Απαριθμητές βάρους στην κωδικοποίηση

ΜΑΡΙΑ ΧΡΙΣΤΟΠΟΥΛΟΥ

ΠΑΡΟΥΣΙΑΣΗ ΣΤΟ ΜΑΘΗΜΑ ΤΗΣ
ΚΩΔΙΚΟΠΟΙΗΣΗΣ

ΙΑΝΟΥΑΡΙΟΣ 2003

Διάλεξη που πραγματοποιήθηκε στα πλαίσια του μεταπτυχιακού μαθήματος Ήκωδικοποίηση΄ στις 24 Ιανουαρίου 2003.Αποτελεί απόδοση στα ελληνικά του κεφαλαίου 13 του βιβλίου **A First Course in Coding theory,** Raymond Hill ,Oxford University Press.
Διδάσκων: Ι. Α. Αντωνιάδης.

Περιεχόμενα

1 Απαριθμητές βάρους **3**

2 Πιθανότητα των μη ανιχνεύσιμων λαθών **8**

1 Απαριθμητές βάρους

Έστω C ένας γραμμικός [n,k]-κώδικας,ο απαριθμητής βάρους του ορίζεται να είναι το πολυώνυμο:

$$\begin{aligned} W_c(z) &= \sum_{i=0}^{n} A_i z^i \\ &= A_0 + A_1 z^1 + ... + A_n z^n, \end{aligned}$$

όπου με A_i δηλώνουμε το πλήθος των κωδικών λέξεων του C που έχουν βάρος i.
Ένας άλλος τρόπος για να γράψουμε το $W_c(z)$ είναι:

$$W_c(z) = \sum_{x \in C} z^{w_(x)}.$$

Παράδειγμα 1.1
i)Έστω C ένας δυαδικός, άρτιου βάρους, κώδικας μήκους 3,δηλαδή ο $C = \{000, 011, 101, 110\}$ με δυικό κώδικα $C^{\perp} = \{000, 111\}$. Οι απαριθμητές βάρους των C και $C^{\perp}$ είναι:

$$W_c(z) = 1 + 3z^2$$

$$W_{c^{\perp}}(z) = 1 + z^3.$$

ii)Ο κώδικας $C = \{00, 11\}$ είναι αυτοδυικός οπότε:

$$W_c(z) = W_{c^{\perp}}(z) = 1 + z^2.$$

Όπως έχουμε ήδη δεί, εάν γνωρίζουμε τον απαριθμητή βάρους ενός κώδικα μπορούμε να υπολογίσουμε την πιθανότητα των μη ανιχνεύσιμων λαθών, όταν ο κώδικας χρησιμοποιείται απολύτως για ανίχνευση λαθών.

Το κύριο αποτέλεσμα αυτού του κεφαλαίου είναι ένας αξιόλογος τύπος του MacWilliams (1963),ο οποίος μας επιτρέπει να βρούμε τον απαριθμητη βαρους ενός γραμμικού κώδικα C από τον απαριθμητή του δυικού του κώδικα $C^{\perp}$.

Για απλότητα θα αποδείξουμε αυτό το αποτέλεσμα, γνωστό σαν ταυτότητα του MacWilliams, μόνο για δυαδικούς κώδικες (θεώρημα 1.5), παρόλο που το γενικό αποτέλεσμα θα εκτεθεί παρακάτω (θεώρημα 1.6).

Τα παρακάτω τρία λήμματα χρειάζονται μόνο για την απόδειξη της ταυτότητας του MacWilliams. Ένας αναγνώστης λιγότερο μαθηματικά καταρτισμένος, που προτιθεται να αποδεχθεί την εγκυρότητα του τύπου χωρίς απόδειξη, μπορεί να παραλείψει αυτά τα λήμματα και την απόδειξη του Θεωρήματος 1.5, χωρίς να χάσει πολλά μιας και τα ακόλουθα παραδείγματα και ασκήσεις χρησιμοποιούν μόνο τον τύπο και όχι την απόδειξή του.

Λήμμα 1.2
Ας είναι C ένας γραμμικός δυαδικός [n,k]-κώδικας και υποθέτουμε ότι y είναι ένα σταθερό διάνυσμα στον $(F_2)^n$ το οποίο δεν ανήκει στο $C^{\perp}$.Τότε το $x \cdot y$ είναι ίσο με 0 και1 εξίσου καθώς το x διατρέχει όλες τις κωδικές λέξεις του C.

