στοιχεία a^e, $\mathrm{wt}(e) = k$, είναι ρίζες του ελάχιστου πολυωνύμου της ακολουθίας). Η τιμή $\binom{n}{k}$ μπορεί να γίνει πολύ μεγάλη για τυπικές τιμές των n, k (όπως για παράδειγμα για $n = 128$, $k = 50$), εξασφαλίζοντας υψηλή γραμμική πολυπλοκότητα. Στο [112] αποδεικνύεται ότι η ίδια ελάχιστη τιμή για τη γραμμική πολυπλοκότητα μπορεί επίσης να επιτευχθεί, υπό κάποιες συνθήκες, ακόμα κι αν άρουμε τον περιορισμό $\gcd(\delta, 2^n - 1) = 1$: για παράδειγμα, το κάτω φράγμα $\binom{n}{k}$ ισχύει πάντα όταν το n είναι πρώτος αριθμός. Στο ίδιο άρθρο επίσης προσδιορίζεται ως κάτω φράγμα της γραμμικής πολυπλοκότητας για τα ισαπέχοντα φίλτρα με αυθαίρετο δ η τιμή $\binom{t}{k}\binom{n}{t}^k$, όπου t ο μικρότερος ακέραιος τέτοιος ώστε $2^n - 1 | \delta(2^t - 1)$. Αντίστοιχα αποτελέσματα για κάτω φράγματα της γραμμικής πολυπλοκότητας αποδεικνύονται τόσο στο [124] όσο και στο [112] για την πρακτικά πιο ενδιαφέρουσα περίπτωση όπου οι μεγιστοβάθμιοι όροι του ισαπέχοντος φίλτρου είναι πολλοί, όλοι χαρακτηριζόμενοι από την ίδια σταθερά δ. Πρόσφατα αποτελέσματα σχετικά με τα ισαπέχοντα φίλτρα αποδεικνύονται στο [80], κάνοντας χρήση ιδιοτήτων που ενυπάρχουν στις λεγόμενες *γενικευμένες ορίζουσες Vandermode (generalized Vandermode determinants)*: συγκεκριμένα, αποδεικνύεται πως αν $4 \leq k \leq n-2$ τότε για την ακολουθία εξόδου y ισχύει $\mathrm{lc}(y) \geq \binom{n}{k} + n$, ενώ για $k = 2, 3, n-1$ έχουμε $\mathrm{lc}(y) \geq \binom{n}{k} + \binom{n}{k-1}$.

Διάφορα άλλα μη γραμμικά φίλτρα, με καλά χαρακτηριστικά ως προς τη γραμμική πολυπλοκότητα, έχουν προταθεί στη βιβλιογραφία. Στο [79] αποδεικνύεται μία συνθήκη ανάλογη της (2.24), η οποία ελέγχει αν ένα στοιχείο α^e με $\mathrm{wt}(e) = k - 1$ είναι ρίζα του ελαχίστου πολυωνύμου της παραγόμενης ακολουθίας. Στο ίδιο άρθρο επίσης περιγράφεται μία νέα κατασκευή φίλτρων, των οποίων ο μεγιστοβάθμιος όρος προσδιορίζεται από τα στοιχεία που απαρτίζουν μια *κανονική βάση (normal basis)* του σώματος $\mathbb{F}_{2^n}$. Τα φίλτρα αυτά ορίζονται ως εξής: έστω $\{\alpha^e, \alpha^{2e}, \ldots, \alpha^{2^{n-1}e}\}$ μία κανονική βάση του $\mathbb{F}_{2^n}$. Ορίζουμε το σύνολο

$$W_{s,k} = \{2^s e \mod N, \ldots, 2^{s+k-1} e \mod N\},$$

το οποίο έχει k στοιχεία ($k \leq n$). Συμβολίζουμε ως $W_{s,k}(1)$ το μικρότερο στοιχείο του $W_{s,k}$, ως $W_{s,k}(2)$ το αμέσως μεγαλύτερο κ.ο.κ., δηλαδή $W_{s,k}(1) < W_{s,k}(2) < \ldots < W_{s,k}(k)$. Ας υποθέσουμε ότι υπάρχουν s, k τέτοια ώστε $W_{s,k}(k) - W_{s,k}(1) < n$. Τότε, το φίλτρο $g(x_1, \ldots, x_n) = x_{t_1} x_{t_2} \ldots x_{t_k}$ ορίζεται ως εξής: αν $(x_{j-1}\ x_{j-2}\ \ldots\ x_{j-n})$ είναι η τρέχουσα

κατάσταση του LFSR κάποια χρονική στιγμή, τότε η έξοδος του φίλτρου είναι

$$x_{j-t_1}x_{j-t_2}\dots x_{j-t_k},$$

όπου τα t_m, $m=1,2,\dots,k$, προσδιορίζονται από την $t_m = W_{s,k}(k)-W_{s,k}(1)+1$. Αποδεικνύεται πως κάθε τέτοιο φίλτρο βαθμού k επιτυγχάνει το ίδιο κάτω φράγμα $\binom{n}{k}$ για τη γραμμική πολυπλοκότητα, όσο και τα ισαπέχοντα φίλτρα. Το ίδιο αποτέλεσμα δίνεται και στο [11], όπου επίσης παρουσιάζεται μία απαρίθμηση αυτών των φίλτρων. Γενικότερες συνθήκες κάτω από τις οποίες ένα μη γραμμικό φίλτρο επιτυγχάνει την παραγωγή ακολουθιών με εγγυημένη ελάχιστη τιμή $\binom{n}{k}$ για τη γραμμική πολυπλοκότητα δίνονται στο [86], για την περίπτωση όπου $\gcd(n,k)=1$.

Η συντριπτική πλειοψηφία των παραπάνω αποτελεσμάτων (όπως η σχέση (2.24)) ισχύουν όχι μόνο για δυαδικές ακολουθίες, αλλά για ακολουθίες σε οποιοδήποτε σώμα με χαρακτηριστική 2. Αποτελέσματα για τη γενικότερη περίπτωση, όπου οι παραγόμενες ακολουθίες παίρνουν τιμές σε κάποιο σώμα $\mathbb{F}_q$ με q δύναμη κάποιου περιττού πρώτου αριθμού, παρουσιάζονται στο [52].

Κρυπτανάλυση σε συστήματα μη γραμμικών φίλτρων

Διάφορες κρυπταναλυτικές τεχνικές έχουν αναπτυχθεί για την ανάλυση συστημάτων που βασίζονται σε μη γραμμικά φίλτρα. Στην πλειοψηφία των περιπτώσεων, τόσο το χαρακτηριστικό πολυώνυμο του LFSR όσο και το μη γραμμικό φίλτρο είναι δημοσίως γνωστά· η μυστικότητα της παραγόμενης ακολουθίας-κλειδιού έγκειται στο ότι μένει μυστική η αρχική κατάσταση του LFSR. Κατά συνέπεια, οι κρυπταναλυτικές τεχνικές αποσκοπούν στον προσδιορισμό αυτής της αρχικής κατάστασης. Η ανάπτυξη κρυπταναλυτικών μεθόδων βοηθάει στο να καθορίζονται συγκεκριμένες απαιτήσεις για τα χαρακτηριστικά ενός συστήματος που βασίζεται σε μη γραμμικό φίλτρο, προκειμένου να είναι κατά το δυνατόν πιο ασφαλές.

Επιθέσεις συσχέτισης: Στο [130] αναλύεται μία μέθοδος κρυπτανάλυσης που βασίζεται σε ιδιότητες της συνάρτησης ετεροσυσχέτισης (cross - correlation function) ανάμεσα στην ακολουθία μεγίστου μήκους που παράγεται από τον LFSR και στην ακολουθία εξόδου του συστήματος. Η τεχνική αυτή, που καλείται *επίθεση συσχέτισης (correlation attack)*, βελτιώνεται περαιτέρω στο [37], όπου επιπροσθέτως αναδεικνύονται κάποιες ιδιότητες που πρέπει να έχουν τα συστήματα αυτά προκειμένου να είναι ανθεκτικά σε επιθέσεις συσχέτισης. Μεταξύ άλλων, ιδιότητες που πρέπει να πληρούνται είναι οι εξής:

i) το χαρακτηριστικό πολυώνυμο του LFSR να αποτελείται από πολλούς όρους, ii) η μη γραμμικότητα του φίλτρου πρέπει να είναι υψηλή, iii) δεν πρέπει να υπάρχουν πολλοί μηδενικοί όροι στο μετασχηματισμό Walsh του φίλτρου.

Επιθέσεις αναστροφής: Μία άλλη τεχνική ανάκτησης της αρχικής κατάστασης του LFSR είναι η *επίθεση αναστροφής (inversion attack)*, η οποία προτάθηκε στο [45]. Μία επίθεση αναστροφής μπορεί να εφαρμοστεί στις περιπτώσεις εκείνες όπου η συνάρτηση φίλτρου g γράφεται είτε στη μορφή

$$g(x_1, x_2, \ldots, x_n) = x_1 + h(x_2, x_3, \ldots, x_n)$$

είτε

$$g(x_1, x_2, \ldots, x_n) = x_n + h(x_1, x_2, \ldots, x_{n-1}),$$

όπου n το πλήθος των βαθμίδων του LFSR που υπεισέρχονται στην είσοδο του φίλτρου. Τότε, αν $u = \{u_i\}_{i\geq 0}$ είναι η ακολουθία μεγίστου μήκους που παράγεται από τον LFSR, η ακολουθία εξόδου y περιγράφεται (για την πρώτη περίπτωση) από σχέση της μορφής $y_i = u_{i+\gamma_1} + h(u_{i+\gamma_2}, \ldots, u_{i+\gamma_n})$, όπου $\gamma_1 > \gamma_2 > \ldots > \gamma_n$ θετικοί ακέραιοι που καθορίζονται από το μη γραμμικό φίλτρο. Άρα, αν το bit y_i είναι γνωστό, τότε προσδιορίζεται το bit $u_{i+\gamma_1}$ αν είναι γνωστά τα προηγούμενα $\gamma_n - \gamma_1$ bits $u_{i+\gamma_1+1}, \ldots, u_{i+\gamma_n}$. Κατά συνέπεια, η ποσότητα $\gamma_n - \gamma_1$ πρέπει να είναι μεγάλη - ιδανικά, ίση με $L-1$, όπου L το μήκος του LFSR. Επίσης, η επίθεση αναστροφής γίνεται ακόμα πιο αποδοτική αν ο μέγιστος κοινός διαιρέτης d των $\gamma_{i+1} - \gamma_i$, $i = 1, 2, \ldots, n-1$ είναι μεγάλος· ιδανικά λοιπόν, θα θέλαμε το μη γραμμικό φίλτρο να ικανοποιεί τη σχέση $d = 1$. Η τεχνική αναστροφής γενικεύτηκε στο [46], έτσι ώστε να μπορεί να εφαρμοστεί σε όλα τα μη γραμμικά φίλτρα χωρίς κανέναν περιορισμό.

Αλγεβρικές επιθέσεις: Αν L το μήκος του LFSR, τότε κάθε bit της ακολουθίας κλειδιού μπορεί να γραφεί ως μία συνάρτηση των L bits της αρχικής κατάστασης. Συνεπώς, γνώση N στοιχείων της κλειδοροής επιτρέπει τον προσδιορισμό της αρχικής κατάστασης του LFSR μέσω επίλυσης ενός μη γραμμικού συστήματος N εξισώσεων με L αγνώστους. Τεχνικές που αποσκοπούν στην επίλυση τέτοιων συστημάτων καλούνται *αλγεβρικές επιθέσεις (algebraic attacks)*. Στο [27] παρουσιάστηκε μία τεχνική με την οποία μπορεί να μειωθεί ο βαθμός των μη γραμμικών εξισώσεων του συστήματος, η οποία μπορεί να εφαρμοστεί όταν η συνάρτηση του φίλτρου g ικανοποιεί κάποια από τις εξής ιδιότητες:

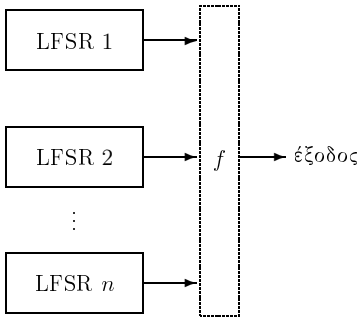
1. υπάρχει συνάρτηση f χαμηλού βαθμού τέτοια ώστε $g * f = h$, όπου η h είναι χαμηλού βαθμού,
2. υπάρχει συνάρτηση f χαμηλού βαθμού τέτοια ώστε $g * f = 0$,
3. υπάρχει συνάρτηση f τέτοια ώστε $g * f = h$, όπου η h είναι χαμηλού βαθμού,

όπου τα f, g, h συμβολίζουν τους αντίστοιχους πίνακες αληθείας των συναρτήσεων, και το $*$ υποδηλώνει το εσωτερικό γινόμενό τους. Στο [103] αποδεικνύεται ότι οι παραπάνω τρεις ιδιότητες είναι ισοδύναμες με την εξής μία: *δεν πρέπει να υπάρχει συνάρτηση χαμηλού βαθμού f τέτοια ώστε είτε $g * f = 0$ ή $(g + 1) * f = 0$.* Κάθε τέτοια συνάρτηση f ονομάζεται *εκμηδενιστής (annihilator)* της g - κατά συνέπεια, οι αλγεβρικές επιθέσεις όρισαν ως βασικό κριτήριο σχεδίασης των μη γραμμικών φίλτρων το να μην έχουν εκμηδενιστές χαμηλού βαθμού. Από τη στιγμή που θα κατασκευαστεί ένα μη γραμμικό σύστημα χαμηλού βαθμού, μπορεί να επιλυθεί με διάφορες τεχνικές, οι κυριότερες εκ των οποίων στηρίζονται στις βάσεις Gröbner [36]. Οι αλγεβρικές επιθέσεις οδήγησαν στον ορισμό ενός νέου κρυπτογραφικού κριτηρίου για τις λογικές συναρτήσεις, της λεγόμενης *αλγεβρικής ανθεκτικότητας (algebraic immunity ή annihilator immunity)*, η οποία ορίζεται ως ο ελάχιστος βαθμός από όλους τους μη μηδενικούς εκμηδενιστές της g ή της $g+1$ [19, 28]. Η αλγεβρική ανθεκτικότητα για κάθε συνάρτηση n μεταβλητών είναι μικρότερη ή ίση από $\lceil \frac{n}{2} \rceil$[27]. Κατασκευές συναρτήσεων υψηλής αλγεβρικής ανθεκτικότητας έχουν προταθεί στα [19, 28]· ωστόσο το ερευνητικό αυτό πεδίο παραμένει ακόμα έντονα ενεργό, μια που αυτές οι συναρτήσεις δεν ικανοποιούν άλλα κρυπτογραφικά κριτήρια.

Παρατήρηση 2.19. Πρόσφατα προτάθηκε μία νέα, πολύ περισσότερο αποδοτική αλγεβρική επίθεση για συστήματα μη γραμμικών φίλτρων [121]. Ωστόσο, αυτή η τεχνική απαιτεί γνώση πολύ περισσότερων δεδομένων από ό,τι απαιτεί μία κλασική αλγεβρική επίθεση - κατά συνέπεια, η μελέτη της αλγεβρικής ανθεκτικότητας συναρτήσεων παραμένει σημαντική και αναγκαία.

2.5.3 Μη γραμμικοί συνδυαστές

Μία δεύτερη τεχνική για την εξάλειψη της εγγενούς γραμμικότητας των LFSRs είναι ο συνδυασμός πολλών LFSRs, με τρόπο τέτοιο ώστε οι έξοδοί τους να τροφοδοτούν μία μη γραμμική λογική συνάρτηση, που καλείται συνάρτηση-συνδυαστής (Σχήμα 2.6). Οι LFSRs που επιλέγονται για την κατασκευή τέτοιων συστημάτων είναι πρωταρχικοί, λόγω των καλών ιδιοτήτων και της υψηλής περιόδου που έχουν. Όμοια με την περίπτωση των μη γραμμικών φίλτρων,



Σχήμα 2.6. Εφαρμογή μη γραμμικού συνδυαστή σε πολλούς LFSRs

η συνάρτηση-συνδυαστής πρέπει να είναι ισοβαρής. Όσον αφορά τη γραμμική πολυπλοκότητα της παραγόμενης ακολουθίας, αποδεικνύεται στο [125] η ακόλουθη ιδιότητα: *Έστω n πρωταρχικοί LFSRs, με μήκη $L_1, L_2, \ldots, L_n$ τέτοια ώστε να είναι ανά δύο διαφορετικά μεταξύ τους και μεγαλύτερα από 2. Τότε, αν η συνάρτηση-συνδυαστής είναι $f(x_1, x_2, \ldots, x_n)$ στην Αλγεβρική Κανονική Μορφή, η γραμμική πολυπλοκότητα της παραγόμενης ακολουθίας ισούται με την τιμή της παράστασης $f(L_1, L_2, \ldots, L_n)$, όπως αυτή υπολογίζεται πάνω σε ακεραίους (και όχι στο $\mathbb{F}_2$).* Κατά συνέπεια, συστήματα αυτής της μορφής απαιτείται να έχουν μία συνάρτηση-συνδυαστή υψηλού βαθμού, προκειμένου να παράγεται κλειδοροή μεγάλης γραμμικής πολυπλοκότητας. Στο [44] αποδεικνύεται πως η ίδια τιμή για τη γραμμική πολυπλοκότητα ισχύει ακόμα και αν οι υπεισερχόμενοι FSRs είναι οποιασδήποτε μορφής (ακόμα και μη γραμμικοί), αρκεί οι περίοδοι των ακολουθιών που παράγονται από κάθε FSR να είναι αριθμοί πρώτοι μεταξύ τους.

Κρυπτανάλυση σε συστήματα μη γραμμικών συνδυαστών

Επιθέσεις συσχέτισης: Στο [129] προτάθηκε η ακόλουθη μέθοδος κρυπτανάλυσης για τους μη γραμμικούς συνδυαστές, η οποία καλείται *επίθεση συσχέτισης (correlation attack)*. Έστω $R_1, R_2, \ldots, R_n$ οι πρωταρχικοί LFSRs που υπεισέρχονται στο σύστημα του Σχήματος 2.6, με αντίστοιχα μήκη $L_1, L_2, \ldots, L_n$. Το πλήθος όλων των πιθανών αρχικών καταστάσεων των LFSRs, οι οποίες αποτελούν το κλειδί του συστήματος, είναι $\prod_{i=1}^{n}(2^{L_i} - 1)$. Ας υποθέσουμε ότι η παραγόμενη κλειδοροή ταυτίζεται με την έξοδο του R_1 με κάποια πιθανότητα $p > \frac{1}{2}$. Τότε, αν είναι γνωστό αρκετά μεγάλο τμήμα της κλειδοροής, η αρχική κατάσταση του R_1 μπορεί να προσδιοριστεί συγκρίνοντας την παραγόμενη κλειδοροή με όλες τις πιθανές ακολουθίες που μπορούν να προκύψουν από τον R_1: εκείνη η αρχική κατάσταση του R_1 που παράγει ακολουθία η οποία ταυτίζεται σε

ποσοστό p με την κλειδοροή είναι και η πραγματική αρχική κατάσταση του R_1. Αυτός ο υπολογισμός λαμβάνει χώρα με $2^{L_1}-1$ ελέγχους. Αν αντίστοιχες συσχετίσεις υπάρχουν μεταξύ της παραγόμενης κλειδοροής και των υπολοίπων LFSRs, τότε το κλειδί του συστήματος μπορεί να υπολογιστεί πραγματοποιώντας $\sum_{i=1}^{n}(2^{L_i}-1)$ ελέγχους· αυτός ο αριθμός είναι πολύ μικρότερος από το σύνολο όλων των πιθανών κλειδιών. Κατά συνέπεια, λόγω των επιθέσεων συσχέτισης, κατέστη αναγκαίο το να επιλέγονται, ως μη γραμμικοί συνδυαστές, συναρτήσεις που να είναι ανθεκτικές σε συσχετίσεις τάξης m, όπου το m να έχει υψηλή τιμή. Ωστόσο, ανακαλώντας το ότι η συνάρτηση-συνδυαστής πρέπει να έχει μεγάλο βαθμό, είναι ανάγκη κατά την επιλογή μίας τέτοιας συνάρτησης να γίνεται προσπάθεια για μία "χρυσή τομή" μεταξύ της τάξης ανθεκτικότητάς της σε συσχετίσεις και του βαθμού της.

Οι επιθέσεις συσχέτισης γίνονται ακόμα πιο αποδοτικές στο [104], όπου χρησιμοποιούνται τεχνικές αποκωδικοποίησης κωδίκων καναλιού για να αποφευχθούν κάποιοι περιττοί έλεγχοι πιθανών αρχικών καταστάσεων ενός LFSR· σε αυτήν την περίπτωση καλούνται *γρήγορες επιθέσεις συσχέτισης (fast correlation attacks)*. Αν υπάρχει συσχέτιση $p > \frac{1}{2}$ μεταξύ της κλειδοροής y και της εξόδου u ενός LFSR μήκους L, τότε η ακολουθία y θεωρείται ως το αποτέλεσμα της μετάδοσης της λέξης u μέσα από ένα δυαδικό συμμετρικό κανάλι με πιθανότητα λάθους $1-p$ (αντίστοιχη κωδικοποίηση, χρησιμοποιώντας τη συμπληρωματική ακολουθία της u, ορίζεται και για την περίπτωση όπου $p < \frac{1}{2}$). Επιπρόσθετα, όλα τα bits της u εξαρτώνται γραμμικά από την αρχική κατάσταση του LFSR, οπότε η u είναι μία κωδική λέξη ενός γραμμικού κώδικα διάστασης L. Άρα, η εύρεση της αρχικής κατάστασης του LFSR ισοδυναμεί με την αποκωδικοποίηση της ακολουθίας y, βάσει του κώδικα που ορίζεται από το χαρακτηριστικό πολυώνυμο του LFSR. Διάφορες αποδοτικές τεχνικές αποκωδικοποίησης έχουν προταθεί, οι οποίες χρησιμοποιούν, μεταξύ άλλων, συγκεραστικούς κώδικες ή κώδικες turbo [61, 62, 63].

Επιθέσεις προσέγγισης χαμηλού βαθμού: Στο [84] προτάθηκε μία μέθοδος κρυπτανάλυσης η οποία καλείται *επίθεση προσέγγισης χαμηλού βαθμού (low degree approximation attack)* και εφαρμόζεται αν η συνάρτηση f του Σχήματος 2.6 μπορεί να προσεγγιστεί ικανοποιητικά από μία συνάρτηση χαμηλότερου βαθμού. Η επίθεση αυτή αποτελεί γενίκευση της *επίθεσης βέλτιστων γραμμικών προσεγγίσεων (best affine approximation attack)* που προτείνεται στο [31]. Ας υποθέσουμε ότι υπάρχει μία συνάρτηση g τέτοια ώστε $\deg(g) < \deg(f)$ και η απόσταση Hamming μεταξύ των f, g να είναι μικρή. Έστω

y η παραγόμενη κλειδοροή του Σχήματος 2.6 και $\hat{y}$ η κλειδοροή που θα προέκυπτε αν η συνάρτηση-συνδυαστής ήταν η g. Λόγω του ότι η γραμμική πολυπλοκότητα της $\hat{y}$ είναι $L_0 = g(L_1, L_2, \ldots, L_n)$, υπάρχει LFSR μήκους L_0 που την παράγει. Άρα, αν γνωρίζουμε ένα τμήμα της ακολουθίας y μπορεί να χρησιμοποιηθεί γρήγορη επίθεση συσχέτισης [104] για τον προσδιορισμό της αρχικής κατάστασης αυτού του LFSR (εφόσον το L_0 είναι μικρό). Αν αυτό επιτευχθεί, τότε ουσιαστικά είμαστε σε θέση να κατασκευάσουμε ολόκληρη την ακολουθία $\hat{y}$, άρα κατ' επέκταση προσδιορίσαμε ολόκληρη την ακολουθία κλειδιού y όπου απλά κάποια λίγα bits είναι λανθασμένα. Συμπερασματικά λοιπόν, δεν πρέπει μία συνάρτηση-συνδυαστής να μπορεί να προσεγγιστεί ικανοποιητικά από κάποια συνάρτηση χαμηλού βαθμού - άρα, η απαίτηση για υψηλή μη γραμμικότητα είναι και εδώ παρούσα.

Αξίζει να σημειωθεί πως κάθε σύστημα που αποτελείται από ένα μη γραμμικό φίλτρο βαθμού k, το οποίο εφαρμόζεται σε έναν LFSR, είναι ισοδύναμο με κάποιο σύστημα μη γραμμικού συνδυαστή, ο οποίος απαρτίζεται από k ίδιους LFSRs, με ολισθημένες αρχικές καταστάσεις. Με άλλα λόγια, πολλές επιθέσεις που λαμβάνουν χώρα στη μία κατηγορία συστημάτων μπορούν να εφαρμοστούν άμεσα και στην άλλη. Για παράδειγμα, αλγεβρικές επιθέσεις μπορούν να λάβουν χώρα και σε συστήματα μη γραμμικών συνδυαστών [26]. Εκτός των ανωτέρω, υπάρχουν και άλλες σημαντικές επιθέσεις για αλγορίθμους ροής οι οποίες μπορούν να εφαρμοστούν είτε σε συστήματα με μη γραμμικά φίλτρα είτε σε συστήματα με μη γραμμικό συνδυαστή. Μία γενική περιγραφή και σύγκριση των διαφόρων επιθέσεων παρουσιάζεται στο [60].

2.6 Άλλα κρυπτογραφικά κριτήρια ακολουθιών

Εκτός από την πολυπλοκότητα (γραμμική ή μη) που ορίστηκε ανωτέρω, καθώς και τα αντίστοιχα προφίλ πολυπλοκότητας, υπάρχουν πολλά ακόμα μέτρα πολυπλοκότητας για μία ακολουθία, όπου το κάθε ένα σχετίζεται με συγκεκριμένα χαρακτηριστικά τα οποία της προσδίδουν ψευδοτυχαιότητα. Μερικά από τα πιο σημαντικά κρυπτογραφικά κριτήρια, τα οποία μπορούν να χρησιμοποιηθούν ως μέτρο αποτίμησης της ψευδοτυχαιότητας μίας ακολουθίας, είναι τα ακόλουθα [110]:

- *Γραμμική πολυπλοκότητα k σφαλμάτων (k-error linear complexity)*: Είναι η ελάχιστη τιμή στην οποία μπορεί να μειωθεί η γραμμική πολυπλοκότητα μίας ακολουθίας, αν μεταβάλλουμε οποιαδήποτε k (το πολύ) στοιχεία της. Αντικατοπτρίζει την κρυπτογραφική

Πίνακας 2.1. Στατιστικοί έλεγχοι του NIST για την ψευδοτυχαιότητα ακολουθιών

1.	Frequency (Monobits) Test (*1ο κριτήριο Golomb*)
2.	Test for Frequency within a Block
3.	Runs Test (*2ο κριτήριο Golomb*)
4.	Test for the Longest Run of Ones in a Block
5.	Random Binary Matrix Rank Test
6.	Discrete Fourier Transform (Spectral) Test
7.	Non-overlapping (Aperiodic) Template Matching Test
8.	Overlapping (Periodic) Template Matching Test
9.	Maurer's Universal Statistical Test
10.	Lempel-Ziv Complexity Test (*μελετάται στο Κεφάλαιο 5*)
11.	Linear Complexity Test
12.	Serial Test
13.	Approximate Entropy Test
14.	Cumulative Sum (Cusum) Test
15.	Random Excursions Test
16.	Random Excursions Variant Test

αδυναμία ακολουθιών που έχουν υψηλή τιμή για τη γραμμική πολυπλοκότητα όπου όμως, αν μεταβληθούν ελάχιστα στοιχεία τους, η τιμή αυτή μειώνεται δραστικά· τυπικό παράδειγμα αποτελεί η περιοδική ακολουθία $00\ldots1$, όπου η γραμμική της πολυπλοκότητα είναι μέγιστη (ίση με την περίοδο της ακολουθίας), αλλά η γραμμική πολυπλοκότητα 1 σφάλματος είναι 0. Για δυαδικές περιοδικές ακολουθίες περιόδου 2^n για κάποιο n, η τιμή της γραμμικής πολυπλοκότητας k σφαλμάτων για οποιοδήποτε k υπολογίζεται από τον αλγόριθμο των Stamp-Martin στο [131], ο οποίος αποτελεί γενίκευση του αλγορίθμου των Games-Chan [38]. Επέκταση του αλγορίθμου των Stamp-Martin έτσι ώστε να υπολογίζει αποδοτικά την τιμή της γραμμικής πολυπλοκότητας k σφαλμάτων για όλες τις πιθανές τιμές του k δίνεται από τους Lauder και Paterson στο [87]. Η περίπτωση της γραμμικής πολυπλοκότητας 1 σφάλματος για δυαδικές περιοδικές ακολουθίες περιόδου $2^n - 1$ μελετάται στο [83].

- *Πολυπλοκότητα Lempel-Ziv (Lempel-Ziv complexity)*: Το μέτρο αυτό πολυπλοκότητας προτάθηκε από τους Lempel και Ziv στο [88] και εκφράζει το ρυθμό με τον οποίο εμφανίζονται νέα τμήματα σε μία ακολουθία, καθώς κινούμαστε κατά μήκος της. Η διαδικασία υπολογισμού αυτού του μέτρου πολυπλοκότητας παίζει επίσης σημαντικό ρόλο στον πολύ γνωστό αλγόριθμο συμπίεσης των Lempel-Ziv. Η πολυπλοκότητα Lempel-Ziv θα

μελετηθεί διεξοδικά στο Κεφάλαιο 5.

- *Δενδρική πολυπλοκότητα (tree complexity)*: Το μέτρο αυτό πολυπλοκότητας προτάθηκε από τους Niederreiter και Vielhaber στο [111] και σχετίζεται με την καταμέτρηση συγκεκριμένων υπο-τμημάτων μίας ακολουθίας.

Πολλά είναι ακόμη τα κρυπτογραφικά κριτήρια των ακολουθιών που έχουν προταθεί. Ο πίνακας 2.1 καταγράφει ονομαστικά τους στατιστικούς ελέγχους που έχει καθιερώσει ο οργανισμός NIST για τη μελέτη των ακολουθιών - πλήρης περιγραφή αυτών δίνεται στο [109]. Αξίζει ωστόσο να σημειωθεί ότι οι έλεγχοι αυτοί δεν είναι οι μοναδικοί που έχουν προταθεί στην ευρύτερη βιβλιογραφία. Η ύπαρξη πιθανών συσχετίσεων και εξαρτήσεων μεταξύ των διαφόρων μέτρων πολυπλοκότητας παραμένει ανοιχτό ερευνητικό πρόβλημα [110]. Το κεφάλαιο 5 κινείται προς αυτήν την κατεύθυνση, αποσαφηνίζοτας τη συσχέτιση μεταξύ της μη γραμμικής πολυπλοκότητας και της πολυπλοκότητας Lempel-Ziv.

Κεφάλαιο 3

Γεννήτριες ακολουθιών στο χώρο καταστάσεων

> One of the principal objects of theoretical research in my department of knowledge is to find the point of view from which the subject appears in its greatest simplicity.
>
> *Josiah Willard Gibbs*

Στο παρόν κεφάλαιο τα συστήματα παραγωγής ακολουθιών μελετώνται υπό μία νέα οπτική γωνία, η οποία βασίζεται σε αρχές της *θεωρίας συστημάτων (system theory)* [66]. Κάθε γεννήτρια ακολουθιών, ως πεπερασμένο αυτόματο, περιγράφεται από ένα ζευγάρι εξισώσεων: η καταστατική εξίσωση περιγράφει την μετάβαση των καταστάσεων της γεννήτριας, ενώ η εξίσωση εξόδου δίνει την έξοδο του συστήματος για την τρέχουσα κατάστασή του. Με αυτόν τον φορμαλισμό, διευρύνεται η έννοια της γεννήτριας ακολουθιών πέραν των καταχωρητών ολίσθησης με ανάδραση. Μελετώντας τα καταστατικά αυτά συστήματα με κλασικές έννοιες της θεωρίας συστημάτων όπως η ελεγξιμότητα και η παρατηρησιμότητα, αναδεικνύονται νέα μέτρα πολυπλοκότητας των παραγόμενων ακολουθιών. Συγκεκριμένα, η κλασική έννοια της πολυπλοκότητας, που ορίζεται με βάση τους καταχωρητές ολίσθησης με ανάδραση ως γεννήτριες ακολουθιών, διευρύνεται έτσι ώστε να αντιστοιχεί στη γενικότερη περίπτωση συστημάτων παραγωγής ακολουθιών. Επίσης, μέσω της ανάλυσης που ακολουθείται, αναδεικνύονται ξεχωριστές ιδιότητες που διέπουν τα συστήματα παραγωγής των ακολουθιών De Brujin.

Οι έννοιες και μαθηματικά εργαλεία που εισάγονται σε αυτό το κεφάλαιο αποτελούν τη βάση για την εξαγωγή των αποτελεσμάτων που παρατίθενται στα επόμενα κεφάλαια.

3.1 Ελεγξιμότητα και παρατηρησιμότητα συστημάτων

Ένα πεπερασμένο αυτόματο $\mathfrak{S} = \langle S, R, f, g, x_0 \rangle$ περιγράφεται από το ακόλουθο ζευγάρι εξισώσεων

$$x_{i+1} = f(x_i) \tag{3.1a}$$

$$y_i = g(x_i)\,. \tag{3.1b}$$

Το πεπερασμένο σύνολο S αποτελεί το *σύνολο καταστάσεων* του $\mathfrak{S}$, R είναι το πεπερασμένο αλφάβητο της εξόδου, $f : S \to S$ είναι η συνάρτηση μετάβασης κατάστασης, $g : S \to R$ είναι η συνάρτηση εξόδου, $x_0 \in S$ η αρχική κατάσταση του $\mathfrak{S}$ και $y = \{y_i\}_{i\geq 0}$ είναι η ακολουθία που παράγεται από το $\mathfrak{S}$. Η εξίσωση (3.1) αποτελεί την *αναπαράσταση στο χώρο καταστάσεων* του συστήματος $\mathfrak{S}$. Ένα πεπερασμένο αυτόματο το οποίο παράγει μία ακολουθία y δημιουργεί μία *υλοποίηση ή πραγματοποίηση (realization)* της y. Κάθε στοιχείο $s \in S$ ονομάζεται *κατάσταση (state)* του $\mathfrak{S}$. Όλα τα συστήματα που περιγράφονται από την (3.1) καλούνται *καταστατικές γεννήτριες ακολουθιών (state space sequence generators)*. Από την (3.1) προκύπτει ότι η παραγόμενη ακολουθία δίνεται από τη σχέση

$$y_i = g\left(f^i(x_0)\right), \qquad i \geq 0$$

όπου με $f^i(z)$ συμβολίζουμε τη i-ιοστής τάξης σύνθεση της f με τον εαυτό της, δηλαδή $f^i(z) = f\left(f^{i-1}(z)\right) = \left(f \circ f^{i-1}\right)(z)$ και $f^0(z) = z$. Ο πληθικός αριθμός $|S|$ του συνόλου S καθορίζει την *τάξη (order)* του συστήματος $\mathfrak{S}$.

Παράδειγμα 3.1. Κάθε FSR μπορεί να αναπαρασταθεί στο χώρο των καταστάσεων και, κατ' επέκταση, αποτελεί μία ειδική περίπτωση καταστατικής γεννήτριας ακολουθιών. Συγκεκριμένα, ένας FSR n βαθμίδων που περιγράφεται από την (2.1) και παράγει την ακολουθία $y = \{y_i\}_{i\geq 0} \in \mathbb{F}_q$, μπορεί να περιγραφεί από ένα ζευγάρι καταστατικών εξισώσεων της μορφής (3.1), όπου

$$\begin{aligned} x_0 &= (y_0\ y_1\ \ldots\ y_{n-1})^T, \\ x_{i+1} &= f(x_i) = f(x_{i,0}, x_{i,1}, \ldots, x_{i,n-1}) \\ &= (x_{i,1}\ x_{i,2}\ \ldots\ h(x_{i,n-1}, x_{i,n-2}, \ldots, x_{i,0}))^T, \\ y_i &= g(x_i) = (1\ 0\ \ldots\ 0)x_i, \end{aligned}$$

και για το σύνολο καταστάσεων S ισχύει $S = \mathbb{F}_q^n$. □

Ένα πεπερασμένο αυτόματο $\mathfrak{S}$ λέγεται *αντιστρέψιμο* αν η συνάρτηση f είναι αντιστρέψιμη. Επίσης, αν το $\mathfrak{S}$ παράγει μία ακολουθία y, τότε καλείται *ελάχιστη πραγματοποίηση (minimal realization)* της y αν δεν υπάρχει άλλη πραγματοποίηση $\mathfrak{S}' = \langle S', R, f', g', x_0' \rangle$ της y τέτοια ώστε $|S'| < |S|$. Για δοθείσα πραγματοποίηση $\mathfrak{S}$ της ακολουθίας y και για κάθε 1-1 και επί συνάρτηση $\phi : S \to S$, μπορεί εύκολα να αποδειχθεί ότι το πεπερασμένο αυτόματο

$$\mathfrak{S}' = \left\langle S, \phi \circ f \circ \phi^{-1}, g \circ \phi^{-1}, \phi(x_0) \right\rangle$$

επίσης παράγει την y (όπου ϕ^{-1} είναι η αντίστροφη συνάρτηση της ϕ). Συνεπώς, εισάγουμε τον ακόλουθο ορισμό *ισοδύναμων* συστημάτων:

Ορισμός 3.2. Τα συστήματα $\mathfrak{S} = \langle S, R, f, g, x_0 \rangle$ και $\mathfrak{S}' = \langle S, R, f', g', x_0' \rangle$ είναι ισοδύναμα αν υπάρχει ένας ισομορφισμός $\phi : S \to S$ τέτοιος ώστε

$$f' = \phi \circ f \circ \phi^{-1}, \quad g' = g \circ \phi^{-1}, \quad \text{and} \quad x_0' = \phi(x_0).$$

Μία κατάσταση $x \in S$ ονομάζεται *τελικά περιοδική (ultimately periodic)* αν υπάρχουν ακέραιοι k, m, με $k > m$, τέτοιοι ώστε $f^k(x) = f^m(x)$. Επειδή το S είναι πεπερασμένο σύνολο, όλες οι καταστάσεις του $\mathfrak{S}$ είναι τελικά περιοδικές. Αντιστοίχως, μία κατάσταση x είναι *περιοδική (periodic)* αν $f^N(x) = x$ για κάποιον ακέραιο $N > 0$. *Αν η συνάρτηση f είναι αντιστρέψιμη, τότε όλες οι καταστάσεις του $\mathfrak{S}$ είναι περιοδικές, αφού η σχέση $f^k(x) = f^m(x)$ οδηγεί στην $f^{k-m}(x) = x$.*

Λήμμα 3.3. *Κάθε σύστημα $\mathfrak{S} = \langle S, R, f, g, x_0 \rangle$ του οποίου η αρχική κατάσταση x_0 είναι περιοδική με περίοδο T, παράγει περιοδική ακολουθία με περίοδο τ τέτοια ώστε $\tau | T$.*

Απόδειξη. Αφού η x_0 είναι περιοδική, ισχύει $f^{i+T}(x_0) = f^i(x_0),\ \forall\, i \geq 0$. Κατά συνέπεια, $g(f^{i+T}(x_0)) = g(f^i(x_0))$, δηλαδή $y(i+T) = y(i)$. Άρα, η y είναι περιοδική και ο αριθμός T είναι μία περίοδος της ακολουθίας, οπότε η στοιχειώδης περίοδος τ της y είναι διαιρέτης του T. □

Ορισμός 3.4. Μία κατάσταση $x \in S$ ονομάζεται *ελέγξιμη (controllable)* αν το σύνολο $R(x) = \{f^i(x), i \geq 0\}$ καλύπτει όλο το σύνολο S, δηλαδή αν $R(x) = S$. Επιπρόσθετα, η γεννήτρια $\mathfrak{S}$ καλείται ελέγξιμη αν όλες της οι καταστάσεις είναι ελέγξιμες.

Προφανώς, αν μία ελέγξιμη κατάσταση x είναι περιοδική, τότε είναι περιοδικές όλες οι καταστάσεις του S και, επιπλέον, όλες έχουν κοινή περίοδο - ίση με $|S|$. Δύο καταστάσεις x

and x' ονομάζονται *αξεχώριστες (output-indistinguishable)* αν $g(f^i(x)) = g(f^i(x'))$ για κάθε $i \geq 0$, δηλαδή αν παράγουν την ίδια έξοδο.

Ορισμός 3.5. Ένα πεπερασμένο αυτόματο $\mathfrak{S}$ καλείται *παρατηρήσιμο (observable)* από την κατάσταση $x \in S$ αν δεν υπάρχει καμία κατάσταση x' που να είναι αξεχώριστη από την x. Επίσης, το $\mathfrak{S}$ καλείται παρατηρήσιμο αν είναι παρατηρήσιμο από όλες του τις καταστάσεις.

Η ελεγξιμότητα ενός συστήματος υποδηλώνει ότι όλες του οι καταστάσεις είναι προσπελάσιμες, ανεξάρτητα από το ποια θα είναι η αρχική. Η παρατηρησιμότητα ενός συστήματος συνεπάγεται πρακτικά ότι υπάρχει η δυνατότητα να υπολογιστεί η αλληλουχία των καταστάσεών του, αν είναι γνωστή η ακολουθία της εξόδου.

3.2 Ελάχιστες καταστατικές υλοποιήσεις ακολουθιών

Στην προηγούμενη ενότητα δεν τέθηκε κανένας περιορισμός στη δομή του συνόλου S. Για αυτή τη γενική περίπτωση συστημάτων, χρησιμοποιούμε τον όρο *πραγματοποίηση σε σύνολο (set realization)* της ακολουθίας y. Στη συνέχεια εισάγουμε μία κατηγοριοποίηση των καταστατικών συστημάτων, η οποία αντιστοιχεί στην πρόσθετη μαθηματική δομή του S:

Ορισμός 3.6. Το αυτόματο $\mathfrak{S}$ καλείται

1. *πραγματοποίηση σε σώμα (field realization)* της ακολουθίας y, αν το $S \supseteq R$ είναι ένα πεπερασμένο σώμα,

2. *γραμμική πραγματοποίηση (linear realization)* της ακολουθίας y, αν το S είναι γραμμικός διανυσματικός χώρος στο R και, επιπρόσθετα, οι f, g είναι γραμμικές συναρτήσεις.

Όλα τα παραπάνω είδη συστημάτων παράγουν ακολουθίες που είναι τελικά περιοδικές, όπως αποδεικνύεται στην ακόλουθη Πρόταση.

Πρόταση 3.7. *Τα ακόλουθα είναι ισοδύναμα:*

1. *υπάρχει μία πραγματοποίηση σε σύνολο για την ακολουθία y.*

2. *η y είναι τελικά περιοδική ακολουθία.*

3. *υπάρχει μία γραμμική πραγματοποίηση για την y.*

4. *υπάρχει μία πραγματοποίηση σε σώμα για την y.*

Απόδειξη. $1 \rightarrow 2$*: Έστω* $\mathfrak{S} = \langle S, R, f, g, x_0 \rangle$ *μία πραγματοποίηση σε σύνολο της* y*. Επειδή το* S *είναι πεπερασμένο, υπάρχουν ακέραιοι* $k > \tau$ *τέτοιοι ώστε* $f^k(x_0) = f^\tau(x_0)$*. Έστω* $t_0 = \tau$ *και* $T = k - t_0$*. Τότε, ισχύει* $f^{T+t_0}(x_0) = f^{t_0}(x_0)$*. Επιπλέον, για κάθε* $i \geq t_0$ *ισχύει*

$$\begin{aligned} y_{i+T} &= y_{i-t_0+T+t_0} = g(f^{i-t_0+T+t_0}(x_0)) = \\ &= g(f^{i-t_0} f^{t_0}(x_0)) = g(f^i(x_0)) = y_i \,, \end{aligned}$$

και άρα η y *είναι τελικά περιοδική.*

$2 \rightarrow 3$*: Αφού η* y *είναι τελικά περιοδική, υπάρχει LFSR που την παράγει [42, 67]. Ο προς απόδειξη ισχυρισμός προκύπτει από τη προφανή διαπίστωση ότι κάθε LFSR μπορεί να περιγραφεί από ένα γραμμικό ζευγάρι εξισώσεων της μορφής* (3.1)*, όπου το σύνολο* S *περιέχει όλα τα διανύσματα στο* R_2^n*, όπου* n *το μήκος του LFSR. (Καταστατικές εξισώσεις που περιγράφουν LFSRs μελετώνται διεξοδικά στο κεφάλαιο 4).*

$3 \rightarrow 4 \rightarrow 1$*: προκύπτει απευθείας από τον ορισμό 3.6.* □

Στο υπόλοιπο τμήμα της ενότητας εξετάζουμε την πιο σημαντική κρυπτογραφικά περίπτωση των δυαδικών ακολουθιών, δηλαδή $R = \mathbb{F}_2$. Για απλούστευση στο συμβολισμό, στο υπόλοιπο του κειμένου δεν θα αναγράφεται το αλφάβητο εξόδου $\mathbb{F}_2$ κατά την περιγραφή ενός καταστατικού συστήματος.

Έχοντας μία πραγματοποίηση συνόλου $\mathfrak{S}$ για μία περιοδική ακολουθία y, μπορούμε να κατασκευάσουμε μία ελάχιστη πραγματοποίηση συνόλου της y μετασχηματίζοντας την $\mathfrak{S}$ σε ισοδύναμη αναπαράσταση που είναι ταυτόχρονα ελέγξιμη και παρατηρήσιμη. Η διαδικασία έχει ως εξής: έστω σύνολο S που περιέχει τουλάχιστον T στοιχεία, όπου T η περίοδος της y. Επιλέγουμε τυχαία ένα υποσύνολο S' του S με kT στοιχεία τα οποία συμβολίζονται ως

$$S' = \left\{ x_{0,0}, x_{0,1}, \ldots, x_{0,T-1}, \quad \cdots \quad , x_{k-1,0}, x_{k-1,1}, \ldots, x_{k-1,T-1} \right\} \tag{3.2}$$

όπου ο ακέραιος k δίνεται από την $k = \lfloor |S|/T \rfloor$. Ορίζουμε επίσης τις συναρτήσεις f, g ως ακολούθως

$$f(x_{j,i}) = x_{j+\lfloor (i+1)/T \rfloor \bmod k,\ i+1 \bmod T} \tag{3.3a}$$

$$g(x_{j,i}) = y_i \tag{3.3b}$$

για κάθε $0 \leq j < k$ και $0 \leq i < T$. Τότε, προκύπτει η αντιστρέψιμη πραγματοποίηση $\langle S, f, g, x_0 \rangle$ της y, όπου ως αρχική κατάσταση x_0 μπορεί να επιλεγεί οποιοδήποτε στοιχείο $x_{j,0}$ από την (3.2). Αν περιορίσουμε το χώρο καταστάσεων στο S' ή, ισοδύναμα, στο $R(x_0) =$

$\{f^i(x_0), i \geq 0\}$, τότε προκύπτει μία ισοδύναμη γεννήτρια με τάξη kT η οποία είναι ελέγξιμη. Από τον ορισμό των f, g είναι εύκολο να δούμε πως δύο οποιεσδήποτε καταστάσεις $x_{i,0}$, $x_{j,0}$, με $i \neq j$, είναι αξεχώριστες. Ορίζονται κατά συνέπεια T κλάσεις ισοδυναμίας στο χώρο των καταστάσεων, όπου η κάθε κλάση $\mathbf{c}_i$ αποτελείται από k καταστάσεις $x_{0,i}, x_{1,i} \ldots, x_{k-1,i}$, $i = 0, 1, \ldots, T-1$, οι οποίες είναι αξεχώριστες. Θεωρώντας ως σύνολο καταστάσεων το χώρο πηλίκο (quotient space) που ορίζεται από αυτές τις κλάσεις ισοδυναμίας, προκύπτει μία ισοδύναμη πραγματοποίηση της y τάξης T. Το ισοδύναμο αυτό σύστημα είναι παρατηρήσιμο και προφανώς αποτελεί ελάχιστη πραγματοποίηση για την y (αφού δεν μπορεί να παραχθεί ακολουθία με περίοδο T από ένα χώρο καταστάσεων με λιγότερα από T στοιχεία).

Με αντίστοιχο τρόπο μπορεί να κατασκευαστεί μία ελάχιστη πραγματοποίηση συνόλου για ακολουθία που είναι τελικά περιοδική. Η τάξη μίας τέτοιας ελάχιστης πραγματοποίησης θα είναι $t_0 + T$, όπου t_0, T η προ-περίοδος και η περίοδος της ακολουθίας αντίστοιχα. Επίσης, λόγω του γεγονότος ότι το σύνολο καταστάσεων σε μία οποιαδήποτε πραγματοποίηση της y πρέπει να έχει τουλάχιστον $t_0 + T$ στοιχεία, προκύπτει άμεσα ότι το σύνολο καταστάσεων σε μία ελάχιστη πραγματοποίηση σώματος της y θα αποτελείται από τα στοιχεία του $\mathbb{F}_{2^n}$, όπου n ο ακέραιος εκείνος που προσδιορίζεται από τη σχέση $2^{n-1} < t_0 + T \leq 2^n$.

Στη συνέχεια εισάγουμε νέα μέτρα πολυπλοκότητας των ακολουθιών, τα οποία καθορίζονται από την τάξη μίας ελάχιστης καταστατικής υλοποίησής τους.

Ορισμός 3.8. Έστω y μια τελικά περιοδική δυαδική ακολουθία. Έστω επίσης $\mathfrak{F}$, $\mathfrak{L}$, and $\mathfrak{S}$ τρεις ελάχιστες καταστατικές υλοποιήσεις της, όπου η κάθε μία είναι σε σώμα, γραμμική, και σε σύνολο αντίστοιχα.

1. Αν $\mathbb{F}_{2^n}$ είναι το πεπερασμένο σώμα στο οποίο παίρνει τιμές το σύνολο καταστάσεων του $\mathfrak{F}$, τότε πολυπλοκότητα σώματος (field complexity) της ακολουθίας ορίζεται ως η διάσταση n του σώματος $\mathbb{F}_{2^n}$ στο $\mathbb{F}_2$.

