Εργασία Πρώτη
" Αριθμητική σε Πεδία Galois GF(2^n)"

1. Γενική περιγραφή της άσκησης

Ο σκοπός της παρούσας άσκησης είναι η υλοποίηση απλής αριθμητικής (πρόσθεση και πολλαπλασιασμός) σε ένα σύνολο αριθμών με πεπερασμένο πλήθος στοιχείων. Η υλοποίηση θα βασιστεί σε απλά συνδεδεμένες λίστες με σταθερό πλήθος κόμβων.

2. Πεδία Galois - Μια εισαγωγή

Ένα πεδίο Galois GF(2^n) αποτελείται από ένα πεπερασμένο πλήθος 2^n στοιχείων, το οποίο μπορεί να απεικονιστεί από το σύνολο

$$\left\{0,1,a,a^2,\ldots,a^{2^n-2}\right\}.$$

Το στοιχείο a ονομάζεται «πρωτεύον στοιχείο», καθώς όλα τα μη μηδενικά στοιχεία του συνόλου προκύπτουν ως δυνάμεις αυτού. Για τον υπολογισμό των υπόλοιπων στοιχείων από το a χρησιμοποιείται ένα «αμείωτο πολυώνυμο» του οποίου το στοιχείο a είναι η ρίζα. Για παράδειγμα, στο GF(4) το αμείωτο πολυώνυμο είναι

$$p(x) = x^2 + x + 1$$

και το στοιχείο a ικανοποιεί τη σχέση

$$a^2 + a + 1 = 0.$$

Επιπλέον, στο πεδίο GF(2^n) η πρόσθεση πραγματοποιείται modulo 2, οπότε προσθέτοντας το a^2 και στα δύο μέλη της παραπάνω σχέσης προκύπτει ότι

$$a^2 = 2a^2 + a + 1 = a + 1.$$

Το πεδίο GF(4) συνεπώς αποτελείται από τα στοιχεία:

$$GF\left(4\right) = \left\{0,1,a,a+1\right\}.$$

Παρόμοια, το πεδίο GF(8) παράγεται από το αμείωτο πολυώνυμο

$$p(x) = x^3 + x^2 + 1$$

με βάση τη σχέση

$$a^3 = a^2 + 1.$$

Οι επιμέρους υπολογισμοί στοιχείων για το πεδίο GF(8) έχουν ως εξής:

$$a^3 = a^2 + 1$$
$$a^4 = a \cdot a^3 = a^3 + a = a^2 + 1 + a = a^2 + a + 1$$
$$a^5 = a \cdot a^4 = a^3 + a^2 + a = a^2 + 1 + a^2 + a = a + 1$$
$$a^6 = a \cdot a^5 = a^2 + a$$

και συνεπώς

$$GF(8) = \left\{0, 1, a, a^2, a^2 + 1, a^2 + a + 1, a + 1, a^2 + a\right\}.$$

Τα στοιχεία του πεδίου GF(2^n) μπορούν να γραφούν ως αθροίσματα δυνάμεων του στοιχείου α, με τις δυνάμεις να κυμαίνονται από α^0 μέχρι α^{n-1}, ενώ λόγω της modulo 2 αριθμητικής ο συντελεστής της κάθε δύναμης είναι 0 ή 1. Συνεπώς κάθε στοιχείο του πεδίου μπορεί να απεικονιστεί από μία n-άδα από 0 ή 1. Για παράδειγμα το στοιχείο α^2 στο GF(4) μπορεί να αναπαρασταθεί και ως (1,1). Το ίδιο στοιχείο στο GF(8) αναπαρίσταται ως (1,0,0) καθώς δε μπορεί να γραφεί ως άθροισμα μικρότερων δυνάμεων.

Οι παρακάτω πίνακες συνοψίζουν τις εναλλακτικές αναπαραστάσεις των στοιχείων στα πεδία GF(4) και GF(8):

Δύναμη	**Αθροισμα**	**n-αδα**
α^0	$0\,\alpha^1 + 1\,\alpha^0$	(0,1)
α^1	$1\,\alpha^1 + 0\,\alpha^0$	(1,0)
α^2	$1\,\alpha^1 + 1\,\alpha^0$	(1,1)

Αναπαράσταση στο GF(4)

Δύναμη	**Αθροισμα**	**n-αδα**
α^0	$0\,\alpha^2 + 0\,\alpha^1 + 1\,\alpha^0$	(0,0,1)
α^1	$0\,\alpha^2 + 0\,\alpha^1 + 1\,\alpha^0$	(0,1,0)
α^2	$1\,\alpha^2 + 0\,\alpha^1 + 0\,\alpha^0$	(1,0,0)
α^3	$1\,\alpha^2 + 0\,\alpha^1 + 1\,\alpha^0$	(1,0,1)
α^4	$1\,\alpha^2 + 1\,\alpha^1 + 1\,\alpha^0$	(1,1,1)
α^5	$0\,\alpha^2 + 1\,\alpha^1 + 1\,\alpha^0$	(0,1,1)
α^6	$1\,\alpha^2 + 1\,\alpha^1 + 0\,\alpha^0$	(1,1,0)