Απόδειξη
Έστω $A = \{x \in C \mid x \cdot y = 0\}$ και $B = \{x \in C \mid x \cdot y = 1\}$.
Ας είναι u μια κωδική λέξη του C τέτοια ώστε $u \cdot y = 1$, (το u υπάρχει αφού $y \notin C^{\perp}$).
Δηλώνουμε με u+A το σύνολο $\{u + x \mid x \in A\}$.
Τότε

$$u + A \subseteq B,$$

διότι εάν $x \in A$, τότε $(u + x) \cdot y = u \cdot y + x \cdot y = 1 + 0 = 1$.
Ομοίως,

$$u + B \subseteq A.$$

Οπότε,

$$|A| = |u + A| \leq |B| = |u + B| \leq |A|.$$

Άρα, $|A| = |B|$ και το λήμμα αποδείχθηκε.□

Λημμα 1.3
Ας είναι C ένας δυαδικός $[n, k]$-κώδικας και y ένα οποιοδήποτε στοιχείο του $(F_2)^n$ Τότε:

$$\sum_{x \in C} (-1)^{x \cdot y} = \begin{cases} 2^k, & \text{εάν } y \in C^{\perp} \\ 0, & \text{εάν } y \notin C^{\perp}. \end{cases}$$

Απόδειξη
Εάν $y \in C^{\perp}$, τότε $x \cdot y = 0$ για όλα τα $x \in C$, οπότε

$$\sum_{x \in C} (-1)^{x \cdot y} = |C| \cdot 1 = 2^k$$

Εάν $y \notin C^{\perp}$, τότε από το λήμμα 1.2, καθώς το x διατρέχει όλα τα στοιχεία του C, το $(-1)^{x \cdot y}$ είναι ίσο με 1 και -1, εξίσου δίνοντας

$$\sum_{x \in C} (-1)^{x \cdot y} = 0. \quad \square$$

Λήμμα 1.4
Έστω x ένα σταθερό διάνυσμα του $(F_2)^n$ και z να είναι ένα οποιοδήποτε διάνυσμα του. Τότε η ακόλουθη πολυωνυμική ταυτότητα έχει:

$$\sum_{y \in (F_2)^n} z^{w_(y)} (-1)^{x \cdot y} = (1 - z)^{w_(x)} (1 + z)^{n - w_(x)}.$$

Απόδειξη:

$$\begin{aligned}\sum_{y\in(F_2)^n} z^{w_(y)}(-1)^{x\cdot y} &= \sum_{y_1=0}^{1}\sum_{y_2=0}^{1}\ldots\sum_{y_n=0}^{1} z^{y_1+y_2+\ldots y_n}(-1)^{x_1\cdot y_1+\ldots+x_n\cdot y_n}\\ &= \sum_{y_1=0}^{1}\sum_{y_2=0}^{1}\ldots\sum_{y_n=0}^{1}(\prod_{i=1}^{n} z^{y_i}(-1)^{x_i\cdot y_i})\\ &= \prod_{i=1}^{n}(\sum_{j=0}^{1} z^j(-1)^{j\cdot x_i})\\ &= (1-z)^{w_(x)}(1+z)^{n-w_(x)},\end{aligned}$$

αφού,

$$\sum_{j=0}^{1} z^j(-1)^{j\cdot x_i} = \begin{cases} 1+z, & \text{εάν } x_i=0\\ 1-z, & \text{εάν } x_i=1\end{cases}. \quad \square$$

Θεώρημα 1.5(Η ταυτότητα του MacWilliams για γραμμικούς δυαδικούς κώδικες)
Έστω C ένας δυαδικός $[n,k]$-κώδικας με δυικό κώδικα $C^\perp$ τότε:

$$W_{C^\perp}(z) = \frac{1}{2^k}(1+z)^n W_C(\frac{1-z}{1+z}).$$

Απόδειξη:
Εκφράζουμε το πολυώνυμο:

$$f(z) = \sum_{x\in C}(\sum_{y\in(F_2)^n}(-1)^{x\cdot y} z^{w(y)})$$

με δύο τρόπους.
Από την μία πλευρά χρησιμοποιώντας το λήμμα 1.4,

$$\begin{aligned} f(z) &= \sum_{x\in C}(1-z)^{w(x)}(1+z)^{n-w(x)}\\ &= (1+z)^n\sum_{x\in C}(\frac{1-z}{1+z})^{w(x)}\\ &= (1+z)^n W_C(\frac{1-z}{1+z}).\end{aligned}$$

Απο την άλλη πλευρά, αντιστρέφοντας την σειρά του αθροίσματος, οπότε έχουμε:

$$\begin{aligned} f(z) &= \sum_{y\in(F_2)^n} z^{w(y)}\Big(\sum_{x\in C}(-1)^{x\cdot y}\Big)\\ &= \sum_{y\in C^\perp} z^{w(y)}2^k \quad \text{από το λήμμα 1.3}\\ &= 2^k W_{C^\perp}(z).\end{aligned}$$

Εξισώνοντας τις δυο εκφράσεις για το $f(z)$ προκύπτει το αποτέλεσμα.$\square$

Η απόδειξη του παρακάτω πιο γενικού αποτελέσματος είναι παρόμοια με αυτή του θεωρήματος 1.5,αφού χρησιμοποιεί γενικότερες εκδόσεις των προηγούμενων λημμάτων, αλλά θα παραλείψουμε τις λεπτομέρειες.

