Δημιουργία Νέων Κωδίκων από υπάρχοντες

Αλέξανδρος Γ. Συγκελάκης *

21 Νοεμβρίου 2005

1 Τρύπημα Κωδίκων(Punctured Codes)

Έστω $\mathcal{C}$, ένας $[n, k, d]$ κώδικας πάνω από το $\mathbb{F}_q$. Τρυπάμε τον $\mathcal{C}$, σβήνοντας το ίδιο ψηφίο i, σε κάθε κωδική λέξη.

Ο καινούριος κώδικας $\mathcal{C}^*$, είναι γραμμικός και το **μήκος** των λέξεών του, είναι προφανώς $n - 1$.

Έστω G ο γεννήτωρ πίνακας του $\mathcal{C}$. Τότε ο γεννήτωρ πίνακας, G^* του $\mathcal{C}^*$ προκύπτει από τον G σβήνοντας την στήλη i (και παραλείποντας μηδενικές ή ίδιες γραμμές που μπορεί να προκύπτουν).

Ερώτημα: Ποιά είναι η διάσταση και η ελάχιστη απόσταση d^* του $\mathcal{C}^*$;

Ο $\mathcal{C}$ (ως γραμμικός κώδικας), περιέχει q^k κωδικές λέξεις, συνεπώς, ο $\mathcal{C}^*$ θα περιέχει λιγότερες μόνο εαν 2 λέξεις του $\mathcal{C}$, είναι ίδιες σε όλα τα ψηφία εκτός από εκείνο στη θέση i.

Σε αυτή την περίπτωση όπου υπάρχουν 2 τέτοιες λέξεις έχουμε ελάχιστη απόσταση $d = 1$ για τον $\mathcal{C}$ και μία τουλάχιστον λέξη βάρους 1 [1], η οποία έχει το μη μηδενικό ψηφίο στη θέση i.

Η ελάχιστη απόσταση μειώνεται κατά 1, εαν μία λέξη ελαχίστου βάρους του $\mathcal{C}$, έχει στη θέση i μη μηδενικό ψηφίο.

Συνοψίζοντας τα παραπάνω έχουμε:

Θεώρημα 1: Έστω $\mathcal{C}$, $[n, k, d]$ κώδικας πάνω από το $\mathbb{F}_q$ και $\mathcal{C}^*$ ο τρυπημένος κώδικας στην i θέση.
(i) Εαν $d > 1$, τότε ο $\mathcal{C}^*$ είναι ένας $[n-1, k, d^*]$ κώδικας, όπου $d^* = d - 1$ εαν ο $\mathcal{C}$ έχει μία ελαχίστου βάρους κωδική λέξη με μη μηδενικό ψηφίο στην i θέση, και $d^* = d$ διαφορετικά.
(ii) Εαν $d = 1$, τότε ο $\mathcal{C}^*$ είναι ένας $[n-1, k, 1]$ κώδικας εαν ο $\mathcal{C}$ δεν έχει κωδική λέξη βάρους 1 της οποίας το μη μηδενικό ψηφίο να είναι στη θέση i, διαφορετικά, εαν $k > 1$, ο $\mathcal{C}^*$ είναι ένας $[n-1, k-1, d^*]$ κώδικας, με $d^* \geq 1$.

*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

[1] Διότι $d(\mathcal{C}) = w(\mathcal{C})$,άρα αφού $d = 1$, θα υπάρχει κωδική λέξη βάρους 1

Παράδειγμα 1.1 : Έστω ο $[5,2,2]$ κώδικας $\mathcal{C}$ με γεννήτορα τον

$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ και $\mathcal{C}_1^*$, $\mathcal{C}_5^*$ οι τρυπημένοι κώδικες στις θέσεις 1 και 5

αντίστοιχα, με γεννήτορες πίνακες $G_1^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ και $G_5^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$.