2. Αν L είναι ο γραμμικός διανυσματικός χώρος στον οποίο παίρνει τιμές το σύνολο καταστάσεων του $\mathfrak{L}$, τότε πολυπλοκότητα γραμμικής πραγματοποίησης (linear state space complexity) της ακολουθίας ορίζεται ως η διάσταση του L στο $\mathbb{F}_2$.

3. Αν S είναι το σύνολο καταστάσεων του $\mathfrak{S}$, τότε ως πολυπλοκότητα συνόλου (set complexity) της ακολουθίας ορίζεται η ποσότητα $\log_2 |S|$.

Τα παραπάνω μέτρα πολυπλοκότητας συμβολίζονται ως $C_f(y)$, $C_l(y)$ και $C_s(y)$ αντίστοιχα. Αφού ένας FSR είναι μία ειδική περίπτωση πεπερασμένου αυτομάτου, ο Ορισμός 3.8 αποτελεί

γενίκευση του Ορισμού 2.4 της κλασικής πολυπλοκότητας $c(y)$ μίας ακολουθίας. Για κάθε ακολουθία y ισχύει

$$C_s(y) \leq C_f(y) \leq c(y) \leq C_l(y)$$

Στο κεφάλαιο 4 θα δούμε πως η πολυπλοκότητα γραμμικής πραγματοποίησης ταυτίζεται με τη γραμμική πολυπλοκότητα της ακολουθίας.

Οι παραπάνω έννοιες αποσαφηνίζονται στο ακόλουθο παράδειγμα.

Παράδειγμα 3.9. Έστω y μία περιοδική δυαδική ακολουθία με περίοδο $T = 21$, όπου τα πρώτα T στοιχεία της δίνονται από το διάνυσμα

$$\boldsymbol{y} = (0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0).$$

Με βάση την προηγούμενη ανάλυση, η πολυπλοκότητα συνόλου της ακολουθίας y ισούται με $C_s(y) = \log_2 21 \approx 4.39$, και κάθε ελάχιστη πραγματοποίηση συνόλου της y θα έχει τάξη 21. Επειδή η περίοδος της y είναι διαιρέτης του αριθμού 2^6-1, ορίζεται ο μετασχηματισμός Fourier της y και μπορεί να χρησιμοποιηθεί για την κατασκευή μίας ελάχιστης πραγματοποίησης συνόλου $\mathfrak{S}$. Συγκεκριμένα, θεωρούμε ως χώρο καταστάσεων του $\mathfrak{S}$ το σύνολο

$$S = \left\{x_i \in \mathbb{F}_{2^6} : x_i = \alpha^{3i}, 0 \leq i < 21\right\}$$

όπου το στοιχείο $\alpha \in \mathbb{F}_{2^6}$ είναι πρωταρχικό στο $\mathbb{F}_{2^6}$ με $\alpha^6 = \alpha + 1$, ενώ επίσης επιλέγουμε ως αρχική κατάσταση του $\mathfrak{S}$ το στοιχείο $x_0 = 1$. Τότε, η αναπαράσταση (2.13) της ακολουθίας οδηγεί στον προσδιορισμό των συναρτήσεων f, g της πραγματοποίησης συνόλου: συγκεκριμένα, αν για κάθε $x \in S$ θέσουμε $f(x) = a^3x$, τότε η συνάρτηση εξόδου g προσδιορίζεται πλήρως από το μετασχηματισμό Fourier της y και ισούται με

$$g(x) = \mathrm{tr}_1^6(\alpha^{14}x^{-1}) + \mathrm{tr}_1^6(\alpha^{54}x^{-3}) + \mathrm{tr}_1^6(\alpha^{34}x^{-5}) + \mathrm{tr}_1^6(\alpha^{21}x^{-7}) + \mathrm{tr}_1^3(\alpha^{54}x^{-9}).$$

Η πολυπλοκότητα σώματος της y ισούται με $C_f = 5$, γιατί $2^4 < 21 < 2^5$. Έστω $\alpha \in \mathbb{F}_{2^5}$ ένα πρωταρχικό στοιχείο του σώματος $\mathbb{F}_{2^5}$ με $\alpha^5 = \alpha^2+1$. Τότε, για μία ελάχιστη πραγματοποίηση σώματος της y με σύνολο καταστάσεων τα στοιχεία του $\mathbb{F}_{2^5}$, ορίζουμε ως αρχική κατάσταση $x_0 = 1$ και ως συνάρτηση μετάβασης κατάστασης f την ακόλουθη

$$f(x) = \begin{cases} \alpha x & \text{αν } x \in \{1, \alpha, \ldots, \alpha^{19}\} \\ 1 & \text{αν } x = \alpha^{20} \\ b(x) & \text{αν } x \in B = \{0, \alpha^{21}, \ldots, \alpha^{30}\} \end{cases}$$

όπου $b : B \to B$ αυθαίρετη συνάρτηση. Για την παραπάνω f, η συνάρτηση εξόδου g μπορεί να υπολογιστεί ως εξής:

- επεκτείνουμε το διάνυσμα $\boldsymbol{y}$ κατά 10 αυθαίρετα στοιχεία του σώματος $\mathbb{F}_2$, έτσι ώστε να προκύψει ένα διάνυσμα $\boldsymbol{y}'$ μήκους $2^5 - 1 = 31$,
- για την ακολουθία περιόδου 31, όπου τα πρώτα 31 ψηφία της δίνονται από το διάνυσμα $\boldsymbol{y}'$, υπολογίζουμε το μετασχηματισμό Fourier της,
- η g προσδιορίζεται από τον αντίστροφο μετασχηματισμό Fourier που υπολογίστηκε ανωτέρω.

Η παραπάνω κατασκευή θα οδηγήσει σε μία συνάρτηση εξόδου g της οποίας το σύνολο τιμών είναι το $\mathbb{F}_2$. Συνεπώς, επεκτείνοντας το $\boldsymbol{y}$ με τα στοιχεία 0 0 0 0 1 0 0 0 0 1 (τυχαία bits), η συνάρτηση εξόδου g που προκύπτει είναι η ακόλουθη:

$$g(x) = \mathrm{tr}_1^5(\alpha^{29}x^{-3}) + \mathrm{tr}_1^5(\alpha^{28}x^{-5}) + \mathrm{tr}_1^5(\alpha^{21}x^{-7}) + \mathrm{tr}_1^5(\alpha^{26}x^{-11}) + \mathrm{tr}_1^5(\alpha^{14}x^{-15}).$$

Όσον αφορά τη μη γραμμική πολυπλοκότητα της ακολουθίας y, παρατηρούμε ότι $y_5^{10} = y_{20}^{25} = 001111$ και $y_{11} \neq y_{26}$, ενώ επίσης δεν υπάρχει άλλο ζευγάρι υπακολουθιών της y με μεγαλύτερα μήκη που να πληρούν αυτήν την ιδιότητα. Άρα, λόγω της Πρότασης 2.7, προκύπτει ότι $c(y) = 7$. Τέλος, με τον Berlekamp-Massey αλγόριθμο υπολογίζουμε τη γραμμική πολυπλοκότητα της ακολουθίας $\mathrm{lc}(y) = 20$, άρα ισχύει και $C_l(y) = 20$ (η ισότητα $\mathrm{lc}(y) = C_l(y)$ αποσαφηνίζεται στο Κεφάλαιο 4). □

Από την ανάλυση που προηγήθηκε γίνεται φανερό ότι η πολυπλοκότητα συνόλου μιας ακολουθίας είναι στενά συνδεδεμένη με την περίοδό της και, συνεπώς, περιγράφει το πώς η περίοδος επιδρά στο χαρακτηρισμό της ακολουθίας ως κρυπτογραφικά κατάλληλης ή μη· πράγματι, επιθυμητό χαρακτηριστικό για μία κρυπτογραφική ακολουθία είναι η μεγάλη περίοδος και, άρα, η μεγάλη πολυπλοκότητα συνόλου. Επίσης, η πολυπλοκότητα σώματος μιας ακολουθίας σχετίζεται με το μήκος του μικρότερου FSR ο οποίος μπορεί να παράγει την ακολουθία αν εφαρμόσουμε μη γραμμικό φίλτρο στις βαθμίδες του: αν $C_f(y) = n$, τότε είναι εύκολο να δούμε ότι δεν υπάρχει FSR μήκους μικρότερου από n που να παράγει την y, ακόμα και αν υπάρχει η δυνατότητα να χρησιμοποιηθεί ένα οποιοδήποτε μη γραμμικό φίλτρο. Αξίζει να αναφερθεί πως αν η περίοδος μίας δυαδικής ακολουθίας είναι ακριβώς $2^n - 1$, τότε η πολυπλοκότητα σώματος n ταυτίζεται με το μήκος του μικρότερου FSR ο οποίος παράγει την

ακολουθία μέσω κατάλληλα επιλεγμένου μη γραμμικού φίλτρου. Ένα τέτοιο σύστημα παραγωγής της ακολουθίας αποτελείται από έναν πρωταρχικό LFSR μήκους n που περνάει από $2^n - 1$ διαφορετικές καταστάσεις, ενώ το κατάλληλο φίλτρο μπορεί να υπολογιστεί με χρήση παρεμβολής Lagrange, έτσι ώστε να εξασφαλίζεται ότι, για κάθε κατάσταση του LFSR, η έξοδος του συστήματος θα ισούται με το επιθυμητό bit.

3.3 Γεννήτριες ακολουθιών De Brujin

Όπως αναφέρθηκε στην Ενότητα 2.1, μία ακολουθία y στο σώμα $\mathbb{F}_q$ καλείται *ακολουθία De Brujin* αν έχει περίοδο q^n για κάποιον θετικό ακέραιο n και, επιπλέον, τα διανύσματα

$$\boldsymbol{x}_i = (y_{i+n-1}\ y_{i+n-2}\ \dots\ y_i), \qquad 0 \leq\ i \leq\ q^n - 1,$$

καλύπτουν όλον το διανυσματικό χώρο $\mathbb{F}_q^n$. Συνδυάζοντας τον ορισμό των ακολουθιών De Brujin και την Πρόταση 2.7, συμπεραίνουμε ότι η μη γραμμική πολυπλοκότητα κάθε ακολουθίας De Brujin περιόδου q^n ισούται με n. Άρα, υπάρχει FSR μήκους n που την παράγει βάσει μίας αναδρομικής σχέσης της μορφής (2.1). Έστω h η συνάρτηση ανάδρασης ενός FSR που παράγει την De Brujin ακολουθία y. Τότε μία καταστατική αναπαράσταση γεννήτριας της y δίνεται από το ζευγάρι (3.1a)-(3.1b), όπου

$$x_0 = (x_{0,0}\ x_{0,1}\ \dots,\ x_{0,n-1}) = (y_{q^n-1}\ y_{q^n-2} \dots\ y_{q^n-n})^T, \tag{3.4}$$

$$\begin{aligned} x_{i+1} &= f(x_i) = f(x_{i,0}, x_{i,1}, \dots, x_{i,n-1}) = \\ &= (h(x_{i,0}, x_{i,1}, \dots, x_{i,n-1})\ x_{i,0}\ \dots\ x_{i,n-2})^T, \end{aligned} \tag{3.5}$$

$$g(x_i) = h(x_i) = h(x_{i,0}, x_{i,1}, \dots, x_{i,n-1}). \tag{3.6}$$

Στο υπόλοιπο της ενότητας, κάθε σύστημα $\mathfrak{S} = \langle \mathbb{F}_q^n, \mathbb{F}_q, f, g, x_0 \rangle$ της παραπάνω μορφής που παράγει ακολουθίες De Brujin στο σώμα $\mathbb{F}_q$ θα καλείται *γεννήτρια De Brujin*.

Θεώρημα 3.10. *Έστω μία γεννήτρια De Brujin $\mathfrak{S} = \langle \mathbb{F}_q^n, \mathbb{F}_q, f, g, x_0 \rangle$. Τότε*

1. *Για κάθε $x \in \mathbb{F}_q^n$, η συνάρτηση f ικανοποιεί την ιδιότητα*

$$f^{q^n}(x) = x \text{ και } f^j(x) \neq x, \text{ για κάθε } j < q^n.$$

2. *Η συνάρτηση $\Phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$*

$$\Phi(x) = \big(g(x)\ g(f(x)) \dots\ g(f^{n-1}(x))\big)^T$$

είναι αντιστρέψιμη.

Αντιστρόφως, κάθε ζευγάρι καταστατικών εξισώσεων (3.1a) - (3.1b) *που ικανοποιεί τις ιδιότητες* 1 *και* 2 *παράγει ακολουθίες De Brujin και αποτελεί μία ελάχιστη υλοποίησή τους.*

Απόδειξη. Η ιδιότητα 1 προκύπτει άμεσα από τον ορισμό των ακολουθιών De Brujin και την (3.5). Για να αποδείξουμε ότι η συνάρτηση Φ είναι αντιστρέψιμη, θεωρούμε δύο διαφορετικές καταστάσεις x_t, x_τ του χώρου $\mathbb{F}_q^n$

$$x_t = (y_{t+n-1}\ y_{t+n-2} \dots\ y_t)^T,$$
$$x_\tau = (y_{\tau+n-1}\ y_{\tau+n-2} \dots\ y_\tau)^T.$$

Τότε, τα διανύσματα

$$\Phi(x_t) = (y_{t+n}\ y_{t+n+1} \dots\ y_{t+2n-1})^T,$$
$$\Phi(x_\tau) = (y_{\tau+n}\ y_{\tau+n+1} \dots\ y_{\tau+2n-1})^T$$

είναι διαφορετικά. Άρα, η συνάρτηση Φ είναι αντιστρέψιμη.

Για το δεύτερο σκέλος της απόδειξης, ορίζουμε τη συνάρτηση $\phi : \mathbb{F}_q^n \to \mathbb{F}_q$ ως

$$\phi(x) = gf^n(\Phi^{-1}(x))$$

Τότε, ισχύουν τα ακόλουθα

$$\begin{aligned}\phi((y_0\ y_1\ \dots y_{n-1})^T) &= \phi((g(x_0)\ g(f(x_0))\ \dots\ g(f^{n-1}(x_0)))^T)\\ &= \phi(\Phi(x_0)) = gf^n(\Phi^{-1}(\Phi(x_0))) = gf^n(x_0) = y_n.\end{aligned}$$

Επίσης, για κάθε $t > n$, θέτουμε $x = f^{t-n}(x_0)$, οπότε:

$$\begin{aligned}\phi((y_{t-n}\ y_{t-n+1}\ \dots\ y_{t-1})^T) &= \phi((g(x)\ g(f(x))\ \dots\ g(f^{n-1}(x)))^T)\\ &= \phi(\Phi(x)) = gf^n(\Phi^{-1}\Phi(x))\\ &= gf^n(x) = gf^n(f^{t-n}(x_0)) = gf^t(x_0) = y_t.\end{aligned}$$

Κατά συνέπεια, αποδείξαμε ότι

$$y_t = \phi((y_{t-n}\ y_{t-n+1}\ \dots\ y_{t-1})^T),\ \forall\ t \geq n.$$

Από την παραπάνω σχέση, καθώς και από το γεγονός ότι η συνάρτηση μετάβασης κατάστασης f περνάει από όλες τις καταστάσεις μία φορά σε κάθε περίοδο, προκύπτει ότι η παραγόμενη ακολουθία y είναι De Brujin, ενώ επιπλέον η συνάρτηση ϕ αποτελεί τη συνάρτηση

ανάδρασης ενός FSR που παράγει την y. Επίσης, αφού το σύνολο καταστάσεων αποτελείται από q^n στοιχεία, όσο και η περίοδος της ακολουθίας, συμπεραίνουμε ότι κάθε τέτοιο σύστημα αποτελεί ελάχιστη πραγματοποίηση της παραγόμενης ακολουθίας. □

Από την προηγούμενη ανάλυση και τον ορισμό των μέτρων πολυπλοκότητας της Ενότητας 3.2, προκύπτει το επόμενο Πόρισμα:

Πόρισμα 3.11. *Ισχύει*

$$C_s(y) = C_f(y) = c(y)$$

αν και μόνο αν η y είναι ακολουθία De Brujin.

Όσον αφορά τη γραμμική πολυπλοκότητα των ακολουθιών De Brujin, άνω και κάτω φράγματα είναι μόνο γνωστά μέχρι σήμερα [35]: για μία δυαδική ακολουθία De Brujin περιόδου 2^n, ισχύει $2^{n-1} + n \leq \mathrm{lc}(y) \leq 2^n - 1$, ενώ επίσης έχει αποδειχτεί ότι δεν υπάρχει δυαδική ακολουθία De Brujin με γραμμική πολυπλοκότητα ίση με $2^{n-1} + n + 1$. Ωστόσο, δεν είναι γνωστό αν για κάθε τιμή c στο διάστημα $\{2^{n-1} + n,\ 2^{n-1} + n + 2,\ 2^{n-1} + n + 3,\ \ldots, 2^n - 1\}$ υπάρχει ακολουθία De Brujin με γραμμική πολυπλοκότητα ίση με c. Η περίπτωση μη δυαδικών ακολουθιών De Brujin έχει μελετηθεί στο [6].

Κεφάλαιο 4

Καταστατικές αναπαραστάσεις και γραμμική πολυπλοκότητα ακολουθιών

One should always generalize.

Carl Jacobi

Στο παρόν κεφάλαιο μελετώνται δυαδικές περιοδικές ακολουθίες οι οποίες παράγονται από γραμμικά καταστατικά συστήματα. Κάνοντας χρήση ιδιοτήτων ελεγξιμότητας και παρατηρησιμότητας, αποδεικνύεται ότι η διάσταση μίας ελάχιστης γραμμικής καταστατικής γεννήτριας μίας ακολουθίας ισούται με τη γραμμική της πολυπλοκότητα. Η προσέγγιση αυτή, η οποία βασίζεται σε εργαλεία της θεωρίας συστημάτων, παρέχει έναν ενιαίο φορμαλισμό που περιγράφει όλες τις ακολουθίες ανεξαρτήτως περιόδου. Αποδεικνύεται ότι οι γεννήτριες δυαδικών ακολουθιών με περίοδο περιττό αριθμό μπορούν να περιγραφούν απο γραμμικά καταστατικά συστήματα των οποίων ο πίνακας μετάβασης κατάστασης είναι διαγώνιος, ενώ αντιστοίχως ένα καταστατικό σύστημα που παράγει ακολουθίες άρτιας περιόδου έχει πίνακα μετάβασης σε κανονική μορφή Jordan. Άμεση απόρροια αυτού είναι μία καινούρια *διανυσματική αναπαράσταση ίχνους* η οποία περιγράφει όλες τις περιοδικές ακολουθίες ανεξαρτήτως περιόδου, γενικεύοντας κατά αυτόν τον τρόπο την κλασική αναπαράσταση ίχνους (σχέση (2.13)) των ακολουθιών περιττής περιόδου· η γενίκευση αυτή επιτρέπει την παραγωγή ακολουθιών που να επιτυγχάνουν οποιαδήποτε επιθυμητή τιμή για τη γραμμική πολυπλοκότητα αφού επιτρέπει, για οποιονδήποτε δοθέντα LFSR, τον προσδιορισμό κατάλληλης αρχικής κατάστασης έτσι ώστε να παράγεται ακολουθία με τη μέγιστη δυνατή γραμμική πολυπλοκότητα - δηλαδή, ίση με το μήκος του LFSR. Άμεση απόρροια της διανυσματικής αναπαράστασης ίχνους είναι ένας νέος *Γενικευμένος Μετασχηματισμός Fourier* ο οποίος ορίζεται για κάθε ακολουθία και επιτρέπει τον άμεσο προσδιορισμό της γραμμικής πολυπλοκότητάς της, όπως και ο GDFT της ενό-

τητας 2.3.1. Σημαντικό πλεονέκτημα του νέου γενικευμένου μετασχηματισμού Fourier που προτείνεται σε αυτό το κεφάλαιο είναι το γεγονός ότι αποτελεί άμεση γενίκευση του κλασικού μετασχηματισμού Fourier, αν ληφθεί υπ'όψιν η ισοδύναμη γραφή των LFSRs ως ζευγάρι καταστατικών εξισώσεων.

Υπό το ίδιο πρίσμα, μελετώνται συστήματα μη γραμμικών φίλτρων τα οποία εφαρμόζονται στις βαθμίδες ενός πρωταρχικού LFSR (αυτά τα συστήματα έχουν περιγραφεί στην ενότητα 2.5.2). Αυτές οι γεννήτριες ακολουθιών περιγράφονται ομοίως από μη γραμμικές καταστατικές εξισώσεις, οι οποίες μετατρέπονται σε γραμμικές κάνοντας χρήση ιδιοτήτων των γινομένων Kronecker. Οι ισοδύναμες γραμμικές αναπαραστάσεις για τα συστήματα μη γραμμικών φίλτρων επιτρέπουν τη διατύπωση συνθηκών οι οποίες καθορίζουν τη γραμμική πολυπλοκότητα της παραγόμενης ακολουθίας. Αποδεικνύεται ότι το γνωστό κριτήριο ύπαρξης ριζών του Rueppel μπορεί επίσης να εξαχθεί μέσω αυτής της προσέγγισης. Τέλος, περιγράφεται μία νέα κατηγορία μη γραμμικών φίλτρων, τα οποία εξασφαλίζουν το ίδιο κάτω φράγμα για τη γραμμική πολυπλοκότητα όσο και τα ισαπέχοντα φίλτρα. Η νέα αυτή οικογένεια μη γραμμικών φίλτρων γενικεύει διάφορες γνωστές οικογένειες φίλτρων με καλά χαρακτηριστικά. Κατά συνέπεια, η κατασκευή που προτείνεται εδώ παρέχει εν τέλει περισσότερες δυνατότητες και μεγαλύτερη ευελιξία όσον αφορά την επιλογή μη γραμμικών φίλτρων με καλά χαρακτηριστικά για σχεδίαση κρυπτογραφικών συστημάτων.

4.1 Ελάχιστες γραμμικές πραγματοποιήσεις ακολουθιών

Κάθε LFSR μήκους n με χαρακτηριστικό πολυώνυμο

$$h(z) = a_0 + a_1 z + \ldots + a_{n-1} z^{n-1} + z^n$$

μπορεί ισοδύναμα να γραφτεί σαν ένα γραμμικό καταστατικό σύστημα $\mathfrak{L} = \langle \boldsymbol{A}, c, x_0 \rangle$ της μορφής

$$x_{i+1} = \boldsymbol{A}\, x_i \tag{4.1a}$$

$$y_i = c^T\, x_i \tag{4.1b}$$

όπου τα $x_i, c = (1\ 0\ \cdots\ 0)^T$ είναι $n \times 1$ διανύσματα, το c^T υποδηλώνει τον ανάστροφο πίνακα

του c και

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{n-1} \end{pmatrix}. \tag{4.2}$$

Η αρχική κατάσταση x_0 του $\mathfrak{L}$ είναι το διάνυσμα $x_0 = (y_0 \ \cdots \ y_{n-1})^T$. Η *διάσταση (dimension)* του συστήματος $\mathfrak{L}$ δίνεται από τον ακέραιο n. Ο πίνακας $\boldsymbol{A}$ είναι ο *πίνακας μετάβασης κατάστασης (state transition matrix)* του συστήματος. Το $\mathfrak{L}$ καλείται *γραμμική πραγματοποίηση (linear realization)* της ακολουθίας y. Μία γραμμική πραγματοποίηση της y είναι *ελάχιστη (minimal)* εάν δεν υπάρχει άλλη γραμμική πραγματοποίηση μικρότερης διάστασης για την ίδια ακολουθία. Οι ελάχιστες γραμμικές πραγματοποιήσεις χαρακτηρίζονται από το ακόλουθο Θεώρημα.

Θεώρημα 4.1 ([23, 67]). *Ένα γραμμικό σύστημα $\mathfrak{L} = \langle \boldsymbol{A}, c, x_0 \rangle$ διάστασης n, που παράγει την περιοδική ακολουθία y, είναι ελάχιστη πραγματοποίηση της y αν και μόνο αν είναι ταυτόχρονα ελέγξιμο και παρατηρήσιμο ή, ισοδύναμα, αν και μόνο αν οι πίνακες ελεγξιμότητας $\boldsymbol{C}$ και παρατηρησιμότητας $\boldsymbol{O}$, που ορίζονται ως*

$$\boldsymbol{C} = \begin{pmatrix} x_0 & \boldsymbol{A}x_0 & \cdots & \boldsymbol{A}^{n-1}x_0 \end{pmatrix} \quad \text{και} \quad \boldsymbol{O} = \begin{pmatrix} c & \boldsymbol{A}^T c & \cdots & (\boldsymbol{A}^{n-1})^T c \end{pmatrix}^T \tag{4.3}$$

έχουν βαθμό (rank) n.

Επιπλέον, αν τα συστήματα $\mathfrak{L} = \langle \boldsymbol{A}, c, x_0 \rangle$ και $\mathfrak{L}' = \langle \boldsymbol{A}', c', x_0' \rangle$ είναι δύο ελάχιστες γραμμικές υλοποιήσεις μίας περιοδικής ακολουθίας y, τότε είναι γραμμικά ισόμορφα ή ισοδύναμα, δηλαδή υπάρχει αντιστρέψιμος πίνακας $\boldsymbol{P}$ τέτοιος ώστε $\boldsymbol{A}' = \boldsymbol{P}\boldsymbol{A}\boldsymbol{P}^{-1}$, $c'^T = c^T\boldsymbol{P}^{-1}$, και $x_0' = \boldsymbol{P}x_0$.

Κάθε τετραγωνικός πίνακας με στοιχεία σε κάποιο αλγεβρικά κλειστό σώμα είναι όμοιος (ισόμορφος) με κάποιον πίνακα ο οποίος είναι σε *κανονική μορφή Jordan (Jordan canonical form)* [53]. Κάθε πίνακας $\boldsymbol{J}$ αυτής της μορφής είναι μπλοκ διαγώνιος (block-diagonal), όπου κάθε μπλοκ $\boldsymbol{J}_\lambda$, που καλείται *Jordan μπλοκ (Jordan block)*, είναι τετραγωνικός πίνακας που όλα τα διαγώνια στοιχεία του έχουν σταθερή τιμή λ, ενώ όλα τα στοιχεία του που βρίσκονται ακριβώς μία θέση πάνω από κάποιο διαγώνιο στοιχείο ισούνται με 1, δηλαδή

$$\boldsymbol{J}_\lambda = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

Το διαγώνιο στοιχείο λ του $\boldsymbol{J}_\lambda$ αποτελεί μία ιδιοτιμή του $\boldsymbol{J}$. Όπως είναι γνωστό, δύο όμοιοι πίνακες έχουν τις ίδιες ιδιοτιμές, με τις ίδιες πολλαπλότητες. Για κάθε πίνακα, η ισοδύναμη μορφή Jordan είναι μοναδική (αν εξαιρέσουμε τη διάταξη των Jordan blocks, που μπορεί να γίνει με οποιονδήποτε τρόπο). Αξίζει να σημειωθεί ότι οι διαγώνιοι πίνακες αποτελούν ειδική περίπτωση πινάκων κανονικής μορφής Jordan, στους οποίους κάθε Jordan μπλοκ έχει διάσταση 1. Κατά συνέπεια, ανακαλώντας το Θεώρημα 4.1, για κάθε περιοδική ακολουθία y υπάρχει πάντα μία ελάχιστη γραμμική πραγματοποίηση (μεταξύ του συνόλου όλων των ισοδύναμων ελαχίστων υλοποιήσεων) τέτοια ώστε ο πίνακας μετάβασης κατάστασης να είναι σε κανονική μορφή Jordan. Τα συστήματα αυτής της μορφής παρουσιάζουν ιδιαίτερο ενδιαφέρον, γιατί η ελεγξιμότητα και η παρατηρησιμότητά τους προσδιορίζονται άμεσα από το ακόλουθο Θεώρημα.

Θεώρημα 4.2 ([23]). *Έστω $\mathfrak{L} = \langle \boldsymbol{A}, c, x_0 \rangle$ μία γραμμική πραγματοποίηση μίας ακολουθίας y, όπου ο $\boldsymbol{A}$ είναι σε κανονική μορφή Jordan. Τότε, το $\mathfrak{L}$ είναι ελέγξιμο (παρατηρήσιμο) αν και μόνο αν*

1. *για κάθε ιδιοτιμή λ του $\boldsymbol{A}$, υπάρχει ακριβώς ένα Jordan μπλοκ $\boldsymbol{J}_\lambda$ που να αντιστοιχεί σε αυτή,*
2. *όλα τα στοιχεία του x_0 (c) στη σχέση (4.1) που αντιστοιχούν στην τελευταία γραμμή (πρώτη στήλη) κάθε Jordan μπλοκ είναι διάφορα του μηδενός.*

Αν ο $\boldsymbol{A}$ είναι διαγώνιος, το $\mathfrak{L}$ αποτελεί ελάχιστη πραγματοποίηση της y τότε και μόνο τότε όταν όλες οι ιδιοτιμές του $\boldsymbol{A}$ είναι ανά δύο διαφορετικές μεταξύ τους και όλα τα στοιχεία των x_0, c είναι μη μηδενικά.

Στο εξής, κάθε γραμμική πραγματοποίηση μίας ακολουθίας που έχει διαγώνιο πίνακα μετάβασης κατάστασης θα καλείται *διαγώνια πραγματοποίηση (diagonal realization)* της ακολουθίας. Αν γνωρίζουμε μία διαγώνια πραγματοποίηση μίας ακολουθίας y, τότε μπορούμε να κατασκευάσουμε μία ελάχιστη διαγώνια πραγματοποίηση της y (δηλαδή, μία γεννήτρια της y που να είναι ταυτόχρονα ελέγξιμη και παρατηρήσιμη) μέσω της ακόλουθης διαδικασίας.

Παρατήρηση 4.3. Έστω ένα σύστημα $\mathfrak{L} = \langle \boldsymbol{D}, c, x_0 \rangle$ διάστασης n, με αρχική κατάσταση $x_0 = (x_{0,0}\ x_{0,1}\ \cdots\ x_{0,n-1})^T$, $c = (c_0\ c_1\ \cdots\ c_{n-1})^T$, και πίνακα μετάβασης κατάστασης $\boldsymbol{D} = \mathrm{diag}(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$. Τότε, η παραγόμενη ακολουθία y δίνεται από την

$$y_i = \sum_{j=0}^{n-1} c_j \lambda_j^i x_{0,j}, \qquad i \geq 0\,. \tag{4.4}$$

Στη συνέχεια ορίζουμε τις διαμερίσεις $P_\mu = \{j : \lambda_j = \mu \text{ και } 0 \leq j < n\}$ για όλες τις διαφορετικές ιδιοτιμές του $\boldsymbol{D}$. Αν υπάρχει τουλάχιστον ένα μη μηδενικό στοιχείο $x_{0,k}$ στο σύνολο $\{x_{0,j} : j \in P_\mu\}$, τότε από την (4.4) προκύπτει ένα ισοδύναμο σύστημα μικρότερης διάστασης αν θέσουμε

$$c_k = c_k + x_{0,k}^{-1} \sum_{j \in P_\mu \setminus \{k\}} c_j x_{0,j} \tag{4.5}$$

και απομακρύνουμε την j-ιοστή γραμμή και στήλη του $\boldsymbol{D}$, καθώς επίσης και τα j-ιοστά στοιχεία των x_0, c για όλα τα $j \in P_\mu \setminus \{k\}$. Διαφορετικά, αν όλα τα στοιχεία $\{x_{0,j} : j \in P_\mu\}$ είναι μηδενικά, ή αν από την (4.5) προκύπτει $c_k = 0$, τότε η παραπάνω διαδικασία μείωσης της διάστασης του συστήματος λαμβάνει χώρα για όλα τα $j \in P_\mu$. Άρα, με αυτόν τον τρόπο το σύστημα μπορεί να μετασχηματιστεί σε ένα άλλο μικρότερης διάστασης που παράγει την ακολουθία y και είναι ελέγξιμο και παρατηρήσιμο λόγω του Θεωρήματος 4.2. Έτσι, κατασκευάζουμε μία ελάχιστη πραγματοποίηση της y.

4.2 Διανυσματική αναπαράσταση ίχνους ακολουθιών

Σε αυτήν την ενότητα θα παρουσιαστεί μία νέα γενικευμένη αναπαράσταση ίχνους που περιγράφει όλες τις ακολουθίες, ανεξαρτήτως περιόδου. Αρχικά, διερευνώνται οι σχέσεις μεταξύ των πραγματοποιήσεων μίας ακολουθίας και του μετασχηματισμού Fourier αυτής.

Λήμμα 4.4. *Έστω y μία περιοδική δυαδική ακολουθία με περίοδο N. Τότε, η y έχει μία διαγώνια πραγματοποίηση $\mathfrak{L}$ αν και μόνο αν υπάρχει ο μετασχηματισμός Fourier αυτής ή, ισοδύναμα, αν και μόνο αν* $\gcd(N, 2) = 1$.

Απόδειξη. Αφού η περίοδος της y είναι N, υπάρχει μία γραμμική πραγματοποίηση $\mathfrak{L} = \langle \boldsymbol{A}, c, x_0 \rangle$ της y διάστασης N, όπου $x_0 = (y_0\ y_1\ \cdots\ y_{N-1})^T$, $c = (1\ 0\ \cdots\ 0)^T$, και ο πίνακας μετάβασης κατάστασης δίνεται από την

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix}. \tag{4.6}$$

Οι ιδιοτιμές του πίνακα $\boldsymbol{A}$ είναι οι ρίζες του χαρακτηριστικού του πολυωνύμου $f(z) = \det(\boldsymbol{A} - z\boldsymbol{I}_N) = z^N - 1$, όπου με $\boldsymbol{I}_N$ υποδηλώνουμε τον $N \times N$ μοναδιαίο πίνακα.

Έστω ότι υπάρχει ο μετασχηματισμός Fourier της y. Αρκεί να αποδειχτεί πως ο πίνακας $\boldsymbol{A}$ που δίνεται από την (4.6) είναι διαγωνοποιήσιμος. Λόγω της ύπαρξης του μετασχηματισμού

Fourier, προκύπτει ότι υπάρχει ρίζα N-ιοστής τάξης της μονάδας σε κάποιο ευρύτερο σώμα ή, ισοδύναμα, $\gcd(N, 2) = 1$ [89]. Άρα, αφού το N είναι περιττός αριθμός, όλες οι ιδιοτιμές του $\boldsymbol{A}$ είναι ανά δύο διαφορετικές μεταξύ τους [89], οπότε ο $\boldsymbol{A}$ διαγωνοποιείται.

Αντίστροφα, ας υποθέσουμε ότι η ακολουθία y έχει μία διαγώνια πραγματοποίηση $\mathfrak{D} = \langle \boldsymbol{D}, d, z_0 \rangle$. Χωρίς βλάβη της γενικότητας, θεωρούμε πως ο $\boldsymbol{D}$ προέκυψε από διαγωνοποίηση του πίνακα $\boldsymbol{A}$ της (4.6), δηλαδή η διάστασή του είναι N. Έστω $N = 2^e m$, όπου m περιττός ακέραιος και $e \geq 0$, και έστω α πρωταρχική ρίζα m-ιοστής τάξης της μονάδας που βρίσκεται στο ευρύτερο σώμα στο οποίο βρίσκονται οι ρίζες του $f(z) = z^N - 1$. Τότε, τα διαγώνια στοιχεία του $\boldsymbol{D}$ είναι τα $1, \alpha, \ldots, \alpha^{m-1}$, το καθένα με πολλαπλότητα 2^e [89, p. 63]. Άρα, ισχύει $\boldsymbol{D}^m = \boldsymbol{I}_N$ και, κατά συνέπεια, η παραγόμενη ακολουθία y έχει περίοδο $m \leq N$. Όμως, αν $m < N$, οδηγούμαστε σε άτοπο λόγω της αρχικής υπόθεσης ότι η y έχει πρωταρχική περίοδο N. Άρα, $e = 0$, το οποίο σημαίνει $\gcd(N, 2) = 1$ - με άλλα λόγια, ο μετασχηματισμός Fourier της y υπάρχει. □

Από την παραπάνω ανάλυση γίνεται φανερό πως αν $\mathfrak{D}$ είναι μία ελάχιστη διαγώνια πραγματοποίηση μίας δυαδικής ακολουθίας y με περίοδο N, τότε οι ιδιοτιμές του πίνακα μετάβασης καταστάσεων του $\mathfrak{D}$ είναι αυτές που θα απομείνουν αν η διαδικασία που περιγράφεται στην Παρατήρηση 4.3 εφαρμοστεί στο σύστημα $\mathfrak{L}$ διάστασης N που δίνεται στην απόδειξη του Λήμματος 4.4. Αν στην (4.4) θέσουμε $\lambda_j = \alpha^{-j}$ και $c_j = 1$, όπου α είναι πρωταρχική ρίζα N-ιοστής τάξης της μονάδας, προκύπτει η σχέση

$$y_i = \sum_{j=0}^{N-1} \alpha^{-ij} x_{0,j}, \qquad i \geq 0\,. \tag{4.7}$$

Συγκρίνοντας τις σχέσεις (2.9) και (4.7) συμπεραίνουμε ότι, αν θέσουμε τις τιμές του $\boldsymbol{c}$ ίσες με 1, τότε η αρχική κατάσταση του $\mathfrak{D}$ ταυτίζεται με τον μετασχηματισμό Fourier της ακολουθίας εξόδου y. Επιπρόσθετα, αν εφαρμόσουμε τη διαδικασία που περιγράφεται στην Παρατήρηση 4.3 έτσι ώστε να κατασκευάσουμε μία ελάχιστη πραγματοποίηση της y, θα προκύψει τελικά σύστημα διάστασης ίσης με το βάρος Hamming του μετασχηματισμού Fourier της y. Άρα, ισχύει το ακόλουθο.

Λήμμα 4.5. *Έστω y περιοδική δυαδική ακολουθία με περίοδο N και μετασχηματισμό Fourier $\boldsymbol{Y}$, όπου $\gcd(N, 2) = 1$. Έστω επίσης α πρωταρχική ρίζα N-ιοστής τάξης της μονάδας. Τότε, η διάσταση μίας ελάχιστης γραμμικής καταστατικής πραγματοποίησης $\mathfrak{L}'$ της y ισούται με τη γραμμική της πολυπλοκότητα. Επιπρόσθετα, το σύστημα $\mathfrak{L}'$ προκύπτει από το σύστημα*

$\mathfrak{L} = \langle \boldsymbol{D}, \mathbf{1}, \boldsymbol{Y} \rangle$ *διάστασης* N*, όπου* $\mathbf{1} = (1\ 1\ \cdots\ 1)^T$ *και*

$$\boldsymbol{D} = \mathrm{diag}(1, \alpha^{-1}, \ldots, \alpha^{-(N-1)}) \tag{4.8}$$

αν αποβάλλουμε από την αρχική κατάσταση $\boldsymbol{Y} = (Y_0\ Y_1\ \ldots\ Y_{N-1})^T$ *τα μηδενικά της στοιχεία, με ταυτόχρονη απομάκρυνση των αντίστοιχων γραμμών και στηλών των πινάκων* $\boldsymbol{D}$ *και* $\boldsymbol{c} = \mathbf{1}$*.*

Παρατήρηση 4.6. Έστω $\boldsymbol{P}$ ο πίνακας ο οποίος διαγωνοποιεί τον πίνακα $\boldsymbol{A}$ της σχέσης (4.6) για περιττό N, δηλαδή $\boldsymbol{D} = \boldsymbol{P}\boldsymbol{A}\boldsymbol{P}^{-1}$, όπου $\boldsymbol{D}$ ο διαγώνιος πίνακας της (4.8). Αποδεικνύουμε στη συνέχεια ότι ο πίνακας $\boldsymbol{P} = [p_{i,j}]$ ικανοποιεί τη σχέση $p_{i,j} = \alpha^{ij}$, $0 \leq i, j < N$, όπου α είναι πρωταρχική ρίζα N-ιοστής τάξης της μονάδας. Πράγματι, σε αυτήν την περίπτωση ισχύει

$$D_{i,j} = \sum_{k=0}^{N-1} \alpha^{ik} \alpha^{-j(k+1)} = \alpha^{-j} \sum_{k=0}^{N-1} \alpha^{(i-j)k} = \begin{cases} \alpha^{-j} & \text{αν } i = j \\ 0 & \text{σε άλλη περίπτωση} \end{cases}$$

αφού ο πολλαπλασιασμός $\boldsymbol{A}\boldsymbol{P}^{-1}$ έχει ως αποτέλεσμα την κυκλική ολίσθηση των γραμμών του $\boldsymbol{P}^{-1}$ κατά μία θέση προς τα πάνω.

Στη συνέχεια αποδεικνύουμε αντίστοιχα αποτελέσματα για την πιο ενδιαφέρουσα περίπτωση όπου ο κλασικός μετασχηματισμός Fourier των ακολουθιών δεν ορίζεται. Αρχικά, αποδεικνύουμε το ακόλουθο αποτέλεσμα.

Λήμμα 4.7. *Έστω* y *δυαδική ακολουθία με άρτια περίοδο* N *η οποία παράγεται από το σύστημα* $\mathfrak{L} = \langle \boldsymbol{J}, c, x_0 \rangle$ *διάστασης* N*, όπου ο* $\boldsymbol{J}$ *είναι πίνακας σε κανονική μορφή Jordan και όμοιος με τον πίνακα* $\boldsymbol{A}$ *της σχέσης* (4.6)*. Τότε ο* $\boldsymbol{J}$ *έχει, για κάθε ιδιοτιμή του, ακριβώς ένα Jordan μπλοκ που να αντιστοιχεί σε αυτή.*

Απόδειξη. Είναι γνωστό από τη γραμμική άλγεβρα πως το πλήθος των τετραγώνων Jordan του $\boldsymbol{J}$ που αντιστοιχούν σε μία ιδιοτιμή ισούται με τη γεωμετρική πολλαπλότητα (geometric multiplicity) της ιδιοτιμής [122]. Λόγω της δομής του πίνακα $\boldsymbol{A}$, ισχύει $\mathrm{rank}(\boldsymbol{A} - \lambda \boldsymbol{I}_N) \geq N-1$ για κάθε ιδιοτιμή λ του $\boldsymbol{A}$. Άρα, η διάσταση του μηδενοχώρου (kernel) του $\boldsymbol{A} - \lambda \boldsymbol{I}_N$ δεν μπορεί να είναι μεγαλύτερη από 1. Κατά συνέπεια, κάθε ιδιοχώρος (eigenspace) του $\boldsymbol{A}$ έχει διάσταση 1 - με άλλα λόγια, η γεωμετρική πολλαπλότητα κάθε ιδιοτιμής του $\boldsymbol{A}$ είναι 1. Άρα, ο $\boldsymbol{J}$ έχει ακριβώς ένα Jordan μπλοκ για κάθε ιδιοτιμή. □

Στη συνέχεια επεκτείνουμε την έννοια της συνάρτησης ίχνους της σχέσης (2.13) έτσι ώστε να δρα όχι σε απλά στοιχεία ενός σώματος αλλά σε διανύσματα. Συγκεκριμένα, αν

$z = (z_1\ z_2\ \cdots\ z_m)^T$ είναι ένα $m \times 1$ διάνυσμα με στοιχεία στο $\mathbb{F}_{2^n}$, τότε ορίζουμε ως *διανυσματική συνάρτηση ίχνους (vectorial trace function)* τη συνάρτηση

$$\mathbf{tr}_1^n(z) = \left(\mathrm{tr}_1^n(z_1)\ \mathrm{tr}_1^n(z_2)\ \cdots\ \mathrm{tr}_1^n(z_m)\right)^T. \tag{4.9}$$

Θεώρημα 4.8. *Έστω $\alpha \in \mathbb{F}_{2^n}$ στοιχείο του σώματος $\mathbb{F}_{2^n}$ τάξης $k > 0$ και ας θεωρήσουμε το πεπερασμένο αυτόματο $\mathfrak{L} = \langle \boldsymbol{J}, \mathbf{1}, x_0 \rangle$ διάστασης m, όπου $x_0 \in \mathbb{F}_{2^n}^m$ και ο $\boldsymbol{J}$ είναι σε κανονική μορφή Jordan*

$$\boldsymbol{J} = \mathrm{diag}(\boldsymbol{J}_1, \boldsymbol{J}_\alpha, \ldots, \boldsymbol{J}_{\alpha^{k-1}}) \tag{4.10}$$

όπου το κάθε μπλοκ $\boldsymbol{J}_{\alpha^i}$ έχει διάσταση d_i, $0 \le i < k$. Η αρχική κατάσταση του $\mathfrak{L}$ γράφεται αντίστοιχα ως $x_0 = (z_0^T\ z_1^T\ \cdots\ z_{k-1}^T)^T$, όπου κάθε $z_i = (z_{i,1}\ z_{i,2}\ \cdots\ z_{i,d_i})^T$ έχει μήκος d_i. Αν το σύστημα $\mathfrak{L}$ ικανοποιεί τις ακόλουθες ιδιότητες

1. *$d_j = d_i$ για κάθε $j \in I_i$,*
2. *$z_{j,r} = z_{i,r}^{2^e}$, $1 \le r \le d_i$, για κάθε $j \in I_i$ τέτοιο ώστε $j \equiv 2^e i \pmod{k}$,*
3. *$z_{i,d_i} \neq 0$ για κάθε $0 \le i < k$*

όπου I_i είναι η κυκλοτομική κλάση modulo k του i, τότε η περιοδική ακολουθία y που παράγεται από το $\mathfrak{L}$ είναι δυαδική και, επιπλέον, το $\mathfrak{L}$ είναι μία ελάχιστη πραγματοποίησή της.

Απόδειξη. Το σύστημα $\mathfrak{L}$ είναι ελάχιστη πραγματοποίηση της y λόγω του Θεωρήματος 4.2. Στη συνέχεια αποδεικνύουμε ότι η ακολουθία $y = \{y_i\}_{i \ge 0}$ είναι δυαδική και περιοδική. Αρχικά, γράφουμε $\boldsymbol{J}_i \triangleq \boldsymbol{J}_{\alpha^i}$ και συμβολίζουμε ως $\mathbf{1}_{d_i}$ το διάνυσμα μήκους d_i που αποτελείται μόνο από 1, $0 \le i < k$. Λόγω της δομής του πίνακα $\boldsymbol{J}$ και της Ιδιότητας 1, η ακολουθία y περιγράφεται από την ακόλουθη έκφραση

$$y_i = \sum_{j=0}^{k-1} \mathbf{1}_{d_j}^T \boldsymbol{J}_j^i z_j = \sum_{j \in I} \mathbf{1}_{d_j}^T \sum_{r \in I_j} \boldsymbol{J}_r^i z_r = \sum_{j \in I} \mathbf{1}_{d_j}^T \sum_{e=0}^{|I_j|-1} \boldsymbol{J}_{2^e j}^i z_{2^e j} \tag{4.11}$$

όπου οι δείκτες λαμβάνονται modulo k και I είναι το σύνολο που απαρτίζεται από τα στοιχεία-οδηγούς όλων των κυκλοτομικών κλάσεων modulo k. Για κάθε $i \ge 0$, αν συμβολίσουμε ως $\gamma_{u,v} \in \mathbb{F}_{2^n}$ το στοιχείο που βρίσκεται στη u-ιοστή γραμμή και στη v-ιοστή στήλη του μπλοκ $\boldsymbol{J}_j^i$, τότε το αντίστοιχο στοιχείο του μπλοκ $\boldsymbol{J}_{2^e j}^i$ ισούται $\gamma_{u,v}^{2^e}$ αφού σε όλους τους υπολογισμούς υπεισέρχεται το $\alpha^{2^e j}$ αντί για το α^j. Άρα, από την (4.11) και την Ιδιότητα 2 προκύπτει

$$y_i = \sum_{j \in I} \mathbf{1}_{d_j}^T\, \mathbf{tr}_1^{n_j}(\boldsymbol{J}_j^i z_j), \qquad i \ge 0 \tag{4.12}$$

όπου $n_j = |I_j|$. Συγκρίνοντας την (4.12) με την (2.13), συμπεραίνουμε ότι η y παίρνει τιμές στο $\mathbb{F}_2$ και είναι περιοδική. □

Αν η Ιδιότητα 3 του Θεωρήματος 4.8 δεν ισχύει, τότε το σύστημα $\mathfrak{L}$ δεν είναι ελάχιστη πραγματοποίηση της y (αφού σε αυτήν την περίπτωση δεν είναι ελέγξιμο). Αν $z_{i,d_i} = 0$ για κάποιο $i = 0, \ldots, k-1$, τότε είναι εύκολο να δειχθεί ότι το $\mathfrak{L}$ μπορεί να μετασχηματιστεί σε ένα ισοδύναμο σύστημα μικρότερης διάστασης αποβάλλοντας το z_{i,d_i} καθώς και τις αντίστοιχες γραμμές και στήλες των πινάκων μετάβασης κατάστασης και εξόδου. Γενικότερα, για $i = 0, \ldots, k-1$ ορίζουμε τους ακέραιους $s_i = \max\{j : z_{i,j} \neq 0 \text{ and } 1 \leq j \leq d_i\}$, όπου για την ειδική περίπτωση όπου όλα τα $z_{i,j}$ είναι μηδενικά ορίζουμε $s_i = 0$. Τότε, λόγω της προηγούμενης παρατήρησης σχετικά με την κατασκευή ισοδύναμου συστήματος μικρότερης διάστασης, γίνεται προφανές ότι η διάσταση $C_l(y)$ της ελάχιστης γραμμικής πραγματοποίησης της y ισούται με

$$C_l(y) = s_0 + s_1 + \cdots + s_{k-1} \,. \tag{4.13}$$

Η προηγούμενη ανάλυση επιτρέπει την περιγραφή ακολουθιών που παράγονται από LFSRs των οποίων το χαρακτηριστικό πολυώνυμο έχει κάποιες ρίζες με πολλαπλότητα μεγαλύτερη από 1 μέσω της διανυσματικής αναπαράστασης ίχνους. Αυτή η περιγραφή δίνεται στο ακόλουθο Θεώρημα.

