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

4^{η} σειρά ασκήσεων

1. Θεωρούμε το γραμμικό κώδικα με γεννήτορα πίνακα

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

στο $\mathbb{F}_3$. Να υπολογίσετε όλες τις κωδικές λέξεις αυτού και την ελάχιστη απόσταση του κώδικα. Είναι ο κώδικας τέλειος; Είναι κυκλικός;

Οι κωδικές λέξεις v του κώδικα προκύπτουν ως

$$v = aG, \quad \forall a \in \mathbb{F}_3^2$$

και είναι οι:

a	$v = aG$
00	0000
01	0112
02	0221
10	1011
11	1120
12	1202
20	2022
21	2101
22	2210

Όπως βλέπουμε από τον πίνακα, για κάθε μή μηδενική κωδική λέξη $v \in C$ ισχύει:

$$w(v) \geq 3 \Longrightarrow d_{min}(C) = w_{min}(C - \mathbf{0}) = 3.$$

Ο κώδικας είναι τέλειος διότι για τις παραμέτρους του $n = 4$, $M = 9$, $q = 3$ και $t = 1$ ισχύει η ισότητα στο φράγμα Hamming:

$$M\left(1 + q - 1\begin{pmatrix} 4 \\ t \end{pmatrix}\right) = 9\left(1 + 2\begin{pmatrix} 4 \\ 1 \end{pmatrix}\right) = 9 \cdot 9 = q^n = 3^4$$

δηλ. τα 2 επιπλέον ψηφία ελέγχου που χρησιμοποιούνται είναι ακριβώς όσα χρειάζονται για να διορθώνει 1 λάθος, ενώ δεν είναι κυκλικός αφού π.χ. δεν περιλαμβάνει την κυκλική μετάθεση 1101 της κωδικής λέξης 1011.

2. Να ορίσετε τον πίνακα οδηγών cosets και συνδρόμων ενός δυαδικού γραμμικού (3,1) κώδικα C_1 που παράγεται από το πολυώνυμο

$$g_1(x) = 1 + x + x^2$$

Κάντε το ίδιο για το δυαδικό γραμμικό $(7, 3)$ κώδικα C_2 που παράγεται από το πολυώνυμο

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

Το πολυώνυμο ελέγχου ισοτιμίας του κώδικα C_1 είναι το

$$h_1(x) = (x^3 + 1)/g_1(x) = x + 1$$

και ισχύει

$$(x^3 + 1) \mod g_1(x) = 0$$

και επειδή το $g_1(x)$ διαιρεί το (x^3+1), ο κώδικας $(3, 1)$ που παράγει είναι κυκλικός. Θεωρούμε τον πίνακα ελέγχου ισοτιμίας H_1 του C_1 στη μορφή

$$H_1 = \begin{bmatrix} 0 & h_{11} & h_{10} \\ h_{11} & h_{10} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

και θεωρούμε ως αρχές των συμπλόκων e, διανύσματα ελαχίστου βάρους για τα οποία ισχύει $s = H_1 e^T$ και να μην ισχύει $s = H_1 e_1^T = H_1 e_2^T$, για $e_1 \neq e_2$. Προκύπτει έτσι ο παρακάτω πίνακας οδηγών συμπλόκων και συνδρόμων:

Αρχή συμπλόκου e	Σύνδρομο s
000	00
100	01
010	11
001	10

Όμοια με πριν

$$h_2(x) = (x^7 + 1)/g_2(x) = x^3 + x^2 + 1$$

άρα

$$H_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Οπότε θεωρούμε ως οδηγούς συμπλόκων e, διανύσματα ελαχίστου βάρους και υπολογίζουμε τα σύνδρομα $s = H_2 e^T$, προσέχοντας να μην ισχύει $s = H_2 e_1^T = H_2 e_2^T$ για $e_1 \neq e_2$. Ο πίνακας οδηγών συμπλόκων και συνδρόμων είναι ο εξής:

Αρχή συμπλόκου e	Σύνδρομο s
0000000	0000
1000000	0001
0100000	0011
0010000	0110
0001000	1101
0000100	1010
0000010	0100
0000001	1000
1100000	0010
0110000	0101
0011000	1011
0001100	0111
0000110	1110
0000011	1100
1000001	1001
0100011	1111

3. Αν C κυκλικός δυαδικός κώδικας, παραγόμενος από το πολυώνυμο

$$g(x) = 1 + x + x^3$$

να αποκωδικοποιήσετε αν είναι δυνατό τα μηνύματα $y_1 = 1110010$, $y_2 = 1110011$, $y_3 = 1110101$.