Θεώρημα 1.6 (Η ταυτότητα του MacWilliams γενικά για γραμμικούς κώδικες)
Εάν C ένας γραμμικός $[n,k]$-κώδικας στο GF(q) με δυικό κώδικα $C^{\perp}$,τότε:

$$W_{C^{\perp}}(z) = \frac{1}{q^k}[1+(q-1)z]^n W_C(\frac{1-z}{1+(q-1)z}).$$

Σημείωση: Εάν ο C είναι ένας δυαδικός $[n,k]$-κώδικας, τότε αφού ο δυικός του $C^{\perp}$ είναι ακριβώς ο C, μπορούμε να γράψουμε την ταυτότητα του MacWilliams στην (πιο χρήσιμη) μορφή:

$$W_C(z) = \tfrac{1}{2^{n-k}}(1+z)^n W_{C^{\perp}}(\tfrac{1-z}{1+z}). \quad (1.7)$$

Παραδείγματα 1.8
Εφαρμόζουμε το Θεώρημα 1.5 στους κώδικες του παραδείγματος 1.1.

ι) Έχουμε $W_C(z) = 1+3z^2$. Έτσι από το θεώρημα 1.5,

$$\begin{aligned} W_{C^{\perp}}(z) &= \frac{1}{4}(1+z)^3 W_C(\frac{1-z}{1+z}) \\ &= \frac{1}{4}[(1+z)^3 + 3(1-z)^2(1+z)] \\ &= 1+z^3, \end{aligned}$$

όπως έχουμε ήδη βρεί απ' ευθείας από το δυικό $C^{\perp}$.
Ας ανταλλάξουμε τους ρόλους των C και $C^{\perp}$ προκειμένου να τσεκάρουμε τον τύπο (1.7). Έχουμε:

$$\begin{aligned} \frac{1}{2}(1+z)^3 W_{C^{\perp}}(\frac{1-z}{1+z}) &= \frac{1}{2}[(1+z)^3 + (1-z)^3] \\ &= 1+3z^2, \end{aligned}$$

το οποίο είναι πράγματι το $W_C(z)$.
ιι) Έχουμε $W_C(z) = 1+z^2$. Τότε:

$$\begin{aligned} W_{C^{\perp}}(z) &= \frac{1}{2}(1+z)^2 W_C(\frac{1-z}{1+z}) \\ &= \frac{1}{2}[(1+z)^2 + (1-z)^2] \\ &= 1+z^2. \end{aligned}$$

Έτσι,$W_{C^{\perp}}(z) = W_C(z)$, όπως περιμέναμε αφού ο C είναι αυτοδυικός.

Για τους πολύ μικρούς κώδικες, η χρήση της ταυτότητας του MacWilliams είναι ένας αναποτελεσματικός τρόπος υπολογισμού των απαριθμητών βάρους, αφού αυτοί μπορούν να υπολογισθούν απευθείας από την λίστα των κωδικών λέξεων.Αλλά υπέθεσε ότι έχουμε να υπολογίσουμε τον αριθμητή βάρους ενος $[n,k]$-κώδικα C στο GF(q) όπου το k είναι αρκετά μεγάλο. Το να απαριθμήσουμε τα βάρη όλων των q^k κωδικών λέξεων μπορεί να είναι πολύ δύσκολο. Ωστόσο, εάν k είναι τόσο μεγάλο ώστε το n-k είναι μικρό, τότε ο δυικός του κώδικας μπορεί να είναι αρκετά

μικρός για να βρεθούν οι απαριθμητές βάρους του και στη συνέχεια μπορεί να χρησιμοποιηθεί η ταυτότητα του MacWilliams , ώστε να βρεθούν οι απαριθμητές βάρους του C.