Θεώρημα 4.9. *Έστω y δυαδική ακολουθία περιόδου $N = 2^e m$, με m περιττό αριθμό και $e > 0$, με ελάχιστο πολυώνυμο $f(z)$ που γράφεται ως*

$$f(z) = f_1(z)^{d_1} f_2(z)^{d_2} \cdots f_r(z)^{d_r} \tag{4.14}$$

όπου $d_s > 0$ και f_s ανάγωγο πολυώνυμο βαθμού n_s, $1 \leq s \leq r$. Έστω επίσης α μια πρωταρχική ρίζα m-ιοστής τάξης της μονάδας και έστω επίσης α^{j_s} μία ρίζα του f_s. Τότε, η ακολουθία y μπορεί να περιγραφεί από τη διανυσματική αναπαράσταση ίχνους

$$y_i = \sum_{1 \leq s \leq r} \mathbf{1}_{d_s}^T \, \mathbf{tr}_1^{n_s}(\boldsymbol{J}_{j_s}^i z_s), \qquad i \geq 0 \tag{4.15}$$

όπου το διάνυσμα $z_s = (z_{s,1} \; z_{s,2} \; \cdots \; z_{s,d_s})$ παίρνει τιμές στο σώμα που βρίσκονται οι ρίζες του $f(z)$ (splitting field του $f(z)$), και το Jordan μπλοκ $\boldsymbol{J}_{j_s}$ έχει διάσταση d_s.

Απόδειξη. Λόγω του Λήμματος 4.7, ο πίνακας της μορφής (4.2) με ελάχιστο πολυώνυμο f είναι ισοδύναμος με τον ακόλουθο Jordan πίνακα

$$\boldsymbol{J} = \mathrm{diag}\big(\boldsymbol{J}_{j_1} \; \cdots \; \boldsymbol{J}_{2^{n_1-1}j_1} \; \bullet\bullet\bullet \; \boldsymbol{J}_{j_r} \; \cdots \; \boldsymbol{J}_{2^{n_r-1}j_r}\big)$$

όπου $\dim(\boldsymbol{J}_{j_s}) = \cdots = \dim(\boldsymbol{J}_{2^{n_s-1}j_s}) = d_s$, για $s = 1, 2, \ldots, r$. Ας θεωρήσουμε το ισοδύναμο καταστατικό σύστημα $\mathfrak{L} = \langle \boldsymbol{J}, \mathbf{1}, x_0 \rangle$, του οποίου η διάσταση είναι $\sum_{s=1}^{r} n_s d_s$. Θα αποδείξουμε ότι η αρχική κατάσταση x_0 ικανοποιεί την ιδιότητα συζυγίας 2 του Θεωρήματος 4.8. Πράγματι, το πλήθος των αρχικών καταστάσεων που ικανοποιούν αυτήν την ιδιότητα είναι $\prod_{s=1}^{r}(2^{n_s})^{d_s}$. Επίσης, από το Θεώρημα 4.2 προκύπτει ότι το σύστημα είναι παρατηρήσιμο και, ως εκ τούτου, οποιεσδήποτε δύο διαφορετικές αρχικές καταστάσεις παράγουν διαφορετικές ακολουθίες [67]. Άρα, υπάρχει μια 1-1 και επί αντιστοιχία μεταξύ του συνόλου των αρχικών καταστάσεων του ισοδύναμου LFSR και αυτών που ικανοποιούν την ιδιότητα συζυγίας. Συνεπώς, το επιθυμητό αποτέλεσμα προκύπτει άμεσα από την ανάλυση που ακολουθείται στην απόδειξη του Θεωρήματος 4.8. Αξίζει να ανακαλέσουμε ότι δυαδικές ακολουθίες των οποίων το ελάχιστο πολυώνυμο δίνεται από την (4.14) έχουν περίοδο $N = 2^{\lceil \log_2 \max\{d_1,\ldots,d_r\} \rceil} \operatorname{lcm}\{N_1, \ldots, N_r\}$, όπου N_s είναι η τάξη του f_s, με $\gcd(N_s, 2) = 1$ για κάθε $1 \leq s \leq r$ [89]. □

Η εξίσωση (4.15) παρέχει μία νέα γενικευμένη αναπαράσταση ίχνους για περιοδικές ακολουθίες των οποίων ο μετασχηματισμός Fourier δεν ορίζεται. Από τα Θεωρήματα 4.8 και 4.9 προκύπτει ότι η γραμμική πολυπλοκότητα *για κάθε* περιοδική ακολουθία ισούται με τη διάσταση της ελάχιστης καταστατικής πραγματοποίησής της. Επίσης, από την (4.15), συμπεραίνουμε ότι υπάρχουν $(2^{n_s})^{d_s-1}(2^{n_s} - 1)$ τρόποι να επιλέξουμε διανύσματα $z_s \in \mathbb{F}_{2^{n_s}}^{d_s}$, για κάθε $1 \leq s \leq r$, των οποίων το τελευταίο στοιχείο να είναι μη μηδενικό. Συνεπώς, το πλήθος των αρχικών καταστάσεων x_0 οι οποίες εν τέλει θα οδηγήσουν στη δημιουργία ακολουθιών με τη μέγιστη δυνατή γραμμική πολυπλοκότητα $\sum_{s=1}^{r} n_s d_s$ είναι $\prod_{s=1}^{r} 2^{n_s d_s}(1 - 2^{-n_s})$. Για κάθε μία από αυτές, η αρχική κατάσταση $\tilde{x}_0$ του ισοδύναμου LFSR προσδιορίζεται εύκολα χρησιμοποιώντας τον πίνακα παρατηρησιμότητας $\boldsymbol{O}$ που περιγράφεται στην (4.3) μέσω της σχέσης $\tilde{x}_0 = \boldsymbol{O}x_0$. Με άλλα λόγια, μπορούμε από οποιονδήποτε LFSR να κατασκευάσουμε ακολουθίες που να έχουν την ίδια περίοδο και γραμμική πολυπλοκότητα όσο και η ακολουθία κρουστικής απόκρισης που προκύπτει από τον συγκεκριμένο LFSR.

Παράδειγμα 4.10. Έστω $\alpha \in \mathbb{F}_{2^6}$ πρωταρχικό στοιχείο του σώματος $\mathbb{F}_{2^6}$, όπου $\alpha^6 = \alpha + 1$, και έστω ο LFSR με χαρακτηριστικό πολυώνυμο $f(z) = (1 + z + z^2)^3(1 + z + z^3)^2$. Οι ρίζες του $f(z)$ είναι οι $\{\alpha^{21}, \alpha^{42}\}$ και $\{\alpha^{27}, \alpha^{54}, \alpha^{45}\}$ με πολλαπλότητες 3 και 2 αντίστοιχα. Ας θεωρήσουμε το ισοδύναμο ελάχιστης διάστασης σύστημα $\mathfrak{L} = \langle \boldsymbol{J}, \mathbf{1}, x_0 \rangle$ όπου ο $\boldsymbol{J}$, διάστασης 12, είναι σε κανονική μορφή Jordan. Τότε, έχουμε

$$\boldsymbol{J} = \operatorname{diag}(\boldsymbol{J}_{21}, \boldsymbol{J}_{42}, \boldsymbol{J}_{27}, \boldsymbol{J}_{54}, \boldsymbol{J}_{45})$$

με $d_{21} = d_{42} = 3, d_{27} = d_{54} = d_{45} = 2$. Έστω

$$x_0 = \left(\alpha^{21}\ \alpha^{42}\ \alpha^{21} \vdots \alpha^{42}\ \alpha^{21}\ \alpha^{42} \vdots \alpha^{18}\ \alpha^{54} \vdots \alpha^{36}\ \alpha^{45} \vdots \alpha^{9}\ \alpha^{27}\right)^T .$$

Η αρχική κατάσταση x_0 ικανοποιεί τις Ιδιότητες 1–3 του Θεωρήματος 4.8. Αν πολλαπλασιάσουμε το διάνυσμα x_0 με τον πίνακα παρατηρησιμότητας $\boldsymbol{O}$ του συστήματος $\mathfrak{L}$, θα προκύψει η αρχική κατάσταση του ισοδύναμου LFSR $\tilde{x}_0 = (0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0)^T$, η οποία εξασφαλίζει την παραγωγή ακολουθίας με γραμμική πολυπλοκότητα 12, δηλαδή τη μέγιστη δυνατή για το συγκεκριμένο LFSR. Η περίοδος της ακολουθίας εξόδου είναι 84, ίση με $\mathrm{ord}(f(z))$ [89].

4.3 Νέος Γενικευμένος Μετασχηματισμός Fourier

Με αφετηρία τη σχέση (4.15) ορίζουμε στη συνέχεια ένα νέο *Γενικευμένο Διακριτό Μετασχηματισμό Fourier (GDFT)* για ακολουθίες με οποιαδήποτε περίοδο της μορφής $N = 2^e m$, όπου ο m είναι περιττός ακέραιος και $e > 0$. Όπως ήδη αναφέρθηκε στην ενότητα 2.3.1, έχουν προταθεί στη βιβλιογραφία διάφοροι μετασχηματισμοί Fourier για να περιγράψουν τις ακολουθίες με περίοδο της παραπάνω μορφής. Ο νέος GDFT που προτείνεται εδώ βασίζεται στην καταστατική αναπαράσταση των LFSRs με πίνακα μετάβασης κατάστασης $\boldsymbol{J}$ σε μορφή Jordan. Στο υπόλοιπο τμήμα της ενότητας θεωρούμε ότι

$$\boldsymbol{J} = \mathrm{diag}\left(\boldsymbol{J}_1, \boldsymbol{J}_{\alpha^{-1}}, \ldots, \boldsymbol{J}_{\alpha^{-(m-1)}}\right) \tag{4.16}$$

όπου α είναι μία πρωταρχική ρίζα m-οστής τάξης της μονάδας στο $\mathbb{F}_2$, η οποία βρίσκεται στο ευρύτερο σώμα (splitting field) όπου το $z^N - 1 = (z^m - 1)^{2^e}$ έχει ρίζες, και κάθε μπλοκ Jordan έχει διάσταση 2^e, σύμφωνα με το Λήμμα 4.7. Έστω y δυαδική ακολουθία περιόδου $N = 2^e m$ η οποία παράγεται από το $\mathfrak{L} = \langle \boldsymbol{J}, \boldsymbol{1}, x_0 \rangle$ διάστασης N, και $\boldsymbol{J} = \boldsymbol{P}_G \boldsymbol{A} \boldsymbol{P}_G^{-1}$, όπου $\boldsymbol{A}$ είναι πίνακας της μορφής (4.6) με χαρακτηριστικό πολυώνυμο $z^N - 1$. Στη συνέχεια συγκρίνουμε τη μορφή του x_0 στο $\mathfrak{L}$ (όπως αυτή περιγράφεται στο Θεώρημα 4.8) με την αντίστοιχη της αρχικής κατάστασης $\boldsymbol{Y}$ του διαγώνιου συστήματος περιττής διάστασης στο Λήμμα 4.5: παρατηρούμε ότι και οι δύο αρχικές καταστάσεις ικανοποιούν μία ιδιότητα συζυγίας και, επίσης, προκύπτουν από το αρχικό καταστατικό σύστημα που περιγράφει τον αντίστοιχο LFSR (άρτιας διάστασης ο πρώτος, περιττής ο δεύτερος) μέσω κατάλληλου μετασχηματισμού ομοιότητας που μετατρέπει τον πίνακα μετάβασης κατάστασης σε κανονική μορφή Jordan (όπου, όταν η περίοδος είναι περιττός αριθμός, ο πίνακας Jordan εκφυλίζεται σε διαγώνιο πίνακα). Με δεδομένο λοιπόν ότι η αρχική κατάσταση $\boldsymbol{Y}$ του συστήματος περιττής διάστασης του Λήμματος 4.5 ισούται με τον DFT της ακολουθίας, προκύπτει ως άμεσο επακόλουθο ο επόμενος ορισμός:

Ορισμός 4.11. Με τον προηγούμενο συμβολισμό, έστω y μία δυαδική ακολουθία περιόδου $N = 2^e m$ που παράγεται από το σύστημα $\mathfrak{L} = \langle \boldsymbol{J}, \mathbf{1}, \boldsymbol{Y} \rangle$ διάστασης N, όπου ο $\boldsymbol{J} = \boldsymbol{P}_G \boldsymbol{A} \boldsymbol{P}_G^{-1}$ δίνεται από την (4.16). Τότε, η αρχική κατάσταση

$$\boldsymbol{Y} = (Y_0 \; Y_1 \; \cdots \; Y_{N-1})^T \tag{4.17}$$

ορίζει το Γενικευμένο Διακριτό Μετασχηματισμό Fourier (GDFT) της y.

Ο παραπάνω ορισμός καλύπτει όλες τις ακολουθίες με τιμές σε κάποιο σώμα με οποιαδήποτε χαρακτηριστική p, αφού τόσο το Θεώρημα 4.8 όσο και η διανυσματική αναπαράσταση ίχνους (4.15) ισχύουν για ακολουθίες σε οποιοδήποτε σώμα (αφού κάθε πίνακας, σε οποιοδήποτε σώμα, είναι όμοιος με κάποιον πίνακα Jordan). Αν $e = 0$ τότε ο GDFT που ορίστηκε παραπάνω καθώς και η διανυσματική αναπαράσταση ίχνους (4.15) συμπίπτουν με τον κλασικό DFT και την απλή αναπαράσταση ίχνους (2.13) αντίστοιχα. Το πλεονέκτημα του GDFT που προτείνεται εδώ, εκτός του ότι αποτελεί άμεση γενίκευση του κλασικού DFT από τη σκοπιά της θεωρίας συστημάτων, είναι το ότι επιτρέπει τον προσδιορισμό της γραμμικής πολυπλοκότητας της ακολουθίας μέσω του βάρους Günther, όπως ακριβώς και ο GDFT που ορίστηκε στο [99]. Πράγματι, ας κατασκευάσουμε από την (4.17) τον ακόλουθο πίνακα

$$\hat{\boldsymbol{Y}} = \begin{pmatrix} Y_{2^e-1} & Y_{2^{e+1}-1} & \cdots & Y_{N-1} \\ Y_{2^e-2} & Y_{2^{e+1}-2} & \cdots & Y_{N-2} \\ \vdots & \vdots & & \vdots \\ Y_0 & Y_{2^e} & \cdots & Y_{N-2^e} \end{pmatrix}.$$

Τότε, λόγω της (4.13), προκύπτει ότι η γραμμική πολυπλοκότητα της y ισούται με το βάρος Günther του πίνακα $\hat{\boldsymbol{Y}}$. Το ακόλουθο παράδειγμα συγκρίνει τον GDFT που προτείνεται εδώ με τον GDFT του [99].

Παράδειγμα 4.12. Ας θεωρήσουμε την περιοδική ακολουθία

$$\boldsymbol{y} = (0\;0\;1\;0\;1\;0\;1\;0\;0\;0\;0\;0)$$

με περίοδο $N = 12$. Από την προηγούμενη ανάλυση και τον Ορισμό 4.11, έχουμε

$$\boldsymbol{Y} = \boldsymbol{P}_G \, \boldsymbol{y} = (0\;0\;0\;1\;\alpha^2\;1\;0\;0\;\alpha\;1\;0\;0)$$

όπου $\alpha \in \mathbb{F}_{2^2}$ με $\alpha^2 = \alpha + 1$. Η ακολουθία y χρησιμοποιείται ως παράδειγμα στο [99], για την οποία ο πίνακας που αντιστοιχεί στον εκεί ορισμένο GDFT είναι ο 4×3 πίνακας $\boldsymbol{Y}'$ που

δίνεται παρακάτω (βλέπε ενότητα 2.3.1 για μία περιγραφή του GDFT του [99]). Συγκρίνοντας τους πίνακες $\hat{\boldsymbol{Y}}$ and $\boldsymbol{Y}'$

$$\hat{\boldsymbol{Y}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & \alpha^2 & \alpha \end{pmatrix}, \qquad \boldsymbol{Y}' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \alpha^2 & \alpha \\ 0 & 0 & 0 \end{pmatrix}$$

συμπεραίνουμε ότι πρόκειται για δύο διαφορετικούς μετασχηματισμούς. Εν τούτοις, και οι δύο περιπτώσεις επιτρέπουν τον προσδιορισμό της γραμμικής πολυπλοκότητας της y μέσω του βάρους Günther - η οποία ισούται με 8.

Ο GDFT πίνακας $\boldsymbol{P}'_G$, που χρησιμοποιείται στο [99] για τον προσδιορισμό του Γενικευμένου Μετασχηματισμού Fourier, δεν ικανοποιεί τη σχέση $\boldsymbol{P}'_G \boldsymbol{A} (\boldsymbol{P}'_G)^{-1} = \boldsymbol{J}$ - συνεπώς, ο GDFT που προτείνεται εδώ είναι διαφορετικός από τον GDFT των Massey-Serconek στο [99].

4.4 Νέα κατασκευή μη γραμμικών φίλτρων

Στη ενότητα αυτή μελετώνται συστήματα μη γραμμικών φίλτρων για την παραγωγή ακολουθιών υψηλής γραμμικής πολυπλοκότητας, κάνοντας χρήση των μαθηματικών εργαλείων που εφαρμόστηκαν νωρίτερα. Έστω LFSR μήκους n του οποίου το χαρακτηριστικό πολυώνυμο f είναι πρωταρχικό και έστω $\alpha \in \mathbb{F}_{2^n}$ ρίζα του f. Ας θεωρήσουμε επίσης ότι ένα μη γραμμικό φίλτρο g βαθμού $k \leq n$ εφαρμόζεται στις βαθμίδες του (σχήμα 2.5), με Αλγεβρική Κανονική Μορφή (βλέπε (2.17))

$$g(x_1, \ldots x_n) = \sum_{t \in \mathbb{F}_2^n, \mathrm{wt}(t) \leq k} a_t \, x_1^{t_1} \cdots x_n^{t_n}, \qquad a_t \in \mathbb{F}_2 \tag{4.18}$$

Τότε, η ακολουθία εξόδου $y = \{y_i\}_{i \geq 0}$ το συστήματος παράγεται από το καταστατικό σύστημα $\mathfrak{N} = \langle \boldsymbol{A}, g, x_0 \rangle$ το οποίο περιγράφεται από τις εξισώσεις

$$x_{i+1} = \boldsymbol{A} x_i \tag{4.19a}$$

$$y_i = g(x_i) \tag{4.19b}$$

όπου $\boldsymbol{A}$ είναι ο πίνακας της μορφής (4.2) διάστασης n με χαρακτηριστικό πολυώνυμο f και $x_0 = (x_{0,1} \; x_{0,2} \; \cdots \; x_{0,n})^T$ η αρχική κατάσταση του LFSR. Η μελέτη αυτών των μη γραμμικών συστημάτων μπορεί να απλοποιηθεί αν *γραμμικοποιηθούν*, δηλαδή αν μετατραπούν σε ισοδύναμο γραμμικό σύστημα (μεγαλώνοντας τον χώρο καταστάσεων). Η γραμμικοποίηση

μπορεί να πραγματοποιηθεί αν κάθε όρος στην Αλγεβρική Κανονική Μορφή της μη γραμμικής συνάρτησης g θεωρηθεί ως μία ξεχωριστή μεταβλητή. Αυτή η διαδικασία γραμμικοποίησης περιγράφεται στη συνέχεια. Αξίζει να σημειωθεί ότι η γραμμικοποίηση μη γραμμικών συστημάτων έχει ήδη χρησιμοποιηθεί στη βιβλιογραφία ως μαθηματικό εργαλείο αντιμετώπισης ζητημάτων πολυπλοκότητας ακολουθιών [21], ωστόσο η διαδικασία που περιγράφεται εδώ (και βασίζεται σε ιδιότητες γινομένων Kronecker) είναι διαφορετική.

Ας θεωρήσουμε τους πίνακες $\boldsymbol{A} = [a_{i,j}]$ και $\boldsymbol{B} = [b_{i,j}]$ διαστάσεων $n \times m$ και $n' \times m'$ αντίστοιχα. Τότε το *γινόμενο Kronecker (Kronecker product)* των $\boldsymbol{A}$ και $\boldsymbol{B}$, το οποίο συμβολίζεται ως $\boldsymbol{A} \otimes \boldsymbol{B}$, ορίζεται ως ο $nn' \times mm'$ πίνακας $\boldsymbol{C} = [c_{i,j}]$ [67]

$$\boldsymbol{C} = \boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{1,1}\boldsymbol{B} & \cdots & a_{1,m}\boldsymbol{B} \\ \vdots & & \vdots \\ a_{n,1}\boldsymbol{B} & \cdots & a_{n,m}\boldsymbol{B} \end{pmatrix}.$$

Επίσης συμβολίζουμε ως $\boldsymbol{A}^{(i)}$ το γινόμενο Kronecker τάξης i του $\boldsymbol{A}$ με τον εαυτό του, δηλαδή $\boldsymbol{A}^{(1)} = \boldsymbol{A}$ και $\boldsymbol{A}^{(i)} = \boldsymbol{A} \otimes \boldsymbol{A}^{(i-1)}$ για $i > 1$. Έστω $z = (z_1\ z_2\ \cdots\ z_n)^T$ και ας θεωρήσουμε το γινόμενο Kronecker $z^{(r)}$, $r \leq k$. Τότε, είναι εύκολο να δούμε ότι το διατεταγμένο γινόμενο $z_{t_1} z_{t_2} \cdots z_{t_r}$, εμφανίζεται στη θέση

$$t = 1 + \textstyle\sum_{j=1}^{r} (t_j - 1) n^{r-j}, \qquad 1 \leq t \leq n^r \tag{4.20}$$

του $z^{(r)}$. Σε κάθε όρο $z_{t_1} z_{t_2} \cdots z_{t_r}$ αντιστοιχούμε το $n^r \times 1$ διάνυσμα $e_t = (0 \cdots 1 \cdots 0)^T$, του οποίου το μοναδικό μη μηδενικό στοιχείο βρίσκεται στη θέση t. Τότε, από την (4.20) προκύπτει ότι $e_t = e_{t_1} \otimes e_{t_2} \otimes \cdots \otimes e_{t_r}$, $1 \leq t_i \leq n$, όπου κάθε διάνυσμα $e_{t_i} = (0 \cdots 1 \cdots 0)^T$ έχει μήκος n και το μη μηδενικό του στοιχείο βρίσκεται στη θέση t_i, $1 \leq i \leq r$. Κατά συνέπεια, η Αλγεβρική Κανονική Μορφή του φίλτρου g στο σύστημα $\mathfrak{N}$ γράφεται στη μορφή $g(z) = \sum_{r=1}^{k} g_r^T z^{(r)}$ ή ισοδύναμα

$$g(z) = \begin{pmatrix} g_1^T & g_2^T & \cdots & g_k^T \end{pmatrix} \cdot \begin{pmatrix} (z^T)^{(1)} & (z^T)^{(2)} & \cdots & (z^T)^{(k)} \end{pmatrix}^T = \mathcal{G}^T \mathcal{Z} \tag{4.21}$$

όπου το διάνυσμα g_r, $1 \leq r \leq k$, αντιστοιχεί στους όρους βαθμού r που υπάρχουν στην (4.18) και δίνεται από τη σχέση

$$g_r = \sum_{t \in \mathbb{F}_2^n,\, \mathrm{wt}(t) = r} a_t\, e_{t_1} \otimes e_{t_2} \otimes \cdots \otimes e_{t_r}\ . \tag{4.22}$$

Το διάνυσμα-στήλη $\mathcal{Z}$ μήκους $\sum_{r=1}^{k} n^r$ περιέχει όλα τα γινόμενα των μεταβλητών $z_1, z_2, \ldots, z_n$ με βαθμό μικρότερο ή ίσο του k. Για να ορίσουμε πλήρως το γραμμικό σύστημα που είναι

ισοδύναμο του (4.19), πρέπει να προσδιορίσουμε επίσης τον πίνακα μετάβασης κατάστασης του νέου συστήματος. Είναι εύκολο να δειχθεί ότι ο πίνακας αυτός περιγράφεται από τη σχέση $\boldsymbol{\mathcal{A}} = \mathrm{diag}(\boldsymbol{A}^{(1)}, \boldsymbol{A}^{(2)}, \ldots, \boldsymbol{A}^{(k)})$ και, συνεπώς, το γραμμικοποιημένο σύστημα τελικά είναι

$$\mathcal{X}_{i+1} = \boldsymbol{\mathcal{A}}\mathcal{X}_i, \tag{4.23a}$$

$$y_i = \mathcal{G}^T \mathcal{X}_i. \tag{4.23b}$$

όπου $\mathcal{X}_0 = \left((x_0^T)^{(1)}\ (x_0^T)^{(2)}\ \cdots\ (x_0^T)^{(k)}\right)^T$. πράγματι, λόγω ιδιοτήτων που χαρακτηρίζουν τα γινόμενα Kronecker, ισχύει

$$\boldsymbol{A}^{(2)} z_i^{(2)} = (\boldsymbol{A} \otimes \boldsymbol{A})(z_i \otimes z_i) = (\boldsymbol{A}z_i) \otimes (\boldsymbol{A}z_i) = z_{i+1} \otimes z_{i+1} = z_{i+1}^{(2)}$$

και, γενικότερα, $\boldsymbol{A}^{(j)} z_i^{(j)} = z_{i+1}^{(j)}$ για κάθε $n \times 1$ διάνυσμα z_i, $1 \leq j \leq k$. Αφού το χαρακτηριστικό πολυώνυμο f του LFSR είναι πρωταρχικό, ο $\boldsymbol{A}$ στην (4.19a) είναι διαγωνοποιήσιμος (οι ιδιοτιμές του είναι όλες διαφορετικές μεταξύ τους). Έστω $\boldsymbol{D} = \mathrm{diag}(\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}})$ ο διαγώνιος πίνακας που είναι όμοιος με τον $\boldsymbol{A}$, δηλαδή $\boldsymbol{D} = \boldsymbol{P}\boldsymbol{A}\boldsymbol{P}^{-1}$, όπου τα διαγώνια στοιχεία του είναι οι ρίζες του f (α είναι πρωταρχικό στοιχείο του σώματος $\mathbb{F}_{2^n}$). Τότε, ο πίνακας $\boldsymbol{P}^{-1}$ έχει την ακόλουθη γενική δομή

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \alpha^{\tau} & \alpha^{2\tau} & \cdots & \alpha^{2^{n-1}\tau} \\ \alpha^{\tau+1} & \alpha^{2(\tau+1)} & \cdots & \alpha^{2^{n-1}(\tau+1)} \\ \vdots & \vdots & & \vdots \\ \alpha^{\tau+n-1} & \alpha^{2(\tau+n-1)} & \cdots & \alpha^{2^{n-1}(\tau+n-1)} \end{pmatrix} \tag{4.24}$$

όπου η παράμετρος τ μπορεί να επιλεγεί αυθαίρετα (κάθε στήλη του $\boldsymbol{P}^{-1}$ είναι ιδιοδιάνυσμα του $\boldsymbol{A}$ - η πρώτη αντιστοιχεί στην ιδιοτιμή α, η δεύτερη στην ιδιοτιμή α^2 κ.ο.κ.). Από την (4.19), αν εφαρμόσουμε το μετασχηματισμό $\tilde{x}_i = \boldsymbol{P}x_i$ προκύπτει το ισοδύναμο σύστημα $\mathfrak{S} = \langle \boldsymbol{D}, \tilde{g}, \tilde{x}_0 \rangle$

$$\tilde{x}_{i+1} = \boldsymbol{D}\tilde{x}_i \tag{4.25a}$$

$$y_i = \tilde{g}(\tilde{x}_i) \tag{4.25b}$$

όπου $\tilde{g}(\tilde{x}_i) \triangleq g(\boldsymbol{P}^{-1}\tilde{x}_i)$. Ορίζουμε επίσης τους πίνακες $\boldsymbol{\mathcal{D}}$ και $\boldsymbol{\mathcal{P}}$ κατά αντίστοιχο τρόπο με τον $\boldsymbol{\mathcal{A}}$. Χρησιμοποιώντας γνωστές ιδιότητες των γινομένων Kronecker μπορεί εύκολα να αποδειχτεί ότι $\boldsymbol{\mathcal{D}} = \boldsymbol{\mathcal{P}}\boldsymbol{\mathcal{A}}\boldsymbol{\mathcal{P}}^{-1}$. Κατά συνέπεια, εφαρμόζοντας το μετασχηματισμό $\tilde{\mathcal{X}}_i = \boldsymbol{\mathcal{P}}\mathcal{X}_i$ βρίσκουμε

$$\tilde{\mathcal{X}}_{i+1} = \boldsymbol{\mathcal{D}}\tilde{\mathcal{X}}_i \tag{4.26a}$$

$$y_i = \tilde{\mathcal{G}}^T \tilde{\mathcal{X}}_i \tag{4.26b}$$

όπου $\tilde{\mathcal{G}}^T = \mathcal{G}^T \boldsymbol{\mathcal{P}}^{-1}$. Άρα, κατασκευάσαμε ένα *διαγώνιο* γραμμικό σύστημα που είναι ισοδύναμο του (4.19). Από την (4.22) και λόγω του ότι $\tilde{\mathcal{G}}^T = \begin{pmatrix} \tilde{g}_1^T & \tilde{g}_2^T & \cdots & \tilde{g}_k^T \end{pmatrix}$, προκύπτει ότι για κάθε $1 \leq r \leq k$ έχουμε

$$\tilde{g}_r^T = g_r^T (\boldsymbol{P}^{-1})^{(r)} = \sum_{t \in \mathbb{F}_2^n,\, \mathrm{wt}(t)=r} a_t \, (e_{t_1}^T \boldsymbol{P}^{-1}) \otimes \cdots \otimes (e_{t_r}^T \boldsymbol{P}^{-1}), \qquad a_t \in \mathbb{F}_2$$

όπου το γινόμενο $e_{t_i}^T \boldsymbol{P}^{-1}$ ισούται με την t_i-ιοστή γραμμή του πίνακα $\boldsymbol{P}^{-1}$. Άρα, με τη διαδικασία γραμμικοποίησης του (4.19) που περιγράφηκε νωρίτερα, κάθε όρος γινομένου που εμφανίζεται στην Αλγεβρική Κανονική Μορφή της g αντιστοιχίζεται τελικά σε κάποιο, μονοσήμαντα ορισμένο, γινόμενο Kronecker γραμμών του $\boldsymbol{P}^{-1}$.

Παρατήρηση 4.13. Η επιλογή του ακεραίου τ στην (4.24) καθορίζει ουσιαστικά την αρχική ολίσθηση της ακολουθίας $x = \{x_i\}_{i \geq 0}$, πάνω στην οποία εφαρμόζεται η συνάρτηση φίλτρου g. Γενικά, ισχύει $g(x_{i-\tau}, \ldots, x_{i-\tau+1-n}) = y_{i-\tau+1}$, συνεπώς η φυσική επιλογή για το τ είναι $\tau = 1$. Εν τούτοις, για οποιαδήποτε άλλη τιμή του τ το αποτέλεσμα είναι μία ακολουθία που αποτελεί κυκλική ολίσθηση της y.

Το διαγώνιο γραμμικό σύστημα $\mathfrak{L} = \langle \boldsymbol{\mathcal{D}}, \tilde{\mathcal{G}}, \tilde{\mathcal{X}}_0 \rangle$ που περιγράφεται στην (4.26) δεν είναι ελάχιστο. Η μετατροπή του στο ισοδύναμο ελάχιστο σύστημα $\mathfrak{M} = \langle \boldsymbol{\mathcal{D}}^*, \tilde{\mathcal{G}}^*, \tilde{\mathcal{X}}_0^* \rangle$ μπορεί να πραγματοποιηθεί μέσω της διαδικασίας που περιγράφεται στη Σημείωση 4.3. Με βάση το [124] και την προηγούμενη ανάλυση, θα χρησιμοποιούμε τη φράση *"το φίλτρο g εκμηδενίζει (degenerates) τα στοιχεία $\{\alpha^i : i \in I_j\}$ για κάποιο $j > 0$"*, αν αυτά δεν εμφανίζονται στη διαγώνιο του $\boldsymbol{\mathcal{D}}^*$ ή, ισοδύναμα, αν δεν είναι ρίζες του ελάχιστου πολυωνύμου της ακολουθίας εξόδου y. Προφανώς, με βάση την ορολογία αυτή μπορούμε να πούμε ότι η γραμμική πολυπλοκότητα της y δίνεται από το πλήθος των στοιχείων που δεν εκμηδενίζονται από το φίλτρο g, αν εφαρμοστεί πάνω στο σύστημα $\mathfrak{L}$ η διαδικασία που περιγράφεται στη Σημείωση 4.3. Αφού $\deg(g) = k$ και ο πίνακας $\boldsymbol{\mathcal{D}}$ έχει στη διαγώνιό του στοιχεία της μορφής $\alpha^i \in \mathbb{F}_{2^n}$ με $\mathrm{wt}(i) \leq k$, γίνεται προφανές ότι κανένα στοιχείο α^i με $\mathrm{wt}(i) > k$ δεν συνεισφέρει στην γραμμική πολυπλοκότητα της y (όπου ανακαλούμε από το Κεφάλαιο 2 το συμβολισμό $\mathrm{wt}(i)$ για το βάρος Hamming της δυαδικής αναπαράστασης του ακεραίου i): αυτή η ανάλυση λοιπόν αποτελεί έναν άλλον τρόπο απόδειξης του γνωστού άνω φράγματος της γραμμικής πολυπλοκότητας $\sum_{i=1}^{k} \binom{n}{i}$, όταν σε πρωταρχικό LFSR μήκους n εφαρμόζεται μη γραμμικό φίλτρο βαθμού $k < n$ [73].

Πρόταση 4.14. *Με τον παραπάνω συμβολισμό, έστω η ακολουθία $y = \{y_i\}_{i\geq 0}$ η οποία παράγεται από το σύστημα $\mathfrak{N}$ της (4.19). Τότε, η συνάρτηση φίλτρου g δεν εκμηδενίζει το στοιχείο $\alpha^s \in \mathbb{F}_{2^n}$ αν και μόνο αν*

$$T_s^g = \sum_{j\in P_s} \tilde{\mathcal{G}}_j \neq 0 \tag{4.27}$$

όπου $P_s = \left\{j : \boldsymbol{\mathcal{D}}_{j,j} = \alpha^s \text{ και } 1 \leq j \leq \sum_{r=1}^{k} n^r\right\}$.

Απόδειξη. Από την (4.26) προκύπτει ότι $y_i = \sum_j \tilde{\mathcal{G}}_j \boldsymbol{\mathcal{D}}^i_{j,j} \tilde{\mathcal{X}}_{0,j}$. Αφού το πολυώνυμο f είναι πρωταρχικό, η γραμμική πολυπλοκότητα της y δεν εξαρτάται από την αρχική κατάσταση του $\mathfrak{N}$ στην (4.19) (δεδομένου ότι όλα τα στοιχεία της είναι μη μηδενικά) ή, ισοδύναμα, από την αρχική κατάσταση $\tilde{x}_0$ του $\mathfrak{S}$ στην (4.25) (η αρχική κατάσταση $\tilde{x}_0$ αποτελείται από τα μη μηδενικά στοιχεία του DFT της ακολουθίας εξόδου x του LFSR - βλέπε Λήμμα 4.5). Χωρίς βλάβη της γενικότητας θεωρούμε $\tilde{x}_0 = \mathbf{1}$, οπότε ισχύει και $\tilde{\mathcal{X}}_0 = \mathbf{1}$. Από τη διαδικασία της Σημείωσης 4.3 προκύπτει ότι το στοιχείο α^s θα υπάρχει στη διαγώνιο του πίνακα μετάβασης κατάστασης του συστήματος $\mathfrak{M}$ αν και μόνο αν η (4.27) ισχύει. Το ίδιο ισχύει για όλα τα στοιχεία του συνόλου $\{\alpha^i : i \in I_s\}$. □

Στη συνέχεια αποδεικνύουμε ότι η συνθήκη που περιγράφεται στην Πρόταση 4.14 είναι ισοδύναμη με το κριτήριο ύπαρξης ριζών του Rueppel [124]. Έστω $\tau = 1$ στην (4.24) και ας θεωρήσουμε ότι στο σύστημα $\mathfrak{N}$, που παράγει την ακολουθία εξόδου $y = \{y_i\}_{i\geq 0}$, το μη γραμμικό φίλτρο g περιέχει στην Αλγεβρική Κανονική Μορφή του μόνο έναν όρο βαθμού k:

$$g(z) = z_{t_1} z_{t_2} \dots z_{t_k}, \qquad 1 \leq t_1 < t_2 < \cdots < t_k \leq n\,.$$

Τότε, το διάνυσμα εξόδου του γραμμικού συστήματος $\mathfrak{L} = \langle \boldsymbol{\mathcal{D}}, \tilde{\mathcal{G}}, \tilde{\mathcal{X}}_0 \rangle$ έχει τη μορφή

$$\begin{aligned} \tilde{\mathcal{G}}^T &= \left(\mathbf{0}_n^T \ \cdots \ \mathbf{0}_{n^{k-1}}^T \ (e_{t_1}^T \boldsymbol{P}^{-1}) \otimes \cdots \otimes (e_{t_k}^T \boldsymbol{P}^{-1})\right) \\ &= \left(\mathbf{0}_n^T \ \cdots \ \mathbf{0}_{n^{k-1}}^T \ (\alpha^{t_1} \cdots \alpha^{2^{n-1}t_1}) \otimes \cdots \otimes (\alpha^{t_k} \cdots \alpha^{2^{n-1}t_k})\right) \end{aligned} \tag{4.28}$$

όπου με $\mathbf{0}_{n^i}$ συμβολίζουμε το διάνυσμα που περιέχει μόνο μηδενικά, διαστάσεων $n^i \times 1$. Έστω $\alpha^s \in \mathbb{F}_{2^n}$ με $\mathrm{wt}(s) = k$, και έστω $s = 2^{s_1} + \cdots + 2^{s_k}$ όπου $0 \leq s_1 < \cdots < s_k \leq n-1$. Προκειμένου να ελέγξουμε αν το φίλτρο g εκμηδενίζει το α^s, πρέπει πρώτα να προσδιορίσουμε το σύνολο P_s που ορίζεται στην Πρόταση 4.14. Αφού $\mathrm{wt}(s) = k$, συμπεραίνουμε αμέσως ότι μόνο το μπλοκ $\boldsymbol{D}^{(k)} = \mathrm{diag}(\alpha, \alpha^2, \dots, \alpha^{2^{n-1}})^{(k)}$ του $\boldsymbol{\mathcal{D}}$ περιέχει το στοιχείο α^s στη διαγώνιό του. Άρα, η (4.27) γίνεται

$$T_s^g = \sum_{j\in P_s} \tilde{g}_{k,j} \neq 0 \tag{4.29}$$

όπου $P_s = \left\{ j : \boldsymbol{D}_{j,j}^{(k)} = \alpha^s \text{ και } 1 \leq j \leq n^k \right\}$. Έστω Π_s το σύνολο όλων των αντιμεταθέσεων της διατεταγμένης k-άδας $(s_1, s_2, \ldots, s_k)$. Τότε, οι θέσεις στις οποίες εμφανίζεται το α^s στον πίνακα $\boldsymbol{D}^{(k)}$ είναι

$$P_s = \left\{ j : j = 1 + \textstyle\sum_{r=1}^{k} \sigma_r n^{k-r} \text{ και } \sigma = (\sigma_1, \ldots, \sigma_k) \in \Pi_s \right\}. \tag{4.30}$$

Από τις (4.28), (4.29), (4.30), προκύπτει ότι ο όρος του $\tilde{g}_k$ στη θέση $1 + \sum_{r=1}^{k} \sigma_r n^{k-r}$ ισούται με $\alpha^{2^{\sigma_1} t_1} \alpha^{2^{\sigma_2} t_2} \cdots \alpha^{2^{\sigma_k} t_k}$, και από την (4.29) οδηγούμαστε στην

$$T_s^g = \sum_{\sigma \in \Pi_s} \alpha^{2^{\sigma_1} t_1} \alpha^{2^{\sigma_2} t_2} \cdots \alpha^{2^{\sigma_k} t_k} \neq 0 \,. \tag{4.31}$$

Προφανώς, η συνθήκη (4.31) είναι το κριτήριο ύπαρξης ριζών του Rueppel που περιγράφεται στην (2.24), για τα στοιχεία $\alpha^s \in \mathbb{F}_{2^n}$ με $\mathrm{wt}(s) = k$· με άλλα λόγια, η προηγούμενη ανάλυση μέσω των γινομένων Kronecker παρέχει μία εναλλακτική απόδειξη για το πολύ γνωστό αυτό αποτέλεσμα του Rueppel.

Όπως ήδη αναφέρθηκε στο Κεφάλαιο 2, ο Rueppel στο [124] αποδεικνύει ότι αν το μη γραμμικό φίλτρο g έχει μόνο ένα μεγιστοβάθμιο όρο βαθμού k ο οποίος είναι ισαπέχων (equidistant), δηλαδή

$$g(z_1, z_2, \ldots, z_n) = z_{t_1} z_{t_1+\delta} \cdots z_{t_1+(k-1)\delta}, \qquad \gcd(\delta, 2^n - 1) = 1$$

τότε η γραμμική πολυπλοκότητα της ακολουθίας που παράγεται είναι μεγαλύτερη ή ίση από την ποσότητα $\binom{n}{k}$, αφού η συνάρτηση g δεν εκμηδενίζει κανένα στοιχείο $\alpha^s \in \mathbb{F}_{2^n}$ τέτοιο ώστε $\mathrm{wt}(s) = k$. Στη συνέχεια, θα παρουσιάσουμε μία καινούρια οικογένεια μη γραμμικών φίλτρων, η οποία γενικεύει την οικογένεια των ισαπεχόντων φίλτρων και εξασφαλίζει το ίδιο κάτω φράγμα για τη γραμμική πολυπλοκότητα. Αρχικά, εισάγουμε τον ακόλουθο ορισμό.

Ορισμός 4.15. Ας θεωρήσουμε τους ακέραιους αριθμούς n και $s < 2^n - 1$, με $\mathrm{wt}(s) = k + 1$ για κάποιον θετικό ακέραιο $k < n$. Τότε, το σύνολο

$$\Lambda_n(s) = \left\{ r : r \equiv s - 2^m \pmod{2^n - 1} \text{ και } \mathrm{wt}(r) = k,\ 0 \leq m < n \right\} \tag{4.32}$$

καλείται *σύνολο μικρότερου βάρους (lower-weight set)* του s.

Παράδειγμα 4.16. Για $n = 4$ και $s = 7$, οπότε έχουμε $k = 2$, ισχύει

$$\Lambda_4(7) = \{6, 5, 3\} \,.$$

Τα στοιχεία του $\Lambda_4(7)$ υπολογίζονται από την (4.32) για $m = 0, 1, 2$ αντίστοιχα. Αξίζει να σημειωθεί ότι για $m = 3$, ο αντίστοιχος αριθμός που προκύπτει από την (4.32) είναι ο $r' = 14$, όπου όμως $\mathrm{wt}(r') = 3 > 2$, άρα $14 \notin \Lambda_4(7)$.

Λήμμα 4.17. *Έστω $\mathfrak{N} = \langle \boldsymbol{A}, g, x_0 \rangle$ ένα σύστημα διάστασης $n > 0$, όπου το χαρακτηριστικό πολυώνυμο f του πίνακα μετάβασης καταστάσεων $\boldsymbol{A}$ είναι πρωταρχικό. Επίσης, για κάποιο θετικό ακέραιο δ με $\gcd(\delta, 2^n - 1) = 1$, το μη γραμμικό φίλτρο g βαθμού $k < n$ αποτελείται από έναν μόνο όρο ο οποίος είναι ισαπέχων - δηλαδή*

$$g(z_1, z_2, \ldots, z_n) = z_{t_1} z_{t_1+\delta} \cdots z_{t_1+(k-1)\delta} \ ,$$

όπου $t_1 > \delta$ ή $t_1 \leq n - k\delta$. Τότε, για όλα τα $\alpha^s \in \mathbb{F}_{2^n}$ που ικανοποιούν τη σχέση $\mathrm{wt}(s) = k+1$ ισχύει

$$\sum_{r \in \Lambda_n(s)} T_r^g \neq 0 \tag{4.33}$$

όπου $\alpha \in \mathbb{F}_{2^n}$ είναι ρίζα του f και το T_r^g δίνεται από την (4.31).

Απόδειξη. Ας υποθέσουμε ότι υπάρχει $\alpha^l \in \mathbb{F}_{2^n}$ με $\mathrm{wt}(l) = k + 1$ τέτοιο ώστε το άθροισμα που υποδηλώνεται στην (4.33) να ισούται με 0. Κατασκευάζουμε ένα άλλο ισαπέχον μη γραμμικό φίλτρο g' από το g, με βαθμό $k + 1$, του οποίου ο μεγιστοβάθμιος όρος είναι

$$g'(z_1, z_2, \ldots, z_n) = z_{t_0} \cdot g(z_1, z_2, \ldots, z_n)$$

όπου $t_0 = t_1 - \delta$ αν $t_1 > \delta$, διαφορετικά $t_0 = t_1 + k\delta$. Συμβολίζουμε με $\tilde{\boldsymbol{\mathcal{D}}}$, $\hat{\boldsymbol{\mathcal{D}}}$ ($\tilde{\mathcal{G}}$, $\hat{\mathcal{G}}$) τους πίνακες μετάβασης καταστάσεων (διανύσματα εξόδου) των ισοδύναμων διαγώνιων γραμμικών συστημάτων που αντιστοιχούν στους γεννήτορες με φίλτρα g, g'. Με βάση την προηγούμενη ανάλυση, μόνο τα τελευταία μπλοκ $\tilde{g}_k$, $\hat{g}_{k+1}$ των $\tilde{\mathcal{G}}$, $\hat{\mathcal{G}}$, με μήκη n^k, n^{k+1} αντίστοιχα, είναι μη μηδενικά. Λόγω της δομής του φίλτρου g', ισχύει

$$\begin{aligned} \hat{g}_{k+1}^T &= (e_{t_0}^T \boldsymbol{P}^{-1}) \otimes (e_{t_1}^T \boldsymbol{P}^{-1}) \otimes \cdots \otimes (e_{t_1+(k-1)\delta}^T \boldsymbol{P}^{-1}) \\ &= (e_{t_0}^T \boldsymbol{P}^{-1}) \otimes \tilde{g}_k^T \ . \end{aligned}$$

Χωρίς βλάβη της γενικότητας, θέτουμε $\tau = 2^n - t_0$ στην (4.24), έτσι ώστε η t_0-ιοστή γραμμή του πίνακα $\boldsymbol{P}^{-1}$ να μετατρέπεται στο διάνυσμα $\mathbf{1}_n^T$ που περιέχει μόνο άσους. Άρα,

$$\hat{g}_{k+1}^T = \mathbf{1}_n^T \otimes \tilde{g}_k^T = \left(\tilde{g}_k^T \ \tilde{g}_k^T \ \cdots \ \tilde{g}_k^T \right) .$$

Για κάθε s τέτοιο ώστε $\mathrm{wt}(s) = k + 1$, μόνο το μπλοκ $\boldsymbol{D}^{(k+1)}$ του $\hat{\boldsymbol{\mathcal{D}}}$ περιέχει το στοιχείο α^s στη διαγώνιό του. Έχουμε ότι

$$\boldsymbol{D}^{(k+1)} = \boldsymbol{D} \otimes \boldsymbol{D}^{(k)} = \left(\alpha \boldsymbol{D}^{(k)} \ \alpha^2 \boldsymbol{D}^{(k)} \ \cdots \ \alpha^{2^{n-1}} \boldsymbol{D}^{(k)} \right)$$

οπότε το μπλοκ $\alpha^{2^m}\boldsymbol{D}^{(k)}$, $0 \leq m < n$, έχει το α^s στη διαγώνιό του αν και μόνο αν το α^{s-2^m} υπάρχει στο $\boldsymbol{D}^{(k)}$, δηλαδή αν και μόνο αν $s - 2^m \in \Lambda_n(s)$, αφού οι όροι στο $\boldsymbol{D}^{(k)}$ είναι εκείνα τα στοιχεία α^r με $\mathrm{wt}(r) \leq k$. Από την προηγούμενη ανάλυση και την Πρόταση 4.14 προκύπτει

$$T_s^{g'} = \sum_{j \in P_s} \hat{g}_{k+1,j} = \sum_{\substack{0 \leq m < n \\ s-2^m \in \Lambda_n(s)}} \sum_{j \in P_{s-2^m}} \tilde{g}_{k,j} = \sum_{\substack{0 \leq m < n \\ s-2^m \in \Lambda_n(s)}} T_{s-2^m}^{g} = \sum_{r \in \Lambda_n(s)} T_r^g$$

Άρα, έχουμε από την υπόθεση $T_l^{g'} = 0$ - άτοπο, αφού το g' είναι ισαπέχον φίλτρο και, ως εκ τούτου, δεν εκμηδενίζει το α^l [124]. □

Θεώρημα 4.18. *Με το συμβολισμό του Λήμματος 4.17, θεωρούμε το μη γραμμικό φίλτρο g το οποίο έχει έναν μόνο όρο βαθμού $k < n$*

$$g(z_1, z_2, \ldots, z_n) = z_{t_1} z_{t_2} \cdots z_{t_k}$$

όπου $t_1 > \delta$ ή $t_k \leq n - \delta$. Αν υπάρχει ακέραιος $1 \leq i \leq k$ τέτοιος ώστε το γινόμενο $g_i(z_1, \ldots, z_n) = z_{t_1} \cdots z_{t_{i-1}} z_{t_{i+1}} \cdots z_{t_k}$ να είναι ισαπέχον με απόσταση δ, τότε η γραμμική πολυπλοκότητα της παραγόμενης ακολουθίας είναι μεγαλύτερη ή ίση από $\binom{n}{k}$.

Απόδειξη. Αρκεί να αποδείξουμε ότι το φίλτρο g δεν εκμηδενίζει τα στοιχεία $\alpha^s \in \mathbb{F}_{2^n}$ με $\mathrm{wt}(s) = k$. Από την υπόθεση έχουμε

$$g(z_1, z_2, \ldots, z_n) = z_{t_i} \cdot g_i(z_1, z_2, \ldots, z_n)$$

για κάποιον ακέραιο $1 \leq i \leq k$, όπου το g_i είναι ισαπέχον φίλτρο βαθμού $k - 1$. Τότε, το Λήμμα 4.17 μπορεί να εφαρμοστεί για τη συνάρτηση g_i και

$$\sum_{r \in \Lambda_n(s)} T_r^{g_i} \neq 0 \tag{4.34}$$

για όλα τα $\alpha^s \in \mathbb{F}_{2^n}$ με $\mathrm{wt}(s) = k$. Εφαρμόζοντας τη διαδικασία του Λήμματος 4.17, κατασκευάζουμε τα ισοδύναμα διαγώνια γραμμικά συστήματα των g, g_i και θέτουμε $\tau = 2^n - t_i$ στην (4.24). Τότε, με ανάλογους συλλογισμούς, θα έχουμε

$$T_s^g = \sum_{r \in \Lambda_n(s)} T_r^{g_i}$$

και το επιθυμητό αποτέλεσμα προκύπτει από την (4.34) για όλα τα $\alpha^s \in \mathbb{F}_{2^n}$ με $\mathrm{wt}(s) = k$. □

Σημείωση 4.19. Τα αποτελέσματα του Λήμματος 4.17 και του Θεωρήματος 4.18 ισχύουν ακόμα και αν η συνάρτηση g περιέχει και άλλους όρους, βαθμού μικρότερου από k.