Συνεπώς ο $\mathcal{C}_1^*$ είναι κώδικας $[4,2,1]$ [2] και ο $\mathcal{C}_5^*$ είναι κώδικας $[4,2,2]$ [3]

Παράδειγμα 1.2 : Έστω ο $[4,2,1]$ κώδικας $\mathcal{D}$ με γεννήτορα πίνακα τον

$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$. Έστω $\mathcal{D}_1^*$ και $\mathcal{D}_4^*$ οι τρυπημένοι κώδικες στις

θέσεις 1 και 4 αντίστοιχα. Τότε αυτοί έχουν γεννήτορες πίνακες τους

$D_1^* = [1\ 1\ 1]$ και $D_4^* = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

Παρατήρηση : Ο κώδικας $\mathcal{D}$ του παραδείγματος 1.2 είναι ο κώδικας $\mathcal{C}_1^*$ του παραδείγματος 1.1. Προφανώς θα μπορούσαμε να έχουμε πάρει τον $\mathcal{D}_4^*$ αμέσως, τρυπώντας τον $\mathcal{C}$ στις θέσεις $\{1,5\}$.

Γενικά, μπορούμε να τρυπήσουμε ένα κώδικα $\mathcal{C}$, σε ένα σύνολο θέσεων $\mathcal{I}$, σβήνοντας από όλες τις λέξεις του κώδικα $\mathcal{C}$, τα ψηφία στις θέσεις που υποδεικνύονται από τα στοιχεία του συνόλου $\mathcal{I}$. Εαν το $\mathcal{I}$ έχει πληθάριθμο t, τότε ο κώδικας που προκύπτει συμβολίζεται συνήθως με $\mathcal{C}^{\mathcal{I}}$ και είναι ένας $[n-t, k^*, d^*]$ κώδικας με $k^* \geq k-t$ και $d^* \geq d-t$ από το Θεώρημα 1 και με επαγωγή.

2 Κόντεμα Κωδίκων(Shortened Codes)

Έστω $\mathcal{C}$, ένας $[n,k,d]$ κώδικας πάνω από το $\mathbb{F}_q$ και έστω $\mathcal{I} \subset \{1,2,\ldots,n\}$ με t στοιχεία.

Ας θεωρήσουμε το σύνολο $\mathcal{C}(\mathcal{I})$ των κωδικών λέξεων του $\mathcal{C}$, που είναι $\bar{0}$ στο σύνολο $\mathcal{I}$ [4]. Προφανώς, το $\mathcal{C}(\mathcal{I})$ είναι υποχώρος του $\mathcal{C}$. [5].

[2]Έχουμε $d = 2 > 1$ και υπάρχει κωδική λέξη $\bar{c_1} = 11000$ με $w(\bar{c_1}) = 2 = d$ και η οποία έχει στην 1^η θέση μη μηδενικό ψηφίο. Άρα $d^* = d-1 = 1$.

[3]Με όμοια διαδικασία, όπως στον $\mathcal{C}_1^*$, βρίσκουμε ότι η ελάχιστη απόσταση του $\mathcal{C}_5^*$ είναι 2.

[4]Δηλαδή έχουν μηδέν σε κάθε θέση $i \in \mathcal{I}$

[5]Εαν $\bar{c}_1, \bar{c}_2 \in \mathcal{C}(\mathcal{I})$, τότε $\bar{c}_1 + \bar{c}_2 \in \mathcal{C}(\mathcal{I})$, αφού η λέξη $\bar{c}_1 + \bar{c}_2$ θα έχει μηδέν σε κάθε θέση $i \in \mathcal{I}$ και όμοια $\lambda{\cdot}\bar{c} \in \mathcal{C}(\mathcal{I})$, $\forall \bar{c} \in \mathcal{C}(\mathcal{I})$ και $\forall\ \lambda \in \mathbb{F}_q$