Για παράδειγμα, ο δυαδικός κώδικας Hamming $Ham(r,2)$ έχει διασταση 2^r-1-r, οπότε ο αριθμός των κωδικών λέξεων του $Ham(r,2)$ ειναι 2^{2^r-1-r}, ένας μεγάλος αριθμός ακόμη και για μικρές τιμές του r. Αλλά ο δυικός του κώδικας έχει μόνο 2^r κωδικές λέξεις και, όπως θα δούμε σύντομα, έχει ένα ιδιαίτερα απλό απαριθμητή βάρους. Εκ τούτου ο απαριθμητής βάρους του $Ham(r,2)$ εύκολα προσδιορίζεται. Ας δούμε αρχικά μια ειδική περίπτωση.

Παράδειγμα 1.9
Έστω C ένας δυαδικός $[7,4]-$Hamming. Τότε ο δυικός του κώδικας $C^\perp$ έχει γεννήτορα πίνακα:

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

Όταν υπολογίζουμε το $W_{c^\perp}(z)$ απ΄ ευθείας, κάνοντας λίστα τις κωδικές λέξεις, βρίσκουμε ότι καθεμιά από τις μη-μηδενικές κωδικές λέξεις έχει βάρος 4 (το επόμενο θεώρημα δείχνει ότι ευτό δεν είναι μεμονωμένο φαινόμενο, όσον αφορά τους κώδικες Hamming.) Έτσι,

$$W_{C^\perp}(z) = 1 + 7z^4,$$

οπότε ο απαριθμητής βάρους του C είναι από την εξίσωση (1.7),

$$\frac{1}{8}[(1+z)^7 + 7(1-z)^4(1+z)^3] = 1 + 7z^3 + 7z^4 + z^7.$$

Θεώρημα 1.10
Αν C ένας δυαδικός κώδικας Hamming $Ham(r,2)$. Τότε κάθε μη μηδενική κωδική λέξη του $C^\perp$ έχει βάρος 2^{r-1}.

Απόδειξη:
Έστω,

$$H = \begin{bmatrix} h_1 \\ h_2 \\ . \\ . \\ . \\ h_r \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & . & . & . & h_{1n} \\ h_{21} & h_{22} & . & . & . & h_{2n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ h_{r1} & h_{r2} & . & . & . & h_{rn} \end{bmatrix}.$$

να είναι ο πίνακας ελέγχου ισοτιμίας του C όπου οι γραμμές του H δηλώνονται με $h_1, h_2, ..., h_r$.Τότε μια μη-μηδενική κωδική λέξη c του $C^\perp$ είναι ένα διάνυσμα με τύπο $c = \sum_{i=1}^r \lambda_i h_i$ για κάποιους αριθμούς $\lambda_1, \lambda_2, ..., \lambda_r$ όχι όλοι μηδέν. Θα βρούμε το βάρος του C υπολογίζοντας τον αριθμό $n_0(c)$ των μηδενικών συνιστωσών του c και μετά αφαιρούμε το $n_0(c)$ από το μήκος n. Τώρα το c θα έχει ένα μηδενικό στην j-οστή θέση αν και μόνο αν $\sum_{i=1}^r \lambda_i h_{ij} = 0$ το οποίο είναι αν και μόνο αν $\sum_{i=1}^r \lambda_i x_i = 0$, όπου $(x_1 x_2 ... x_r)^\top$ είναι η j-οστή στήλη του H. Αφού ο C είναι ένας Hamming κώδικας, οι στήλες του H είναι τα μη μηδενικά διανύσματα του $V(r,2)$ και έτσι το $n_0(c)$ είναι ίσο με τον αριθμό των μη-μηδενικών διανυσμάτων του συνόλου:

$$X = \{(x_1 x_2 ... x_r) \in V(r,2) | \sum_{i=1}^r \lambda_i x_i = 0\},$$

το οποίο είναι $n_0(c) = |X| - 1$.
Είναι εύκολο να δούμε ότι το X είναι ένας υπόχωρος του $V(r,2)$, $(r-1)$ διασταση (για παράδειγμα δές το X σαν το δυικό κώδικα του $[r,1]-$κώδικα, ο οποίος έχει πινακα γεννήτορα $[\lambda_1 \lambda_2 ... \lambda_r]$,

έτσι ώστε $dim(X) = r - 1$). Έτσι,

$$|X| = 2^{r-1} \text{ και τότε } n_0(c) = 2^{r-1} - 1.$$

(Σημειώνουμε ότι το $n_0(c)$ είναι ανεξάρτητο της επιλογής των μη-μηδενικών λέξεων c του $C^{\perp}$). Έτσι,

$$\begin{aligned} w(c) &= n - n_0(c) = 2^r - 1 - (2^{r-1} - 1) \\ &= 2^{r-1}. \square \end{aligned}$$