Η αποκωδικοποίηση στους γραμμικούς κυκλικούς κώδικες γίνεται

- είτε με χρήση του πίνακα οδηγών συμπλόκων και συνδρόμων, αφού υπολογισθεί ο H σε μία από τις δύο γνωστές μορφές για κυκλικούς κώδικες (βάσει του πολυωνύμου ελέγχου ισοτιμίας $h(x)$ ή σε κανονική μορφή υπολοίπων του $g(x)$)
- είτε με τον αλγόριθμο αποκωδικοποίησης για κυκλικούς κώδικες εφόσον γνωρίζουμε τη διορθωτική ικανότητα t του κώδικα με την τεχνική 'παγίδευσης λάθους' (error trapping), ο οποίος σχετίζεται άμεσα με τον κανονικό πίνακα ελέγχου ισοτιμίας H.

Για την πρώτη περίπτωση, κάθε στήλη j του κανονικού πίνακα ελέγχου ισοτιμίας H είναι η διανυσματική αναπαράσταση του υπολοίπου $x^j \mod g(x)$, οπότε

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Παρατηρούμε ότι ο H περιλαμβάνει όλα τα μη μηδενικά διανύσματα του $\mathbb{F}_2^3$ τα οποία ανά δύο είναι γραμμικά ανεξάρτητα ενώ ανά τρία είναι γραμμικώς εξαρτημένα, επομένως $mld(H) = d_{min}(C) = 3$ και ο κώδικας C είναι ο κώδικας Hamming $[7, 4]$. Επιπλέον η πράξη $s = He^T$ ισοδυναμεί με την πράξη $s(x) = e(x) \mod g(x)$ στο χώρο των πολυωνύμων *modulo*-(x^7+1).

Ο πίνακας οδηγών συμπλόκων και συνδρόμων δίνεται στο σχ. 1. Άρα,

Οδηγός Συμπλόκου		Σύνδρομο		Παρατηρήσεις
Διάνυσμα e	Πολ/μο $e(x)$	Διάνυσμα s	Πολ/μο $s(x)$	
0000000	0	000	0	
1000000	1	100	1	$e=(e_3,\mathbf{0}_4)$, $e_3=s$
0100000	x	010	x	$e(x)=s(x)$
0010000	x^2	001	x^2	
0001000	x^3	110	$1+x$	
0000100	x^4	011	$x+x^2$	
0000010	x^5	111	$1+x+x^2$	
0000001	x^6	101	$1+x^2$	

Σχήμα 1: Πίνακας οδηγών συμπλόκων και συνδρόμων του C.

- $s_1 = Hy_1 = 0$, η y_1 είναι κωδική λέξη $u_1 = y_1$ (u_1 η κωδική λέξη που στάλθηκε),
- $s_2 = Hy_2 = (1, 0, 1)$ οπότε από τον πίνακα $u_2 = y_2 + 0000001 = u_1$ και
- $s_3 = Hy_3 = (0, 0, 1)$ οπότε από τον πίνακα $u_3 = y_3 + 0010000 = 1100101$.

Ο αλγόριθμος αποκωδικοποίησης κυκλικών (n, k) κωδίκων προσπαθεί με διαδοχικές κυκλικές μεταθέσεις $x^i e(x) \mod (x^n + 1)$ του οδηγού συμπλόκου $e(x) = u(x) + y(x)$ κατά i θέσεις $(0 \leq i \leq n-1)$ να το 'φθάσει' σε ένα πολυώνυμο $x^j e(x) \mod (x^n + 1)$ για το οποίο να ισχύει

$$s^{(j)}(x) = x^j e(x) \mod g(x) = x^j e(x) \mod (x^n + 1) \tag{1}$$

όπου δηλ. γνωρίζοντας το σύνδρομο-υπόλοιπο γνωρίζουμε στην ουσία τον ίδιο τον οδηγό και μάλιστα στην πολυωνυμική τους μορφή ισχύει η ισότητα μεταξύ τους, όπως βλέπουμε στον πίνακα του σχ.1, για το παράδειγμα του Hamming $[7, 4]$.