Τρυπάμε τώρα τον κώδικα $\mathcal{C}(\mathcal{I})$, [6] στο $\mathcal{I}$ και έτσι παίρνουμε ένα κώδικα πάνω από το $\mathbb{F}_q$, μήκους $n-t$ ο οποίος καλείται **Κοντεμένος (Shortened) Κώδικας** του $\mathcal{C}$, πάνω στο $\mathcal{I}$ και συμβολίζεται με $\mathcal{C}_{\mathcal{I}}$. Άρα $(\mathcal{C}(\mathcal{I}))^{\mathcal{I}} := \mathcal{C}_{\mathcal{I}}$

Παράδειγμα 2.1 :

$1^{ος}$ Τρόπος προσέγγισης (Αναγραφή των στοιχείων του Κώδικα $\mathcal{C}$)

Έστω $\mathcal{C}$, ο $[6,3,2]$ 2-αδικός κώδικας με γεννήτορα τον

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

Τότε όπως γνωρίζουμε, ο $\mathcal{C}$ παράγεται από τον G, ως γραμμικός συνδιασμός των γραμμών του δηλαδή $\lambda_1 \cdot (100111) + \lambda_2 \cdot (010111) + \lambda_3 \cdot (001111)$, $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$. Πρόκειται λοιπόν για τον κώδικα

$$\mathcal{C} = \{\ 000000, 010111, 001111, 011000, 100111, 110000, 101000, 111111\}$$

Άς θεωρήσουμε τώρα το σύνολο $\mathcal{I} = \{5,6\}$.

Τότε ο κώδικας $\mathcal{C}(\mathcal{I})$, θα περιέχει, όπως είδαμε, τις λέξεις που έχουν 0 στις θέσεις $\{5,6\}$. Άρα

$$\mathcal{C}(\mathcal{I}) = \{000000, 011000, 110000, 101000\}$$

και συνεπώς, ο τρυπημένος κώδικας αυτού, θα είναι ο κοντεμένος κώδικας

$$\mathcal{C}_{\mathcal{I}} = \{0000, 0110, 1100, 1010\}$$

Ένας γεννήτορας πίνακας του κώδικα αυτού είναι εκείνος που προκύπτει εαν πάρουμε 2 γραμμικώς ανεξάρτητες λέξεις του κώδικα $\mathcal{C}$, έστω τις $1010, 0110$ και τότε :

$$G_{\mathcal{I}} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Από την άλλη, τρυπώντας τον $\mathcal{C}$ στο $\mathcal{I}$ παίρνουμε τον τρυπημένο κώδικα του $\mathcal{C}$,

$$\mathcal{C}^{\mathcal{I}} = \{0000, 0101, 0011, 0110, 1001, 1100, 1010, 1111\}$$

[6] Ο $\mathcal{C}(\mathcal{I})$ ως υποχώρος του $\mathcal{C}$ καθίσταται και ο ίδιος, κώδικας

με γεννήτορα πίνακα τον

$$G^{\mathcal{I}} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

αφού το σύνολο

$$\{1001, 0101, 0011\}$$

αποτελείται από γραμμικώς ανεξάρτητες λέξεις του $\mathcal{C}^{\mathcal{I}}$.

Συμπέρασμα: Για να βρω τον $G^{\mathcal{I}}$ από τον G αρκεί να αφαιρέσω από τον G τις στήλες i για τις οποίες $i \in \mathcal{I}$.

$2^{ος}$ Τρόπος προσέγγισης

Θα προσπαθήσουμε με απλές γνώσεις Γραμμικής Άλγεβρας να βρούμε τον γεννήτορα πίνακα $G_{\mathcal{I}}$, του κοντεμένου κώδικα από τον γεννήτορα πίνακα G, του $\mathcal{C}$, χωρίς να χρειαστεί πρώτα να βρούμε τον $\mathcal{C}$ και στη συνέχεια τον $\mathcal{C}_{\mathcal{I}}$.