Πόρισμα 1.11
Ο απαριθμητής βάρους του δυαδικού κώδικα Hamming $Ham(r, 2)$. μήκους $n = 2^r - 1$, είναι:

$$\frac{1}{2^r}[(1+z)^n + n(1-z^2)^{(n-1)/2}(1-z)].$$

Απόδειξη:
Αυτό προκύπτει άμεσα από την ταυτότητα του MacWilliams. Ξέρουμε ότι όλες οι μη-μηδενικές κωδικές λέξεις του δυικού κώδικα $C^{\perp}$ του Hamming $Ham(r, 2)$ έχουν βάρος 2^{r-1}, (Θεώρημα 1.10) τοτε ο απαριθμητής βάρους του είναι

$$W_{C^{\perp}}(z) = 1 + (2^r - 1)z^{2^{r-1}} = 1 + nz^{2^{r-1}}$$

Χρησιμοποιούμε την ταυτότητα του MacWilliams για να βρούμε τον απαριθμητή βάρους του C, ο οποίος είναι:

$$\begin{aligned} W_C &= \frac{1}{2^r}(1+z)^n W_{C\perp}\Big(\frac{1-z}{1+z}\Big) \\ &= \frac{1}{2^r}(1+z)^n[1 + n\Big(\frac{1-z}{1+z}\Big)^{2^{r-1}}] \\ &= \frac{1}{2^r}(1+z)^n[1 + n\Big(\frac{1-z}{1+z}\Big)^{2^{(n+1)/2}}] \\ &= \frac{1}{2^r}[(1+z)^n + n(1-z^2)^{(n-1)/2}(1-z)]. \end{aligned}$$

2 Πιθανότητα των μη ανιχνεύσιμων λαθών

Θέλουμε να βρούμε το $P_{undetec}(C)$ για ένα δυαδικό $[n, k]-$κώδικα C.
Θεώρημα 2.1
Ας είναι C ένας δυαδικός $[n, k]-$κώδικας και έστω ότι με A_i δηλώνουμε το πλήθος των κωδικών λέξεων του C με βάρος i .Τότε, εάν ο C χρησιμοποιείται για ανίχνευση λαθών, η πιθανότητα να λαμβάνεται ένα λανθασμένο μήνυμα χωρίς να ανιχνευτεί είναι,

$$P_{undetec}(C) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}.$$

Σημείωση:
Κάθε σύμβολο που λαμβάνεται έχει την ίδια πιθανότητα λάθους p.
Εάν μια δυαδική κωδική λέξη μήκους n εκπέμπεται η πιθανότητα να μην επέλθει κανένα λάθος είναι $(1-p)^n$, ενώ η πιθανότητα να έχει λάθος ακριβώς σε ι συγκεκριμένες θέσεις είναι $p^i(1-p)^{n-i}$.

Τότε θα είναι:

$$\begin{aligned} P_{undetec}(C) &= \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} \\ &= (1-p)^n \sum_{i=1}^{n} A_i (\frac{p}{1-p})^i. \end{aligned}$$

Εφόσον,

$$W_C(\frac{p}{1-p}) = \sum_{i=0}^{n} A_i (\frac{p}{1-p})^i.$$

και επειδή $A_0 = 1$, έχουμε:

$$P_{undetec}(C) = (1-p)^n [W_C(\frac{p}{1-p}) - 1] \quad (2.2)$$

Εάν ξέρουμε το $W_C(z)$, τότε μπορούμε να βρούμε το $P_{undetec}(C)$ από την εξίσωση (2.2). Εάν ξέρουμε μόνο το $W_{C^\perp}(z)$ για να αρχίσουμε, τότε χρησιμοποιούμε την ταυτότητα του MacWilliams (1.7) για να υπολογίσουμε το $W_C(z)$, και μετά χρησιμοποιήσουμε την εξίσωση (2.2). Εναλλακτικά, μπορουμε να χρησιμοποιήσουμε τον τύπο:

$$P_{undetec}(C) = \frac{1}{2^{n-k}} W_{C^\perp}(1-2p) - (1-p)^n.$$

που δίνει το $P_{undetec}(C)$ απευθείας συναρτήσει του $W_{C^\perp}(z)$ αποφεύγοντας τους ενδιάμεσους υπολογισμούς του $W_C(z)$.

Παραπομπές

1) MacWilliams, F.J.(1963). A theorem on the distribution of weights in a systematic code. *Bell Syst. Tech.* J . **42**, 79-94. [13]

2) Sloane, N . J . A .(1977).*The theory of error-correcting codes.* North-Holland, Amsterdam. [Pref., 2, 8, 9, 11-15, 16]