Τα πολυώνυμα $s^*(x) = s^{(j)}(x)$ με αυτή την ιδιότητα, αντιστοιχούν στα σύνδρομα $s^* = He^{*T}$ με $w(s^*) \leq t$ ή αλλιώς είναι οι οδηγοί συμπλόκων $e^*(x) = x^j e(x) \mod (x^n + 1)$ της διανυσματικής μορφής $e^* = (e^*_{n-k}, \mathbf{0}_k)$ με $e^*_{n-k} = s^{*T}$ (όπως φαίνεται και στον πίνακα του σχ.1), υπό την προυπόθεση ο πίνακας H να είναι στην κανονική μορφή

$$H = \left[\begin{array}{cc} I_{n-k} & A \end{array}\right]$$

για γραμμικούς κυκλικούς κώδικες. (Γενικότερα για γραμμικούς κώδικες με πίνακα ελέγχου ισοτιμίας αυτής της μορφής ισχύει $s = H(s^T, \mathbf{0}_k)$, οπότε για τους οδηγούς e^* προκύπτει $s^{*T} = e^*_{n-k}$).

Το υπόλοιπο $s^{(i)}$ υπολογίζεται κάθε φορά ως

$$\begin{aligned} s^{(i)}(x) &= (x^i e(x) \mod (x^n + 1)) \mod g(x) \\ &= x^i e(x) \mod g(x) \\ &= x^i (u(x) + y(x)) \mod g(x) \\ &= x^i s(x) \mod g(x) \end{aligned} \tag{2}$$

με $s(x) = y(x) \mod g(x)$. Αν βρεθεί μέσω της (2) τέτοιο j, τότε από την (1)

$$e(x) = \frac{x^n}{x^j} s^{(j)} \tag{3}$$

Η τελευταία ισότητα δεν είναι τίποτε άλλο από την κυκλική μετάθεση κατά την αντίθετη φορά του $s^{(j)} = x^j e(x) \mod (x^n + 1)$, ώστε να γυρίσουμε στο ζητούμενο οδηγό $e(x)$.

Με άλλα λόγια ο αλγόριθμος υπολογίζει τον οδηγό $e(x) = y(x) + u(x)$ όταν $w(e) \leq t$ έχοντας ως είσοδο μόνο το υπόλοιπο $s(x) = y(x) \mod g(x) = e(x) \mod g(x)$ και υπό ένα περιορισμό: να υπάρχει κυκλική μετάθεση $x^i e(x)$ του $e(x)$ για την οποία ο οδηγός $x^i e(x) \mod (x^7 + 1)$ να ισούται με το υπόλοιπό (σύνδρομό) του δηλ. το $x^i e(x) \mod g(x)$.

Στη γενική περίπτωση ενός κυκλικού (n, k) κώδικα, καμία τέτοια κυκλική μετάθεση δεν υπάρχει για τους οδηγούς συμπλόκων της μορφής

$$e(x) = 1 + \sum_{l=1}^{m-1} e_l x^l + x^m, \quad e_l \in \mathbb{F}_2, \quad w(e) \leq t$$

ή σε μορφή διανύσματος

$$e = (1 e_1 e_2 \ldots e_{m-1} 1, \mathbf{0}_{n-m-1})$$

(οπότε και για όλες τις κυκλικές τους μεταθέσεις), εάν $m \geq \deg(g) = n - k$. Ο αλγόριθμος θα εξαντλήσει όλες τις δυνατές ολισθήσεις χωρίς να αποκωδικοποιήσει τη ληφθήσα λέξη, διότι θα βρίσκει $s^{(i)}(x)$ με $w(s^{(i)}) > t$ ή αλλιώς επειδή ο e δεν είναι ένας από τους οδηγούς $e^* = (e^*_{n-k}, \mathbf{0}_k)$, όπως φαίνεται από τη διανυσματική μορφή του, αφού $n - m - 1 < k$ για $m \geq n - k$. Από τη μορφή όμως αυτών των ('προβληματικών' για τον αλγόριθμο) οδηγών συμπλόκων, προκύπτει ότι αντιστοιχούν σε περιπτώσεις περισσοτέρων του ενός λαθών διότι $w(e) \geq 2$ και επομένως ο αλγόριθμος διορθώνει όλες τις περιπτώσεις ενός λάθους, σε κάθε κυκλικό κώδικα με $t \geq 1$. Αφού για τον C ισχύει $t = 1$, ο αλγόριθμος αποκωδικοποιεί όλες τις λέξεις που λαμβάνονται και επομένως θα αποκωδικοποιήσει και τις y_1, y_2, y_3. Στον πίνακα που ακολουθεί φαίνεται ο αριθμός των κυκλικών μεταθέσεων j που απαιτούνται για κάθε οδηγό e μέχρι να 'φθάσουμε' στον οδηγό $x^j e(x) \mod (x^n + 1)$ μέσω της (2):