Καταρχήν, ο $\mathcal{C}$ υπενθυμίζουμε οτι είναι γραμμικός, συνεπώς παίρνοντας ένα γραμμικό συνδιασμό των γραμμών του γεννήτορα πίνακα G, και αντικαθιστώντας τον σε κάποια γραμμή, ο κώδικας $\mathcal{C}$ δεν αλλάζει. [7]

Αρχικά λοιπόν, παίρνω $i \in \mathcal{I}$ και μία γραμμή του G η οποία να μην έχει μηδέν στην θέση i και την προσθέτω σε κάθε γραμμή του G με μη μηδενική θέση i, τόσες φορές ώστε να πάρουμε 0. Έτσι στην στήλη i, έχουμε σε όλες τις θέσεις 0 εκτός από εκείνη τη θέση, της οποίας την γραμμή προσθέταμε σε κάθε άλλη γραμμή. Εαν δε, όλες οι γραμμές έχουν 0 στην θέση i τότε τις αφήνω όπως έχουν και συνεχίζω με διαφορετικό $j \in \mathcal{I}$, με $j \neq i$. Συνεχίζω έτσι με όλα τα στοιχεία του $\mathcal{I}$. Με το πέρας της διαδικασίας, θέλουμε να κρατήσουμε εκείνες τις μη μηδενικές και διαφορετικές γραμμές του καινούριου πίνακα G', που παράγουν τον κώδικα $\mathcal{C}_{\mathcal{I}}$. Αυτό πολύ απλά θα γίνει, διώχνοντας εκείνες τις γραμμές του G' που δεν έχουν 0 στις θέσεις $i \in \mathcal{I}$. Ο πίνακας που παράγεται με αυτή την απλή διαδικασία είναι και ο γεννήτορας πίνακας $G(\mathcal{I})$, του κώδικα $\mathcal{C}(\mathcal{I})$. Για να πάρουμε από εκείνον, τον γεννήτορα πίνακα του $\mathcal{C}_{\mathcal{I}}$, αρκεί όπως είδαμε παραπάνω να διώξουμε τις $i \in \mathcal{I}$ στήλες, του πίνακα $G(\mathcal{I})$.

Στο παράδειγμά μας λοιπόν, προσθέτουμε την $1^{η}$ γραμμή του G στις υπόλοιπες 2 γραμμές και έτσι παίρνουμε 0 στην θέση $5 \in \mathcal{I}$ αλλά και (τυχαία) στην θέση $6 \in \mathcal{I}$.Διώχνουμε την πρώτη γραμμή η οποία είναι μη μηδενική στο $\mathcal{I}$ και ο καινούριος πίνακας είναι ο γεννήτορας $G(\mathcal{I})$ του κώδικα $\mathcal{C}(\mathcal{I})$. Έπειτα, διώχνουμε την $5^{η}$ και $6^{η}$ στήλη του $G(\mathcal{I})$ και παίρνουμε τον γεννήτορα πίνακα $G_{\mathcal{I}}$ του κοντεμένου κώδικα $\mathcal{C}_{\mathcal{I}}$:

$$G_{\mathcal{I}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

[7] Το μόνο που αλλάζει είναι ο γεννήτορας πίνακας

Παρατήρηση: Με τους 2 διαφορετικούς τρόπους προσέγγισης, βρήκαμε 2 διαφορετικούς γεννήτορες πίνακες του κοντεμένου κώδικα. Προφανώς και οι 2 παράγουν τον ίδιο κώδικα και είναι γραμμοϊσοδύναμοι.