Παράδειγμα 4.20. Ας θεωρήσουμε το σύστημα $\mathfrak{N} = \langle \boldsymbol{A}, g_i, x_0 \rangle$, όπου ο πίνακας $\boldsymbol{A}$ είναι της μορφής (4.2) με χαρακτηριστικό πολυώνυμο το πρωταρχικό $f(z) = 1+z+z^6$ και η συνάρτηση εξόδου είναι κάποιο από τα ακόλουθα μη γραμμικά φίλτρα βαθμού 4

$$g_1(z_1, \ldots, z_6) = z_1 z_2 z_3 z_5 \qquad g_2(z_1, \ldots, z_6) = z_1 z_2 z_3 z_6$$
$$g_3(z_1, \ldots, z_6) = z_1 z_3 z_4 z_5 \qquad g_4(z_1, \ldots, z_6) = z_1 z_4 z_5 z_6$$

και τα ισοδύναμά τους βάσει ολισθήσεων (βλέπε Σημείωση 4.13). Σύμφωνα με το Θεώρημα 4.18, η γραμμική πολυπλοκότητα της ακολουθίας εξόδου του $\mathfrak{N}$ είναι κάτω φραγμένη από την ποσότητα $\binom{6}{4}$. Πράγματι, θεωρούμε το φίλτρο g_3 (η ανάλυση ισχύει για όλα τα υπόλοιπα φίλτρα): αυτό γράφεται ως $g_3(z_1, \ldots, z_6) = z_1 \cdot g(z_1, \ldots, z_6)$, όπου το φίλτρο $g(z_1, \ldots, z_6) = z_3 z_4 z_5$ είναι ισαπέχον με $\delta = 1$. Οι κυκλοτομικές κλάσεις modulo 63 με βάρος 4 είναι οι I_{15}, I_{23}, και I_{27}. Κάνοντας πράξεις στο σώμα $\mathbb{F}_{2^6}$ έχουμε

$$T_{15}^{g_3} = T_{14}^{g} + T_{13}^{g} + T_{11}^{g} + T_{07}^{g} = \alpha^{07} \neq 0\,,$$
$$T_{23}^{g_3} = T_{22}^{g} + T_{21}^{g} + T_{19}^{g} + T_{07}^{g} = \alpha^{48} \neq 0\,,$$
$$T_{27}^{g_3} = T_{26}^{g} + T_{25}^{g} + T_{19}^{g} + T_{11}^{g} = \alpha^{54} \neq 0\,.$$

Αξίζει να σημειωθεί εκ νέου ότι οι παραπάνω τιμές των $T_{15}^{g_3}, T_{23}^{g_3}, T_{27}^{g_3}$ προσδιορίζονται από την (4.27), όπου το ισοδύναμο διαγώνιο γραμμικό σύστημα έχει κατασκευαστεί θέτοντας $\tau = 0$ στην (4.24) - άρα, οι τιμές αυτές δεν είναι οι ίδιες με αυτές που θα προέκυπταν από την (4.31), οι οποίες αντιστοιχούν στο ισοδύναμο γραμμικό σύστημα που προκύπτει για $\tau = 1$. Ωστόσο, ανακαλώντας τη Σημείωση 4.13, η επιλογή του τ δεν παίζει ουσιαστικά ρόλο στη γραμμική πολυπλοκότητα της παραγόμενης ακολουθίας, αφού καθορίζει μόνο την αρχική ολίσθησή της.

Το Θεώρημα 4.18 γενικεύει τα αποτελέσματα του Rueppel, αφού περιγράφει φίλτρα τα οποία είναι ελάχιστα διαφορετικά από τα ισαπέχοντα, αλλά εν τούτοις έχουν την ίδια με αυτά συμπεριφορά ως προς τη γραμμική πολυπλοκότητα της ακολουθίας εξόδου. Από την παραπάνω ανάλυση μπορούμε να δούμε ότι τα αποτελέσματα που αποδείχτηκαν εδώ γενικεύουν ομοίως όχι μόνο τα ισαπέχοντα φίλτρα αλλά και άλλες οικογένειες φίλτρων οι οποίες επιτυγχάνουν κάποιο συγκεκριμένο κάτω φράγμα για τη γραμμική πολυπλοκότητα - κι αυτό γιατί στις αποδείξεις, τόσο του Λήμματος 4.17 όσο και του Θεωρήματος 4.18, χρησιμοποιήθηκε ουσιαστικά η ιδιότητα του μη εκμηδενισμού συγκεκριμένων στοιχείων η οποία εξασφαλίζεται από τα ισαπέχοντα φίλτρα, και όχι αυτή καθ' αυτή η δομή των φίλτρων. Με άλλα λόγια, μπορούμε να διατυπώσουμε το ακόλουθο γενικότερο αποτέλεσμα.

Θεώρημα 4.21. *Με το συμβολισμό του Λήμματος 4.17, έστω η συνάρτηση*

$$g(z_1, \ldots, z_n) = z_{t_1} \cdots z_{t_{k-1}}$$

βαθμού $k-1$, η οποία ανήκει σε κάποια οικογένεια μη γραμμικών φίλτρων που εξασφαλίζει συγκεκριμένο κάτω φράγμα για τη γραμμική πολυπλοκότητα. Αν υπάρχει $1 \leq t_k \leq n$ τέτοιο ώστε το μη γραμμικό φίλτρο $\tilde{g}(z_1, \ldots, z_n) = z_{t_k}\, g(z_1, \ldots, z_n)$, βαθμού k, να ανήκει στην ίδια οικογένεια μη γραμμικών φίλτρων με το g, τότε όλα τα φίλτρα βαθμού k της μορφής

$$g'(z_1, \ldots, z_n) = z_{t'_k}\, g(z_1, \ldots, z_n), \qquad 1 \leq t'_k \leq n$$

εξασφαλίζουν το ίδιο κάτω φράγμα για τη γραμμική πολυπλοκότητα, όσο και το $\tilde{g}$.

Το ακόλουθο παράδειγμα εφαρμόζει το Θεώρημα 4.21 στην οικογένεια των μη γραμμικών φίλτρων των οποίων η μορφή καθορίζεται από τα στοιχεία μιας κανονικής βάσης του σώματος, όπως αυτά τα φίλτρα ορίστηκαν στο [79] (και περιγράφονται επίσης και στα [11] και [86]). Όπως έχει ήδη αναφερθεί και στην ενότητα 2.5.2, ένα τέτοιο φίλτρο βαθμού k που εφαρμόζεται σε πρωταρχικό LFSR μήκους n παράγει ακολουθίες με γραμμική πολυπλοκότητα μεγαλύτερη ή ίση από $\binom{n}{k}$ - δηλαδή, παρουσιάζουν το ίδιο κάτω φράγμα με τα ισαπέχοντα φίλτρα.

Παράδειγμα 4.22. Έστω ο LFSR με χαρακτηριστικό πολυώνυμο το πρωταρχικό $f(z) = 1 + z^2 + z^3 + z^4 + z^8$ και έστω $\alpha \in \mathbb{F}_{2^8}$ μία ρίζα του $f(z)$. Τα στοιχεία του συνόλου $\{\alpha^{127}, \alpha^{254}, \alpha^{253}, \alpha^{251}, \alpha^{247}, \alpha^{239}, \alpha^{223}, \alpha^{191}\}$ αποτελούν μία κανονική βάση στο σώμα $\mathbb{F}_{2^8}$. Με την ορολογία του [79] (βλέπε επίσης την περιγραφή αυτών των φίλτρων στην ενότητα 2.5.2), ορίζουμε $W = \{247, 251, 253\}$. Τότε, το μη γραμμικό φίλτρο που προσδιορίζεται από το σύνολο W είναι το $g(z_1, z_2, \ldots, z_8) = z_2 z_4 z_8$ (όπου η μεταβλητή z_1 αντιστοιχεί στη δεξιότερη βαθμίδα του 2.5 κ.ο.κ.) και παράγει ακολουθίες με γραμμική πολυπλοκότητα τουλάχιστον ίση με $\binom{8}{3}$. Η συνάρτηση g ικανοποιεί τις συνθήκες του Θεωρήματος 4.21 αφού το φίλτρο $\tilde{g}(z_1, z_2, \ldots, z_8) = z_1 z_2 z_4 z_8$ ανήκει στην ίδια οικογένεια φίλτρων (αντιστοιχεί στο σύνολο $\tilde{W} = \{247, 251, 253, 254\}$). Άρα, τα φίλτρα

$$g_1(z_1, \ldots, z_8) = z_2 z_3 z_4 z_8, \qquad g_2(z_1, \ldots, z_8) = z_2 z_4 z_5 z_8,$$
$$g_3(z_1, \ldots, z_8) = z_2 z_4 z_6 z_8, \qquad g_4(z_1, \ldots, z_8) = z_2 z_4 z_7 z_8,$$

παράγουν ακολουθίες με γραμμική πολυπλοκότητα τουλάχιστον ίση με $\binom{8}{4}$. Οι κυκλοτομικές κλάσεις modulo 255 βάρους 4 είναι οι I_{15}, I_{23}, I_{27}, I_{29}, I_{39}, I_{43}, I_{45}, I_{51}, I_{53} and I_{85}. Άρα, για κάθε φίλτρο g_i, $i = 1, 2, 3, 4$, ισχύει

$$T_{15}^{g_i} = T_{14}^{g} + T_{13}^{g} + T_{11}^{g} + T_{07}^{g} \neq 0,$$

$$T_{23}^{g_i} = T_{22}^{g} + T_{21}^{g} + T_{19}^{g} + T_{07}^{g} \neq 0,$$
$$T_{27}^{g_i} = T_{26}^{g} + T_{25}^{g} + T_{19}^{g} + T_{11}^{g} \neq 0,$$
$$T_{29}^{g_i} = T_{28}^{g} + T_{25}^{g} + T_{21}^{g} + T_{13}^{g} \neq 0,$$
$$T_{39}^{g_i} = T_{38}^{g} + T_{37}^{g} + T_{35}^{g} + T_{07}^{g} \neq 0,$$
$$T_{43}^{g_i} = T_{42}^{g} + T_{41}^{g} + T_{35}^{g} + T_{11}^{g} \neq 0,$$
$$T_{45}^{g_i} = T_{44}^{g} + T_{41}^{g} + T_{37}^{g} + T_{13}^{g} \neq 0,$$
$$T_{51}^{g_i} = T_{50}^{g} + T_{49}^{g} + T_{35}^{g} + T_{19}^{g} \neq 0,$$
$$T_{53}^{g_i} = T_{52}^{g} + T_{49}^{g} + T_{37}^{g} + T_{21}^{g} \neq 0,$$
$$T_{85}^{g_i} = T_{84}^{g} + T_{81}^{g} + T_{69}^{g} + T_{21}^{g} \neq 0,$$

εξασφαλίζοντας ότι κάθε ένα από τα φίλτρα παράγει ακολουθίες με γραμμική πολυπλοκότητα μεγαλύτερη ή ίση από $\binom{8}{4}$. (Σημειώνουμε για άλλη μία φορά ότι κάθε $T_m^{g_i}$, $m = 15, \ldots, 85$ υπολογίζεται από την (4.27), όπου το ισοδύναμο διαγώνιο γραμμικό σύστημα έχει κατασκευαστεί θέτοντας κάθε φορά την κατάλληλη τιμή του τ στο (4.24).

Από το Θεώρημα 4.21 γίνεται φανερό ότι τα αποτελέσματα αυτής της ενότητας μπορούν να γενικεύσουν πολλές κατασκευές φίλτρων (αρκεί να ικανοποιούν τις συνθήκες του Θεωρήματος), και άρα μπορούν να έχουν εφαρμογή ακόμη και σε κατασκευές μη γραμμικών φίλτρων που προταθούν στο μέλλον. Κατά συνέπεια, η προτεινόμενη γενίκευση παρέχει περισσότερες δυνατότητες στη σχεδίαση κρυπτογραφικών συστημάτων.

Κεφάλαιο 5

Μη γραμμική πολυπλοκότητα και Lempel-Ziv πολυπλοκότητα

> If there is a problem you can't solve, then there is an easier problem you can't solve: find it.
>
> *George Pólya*

Βασικό αντικείμενο αυτού του κεφαλαίου αποτελεί η μη γραμμική πολυπλοκότητα ακολουθιών, η οποία (όπως έχει ήδη επισημανθεί στο Κεφάλαιο 2) έχει μελετηθεί στη βιβλιογραφία σε πολύ μικρότερο βαθμό από ό,τι η γραμμική. Γενικά, ένας μη γραμμικός FSR μήκους m που παράγει την $y \in \mathbb{F}_q$ μπορεί να περιγραφεί, ως σύστημα καταστατικών εξισώσεων, ως εξής:

$$x_{i+1} = f(x_i) \tag{5.1a}$$

$$y_i = c^T \, x_i \tag{5.1b}$$

όπου $x_0 = (y_0 \; y_1 \; \ldots \; y_{m-1})^T$ και $c = (1 \; 0 \; \ldots \; 0)^T$ είναι διανύσματα μήκους m, ενώ η συνάρτηση $f : \mathbb{F}_q^m \to \mathbb{F}_q^m$, για κάθε $x_i = (x_{i,1} \; x_{i,2} \; \ldots \; x_{i,m})^T$, $i \geq 0$ δίνεται από την

$$f(x_i) = x_{i+1} = (x_{i,2} \; \ldots \; x_{i,m} \; h(x_i))^T$$

όπου h η (μη γραμμική) συνάρτηση ανάδρασης του FSR. Κατά συνέπεια, η μη γραμμική πολυπλοκότητα της y, ως το μήκος του μικρότερου FSR που την παράγει, μπορεί να περιγραφεί ως η ελάχιστη διάσταση ενός καταστατικού συστήματος της μορφής (5.1) που παράγει την y.

Στο κεφάλαιο αυτό θα παρουσιαστούν ιδιότητες που χαρακτηρίζουν το προφίλ της μη γραμμικής πολυπλοκότητας για ακολουθίες με τιμές σε οποιοδήποτε πεπερασμένο σώμα. Από τις ιδιότητες αυτές, αναπτύσσεται ένας νέος αλγόριθμος ο οποίος υπολογίζει αναδρομικά τον μικρότερο FSR που παράγει μία δοθείσα δυαδική ακολουθία. Με άλλα λόγια, ο αλγόριθμος που

προτείνεται εδώ αποτελεί γενίκευση του αλγορίθμου των Berlekamp-Massey στη μη γραμμική περίπτωση και είναι ο *πρώτος αναδρομικός αλγόριθμος* που προτείνεται στη βιβλιογραφία για τον υπολογισμό του ελάχιστου, μη γραμμικού, FSR.

Στο παρόν κεφάλαιο διερευνάται επίσης η σχέση που υπάρχει μεταξύ της μη γραμμικής πολυπλοκότητας και της πολυπλοκότητας Lempel-Ziv - μία σχέση η οποία αναφέρεται στο [110] ως ανοιχτό πρόβλημα. Η πολυπλοκότητα Lempel-Ziv ορίζεται στο [88] και περιγράφεται αναλυτικά στην ενότητα 5.2. Στο ίδιο άρθρο, οι Lempel και Ziv ορίζουν το *προφίλ ιδιοτιμής (eigenvalue profile)* ως εναλλακτικό μέτρο αποτίμησης της πολυπλοκότητας μίας ακολουθίας, το οποίο όμως σχετίζεται με την πολυπλοκότητα Lempel-Ziv. Στο τρέχον κεφάλαιο αποδεικνύεται ότι *αν δύο ακολουθίες έχουν το ίδιο προφίλ ιδιοτιμής, τότε έχουν και το ίδιο προφίλ μη γραμμικής πολυπλοκότητας*. Για τον υπολογισμό της πολυπλοκότητας Lempel-Ziv λαμβάνει χώρα μία συγκεκριμένη κατάτμηση της ακολουθίας, η οποία εν συνεχεία αποτέλεσε τη βάση για τον πολύ γνωστό αλγόριθμο συμπίεσης δεδομένων των Lempel-Ziv που προτάθηκε το 1977 [139]. Η πρώτη αυτή έκδοση του αλγορίθμου συναντάται συχνά στη βιβλιογραφία με τον όρο LZ77· ακολούθησε μία δεύτερη έκδοσή του ένα χρόνο μετά [140], γνωστή ως LZ78. Και οι δύο αλγόριθμοι συμπίεσης είναι ασυμπτωτικά βέλτιστοι, υπό την έννοια ότι ο λόγος συμπίεσης προσεγγίζει την εντροπία της πηγής για κάθε στατική εργοδική πηγή με πεπερασμένο αλφάβητο [140, 136]. Ωστόσο, πρέπει να σημειωθεί ότι για μία πεπερασμένη ακολουθία, ο λόγος συμπίεσής της μπορεί να απέχει πολύ από τη βέλτιστη τιμή. Η ικανότητα συμπίεσης μίας ακολουθίας αποτελεί σημαντικό κρυπτογραφικό της χαρακτηριστικό, αφού μία ακολουθία που μπορεί να συμπιεστεί σε μεγάλο βαθμό δεν μπορεί να θεωρείται ψευδοτυχαία. Ως προς αυτήν την κατεύθυνση, το τρέχον κεφάλαιο μελετάει την εξάρτηση μεταξύ της μη γραμμικής πολυπλοκότητας μίας ακολουθίας και του βαθμού συμπίεσής αυτής· συγκεκριμένα, αποδεικνύεται ένα κάτω φράγμα του βαθμού συμπίεσης για δυαδικές περιοδικές ακολουθίες, το οποίο εξαρτάται από την πολυπλοκότητά τους. Επιπρόσθετα, περιγράφεται μία οικογένεια ακολουθιών που μπορεί να συμπιεστεί σε μεγάλο βαθμό, για οποιαδήποτε επιθυμητή τιμή της πολυπλοκότητάς τους, αναδεικνύοντας την κρυπτογραφική αξία του βαθμού συμπίεσης.

5.1 Ιδιότητες του προφίλ μη γραμμικής πολυπλοκότητας

Σε αυτήν την ενότητα παρουσιάζουμε ιδιότητες οι οποίες χαρακτηρίζουν το προφίλ της (μη γραμμικής) πολυπλοκότητας ακολουθίας $y^N = y_0 y_1 \dots y_{N-1}$ πεπερασμένου μήκους N, με τιμές σε οποιοδήποτε σώμα. Η ακόλουθη Πρόταση έχει αποδειχτεί στο [58] και έχει ήδη αναφερθεί

στο Κεφάλαιο 2.

Πρόταση 5.1 ([58, 59]). *Έστω L το μήκος της μεγαλύτερης υπακολουθίας της y^N η οποία εμφανίζεται δύο φορές στην y^N με διαφορετικό επόμενο στοιχείο (δηλαδή, υπάρχουν $0 \leq i < j \leq N-1-L$ τέτοια ώστε $y_i^{i+L-1} = y_j^{j+L-1}$ και $y_{i+L} \neq y_{j+L}$). Τότε, ισχύει $c(y^N) = L+1$.*

Η βασική ιδέα της απόδειξης είναι η εξής: έστω $c(y^N) = m \leq L$ και ας θεωρήσουμε, για έναν ελάχιστο FSR της y^N μήκους m, το ισοδύναμο σύστημα της μορφής (5.1). Τότε, υπάρχουν διαφορετικά i, j τέτοια ώστε $x_i = x_j$ και $x_{i+1} \neq x_{j+1}$ - άτοπο. Αξίζει να σημειωθεί ότι η Πρόταση 5.1 ισχύει για τη γενικότερη περίπτωση όπου ο σταθερός όρος της συνάρτησης ανάδρασης του FSR μπορεί να είναι μη μηδενικός. Αν περιοριστούμε στην περίπτωση όπου ο όρος αυτός είναι 0, τότε ισχύει $c(y^N) = \max\{L+1, M+1\}$, όπου M είναι το μήκος της μεγαλύτερης υπακολουθίας της y^N που αποτελείται μόνο από μηδενικά (και δεν βρίσκεται στο τέλος της y^N). Προφανώς, $M \leq L+1$, αφού η παρουσία M διαδοχικών 0 ακολουθούμενων από 1 υποδηλώνει ότι $L \geq M-1$. Στο υπόλοιπο τμήμα του κεφαλαίου θα αναφερόμαστε πάντα στη γενική περίπτωση αυθαίρετου σταθερού όρου - δηλαδή, η πολυπλοκότητα θα δίνεται πάντα από την Πρόταση 5.1.

Πρόταση 5.2. *Έστω $c(y^{n-1}) = m$ και έστω ότι ο ελάχιστος FSR της y^{n-1} δεν παράγει την y^n. Τότε, $c(y^n) = m$ αν και μόνο αν η υπακολουθία y_{n-m-1}^{n-2} δεν εμφανίζεται νωρίτερα μέσα στην y^{n-1}.*

Απόδειξη. Έστω $c(y^n) = m$ και ας θεωρήσουμε ότι υπάρχει ακέραιος $0 \leq i < n-m-1$ με την ιδιότητα $y_i^{i+m-1} = y_{n-m-1}^{n-2}$. Αφού ο ελάχιστος FSR της y^{n-1} δεν παράγει το τελευταίο στοιχείο y_{n-1} της y^n, ισχύει $y_{i+m} \neq y_{n-1}$ και από την πρόταση 5.1 προκύπτει ότι $c(y^n) \geq m+1$ - άτοπο. Αντίστροφα, αφού $c(y^{n-1}) = m$ και η τελευταία υπακολουθία μήκους m της y^{n-1} δεν εμφανίζεται νωρίτερα μέσα στην y^{n-1}, προκύπτει ότι $c(y^n) = m$ λόγω της Πρότασης 5.1. □

Πόρισμα 5.3. *Έστω $c(y^{n-1}) = m$ και ας θεωρήσουμε ότι ο ελάχιστος FSR της y^{n-1} δεν παράγει την y^n. Τότε, ισχύει $c(y^n) > m$ αν και μόνο αν υπάρχει ακέραιος $0 \leq i < n-m-1$ τέτοιος ώστε $y_i^{i+m-1} = y_{n-m-1}^{n-2}$ και $y_{i+m} \neq y_{n-1}$.*

Τα παραπάνω καθορίζουν μία ικανή και αναγκαία συνθήκη για να υπάρχει αύξηση στην πολυπλοκότητα μίας ακολουθίας κατά την έλευση του n-ιοστού στοιχείου της. Επιπρόσθετα όμως μπορεί να υπολογιστεί, για κάθε $n \geq 2$, η *ακριβής τιμή* $c(y^n) - c(y^{n-1})$ της αύξησης της πολυπλοκότητας από το ακόλουθο Θεώρημα.

Θεώρημα 5.4. *Με το συμβολισμό της Πρότασης 5.2, έστω* $c(y^{n-1}) = m < c(y^n)$. *Συμβολίζουμε με* $i \leq n-m-1$ *τον μικρότερο ακέραιο τέτοιον ώστε* $y_j^{j+m-1} = y_i^{i+m-1}$ *για κάποιο* $0 \leq j < i$. *Τότε*

$$c(y^n) = c(y^{n-1}) + (n-m-i) = n-i\,.$$

Απόδειξη. Λόγω του Πορίσματος 5.3, υπάρχει πάντα ακέραιος i που ικανοποιεί την παραπάνω ιδιότητα, αφού ο $i = n-m-1$ εμπίπτει πάντα σε αυτήν την περίπτωση. Έστω $k = n-m-i$. Αφού $c(y^{n-1}) = m$, λόγω της Πρότασης 5.1 προκύπτει ότι

$$y_j^{j+m-1+l} = y_i^{i+m-1+l}, \qquad \text{για κάθε } 0 \leq l < k\,.$$

Λόγω του Πορίσματος 5.3, η υπόθεση $c(y^n) > c(y^{n-1})$ οδηγεί στη σχέση $y_{j+m-1+k} \neq y_{i+m-1+k}$ ή, ισοδύναμα, $y_{j+n-i-1} \neq y_{n-1}$. Κατά συνέπεια, οι υπακολουθίες $y_j^{j+m-2+k}$ και $y_i^{i+m-2+k}$ είναι όμοιες και διαφέρουν στο επόμενό τους στοιχείο. Άρα, ανακαλώντας την Πρόταση 5.1, η πολυπλοκότητα της y^n ισούται με το μήκος της $y_i^{i+m-2+k} = y_i^{n-2}$ συν 1, δηλαδή $n-i$. Κατά συνέπεια, η αύξηση στην πολυπλοκότητα $c(y^n) - c(y^{n-1})$ που προκαλεί η έλευση του στοιχείου y_{n-1} είναι $n-m-i$. □

Το Θεώρημα 5.4 μπορεί επίσης άμεσα να εξαχθεί από το [58, pp. 68–69], στο οποίο η αύξηση της πολυπλοκότητας εκφράζεται ως συνάρτηση της περιοδικότητας των καταστάσεων του FSR. Είναι επίσης εύκολο να δειχθεί ότι ο ακέραιος i στο Θεώρημα 5.4 ισούται με $t_0^{(n-1)} + T^{(n-1)}$, όπου $t_0^{(n-1)}, T^{(n-1)}$ είναι η προ-περίοδος και η περίοδος αντίστοιχα της ακολουθίας πεπερασμένου μήκους y^{n-1}· πράγματι, ισχύει $y_{i+l} = y_{j+l}$ για κάθε $0 \leq l < n-1-i$, όπου το j ορίζεται όπως στο Θεώρημα 5.4. Άρα, $t_0^{(n-1)} = j$ και $T^{(n-1)} = i-j$, οπότε η αύξηση $k = c(y^n) - c(y^{n-1})$ στην πολυπλοκότητα δίνεται από την

$$k = n-m-(t_0^{(n-1)} + T^{(n-1)})\,. \tag{5.2}$$

Παράδειγμα 5.5. Έστω η ακολουθία $y^{10} = 0100110011$. Από την Πρόταση 5.1 βρίσκουμε $c(y^{10}) = 3$, ενώ επίσης ισχύει $t_0^{(10)} = 1$ και $T^{(10)} = 4$. Αν επεκτείνουμε την y^{10} με το στοιχείο $y_{10} = 1$ τότε, στη νέα ακολουθία y^{11}, η υπακολουθία 10011 εμφανίζεται δύο φορές με διαφορετικά διαδοχικά bits μετά από κάθε εμφάνισή της - άρα, $c(y^{11}) > c(y^{10})$. Σύμφωνα με την (5.2), η αύξηση στην πολυπλοκότητα ισούται με $11-3-5 = 3$ - κατά συνέπεια, $c(y^{11}) = 6$.

Λήμμα 5.6. *Έστω ακολουθία* y^n *τέτοια ώστε* $c(y^{n-1}) = m$ *και* $c(y^n) = m+k$ *για κάποιον ακέραιο* $k \geq 1$. *Τότε, όλες οι υπακολουθίες μήκους* $m+k$ *της* y^n *είναι ανά δύο διαφορετικές μεταξύ τους.*

Απόδειξη. Αφού ισχύει $c(y^n) > c(y^{n-1}) = m$, από την Πρόταση 5.1 προκύπτει ότι η υπακολουθία y_{n-m-1}^{n-1} μήκους $m+1$ εμφανίζεται μόνο μία φορά μέσα στην y^n. Κατά συνέπεια, η υπακολουθία y_{n-m-k}^{n-1} μήκους $m+k$ εμφανίζεται επίσης μόνο μία φορά μέσα στην y^n. Ας υποθέσουμε ότι υπάρχουν δύο ίδιες υπακολουθίες στην y^n μήκους $m+k$, δηλαδή υπάρχουν $j < i$ τέτοια ώστε $y_j^{j+m+k-1} = y_i^{i+m+k-1}$. Λόγω του ότι $c(y^n) = m+k$, από το Πόρισμα 5.3 προκύπτει

$$y_{j+l}^{j+m+k-1+l} = y_{i+l}^{i+m+k-1+l}, \quad \forall\, 0 \le l \le n-m-k-i\,.$$

Άρα, η υπακολουθία y_{n-m-k}^{n-1} ταυτίζεται με κάποια άλλη υπακολουθία που βρίσκεται μέσα στην y^n - άτοπο. □

Πρόταση 5.7. *Έστω y^n ακολουθία με $c(y^{n-1}) = m$ και $c(y^n) = m+k$ για κάποιο $k \ge 1$. Αν η y^n επεκταθεί με k αυθαίρετα στοιχεία, τότε η πολυπλοκότητα της νέας ακολουθίας y^{n+k} παραμένει $m+k$.*

Απόδειξη. Λόγω του Λήμματος 5.6, όλες οι υπακολουθίες μήκους $m+k$ της y^n είναι ανά δύο διαφορετικές μεταξύ τους· επιπρόσθετα, η υπακολουθία y_{n-m-1}^{n-1} μήκους $m+1$ δεν εμφανίζεται δεύτερη φορά μέσα στην y^n. Ας θεωρήσουμε τις τελευταίες $k-1$ υπακολουθίες μήκους $m+k$ της επεκταμένης ακολουθίας y^{n+k-1}, δηλαδή

$$y_{n-m-k+1}^{n}\,,\quad y_{n-m-k+2}^{n+1}\,,\quad \ldots\,,\quad y_{n-m-1}^{n+k-2}\,.$$

Όλες αυτές οι υπακολουθίες περιέχουν την y_{n-m-1}^{n-1}, συνεπώς είναι ανά δύο διαφορετικές μεταξύ τους. Συνδυάζοντας τα παραπάνω, καταλήγουμε ότι όλες οι υπακολουθίες μήκους $m+k$ της y^{n+k-1} είναι ανά δύο διαφορετικές μεταξύ τους, οπότε $c(y^{n+k-1}) = c(y^n)$ λόγω του Πορίσματος 5.3. Επίσης, $c(y^{n+k}) = c(y^{n+k-1})$ ανεξάρτητα της τιμής του τελευταίου στοιχείου y_{n+k-1}, λόγω της Πρότασης 5.1. □

5.2 Πολυπλοκότητα Lempel-Ziv

Η *Lempel-Ziv πολυπλοκότητα* μίας ακολουθίας ισούται με το πλήθος των υπακολουθιών στις οποίες η ακολουθία διασπάται, με βάση κάποιους συγκεκριμένους κανόνες [88]. Αυτή η διαδικασία κατάτμησης της ακολουθίας αποτελεί τη βάση του πολύ γνωστού αλγόριθμου συμπίεσης των Lempel-Ziv [139]. Στη συνέχεια υπενθυμίζουμε τους βασικούς ορισμούς που αναφέρονται στο [88], έτσι ώστε να αποσαφηνιστεί η σχέση που υπάρχει μεταξύ της πολυπλοκότητας Lempel-Ziv και της μη γραμμικής πολυπλοκότητας.

Μία ακολουθία πεπερασμένου μήκους y^N είναι *αναπαραγώγιμη (reproducible)* από το (γνήσιο) πρόθεμά της $y^j = y_0 y_1 \dots y_{j-1}$, $j < N$, αν υπάρχει ακέραιος $p < j$ τέτοιος ώστε $y_{j+i} = y_{p+i}$ για κάθε $0 \leq i < N - j$· χρησιμοποιούμε το συμβολισμό $y^j \to y^N$. Η y^N είναι *παραγώγιμη (producible)* από το (γνήσιο) πρόθεμά της y^j αν είναι αναπαραγώγιμη από το y^j, με πιθανή εξαίρεση το τελευταίο της στοιχείο· συμβολίζεται ως $y^j \Rightarrow y^N$.

Παράδειγμα 5.8. Για την ακολουθία $y^4 = 0110$ και το πρόθεμά της $y^2 = 01$ ισχύει $01 \Rightarrow 0110$ και $01 \nrightarrow 0110$.

Η *διαδικασία παραγωγιμότητας (production process)* $S(y^N)$, *ή ιστορία (history)*, μίας ακολουθίας y^N ορίζεται κάθε κατάτμηση της μορφής

$$S(y^N) = y_0^{h_0}\, y_{h_0+1}^{h_1} \dots y_{h_{s-1}+1}^{h_s} \tag{5.3}$$

όπου $h_0 = 0$, $h_s = N-1$, $h_{i-1} < h_i$ και $y_0^{h_{i-1}} \Rightarrow y_0^{h_i}$, $1 \leq i \leq s$. Οι θέσεις $h_0, \dots, h_s$ καλούνται *σημεία (points)* της ιστορίας, ενώ κάθε υπακολουθία $y_{h_{i-1}+1}^{h_i}$ ονομάζεται *λέξη (word)* της ιστορίας (όπου ορίζουμε $h_{-1} \triangleq -1$). Μία λέξη $y_{h_{i-1}+1}^{h_i}$ ονομάζεται *εξαντλητική (exhaustive)* αν $y_0^{h_{i-1}} \nrightarrow y_0^{h_i}$. Αν όλες οι λέξεις μίας ιστορίας είναι εξαντλητικές (εξαιρουμένης πιθανώς της τελευταίας λέξης), τότε η ιστορία ονομάζεται *εξαντλητική*. Από τους ορισμούς αυτούς γίνεται προφανές ότι κάθε ακολουθία y^N έχει μία μοναδική εξαντλητική ιστορία $S_e(y^N)$. Στο [88] αποδεικνύεται ότι, μεταξύ όλων των ιστοριών μίας ακολουθίας, η εξαντλητική είναι αυτή με το μικρότερο πλήθος λέξεων.

Ορισμός 5.9. Για μία πεπερασμένου μήκους ακολουθία y^N, το πλήθος $LZ(y^N)$ των λέξεων της εξαντλητικής ιστορίας της ονομάζεται *Lempel-Ziv πολυπλοκότητα (Lempel-Ziv complexity)* της y^N.

Παράδειγμα 5.10. Η ακολουθία $y^{10} = 0101110110$ έχει την ακόλουθη εξαντλητική ιστορία

$$S_e(y^{10}) = 0 \cdot 1 \cdot 011 \cdot 10110 \cdot$$

Κατά συνέπεια, ισχύει $LZ(y^{10}) = 4$ και τα σημεία της $S_e(y^{10})$ είναι τα $0, 1, 4, 9$.

Όπως αποδεικνύεται στο [88], ισχύει

$$LZ(y^N) < \frac{N}{(1-\epsilon_n)\log_a(N)}\,,$$

με $\epsilon_n = 2^{\frac{1+\log_a \log_a(aN)}{\log_a(N)}}$, όπου a η πληθικότητα του αλφαβήτου στο οποίο η y^N παίρνει τιμές. Η Lempel-Ziv πολυπλοκότητα των κρυπτογραφικών ακολουθιών πρέπει να προσεγγίζει την τιμή αυτή.

Το *λεξικό (vocabulary)* μίας ακολουθίας y^N είναι το σύνολο που αποτελείται από όλες τις υπακολουθίες y_i^j, $0 \leq i \leq j \leq N-1$. Μία υπακολουθία y_i^j ονομάζεται *ιδιολέξη (eigenword)* αν δεν ανήκει στο λεξικό κανενός γνησίου προθέματος της y^N. Η *ιδιοτιμή (eigenvalue)* $k(y^N)$ της ακολουθίας ορίζεται ως το πλήθος του συνόλου των ιδιολέξεων. Το *προφίλ ιδιοτιμής (eigenvalue profile)* της y^N είναι η ακολουθία ακεραίων τιμών που καθορίζεται από τα $k(y^i)$, $i = 1, 2, \ldots, N$ - ένας ορισμός που είναι σε πλήρη αναλογία με τον ορισμό 2.5 του προφίλ πολυπλοκότητας.

Πρόταση 5.11 ([88]). *Η ιδιοτιμή $k(y^N)$ της ακολουθίας y^N ισούται με τον μικρότερο ακέραιο l τέτοιον ώστε η y^N να είναι αναπαραγώγιμη από την y^l.*

Παράδειγμα 5.12. Το λεξικό και οι ιδιολέξεις της $y^4 = 0111$ είναι

$$\{0, 1, 01, 11, 011, 111, 0111\} \text{ και } \{111, 0111\}$$

αντίστοιχα· άρα, $k(y^4) = 2$. Είναι εύκολο να δει κανείς ότι $y^2 \to y^4$ και $y^1 \nrightarrow y^4$. Το προφίλ ιδιοτιμής της y^4 είναι 1222.

Αν και δεν επισημαίνεται ρητά στο [88], η Πρόταση 5.11 είναι ισοδύναμη με το ακόλουθο αποτέλεσμα.

Πόρισμα 5.13. *Για κάθε πεπερασμένου μήκους ακολουθία y^N ισχύει $k(y^N) = t_0^{(N)} + T^{(N)}$, όπου $t_0^{(N)}, T^{(N)}$ είναι η προ-περίοδος και η περίοδος αντίστοιχα της y^N.*

Μία λέξη $y_{h_{i-1}+1}^{h_i}$ που εμφανίζεται σε κάποια ιστορία της y^N καλείται *πρωταρχική (primitive)* αν ο h_i είναι ο μικρότερος ακέραιος με την ιδιότητα $k(y_0^{h_i}) > k(y_0^{h_{i-1}})$. Αν όλες οι λέξεις της ιστορίας, εξαιρουμένης ενδεχομένως της τελευταίας, είναι πρωταρχικές, τότε η ιστορία στο σύνολό της καλείται επίσης *πρωταρχική*. Κάθε ακολουθία έχει μία μοναδική πρωταρχική ιστορία.

Παράδειγμα 5.14. Ας θεωρήσουμε εκ νέου την ακολουθία y^{10} του Παραδείγματος 5.10. Το προφίλ ιδιοτιμής αυτής είναι 1222445557 και, ως εκ τούτου, η πρωταρχική ιστορία της είναι

$$S_p(y^{10}) = 0 \cdot 1 \cdot 011 \cdot 10 \cdot 110 \cdot$$

Το ακόλουθο Θεώρημα ουσιαστικά αναφέρει ότι τα σημεία του πρωταρχικής ιστορίας προσδιορίζουν πλήρως τα σημεία της εξαντλητικής ιστορίας.

Θεώρημα 5.15 ([88]). *Μία λέξη $y_{h_{i-1}+1}^{h_i}$ είναι εξαντλητική αν και μόνο αν ο h_i είναι ο μικρότερος ακέραιος τέτοιος ώστε $k(y^{h_i+1}) > h_{i-1} + 1$.*

Οι Lempel και Ziv στο [88] αναφέρουν ότι το πλήθος των λέξεων της πρωταρχικής ιστορίας μπορεί να χρησιμοποιηθεί ως εναλλακτικό μέτρο αποτίμησης της πολυπλοκότητας μίας ακολουθίας, αντί για το πλήθος των λέξεων της εξαντλητικής ιστορίας.

Με βάση την ανάλυση του Κεφαλαίου 3, το άθροισμα $t_0^{(N)} + T^{(N)}$ για μία πεπερασμένου μήκους ακολουθία y^N ισούται με το πλήθος του συνόλου των καταστάσεων σε μία ελάχιστη καταστατική πραγματοποίηση της ακολουθίας σε σύνολο. Άρα, ανακαλώντας τον Ορισμό 3.8, συμπεραίνουμε ότι η πολυπλοκότητα συνόλου της y^N ισούται με $\log_2(k(y^N))$, αναδεικνύοντας κατά αυτόν τον τρόπο τη σύνδεση μεταξύ των δύο αυτών μέτρων πολυπλοκότητας.

Παρατήρηση 5.16. Άμεση απόρροια του Πορίσματος 5.13 είναι η σχέση $k(y^n) = n - s_n$, όπου με s_n συμβολίζουμε το μήκος του μεγαλύτερου επιθέματος $y_{n-s_n}^{n-1}$ της y^n τέτοιο ώστε η υπακολουθία που προσδιορίζεται από το $y_{n-s_n}^{n-1}$ να εμφανίζεται και άλλη φορά νωρίτερα μέσα στην y^n. Έστω $j < n - s_n$ ο μεγαλύτερος ακέραιος με την ιδιότητα $y_j^{j+s_n-1} = y_{n-s_n}^{s_n-1}$. Τότε, αφού $y_{j-1} \neq y_{n-s_n-1}$, έχουμε $t_0^{(n)} = j$ και $T^{(n)} = n - s_n - j$.

Στη συνέχεια, αναδεικνύουμε τη σχέση που υπάρχει μεταξύ του προφίλ ιδιοτιμής και του προφίλ μη γραμμικής πολυπλοκότητας για μία ακολουθία.

Θεώρημα 5.17. *Έστω $c(y^{n-1}) = m$ και ας υποθέσουμε ότι ο ελάχιστος FSR της y^{n-1} δεν παράγει την y^n. Τότε, ισχύει*

$$c(y^n) = \max\{c(y^{n-1}), n - k(y^{n-1})\} \tag{5.4}$$

Απόδειξη. Ας υποθέσουμε ότι $k(y^{n-1}) < n - m$. Τότε, η υπακολουθία μήκους m y_{n-m-1}^{n-2} (δηλαδή τα τελευταία m στοιχεία της y^{n-1}) εμφανίζεται τουλάχιστον δύο φορές μέσα στην y^{n-1}. Άρα, από το Πόρισμα 5.3, προκύπτει ότι $c(y^n) > c(y^{n-1})$. Επιπλέον, η ακριβής τιμή του $c(y^n)$ προσδιορίζεται από την (5.2). Λόγω του Πορίσματος 5.13, το άθροισμα $t_0^{(n-1)} + T^{(n-1)}$ που εμφανίζεται στην (5.2) ισούται $k(y^{n-1})$, συνεπώς καταλήγουμε στη σχέση $c(y^n) = n - k(y^{n-1}) > c(y^{n-1})$.

Στη συνέχεια, ας θεωρήσουμε την περίπτωση όπου $k(y^{n-1}) \geq n - m$. Τότε, η υπακολουθία y_{n-m-1}^{n-2} μήκους m εμφανίζεται μόνο μία φορά μέσα στην y^{n-1}. Άρα, ισχύει $c(y^n) = c(y^{n-1})$ ανεξαρτήτως της τιμής του y_{n-1} λόγω της Πρότασης 5.2. Κατά συνέπεια, ισχύει σε κάθε περίπτωση η (5.4). □

Πόρισμα 5.18. *Με το συμβολισμό του Θεωρήματος 5.17, ισχύει*

$$c(y^n) = \max\{c(y^{n-1}), s_{n-1} + 1\}$$

όπου s_{n-1} είναι το μήκος του μεγαλύτερου επιθέματος $y_{n-s_{n-1}-1}^{n-2}$ της y^{n-1} το οποίο υπάρχει τουλάχιστον δύο φορές μέσα στην y^{n-1}.

Απόδειξη. Άμεση απόρροια της Σημείωσης 5.16 και της (5.4). □

Το ακόλουθο αποτέλεσμα δίνεται επίσης και στο [58, p. 67]· μία άλλη απόδειξη παρουσιάζεται εδώ, η οποία βασίζεται στο Θεώρημα 5.17.

Πόρισμα 5.19. *Με το συμβολισμό του Θεωρήματος 5.17, ισχύει $c(y^n) > c(y^{n-1})$ μόνο αν $c(y^{n-1}) < \frac{n}{2}$.*

Απόδειξη. Ας υποθέσουμε ότι ισχύει $c(y^{n-1}) \geq \frac{n}{2}$. Τότε, λόγω του ότι $k(y^{n-1}) > c(y^{n-1})$, έχουμε

$$n - k(y^{n-1}) < n - c(y^{n-1}) \leq \frac{n}{2} \leq c(y^{n-1}),$$

το οποίο, σε συνδυασμό με την (5.4), ολοκληρώνει την απόδειξη. □

Στο επόμενο Θεώρημα αποδεικνύουμε ότι το προφίλ ιδιοτιμής καθορίζει μονοσήμαντα το προφίλ της μη γραμμικής πολυπλοκότητας.

Θεώρημα 5.20. *Αν δύο ακολουθίες έχουν το ίδιο προφίλ ιδιοτιμής, τότε έχουν υποχρεωτικά και το ίδιο προφίλ μη γραμμικής πολυπλοκότητας.*

Απόδειξη. Αρχικά, θα αποδείξουμε ότι το προφίλ ιδιοτιμής μίας ακολουθίας y^N προσδιορίζει πλήρως τις θέσεις στις οποίες η μη γραμμική πολυπλοκότητα αυξάνει. Από το Θεώρημα 5.17 προκύπτει ότι εάν $c(y^{n-1}) = m$ και $k(y^{n-1}) \geq n-m$ για κάποιο $n \leq N$, τότε ισχύει $c(y^n) = m$. Από την άλλη πλευρά, αν $k(y^{n-1}) < n - m$, τότε υπάρχουν $0 \leq j_1 < \ldots < j_r < n - m - 1$ τέτοια ώστε $y_{j_i}^{j_i+m-1} = y_{n-m-1}^{n-2}$ και, αφού $c(y^{n-1}) = m$, από την Πρόταση 5.1 προκύπτει $y_{j_1+m} = \cdots = y_{j_r+m}$. Επιπρόσθετα, μπορούμε να έχουμε μία από τις ακόλουθες περιπτώσεις:

- $k(y^n) = k(y^{n-1})$: τότε, από την Πρόταση 5.11 προκύπτει $y^{k(y^{n-1})} \to y^n$ και, κατά συνέπεια, $y_{j_i+m} = y_{n-1}$, για κάθε $i = 1, 2, \ldots, r$. Άρα, $c(y^n) = c(y^{n-1})$.

- $k(y^n) > k(y^{n-1})$: τότε, $y^{k(y^{n-1})} \nrightarrow y^n$. Όμως, λόγω του ότι $y^{k(y^{n-1})} \to y^{n-1}$, ισχύει $y_{j_i+m} \neq y_{n-1}$, για $i = 1, 2, \ldots, r$. Άρα, από το Πόρισμα 5.3 προκύπτει $c(y^n) > c(y^{n-1})$.

Συνεπώς, μένει να αποδειχτεί ότι, για τη δεύτερη περίπτωση, η ακριβής τιμή της πολυπλοκότητας $c(y^n)$ μπορεί πλήρως να προσδιοριστεί από το προφίλ ιδιοτιμής. Πράγματι, το Θεώρημα

5.17 υποδηλώνει ότι, για αυτήν την περίπτωση, ισχύει $c(y^n) = n - k(y^{n-1})$· ως εκ τούτου, η απόδειξη ολοκληρώθηκε. □

Παράδειγμα 5.21. Ας θεωρήσουμε όλες τις δυαδικές ακολουθίες μήκους 10, των οποίων το προφίλ ιδιοτιμής είναι 1223346666. Ύστερα από εξαντητική αναζήτηση, οι ακολουθίες αυτές είναι οι εξής

$$y_1 = 0100011000, \qquad y_2 = 0100011111,$$
$$y_3 = 0110100000, \qquad y_4 = 0110100100,$$
$$y_5 = 0110100110,$$

καθώς και οι συμπληρωματικές τους. Για όλες αυτές τις ακολουθίες, τα σημεία των εξαντλητικών τους ιστοριών συμπίπτουν - αυτά είναι τα $0, 1, 3, 6$. Κατά συνέπεια, η Lempel-Ziv πολυπλοκότητα αυτών ισούται με 4 - ίση δηλαδή με το πλήθος των εξαντλητικών λέξεων. Επιπρόσθετα, όλες αυτές οι ακολουθίες έχουν το ίδιο προφίλ μη γραμμικής πολυπλοκότητας, το οποίο είναι 0112233333.

Το αντίστροφο δεν ισχύει πάντα: για παράδειγμα, τα σημεία της εξαντλητικής ιστορίας της ακολουθίας $\tilde{y} = 0100011001$ είναι επίσης $0, 1, 3, 6$ αλλά, εν τούτοις, τα προφίλ ιδιοτιμής και μη γραμμικής πολυπλοκότητας αυτής είναι 1223346667 και 0112233334 αντίστοιχα. Επίσης, η ακολουθία $\hat{y} = 0110101010$ έχει το ίδιο προφίλ μη γραμμικής πολυπλοκότητας 0112233333 με τις y_i, $1 \leq i \leq 5$. Ωστόσο, όπως μπορεί εύκολα να δειχθεί, τα σημεία του εξαντλητικής ιστορίας της $\hat{y}$ είναι $0, 1, 3$ (και, ως εκ τούτου, η Lempel-Ziv πολυπλοκότητά της είναι 3 και όχι 4), ενώ το προφίλ ιδιοτιμής είναι 1223344444.

Από την παραπάνω ανάλυση προκύπτει ότι η εξαντλητική ιστορία, η οποία προσδιορίζει πλήρως τη Lempel-Ziv πολυπλοκότητα, δεν καθορίζει πλήρως το προφίλ της μη γραμμικής πολυπλοκότητας και αντιστρόφως. Ωστόσο, υπάρχει συσχέτιση μεταξύ τους λόγω των ιδιοτήτων του προφίλ ιδιοτιμής. Συγκεκριμένα, με βάση τα Θεωρήματα 5.15 και 5.20, για κάθε ακολουθία y με δοθείσα εξαντλητική ιστορία (προφίλ μη γραμμικής πολυπλοκότητας), το προφίλ ιδιοτιμής αυτής δεν μπορεί να είναι οποιοδήποτε· άρα, αν υπάρχουν M πιθανά προφίλ ιδιοτιμής για την y, τότε το προφίλ μη γραμμικής πολυπλοκότητας (εξαντλητική ιστορία) ισούται υποχρεωτικά με κάποιο από M πιθανά - κάθε ένα εκ των οποίων προσδιορίζεται από το προφίλ ιδιοτιμής.