e			$x^j e(x) \mod (x^7+1) = s^{(j)}$	
Διάνυσμα	Πολυώνυμο	j	Διάνυσμα	Πολυώνυμο
1000000	1	0	1000000	1
0100000	x	0	0100000	x
0010000	x^2	0	0010000	x^2
0001000	x^3	4	1000000	1
0000100	x^4	3	1000000	1
0000010	x^5	2	1000000	1
0000001	x^6	1	1000000	1

Επαληθεύοντας:

- Για τη λέξη $y_1(x)$, $s_1(x) = 0$ και είναι κωδική λέξη $u_1(x) = y_1(x)$.

$f(x), \quad 2 \le deg(f) \le 4$
$1+x+x^2$
$1+x+x^3$
$1+x^2+x^3$
$1+x+x^4$
$1+x^2+x^4$
$1+x^3+x^4$
$1+x+x^2+x^3+x^4$

Σχήμα 2: Πίνακας υπό εξέταση πολυωνύμων.

- Για τη λέξη $y_2(x)$, $s_2(x) = 1 + x^2$, $w(s_2) = 2 > t$ οπότε μέσω της (2) $s^{(1)} = 1$, $w(100) = 1 = t$, άρα $j = 1$ και από την (3) $e_2(x) = x^6 \cdot 1$, $u_2(x) = y_2(x) + e_2(x) = u_1(x)$.
- Τέλος, για τη λέξη $y_3(x)$, $s_3(x) = x^2$, $w(001) = 1 = t$, $j = 0$ και $e_3(x) = s_3(x) = x^2$. Επομένως,

$$u_3(x) = y_3(x) + e_3(x) = 1 + x + x^2 + x^4 + x^6 + x^2 = 1 + x + x^4 + x^6.$$

4. (α′) Αν $f(x) \in \mathbb{F}_2[x]$, ανάγωγο, $deg(f) \ge 2$, τότε έχει περιττό αριθμό μή-μηδενικών συντελεστών.

   Έστω
   $$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \quad n \ge 2 \tag{4}$$
   με m μή μηδενικούς και $n+1-m$ μηδενικούς συντελεστές. Εφόσον το $f(x)$ είναι ανάγωγο και $n = deg(f) \ge 2$, ισχύει ότι

   $$(f(0) =) f(1) = 1 \Longrightarrow \sum_{i=0}^{n} a_i = 1 \Longrightarrow \sum_{k=1}^{m} 1 + \sum_{l=1}^{n+1-m} 0 = \sum_{k=1}^{m} 1 = 1 \Longrightarrow m \text{ περιττός.}$$

   Κάτι που βοηθάει στην επίλυση του (β′) υποερωτήματος είναι το εξής: αφού στην παραπάνω σχέση ισχύει και $f(0) = 1 \Longrightarrow a_0 = 1$. Οπότε συνολικά για κάθε $f(x)$ όπως στην (4) έχουμε

   $$\text{το } f(x) \text{ είναι ανάγωγο } \Longrightarrow a_0 = 1 \text{ και } m \text{ περιττός}$$

   (β′) Να καταγράψετε όλα τα ανάγωγα πολυώνυμα του $\mathbb{F}_2[x]$ βαθμού 1 εώς 4. Στη συνέχεια να κατασκευάσετε το σώμα με 8 στοιχεία.

   Τα πολυώνυμα βαθμού $n = 1$ και $n = 0$ είναι ανάγωγα αφού δε γίνεται να γραφούν ως γινόμενο δύο πολυωνύμων με βαθμό μικρότερο του n. Αυτά είναι τα 0, 1, x, $(x+1)$. Αν τα πολυώνυμα $f(x)$ με $2 \le deg(f) \le 4$ είναι ανάγωγα τότε (όπως αποδείχθηκε στο (α′) υποερώτημα) έχουν περιττό αριθμό μη μηδενικών συντελεστών και $a_0 = 1$ (αναγκαία αλλά όχι ικανή συνθήκη).