Ας πάρουμε τώρα τον δυϊκό κώδικα $\mathcal{C}^{\perp}$, του οποίου ο γεννήτορας πίνακας $G^{\perp}$ [8], είναι ο

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

Θεωρώντας και πάλι $\mathcal{I} = \{5, 6\}$, αφαιρούμε την 5^{η} και 6^{η} στήλη καθώς επίσης και την ίδια γραμμή που προκύπτει, και έτσι παίρνουμε τον γεννήτορα πίνακα $(G^{\perp})^{\mathcal{I}}$, του τρυπημένου κώδικα $(\mathcal{C}^{\perp})^{\mathcal{I}}$

$$(G^{\perp})^{\mathcal{I}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Από την άλλη, ο γεννήτορας πίνακας $G^{\perp}$ του δυϊκού κώδικα $\mathcal{C}^{\perp}$ είναι ήδη στην μορφή που περιγράψαμε στον 2^{o} τρόπο προσέγγισης παραπάνω, αφού η 5^{η} και 6^{η} στήλη έχει παντού 0 εκτός από μία θέση. Αφαιρώ λοιπόν διαδοχικά, τις αντίστοιχες γραμμές οι οποίες, στις θέσεις 5 και 6, αντίστοιχα, έχουν μη μηδενικά στοιχεία. Κατόπιν αφαιρούμε την 5^{η} και 6^{η} στήλη και έτσι έχουμε τον κοντεμένο γεννήτορα πίνακα $(G^{\perp})_{\mathcal{I}}$, του κώδικα $(\mathcal{C}^{\perp})_{\mathcal{I}}$

$$(G^{\perp})_{\mathcal{I}} = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

Εαν στο σημείο αυτό πάρουμε τον δυϊκό κώδικα του $\mathcal{C}_{\mathcal{I}}$, τότε έχουμε τον $(\mathcal{C}_{\mathcal{I}})^{\perp}$ με γεννήτορα πίνακα τον

$$(G_{\mathcal{I}})^{\perp} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

και εαν πάρουμε τον δυϊκό του $\mathcal{C}^{\mathcal{I}}$, τότε έχουμε τον $(\mathcal{C}^{\mathcal{I}})^{\perp}$ με γεννητορα πίνακα τον

$$(G^{\mathcal{I}})^{\perp} = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

Οι πίνακες $(G_{\mathcal{I}})^{\perp}$ και $(G^{\perp})^{\mathcal{I}}$ παράγουν τον ίδιο κώδικα αφού είναι γραμμοϊσοδύναμοι, συνεπώς $(\mathcal{C}_{\mathcal{I}})^{\perp} = (\mathcal{C}^{\perp})^{\mathcal{I}}$. Όμοια $(\mathcal{C}^{\mathcal{I}})^{\perp} = (\mathcal{C}^{\perp})_{\mathcal{I}}$.

Θα δείξουμε οτι αυτό ισχύει γενικότερα:

[8] Ο γεννήτορας πίνακας G, του $\mathcal{C}$ είναι σε standard μορφή.

Θεώρημα 2: Έστω $\mathcal{C}$ ένας $[n, k, d]$ κώδικας πάνω από το σώμα $\mathbb{F}_q$. Έστω $\mathcal{I} \subset \{1, 2, \ldots, n\}$ με t στοιχεία. Τότε :

(i) $(\mathcal{C}^{\perp})_{\mathcal{I}} = (\mathcal{C}^{\mathcal{I}})^{\perp}$ και $(\mathcal{C}^{\perp})^{\mathcal{I}} = (\mathcal{C}_{\mathcal{I}})^{\perp}$

(ii) Εαν $t < d$, τότε οι $\mathcal{C}^{\mathcal{I}}$ και $(\mathcal{C}^{\perp})_{\mathcal{I}}$ έχουν διαστάσεις k και $n-t-k$ αντίστοιχα.