Σύμφωνα με το Πόρισμα 5.13, η ιδιοτιμή $k(y^N)$ μίας ακολουθίας y^N ισούται με το μήκος του μικρότερου FSR ο οποίος παράγει την y^N, για τον οποίον όμως η συνάρτηση ανάδρασης

δεν είναι οποιαδήποτε αλλά περιορίζεται στη μορφή

$$h(x_1, x_2, \ldots, x_{k(y^N)}) = x_l, \qquad 1 \leq l \leq k(y^N)\,. \tag{5.5}$$

Αν επιτραπεί οποιαδήποτε συνάρτηση ανάδρασης για τον FSR, έτσι ώστε να μην περιορίζεται στη μορφή (5.5), τότε το μήκος του μικρότερου FSR που παράγει την ακολουθία ισούται με την πολυπλοκότητά της $c(y^N)$. Συνεπώς, υπάρχει μία αντιστοίχιση μεταξύ των $k(y^N)$ και $c(y^N)$. Επίσης, ως άμεση επέκταση, υπάρχει αντιστοίχιση μεταξύ του πλήθους $n_{k(y^N)}$ των σημείων της πρωταρχικής ιστορίας της ακολουθίας με το πλήθος $n_{c(y^N)}$ των σημείων του προφίλ μη γραμμικής πολυπλοκότητας στα οποία εμφανίζεται αύξηση της πολυπλοκότητας. Προφανώς, ισχύει $c(y^N) < k(y^N)$ και, επίσης, $n_{c(y^N)} \leq n_{k(y^N)}$ (βλέπε την απόδειξη του Θεωρήματος 5.20). Αυτές οι ανισότητες υποδηλώνουν το κέρδος που αποκομίζουμε για την παραγωγή μίας ακολουθίας αν, κατά τη διαδικασία παραγωγής της, χρησιμοποιούνται σύνθετες λειτουργίες (μη γραμμικές πράξεις) έναντι απλών λειτουργιών.

Η μέχρι τώρα ανάλυση ισχύει για όλες τις ακολουθίες, ανεξάρτητα από το σώμα στο οποίο παίρνουν τιμή. Στο υπόλοιπο τμήμα του κεφαλαίου περιοριζόμαστε στις δυαδικές ακολουθίες.

5.3 Εύρεση του ελάχιστου FSR μίας ακολουθίας

Σε αυτήν την ενότητα αναπτύσσεται και παρουσιάζεται ένας καινούριος αναδρομικός αλγόριθμος ο οποίος υπολογίζει τον ελάχιστο FSR που παράγει μία δοθείσα δυαδική ακολουθία. Ο αλγόριθμος βασίζεται στις ιδιότητες του προφίλ πολυπλοκότητας, οι οποίες περιγράφονται στις ενότητες 5.1 και 5.2. Ας θεωρήσουμε μία πεπερασμένου μήκους δυαδική ακολουθία $y^{n-1} = y_0 y_1 \ldots y_{n-2}$ τέτοια ώστε $c(y^{n-1}) = m$ και έστω $h^{(n-1)}(x_1, x_2, \ldots, x_m)$ ένα ελάχιστο μη γραμμικό πολυώνυμο αυτής, όπως ορίζεται στην ενότητα 2.4 (όπου η μεταβλητή x_1 αντιστοιχεί στην αριστερότερη βαθμίδα του FSR στο Σχήμα 2.1 κ.ο.κ.). Ας θεωρήσουμε επίσης ότι για το επόμενο bit y_{n-1} ισχύει

$$y_{n-1} = h^{(n-1)}(y_{n-2}, \ldots, y_{n-m-1})\,. \tag{5.6}$$

Τότε, ο ελάχιστος FSR της y^{n-1} με συνάρτηση ανάδρασης $h^{(n-1)}$ παράγει επίσης την y^n και, κατά συνέπεια, $c(y^n) = c(y^{n-1}) = m$. Από την άλλη πλευρά, εάν η (5.6) δεν ισχύει, τότε θα λέμε ότι εμφανίζεται *ασυμφωνία (discrepancy)* και η συνάρτηση ανάδρασης πρέπει να μεταβληθεί. Λόγω της Πρότασης 5.2, αν η y_{n-m-1}^{n-2} εμφανίζεται μόνο μία φορά μέσα στην y^{n-1}, τότε η πολυπλοκότητα δεν αυξάνεται· διαφορετικά, $c(y^n) > m$. Στη συνέχεια αναλύουμε την

κάθε περίπτωση ξεχωριστά, έτσι ώστε να κατασκευάσουμε τον ελάχιστο FSR της y^n και για τις δύο περιπτώσεις.

Περίπτωση 1: έστω ότι εμφανίζεται ασυμφωνία με την έλευση του y_{n-1} και $c(y^n) = c(y^{n-1})$. Ας θεωρήσουμε τη συνάρτηση $h^{(n)} = h^{(n-1)} + f^{(n-1)}$, όπου

$$f^{(n-1)}(x_1, \ldots, x_m) = (x_1 + y'_{n-2}) \cdots (x_m + y'_{n-m-1}) \, .$$

Οι προσθέσεις είναι modulo 2. Ισοδύναμα, η $f^{(n-1)}$ είναι ο ελαχιστόρος που αντιστοιχεί στο διάνυσμα μήκους m που καθορίζεται από την υπακολουθία $y_{n-2} \ldots y_{n-m-1}$. Αφού ισχύει $f^{(n-1)} = 1$ μόνο όταν η f υπολογίζεται σε αυτό το διάνυσμα (και $f^{(n-1)} = 0$ σε όλες τις άλλες περιπτώσεις), η νέα συνάρτηση ανάδρασης $h^{(n)}$ παράγει την y^n και, προφανώς, αποτελεί ελάχιστο μη γραμμικό πολυώνυμο αυτής.

Περίπτωση 2: έστω ότι εμφανίζεται ασυμφωνία με την έλευση του y_{n-1} και $c(y^n) > c(y^{n-1})$. Η αύξηση k στην πολυπλοκότητα προσδιορίζεται από το Θεώρημα 5.4 ή, ισοδύναμα, από την (5.2). Επιπρόσθετα, είναι εύκολο να δειχθεί ότι ο FSR μήκους $m + k$ με συνάρτηση ανάδρασης $h^{(n-1)}$ παράγει επίσης την ακολουθία y^{n-1}, εάν η αρχική του κατάσταση είναι τα πρώτα $m + k$ bits της y^{n-1}. Αντίστοιχα λοιπόν με την Περίπτωση 1, ο FSR με συνάρτηση ανάδρασης $h^{(n)} = h^{(n-1)} + f^{(n-1)}$, όπου η $f^{(n-1)}$ είναι ο ελαχιστόρος που αντιστοιχεί στην υπακολυθία $y_{n-2} \ldots y_{n-m-k-1}$ μήκους $m+k$, παράγει την y^n. Άρα, το $h^{(n)}$ είναι ένα ελάχιστο μη γραμμικό πολυώνυμο της y^n.

Συνδυάζοντας τα παραπάνω, καταλήγουμε στο ότι αν μία συνάρτηση $h^{(n-1)}$ παράγει την y^{n-1} αλλά όχι την y^n, τότε υπάρχει πάντα μία συνάρτηση $f^{(n-1)}$ (η οποία καθορίζεται πλήρως από κάποιον ελαχιστόρο), τέτοια ώστε η $h^{(n)} = h^{(n-1)} + f^{(n-1)}$ να παράγει την y^n. Κατά συνέπεια, η προηγούμενη ανάλυση αποτελεί τη βάση για την κατασκευή ενός αναδρομικού αλγορίθμου για τον υπολογισμό του ελάχιστου μη γραμμικού πολυωνύμου μίας δυαδικής ακολουθίας y^N. Ο αλγόριθμος αυτός παρουσιάζεται στο Σχήμα 5.1. Λόγω της χρήσης των ελαχιστόρων που περιγράφηκε νωρίτερα, το ελάχιστο μη γραμμικό πολυώνυμο h δίνεται σε αναπαράσταση της μορφής ESOP. Επίσης, λόγω της αναδρομικής φύσης του αλγορίθμου, για κάθε πρόθεμα y^n, $1 \leq n \leq N$, της ακολουθίας, το ελάχιστο μη γραμμικό πολυώνυμο αυτού ισούται με

$$h^{(n)}(x_1, \ldots, x_m) = \sum_{i=1}^{n} f^{(i-1)}(x_1, \ldots, x_m) \, . \tag{5.7}$$

```
1:  k ← 0                                          % jump
2:  m ← 0                                          % complexity
3:  h ← y_0                                        % feedback
4:  for n ← 1, ..., N − 1 do
5:      d ← y_n − h(y_{n−1}, ..., y_{n−m})         % discrepancy
6:      if d ≠ 0 then
7:          if m = 0 then
8:              k ← n
9:              m ← n
10:         else if k ≤ 0 then
11:             t ← EIGENVALUE(y^n)                % period + preperiod
12:             if t < n + 1 − m then
13:                 k ← n + 1 − t − m
14:                 m ← n + 1 − t
15:             end
16:         else
17:             k ← k − 1
18:         end
19:         f ← (x_1 + y'_{n−1}) ··· (x_m + y'_{n−m})   % minterm
20:         h ← h + f
21:     else
22:         k ← k − 1
23:     end
24: end
```

Σχήμα 5.1. Αλγόριθμος για τον αναδρομικό υπολογισμό του ελάχιστου FSR μίας δυαδικής ακολουθίας y^N

Στις γραμμές $11, 12$ του αλγορίθμου στο Σχήμα 5.1, εξετάζεται το αν υπάρχει αύξηση στην πολυπλοκότητα της ακολουθίας, με βάση το Θεώρημα 5.17· αν η πολυπλοκότητα αυξάνεται, τότε η νέα τιμή αυτής υπολογίζεται στη γραμμή 13, κάνοντας χρήση του Θεωρήματος 5.4. Με βάση το Πόρισμα 5.18, τόσο η ιδιοτιμή όσο, κατ' επέκταση, και η αύξηση $c(y^{n+1}) - c(y^n)$ της πολυπλοκότητας μπορούν να υπολογιστούν εύκολα μέσω αναζήτησης του μήκους s_n μεγαλύτερου επιθέματος της y^n το οποίο βρίσκεται τουλάχιστον δύο φορές μέσα στην y^n. Η υπολογιστική πολυπλοκότητα αυτής της αλγοριθμικής διαδικασίας είναι γραμμική, λόγω του πολύ γνωστού αλγορίθμου *Knuth-Morris-Pratt* (KMP) που χρησιμοποιείται για *ταύτιση προτύπων (pattern matching)*, δηλαδή για εύρεση της θέσης μίας ακολουθίας μέσα σε μία μεγαλύτερη ακολουθία [24]. Συγκεκριμένα, ο αλγόριθμος KMP χρησιμοποιεί μία *συνάρτηση προθέματος (prefix function)* $\pi_{y^m} : \{0, 1, \ldots, m-1\} \to \{0, 1, \ldots, m-1\}$ για μία ακολουθία y^m, προκειμένου να ελέγξει την εμφάνιση της y^m μέσα σε κάποια μεγαλύτερη ακολουθία, όπου η $\pi_{y^m}(i)$ ισούται με το μήκος του μεγαλύτερου προθέματος της y^{i+1} το οποίο ισούται με κάποιο γνήσιο επίθεμα της y^{i+1}, $0 \leq i < m$. Η υπολογιστική πολυπλοκότητα του αλγορίθμου υπολογισμού της συνάρτησης π_{y^m} είναι $O(m)$; προφανώς, αν θέσουμε $\hat{y}^n = y_{n-1} \ldots y_1 y_0$, τότε

```
Input: Sequence P = P_1 P_2 ... P_m
Output: Prefix function π
 1:  π[1] ← 0
 2:  k ← 0
 3:  for q ← 2 to m do
 4:      while k > 0 and P_{k+1} <> P_q do
 5:          k ← π[k]
 6:      if P_{k+1} = P_q then
 7:          k ← k + 1
 8:      π[q] ← k
 9:  end
10:  return π
```

Σχήμα 5.2. Υπολογισμός της συνάρτησης προθέματος (prefix function) π του αλγορίθμου KMP

$s_n = \max_{0 \le i < n}\{\pi_{\hat{y}^n}(i)\}$. Η διαδικασία υπολογισμού της συνάρτησης προθέματος, όπως αυτή χρησιμοποιείται στον KMP, δίνεται στο Σχήμα 5.2. Άρα, με βάση την προηγούμενη ανάλυση γίνεται φανερό ότι ο υπολογισμός της νέας τιμής της πολυπλοκότητας είναι μια γραμμική αλγοριθμική διαδικασία. Εναλλακτικά, ένας γράφος DAWG μπορεί να χρησιμοποιηθεί για τον υπολογισμό της αύξησης της πολυπλοκότητας, όπως περιγράφεται στο [58].

Ανακαλώντας επίσης την Πρόταση 5.7, αν $c(y^{n+1}) - c(y^n) = k$ τότε τα επόμενα k bits της ακολουθίας δεν προκαλούν αύξηση στην πολυπλοκότητά της. Κατά συνέπεια, κάθε έλεγχος μέσα στις επόμενες k επαναλήψεις για ενδεχόμενη αύξηση της πολυπλοκότητας είναι περιττός. Άρα, αν η συνθήκη στη γραμμή 10 στο Σχήμα 5.1 δεν ικανοποιείται, τότε ο αλγόριθμος απλά μεταπηδά στη γραμμή 17, αφού δεν χρειάζεται να υπολογιστεί η ιδιοτιμή της ακολουθίας. Αξίζει να τονιστεί ότι στις γραμμές $5, 19, 20$ του αλγορίθμου, στις οποίες υπεισέρχονται πράξεις σε λογικές συναρτήσεις, οι προσθέσεις γίνονται modulo 2.

Εφόσον, σε κάθε βήμα, ο προσδιορισμός της τιμής της πολυπλοκότητας της ακολουθίας απαιτεί γραμμική αλγοριθμική λειτουργία, η υπολογιστική πολυπλοκότητα του αλγορίθμου του Σχήματος 5.1 καθορίζεται από τη γραμμή 5, στην οποία αποτιμάται η έξοδος της λογικής συνάρτησης $h^{(n)}$. Για κάθε $n \le N$, η αναπαράσταση ESOP της $h^{(n)}$ αποτελείται από λιγότερους από n όρους γινομένου, όπου ο κάθε όρος αποτελείται από το πολύ $c(y^n) \le n$ μεταβλητές. Άρα, στη χειρότερη περίπτωση, η υπολογιστική πολυπλοκότητα αυτού του βήματος είναι $O(n^2)$. Συνεπώς, λόγω της αναδρομικής φύσης του αλγορίθμου, για μία ακολουθία μήκους N η υπολογιστική πολυπλοκότητα του αλγορίθμου είναι $O(N^3)$ στη χειρότερη περίπτωση. Ωστόσο, αφού κανένας όρος στην ESOP αναπαράσταση της $h^{(n)}$ δεν έχει περισσότερες από $c(y^N)$ μεταβλητές, γίνεται σαφές ότι η υπολογιστική πολυπλοκότητα του αλγορίθμου στη

n	y_n	$y_{n-1}\dots y_{n-m}$	d	EIGENVALUE(y^n)	k	m	$f^{(n)}$
0	0	–	–	–	0	0	–
1	0	0	0	1	−1	0	0
2	1	0	1	1	2	2	$x'_1x'_2$
3	1	10	1	3	1	2	$x_1x'_2$
4	0	11	0	3	0	2	0
5	1	01	1	4	0	2	x'_1x_2
6	1	10	0	4	−1	2	0
7	1	11	1	4	2	4	$x_1x_2x'_3x_4$
8	0	1110	0	6	1	4	0
9	0	0111	1	6	0	4	$x'_1x_2x_3x_4$
10	1	0011	0	8	−1	4	0
11	0	1001	1	8	−1	4	$x_1x'_2x'_3x_4$
12	1	0100	0	10	−2	4	0
13	1	1010	0	10	−3	4	0
14	1	1101	0	10	−4	4	0
15	0	1110	0	10	−5	4	0
16	1	0111	1	10	3	7	$x'_1x_2x_3x_4x'_5x_6x'_7$
17	1	1011101	0	13	2	7	0
18	0	1101110	1	13	1	7	$x_1x_2x'_3x_4x_5x_6x'_7$

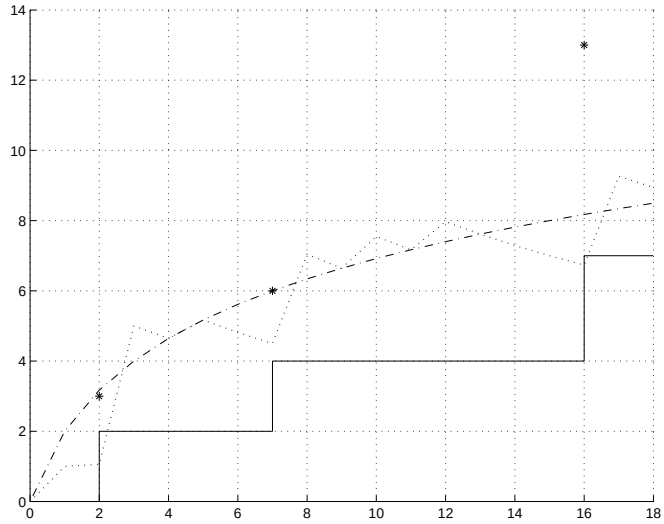
Σχήμα 5.3. Υπολογισμός του ελάχιστου FSR της ακολουθίας y^{19} του Παραδείγματος 5.22.

μέση περίπτωση εξαρτάται από την αναμενόμενη τιμή της μη γραμμικής πολυπλοκότητας τυχαίων δυαδικών ακολουθιών μήκους N. Όπως αποδεικνύεται στο [58], για μεγάλες τιμές του N ισχύει $E(c(y^N)) \approx 2\log_2 N$, οπότε η πολυπλοκότητα του αλγορίθμου είναι κατά μέσο όρο $O(N^2 \log_2 N)$. Αξίζει να σημειωθεί ότι ο αλγόριθμος που προτείνεται εδώ έχει την ίδια υπολογιστική πολυπλοκότητα με τον αλγόριθμο που προτείνεται στο [58] για την εύρεση του ελάχιστου FSR μίας ακολουθίας, ο οποίες βασίζεται στη χρήση γράφου DAWG. Ωστόσο, η αναδρομική δομή του αλγορίθμου του Σχήματος 5.1 συνιστά σημαντικό πλεονέκτημά του, αφού πλέον δεν χρειάζεται να γνωρίζουμε εξ αρχής ολόκληρη την ακολουθία, ενώ επίσης σε κάθε βήμα του αλγορίθμου αξιοποιείται αποδοτικά η πληροφορία που έχουμε αποκομίσει από προηγούμενα βήματα.

Παράδειγμα 5.22. Ας θεωρήσουμε την ακολουθία

$$y^{19} = 0011011100101110110\,.$$

Εκτελώντας τον αλγόριθμο του Σχήματος 5.1, στη φάση αρχικοποίησης θα έχουμε $m = k = 0$ και $h^{(0)} = y_0 = 0$ (βλέπε Σχήμα 5.3 για μία βήμα προς βήμα περιγραφή της εκτέλεσης του αλγορίθμου). Σε κάθε βήμα, η τρέχουσα κατάσταση του FSR είναι η $y_{n-1}\dots y_{n-m}$ και $d = y_n - h^{(n)}(y_{n-1},\dots,y_{n-m})$, όπου m είναι η πολυπλοκότητα της y^n και η $h^{(n)}$ δίνεται από την (5.7). Άρα, αν $d = 1$ τότε έχουμε ασυμφωνία. Για κάθε n, ο αλγόριθμος υπολογίζει την ιδιοτιμή της



Σχήμα 5.4. Το προφίλ της μη γραμμικής πολυπλοκότητας της ακολουθίας y^{19} του Παραδείγματος 5.22

y^n μόνο αν $d = 1$ και $k \leq 0$ (αφού μόνο σε αυτήν την περίπτωση μπορεί να υπάρξει αύξηση της μη γραμμικής πολυπλοκότητας)· συνεπώς, η ιδιοτιμή υπολογίζεται μόνο στις περιπτώσεις για $n = 2, 5, 7, 11, 16$. Οποτεδήποτε υπάρχει ασυμφωνία, ο κατάλληλος ελαχιστόρος προστίθεται στη συνάρτηση ανάδρασης, διαφορετικά η συνάρτηση ανάδρασης μένει αμετάβλητη. Για κάθε n, η μεταβλητή m στη n-ιοστή γραμμή ισούται με $c(y^{n+1})$. Όπως φαίνεται από το Σχήμα 5.3, για τη συγκεκριμένη ακολουθία y^{19} ισχύει $c(y^{19}) = 7$.

Ο παραπάνω αλγόριθμος εύρεσης του ελάχιστου FSR μίας ακολουθίας προσομοιάζει τον αλγόριθμο των Berlekamp-Massey, ο οποίος υπολογίζει τον ελάχιστο LFSR μίας ακολουθίας (Σχήμα 2.4)· πράγματι, τόσο στον BMA όσο και στον προτεινόμενο εδώ αλγόριθμο, αν υπάρχει ασυμφωνία με την έλευση του y_{n-1}, τότε μία πλήρως ορισμένη διορθωτική συνάρτηση προστίθεται στη συνάρτηση ανάδρασης του ελάχιστου FSR της y^{n-1}, προκειμένου να προσδιοριστεί ο ελάχιστος FSR της y^n. Η αναδρομική σχέση που χρησιμοποιείται για τον υπολογισμό του μήκους του ελάχιστου LFSR που παράγει την y^n (δηλαδή τη γραμμική πολυπλοκότητα $\mathrm{lc}(y^n)$ της y^n) είναι

$$\mathrm{lc}(y^n) = \max\left\{\mathrm{lc}(y^{n-1}), n - \mathrm{lc}(y^{n-1})\right\}, \tag{5.8}$$

όπως αυτή προκύπτει από την ανάλυση των ιδιοτήτων του προφίλ της γραμμικής πολυπλοκότητας που παρουσιάζεται στην ενότητα 2.4. Συγκρίνοντας την (5.8) με την (5.4), αναδεικνύονται τα όμοια χαρακτηριστικά των προφίλ γραμμικής και μη γραμμικής πολυπλοκότητας. Συγκεκριμένα, ανακαλώντας το Πόρισμα 5.19, τόσο η γραμμική όσο και η μη γραμμική πολυ-

πλοκότητα της y^{n-1} δεν αυξάνουν αν είναι μεγαλύτερες ή ίσες από την τιμή $\frac{n}{2}$. Από την άλλη πλευρά, αν οποιαδήποτε από αυτές είναι μικρότερη από $\frac{n}{2}$ και, με την έλευση του επόμενου bit, η πολυπλοκότητα αυξάνεται, τότε η γραμμική πολυπλοκότητα γίνεται $n - \mathrm{lc}(y^{n-1})$, ενώ η μη γραμμική πολυπλοκότητα αυξάνεται σε $n - k(y^{n-1}) < n - c(y^{n-1})$.

Τα παραπάνω αποτυπώνονται στο Σχήμα 5.4, όπου η συνεχής γραμμή περιγράφει το προφίλ της μη γραμμικής πολυπλοκότητας για την ακολουθία y^{19} του Παραδείγματος 5.22, ενώ η καμπύλη αντιστοιχεί στην αναμενόμενη τιμή $E(c(y^{n+1})) = 2\log_2(n+1)$. Η διάστικτη γραμμή αντιστοιχεί στην τιμή της ποσότητας $\mathrm{nc}(y^{n+1}) = \big(c(y^n) + k(y^n)\big)\frac{E(c(y^{n+1}))}{n+1}$, η οποία καθορίζει το αν η πολυπλοκότητα αυξάνεται όταν υπάρχει ασυμφωνία μέσω του ελέγχου

$$\begin{aligned} \mathrm{nc}(y^{n+1}) \geq E(c(y^{n+1})) \;&\Leftrightarrow\; c(y^n) + k(y^n) \geq n+1 \\ &\Leftrightarrow\; c(y^{n+1}) = c(y^n). \end{aligned}$$

Οι ομοιότητες της παραπάνω έκφρασης με την $\mathrm{lc}(y^{n+1}) \geq E(\mathrm{lc}(y^{n+1})) = \frac{n+1}{2} \Leftrightarrow \mathrm{lc}(y^{n+1}) = \mathrm{lc}(y^n)$ είναι προφανείς. Τέλος, οι αστερίσκοι "*" στο Σχήμα 5.4 αντιστοιχούν στη νέα τιμή $(n+1) - c(y^n)$ που θα προέκυπτε για την πολυπλοκότητα με βάση την (5.8), εάν αυτή ήταν η γραμμική πολυπλοκότητα και αν, επίσης, ίσχυε $\mathrm{lc}(y^n) = c(y^n)$ για $n = 2, 7, 16$.

5.4 Συσχετίσεις της πολυπλοκότητας με τον βαθμό συμπίεσης

Σε αυτήν την ενότητα μελετάται το πώς η πολυπλοκότητα μίας ακολουθίας επηρεάζει την ικανότητά συμπίεσης της, όπως αυτή καθορίζεται από τον ευρέως διαδεδομένο αλγόριθμο συμπίεσης των Lempel-Ziv. Συγκεκριμένα θα μελετήσουμε τη δεύτερη έκδοση του αλγορίθμου, γνωστή ως LZ78 [140]. Μία ακολουθία y^N με τιμές σε ένα πεπερασμένο αλφάβητο χωρίζεται σε ανά δύο διαφορετικές μεταξύ τους λέξεις $w_1, w_2, \ldots$, όπως φαίνεται στην (5.3), με μία πιθανή εξαίρεση για την τελευταία λέξη (για την οποία μπορεί να υπάρχει μία προηγούμενη λέξη ίδια με αυτή). Με βάση την (5.3), έχουμε

$$w_1 = y_0 \quad \text{και} \quad w_i = y_{h_{i-2}+1}^{h_{i-1}} \;\; \forall\, i \geq 2\,.$$

Η διαδικασία κατάτμησης της ακολουθίας σε λέξεις στον LZ78 είναι τέτοια ώστε το πρόθεμα $w_i^{\ell(w_i)-1}$ κάθε λέξης w_i μήκους $\ell(w_i) > 1$ να ταυτίζεται με κάποια προηγούμενη λέξη w_j για κάποιο $j < i$.

Παράδειγμα 5.23. Αν εφαρμοστεί ο LZ78 στη δυαδική ακολουθία

$$y^{11} = 11001000110,$$

τότε αυτή χωρίζεται στις λέξεις

$$1 \cdot 10 \cdot 0 \cdot 100 \cdot 01 \cdot 10$$

όπου η απουσία της τελείας στο τέλος υποδηλώνει ότι η τελευταία λέξη 10 έχει ήδη εμφανιστεί νωρίτερα.

Για μία δυαδική ακολουθία y^N, η συμπίεση επιτυγχάνεται με το να μετατρέπεται κάθε λέξη w_i σε μία νέα κωδική λέξη c_i αποτελούμενη από δύο τμήματα: το πρώτο τμήμα της c_i είναι η δυαδική αναπαράσταση του ακεραίου j που ορίζεται μονοσήμαντα από την $w_j = w_i^{\ell(w_i)-1}$, ενώ το δεύτερο τμήμα της c_i είναι απλά το τελευταίο στοιχείο της w_i. Άρα, αν $p(y^N)$ είναι το πλήθος των λέξεων που θα προκύψουν κατά τη διαδικασία κατάτμησης της ακολουθίας, τότε ο *λόγος συμπίεσης (compression ratio)* της y^N ισούται με

$$\rho_{y^N} = \frac{1}{N} \sum_{i=1}^{p(y^N)} \ell(c_i) = \frac{1}{N} \sum_{i=1}^{p(y^N)} \lceil \log_2(2i) \rceil \tag{5.9}$$

αφού $\ell(c_i) = \lceil \log_2(i) \rceil + 1 = \lceil \log_2(2i) \rceil$ [140]. Ο λόγος συμπίεσης για μία μεμονωμένη λέξη w_i ορίζεται αντίστοιχα ως $\frac{\ell(c_i)}{\ell(w_i)}$. Η αποσυμπίεση γίνεται με την αντίστροφη διαδικασία. Από την (5.9) προκύπτει ότι, όσο η ποσότητα ρ_{y^N} ελαττώνεται, τόσο καλύτερη (μεγαλύτερη) συμπίεση επιτυγχάνεται. Άρα, οι κρυπτογραφικές ακολουθίες πρέπει να έχουν μεγάλες τιμές για τα $c(y^N)$ και ρ_{y^N}. Έστω $\bar{w}$ και $\bar{c}$ το μέσο μήκος των λέξεων και των κωδικών λέξεων αντίστοιχα, δηλαδή $\bar{w} = \frac{N}{p(y^N)}$ και $\bar{c} = \frac{1}{p(y^N)} \sum_{i=1}^{p(y^N)} \ell(c_i)$. Τότε, ο λόγος συμπίεσης της y^N, όπως ορίζεται στην (5.9), μπορεί ισοδύναμα να γραφεί ως

$$\rho_{y^N} = \frac{\bar{c}}{\bar{w}}\,. \tag{5.10}$$

Από την (5.10) προκύπτει άμεσα το ακόλουθο αποτέλεσμα.

Πόρισμα 5.24. *Έστω οι δυαδικές ακολουθίες y_1, y_2 οι οποίες διασπώνται, αν εφαρμοστεί η διαδικασία κατάτμησης του LZ78, σε $p(y_1)$ και $p(y_2)$ λέξεις αντίστοιχα. Τότε, ισχύει $\rho_{y_1} < \rho_{y_2}$ αν και μόνο αν $\bar{w}_1 > \frac{\bar{c}_1}{\bar{c}_2}\bar{w}_2$.*

Παρατήρηση 5.25. Σε διάφορες υλοποιήσεις του LZ78, το μέγεθος κάθε κωδικής λέξης είναι σταθερό και ίσο με $\lceil \log_2(p(y^N)) \rceil + 1$. Συγκεκριμένα, για αυτήν την έκδοση του LZ78, πραγματοποιείται πρώτα μία αρχική σάρωση της ακολουθίας προκειμένου να σχηματιστούν όλες

οι λέξεις κατά τη διαδικασία κατάτμησης, και στη συνέχεια, με μία δεύτερη σάρωση, κάθε λέξη w_i κωδικοποιείται με βάση τους παραπάνω κανόνες, όπου όμως για το πρώτο τμήμα της c_i χρησιμοποιούνται πάντα $\lceil \log_2(p(y^N)) \rceil$ bits. Αυτή η παραλλαγή έχει ως αποτέλεσμα μία πιο εύκολη διαδικασία αποκωδικοποίησης· ωστόσο, ο λόγος συμπίεσης που προκύπτει είναι μεγαλύτερος - δηλαδή, δεν επιτυγχάνεται εξίσου καλή συμπίεση.

Από την περιγραφή του LZ78 προκύπτει ότι κάθε δυαδική ακολουθία $y^N = y_0 y_1 \dots y_{N-1}$ της μορφής

$$y^N = a_1 \;\; a_1 a_2 \;\; a_1 a_2 a_3 \;\; \dots \;\; a_1 a_2 a_3 \dots a_s \tag{5.11}$$

όπου $N = \frac{1}{2}s(s+1)$, χωρίζεται στο ελάχιστο δυνατό πλήθος λέξεων s ως προς το μήκος της N· με άλλα λόγια, για κάθε άλλη ακολουθία $\tilde{y}^N$ μήκους N ισχύει $p(y^N) \geq s$. Έτσι, οδηγούμαστε στον ακόλουθο ορισμό.

Ορισμός 5.26. Κάθε δυαδική ακολουθία y^N τέτοια ώστε

- $p(y^N) = s$ για κάποιον ακέραιο $s \geq 2$ και
- $N = \frac{1}{2}s(s+1)$,

ονομάζεται *s-βέλτιστη (s-optimal)* ακολουθία και συμβολίζεται ως y^s_{opt}. Ο λόγος συμπίεσης μίας s-βέλτιστης ακολουθίας συμβολίζεται ως ρ^s_{opt}.

Από τον Ορισμό 5.26 προκύπτει ότι κάθε s-βέλτιστη ακολουθία μπορεί να περιγραφεί πλήρως από τα τελευταία s στοιχεία της $a_1 a_2 \dots a_s$. Άρα, υπάρχουν 2^s s-βέλτιστες ακολουθίες. Στο υπόλοιπο της ενότητας, θα αναφερόμαστε σε αυτές με το συμβολισμό $y^N =_{\text{opt}} \langle a_1, \dots, a_s \rangle$.

Στη συνέχεια, αποδεικνύουμε μία σχέση μεταξύ της μη γραμμικής πολυπλοκότητας και του βαθμού συμπίεσης. Προς αυτήν την κατεύθυνση, θα παρουσιαστούν αρχικά σημαντικές ιδιότητες των s-βέλτιστων ακολουθιών, οι οποίες εξ ορισμού είναι υψηλά συμπιέσιμες. Από τις ιδιότητες αυτών θα προκύψει ένα κάτω φράγμα του βαθμού συμπίεσης κάθε δυαδικής ακολουθίας, το οποίο εξαρτάται από την πολυπλοκότητά της.

Λήμμα 5.27. *Για κάθε $n \geq 1$, ισχύει $(2^n - 1)(n-1) = \sum_{i=1}^{2^n-1} \lceil \log_2(i) \rceil$.*

Απόδειξη. Για κάθε $n \geq 1$ έχουμε

$$\sum_{i=1}^{2^n-1} \lceil \log_2(i) \rceil = \sum_{i=0}^{n-1} \sum_{j=1}^{2^i} \lceil \log_2(2^i + j) \rceil - n$$

$$= \sum_{i=0}^{n-1}(i+1)2^i - n$$
$$= (2^n - 1) + 2\sum_{i=0}^{n-2}(i+1)2^i - n$$

όπου χρησιμοποιήσαμε τη σχέση $\sum_{i=0}^{n-1}(i+1)2^i = \sum_{i=0}^{n-1} 2^i + \sum_{i=1}^{n-1} i\,2^i$. Αν εφαρμόσουμε αναδρομικά αυτήν την ιδιότητα $n-2$ φορές καταλήγουμε στην

$$\sum_{i=1}^{2^n-1}\lceil \log_2(i)\rceil = \sum_{i=0}^{n-1} 2^i(2^{n-i}-1) - n$$
$$= n(2^n-1) - \sum_{i=0}^{n-1} 2^i$$

το οποίο ολοκληρώνει την απόδειξη. □

Η ακόλουθη Πρόταση αποδεικνύει ότι, όταν αυξάνεται το s, ο λόγος συμπίεσης των s-βέλτιστων ακολουθιών μειώνεται.

Πρόταση 5.28. *Για κάθε $s \geq 3$, ισχύει $\rho_{opt}^{s} > \rho_{opt}^{s+1}$.*

Απόδειξη. Εξ ορισμού, οι s-βέλτιστες ακολουθίες ικανοποιούν τη σχέση $\bar{w}_s = \frac{1}{2}(s+1)$. Σύμφωνα με το Πόρισμα 5.24 ισχύει $\rho_{\rm opt}^{s} > \rho_{\rm opt}^{s+1}$ αν και μόνο αν $\bar{w}_{s+1} > \frac{\bar{c}_{s+1}}{\bar{c}_s}\bar{w}_s$. Από αυτήν τη σχέση καταλήγουμε, μετά από πράξεις, στα εξής:

$$\rho_{\rm opt}^{s} > \rho_{\rm opt}^{s+1} \Leftrightarrow (s+2)\sum_{i=1}^{s}\lceil\log_2(2i)\rceil > s\sum_{i=1}^{s+1}\lceil\log_2(2i)\rceil$$
$$\Leftrightarrow 2\sum_{i=1}^{s}\lceil\log_2(2i)\rceil > s\lceil\log_2(2(s+1))\rceil$$
$$\Leftrightarrow 2\sum_{i=1}^{s}\lceil\log_2(i)\rceil - s\lceil\log_2\tfrac{s+1}{2}\rceil > 0\,. \qquad (5.12)$$

Έστω $k \geq 1$ ο μοναδικός ακέραιος που προσδιορίζεται από την $2^k \leq s < 2^{k+1}$, οπότε $s = 2^k + r$ για κάποιο $0 \leq r < 2^k$. Κατά συνέπεια, έχουμε $\lceil\log_2\frac{s+1}{2}\rceil = k$. Αφού από την υπόθεση έχουμε $s \geq 3$, προκύπτει ότι $r = 1 > 0$ αν $k = 1$. Αντικαθιστώντας το s στην (5.12), προκύπτει

$$2\left(\sum_{i=1}^{2^k}\lceil\log_2(i)\rceil + \sum_{i=2^k+1}^{2^k+r}\lceil\log_2(i)\rceil\right) - (2^k+r)k$$
$$= 2\big(2^k(k-1) + 1 + r(k+1)\big) - (2^k+r)k$$
$$= (2^k+r)(k-2) + 2(2r+1)$$

όπου $\sum_{i=1}^{2^k}\lceil\log_2(i)\rceil = 2^k(k-1)+1$ λόγω του Λήμματος 5.27. Όμως, η τελευταία παράσταση είναι πάντα θετική για κάθε $k \geq 1$ (αφού, για $k=1$, έχουμε $r=1$). Άρα, η (5.12) ισχύει. □

Πρόταση 5.29. *Έστω y^N μία δυαδική ακολουθία μήκους N, και έστω s ο ελάχιστος ακέραιος με την ιδιότητα $N \leq \frac{1}{2}s(s+1)$. Τότε, ισχύει $\rho_{y^N} \geq \rho^s_{opt}$.*

Απόδειξη. Από την υπόθεση έχουμε ότι $\frac{1}{2}(s-1)s < N$, δηλαδή το μήκος της y^N είναι μεγαλύτερο από το μήκος μίας $(s-1)$-βέλτιστης ακολουθίας. Αυτό, σε συνδυασμό με τον Ορισμό 5.26, μας οδηγεί στην $p(y^N) \geq s$. Από την (5.9) έχουμε

$$\begin{aligned}\rho_{y^N} &= \frac{1}{N}\left(\frac{s(s+1)}{2}\rho^s_{\rm opt} + \sum_{i=s+1}^{p(y^N)}\ell(c_i)\right) \geq \frac{s(s+1)}{2N}\rho^s_{\rm opt}\\ &\geq \rho^s_{\rm opt}\end{aligned}$$

αφού $s(s+1) \geq 2N$. □

Θεώρημα 5.30. *Έστω y μία περιοδική δυαδική ακολουθία με περίοδο N και $c(y)=m$, και έστω y^N το περιοδικό τμήμα της y, δηλαδή η ακολουθία που προκύπτει από τα πρώτα N bits της y. Αν n είναι ο μεγαλύτερος ακέραιος με την ιδιότητα $2^n \leq m < 2^{n+1}$, τότε ισχύει*

$$\rho_{y^N} > \min\left\{\tfrac{1}{m}\lceil\log_2(2m)\rceil, \tfrac{1}{2^n}(n+1)\right\}. \tag{5.13}$$

Απόδειξη. Έστω $w_1,\ldots,w_k$ οι λέξεις στις οποίες χωρίζεται η y^N, μετά τη διαδικασία κατάτμησης στην οποία υπόκειται από τον LZ78. Από την (5.9) θα έχουμε

$$\rho_{y^N} = \frac{1}{N}\sum_{i=1}^{k}\ell(w_i)\frac{\lceil\log_2(2i)\rceil}{\ell(w_i)} > \frac{\sum_{i=1}^{k}\ell(w_i)\rho_{\min}}{N} = \rho_{\min},$$

όπου $\rho_{\min} = \min_{1\leq i\leq k}\left\{\frac{1}{\ell(w_i)}\lceil\log_2(2i)\rceil\right\}$ είναι ο μικρότερος λόγος συμπίεσης μεταξύ των λόγων συμπίεσης όλων των λέξεων. Αφού για κάθε $1 \leq i \leq k$ ισχύει $\ell(w_i) \leq i$ (όπου, αν $\ell(w_i) = i$ για κάθε i, τότε η y^N είναι k-βέλτιστη), προκύπτει

$$\rho_{\min} \geq \min_{1\leq i\leq k}\left\{\tfrac{1}{i}\lceil\log_2(2i)\rceil\right\}.$$

Επίσης, αφού από την υπόθεση έχουμε $c(y)=m$, δεν υπάρχει ζευγάρι όμοιων υπακολουθιών μέσα στην y^N και, ως εκ τούτου, το μέγιστο δυνατό μέγεθος λέξης που μπορεί να εμφανιστεί μετά τη διαδικασία κατάτμησης είναι m· διαφορετικά, αν $\ell(w_l) > m$ για κάποιο $m+1 \leq l \leq k$, τότε η w_l^m θα είχε εμφανιστεί νωρίτερα. Άρα, συνδυάζοντας τα παραπάνω, καταλήγουμε στη σχέση

$$\rho_{y^N} > \min_{1\leq i\leq m}\left\{\tfrac{1}{i}\lceil\log_2(2i)\rceil\right\}.$$

Η συνάρτηση $f(x) = \frac{1}{x}\lceil \log_2(2x) \rceil$ είναι γνησίως φθίνουσα στο διάστημα $(2^n, 2^{n+1}]$ για κάθε $n \geq 1$. Ωστόσο, ισχύει $f(2^n) < f(2^n + j)$ για $1 \leq j \leq \epsilon_n$, όπου ο ακέραιος ϵ_n εξαρτάται από το n. Κατά συνέπεια, ισχύει τελικά

$$\rho_{y^N} > \min\big\{ f(m), f(2^n) \big\} .$$

Ο ακέραιος ϵ_n που περιγράφηκε ανωτέρω μπορεί να υπολογιστεί ως εξής: αφού $m = 2^n + a$ για κάποιο $0 \leq a < 2^n$, τότε ισχύει $\lceil \log_2(2m) \rceil = n + 2$ και, συνεπώς, θα έχουμε $f(2^n) \leq f(m)$ αν και μόνο αν

$$\begin{aligned} \frac{n+1}{2^n} \leq \tfrac{1}{m}\lceil \log_2(2m) \rceil &\Leftrightarrow (2^n + a)(n+1) \leq 2^n(n+2) \\ &\Leftrightarrow a \leq \frac{1}{n+1} 2^n. \end{aligned}$$

□

Παρατήρηση 5.31. Από τις Προτάσεις 5.28 και 5.29 μπορούμε να συμπεράνουμε εύκολα ότι αν $c(y) = m$ είναι η πολυπλοκότητα της περιοδικής δυαδικής ακολουθίας y και m είναι ο μικρότερος ακέραιος τέτοιος $N \leq \frac{1}{2}m(m+1)$, όπου N είναι η περίοδος της ακολουθίας, τότε ο λόγος συμπίεσης της y^N είναι μεγαλύτερος ή ίσος από τον αριθμό $\rho^m_{\rm opt}$. Αυτό το κάτω φράγμα είναι υψηλότερο από αυτό της (5.13). Πράγματι, έστω $2^n \leq m < 2^{n+1}$ για κάποιο $n \geq 1$ όπως ακριβώς στο Θεώρημα 5.30, και ας υποθέσουμε αρχικά ότι $m = 2^n$. Τότε, θα έχουμε

$$\rho^{2^n}_{\rm opt} > \rho^{2^{n+1}-1}_{\rm opt} = \tfrac{1}{2^n}(n+1)$$

λόγω της Πρότασης 5.28. Διαφορετικά, αν $m > 2^n$, ισχύει $m = 2^n + r$ με $1 \leq r < 2^n$, οπότε για να αποδείξουμε ότι $\rho^m_{\rm opt} > f(m)$ αρκεί να δείξουμε ότι η ακόλουθη παράσταση είναι πάντα θετικός αριθμός:

$$\begin{aligned} &2\sum_{i=1}^{m} \lceil \log_2(2i) \rceil - (m+1)\lceil \log_2(2m) \rceil \\ &\quad = 2\left(\sum_{i=1}^{m} \lceil \log_2(i) \rceil - 1 \right) - (m+1)\Big(\lceil \log_2(m) \rceil - 1 \Big) \\ &\quad = 2\left(\sum_{i=1}^{2^n} \lceil \log_2(i) \rceil - 1 + r(n+1) \right) - (2^n + r + 1)n \\ &\quad = 2\Big(2^n(n-1) + r(n+1) \Big) - (2^n + r + 1)n \\ &\quad = (2^n + r - 1)(n-2) + 2(2r-1) \end{aligned}$$

όπου θέσαμε $\sum_{i=1}^{2^n}\lceil\log_2(i)\rceil = 2^n(n-1)+1$ χρησιμοποιώντας το Λήμμα 5.27. Η τελική παράσταση που προκύπτει είναι θετική για $n > 1$, ενώ αν $n = 1$ (οπότε υποχρεωτικά θα έχουμε $r = 1$) γίνεται $3(r-1) = 0$· συνεπώς, αν $m = 3$, τα δύο κάτω φράγματα συμπίπτουν.

Όπως αναδεικνύεται στην απόδειξη του Θεωρήματος 5.30, το κάτω φράγμα της (5.13) μειώνεται καθώς η πολυπλοκότητα $c(y)$ της περιοδικής ακολουθίας y αυξάνεται. Κατά συνέπεια, είναι πιθανό να υπάρχουν ακολουθίες πολύ υψηλής πολυπλοκότητας, οι οποίες όμως να είναι υψηλά συμπιέσιμες. Με δεδομένο ότι τυχαίες ακολουθίες δεν αναμένεται να έχουν αυτά τα χαρακτηριστικά, συμπεραίνουμε ότι ο βαθμός συμπίεσης μίας κρυπτογραφικής ακολουθίας πρέπει να εξετάζεται ταυτόχρονα με την πολυπλοκότητά της, έτσι ώστε να απορρίπτονται ακολουθίες που παρουσιάζουν αυτήν τη συμπεριφορά. Από την ανάλυση αυτή γίνεται φανερό ότι ανακύπτει η ανάγκη της κατά το δυνατόν ταυτοποίησης των δυαδικών ακολουθιών πολυπλοκότητας m των οποίων ο λόγος συμπίεσης είναι κοντά στο κάτω φράγμα (5.13), αφού αυτές οι ακολουθίες δεν πρέπει να θεωρούνται κατάλληλες για κρυπτογραφικές εφαρμογές. Προς αυτήν την κατεύθυνση, μελετούμε στη συνέχεια ιδιότητες της μη γραμμικής πολυπλοκότητας για τις s-βέλτιστες ακολουθίες, αφού αυτές παρουσιάζουν χαμηλούς λόγους συμπίεσης.

Πρόταση 5.32. *Έστω $y^s_{opt} =_{opt} \langle a_1, \ldots, a_s\rangle$, όπου $s \geq 4$. Τότε, η y^s_{opt} περιέχει τουλάχιστον δύο όμοιες υπακολουθίες μήκους s.*

Απόδειξη. Όπως προκύπτει από τον Ορισμό 5.26, η λέξη w_i, για $1 \leq i \leq s$, που προκύπτει από την κατάτμηση που επιφέρει ο LZ78, ισούται με $w_i = a_1 \ldots a_i$. Χωρίς βλάβη της γενικότητας θεωρούμε ότι $a_1 = 1$ (η περίπτωση $a_1 = 0$ μπορεί να αντιμετωπιστεί ομοίως). Εάν ισχύει $a_s = 1$, τότε προκύπτει άμεσα ότι $w_{s-1}a_1 = w_s$. Διαφορετικά, για την πιο ενδιαφέρουσα περίπτωση όπου $a_s = 0$, διαχωρίζουμε τις ακόλουθες περιπτώσεις σχετικά με τις τιμές που μπορεί να έχει η $w_s = a_1a_2a_3a_4 \ldots a_{s-4}a_{s-3}a_{s-2}a_{s-1}a_s$ (όπου το σύμβολο "*" υποδηλώνει ότι η αντίστοιχη τιμή του bit μπορεί να είναι είτε 0 είτε 1):

- $10{**}\ldots{***}10$: τότε $w_{s-2}a_1a_2 = w_s$,
- $11{**}\ldots{***}10$: τότε $w_{s-2}a_1a_2 = w_{s-1}a_1$,
- $1{***}\ldots{**}000$: τότε $a_{s-2}w_{s-1} = a_{s-1}w_s^{s-1}$,
- $100{*}\ldots{**}100$: τότε $w_{s-3}a_1a_2a_3 = w_s$,
- $101{*}\ldots{**}100$: τότε $w_{s-3}a_1a_2a_3 = w_{s-1}a_1$,

- 111*...01100: τότε $w_{s-3}a_1a_2a_3 = w_{s-2}a_1a_2$,
- 1100...01100: τότε $w_{s-4}a_1a_2a_3a_4 = w_s$,
- 1101...01100: τότε $w_{s-4}a_1a_2a_3a_4 = w_{s-1}a_1$,
- 11**...00100: τότε $a_{s-4}w_{s-3}a_1a_2 = a_{s-3}w_{s-2}a_1$,
- 11**...11100: τότε $a_{s-4}w_{s-3}a_1a_2 = a_{s-3}w_{s-2}a_1$,
- 1***...10100: τότε $a_{s-4}a_{s-3}w_{s-2} = a_{s-2}a_{s-1}w_s^{s-2}$.