   Τα πολυώνυμα αυτής της μορφής είναι αυτά του πίνακα στο σχ. 2.

Στη συνέχεια πρέπει να εξαιρέσουμε από τον πίνακα του σχ. 2, τα πολυώνυμα τα οποία αναλύονται ως:

$$f(x) = a_1(x)a_2(x)\dots a_k(x) \tag{5}$$

όπου $a_i(x)$ ανάγωγα πολυώνυμα με $0 < deg(a_i) < deg(f)$ και $\sum_{i=1}^{k} deg(a_i) = \deg(f)$.
Στην περίπτωση του $f(x) = 1 + x + x^2$ πρέπει να εξετάσουμε αν το $f(x)$ μπορεί να αναλυθεί σε γινόμενο $k = 2$ αναγώγων παραγόντων-πολυωνύμων βαθμού 1 που στο $\mathbb{F}_2[x]$ είναι τα $a(x) = x - 0 = x$ και $b(x) = x - 1 = x + 1$, αφού

$$deg(a) = deg(b) = 1 < deg(f) = 2.$$

Με άλλα λόγια πρέπει να εξετάσουμε εάν το $f(x)$ έχει ρίζες το 0 ή το 1. Κάτι τέτοιο δε συμβαίνει γιατί $f(c) \neq 0$, για κάθε $c \in \mathbb{F}_2$, οπότε $f(x) \neq (x-c)(x-d)$ για οποιαδήποτε $c, d \in \mathbb{F}_2$. Άρα το $f(x)$ είναι ανάγωγο.
Για τα πολυώνυμα $f(x)$ 3ου βαθμού του πίνακα του σχ. 2, οι πιθανές παραγοντοποιήσεις στη μορφή της (5) είναι:

- $k = 3$ ανάγωγα πολυώνυμα βαθμού 1 ή
- $k = 2$ ανάγωγα πολυώνυμα, ένα βαθμού 1 και ένα βαθμού 2.

Και οι δύο μορφές παραγοντοποίησης είναι αδύνατες διότι όπως και πριν $f(x) \neq 0$. Επομένως και τα πολυώνυμα βαθμού 3 του πίνακα του σχ. 2 είναι ανάγωγα. Γενικότερα, ισχύει ότι 'το $f(x) \in \mathbb{F}_q[x]$, $2 \leq \deg(f) \leq 3$, είναι ανάγωγο εάν και μόνο εάν δεν έχει ρίζες στο $\mathbb{F}_q$', ακριβώς γιατί όλες οι πιθανές παραγοντοποιήσεις του $f(x)$, περιλαμβάνουν τους λεγόμενους 'γραμμικούς παράγοντες' $(x - c)$, βαθμού 1, όπως είδαμε.
Για τα πολυώνυμα $f(x)$ 4ου βαθμού του πίνακα του σχ. 2, οι πιθανές παραγοντοποιήσεις στη μορφή της (5) είναι:

- $k = 4$ ανάγωγα πολυώνυμα βαθμού 1 ή
- $k = 3$ ανάγωγα πολυώνυμα, δύο βαθμού 1 και ένα βαθμού 2
- $k = 2$ ανάγωγα πολυώνυμα βαθμού 2.

Οι δύο πρώτες μορφές παραγοντοποίησης είναι αδύνατες διότι όπως και πριν $f(x) \neq 0$. Για την τρίτη μορφή παρατηρούμε (στον πίνακα του σχ. 2) ότι το μοναδικό ανάγωγο πολυώνυμο βαθμού 2 είναι το $1 + x + x^2$. Άρα, ο μόνος τρόπος να προκύψει ένα πολυώνυμο $f(x)$ βαθμού 4, ως το γινόμενο δύο αναγώγων πολυωνύμων του $\mathbb{F}_2$ είναι ως

$$f(x) = (1 + x + x^2)(1 + x + x^2) = 1 + x^2 + x^4.$$

Επομένως πρέπει να εξαιρέσουμε το πολυώνυμο $f(x)$ από τον πίνακα του σχ. 2 διότι αφού αναλύεται σε παράγοντες δεν είναι ανάγωγο.
Τελικά, τα ανάγωγα πολυώνυμα $f(x)$, $2 \leq deg(f) \leq 4$ είναι τα εξής:

$f(x), \quad 2 \leq deg(f) \leq 4$
$1 + x + x^2$
$1 + x + x^3$
$1 + x^2 + x^3$
$1 + x + x^4$
$1 + x^3 + x^4$
$1 + x + x^2 + x^3 + x^4$

