ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
Θεωρία Πληροφορίας και Κωδικοποίησης
Φθινόπωρο 2002

5^{η} σειρά ασκήσεων

1. Το πολυώνυμο

$$g(x) = x^6 + 2x^5 + 3x^4 + 3x^3 + 3x^2 + 2x + 1 \ \in \mathbb{F}_4[x],$$

είναι πολυώνυμο γεννήτορας ενός κυκλικού κώδικα ως προς το $\mathbb{F}_4[x]$ τύπου $(15, 9)$.

(α') Κωδικοποιήστε το πολυώνυμο $u(x) = x^8 + 2x^2 + x + 1$.

Η κωδική λέξη για το $u(x)$ είναι το πολυώνυμο

$$\begin{aligned} u(x)g(x) &= x^{14} + 2x^{13} + 3x^{12} + 3x^{11} + 3x^{10} + 2x^9 + 3x^8 + \\ & \quad x^7 + x^6 + 3x^5 + 2x^3 + 3x^2 + 3x + 1. \end{aligned}$$

(β') Υπολογίστε το πολυώνυμο ελέγχου ισοτιμίας.

Το πολυώνυμο ελέγχου ισοτιμίας είναι το

$$h(x) = \frac{x^{15} - 1}{g(x)} = x^9 + 2x^8 + x^7 + x^6 + 2x^5 + 2x^4 + 3x^3 + 3x^2 + 2x + 3.$$

(γ') Είναι το πολυώνυμο $y_1(x) = x^{11} + 3x^2 + x + 2$ κωδική λέξη;

Αφού

$$y_1(x) \mod g(x) = 3x^5 + x^4 + x^3 + 3x \neq 0$$

το πολυώνυμο $y_1(x)$ δεν είναι κωδική λέξη.

(δ') Υπολογίστε το σύνδρομο του $y_2(x) = x^{10} + 3x^2 + x + 2$.

Το σύνδρομο $s_2(x)$ είναι το αποτέλεσμα της πράξης

$$s_2(x) = y_2(x) \mod g(x) = 2x^5 + 3x^4 + 3x^3 + 3x^2$$

εάν θεωρήσουμε ως στήλες του πίνακα ελέγχου ισοτιμίας H τη διανυσματική μορφή των υπολοίπων $x^j \mod g(x)$, $j \in \{0, 1, \ldots, 14\}$.

2. Να γράψετε τον πίνακα πολλαπλασιασμού για το δακτύλιο $\frac{\mathbb{F}_2[x]}{<x^2+1>}$. Είναι σώμα; Γιατί;

   Ο πίνακας πολλαπλασιασμού του δακτυλίου είναι ο εξής:

$\cdot$	1	x	$x+1$
1	1	x	$x+1$
x	x	1	$x+1$
$x+1$	$x+1$	$x+1$	0

   Από τον πίνακα παρατηρούμε ότι το στοιχείο $x+1$ είναι διαιρέτης του μηδενός αφού

$$(x+1)(x+1) = 0$$

   και επομένως ο δακτύλιος δεν είναι ακέραια περιοχή, οπότε δεν είναι σώμα. Αλλιώς, το μή μηδενικό στοιχείο $x+1$ του δακτυλίου δεν έχει πολλαπλασιαστικό αντίστροφο και επομένως ο δακτύλιος δεν είναι σώμα.

   Πάντως, το ότι ο δακτύλιος δεν είναι σώμα, προκύπτει άμεσα από το ότι το x^2+1 δεν είναι ανάγωγο στο $\mathbb{F}_2[x]$, χωρίς να απαιτείται ο υπολογισμός του πίνακα πολλαπλασιασμού του δακτυλίου.

3. (α΄) Παραγοντοποιήστε το $x^5 - 1 \in \mathbb{F}_2[x]$ σε γινόμενο αναγώγων πολυωνύμων.

   Έχουμε ότι

$$x^5 - 1 = 1 \cdot (x+1)(x^4 + x^3 + x^2 + x + 1)$$

   και

$$g_0(x) = 1,$$
$$g_1(x) = x + 1$$

   και

$$g_2(x) = x^4 + x^3 + x^2 + x + 1$$

   είναι τα ανάγωγα πολυώνυμα της ανάλυσης του $x^5 - 1$.

   (β΄) Γράψτε όλους τους δυνατούς κυκλικούς κώδικες μήκους 5.

   Οι πολυωνυμικοί γεννήτορες των κυκλικών κωδίκων μήκους 5 που προκύπτουν είναι οι εξής:

Γεννήτορας	Παρατηρήσεις
$g_0(x) = 1$	$C_0 = \mathbb{F}_2^5$
$g_1(x) = x + 1$	
$g_2(x) = x^4 + x^3 + x^2 + x + 1$	$C_2 = \{00000, 11111\}$
$g_3(x) = g_1(x)g_2(x) = x^5 + 1$	$C_3 = \{00000\}$

   (γ΄) Σε κάθε έναν κώδικα, κωδικοποιήστε και αποκωδικοποιήστε ένα μήνυμα.

4. Στο παράδειγμα του μαθήματος ($\mathbf{F} = \frac{\mathbb{F}_2[x]}{<x^4+x+1>}$, το σώμα με 16 στοιχεία) να διορθώσετε τα λάθη αν το σύνδρομο της λέξης που πήραμε είναι το $(10010110)^T$. Να υπολογίσετε το γεννήτορα πίνακα του κώδικα.

   Τα λάθη προκύπτουν ως λύση της εξίσωσης

$$S_1 Y^2 + S_1^2 Y + (S_1^3 - S_3) = 0 \tag{1}$$

   ως προς $Y = \zeta^a$, όπου ζ είναι αρχέτυπο στοιχείο του $\mathbb{F}_2^4$, $(\zeta^4 + \zeta + 1 = 0)$ και a είναι οι θέσεις των λαθών. Αφού το σύνδρομο είναι το $(10010110)^T$, έχουμε

$$S_1 = 1 + \zeta^3 = \zeta^{14}$$

   και

$$S_3 = \zeta + \zeta^2 = \zeta^5.$$

   Επίσης,

$$S_1^2 = \zeta^{28 \mod 15} = \zeta^{13} = \zeta^3 + \zeta^2 + 1$$
$$S_1^3 = \zeta^{12} = \zeta^3 + \zeta^2 + \zeta + 1,$$

   οπότε η (1) γίνεται

$$\zeta^{14} \cdot \zeta^{2a} + \zeta^{13} \cdot \zeta^a + \zeta^{14} = 0 \tag{2}$$

   Δοκιμάζοντας για $a \in \{0, 1, \ldots, 14\}$, βρίσκουμε ότι η (2) ικανοποιείται από τις θέσεις λαθών $a = 2$ και $a = 13$ ξεκινώντας τη μέτρηση των θέσεων από το μηδέν. Επομένως το πολυώνυμο λάθους είναι το

$$e(X) = X^2 + X^{13}.$$

   Ο γεννήτορας πίνακας G προκύπτει από τον πολυωνυμικό γεννήτορα

$$g(X) = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1) = X^8 + X^7 + X^6 + X^4 + 1$$

   και είναι ο εξής:

$$G = \begin{bmatrix} g \\ Xg \\ X^2g \\ X^3g \\ X^4g \\ X^5g \\ X^6g \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$