Η 4-βέλτιστη ακολουθία $y^4_{\rm opt} =_{\rm opt} \langle 1,1,0,0\rangle$ δεν καλύπτεται από τις παραπάνω περιπτώσεις, αλλά και αυτή ικανοποιεί την επιθυμητή ιδιότητα αφού ισούται με την $y = 1111101100$ και, προφανώς, έχουμε $y_0^3 = y_1^4$. □

Λήμμα 5.33. *Έστω η ακολουθία y^m_{opt} με πολυπλοκότητα $c(y^N) = m \geq 4$ και μήκος $N = \frac{1}{2}m(m+1)$. Τότε, υπάρχει ακέραιος $0 \leq i < N-m$ τέτοιος ώστε $y_i^{i+m-1} = y_{N-m}^{N-1}$.*

Απόδειξη. Ας υποθέσουμε ότι δεν υπάρχει ακέραιος i με την παραπάνω ιδιότητα. Τότε, από την Πρόταση 5.32, υπάρχουν δύο ακέραιοι $0 \leq n_1 < n_2 < N-m$ τέτοιοι ώστε $y_{n_1}^{n_1+m-1} = y_{n_2}^{n_2+m-1}$. Συνεπώς, αφού η υπακολουθία y_{N-m}^{N-1} δεν εμφανίζεται νωρίτερα στην y^N, υπάρχει $1 \leq j \leq N-n_2-m$ τέτοιο ώστε

$$y_{n_1}^{n_1+m-1+j} \neq y_{n_2}^{n_2+m-1+j}$$

Άρα, από την Πρόταση 5.1 προκύπτει ότι $c(y^N) > m$ - άτοπο. □

Πρόταση 5.34. *Έστω η ακολουθία $y^N =_{opt} \langle a_1,\ldots,a_m\rangle$ με $c(y^N) = m \geq 4$, και έστω επίσης η ακολουθία $\tilde{y}^L =_{opt} \langle a_1,\ldots,a_{m+1}\rangle$, δηλαδή $\tilde{y}_0^{N-1} = y^N$. Τότε, ισχύει $c(\tilde{y}^L) > m$.*

Απόδειξη. Από την υπόθεση έχουμε ότι $L = N+m+1$. Επίσης, από τον Ορισμό 5.26, γνωρίζουμε ότι κάθε λέξη w_i, για $1 \leq i \leq m+1$, η οποία δημιουργείται από την κατάτμηση που επιφέρει ο LZ78, ισούται με $w_i = a_1\ldots a_i$. Άρα, ισχύει $w_m = w_{m+1}^m$ ή, ισοδύναμα,

$$\tilde{y}_{N-m}^{N-1} = \tilde{y}_N^{N+m-1}\,. \tag{5.14}$$

Ας υποθέσουμε ότι $c(\tilde{y}^L) = m$. Τότε, λόγω της Πρότασης 5.1 συμπεραίνουμε ότι $\tilde{y}_N = \tilde{y}_{N+m} \Rightarrow a_1 = a_{m+1}$. Επίσης, σύμφωνα με το Λήμμα 5.33, υπάρχει $i < N-m$ τέτοιο ώστε

$$\tilde{y}_i^{i+m-1} = \tilde{y}_{N-m}^{N-1}\,. \tag{5.15}$$

Λόγω της υπόθεσης ότι $c(\tilde{y}^L) = m$, όλες οι υπακολουθίες που διαδέχονται τις $\tilde{y}_i^{i+m-1}$ και $\tilde{y}_{N-m}^{N-1}$ ταυτίζονται μεταξύ τους (σε αντίθετη περίπτωση, η πολυπλοκότητα της $\tilde{y}^L$ θα αύξανε). Άρα, από αυτήν την παρατήρηση οδηγούμαστε στη σχέση

$$\tilde{y}_{i+m}^{i+2m-1} = \tilde{y}_N^{N+m-1} \,. \tag{5.16}$$

Συνδυάζοντας τις (5.14), (5.15) και (5.16), καταλήγουμε στην ισότητα

$$\tilde{y}_i^{i+2m-1} = w_m w_m \,.$$

Αφού $c(\tilde{y}^L) = m$, συμπεραίνουμε ότι η ακολουθία $\tilde{y}^L$ αποτελείται από διαδοχικές επαναλήψεις της w_m, οι οποίες ξεκινούν να εμφανίζονται από τη θέση του $\tilde{y}_i$· αν δεν ίσχυε αυτό, τότε θα προέκυπτε ότι $c(\tilde{y}^L) > m$ από την Πρόταση 5.1. Ας υποθέσουμε αρχικά ότι $i = N - km$, για κάποιο $k \geq 2$. Τότε, λόγω των διαδοχικών επαναλήψεων του w_m, λαμβάνουμε από τις (5.14) και (5.15) (για $k = 2$):

$$\tilde{y}_{N-2m}^{N-m-1} = \tilde{y}_{N-m}^{N-1} = \tilde{y}_N^{N+m-1} \,.$$

Επίσης, η σχέση $w_{m-1} = w_m^{m-1}$ μας οδηγεί στην ισότητα $\tilde{y}_{N-2m+1}^{N-m-1} = \tilde{y}_{N-m}^{N-2}$, η οποία, συνδυαζόμενη με τα προηγούμενα, δίνει

$$\tilde{y}_{N-m}^{N-2} = \tilde{y}_{N-m+1}^{N-1} \;\Rightarrow\; a_1 = \cdots = a_m = a_{m+1}$$

το οποίο αντιβαίνει στο γεγονός ότι $c(\tilde{y}^L) = m \geq 4$. Στη συνέχεια, θεωρούμε την περίπτωση όπου $i \neq N - km$. Τότε, λόγω των διαδοχικών επαναλήψεων του w_m, αρκεί να εξετάσουμε την περίπτωση $N - 2m < i < N - m$· έστω λοιπόν $i = N - 2m + j$, όπου $1 \leq j < m$. Προφανώς, η θέση i αντιστοιχεί στον όρο a_j της λέξης w_{m-1}. Άρα, χρησιμοποιώντας τη σχέση $\tilde{y}_i^{i+2m-1} = w_m w_m$, καταλήγουμε στα ακόλουθα:

$$(a_j, a_{j+1}, \ldots, a_{m-1}) = (a_1, a_2, \ldots, a_{m-j}) \,, \tag{5.17a}$$

$$(a_1, \ldots, a_{j-1}, a_j) = (a_{m-j+1}, \ldots, a_{m-1}, a_m) \,, \tag{5.17b}$$

$$(a_{j+1}, a_{j+2}, \ldots, a_m) = (a_1, a_2, \ldots, a_{m-j}) \,. \tag{5.17c}$$

Άρα τα διανύσματα του αριστερού μέλους των (5.17a) και (5.17c) συμπίπτουν, οπότε $a_j = \cdots = a_m$. Από αυτήν την ισότητα, από το γεγονός ότι $a_1 = a_{m+1}$ και από τις εξισώσεις 5.17 προκύπτει $a_1 = \cdots = a_m = a_{m+1}$ το οποίο αντιβαίνει στο γεγονός ότι $c(\tilde{y}^L) = m > 0$. Άρα, πάντα θα ισχύει $c(\tilde{y}^L) > m$. □

Πόρισμα 5.35. *Για κάθε s-βέλτιστη ακολουθία $y_{opt}^s =_{opt} \langle a_1, \ldots, a_s \rangle$, όπου $s \geq 4$ και $y_{opt}^s \neq \mathbf{0}, \mathbf{1}$, ισχύει $c(y_{opt}^s) \geq s$.*

Απόδειξη. Για κάθε $1 \leq i \leq s$, η λέξη w_i που προκύπτει από την κατάτμηση του αλγορίθμου LZ78 δίνεται από την $w_i = a_1 \dots a_i$. Εάν υποθέσουμε ότι $a_1 = \cdots = a_{s-1}$ και $a_s \neq a_1$, τότε από την Πρόταση 5.1 έχουμε $c(y^s_{\text{opt}}) > \frac{1}{2}(s-1)s > s$. Έστω ότι υπάρχει τουλάχιστον ένα $0 < j < \frac{1}{2}(s-1)s$ τέτοιο ώστε $y_j \neq y_0$. Η απόδειξη θα γίνει επαγωγικά ως προς το s. Ο ισχυρισμός είναι αληθής για $s = 4$ - για παράδειγμα, η ακολουθία $y^4_{\text{opt}} =_{\text{opt}} \langle 1,1,0,0\rangle$, έχει πολυπλοκότητα 5 (όλες οι 4-βέλτιστες ακολουθίες μπορούν εύκολα να ελεγθούν). Έστω ότι ο ισχυρισμός αληθεύει για $s = k$. Τότε, θα αποδείξουμε ότι αληθεύει επίσης για όλες τις $(k+1)$-βέλτιστες ακολουθίες. Έστω $K = \frac{1}{2}k(k+1)$. Από την επαγωγική υπόθεση, έχουμε $c(y_0^{K-1}) \geq k$. Αν $c(y_0^{K-1}) > k$ τότε προφανώς ισχύει $c(y_0^{K+k}) \geq k+1$. Διαφορετικά, αν $c(y_0^{K-1}) = k$, τότε $c(y_0^{K+k}) > k$ από την Πρόταση 5.34. □

Από τα παραπάνω προκύπτει ότι όλες οι πεπερασμένου μήκους s-βέλτιστες ακολουθίες με πολυπλοκότητα m υπάγονται υποχρεωτικά στο σύνολο των s'-βέλτιστων ακολουθιών με $s' \leq m$. Μεταξύ αυτών, οι m-βέλτιστες ακολουθίες έχουν το χαμηλότερο λόγο συμπίεσης, όπως υποδηλώνει η Πρόταση 5.28. Επίσης, από την προηγούμενη ανάλυση γίνεται φανερό ότι κάθε υψηλά συμπιέσιμη ακολουθία σχετίζεται με τις s-βέλτιστες ακολουθίες· πράγματι, αφού για κάθε περιοδική ακολουθία y πολυπλοκότητας m, το μήκος των λέξεων που σχηματίζονται από τον LZ78 είναι μικρότερο από m (όπως προκύπτει από την Πρόταση 5.32 και από το γεγονός ότι σε μία περίοδο της y δεν μπορούν να υπάρχουν δύο ίδιες υπακολουθίες μήκους m), τότε η y μπορεί να θεωρηθεί ότι έχει προέλθει από κάποια y^s_{opt}, $s \leq m$, με κατάλληλη τροποποίηση ή προσθήκη λέξεων έτσι ώστε να προκύψει ακολουθία πολυπλοκότητας m. Άρα, η οικογένεια των s-βέλτιστων ακολουθιών με τη μικρότερη δυνατή πολυπλοκότητα s (με βάση το Πόρισμα 5.35) αποκτά ιδιαίτερη σημασία, αφού αν τροποποιηθούν ελάχιστα μπορούν να δημιουργήσουν ακολουθίες με λόγο συμπίεσης ο οποίος να προσεγγίζει το κάτω φράγμα (5.13). Αυτό αποσαφηνίζεται στο ακόλουθο παράδειγμα.

Παράδειγμα 5.36. Έστω y^{136} η 16-βέλτιστη δυαδική ακολουθία που δίνεται από την

$$y^{136} =_{\text{opt}} \langle 1,0,0,0,0,0,0,0,1,0,0,0,1,1,0,0\rangle$$

με πολυπλοκότητα 16 (η ελάχιστη δυνατή). Η περιοδική ακολουθία y η οποία έχει ως περιοδικό τμήμα της την y^{136} έχει πολυπλοκότητα 18. Έστω y^{134} η ακολουθία η οποία προκύπτει από την y^{136} αν απομακρύνουμε τα τελευταία δύο bits αυτής, και έστω $\tilde{y}$ η περιοδική επέκταση της y^{134}. Για την $\tilde{y}$ ισχύει $c(\tilde{y}) = 16$, όπως υπολογίζεται από τον αλγόριθμο του Σχήματος 5.1. Ο

Πίνακας 5.1. Απαρίθμηση όλων των s-βέλτιστων ακολουθιών πολυπλοκότητας s, για $4 \leq s \leq 15$

s	Πλήθος s-βέλτιστων ακολουθιών	s	Πλήθος s-βέλτιστων ακολουθιών
4	2	10	16
5	6	11	40
6	6	12	72
7	4	13	130
8	12	14	246
9	12	15	448

λόγος συμπίεσης της y^{134} ισούται με

$$\rho_{y^{134}} = \frac{1}{134}\sum_{i=1}^{16}\lceil \log_2(2i)\rceil = \frac{65}{134} = 0.485$$

ο οποίος προσεγγίζει το κάτω φράγμα $\frac{1}{136}\sum_{i=1}^{16}\lceil \log_2(2i)\rceil = 0.478$ το οποίο ισχύει για ακολουθίες πολυπλοκότητας 16 και περιόδου μικρότερης ή ίσης 136 (βλέπε Σημείωση 5.31). Επιπρόσθετα, η γραμμική πολυπλοκότητα της $\tilde{y}$, όπως μπορεί να υπολογιστεί από τον αλγόριθμο Berlekamp-Massey, ισούται με την περίοδο αυτής, δηλαδή 134, η οποία είναι η μέγιστη δυνατή. Αυτές οι παρατηρήσεις ενισχύουν την αξία του βαθμού συμπίεσης ως κρυπτογραφικό κριτήριο.

Το πλήθος όλων των s-βέλτιστων ακολουθιών, για $4 \leq s \leq 15$, οι οποίες έχουν πολυπλοκότητα s, αναγράφεται στον Πίνακα 5.1 - όπως αυτές υπολογίστηκαν με εξαντλητικούς ελέγχους σε υπολογιστή. Με βάση τα αποτελέσματα αυτά, εικάζουμε ότι για κάθε $s \geq 4$ υπάρχει s-βέλτιστη ακολουθία με πολυπλοκότητα την ελάχιστη δυνατή, δηλαδή s.

Κεφάλαιο 6

Δευτέρου βαθμού προσεγγίσεις λογικών συναρτήσεων

> Although this may seem a paradox, all exact science is dominated by the idea of approximation
>
> *Bertrand Russell*

Όπως έχει ήδη αναφερθεί στα κεφάλαια 1 και 2, οι λογικές συναρτήσεις χρησιμοποιούνται σε μεγάλο βαθμό σε κρυπτογραφικά συστήματα, τόσο σε αλγορίθμους ροής (ως φίλτρα ή συνδυαστές) όσο και σε αλγορίθμους τμήματος (ως μονάδες αντικατάστασης (S-boxes)). Τα κρυπτογραφικά χαρακτηριστικά αυτών των συστημάτων εξαρτώνται σε μεγάλο βαθμό από τις ιδιότητες των λογικών συναρτήσεων που ενυπάρχουν σε αυτά. Για παράδειγμα, στο Κεφάλαιο 2 αναφέρθηκε πως στους αλγορίθμους ροής η συνάρτηση ενός μη γραμμικού φίλτρου ή ενός μη γραμμικού συνδυαστή πρέπει να είναι υψηλού βαθμού, έτσι ώστε η παραγόμενη κλειδοροή να έχει υψηλή γραμμική πολυπλοκότητα. Άλλο επίσης σημαντικό κρυπτογραφικό χαρακτηριστικό των λογικών συναρτήσεων είναι η μη γραμμικότητα (ενότητα 2.5.1), η οποία πρέπει να είναι υψηλή, προκειμένου τα συστήματα να είναι ανθεκτικά σε επιθέσεις *βέλτιστων γραμμικών προσεγγίσεων (best affine approximations)* [31] και *γραμμικής κρυπτανάλυσης (linear cryptanalysis)* [101]. Πρόσφατες κρυπταναλυτικές επιθέσεις όπως οι *αλγεβρικές (algebraic attacks)* [27] και οι *επιθέσεις βάσει προσεγγίσεων χαμηλού βαθμού (low order approximation attacks)* [84] (ενότητες 2.5.2 και 2.5.3) ανέδειξαν την ανάγκη να χρησιμοποιούνται κρυπτογραφικές λογικές συναρτήσεις οι οποίες να μην μπορούν να προσεγγιστούν ικανοποιητικά από κάποια συνάρτηση χαμηλού βαθμού. Κατά συνέπεια, η αναγκαιότητα για υψηλή μη γραμμικότητα γενικεύτηκε στην απαίτηση για υψηλή *μη γραμμικότητα βαθμού r (rth order nonlinearity)*, η

οποία ορίζεται ως [76]

$$\mathcal{NL}_f^r = \min_{g \in \mathfrak{R}(r,n)} \left\{ \mathrm{wt}(f+g) \right\} . \tag{6.1}$$

Άμεση απόρροια της (6.1) είναι ο ορισμός του *προφίλ μη γραμμικότητας (nonlinearity profile)* των λογικών συναρτήσεων [17], το οποίο ορίζεται ως η ακολουθία των τιμών του $\mathcal{NL}_f^r$, για $r = 1, 2, \ldots, n-1$. Πρέπει να σημειωθεί ότι υπάρχει μία άμεση συσχέτιση μεταξύ της μη γραμμικότητας βαθμού r και της *ακτίνας κάλυψης (covering radius)* του Reed-Muller κώδικα $\mathfrak{R}(r,n)$ τάξης r. Η τελευταία ορίζεται ως ο μικρότερος ακέραιος $\rho = \rho(r,n)$ τέτοιος ώστε κάθε διάνυσμα στο $\mathbb{F}_2$ μήκους 2^n βρίσκεται σε απόσταση Hamming ρ από κάποια κωδική λέξη $\mathfrak{R}(r,n)$ [95]· κατά συνέπεια, ισχύει [9, 84]

$$\rho(r,n) = \max_{f \in \mathbb{B}_n} \min_{g \in \mathfrak{R}(r,n)} \left\{ \mathrm{wt}(f+g) \right\} . \tag{6.2}$$

Σύγκριση της (6.2) με την (6.1) οδηγεί στο συμπέρασμα ότι η ακτίνα κάλυψης $\rho(r,n)$ αντιστοιχεί στη μέγιστη δυνατή μη γραμμικότητα βαθμού r που μπορεί να έχει μία λογική συνάρτηση n μεταβλητών.

Μέχρι σήμερα, ελάχιστα αποτελέσματα είναι γνωστά όσον αφορά τις χαμηλού βαθμού προσεγγίσεις των λογικών συναρτήσεων, ακόμα και για $r = 2$ (αυτές οι προσεγγίσεις θα αναφέρονται στο υπόλοιπο του κειμένου ως *τετραγωνικές προσεγγίσεις (quadratic approximations)*). Ο υπολογισμός τόσο των βέλτιστων τετραγωνικών προσεγγίσεων μίας συνάρτησης όσο και της μη γραμμικότητας δευτέρου βαθμού είναι δύσκολο πρόβλημα στη γενική του περίπτωση [17]. Μία πρώτη αντιμετώπιση του προβλήματος υπήρξε στο [106], όπου αναπτύσσεται αλγόριθμος για την εύρεση καλών (αλλά όχι απαραίτητα βέλτιστων) τετραγωνικών προσεγγίσεων. Αλγόριθμος για τον υπολογισμό της μη γραμμικότητας δευτέρου βαθμού έχει προταθεί στο [65], όπου όμως είναι αποδοτικός μόνο για $n \leq 11$ ή, για κάποιες περιπτώσεις, για $n \leq 13$. Επίσης, για κάποιες ειδικές περιπτώσεις συναρτήσεων, έχουν αποδειχθεί κάποια (αρκετά χαμηλά) κάτω φράγματα της μη γραμμικότητας βαθμού r [18], ενώ ασυμπτωτικό άνω φράγμα της ακτίνας κάλυψης $\rho(r,n)$ για $r \geq 2$ δίνεται από τους Carlet και Mesnager στο [20]:

$$\rho(r,n) \leq 2^{n-1} - \frac{\sqrt{15}}{2}(1+\sqrt{2})^{r-2} 2^{n/2} + \mathcal{O}(n^{r-2}) .$$

Σε αυτό το κεφάλαιο παρουσιάζεται μία νέα αποδοτική αλγοριθμική τεχνική για τον υπολογισμό των βέλτιστων τετραγωνικών προσεγγίσεων για συγκεκριμένες οικογένειες συναρτήσεων βαθμού 3 και 4. Αυτό επιτυγχάνεται κάνοντας χρήση της αναπαράστασης των λογικών

συναρτήσεων βάσει του αναπτύγματος κατά Shannon (σχέση (2.20)) και υπολογίζοντας τις βέλτιστες γραμμικές προσεγγίσεις των υπεισερχομένων συναρτήσεων βαθμού 2. Για τον τελευταίο υπολογισμό αναπτύσσεται τεχνική άμεσου προσδιορισμού των βέλτιστων γραμμικών προσεγγίσεων, χωρίς να απαιτείται η χρήση του μετασχηματισμού Walsh (ενότητα 6.1). **Τα αποτελέσματα αυτά ισχύουν για συναρτήσεις οποιουδήποτε πλήθους μεταβλητών**. Η ανάλυση που ακολουθεί αναδεικνύει το ότι κάποιες γνωστές κατασκευές κρυπτογραφικών συναρτήσεων που έχουν προταθεί λόγω καλών χαρακτηριστικών (όπως για παράδειγμα κατασκευές κάποιων συναρτήσεων bent) παρουσιάζουν χαμηλή μη γραμμικότητα δευτέρου βαθμού. Κατά συνέπεια, τα αποτελέσματα αυτού του κεφαλαίου ορίζουν νέες σχεδιαστικές παραμέτρους για την κατασκευή μίας κρυπτογραφικής λογικής συνάρτησης, η μη τήρηση των οποίων μπορεί να οδηγήσει σε κρυπτογραφικές αδυναμίες των τελικών συστημάτων. Αξίζει να σημειωθεί ότι στη βιβλιογραφία έχουν προταθεί διάφορα κρυπτογραφικά συστήματα τα οποία στηρίζονται σε συναρτήσεις δευτέρου και τρίτου βαθμού λόγω της εύκολης υλοποίησής τους (όπως για παράδειγμα στα [2] και [39]). Συνεπώς, οι τεχνικές που αναπτύσσονται σε αυτό το κεφάλαιο έχουν εφαρμογή στην κρυπτανάλυση κρυπτογραφικών συστημάτων.

6.1 Βέλτιστες γραμμικές προσεγγίσεις για συναρτήσεις βαθμού 2

Σε αυτήν την ενότητα παρουσιάζονται κάποιες γνωστές ιδιότητες των τετραγωνικών συναρτήσεων, βάσει των οποίων θα αναπτυχθεί τεχνική για τον πλήρη προσδιορισμό όλων των βέλτιστων γραμμικών προσεγγίσεων για οποιαδήποτε τετραγωνική συνάρτηση. Έστω $f \in \mathbb{B}_n$ μία τετραγωνική λογική συνάρτηση και έστω $x = (x_1, \ldots, x_n)$. Τότε, η f μπορεί να εκφραστεί ως $f(x) = xQx^T + Lx^T + \epsilon$ όπου Q είναι άνω τριγωνικός πίνακας με τιμές στο $\mathbb{F}_2$, L διάνυσμα με τιμές στο $\mathbb{F}_2$, και $\epsilon \in \mathbb{F}_2$ σταθερά. Το γινόμενο xQx^T εκφράζει το *τετραγωνικό τμήμα (quadratic part)* της f, δηλαδή εκείνους τους όρους στην Αλγεβρική Κανονική Μορφή της f που έχουν βαθμό 2. Ο βαθμός (rank) του συμπλεκτικού πίνακα $B = Q + Q^T$ ισούται με $2h$ για κάποιο $1 \leq h \leq \lfloor n/2 \rfloor$ - με άλλα λόγια, ο βαθμός του πίνακα B είναι άρτιος αριθμός [95, pp. 434–442]. Το Θεώρημα του Dickson [95] βεβαιώνει ότι υπάρχει αντιστρέψιμος πίνακας $R = (r_{i,j})_{i,j=1}^n$ τέτοιος ώστε τα μη μηδενικά στοιχεία του πίνακα $\tilde{B} = (\tilde{b}_{i,j})_{i,j=1}^n = R^{-1}B(R^{-1})^T$ να βρίσκονται στις θέσεις που καθορίζονται από τη σχέση $\tilde{b}_{2i-1,2i} = \tilde{b}_{2i,2i-1} = 1$, $1 \leq i \leq h$.

Εφαρμόζοντας το μετασχηματισμό $g = xR$, η f μετατρέπεται στην ακόλουθη μορφή:

$$f = g_0 + \sum_{i=1}^{h} g_{2i-1}g_{2i}\,, \qquad \deg(g_0) \leq 1 \text{ and } \deg(g_j) = 1 \tag{6.3}$$

όπου $g_0 = \tilde{g} + \tilde{L}g^T + \epsilon$ με την $\tilde{g}$ να είναι γραμμική συνάρτηση και $\tilde{L} = L(R^{-1})^T$, ενώ οι $\{g_1, \ldots, g_{2h}\}$ είναι γραμμικές συναρτήσεις οι οποίες είναι γραμμικά ανεξάρτητες (ισχύει $g_j = \sum_{i=1}^{n} r_{i,j}x_i$ για κάθε $j = 1, 2, \ldots, 2h$). Προφανώς, για κάθε τετραγωνική συνάρτηση f, η παράμετρος $h \triangleq h_f$ είναι μονοσήμαντα ορισμένη και καθορίζεται μόνο από το τετραγωνικό τμήμα της f. Αν $h_f = 0$ τότε $f \in \mathfrak{R}(1, n)$. Η παράμετρος h_f καθορίζει τις τιμές του μετασχηματισμού Walsh της f, όπως φαίνεται στο ακόλουθο Θεώρημα.

Θεώρημα 6.1 ([95]). *Έστω $\mathcal{B}_f = \{f + v : v \in \mathfrak{R}(1, n)\}$ για μία συγκεκριμένη τετραγωνική λογική συνάρτηση $f \in \mathfrak{R}(2, n)$. Τότε, ισχύει*

$$\mathrm{wt}(f + v) = \begin{cases} 2^{n-1} - 2^{n-h_f-1}, & \text{για } 2^{2h_f} \text{ φορές;} \\ 2^{n-1}, & \text{για } 2^{n+1} - 2^{2h_f+1} \text{ φορές;} \\ 2^{n-1} + 2^{n-h_f-1}, & \text{για } 2^{2h_f} \text{ φορές.} \end{cases}$$

Το Θεώρημα 6.1 είναι γνωστό από τη Θεωρία Κωδίκων, όπου στην ουσία εκφράζει την κατανομή βαρών του $\mathfrak{R}(1, n)$ στο $\mathfrak{R}(2, n)$. Κατά συνέπεια, ο μετασχηματισμός Walsh μίας τετραγωνικής συνάρτησης f με n μεταβλητές μπορεί να πάρει τις τιμές $\{0, \pm 2^{n-h_f}\}$, δηλαδή η f είναι συνάρτηση plateaued. Λόγω της σχέσης (2.22), προκύπτει ότι η μη γραμμικότητα κάθε τετραγωνικής συνάρτησης $f \in \mathbb{B}_n$ ισούται με $2^{n-1} - 2^{n-h_f-1}$.

Στο επόμενο Θεώρημα προσδιορίζονται πλήρως οι βέλτιστες γραμμικές προσεγγίσεις κάθε τετραγωνικής συνάρτησης.

Θεώρημα 6.2. *Έστω $f \in \mathfrak{R}(2, n)$ τετραγωνική λογική συνάρτηση που δίνεται από την* (6.3). *Τότε, για $b = (b_1, \ldots, b_{2h}) \in \mathbb{F}_2^{2h_f}$ ισχύει*

$$\mathcal{A}_f = \left\{\lambda_f^b \in \mathfrak{R}(1, n) : \lambda_f^b = g_0 + \sum_{i=1}^{2h_f} b_i g_i + \sum_{i=1}^{h_f} b_{2i-1}b_{2i},\ b \in \mathbb{F}_2^{2h_f}\right\}. \tag{6.4}$$

Απόδειξη. Όλες οι συναρτήσεις λ_f^b είναι ανά δύο διαφορετικές μεταξύ τους αφού οι $\{g_1, \ldots, g_{2h}\}$ είναι γραμμικά ανεξάρτητες συναρτήσεις. Κατά συνέπεια, προκύπτει ότι το πλήθος των συναρτήσεων που ορίζονται στην (6.4) ισούται με 2^{2h_f}. Για κάθε $b \in \mathbb{F}_2^{2h_f}$, η απόσταση Hamming της λ_f^b από την f ισούται με το βάρος Hamming της ακόλουθης συνάρτησης

$$f + \lambda_f^b = \sum_{i=1}^{h_f} \left(g_{2i-1}g_{2i} + b_{2i-1}g_{2i-1} + b_{2i}g_{2i} + b_{2i-1}b_{2i}\right)$$

$f(x_1, x_2, \ldots, x_n) = \sum_{1 \le i < j \le n} a_{i,j} x_i x_j$

1 Choose $1 \le k, \ell \le n$ such that $a_{k,\ell} = 1$ and

$f = x_k(x_\ell + \sum_{j \ne k,\ell} a_{k,j} x_j) + x_\ell \sum_{i \ne k,\ell} a_{i,\ell} x_i + v$

$= (x_k + \sum_{i \ne k,\ell} a_{i,\ell} x_i)(x_\ell + \sum_{j \ne k,\ell} a_{k,j} x_j) + u$

where v, u do not depend on x_k, x_ℓ

2 $f = y_k y_\ell + u$ by setting

$\diamond$ $y_k = x_k + \sum_{i \ne k,\ell} a_{i,\ell} x_i$

$\diamond$ $y_\ell = x_\ell + \sum_{j \ne k,\ell} a_{k,j} x_j$,

$\diamond$ $y_r = x_r$ for $r \ne k, \ell$

3 Repeat for $h \le \lfloor n/2 \rfloor$ times: complexity $\mathcal{O}(n^3)$

Σχήμα 6.1. Μετασχηματισμός μίας τετραγωνικής συνάρτησης f στην ισοδύναμη αναπαράστασή της με βάση το Θεώρημα Dickson

$$= \sum_{i=1}^{h_f} \big(g_{2i-1} + b_{2i}\big)\big(g_{2i} + b_{2i-1}\big) \; . \tag{6.5}$$

Αφού οι $\{g_1 + b_2, \ldots, g_{2h_f} + b_{2h_f-1}\}$ είναι επίσης γραμμικά ανεξάρτητες, προκύπτει ότι για κάθε επιλογή του $b \in \mathbb{F}_2^{2h_f}$ ισχύει $\mathrm{wt}(f + \lambda_f^b) = 2^{n-1} - 2^{n-1-h_f}$ [95], το οποίο ισούται με τη μη γραμμικότητα της f. Επίσης, με δεδομένο ότι το πλήθος των βέλτιστων γραμμικών προσεγγίσεων της f ισούται με 2^{2h_f} (ίσο με το πλήθος των διαφορετικών λ_f^b της (6.4)), προκύπτει τελικά ότι όλες οι βέλτιστες γραμμικές προσεγγίσεις της f δίνονται από την (6.4). □

Αν και η αναπαράσταση της f στη μορφή (6.3) εξαρτάται από την επιλογή του πίνακα R, το σύνολο $\mathcal{A}_f$ της (6.4) είναι *μοναδικό*, εάν τα στοιχεία του εκφραστούν ως προς τις $x_1, \ldots, x_n$ μέσω του αντίστροφου μετασχηματισμού $x = gR^{-1}$. Το Θεώρημα 6.2 επιτρέπει τον προσδιορισμό όλων των βέλτιστων γραμμικών προσεγγίσεων μίας τετραγωνικής συνάρτησης χωρίς τη χρήση του μετασχηματισμού Walsh, καθιστώντας τη διαδικασία εύρεσης των βέλτιστων αυτών προσεγγίσεων πολύ αποτελεσματική. Πράγματι, η υπολογιστική πολυπλοκότητα του μετασχηματισμού Walsh ισούται με $\mathcal{O}(n2^n)$ (αν χρησιμοποιηθεί ο γρήγορος μετασχηματισμός Walsh (fast Walsh transform)), ενώ η πολυπλοκότητα της μεθόδου που παρουσιάζεται στο Θεώρημα 6.2 καθορίζεται μόνο από τη διαδικασία εύρεσης της αναπαράστασης (6.3)· η μεθοδολογία που ακολουθείται για τον υπολογισμό της αναπαράστασης (6.3) αποτυπώνεται στο Σχήμα 6.1 και απαιτεί χρόνο $\mathcal{O}(n^3)$ [95, pp. 438–440], [89, pp. 286], [25].

Παράδειγμα 6.3. Έστω $f \in \mathbb{B}_5$ μία τετραγωνική συνάρτηση που δίνεται από την

$$f(x_1, \ldots, x_5) = x_1x_2 + x_1x_5 + x_2x_3 + x_3x_5 + x_2 + x_4 \, .$$

Μετατρέποντας την f στην αναπαράσταση της μορφής (6.3), προκύπτει η ακόλουθη έκφραση:

$$f(x_1, \ldots, x_5) = (x_1 + x_3)(x_2 + x_5) + x_2 + x_4$$

Κατά συνέπεια, οι βέλτιστες γραμμικές προσεγγίσεις της f, όπως προσδιορίζονται μέσω του Θεωρήματος 6.2, είναι οι ακόλουθες:

$$\lambda_f^0 = x_2 + x_4 \, , \qquad \lambda_f^1 = x_1 + x_2 + x_3 + x_4 \, ,$$
$$\lambda_f^2 = x_4 + x_5 \, , \qquad \lambda_f^3 = x_1 + x_3 + x_4 + x_5 + 1 \, .$$

Σε ορισμένες περιπτώσεις, μία βέλτιστη γραμμική προσέγγιση μίας τετραγωνικής συνάρτησης μπορεί να προκύψει απευθείας από το γραμμικό της τμήμα (όπως για παράδειγμα η λ_f^0 στο παράδειγμα 6.3, η οποία ταυτίζεται με το γραμμικό τμήμα της f). Αυτό αποσαφηνίζεται στην Πρόταση 6.5 που ακολουθεί. Πρώτα παρουσιάζουμε το επόμενο, γνωστό στη βιβλιογραφία, Λήμμα [17].

Λήμμα 6.4. *Έστω $f \in \mathbb{B}_n$ και $v \in \mathfrak{R}(1, n)$. Τότε, $\lambda + v \in \mathcal{A}_{f+v}$ αν και μόνο αν $\lambda \in \mathcal{A}_f$, ενώ τα σύνολα $\mathcal{A}_{f+v}$ και $\mathcal{A}_f$ έχουν την ίδια πληθικότητα. Ισοδύναμα, $\lambda_{f+v} = \lambda_f + v$ για κάθε γραμμική συνάρτηση v και για κατάλληλη επιλογή των λ_f, λ_{f+v}.*

Πρόταση 6.5. *Έστω η τετραγωνική συνάρτηση $f \in \mathfrak{R}(2, n)$ η οποία έχει ως τετραγωνικό και γραμμικό τμήμα τα q, l αντίστοιχα - δηλαδή, $f = q + l$. Τότε, η συνάρτηση $l + \epsilon$, $\epsilon \in \mathbb{F}_2$, είναι βέλτιστη γραμμική προσέγγιση της f αν και μόνο αν η συνάρτηση q είναι ισοβαρής.*

Απόδειξη. Από το Θεώρημα 6.1 προκύπτει ότι $\widehat{\chi}_q(a) \in \left\{0, \pm 2^{n-h_f}\right\}$ για κάθε $a \in \mathbb{F}_2^n$, όπου $\widehat{\chi}_q(0) \neq 0$ αν και μόνο αν η συνάρτηση q δεν είναι ισοβαρής (λόγω της (2.21)). Άρα, αν η q είναι ισοβαρής, δηλαδή $\mathrm{wt}(q) = 2^{n-1}$, ούτε η συνάρτηση $l_1 = 0$ ούτε η $l_2 = 1$ είναι βέλτιστες γραμμικές προσεγγίσεις της q. Από την άλλη πλευρά, αν $wt(q) < 2^{n-1}$, τότε προφανώς $\widehat{\chi}_q(0) = 2^{n-h_q}$ και άρα $l_1 = 0 \in \mathcal{A}_q$, ενώ αν $wt(q) > 2^{n-1}$ τότε $\widehat{\chi}_q(0) = -2^{n-h_q}$, οπότε $l_1 = 1 \in \mathcal{A}_q$. Συνεπώς, από το Λήμμα 6.4, καταλήγουμε στο ότι η $\lambda_f = l + \epsilon$ είναι μία βέλτιστη γραμμική προσέγγιση της f αν και μόνο αν η q δεν είναι ισοβαρής. □

Πόρισμα 6.6. *Έστω $f = q + l$ συνάρτηση n μεταβλητών όπως στην Πρόταση 6.5, η οποία μπορεί να μετασχηματιστεί στην ισοδύναμη μορφή (6.3). Τότε, αν η q είναι ισοβαρής συνάρτηση, ισχύει $\tilde{g} \neq 0$.*

Απόδειξη. Λόγω της Πρότασης 6.5, αν $\mathrm{wt}(q) < 2^{n-1}$ τότε το γραμμικό τμήμα l της f αποτελεί μία βέλτιστη γραμμική προσέγγισή της, ενώ αν $\mathrm{wt}(q) > 2^{n-1}$ τότε η $l+1$ είναι μία βέλτιστη γραμμική προσέγγιση της f. Από την άλλη πλευρά, αν $\mathrm{wt}(q) = 2^{n-1}$, τότε ούτε η l ούτε η $l+1$ είναι βέλτιστες γραμμικές προσεγγίσεις της f. Έστω η αναπαράσταση (6.3) της f. Επειδή $\mathrm{wt}(\sum_{i=1}^{h_f} g_{2i-1}g_{2i}) = 2^{n-1} - 2^{n-h_f} - 1 < 2^{n-1}$, συμπεραίνουμε με ανάλογους ισχυρισμούς ότι η $g_0 = \tilde{g} + \tilde{L}g^T + \epsilon$ είναι μία βέλτιστη γραμμική προσέγγιση της f. Αν εφαρμόσουμε τον αντίστροφο μετασχηματισμό $x = gR^{-1}$ στην (6.3), το τμήμα $\tilde{L}g^T + \epsilon$ θα μετατραπεί στο γραμμικό τμήμα l της f - άρα, προκύπτει ότι $\mathrm{wt}(q) = 2^{n-1} \Rightarrow \tilde{g} \neq 0$. □

Παράδειγμα 6.7. Έστω $f \in \mathbb{B}_5$ τετραγωνική συνάρτηση με Αλγεβρική Κανονική Μορφή $f(x_1, \ldots, x_5) = x_1x_3 + x_1x_5 + x_3x_5 + x_2 + x_4$. Η συνάρτηση $q = x_1x_3 + x_1x_5 + x_3x_5$ είναι ισοβαρής. Από την προηγούμενη ανάλυση, η f μπορεί να γραφεί ως $f(x_1, \ldots, x_5) = (x_1 + x_5)(x_3 + x_5) + x_2 + x_4 + x_5$. Παρατηρούμε ότι η συνάρτηση $\tilde{g} = x_5$ προστίθεται στο γραμμικό τμήμα της f· άρα, στην αναπαράσταση κατά Dickson ισχύει $\tilde{g} = x_5 \neq 0$, κάτι που αναμενόταν λόγω του Πορίσματος 6.6. Οι βέλτιστες γραμμικές προσεγγίσεις της f, όπως προκύπτουν από το Θεώρημα 6.2, είναι οι ακόλουθες:

$$\lambda_f^0 = x_2 + x_4 + x_5\,, \qquad \lambda_f^1 = x_1 + x_2 + x_4\,,$$
$$\lambda_f^2 = x_2 + x_3 + x_4\,, \qquad \lambda_f^3 = x_1 + x_2 + x_3 + x_4 + x_5 + 1\,.$$

Αφού το τετραγωνικό τμήμα της f είναι ισοβαρές, ούτε το γραμμικό της τμήμα $x_2 + x_4$ αλλά ούτε το συμπληρωματικό του $x_2 + x_4 + 1$ είναι βέλτιστες γραμμικές προσεγγίσεις της f (Πρόταση 6.5).

Άλλα κρυπτογραφικά χαρακτηριστικά των τετραγωνικών συναρτήσεων μελετώνται στο [114].

6.2 Βέλτιστες τετραγωνικές προσεγγίσεις κυβικών συναρτήσεων

Σε αυτήν την ενότητα μελετάται η *μη γραμμικότητα δευτέρου βαθμού (second order nonlinearity)* μίας λογικής συνάρτησης f με n μεταβλητές, η οποία συμβολίζεται ως $\mathcal{NQ}_f \triangleq \mathcal{NL}_f^2$ και ορίζεται ως

$$\mathcal{NQ}_f = \min_{u \in \mathfrak{R}(2,n)} \{\mathrm{wt}(f+u)\}\,. \tag{6.6}$$

Από τις σχέσεις (2.22) και (6.6) γίνεται φανερό ότι $\mathcal{NQ}_f \leq \mathcal{NL}_f$. Κάθε τετραγωνική συνάρτηση u με την ιδιότητα $\mathrm{wt}(f+u) = \mathcal{NQ}_f$ καλείται *βέλτιστη τετραγωνική προσέγγιση (best quadratic approximation)* της f και συμβολίζεται ως ξ_f, ενώ το σύνολο όλων των βέλτιστων τετραγωνικών προσεγγίσεων της f συμβολίζεται ως $\mathcal{Q}_f \subseteq \mathfrak{R}(2,n)$.

Λήμμα 6.8. *Έστω $f, g \in \mathfrak{R}(3,n)$ κυβικές λογικές συναρτήσεις με το ίδιο κυβικό τμήμα. Τότε, ισχύει $\mathcal{NQ}_f = \mathcal{NQ}_g$.*

Απόδειξη. Από τον ορισμό της μη γραμμικότητας δευτέρου βαθμού προκύπτει ότι αν $\xi_f \in \mathcal{Q}_f$, τότε ισχύει $\mathcal{NQ}_f = \mathrm{wt}(f+\xi_f) \leq \mathrm{wt}(f+u)$ για κάθε $u \in \mathfrak{R}(2,n)$. Η συνάρτηση $f+g$ είναι δευτέρου βαθμού, λόγω του ότι οι f και g έχουν το ίδιο κυβικό τμήμα. Κατά συνέπεια, θέτοντας $u = (f+g)+\xi_g$ καταλήγουμε στο ότι $\mathcal{NQ}_f \leq \mathrm{wt}(g+\xi_g) = \mathcal{NQ}_g$. Με ανάλογο τρόπο μπορούμε επίσης να εξάγουμε τη σχέση $\mathcal{NQ}_g \leq \mathcal{NQ}_f$. Άρα, συμπεραίνουμε ότι $\mathcal{NQ}_f = \mathcal{NQ}_g$. □

Το Λήμμα 6.8 αποτελεί ουσιαστικά γενίκευση του Λήμματος 6.4 για την τετραγωνική περίπτωση. Με αντίστοιχους ισχυρισμούς μπορεί να αποδειχτεί η ακόμα γενικότερη περίπτωση: αν προσθέσουμε μία συνάρτηση βαθμού το πολύ r σε μία συνάρτηση f με $\deg(f) > r$, τότε η $\mathcal{NL}_f^r$ παραμένει αμετάβλητη (μία ιδιότητα ήδη γνωστή - [17]).

Για τις βέλτιστες τετραγωνικές προσεγγίσεις συναρτήσεων οποιουδήποτε βαθμού ισχύει η ακόλουθη Πρόταση.

Πρόταση 6.9. *Έστω $f \in \mathbb{B}_n$ μία λογική συνάρτηση με βαθμό $r > 2$, και έστω $f = f_0 \|_j f_1$ για κάποιο $1 \leq j \leq n$, τέτοιο ώστε να υπάρχουν $\xi_{f_0} \in \mathcal{Q}_{f_0}$ και $\xi_{f_1} \in \mathcal{Q}_{f_1}$ που να έχουν το ίδιο τετραγωνικό τμήμα. Τότε, $u = \xi_{f_0} \|_j \xi_{f_1} \in \mathcal{Q}_f$.*

Απόδειξη. Για την συνάρτηση u, η οποία είναι προφανώς βαθμού 2, ισχύει $\mathrm{wt}(f+u) = \mathcal{NQ}_{f_0} + \mathcal{NQ}_{f_1}$. Επίσης, για οποιαδήποτε άλλη τετραγωνική συνάρτηση $u' = u'_0 \|_j u'_1$, όπου οι $u'_0, u'_1 \in \mathbb{B}_{n-1}$ έχουν το ίδιο τετραγωνικό τμήμα, ισχύει $\mathrm{wt}(f+u') = \mathrm{wt}(f_0+u'_0)+\mathrm{wt}(f_1+u'_1) \geq \mathcal{NQ}_{f_0} + \mathcal{NQ}_{f_1}$. Άρα, $u \in \mathcal{Q}_f$. □

Στη συνέχεια εισάγουμε την ακόλουθη ομαδοποίηση των συναρτήσεων βαθμού 3.

Ορισμός 6.10. Μία κυβική λογική συνάρτηση $f \in \mathfrak{R}(3,n)$ καλείται *συνάρτηση κλάσης-m (class-m function) αν m είναι ο μικρότερος ακέραιος με την ακόλουθη ιδιότητα: υπάρχει σύνολο $\mathcal{J} = \{j_1, \ldots, j_m\}$, $1 \leq j_1 < \cdots < j_m \leq n$, τέτοιο ώστε κάθε όρος βαθμού 3 σε κάποια συνάρτηση $f' \in \{g : g = f(Ax+b)\}$, όπου A αντιστρέψιμος $n \times n$ πίνακας, να περιλαμβάνει τουλάχιστον μία μεταβλητή με δείκτη στο σύνολο $\mathcal{J}$.*

Κάθε κυβική λογική συνάρτηση $f \in \mathbb{B}_n$ τέτοια ώστε $2^{n-3} \leq \mathrm{wt}(f) < 2^{n-2}$ μπορεί να γραφεί, υπό κάποιον γραμμικό μετασχηματισμό, σε κάποια από τις ακόλουθες μορφές [69],[95, p. 446]:

1. $x_1(x_2x_3 + \cdots + x_{2\mu}x_{2\mu+1})$, for $1 \leq \mu \leq \lfloor (n-1)/2 \rfloor$;
2. $x_1x_2x_3 + x_4x_5x_6$, for $n \geq 6$.

Με βάση τον Ορισμό 6.10, οι παραπάνω δύο οικογένειες είναι συναρτήσεις κλάσης-1 και κλάσης-2, με $\mathcal{J} = \{1\}$ και $\mathcal{J} = \{1, 4\}$ αντίστοιχα. Στη γενική περίπτωση, το σύνολο $\mathcal{J}$ δεν είναι μοναδικό για μία δοθείσα συνάρτηση, αφού πολλές από τις $\binom{n}{m}$ δυνατές επιλογές του $\mathcal{J}$ είναι πιθανό να ικανοποιούν τη συνθήκη του Ορισμού 6.10. Αν $2^{n-3} \leq \mathrm{wt}(f) < 2^{n-2} + 2^{n-4}$, τότε το πλήθος των οικογενειών στις οποίες μπορεί να υπάγεται μία κυβική συνάρτηση αυξάνει· ωστόσο, όλες αυτές οι συναρτήσεις είναι κλάσης-m, όπου $1 \leq m \leq 3$ [70]. Από τον Ορισμό 6.10, προκύπτει ότι κάθε κυβική συνάρτηση ανήκει σε μία μόνο κλάση. Επίσης, από τον Ορισμό 6.10 προκύπτει άμεσα η ακόλουθη Πρόταση.

Πρόταση 6.11. *Κάθε συνάρτηση $f \in \mathfrak{R}(3, n)$ κλάσης-m, όπου $\mathcal{J} = \{j_1, \ldots, j_m\}$, ικανοποιεί τις ακόλουθες ιδιότητες:*

1. *Έστω $\mathcal{J}' \subset \mathcal{J}$ με πληθικότητα k, $1 \leq k \leq m-1$. Τότε, όλες οι υπο-συναρτήσεις $f_i \in \mathbb{B}_{n-k}$ στο ανάπτυγμα $f = f_0 \,\|_{\mathcal{J}'}\, \cdots \,\|_{\mathcal{J}'}\, f_{2^k-1}$ είναι κλάσης-$(m-k)$ κυβικές συναρτήσεις με το ίδιο κυβικό τμήμα.*
2. *Ο αριθμός m είναι ο μικρότερος ακέραιος τέτοιος ώστε στο ανάπτυγμα $f = f_0 \,\|_{\mathcal{J}}\, \cdots \,\|_{\mathcal{J}}\, f_{2^m-1}$ όλες οι υπο-συναρτήσεις f_i, $0 \leq i < 2^m$, έχουν βαθμό μικρότερο από 3.*

Μία υπο-οικογένεια των κυβικών συναρτήσεων κλάσης-m αποτελούν οι *διαχωρίσιμες συναρτήσεις κλάσης-m (separable class-m functions)*, στις οποίες κάθε όρος βαθμού 3 περιέχει *ακριβώς μία* μεταβλητή με δείκτη στο σύνολο $\mathcal{J}$. Με άλλα λόγια, το κυβικό τμήμα αυτών των συναρτήσεων δίνεται από τη σχέση $c = \sum_{i=1}^{m} x_{j_i} q_i$, όπου οι συναρτήσεις $q_i \in \mathbb{B}_{n-m}$ είναι βαθμού 2 και δεν εξαρτώνται από καμία μεταβλητή που να σχετίζεται με το σύνολο $\mathcal{J}$. Το επόμενο Λήμμα περιγράφει μία ιδιότητα που χαρακτηρίζει το ανάπτυγμα κατά Shannon των διαχωρίσιμων συναρτήσεων.