Θεωρούμε το ανάγωγο πολυώνυμο $f(x) = x^3 + x + 1$ και κατασκευάζουμε το σώμα

$$\mathbf{F} = \frac{\mathbb{F}_2[x]}{< f(x) >}$$

των πολυωνύμων modulo-$f(x)$ με 8 στοιχεία:

Δυαδικό ισοδύναμο	Πολυώνυμο του $\mathbf{F}$
000	0
001	1
010	x
011	$x+1$
100	x^2
101	x^2+1
110	x^2+x
111	x^2+x+1

5. Να βρείτε όλους τους τριαδικούς κυκλικούς κώδικες μήκους 4 και να γράψετε ένα γεννήτορα πίνακα για καθέναν από αυτούς.

   Οι πολυωνυμικοί γεννήτορες των κυκλικών τριαδικών κωδίκων μήκους 4 παράγονται από την παραγοντοποίηση του πολυωνύμου $f(x) = x^4 - 1$ σε ανάγωγα πολυώνυμα $g_i(x)$ και προκύπτουν ως το γινόμενο 2 ή περισσοτέρων από τα $g_i(x)$. Αφού $f(1) = 0$ ισχύει $f(x) = (x-1)(x^3 + x^2 + x + 1)$ και $g_1(x) = x - 1 = x + 2$. Θέτοντας $a_1(x) = x^3 + x^2 + x + 1$ παρατηρούμε ότι $a_1(2) = 0$. Επομένως $a_1(x) = (x-2)(x^2+1)$ και $g_2(x) = x - 2 = x + 1$. Θέτοντας $a_2(x) = x^2 + 1$ έχουμε $a_2(v) \neq 0, \forall v \in \mathbb{F}_3$. Επομένως $g_3(x) = x^2 + 1$ και

$$f(x) = g_0(x)g_1(x)g_2(x)g_3(x)$$

   θέτοντας $g_0(x) = 1$. Οι κώδικες που προκύπτουν είναι οι εξής:

Γεννήτορας	Παρατηρήσεις
$g_0(x) = 1$	$C_0 = \mathbb{F}_3^4$
$g_1(x) = x + 2$	
$g_2(x) = x + 1$	
$g_3(x) = x^2 + 1$	C_3
$g_4(x) = g_1(x)g_2(x) = x^2 + 2$	C_4
$g_5(x) = g_1(x)g_3(x) = x^3 + 2x^2 + x + 2$	
$g_6(x) = g_2(x)g_3(x) = x^3 + x^2 + x + 1$	
$g_7(x) = g_1(x)g_2(x)g_3(x) = x^4 + 1$	$C_7 = \{0000\}$

   Ο γεννήτορας πίνακας του κώδικα C_j με πολυωνυμικό γεννήτορα το $g_j(x)$, $0 \leq j \leq 6$ μπορεί να έχει τη μορφή

$$G_j = \begin{bmatrix} g_j \\ xg_j \\ \vdots \\ x^{k-1}g_j \end{bmatrix}$$

όπου $k = 4 - deg(g_j)$. Για τους κώδικες C_3 και C_4:

$$G_3 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

και

$$G_4 = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix}$$

και όμοια υπολογίζονται οι πίνακες των υπολοίπων πέντε μή μηδενικών κωδίκων.

6. Να κατασκευάσετε ένα γεννήτορα πίνακα του τριαδικού κώδικα Hamming C_2 τύπου $(4, 2, 3)$. Συνδυάστε με τα αποτελέσματα των ασκήσεων 1, 5 και αποδείξτε ότι ο κώδικας δεν είναι κυκλικός.

   Για τις στήλες του πίνακα ελέγχου ισοτιμίας H_2 του C_2 αρκεί να μην είναι η μία πολλαπλάσια κάποιας από τις άλλες, οπότε

   $$H_2 = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{bmatrix}$$

   σε κανονική μορφή. Άρα,

   $$G_2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

   και $G_2 = G$ όπου G ο γεννήτορας πίνακας του κώδικα της 1ης άσκησης για τον οποίο έχει δειχθεί ότι δεν είναι κυκλικός. Αλλιώς, από την 5η άσκηση διαπιστώνουμε ότι κανένα από τα 2ου βαθμού πολυώνυμα $g_3(x)$ και $g_4(x)$ δε διαιρεί ακριβώς π.χ. την 1η γραμμή του G_2 δηλ. την κωδική λέξη $1011 = 1 + x^2 + x^3$ του C_2. Μια άλλη αιτιολόγηση είναι ότι η ελάχιστη απόσταση του C_2 είναι 3 ενώ των κυκλικών κωδίκων C_3 και C_4 της 5ης άσκησης είναι 2.