(iii) Εαν $t = d$, και υπάρχει λέξη του $\mathcal{C}$ της οποίας τα μη μηδενικά ψηφία είναι στις θέσεις $i \in \mathcal{I}$ [9], τότε $\dim(\mathcal{C}^{\mathcal{I}}) = k - 1$ και $\dim((\mathcal{C}^{\perp})_{\mathcal{I}}) = n - d - k + 1$

Απόδειξη:

(i) Έστω $\bar{c} \in \mathcal{C}^{\perp}$ η οποία έχει μηδενικά στις θέσεις $i \in \mathcal{I}$ και $\bar{c}^*$, η λέξη $\bar{c}$ τρυπημένη στο $\mathcal{I}$. Άρα $\bar{c}^* \in (\mathcal{C}^{\perp})_{\mathcal{I}}$.
Εαν $\bar{x} \in \mathcal{C}$, τότε $\bar{x}^* \cdot \bar{c}^* = \bar{x} \cdot \bar{c} = \bar{0}$, όπου $\bar{x}^*$ είναι η λέξη $\bar{x}$ τρυπημένη στο $\mathcal{I}$. Άρα, $\bar{x}^* \in \mathcal{C}^{\mathcal{I}}$ και συνεπώς, $\bar{c}^* \in (\mathcal{C}^{\mathcal{I}})^{\perp}$ άρα $(\mathcal{C}^{\perp})_{\mathcal{I}} \subseteq (\mathcal{C}^{\mathcal{I}})^{\perp}$.

Έστω τώρα το $\bar{c} \in (\mathcal{C}^{\mathcal{I}})^{\perp}$. Μπορούμε να το επεκτείνουμε, προσθέτοντας μηδενικά στις θέσεις του $\mathcal{I}$. Έτσι παίρνουμε το $\hat{\bar{c}}$. Παίρνουμε τώρα $\bar{x} \in \mathcal{C}$, και τρυπάμε το $\bar{x}$ στο $\mathcal{I}$ και έτσι παίρνουμε $\bar{x}^* \in \mathcal{C}^{\mathcal{I}}$.
Όμως, $\bar{x} \cdot \hat{\bar{c}} = \bar{x}^* \cdot \bar{c} = \bar{0}$. Συνεπώς, $\hat{\bar{c}} \in \mathcal{C}^{\perp}$ άρα $\bar{c} \in (\mathcal{C}^{\perp})_{\mathcal{I}}$.

Βάζοντας τώρα, όπου $\mathcal{C}$, τον $\mathcal{C}^{\perp}$ και λαμβάνοντας υπόψη ότι $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$, έχουμε διαδοχικά:

$$\begin{aligned} ((\mathcal{C}^{\perp})^{\perp})_{\mathcal{I}} &= ((\mathcal{C}^{\perp})^{\mathcal{I}})^{\perp} \\ \mathcal{C}_{\mathcal{I}} &= ((\mathcal{C}^{\perp})^{\mathcal{I}})^{\perp} \\ (\mathcal{C}_{\mathcal{I}})^{\perp} &= (((\mathcal{C}^{\perp})^{\mathcal{I}})^{\perp})^{\perp} \\ (\mathcal{C}_{\mathcal{I}})^{\perp} &= (\mathcal{C}^{\perp})^{\mathcal{I}} \end{aligned}$$

(ii) Έστω $1 \leq t < d$. Τότε, έχουμε διαδοχικα:

$$\begin{aligned} -d &< -t \\ n-d &< n-t \\ n-d &\leq n-t-1 \\ n-d+1 &\leq n-t \end{aligned}$$

[9] Η λέξη αυτή έχει ελάχιστο βάρος αφού $t = d$

Η τελευταία, από αντίστοιχο θεώρημα, λέει, οτι εαν πάρω οποιεσδήποτε $n - t$ στήλες του γεννήτορα πίνακα G, του κώδικα $\mathcal{C}$, περιέχουν σύνολο πληροφορίας για τον $\mathcal{C}$.