Λήμμα 6.12. *Έστω $f \in \mathfrak{R}(3, n)$ μία διαχωρίσιμη συνάρτηση κλάσης-m, με κυβικό τμήμα $c = \sum_{i=1}^{m} x_{j_i} q_i$, όπου, για κάθε i, η $q_i \in \mathbb{B}_{n-m}$ είναι τετραγωνική συνάρτηση που δεν εξαρτάται από καμία μεταβλητή της οποίας ο δείκτης να ανήκει στο $\mathcal{J} = \{j_1, \ldots, j_m\}$. Τότε,*

εφαρμόζοντας το ανάπτυγμα $f = f_0 \parallel_{\mathcal{J}} \cdots \parallel_{\mathcal{J}} f_{2^m-1}$ *προκύπτει*

$$f_r = q + \langle r, p\rangle + l_r\,, \qquad 0 \le r < 2^m \tag{6.7}$$

όπου η $q \in \mathbb{B}_{n-m}$ *είναι τετραγωνική συνάρτηση και οι* $l_r \in \mathbb{B}_{n-m}$ *γραμμικές, με* $p = (q_1, \ldots, q_m)$ *και* $r = (r_1, \ldots, r_m)$ *η δυαδική αναπαράσταση του ακέραιου* r*.*

Απόδειξη. Η συνάρτηση f γράφεται ως $f = c + q + l$, όπου τα c, q, και l είναι το κυβικό, τετραγωνικό, και γραμμικό της τμήμα αντίστοιχα. Από την υπόθεση, η f είναι κυβική συνάρτηση κλάσης-m, άρα από τον Ορισμό 6.10 εχουμε ότι $q_1, \ldots, q_m \neq 0$. Επίσης, οι συναρτήσεις q_i είναι γραμμικά ανεξάρτητες· πράγματι, ας θεωρήσουμε ότι υπάρχουν $a_1, \ldots, a_m \in \mathbb{F}_2$, χωρίς να είναι ταυτόχρονα όλα μηδενικά, τέτοια ώστε $a_1q_1 + \cdots + a_mq_m = 0$ και, χωρίς βλάβη της γενικότητας, $a_m = 1$. Τότε, θα έχουμε $c = (x_{j_1} + a_1x_{j_m})q_1 + \cdots + (x_{j_{m-1}} + a_{m-1}x_{j_m})q_{m-1}$, και υπάρχει ένας αντιστρέψιμος γραμμικός μετασχηματισμός τέτοιος ώστε η f να γίνεται κυβική συνάρτηση κλάσης-$(m-1)$—άτοπο (ο μετασχηματισμός με αυτήν την ιδιότητα αντιστοιχίζει το $x_{j_i} + a_ix_{j_m}$ στο x_{j_i} για κάθε $1 \le i < m$, ενώ αφήνει όλες τις υπόλοιπες μεταβλητές αναλλοίωτες). Αντίστοιχα, το τετραγωνικό και το γραμμικό τμήμα της f γράφονται

$$q = \sum_{i=1}^{m-1}\sum_{k=i+1}^{m} x_{j_i}x_{j_k}\epsilon_{i,k} + \sum_{i=1}^{m} x_{j_i}l_i + q' \quad \text{και} \quad l = \sum_{i=1}^{m} x_{j_i}\epsilon_i + l' \tag{6.8}$$

για κάποια τετραγωνική συνάρτηση $q' \in \mathbb{B}_{n-m}$ και γραμμικές συναρτήσεις $l', l_i \in \mathbb{B}_{n-m}$ που δεν εξαρτώνται από τα $x_{j_1}, \ldots, x_{j_m}$. Στη συνέχεια θεωρούμε τις συναρτήσεις

$$g^s = \left(\sum_{i=1}^{s} x_{j_i}q_i\right) + \left(\sum_{i=1}^{s-1}\sum_{k=i+1}^{s} x_{j_i}x_{j_k}\epsilon_{i,k} + \sum_{i=1}^{s} x_{j_i}l_i + q'\right) + \left(\sum_{i=1}^{s} x_{j_i}\epsilon_i + l'\right)$$

όπου οι παρενθέσεις χρησιμοποιούνται για να διαχωρίσουν το κυβικό, τετραγωνικό και γραμμικό τμήμα αντίστοιχα. Ισχύει $g^m = f$, $g^0 = q' + l'$ και

$$h_i^s = \sum_{k=1}^{s} x_{j_k}\epsilon_{k,i} + \sum_{k=i+1}^{m} r_k\epsilon_{i,k}\,, \qquad 0 \le s < i \le m$$

όπου $r_k \in \mathbb{F}_2$. Εφαρμόζοντας το ανάπτυγμα κατά Shannon, στο πρώτο βήμα θα έχουμε $f = f_0 \parallel_{j_m} f_1$, όπου $f_{r_m} = g^{m-1} + r_m(q_m + l_m + \epsilon_m + h_m^{m-1})$ για $r_m = 0, 1$. Εφαρμόζοντας ξανά το ανάπτυγμα κατά Shannon για αυτές τις υπο-συναρτήσεις, προκύπτει $f = (f_0 \parallel_{j_{m-1}} f_1) \parallel_{j_m} (f_2 \parallel_{j_{m-1}} f_3)$, όπου

$$f_r = g^{m-2} + \sum_{i=m-1}^{m} r_i\big(q_i + l_i + \epsilon_i + h_i^{m-2}\big)\,, \qquad 0 \le r < 4$$

και $r = r_{m-1} + 2r_m$ είναι η δυαδική αναπαράσταση του ακέραιου r. Συνεχίζοντας με τον ίδιο τρόπο, κατασκευάζουμε το ανάπτυγμα $f = f_0 \parallel_{\mathcal{J}} \cdots \parallel_{\mathcal{J}} f_{2^m-1}$, όπου για όλα τα $0 \leq r < 2^m$ θα ισχύει

$$f_r = q' + \sum_{i=1}^{m} r_i q_i + \left(l' + \sum_{i=1}^{m} r_i \big(l_i + \epsilon_i + \textstyle\sum_{k=i+1}^{m} r_k \epsilon_{i,k} \big) \right) \tag{6.9}$$

και $r = r_1 + 2r_2 + \cdots + 2^{m-1} r_m$ είναι η δυαδική αναπαράσταση του ακέραιου r. Άρα, η (6.7) προκύπτει με την παρατήρηση ότι η παράσταση εντός της παρένθεσης στην (6.9) αντιστοιχεί στο l_r, το q' αντιστοιχεί στο q, και $\langle r, p \rangle = \sum_{i=1}^{m} r_i q_i$. □

Οι κυβικές συναρτήσεις κλάσης-1 χαρακτηρίζονται από την ιδιότητα ότι μία μεταβλητή τους είναι παρούσα σε όλους τους όρους της συνάρτησης με βαθμό 3. Άρα, αν x_j είναι η εν λόγω μεταβλητή, το ανάπτυγμα κατά Shannon της f ως προς τη μεταβλητή x_j είναι της μορφής

$$f = (q + l_0) \parallel_j (q + q_j + l_1), \tag{6.10}$$

όπου $\deg(q_j) = 2$, $\deg(q) \leq 2$ και $\deg(l_0) = \deg(l_1) = 1$ (ουσιαστικά, η κυβική συνάρτηση $x_j q_j$ αποτελεί το κυβικό τμήμα της f). Στο ακόλουθο Θεώρημα αναδεικνύεται μία αποδοτική αλγοριθμική τεχνική για τον υπολογισμό όλων των βέλτιστων τετραγωνικών προσεγγίσεων για κάθε κυβική συνάρτηση αυτής της κατηγορίας.

Θεώρημα 6.13. *Έστω κυβική λογική συνάρτηση κλάσης-1 n μεταβλητών, η οποία περιγράφεται από την (6.10). Τότε, κάθε βέλτιστη τετραγωνική προσέγγιση της f ανήκει σε μία από τις παρακάτω οικογένειες:*

i. $\xi_f^0 = (q + l_0) \parallel_j (q + l_1 + \lambda_{q_j})$,

ii. $\xi_f^1 = (q + q_j + l_0 + \lambda_{q_j}) \parallel_j (q + q_j + l_1)$.

Απόδειξη. Αρχικά, σημειώνουμε ότι κάθε λογική συνάρτηση ξ που ανήκει στην οικογένεια είτε της ξ_f^0 είτε της ξ_f^1 είναι πράγματι τετραγωνική, αφού εφαρμόζοντας σε αυτήν το ανάπτυγμα κατά Shannon ως προς τη μεταβλητή x_j προκύπτουν υπο-συναρτήσεις με το ίδιο τετραγωνικό τμήμα. Ας θεωρήσουμε στη συνέχεια μία τετραγωνική συνάρτηση $\xi \in \mathbb{B}_n$ που ανήκει στην οικογένεια της ξ_f^0. Τότε, ισχύει $f + \xi = 0 \parallel_j (q_j + \lambda_{q_j})$, από την οποία σχέση οδηγούμαστε στο ακόλουθο

$$\mathrm{wt}(f + \xi) = \mathrm{wt}(q_j + \lambda_{q_j}) = \mathcal{NL}_{q_j}$$

αφού η λ_{q_j} είναι βέλτιστη γραμμική προσέγγιση της $q_j \in \mathfrak{R}(2, n-1)$. Άρα, από το Θεώρημα 6.1, προκύπτει ότι $\mathrm{wt}(f + \xi) = 2^{n-2} - 2^{n-2-h_{q_j}}$. Με ανάλογους ισχυρισμούς μπορεί εύκολα να

αποδειχτεί ότι το ίδιο ισχύει για κάθε συνάρτηση της οικογένειας ξ_f^1. Κατά συνέπεια, όλες οι τετραγωνικές συναρτήσεις των οικογενειών ξ_f^0, ξ_f^1 απέχουν την ίδια απόσταση Hamming από την f.

Στη συνέχεια, θα αποδείξουμε ότι η απόσταση Hamming οποιασδήποτε άλλης τετραγωνικής συνάρτησης από την f είναι μεγαλύτερη από $2^{n-2} - 2^{n-2-h_{q_j}}$. Έστω ότι υπάρχει συνάρτηση $u \in \mathfrak{R}(2,n)$, που δεν ανήκει σε καμία από τις οικογένειες των ξ_f^0, ξ_f^1, τέτοια ώστε

$$\mathrm{wt}(f+u) \leq 2^{n-2} - 2^{n-2-h_{q_j}} \ . \tag{6.11}$$

Εφαρμόζοντας στην τετραγωνική συνάρτηση u το ανάπτυγμα κατά Shannon ως προς τη μεταβλητή x_j, τότε η u γράφεται ως $u = u_0 \parallel_j u_1$ με $u_i = q' + l_i'$ όπου q' είναι το τετραγωνικό τμήμα της u_i και l_i' το γραμμικό τμήμα της u_i για $i = 1, 2$ (οι u_0, u_1 έχουν το ίδιο τετραγωνικό τμήμα q'). Από την υπόθεση προκύπτει ότι $q' \neq q, q+q_j$, γιατί αν $q' = q$ $(q' = q + q_j)$, τότε η συνάρτηση u θα ανήκε στην οικογένεια της ξ_f^0 (ξ_f^1)· πράγματι, αν ίσχυε $q' = q$, θα είχαμε $\mathrm{wt}(f+u) = \mathrm{wt}(l_0 + l_0') + \mathrm{wt}(q_j + l_1 + l_1')$, το οποίο ελαχιστοποιείται αν και μόνο αν ισχύουν ταυτόχρονα $l_0' = l_0$ και $l_1' \in \mathcal{A}_{q_j + l_1}$, οπότε και θα είχαμε

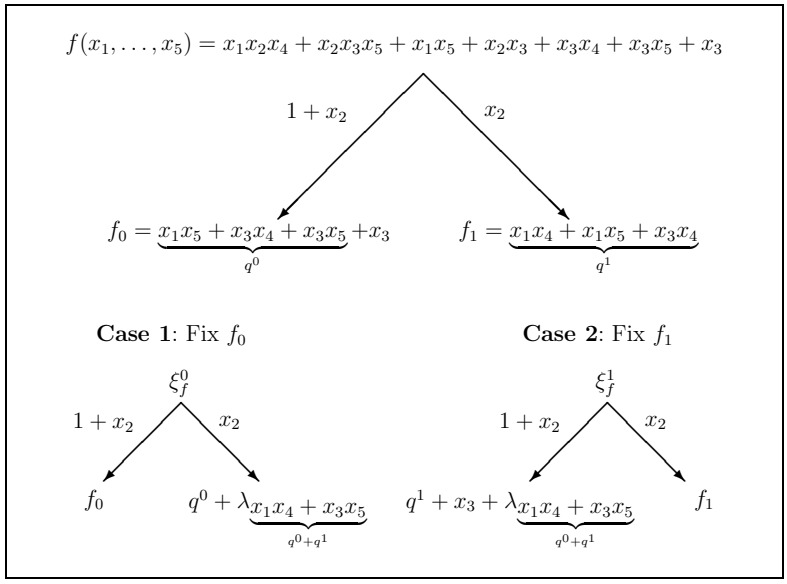
$$\mathrm{wt}(f+u) = \mathrm{wt}(l_0 + l_0) + \mathrm{wt}(q_j + l_1 + \lambda_{q_j+l_1}) = \mathcal{NL}_{q_j+l_1} = \mathcal{NL}_{q_j} \ .$$

Κατά συνέπεια, έχουμε ότι $u = (q + l_0) \parallel_j (q + l_1 + \lambda_{q_j})$—άτοπο. Στο ίδιο άτοπο θα καταλήγαμε με όμοιο τρόπο αν κάναμε την υπόθεση $q' = q + q_j$. Άρα, πράγματι ισχύει $q' \neq q, q+q_j$, και έχουμε

$$\begin{aligned} \mathrm{wt}(f+u) &= \mathrm{wt}(q' + q + l_0' + l_0) + \mathrm{wt}(q' + q + q_j + l_1' + l_1) \\ &\geq \mathrm{wt}(q' + q + \lambda_{q'+q}) + \mathrm{wt}(q' + q + q_j + \lambda_{q'+q+q_j}) \\ &= 2^{n-1} - 2^{n-2-h_{q'+q}} - 2^{n-2-h_{q'+q+q_j}} \end{aligned}$$

με την ισότητα να ισχύει αν και μόνο αν $l_i' + l_i \in \mathcal{A}_{q'+q+iq_j} \Leftrightarrow l_i' \in \mathcal{A}_{q'+q+iq_j+l_i}$ για $i = 0, 1$, λόγω του Λήμματος 6.4. Ακόμα και αν το q' είναι τέτοιο ώστε $h_{q'+q} = h_{q'+q+q_j} = 1$ (οπότε και το βάρος Hamming της $f+u$ ελαχιστοποιείται), θα ισχύει $\mathrm{wt}(f+u) = 2^{n-2} > 2^{n-2} - 2^{n-2-h_{q_j}}$ για κάθε $1 \leq h_{q_j} \leq \lfloor (n-1)/2 \rfloor$. □

Πόρισμα 6.14. *Με το συμβολισμό του Θεωρήματος 6.13, για κάθε κυβική συνάρτηση f κλάσης-1 n μεταβλητών, η δευτέρου βαθμού μη γραμμικότητά της ισούται με $\mathcal{NQ}_f = 2^{n-2} - 2^{n-2-h_{q_j}}$, για κάποιο $1 \leq h_{q_j} \leq \lfloor (n-1)/2 \rfloor$.*



Σχήμα 6.2. Διάγραμμα υπολογισμού των βέλτιστων τετραγωνικών προσεγγίσεων της κυβικής συνάρτησης f του παραδείγματος 6.15

Το Θεώρημα 6.13 είναι σημαντικό γιατί επιτρέπει τον προσδιορισμό όλων των τετραγωνικών προσεγγίσεων μίας οποιασδήποτε κυβικής συνάρτησης n μεταβλητών, υπολογίζοντας τις βέλτιστες γραμμικές προσεγγίσεις μίας τετραγωνικής συνάρτησης $n-1$ μεταβλητών - κάτι που μπορεί να γίνει άμεσα χρησιμοποιώντας το Θεώρημα 6.2.

Παράδειγμα 6.15. Έστω η κυβική συνάρτηση

$$f(x_1,\ldots,x_5) = x_1x_2x_4 + x_2x_3x_5 + x_1x_5 + x_2x_3 + x_3x_4 + x_3x_5 + x_3\ .$$

Προφανώς η f είναι κλάσης-1, συνεπώς οι βέλτιστες τετραγωνικές προσεγγίσεις της μπορούν να υπολογιστούν από το Θεώρημα 6.13, όπου $\mathcal{J} = \{2\}$. Κατά συνέπεια, η f γράφεται ως

$$f = f_0 \parallel_2 f_1 = (x_1x_5 + x_3x_4 + x_3x_5 + x_3) \parallel_2 (x_1x_4 + x_1x_5 + x_3x_4)$$

οπότε μένει ο υπολογισμός των βέλτιστων γραμμικών προσεγγίσεων της τετραγωνικής συνάρτησης $q_2 = x_1x_4 + x_3x_5$. Από το Θεώρημα 6.2 μπορούν άμεσα να υπολογιστούν οι $2^{2h_{q_2}} = 2^{2\times 2} = 16$ βέλτιστες γραμμικές προσεγγίσεις της q_2. Το Σχήμα 6.2 αποτυπώνει τη διαδικασία υπολογισμού των βέλτιστων τετραγωνικών προσεγγίσεων της f, όπως αυτή περιγράφεται στο Θεώρημα 6.13. Όλες οι βέλτιστες τετραγωνικές προσεγγίσεις της f αναγράφονται στην αριστερή στήλη του πίνακα 6.1. Για κάθε λ_{q_2}, ο πίνακας 6.1 αναγράφει τις αντίστοιχες βέλτιστες τετραγωνικές προσεγγίσεις της κυβικής συνάρτησης f. Είναι εύκολο να δούμε ότι $\mathcal{NQ}_f = \mathcal{NL}_{q_2} = 6$ (αφού $h_{q_2} = 2$).

Πίνακας 6.1. Υπολογισμός όλων των βέλτιστων τετραγωνικών προσεγγίσεων της κυβικής συνάρτησης f του Παραδείγματος 6.15

λ_{q_2}	ξ_f^0	ξ_f^1
0	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_3 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 +$ $x_2x_3 + x_3$
x_5	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_3 + x_2x_5 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 +$ $x_2x_3 + x_2x_5 + x_3 + x_5$
x_3	$x_1x_5 + x_3x_4 + x_3x_5 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4$
$x_3 + x_5 +$ 1	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_5 + x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 +$ $x_2x_5 + x_2 + x_5 + 1$
x_4	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_3 + x_2x_4 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 +$ $x_2x_3 + x_2x_4 + x_3 + x_4$
$x_4 + x_5$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_3 + x_2x_4 + x_2x_5 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_2x_3 +$ $x_2x_4 + x_2x_5 + x_3 + x_4 + x_5$
$x_3 + x_4$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_4 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 +$ $x_2x_4 + x_4$
$x_3 + x_4 +$ $x_5 + 1$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_4 + x_2x_5 + x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_2x_4 +$ $x_2x_5 + x_2 + x_4 + x_5 + 1$
x_1	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_3 + x_1x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 +$ $x_2x_3 + x_1x_2 + x_1 + x_3$
$x_1 + x_5$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_2x_3 + x_2x_5 + x_1x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_2x_3 +$ $x_1x_2 + x_2x_5 + x_1 + x_3 + x_5$
$x_1 + x_3$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_1x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 +$ $x_1x_2 + x_1$
$x_1 + x_3 +$ $x_5 + 1$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_1x_2 + x_2x_5 + x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_1x_2 +$ $x_2x_5 + x_1 + x_2 + x_5 + 1$
$x_1 + x_4 +$ 1	$x_1x_5 + x_3x_4 + x_3x_5 + x_2x_3 +$ $x_1x_2 + x_2x_4 + x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_2x_3 +$ $x_1x_2 + x_2x_4 + \sum_{i=1}^{4} x_i + 1$
$x_1 + x_4 +$ $x_5 + 1$	$x_1x_5 + x_3x_4 + x_3x_5 + x_2x_3 +$ $x_1x_2 + x_2x_4 + x_2x_5 + x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_2x_3 +$ $x_1x_2 + x_2x_4 + x_2x_5 + \sum_{i=1}^{5} x_i + 1$
$x_1 + x_3 +$ $x_4 + 1$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_1x_2 + x_2x_4 + x_2 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_1x_2 +$ $x_2x_4 + x_1 + x_2 + x_4 + 1$
$x_1 + x_3 +$ $x_4 + x_5$	$x_1x_5 + x_3x_4 + x_3x_5 +$ $x_1x_2 + x_2x_4 + x_2x_5 + x_3$	$x_1x_4 + x_1x_5 + x_3x_4 + x_1x_2 +$ $x_2x_4 + x_2x_5 + x_1 + x_4 + x_5$

Στη συνέχεια, αποδεικνύουμε ότι για τη γενικότερη περίπτωση μίας κυβικής συνάρτησης κλάσης-m, με $m \geq 2$, οι βέλτιστες τετραγωνικές προσεγγίσεις της δεν μπορούν να υπολογι-

στούν με χρήση των βέλτιστων τετραγωνικών προσεγγίσεων των κλάσης-1 υπο-συναρτήσεών της.

Πρόταση 6.16. *Με το συμβολισμό του Λήμματος 6.12, έστω $f \in \mathbb{B}_n$ μία διαχωρίσιμη συνάρτηση κλάσης-2 με $\mathcal{J} = \{i, j\}$ και έστω $f = f_0 \parallel_j f_1$. Τότε, δεν υπάρχει ζευγάρι συναρτήσεων $(\xi_{f_0}, \xi_{f_1}) \in \mathcal{Q}_{f_0} \times \mathcal{Q}_{f_1}$ που να έχουν το ίδιο τετραγωνικό τμήμα.*

Απόδειξη. Από την απόδειξη του Λήμματος 6.12 γίνεται φανερό ότι η f γράφεται ως $f = (x_i q_i + x_j q_j) + (x_i x_j \epsilon_{i,j} + x_i l_i + x_j l_j + q') + (x_i \epsilon_i + x_j \epsilon_j + l')$, όπου οι παρενθέσεις υποδηλώνουν το κυβικό, τετραγωνικό και γραμμικό τμήμα αντίστοιχα. Ανακαλώντας την Πρόταση 6.11, οι f_0, f_1 είναι κυβικές συναρτήσεις κλάσης-1 και, από το Λήμμα 6.12, προκύπτει ότι

$$f_0 = (q' + l_0) \parallel_i (q' + q_i + l_1) \tag{6.12a}$$

$$f_1 = (q' + q_j + l_2) \parallel_i (q' + q_i + q_j + l_3) \tag{6.12b}$$

όπου $l_{r_i + 2r_j} = l' + r_i(l_i + \epsilon_i) + r_j(l_j + \epsilon_j) + r_i r_j \epsilon_{i,j}$ και $r_i, r_j \in \mathbb{F}_2$. Άρα, οι βέλτιστες τετραγωνικές προσεγγίσεις τως f_0, f_1, όπως αυτές υπολογίζονται από το Θεώρημα 6.13, είναι

$$\begin{aligned}
\xi^0_{f_0} &= q' + x_i(l_0 + l_1 + \lambda_{q_i}) + l_0 \,, \\
\xi^1_{f_0} &= q' + q_i + x_i(l_0 + l_1 + \lambda_{q_i}) + l_0 + \lambda_{q_i} \,, \\
\xi^0_{f_1} &= q' + q_j + x_i(l_2 + l_3 + \lambda_{q_i}) + l_2 \,, \\
\xi^1_{f_1} &= q' + q_i + q_j + x_i(l_2 + l_3 + \lambda_{q_i}) + l_2 + \lambda_{q_i} \,.
\end{aligned}$$

Ακόμα και αν ισχύει $l_2 + l_3 = l_0 + l_1 + \epsilon_{i,j}$ (οπότε οι τετραγωνικοί όροι των $\xi^0_{f_0}, \xi^1_{f_0}, \xi^0_{f_1}, \xi^1_{f_1}$ που εμπεριέχουν τη μεταβλητή x_i συμπίπτουν), τα τετραγωνικά τμήματα των $\xi^0_{f_0}, \xi^1_{f_0}, \xi^0_{f_1}, \xi^1_{f_1}$ δεν είναι ποτέ κοινά λόγω του ότι $q_i, q_j \neq 0$ και $q_i \neq q_j$ (όπως αναδεικνύεται και στην απόδειξη του Λήμματος 6.12). □

Συνδυάζοντας την Πρόταση 6.16 με την Πρόταση 6.9, γίνεται σαφές ότι μπορούμε να κατασκευάσουμε κυβική συνάρτηση f κλάσης-2 τέτοια ώστε $\mathcal{NQ}_f > max_{\text{class-1}}\{\mathcal{NQ}\}$: αυτό μπορεί να επιτευχθεί με τη συνένωση δύο συναρτήσεων κλάσης-1, με την κάθε μία από αυτές να έχει τη μέγιστη δυνατή μη γραμμικότητα δευτέρου βαθμού, όπως αυτή προσδιορίζεται από το Πόρισμα 6.14. Με βάση αυτό το σκεπτικό μπορεί αναδρομικά να κατασκευαστεί επίσης συνάρτηση g κλάσης-m, $m > 2$, τέτοια ώστε $\mathcal{NQ}_g > max_{\text{class-1}}\{\mathcal{NQ}\}$. Άρα, από την παραπάνω ανάλυση οδηγούμαστε στο συμπέρασμα ότι οι συναρτήσεις κλάσης-1 είναι σε γενικές γραμμές οι πιο "ασθενείς" σε σχέση με άλλες κυβικές συναρτήσεις, όσον αφορά τη χαμηλή μη γραμμικότητα δευτέρου βαθμού.

6.3 Γενίκευση για συναρτήσεις υψηλότερου βαθμού

Σε αυτήν την ενότητα εξετάζονται βέλτιστες προσεγγίσεις συναρτήσεων βαθμού μεγαλύτερου από 3, χρησιμοποιώντας τα συναφή αποτελέσματα των προηγούμενων ενοτήτων. Αρχικά, παρουσιάζουμε το ακόλουθο Θεώρημα, το οποίο προσδιορίζει βέλτιστες τετραγωνικές προσεγγίσεις για συγκεκριμένη οικογένεια συναρτήσεων βαθμού 4.

Θεώρημα 6.17. *Έστω $f \in \mathfrak{R}(4,n)$ μία λογική συνάρτηση βαθμού 4, όπου υπάρχει $1 \leq j \leq n$, τέτοιο ώστε, αν $f = f_0 \parallel_j f_1$, η f_0 είναι κυβική συνάρτηση κλάσης-1 και η $f_1 = q + l$ είναι τετραγωνική συνάρτηση, όπου τα q, l υποδηλώνουν το τετραγωνικό και το γραμμικό της τμήμα αντίστοιχα. Αν $\mathcal{NL}_{f_0+q} \leq 2^{n-2} - 2^{n-4}$, τότε οι συναρτήσεις*

$$u = (q + \lambda_{f_0+q}) \parallel_j f_1 \tag{6.13}$$

είναι βέλτιστες τετραγωνικές προσεγγίσεις της f και $\mathcal{NQ}_f = \mathcal{NL}_{f_0+q}$. Διαφορετικά, ισχύει $\mathcal{NQ}_f > 2^{n-2} - 2^{n-4}$.

Απόδειξη. Κάθε συνάρτηση της μορφής (6.13) είναι προφανώς τετραγωνική, αφού οι υποσυναρτήσεις που προκύπτουν από το ανάπτυγμά της κατά Shannon ως προς τη μεταβλητή x_j έχουν το ίδιο τετραγωνικό τμήμα. Επιπρόσθετα, ισχύει $\mathrm{wt}(f+u) = \mathrm{wt}\big((f_0 + q + \lambda_{f_0+q}) \parallel_j 0\big) = \mathcal{NL}_{f_0+q}$, το οποίο, λόγω της υπόθεσης, είναι μικρότερο ή ίσο του $2^{n-2} - 2^{n-4}$. Κατά συνέπεια, αρκεί να αποδείξουμε ότι $\mathrm{wt}(f+u') \geq 2^{n-2} - 2^{n-4}$ για κάθε τετραγωνική συνάρτηση u' η οποία δεν ανήκει στην οικογένεια συναρτήσεων που περιγράφει η (6.13). Κάθε τέτοια συνάρτηση u' γράφεται ως $u' = (q'+l_0) \parallel_j (q'+l_1)$, όπου $q' \in \mathbb{B}_{n-1}$ είναι τετραγωνική συνάρτηση με $q' \neq q$ και οι $l_0, l_1 \in \mathbb{B}_{n-1}$ είναι γραμμικές συναρτήσεις. Με αυτόν το συμβολισμό, έχουμε

$$\mathrm{wt}(f+u') = \mathrm{wt}(f_0 + q' + l_0) + \mathrm{wt}(q + q' + l + l_1) \geq \mathcal{NL}_{f_0+q'} + \mathcal{NL}_{q+q'}$$

με την ισότητα να ισχύει αν και μόνο αν $l_0 \in \mathcal{A}_{f_0+q'}$ και $l_1 \in \mathcal{A}_{q+q'+l}$. Αφού $q + q' \in \mathbb{B}_{n-1}$, από το Θεώρημα 6.1 προκύπτει $\mathcal{NL}_{q+q'} \geq 2^{n-3}$. Επίσης, λόγω του Πορίσματος 6.14 έχουμε ότι $\mathcal{NL}_{f_0+q'} \geq 2^{n-4}$ αφού η συνάρτηση $f_0 + q' \in \mathbb{B}_{n-1}$ είναι κυβική συνάρτηση κλάσης-1. Συνεπώς, συμπεραίνουμε ότι $\mathrm{wt}(f+u') \geq 3\,2^{n-4} = 2^{n-2} - 2^{n-4}$. □

Παρατήρηση 6.18. Το Θεώρημα 6.17 ισχύει ακόμα και αν η f_0 είναι τετραγωνική και η f_1 κυβική συνάρτηση κλάσης-1. Σε αυτήν την περίπτωση, η (6.13) γίνεται $u = f_0 \parallel_j (q + \lambda_{f_1+q})$ και $\mathcal{NQ}_f = \mathcal{NL}_{f_1+q}$ αν $\mathcal{NL}_{f_1+q} \leq 2^{n-2} - 2^{n-4}$.

Παράδειγμα 6.19. Έστω $f \in \mathbb{B}_5$ μία συνάρτηση βαθμού 4 που δίνεται από την

$$f(x_1,\ldots,x_5) = x_2 + x_4 + x_1x_2 + x_1x_4 + x_1x_5 + x_4x_5 + x_1x_2x_4 + x_1x_3x_4 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + x_1x_2x_3x_4 + x_1x_2x_3x_5 \,.$$

Εφαρμόζοντας το ανάπτυγμα κατά Shannon ως προς τη μεταβλητή x_1, η f γράφεται ως $f = (x_2x_3x_4 + x_2x_3x_5 + x_4x_5 + x_2 + x_4) \parallel_1 (x_2x_4 + x_3x_4 + x_5) = f_0 \parallel_1 f_1$. Συνεπώς, ο υπολογισμός των βέλτιστων τετραγωνικών προσεγγίσεων της f ανάγεται, λόγω του Θεωρήματος 6.17, στον προσδιορισμό βέλτιστων γραμμικών προσεγγίσεων της $f_0+x_2x_4+x_3x_4$ μέσω του μετασχηματισμού Walsh, οι οποίες είναι οι $\lambda = x_3 + x_4 + x_5$ και $\lambda' = x_2$. Αφού ισχύει $\mathcal{NL}_{f_0+x_2x_4+x_3x_4} = 4 < 3\,2^{5-4}$, προκύπτει ότι οι βέλτιστες τετραγωνικές προσεγγίσεις της f είναι οι

$$\xi_f = x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4 + x_3 + x_4 + x_5 \,,$$
$$\xi'_f = x_1x_2 + x_1x_5 + x_2x_4 + x_3x_4 + x_2 \,,$$

και ισχύει $\mathcal{NQ}_f = 4$.

Πρόταση 6.20. *Έστω $f \in \mathbb{B}_n$ μία λογική συνάρτηση βαθμού r, και έστω ότι υπάρχει σύνολο $\mathcal{J} = \{j_1,\ldots,j_{r-3}\}$ τέτοιο ώστε αν $f = f_0 \parallel_{\mathcal{J}} \cdots \parallel_{\mathcal{J}} f_{2^{r-3}-1}$, τότε η f_i είναι κυβική συνάρτηση κλάσης-1 για κάποιο $0 \le i < 2^{r-3}$ και $f_k \in \mathfrak{R}(2, n-r+3)$ για όλα τα $k \neq i$. Τότε, ισχύει $2^{n-r} \le \mathcal{NL}_f^{r-1} \le 2^{n-r+1} - 2^{\lceil (n-r)/2 \rceil}$.*

Απόδειξη. Έστω $f' = f_0 \parallel_{\mathcal{J}} \cdots \parallel_{\mathcal{J}} f_{i-1} \parallel_{\mathcal{J}} \xi_{f_i} \parallel_{\mathcal{J}} f_{i+1} \parallel_{\mathcal{J}} \cdots \parallel_{\mathcal{J}} f_{2^{r-3}-1}$, η οποία προκύπτει από την f αντικαθιστώντας την υποσυνάρτηση f_i με μία βέλτιστη τετραγωνική της προσέγγιση ξ_{f_i}. Τότε, ισχύει $\deg(f') = r-1$ και $\mathrm{wt}(f+f') = \mathcal{NQ}_{f_i}$. Αφού $f_i \in \mathbb{B}_{n-r+3}$, εφαρμόζοντας το Πόρισμα 6.14 καταλήγουμε στη σχέση

$$2^{n-r} \le \mathcal{NQ}_{f_i} \le 2^{n-r+1} - 2^{\lceil (n-r)/2 \rceil} \,.$$

Επίσης, δεν υπάρχει συνάρτηση $u' \in \mathfrak{R}(r-1,n)$ τέτοια ώστε $\mathrm{wt}(f+u') < 2^{n-r}$, αφού $\deg(f+u') = r$ και, κατά συνέπεια, το βάρος της $f+u'$ είναι μεγαλύτερο ή ίσο του 2^{n-r} [95]· έτσι, καταλήγουμε στην ορθότητα του ισχυρισμού. □

6.4 Δευτέρου βαθμού προσεγγίσεις σε γνωστές συναρτήσεις

Από την παραπάνω ανάλυση γίνεται σαφές ότι κάθε κατασκευή κρυπτογραφικών συναρτήσεων η οποία βασίζεται σε συνένωση άλλων συναρτήσεων χαμηλότερου βαθμού με λιγότερες

μεταβλητές πρέπει να γίνεται με ιδιαίτερη προσοχή, όσον αφορά τα χαρακτηριστικά των υποσυναρτήσεων αυτών που επιλέγονται - κι αυτό γιατί οι τελικές συναρτήσεις που κατασκευάζονται μπορεί να είναι ευάλωτες σε επιθέσεις προσέγγισης χαμηλού βαθμού. Στη βιβλιογραφία έχουν ήδη προταθεί διάφορες κατασκευές κρυπτογραφικών συναρτήσεων που εμπίπτουν σε αυτές τις σχεδιαστικές αρχές. Σε αυτήν την ενότητα λοιπόν μελετώνται αυτές οι κατασκευές όσον αφορά τη μη γραμμικότητα δευτέρου βαθμού των συναρτήσεων που παράγονται.

6.4.1 Κατασκευή Maiorana-McFarland

Έστω n θετικός ακέραιος, $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ μία συνάρτηση αντικατάστασης πάνω στα στοιχεία του διανυσματικού χώρου $\mathbb{F}_2^n$ και $g : \mathbb{F}_2^n \to \mathbb{F}_2$ μία οποιαδήποτε λογική συνάρτηση. Τότε, η $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \simeq \mathbb{F}_2^{2n} \to \mathbb{F}_2$, η οποία ορίζεται ως

$$f(x, y) = \langle x, \phi(y) \rangle + g(y) , \qquad x, y \in \mathbb{F}_2^n \tag{6.14}$$

είναι μία *συνάρτηση Maiorana-McFarland* [30]. Είναι γνωστό ότι όλες οι συναρτήσεις αυτής της μορφής είναι bent (με τον μέγιστο δυνατό βαθμό αν η g επιλεγεί κατάλληλα). Επιπρόσθετα, η f μπορεί να θεωρηθεί ως συνένωση 2^n γραμμικών υποσυναρτήσεων n μεταβλητών [16]. Όπως αναδεικνύεται στη συνέχεια, η δευτέρου βαθμού μη γραμμικότητα για κυβικές Maiorana-McFarland συναρτήσεις είναι πολύ χαμηλή σε κάποιες περιπτώσεις, παρόλο που η γραμμικότητά τους είναι η μέγιστη δυνατή.

Η διαφορά που εμφανίζεται μεταξύ των μη γραμμικοτήτων πρώτου και δευτέρου βαθμού στις Maiorana-McFarland συναρτήσεις είναι εμφανής ακόμα και για μικρές τιμές του n. Ας θεωρήσουμε την ειδική περίπτωση όπου η ϕ είναι ένας γραμμικός αντιστρέψιμος μετασχηματισμός, οπότε η $\langle x, \phi(y) \rangle$ είναι βαθμού 2. Τότε, αν $n = 3$, προκύπτει ότι η g (άρα και η f) είναι κυβική συνάρτηση κλάσης-1 και οι μη γραμμικότητες πρώτου και δευτέρου βαθμού για την f είναι 28 and 8 αντίστοιχα, λόγω του Πορίσματος 6.14. Αντίστοιχες παρατηρήσεις μπορούν να γίνουν και για συναρτήσεις υψηλότερου βαθμού οι οποίες προκύπτουν από την (6.14)· η συμπεριφορά αυτή οφείλεται στο ότι η μη γραμμικότητα δευτέρου βαθμού της f καθορίζεται από τη μη γραμμικότητα δευτέρου βαθμού της g, η οποία αποτελείται απο λιγότερες μεταβλητές. Αυτό αποσαφηνίζεται στο ακόλουθο παράδειγμα.

Παράδειγμα 6.21. Έστω $f \in \mathbb{B}_8$ βαθμού 4 που δίνεται από την (6.14), όπου ϕ ο μετασχηματισμός που διατηρεί όλες τις μεταβλητές αναλλοίωτες και $g = x_5x_6x_7x_8 + x_5x_7x_8 + x_6x_7$ - δηλαδή,

$$f = x_5x_6x_7x_8 + x_5x_7x_8 + x_1x_5 + x_2x_6 + x_3x_7 + x_4x_8 + x_6x_7 .$$

Τότε, $f = f_0 \parallel_5 f_1$, όπου

$$f_0(x_1, \ldots, x_8) = x_2x_6 + x_3x_7 + x_4x_8 + x_6x_7 \,,$$
$$f_1(x_1, \ldots, x_8) = x_6x_7x_8 + x_2x_6 + x_3x_7 + x_4x_8 + x_6x_7 + x_7x_8 + x_1 \,,$$

και η f_1 είναι κυβική συνάρτηση κλάσης-1. Ανακαλώντας τη Σημείωση 6.18 και την (2.21), βρίσκουμε ότι η x_1 είναι μία βέλτιστη γραμμική προσέγγιση της συνάρτησης $f_0 + f_1 = x_6x_7x_8 + x_7x_8 + x_1$ και $\mathcal{NL}_{f_0+f_1} = 16 < 48 = 2^{8-2} - 2^{8-4}$. Άρα, λόγω της Παρατήρησης 6.18 προκύπτει ότι η συνάρτηση $\xi_f = f_0 \parallel_5 (f_0 + x_1) = x_1x_5 + x_2x_6 + x_3x_7 + x_4x_8 + x_6x_7$ είναι μία βέλτιστη τετραγωνική προσέγγιση της f με $\mathcal{NQ}_f = 16$. Αφού η f είναι συνάρτηση bent, η μη γραμμικότητά της είναι η μέγιστη δυνατή, δηλαδή $\mathcal{NL}_f = 2^{8-1} - 2^{8/2-1} = 120$.

Στις περιπτώσεις που μελετήθηκαν μέχρι τώρα, η μη γραμμικότητα δευτέρου βαθμού των Maiorana-McFarland συναρτήσεων δεν είναι υψηλή, ενώ επιπλέον ο ταχύς υπολογισμός των βέλτιστων τετραγωνικών προσεγγίσεών τους είναι εφικτός. Γίνεται φανερό λοιπόν ότι υψηλή μη γραμμικότητα δεν εξασφαλίζει υψηλή μη γραμμικότητα δευτέρου βαθμού. Η συμπεριφορά αυτή δείχνει να βελτιώνεται για τις *γενικευμένες Maiorana-McFarland συναρτήσεις (general Maiorana-McFarland functions)* [12]. Αυτές οι συναρτήσεις κατασκευάζονται ως εξής: για άρτιο $n = r + s$ με $r \leq s$, οποιαδήποτε αντιστρέψιμη συνάρτηση $\phi : \mathbb{F}_2^s \to \mathbb{F}_2^r$ και οποιαδήποτε συνάρτηση $g : \mathbb{F}_2^s \to \mathbb{F}_2$, ορίζεται η συνάρτηση $f : \mathbb{F}_2^s \times \mathbb{F}_2^r \simeq \mathbb{F}_2^n \to \mathbb{F}_2$ που περιγράφεται από τη σχέση

$$f(x, y) = \big\langle x, \phi(y) \big\rangle + g(y) = \sum_{i=1}^{r} x_i\phi_i(y) + g(y) \,, \qquad x \in \mathbb{F}_2^r,\ y \in \mathbb{F}_2^s \,. \tag{6.15}$$

Τότε, η f είναι συνάρτηση bent αν για κάθε $a \in \mathbb{F}_2^r$ το σύνολο $\phi^{-1}(a)$ είναι γραμμικός υπόχωρος του $\mathbb{F}_2^s$ διάστασης $n - 2r$, και αν (για την περίπτωση όπου $n > 2r$) ο περιορισμός της g στο $\phi^{-1}(a)$ είναι συνάρτηση bent για κάθε $a \in \mathbb{F}_2^r$ (αν $n = 2r$, κανένας περιορισμός για την επιλογή της g δεν απαιτείται) [16]. Επίσης, αν κάθε στοιχείο του $\phi(\mathbb{F}_2^s)$ έχει βάρος Hamming μεγαλύτερο από k, τότε η f είναι ανθεκτική σε συσχετίσεις τάξης m, για $m \geq k$. Μία τέτοια κατασκευή παρουσιάζεται στο ακόλουθο παράδειγμα.

Παράδειγμα 6.22. Στο [12] κατασκευάζεται, μέσω της γενικευμένης Maiorana-McFarland κατασκευής, η ακόλουθη συνάρτηση $f \in \mathbb{B}_7$ που είναι ισοβαρής, ανθεκτική σε συσχετίσεις τάξης 2 και έχει βαθμό 4 (τον μέγιστο δυνατό):

$$f = \ x_1x_5x_6x_7 + x_4x_5x_6x_7 + x_1x_5x_6 + x_1x_5x_7 +$$

$$x_2x_5x_6 + x_2x_5x_7 + x_3x_5x_7 + x_4x_5x_7 + x_1x_6 +$$
$$x_1x_7 + x_2x_5 + x_3x_5 + x_2x_6 + x_2x_7 + x_1 + x_3 + x_4$$

Η συνάρτηση f μπορεί να γραφεί ως $f = f_0 \,\|_5\, f_1$, όπου

$$\begin{aligned} f_0 &= x_1x_6 + x_1x_7 + x_2x_6 + x_2x_7 + x_1 + x_3 + x_4 \\ &= q + x_1 + x_3 + x_4, \\ f_1 &= x_1x_6x_7 + x_4x_6x_7 + x_3x_7 + x_4x_7 + x_1 + x_2 + x_4, \end{aligned}$$

όπου $q = x_1x_6 + x_1x_7 + x_2x_6 + x_2x_7$. Για τη συνάρτηση $f_1 + q$ υπολογίζουμε, μέσω του μετασχηματισμού Walsh, ότι $\mathcal{NL}_{f_1+q} = 24 = 2^{7-2} - 2^{7-4}$, οπότε μπορούμε να χρησιμοποιήσουμε τη Σημείωση 6.18 για τον υπολογισμό βέλτιστων τετραγωνικών προσεγγίσεων της f. Για παράδειγμα, μπορούμε να υπολογίσουμε ότι $x_4 \in \mathcal{A}_{f_1+q}$, άρα μία βέλτιστη τετραγωνική προσέγγιση της f δίνεται από τη σχέση

$$\xi_f = f_0 \,\|_5\, (q + x_4) = q + x_1x_5 + x_3x_5 + x_1 + x_3 + x_4$$

και, προφανώς, έχουμε $\mathcal{NQ}_f = 24$.

6.4.2 Κατασκευή Charpin-Pasalic-Tavernier

Στο [22] έχει προταθεί μία κατασκευή συναρτήσεων bent βαθμού 3, η οποία βασίζεται στη συνένωση δύο τετραγωνικών semi-bent συναρτήσεων $f_b, f_c \in \mathbb{B}_n$ για περιττό ακέραιο n, όπου για τα διανύσματα b, c ισχύει $\mathrm{wt}(b) \not\equiv \mathrm{wt}(c) \pmod 2$, και κάθε συνάρτηση είναι της μορφής

$$f_a(x) = \sum_{i=1}^{(n-1)/2} a_i \,\mathrm{tr}\big(x^{2^i+1}\big)\,, \qquad x \in \mathbb{F}_{2^n} \text{ and } a \in \mathbb{F}_2^{(n-1)/2} \tag{6.16}$$

όπου $a = (a_1, \ldots, a_{(n-1)/2})$ και $\mathrm{tr}(x) = x + x^2 + \cdots + x^{2^{n-1}}$ είναι η συνάρτηση ίχνους, η οποία αντιστοιχίζει στοιχεία του σώματος $\mathbb{F}_{2^n}$ στο $\mathbb{F}_2$ (βλέπε ενότητα 2.3). Υπό αυτήν τη θεώρηση, κατασκευάζεται η συνάρτηση bent $f \in \mathbb{B}_{n+1}$ μέσω της συνένωσης $f = f_b \,\|\, f_c$, η οποία προφανώς είναι κυβική συνάρτηση κλάσης-1. Στη συνέχεια, αποδεικνύουμε ότι με αυτήν την κατασκευή μπορούν να προκύψουν συναρτήσεις bent βαθμού 3 με τη μέγιστη δυνατή μη γραμμικότητα δευτέρου βαθμού.

Πρόταση 6.23. *Με τον παραπάνω συμβολισμό, έστω $f_b, f_c \in \mathbb{B}_{n+1}$ τετραγωνικές συναρτήσεις semi-bent τέτοιες ώστε η $f_b + f_c$ να είναι semi-bent συνάρτηση βαθμού 2. Τότε, η μη γραμμικότητα δευτέρου βαθμού της κλάσης-1 κυβικής bent συνάρτησης $f = f_b \,\|\, f_c$ ισούται με $\mathcal{NQ}_f = 2^{n-1} - 2^{(n-1)/2} = \max_{class\text{-}1}\{\mathcal{NQ}\}$.*

Απόδειξη. Από το Θεώρημα 6.13 προκύπτει ότι η λογική συνάρτηση $\xi_f^0 = f_b \parallel (f_b + \lambda_{f_b+f_c})$ είναι μία βέλτιστη τετραγωνική προσέγγιση της f και η μη γραμμικότητα δευτέρου βαθμού της f ισούται με $\mathcal{NQ}_f = \mathcal{NL}_{f_b+f_c} = 2^{n-1} - 2^{(n-1)/2}$, αφού $h_{f_b+f_c} = (n-1)/2$ (λόγω του ότι ο ακέραιος n είναι περιττός και η $f_b + f_c$ είναι semi-bent συνάρτηση στο $\mathbb{B}_n$). Ανακαλώντας το Πόρισμα 6.14, αυτή είναι η μέγιστη δυνατή μη γραμμικότητα δευτέρου βαθμού που μπορεί να έχει μία οποιαδήποτε κλάσης-1 κυβική συνάρτηση $n+1$ μεταβλητών. □

Γενίκευση της παραπάνω διαδικασίας έχει προταθεί στα [13, 22], έτσι ώστε να προκύπτουν συναρτήσεις τόσο bent όσο και semi-bent οποιουδήποτε βαθμού. Πιο συγκεκριμένα, για κάθε δύο συναρτήσεις bent $f, f' \in \mathbb{B}_{n+1}$, με n περιττό ακέραιο, τέτοιες ώστε $f = f_b \parallel f_c$ και $f' = f_d \parallel f_e$, όπου οι f_b, f_c, f_d, f_e είναι τετραγωνικές semi-bent συναρτήσεις της μορφής (6.16), τα $\mathrm{wt}(b), \mathrm{wt}(d)$ είναι περιττοί αριθμοί και τα $\mathrm{wt}(c), \mathrm{wt}(e)$ άρτιοι, κατασκευάζονται οι συναρτήσεις

$$g = f \parallel f' \in \mathbb{B}_{n+2} \quad \text{and} \quad g' = f \parallel f' \parallel (1+f) \parallel f' \in \mathbb{B}_{n+3}\,. \tag{6.17}$$

Τότε η g είναι semi-bent και η g' συνάρτηση bent· ο βαθμός τους είναι 4 αν $f_b + f_c + f_d + f_e \neq 0$. Αυτή η διαδικασία συνένωσης συναρτήσεων μπορεί να συνεχιστεί αναδρομικά, κατασκευάζοντας συναρτήσεις bent και semi-bent οποιουδήποτε βαθμού.

Πρόταση 6.24. *Για τις συναρτήσεις g, g' που περιγράφονται στην* (6.17)*, η μη γραμμικότητα δευτέρου βαθμού ικανοποιεί τις σχέσεις $\mathcal{NQ}_g \geq \mathcal{NQ}_f + \mathcal{NQ}_{f'}$ και $\mathcal{NQ}_{g'} \geq 2\big(\mathcal{NQ}_f + \mathcal{NQ}_{f'}\big)$.*

Απόδειξη. Άμεση απόρροια της Πρότασης 6.9 και του Λήμματος 6.8, αφού η f και η $1+f$ έχουν την ίδια μη γραμμικότητα δευτέρου βαθμού. □

Αν στην παραπάνω κατασκευή θεωρήσουμε ότι $f_e = f_b + f_c + f_d$, τότε οι g, g' γίνονται κυβικές συναρτήσεις με $g = f_b + x_{n+1}(f_b + f_c) + x_{n+2}(f_b + f_d)$ και $g' = g + x_{n+3}(1 + x_{n+2})$. Κατά συνέπεια, συνεχίζοντας με ανάλογο τρόπο, μπορούμε να κατασκευάσουμε κυβικές συναρτήσεις κλάσης-m, για $m > 2$, των οποίων η μη γραμμικότητα δευτέρου βαθμού είναι μεγαλύτερη από αυτήν της Πρότασης 6.23.

6.4.3 Κατασκευή Siegenthaler

Ο Siegenthaler στο [129] εισάγει για πρώτη φορά τον ορισμό της ανθεκτικότητας σε συσχετίσεις για μία λογική συνάρτηση και προτείνει μία αναδρομική διαδικασία κατασκευής τέτοιων συναρτήσεων. Η κατασκευή βασίζεται στην ιδιότητα ότι αν $g, g' \in \mathbb{B}_n$ είναι ανθεκτικές σε

συσχετίσεις τάξης m, τότε η συνάρτηση $f = g' \parallel g \in \mathbb{B}_{n+1}$ είναι επίσης ανθεκτική σε συσχετίσεις τάξης m. Με αυτόν τον τρόπο μπορούν να κατασκευαστούν συναρτήσεις ανθεκτικές τάξης m με n μεταβλητές, για οποιουσδήποτε ακεραίους $1 \leq m < n-2$, οι οποίες να έχουν το μέγιστο δυνατό βαθμό $n-m-1$ (αν $m = n-2$, τότε η προκύπτουσα συνάρτηση είναι γραμμική· κατασκευές για αυτές τις συναρτήσεις δεν έχουν νόημα). Η κατασκευή που προτείνεται λαμβάνει χώρα μέσα σε $n-m-2$ βήματα· κάθε βήμα έχει ως αφετηρία μία συνάρτηση g η οποία έχει προέλθει από το προηγούμενο βήμα και είναι ανθεκτική σε συσχετίσεις τάξης m, και στη συνέχεια υπολογίζεται η $g' = g \circ \pi$ η οποία προκύπτει από την g με αντιμετάθεση των μεταβλητών της, βάσει κάποιας συνάρτησης αντιμετάθεσης $\pi \in \mathcal{P}_n$ (η π είναι κατάλληλα επιλεγμένη έτσι ώστε οι μεγιστοβάθμιοι όροι των g, g' να μη συμπίπτουν πλήρως)· από τις g, g' κατασκευάζεται εν συνεχεία η $g' \parallel g$, για την οποία ισχύει $\deg(g' \parallel g) = \deg(g) + 1$.