Αναπαράσταση στο GF(8)

2.1. Αριθμητική

Στο πεδίο GF(2^n) ορίζονται οι πράξεις της πρόσθεσης και του πολλαπλασιασμού μεταξύ στοιχείων. Στην πρόσθεση αθροίζονται modulo 2 οι συντελεστές των δυνάμεων που αναπαριστούν τα στοιχεία, π.χ.

$$GF(4): a^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1$$
$$GF(8): a^4 + a^3 = (a^2 + a + 1) + (a^2 + 1) = 2a^2 + a + 2 = a$$

Στον πολλαπλασιασμό αθροίζονται modulo 2^n-1 οι εκθέτες των στοιχείων, π.χ.

$$GF(4): a^2 \cdot a^2 = \alpha^4 = a \cdot a^3 = a \cdot 1 = a$$

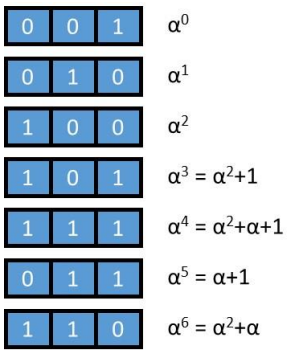
$$GF(8): a^4 \cdot a^5 = a^9 = a^2 \cdot a^7 = a^2 \cdot 1 = a^2$$

Μπορείτε εύκολα να ελέγξετε ότι ισχύει η παρακάτω σχέση:

$$a^{2^n-1} = 1$$

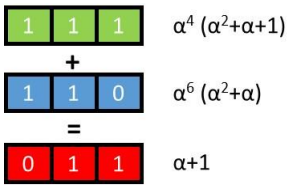
3. Υλοποίηση με συνδεδεμένες λίστες

Χρησιμοποιώντας την αναπαράσταση με n-άδες, κάθε στοιχείο του GF(2^n) μπορεί να αναπαρασταθεί με μια συνδεδεμένη λίστα με n κόμβους. Η θέση του κόμβου αντιστοιχεί σε μία δύναμη του a και τα δεδομένα του κόμβου αντιστοιχούν στο συντελεστή 0 ή 1 της εν λόγω δύναμης.



3.1. Αθροισμα και γινόμενο δύο στοιχείων του GF(2^n)

Η πρόσθεση δύο στοιχείων ισοδυναμεί με την πρόσθεση modulo 2 των δεδομένων στους αντίστοιχους κόμβους στις δύο συνδεδεμένες λίστες.

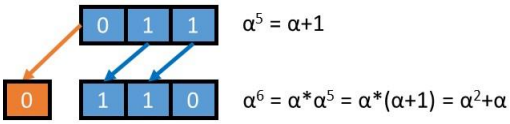


Για τον πολλαπλασιασμό των στοιχείων δεν απαιτείται κάποια ενέργεια στις συνδεδεμένες λίστες, παρά μόνο ο υπολογισμός του νέου εκθέτη.

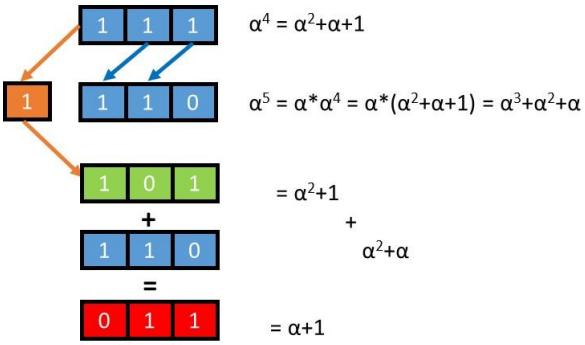
3.2. Υπολογισμός των στοιχείων του GF(2^n)

Παρατηρήστε ότι με την αναπαράσταση με n-άδες μπορεί κανείς να υπολογίσει διαδοχικά όλες τις δυνάμεις του α ξεκινώντας από το α^0. Συγκεκριμένα:

- Βήμα Ι: Ο πολλαπλασιασμός με α μετακινεί προς τα αριστερά τα δεδομένα σε όλους τους κόμβους της συνδεδεμένης λίστας, ενώ εισάγεται ο συντελεστής 0 στον τελευταίο κόμβο.



- Βήμα ΙΙ: Εάν ο πρώτος κόμβος είχε συντελεστή 1, τότε ο πολλαπλασιασμός έχει ως αποτέλεσμα την εμφάνιση της δύναμης a^n. Αυτή θα πρέπει (α) να αναλυθεί σε μικρότερες δυνάμεις με βάση την εξίσωση που προκύπτει από το αμείωτο πολυώνυμο, και (β) να μεταβάλλει το αποτέλεσμα του προηγούμενου βήματος στους κατάλληλους κόμβους, π.χ. με την πρόσθεση της n-άδας που αντιστοιχεί στο στοιχείο a^n.