Τρυπώντας λοιπόν τον $\mathcal{C}$ στο $\mathcal{I}$, αφαιρώντας δηλαδή t στήλες από τον γεννήτορα πίνακα, οι υπόλοιπες $n-t$ στήλες συνεχίζουν να περιέχουν σύνολο πληροφορίας.[10] Άρα η βαθμίδα του γεννήτορα πίνακα, $\mathrm{rank}(G^{\mathcal{I}}) = k$ συνεπώς η διάσταση του $\mathcal{C}^{\mathcal{I}}$ δεν αλλάζει. Άρα $\dim(\mathcal{C}^{\mathcal{I}}) = k$.

Εφόσον $\dim(\mathcal{C}^{\mathcal{I}}) = k$ και ο $\mathcal{C}^{\mathcal{I}}$ είναι $[n - t, k]$ κώδικας, θα έχουμε οτι $\dim((\mathcal{C}^{\mathcal{I}})^{\perp}) = n-t-k$. [11] Όμως από το (i) : $(\mathcal{C}^{\mathcal{I}})^{\perp} = (\mathcal{C}^{\perp})_{\mathcal{I}}$, άρα $\dim((\mathcal{C}^{\perp})_{\mathcal{I}}) = n - t - k$.

(iii) Έστω $\mathcal{I}_1 \subset \mathcal{I}$ με $|\mathcal{I}_1| = d - 1 (= t - 1$, αφού $t = d)$. Τότε ο κώδικας $\mathcal{C}^{\mathcal{I}_1}$, σύμφωνα με το (ii) έχει διάσταση k διότι $d-1 < d$. Ο κώδικας $\mathcal{C}^{\mathcal{I}_1}$ έχει ελάχιστη απόσταση 1, διότι εαν η ελάχιστη απόσταση ήταν ≥ 2 τότε, με την υπόθεση οτι υπάρχει μία λέξη, έστω $\bar{c}$, που έχει τα μη μηδενικά ψηφία στις θέσεις $i \in \mathcal{I}$, θα είχαμε ότι $w(\bar{c}) \geq d - 1 + 2 = d + 1$, άτοπο διότι η $\bar{c}$ είναι ελαχίστου βάρους κωδική λέξη.[12]

Συνεπώς η ελάχιστη απόσταση είναι 1.

Τον $\mathcal{C}^{\mathcal{I}}$ τον παίρνουμε από τον $\mathcal{C}^{\mathcal{I}_1}$, τρυπώντας τον, στην μη μηδενική θέση μίας λέξης βάρους 1. Από το Θεώρημα 1(ii), $\dim(\mathcal{C}^{\mathcal{I}}) = k - 1$ και ο $\mathcal{C}^{\mathcal{I}}$ είναι $[n - t, k - 1]$ κώδικας δηλαδή $[n - d, k - 1]$ κώδικας αφού $t = d$. Άρα

$$dim((\mathcal{C}^{\mathcal{I}})^{\perp}) = n - d - k + 1$$

και αφού $(\mathcal{C}^{\mathcal{I}})^{\perp} = (\mathcal{C}^{\perp})_{\mathcal{I}}$, έχουμε τελικά :

$$\dim((\mathcal{C}^{\perp})_{\mathcal{I}}) = n - d - k + 1$$

Αναφορές

[1] Raymond Hill, A First Course in Coding Theory p. 1–80.

[2] W. C. Huffman, Vera Pless, Fundamentals of Error-Correcting Codes (2003) p. 13–17.

[10] Οι $n - d - 1$ στήλες γνωρίζουμε οτι περιέχουν σύνολο πληροφορίας, συνεπώς περιέχουν k γραμμικώς ανεξάρτητες στήλες. Αφού έχουμε $n - t \geq n - d - 1$, οι $n - t$ στήλες εξακολουθούν να περιέχουν k γραμμικώς ανεξάρτητες στήλες.

[11] Θυμίζουμε, οτι εαν ο $\mathcal{C}$ είναι ένας $[n, k]$ κώδικας τότε ο $\mathcal{C}^{\perp}$ είναι $[n, n - k]$ κώδικας

[12] Διότι $t = d$