Στο αρχικό βήμα της όλης διαδικασίας, επιλέγεται η γραμμική συνάρτηση $g(x_1, \ldots, x_{m+2}) = x_1 + \cdots + x_{m+1}$ η οποία είναι ανθεκτική τάξης m, ενώ ως συνάρτηση αντιμετάθεσης π επιλέγεται εκείνη που απλά αντιμεταθέτει τις μεταβλητές x_{m+1}, x_{m+2}. Κατά συνέπεια, δοθείσης της παραπάνω g, προκύπτει η $g'(x_1, \ldots, x_{m+2}) = x_1 + \cdots + x_m + x_{m+2}$. Έτσι, στο τέλος του πρώτου σταδίου, έχουμε τη δευτέρου βαθμού συνάρτηση $g \parallel g'$ που έχει $m+3$ μεταβλητές και είναι ανθεκτική τάξης m. Για τα επόμενα βήματα προχωράμε όπως ακριβώς περιγράφεται παραπάνω. Όταν όλη η κατασκευή ολοκληρωθεί, λαμβάνουμε συνάρτηση n μεταβλητών που είναι ανθεκτική τάξης m, με το μέγιστο δυνατό βαθμό $n-m-1$ (αξίζει να σημειωθεί ότι, αρχίζοντας την κατασκευή από γραμμικές συναρτήσεις που είναι πάντα ισοβαρείς, η τελική συνάρτηση είναι επίσης ισοβαρής).

Είναι εύκολο να δειχθεί ότι η f που κατασκευάζεται ανωτέρω είναι ουσιαστικά η συνένωση 2^{n-m-2} συναρτήσεων με $m+2$ μεταβλητές. Επίσης, αν η f είναι ανθεκτική σε συσχετίσεις τάξης $n-4$, τότε είναι κυβική κλάσης-1 συνάρτηση όπως αυτό προκύπτει από την Πρόταση 6.11. Κατά συνέπεια, *υψηλή ανθεκτικότητα σε συσχετίσεις δεν εξασφαλίζει υψηλή μη γραμμικότητα δευτέρου βαθμού*. Επιπλέον, αν δεν γίνει προσεχτική επιλογή των συναρτήσεων-μεταθέσεων σε κάθε βήμα, είναι πιθανό να προκύπτουν τελικές συναρτήσεις μεγάλου βαθμού για τις οποίες ωστόσο ο υπολογισμός των βέλτιστων τετραγωνικών προσεγγίσεών τους να είναι εφικτός - κάτι που βέβαια δεν είναι επιθυμητό για κρυπτογραφικές εφαρμογές. Αυτή η περίπτωση περιγράφεται στο ακόλουθο παράδειγμα.

Παράδειγμα 6.25. Στο [129] κατασκευάζεται μία λογική συνάρτηση $f \in \mathbb{B}_7$ βαθμού 4, η οποία είναι ανθεκτική τάξης 2. Η κατασκευή ξεκινάει από τη γραμμική συνάρτηση $g(x_1, \ldots, x_4) =$

$x_1 + x_2 + x_3$ και ολοκληρώνεται μετά από 3 βήματα, όπου στο i-ιοστό βήμα ($i = 1, 2, 3$) εφαρμόζεται η συνάρτηση μετάθεσης π_i. Για κάθε βήμα, χρησιμοποιούνται αντίστοιχα οι συναρτήσεις

- $\pi_1 : (1, 2, 3, 4) \rightarrow (1, 2, 4, 3)$,
- $\pi_2 : (1, 2, 3, 4, 5) \rightarrow (2, 4, 3, 5, 1)$,
- $\pi_3 : (1, 2, 3, 4, 5, 6) \rightarrow (3, 4, 5, 6, 1, 2)$.

Μόλις ολοκληρωθεί το δεύτερο βήμα (και πριν εφαρμόσουμε τη μετάθεση π_3), έχουμε την ακόλουθη κυβική συνάρτηση κλάσης-1:

$$\begin{aligned} g =& x_1x_4x_6 + x_1x_5x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_4 + \\ & x_1x_5 + x_1x_6 + x_3x_6 + x_4x_6 + x_5x_6 + x_2 + x_3 + x_5 \ . \end{aligned}$$

Κάνοντας χρήση του Θεωρήματος 6.13, προκύπτει ότι η συνάρτηση $\xi_g = x_1x_4 + x_1x_5 + x_1x_6 + x_3x_6 + x_4x_6 + x_5x_6 + x_2 + x_3 + x_5$ είναι μία βέλτιστη τετραγωνική προσέγγιση της g. Αν στο τρίτο βήμα χρησιμοποιήσουμε τη μετάθεση $\pi_3' : (1, 2, 3, 4, 5, 6) \rightarrow (1, 2, 3, 5, 4, 6)$ αντί για την π_3, η οποία μετάθεση π_3' ικανοποιεί επίσης τους περιορισμούς που θέτει ο Siegenthaler στην κατασκευή του, τότε μπορούμε εύκολα να δούμε ότι η συνάρτηση g' που θα προκύψει από την g θα έχει ως βέλτιστη τετραγωνική προσέγγιση την $\xi_{g'} = \xi_g + x_4 + x_5$, η οποία έχει το ίδιο τετραγωνικό τμήμα με την ξ_g. Άρα, λόγω της Πρότασης 6.9, η συνάρτηση $\xi_f = \xi_{g'} \parallel \xi_g$ είναι μία βέλτιστη τετραγωνική προσέγγιση της $f = g' \parallel g$, με $\mathcal{NQ}_f = 24$.

6.4.4 Αλγόριθμος ροής Achterbahn

Ο αλγόριθμος ροής Achterbahn είναι ένας από τους αλγορίθμους που υποβλήθηκαν στο eSTREAM project ως υποψήφιος για προτυποποίηση [39]. Η σχεδίασή του βασίζεται σε 8 μη γραμμικούς καταχωρητές ολίσθησης με ανάδραση, με μεγέθη από 22 μέχρι 31, οι έξοδοι των οποίων συνδυάζονται από τη συνάρτηση-συνδυαστή:

$$f(x_1, \ldots, x_8) = x_1 + x_2 + x_3 + x_4 + x_5x_7 + x_6x_7 + x_6x_8 + x_5x_6x_7 + x_6x_7x_8$$

Η πρώτη αυτή έκδοση αποδείχτηκε μη ασφαλής [64]· η κρυπτανάλυση που προτάθηκε βασίστηκε στην όχι καλή συνάρτηση-συνδυαστή f (παρατηρήθηκε ότι αν $x_5 = x_6 = 0$, τότε η f γίνεται γραμμική), καθώς επίσης και στη μικρή περίοδο των ακολουθιών που παράγει κάθε ένας από τους 8 FSRs (λόγω των μικρών μηκών τους). Ως απάντηση στην επίθεση [64],

οι κατασκευαστές του Achterbahn πρότειναν μία δεύτερη βελτιωμένη έκδοση, γνωστή ως Acterbahn-version 2 [40]. Η δεύτερη αυτή έκδοση χρησιμοποιεί 10 FSRs αντί για 8, ενώ η συνάρτηση-συνδυαστής είναι μεγαλύτερη όσον αφορά το πλήθος των όρων στην Αλγεβρική Κανονική Μορφή της (και, φυσικά, το πλήθος των μεταβλητών της). Και η δεύτερη έκδοση του Achterbahn ωστόσο υπέστη επιτυχή κρυπτανάλυση [50], η οποία βασίστηκε στη χρήση κάποιας τετραγωνικής προσέγγισης για τη συνάρτηση-συνδυαστή (χωρίς να αποσαφηνίζεται αν είναι βέλτιστη τετραγωνική προσέγγιση ούτε ο τρόπος με τον οποίο αυτή υπολογίστηκε). Η τελευταία έκδοση του Achterbahn καλείται Acterbahn-128/80 [41], όπου στην ουσία είναι δύο διαφορετικές παραλλαγές, μία με μήκος κλειδιού 80 bits και μία με 128 bits. Όμως και αυτή η τελευταία έκδοση υπέστη επιτυχή κρυπτανάλυση [51, 113], βελτιώνοντας τις τεχνικές κρυπτανάλυσης του [50]. Ο Achterbahn δεν επελέγη τελικά για τη συνέχεια της τρίτης φάσης του eStream project (η οποία είναι σε εξέλιξη τη στιγμή που γράφονται αυτές οι γραμμές).

Είναι εύκολο να δει κανείς ότι η συνάρτηση-συνδυαστής f στην πρώτη έκδοση του Achterbahn είναι μία κυβική συνάρτηση κλάσης-1. Στην κρυπτανάλυση [64] χρησιμοποιήθηκε η γραμμική προσέγγιση $v = x_1 + x_2 + x_3 + x_4 + x_6$, για την οποία ισχύει $\mathrm{wt}(f + v) = 64$ (με άλλα λόγια, ισχύει $f = u$ με πιθανότητα $3/4$). Επειδή η f είναι κλάσης-1, μπορούμε να υπολογίσουμε όλες τις βέλτιστες τετραγωνικές προσεγγίσεις της με βάση το Θεώρημα 6.13 - για παράδειγμα, μία εξ αυτών θα είναι

$$\begin{aligned}\xi_f &= (x_5x_7 + x_1 + x_2 + x_3 + x_4) \parallel_6 (x_5x_7 + \lambda_{x_7x_8+x_5x_7+x_1+x_2+x_3+x_4+x_7+x_8}) \\ &= x_5x_7 + x_6x_8 + x_1 + x_2 + x_3 + x_4,\end{aligned}$$

όπου θέσαμε $\lambda_{x_7x_8+x_5x_7+x_1+x_2+x_3+x_4+x_7+x_8} = x_1 + x_2 + x_3 + x_4 + x_8$. Άρα, ισχύει $\mathcal{NQ}_f = \mathrm{wt}(f + \xi_f) = 32$ - ή διαφορετικά, ισχύει $f = \xi_f$ με πιθανότητα $7/8 > 3/4$. Κατά συνέπεια, εφαρμόζοντας τα αποτελέσματα που παρουσιάστηκαν σε αυτό το κεφάλαιο, είναι πολύ πιθανό να επιτύχουμε μία ακόμα αποδοτικότερη κρυπτανάλυση στον Achterbahn (που θα στηρίζεται σε προσεγγίσεις χαμηλότερου βαθμού), ακόμα ίσως και για την τελευταία έκδοσή του (αποτελεί ήδη τρέχον αντικείμενο έρευνας). Γίνεται φανερό λοιπόν ότι τα αποτελέσματα αυτού του κεφαλαίου καθορίζουν νέες σχεδιαστικές παραμέτρους που πρέπει να λαμβάνονται υπ' όψιν στη σχεδίαση ασφαλών συστημάτων.

Κεφάλαιο 7

Σύνοψη - Μελλοντική έρευνα

> We can only see a short distance ahead, but we can see plenty there that needs to be done
>
> *Alan Turing*

Η παρούσα διατριβή πραγματεύτηκε θέματα ασφάλειας των συμμετρικών αλγορίθμων κρυπτογράφησης. Μελετήθηκαν ποιοτικά χαρακτηριστικά των ακολουθιών οι οποίες χρησιμοποιούνται στα συστήματα αυτά ως ακολουθίες κλειδιού, με κύρια έμφαση τόσο στη γραμμική όσο και στη μη γραμμική πολυπλοκότητα. Επίσης αναλύθηκαν ιδιότητες λογικών συναρτήσεων οι οποίες χρησιμοποιούνται για την παραγωγή κρυπτογραφικών ακολουθιών. Τα νέα αποτελέσματα που απορρέουν από την παρούσα εργασία περιγράφονται συνοπτικά στη συνέχεια:

Γραμμική πολυπλοκότητα: Παρουσιάστηκε μία νέα αναπαράσταση ίχνους των περιοδικών ακολουθιών, η οποία με τη σειρά της οδήγησε στον ορισμό ενός νέου Γενικευμένου Διακριτού Μετασχηματισμού Fourier. Αυτές οι αναπαραστάσεις περιγράφουν όλες τις ακολουθίες *ανεξαρτήτως περιόδου*, γενικεύοντας κατά αυτόν τον τρόπο την κλασική αναπαράσταση ίχνους και τον απλό μετασχηματισμό Fourier [89, 99] που ισχύουν για ακολουθίες συγκεκριμένης περιόδου. Η γενίκευση αυτή επιτρέπει πλέον τον προσδιορισμό, για *οποιονδήποτε* LFSR, όλων των αρχικών καταστάσεών του οι οποίες επιτρέπουν την παραγωγή ακολουθίας με τη μέγιστη δυνατή γραμμική πολυπλοκότητα. Τα μαθηματικά εργαλεία που χρησιμοποιήθηκαν για αυτό το στόχο εντάσσονται στο χώρο της θεωρίας συστημάτων: συγκεκριμένα, κάθε LFSR αναπαρίσταται στο χώρο καταστάσεων, οπότε η γραμμική πολυπλοκότητα μίας ακολουθίας προσδιορίζεται από τη διάσταση ενός ελέγξιμου και παρατηρήσιμου γραμμικού καταστατικού συστήματος. Γενικεύοντας αυτόν τον συλλογισμό σε καταστατικά συστήματα οποιασδήποτε

μορφής, προκύπτει ο ορισμός νέων μέτρων πολυπλοκότητας. Επίσης, η μελέτη μη γραμμικών φίλτρων υπό το πρίσμα της θεωρίας συστημάτων οδήγησε στην κατασκευή καινούριων μη γραμμικών φίλτρων που παράγουν ακολουθίες εγγυημένα υψηλής γραμμικής πολυπλοκότητας. Η νέα οικογένεια φίλτρων που προτείνεται γενικεύει τα ισαπέχοντα φίλτρα του Rueppel [124], ενώ επίσης μπορεί να γενικεύσει και άλλες οικογένειες φίλτρων με καλά χαρακτηριστικά.

Μη γραμμική πολυπλοκότητα: Παρουσιάστηκε η συσχέτιση του προφίλ της μη γραμμικής πολυπλοκότητας μίας ακολουθίας με το προφίλ ιδιοτιμής, το οποίο με τη σειρά του καθορίζει μονοσήμαντα την πολυπλοκότητα Lempel-Ziv (η συσχέτιση αυτή έχει διατυπωθεί ως ανοιχτό ερευνητικό πρόβλημα [110]): συγκεκριμένα, αποδείχτηκε ότι δύο ακολουθίες με το ίδιο προφίλ ιδιοτιμής έχουν υποχρεωτικά το ίδιο προφίλ μη γραμμικής πολυπλοκότητας. Αναπτύχθηκε επίσης ένας νέος αποδοτικός αναδρομικός αλγόριθμος για τον υπολογισμό του ελάχιστου FSR που παράγει μία δυαδική ακολουθία, γενικεύοντας έτσι *για πρώτη φορά* τον πολύ γνωστό αλγόριθμο των Berlekamp-Massey [97] για τη μη γραμμική περίπτωση. Ο αλγόριθμος χρησιμοποιεί την ESOP αναπαράσταση των λογικών συναρτήσεων, καθώς επίσης και τον γνωστό αλγόριθμο των Knuth-Morris-Pratt για ταύτιση προτύπων σε μία ακολουθία. Επίσης, αποδεικνύεται ένα κάτω φράγμα του βαθμού συμπίεσης μίας ακολουθίας (όπως αυτός προσδιορίζεται από τον αλγόριθμο συμπίεσης των Lempel-Ziv [140]) το οποίο εξαρτάται από τη μη γραμμική πολυπλοκότητα αυτής, καταδεικνύοντας το ότι μπορούν να υπάρξουν υψηλά συμπιέσιμες ακολουθίες μεγάλης πολυπλοκότητας.

Χαμηλού βαθμού προσεγγίσεις λογικών συναρτήσεων: Αναπτύχθηκαν αποδοτικές μέθοδοι για τον υπολογισμό βέλτιστων προσεγγίσεων χαμηλού βαθμού για λογικές συναρτήσεις οποιουδήποτε πλήθους μεταβλητών. Συγκεκριμένα, καθίσταται πλέον εφικτός ο υπολογισμός βέλτιστων τετραγωνικών προσεγγίσεων για μία σημαντική οικογένεια συναρτήσεων βαθμού 3 και 4 - ένα πρόβλημα το οποίο έχει χαρακτηριστεί ως δύσκολο στο [17]. Η τεχνική που προτείνεται εδώ είναι η πρώτη στη βιβλιογραφία η οποία δίνει τις βέλτιστες τετραγωνικές προσεγγίσεις μίας συνάρτησης ανεξαρτήτως του πλήθους των μεταβλητών της. Μέσω της τεχνικής αυτής αναδεικνύονται συγκεκριμένες ιδιότητες οι οποίες, εφόσον ικανοποιούνται από μία συνάρτηση, επιτρέπουν τον προσδιορισμό των βέλτιστων τετραγωνικών προσεγγίσεων αυτής: κατά συνέπεια, προκύπτει το συμπέρασμα ότι αυτές οι ιδιότητες δεν πρέπει να ικανοποιούνται από μία κρυπτογραφική συνάρτηση, κάτι που οδηγεί στον προσδιορισμό νέων σχεδιαστικών κριτηρίων για τις κρυπτογραφικές λογικές συναρτήσεις. Μελετώνται επίσης διάφορες κατα-

σκευές κρυπτογραφικών συναρτήσεων που έχουν προταθεί στη βιβλιογραφία [12, 22, 30, 129], καταδεικνύοντας το ότι μπορούν να οδηγήσουν στη δημιουργία συναρτήσεων με χαμηλή μη γραμμικότητα δευτέρου βαθμού - κάτι το οποίο είναι μη επιθυμητό. Συνεπώς, τα αποτελέσματα της παρούσας εργασίας μπορούν να έχουν άμεση εφαρμογή σε υπάρχοντα κρυπτογραφικά συστήματα.

7.1 Μελλοντικές ερευνητικές κατευθύνσεις

Η έρευνα στο χώρο της κρυπτογραφίας, και ειδικότερα στους τομείς που εντάσσεται η παρούσα διατριβή, είναι διαρκής και σε συνεχή εξέλιξη. Πολλά είναι τα ανοιχτά ερωτήματα, όπως επίσης διαφαίνονται και πολλές κατευθύνσεις για περαιτέρω εξαγωγή νέων αποτελεσμάτων. Στη συνέχεια παρουσιάζουμε ερευνητικές κατευθύνσεις συναφείς με την παρούσα διατριβή, οι οποίες προσφέρονται για μελλοντική έρευνα.

Βέλτιστες τετραγωνικές προσεγγίσεις ευρύτερης οικογένειας συναρτήσεων: Από την ανάλυση του Κεφαλαίου 6 γίνεται φανερό ότι η επέκταση των αποτελεσμάτων σε ευρύτερες οικογένειες κυβικών συναρτήσεων κλάσης-m, $m \geq 2$, καθώς επίσης και σε συναρτήσεις μεγαλύτερου βαθμού, είναι πολύ σημαντική. Ήδη, σε πρόσφατη εργασία [81], γενικεύτηκε το Θεώρημα 6.13 ώστε να καλύπτει *όλες τις διαχωρίσιμες κυβικές συναρτήσεις κλάσης-m, για κάθε m*. Άμεση απόρροια αυτής της γενίκευσης είναι ένα *νέο κάτω φράγμα της ακτίνας κάλυψης του Reed-Muller κώδικα δεύτερης τάξης* $\mathfrak{R}(2, n)$. Η ερευνητική προσπάθεια συνεχίζεται με στόχο την επέκταση της μεθοδολογίας έτσι ώστε να είναι εφικτός ο υπολογισμός βέλτιστων τετραγωνικών προσεγγίσεων για συναρτήσεις υψηλότερου βαθμού. Επίσης, εφόσον ελάχιστα πράγματα ήταν μέχρι σήμερα γνωστά σχετικά με τη δευτέρου βαθμού μη γραμμικότητα συναρτήσεων, υπάρχουν πλέον οι δυνατότητες για διερεύνηση συσχετίσεων μεταξύ αυτής και άλλων κρυπτογραφικών κριτηρίων λογικών συναρτήσεων. Προς αυτήν την κατεύθυνση, η ανάλυση της ενότητας 6.4 μπορεί να επεκταθεί σε άλλες γνωστές κατασκευές συναρτήσεων - όπως, για παράδειγμα, για τις συναρτήσεις υψηλής αλγεβρικής ανθεκτικότητας.

Κρυπταναλυτικές επιθέσεις προσεγγίσεων χαμηλού βαθμού: Τα αποτελέσματα του Κεφαλαίου 6, όπως έχει ήδη αναφερθεί, μπορούν να εφαρμοστούν για τον έλεγχο της ασφάλειας σύγχρονων κρυπτογραφικών αλγορίθμων, όσον αφορά κρυπταναλυτικές επιθέσεις που βασίζονται σε προσεγγίσεις δευτέρου βαθμού. Ήδη, στην ενότητα 6.4, αναφέρθηκε ότι ο αλγό-

ριθμος Achterbahn χρησιμοποιεί μία λογική συνάρτηση f της οποίας μία βέλτιστη τετραγωνική προσέγγιση μπορεί πλέον εύκολα να υπολογιστεί μέσω της μεθοδολογίας που αναπτύχθηκε στο Κεφάλαιο 6: επιπλέον, η βέλτιστη αυτή τετραγωνική προσέγγιση προσεγγίζει πολύ ικανοποιητικά την f. Αντίστοιχες συναρτήσεις, με αυτό το όχι επιθυμητό χαρακτηριστικό, είναι πιθανό να είναι παρούσες και σε άλλους σύγχρονους αλγορίθμους. Άρα, τα αποτελέσματα της διατριβής μπορούν άμεσα να χρησιμοποιηθούν για τον έλεγχο της παρεχόμενης ασφάλειας από γνωστούς αλγορίθμους ροής - αποτελεί ήδη τρέχον αντικείμενο έρευνας. Επίσης, με δεδομένο ότι έχουν εφαρμοστεί αντίστοιχες κρυπταναλυτικές επιθέσεις και σε αλγορίθμους τμήματος, οι οποίες βασίζονται σε χαμηλού βαθμού προσεγγίσεις των S-boxes (όπως για παράδειγμα στο [57]), γίνεται φανερό ότι τα αποτελέσματα του Κεφαλαίου 6 μπορούν ενδεχομένως να εφαρμοστούν και σε αλγορίθμους τμήματος - κάτι που χρήζει περαιτέρω έρευνας.

Κρυπτογραφικά κριτήρια ακολουθιών: Οι ενδεχόμενες συσχετίσεις διαφόρων κρυπτογραφικών κριτηρίων των ακολουθιών παραμένει ένα πολύ σημαντικό ερώτημα. Το Κεφάλαιο 5 έδωσε απαντήσεις για τη σχέση μεταξύ της μη γραμμικής πολυπλοκότητας, της πολυπλοκότητας Lempel-Ziv και του βαθμού συμπίεσης μίας ακολουθίας. Στο ίδιο Κεφάλαιο ορίστηκαν οι s-βέλτιστες ακολουθίες, ως υψηλά συμπιέσιμες. Όπως ήδη αναφέρθηκε στο Κεφάλαιο αυτό, πειραματικά αποτελέσματα οδηγούν στην εικασία ότι για κάθε τιμή του s, υπάρχουν s-βέλτιστες ακολουθίες με πολυπλοκότητα s (βλέπε Πίνακα 5.1)· ωστόσο, αυτή η πειραματική παρατήρηση μένει να αποδειχτεί. Επίσης, με βάση τα πειραματικά αποτελέσματα, διαφαίνεται ότι οι περιοδικές επεκτάσεις των s-βέλτιστων ακολουθιών παρουσιάζουν πολύ υψηλή γραμμική πολυπλοκότητα - για την ακρίβεια, στη πολύ μεγάλη πλειοψηφία τους, έχουν τη μέγιστη δυνατή (ίση με την περίοδό τους). Εφόσον αποδειχτεί ότι αυτό ισχύει πάντοτε, γίνεται φανερό ότι ο λόγος συμπίεσης μίας ακολουθίας, όπως ορίζεται με βάση τον αλγόριθμο συμπίεσης των Lempel-Ziv, αποκτά ιδιαίτερη κρυπτογραφική αξία. Αξίζει να σημειωθεί επίσης ότι ο στατιστικός έλεγχος του Maurer (Maurer's Universal Statistical Test) [102], ο οποίος ανήκει στη λίστα κρυπτογραφικών κριτηρίων του NIST του Πίνακα 2.1, σχετίζεται με την ικανότητα συμπίεσης της ακολουθίας. Κατά συνέπεια, ο έλεγχος της συσχέτισής του με τη μη γραμμική πολυπλοκότητα ανακύπτει ως άμεσο επακόλουθο του Κεφαλαίου 5.

Εύρεση ελάχιστου FSR μίας ακολουθίας: Ο αλγόριθμος που προτάθηκε στο Κεφάλαιο 5 (Σχήμα 5.1) υπολογίζει αποδοτικά τον ελάχιστο FSR ο οποίος παράγει μία δοθείσα δυαδική ακολουθία y. Όπως έχει ήδη αναφερθεί, αν m είναι η πολυπλοκότητα της ακολουθίας y, τότε

στη γενική περίπτωση υπάρχουν πολλοί FSRs μήκους m που παράγουν την y. Συγκεκριμένα, όπως μπορεί να εξαχθεί εύκολα από την ανάλυση του Κεφαλαίου 5 (βλέπε επίσης και τα [58, 59]), αν k είναι το πλήθος των διαφορετικών υπακολουθιών μήκους m που υπάρχουν στην y, τότε το πλήθος των ελάχιστων FSRs για την ακολουθία y είναι 2^{2^m-k} (αφού το πλήθος των καταστάσεων από τις οποίες δεν θα περάσει ο ελάχιστος FSR της y είναι 2^m-k και, συνεπώς, η συνάρτηση ανάδρασης του FSR μπορεί να λαμβάνει οποιαδήποτε τιμή σε αυτές τις καταστάσεις). Συνεπώς, ο αλγόριθμος του Σχήματος 5.1 υπολογίζει έναν από τους 2^{2^m-k} ελάχιστους FSRs της y. Ένα ενδιαφέρον ερώτημα που ανακύπτει είναι ο προσδιορισμός του ελάχιστου FSR της y ο οποίος είναι βέλτιστος ως προς κάποιο κριτήριο - όπως, για παράδειγμα, είτε ως προς το πλήθος των όρων στην Αλγεβρική Κανονική Μορφή της συνάρτησης ανάδρασης ή ως προς τον βαθμό αυτής.

Γραμμική πολυπλοκότητα k σφαλμάτων: Ο ορισμός της γραμμικής πολυπλοκότητας k σφαλμάτων έχει ήδη αναφερθεί στην ενότητα 2.6. Οι ακολουθίες που έχουν κυρίως μελετηθεί στη βιβλιογραφία ως προς αυτό το κρυπτογραφικό κριτήριο είναι οι δυαδικές ακολουθίες περιόδου 2^n, λόγω ειδικών ιδιοτήτων της γραμμικής πολυπλοκότητας αυτών των ακολουθιών οι οποίες αναδεικνύονται από τον αλγόριθμο των Games-Chan [38]. Για κάθε τέτοια ακολουθία, εφόσον αναπαρασταθεί στη διανυσματική αναπαράσταση ίχνους που ορίστηκε στο Κεφάλαιο 4, προκύπτει ότι ο πίνακας μετάβασης κατάστασης του αντίστοιχου καταστατικού συστήματος που την παράγει αποτελείται από ένα μόνο Jordan μπλοκ (η μόνη ιδιοτιμή του χαρακτηριστικού πολυωνύμου $z^{2^n}-1$ του πίνακα είναι η μονάδα). Αυτή η ιδιαίτερη δομή του καταστατικού συστήματος παραγωγής της ακολουθίας αποτελεί εναλλακτικό τρόπο προσέγγισης των προβλημάτων που σχετίζονται με τη γραμμική πολυπλοκότητα k σφαλμάτων.

Ένα από τα ανοιχτά προβλήματα σε αυτό το πεδίο είναι ο προσδιορισμός των *κρίσιμων σημείων (critical points)* που μπορεί να έχει μία τέτοια ακολουθία y, όπου ως κρίσιμο σημείο ορίζεται κάθε ζεύγος ακεραίων $(k, c_k(y))$ με τις παρακάτω ιδιότητες:

- υπάρχει ακολουθία e περιόδου 2^n με $\mathrm{wt}(e)=k$, τέτοια ώστε να ισχύει $\mathrm{lc}(y+e)=c_k(y)$, ενώ δεν υπάρχει ακολουθία e' με $\mathrm{wt}(e')=k$ τέτοια ώστε $\mathrm{lc}(y+e')<c_k(y)$,
- για κάθε ακολουθία $\hat{e}$ με $\mathrm{wt}(\hat{e})<k$ ισχύει $\mathrm{lc}(y+\hat{e})>c_k(y)$.

Άρα, αν $(k, c_k(y))$ είναι ένα κρίσιμο σημείο της y, τότε η γραμμική πολυπλοκότητα k σφαλμάτων της y ισούται με $c_k(y)$, ενώ η πολυπλοκότητα $k-1$ σφαλμάτων είναι μεγαλύτερη από $c_k(y)$. Για μία δοθείσα ακολουθία περιόδου 2^n, ο αλγόριθμος των Lauder-Paterson στο [87]

υπολογίζει όλα τα κρίσιμα σημεία της. Ωστόσο, παραμένει ανοιχτό ερώτημα το πλήθος των κρίσιμων σημείων που μπορεί να έχει μία ακολουθία συναρτήσει του n. Ήδη μελετάται αυτό το πρόβλημα, κάνοντας χρήση ιδιοτήτων που ανακύπτουν από τον αλγόριθμο στο [87].

Βιβλιογραφία

[1] R. Anderson, "A5 - the GSM encryption algorithm," *sci.crypt post*, 1994.

[2] C. Berbain, O. Billet, A. Canteaut, et. al.: "DECIM - a new stream cipher for hardware applications," *eSTREAM, ECRYPT Stream Cipher Project, Report 2005/004*, 2005, `http://www.ecrypt.eu.org/stream`.

[3] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[4] E. Biham, R. J. Anderson and L. R. Knudsen, "Serpent: A new block cipher proposal," in *Fast Software Encryption–FSE '98* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1998, vol. 1372, pp. 222–238.

[5] S. Blackburn, "A generalisation of the discrete Fourier transform: determining the minimal polynomial of a periodic sequence," *IEEE Trans. Inform. Theory*, vol. 40, no. 5, pp. 1702–1704, 1994.

[6] S. Blackburn, T. Etzion and K. Paterson, "Permutation polynomials, De Bruijn sequences and linear complexity," *J. Combin. Theory*, Ser. A, vol. 76, no. 5, pp. 55–82, 1996.

[7] R. E. Blahut, *Theory and Practice of Error Control Codes*. Reading, MA: Addison-Wesley, 1984.

[8] Bluetooth SIG, Specification of the Bluetooth system, version 1.1, February 22, 2001, `http://www.bluetooth.com`.

[9] Y. Borissov, A. Braeken, S. Nikova and B. Preneel, "On the covering radii of binary Reed-Muller codes in the set of resilient boolean functions," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 1182–1189, 2005.

[10] P. Caballero-Gil, "Regular cosets and upper bounds on the linear complexity of certain sequences," in Sequences and Their Applications (Discrete Mathematics and Theoretical Computer Science). Berlin, Germany: Springer-Verlag, 1999, pp. 242–256.

[11] P. Caballero-Gil and A. Fúster-Sabater, "A wide family of nonlinear filter functions with large linear span," *Inform. Sci.*, vol. 164, no. 1-4, pp. 197–207, 2004.

[12] P. Camion, C. Carlet, P. Charpin and N. Sendrier, "On correlation-immune functions," in *Advances in Cryptology–Crypto '91* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1991, vol. 576, pp. 86–100.

[13] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Trans. Inform. Theory*, vol. 49, no. 8, pp. 2004–2019, 2003.

[14] C. Carlet, "Partially-bent functions," *Des. Codes Cryptogr.*, vol. 3, no. 2, pp. 135–145, 1993.

[15] C. Carlet, "Two new classes of bent functions," in *Advances in Cryptology–Eurocrypt '93* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1994, vol. 765, pp. 77–101.

[16] C. Carlet, "Boolean functions for cryptography and error correcting codes," Chapter of the monography Boolean Methods and Models, Y. Crama and P. Hammer eds, Cambridge University Press, to appear. Preliminary version available at `http://wwwrocq.inria.fr/codes/Claude.Carlet/pubs.htm`

[17] C. Carlet, "Recursive lower bounds on the nonlinearity profile of boolean functions and its applications," *Cryptology ePrint Archive*, no. 459, 2006.

[18] C. Carlet, "On the higher order nonlinearities of algebraic immune functions," in *Advances in Cryptology–Crypto '06* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2006, vol. 4117, pp. 584–601.

[19] C. Carlet, D. Dalai, K. Gupta and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: analysis and construction," *IEEE Trans. Inform. Theory*, vol. 52, no. 7, pp. 3105–3121, 2006.

[20] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 1, pp. 162–173, 2007.

[21] A. H. Chan, M. Goresky, and A. Klapper, "On the linear complexity of feedback registers," *IEEE Trans. Inform. Theory*, vol. 36, no. 3, pp. 640–644, 1990.

[22] P. Charpin, E. Pasalic, C. Tavernier, "On bent and semi-bent quadratic boolean functions," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4286–4298, 2005.

[23] C. Chen, *Linear System Theory and Design*. CBS College Publishing, 1984.

[24] T. H. Cormen, C. E. Leiserson, R. L. Rivest, *Introduction to Algorithms*. MIT Press, 1990.

[25] N. Courtois, L. Goubin, W. Meier, and J. Tacier, "Solving underdefined systems of multivariate quadratic equations," in *Public Key Cryptography–PKC 2002* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2002, vol. 2274, pp. 211–227.

[26] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology–Crypto '03* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2729, pp. 176–194.

[27] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology–Eurocrypt '03* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2656, pp. 345–359.

[28] D. K. Dalai, S. Maitra and S. Sarkar, "Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity," *Des. Codes Cryptogr.*, vol. 40, no. 1, pp. 41–58, 2006.

[29] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[30] J. F. Dillon, *Elementary Hadamard Difference Sets*. Ph.D. Thesis, University of Maryland, 1974.

[31] C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*. Lecture notes in Computer Science, Springer-Verlag, vol. 561, 1991.

[32] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Advances in Cryptology–Fast Software Encyption '93* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1994, vol. 1008, pp. 61–74.

[33] D. Erdmann and S. Murphy, "An approximate distribution for the maximum order complexity," *Des. Codes Cryptogr.*, vol. 10, no. 3, pp. 325–339, 1997.

[34] eSTREAM: ECRYPT Stream Cipher Project, IST-2002-507932. Available at `http://www.ecrypt.eu.org/stream/`, 2005.

[35] T. Etzion, "Linear complexity of De Brujin sequences - old and new results," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 693–698, 1999.

[36] J.-C. Faugère and G. Ars, "An algebraic cryptanalysis of nonlinear filter generators using Gröbner bases," *Technical Report* 4739, INRIA, 2003. Available at `ftp://ftp.inria.fr/INRIA/publication/publi-pdf/RR/RR-4739.pdf`.

[37] R. Forré, "A fast correlation attack on nonlinearly feedforward filtered shift-register sequences," in *Advances in Cryptology–Eurocrypt '89* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1990, vol. 434, pp. 586–595.

[38] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 1, pp. 144–146, 1983.

[39] B. Gammel, R. Göttfert and O. Kniffler, "The Achterbahn stream cipher," *eSTREAM, ECRYPT Stream Cipher Project, Report 2005/002*, 2005.

[40] B. Gammel, R. Göttfert and O. Kniffler, "Status of Achterbahn and tweaks," *eSTREAM, ECRYPT Stream Cipher Project, Report 2006/027*, 2006.

[41] B. Gammel, R. Göttfert and O. Kniffler, "Achterbahn-128/80," *eSTREAM, ECRYPT Stream Cipher Project, Report 2006/001*, 2006.

[42] S. W. Golomb, *Shift Register Sequences*. Holden-Day, San Francisco, 1967.

[43] S. W. Golomb, G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. New York, Cambridge University Press, 2005.

[44] J. D. Golić, "On the linear complexity of functions of periodic GF_q sequences," *IEEE Trans. Inform. Theory*, vol. 35, no. 1, pp. 69–75, 1989.

[45] J. D. Golić, "On the security of nonlinear filter generators," in *Fast Software Encyption '96* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1996, vol. 1039, pp. 173–188.

[46] J. D. Golić, A. Clark and E. Dawson, "Generalized inversion attack on nonlinear filter generators," *IEEE Trans. Comput.*, vol. 49, no. 10, pp. 1100–1109, 2000.

[47] E. J. Groth, "Generation of binary sequences with controllable complexity," *IEEE Trans. Inform. Theory*, vol. IT-17, no. 3, pp. 288–296, 1971.

[48] C. G. Günther, "A finite field Fourier transform for vectors of arbitrary length," in *Communications and Cryptography: Two Sides of One Tapestry.* Norwell, MA: Kluwer Academic Publishers, 1994, pp. 141–153.

[49] X. Guo-Zhen and J. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inform. Theory*, vol. 34, no. 3, pp. 569–571, 1988.

[50] M. Hell and T. Johansson, "Cryptanalysis of Achterbahn-version 2," *eSTREAM, ECRYPT Stream Cipher Project, Report 2006/042*, 2006.

[51] M. Hell and T. Johansson, "Cryptanalysis of Achterbahn-128/80," *eSTREAM, ECRYPT Stream Cipher Project, Report 2006/054*, 2006.

[52] T. Herlestam, "On functions of linear shift register synthesis," in *Advances in Cryptology–Eurocrypt '85* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1986, vol. 219, pp. 119–129.

[53] I. N. Herstein, *Topics in Algebra.* Xerox College Publishing, 1964.

[54] A. E. Heydtmann and J. M. Jansen, "On the equivalence of the Berlekamp-Massey and the Euclidean algorithms for decoding," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2614–2624, 2000.

[55] X.-D. Hou, and P. Langevin, "Results on bent functions," *J. Combin. Theory Ser. A*, vol. 80, no. 2, pp.232–246, 1997.

[56] K. Imamura and W. Yoshida, "A simple derivation of the Berlekamp-Massey algorithm and some applications," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 1, pp. 146–150, 1987.

[57] T. Jacobsen, "Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree," in *Advances in Cryptology–CRYPTO '98* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 1462, pp. 212–222, 1998.

[58] C. J. A. Jansen, *Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods*. PhD thesis, Technical University of Delft, 1989.

[59] C. J. A. Jansen and D. E. Boekee, "The shortest feedback shift register that can generate a given sequence," in *Advances in Cryptology–CRYPTO '89* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 435, pp. 90–99, 1990.

[60] S. Jiang and G. Gong, "Cryptanalysis of stream ciphers - A survey," *Technical Report 2002/29*, Centre for Applied Cryptographic Research: The University of Waterloo.

[61] T. Johansson and F. Jönsson, "Improved fast correlation attack on stream ciphers via convolutional codes," in *Advances in Cryptology–Eurocrypt '99* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 1592, pp. 347–362, 1999.

[62] T. Johansson and F. Jönsson, "Fast correlation attacks based on turbo code techniques," in *Advances in Cryptology–CRYPTO '99* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 1666, pp. 181–197, 1999.

[63] T. Johansson and F. Jönsson, "Fast correlation attacks through reconstruction of linear polynomials," in *Advances in Cryptology–Crypto '00* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 1880, pp. 300–315, 2000.

[64] T. Johansson, W. Meier and F. Muller, "Cryptanalysis of Achterbahn," in *Fast Software Encryption (FSE) 2006* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2006, vol. 4047, pp. 1–14.

[65] G. Kabatiansky and C. Tavernier, "List decoding of second order Reed-Muller codes," in Proc. 8th Intern. Simp. Comm. Theory and Applications. Ambelside, UK, 2005.

[66] R. Kalman, P. Falb and M. Arbib, *Topics in Mathematical System Theory*. McGraw-Hill, 1969.

[67] N. Kalouptsidis, *Signal Processing Systems*. Telecommunications and Signal Processing Series, John Wiley & Sons, 1996.

[68] N. Kalouptsidis and K. Limniotis, "Nonlinear span, minimal realizations of sequences over finite fields and De Brujin generators," in *Int. Symp. Inf. Theory and Appl.*, 2004, pp. 794–799.

[69] T. Kasami and N. Tokura, "On the weight structure of Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. IT-16, no. 6, pp. 752–759, 1970.

[70] T. Kasami, N. Tokura and S. Azumi, "On the weight enumeration of weights less than $2.5d$ of Reed-Muller codes," *Inform. and Control*, vol. 30, no. 4, pp. 380–395, 1976.

[71] S. Kavut, S. Maitra, and M. D. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1743–1751, 2007.

[72] A. Kerckhoffs, "La Cryptographie Militaire," *Journal des Sciences Militaires*, 9th series, IX(Jan 1883): pp. 5-38, (Feb 1883): pp. 161-191.

[73] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 732–736, 1976.

[74] K. Khoo, G. Gong and D. Stinson, "A new characterization of semi-bent and bent functions on finite fields," *Des. Codes Cryptogr.*, vol. 38, no. 2, pp. 279–295, 2006.

[75] A. Klimov and A. Shamir, "Cryptographic applications of T-functions," in *Selected Areas in Cryptography–SAC 2003* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2004, vol. 3006, pp. 248–261.

[76] L. R. Knudsen and M. J. B. Robshaw, "Non-linear approximations in linear cryptanalysis," in *Advances in Cryptology–Eurocrypt '96* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 1070, pp. 224–236, 1996.

[77] Z. Kohavi, *Switching and Finite Automata Theory*. McGraw-Hill Book Company, 1978.

[78] N. Kolokotronis, "Cryptographic properties of stream ciphers based on T-functions," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1604–1608, 2006.

[79] N. Kolokotronis and N. Kalouptsidis, "On the linear complexity of nonlinearly filtered PN-sequences," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3047–3059, 2003.

[80] N. Kolokotronis, K. Limniotis and N. Kalouptsidis, "Lower bounds on sequence complexity via generalised Vandermode determinants," in *Sequences and Their Applications*. Berlin, Germany: Springer-Verlag, vol. 4086, pp. 271–284, 2006.

[81] N. Kolokotronis, K. Limniotis and N. Kalouptsidis, "Efficient computation of the best quadratic approximations of cubic boolean functions," to appear in *11th IMA International Conference on Cryptography and Coding*, (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2007.

[82] N. Kolokotronis, K. Limniotis and N. Kalouptsidis, "Best affine approximations of boolean functions and applications to low order approximations," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1836–1840, 2007.

[83] N. Kolokotronis, P. Rizomiliotis and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Trans. Inform. Theory*, vol. 48, no. 10, pp. 2758–2764, 2002.

[84] K. Kurosawa, T. Iwata and T. Yoshiwara, "New covering radius of Reed-Muller codes for t-resilient functions," *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 468–475, 2004.

[85] X. Lai and J. L. Massey, "A proposal for a new Block Encryption Standard," in *Advances in Cryptology–Eurocrypt '90* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1991, vol. 473, pp. 389–404.

[86] C. Lam and G. Gong, "A lower bound for the linear span of filtering sequences," in *State of the Art of Stream Ciphers—SASC*, 2004, pp. 220–233.

[87] A. G. B. Lauder and K. Paterson, "Computing the error linear complexity spectrum of a binary sequence with period 2^n," *IEEE Trans. Inform. Theory*, vol. 49, no. 1, pp. 273–281, 2003.

[88] A. Lempel and J. Ziv, "On the complexity of finite sequences," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 1, pp. 75–81, 1976.

[89] R. Lidl and H. Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1996, 2nd ed.

[90] K. Limniotis, N. Kolokotronis and N. Kalouptsidis, "On the nonlinear complexity and Lempel–Ziv complexity of finite length sequences," to be published in *IEEE Trans. Inform. Theory*, 2007.

[91] K. Limniotis, N. Kolokotronis and N. Kalouptsidis, "New results on the linear complexity of binary sequences," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2003–2007, 2006.

[92] K. Limniotis, N. Kolokotronis and N. Kalouptsidis, "Nonlinear complexity of binary sequences and connections with Lempel–Ziv compression," in *Sequences and Their Applications*. Berlin, Germany: Springer-Verlag, vol. 4086, pp. 168–179, 2006.

[93] K. Limniotis, N. Kolokotronis and N. Kalouptsidis, "On the linear complexity of sequences obtained by state-space generators," under minor revision in *IEEE Trans. Inform. Theory*.

[94] S. Lin and D. J. Costello, *Error Control Coding - Fundamentals and Applications*. Pearson Prentice Hall, 2004, 2nd ed.

[95] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands, North-Holland, 1977.

[96] S. Maitra and E. Pasalic, "Further constructions of resilient boolean functions with very high nonlinearity," *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp.1825–1834, 2002.

[97] J. L. Massey, "Shift register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, no. 1, pp.122–127, 1969.

[98] J. L. Massey and S. Serconek, "A Fourier transform approach to the linear complexity of nonlinearly filtered sequences," in *Advances in Cryptology–CRYPTO '94* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1994, vol. 839, pp. 332–340.

[99] J. L. Massey and S. Serconek, "Linear complexity of periodic sequences: a general theory," in *Advances in Cryptology–CRYPTO '96* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1996, vol. 1109, pp. 358–371.

[100] P. Mathys, "A generalization of the discrete Fourier transform in finite fields," in *IEEE Symp. Inf. Theory*, 1990, pp. 14–19.

[101] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology - Eurocrypt '93* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 386–397.

[102] U. M. Maurer, "A universal statistical test for random bit generators," *J. Cryptology*, vol. 5, no. 2, pp. 89–105, 1992.

[103] W. Meier, E. Pasalic, and C. Carlet, "Algebraic Attacks and decomposition of Boolean Functions," in *Advances in Cryptology–Eurocrypt 2004* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2004, vol. 3027, pp. 474–491.

[104] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers," in *Advances in Cryptology–Eurocrypt '88* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1988, vol. 330, pp. 301–314.

[105] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[106] W. L. Millan, "Low order approximation of cipher functions," in *Cryptology: Policy and Algorithms Conference '95* (Lecture Notes in Computes Science). Berlin, Germany: Springer-Verlag, 1995, vol. 1029, pp. 144–155.

[107] National Institute of Standards and Technology, 2001. `http://csrc.nist.gov/CryptoToolkit/aes/rijndael/`.

[108] National Institute of Standards and Technology, 1999. `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`.

[109] The NIST Test Suite, `http://csrc.nist.gov/rng/`

[110] H. Niederreiter, "Some computable complexity measures for binary sequences," in *Sequences and Their Applications*, Discrete Mathematics and Theoretical Computer Science, Springer-Verlag, pp. 67–78, 1999.

[111] H. Niederreiter and M. Vielhaber, "Tree complexity and a doubly exponential gap between structured and random sequences," *J. Complexity*, vol. 12, pp. 187–198, 1996.

[112] K. G. Paterson, "Root counting, the DFT and the linear complexity of nonlinear filtering," *Des. Codes Cryptogr.*, vol. 14, no. 3, pp. 247–259, 1998.

[113] M. N. Plasencia, "Cryptanalysis of Achterbahn-128/80," *eSTREAM, ECRYPT Stream Cipher Project, Report 2006/055*, 2006.

[114] B. Preneel, R. Govaerts and J. Vandewalle, "Cryptographic properties of quadratic boolean functions," *Int. Symp. Finite Fields and Appl.*, 1991.

[115] P. Rizomiliotis, "Constructing Periodic Binary Sequences of Maximum Nonlinear Span," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4257–4261, 2006.

[116] P. Rizomiliotis and N. Kalouptsidis, "Results on the nonlinear span of binary sequences," *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp.1555–1563, 2005.

[117] P. Rizomiliotis, N. Kolokotronis and N. Kalouptsidis, "On the quadratic span of binary sequences," *IEEE Trans. Inform. Theory*, vol. 51, no. 5, pp. 1840–1848, 2005.

[118] R. L. Rivest, "The RC4 encryption algorithm," *RSA Data Security Inc.*, March 1992.

[119] R. L. Rivest, M. J. B. Robshaw and Y. L. Yin, "RC6 as the AES," in *AES Candidate Conference 2000*, pp 337-ὐ342.

[120] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *ACM J. Comm.*, vol. 21, no. 2, pp. 120–126, 1978.

[121] S. Rønjom and T. Helleseth, "A new attack on the filter generator," *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1752–1758, 2007.

[122] K. H. Rosen, J. G. Michaels, J. L. Gross, J. W. Grossman, and D. R. Shier, *Handbook of Discrete and Combinatorial Mathematics*. CRC Press, 2000.

[123] O. S. Rothaus, "On bent functions," *J. Combin. Theory Ser. A*, vol. 20, pp. 300–305, 1976.

[124] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Berlin, Germany: Springer-Verlang, 1986.

[125] R. A. Rueppel and O. J. Staffelbach, "Products of linear recurring sequences with maximum complexity," *IEEE Trans. Inform. Theory*, vol. 33, no. 1, pp. 124–131, 1987.

[126] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[127] A. Shimizu and S. Miyaguchi, "Fast Data Encryption Algorithm FEAL," in *Advances in Cryptology–Eurocrypt '87* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1987, vol. 304, pp. 267–278.

[128] B. Schneier, J. Kelsey, D. Whiting, D. Wagner and N. Ferguson, "Comments on Twofish as an AES Candidate," in *AES Candidate Conference 2000*, pp. 355–356.

[129] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inform. Theory*, vol. 30, no. 5, pp. 776–780, 1984.

[130] T. Siegenthaler, "Cryptanalysts representation of nonlinearly filtered m-sequences," in *Advances in Cryptology–Eurocrypt '85* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1986, vol. 219, pp. 103–110.

[131] M. Stamp and F. Y. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1398–1401, 1993.

[132] S. Stergiou, D. Voudouris and G. Papakonstantinou, "Multiple-value exclusive-or sum-of-products minimization algorithms," *IEICE Trans. on Fundamentals*, vol. E.87-A, no. 5, pp. 1226–1234, 2004.

[133] Y. V. Tarannikov, "On resilient boolean functions with maximum possible nonlinearity," in *Advances in Cryptology–Indocrypt 2000* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2000, vol. 1977, pp. 19–30.

[134] Y. V. Tarannikov, "New constructions of resilient boolean functions with maximal nonlinearity," in *Advances in Cryptology–Fast Software Encryption 2001* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2002, vol. 2355, pp. 66–77.

[135] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Journal American Institute of Electrical Engineers*, vol. 55, pp. 109–115, 1926.

[136] A. D. Wyner and J. Ziv, "The sliding-window Lempel-Ziv algorithm is asymptotically optimal," *Proceedings of the IEEE*, vol. 82, no. 6, pp. 872–877, 1994.

[137] X. M. Zhang and Y. Zheng, "Cryptographically resilient functions," *IEEE Trans. Inform. Theory*, vol. 43, no. 5, pp. 1740–1747, 1997.

[138] Y. Zheng, and X. M. Zhang, "On plateaued functions," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1215–1223, 2001.

[139] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 3, pp. 337–343, 1977.

[140] J. Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 5, pp. 530–536, 1978.

Ευρετήριο