7. Αν C δυαδικός γραμμικός κυκλικός κώδικας περιττού μήκους, να αποδείξετε ότι ο C περιέχει μια κωδική λέξη περιττού βάρους ακριβώς τότε όταν η $111\ldots1$ είναι κωδική λέξη του C.

   Λύση 1: Έστω ότι είναι n το μήκος του κώδικα. Τότε αν $f(x) = x^n + 1$ ισχύει

   $$f(x) = g(x)h(x) \tag{6}$$

   όπου $g(x)$, $h(x)$ είναι ο πολυωνυμικός γεννήτορας και το πολυώνυμο ελέγχου ισοτιμίας αντίστοιχα, του C. Αφού $f(1) = 0$, το $x + 1$ διαιρεί το $f(x)$ και

   $$f(x) = (x + 1)(x^{n-1} + x^{n-2} + \ldots + x + 1) \tag{7}$$

   όπου $(x^{n-1} + x^{n-2} + \ldots + x + 1)$ η πολυωνυμική μορφή της λέξης $111\ldots1$. Έστω $u(x) = b(x)g(x)$ η κωδική λέξη περιττού βάρους του C. Τότε $u(1) = 1$ που συνεπάγεται ότι $b(1) = g(1) = 1$ οπότε το $x+1$ δε διαιρεί το $g(x)$. Αλλά τότε, από τη (6) συμπεραίνουμε ότι το $x + 1$ διαιρεί το $h(x)$ (αφού διαιρεί το $f(x)$). Άρα υπάρχει $c(x)$ τέτοιο ώστε $h(x) = (x + 1)c(x)$ και από την (6):

   $$f(x) = g(x)(x + 1)c(x) \tag{8}$$

Από τις (7), (8) έχουμε

$$(x{+}1)(x^{n-1}{+}x^{n-2}{+}\ldots{+}x{+}1) = (x{+}1)c(x)g(x) \Longrightarrow x^{n-1}{+}x^{n-2}{+}\ldots{+}x{+}1 = c(x)g(x)$$

οπότε η λέξη $111\ldots1$ είναι κωδική λέξη. Για το αντίστροφο, η $111\ldots1$ έχει βάρος n, δηλ. περιττό. Επομένως, αφού είναι κωδική λέξη, ο κώδικας C περιλαμβάνει μια λέξη περιττού βάρους και δεν υπάρχει κάτι άλλο προς απόδειξη.

Λύση 2:(για το ευθύ) Έστω

$$a = a_0a_1a_2\ldots a_{n-1}$$

η κωδική λέξη περιττού βάρους του κώδικα. Τότε

$$\bigoplus_{i=0}^{n-1} a_i = 1 \tag{9}$$

Οι $n-1$ κυκλικές μεταθέσεις της a ανήκουν στον κώδικα και το άθροισμα συνολικά των n διανυσμάτων επίσης. Επομένως,

$$\begin{array}{rccccc}
 & [a_0 & a_1 & \ldots & a_{n-2} & a_{n-1}] \\
\oplus & & & & & \\
 & [a_{n-1} & a_0 & \ldots & a_{n-3} & a_{n-2}] \\
\oplus & & & & & \\
 & [a_{n-2} & a_{n-1} & \ldots & a_{n-4} & a_{n-3}] \\
\oplus & & & & & \\
 & \vdots & & \vdots & & \vdots \\
\oplus & & & & & \\
 & [a_2 & a_3 & \ldots & a_0 & a_1] \\
\oplus & & & & & \\
 & [a_1 & a_2 & \ldots & a_{n-1} & a_0] \\ \hline
= & [\bigoplus_{i=0}^{n-1} a_i & \bigoplus_{i=0}^{n-1} a_i & \ldots & \bigoplus_{i=0}^{n-1} a_i & \bigoplus_{i=0}^{n-1} a_i] \\
(\text{λόγω της } (9)\ ) = & [1 & 1 & \ldots & 1 & 1] \in C.
\end{array}$$