Ζητούμενο 1 (Βάρος 50%) - Υπολογισμός των στοιχείων του GF(2^n)

Υλοποιήστε κώδικα ο οποίος θα παράγει και θα εκτυπώνει όλα τα στοιχεία ενός πεδίου GF(2^n) σε μορφή n-άδας. Το μέγεθος n θα δίνεται από το χρήστη και η υλοποίησή σας θα βασιστεί σε συνδεδεμένες λίστες και όχι πίνακες. Προτείνεται:

- ο υπολογισμός των στοιχείων να γίνεται βάση των βημάτων Ι και ΙΙ της προηγούμενης ενότητας,
- η υλοποίηση μιας συνάρτησης «πρόσθεσης modulo 2» που θα χρησιμεύσει τόσο στο βήμα ΙΙ όσο και σε επόμενα ζητούμενα,
- η αποθήκευση των συνδεδεμένων λιστών (π.χ. μέσω ενός πίνακα δεικτών).

Τα αμείωτα πολυώνυμα δίνονται στον παρακάτω πίνακα:

n	**p(x)**
2	x^2+x+1
3	x^3+x^2+1
4	x^4+x^3+1
5	x^5+x^3+1

6	x^6+x^5+1
7	x^7+x^6+1
8	$x^8+x^6+x^3+x^2+1$
9	$x^9+x^8+x^4+x^2+1$
10	$x^{10}+x^7+1$

Ζητούμενο 2 (Βάρος 40%) – Αριθμητική

Υλοποιήστε τις πράξεις της πρόσθεσης και του πολλαπλασιασμού μεταξύ δύο στοιχείων που δίνονται από το χρήστη. Το αποτέλεσμα θα πρέπει να εμφανίζεται τόσο με τη μορφή δύναμης όσο και με τη μορφή n-άδας, π.χ.

$$GF(8): a^5 + a^6 = a^2 + 1,$$
$$a^2 + 1 = a^3.$$
$$GF(8): a^5 \cdot a^6 = a^{11} = a^4,$$
$$a^4 = a^2 + a + 1.$$

Στην πρόσθεση το άθροισμα θα προκύπτει σε μορφή n-άδας, επομένως θα πρέπει να συγκρίνετε τη n-άδα που παράγετε με τις όλες n-άδες που αποθηκεύσατε μέσω του πίνακα δεικτών στο προηγούμενο ερώτημα.

Στον πολλαπλασιασμό αρκεί να εκτυπώνετε την αποθηκευμένη n-άδα που αντιστοιχεί στον εκθέτη του γινομένου.

Ζητούμενο 3 (Βάρος 10%) – Λογάριθμοι του Zech

Ο «λογάριθμος» Zech *Z(k)* ενός στοιχείου *k* ικανοποιεί τη σχέση

$$a^{Z(k)} = \alpha^k + 1$$

και μπορεί να χρησιμοποιηθεί για να υπολογίσετε τη δύναμη ενός αθροίσματος χωρίς να διασχίζετε κάθε φορά όλες τις αποθηκευμένες n-άδες. Συγκεκριμένα ισχύει ότι:

$$\alpha^p + \alpha^q = \alpha^q \cdot \left(\alpha^{p-q} + 1\right) = \alpha^{q+Z(p-q)}.$$

Για παράδειγμα στο πεδίο GF(8)

$$a^5 = a + 1 \Rightarrow Z(1) = 5$$

και επομένως

$$GF(8): a^5 + a^6 = a^{5+Z(1)} = a^{5+5} = a^{10} = a^3.$$

Χρησιμοποιήστε την αριθμητική που υλοποιήσατε στα προηγούμενα ερωτήματα για να υπολογίσετε τους λογαρίθμους του Zech. *Υπόδειξη: Θα χρειαστεί να*

εξετάσετε όλα τα δυνατά αθροίσματα μεταξύ n-άδων, καθώς και τη σχέση υπολογισμού του λογαρίθμου

$$\alpha^k + a^{Z(k)} + \alpha^0 = 0$$

Παραδοτέα

1. Κώδικας με σχόλια και όποια εξωτερικά αρχεία χρησιμοποιήσετε. Ο κώδικας πρέπει να αναφέρει τα μέλη της ομάδας (μέχρι δύο άτομα) και να ανέβει στο e-class μέχρι την ημερομηνία υποβολής. Ο κώδικας θα πρέπει να τρέχει σωστά σε μηχάνημα του Τμήματος (π.χ. Helios, εργαστήριο Dell/Alienware).
2. Αναφορά σε έντυπη μορφή στην οποία θα πρέπει να παράγετε αποτελέσματα για ενδεικτικές εκτελέσεις. Η αναφορά δε θα ανέβει στο e-class, αλλά θα την έχετε μαζί σας κατά την εξέταση της εργασίας.

Καλή Επιτυχία